令和4年度
中小企業サイバーセキュリティ対策継続支援事業

令和4年
サイバーセキュリティ
人材育成
社内体制整備支援

INDEX　目次

セミナー
～第1回～　セミナー開催日：令和4年7月26日

INDEX　目次

セミナー
～第2回～　セミナー開催日：令和4年8月9日

INDEX　目次

セミナー
～第3回～　セミナー開催日：令和4年8月23日

INDEX　目次

セミナー
～第4回～　セミナー開催日：令和4年9月13日

INDEX　目次

セミナー
～第5回～　セミナー開催日：令和4年10月11日

INDEX　目次

セミナー
～第6回～　セミナー開催日：令和4年10月25日

INDEX　目次

セミナー
～第7回～　セミナー開催日：令和4年11月15日

INDEX　目次

セミナー
～第8回～　セミナー開催日：令和4年12月6日

INDEX　目次

セミナー
～第9回～　セミナー開催日：令和4年12月20日

INDEX　目次

セミナー
～第10回～　セミナー開催日：令和5年1月24日

令和4年度

中小企業サイバーセキュリティ対策継続支援事業

第1回

セミナー開催日：令和4年7月26日

私が
セキュリティ担当
ですか？

『わが社もセキュリティを強化する』

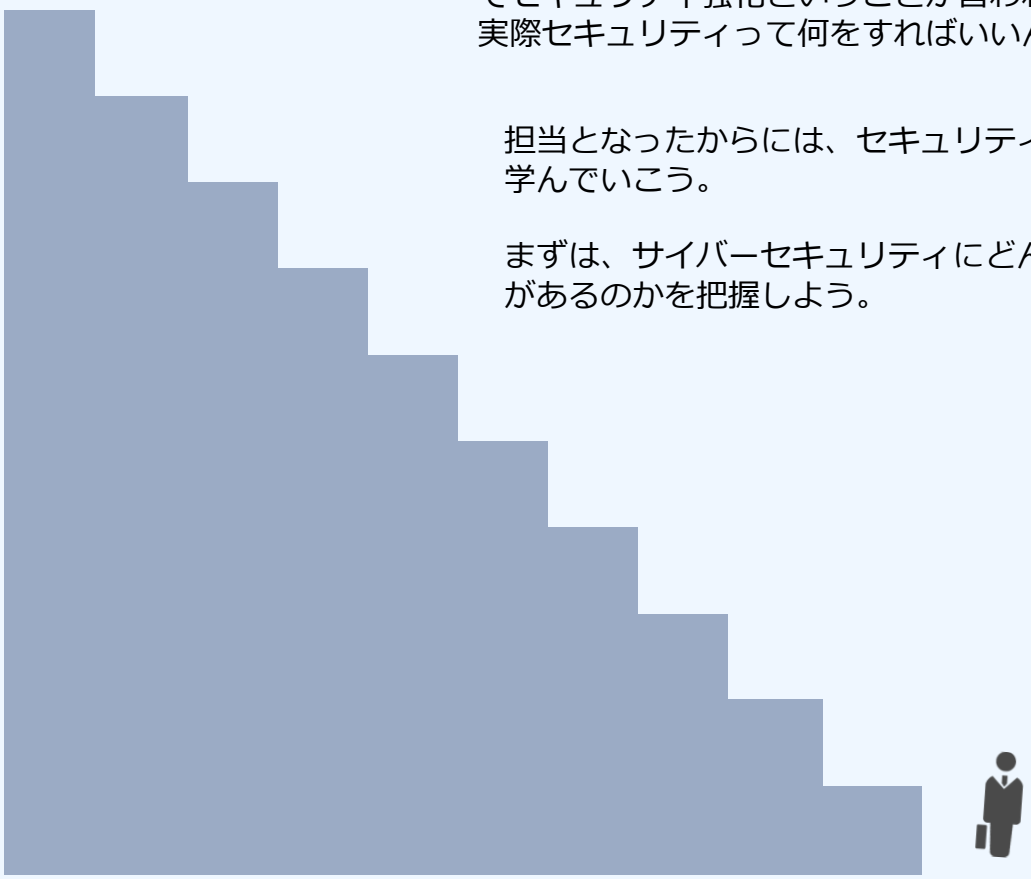
「セキュリティの担当を任せた」と言われたけれども・・・具体的に一体何をすればいいのだろう？今までも個人情報保護や書類の紛失など自分でも気を付けてきたけれども。さらにセキュリティ強化といっても、実際に何をするのがよいのやら？

あれもセキュリティの仕事？これもセキュリティの仕事？どこまでやればセキュリティをやっていると言えるのか？最近は・・・「えっ！それもセキュリティの仕事ですか」ということも増えてきているような。本業もあるのに。

みんなが言っているからやらないといけない雰囲気になっていて、考えたことなかったけれど、そもそも何でセキュリティ強化ということが言われるのだろう？実際セキュリティって何をすればいいんだ？

担当となったからには、セキュリティをしっかりと学んでいこう。

まずは、サイバーセキュリティにどんな仕事や担当があるのかを把握しよう。



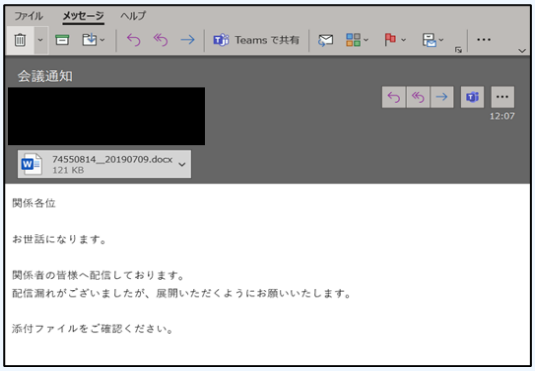
Day1
1.セキュリティが必要な理由

セキュリティの最新状況①
～Emotet～

Emotet(エモテット)とは、サイバー攻撃で使われるウィルスの名称です。情報搾取などを目的として、他のウィルスへの感染などを引き起こします。 Emotetは不正なメール(攻撃メール)に添付されるなどして、感染の拡大が行われます。

Point① こんなメールに要注意

Emotetはメールの添付やダウンロード指示によりMicrosoftのOfficeファイルを対象者に送付します。ファイルには悪意のあるマクロが埋め込まれており、これが実行されると感染します。
2022年4月には、メールに添付されたショートカットファイルを開くだけで感染させる手口も確認されています。



Point② 感染するとこんな事態に

Emotetに感染すると、多様な被害に!

感染事例
1. 社内の他の端末に感染する
2. Emotet感染を目的としたメールを社外へ送信する
3. 重要な情報が盗み取られる
4. ランサムウェアなど他ウィルスへ感染する

感染は1台とは限りません。もし1台でも確認されたら、他の端末が問題ないか確認をしましょう。また、お客様へ予期せぬメール送信がないかの確認も必要です。

Point③ もし感染してしまったら

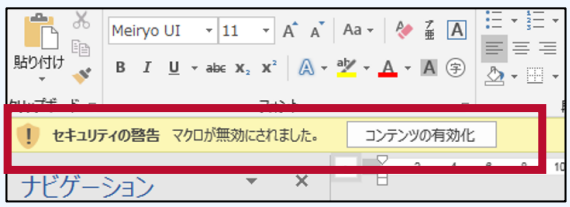
感染の可能性がある場合、次の対処を!

対応事例
1. 端末の隔離
2. 端末で利用していたパスワードの変更
3. 他端末の調査

もし感染の可能性が疑われる場合には、端末をネットワークから切り離しましょう。また、メールアカウントのパスワードはすぐに変更しましょう。

Point④ 被害にあわないために

Emotetはメールの仕組みやマクロを使って感染を拡大します。対策として、以下を実施しましょう。



- 組織内への注意喚起の実施
- Word マクロの自動実行の無効化
- メールセキュリティ製品の導入によるマルウェア付きメールの検知
- メールの監査ログの有効化
- OS に定期的にパッチを適用 (SMBの脆弱性をついた感染拡大に対する対策)
- 定期的なオフラインバックアップの取得（標的型ランサムウェア攻撃に対する対策）

出典：JPCERT/CC
マルウェア Emotet の感染に関する注意喚起
https://www.jpcert.or.jp/at/2019/at190044.html

Day1
1.セキュリティが必要な理由

セキュリティの最新状況②
～サプライチェーンの影響～

サプライチェーン攻撃では、標的とする企業を直接狙うのではなく、関連企業や取引先企業といったセキュリティ対策が不十分であろう企業を狙います。関連企業や取引先企業を経由して、標的となる企業へ侵入やサイバー攻撃をしかけます。

Point① お客様からの信頼のために

サプライチェーン攻撃は、お客様にも被害が発生する可能性があります。自社のセキュリティを強化することは、お客様の安全・安心を守ることにもつながります。

お客様から求められる代表的なこと
セキュリティルールの策定・実行・見直し
従業員教育
監査等への協力

セキュリティルールの策定や従業員教育をして、セキュリティ事故を起こさないように努める必要があります。セキュリティ対策に不備があった場合、責任を問われる可能性があります。

Point② サプライチェーンの被害にあわないために

自分の会社も委託先の影響により、サプライチェーン攻撃の被害にあう可能性があります。関係者が協力しあい、セキュリティ強化を目指していくことが大切です。

関係者との連携
委託先との契約の明確化
委託先の監督・改善要望

自社の委託先がセキュリティ事故を起こさないという保証はどこにもありません。委託先との契約を明確化し、セキュリティ事故を起こさないように監督しましょう。

One point

2022年2月、自動車メーカーが『国内仕入先におけるシステム障害の影響を受け、3/1（火）（1直・2直ともに）国内全14工場28ラインの稼働を停止することを決定いたしました。お客様及び関連仕入先の方々には、様々なご不便をお掛けすることをお詫び申し上げます。』と発表しました。国内仕入先企業も3月7日には『システム障害事案発生のお詫び』という発表をしています。

国内仕入先企業は自動車メーカーの部品製造を担い、サプライチェーンを担う1社でした。この1社がサイバー攻撃を受け、業務が停止したことにより、自動車メーカーの工場が停止するという事態になりました。まさに、サプライチェーン攻撃です。

国内仕入先企業は攻撃発覚後ネットワークを遮断し対応にあたっています。これにより、業務も一時中断せざるを得ない状態となり、自動車メーカーへの部品供給の停止、工場の停止につながりました。セキュリティ対策としては、対策本部の立ち上げや侵害の調査を、セキュリティ専門家(外部含む)と一緒に対応していただろうことがうかがえます。

自動車業界にかかわらず、どの企業も1社ですべて製品やサービスが完結するということは少なくなっています。

セキュリティを強化することは、お客様や関係者を守るということにもつながっています。

Day1
1.セキュリティが必要な理由

セキュリティの最新状況③
～最近の攻撃トレンド～

Emotetやサプライチェーン攻撃に限らず、サイバー攻撃の危険性は高まっています。サイバー攻撃の流行を適切に押さえ、攻撃の対策を考えていくこともセキュリティの大切な仕事です。

Point①
ランサムウェアの脅威

ランサムウェアに感染するとデータの暗号化が行われます。そして、その復旧(暗号化解除)と引き換えに金銭を要求します。最近は、データの暗号化と合わせて情報の搾取を行い、公開するという脅しと合わせた2重の攻撃も出回っています。
対策として、バックアップ取得・復旧手順の確認をしておきましょう。

Point②
標的型攻撃

標的型攻撃とは、特定の組織や個人を狙う攻撃です。標的の情報を徹底的に調べることで、標的に最適な攻撃を行ってきます。機密情報の搾取や金銭の振込など、多くの被害が出ています。
対策として、業務ルール・セキュリティルールの整備、従業員教育などをしましょう。

Point③
フィッシング攻撃

フィッシング攻撃とは、実在する組織を騙って、ユーザー情報やパスワードなどの個人情報を搾取する攻撃です。偽のWebサーバなどにアクセスさせ、そこに情報を打ち込むと情報漏洩につながります。
対策として、信頼できない発行元のリンクはアクセスしない・本来のWebサイトのドメインであるか確認することが有効です。

One point

フィッシングサイトの見分け方として、一昔前には『https』であるかどうかを確認するというものがありました。httpsから始まるURLは通信内容が暗号化されます。http://から始まるURLの通信は、内容を暗号化せずに平文で送信するため、通信内容を盗聴する悪意のある第三者がいた場合、通信内容が流出してしまいます。これではクレジットカード番号など重要情報が漏えいすることになります。httpsの通信が増え、フィッシングサイトもhttps化していく流れとなりました。そのため、『https』であるから安心ということはありません。フィッシング対策の心得を理解し、インターネットを楽しく・有効に使いましょう。

フィッシング対策３つの心得

STOP. 立ち止まって理解する
THINK. 何が起こるか考える
CONNECT. 安心してインターネットを楽しむ

出典：フィッシング対策協議会
利用者向けフィッシング詐欺対策 ガイドライン(2022年度版)
https://www.antiphishing.jp/

セキュリティの最新状況④
～セキュリティの被害～

セキュリティ事故が万一起こってしまったら。あまり考えたくないことかもしれません。しかしながら、セキュリティ事故が起こってしまったことを正しく想定しておくことは非常に重要です。

Point① 金銭的損害

セキュリティ事故発生時には多くの費用が掛かります。損害賠償などはイメージしやすいかもしれませんが、他にも費用が発生してくるものは多いです。

Point② 無形損害

セキュリティ事故の発生による影響は金銭的な被害だけには及びません。お金で換算できない被害も発生します。

セキュリティ事故発生時の金銭的損害

事故対応損害：セキュリティ事故対応にかかる損害
賠償損害：損害賠償による損害
利益損害：事業中断による利益損失
金銭損害：サイバー攻撃による直接的な金銭損害
行政損害：法令違反による課徴金

セキュリティ事故が発生すると、業務停止により、予定した売上が立たないといった影響を受ける可能性があります。

セキュリティ事故発生時の無形損害

風評被害
ブランドイメージ低下
株価下落

セキュリティ事故が起きたという事実は消えず、インターネット上に情報が残り続けます。

One point

セキュリティ事故が起こった場合にどの程度の金銭的な負担が生じるのか？結構お金がかかりそうというイメージはあるかもしれません。セキュリティ事故の一つに個人情報の漏洩というものがあります。個人情報一人当たりの金額を調査しています。

日本ネットワークセキュリティ協会のインシデント被害調査ワーキンググループでは、インシデント損害額調査レポートというものを発行しています。一人当たり平均想定損害賠償額では、 28,308円であり、この金額がセキュリティ事故における、個人情報の金額と考えることができます。

被害にあわれた方からすると、この金額が妥当であるか否かの判断は分かれるところではありますが、セキュリティ事故を担当する人は参考にできる値といえます。

では、皆さんの会社に個人情報は何件ありますか？正確に把握できていますか？

調査年	一人当たり平均想定損害賠償額
2016年	31,646円
2017年	23,601円
2018年	29,768円
3ヶ年平均	28,308円

出典：日本ネットワークセキュリティ協会(JNSA)
インシデント損害額調査レポート　2021年版
https://www.jnsa.org/result/incidentdamage/2021.html

Day1

1.セキュリティが必要な理由

セキュリティの最新状況⑤
～中小企業を取り巻くセキュリティ～

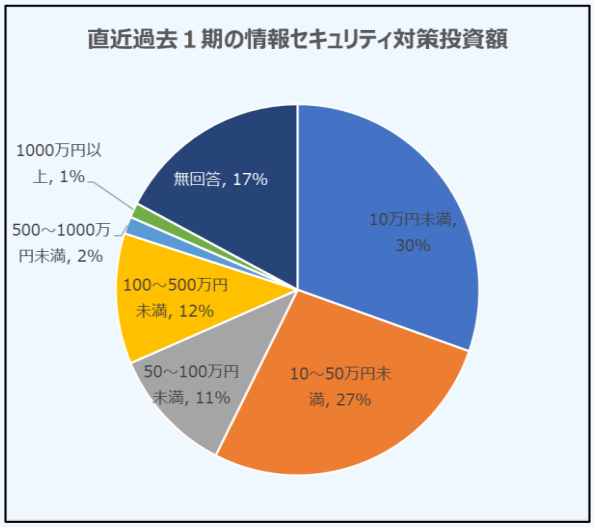
セキュリティは大企業だけやればいいというものではありません。また、企業だけがやればいいというものでもありません。セキュリティは全員が参加しみんなで実施していく必要があります。

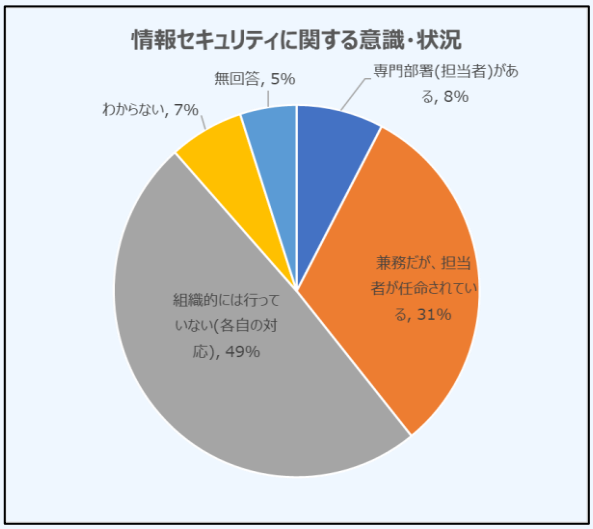
Point① セキュリティ投資

中小企業では、セキュリティ対策にどの程度投資しているのでしょうか？セキュリティ対策をないがしろにすると事故が発生した際に被害が大きくなる可能性があります。しっかりと準備をしていきましょう。

Point② セキュリティの意識

中小企業の半分は組織的なセキュリティ対策を行っていないという結果となっています。まずは担当者を任命し、セキュリティ意識を高めていきましょう。





出典：情報処理推進機構（IPA）
2021年度中小企業における 情報セキュリティ対策に関する実態調査 – 調査報告書 –
https://www.ipa.go.jp/security/fy2021/reports/sme/index.html

One point

セキュリティの必要性は最近特によく言われています。しかしながら、昔からセキュリティ事故は発生しており、危険性はありました。例えば、日本年金機構へのサイバー攻撃は2015年のことで、7年前(記載時2022年)のことです。そのため、中小企業としてはサイバーセキュリティの課題や危険性を数年来抱えているということも考えられます。

情報処理推進機構（IPA）が調査をした、『2021年度中小企業における 情報セキュリティ対策に関する実態調査 ― 調査報告書』※1では、前回調査との比較を行っています。
セキュリティ投資をしていない企業が減り、100万円未満の投資をしている企業が増えたり、セキュリティ教育をしている企業が増えたりと少しずつ中小企業でもセキュリティの意識が高まっていることがうかがえます。半面、組織体制では大きな変化がないという状況もあります。よりセキュリティを強化していくために、体制にも意識を向けた取り組みが求められているのかもしれません。

※1　情報処理推進機構（IPA）
2021年度中小企業における 情報セキュリティ対策に関する実態調査 – 調査報告書 –
https://www.ipa.go.jp/security/fy2021/reports/sme/index.html

ミニワーク
～振り返ってみよう～

ミニワークテーマ

自身が所属する組織で起こったセキュリティ事故・ヒヤリハットはどのようなものがありましたか？

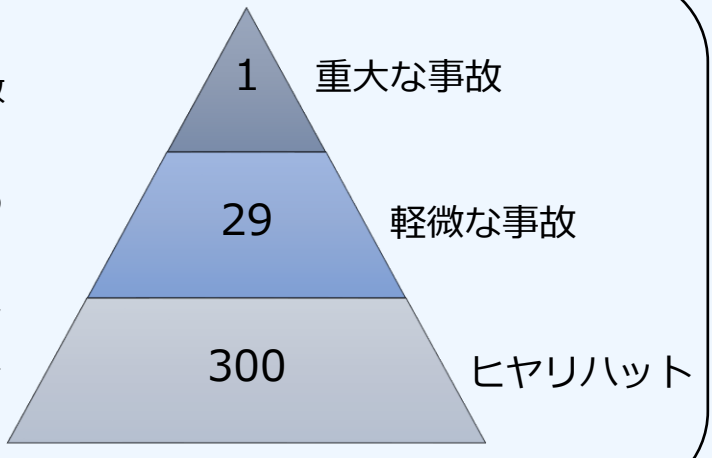
もし、過去にセキュリティ事故・ヒヤリハットがない場合どのような危険性がありそうですか？

セキュリティ事故

ヒヤリハット

ハインリッヒの法則は「1:29:300の法則」とも呼ばれます。30件の事故の下には、300件のヒヤリハットが存在します。また、30件の事故のうち1件は重大な事故になりえるというものです。

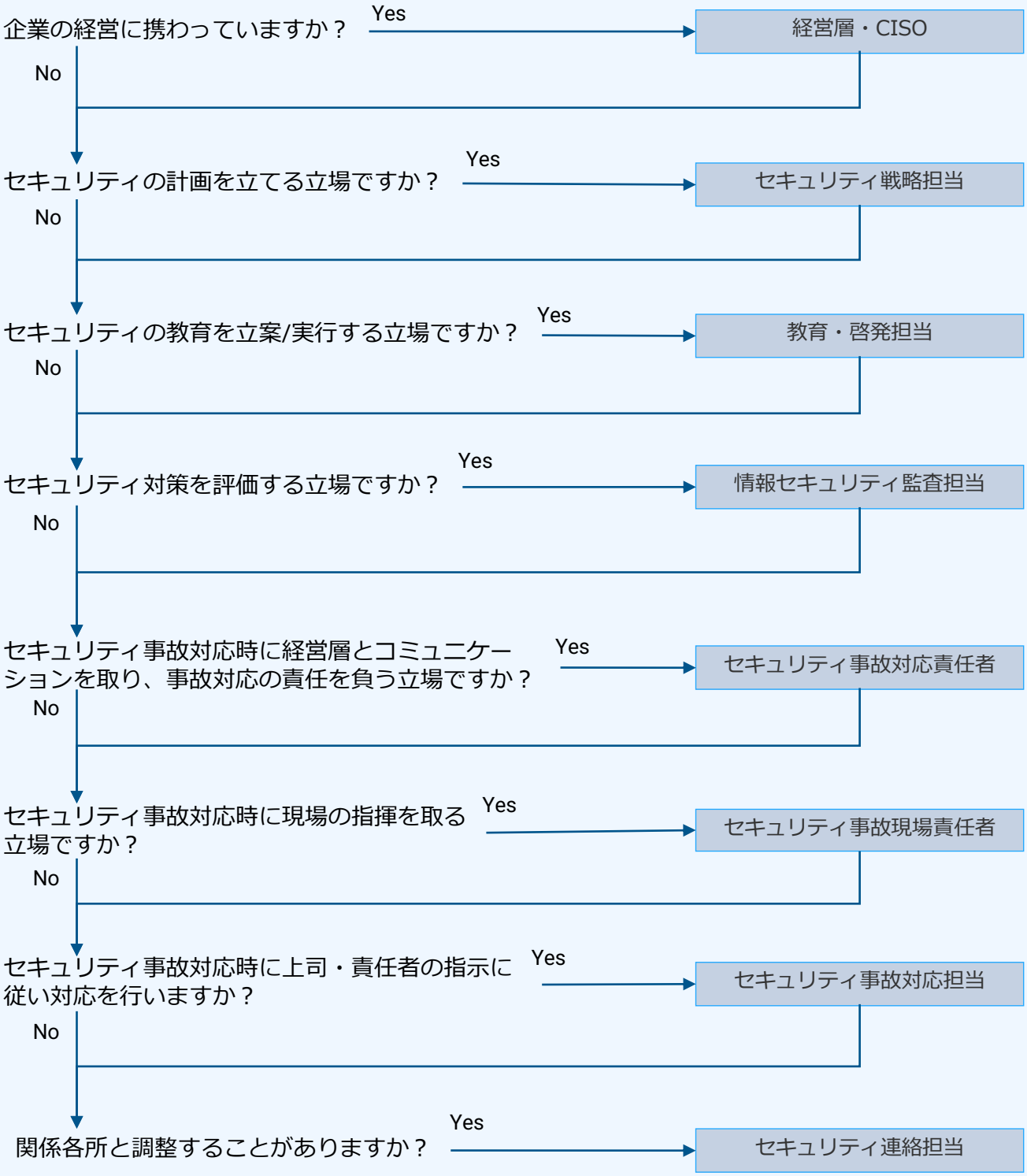
事故を防ぐためにはヒヤリハットを少なくしていくことが重要です。ヒヤリハットを少なくしていくことで、上位の軽微な事故や重大な事故を減らしていくことにつながります。



Day1

2.セキュリティの主な業務内容

あなたの担当は？
～該当はいくつある？～



Day1
2.セキュリティの主な業務内容

セキュリティの仕事
～セキュリティ体制の全体像～

平時の際のセキュリティ体制

主な外部活用
- 脆弱性診断担当 P31
- フォレンジック担当 P32
- 情報分析担当
- 捜査/調査担当
- 情報収集担当
- 法律担当

- 経営層・CISO P22
- セキュリティ戦略担当 P23
- セキュリティシステム担当 P27
- 教育・啓発担当 P24
- 情報セキュリティ監査担当 P25
- セキュリティ連絡担当 P28

●一般的な情報セキュリティ相談

情報処理推進機構(IPA) 情報セキュリティ安心相談窓口
https://www.ipa.go.jp/security/anshin/
TEL：03-5978-7509　FAX：03-5978-7518
mail：anshin@ipa.go.jp
受付時間：10:00～12:00
13:30～17:00(土日祝日・年末年始を除く)

中小企業サイバーセキュリティ相談窓口
【電話相談窓口】03-5320-4773
【相談フォーム】：https://www.shinsei.elg-front.jp/tokyo2/uketsuke/form.do?id=1461031266630
【窓口でのご相談】 東京都産業労働局商工部内 Tcyss事務局
(東京都新宿区西新宿2丁目8番1号都庁第一本庁舎20階北側)

●法律相談

日本司法支援センター法テラス
https://www.houterasu.or.jp/

有事の際のセキュリティ体制

主な外部活用
- フォレンジック担当
- 捜査/調査担当
- 法律担当 P32

- 経営層・CISO P22
- セキュリティ事故対応責任者 P26
- セキュリティ事故現場責任者 P29
- セキュリティ事故対応担当 P30
- セキュリティ連絡担当 P28

●犯罪の可能性がある場合の相談窓口

サイバー犯罪相談窓口(警視庁)
https://www.keishicho.metro.tokyo.lg.jp/sodan/madoguchi/sogo.html
電話：03-5805-1731
受付時間：8:30～17:15（平日のみ）

●被害の報告・連絡・相談窓口

コンピュータウイルス・不正アクセスに関する届出について(IPA)
https://www.ipa.go.jp/security/outline/todokede-j.html
フィッシング詐欺(フィッシング対策協議会)
https://www.antiphishing.jp/
迷惑メール(日本データ通信協会 迷惑メール相談センター)
https://www.dekyo.or.jp/soudan/
なりすましECサイト(なりすましECサイト対策協議会)
https://www.saferinternet.or.jp/e-commerce/narisumashi/
インシデント報告・届出(JPCERT/CC)
https://form.jpcert.or.jp/
インシデント報告・届出 (IPA J-CRAT 標的型サイバー攻撃特別相談窓口)
https://www.ipa.go.jp/security/tokubetsu/index.html
個人情報保護委員会
https://www.ppc.go.jp/personalinfo/legal/leakAction/

中小企業サイバーセキュリティ相談窓口
【電話相談窓口】03-5320-4773
【相談フォーム】：https://www.shinsei.elg-front.jp/tokyo2/uketsuke/form.do?id=1461031266630
【窓口でのご相談】 東京都産業労働局商工部内 Tcyss事務局
(東京都新宿区西新宿2丁目8番1号都庁第一本庁舎20階北側)

Day1

2.セキュリティの主な業務内容

担当①
～経営層・CISO～

セキュリティの最高責任者

情報セキュリティの責任者は経営層です。社内のセキュリティ体制を整え、積極的に推進していきます。社長やCISO※1が責任を放棄することはできません。

※1:Chief Information Security Officer

経営者はセキュリティのプロフェッショナルではありません。セキュリティを担う人材と連携した対応が求められます。

求められるミッション

- 社内の情報セキュリティを統括する。
- セキュリティの推進、体制の構築（リソースの手配、予算の確保）をする。
- ビジネスの視点でセキュリティ対策や事故発生時の影響を検討する。
- 組織の方針や規程について承認をする。または、承認者へ権限譲渡をする。

求められるスキルやノウハウ

- 経営に関するスキル

One point

日本には約386万社の企業があると言われています。単純な計算では、延べ386万人の経営者がいるということです。そして、386万社でセキュリティは必要です。

では、386万人のセキュリティ人材はいるのでしょうか？おそらく、いないでしょう。すなわち、会社のセキュリティを高めるためには、外から人材を登用するか、外部のサービス利用、自社社員の育成という方法を考えるしかありません。人材を登用しようと思ってもなかなか人材がいない、外部のサービス利用はお金がかかるとなってくると、自社社員の育成という方法が一番可能性があるのではないでしょうか？セキュリティを学び、経営者のサポートをしていきましょう。

こんな事例も

セキュリティを強化するということが社長からではなく、現場から起こる事例があります。ある会社では、日々お客様とやり取りをする中で、お客様からセキュリティを求められてきました。特に、従業員は、個人情報を取り扱ったり、モバイルパソコンを持ち運んだりとセキュリティリスクに近い立場にいるため、個人でもセキュリティ事故を起こさないように努力をしているケースがあります。

現場からセキュリティの重要性を訴えかける状態はセキュリティ強化を目指すうえでは非常に良い状態です。従業員のモチベーションが高まっているからです。実は、皆さんの会社でも従業員のセキュリティ意識は高まっており、会社が動き出すのを待っているかもしれません。

Day1
2.セキュリティの主な業務内容

担当②
～セキュリティ戦略担当～

自社のセキュリティ戦略を立案

情報セキュリティの計画を立てていきます。セキュリティ戦略担当は社内セキュリティの中心人物です。

計画がない取り組みはうまくいきません。行き当たりばったりになり、つながりが生まれないからです。個々の取り組みの計画を立て長期的な視点でセキュリティの成熟度を高めていきます。

求められるミッション

- 自社の事業計画に合わせたセキュリティ戦略を策定する。
- リスク分析や資産管理を通してセキュリティ対応策を考え、実行し、評価する。
- セキュリティ上の課題を発見し対処する。

求められるスキルやノウハウ

- リスクアセスメントスキル・ノウハウ
- セキュリティマネジメントのスキル・ノウハウ
- 資産管理のスキル・ノウハウ
- 計画の立て方のスキル・ノウハウ
- 経営・予算管理に関するスキル
- 経営層への説明スキル

One point

自社のセキュリティ戦略を立案する人材が中小企業では不足しています。東京都サイバーセキュリティ対策継続支援事業では、セキュリティ戦略担当が担うミッションを主に学んでいきます。

各社の状況が違うため、求められるセキュリティ戦略も各社違ってきます。「あの会社がやっているから」では失敗するケースもあります。しっかりと自社のことを分析し、セキュリティ対策の計画・実行を進めていく必要があります。

特にセキュリティ戦略担当は経営層やCISOともコミュニケーションを取っていく必要があります。経営に関する知識も養っていきましょう。

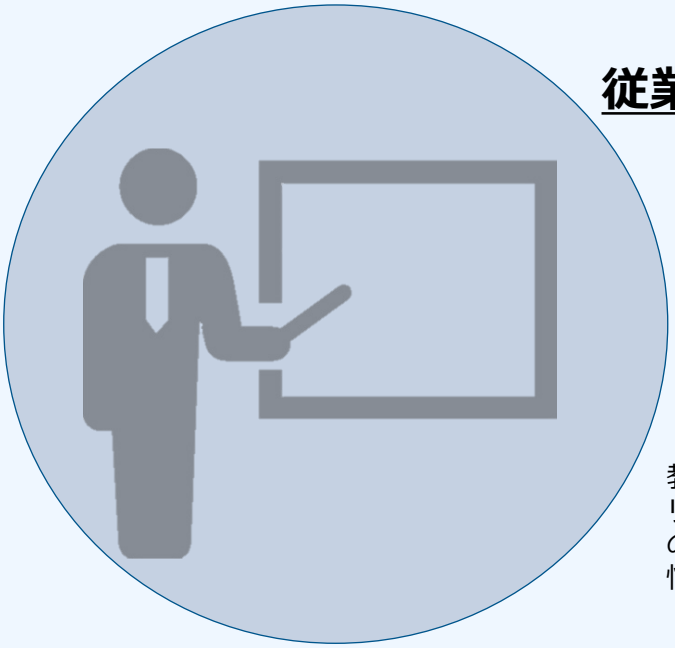
こんな事例も

ある会社では、社長の号令のもとセキュリティの取り組みを開始しました。特に各担当は設けず、社長自らリーダーシップを発揮しました。

しかし、社長もセキュリティのプロではありません。対策や取り組みに計画性がなく、朝令暮改ということもありました。従業員も何が最新のルールなのか把握することができませんでした。一連の取り組みは従業員の業務負荷を高め、モチベーションを下げる結果となってしまいました。

セキュリティ対策は一人ではできません。従業員の協力も必要です。戦略を立てるということは業務とセキュリティのバランスを取っていくことにもつながります。

担当③
～教育・啓発担当～



従業員のセキュリティの指導者

セキュリティの教育や啓発活動を主に担当します。セキュリティの情報を伝え従業員を導きます。

教育はすぐにでも取り入れられるセキュリティ対策の取り組みの一つです。自社のルールの説明や最近のセキュリティ事情など、従業員に伝えていきましょう。

求められるミッション
- 教育計画や目標・スケジュールを策定する。
- 研修テキスト・教材・テストの選定を行う。
- 講師として従業員への教育を行う。

求められるスキルやノウハウ
- 講師としてのコミュニケーションスキル・ノウハウ
- 指導方法や評価のスキル・ノウハウ
- 情報収集スキル

One point

●こんなにあるセキュリティ対策の教材

映像で知る情報セキュリティ(IPA)
https://www.ipa.go.jp/security/keihatsu/videos/

「小さな中小企業とNPO向け情報セキュリティハンドブック 」(NISC)
https://security-portal.nisc.go.jp/guidance/blue_handbook.html

インターネットの安全・安心ハンドブック(NISC)
https://security-portal.nisc.go.jp/guidance/handbook.html

中小企業向けサイバーセキュリティ対策の極意(東京都)
https://www.cybersecurity.metro.tokyo.lg.jp/security/guidebook/#page1

国民のためのサイバーセキュリティサイト(総務省)
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/index.html

Day1
2.セキュリティの主な業務内容

担当④
～情報セキュリティ監査担当～

セキュリティの取り組みを確認

情報セキュリティ監査担当はセキュリティ機能が正しく働いているか、取り組みがしっかりとできているかを評価します。

情報セキュリティの取り組みは計画を立てて実行するだけでは上手くいっているかわかりません。また、正しいリスク対策となっていることの確認も必要です。

求められるミッション

- 社内の情報セキュリティマネジメントや各種対策が効果的に実行できているかを監査する。
- できていない場合には指摘をし、是正措置のヒントを与える。

求められるスキルやノウハウ

- リスクアセスメントスキル・ノウハウ
- 資産管理のスキル・ノウハウ
- セキュリティマネジメントのスキル・ノウハウ
- コミュニケーションスキル
- 各種対策に関するスキル・ノウハウ

One point

セキュリティの監査には主に2つの方法があります。適切に使い分けることで効果的な監査にしていきましょう。

1、第3者が監査する方法
ISMS認証やPマークなどは外部の担当者が監査する代表例です。主に認証や第3者評価が必要な場合に実施します。第3者が実施することにより、公平・公正な監査となります。

2、社内担当者が監査する方法
社内担当者が監査をする場合には、時間や費用の制限が少ないという利点があります。自社ができていない点を見つめなおし、今後の対策に活かしていくことができます。

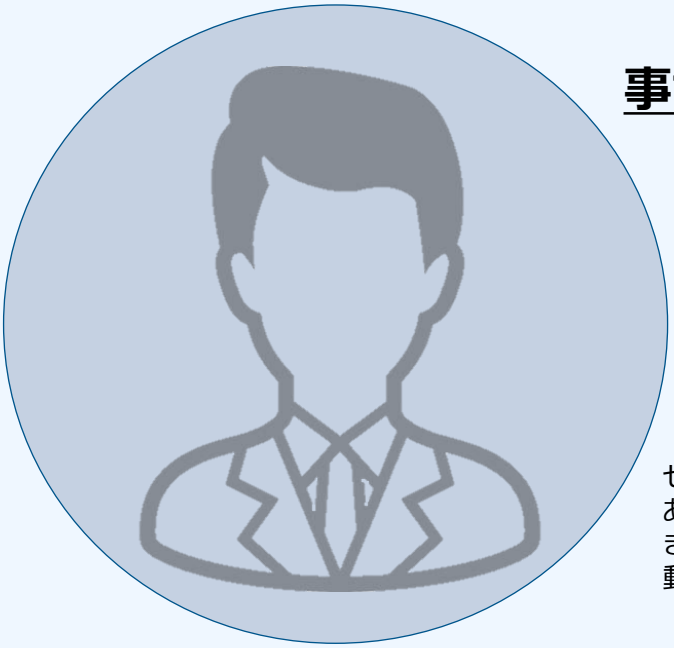
こんな事例も

セキュリティの監査を担当する人材がいないということはよくあります。ある会社ではこの危機を部署間監査という方法で乗り切りました。

同じ部署の人間が監査をすると、先入観や部内のつながりにより、正しく監査ができないという懸念があります。この会社では、事業においてあまり関わりがない部門の担当者が内部監査をしました。これにより、情報セキュリティ監査担当者は計画や監査評価に集中することができます。

そして、この監査にはもう一つ利点がありました。業務内容すら知らなかったそれぞれの部門がお互いの業務を把握するきっかけとなり、社内の連携がより活発化していきました。

担当⑤
～セキュリティ事故対応責任者～



事故発生時の対応責任者

セキュリティ事故対応責任者は、
セキュリティ事故が発生した際に
経営層と現場の間に入る人材です。

セキュリティ事故ゼロに越したことは
ありませんが、事故は必ずどこかで起
きます。企業の被害を抑えるための行
動が求められます。

求められるミッション

- セキュリティ事故発生時に全社の統括を行う。
- 優先順位を決め対応有無の判断を行う。
- CISOや経営層と連携をし、CISOや経営層の意思決定をサポートする。

求められるスキルやノウハウ

- リスクアセスメントスキル・ノウハウ
- 資産管理のスキル・ノウハウ
- セキュリティマネジメントのスキル・ノウハウ
- 経営層への説明スキル
- 経営・予算管理に関するスキル
- コミュニケーションスキル

One point

トリアージという言葉を聞いたことはありますか？治療の緊急度において、けが人の振り分けを行う際に使われる言葉というのが一般的です。

セキュリティでは、セキュリティ事故が発生した際にどの対応から行っていくか、数多くある危険性の中から何を優先して対処していくかという意味で使われます。

特にトリアージは会社の大切なものや判断基準などに影響されるため、外部の会社(セキュリティ事故をフォローするベンダなど)では最終判断ができない場合があります。

自分たちが何を守るのかを平時の際から認識し、トリアージの判断に時間をかけないようにしていきましょう。

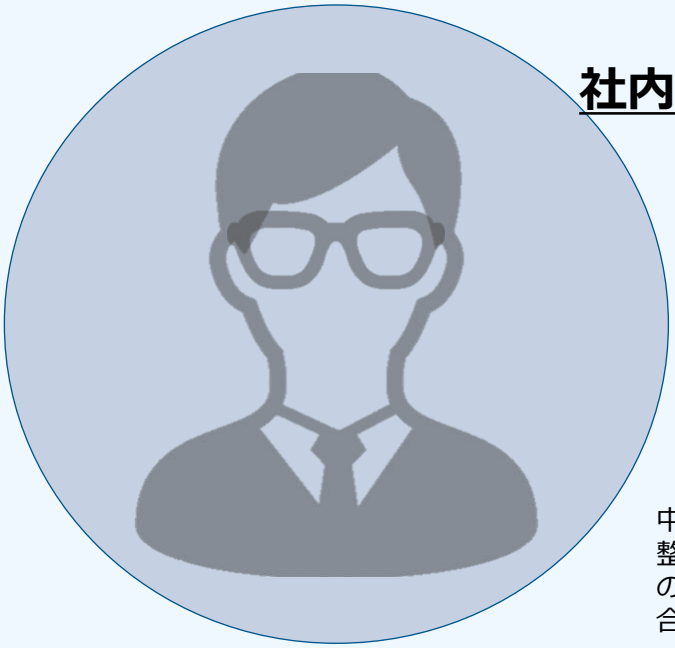
こんな事例も

セキュリティ事故の対応では、自社のシステム停止などの判断が求められるケースがあります。ある会社では、システム停止を訴えるセキュリティ事故対応責任者とシステムの稼働を継続したい経営者という対立が事故対応中に発生しました。

経営層のセキュリティ理解の問題もあれば、セキュリティ事故対応責任者の説明に問題があるケースもあります。セキュリティ事故発生時に責任者を任命したことで、日ごろのコミュニケーションが不足し、認識を合わせることが難しかったことが要因だと考えられます。

日頃から体制を整えておき、コミュニケーションを取っていくことが重要です。

担当⑥
～セキュリティシステム担当～



社内インフラ・IT環境を守る

セキュリティシステム担当はセキュリティ機器やIT環境が正しく働いているか、社内で必要な機器はどのようなものかを検討します。有事の際にはセキュリティ事故対応担当との連携や、事故対応担当そのものを担う場合もあります。

中小企業では、社内インフラ・IT環境の整備を担うシステム担当がセキュリティのシステムについても担当するという場合があります。

求められるミッション

- セキュリティ機器類の導入計画や設計を行う。
- 現在導入されている機器の有効性の評価を行う。
- システム周りの保守や監視を行う。

求められるスキルやノウハウ

- システム操作などの技術スキル
- セキュリティ機器のスキルやノウハウ
- リスクアセスメントスキル・ノウハウ
- 各種ログの調査分析スキル
- ガイドラインや規程の知識

One point

セキュリティの対策としてまず思いつくのは、セキュリティ機器の導入です。しかしながら、セキュリティ機器を導入したからといって、セキュリティ対策が万全になるわけではありません。そのためセキュリティ対策に終わりはなく、何かしらの検討をしていくことになります。その際には、新しい機器の導入なども検討されるかもしれません。

リスク分析の結果必要ならば適切なセキュリティ機器を導入すべきです。しかし、既存のセキュリティ機器でできることもあるのではないでしょうか？設定の見直しやチューニングをすることで既存の機器のセキュリティ対策を見直してみてはいかがでしょうか？

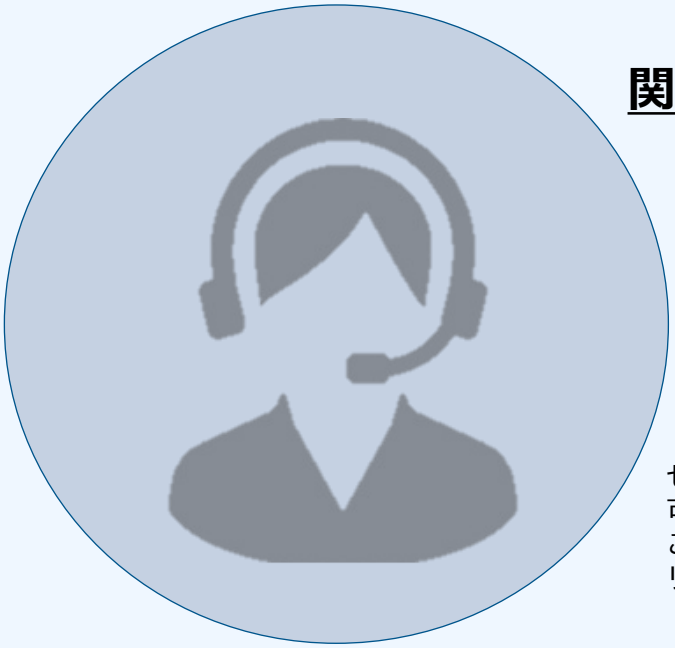
こんな事例も

「セキュリティ機器を入れたはいいものの、その後どうしたらいいのか？」という相談を受けるケースは多いです。設定ができない、細かいメンテナンス方法がわからない、使いこなせないなどよく聞きます。

この原因を探ると、導入時の検討の甘さに行きつきます。機器を導入する際に、導入後のことまで考慮ができないという点です。ベンダとの交渉や連携をしっかりとして、導入の目的、成し遂げたいことを考える必要があります。

導入計画、導入により何を目指すのか、運用体制や機器の操作方法は自社で対応可能か、このあたりを改めて考えることがセキュリティシステム担当には求められます。

担当⑦
～セキュリティ連絡担当～



関係各所と調整する渉外

セキュリティ連絡担当は社内外の関係者と調整を行います。また、自社内に情報を発信することも担います。

セキュリティの強化には『連携』が不可欠です。関係者との連携を強化することは情報収集に効果があり、セキュリティ強化につながります。

求められるミッション

- 外部組織（JPCERT/CC、NISC、警察、監督官庁）や社内（法務・広報・IT部門）との調整を行い、情報連携する。
- 脆弱性の発見や他社の事故事例などの情報を収集し社内へ共有する。

求められるスキルやノウハウ

- コミュニケーションスキル
- リスクアセスメントスキル・ノウハウ
- セキュリティマネジメントのスキル・ノウハウ
- 情報収集スキル・ノウハウ
- 情報発信スキル

One point

セキュリティ対策は各社のリスクや資産により最適解が変わってきます。では、なぜ連携が必要なのでしょうか？

連携のメリットとして、
1. 攻撃事例など対策に必要な情報を入手
2. 脆弱性情報の入手
3. 最新の対策事例の入手
などがあげられます。

今回の事業でも、グループワークを通して事例の発信や収集を体験していきます。今後もぜひ連携しセキュリティ強化を一緒にしていきましょう。

こんな事例も

ある会社の担当者は、自分が覚えたものを従業員に伝えていくことで、自身の学びとしました。他社の事故事例や取り組み事例を調査し、社内へ情報発信します。また、外部機関が発表する情報を収集し、これも社内へ発信しました。

自分が覚えたものを従業員に伝えていくことで自身の学びとし、連絡担当から教育担当も担うようになり、今ではセキュリティ戦略の立案まで担当しています。

はじめは緊張した外部への相談も、今では専門用語を理解し、より濃密なコミュニケーションが取れるようになりました。

情報発信をすることで従業員のセキュリティ意識も高まり、成熟度が上がっています。

担当⑧
～セキュリティ事故現場責任者～

事故現場を取りまとめる現場監督

セキュリティ事故が発生した際に現場を取り仕切ります。セキュリティ事故対応担当者を取りまとめ、被害を最小限にし、収束を目指します。

セキュリティ事故対応では、現場で判断をしないといけない場合があります。セキュリティ事故対応責任者と連携し作業にあたります。

求められるミッション

- セキュリティ事故発生時に現場で指揮をとり、対応に取り組む。
- セキュリティ事故対応責任者と連携しセキュリティ被害を最小限に食い止める。
- 対応の振り返りや事故事例の分析、訓練を行う。

求められるスキルやノウハウ

- システム操作などの技術スキル
- セキュリティ機器のスキルやノウハウ
- リスクアセスメントスキル・ノウハウ
- 各種ログの調査分析スキル
- 攻撃や脆弱性の知識

One point

現場責任者の仕事は、セキュリティ事故発生時に現場で指揮をとり、対応に取り組む、被害を最小限にするということです。ただ、現場監督の難しいところはそれだけではありません。

事故対応時には、長時間稼働になったり、徹夜での作業となる場合もあります。セキュリティ事故対応担当者の体調管理や稼働管理もセキュリティ事故現場責任者が意識する必要があります。また、セキュリティ事故現場責任者自身も休憩を取ったり、休んだりする必要があります。セキュリティ事故現場責任者が不在の場合に責任者となるべき人はだれなのか？を明確にすることも重要です。

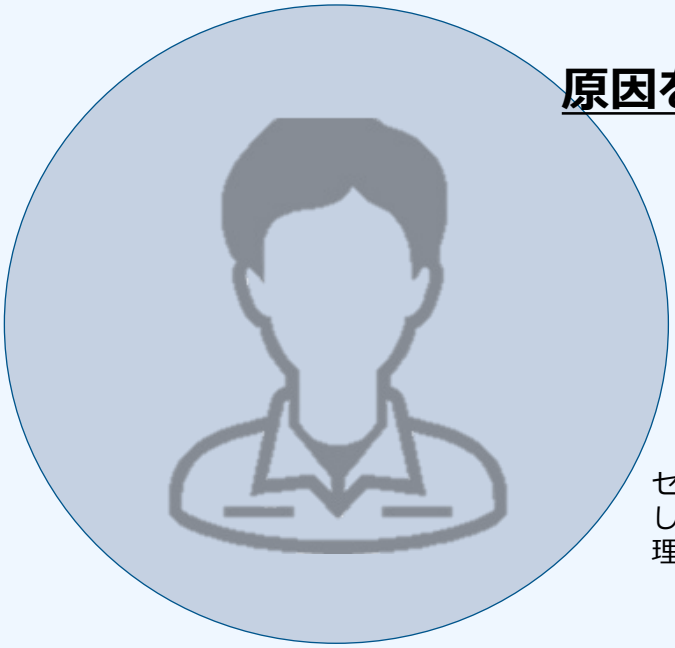
こんな事例も

ある会社では、セキュリティ事故の対応の一環として、バックアップからデータ復旧を試みました。いざ実施を試みても、そもそもバックアップから復旧すること自体が初めてと気づきました。復旧手順を保守会社に確認するなどしたため、予想より多くの時間がかかってしまったそうです。

現場責任者は、このような場合に備えて、事故事例の分析や事故対応訓練などを平時の際に行うことがよいとされています。消防訓練や避難訓練と同じ扱いをし、事故対応訓練も実施していきましょう。

Day1
2.セキュリティの主な業務内容

担当⑨
～セキュリティ事故対応担当～



原因を究明し、復旧を目指す

セキュリティ事故現場責任者と連携し、機器操作やログ調査をしながら、システムを復旧させ、原因究明を目指すのが、セキュリティ事故対応担当です。

セキュリティ事故対応では、機器の調査をし原因の究明を行います。自社システムを理解し、早期復旧を目指します。

求められるミッション
- 発生しているセキュリティ事故に対応する。
- 関連するシステムの防御や復旧の対応などを行う。
- 対応の振り返りや事故事例の分析、訓練を行う。

求められるスキルやノウハウ
- システム操作などの技術スキル
- セキュリティ機器のスキルやノウハウ
- 各種ログの調査分析スキル
- 攻撃や脆弱性の知識

One point

セキュリティ事故対応をスムーズに行うためには、各種資料が充実していることも重要です。これらの情報がないために、まずは社内の把握からという状態になりかねません。平時の際から情報を整理し、資料としてまとめておくことが重要です。

セキュリティ事故対応時に欲しい資料
- ネットワーク構成図
- IPアドレス管理表
- サーバの機能管理表
- 搭載OS情報
- インストールアプリの情報
- 関係者の連絡体制図

こんな事例も

セキュリティ事故対応担当は平時の際にはセキュリティシステム担当(または社内のIT全般)を兼務する事例が多いです。常日頃から自社のシステムを理解し対応していることは、セキュリティ事故対応においても優位に働きます。

中小企業の場合、セキュリティ事故対応責任者やセキュリティ事故現場責任者より技術に詳しいということが多いです。そのため、報告や相談が遅くなったり、原因究明に対応の比重が多くなってしまい、結果的にセキュリティ事故対応に時間がかかってしまったという話も聞きます。有事の際だからこそ、コミュニケーションをしっかりととり、社内で連携をしていくことが重要になります。

その他の担当①

～脆弱性診断士・情報分析担当・情報収集担当～

脆弱性診断士

有力な情報を与える強い味方

社内のシステムやWebアプリケーションに対して、脆弱な部分が無いかを調査します。また、見つかった脆弱な部分に対しての対処方法を提供します。

情報分析担当

情報収集担当が収集した情報をもとに、攻撃の特徴や傾向を分析します。今後のリスクアセスメントなどに役立つ有益な情報を提供します。

情報収集担当

脆弱性の発見情報や攻撃被害の情報など各種セキュリティの情報を収集します。収集した情報をSNSで発信する方々もおり、SNSから有益な情報を得ることができます。

One point

セキュリティの強化をしていくためには、いち早く正確な情報をつかむことが求められます。例えば、使用しているアプリケーションで重大な脆弱性が発見されたという情報を即座に得れば、危険性を最小限にするため対策を講じることができます。どこから情報を得るのがよいのか、その情報は正しいのかを考慮し、信用できる情報源を確保しましょう。

セキュリティ情報の収集源として役立つ国内の行政関連のWebサイト

JPCERT / CC
https://www.jpcert.or.jp/

NISC 内閣サイバーセキュリティセンター
https://www.nisc.go.jp/

IPA 情報処理推進機構
https://www.ipa.go.jp/

JNSA　日本ネットワークセキュリティ協会
https://www.jnsa.org/

他にも、ネットニュースやSNSなど多くの情報源があります。ぜひお気に入りの情報源を見つけて、定期的に情報を集めるようにしていきましょう。

その他の担当②

～フォレンジック担当・捜査/調査担当・法律担当～

会社を守る強い味方

フォレンジック担当

ウィルス感染や実行履歴などの痕跡を見つけ出し、セキュリティ事故対応に有益な情報・証拠を提供します。

捜査/調査担当

内部犯罪の可能性やサイバー犯罪において警察と連携し操作や調査を行います。

法律担当

コンプライアンスや法的要求内容において、法令の解釈など法律の観点から助言を行います。

こんな事例も

中小企業においては、各担当を一人で担っていくというケースがほとんどです。では、セキュリティの各種担当を担っている方々はどのような成長を遂げてきたのでしょうか？

担当者の成長モデル①

セキュリティ戦略担当 → セキュリティ連絡担当 → 教育・啓発担当 →セキュリティ戦略担当

もともとセキュリティ戦略担当としてセキュリティ業務を遂行していましたが、知識不足に悩まされていました。そこで、セキュリティに関する情報を集めながら勉強しました。集めた情報の社内への発信したことで連絡担当となり、教育・啓発につながりました。今では勉強の成果もあり、自信を持ってセキュリティの戦略を立てることができる、真のセキュリティ戦略担当者になりました。

担当者の成長モデル②

セキュリティシステム担当(セキュリティ事故対応担当) → セキュリティ戦略担当

IT機器の管理やログ管理などを行う業務をしていましたが、デジタル化推進の一環としてセキュリティも担当するようになりました。セキュリティシステムの設定を検討していくうちに、リスクアセスメントの理解も深まり、今ではセキュリティ戦略担当も担い、自社の機器導入などを進めています。

ミニワーク
～振り返ってみよう～

ミニワークテーマ

セキュリティの仕事は多くの担当がありました。では、自分に求められている担当とは実際にどのようなものでしょうか？

各担当のミッションやP11も参考にしながら考えてみましょう。

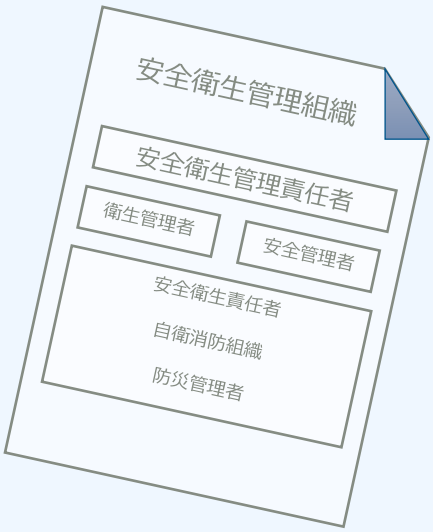
自身に求められている担当に〇をつけてみましょう。また、担当として、どのような仕事・ミッションがあるか書き出してみましょう。

- 経営層・CISO
- セキュリティ戦略担当
- 教育・啓発担当
- 情報セキュリティ監査担当
- セキュリティ事故責任者
- セキュリティ事故現場責任者
- セキュリティ事故対応担当
- セキュリティ連絡担当

社内連携の事例紹介①
～既存の仕組みを使った社内連携～

安全衛生管理組織を活用した社内連携

セキュリティの社内連携は、組織が大きくなればなるほど、全体に行き渡らせることが難しくなります。よくある例としては、各部門ごとに担当者や個人情報部門責任者などを任命し、セキュリティの連携を図っていきます。業務の担当や責任は明確になるものの、企業にセキュリティ強化を進めていく文化の土壌がないとなかなか連携がうまくいきません。また、任命された担当者の意識の差がそのまま部門の温度差として現れる場合もあります。特に、セキュリティの情報共有が少ないと連絡体制として機能しなくなる場合もあります。温度感の低い部門では、連絡不備が起こり、セキュリティ事故の可能性を高めてしまうことでしょう。



新規に立ち上げた連携体制では上手く機能しない可能性がある場合に、既存のもので使える仕組みがないかを検討することができます。例えば安全衛生管理の仕組みです。安全衛生管理は法律でも定められた設置義務があるので、どの企業でも最低限度の体制が整っています。セキュリティとは一線を画す体制ではありますが、「労働者の安全や衛生を管理し、安心して働くことができるような環境づくりを行う」組織として連絡体制の構築がすでに出来上がっています。

ある会社では、この安全衛生管理の仕組みを利用しセキュリティの情報共有を行いました。元々連絡や共有をすることが業務の一環だったため、セキュリティの情報共有においても、スムーズに共有することができました。また、定期的に安全衛生上の会議をしていたことで、ヒヤリハットのような情報も共有することができています。これにより、社内の担当者もどのような対策を打ち出していくのが効果的かの情報を収集することができました。セキュリティ体制の構築も新規で体制を整えるよりも早く整えることができたと言えます。

セキュリティの体制の構築というと難しく考えがちで、新しく整えていかないといけないと思われるかもしれません。しかしながら、セキュリティ体制の構築の目的は、セキュリティ情報を正しく素早く全従業員へ浸透させることです。すでにある仕組みを使い素早く体制が整うのであれば、これも一つの選択肢といえます。

Day1

3.担当者に求められること

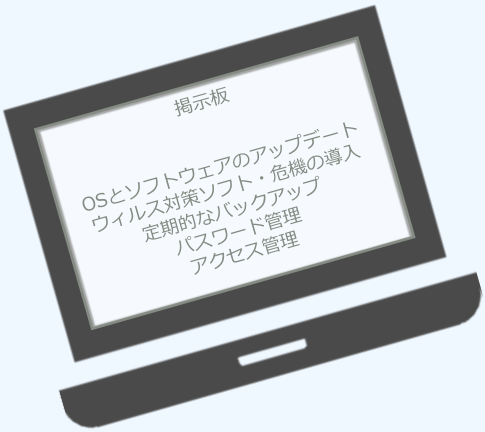
社内連携の事例紹介②

～デジタル活用による情報共有を進めた社内連携～

クラウドシステムを活用した社内連携

社内の連携にデジタルを活用するというのも一般的になっています。朝礼で全社員に伝えるというやり方から、メールやチャットツールで情報を発信しているという企業も多いのではないでしょうか？もちろん、朝礼で全社員に伝えることも立派な社内連携です。しかし、コロナ渦中での時差出勤や在宅勤務などの影響もあり、全社員が朝礼に集まりづらくなったという時代背景もあり、コミュニケーションの取り方を考える必要性がある時代となっています。

ある会社ではクラウドシステムを導入し、そこで社内連携を進めるようにしました。契約したクラウドサービスには掲示板機能があったので、掲示板に必要なセキュリティ情報を記載し全従業員に確認してもらうという方法です。有効なセキュリティ対策を実施しても従業員に届かなくては意味がありません。掲示板で表示すれば従業員が出社したタイミングで閲覧することができるため、聞き逃したという事態を避けることができます。



しかし、クラウド導入にあたり、心配な事案がありました。それは、元々デジタルに慣れた社員ばかりではなかったので、クラウド化自体にも抵抗があったことです。 SaaS型のクラウドサービスは色々な機能が盛り込まれているため便利な反面、覚えることが多くなるので使われないという危険性があります。そこで、まずは掲示板の機能を徹底的に使い、それに慣れてきたら次を使うというように浸透を進めていきました。クラウドサービスへの接続や掲示板の表示はパソコンを起動すると自動で掲示板が立ち上がるように設定し、情報の見落としを減らし、すぐに目に入るように工夫をしました。苦手な従業員も勝手に情報が表示されてくるため、特に大きな不満もなく掲示板の利用は浸透しました。不思議なもので、一度使って便利さを感じると他の機能に対しての抵抗が薄くなり、今ではファイル共有やチャットコミュニケーションも多くの従業員が使いこなしています。

社内連携の仕方は各社それぞれであり、有効な手段を検討していく必要があります。最近では、デジタルを活用した共有・連携が多いのではないでしょうか？デジタルに慣れている従業員には不都合はないかもしれませんが、全従業員へ情報を届けるためには情報を発信する側の工夫も必要です。自社にとっての最適な連携は何かを突き詰めていきましょう。

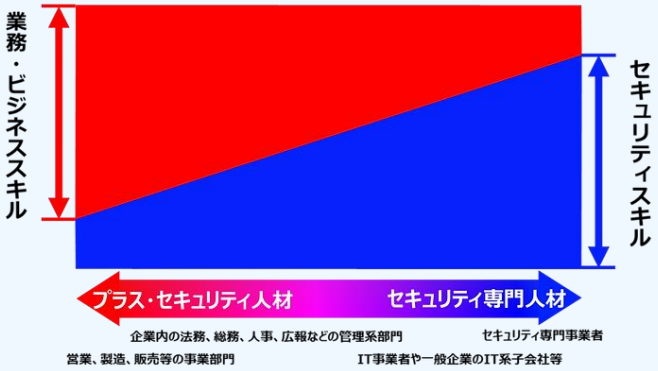
Day1

3.担当者に求められること

プラスセキュリティ人材

今求められるプラスセキュリティ人材

　自らの業務遂行にあたってセキュリティを意識し、必要かつ十分なセキュリティ対策を実現できる能力を身につけること、あるいは身につけている状態のことを、「プラスセキュリティ」と定義し「プラスセキュリティ」の状態にある人材、あるいは状態にあることが求められる業務に従事している人材をプラスセキュリティ人材といいます。



出典：一般財団法人日本サイバーセキュリティ人材キャリア支援協会
https://www.j-tag.or.jp/

自社の契約書雛形に盛り込むセキュリティ対策について検討する法務部担当者

新規事業戦略立案時にサイバー関連の脅威への対策を検討する事業部の企画担当者

代表的なプラスセキュリティ人材

工場の OT システムの保安対策の一環としてサイバー攻撃対策を検討する設備担当者

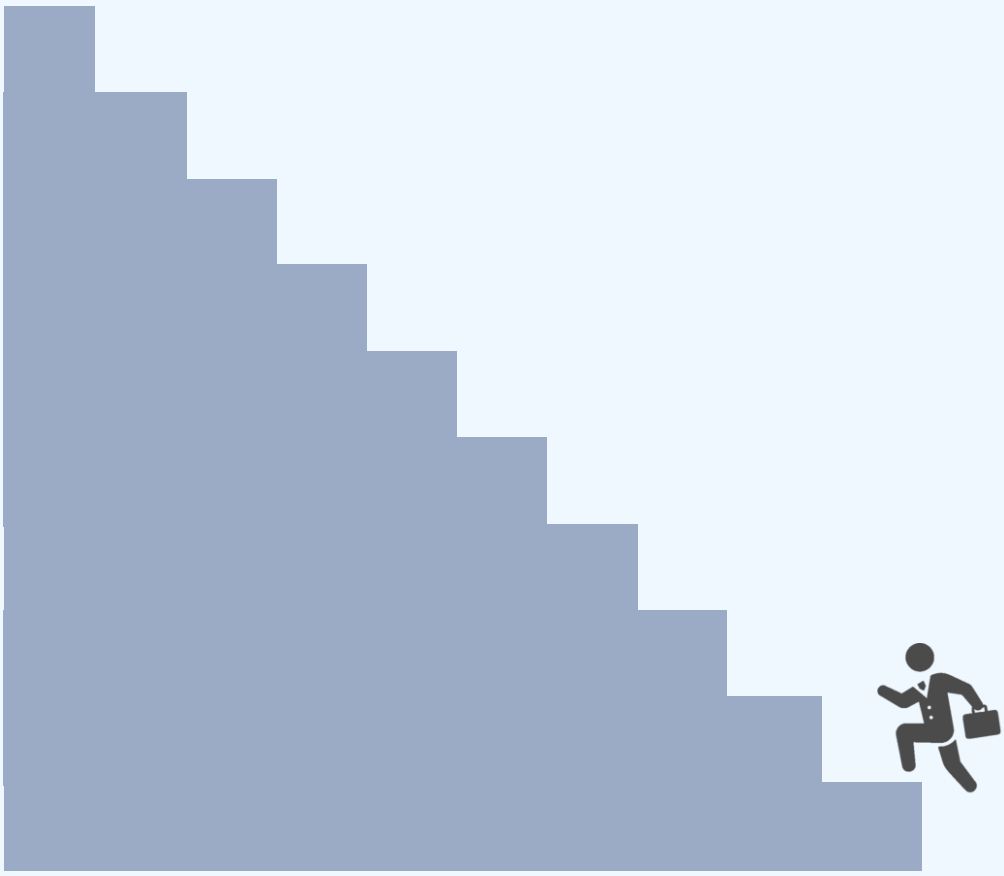
自社 CSIRT の PoC（Point of Contact）機能を兼務する広報担当者

　セキュリティ関連業務が増加する今日において、プラスセキュリティ人材との連携は、セキュリティの各担当者として必須のアクションです。しかしながら、プラスセキュリティという考え方自体が最近出てきたものです。社内にはまだいないという企業も多いです。
　セキュリティの各担当者として成長していくことはもちろんのこと、プラスセキュリティ人材候補を見つけ知識を共有しあい、一緒に成長していけるように、セキュリティ推進の協力者として連携していきましょう。

セキュリティの担当と一言で言ってもその中にはより細かい担当があり、多くの業務があるそうだ。うちの会社で求められている担当をはっきりと確認しておこう。おそらく任せるといった社長も正しく理解していないだろうから、しっかりと教えてあげないといけない。これは、教育・啓発担当としての仕事かな？

まず自分ができることは何だろうか？いきなりリスクアセスメントをするようなセキュリティ戦略担当の仕事をするのは正直自信がない。セミナー中に教わった、情報を調べて社内に共有していくセキュリティ連絡担当ならできそうだ。外部との連携はまだ自信がないから社内の連携をしていこう。セキュリティの取り組みに協力してくれる人も出てくるかもしれない。プラスセキュリティ人材の候補にもなる。まずは主体的に動いていくことが大切だ！

私が **セキュリティ担当** です



コラム
～セキュリティ業務の担当分担をしていると～

『セキュリティ』を強化するために、社内のルールや基準・対応方法を明確にするところから始めていきます。これらが規程になったり、マニュアルや手順書として明文化されていきます。この中には“どのような体制でセキュリティのマネジメントを行っていくか”ということも含んでいます。

セキュリティのマネジメントを行っていくことは、ルールなどの承認フローやセキュリティ事故の可能性があるときの連絡フローなど、多くの連携が必要になってきます。また、業務内容が多岐にわたるため、本書で紹介したような担当制をお勧めする場合もあります。しかしながら、中小企業のご担当者様とお話をしながら決めていくと、「すべて私が担当です」という企業様もいらっしゃいます。兼務されている方も多いため、業務負荷が心配になることもしばしばです。

人がいないから自分が担当するしかないという気持ちで、各担当を受けられる企業のご担当者様には頭が下がります。細かく担当を分ければ分けるほど、最終的に出来上がった体制図には同じ名前が並ぶということもあります。出来上がった体制図を見ながら担当者様と苦笑したこともありました。また、管理監督の関係から、どうしても担当を分けた方がよいということもあります。この場合には、管理監督する立場を担当者様に担ってもらい、別の方を作業者として体制を組むようにしています。

『人がいない』ということを理由に、セキュリティ対策をしなくてもよいということはありません。体制を考えたときに一人に担当が多くなるようであれば、複数人で分担して担当するなど検討してみてください。

あとがき

中小企業サイバーセキュリティ対策継続支援事業では、セキュリティ対策の基本を再確認し、課題解決などの手法を学ぶことで継続的なセキュリティ対策ができる人材の育成を目指しています。企業のセキュリティの取り組みの中心となる人材です。セキュリティは対岸の火事ではありません。自分事としてセキュリティの対策をし、強化をしていく必要があります。

1回目のテキストをお読みいただきありがとうございます。どのような感想を持たれましたか？引き続き必要なセキュリティのことをわかりやすく・楽しく伝えていけるように講師一同心掛けて参ります。よろしくお願いします。

令和4年度

中小企業サイバーセキュリティ対策継続支援事業

第2回

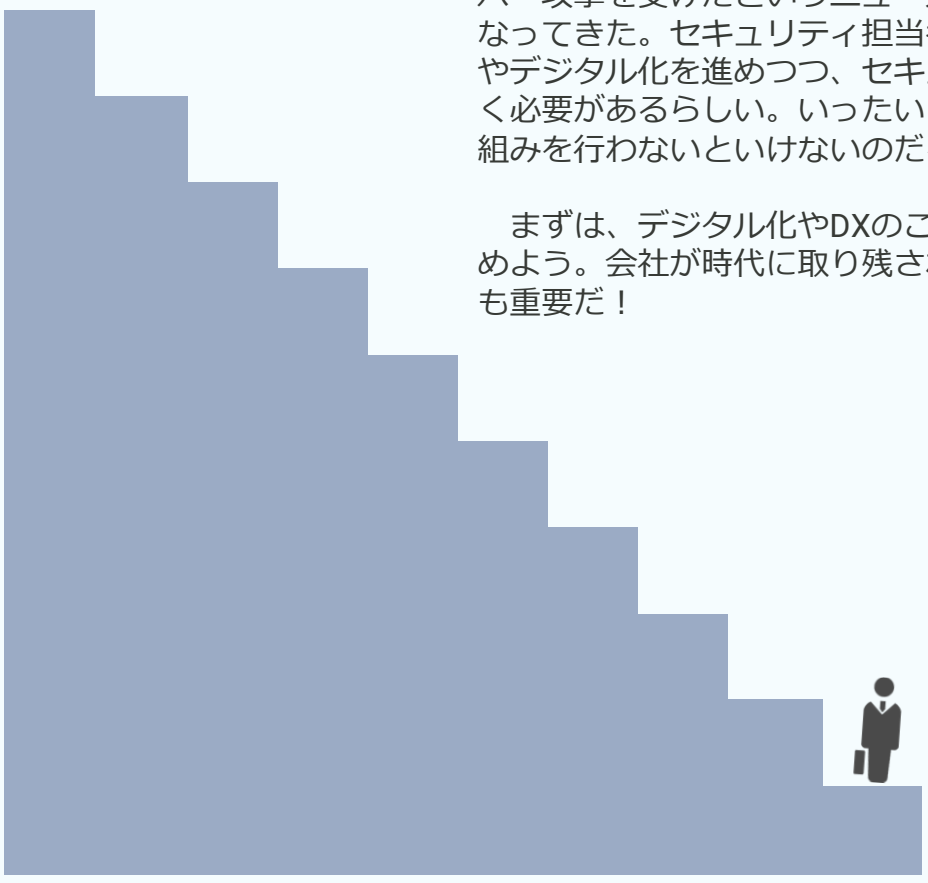
セミナー開催日：令和4年8月9日

デジタル化？
DX？
セキュリティと関係ありますか？

最近、「DX」というのが流行っているらしい

そもそも、DXというのは何だろうか？デジタル化とは違うことなのだろうか？何かの略語らしいけれども・・・例えば「名刺管理のシステムをクラウド化しました！」「遠方の顧客とオンライン会議できるようにします！」ということを聞くけれども、これはデジタル化？それともDX？

今のままでも十分業務はできているのにデジタル化って、なんだか難しそう。それを上回るメリットが本当にあるの？



急速にデジタル化が進む一方で、危険も増えているらしい。セキュリティを意識するようになると、サイバー攻撃を受けたというニュースに目が行くようになってきた。セキュリティ担当者である自分は、DX化やデジタル化を進めつつ、セキュリティを強化していく必要があるらしい。いったいどんな対策をし、取り組みを行わないといけないのだろう？

まずは、デジタル化やDXのことを知るところから始めよう。会社が時代に取り残されないようにすることも重要だ！

Day2
1.DXとセキュリティ

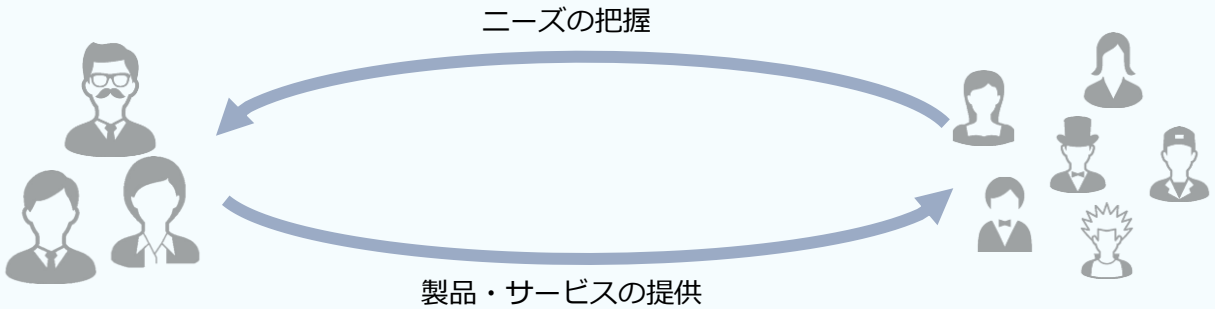
デジタルトランスフォーメーション

企業がビジネス環境の激しい変化に対応し、データとデジタル技術を活用して、顧客や社会のニーズを基に、製品やサービス、ビジネスモデルを変革するとともに、業務そのものや、組織、プロセス、企業文化・風土を変革し、競争上の優位性を確立すること。

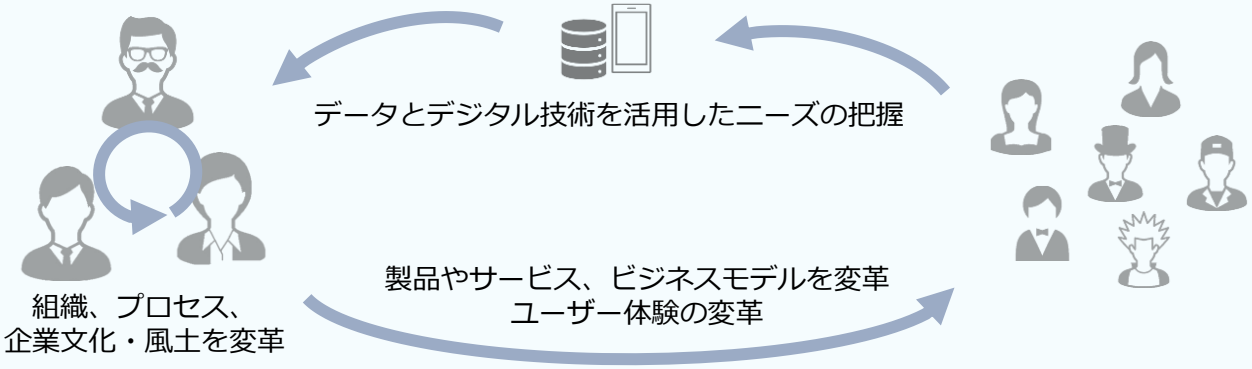
出典：経済産業省
デジタルトランスフォーメーションを推進するためのガイドライン（DX 推進ガイドライン）ver1.0
https://www.meti.go.jp/policy/it_policy/dx/dx_guideline.pdf

※「デジタルトランスフォーメーション」という言葉の定義は使う人や場面によって違いがみられ、統一されていません。本書の「デジタルトランスフォーメーション」は、「デジタルトランスフォーメーションを推進するためのガイドライン（DX 推進ガイドライン）ver1.0」（平成30年12月発表）におけるものを引用しています。

従来のビジネスの姿



DX推進の姿



Day2
1.DXとセキュリティ

デジタルトランスフォーメーションとデジタル化の違い

デジタルトランスフォーメーション（DX）を行っていくためには、デジタル化・デジタル活用の土壌が求められます。デジタルトランスフォーメーションの定義にも、「データとデジタル技術を活用」「業務そのものや、組織、プロセス、企業文化・風土を変革し、競争上の優位性を確立すること」というように、デジタルトランスフォーメーションとデジタル化は密接に関係しています。

デジタルトランスフォーメーションとデジタル化

Digitization（デジタイゼーション）

既存の紙のプロセスを自動化するなど、物質的な情報をデジタル形式に変換すること

Digitalization（デジタライゼーション）

組織のビジネスモデル全体を一新し、クライアントやパートナーに対してサービスを提供するより良い方法を構築すること

Digital Transformation（デジタルトランスフォーメーション/DX）

企業がビジネス環境の激しい変化に対応し、データとデジタル技術を活用して、顧客や社会のニーズを基に、製品やサービス、ビジネスモデルを変革するとともに、業務そのものや、組織、プロセス、企業文化・風土を変革し、競争上の優位性を確立すること

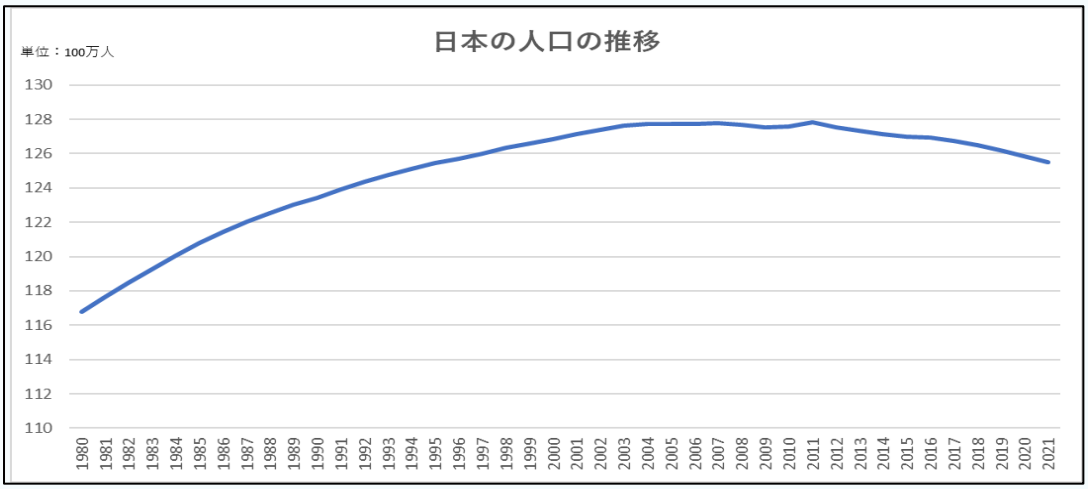
Day2

1.DXとセキュリティ

DXが求められる理由①

ビジネス環境は激しい変化をしています。特に日本は、人口の減少や生産性が低いということが問題視されています。

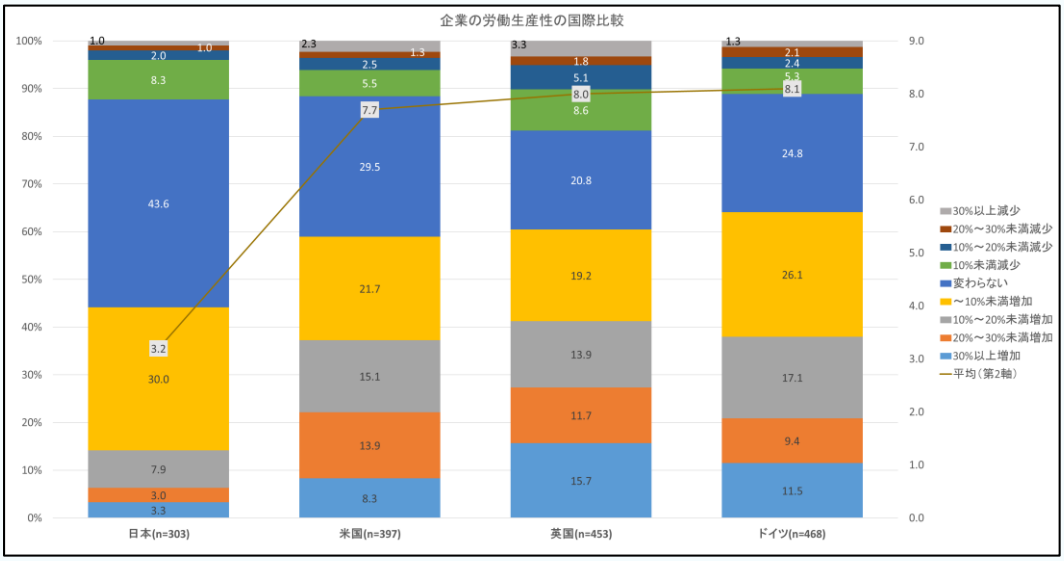
Point① 日本の人口は2011年を境に減少



出典：総務省統計局
「人口推計」をもとに作成
https://www.stat.go.jp/data/jinsui/new.html

人口減少に伴い、マーケットの縮小や労働人口の減少につながっています。
ビジネスチャンスを拡大させることや不足する労働力を補う対応が求められます。

Point② 伸び悩む日本の生産性



出典：総務省
「「ICTによるイノベーションと新たなエコノミー形成に関する調査研究」（平成30年）」をもとに作成
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h30/html/ne220000.html

日本、米国、英国、ドイツを比べると、労働生産性において日本は伸び悩んでいることがうかがえます。これは、日本の競争力低下にもつながります。これらの解消に向けてDXの期待値が高まっています。

Day2
1.DXとセキュリティ

DXが求められる理由②

DXは社内の文化や風土を変えていくことにも影響を及ぼします。DXによって、社員の働き方を変えたり、業務の効率化を進めたりして、従業員の労働環境を変えていくことが求められます。

Point③ 新たな企業文化醸成へ

社内に閉じた働き方

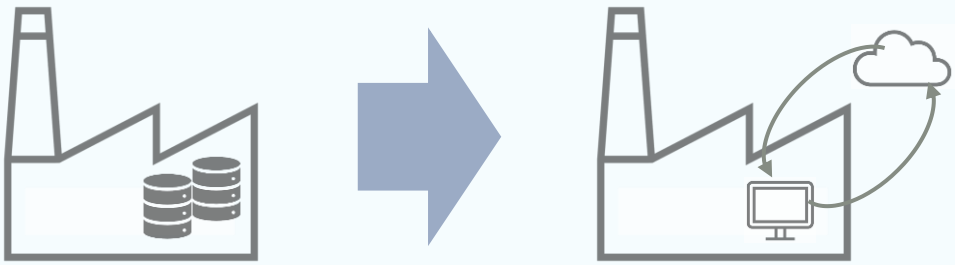
会社で画一的な働き方をする

場所を問わない働き方へ

労働環境の変化による
場所に縛られない働き方

働き方に選択肢が出ることは従業員の生産性を上げたり、社員のモチベーションに影響を与えることにつながります。また、これらを実現するためにもデジタル化の対応が求められます。

Point④ 老朽化システムからの脱却



老朽化・複雑化した社内システムでは、サポート終了などによりメンテナンスがされず、サイバーセキュリティのリスクが高まります。これらに対応しようとすると、保守やサイバーセキュリティ関連費用の増加や対応できる人材の不足という問題が発生してきます。

老朽化システムから脱却することは費用の問題だけでなく、データの収集や活用といったデジタル化の対応につながり、ゆくゆくは新たなビジネスモデルの創造や社内業務変革などにつながっていきます。

Day2

1.DXとセキュリティ

DX時代のセキュリティ①

「守りのIT 」よりも「攻めのIT 」に注目が集まっています。「セキュリティ」と聞くとセキュリティは社内を守るもの、売上を上げないものといった考えを持つ人は多いのではないでしょうか？

守りのIT

従来の社内業務の効率化・利便性の向上を目的としたIT

社内のIT環境を安全に利用するために必要なセキュリティ。
売上を上げることには繋がりづらい。

攻めのIT

新事業への進出や既存ビジネスの強化など企業価値を向上させるIT

新事業への進出や既存ビジネスを顧客へ安全に提供するために必要なセキュリティ。
売上・企業価値向上につながる。

DX ＝（共存の関係）＝ **セキュリティ**

企業の売上を上げていく事業部門や事業をDX化を適切に管理します。
尚、社内のデジタルをより安全に利用するためにも、セキュリティの役割は重要となります。

企業の売上を上げていく事業部門や事業を加速していくことを表します。デジタル活用をし、顧客にとっての新たな価値やユーザー体験を提供していきます。

One point

従来の社内業務の効率化・利便性の向上を目的とした守りのITとはいえ、クラウドの利用やテレワークなど社内業務のあり方は大きく変わりました。現在では、セキュリティを考えるポイントは社内だけではありません。クラウドの利用やテレワークでは、重要な情報が社外に存在します。現在のセキュリティでは、社外における守り方を考えることも重要です。デジタルをより安全に利用するためにも、セキュリティの役割は重要となっています。

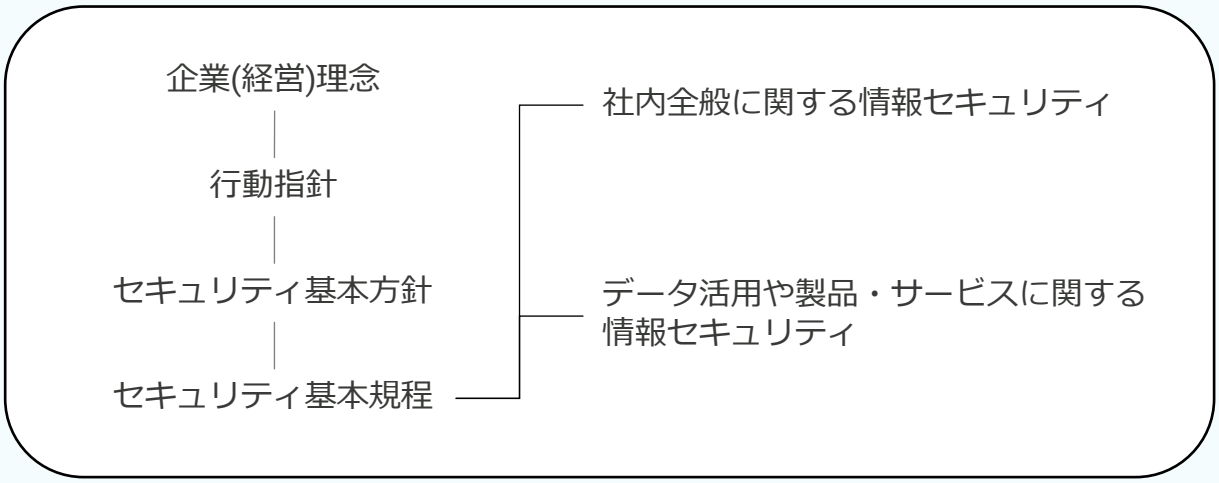
Day2

1.DXとセキュリティ

DX時代のセキュリティ②

DXでは、「ビジネス環境の激しい変化に対応しデータとデジタル技術を活用する。」「顧客や社会のニーズを基に製品やサービス、ビジネスモデルを変革する。」ということが求められます。そのため、データ活用や製品・サービスへのセキュリティをより考慮する必要があります。

DX時代のセキュリティの構成例



社内全般に関する情報セキュリティ

会社が保有する情報や重要な情報などを守ることを主に目的とします。

主な範囲
- 個人情報
- 経営に関する情報
- 見積もり、契約に関する情報
- 社内のシステム環境
- 企業が蓄積したノウハウなどに関する情報

社員の情報やお客様の情報など価値がある情報などを守るためのセキュリティです。

データ活用や製品・サービスに関する情報セキュリティ

製品やサービスを提供するために守るセキュリティです。

主な範囲
- 製品
- サービスシステム環境
- サービス提供のための顧客向け対応(対策)

製品やサービス提供においてもセキュリティは重要です。ビジネスモデルを変革し、お客様ニーズを満たしていくだけでなく、安全な製品・サービス提供を考えていく必要があります。

Day2
1.DXとセキュリティ

「Cybersecurity for All」
～誰も取り残さないサイバーセキュリティ～

サイバーセキュリティは個人・企業の問題だけにとどまりません。国としてもサイバーセキュリティを重視し、対策や施策を打ち出しています。今回は、令和3年9月28日に内閣サイバーセキュリティセンターから発表された「サイバーセキュリティ戦略」をもとにご紹介します。

日本を取り巻く時代認識：「ニューノーマル」とデジタル社会の到来

デジタル経済の浸透・デジタル改革の推進	新型コロナウイルスの影響/経験テレワーク、オンライン教育等の進展	厳しさを増す安全保障環境	SDGsへのデジタル技術の貢献期待	東京オリンピック・パラリンピックに向けて行ってきた取り組み

サイバー空間をとりまく課題認識：国民全体のサイバー空間への参画

• サイバー空間は、国民全体等あらゆる主体が参画し公共空間化 • サイバー・フィジカルの垣根を超えた各主体の相互連関・連鎖の深化 • 攻撃者に狙われ得る弱点となる可能性がある	地政学的緊張を反映 、国家間競争の場に安全保障上の課題にも	不適切な利用は国家分断、人権の阻害へ	官民の取り組みの活用

あらゆる主体にとってサイバーセキュリティの確保は
自らの問題に５つの基本原則※は堅持

※情報の自由な流通の確保、法の支配、開放性、自律性、多様な主体の連携

「Cybersecurity for All」
～誰も取り残さないサイバーセキュリティ～

デジタルトランスフォーメーション
とサイバーセキュリティの同時推進

安全保障の観点からの取り組み強化

公共空間化と相互連関・連鎖が進展する
サイバー空間全体を俯瞰した 安全・安心の確保

「自由、公正かつ安全なサイバー空間」の確保

出典：内閣サイバーセキュリティセンター
「サイバーセキュリティ戦略」をもとに作成
https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021.pdf
「サイバーセキュリティ戦略の概要」をもとに作成
https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-gaiyou.pdf

Day2

1.DXとセキュリティ

ミニワーク
～振り返ってみよう～

ミニワークテーマ

DXと聞いてどんなことをイメージしますか？

難しそう・まだよくわからない・社内ですでに取り組んでいるなど、いろいろなご意見があると思います。まずはDXの自分なりのイメージを書き出してみましょう。

One point

Digital Transformation（デジタルトランスフォーメーション）は、『DX』と略されます。今回のセミナーのタイトルである、「セキュリティとDXは同時進行？一緒にやらないといけないんですか？」にも含まれているDXです。

デジタルトランスフォーメーションとは、デジタルの変化・変形という意味合いとなってきます。Transformation には「変化・変形」という意味があります。

では、なぜTransformationが X となるのでしょう。 Digital Transformation（デジタルトランスフォーメーション）、「DTでは？」と思われた方もいるのではないでしょうか？ Transformation の Trans には 「交差する」という意味があります。このTransを1文字であらわす際に 『X』 が用いられます。そのため、 Digital Transformation は DX といわれます。

Day2

2.DXを進める！

DX推進に必要なこと

DXを推進していくと言っても、何から始めればよいのかわからないという声もよく聞きます。DXを進めるために必要なことはどんなことなのかを知っていきましょう。特にDX推進が目的にならないように注意し、DX推進の先にどのような企業になっているかを考えることが重要です。

Point① 経営者のリーダーシップ

経営者自らがDX推進においてリーダーシップを発揮し、「なぜDXを進めるのか」など目的を定める必要があります。そして、経営者自らも変化をしていくことが重要です。

Point② 従業員の学び直し

経営者だけでなく、従業員もDX推進を理解し取り組みに協力していくことが必要です。そのためにも、デジタル理解やリテラシー向上を目指した学び直しが重要です。

Point③ デジタル環境の見直し

今後の会社の目指す目的に合わせて、適切なデジタル環境を用意することが必要です。販売会社と協力をしながら、自分たちのやりたいことが実現できるデジタル環境を用意することが重要です。

Day2

2.DXを進める！

経営者に求められるリーダーシップ

DXを推進していくためには、経営者のリーダーシップが必要不可欠です。経営者が積極的に関わり、経営の在り方や仕組みを変えていく必要があります。

DX推進のための経営の在り方、仕組み

1、経営戦略・ビジョンの提示

想定される破壊的イノベーションを念頭に、データとデジタル技術の活用によって、どの事業分野でどのような新たな価値（新ビジネス創出、即時性、コスト削減等）を生み出すことを目指すか、そのために、どのようなビジネスモデルを構築すべきかについての経営戦略やビジョンが提示できているか。

2、経営トップのコミットメント

DXを推進するに当たっては、ビジネスや仕事の仕方、組織・人事の仕組み、企業文化・風土そのものの変革が不可欠となる中、経営トップ自らがこれらの変革に強いコミットメントを持って取り組んでいるか。

3、DX 推進のための体制整備

経営戦略やビジョンの実現と紐づけられた形で、経営層が各事業部門に対して、データやデジタル技術を活用して新たなビジネスモデルを構築する取り組みについて、新しい挑戦を促し、かつ挑戦を継続できる環境を整えているか。

4、投資等の意思決定のあり方

DX 推進のための投資等の意思決定をしているか
① コストのみでなくビジネスに与えるプラスのインパクトを勘案して判断しているか。
② 他方、定量的なリターンやその確度を求めすぎて挑戦を阻害していないか。
③ 投資をせず、DX が実現できないことにより、デジタル化するマーケットから排除されるリスクを勘案しているか。

5、DX により実現すべきもの： スピーディーな変化への対応力

ビジネスモデルの変革が、経営方針転換やグローバル展開等へのスピーディーな対応を可能とするものになっているか。

出典：経済産業省
デジタルトランスフォーメーションを推進するためのガイドライン（DX 推進ガイドライン）ver1.0
https://www.meti.go.jp/policy/it_policy/dx/dx_guideline.pdf

One point

DXを担当者に丸投げしてしまうという事態はよく起こりがちです。さらに、DXの目的の思考までを任せきりにしてしまうケースも少なくありません。その結果、どうなるかというと・・・

・開発したITシステムが満足できるものにならない
・自社の IT システムを把握できず、保守業者に任せきりになってしまう
・無理な要求に対して現場から不満が噴出する

このような事態に陥ってしまうと、DXが進みません。担当者は疲弊し、従業員は混乱します。DXを成功に導いている企業の経営者に共通していることは、経営者が自らDXの指揮を執って積極的に関与し、DXに必要な人材・資金などの経営資源を最後まで投入して成果に結びつけている点が挙げられます。

Day2
2.DXを進める！

DXに求められる学び直しの必要性①

いきなりDXを進めるといっても、社内に文化の醸成が必要です。その一つとして行うことがリスキリングです。職業能力の再開発、再教育という意味になります。経済産業省は「デジタル時代の人材政策に関する検討会」において、“新しい職業に就くために、あるいは、今の職業で必要とされるスキルの大幅な変化に適応するために、必要なスキルを獲得する／させること”と定義しています。

Point① 世界が急ぐリスキリング

世界経済会議（ダボス会議）では、「2030年までに全世界で10億人をリスキリングする」という宣言がなされ、「第4次産業革命により、数年で8000万件の仕事が消失する一方で9700万件の新たな仕事が生まれる」と提唱されています。大手企業は、従業員にリスキリングすると発表したり、コロナにともなう失業者にリスキリングを支援したりするなど、リスキリングに注力しています。

Point② 何をリスキリングしていくか？

DXで活用されるデータ・技術（ビジネスの場で活用されているデータやデジタル技術に関する知識）

データ	デジタル技術
社会におけるデータ	AI
データを読む・説明する	クラウド
データを扱う	ハードウェア・ソフトウェア
データによって判断する	ネットワーク

データ・技術の活用（ビジネスの場でデータやデジタル技術を活用する方法や留意点に関する知識）

活用方法・事例	データ・デジタル技術の活用事例	ツール活用	
留意点	セキュリティ	モラル	コンプライアンス

出典：経済産業省
「DXリテラシー標準」をもとに作成
https://www.meti.go.jp/policy/it_policy/jinzai/skill_standard/DX_Literacy_standard_ver1.pdf

One point

リスキリングという言葉以外にも、リカレント教育という言葉を聞いたことがある人もいるのではないでしょうか？リスキリングに対して、リカレント教育は『働き・学ぶ・働く』というサイクルにおいて、一度職を離れることが前提となっています。学び直しという点においては、リカレント教育を進めていくことも選択肢の一つです。

しかしながら、一度職を離れるという点に不安を覚える方はいらっしゃるのではないでしょうか？そのため、必要とされるスキルの大幅な変化に適応するためには働きながら必要なスキルを獲得することになります。

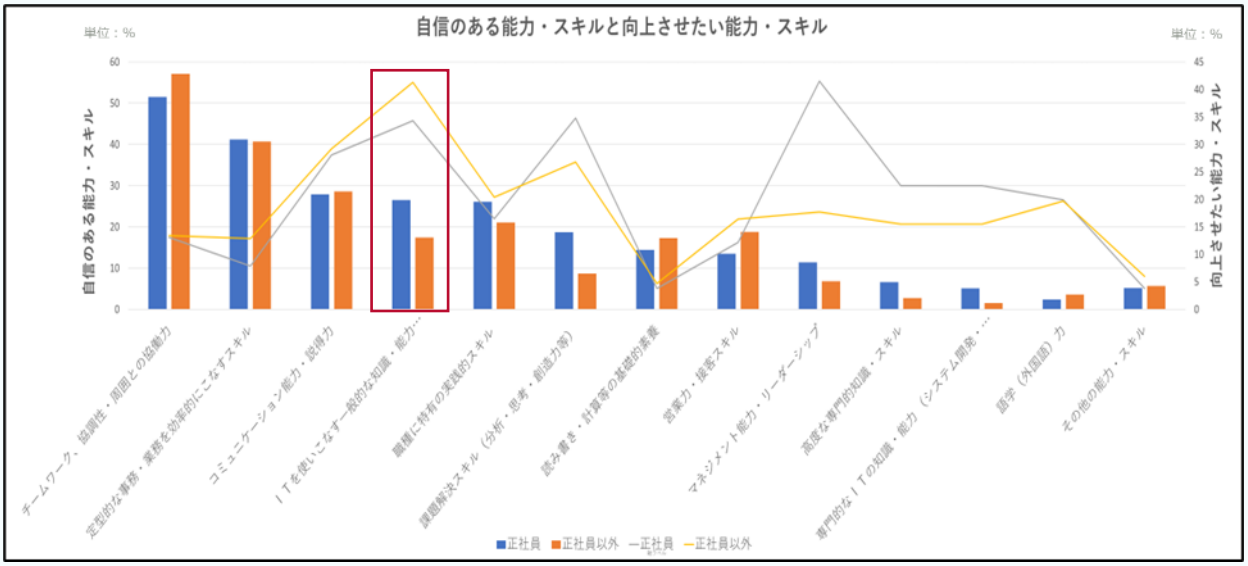
働きながらスキルを習得するためには、経営層の理解も必要になるとともに、従業員の働き方の改革、学ぶための予算が重要になってきます。いずれにしても、学びの必要性を理解して取り組む従業員の意識も大切です。

Day2

2.DXを進める！

DXに求められる学び直しの必要性②

学び直しの一つに、「デジタル」があります。デジタルリテラシーの向上はDX推進のために、全ビジネスパーソンに求められるものになってきています。デジタルの利活用が進むにあたってセキュリティの重要性も増しています。セキュリティ担当者はより高いデジタルリテラシーを意識する必要があります。



出典：厚生労働省
「令和３年度「能力開発基本調査」 」をもとに作成
https://www.mhlw.go.jp/toukei/list/dl/104-03b.pdf

ITを使いこなす一般的な知識・能力（ＯＡ・事務機器操作（オフィスソフトウェア操作など））は正社員で26.5%、正社員以外で17.4%と、自信がある能力・スキルと回答した人は少ない結果でした。しかしながら、向上させたい能力・スキルでは正社員で34.3%、正社員以外41.3%と高い数値を示しています。特に正社員以外では、ITを使いこなす一般的な知識・能力が向上させたい能力・スキルの中で一番高く、注目度や意識が高いことがうかがえます。向上させたいという気持ちに対して、向上できる環境を用意していくことも学び直しには必要です。

One point

学び直しというと研修を受けたり、資格を取ったりということが思い浮かぶのではないでしょうか？環境によっては、新しい部署で業務を覚えてもらうということでリスキリングに近しいことをしている企業もあることでしょう。最近はコロナの影響もあり、オンライントレーニングも充実しています。

経済産業省からは、「巣ごもりDXステップ講座」※1として、デジタルスキルを学ぶ機会がなかった人にも、新たな学習を始めるきっかけを得られるよう、誰でも、無料で、デジタルスキルを学ぶことのできるオンライン講座を紹介しています。

また、対面型のセミナーも増えてきました。このメリットは、他の会社の方の意見を聞くことで刺激を得られることです。仕事も忙しい中、なかなか業務を止めて研修に行くことは難しいという人もいるかもしれません。しかし、あえて対面で研修に参加することで、事例を聞けたり、他の会社の方の状況を知ることや悩みを相談できることは研修参加のメリットです。ぜひ学び直しを積極的に行っていきましょう。

「巣ごもりDXステップ講座」※1 https://www.meti.go.jp/policy/it_policy/jinzai/sugomori/index.html

Day2

2.DXを進める！

まずはデジタル化を！

DXを進めるための手段の一つに、「デジタル化」があります。いきなりDXを進めようとしても、デジタル化・デジタル活用の文化がないとなかなかDXは進んでいきません。かといって、何も考えずにデジタル化をすると上手く行かないということになりかねません。

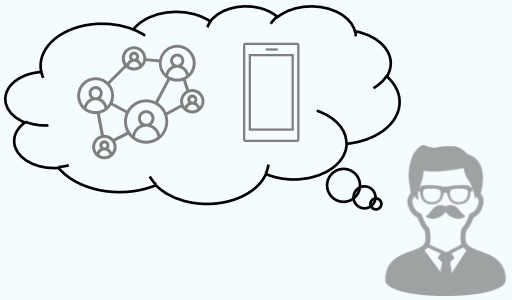
デジタル化を進めるSTEP

1、今後、会社をどうしていきたいのか？

まずは、目的を決めていきます。「なぜ取り組むのか」、「何を成し遂げたいのか」を考えましょう。
例：従業員がリモートで働けるようにしたい

2、そのためにすることは何か？

「なぜ取り組むのか」、「何を成し遂げたいのか」についてその為に実行すべきことを考えます。
例：リモートで働くための環境を用意する

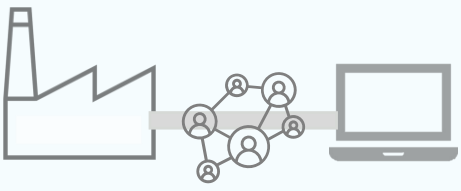


3、具体的に何を実現すればよいか？

実行すべきことを実現するためにどのようなことをすればよいのかを考えます。
例：モバイル端末の用意、安全な通信環境の用意

4、デジタル化・IT化を進めるか？

実現するために行うことはデジタル・ITを使って実現できるか、するべきかを考えます。
例：モバイル端末を支給し、VPN接続し社内アクセスする



5、製品・サービスは何が良いか？

実際にどのような製品・サービスを導入すればよいのかを考えます。
例：タブレット、VPN接続ツール

Day2
2.DXを進める！

デジタル化に伴い気を付けるべきセキュリティ①

デジタル化を進めていくということは、今までになかった危険性を持つことにもつながります。そのため、セキュリティが重要になります。ただ、危険性があるからデジタル化を行わないということにならないように注意しましょう。

Point① クラウドサービス利用の注意点

想定される使い方	危険性	対策
クラウドを基幹システムとして利用し、情報を置き、どこからでもアクセスできるようにする	クラウドへの不正アクセス	2要素認証の導入 パスワードルールの強化 接続元の制限
	クラウドの設定ミスによる情報漏洩	設定時のWチェック 手順書外作業の禁止
	不適切な情報開示	アクセス権限の適用 認証の徹底

Point② モバイル端末利用の注意点

想定される使い方	危険性	対策
リモートワーク、外出先での業務	紛失による情報漏洩	PCへのID・パスワードの設定 ハードディスクの暗号化 MDMなどの管理サービスの導入
	通信の盗聴	Free Wi-Fiの利用を制限 VPNなどの利用
	作業中の盗み見	スクリーンロックの徹底 覗き見防止フィルタの利用

こちらに挙げた危険性と対策は一部です。会社での利用の仕方や環境、設定内容により危険性は変わります。各社で状況が異なりますので、これだけをすれば安心ということはありません。

One point

デジタル化を行う際にセキュリティは必要不可欠です。そのため、製品やサービスを提供する会社もセキュリティには高い意識を持っています。しかしながら、提供会社も導入する会社のすべてを理解しセキュリティ対策にあたっているわけではありません。だからといってセキュリティ事故は提供会社が悪いということでもありません。導入にあたり提供会社と社内のセキュリティの担当者がしっかりと議論し、危険性や対策を検討することが本来あるべき姿ではないでしょうか？そのためには、社内でセキュリティがわかる人材というのは必要不可欠になっています。

Day2
2.DXを進める！

デジタル化に伴い気を付けるべきセキュリティ②

チェックBOX	サービス関連のチェック項目
	サービスを提供する時間帯（設備やネットワーク等の点検／保守のための計画停止時間の記述を含む）は適切か？ 例：24時間 365日 （計画停止／定期保守を除く）
	定期的な保守停止に関する事前連絡確認（事前通知のタイミング／方法の記述を含む）はあるか？ 例：30 日前にメール／ホームページで通知
	サービスを利用できる確率（（計画サービス時間－停止時間）÷ 計画サービス時間）は高いか？ 例：99.9%以上（基幹業務）99%以上（基幹業務以外）
	災害発生時のシステム復旧／サポート体制はあるか？ 例：遠隔地のバックアップ用データセンターで保管している日次バックアップデータと予備システムへの切り替え
	早期復旧が不可能な場合の代替措置はあるか？ 例：バックアップデータの取得が可能なホームページを用意
	代替措置で提供されるデータ形式の定義は記述されているか？ 例：CSV あるいはExcel ファイルで提供
	バージョンアップ／変更管理／パッチ管理の方針はあるか？ 例：年2回の定期バージョンアップを実施
	障害発生から修理完了までの平均時間（修理時間の和÷故障回数）は適切か？ 例：1時間以内（基幹業務）12時間以内（基幹業務以外）
	システム監視基準（監視内容／監視・通知基準）の設定に基づく監視はあるか？ 例：1日4回のハードウェア／ネットワーク／パフォーマンス監視
	障害発生時の連絡プロセス（通知先／方法／経路）はあるか？ 例：指定された緊急連絡先にメール／電話で連絡し、併せてホームページで通知
	異常検出後に指定された連絡先に通知するまでの時間は適切か？ 例：15分以内（基幹業務） 2時間以内（基幹業務以外）
	障害や事故の収集／集計する時間間隔は適切か？ 例：1分以内（基幹業務） 15 分（基幹業務以外）
	サービス提供状況を報告する方法／時間間隔は適切か？ 例：月に一度ホームページ上で公開
	利用者に提供可能なログの種類（アクセスログ、操作ログ、エラーログ等）は適切か？ 例：セキュリティ（不正アクセス） ログ／バックアップ取得結果ログを利用者の要望に応じて提供
	バッチ処理（一括処理）の作業時間は適切か？ 例：4時間以下
	カスタマイズ（変更）が可能な事項／範囲／仕様等の条件とカスタマイズに必要な情報はあるか？ 例：利用画面上の項目配置変更や新規項目の追加が設定画面より可能
	既存システムや他の SaaS 等の外部のシステムとの接続仕様（API、開発言語等）はあるか？ 例：API（プログラム機能を外部から利用するための手続き）を公開
	オンラインの利用者が同時に接続してサービスを利用可能なユーザー数は適切か？ 例：50ユーザー（保証型）

チェックBOX	サポート関連のチェック項目
	障害対応時の問合せ受付業務を実施する時間帯は適切か？ 例：24 時間 365 日（電話）
	一般問合せ時の問合せ受付業務を実施する時間帯は適切か？ 例：電話：営業時間内（年末年始・土日・祝祭日を除く）、メール：24 時間 365 日

チェックBOX	データ管理のチェック項目
	バックアップ内容（回数、復旧方法など）、データ保管場所／形式、利用者のデータへのアクセス権など、利用者に所有権のあるデータの取扱方法は適切か？ 例：日次でフルバックアップ。遠隔地のデータセンターにテープ形式保管。アクセス権はシステム管理者のみに制限。復旧／利用者への公開の方法は別途規定
	データをバックアップした媒体を保管する期限は適切か？ 例：5年以上（基幹業務）3ヶ月以上（基幹業務以外）
	サービス解約後の、データ消去の実施有無／タイミング、保管媒体の破棄の実施有無／タイミング、およびデータ移行など、利用者に所有権のあるデータの消去方法はあるか？ 例：サービス解約後 1ヶ月以内にデータおよび保管媒体を破棄。

チェックBOX	セキュリティ関連のチェック項目
	JIPDEC や JQA 等で認定している情報処理管理に関する公的認証 （ISMS、プライバシーマーク等） が取得されているか？ 例： ISMS 認証取得プライバシーマーク取得をしている
	不正な侵入、操作、データ取得等への対策について、第三者の客観的な評価を得ているか？ 例：年１回、外部機関によりサービスの脆弱性に関する評価を受け、速やかに指摘事項に対して対策を講じる
	利用者のデータにアクセスできる利用者が限定されているか？ 例：利用者のデータにアクセスできる社員等はセキュリティ管理者の許可を得た者に限る
	提供者側でのデータ取扱環境が適切に確保されているか？ 例：オフィスは ICカードによる 運用で執務室に入室可能な社員等を最小限に制限しており、PC はすべてシンクライアントである
	システムとやり取りされる通信の暗号化強度は適切か？ 例： TLS1.2以上など

出典：経済産業省
「SaaS 向け SLA ガイドライン」をもとに作成
https://www.meti.go.jp/policy/netsecurity/secdoc/contents/downloadfils/080121saasgl.pdf

Day2

2.DXを進める！

ミニワーク
～振り返ってみよう～

ミニワークテーマ

社内で行われている学び直しの振り返り

学び直しの事例を探してみましょう。もしあまり取り組まれていないということでしたら、どんな学び直しをしたいかを考えてください。

Day2
3.DXを進めるための組織強化を目指して

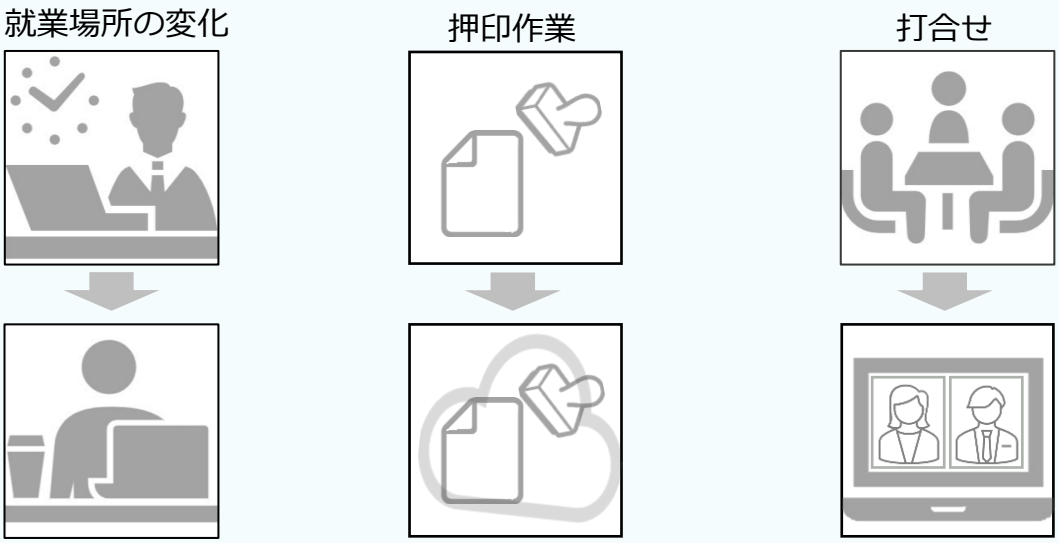
経営層を中心に土台を固める

DXを進めていくためには、デジタイゼーションやデジタライゼーションといったデジタル化の土壌やリスキリングといった学び直しの意識が重要になります。これらを実現するためには、経営層が中心となって組織の土台を固めていくことが重要です。

Point① DXの土台としてのデジタル化

デジタルトランスフォーメーション
業務そのものや、組織、プロセス、企業文化・風土を変革

デジタイゼーション・デジタライゼーション



Point② DXを実現するための人材づくり

経営者は学び直しがしやすい土壌を用意し、人材の変化を促す必要があります。人材の変化のためリスキリングは5ステップで行うと効果的です。

リスキリングを進めるための5ステップ

1. 事業戦略に基づき、人材像やスキルを定める
2. リスキリングのプログラムを定める
3. リスキリングで使用するコンテンツを定める
4. 各従業員に取り組んでもらう
5. リスキリングで習得したスキルや知識を実践で活用する

経営者が認識すべき３原則

経営者は、以下の３原則を認識し、対策を進めることが重要であると、経済産業省が提唱しています。

原則1　経営者は、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要

ビジネス展開や企業内の生産性の向上のためにITサービス等の提供やITを利活用する機会は増加傾向にあり、サイバー攻撃が避けられないリスクとなっている現状において、経営戦略としてのセキュリティ投資は必要不可欠かつ経営者としての責務です。

このため、サイバーセキュリティリスクを多様な経営リスクの一つとして位置づけ、サイバーセキュリティ対策を実施する上での責任者となる担当幹部（CISO等）を任命するとともに、経営者自らがリーダーシップを発揮して適切な経営資源の配分を行うことが必要です。

原則2　自社は勿論のこと、ビジネスパートナーや委託先も含めたサプライチェーンに対するセキュリティ対策が必要

サプライチェーンのビジネスパートナーやシステム管理等の委託先がサイバー攻撃に対して無防備であった場合、自社から提供した重要な情報が流出してしまうなどの問題が生じ得ます。

このため、自社のみならず、サプライチェーンのビジネスパートナーやシステム管理等の委託先を含めたセキュリティ対策を徹底することが必要です。

原則3　平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策に係る情報開示など、関係者との適切なコミュニケーションが必要

万一サイバー攻撃による被害が発生した場合、関係者と、平時から適切なセキュリティリスクのコミュニケーションができていれば、関係者の不信感の高まりを抑えることができます。

このため、平時から実施すべきサイバーセキュリティ対策を行っていることを明らかにするなどのコミュニケーションを積極的に行うことが必要です。

出典：経済産業省
サイバーセキュリティ経営ガイドライン Ver2.0
https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide2.0.pdf

サイバーセキュリティ経営の重要１０項目

経営者は、サイバーセキュリティ対策を実施する上での責任者となる担当幹部（CISO等）に対して以下の重要１０項目を指示すべきであると、経済産業省が提唱しています。

項目1 サイバーセキュリティリスクの認識、組織全体での対応方針の策定

サイバーセキュリティリスクを経営リスクの一つとして認識し、組織全体での対応方針（セキュリティポリシー）を策定させます。

項目2 サイバーセキュリティリスク管理体制の構築

サイバーセキュリティ対策を行うため、サイバーセキュリティリスクの管理体制（各関係者の責任の明確化も含む）を構築させます。その際、組織内のその他のリスク管理体制とも整合を取らせます。

項目3 サイバーセキュリティ対策のための資源（予算、人材等）確保

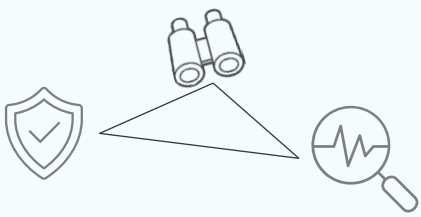
サイバーセキュリティリスクへの対策を実施するための予算確保とサイバーセキュリティ人材の育成を実施させます。

項目4 サイバーセキュリティリスクの把握とリスク対応に関する計画の策定

経営戦略の観点から守るべき情報を特定させた上で、サイバー攻撃の脅威や影響度からサイバーセキュリティリスクを把握し、リスクに対応するための計画を策定させます。その際、サイバー保険の活用や守るべき情報について専門ベンダへの委託を含めたリスク移転策も検討した上で、残留リスクを識別させます。

項目5 サイバーセキュリティリスクに対応するための仕組みの構築

サイバーセキュリティリスクに対応するための保護対策（防御・検知・分析に関する対策）を実施する体制を構築させます。

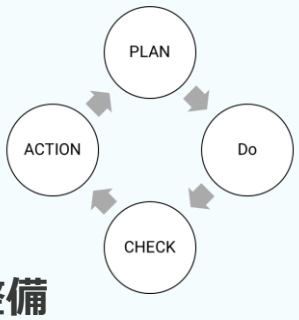


出典：経済産業省
サイバーセキュリティ経営ガイドライン Ver2.0
https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide2.0.pdf

サイバーセキュリティ経営の重要１０項目

項目6　サイバーセキュリティ対策におけるPDCAサイクルの実施

計画を確実に実施し、改善していくため、サイバーセキュリティ対策をPDCAサイクルとして実施させます。定期的に経営者に対策状況を報告させた上で、問題が生じている場合は改善させ、対策状況を開示させます。



項目7　インシデント発生時の緊急対応体制の整備

インシデント発生時の組織内の対応体制（CSIRT等）を整備させます。被害発覚後の通知先や開示が必要な情報を把握させるとともに、情報開示の際に経営者が組織の内外へ説明できる体制を整備させます。また、インシデント発生時の対応について、適宜実践的な演習を実施させます。

項目8　インシデントによる被害に備えた復旧体制の整備

インシデントにより業務停止等に至った場合、企業経営への影響を考慮していつまでに復旧すべきかを特定し、復旧に向けた手順書策定や、復旧対応体制の整備をさせます。組織全体として整合の取れた復旧目標計画を定めさせます。また、業務停止等からの復旧対応について、適宜実践的な演習を実施させます。

項目9　ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握

監査の実施や対策状況の把握を含むサイバーセキュリティ対策のPDCAについて、系列企業、サプライチェーンのビジネスパートナーやシステム管理の運用委託先等を含めた運用をさせます。システム管理等の委託について、自組織で対応する部分と外部に委託する部分で適切な切り分けをさせます。

項目10 情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供

社会全体において最新のサイバー攻撃に対応した対策が可能となるよう、サイバー攻撃に関する情報共有活動へ参加し、積極的な情報提供及び情報入手を行わせます。また、入手した情報を有効活用するための環境整備をさせます。

出典：経済産業省
サイバーセキュリティ経営ガイドライン Ver2.0
https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide2.0.pdf

Day2
3.DXを進めるための組織強化を目指して

セキュリティトレンドの変化

世の中の変化に合わせて新しい製品やサービスが出るように、セキュリティにもトレンドがあります。世の中で流行っている攻撃や働き方によりトレンドも変化します。自社の状況と合わせるだけでなく、セキュリティのトレンドに合わせて見直しをしていく必要があります。

Point① ゼロトラストセキュリティ

これまでのセキュリティ対策は、信頼できるネットワーク（内部）と、信頼できないネットワーク（外部）に分けて考えていました。境界にファイアウォールや境界防御型ゲートウェイなどのセキュリティ製品を設置し、不正な通信を監視し、防御するという方法が一般的でした。この従来のセキュリティ対策は、保護すべき情報やシステム等の重要な情報が信頼できるネットワークの内側にあることを前提としています。

しかし、昨今はクラウドが普及したことにより、インターネット上に保護すべき重要な情報が存在するケースも珍しくなくなりました。これは、信頼できるネットワーク外に重要な情報が置かれることになります。また最近では、リモートワークやテレワークといった働き方も主流となっていることから、データを扱う人も信頼できるネットワークの内側にいないといった状況になっています。環境変化に伴い、今までとは違ったセキュリティ対策が必要です。そのため、今後のセキュリティ対策はすべての通信を信頼しないことを前提とした、「ゼロトラスト」の考え方が主流となりつつあります。「ゼロトラスト」に基づいたセキュリティモデルを「ゼロトラストセキュリティ」と呼び、ゼロトラストセキュリティを実現したネットワークを「ゼロトラストネットワーク」と呼びます。

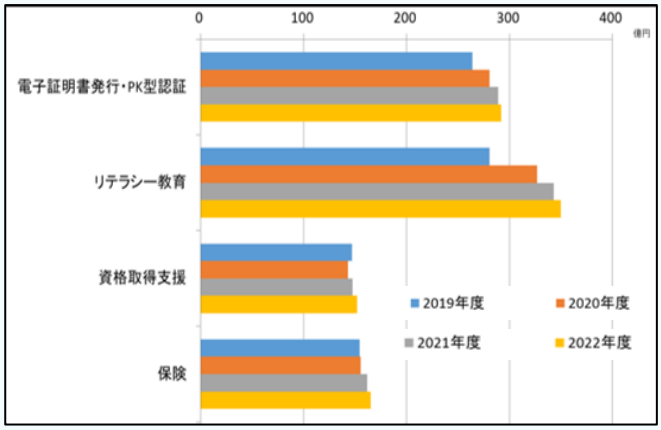
働き方やデータの保管の変化により、個人の認証は多要素認証が主流となったり、リモートワーク対策のセキュリティ導入が進んだりと変化が見られます。

Point② サイバー保険の活用

攻撃を防ぎ、事故にあわないように取り組むことは重要です。しかしながら事故が起こらないという保証をすることはできません。最近ではこれらに対応するためにサイバー保険というものがあり、市場でも伸びてきています。

サイバー保険は、通常の保険のイメージと全く同じです。病気などの際に保険金が払われるように、サイバー攻撃などによるセキュリティ被害に対して保険金が支払われます。

事故を起こさないようにすることはもちろんですが、何か重要な取り組み、リスクを伴う取り組みの際には検討してみてはいかがでしょうか？



出典：NPO日本ネットワークセキュリティ協会（JNSA）
市場調査ワーキンググループ国内情報セキュリティ市場 2021年度調査報告
https://www.jnsa.org/result/surv_mrk/2022/index.html

Day2

3.DXを進めるための組織強化を目指して

DX推進の事例紹介①

～クラウド導入で企業の文化を変革～

クラウド導入から企業文化を変革

ある企業では、自社の情報をクラウドを利用して共有することにしました。もともとクラウドを利用しようと思ったのは、業績の低迷を受け、生産性アップを目指したからです。

しかしながら、クラウド導入には社内の年配社員から反発もありました。この反発を社長のリーダーシップで乗り切りました。トップダウンの命令ではなく、社長自らプレゼンを行い、導入のメリットを説いたのです。

導入後は、売上情報やノルマの情報を共有するようになりました。即座に情報が把握できるようになり、売上などが見える化したことで、モチベーションアップにもつながっています。また、不良品の状況やクレームの情報も共有し品質向上にもつなげ、社員が不良品を出さないように意識できるようになりました。

デジタル化を進めるSTEP

1、今後、会社をどうしていきたいのか？

2、そのためにすることは何か？

3、具体的に何を実現すればよいか？

4、デジタル化・IT化を進めるか？

5、製品・サービスは何が良いか？

今回の導入がうまくいったポイントの一つとして考えられるのは、クラウド機能の利用順番です。全部の機能を最初から全て使うのではなく、一つの機能をまずは浸透させて、浸透したら次の機能を使っていくというやり方で進めました。

一番初めに使った機能は掲示板の機能です。パソコンが起動したら掲示板が立ち上がるようにし、情報を目に止めやすくする工夫をしました。

不思議なもので一度便利さに気付くと、反発していた年配社員も利用するようになります。情報共有が円滑に進むということは社内の風通しもよくなります。導入前以上にコミュニケーションが活性化しました。

クラウド導入の効果はこれだけでなく、社員の平均年齢にも表れるようになりました。年配社員が多かったのが、最近ではデジタル活用をしているという点で若手社員も採用面接を受けに来るようになり、実際社員の平均年齢も下がることにつながっています。クラウド導入というデジタル化の一つの取り組みを突き詰めていくことで、企業の文化が変わり、風土が変わるという点はまさにDXといえます。

DX推進の事例紹介②
～自社ノウハウのサービス提供事例～

自社ノウハウをクラウドサービスとして提供

ある会社では、自社で培ったノウハウをクラウドサービスで提供しました。今までの事業で培った経験やノウハウは顧客ニーズがあるため、お客様へのサービス提供を決めました。クラウドは社内で使っているけれども、サービスとして提供するためにクラウドを利用することは初めてのことでした。これにチャレンジしていくきっかけとなったのは、変革意識や初期投資であり、何しろ、社長のリーダーシップと取り組みにあたってのコミットメントがあったからです。

このサービス提供にあたって大変だったことの一つがセキュリティでした。お客様もセキュリティには細心の注意を払っています。もし提供するクラウドシステムから情報が流出するようなことがあれば、大問題です。そのため、サービス提供するクラウドシステムのセキュリティレベルも高いものが求められました。大きな企業と契約する際に、セキュリティチェックを求められた経験をした人も多いのではないでしょうか？
今回は、意見をもらいながらサービスセキュリティを高めていきました。担当の方は大変だったそうですが、今までの事業とは違ったサービス立ち上げを行ったことで、ビジネスの可能性が高まっています。

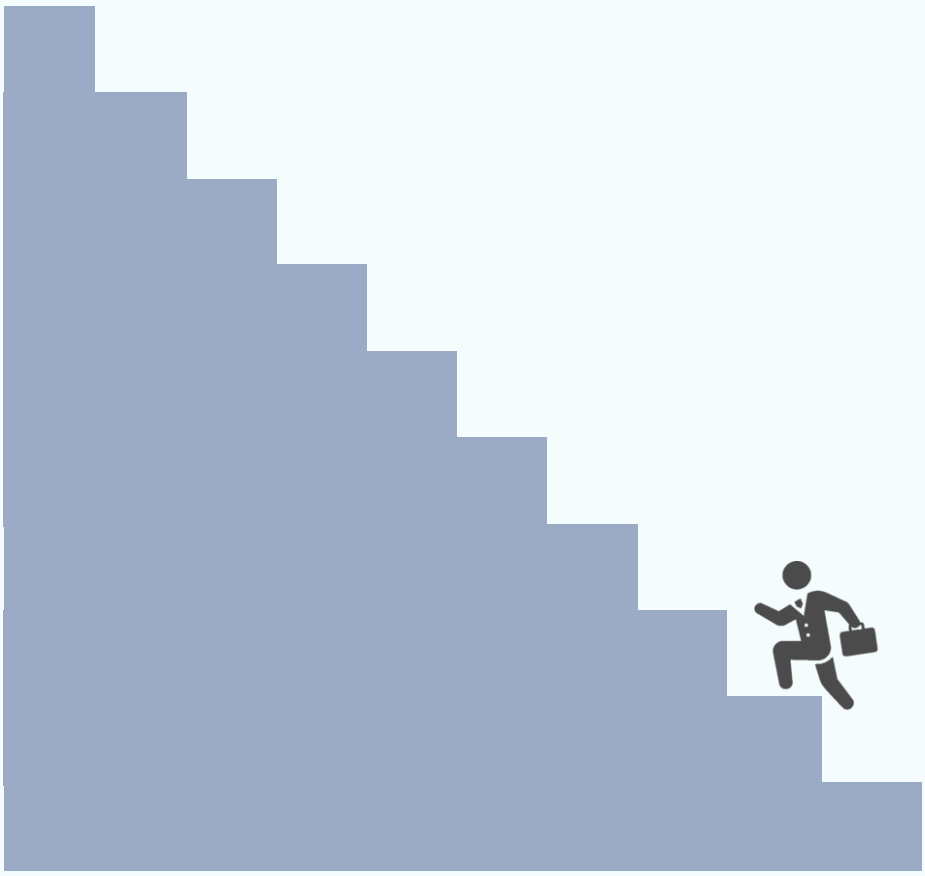
自分たちでは当たり前と思っていることが実は顧客ニーズがあるということはよくあります。まずはニーズがあることを知ることが重要ではないでしょうか？
ニーズを把握できれば、あとはどのような形でサービスを提供していくかということになります。ここで専門的なスキルや知識が必要になるケースがあり、あきらめてしまう場合もあります。人がいないことをやらない理由にするのではなく、どうすれば実行できるかを考えていくことが重要になります。そして、これを乗り越えサービスを提供することができれば、製品やサービス、ビジネスモデルを変革することにつながっていきます。

自分たちの持っているものを売れるようにしていくことで新たなビジネスを広げていくということは、企業文化や風土を変革し、競争上の優位性を確立していくことにつながる行動です。こういった事例はDXといえるのではないでしょうか？

ここ数年で、世界はガラッと変わった気がする。オンライン会議も平然と行っているし、買い物も電子マネーを使うようになった、レストランに入ればロボットが給仕をしている。世の中はどんどん変わっていて便利になっているけれど、自分の会社は何か変わっただろうか？正直昔から大して変わっていないような気も・・・

DXも、セキュリティも、「しなければならないこと」。
DXやデジタル化を進めるためには、セキュリティを一緒に考えなければいけない。今までは、社内を守るものということでセキュリティは利益が出ないものとし、コストと考えていた。「ビジネス環境の激しい変化に対応し、データとデジタル技術を活用して、顧客や社会のニーズを基に、製品やサービス、ビジネスモデルを変革するとともに、業務そのものや、組織、プロセス、企業文化・風土を変革し、競争上の優位性を確立する」ためにも投資ととらえていかないといけない。
安全なDXにするためにも、しっかりとしたセキュリティの基盤をつくっていこう。安心・安全なDXを実現するために、もっとセキュリティのことを知っていこう。

DXとセキュリティ
バランスを取りながら共存へ



コラム
～新しいサービスを導入する～

DX推進の要素の一つにはデジタル化も含まれます。新しいサービスを社内に導入することもデジタル化にあたります。皆さんは、新しいサービスや製品を社内に導入する際にはどのように決めていますか？製品やサービスを導入することが目的になっていませんか？

製品やサービスを導入する際にまず重要なことは、「何を成し遂げたいか？」を考えることです。目的をはっきりさせたうえで、成し遂げるために必要な機能を満たした製品やサービスを探しましょう。その際に気を付けることの一つがセキュリティです。

DX with Cybersecurityというように、デジタルを活用・導入する際にセキュリティを一緒に考えることは一般的となっています。セキュリティを考える際には、自社のセキュリティルールを満たしているかという製品面のセキュリティだけでなく、必要に応じて販売元のセキュリティ体制などについても検討の材料とします。

実際導入するサービスや製品が自社のセキュリティルールを完全に満たしているというケースは多くないかもしれません。それは、各社のルールがそれぞれ異なり、気を付けるポイントも各社によって違うからです。だからこそ、あの会社が入れた製品だからという理由では、製品の検討はできないことになります。もし求めるセキュリティに達していなかったら、どんなに優秀な製品やサービスでも「あきらめる」ということを考えないといけなくなります。

しかしながら、「何を成し遂げたいか？」という目的に照らし合わせて考えた場合、なかなかあきらめきれないということも事実です。DXとセキュリティは一緒に考え、バランスを取りながら共存させていく必要があります。

あとがき

新しいことを始める際に、手段の一つとしてデジタルを活用するということは選択肢として必ず上がってきます。正直これはDXなのか、ただのデジタル化なのかという疑問は導入を進めながらも考えてしまいます。デジタル化かDX化を分けるポイントは、デジタル化をした先に何が変わるかではないかと思います。手段の代替では何も変わりません。デジタルにより変化が生まれ、変化が変化を呼び企業が変わっていく、これがDXだと今では思っています。

デジタル化をしただけではDXと言えないかもしれませんが、DXのスタートを切ったとは言えるのかもしれません。そのDXがただのデジタル活用で終わるのか本当のDXになるのかは、これからの活動が重要になってきそうです。

令和4年度

中小企業サイバーセキュリティ対策継続支援事業

第3回

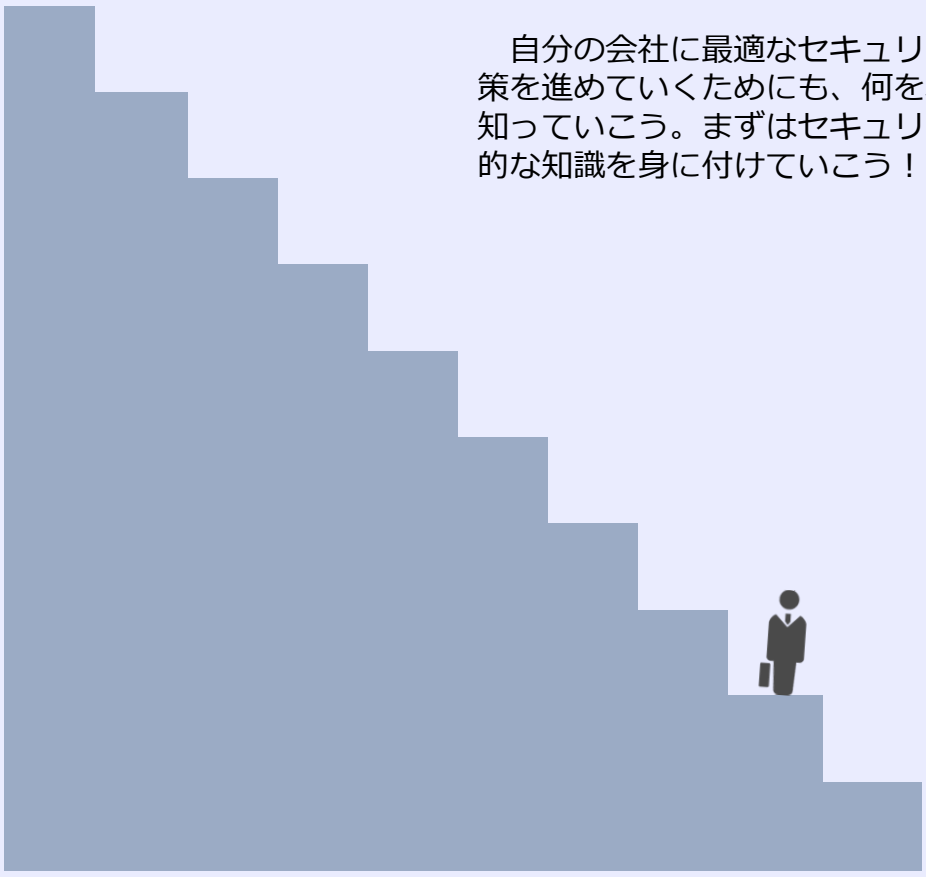
セミナー開催日：令和4年8月23日

資産？
リスク？
フレームワーク？

セキュリティ担当として、やるべきことがたくさんあることはわかってきた。特に、DXを進める会社としては、セキュリティを強化していく必要がある。だから、セキュリティについてもっと詳しく知っていかないといけない。

そもそも、うちの会社は何を守るのだろうか？顧客の個人情報、契約書の内容、社用PCのパスワードなんかも、守るべき情報なんだろうか？守るべき情報は防御するだけでは不十分と聞いたがセキュリティって防御することが重要で、事故を起こさないようにすることが重要じゃないの？

でも・・・もしサイバー攻撃を受けたらどうなるんだろう？会社は存続できるのだろうか？サイバー攻撃を受けたことも想定して準備をしておかないといけない。効率よく対応をする方法も学び、限りある資源を有効に使おう。



自分の会社に最適なセキュリティ対策、効率的な対策を進めていくためにも、何を基準にすれば良いかを知っていこう。まずはセキュリティの概要を学び基本的な知識を身に付けていこう！

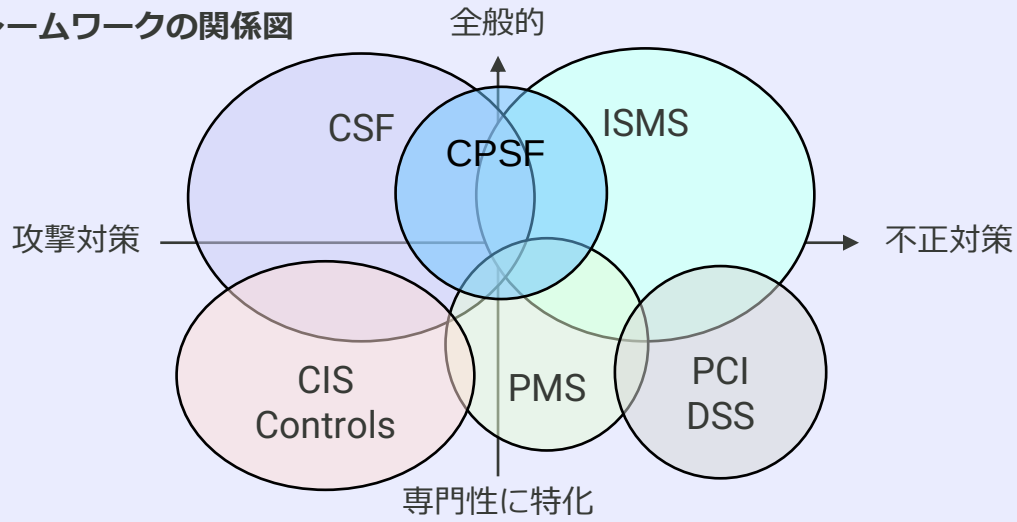
Day3
1.セキュリティの概念

情報セキュリティに関する各種フレームワーク

デジタル分野の発展に伴い、セキュリティの必要性が日に日に増してきています。考え方を標準化したフレームワークにもいろいろな種類があり、特徴があります。

名称	特徴	概要
ISMS	情報セキュリティ対策が中心	ISO/IEC 27001（JIS Q 27001）の国際規格。要求事項に則り、情報資産の保護が対象となる。
CSF	サイバー攻撃対策が中心	サイバー攻撃等を受けたときの検知、対応、復旧といった事後対応についても多くの対応策が盛り込まれている。
PMS	個人情報の取り扱いが中心	JISQ15001に準じた国内規格。企業が保有している個人情報を確実に保護するように要求。
PCI DSS	クレジットカード情報が中心	クレジットカード情報の保護。
CIS Controls	技術的な対策状況確認が中心	技術的な対策に重点を置いたガイドライン。
CPSF	情報セキュリティ対策 サイバー攻撃対策が中心	経済産業省が公表。ISMS、CSFを包含し、サイバー空間とフィジカル空間におけるつながりの信頼性を確保。

フレームワークの関係図



ISMSは、『個別の問題毎の技術対策の他に、組織のマネジメントとして、自らのリスクアセスメントにより必要なセキュリティレベルを決め、計画を定め、資源を配分して、システムを運用すること』としています。ISO/IEC 27001（JIS Q 27001）で要求事項を定めた規格であり、組織がISMSを確立し、実施し、維持し、継続的に改善するための要求事項を提供することを目的として作成されています。政府機関から提示されている各種ガイドブック、ハンドブック、テキスト類は、ISMSの仕組みがベースとなっています。ISMSは現在、サイバーセキュリティ脅威や新しいセキュリティ技術の進化に合せて、改訂作業が進められています。

ISMSは事前の対策に強みがあり、サイバー攻撃等を受けたときの管理策が薄くなりがちという特徴があります。それを補う考えとして、サイバーセキュリティフレームワーク(CSF)という考えが浸透してきています。「サイバーセキュリティ経営ガイドライン Ver 2.0 」では、「付録A サイバーセキュリティ経営チェックシート」でCSFとの対応関係も提示されました。ただし、CSFは、「どのように利用するかは、それを実施する組織に委ねる。」とされている汎用的なフレームワークとして、指示書やノウハウ集ではありません。

経済産業省では、ISMS、CSFを包含した「サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF)を提唱しています。サイバー空間とフィジカル空間のそれぞれにおけるリスクを洗い出し、そのセキュリティ対策を整理するためのフレームワークとして期待されています。

セキュリティの3要素

企業や組織におけるセキュリティとは、企業や組織の守るべき情報を「機密性」・「完全性」・「可用性」の特性においてバランスをとり維持していく事です。

守るべき情報とは、企業にとって価値がある情報です。顧客情報や経営に関係する情報を指します。また、それらの価値ある情報が記載されている「紙」や「電子ファイル」も守るべき情報です。さらに、「電子ファイル」が保存されているパソコンやサーバ、外部記憶媒体もセキュリティの対象です。

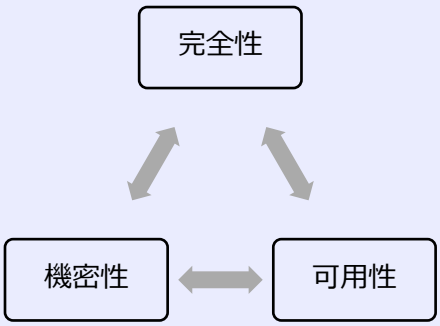
セキュリティでは、 各守るべき価値がある情報の特性を検討し「機密性」・「完全性」・「可用性」のバランスを考慮していく必要があります。セキュリティと言うと機密性を意識しがちですが、完全性や可用性にも目を向けることが重要です。特に、可用性の意識が乏しいことから、天災などにより事業が継続できないといったことがないようにしましょう。

本章『セキュリティの概要』での説明事項は、各種認証や要求事項に特化した記載ではありません。

セキュリティの3要素

機密性（Confidentiality）

許可された者だけが情報にアクセスできるようにすることです。許可されていない利用者は、コンピュータやデータベースにアクセスすることができないようにしたり、データを閲覧することはできるが書き換えることはできないようにしたりします。



完全性（Integrity）

保有する情報が正確であり、完全である状態を保持することです。情報が不正に改ざんされたり、破壊されたりしないことを指します。

可用性（Availability）

許可された者が必要なときにいつでも情報にアクセスできるようにすることです。つまり、可用性を維持するということは、情報を提供するサービスが常に動作するということを表します。

出典：総務省
「国民のためのサイバーセキュリティサイト」をもとに作成
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/business/business_executive_02.html
経済産業省
「『第３層：サイバー空間におけるつながり』の 信頼性確保に向けたセキュリティ対策検討タスクフォース の検討の方向性」 」をもとに作成
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/daisanso/pdf/001_04_00.pdf

セキュリティの付加的な4要素

企業や組織におけるセキュリティにおいて、「機密性」・「完全性」・「可用性」に加えて、「真正性」・「信頼性」・「責任追跡性」・「否認防止」と言う４要素も重要になっています。これら７要素を意識したセキュリティ対策を目指していきましょう。

セキュリティの付加的な4要素

真正性（Authenticity）

守るべき価値ある情報に対して、「本当に情報へアクセスすべき人か」を司る特性です。関係ない人が情報へアクセスしてしまうと情報漏洩やデータが破壊されるといった懸念が発生します。

信頼性（Reliability）

設定や操作が意図した通りに動くことを司る特性です。守るべき価値ある情報が保存されているサーバなどがバグや手順の不備により、意図した通りに動かない場合に、情報漏洩などの危険性があります。また、出力結果が誤った場合、情報の価値が無くなってしまいます。

責任追及性（Accountability）

守るべき価値ある情報へのアクセスについて、いつ・誰が・どこからといったように追跡できることを司る特性です。この特性により、セキュリティ事故が発生した場合にも調査が可能となります。

否認防止（non-repudiation）

守るべき価値ある情報へのアクセスや対象機器の操作などにおいて、実施した行動や作業を、事実として否定することができないようにすることを司る特性です。いわゆる証拠保全となり、誰が行ったのか、または行わなかったのかを表すことに繋がります。

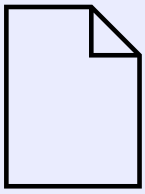
出典：経済産業省
「『第３層：サイバー空間におけるつながり』の 信頼性確保に向けたセキュリティ対策検討タスクフォース の検討の方向性」」をもとに作成
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/daisanso/pdf/001_04_00.pdf

守るべき資産とは

セキュリティにおいて、企業が守るべき価値がある情報のことを、資産と言います。

Point① 資産とは企業にとって価値ある情報

守るべき情報とは、企業にとって価値がある情報です。価値がある情報は企業によって変わるため、それぞれの会社で資産とは何かを考えることが重要になっています。



資産

情報資産の例

人に関する情報	契約・販売に関する情報	会社のシステムに関する情報
顧客の個人情報	企業間で交わした契約書	社内システムのID・パスワード
購入履歴	企業間で交わした覚書	社内システムのプログラム・OS
従業員情報	経営会議情報	社内システムのログ
マイナンバー情報	技術ノウハウや特許情報	ネットワーク機器構成図
健康診断情報	仕入れ先情報	機器管理・IPアドレス管理

Point② 守るべき資産を特定する

セキュリティをしっかりと取り組んでいくためには、守るべき資産を特定し管理していくことが重要となります。また、その資産がどこにあるのか（保存・保管されているのか）を把握することも重要です。

資産管理台帳のサンプル

NO	資産分類	情報資産名	情報管理区分	許容範囲	リスク所有者	媒体分類	保管場所
1	事業情報	名刺	秘密	個人	部門長	ドキュメント(紙)	各担当者袖机保管
2	事業情報	見積書(紙)	社外秘	部門	部門長	ドキュメント(紙)	本社鍵付きキャビネット
3	事業情報	見積書(データ)	社外秘	部門	部門長	ドキュメント(電磁記録媒体)	クラウドサービス(Office365)
4	事業情報	契約書一式(紙)	社外秘	部門	部門長	ドキュメント(紙)	本社鍵付きキャビネット
5	事業情報	契約書一式(データ)	社外秘	部門	部門長	ドキュメント(電磁記録媒体)	クラウドサービス(Office365)
6	事業情報	注文書・請書(紙)	社外秘	部門	部門長	ドキュメント(紙)	本社鍵付きキャビネット
7	事業情報	注文書・請書(データ)	社外秘	部門	部門長	ドキュメント(電磁記録媒体)	クラウドサービス(Office365)

※資産管理台帳の作成方法はDay4に行います。

Day3
1.セキュリティの概念

自社を脅かす脅威とは

セキュリティにおいて、資産を脅かすものを脅威と言います。

Point① 脅威とは

資産を脅かすものを脅威といいます。資産が各社によって変わるので、脅威も会社によって変わります。自社にとっての脅威とは何かを考えること、把握することが対策の一歩となります。

脅威

脅威の例

脅威の種類		例
環境	自然災害	火災・台風・地震・洪水・感染症、など
	障害・故障	システム障害・機器障害・ネットワーク障害、など
人間	偶発的	間違い操作・誤削除・認識違い、など
	計画的※1	システムハッキング・改ざん・盗聴・覗き見、など

※1：人間が行う計画的な脅威として『攻撃』があげらます。技術的に作成されたものやネットワーク上で行われるものを、技術的脅威と表現する場合もあります。

出典：独立行政法人情報処理推進機構（IPA）情報セキュリティ10 大脅威（各年代）
https://www.ipa.go.jp/security/vuln/10threats2022.html
総務省 「国民のためのサイバーセキュリティサイト」
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/basic/basic_risk.html
など、複数の資料をもとに作成

※脅威の把握・検討についてはDay5に行います。

One point

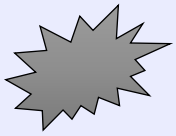
昨年順位	個人	順位	組織	昨年順位
2位	フィッシングによる個人情報等の詐取	**1位**	ランサムウェアによる被害	1位
3位	ネット上の誹謗・中傷・デマ	**2位**	標的型攻撃による機密情報の窃取	2位
4位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	**3位**	サプライチェーンの弱点を悪用した攻撃	4位
5位	クレジットカード情報の不正利用	**4位**	テレワーク等のニューノーマルな働き方を狙った攻撃	3位
1位	スマホ決済の不正利用	**5位**	内部不正による情報漏えい	6位
8位	偽警告によるインターネット詐欺	**6位**	脆弱性対策情報の公開に伴う悪用増加	10位
9位	不正アプリによるスマートフォン利用者への被害	**7位**	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	NEW
7位	インターネット上のサービスからの個人情報の窃取	**8位**	ビジネスメール詐欺による金銭被害	5位
6位	インターネットバンキングの不正利用	**9位**	予期せぬIT基盤の障害に伴う業務停止	7位
10位	インターネット上のサービスへの不正ログイン	**10位**	不注意による情報漏えい等の被害	9位

独立行政法人情報処理推進機構（IPA）では、情報セキュリティ10 大脅威を発表しています。順位が高いか低いかに関わらず、自身または組織が置かれている立場や環境を考慮して優先度を付け、適切な対応を取りましょう。ランク下位の脅威だから対策を行わなくて良いということではありません。しっかりと対策を行い、脅威が顕在化しないように取り組みましょう。

出典：独立行政法人情報処理推進機構（IPA）
情報セキュリティ10 大脅威 2022
https://www.ipa.go.jp/security/vuln/10threats2022.html

自社の弱点、脆弱性とは

資産を守るためには、まず弱点を知ることが重要です。セキュリティにおいて、この弱点のことを脆弱性と言います。



脆弱性

Point① 脆弱性に対処する

資産を保存している環境や運用ルールに潜む弱点が脆弱性です。脆弱性が現在はなくても、時間の流れとともに顕在化する場合もあります。

脆弱性の例

脆弱性の種類	例
人の脆弱性	ルールの認識不足、適切ではない権限貸与、物忘れ、など
システムの脆弱性	OSバージョン・設定・アクセス権限の不備、など
ネットワークの脆弱性	通信経路の不備、アクセスリストの不備、など
運用の脆弱性	承認プロセスの不備、確認の不備、監視の不足、など

出典：総務省
「国民のためのサイバーセキュリティサイト」をもとに作成
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/basic/basic_risk_11.html

※脆弱性の把握・検討についてはDay5に行います。

Point② サイバー攻撃に悪用される脆弱性

攻撃しようとした場合、攻撃者はシステムを調べるところから始めます。システムで利用されているOSのバージョン情報や動いているソフトウェアの情報などを偵察します。もし、システム内で動いているOSやソフトウェアに脆弱性があれば、その脆弱性をついて攻撃を行います。攻撃が成功すると、遠隔操作などが可能となります。

One point

近年、脆弱性がコンピュータウイルスや不正アクセス等の攻撃に悪用されるケースが増加しています。また、脆弱性に関する情報の公開後に、その脆弱性を狙う攻撃方法が作られ、広まるまでの期間が短くなる傾向があり、対策前にコンピュータウイルスに感染する危険性、公開サーバが攻撃され大きな被害を受ける危険性、および脆弱性を放置したことにより第三者が被害を受ける危険性も増大しています。

脆弱性については、対策がとられないまま放置されたり、対策がとられない状況で悪用可能な情報が先に公開されたりする場合の問題が指摘され、このような問題に対処するために、関係者間の適切な脆弱性に関する情報の共有と連携が強く求められています。

出典：独立行政法人情報処理推進機構（IPA）
IPA脆弱性対策コンテンツリファレンス
https://www.ipa.go.jp/files/000051352.pdf

Day3

1.セキュリティの概念

リスクとは

セキュリティでは、資産が持つ価値に対して、どのような脅威が存在しているのか、どの程度脆弱性を保有しているのかを把握すること、つまり、リスクを把握することが重要です。

国際規格（ISO/IEC31000）においてリスクとは、目的に対する**不確かさ**の**影響**とされています

不確かさとは、事象、その結果またはその起こりやすさに関する、情報、理解または知識に、たとえ部分的にでも不備がある状態をいいます。

影響とは、期待されていることから、好ましい方向または好ましくない方向に乖（かい）離することをいいます。

もっと詳しく！

- リスクは、起こり得る“事象”、“結果”、またはこれらの組合せについて述べることによって、その特徴を示すことが多いです。
- リスクは、ある“事象”（その周辺状況の変化を含む。）の結果とその発生の“起こりやすさ”との組合せとして表現されることが多いです。
- 情報セキュリティリスクは、情報セキュリティ目的に対する不確かさの影響として表現することがあります。
- 情報セキュリティリスクは、脅威が情報資産の脆弱性または情報資産グループの脆弱性に付け込み、その結果、組織に損害を与える可能性に伴って生じます。

※リスク把握・検討についてはDay5に行います。

One point

リスクとは、『目的に対する不確かさの影響』とされていますが、セキュリティにおける影響でより注意が必要なのは、好ましくない方向に乖離することです。マイナス影響を受けてしまうと、損害などが発生する可能性があります。

しかし、影響が出ないように注意しようにも、これはセキュリティに限った話ではなく、予期しない影響は必ず発生するものです。このために、『予期しない場合（想定外）を想定した対応』を検討する必要性も出てきます。

想定外の事象が発生したときにどのような対応を取ることがよいかを事前に考えておくことによって、事象が発生した際にも慌てずに対処ができます。難しいのは、どの対処を想定して準備しておけばよいのかということです。

残念ながらこの答えの正解は一つではありません。企業がそれぞれ違うように、答えもそれぞれ違います。まずは、自社の守るべき資産を把握し、脅威や脆弱性を理解し、対策を検討していきましょう。

リスクの考え方

セキュリティにおけるリスクは計算式で把握していきます。まずは、各資産においてどの程度のリスクの可能性があるのかを把握できるようにしていきましょう。

リスクを算出する計算式

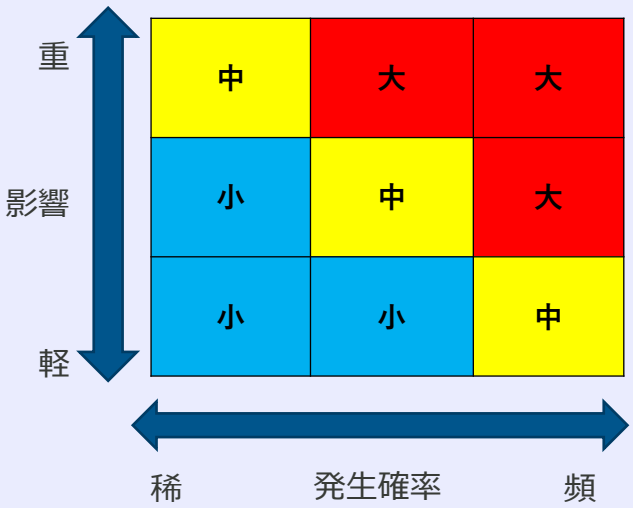
リスク = 資産価値 × 脅威 × 脆弱性 × 発生可能性

資産価値：資産が持っている、自社にとっての価値
脅威：資産を脅かすもの
脆弱性：資産を保存している環境や運用ルールに潜む弱点
発生可能性：損失を発生させる可能性

※リスク把握・検討についてはDay５・Day6に行います。

Point① リスク評価

リスクの計算式で算出した結果を評価していく必要があります。計算結果で算出された数値をもとに、リスクが高い・低いを判断し、高いものから対処していくことが一般的です。



また、簡易的な方法として、マトリックスに照らし合わせた評価方法もあります。

縦軸に影響、横軸に発生確率を置きます。

<u>影響</u>
重：会社の存続に影響するような大きな損失
中：事業の存続に影響するような大きな損失
軽：業務へ影響するような損失

<u>発生確率</u>
頻：常態的に頻発することが想定される
中：時々、発生することが想定される
稀：発生の可能性を排除できない

リスクの計算式とマトリックスを組み合わせて、各資産のリスクを把握する癖をつけることで、何からセキュリティ対応を進めていけばよいのかを判断することができます。影響度が大きく、発生確率が高いリスクに対して早急に対応を進める必要があります。優先順位付けを行い、より危険性が高いものから対応をしていきましょう。

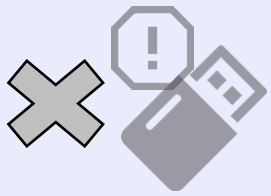
リスク対応策

リスク評価が完了したら、リスクに対して対応策を考えなくてはいけません。リスク対応策は大きく４つに分けられます。

①リスク回避

仕事のやり方を変える、情報システムの利用方法を変えるなどして、想定されるリスクそのものをなくします。

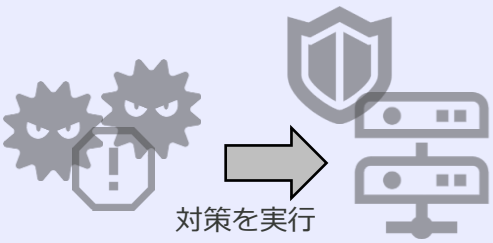
例えば、従来は商品の発送先である住所や氏名などの個人情報を発送完了後もパソコンに保存し続けていたが、保存中の漏えいを避けるために、利用後はすぐに消去する、インターネットバンキングに使用するパソコンでメールやウェブ閲覧をしていたが、ウイルスに感染しないようにインターネットバンキング専用のパソコンを設置し、ウイルス感染の原因となるメールやウェブ閲覧に利用せず、USBメモリ、外付けHDDも接続を禁止する、などがあります。



リスクがあるものは持たない

②リスク低減

自社で実行できる情報セキュリティ対策を導入ないし強化することで、脆弱性を改善し、事故が起きる可能性を下げます。



対策を実行

③リスク転嫁

自社よりも有効な対策を行っている、あるいは保証能力がある他社のサービスを利用することで自社の負担を下げます。

例えば、商品を販売するウェブサイトではクレジットカード番号を非保持化し、セキュリティ対策を十分に行っている外部の決済代行サービスに決済業務を委託する、社内のサーバで運用していた業務システムをセキュリティ対策の充実した外部クラウドサービスに移行する、情報漏えい、システム障害などの事故発生に伴う損失に対して保険金が支払われる情報セキュリティに関連した保険商品に加入する、などがあります。

自社　他社へリスクを負担してもらう　他社

④リスク受容

事故が発生しても受容できる、あるいは対策に係る費用が損害額を上回る場合などは対策を講じず、現状を維持します。

リスクを受け入れる

出典：独立行政法人情報処理推進機構（IPA）
中小企業の情報セキュリティ対策ガイドライン第3版
https://www.ipa.go.jp/files/000055520.pdf

One point

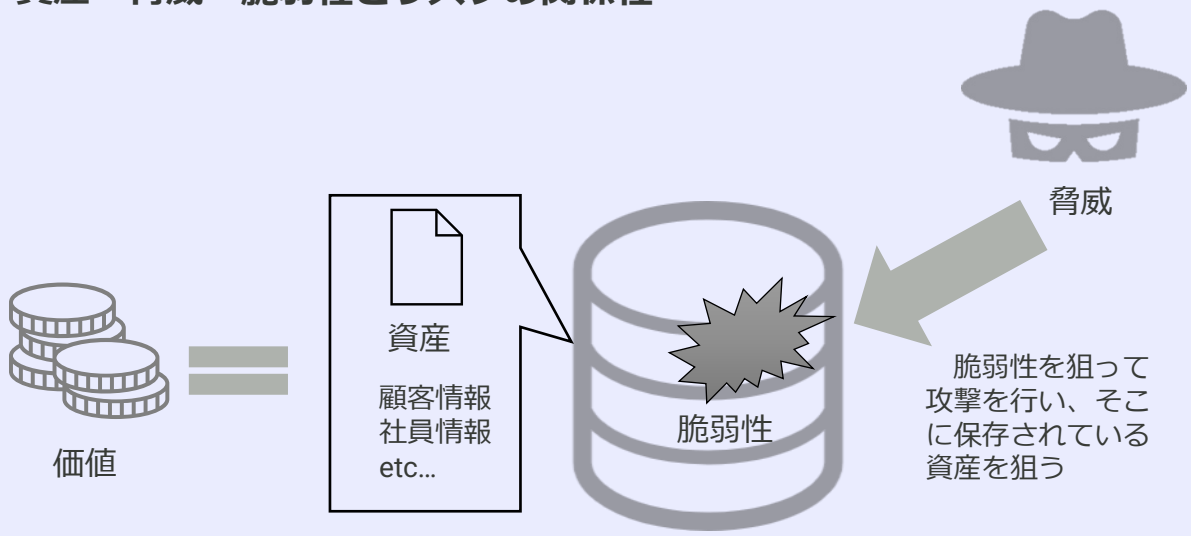
リスク対応において一番に思いつくのは低減策の実行です。セキュリティ対策の多くはリスク低減策を実行するものとなります。低減策として、どの程度リスクに対して対応を行うのかを考えることが重要です。

また、リスクをゼロにすることはできません。最終的には、リスクに対して受容をする必要があります。

資産・脅威・脆弱性とリスク

資産価値を変えることはできませんが、そもそもその資産が必要なものかを検討することはできます。過剰な資産を持たない、取得しないということもリスク回避の方法です。

資産・脅威・脆弱性とリスクの関係性



リスク = 資産価値 × 脅威 × 脆弱性 × 発生可能性

どんなに脅威、脆弱性、発生可能性が高くても、資産価値が無ければリスクにはなりえません。逆に、どんなに資産価値が高くても、発生可能性が無ければリスクにはなりえません。これらの計算値においてリスク対応をしていくことが重要です。

資産価値	すぐには変わらない特性があり、企業活動を維持するためには、資産を破棄することは難しい。ただし、不要な資産を持つと流出リスクを高める結果となる。
脅威	自社で影響を少なくすることは難しく、脅威は存在すると思って対策を立てる必要がある。
脆弱性	自社に存在する脆弱性のため、自社の対応により少なくすることができる。この脆弱性を少なくする行為がリスク低減策の一つとなる。ただし、時間とともに脆弱性が変わる、新たに発見されるケースがあるため、定期的な見直しが必要である。
発生可能性	損害等が起こる発生の可能性。外部からの攻撃だけでなく、社内での紛失なども考慮する必要がある。 発生の可能性を減らすこともリスク低減策の一つである。

ミニワーク
～振り返ってみよう～

ミニワークテーマ

リスクについて考えましょう。
回避した事例、転嫁した事例、低減した事例、受容した事例

どのような事例があるかを思い起こして書いてみましょう。

回避した事例

転嫁した事例

低減した事例

受容した事例

サイバーセキュリティフレームワーク①

セキュリティの状況を整理するためには、フレームワークを活用すると便利です。今回はNIST（米国国立標準技術研究所）のサイバーセキュリティフレームワーク(CSF)を紹介します。業界や組織の規模を問わず、サイバーセキュリティ対策の指針として利用できるフレームワークです。なお、本フレームワークでは、「サイバーセキュリティ経営ガイドライン Ver 2.0　付録A サイバーセキュリティ経営チェックシート」においても対応関係が提示されています。

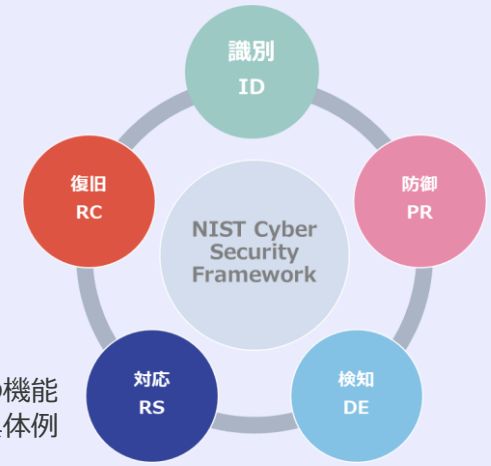
※セキュリティには、サイバーセキュリティフレームワークだけでなく、それぞれ特徴を持ったフレームワークが存在します。従来のセキュリティ対策関連の資料は、ISMSのフレームワークをベースにしてきたものが多かったですが、現在ではCSFを意識した対策が普及しつつあります。自社に一番合ったものや取得したい認証に合わせた利用を考えてください。

フレームワークを構成する3つの要素

フレームワークコア

セキュリティ対策を検討する際に、組織に不足している対策を明確にし、必要なツールを導入するための指針となるものです。「識別(特定)（Identify）」、「防御（Protect）、「検知（Detect）」、「対応（Respond）」、「復旧（Recover）」という5つのコア機能と、23のカテゴリーで構成されています。

コア機能：業種・業態を問わないサイバーセキュリティ対策の機能
カテゴリー：サイバーセキュリティ対策として取り組むべき具体例



フレームワークインプリメンテーションティア

組織のサイバーセキュリティ対策のレベルを評価する基準を示すものです。「ティア1（部分的である）」から、「ティア4（適応している）」の4段階に分かれており、組織が置かれている状況等から総合的に判断します。

ティア	定義の概要
ティア1: 部分的である	場当たり的に対処されている状態
ティア2: リスク情報を活用している	意識はあるが、リスクを管理するための組織全体にわたる取り組みは定められていない状態
ティア3: 繰り返し適用可能である	一貫した手法が存在しており、知識とスキルを持っている状態
ティア4: 適応している	自組織において適切なセキュリティ運用・体制・ルールが確立している状態

フレームワークプロファイル

組織のサイバーセキュリティ対策の現状（As-IS）と、あるべき姿（To-Be）を比較することにより、サイバーセキュリティ対策を改善する機会を識別するために使用するものです。
あるべき姿は会社によって違いがあります。しっかりと考えていくポイントです。

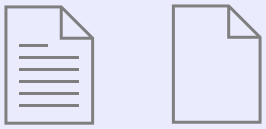
出典：National Institute of Standards and Technology
「Framework for Improving Critical Infrastructure Cybersecurityv1.1」をもとに作成
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

サイバーセキュリティフレームワーク②

サイバーセキュリティフレームワーク(CSF) は5つのコア機能と、23のカテゴリーで構成されます。まずは、 5つのコア機能を中心としてセキュリティの検討ができるように取り組みましょう。

識別(特定)： セキュリティ対策が必要なリソースを明確にする

システム、人、資産、データ、機能に対するサイバーセキュリティリスクの管理に必要な理解を深めます。組織はビジネスを取り巻く状況、重要な機能を支える資源、関連するサイバーセキュリティリスクを理解することで、組織が取り組むべき対象を絞って、優先順位付けを行うことを可能にします。

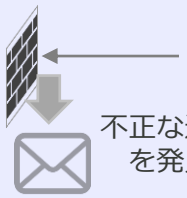


防御： ルールを策定しセキュリティリスクをコントロールする

重要サービスの提供を確実にするための適切な保護対策を検討し、実施します。大きな特徴は、発生する可能性のあるセキュリティ事故がもたらす影響を抑制することです。セキュリティ対策などで一番考えられる部分が防御であり、脅威の影響を防ぎます。

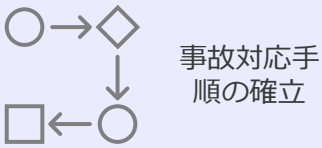
検知： 事故の発生を即時に把握するための仕組みをつくる

セキュリティ事故の発生を識別するのに適した対策を検討し、実施します。セキュリティ事故のタイムリーな発見を可能にします。



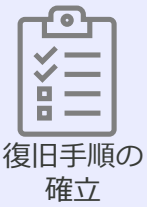
対応： 事故に対する対策を用意する

検知されたセキュリティ事故に対処するための適切な対策を検討し、実施します。発生する可能性のあるセキュリティ事故がもたらす影響を封じ込めることを支援します。



復旧： システムを正常な状態に戻すための必要なタスクを明確にする

復旧を実現するための計画を策定・維持し、セキュリティ事故によって阻害されたあらゆる機能やサービスを元に戻すための適切な対策を検討し、実施します。セキュリティ事故がもたらす影響を軽減するために、通常の運用状態へタイムリーに復旧するのを支援します。



One point

NISTとは、National Institute of Standards and Technologyの略で「米国国立標準技術研究所」という機関です。NISTではセキュリティに関するガイドラインを多く発表しています。その中の代表的なものに、NIST SP800-171というものがあります。「NIST SP800-171」 というガイドラインは、アメリカ政府が基準への準拠を求めたもので、14種類のセキュリティ要件に分けています。この要件に見合わないと、政府の調達基準を満たさないということになります。このため、アメリカ政府とビジネスを行うためには、 NIST SP800-171を遵守する必要があります。

インシデントが発生した時の対応方法①

インシデントとは、「事件」「出来事」といった意味をもった言葉で、情報セキュリティの世界では、システムの運用におけるセキュリティ上の問題として捉えられる事象、（これらに繋がる可能性のある事象を含みます）を意味します。
セキュリティ対策の主要な目的は、インシデントによるビジネスへの悪影響を極小化することにあります。しかし、適切な対策を実施したとしても、インシデントの発生を100%なくすことはできません。したがって、インシデントが発生した場合、事後的な対応、つまり、その被害を抑え、迅速な復旧・回復を図るための各種対応も必要となります。

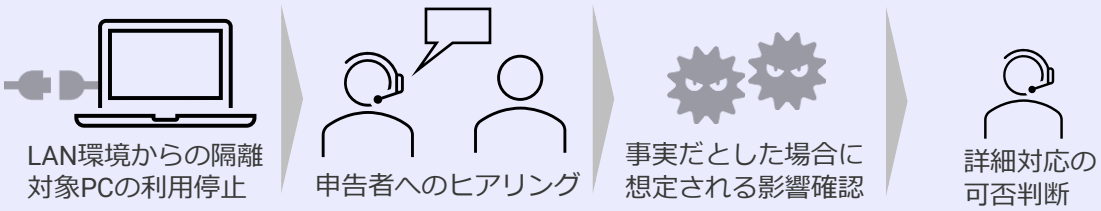
出典：日本ネットワークセキュリティ協会（JNSA） インシデント被害調査WG
インシデント損害額調査レポート
https://www.jnsa.org/result/incidentdamage/data/incidentdamage_20210910.pdf

現在では、インシデントが起こらないと考えることは現実的ではなく、対応（事故に対する対策を用意する）、復旧（システムを正常な状態に戻すための必要なタスクを明確にする）まで考慮したセキュリティ対策が求められています。そのため、インシデント対応フローを事前に準備しておくことが重要です。

インシデント対応フローの例

検知／連絡受付
インシデントの可能性は 社内 または 外部の企業・機関 より連絡を受けます。

トリアージ （優先順位付け）
連絡を受けた情報を基に、事実確認と対応すべき事案かを検討します。

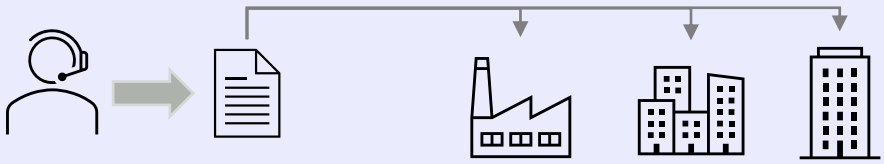


インシデントレスポンス(対応)
トリアージの結果対応すべきとなったものについて対処していきます。

インシデントが発生した時の対応方法②

報告／情報公開

関係省庁、申告者、お客様への情報公開範囲を決定します



対応・復旧

事業継続のための暫定対策の実施、復旧作業を行います。

対策の立案

再発防止のための対策案を検討します。

出典：一般社団法人JPCERTコーディネーションセンター
「インシデントハンドリングマニュアル」をもとに作成
https://www.jpcert.or.jp/csirt_material/files/manual_ver1.0_20211130.pdf

One point

インシデントを起こさないようにセキュリティ対策をすることは大切です。しかしながら、セキュリティインシデントが起こる可能性をゼロにすることはできません。そのため、インシデントが発生した場合を考えて対応を準備しておくことが重要になります。

インシデントが起こってから、体制整備や対応手順の確認を始めるとその分だけインシデント収束までの時間がかかります。インシデント発生時にすぐに対応を開始できるように準備しておくことは、日ごろの避難訓練や防災訓練と同じような意味合いとなります。

避難訓練や防災訓練の日があるように、インシデント対応訓練の日というサイバー演習を設ける企業も増えています。全社サイバーセキュリティ訓練日を設けてみませんか？

対応が後手になったインシデント対応	理想のインシデント対応
	体制整備
	対応手順確認
インシデント発生	
体制整備	インシデント対応
対応手順確認	インシデント収束
インシデント対応	
インシデント収束	

時間の流れ

セキュリティ対策の種類①

情報セキュリティ対策は、情報を取り扱う過程全てにおいて取り組む必要があります。すなわち、技術、人、組織、物理の4領域の各々において、確実に実施されなければなりません。その全てがうまく機能して情報セキュリティを守ることで、初めて整合性の取れた情報セキュリティ対策が実現するといえます。

組織的対策

企業や組織が適切な情報セキュリティを維持できるように、行うべき対策です。

対応内容
・セキュリティ運用指針の策定、計画立案
・セキュリティ管理体制の構築

対応及び対応結果
・情報セキュリティの運用指針を定めた文書(規程)
・セキュリティ管理体制の組織化
・現状のセキュリティレベルの可視化

人的対策

従業員がセキュリティ事故を起こさないように、ルールの浸透やセキュリティ管理の重要性を理解する対策です。

対応内容
・ルールや規約の内容を浸透させる啓発活動
・攻撃に備えたトレーニング活動

対応及び対応結果
・啓発活動に伴う、ルールや規約の浸透
・トレーニングによる、セキュリティ意識強化

One point

企業で実施しているセキュリティ対策状況を可視化できるようにして、定期的にチェックすることは大切です。独立行政法人情報処理推進機構（IPA）は、情報セキュリティレベルの診断や、経営可視化ツールを公開しています。設問に回答していくだけでセキュリティ対策のセルフチェックができるので、上手に活用しましょう。

5分でできる！自社診断
https://security-shien.ipa.go.jp/diagnosis/selfcheck/index.html

情報セキュリティ対策ベンチマーク
https://security-shien.ipa.go.jp/diagnosis/benchmark/index.html?bm_id=1

サイバーセキュリティ経営可視化ツール
https://security-shien.ipa.go.jp/diagnosis/benchmark/index.html?bm_id=2

セキュリティ対策の種類②

技術的対策

ネットワークやサーバ、PCなどの機器、保存されているデータを守るための対策です。

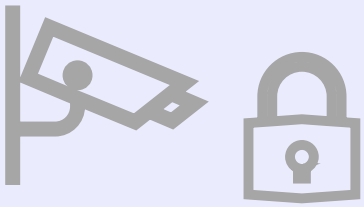
対応内容
・PCのウイルス対策ソフトを導入
・ファイアウォールの導入

対応及び対応結果
・各種セキュリティ強化製品、サービスの導入

物理的対策

紙やUSB、パソコンなどの紛失から情報流出を防ぐための対策です。

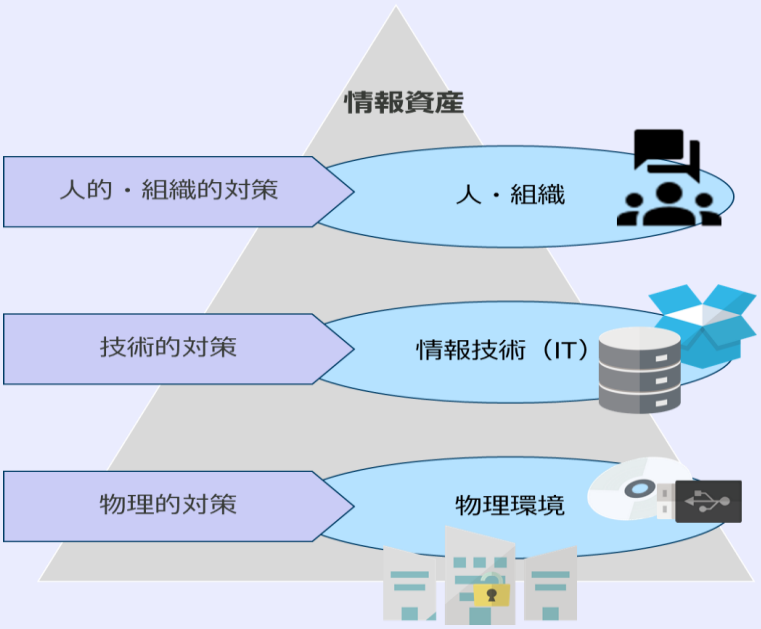
対応内容
・USBなどによる情報持ち出しの禁止通達
・個人情報の持ち出しに対する記録の取得
・監視カメラを設置



対応及び対応結果
・セキュリティ区画の制定
・防犯対策の実施（鍵の交換、保存場所の適切化）

※対策の検討についてはDay7.8に行います。

技術、人、組織、物理の4領域はマイナンバーガイドラインにも記載されています。
個人情報保護委員会『マイナンバーガイドライン入門 （事業者編）』
（https://www.ppc.go.jp/files/pdf/my_number_introduction_jigyosha.pdf）

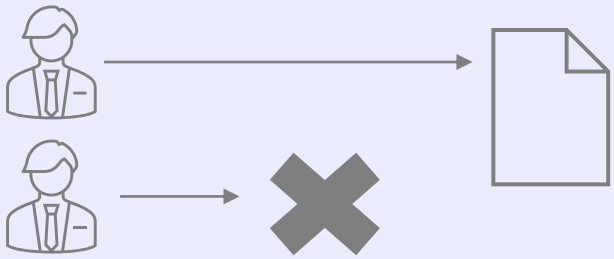


意識する３つの特性

セキュリティの考え方にはNeed-To-Know（知る必要性）、Least Privilege（最小権限）、Separation of Duties（職務分掌）という、3つの特性があります。各資産においてリスク分析をする中で、公開してよい情報か、開示の範囲を制限すべき情報かを考えることが重要になっています。 DXの時代において情報をオープンにしていくという考え方もあります。情報の公開範囲の検討が重要です。

①Need-To-Know（知る必要性）

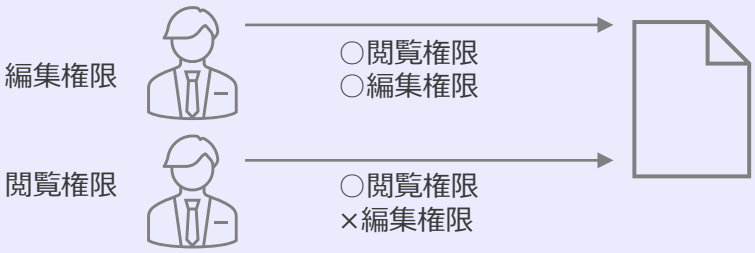
対象の情報を誰に開示するかを取り決め、開示範囲を制限することです。



情報が誰でも見られるものでないということは、開示範囲が設けられるということです。その情報を知る必要がない者にまでアクセス権を付与してしまうと、情報漏えいリスクを不必要に高めてしまうこととなります。

②Least Privilege（最小権限）

場面に応じて必要最小限の権限だけを与えるようにすることです。



同じ情報にアクセスする人でも、アクセス目的は異なります。編集が必要ならば編集権限を付与しますが、閲覧が目的の場合には閲覧権限のみを付与します。閲覧のみを行う人に、編集権限を付与することは過剰権限となり、リスクを高めることになります。

③Separation of Duties（職務分掌）

役職や個人の取り組む内容を明確にし、監視や監督を行い不正などを未然に防ぐことを目的としています。

編集などの業務を執行する人と変更確認の承認者を分けることで不正を抑止する効果が見込めます。

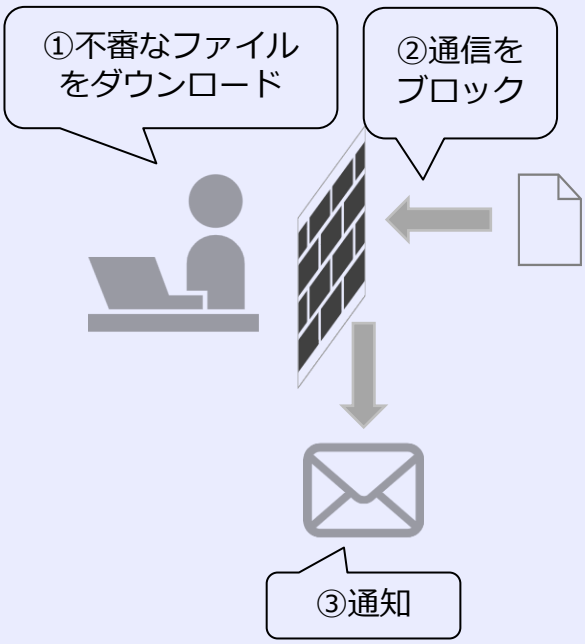
セキュリティ対策の具体例
～防御から検知へ～

検知を重視しセキュリティインシデントの早期収束を

ある企業では、セキュリティインシデントゼロを目指していました。「ウイルス感染をしないように」、「フィッシングサイトにアクセスしないように」ということを意識し、従業員へも意識啓発を行っていました。

もちろんインシデントにあわないようにすることは重要です。しかし、最近の攻撃は巧妙化しています。従業員の中には、影響が出ていないからという理由で、報告をしない人も出ていたということでした。怒られるという心理状態から、「隠す」ということをしてしまうと、セキュリティインシデント発生がわからなくなってしまいます。

そこで、「ウイルス感染をしないように」、「フィッシングサイトにアクセスしないように」という考えから、「情報を流出させない」、「事業をセキュリティ起因で止めない」というように考えを改めました。仮にウイルス感染をしたとしても、情報が流出しなければお客様はじめ従業員が被害にあう可能性は限りなく低くなります。また、事業が止まらなければ、売上への影響も大きな問題にはなりません。



これを実現するためには、検知の仕組みをより強化する必要がありました。例えば通信の検知を強化し、「会社とは関係ないクラウドへのファイルのアップロードが無いか」、「ファイルへのアクセスは適切に行われているか」を把握することに成功しました。イレギュラーな通信が発生するとアラームが上がり、調査をすることができ、初動対応が早くなりました。

また、検知としては従業員からの報告も重視しました。報告を受ける側にも怒らないようにすることを求めました。「情報を流出させない」、「事業をセキュリティ起因で止めない」という目的のため、インシデントの可能性がある場合には報告するように従業員に啓発しています。セキュリティインシデントゼロ時代の意識や、何を報告すべきなのかという悩みが完全には解決できていませんが、現在この改善に向けて取り組んでいます。

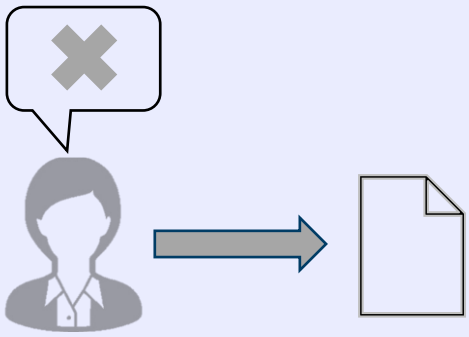
「セキュリティインシデントは起こっていません」と自信をもって言うことはできますか？実はインシデントが発生しているのに気づいていないだけということはないでしょうか？インシデントが起こったときに気付けるようにしておくこともセキュリティ対策では重要です。

セキュリティ対策の具体例
～技術的対策を活用～

技術的対策で人的ミスを削減

組織的対策、人的対策、物理的対策、技術的対策の4つは完全に切り離すことはできません。例えば、パスワードを使った認証などは技術的な対策と考えることができます。しかし、パスワードを利用する人からの流出をしないように強化するのは、人的対策ということもできます。

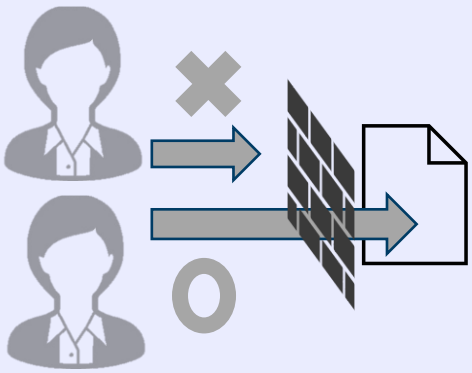
ある企業では、人的な対策を中心に対応を進めていました。人的対策は技術的対策に比べてシステムに関する費用が掛からないといった点にメリットがあります。しかしながら、人の入れ替わりやルールの認識間違い、うっかりミスなどによるヒヤリハットは少なくなりませんでした。



本来ならアクセスしてはならないがアクセスしてしまった

そこで、一部を技術的対策に変えていきました。技術的対策では初期投資こそかかりましたが、決まったルールをシステマチックに実施できます。ルールを知らない人が間違いを犯すことや、うっかりミスが減少し、人的対策をしていたころに比べて、セキュリティにかける対応の時間が減り、減った時間でセキュリティ計画を立てたりと、未来にかける時間が増えてきました。

現在では、セキュリティ対策は技術的な対策を優先的に考え、それを補完する形で人的対策を導入しています。



しかしながら、技術的対策が万能というわけではありません。だんだんと時間がたってくると、アクセス権限の見直しがされず、本来ならアクセスすべきでない部署異動した人にアクセス権限があるという状態になりました。本来なら知る必要性がない情報を知ることになり、情報流出等の危険性が増すことになります。

そこで、定期的な見直しや異動時のアクセス権限のルールなどを定めました。最初はセキュリティ担当者が人事異動の情報をもとに設定を直していましたが、タイムリーに対応をすることは難しく、権限変更まで時間がかかってしまいました。そこで、異動に伴うアクセス権の削除は異動前の役職者が担当し、アクセス権の付与は異動後の役職者の権限で行えるようにしました。セキュリティ担当者は正しいアクセス権となっているか、イレギュラーなアクセス権があった場合に役職者に確認する対応をすることで、現在ではチェックの機能も働き、適切な運用となっています。

このように、取り組みを進めることで新たな課題が出てくることはあります。新たな課題に対して対処していくため、PDCAを回していくことで成長につながっていきます。

ミニワーク
～振り返ってみよう～

ミニワークテーマ

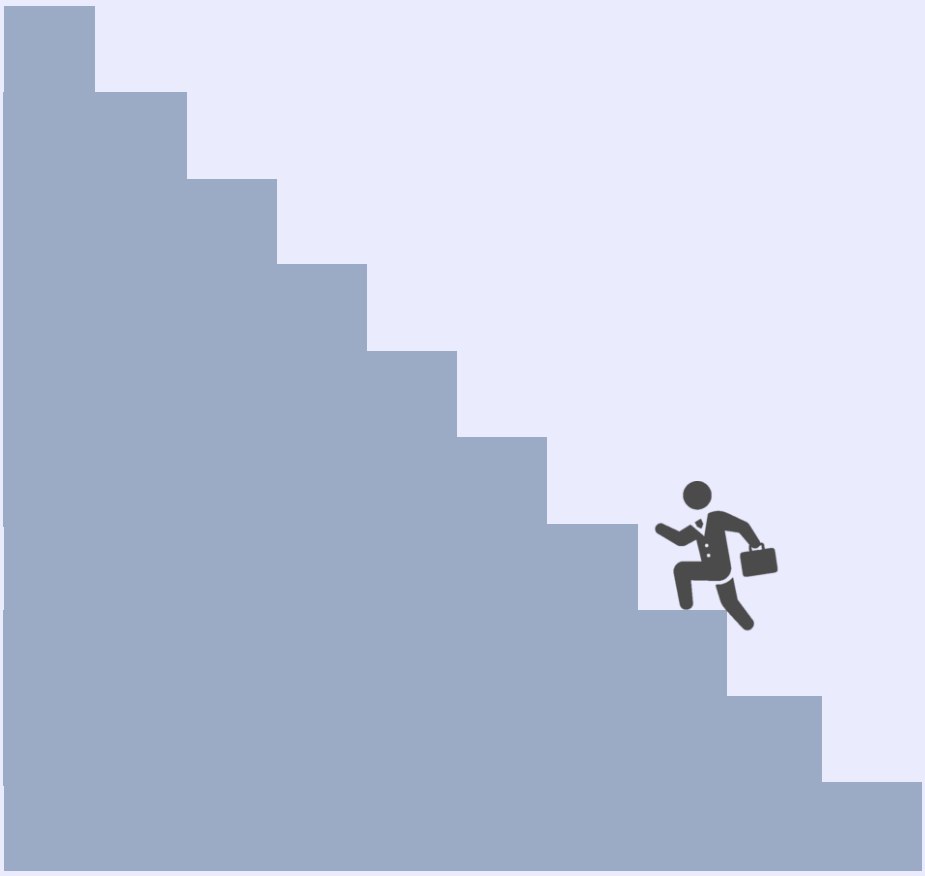
自社にとっての最悪の事態とは何かを考えましょう！

最悪な事態が起こってしまった際には会社にとって大きな影響が出ます。最悪な事態を想定し、最悪な事態が起こらないようにしましょう。

セキュリティの概要を知ると、本当に自分でできるのと不安になる・・・覚えることも多いし、今後より詳細な手法や手段も覚えていかないといけない。一つ一つ実践も交えながら、取り組んでいこう。

サイバーセキュリティフレームワークでうちの会社のセキュリティを振り返ってみると、防御ばかりに気を取られて、検知について考えられていないことがよく分かった。それどころか、セキュリティ対策が必要な守るべき資産について、すべてを把握できていないんじゃないだろうか。もしかしたら、自分が知らない資産だってあるかもしれない。システム管理者が把握していない公開サービスもあるかもしれない。
まずは、しっかりと資産や脅威、脆弱性を把握できるようにしていこう。そして、インシデントが起こった後の対応方法ばかり意識するのではなく、インシデントを未然に防ぐセキュリティ対策も考えていこう。

セキュリティを知る手段を学ぶ



コラム
～入口・内部・出口対策～

セキュリティ対策というと一昔前までは入口対策が主流でした。入口対策とはどのような攻撃を受けても侵入されないようにすることを目指したものです。しかしながら外部から入ってくる通信を止めることには限界があります。特に最近では、テレワークなどの関係で社外から社内へアクセスする機会も増えています。また、標的型メールのような攻撃を完全に防ぐことは不可能といえます。

そのため現在では、内部対策や出口対策にも重きを置く必要があります。現在のセキュリティにおいてよく聞くゼロトラストというキーワードも内部対策や出口対策を考慮したものです。

内部対策で主流といえるのがログ監視です。誰がアクセスしているのかなどを監視することで、異常にいち早く気づくことができます。また、最近は情報を暗号化する対策も増えてきています。情報を暗号化しておくことで、仮に流出したとしても、解読できない状態にしておくといった対策です。

出口対策は、内部から外部の通信を監視するなどで情報の持ち出し・流出を検知します。また、不正なサイトへのアクセスなどを監視することで被害を抑える効果があります。

現在のセキュリティ対策を考えるときには技術、人、組織、物理というカテゴリー軸の対策と合わせて、通信の流れなどを意識した時間軸での入口・内部・出口の対策も考えてみてはいかがでしょうか？

あとがき

いよいよ本格的にセキュリティの話に入ってきました。聞きなれない言葉や馴染みがない単語も多く出てきたのではないでしょうか？特にDay 3 はセキュリティの概要や基礎をテーマとしました。今後リスク分析の手法など、より詳細に取り組んでいくこととなります。

今回特に思ったのは、セキュリティと一言で言っても、人によっていろいろな解釈や考えがあるのだなということです。会社のことを理解し、会社に寄り添ったセキュリティの支援ができる人と出会えることは非常に貴重なことだと感じます。ぜひそのような人と出会った場合には、出会いを大切にし、セキュリティの取り組み強化に向けて加速してください！

サイバーセキュリティフレームワーク参考資料

識別 (ID)		ティア 1 部分的である （Partial） 場当たり的、属人的である	ティア 2 リスク情報を活用している （Risk Informed） 初期プロセスが整備されている	ティア 3 繰り返し適用可能である （Repeatable） プロセスが継続的に回っている	ティア 4 適応している （Adaptive） プロセス自身の継続的改善に努めている
資産管理（ID.AM） 自組織が事業目的を達成することを可能にするデータ、人員、デバイス、システム、施設が、識別され、組織の目的と自組織のリスク戦略における相対的な重要性に応じて管理されている。		適用範囲における自組織の資産の一部のみ目録化（台帳管理）しているが、大部分は記憶や慣習において管理している。	適用範囲における自組織の資産は目録化（台帳管理）にて、管理している。	適用範囲における目録（台帳管理）を定期的に更新している.	適用範囲における目録（台帳管理）が定期的に更新されており、より良い管理に向けて、効率化や最適化の検討を行なっている。
ID.AM-1:	自組織内の物理デバイスとシステムが、目録作成されている。	☐	☐	☐	☐
ID.AM-2:	自組織内のソフトウェアプラットフォームとアプリケーションが、目録作成されている。	☐	☐	☐	☐
ID.AM-3:	組織内の通信とデータフロー図が、作成されている。	☐	☐	☐	☐
ID.AM-4:	外部情報システムが、カタログ作成されている。	☐	☐	☐	☐
ID.AM-5:	リソース（例:ハードウェア、デバイス、データ、時間、人員、ソフトウェア）が、それらの分類、重要度、ビジネス上の価値に基づいて優先順位付けられている。	☐	☐	☐	☐
ID.AM-6:	全労働力と利害関係にある第三者（例:サプライヤー、顧客、パートナー）に対してのサイバーセキュリティ上の役割と責任が、定められている。	☐	☐	☐	☐
ビジネス環境（ID.BE） 自組織のミッション、目標、利害関係者、活動が、理解され、優先順位付けが行われている。この情報は、サイバーセキュリティ上の役割、責任、リスクマネジメント上の意思決定を伝えるために使用されている。		従業員に対して、会社が目指すミッションや目標の伝達方法が曖昧となっている。そのため、役割、責任、リスクマネジメント上の意思決定も曖昧なまま活動している。	従業員に対して、会社が目指すミッションやビジョン・目標が伝達され、従業員も理解した上で、役割、責任、リスクマネジメント上の意思決定が行われている。	従業員は、会社が目指すミッションやビジョン・目標に従って行動や判断を行なえるように周知などの機会を定期的に用意するよう努め、役割、責任、リスクマネジメント上の意思決定に最新の情報が使用されている	組織は時勢に合わせたミッションやビジョン・目標を立案し、従業員が知る機会やアップデートする機会をもうけ、役割、責任、リスクマネジメント上の意思決定に最新の情報が使用されている。
ID.BE-1:	サプライチェーンにおける自組織の役割が、識別され、周知されている。	☐	☐	☐	☐
ID.BE-2:	重要インフラとその産業分野における自組織の位置付けが、識別され、周知されている。	☐	☐	☐	☐
ID.BE-3:	組織のミッション、目標、活動の優先順位が、定められ、周知されている。	☐	☐	☐	☐
ID.BE-4:	重要サービスを提供する上での依存関係と重要な機能が、定められている。	☐	☐	☐	☐
ID.BE-5:	重要サービスの提供を支援するレジリエンスに関する要求事項が、すべてのオペレーション状況（例：脅迫・攻撃下、復旧時通常時等）について定められている。	☐	☐	☐	☐

識別 (ID)		ティア 1 部分的である (Partial) 場当たり的、属人的である	ティア 2 リスク情報を活用している (Risk Informed) 初期プロセスが整備されている	ティア 3 繰り返し適用可能である (Repeatable) プロセスが継続的に回っている	ティア 4 適応している (Adaptive) プロセス自身の継続的改善に努めている
ガバナンス（ID.GV） 自組織に対する規制、法律、リスク、環境、運用上の要求事項を、管理し、モニタリングするためのポリシー、手順、プロセスが理解されており、経営層にサイバーセキュリティリスクについて伝えている。		組織のポリシー・手順・プロセスが策定されていない（または制定されていても認識されていない）ため、それぞれの思う方法で対応している。	組織のポリシー・手順・プロセスが策定されており、作成されたポリシー・手順・プロセスに則った方法で対応している。	組織のポリシー・手順・プロセスの見直しを定期的に行なっている。	組織のポリシー・手順・プロセスが現場の声を反映し、組織が目指す理想の姿の実現に向けた最適な方法となるように検討している。
ID.GV-1:	組織のサイバーセキュリティポリシーが、定められ、周知されている。	☐	☐	☐	☐
ID.GV-2:	サイバーセキュリティ上の役割と責任が、内部の担当者と外部パートナーとで調整・連携されている。	☐	☐	☐	☐
ID.GV-3:	プライバシーや人権に関する義務を含む、サイバーセキュリティに関する法規制上の要求事項が、理解され、管理されている。	☐	☐	☐	☐
ID.GV-4:	ガバナンスとリスクマネジメントプロセスが、サイバーセキュリティリスクに対処している。	☐	☐	☐	☐
リスクアセスメント（ID.RA） 自組織は、（ミッション、機能、イメージ、評判を含む）組織の業務、組織の資産、個人に対するサイバーセキュリティリスクを把握している。		適用範囲において組織の資産が網羅的に特定できていないため、守る対象や想定される脅威、脆弱性が一部のみで判断している。適用範囲に対して組織の資産は特定できているが、脆弱性や脅威の想定・把握が部分的となっており、リスクアセスメントの結果にばらつきが発生している。	適用範囲において組織の資産が網羅され、脅威・脆弱性の情報が管理されており、リスクアセスメントの結果リスクを把握している。資産の洗いだし方法や脅威・脆弱性の収集方法が文書化され管理されている。	資産の洗いだし方法や脅威・脆弱性の収集が文書化された方法で実施され、資産に対してリスクアセスメントが定期的に実行されている。	資産の洗いだし方法や脅威・脆弱性の収集をより良い方法となるように文書の見直しが行われ、情報を能動的に取得するとともに、システムの入れ替え等が発生した場合にも早期に必要な情報が収集できている
ID.RA-1:	資産の脆弱性が、識別され、文書化されている。	☐	☐	☐	☐
ID.RA-2:	サイバー脅威に関する情報が、複数の情報共有フォーラムおよび複数のソースから入手されている。	☐	☐	☐	☐
ID.RA-3:	内部および外部からの脅威が、識別され、文書化されている。	☐	☐	☐	☐
ID.RA-4:	ビジネスに対する潜在的な影響とその発生可能性が、識別されている。	☐	☐	☐	☐
ID.RA-5:	脅威、脆弱性、発生可能性、影響が、リスクを判断する際に使用されている。	☐	☐	☐	☐
ID.RA-6:	リスク対応が、識別され、優先順位付けされている。	☐	☐	☐	☐
リスクマネジメント戦略（ID.RM） 自組織の優先順位、制約、リスク許容度、想定が、定められ、運用リスクに対する意思決定を支援するために利用されている。		リスクの管理方法や許容度の指標が策定されていない（または制定されていても認識されていない）ため、それぞれの思う方法で判断・対応している。	リスクの管理方法や許容度の指標が定まっており、判断材料として活用されている。	同等事業の中でリスク管理方法を活用し、運用リスクの判断を行なっている。	組織の社会的地位の変化や、提供サービスの変化、DXを見据えた変化においても、現行のリスク管理プロセスを参考として、新事業や新システム導入などの変化に対応しリスク管理プロセスを実行している。
ID.RM-1:	リスクマネジメントプロセスが、組織の利害関係者によって定められ、管理され、承認されている。	☐	☐	☐	☐
ID.RM-2:	組織のリスク許容度が、決定され、明確に表現されている。	☐	☐	☐	☐
ID.RM-3:	自組織によるリスク許容度の決定が、重要インフラにおける組織の役割と、その分野に特化したリスク分析の結果に基づいて行われている。	☐	☐	☐	☐

識別 (ID)		ティア 1 部分的である (Partial) 場当たり的、属人的である	ティア 2 リスク情報を活用している (Risk Informed) 初期プロセスが整備されている	ティア 3 繰り返し適用可能である (Repeatable) プロセスが継続的に回っている	ティア 4 適応している (Adaptive) プロセス自身の継続的改善に努めている
サプライチェーンリスクマネジメント （ID.SC） 自組織の優先順位、制約、リスク許容度、想定が、定められ、サプライチェーンリスクマネジメントに関連するリスクに対する意思決定を支援するために利用されている。自組織は、サプライチェーンリスクを識別し、分析・評価し、管理するためのプロセスを定め、実装している。		自組織・利害関係者双方がセキュリティに対しての意識が低く、サプライチェーンとしてのセキュリティに対して担当者依存となっている。	自組織・利害関係者双方がセキュリティに対しての意識を持ち、必要な確認作業などに協力している。	サプライチェーンに加わることに対してセキュリティの取り組みを理解し、協力しあえる利害関係者を選定している。	サプライチェーンの安全性を高めるために日頃から協力しあい、啓発活動などを連携している。
ID.SC-1:	サイバーサプライチェーンのリスクマネジメントプロセスが、組織の利害関係者によって、識別され、定められ、評価され、管理され、承認されている。	☐	☐	☐	☐
ID.SC-2:	情報システム、コンポーネント、サービスのサプライヤーと第三者であるパートナーが、識別され、優先順位付けられ、サイバーサプライチェーンのリスクアセスメントプロセスにより評価されている。	☐	☐	☐	☐
ID.SC-3:	サプライヤーおよび第三者であるパートナーとの契約が、組織のサイバーセキュリティプログラムやサイバーサプライチェーンのリスクマネジメント計画の目的を達成するための適切な対策の実施に活用されている。	☐	☐	☐	☐
ID.SC-4:	サプライヤーおよび第三者であるパートナーが、監査、テストの結果、またはその他の評価に基づき、契約上の義務を満たしているか、定期的に評価されている。	☐	☐	☐	☐
ID.SC-5:	対応・復旧計画の策定とテストが、サプライヤーおよび第三者プロバイダーと共に行なわれている。	☐	☐	☐	☐

防御（PR）		ティア 1 部分的である （Partial） 場当たり的、属人的である	ティア 2 リスク情報を活用している （Risk Informed） 初期プロセスが整備されている	ティア 3 繰り返し適用可能である （Repeatable） プロセスが継続的に回っている	ティア 4 適応している （Adaptive） プロセス自身の継続的改善に努めている
アイデンティティ管理、認証／アクセス制御（PR.AC） 物理的・論理的資産および関連施設へのアクセスが、認可されたユーザ、プロセス、デバイスに限定されている。またこれらのアクセスは、認可された活動およびトランザクションに対する不正アクセスのリスクアセスメントと一致して、管理されている。		細かい制限等がなされていないため、全従業員といったような設定となっている。 最新（または推奨）の技術を用いた通信や通信設備の管理が部分的なシステムで行われている。（組織の全てのシステムで実施されていない。）	必要な資産に対して、適切な制限のもと、制限をかけるための手順や基準が体系化している。 組織内の資産・システムにおいて、最新（または推奨）の技術を用いた通信や通信設備の管理が行われている。	資産に対しての制限が定期的に見直され、定める期間内において変更が実施されている。 最新（または推奨）の技術の情報を把握し、更新手順やスケジュール立案が円滑に行われている。	脅威や資産価値に即したアクセス制限方法を検討し、検討の結果を基にした実施方法を実現するための計画や手順として体系化されている。
PR.AC-1:	認可されたデバイス、ユーザ、プロセスのアイデンティティと証明書が、発行、管理、検証、取り消し、監査されている。	☐	☐	☐	☐
PR.AC-2:	資産に対する物理アクセスが、管理され、保護されている。	☐	☐	☐	☐
PR.AC-3:	リモートアクセスが、管理されている。	☐	☐	☐	☐
PR.AC-4:	アクセスの許可および認可が、最小権限の原則および役割の分離の原則を組み入れて、管理されている。	☐	☐	☐	☐
PR.AC-5:	ネットワークの完全性が、保護されている（例：ネットワークの分離、ネットワークのセグメント化）。	☐	☐	☐	☐
PR.AC-6:	IDは、ID利用者の本人確認がなされ、証明書に紐付けられ、インタラクションで使用されている。	☐	☐	☐	☐
PR.AC-7:	ユーザ、デバイス、その他の資産は、トランザクションのリスク（例：個人のセキュリティおよびプライバシー上のリスク、その他組織にとってのリスク）の度合いに応じた認証（例：一要素、多要素）が行われている。	☐	☐	☐	☐
意識向上およびトレーニング（PR.AT） 自組織の人員およびパートナーは、関連するポリシー、手順、契約に基づいた、サイバーセキュリティに関する義務と責任を果たせるようにするために、サイバーセキュリティ意識向上教育とトレーニングが実施されている。		関連するポリシー、手順、契約などが理解されておらず、各自の判断で義務と責任を果たそうとしている。または果たしている。	教育・トレーニングが実行されており、関連するポリシー手順、契約を理解した上で、義務と責任が果たされている。	関連するポリシー、手順、契約を理解した上で、義務と責任を果たすために、教育・トレーニングが会社の課題などに紐づき、企画から行われ実行されている。	関連するポリシー、手順、契約を理解した上で、義務と責任を果たすために、教育・トレーニングの企画・実施の方法が見直しされている。
PR.AT-1:	すべてのユーザは、情報が周知され、トレーニングが実施されている。	☐	☐	☐	☐
PR.AT-2:	権限を持つユーザが、自身の役割と責任を理解している。	☐	☐	☐	☐
PR.AT-3:	第三者である利害関係者（例：サプライヤー、顧客、パートナー）が、自身の役割と責任を理解している。	☐	☐	☐	☐
PR.AT-4:	上級役員（セキュリティ担当役員）が、自身の役割と責任を理解している。	☐	☐	☐	☐
PR.AT-5:	物理セキュリティおよびサイバーセキュリティの担当者が、自身の役割と責任を理解している。	☐	☐	☐	☐

防御（PR）		ティア 1 部分的である （Partial） 場当たり的、属人的である	ティア 2 リスク情報を活用している （Risk Informed） 初期プロセスが整備されている	ティア 3 繰り返し適用可能である （Repeatable） プロセスが継続的に回っている	ティア 4 適応している （Adaptive） プロセス自身の継続的改善に努めている
データセキュリティ（PR.DS） 情報と記録（データ）が、情報の機密性、完全性、可用性を保護するための自組織のリスク戦略に従って管理されている。		適用範囲において、資産の撤去、譲渡、廃棄のプロセス・ルール・手順、その他バックアップの取得、暗号化は一部の情報と記録（データ）のみに適用している。	適用範囲において、情報と記録（データ）が目録化（台帳管理）され、資産のリスクアセスメントに基づいた撤去、譲渡、廃棄のプロセス・ルール・手順、その他バックアップの取得、暗号化を実施している。	適用範囲において、情報と記録（データ）の変化があった際に、定めた期間内に目録化（台帳管理）され、資産のリスクアセスメントに基づいた撤去、譲渡、廃棄のプロセス・ルール・手順、その他バックアップの取得、暗号化を実施している。	適用範囲において、情報と記録（データ）の変化があった際に、すぐに目録化（台帳管理）が更新され、資産のリスクアセスメントを行い、撤去、譲渡、廃棄のプロセス・ルール・手順、その他バックアップの取得、暗号化を実施している。
PR.DS-1:	保存されているデータが、保護されている。	☐	☐	☐	☐
PR.DS-2:	伝送中のデータが、保護されている。	☐	☐	☐	☐
PR.DS-3:	資産は、撤去、譲渡、廃棄に至るまで、正式に管理されている。	☐	☐	☐	☐
PR.DS-4:	可用性を確保するのに十分な容量が、維持されている。	☐	☐	☐	☐
PR.DS-5:	データ漏えいに対する防御対策が、実装されている。	☐	☐	☐	☐
PR.DS-6:	完全性チェックメカニズムが、ソフトウェア、ファームウェア、および情報の完全性を検証するために使用されている。	☐	☐	☐	☐
PR.DS-7:	開発・テスト環境が、実稼働環境から分離されている。	☐	☐	☐	☐
PR.DS-8:	完全性チェックメカニズムが、ハードウェアの完全性を検証するために使用されている。	☐	☐	☐	☐

防御（PR）		ティア 1 部分的である （Partial） 場当たり的、属人的である	ティア 2 リスク情報を活用している （Risk Informed） 初期プロセスが整備されている	ティア 3 繰り返し適用可能である （Repeatable） プロセスが継続的に回っている	ティア 4 適応している （Adaptive） プロセス自身の継続的改善に努めている
情報を保護するためのプロセスおよび手順（PR.IP） （目的、範囲、役割、責任、経営コミットメント、組織間の調整について記した）セキュリティポリシー、プロセス、手順が、維持され、情報システムと資産の防御の管理に使用されている。		セキュリティポリシー、プロセス、手順が体系化されておらず、適用範囲内の情報システムと資産が担当者の判断により保護されいる。	適用範囲内の全ての情報システムと資産が、セキュリティポリシー、プロセス、手順が維持管理され、定められた対応手順に従って運用している。	適用範囲内の全ての情報システムと資産に更新がある場合には、セキュリティポリシー、プロセス、手順が維持管理され、定めた期間内で見直しを行なっている。	事業変更やリスク分析などにより即時の変更が求められる場合には、セキュリティポリシー、プロセス、手順を直ちに見直し、見直されたプロセス、手順で情報システムと資産の保護を実施している。
PR.IP-1:	情報技術/産業用制御システムのベースラインとなる構成は、セキュリティ原則（例：最低限の機能性の概念）を組み入れて、定められ、維持されている。	☐	☐	☐	☐
PR.IP-2:	システムを管理するためのシステム開発ライフサイクルが、実装されている。	☐	☐	☐	☐
PR.IP-3:	構成変更管理プロセスは、策定されている。	☐	☐	☐	☐
PR.IP-4:	情報のバックアップが、実施され、維持され、テストされている。	☐	☐	☐	☐
PR.IP-5:	組織の資産の物理的な運用環境に関するポリシーと規制が、満たされている。	☐	☐	☐	☐
PR.IP-6:	データは、ポリシーに従って破壊されている。	☐	☐	☐	☐
PR.IP-7:	防御プロセスは、改善されている。	☐	☐	☐	☐
PR.IP-8:	防御技術の有効性に関する情報が、共有されている。	☐	☐	☐	☐
PR.IP-9:	（インシデント対応および事業継続）対応計画と（インシデントからの復旧および災害復旧）復旧計画が、策定され、管理されている。	☐	☐	☐	☐
PR.IP-10:	対応計画と復旧計画が、テストされている	☐	☐	☐	☐
PR.IP-11:	サイバーセキュリティには、人事に関わるプラクティス（例:アクセス権限の無効化、人員のスクリーニング）が含まれている。	☐	☐	☐	☐
PR.IP-12:	脆弱性管理計画が、作成され、実装されている。	☐	☐	☐	☐
保守（PR.MA） 産業用制御システムと情報システムのコンポーネントの保守と修理が、ポリシーと手順に従って実施されている。		適用範囲において、システム関係の保守契約がなされていない。または保守契約がシステムの目的を達成するための内容・方法になっている。 保守と修理がポリシーや手順に文書化されておらず、担当者の経験や勘により対応されている。	適用範囲において、システム関係の保守と修理がポリシーや手順に文書化されており、文書に基づいたシステムが果たすべき目的を達成するための内容・方法となっている。	保守と修理が求められるシステム関係が追加・更新された際には、ポリシーや手順に基づき、システムが果たすべき目的を達成するための内容・方法となっていることを確認している。	導入される各システムは定められたポリシーや手順の保守条件を満たすものであり、条件が満たされない場合には、リスクアセスメントなどを行い適切な対応を行なっている。
PR.MA-1:	組織の資産の保守と修理は、承認・管理されたツールを用いて実施され、ログが記録されている。	☐	☐	☐	☐
PR.MA-2:	組織の資産に対する遠隔保守は、承認を得て、ログが記録され、不正アクセスを防止した形式で実施されている。	☐	☐	☐	☐

防御（PR）		ティア 1 部分的である （Partial） 場当たり的、属人的である	ティア 2 リスク情報を活用している （Risk Informed） 初期プロセスが整備されている	ティア 3 繰り返し適用可能である （Repeatable） プロセスが継続的に回っている	ティア 4 適応している （Adaptive） プロセス自身の継続的改善に努めている
保護技術（PR.PT） 技術的なセキュリティソリューションが、関連するポリシー、手順、契約に基づいて、システムと資産のセキュリティとレジリエンスを確保するために管理されている。		適用範囲において、ポリシーやルールが明確でないかつ、導入されている機器や資産の機能を把握できていないため、ほとんどの機能がデフォルトの設定のまま利用している。	適用範囲において、ポリシーやルールに定められた重要度や影響度に従って機器や資産の設定や保護方法を実施している。	適用範囲において、ポリシーやルールに定められた重要度や影響度をリスクアセスメントとともに見直し、リスクアセスメントの結果を踏まえた設定や保護方法へ更新している。	機器や資産保護方法を提供するサービスなどの選定をポリシーやルールに基づき行い、必要な設定や保護方法を実装するソリューションを導入している。
PR.PT-1:	監査記録/ログ記録の対象が、ポリシーに従って決定され、文書化され、実装され、その記録をレビューされている。	☐	☐	☐	☐
PR.PT-2:	リムーバブルメディアは、保護され、その使用がポリシーに従って制限されている。	☐	☐	☐	☐
PR.PT-3:	最低限の機能性の原則が、必須の機能のみ提供するようにシステムを構成することによって組み入れられている。	☐	☐	☐	☐
PR.PT-4:	通信（情報）ネットワークと制御ネットワークが、保護されている。	☐	☐	☐	☐
PR.PT-5:	メカニズム（例：フェールセーフ、ロードバランシング、ホットスワップ）が、平時及び緊急時においてレジリエンスに関する要求事項を達成するために実装されている。	☐	☐	☐	☐

検知 (DE)		ティア 1 部分的である （Partial） 場当たり的、属人的である	ティア 2 リスク情報を活用している （Risk Informed） 初期プロセスが整備されている	ティア 3 繰り返し適用可能である （Repeatable） プロセスが継続的に回っている	ティア 4 適応している （Adaptive） プロセス自身の継続的改善に努めている
異常とイベント（DE.AE） 異常な活動は、検知されており、イベントがもたらす潜在的な影響が、把握されている。		何をもって異常と判断するかの閾値が組織内で熟慮されておらず、担当者の経験や勘により異常・正常の判断をしている。	異常と正常の判断を行う指標（閾値など）が定まり文書化しており、それらの指標が及ぼす影響度を認識している。	異常と正常の判断を行う指標（閾値など）は異常がもたらす影響度などにより見直しを行っている。	脅威の情報やリスクアセスメントの結果などに基づき、異常の定義を見直し、検知できるようにしている。
DE.AE-1:	ネットワーク運用のベースラインと、ユーザとシステムで期待されるデータフローが、定められ、管理されている。	☐	☐	☐	☐
DE.AE-2:	検知したイベントは、攻撃の標的と手法を理解するために分析されている。	☐	☐	☐	☐
DE.AE-3:	イベントデータは、複数の情報源やセンサーから収集され、相互分析されている。	☐	☐	☐	☐
DE.AE-4:	イベントがもたらす影響が、判断されている	☐	☐	☐	☐
DE.AE-5:	インシデント警告の閾値が、定められている。	☐	☐	☐	☐
セキュリティの継続的なモニタリング（DE.CM） 情報システムと資産は、サイバーセキュリティイベントを識別し、保護対策の有効性を検証するために、モニタリングされている。		適用範囲における、ネットワーク・物理環境・個人の活動・外部サービスプロバイダの活動などをモニタリングが一部のみで実施されている。（モニタリングされていないイベントや対象がある。）	適用範囲において、ネットワーク、物理環境、個人の活動、外部サービスプロバイダの活動がモニタリングされ、ログとして保管し不審・悪質なものが検知されている。	適用範囲において、対象のモニタリングが適切に行われているかを確認するため、チェックを行うとともに、脆弱性診断等を行い、システムの健全性を確認している。	脅威の情報やリスクアセスメントなどに基づき、モニタリング対象や内容を定期的に見直ししている。
DE.CM-1:	ネットワークは、サイバーセキュリティの潜在的なイベントを検知できるようにモニタリングされている。	☐	☐	☐	☐
DE.CM-2:	物理環境は、サイバーセキュリティの潜在的なイベントを検知できるようにモニタリングされている。	☐	☐	☐	☐
DE.CM-3:	人員の活動は、サイバーセキュリティの潜在的なイベントを検知できるようにモニタリングされている。	☐	☐	☐	☐
DE.CM-4:	悪質なコードは、検知されている。	☐	☐	☐	☐
DE.CM-5:	不正なモバイルコードは、検知されている。	☐	☐	☐	☐
DE.CM-6:	外部サービスプロバイダの活動は、潜在的なサイバーセキュリティイベントを検知できるようにモニタリングされている。	☐	☐	☐	☐
DE.CM-7:	権限のない人員、接続、デバイス、ソフトウェアのモニタリングが、実施されている。	☐	☐	☐	☐
DE.CM-8:	脆弱性スキャンが、実施されている。	☐	☐	☐	☐

検知 (DE)		ティア 1 部分的である （Partial） 場当たり的、属人的である	ティア 2 リスク情報を活用している （Risk Informed） 初期プロセスが整備されている	ティア 3 繰り返し適用可能である （Repeatable） プロセスが継続的に回っている	ティア 4 適応している （Adaptive） プロセス自身の継続的改善に努めている
検知プロセス（DE.DP） 検知プロセスおよび手順が、異常なイベントに確実に気付くために維持され、テストされている。		検知した情報を異常として判断するプロセス・手順・報告体制が定まっておらず、担当者の経験と勘で実施している。	検知した情報を異常として判断するプロセス・手順・報告体制が定まり、異常の判断ができている。	異常な判断に気づくプロセス・方法がテストされ、異常な状態がないことが正常であることを確認している。	異常な状態を検知する仕組みを脅威の情報やインシデントなどに基づき見直ししている。
DE.DP-1:	検知に関する役割と責任は、説明責任を果たせるように明確に定義されている。	☐	☐	☐	☐
DE.DP-2:	検知活動は、該当するすべての要求事項を準拠している。	☐	☐	☐	☐
DE.DP-3:	検知プロセスが、テストされている。	☐	☐	☐	☐
DE.DP-4:	イベント検知情報が、周知されている。	☐	☐	☐	☐
DE.DP-5:	検知プロセスが、継続的に改善されている	☐	☐	☐	☐

対応 (RS)		ティア 1 部分的である （Partial） 場当たり的、属人的である	ティア 2 リスク情報を活用している （Risk Informed） 初期プロセスが整備されている	ティア 3 繰り返し適用可能である （Repeatable） プロセスが継続的に回っている	ティア 4 適応している （Adaptive） プロセス自身の継続的改善に努めている
対応計画（RS.RP） 対応プロセスおよび手順が、検知したサイバーセキュリティインシデントに対応できるように実施され、維持されている。		インシデント発生時の基本的な対応手順が組織内で定まっておらず、場当たり的な対応になっている。 インシデント発生時の基本的な対応手順が定まっているが、組織に浸透していないため、担当者によって対応方法が異なる。	インシデント発生時の基本的な対応手順が組織内で定まっており、手順は組織に浸透している。	インシデント発生時の基本的な対応手順を、従業員は発生した事象に合わせて実施することができる。	未知のインシデントに対して蓄積・手順化した組織の知見から、対応方針や対応手法を協議し対応を行なっている。
RS.RP-1:	対応計画が、インシデントの発生中または発生後に実行されている。	☐	☐	☐	☐
コミュニケーション（RS.CO） 対応活動が、内外の利害関係者との間で調整されている（例：法執行機関からの支援）。		組織図などを作成しておらず、その場その場で必要な人や連絡先を考えて調整から行なっている。	対応活動を行うための関係者が整理されており、連絡が取り合えるように調整がされている。	定期的に有事の際を想定したコミュニケーション手法（連絡先や方法）を日頃から確認している。	組織体制の最適化や関係者を巻き込んだプロセスの改善の検討を日頃から行なっている。
RS.CO-1:	人員は、対応が必要になった時の自身の役割と行動の順序を認識している。	☐	☐	☐	☐
RS.CO-2:	インシデントが、定められた基準に沿って報告されている。	☐	☐	☐	☐
RS.CO-3:	対応計画に従って、情報が共有されている	☐	☐	☐	☐
RS.CO-4:	利害関係者との間で調整が、対応計画に従って行なわれている。	☐	☐	☐	☐
RS.CO-5:	サイバーセキュリティに関する状況認識を広げるために、外部利害関係者との間で自発的な情報共有が行なわれている。	☐	☐	☐	☐
分析 （RS.AN） 分析は、効果的な対応を確実にし、復旧活動を支援するために実施されている。		取得しているログの期間が短い、網羅性がないため、必要な情報が必要なときに準備ができないため、経験や勘に頼った分析をしている。	取得するログの範囲や上記の取得期間等のルールが文書化されており、ログが正しく取得できていることを確認している。	必要なログを定める期間に従い確認しており、ログの精査を行うことで、自社のリスク分析に活用している。	円滑なインシデント対応ができるために、対応・復旧などの手順に紐づいた見直し・改善を行なっている。
RS.AN-1:	検知システムからの通知は、調査されている。	☐	☐	☐	☐
RS.AN-2:	インシデントがもたらす影響は、把握されている。	☐	☐	☐	☐
RS.AN-3:	フォレンジックが、実施されている。	☐	☐	☐	☐
RS.AN-4:	インシデントは、対応計画に従って分類されている。	☐	☐	☐	☐
RS.AN-5:	プロセスは、内外のソース（例：内部テスト、セキュリティ情報、セキュリティ研究者）から報告された脆弱性情報を、自組織が受け取り、分析し、対応するために定められている。	☐	☐	☐	☐

対応 (RS)		ティア 1 部分的である （Partial） 場当たり的、属人的である	ティア 2 リスク情報を活用している （Risk Informed） 初期プロセスが整備されている	ティア 3 繰り返し適用可能である （Repeatable） プロセスが継続的に回っている	ティア 4 適応している （Adaptive） プロセス自身の継続的改善に努めている
低減（RS.MI） 活動は、イベントの拡大を防ぎ、その影響を緩和し、インシデントを解決するために実施されている。		適用範囲において、インシデントによる影響を正しく把握・認識しておらず、原因究明の為の対応に集中している。 インシデントの対応が場当たり的になっており、担当者の経験や知識のみで判断を行なっている。	インシデントによる影響を最小限に抑えるために担当者が意識を持って対応している。（原因究明や攻撃手法解析などに集中したインシデント対応となっていない。）	インシデント発生時に注意する点などが文書化されており、インシデント発生時にスムーズにインシデント対応に入り、対応を開始している。	リスクアセスメントの結果や脅威の状況、被害実態などの情報を収集し、インシデントを封じ込め、緩和するために必要な行動や注意点を更新している。
RS.MI-1:	インシデントは、封じ込められている。	☐	☐	☐	☐
RS.MI-2:	インシデントは、緩和されている。	☐	☐	☐	☐
RS.MI-3:	新たに識別された脆弱性は、許容できるリスクである場合にはその旨を文書化され、そうでない場合にはリスクが緩和されている。	☐	☐	☐	☐
改善（RS.IM） 組織の対応活動は、現在と過去の検知/対応活動から学んだ教訓を取り入れることで改善されている。		対応の為の活動の履歴や記録を文書化しておらず、担当者の記憶に頼っている。	手順が文書化されており、活動の振り返りを行なっている。	振り返りを元に、改善を行い、手順等を更新している。	模擬訓練や検知で得た情報などをもとに振り返りを行い、改善し手順等を更新している。
RS.IM-1:	対応計画は、学んだ教訓を取り入れられている。	☐	☐	☐	☐
RS.IM-2:	対応戦略は、更新されている。	☐	☐	☐	☐

復旧 (RC)		ティア 1 部分的である （Partial） 場当たり的、属人的である	ティア 2 リスク情報を活用している （Risk Informed） 初期プロセスが整備されている	ティア 3 繰り返し適用可能である （Repeatable） プロセスが継続的に回っている	ティア 4 適応している （Adaptive） プロセス自身の継続的改善に努めている
復旧計画（RC.RP） 復旧プロセスおよび手順は、サイバーセキュリティインシデントによる影響を受けたシステムや資産を復旧できるよう実行され、維持されている。		インシデント発生時の基本的な復旧手順が文書化されておらず、担当者の経験と知識で対応している。	インシデント発生時の基本的な復旧手順が定まっており、文書化している。	従業員はインシデント発生時の基本的な復旧手順を理解しており、発生した事象に合わせて復旧手順を実施している。	想定外の事象に対して蓄積・手順化した組織の知見から、対応方針や対応手法を協議し対応を行なっている。
RC.RP-1:	復旧計画が、サイバーセキュリティインシデントの発生中または発生後に実施されている。	☐	☐	☐	☐
改善（RC.IM） 復旧計画およびプロセスが、学んだ教訓を将来の活動に取り入れることで改善されている。		復旧の為の活動の履歴や記録を文書化しておらず、担当者の記憶に頼っている。	手順が文書化されており、活動の振り返りを行なっている。	振り返りを元に、改善を行い、手順等を更新している。	模擬訓練などを定期的に行う中で振り返りを行い、改善し手順等を更新している。
RC.IM-1:	復旧計画は、学んだ教訓を取り入れている。	☐	☐	☐	☐
RC.IM-2:	復旧戦略は、更新されている。	☐	☐	☐	☐
コミュニケーション（RC.CO） 復旧活動は、内外の関係者（例：コーディネーティングセンター、インターネットサービスプロバイダ、攻撃システムのオーナー、被害者、他組織のCSIRT、ベンダ）との間で調整されている。		組織図などを作成しておらず、その場その場で必要な人や連絡先を考えて調整から行なっている。	復旧活動を行うための関係者が整理されており、連絡が取り合えるように調整がされている。	定期的に有事の際を想定したコミュニケーション手法（連絡先や方法）を確認している。	組織体制の最適化や関係者を巻き込んだプロセスの改善の検討を日頃から行なっている。
RC.CO-1:	広報活動が、管理されている。	☐	☐	☐	☐
RC.CO-2:	評判は、インシデント発生後に回復されている。	☐	☐	☐	☐
RC.CO-3:	復旧活動は、内外の利害関係者だけでなく役員と経営陣にも周知されている。	☐	☐	☐	☐

令和4年度

中小企業サイバーセキュリティ対策継続支援事業

第4回

セミナー開催日：令和4年9月13日

価値あるもの
守るもの
資産

セキュリティの対策はやみくもにやってもダメだ。予算も時間も無限にあるわけではない。限りある資源(リソース)を有効に活用するためには、守るものをしっかりと把握し、それに見合った対策を考えていく必要がある。いままでは何か対策をしなくてはいけないと焦っていたけど、まずは守るものを整理しよう。実は対策が行き届いていない資産があるかも知れない。

でも、そもそも資産ってどうやって整理すればいいのだろうか？自分達が保有しているものなのに改めて考えると正しく把握できていない気がする。部署ごとに資産は異なるかもしれないし、１つの部署でしか取り扱っていない資産もあるはずだ。古くからある資産を正しく把握しているのは誰だろうか？最近はクラウドも利用している。そうすると社外に置かれる資産もある。協力会社と共有している資産もある。社外の資産も正しく把握し、管理をしなくてはならない。そして、どの資産がどれだけ重要かという優先度はつけられるだろうか？

考えすぎると、どれも重要に感じてしまう。対策の優先度をつけるためにも、整理をして重要度を把握していこう。

自社の資産とは何か？

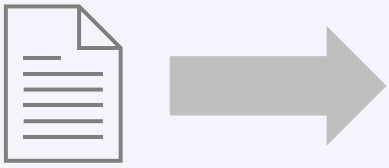
資産とは、自社にとって価値のあるものです。しかし、価値のあるものは会社によって異なります。自社の資産とは何かを考え、把握することはセキュリティ対策の第一歩です。

資産の例



人に関する情報	契約・販売に関する情報	会社のシステムに関する情報
顧客の個人情報	企業間で交わした契約書	社内システムのID・パスワード
購入履歴	企業間で交わした覚書	社内システムのプログラム・OS
従業員情報	経営会議情報	社内システムのログ
マイナンバー情報	技術ノウハウや特許情報	ネットワーク機器構成図
健康診断情報	仕入れ先情報	機器管理・IPアドレス管理

※Day3 テキストより再掲



紙やデータといった、情報が直接書かれている・記録されているものは重要な資産です。

紙やデータを保存するものも重要な資産です。また、これらを管理するIDやパスワードも資産となります。

こんな事例も

「経営資源」とは「人」「物」「金」というのが一昔前によく言われていたことです。最近では、この資源に「情報」と「時間」を加えることが多くなっています。**その会社にしかないノウハウや顧客データ、関係各所とのつながりの情報は企業価値を高める重要な資産です。**またインターネットの普及により、世界の各国とつながることが可能となりました。

特にパーソナルデータはビッグデータやオープンデータの活用により、情報の価値がより高くなっています。**パーソナルデータを安全に、簡単に、やり取りしてくれるしくみ**として、「情報銀行」という概念があります。すでにサービスを提供している事業者もあり、情報はお金と同等の管理をされるほどです。また、銀行なので預けるだけでなく、**「流通・活用」**の機能も果たしています※1。改めて情報の価値を見直し、適切な管理と利用を考えていく時代が到来しています。

※1： 総務省　情報銀行の取組
https://www.soumu.go.jp/main_content/000791752.pdf

資産管理の重要性

資産を管理することは重要です。守るべき対象として正しく対策を行うことはもちろんですが、万が一漏えいした際に自社の情報なのかすらわからないということがないようにしないといけません。

Point① 資産を把握し適切な対策を

資産は企業にとって価値がある情報です。セキュリティ対策としては漏れなく行う必要があります。適切な対策がなされているかを認識するためには資産が把握できていないと対策漏れの原因になります。

資産名	対策
契約書	○
顧客情報	○
サーバ	○
パソコン	○
クラウド	○
USB？	？

Point② 資産を把握しインシデントレスポンスを素早く対応

資産の流出は対岸の火事ではありません。万が一資産が流出した場合、それは自分たちのものだと気付くことはできますか？

資産名	対策	保管場所
契約書	○	サーバ
顧客情報	○	サーバ
サーバ	○	サーバルーム
パソコン	○	各自保管
クラウド	○	社外
顧客情報②	？	？

サーバがウイルス感染をしたことにより、サーバ内に保管されていた顧客情報が流出した可能性があるとすぐに判断できる

どこに保管されたのか、どのような資産なのかが明確にならず、流出自体にも気づけない可能性がある

資産管理台帳の作成

資産を管理する際には、資産管理台帳を作成します。セキュリティ確保の最重要な管理策です。単純な台帳機能だけでなく、重要度や各資産に対しての簡易脅威分析や脆弱性判断を併せて行う場合もあります。

どのような資産があるか洗い出し、重要度を把握する

1、資産管理台帳の作成

資産を管理する台帳を作成します。以下のような項目を入れることが一般的です。

保有部門	資産名	管理区分	利用範囲
例：部署名	例：文書名	例：機密	例：部門内
資産管理者	**媒体分類**	**保管場所**	**保管期間**
例：部長	例：紙	例：キャビネット	例：1年

パソコンのハードディスクや机の引き出しを見るのではなく、日常どのような電子データや書類を利用して業務を行っているかを考えて洗い出すと、作成しやすくなります。電子データや書類を保存する際のまとめ方は様々ですが、管理方法や重要度が同じ情報は1件にまとめて記入することで作業負荷を減らすことができます。

2、資産ごとの機密性・完全性・可用性の評価

機密性、完全性、可用性が損なわれた場合の事業への影響や、法律で安全管理義務があるなど、評価基準を参考に評価値２～０を記入します。

資産名	機密性	完全性	可用性
顧客マスタデータ	2	2	2
企業パンフレット	0	1	1

部門数が多い企業などの場合、管理部署ごとにシートを分けて作成すると、内容の見直しの際に便利です。

3、重要度を算定する

重要度は、機密性、完全性、可用性いずれかの最大値で診断し、重要度を算定します。

資産名	機密性	完全性	可用性	重要度
顧客マスタデータ	2	2	2	**2**
企業パンフレット	0	1	1	**1**

重要度は資産との関係性や立場によって見方が異なることがあります。記入する前に「重要ではない」と診断するのではなく、記入した後に組織的に重要度を診断しましょう。また、「重要度」は時間経過とともに変化することがありますが、現時点の評価値を記入してください。時間経過に伴う重要度の変化を把握するためには、定期的な資産の洗い出しを行うことが有効です。

Day4
1.資産管理の実践

IPAの資産管理台帳の紹介

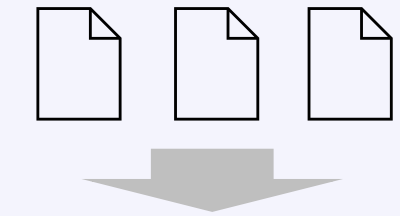
IPA（独立行政法人情報処理推進機構）では、中小企業の情報セキュリティ対策に関する検討を行い、より具体的な対策を示す「中小企業の情報セキュリティ対策ガイドライン」を公開しています。その資料の中には、リスク分析シートという情報資産管理台帳が公開されています。

リスク分析シート情報資産管理台帳

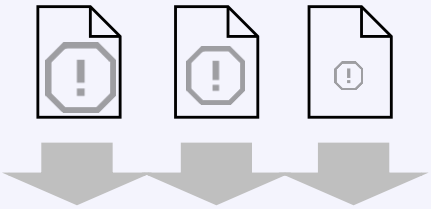
業務分類	情報資産名称	備考	利用者範囲	管理部署	媒体・保存先	個人情報の種類			評価値				保存期限	登録日	現状から想定されるリスク（入力不要・自動表示）					
						個人情報	要配慮個人情報	特定個人情報	機密性	完全性	可用性	重要度			脅威の発生頻度 ※「脅威の状況」シートに入力すると表示	脆弱性 ※「対策状況チェック」シートに入力すると表示		被害発生可能性		リスク値
人事	社員名簿	社員基本情報	人事部	人事部	事務所PC	有			2	0	0	2		2016/7/1	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	4	リスク大
人事	社員名簿	社員基本情報	人事部	人事部	書類	有			2	2	2	2		2016/7/1	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	2	リスク中
人事	健康診断の結果	雇入時・定期健康診断	人事部	人事部	書類		有		2	2	1	2	5年	2016/7/1	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	2	リスク中
経理	給与システムデータ	税務署提出用源泉徴収票	給与計算担当	人事部	事務所PC			有	2	2	1	2	7年	2016/7/1	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	4	リスク大
経理	当社宛請求書	当社宛請求書の原本（過去3年分）	総務部	総務部	書類				1	1	1	1		2016/7/1	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	1	リスク中
経理	発行済請求書控	当社発行の請求書の控え（過去3年分）	総務部	総務部	書類				1	1	1	1		2016/7/1	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	1	リスク中
共通	電子メールデータ	重要度は混在のため最高値で評価	担当者	総務部	事務所PC	有			2	2	2	2		2016/7/1	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	4	リスク大
共通	電子メールデータ	Gmailに転送	担当者	総務部	社外サーバー	有			2	2	2	2		2016/7/1	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	4	リスク大

リスク分析シートというファイルには、7つのシートが存在します。利用方法や記入方法も例示されているので、わかりやすく活用できます。また、リスク分析シートというファイルは単純な資産管理台帳だけでなく、対策検討・実施の要否まで算出してくれるという特徴があります。

【手順１】 情報資産の洗い出し
「台帳記入例」を参考に、業務で利用している情報資産を洗い出して各項目に記入します。



【手順２】 リスク値の算定
対策の優先度を決めるため、情報資産ごとにリスク値（リスクの大きさ）を算定します。リスク値は「重要度」「脅威」「脆弱性」の数値から算定します。



［手順３］ 情報セキュリティ対策の決定
【手順１】と【手順２】が完了すると、情報セキュリティ対策の種類ごとに「情報セキュリティ関連規程策定の必要性」「対策状況チェックの診断結果（対策の実施率）」「対策検討・実施の要否」が表示されます。

リスク回避　リスク移転　リスク受容

「中小企業の情報セキュリティ対策ガイドライン　リスク分析シート」内にも利用方法の記載があります。

出典：情報処理推進機構（IPA）
中小企業の情報セキュリティ対策ガイドライン　リスク分析シート
https://www.ipa.go.jp/files/000055520.pdf

ミニワーク
～振り返ってみよう～

ミニワークテーマ

自社にとってこんな資産はありますか？

資産の一覧で記載した資産は会社にとって価値があるものでしょうか？

資産の価値は会社によって変わります。

皆さんの会社での以下の資産の価値を考えてください。

資産の一覧

(例)サービス設計書　重要度：高　価値：高

経営会議情報

営業マニュアル

従業員名簿

パンフレット

顧客の連絡先・住所

社内のフロアレイアウト図

情報資産のライフサイクル

情報資産は、発生から破棄するまでのライフサイクルが存在します。資産のライフサイクルを意識することで注意点等を意識することにつながります。

資産のライフサイクル

①生成： 新規作成や複写、他からの取得により情報資産は生成されます。
生成のタイミングでは、資産管理台帳への記載がされておらず把握ができないなどの懸念が考えられます。

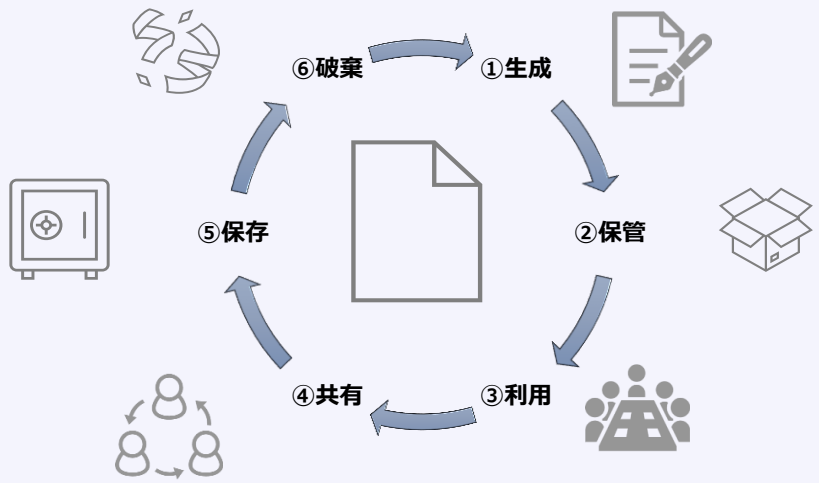
②保管： 利用頻度が高い資産を取り出しやすいように管理をします。
アクセス管理などを設定し、正しい人が正しく使えるようにすることが重要になります。

③利用： 資産をビジネスや事業で利用します。
情報の持ち出しや移動が発生し、漏洩・紛失のリスクが高まります。

④共有： 他者と資産を共有します。
共有のため、メール送付などにより資産の移動が発生する場合があります。

⑤保存： 利用頻度が低い文書を維持しながら管理をします。
保存義務が発生する文書などを保存する必要があります。利用頻度が低いからこそ適切な管理が求められます。

⑥破棄： 利用予定がなくなった資産を破棄します。
正しく破棄されないと流出などの危険性が発生します。



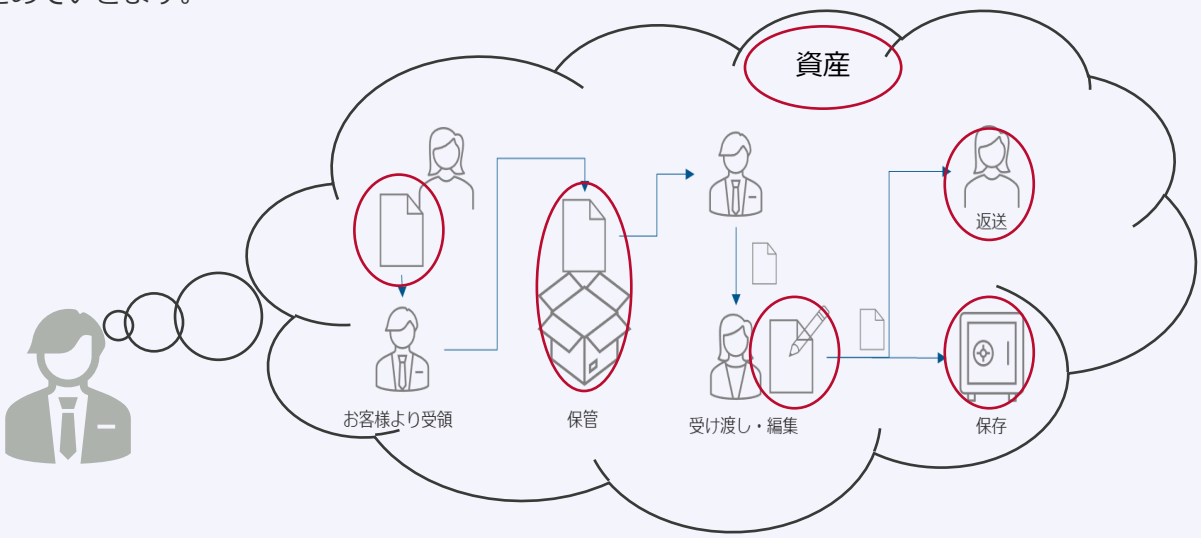
出典：日本ネットワークセキュリティ協会（JNSA）
「情報のライフサイクル管理」をもとに作成
https://www.jnsa.org/ikusei/01/02-02.html

資産を洗い出す

資産を洗い出す際には、やみくもに洗い出すと漏れが発生します。業務内容や情報資産のライフサイクルに従い洗い出していくことで漏れを防ぐ効果があります。

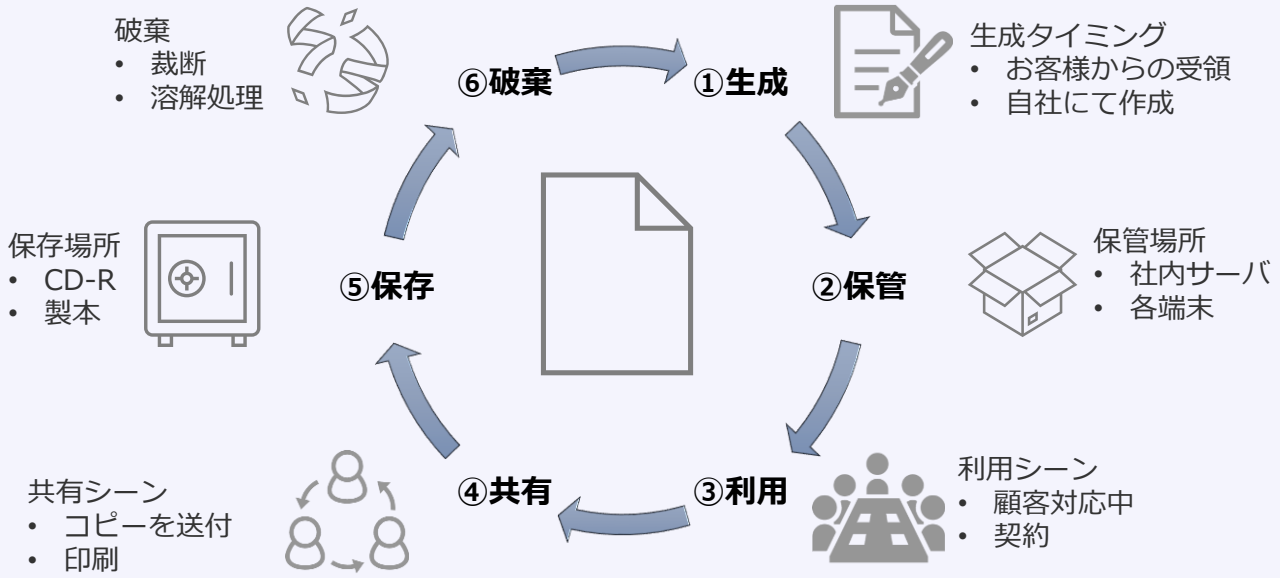
Point① 業務内容から資産を洗い出す

一連の業務の流れを整理し資産を管理します。日頃から行っている業務を思い起こしながら資産をまとめていきます。



Point② 「資産のライフサイクル」から資産を洗い出す

各情報資産において、資産のライフサイクルに該当するシチュエーションに従い関係する資産を洗い出します。各資産において不足する観点が無いかを確認することができます。



Day4

2.資産を洗い出す

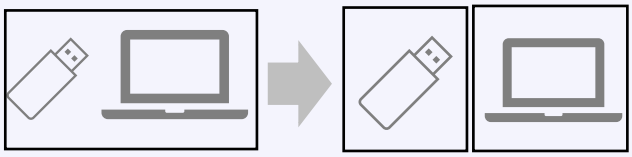
資産洗い出しの注意点

資産を洗い出すと言っても全社規模で洗い出しを行うと、膨大な数の資産が出てきます。全ての資産を一つ一つ確認していくことは非常に労力がかかる作業です。また、漏れや管理のしづらさなどから、継続が困難になります。資産の種類や重要度、運用方法によってわかりやすい管理方法を構築することで、資産管理を円滑に継続していくことができます。

Point① 資産をまとめて管理

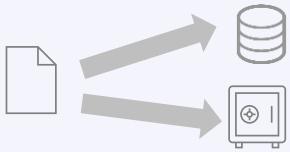
資産には契約書など同じカテゴリーの資産が登場します。これらの資産は、一つにまとめて管理をすることも可能です。ただし、保存先の違いや重要度が違うものは纏めずに管理すると良いでしょう。

Point② 資産をあえて分割



一緒に使うため管理上は一つの資産として管理したいところですが、あえて分割して管理した方が良い場合があります。重要度の考慮や対策の立てやすさにも影響があります。

Point③ バックアップとセットで管理



資産は一つの保存場所だけでなく、バックアップのため、複数の場所に保存されている場合があります。一つの資産を洗い出したら、他の保存先も考えてみましょう。

Point④ 見直し間隔を定め定期的に管理

資産の見直し間隔は資産のライフサイクルを考慮して考えると良いです。間隔が長いと資産の入れ替わりが早く見直しに時間がかかります。会社にとって適切な間隔を見つけましょう。

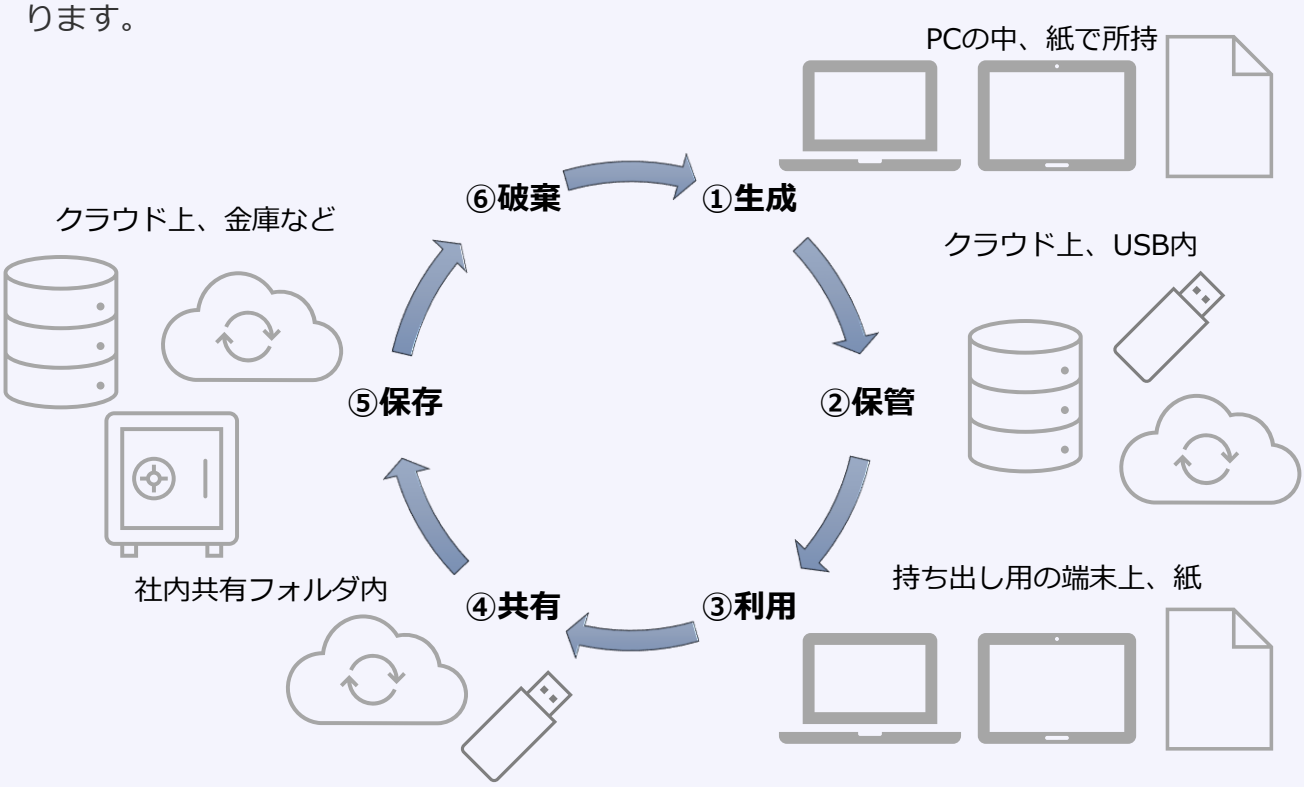
こんな事例も

資産の見直し間隔が不適切だと、対策にも影響が出ます。ある企業では、資産管理台帳の資産で重要度が高いと判断した資産に対策を行おうとしていました。しかし、保存されていると思われた場所を探してみても、その資産は見当たりません。関係がありそうな人に聞いてもわからないという状況でした。完全性の喪失、情報流出の可能性など最悪のパターンが予想されました。

時間をかけて調査すると、実はその資産は既に廃棄していることがわかりました。ただ、資産管理台帳から消されていなかったため、対策を立てる話が上がったのでした。今回は対策を立てる前に気づいたため、余計な対策をすることはなかったですが、これを機会に、資産管理台帳を見直し、多くの過不足を発見することができました。対策の見直しや新規対策の追加、不要な対策の取りやめなどより効果的にセキュリティの対応をすることができるようになりました。

資産の保管場所

資産がどこに保管・保存され、利用時には何の媒体によって使われるかを考える必要もあります。また共有方法などにより、一時的に保管される資産もあります。これらの資産の保管場所をきちんと把握できていないとそこから情報漏洩につながります。



資産のライフサイクルをベースに考えると、その資産のライフサイクルシーンにおいて、どこに資産があるかを考えることができます。また、資産の洗い出しに行き詰まった際には、資産の保管場所から他にどのような資産があるかを考えることで、視点が変わり資産を網羅的に検討できます。

One point

資産の保管場所だけでなく、利用中の資産について考えることも重要です。単純に作業している時ならば、後ろから覗かれないようにするなどの対策が求められます。また、作業端末自体のパスワード保護などは一般的になっています。

しかし、機密情報が書かれたファイルをメールで送信するときや、クラウドへアップロードするときの対策は十分でしょうか？攻撃者によっては、通信を傍受して情報を取得しようとする場合もありますし、ファイルをアップロードした場所が誰でも見られるような設定になっていると情報漏洩のリスクが高まります。ネットワークを盗聴されないようにすることや、クラウドやサーバに適切なアクセス管理をするなどの対策が重要になります。また、社内インフラなどにおいては、ネットワーク機器やサーバが直接操作されないように、サーバルームを用意することや鍵がかかるラックの中で機器を管理するなど物理的な検討もすべきです。「資産がどこにあるのか？」、「保管場所はどのような対策がしてあるのか？」を考えていくと、多層防御※1の考えとなり、より強固なセキュリティ対策を検討することができます。

※1：物理層・ネットワーク層からデータ層まで各層においてそれぞれ対策を実行し多層にセキュリティ保護を行うこと。これにより、未知のマルウェアや新たな攻撃手法の登場により容易に突破されるリスクの軽減が期待される

資産保管場所に特有の注意点

資産がどこに保存されているのかを正しく把握することは、どこで対策を立てるかを考えるために重要です。資産の保有場所を正しく把握できず対策がおろそかになると、そこから情報漏洩につながる可能性があります。また、複数の保管場所に資産が保管・保存されている場合もあります。

想定される資産の保管・保存場所

パソコン

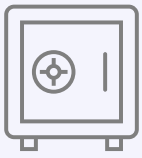
資産の利用時や保管時に主に利用されます。従業員１人１台が一般的となっており、各案件やプロジェクトにより保有する資産も変わってきます。物理的な紛失・ウイルス対策、ルールが守られているかの確認が必要です。

タブレット

パソコンよりも持ち運びがしやすいため、外出時などによく利用されます。パソコンと同様に、物理的な紛失・ウイルス対策、ルールが守られているかの確認が必要です。

社内サーバ

社内のデータが保管されます。企業によってはすべてのデータが集約されている場合もあります。アクセス権限などを適切に行うとともに、バックアップなども重要になります。また、日ごろのメンテナンスを行い、パッチ適用などの対処が求められます。



キャビネット・金庫

データが保存されている電子媒体、紙などの資産を保管します。鍵がかかるキャビネットや耐火金庫など、物理的な対策が有効です。また、広義の考えでは、部屋なども鍵の管理や入退室管理といった対処が求められます。鍵の管理や情報の出し入れの記録など、電子的な記録が残らないため、ルールの整備が求められます。

社外サーバ（クラウドなど）

社外サーバ（クラウド）は資産が社外に置かれる点がポイントです。クラウドサービスを利用する場合には、データが置かれている場所は適切か、ルール通りの運用がされているかといった、委託先運営会社のセキュリティに対しての監督・確認が求められます。

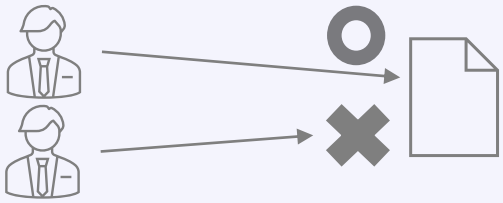
外付けの記憶媒体

パソコンなどに接続して利用します。大きいものではないので、紛失などには特に注意が必要です。持ち運び時のルールなどを明確化した運用が求められます。

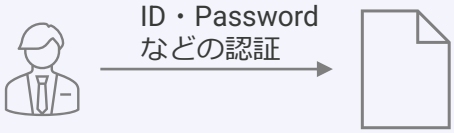
資産の管理者の注意点

資産の管理者は、資産に対してのアクセス制御や認証など、誰に資産を公開するのかを考え、適切な管理をする必要があります。

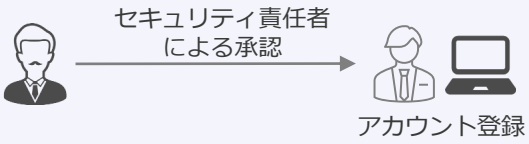
1.アクセス制御
社外秘又は極秘の情報資産を扱う情報システム又はサービスに対するアクセス制御を利用者範囲に基づいて設定し運用します。



2.利用者の認証
社外秘又は極秘の情報資産を扱う社内情報システムは、利用者の認証を行います。



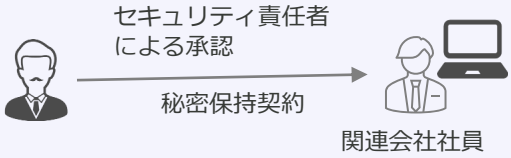
3.利用者アカウントの登録
利用者の認証に用いるアカウントは、代表取締役又はセキュリティにおける責任ある立場の方の承認に基づき登録します。



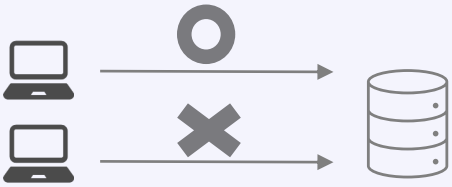
4.利用者アカウントの管理
利用者の認証に用いるアカウントが不要になった場合、管理者は、当該アカウントの削除又は無効化を、当該アカウントが不要になる日の翌日までに実施します。

5.パスワードの設定、必要に応じて2要素認証なども導入
利用者の確認にはパスワードなどの認証を導入します。必要に応じて生体認証などと組み合わせた認証を用います。

6.従業員以外の者に対する利用者アカウントの発行
従業員以外の者にアカウントを発行する場合は、代表取締役又はセキュリティにおける責任ある立場の方の承認を得たうえで発行します。この際、秘密保持契約を締結することが望ましいです。



7.機器の識別による認証の検討
社外秘又は極秘の情報資産を扱う情報システムにアクセスする際には、機器の識別による認証などID・パスワード以外の認証を検討します。



8.端末のタイムアウト機能
社外秘又は極秘の情報資産を扱う情報システムの端末もしくは情報機器には、接続時間制限やタイムアウト等機能を利用します。

出典：情報処理推進機構（IPA）
「中小企業の情報セキュリティ対策ガイドライン 情報セキュリティ関連規程」をもとに作成
https://www.ipa.go.jp/security/keihatsu/sme/guideline/

資産の利用者の注意点

資産管理において、その資産を誰が使うのかを把握することは非常に重要です。利用者を想定した対応や対策を考えることにつながります。

想定される利用者

事業部門

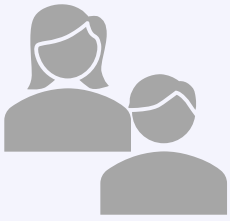
事業部門に所属している従業員は、お客様情報や事業に関する資産を多く利用します。セキュリティ担当は、社内のセキュリティ対策を実施し、事業部門が生産性を上げつつ、安全なセキュリティ対策を実行できるようにすることが求められます。

社内部門

総務や経理など社内業務を主に行う従業員は社員情報を多く利用します。また、契約処理などにおいてはお客様やパートナー企業の情報管理を行います。セキュリティ担当は、個人情報の管理や、契約に伴う注意点、振込や支払いに関するセキュリティ対策の実施など、多岐に渡り取り組みを行います。

情報システム部門

情報システム部門は主に従業員の保有する端末や社内インフラなどにおける資産を利用します。セキュリティ担当は、社内システムへのアクセス制限やバックアップなど技術的な対策やルール策定を行います。セキュリティ担当が技術知識に自信がない場合には、連携してセキュリティ強化を取り組むこととなります。



パート・アルバイト

社員ではないが、業務遂行上に必要な場合には資産の閲覧や利用等を許可されます。これにより、パート・アルバイトもセキュリティ対策を遵守する必要があり、セキュリティ担当も利用する前提で対策や取り組みを実行する必要があります。

委託先

委託先は自社のセキュリティ方針や規程の影響が出せないという特徴があります。自分たちの資産は委託先のセキュリティルールで管理されます。セキュリティ担当は定められたセキュリティルールや取り組みが求める水準に達しているか、資産を預けるに足る委託先かを見定める必要があり、定期的に監督する必要があります。一般的には、自社で行っているセキュリティ対応相当が求められ契約書などにまとめられます。場合によっては契約に基づいて（立入）検査を行うケースもあります。

Day4

2.資産を洗い出す

資産洗い出しの協力体制

資産の洗い出しには、各部署の連携が必要不可欠です。資産管理の部門の中心人物に協力してもらい、資産の整理をしましょう。

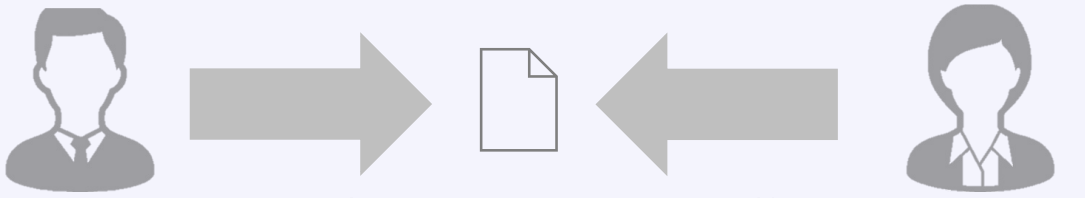
Point① 部門担当者の選出

資産の洗い出しにおいて、部門の誰が協力者となるかは重要になります。各部門の業務を理解しているような人が関わるとスムーズです。

- ☐ 部門の業務に精通している
- ☐ 部門内でリーダーシップが取れる
- ☐ セキュリティの理解がある

Point② 重要度は客観的な視点を

自部門が保有してる資産の重要度を当該部門で資産管理をすると重要と考えがちです。これは、資産の価値を一番わかっているという側面もありますが、過剰に考えてしまうという側面もあります。客観的な評価を行い、バランスを整えることも判断をする上では重要です。



こんな事例も

ある会社では若手を中心としたセキュリティチームを組むことになりました。資産の洗い出しを行う際に、各部門への協力を行いました。しかし、仕事を増やされたくない部門の従業員はあまり乗り気ではありません。結局チームに参加している若手が一人で資産の洗い出しを行いました。

しかしながら、若手が知っている業務はその部署の一部でした。他の部員が何をしているのかをよく知らなかったため、多くの資産が台帳から漏れるという事態が発生してしまいました。

資産管理をする際には、部門長のようなリーダーシップがある人、プラスセキュリティのようなセキュリティに理解がある人、経験が豊富な人の協力が不可欠です。

Day4

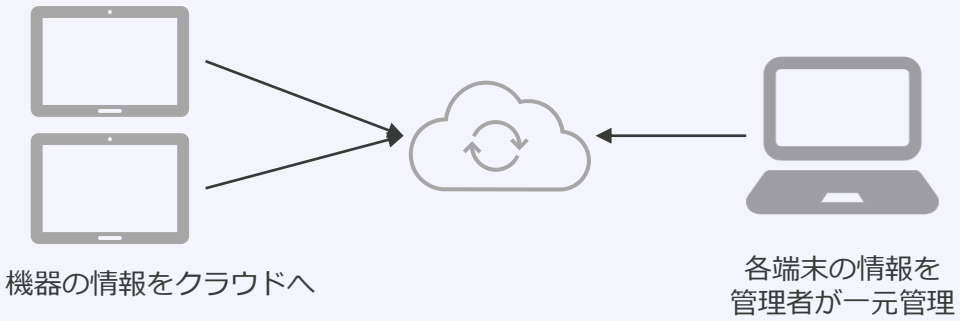
2.資産を洗い出す

効率的に資産管理を行うために

資産数が増えてくると洗い出しに時間がかかったり、見落としなどの危険性があります。効率よく資産管理するためには、資産管理ツールなどの製品やサービスを利用することも効果的です。

Point① デジタル機器をIT資産管理で

デジタル機器の数が多い場合には、クライアント運用管理の製品やサービスを利用すると多くの情報が一元管理されます。



機器の情報をクラウドへ

各端末の情報を
管理者が一元管理

資産管理・ログ管理・OS/ソフトウェア管理などの情報を
一元管理し紛失や適切な端末管理を実現

Point② 機能が充実

最近の資産管理ツールは多くの機能を備えています。自社にとって必要な機能を備えることで、一つのツールで様々なことを可能にします。

資産管理ツール導入パソコン

ログ管理	電子メール監視
デバイス制御	リモートコントロール
Webフィルタリング	PC更新管理
アプリケーション配布	個人情報検索

※製品により機能が異なります。

こんな事例も

デジタル機器の資産管理をエクセルでしていたある会社は、パソコンの台数増加に伴いIT資産管理ツールを導入しました。初期設定に時間はかかったものの、定期的な資産の管理の時間は従来の半分以下になりました。さらに、ソフトウェアのバージョンやログも管理ができ、充実した資産管理につながりました。しかしながら、常時使われていないパソコンなどは、電源が入っておらず監視がしづらいといった課題も出ています。パソコンの利用方法も検討して資産管理をすることで網羅的な管理につながります。

ミニワーク
～振り返ってみよう～

ミニワークテーマ

資産管理のキーマンを考えてみましょう

資産管理台帳を作成する際に調整や協力をお願いする人をイメージしてみましょう。

部署名　お名前　キーマンの理由 を記載しましょう。

Day4

3.個人情報保護

個人情報保護法について

資産の中で重要なものの一つに、「個人情報」があります。全ての企業・法人が守ることを定められており、対応・対策が求められます。

個人情報の保護に関する法律（個人情報保護法）とは

個人情報保護法は、平成15年5月に公布され、平成17年4月に全面施行されました。その後、情報通信技術の発展や事業活動のグローバル化等の急速な環境変化により、個人情報保護法が制定された当時は想定されなかったパーソナルデータの利活用が可能となったことを踏まえ、「定義の明確化」「個人情報の適正な活用・流通の確保」「グローバル化への対応」等を目的として、平成27年9月に改正個人情報保護法が公布され、平成29年5月30日に全面施行されました。

令和3年4月には、個人の権利利益の保護などを目的として、改正個人情報保護法が施行されました。事業者としては、漏洩報告や安全管理措置の公表が求められます。また、第三者提供の在り方や加工情報などにも言及されました。

出典：東京都
「個人情報保護法の概要」をもとに作成
https://www.johokokai.metro.tokyo.lg.jp/kojinjoho/hogohou/index.html

海外の個人情報保護規制

ビジネスのグローバル化により、世界的にみても個人情報の取り扱いは重要になっています。日本だけでなく、世界でも個人情報保護の取り組みは進められており、準拠が求められる場合があります。代表的なものに、EUの一般データ保護規則（GDPR）があります。また、アメリカ、中国とそれぞれ特徴がありますので、ビジネス上で関係する国の個人情報保護について理解を深めましょう。ここでは、代表してGDPRを紹介します。

一般データ保護規則（GDPR）/ EU

- 個人データの取得には本人の明確な同意取得が必要、また個人データの削除や利用制限を管理者に要求できる
- 個人データの移転はEU域外へは原則禁止。一定以上の基準の個人データ保護が実施済みと認定された国なら移転可能
- 情報漏えいなどの違反行為があれば、72時間以内に規制当局へ通知
- 所在地にかかわらず、EU域内に在住する個人のデータを扱う企業・組織すべてが対象になる

インターネットを利用したアンケートフォームなどを利用してEU域内の顧客の個人データを取得する場合、Webサーバやデータベースは EU域外に設置（例えば日本国内など）してあっても GDPRの対象になります。

出典：個人情報保護委員会
GDPR（General Data Protection Regulation：一般データ保護規則）をもとに作成
https://www.ppc.go.jp/enforcement/infoprovision/laws/GDPR/

One point

日本の個人情報保護は「個人情報保護委員会」が推進を行っています。個人情報保護委員会では、『中小企業の皆様（中小企業サポートページ）』として、役立つ情報を公開しています。

個人情報保護委員会　中小企業の皆様（中小企業サポートページ）
https://www.ppc.go.jp/purpose/SMEs/

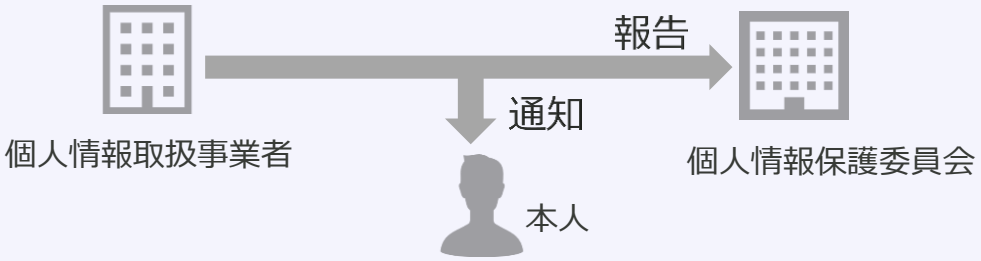
個人情報保護法の改定について

令和4年4月1日に、改正個人情報保護法が施行されました。すぐに取り組むべき重点ポイントについて確認し、しっかりと対策を行っていきましょう。

Point①

万が一に備え、漏えい等報告・本人通知の手順を整備しましょう

個人の権利利益を害するおそれが大きい、漏えい等の事態が発生した場合に、個人情報保護委員会への報告及び本人への通知が義務化されます。



Point②

個人データを外国の第三者へ提供しているか確認しましょう

外国にある第三者への個人データの提供時に、提供先の第三者における個人情報の取り扱いに関する本人への情報提供の充実等が求められます。

改正前 外国にある第三者に個人データを提供できる要件

- 本人の同意
- 基準に適合する体制を整備した事業者
- 日本と同等の水準国（EU・英国）

改正後 各要件に基づく個人データの移転時、以下を義務付け

追加 → 本人からの同意取得時に、以下の情報を提供すること
- 移転先の所在国の名称
- 当該外国における個人情報の保護に関する制度
- 移転先が講ずる個人情報の保護のための措置

追加 →
① 移転先が必要な措置をとること
- 移転先における適正な取り扱い状況などの定期的な確認
- 移転先における適正な取り扱いに問題が生じた場合の対応

② 本人の求めに応じて必要な措置等に関する情報を提供すること

Point③

安全管理措置を公表する等本人の知り得る状態に置きましょう

どのような安全管理措置が講じられているかについて、本人が把握できるようにする観点から、原則として、安全管理のために講じた措置の公表等が義務化されます。外国において個人データを取り扱う場合、当該外国の個人情報の保護に関する制度等を把握した上で、安全管理措置を講じる必要があります。

個人情報保護法の改定について

Point④ 保有個人データを棚卸し、開示請求等に備えましょう

６か月以内に消去するデータについて、開示請求の対象となります。また、個人データを第三者に提供した記録も開示請求の対象となります。なお、開示方法については、本人が指示できるようになります。このほか、本人による個人データの利用停止・消去等の個人の請求権が拡充されました。

＜利用停止・消去等の請求権の拡充例＞

① 利用する必要がなくなった場合。	ダイレクトメールを送付するために保有していた情報について、本人からの求めを受けてダイレクトメールの送付を停止した後、本人が消去を請求した場合　等
② 個人情報保護委員会への報告義務のある、重大な漏えい等が発生した場合。	クレジットカード番号を含む個人データが漏えいした場合、不正アクセスにより個人データが漏えいした場合　等
③ 本人の権利又は正当な利益が害されるおそれがある場合。	退職した従業員の情報を自社のホームページに掲載し続け、本人の不利益になった場合　等

Point⑤ 個人情報を不適正に利用していないか確認しましょう

違法な行為を営むことが疑われる事業者に、違法又は不当な行為を助長するおそれが想定されるにもかかわらず、個人情報を提供すること等、不適正な方法により個人情報を利用することが禁じられることが明確化されます。

事業目的で取得した個人情報

性別、戸籍等の特定の属性のみにより、正当な理由なく本人に対する違法な差別的取り扱いを行う

Point⑥ 個人関連情報の利用状況や提供先を確認しましょう

個人関連情報の第三者提供の制限等として、提供元では個人データに該当しないものの、提供先において個人データとなることが想定される情報の第三者提供について、本人同意が得られていること等の確認が義務付けられます。個人関連情報には、端末識別子を通じて収集されたサイト閲覧履歴や、商品購買履歴、位置情報等が該当します。（なお、これらの例でも、個人情報に該当する（特定の個人を識別できる）ものは、個人関連情報にはあたりません。）

出典：個人情報保護委員会
「改正個人情報保護法」をもとに作成
https://www.ppc.go.jp/news/kaiseihou_feature/
https://www.ppc.go.jp/news/kaiseihogohou_checkpoint/

個人情報保護法で定める情報

個人情報保護法とプライバシーマークでは情報において以下のような言葉が出てきます。

①個人情報

●生存する特定の個人を識別できる情報
- 個人識別符号が含まれるもの
- 他の情報と容易に照合することができ、それにより個人が誰であるかを識別することができることとなるものを含む

●要配慮個人情報
- 本人の人種、信条、社会的身分、病歴、犯罪経歴、犯罪被害の事実

②個人データ

●①のうち、紙媒体、電子媒体を問わず特定の個人情報を検索できるように体系的に構成したデータベース等に含まれる個人情報

③保有個人データ

●②のうち、開示、訂正、消去などの権限を有し、かつ6か月を超えて保有するもの

個人を特定することができる情報

個人情報がデータベース化されたもの

事業者において管理義務が発生するもの

出典：個人情報保護委員会
「「個人情報」「個人データ」「保有個人データ」とは、どのようなものですか。」 をもとに作成
https://www.ppc.go.jp/all_faq_index/faq3-q2-1/

One point

DX時代における情報は非常に大きな価値を持っており、情報を積極的に利用していくことが求められています。反面、個人情報保護法や各社のセキュリティの取り組みにより、個人に不利益が出ないように対策を行うべきです。個人情報保護法でも、匿名加工情報というものがあり、「特定の個人を識別できないように個人情報を加工して得られる個人に関する情報であって、当該個人情報を復元できないようにしたもの」と定められています。本人の同意を得ずに第三者に提供することが可能なため、データ分析などにもよく使われます。

2020年の改正(2022年4月施行)ではここに、仮名加工情報という考えが加わりました。他の情報と照合しない限り特定の個人を識別できないように加工した個人に関する情報です。第三者提供の禁止や目的外利用の禁止など定められています。企業による情報の利活用が期待されています。

Day4

3.個人情報保護

プライバシー保護

中小企業のクラウド導入やIoT活用、海外展開が拡大している状況において、従来の個人情報保護の在り方では対応しきれない場合があります。

個人情報とプライバシー

個人情報
本人の氏名、生年月日、住所などの記述等により特定の個人を識別できる情報

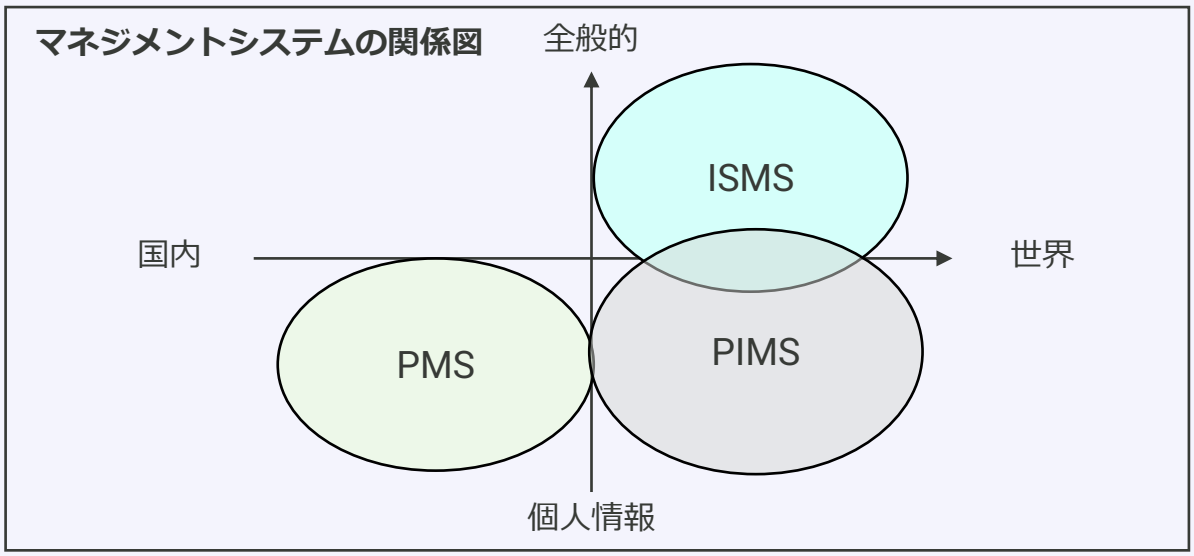
プライバシー
「個人や家庭内の私事・私生活。個人の秘密。また、それが他人から干渉・侵害を受けない権利。」という意味があるほか、最近では、「自己の情報をコントロールできる権利」という意味も含めて用いられる。

出典：一般財団法人日本情報経済社会推進協会
1-3.「個人情報」と「プライバシー」の違い
https://privacymark.jp/wakaru/kouza/theme1_03.html#:~:text=%E6%9C%AC%E4%BA%BA%E3%81%AE%E6%B0%8F%E5%90%8D%E3%80%81%E7%94%9F%E5%B9%B4%E6%9C%88,%E4%BE%B5%E5%AE%B3%E3%82%92%E5%8F%97%E3%81%91%E3%81%AA%E3%81%84%E6%A8%A9%E5%88%A9%E3%80%82%E3%80%8D

中小企業でも個人情報保護法の施行(2022年4月)を受けて、対応を行っているという企業も多いです。また、それだけでなくクラウドを用いたサービス展開や、海外向けのサービス展開など、海外国籍の方がサービス利用者となるケースも珍しくありません。海外の動向や国際規格に準拠したセキュリティが求められつつあります。そこで最近注目を集めているのは、プライバシー保護の国際規格であるISO/IEC 27701:2019※1です。GDPRなど世界各国のプライバシーに関する法規制に対応し、運用体制や仕組みに準拠しています。

※1：ISO/IEC 27701:2019は2019年8月に発行され、情報セキュリティマネジメントシステム（ISMS）要求事項で、情報セキュリティ管理策の実践のための規範 ISO/IEC 27001 と、情報セキュリティ管理策の実践のための規範 ISO/IEC 27002 のセキュリティ対策をPII（個人識別可能情報）の保護へと拡張したPIMS（Privacy information Management System）の規格。

出典：一般財団法人日本情報経済社会推進協会
ISO/IEC 27701
https://www.jipdec.or.jp/library/word/u71kba0000010ghu.html



Cookie等も個人情報に？

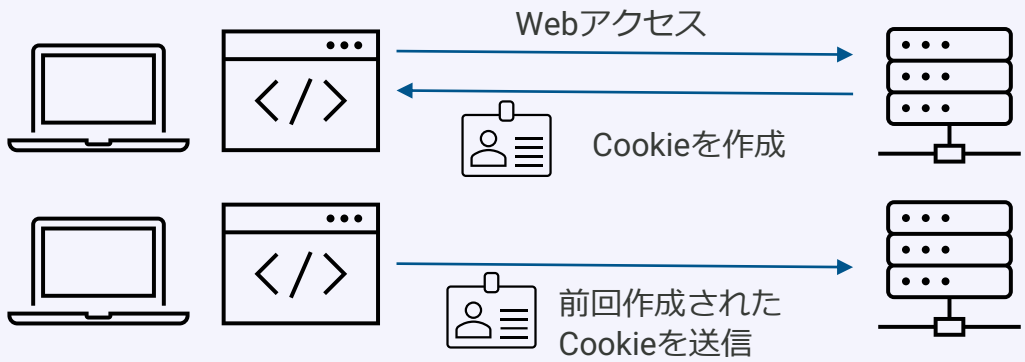
インターネットを見ていると、以下のようなポップアップが出るケースが多くなっています。また、個人情報保護規程に盛り込まれている企業も増えています。Web利用におけるCookie等も個人情報に該当するケースがあり、注意が必要です。

Cookieのポップアップの例

個人情報保護規程の例

クッキー（Cookie）等による個人情報の取得
当社ウェブサイトでは、利便性の向上、広告の配信及び統計データの取得のため、クッキー（Cookie）のほかアクションキー、webバグ等のトラッキングツールを使用しております。これらのツールによりページをご覧いただく際に必要なシステム情報や、ご利用者が同一人物であると確認するための情報、ご利用者の行動履歴（アクセスしたページ、閲覧したコンテンツ等）、端末情報及び位置情報等を取得することがあります。これらの情報には、個人が特定されるような情報は含んでおりませんが、当社が保有する情報との照合により個人を特定し、利用目的の範囲で利用する場合がございます。

Cookieとは何か？
ホームページを閲覧した際に、Webサーバが利用者のコンピュータに保存する管理用のファイルのこと。利用者の登録情報や今までのショッピングカートの内容などを利用者のコンピュータに保存しておくことで、次回その利用者が同じWebサイトを訪問した場合に、それらのデータを利用できるようにする仕組みです。たとえば、Cookieを利用すると、ログイン情報を保管することもできるため、次回利用するときにログイン処理を省略できるようになるといった利点があります。



出典：総務省
「国民のためのサイバーセキュリティサイト」をもとに作成
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/intro/intro.html

Cookieは個人情報に該当するの？
個別の事案ごとに判断することとなりますが、Cookie等の端末識別子について、個人情報に該当しない場合には、通常、当該端末識別子に係る情報端末の利用者に関する情報として、「個人に関する情報」に該当し、個人関連情報に該当することとなると考えられます。

出典：個人情報保護委員会
Cookie等の端末識別子は個人関連情報に該当しますか。家族等で情報端末を共用している場合はどうですか。
https://www.ppc.go.jp/all_faq_index/faq1-q8-1/

資産管理の事例
～資産の利用と管理～

資産の管理を行う

資産管理台帳は作成にも時間がかかりますが、棚卸も非常に労力がかかります。資産は保管・保存されているだけでなく、利用や共有も行われます。利用中は資産が個人のパソコンに存在したり、共有としてパートナー企業や委託先企業に渡ることもあります。これらの資産の動きは毎日のように発生します。定期的な棚卸を行ったとしても、どうしても乖離が発生してしまい、実態と合わないケースが出てきます。ある時までは、資産管理台帳を適切に運用し乖離をなくしていくことを検討していました。
とは言うものの、修正などの作業が膨大で実質管理が煩雑になっています。

特に、事業成長や顧客数増加などにより管理が大変になってきます。また、従業員の意識などでも変わってきました。人数が増えると、新しく入った従業員はルールの理解が追いつかない場合もあります。逆に長くいる社員が教育を受ける機会がなく、忘れていくケースもあります。最近ではデジタル化の影響もあり、外部のクラウドサービスを利用するケースも増えており、新しくできたルールに対応が追いつかないということも起こります。そして、従業員の個人情報を委託先の会社に提供する場合のルールなどは特に注意が必要です。

ある企業では委託先から個人情報が流出するといった事態が発生しました。委託先の企業からすぐに連絡が入り状況の把握はできました。また、委託先から対策が明示されましたが、ユーザーのパスワード変更対応が余儀なくされ、社内には混乱が発生しました。

実は、委託先の企業に対して個人情報を渡して良いのかなどの検討をしていませんでした。金額だけを見て企業を選定したためです。本来であれば、個人情報を提供するにあたり、適切な対策をとっているか、プライバシーマーク（Pマーク）※1などの認定を受けているかといった点は確認すべきでした。

今回の事件をきっかけに、個人情報を含む資産を委託している企業に実態の確認を行いました。基本的にはどこの企業もしっかりと対応していました。ISMS認証やPマークの保有なども確認しました。

今回のケースでは、台帳を作ることが目的になっていました。資産管理台帳を正しく管理することも重要ですが、資産が正しく守られているかが一番重要です。社内にある資産への対策だけでなく、社外の資産や委託されている資産が正しく管理されているかも重要です。今回の事故をきっかけに、資産管理台帳に記載されている資産の中で委託しているものについては、委託先とも連携し管理強化に努めています。

※1：プライバシーマークは、日本産業規格「JIS Q 15001個人情報保護マネジメントシステム－要求事項」に準拠した「プライバシーマークにおける個人情報保護マネジメントシステム構築・運用指針」に基づいて、第三者機関である「一般財団法人日本情報経済社会推進協会（JIPDEC）」及びその指定機関が審査し、個人情報について適切な保護措置を講ずる体制を整備している事業者へ付与されます。

Day4

4.事例紹介

資産洗い出しの事例

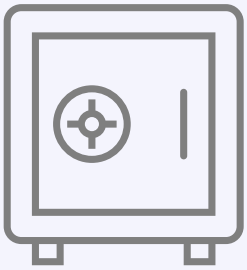
～個人情報から洗い出す～

個人情報から資産管理の文化を

資産の洗い出しを行う際には、何が資産なのかと疑問に思う人がいます。特に部署ごとに資産の洗い出しを行うと、部署の担当者から「これは資産なのか？」という質問を受けることがよくあります。

ある会社では最初に、個人情報から資産をまとめていくことにしました。個人情報の管理は法律で定められていることから、誰でも重要なものだということがわかります。そして、流出等があった場合の影響が大きいということも理解が得やすいです。各部署に最低一人は協力してもらう担当者を選出してもらい、個人情報が記載されている資産を洗い出すように指示を出しました。

一部の部署からは、「名前だけは資産なのか？」「名前と連絡先ではどうか」と言った質問が出ました。基本に立ち返り、「個人が特定できるものは個人情報保護の対象」というルールの元、棚卸をしました。部署ごとに判断基準が変わることを避けるため、悩むようなら、台帳に記載するようにし、洗い出しを進めました。一部は契約書などのカテゴリーで資産をまとめましたが、非常に多くの個人情報を含む資産が洗い出されました。



作業をした部署に話を聞くと、「すでに使わない個人情報が書かれた資産もあり、廃棄の対応をした方が良いことに気づいた」という意見がありました。もしかしたら使うかもしれないという心理もあり、保存をしていましたが、そのまま忘れられてしまったようです。また、個人のパソコンなどに過去の案件で利用した資産があり、そこにも個人情報が書かれていました。これは非常に危険な状態だと気付けたという意見もありました。あえて部署ごとに棚卸をしたことで、部署内でも気づいていなかった個人情報の管理の実態が把握でき、危険性に気づけたようです。

早速これらの対策を講じ、個人情報に対しての意識が社内で上がったとセキュリティ担当者も感じています。

個人情報で資産管理台帳の使い方を把握したことで、資産管理の作業に対する抵抗が和らぎ、他の資産についても洗い出しをしやすくなりました。また、資産管理をするメリットも感じることができたので、当初よりも協力的に資産管理台帳の棚卸を進められるようになりました。ただ、繁忙期にあたる時期は各部署とも業務が優先的になるので、実施のタイミングはセキュリティ担当の方で計りつつ、お互いに協力しあいながら取り組みを継続しています。

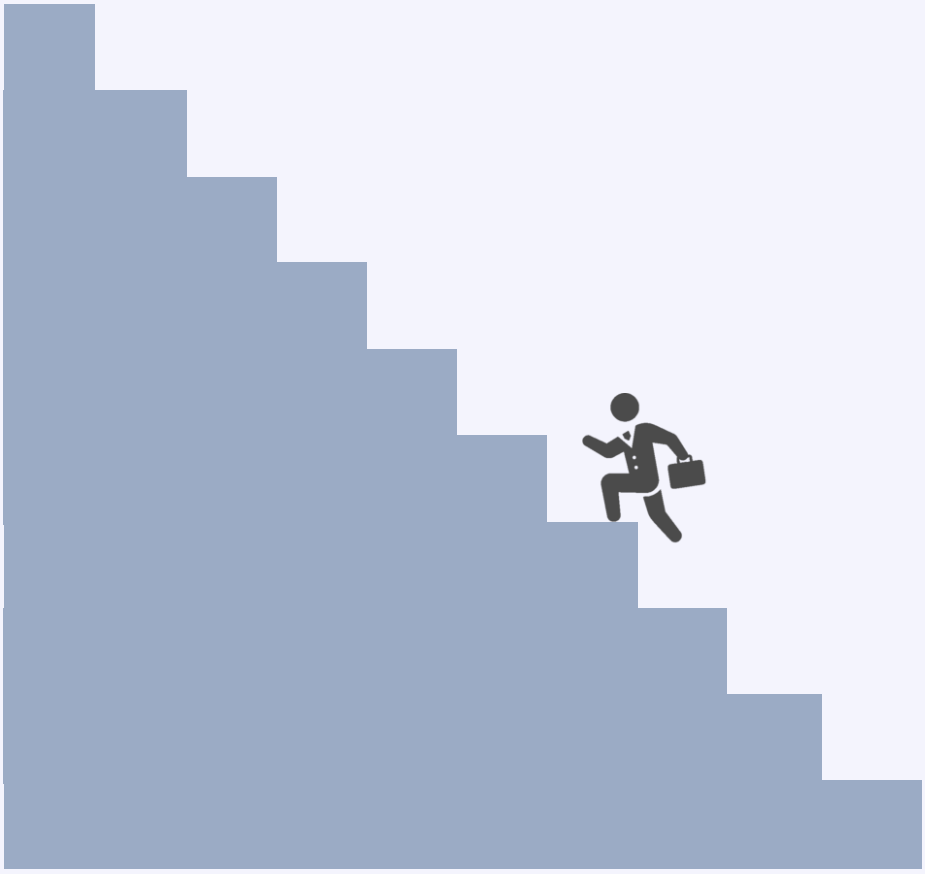
資産を把握するためには、資産管理台帳で管理をしていくのが良いようだ。いままではどこに何があるかを暗黙知で把握し共有していたけれど、資産管理台帳を作ればどこに何があるかが把握しやすく、万が一資産の紛失や情報漏洩があった場合も対処しやすい。ただ、数が多くなるので更新が大変そうだ。資産は破棄まで考える必要があるから、破棄した資産は台帳から消していき、管理負荷を減らす工夫もしていこう。

資産の洗い出しには、業務フローや資産のライフサイクルで考えるといいらしい。うちの場合には、業務フローから考えるとわかりやすそうだ。事業部門の従業員にも協力してもらいながら業務整理をし、資産を把握しよう。いくつかの業務でまずは資産とその流れについて整理をしていこう。

気になったこととして、資産が複数の箇所にあればバックアップの機能を果たすかもしれない。最近では社内サーバとクラウドに保存されている。ただ実際は一箇所にしかない資産が存在するのではないかと感じている。バックアップが必要な資産なのかも併せて考えることも重要だろう。資産管理は保存先まで把握する必要があるらしいので、適切なバックアップができているかも把握することができそうだ。

まずは資産を把握して何を守るのかを明確化していこう。

資産を把握
守るものを知る



コラム
～ISMS認証も資産管理から～

ISMS認証とは組織の構築した情報セキュリティマネジメントシステムがISO/IEC27001に基づいて適切に管理されているかを第三者であるISMS認証機関が、審査し証明することです。マネジメントシステムとある通り、対策を一つすれば終わりというものではありません。方針やマニュアル、ガイドラインを定め教育などを行い、記録をつけ日々運用する体制や仕組みが評価されます。

同じような認証に個人情報に関するPマークがあります。Pマークは個人情報に特化しており、また、日本工業規格が定める「JISQ15001」に準じた「国内規格」という違いがあります。

※ISO/IEC27001は、ISMSの要求事項を定めた国際規格

ISMSが認証されるためにも、資産管理が重要です。

適用範囲という、マネジメントシステムが適用される範囲にどのような資産があるかを把握します。そして、その中の資産が適切に守られているか、対策ができているかが大切です。リスク分析の結果、リスクを受容できるまでの対策が施されていない場合には早急に対策が必要です。

審査の際には、資産管理台帳から対策の状況などを確認される場合があります。マネジメントサイクルですので、対策が継続されているかもポイントです。計画・実行・記録・見直しをしっかりと対応することがマネジメントを回すことになります。資産管理の定期的な見直しはもちろん、そこから対策や効果を見ていくことが重要です。

あとがき

今回のテーマは資産管理についてです。自分たちが守らなければならないものは何かというのは、非常に重要になります。各資産においてしっかりと対策が立てられていることがセキュリティの第一歩です。

しかしながら、資産も数多く存在し、洗い出すこと自体にも苦労するケースがあります。担当がすべて洗い出すのではなく、協力していくことが非常に重要です。1回目のセミナーでも取り上げた、「協力してくれる人を見つける」ということを思い出し、自分たちの資産をしっかりと管理してください。そして、次回からはリスク分析に入っていきます。これらの資産をどう守っていくのか、何から守っていくのかを考えていきましょう。

令和4年度

中小企業サイバーセキュリティ対策継続支援事業

第5回

セミナー開催日：令和4年10月11日

脆弱性？
脅威？
どこから考えればいいのでしょうか？

守るべきは資産ということがわかった。とはいうものの、どのように守っていけばいいのだろう？予算が潤沢にあるわけではないし、全ての業務を資産管理に費やせるわけではない。資産も数多くあり、全てを同じように守ることも難しそうだ。特に最近では、クラウドの利用など新しいサービスの導入が行われている。本来ならばリスクをしっかり把握し対応策を検討してから導入すべきなのだが・・・

常日頃から守る方法や優先順位を考えておかないといけない。これをリスクマネジメントというらしい。ビジネスの変化が激しいからこそ、脅威や脆弱性を自分たちで把握し、検討できるようになることでスピーディーな対応が取れるようになるのではないだろうか？新しいサービスを導入していくような投資をする際には、適切にリスクマネジメントを行いリスクを管理していこう。

現状では、一番守らなければいけない資産は守れているのか？実はリスクの対応ができていない資産が存在するのではないだろうか？資産を保有する部門に協力をしてもらいつつ、セキュリティ担当として、先入観にとらわれず客観的な評価をしてリスク管理をしていこう。

自社を脅かす脅威

セキュリティにおいて、情報資産を脅かすものを脅威と言います。今回は、それぞれの脅威について詳しく見ていきましょう。

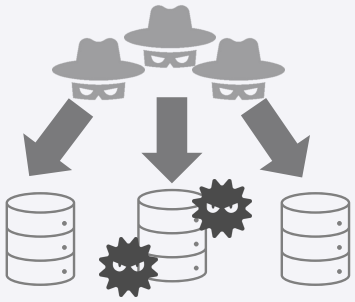
Point① 人の脅威

偶発的

人が脅威となることもあります。メールの誤送信や添付ファイル間違い、書類や記憶媒体の廃棄の方法を誤ったり、携帯電話やスマートフォンを紛失したり、といった過失が多く発生しています。操作ミスや設定ミス、紛失などといった、「つい、うっかり」の過失（ヒューマンエラー）が偶発的な脅威です。企業や組織における情報漏えいの原因のほとんどが、このような人の「つい、うっかり」やITリテラシーの不足によるものが多いと言われています。

計画的

組織などの内部犯行や外部からの攻撃なども脅威といえます。対象組織を狙い、組織に合わせた攻撃をしてくる場合もあります。ウイルス感染や改ざん・盗聴など、主に技術を用いた脅威でもあるため、技術的脅威と呼ぶ場合もあります。



Point② 環境の脅威

自然災害

自然災害は、頻繁に起こる問題ではありません。しかしながら最近の日本では、大雨や台風・地震などの自然災害が、頻繁に起こっています。ひとたび発生すれば企業や組織に甚大な被害や影響を与えます。

障害・故障

システムには物理的な機器が存在します。そのため機器の故障やケーブルの故障といった脅威が存在します。重要なシステムが故障し障害が発生した場合には、業務を継続することが難しくなる場合もあります。あらかじめ事故や障害・災害が発生した場合の対策を講じておく必要があります。

障害などを考慮した対策をすることもセキュリティの一環です。

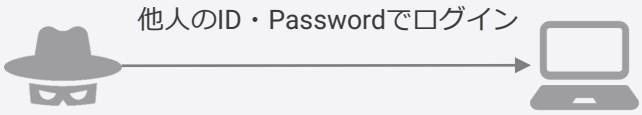
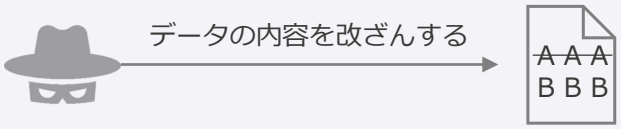
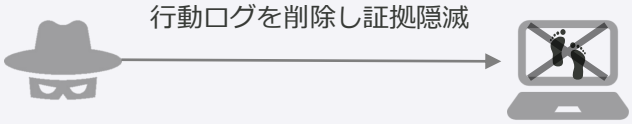
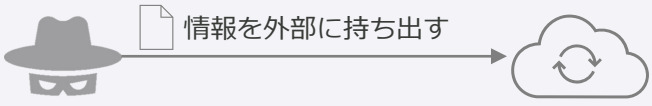
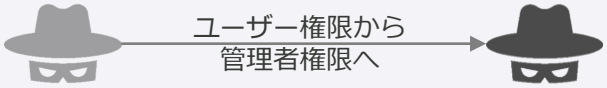
Day5
1.脅威と脆弱性に対応する

脅威分析～STRIDE～

Day3で紹介した通り、セキュリティにおいて、情報資産を脅かすものを脅威と言います。脅威といっても世の中には様々なものがあります。体系立てて考えることで、自社の脅威を把握しやすくなります。

リスクを把握するためには、脅威の把握が重要になります。攻撃側の視点に立ち、攻撃手法などから脅威を考察していきます。と言っても、ゼロベースで攻撃手法を考えていくことは、企業のセキュリティ担当者としては負担がかかる作業です。 STRIDEのように構造化されたモデルを使うことで、より素早く考察ができるようになります。

STRIDEの概要

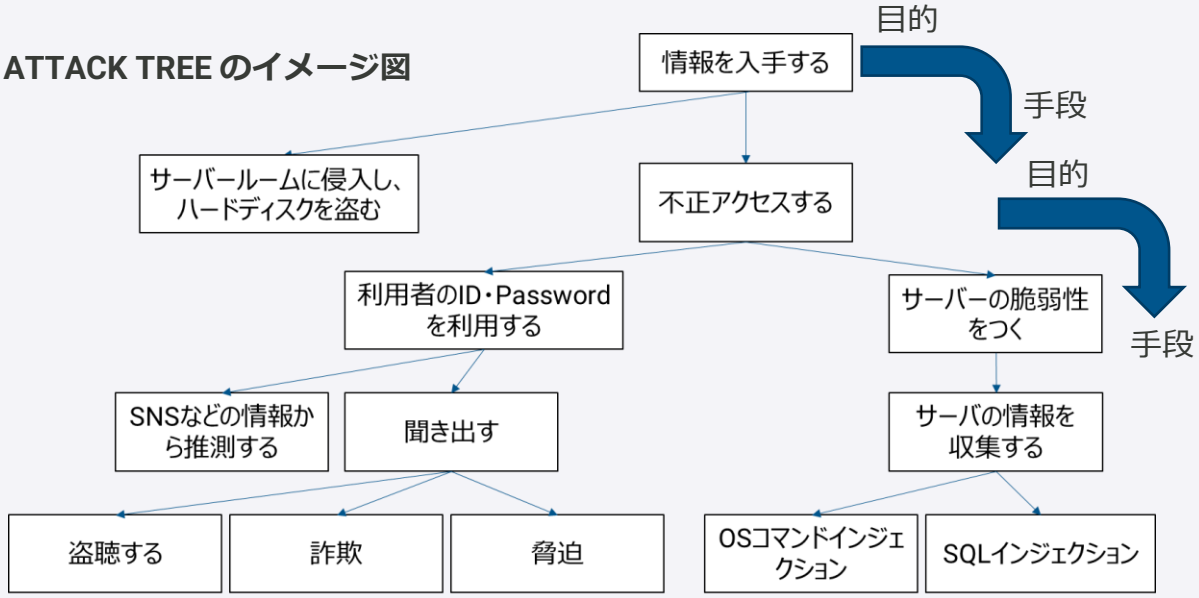
要素名	脅威例
Spoofing （なりすまし）	第三者が正規のユーザーになりすます 
Tampering （改ざん）	データを改ざんする 
Repudiation （否認）	ログを消去することで証拠隠滅を図る 
Information Disclosure （情報漏えい）	情報資産が流出する 
Denial of Service （サービス妨害）	システムに多大な負荷をかける 
Elevation of Privilege （権限昇格）	管理者権限を取得する 

出典：経済産業省
「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き」をもとに作成
https://www.meti.go.jp/press/2021/04/20210419003/20210419003-1.pdf

脅威分析 ～ATTACK TREE～

発見された脅威を引き起こす攻撃手法を列挙する手法として Attack Tree があります。Attack Tree はツリー構造で表現され、分析対象の脅威についての攻撃手段を可視化できます。STRIDE によって抽出される脅威は一般に抽象度が高いですが、Attack Tree を作成することで、脅威を実現させうる具体的な攻撃手法を洗い出すことができます。

ATTACK TREE のイメージ図



Attack Tree の作成手順

【手順１】自社にとって起こってほしくない事象を決め、起点とします。
【手順２】起点に定めた事象を実現させうる攻撃手段を一段下に記載します。
※攻撃手段を考える際には、STRIDEの観点で考えてみましょう。
【手順３】このような作業を繰り返し行い、脅威を実現させる手段を洗い出します。
※Attack Tree の上下のつながりの関係は、目的と手段の関係になっています。

One point

Attack Tree の作成には相応の時間を要するため、すべての脅威に対して Attack Tree を作成することは現実的ではありません。そのため、対象の脅威を絞り込む必要があります。ここでは、脅威を絞り込む上での指針の例を 3 点示します。

①インタフェースに着目する方法
　通信インタフェースにおける脅威はネットワークからの攻撃が可能な場合があり、物理的なアクセス等を必要とする脅威に比べて攻撃元が広範です。

② データの入出力に着目する方法
　機器に対する脅威としては、出力されるデータよりも入力されるデータのほうが重大な脅威になりやすいことが多いため、入力されるデータに対する分析の優先度を上げることを検討します。

③脅威が実現した場合の影響に着目する方法
　例えば、機密性の観点で、機器の任意の情報が漏えいしうる脅威が存在した場合、一部の情報が漏えいするような脅威と比べると優先度が高いです。

出典：経済産業省
機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き(別冊 1 脅威分析及びセキュリティ検証の詳細解説書)
https://www.meti.go.jp/policy/netsecurity/wg3/2_bessatsu1_20210419.pdf

Day5
1.脅威と脆弱性に対応する

クラウド導入を想定した脅威分析

クラウドサービスは、利用者側が最低限のインターネット接続環境を用意すれば、インターネットを通じてアプリケーションやストレージなどのさまざまなサービスの提供が受けられます。企業や組織ではクラウドサービスの利用が進んでいます。ただし、クラウド導入時には想定される脅威を意識し、クラウド事業者が対応するセキュリティ対策、社内で対応しないといけないセキュリティ対策を意識し、脅威に対応できるのかを検討する必要があります。

Point① クラウドサービスを利用する際の脅威の例

クラウドサービスを利用する際は以下のような脅威が想定されます。長期的な活用にあたってはクラウドサービス提供事業者の事業運営などを検討しないといけない場合もあります。

脅威の例	脅威に対する対策の例
盗聴 インターネット回線を利用してデータのやり取りを行うため、通信の盗聴等の可能性がある	通信の暗号化が行われている
なりすまし ID管理の不備、認証の不備などで第三者が正規のユーザーとしてログインできる	２要素認証機能やアクセス制限、環境分離が行われている
情報漏えい データの管理方法や運用方法のセキュリティ対策が不十分となっている	保存時や持ち出し時は暗号化している

Point② システム面だけでなく運営会社についても確認

クラウドサービス提供事業者自体がセキュリティをおろそかにしていると、安心してサービスを利用できません。企業運営の中でセキュリティ対策をどのようにしているかを確認することも重要になります。

- ◆ JIPDEC や JQA 等で認定している情報管理に関する公的認証 （ISMS、プライバシーマーク等） が取得されているか？
- ◆ 侵入、操作、データ取得等への対策について、第三者の客観的な評価を得ているか？
- ◆ データにアクセスできる利用者が限定されているか？
- ◆ 提供者側でのデータ取扱環境が適切に確保されているか？
- ◆ システムとやり取りされる通信の暗号化強度は適切か？

テキスト第2回より再掲

個人情報や社内セキュリティの規程の確認、システムへのアクセス権限、第三者評価の有無などを把握するため、クラウドサービス提供事業者へ質問票などを使い状況をヒアリングする場合もあります。

自社の脆弱性

セキュリティにおいて、弱点のことを脆弱性と言います。今回は、脆弱性について詳しく見ていきましょう。

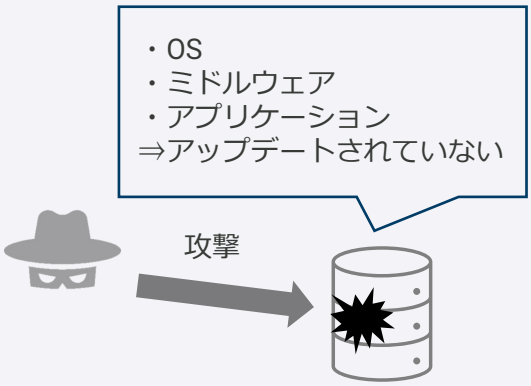
Point① 人の脆弱性

どれだけシステムを強化しても人が介在する場合、人が脆弱性となる可能性があります。ルールの認識不足により発生する行動や物忘れなども人の脆弱性といえます。

Point② システムの脆弱性

システムを構成する機器を正しく管理しないと、脆弱な部分を残したまま稼働する状態となります。システムをより安定した状態で稼働させるためには、OSやアプリケーションのバージョン、アクセス権限や閲覧権限などの設定を正しくする必要があります。

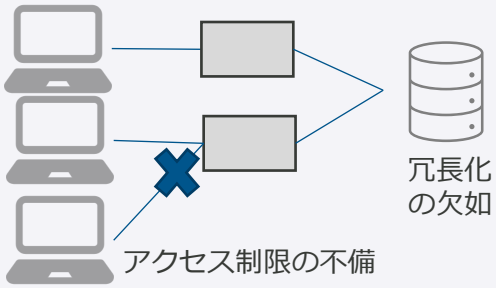
また、OSやアプリケーションにはバグが存在する場合もあり現在は正常でも今後脆弱性が発生する可能性があります。



Point③ ネットワークの脆弱性

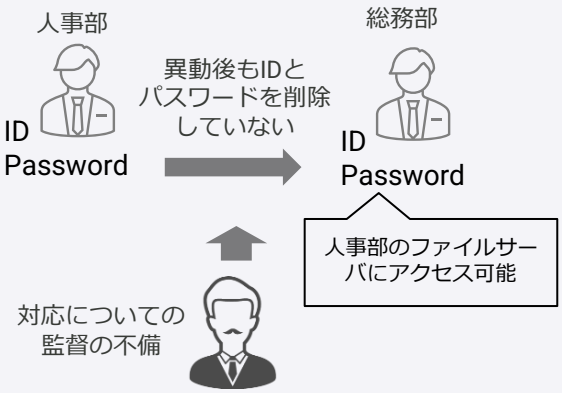
通信環境においても正しく設定や管理を行う必要があります。アクセスリストの不備などにより本来通信できない人が通信できてしまうなどの脆弱性につながります。

設定不備はもちろんのこと、経路の障害で通信ができなくなると可用性の喪失といったことにもなり脆弱な部分とも言えます。



Point④ 運用の脆弱性

事業運営におけるプロセスにおいて脆弱性が出ることもあります。例えば、承認フローの不備などが事故につながってしまう場合があります。また、監督等がおろそかになることで、セキュリティ事故が起きてしまうこともあります。運用面で脆弱性が無いかを検討し、運用ルールを見直すことも重要です。



Day5

1.脅威と脆弱性に対応する

システムの脆弱性をチェック

システムを構成する機器類は適切な管理をしないと、脆弱性が発生します。代表的な脆弱性を記載しますので、自社のシステムで脆弱性の有無や影響の可能性について確認をしてみましょう。

機器に内在しうる代表的な脆弱性の確認

項目	代表的な脆弱性	概要・脆弱性が悪用された場合の影響	チェック
アクセス制御の不備	適切でない権限管理	特定の権限を必要とする機能やファイルに、許可されていない利用者がアクセス可能となる。	
	最小権限の原則の違反	最小権限の原則が守られておらず、許可されていない権限が付与されている。	
	適切でない認可	本来アクセスできない機能やファイルに、許可されていない利用者がアクセス可能となる。	
	デフォルトアクセス設定の不備	機能やファイルのデフォルトアクセス設定が適切に設定されておらず、許可されていない利用者がアクセス可能となる。	
入力検証の不備	クロスサイトスクリプティング	機器に付随する Webコンソールにおいて、不正なスクリプトが実行可能となる。	
	OSコマンドインジェクション	機器に付随する Webコンソールにおいて、不正なOS コマンドが実行可能となる。	
通信暗号化機能の欠如	十分でない資格情報の保護	通信上の認証資格情報が第三者によって盗聴される可能性がある。	
	重要情報の非暗号化	重要情報が平文で通信されており、第三者によって盗聴される可能性がある。	
	脆弱な暗号化方式	使用が推奨されない暗号化方式を使用しているため、暗号を解読される可能性がある。	
	十分でないデータ真正性の確保	通信データに関して十分な検証がなされず、中間者攻撃によってなりすましや不正コードの挿入を受ける可能性がある。	
認証情報管理の不備	平文での認証情報の格納	認証情報が平文で格納されており、第三者が不正アクセス等によって窃取できる。	
	ハードコーディングされた認証情報	認証情報がプログラムに埋め込まれており、利用者によって変更することが難しく、悪用される可能性がある。	
	脆弱な認証情報	第三者が容易に推測できる ID・パスワードが使用されており、不正アクセスを受ける可能性がある。	
認証設定の不備	ブルートフォース攻撃	ID・パスワードの総当たり攻撃によって、認証が回避可能。	
	認証機構の迂回	正規の認証機能を迂回することができ、認証情報を有さない第三者からの不正アクセスを受ける可能性がある。	
	バッファオーバーフロー	許容以上のデータを挿入することで、メモリ上のバッファ領域を超えてデータの書き換えが可能となる。	
	フォーマット文字列攻撃	書式文字列関数（※1）の機能を悪用し、不正コー ドが実行可能となる。 ※1：C 言語の場合、printf()関数や syslog()関数等のライブラリ関数を指す	

出典：経済産業省
機器のサイバーセキュリティ確保のための セキュリティ検証の手引き
https://www.meti.go.jp/press/2021/04/20210419003/20210419003-1.pdf

Day5
1.脅威と脆弱性に対応する

システムの脆弱性に対処する

システムを構成する機器類は適切な管理をすることで脆弱性をいち早く発見・認識し対応することが求められます。

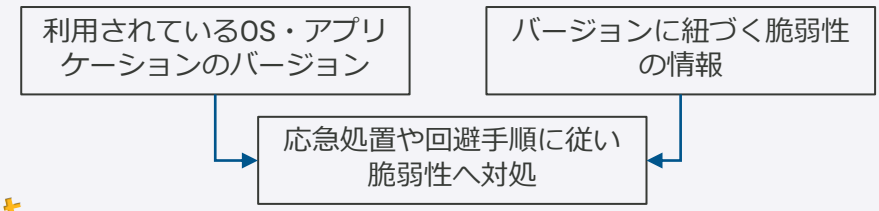
Point① システムを管理し脆弱性を把握する

システムの脆弱性に対処するために、以下のような情報を整理することが重要になります。

<table>
<tr><th>ドキュメント</th><th>概要</th></tr>
<tr><td>ネットワーク構成図</td><td>物理構成図や論理構成図により管理を行います。クラウド利用などがある場合には、社内だけでなく、外部の情報が盛り込まれる場合もあります。</td></tr>
<tr><td>機器管理表</td><td>システムを構成する機器について管理を行います。機器管理表には以下のような情報を整理します
<table>
<tr><td>OSバージョン</td><td>ミドルウェアバージョン</td></tr>
<tr><td>管理責任者</td><td>シリアル情報</td></tr>
<tr><td>IPアドレス</td><td>保守期間</td></tr>
</table></td></tr>
<tr><td>アプリケーション管理表</td><td>サーバやパソコンで利用しているアプリケーションの管理を行います。
<table>
<tr><td>アプリケーション
バージョン</td><td>主な利用方法</td></tr>
<tr><td>管理責任者</td><td>契約期間</td></tr>
</table></td></tr>
</table>

Point② 脆弱性に対処する

バージョン情報を管理することで、そのバージョンに存在する脆弱性をより早く把握することにつながります。



One point

近年、クラウドサービスは企業だけでなく、個人でも活用されています。特にクラウドストレージのようにファイルをアップロードできるようなサービスは無償で利用できるものも多いです。これら個人のサービスを管理部門の許可・承認なしに利用することを『シャドーIT』と呼ばれています。現在これらのシャドーITが問題になる場合が多くなっています。

シャドーITは、個人用アカウントのクラウドサービスに、社内の機密情報を含むファイルをアップロードしてしまう等、情報漏えいのリスクを高めることになります。

Day5

1.脅威と脆弱性に対応する

機器管理表の作成

機器管理表はホストコンピュータやサーバ及びPC等のハードウェア資産を一覧形式で記述したものです。機器情報を管理することで、脆弱性についていち早く把握することにつながります。

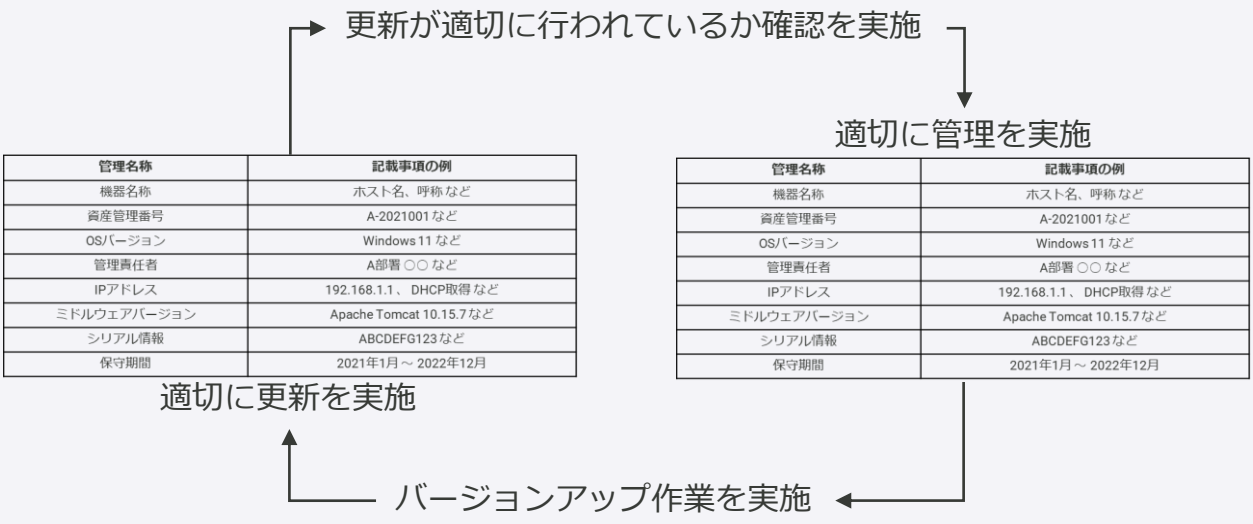
Point① 機器管理表の作成

機器管理表の作成のため、以下のような項目をもとに一覧で管理します。ネットワーク構成図などとも連動するように管理することで、「不要な機器が社内ネットワークに接続されていないか」などという確認を行うことができます。

管理名称	記載事項の例
機器名称	ホスト名、呼称 など
資産管理番号	A-2021001 など
OSバージョン	Windows 11 など
管理責任者	A部署 ○○ など
IPアドレス	192.168.1.1 、 DHCP取得 など
ミドルウェアバージョン	Apache Tomcat 10.15.7 など
シリアル情報	ABCDEFG123 など
保守期間	2021年1月 ～ 2022年12月

Point② 機器管理表を運用する

機器管理表を作成して終了ではありません。各種アップデートを行った場合には、適切に運用を行う必要があります。作業後には差分箇所を更新することを忘れず、定期的に更新が適切にされているかの確認を行います。確認は実際に機器を確認する場合もあれば、例えば作業計画書や報告書と照らし合わせて確認をするという方法もあります。



Day5

1.脅威と脆弱性に対応する

アプリケーション管理表の作成

パソコンやサーバでは多くのアプリケーションやソフトウェアが動作しています。これらにも脆弱性が発生する可能性はあり、管理しておくことが重要となります。

Point① アプリケーション管理表の作成

アプリケーション管理表の作成のため、以下のような項目をもとに一覧管理します。また、ソフトウェアも併せて管理を行います。

管理名称	記載事項の例
アプリケーション・ソフトウェア名称	Zoom、DropBox など
バージョン情報	10.15.7
管理責任者	A部署 ○○ など
利用用途	オンライン会議で利用
利用機器・利用者	ホスト名、ユーザー名

Point② 目に見えない資産を管理する

アプリケーションやソフトウェアは物理的なものではないため目に見えません。そのため、パソコンやサーバといった機器を操作しながら把握する必要性があります。まずは、自分たちが利用しているアプリケーションやソフトウェアにはどのようなものがあるかを考えましょう。

また、一つのパソコンで複数のアプリケーションやソフトウェアが動いていることが一般的です。一つ一つ整理をしながら管理をしていきましょう。

Webブラウザ：Google（バージョンXXXXXXXX）
コミュニケーション：Zoom（バージョンXXXXX）
メール：Outlook（バージョンXXXXXXXX）
ドキュメント：Office（バージョンXXXXXXXX）
PDF：Acrobat Reader（バージョンXXXXXXXX）

One point

アプリケーションやソフトウェアの利用には使用許諾（ライセンス）が必要となります。適切な管理がなされていないと、ライセンスが不足するなど、事業運営に直接的な影響を及ぼす可能性もあります。また、購入したソフトウェアが「使用許諾契約書通りに使われてれているか」を管理する事も重要となり、万が一ライセンス利用違反ということになれば犯罪にあたります。

また、違法ソフトウェアのダウンロードやソフトウェアの不正コピーなども犯罪です。購入されているライセンスが適切に利用されているかを確認するだけでなく、アプリケーション管理表などと合わせて管理をします。違法なライセンスにより、アプリケーションが利用されていないかなどを確認することも求められます。

Day5

1.脅威と脆弱性に対応する

人の脆弱性に対処する

システムやネットワークの運用をどんなに管理し、脆弱性に対応したとしても、最終的に操作をする人が脆弱性に対処する必要があります。

Point① ソーシャルエンジニアリングへの対処

ソーシャルエンジニアリングとは、技術的な要素を用いることなく、ユーザーIDやパスワードなどの重要な情報を入手する方法です。

他にも、以下のような事例があります。

・従業員が機密情報を書いたメモ用紙をゴミ箱に捨ててしまい、悪意のある第三者がごみ箱の中からメモ用紙を探し出した結果、情報が漏えいした。
・悪意のある第三者が電話で役職者やヘルプデスクの担当者を名乗り、電話の受信者がそれを信用してしまったため、情報を聞き出されてしまった。

これらに対処するためには、攻撃手法を理解して、社内のルールを把握することが重要です。必要に応じて教育を行う、行動できているかのチェックを行うことが有効です。

Point② 標的型メールへの対処

事例として多い事象にメールに関するものが多く見受けられます。ビジネスツールとしてメールは多くのシーンで利用されています。そのため、攻撃者が送ってきた不審な添付ファイルを利用者が開いてしまい、ウイルスに感染してしまうというものです。

誤送信防止のため、メールアドレス内の文字に注意
m → rn、w → vv 、l(アイ) と I(エル)　など

添付ファイルに注意
- 見知らぬ相手からの添付ファイル
- 拡張子とアイコンに相違がある
- 開いたらマクロの有効を求められる

メールに関係する攻撃はEmotetに代表されるように、多くの事例が確認され、さらに一度収束したような攻撃が時を置いてまた活発化する事例も見られます。攻撃手法を理解して受信者が気を付けることが重要です。

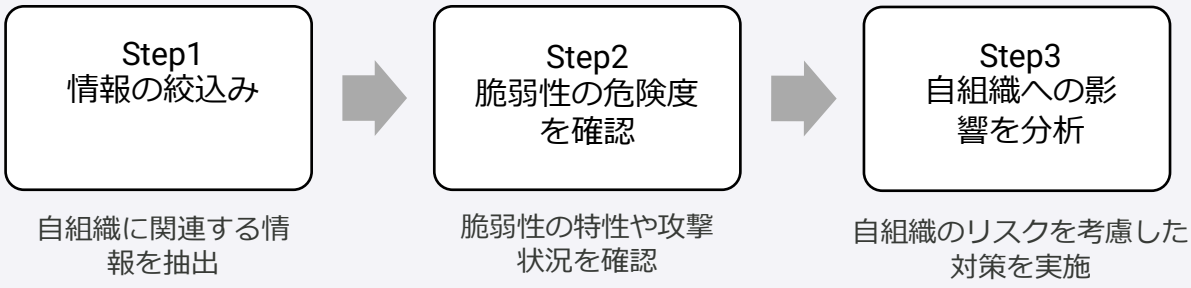
One point

人の脆弱性は体調によっても変化をします。日頃セキュリティ意識が高い人でも、仕事が忙しく疲労がたまっている時には、判断を誤る可能性があります。また熱などの風邪のときには注意力が散漫になりがちです。
車の運転と同じように、注意力が散漫になっているなと感じたら休憩を取りながら業務をすることも重要です。自分の体調を意識し、危険な可能性があるということを理解し場合によっては休むことで減らせるセキュリティ事故もあります。

脆弱性を調査する

効果的な脆弱性対策を実施するには、多数の情報から自組織に関連する脆弱性情報の収集を行い、組織への影響度も考慮したうえで早期に対応を判断することが重要となります。

情報収集から分析までのSTEP



情報の絞込み

多数の脆弱性関連情報から自組織に関係があるソフトウェアやアプリケーションの情報を収集します。情報の収集、絞り込みにはIPAなどが提供するサービスやツールなどを使用するといった方法があります。日々多くの脆弱性が発見されており、自社に関係あるものを絞り込んでいくためには、自社で使っているソフトウェアやアプリケーションの管理表と合わせて対応していくことが重要です。

脆弱性の危険度(深刻度)を確認

脆弱性関連情報データベースにて公開している脆弱性関連情報において危険性を確認します。どのようなシーンで攻撃が可能なのか、攻撃の難易度はどの程度なのかを確認します。

自組織への影響を分析

最終的には公開された脆弱性は自社にとって影響が出るか確認を行います。分析では以下を中心に見ていきます。

攻撃の可能性有無の確認	攻撃が自社の環境において実現可能かを確認します。
利用されている機器などの数	社内でどの程度ツールを利用しているか確認します。
利用している機器の重要度	機器の重要度がどの程度か確認します。 ※機器に保存されている資産などについても考慮します。

出典：情報処理推進機構（IPA）
「脆弱性対策の効果的な進め方（実践編）第 2 版～脆弱性情報の早期把握、収集、活用のスヽメ～」をもとに作成
https://www.ipa.go.jp/files/000071660.pdf

Day5

1.脅威と脆弱性に対応する

脆弱性を調査する

脆弱性の情報は日々更新されています。また、自社には関係ない情報もあります。いかに早期に情報を把握・収集するかが大切です。情報処理推進機構（IPA）では脆弱性対策情報の早期把握、収集、活用のそれぞれのフェーズに役立つ支援ツールやサービスを公開しています。

IPA が提供する脆弱性対策支援サービス・ツールの抜粋

フェーズ	目的	サービス・ツール名	関連リンク等
早期把握	脆弱性情報の収集（緊急度・危険度高） 脆弱性情報の受信（組織内への案内等）	IPA 重要なセキュリティ情報	https://www.ipa.go.jp/security/announce/about.html（概要）
			https://www.ipa.go.jp/security/announce/alert.html（一覧）
			https://twitter.com/ICATalerts/（twitter @ICATalerts）
		注意警戒情報サービス	https://jvndb.jvn.jp/alert/
	脆弱性情報の受信（組織内への案内等）	サイバーセキュリティ注意喚起サービスicat for JSON	https://www.ipa.go.jp/security/vuln/icat.html
収集	脆弱性情報の収集（すべての脆弱性）	脆弱性対策情報データベース JVN iPedia	http://jvndb.jvn.jp/
			https://twitter.com/jvnipedia/（twitter @JVNiPedia）
	脆弱性情報の収集（自組織すべて）（システム毎）（開発製品毎）	MyJVN 脆弱性対策情報収集ツール	http://jvndb.jvn.jp/apis/myjvn/mjcheck3.html（Adobe Air 版）
	脆弱性情報の収集（日本で広く利用されているサーバ用オープンソースソフトウェア）	サーバ用オープンソースソフトウェアに関する製品情報およびセキュリティ情報	https://www.ipa.go.jp/security/announce/sw_securityinfo.html
活用	自組織への脆弱性の影響度を確認	CVSS 計算ソフトウェア	https://jvndb.jvn.jp/cvss/ja/v31.html
	PCの主要ソフトウェアが最新かを確認	MyJVN バージョンチェッカ	http://jvndb.jvn.jp/apis/myjvn/vccheckdotnet.html（.Net Framework 版）

出典：情報処理推進機構（IPA）
脆弱性対策の効果的な進め方（実践編）第 2 版～脆弱性情報の早期把握、収集、活用のスヽメ～
https://www.ipa.go.jp/files/000071660.pdf

こんな事例も

自社に対する脆弱性の情報把握には、システムに関する知識など技術的な要素が求められます。しかしながら、セキュリティ担当者が必ずしも技術に詳しいというわけではありません。技術に詳しい社員に協力をしてもらったり、システムや機器の保守を依頼している企業との連携も重要になります。

保守担当者が脆弱性の情報にいち早く気づき顧客へ対応の打診をしたところ、業務が忙しいためにアップデートに対応する時間が無いといった事例はよくあります。セキュリティの担当者は脆弱性の理解を高め、保守担当者と連携して、対応を検討していくことも重要です。

JVNを利用した脆弱性の確認

JVNとは、国内外の脆弱性対策情報を収集・蓄積しているデータベースです。脆弱性の概要や CVSS 値、関連リンク等を掲載しています。CVSS 値を確認することで、脆弱性自体の深刻度を確認することができます。

活用方法

【手順１】JVN iPedia 検索ページへアクセスします。
http://jvndb.jvn.jp/search/index.php?mode=_vulnerability_search_IA_VulnSearch&lang=ja

【手順２】キーワード または 自組織・開発製品で利用しているソフトウェアを指定して検索を実施します。

【手順３】検索により、脆弱性対策情報一覧が表示されます。IDのリンクを開くとより詳細な情報を確認することができます。

ID	タイトル
JVNDB-2014-006127 (JVNVU#90369988)	Android 用 ZOOM Cloud Meetings アプリケーションにおけるサーバになりすまされる脆弱性

【手順4】脆弱性の概要や CVSS 値、影響を受けるソフトウェアや対象バージョン、対策方法を確認します。

JVNDB-2014-006127

Android 用 ZOOM Cloud Meetings アプリケーションにおけるサーバになりすまされる脆弱性

概要

Android 用 ZOOM Cloud Meetings (別名 us.zoom.videomeetings) アプリケーションは、SSL サーバからの X.509 証明書を検証しないため、サーバになりすまされ、重要な情報を取得される脆弱性が存在します。

CVSS による深刻度 (CVSS とは?)

CVSS v2 による深刻度
基本値: 5.4 (警告) [NVD値]

- 攻撃元区分: 隣接
- 攻撃条件の複雑さ: 中
- 攻撃前の認証要否: 不要
- 機密性への影響(C): 部分的
- 完全性への影響(I): 部分的
- 可用性への影響(A): 部分的

想定される影響

中間者攻撃 (man-in-the-middle attack) により、巧妙に細工された証明書を介して、サーバになりすまされ、重要な情報を取得される可能性があります。

対策

ベンダ情報および参考情報を参照して適切な対策を実施してください。

ベンダ情報

zoom

- Google play : us.zoom.videomeetings

CWEによる脆弱性タイプ一覧 CWEとは?

1. 暗号の問題(CWE-310) [NVD評価]

共通脆弱性識別子(CVE) CVEとは?

1. CVE-2014-5811

参考情報

1. JVN : JVNVU#90369988
2. National Vulnerability Database (NVD) : CVE-2014-5811
3. US-CERT Vulnerability Note : VU#582497

出典：JVN iPedia
「脆弱性対策情報データベース」をもとに作成
https://jvndb.jvn.jp/

脆弱性を狙った攻撃事例

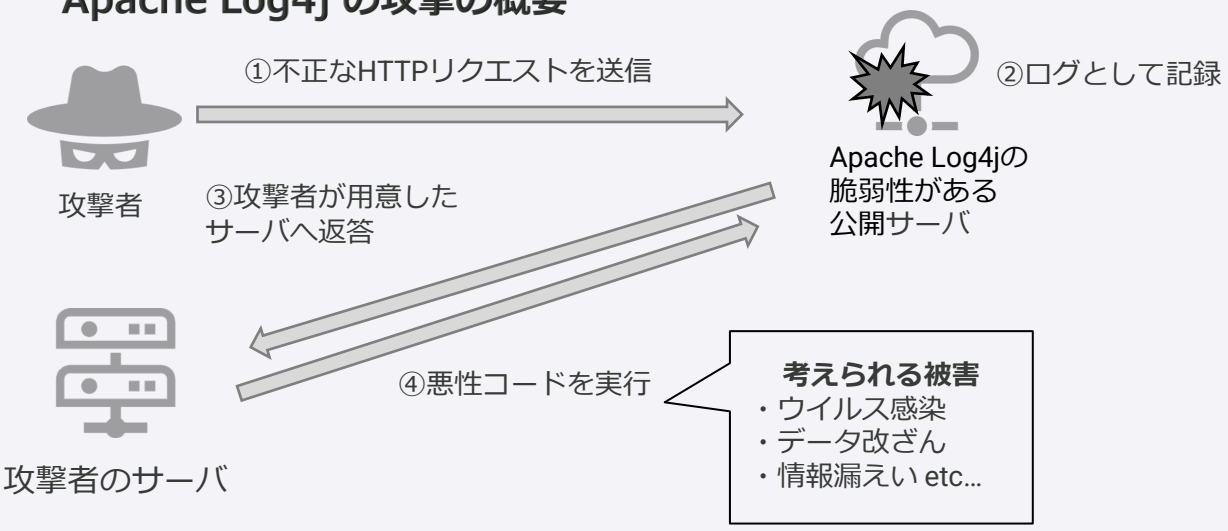
毎日、様々な脆弱性が見つかっています。今回は、2021年12月に公表された、Apache Log4j の脆弱性について紹介します。

Point① Apache Log4j の概要

Apache Log4jとは、Apache Software Foundation がオープンソースで提供している Java ベースのロギングライブラリです。 主にWebサーバなどのログ管理で利用されています。この Apache Log4j において、任意のコードが実行可能な脆弱性が発見されました。深刻度も最大10.0と緊急での対応が求められるほどでした。想定される影響として、「遠隔の攻撃者により細工された文字列を Log4j がログに記録することにより、システム上で任意の Java コードが実行される可能性がある」ためです。

この脆弱性の出現により、多くの企業で対応に迫られたのではないでしょうか？

Apache Log4j の攻撃の概要



Point② Apache Log4j の脆弱性への対策

開発者により、本脆弱性を修正した以下のバージョンが提供されています。開発者が提供する情報をもとに、最新版にアップデートしてください。なお、本アップデートでは、Log4j のLookup 機能が削除されており、JNDI へのアクセスがデフォルトで無効化されています。

* Java 8のユーザ向け修正版
  * Log4j 2.17.1
* Java 7のユーザ向け修正版
  * Log4j 2.12.4
* Java 6のユーザ向け修正
  * Log4j 2.3.2

出典：JVN iPedia
脆弱性対策情報データベース
https://jvndb.jvn.jp/ja/contents/2021/JVNDB-2021-005429.html

Day5
2.リスクを検討する

リスクとは

脅威・脆弱性を把握した後に、自社のリスクを把握していきます。把握したリスクに対して対策を立てていくことになるので、リスクについて正しく検討していくことが重要です。

Point① リスクとは

リスク とは、将来のいずれかの時において、何か悪い事象が起こる可能性をいいます。セキュリティにおける悪い事象とは、情報資産の3要素（機密性・完全性・可用性）が侵害されることです。なお、リスクは「資産価値 × 脅威 × 脆弱性 × 発生可能性」によって算定されます。

Point② リスクをマネジメントする

リスク評価に基づき、リスクへの対応を行います。リスクを検討する際には、経営リスク管理の一環として判断・選択をすることが望ましいです。自社にとって最適の対応を選びます。

特定	どのようなリスクが存在するのか特定する
分析	影響度や発生確率を検討しリスクを分析する
対応	対応方法の検討や作業担当の分担を行い顕在するリスクに対応する
評価	取り巻く環境の変化に対応するため現状の評価を行い、定常的な評価や改善を行う

One point

継続したリスクマネジメントを行うためには、攻撃のトレンドや脆弱性を情報収集し分析や評価をする必要があります。情報セキュリティに対するリスクは、会社にとって様々です。すなわち、他社のリスクを聞いて対策を取るということは、本来のセキュリティ対策とはなりません。

リスクマネジメントは、顕在するリスクに対して、効率的な対策を施すことです。やみくもに対応をするのではなく、最小限の費用で最大の効果を目指します。また、セキュリティリスクも時代と共に変化することを意識し定期的な見直しが求められます。

Day5
2.リスクを検討する

CSFを利用した セキュリティリスクのマネジメント

サイバーセキュリティフレームワークは、組織の目的に対するサイバーセキュリティリスクのマネジメントを改善することで、リスクを低減するように設計されています。

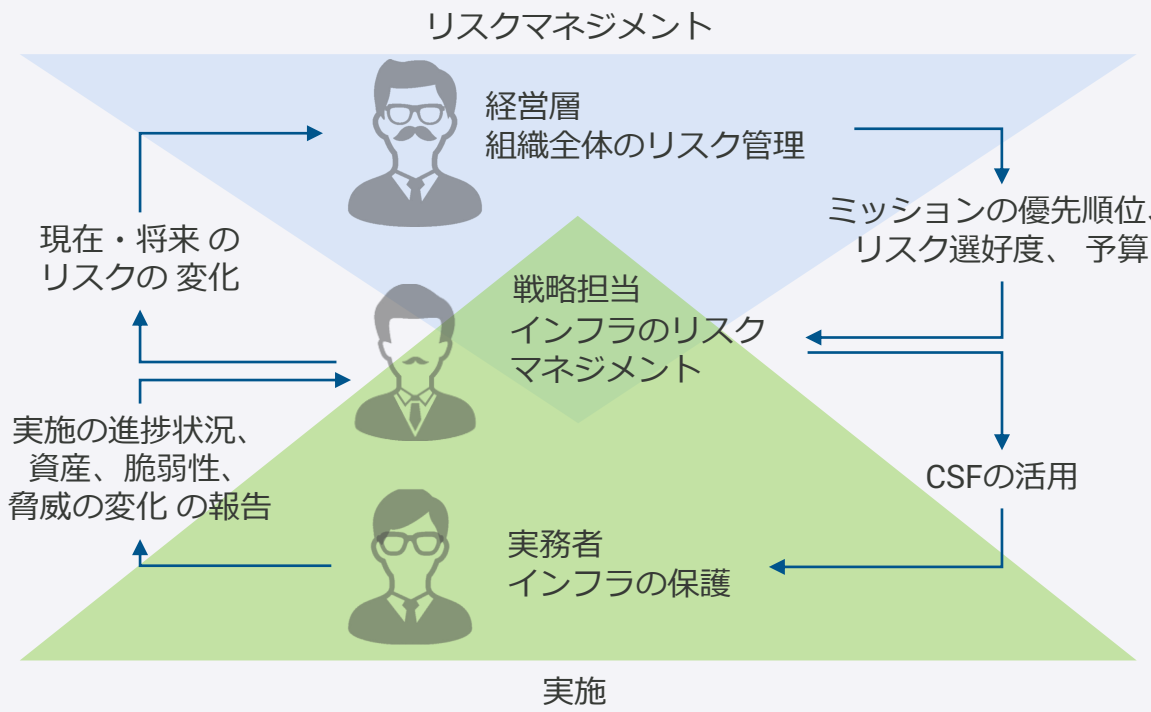
第3回のセミナーで紹介したサイバーセキュリティフレームワークを使い、現状の把握や目指すティアの検討を繰り返していくことがリスクマネジメントにつながります。特定・分析・対応・評価をCSFと合わせて実施することで、理想と現実のギャップ解消やリスク対応における優先度の把握、予算の割り当てなどのポイントを整理しやすくなります。

なお、必ずしも全てにおいてティア4を目指すことが重要ではなく、組織のビジネス上の要求事項、リスクの許容度、割り当て可能なリソースに応じて、カテゴリー毎に目指すべきティアを設定する事が重要です。

CSFを用いたリスクマネジメント

1. 現在行っているサイバーセキュリティ対策が目標のティアの選択にどのように影響するかを把握します。
2. 現在のティアの状況を確認・判断し、自組織のサイバーセキュリティリスクマネジメントに対する対応を評価します。
3. サイバーセキュリティ対策の現在の状態と目指す目標の状態を作成することで、サイバーセキュリティ上の優先順位を付けます。
4. 現在の状態を評価することで、個別のサイバーセキュリティ対策の手順が、期待されるサイバーセキュリティ上の成果をどの程度達成しているか把握します。

組織内の情報と意思決定の流れ（概略図）



出典：情報処理推進機構（IPA）
Framework for Improving Critical Infrastructure Cybersecurityをもとに作成
https://www.ipa.go.jp/files/000071204.pdf

Day5

2.リスクを検討する

リスクアセスメントを行う

リスクアセスメントとは、リスクを分析して評価することです。リスクアセスメントを行うことで、組織やシステムに内在するリスクの大きさや影響度を知ることができます。リスクアセスメントには下記のようなアプローチを行います。

詳細リスク分析

分析対象のシステム自体に対して、そのシステムもしくはそれにより実現されている事業を、「重要度」（あるいは損なわれた場合の被害レベル）「脅威」「脆弱性」の評価指標の下で、リスク分析を実施します。

ベースラインアプローチ

既存の標準や基準をもとに、想定する典型的なシステムに対して、予め一定の確保すべきセキュリティレベルを設定し、それを達成するためのセキュリティ対策要件を定め、分析対象となるシステムの対策の適合性等をチェックします。

非形式的アプローチ

組織や担当者の経験や判断によってリスク分析を実施します。

組み合わせアプローチ

複数のアプローチを併用し、作業の効率化、異なった評価視点の活用によって、分析精度の向上と、作業工数増大の回避を図ります。

手法	長所	短所
詳細リスク分析	・正確なリスク分析が可能 ・一度実施すると、ベースとして継続的にセキュリティレベル向上が可能 ・セキュリティ投資の優先順位等、組織として戦略的に検討していくことができる	・規模や手法によっては、かなりの工数がかかる
ベースラインアプローチ	・決められた対策要件をチェックするため、作業工数が小さい ・既存の基準としレベルの評価をするため、目安としては利用できる	・基準への適合具合のチェックであり、自社のシステムの状況に沿ったリスク分析にならない場合がある ・事業被害を起こさない裏づけには間接的にしかならない ・自社のシステムに沿った選択基準が得られない可能性がある
非形式的アプローチ	・経験値を活用するので、属人的ではあるが工数は小さい	・厳密にはリスク分析にならない ・起こりうる脅威、あるいは新たな脅威に対しての対応が困難である ・属人的であり、継続的なセキュリティレベルの向上は困難である
組み合わせアプローチ	・上記、各手法の長所の取り込みが可能 ・上記、各手法の短所の改善が可能	・どう組み合わせるのか、それぞれのシステムや事業者によって異なってくるが、その指針は示されていない。

出典：情報処理推進機構（IPA）
「制御システムのセキュリティリスク分析ガイド第２版」をもとに作成
https://www.ipa.go.jp/files/000080712.pdf

ミニワーク
～考えてみよう～

ミニワークテーマ

ATTACKツリーを埋めてみましょう。

ATTACKツリーのサンプルを用意しました。今回は物理的な被害を想定して考えてみましょう。

鍵付きキャビネットが利用できない

キャビネットが利用できなくなるような要因を2つ考えてみましょう。

右側で上げた要因が起こりうる、原因を2つ考えてみましょう。

右側で上げた原因が起こりうる、状況を2つ考えてみましょう。

Day5
2.リスクを検討する

リスクを算出する

リスクを分析して評価するためには、計算式などを用いて数値化していきます。最終的には受容できるリスクの数値を定め、リスク低減策などの実行の結果、リスクが受容できるかを検討します。ここでは、詳細リスク分析をもとに算出していきます。

【手順１】資産を洗い出し、脅威と脆弱性を各資産ごとに検討する
※資産の洗いだしや脅威と脆弱性の整理には、独立行政法人情報処理推進機構(IPA)が公開しているリスク分析シートが便利です。

リスク分析シート情報資産管理台帳

業務分類	情報資産名称	備考	利用者範囲	管理部署	媒体・保存先	個人情報の種類			評価値				保存期限	登録日	現状から想定されるリスク（入力不要・自動表示）				
						個人情報	要配慮個人情報	特定個人情報	機密性	完全性	可用性	重要度			脅威の発生頻度 ※「脅威の状況」シートに入力すると表示	脆弱性 ※「対策状況チェック」シートに入力すると表示	被害発生可能性		リスク値
人事	社員名簿	社員基本情報	人事部	人事部	事務所PC	有			2	0	0	2		2016/7/1	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	4 リスク大
人事	社員名簿	社員基本情報	人事部	人事部	書類	有			2	2	2	2		2016/7/1	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	2 リスク中
人事	健康診断の結果	雇入時・定期健康診断	人事部	人事部	書類		有		2	2	1	2	5年	2016/7/1	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	2 リスク中
経理	給与システムデータ	税務署提出用源泉徴収票	給与計算担当	人事部	事務所PC			有	2	2	1	2	7年	2016/7/1	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	4 リスク大
経理	当社宛請求書	当社宛請求書の原本（過去3年分）	総務部	総務部	書類				1	1	1	1		2016/7/1	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	1 リスク中
経理	発行済請求書控	当社発行の請求書の控え（過去3年分）	総務部	総務部	書類				1	1	1	1		2016/7/1	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	1 リスク中
共通	電子メールデータ	重要度は混在のため最高値で評価	担当者	総務部	事務所PC	有			2	2	2	2		2016/7/1	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	4 リスク大
共通	電子メールデータ	Gmailに転送	担当者	総務部	社外サーバー	有			2	2	2	2		2016/7/1	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	4 リスク大

出典：情報処理推進機構（IPA）
中小企業の情報セキュリティ対策ガイドライン　リスク分析シート
https://www.ipa.go.jp/security/keihatsu/sme/guideline/

【手順2】洗い出した情報資産ごとにリスク値を算出する

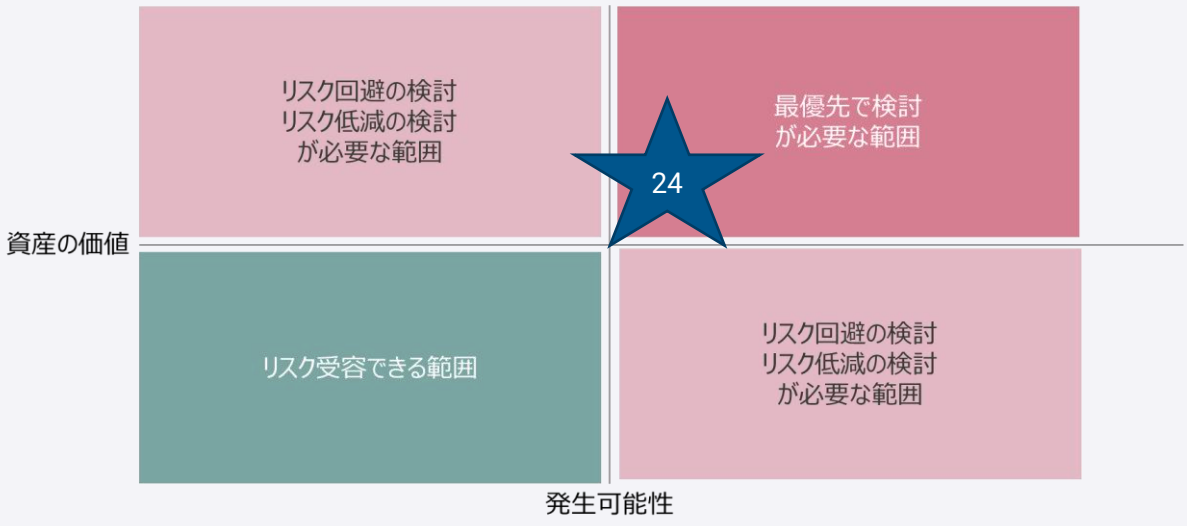
リスクを算出する計算式

リスク ＝ 資産価値 × 脅威 × 脆弱性 × 発生可能性

リスク算出の例

リスク＝評価値(2) × 脅威有(2) × 脆弱性有(2) × 発生可能性は高い(3) ＝ 24

※受容できる数値は各企業ごとに判断をして決めていきます。



Day5
2.リスクを検討する

リスクを算出する

リスク分析の手法は一つではありません。米国標準技術院（NIST）が推奨する定量的リスクアセスメントの手法として、ALE法というものがあります。ALE法の最大の特徴は金額でリスクを算出することです。年間の予想損失額 ALE（Annualized Loss Expectancy）を求めることにより、年間のセキュリティ予算を決定するための指標やセキュリティ対策の費用対効果を測定する指標となります。

Point① 年間予想被害額を求める計算式

年間予想被害額を ALE (Annualized Loss Expectancy) とします。

ALE （年次損失予測） = SLE（単一損失予測） × ARO（年次発生率）

・EF (Exposure Factor) = 特定の脅威によって起こる資産損失のパーセンテージ
・AV（Asset Value） = 資産価値
・SLE (Single Loss Expectancy) 単一損失予測 = AV（資産価値） × EF（資産損失確率）
・ARO (Annualized Rate of Occurrence) 年次発生率 =1 年間に脅威が起こる頻度の推定値

出典：JNSA
「情報セキュリティ会計に関する検討報告書～ガイドライン策定に向けて～」をもとに作成
https://www.jnsa.org/houkoku2004/kaikei_report.pdf

～Note～

Day5
2.リスクを検討する

計算式で出した損失予想

ALE法にのっとり、個人情報漏えいが発生した場合の想定被害金額を試算してみましょう。

企業プロファイル（想定）

想定する企業は、ECサイトで販売をおこなう事業者です。個人情報は分散されたサーバに保管しており、約５万人の個人情報を保有しています。毎年ヒヤリハットの統計をしており、セキュリティ事故の可能性は約10年に1回程度となっています。サーバが分割されているので、基本的には全ての情報が流出するとは考えておらず、1回の被害で全体の40%程度と想定しています。

セキュリティ事故に伴う費用の換算

セキュリティ事故が発生した際にかかる費用は1回の事故で以下のように考えています。

項目		費用（想定）
業務継続費用	対策組織業務に係る人件費（1か月分）	500万円
	損害賠償費用（訴訟参加費＝0.1%）	36万円
	弁護士費用・裁判費用	30万円
見舞い品費用	見舞い品代＋送料他（2万人分）	1400万円
謝罪訪問費	謝罪訪問に掛かる費用（10人分）	110万円
広報費用	謝罪広告費	なし
	情報公開ページ作成費用（2回）	10万円
臨時的な対策費用	コールセンター設置費用（1ヶ月分）	500万円
	問い合わせ窓口常駐人員（1ヶ月分）	200万円
合計		2786万円

出典：JNSA
「発生確率調査と2010年個人情報漏えい調査の報告」をもとに作成
https://www.jnsa.org/seminar/2011/0608/data/1C_incident.pdf

被害損額の算出の計算

流出人数： 50000 × 0.4 = 20000人
SLE：事故1回あたり対応費用 = 2786万円
ARO：1 ÷ 10 = 10%（1年間の発生確率）
ALE： 2786万円 ×10% = 278.6万円

対策費用等の検討

ALEの算出結果として278.6万円という結果が出ました。1年間の個人情報流出にかかわるセキュリティ対策の金額の基準といえます、278.6万円を下回る対策が立てられれば投資対効果として優れていると言えます。また、もしこの金額を対策費として大きく超えるようならば、リスク回避の検討も対策の一つといえます。

ミニワーク
～考えてみよう～

ミニワークテーマ

リスクを算出してみましょう。

こんなシチュエーションにおける年間予想損失額を考えてみましょう。

ある会社では、1000人の個人情報を保有しており、一人当たりの資産価値を3万円とし換算しています。この会社では、個人情報流出のセキュリティ事故の可能性を考えたとき、すべての情報が一度に流出する可能性は低いと考えています。しかしながら一部の情報が流出する可能性が高く、分析の結果、保有する個人情報の10%が漏えいする可能性があるとしています。また、過去の経験から漏えいのようなセキュリティ事故は5年に1回です。

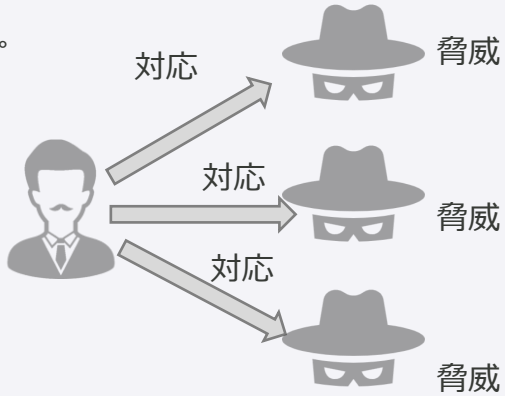
この時、この会社の個人情報漏えいのリスクにおける年間予想損失額はいくらになるでしょうか？

～Note～

脅威分析の具体例
～STRIDEの利用～

STRIDEを利用した脅威分析を行った事例

ある企業では、脅威分析に課題を持っていました。脆弱性は自分達のことなので、ヒアリングや業務の見直し、脆弱性診断などで把握ができました。しかし、脅威については、なかなか把握がしづらい状況でした。自分たちの会社も攻撃の対象になるかもしれないと常に心配していました。しかし、すでに出回っている攻撃の対応では、これから起こる脅威には対応ができません。よりセキュリティを強化していくためには、これから起こる可能性がある脅威に対応をしていきたいと考えていました。



そこで、 脅威分析の一つの考え方であるSTRIDEを使って分析を行いました。現在発生している攻撃から脅威を考えるのではなく、攻撃の要素となるSTRIDEをもとに脅威を考えることにしました。初めはSTRIDEだけで考えようとしていましたが、なかなかうまくいきませんでした。考えが四方八方に広がり、まとまらなかったのです。ネットワーク構成図や業務フロー図を見ながら検討をすることで、自社にとっての脅威がわかるようになってきました。

STRIDE分析の例	
要素名	**分析結果**
Spoofing （なりすまし）	ID・パスワードの管理が不十分でなりすましに利用される 共有アカウントがあり操作履歴等が取れず、なりすましが可能になる
Tampering （改ざん）	ファイルへのアクセス制限が不十分で偶発的な改ざんの可能性がある
Repudiation （否認）	アクセス権限を設定していないので、不正なアクセスが実行できる
Information Disclosure （情報漏えい）	社内通信や社内サーバの情報は暗号化されていないので情報を見ることができる。
Denial of Service （サービス妨害）	Webサーバに攻撃の可能性がある。ただし、ニュースリリースや問い合わせの情報しかないので、大きなリスクはないと考えられる
Elevation of Privilege （権限昇格）	特権ユーザーは一部の社員のみであり、セキュリティ研修も他社以上に実施している。脆弱性が発見された場合に顕在化する可能性がある

STRIDE分析の結果悪いところだけでなく、対策ができているところや対策が弱いところまで検討することができました。これにより、余計に対策を検討する必要性がなくなり、本当に必要なところに対策のリソースをさくことができました。

Day5
2.リスクを検討する

リスクアセスメントの具体例
～リスクを把握し評価する～

リスクアセスメントの事例

リスクアセスメントはさまざまな場面で行います。最近ではDXやデジタル化の影響もあり、今までのビジネスのあり方から変化するにあたり、リスクアセスメントが求められるシーンが増えてきています。ある会社では、クラウドを利用した新サービスを導入することとしました。社員が利用するだけでなく、社外の人も利用する予定のクラウドシステムです。今までに無かった使い方なので、リスクアセスメントもより慎重に行うこととしました。脅威や脆弱性の洗いだしでは、サービス提供会社の状況まで確認し、リスク分析に活かしました。

まず行ったことは、これらシステムの資産価値の分析です。今回のクラウドサービス導入の目的と照らし合わせて考えます。今回の目的は、社外の特定ユーザーに会社の情報を届けることです。また社外ユーザー間でもコミュニケーションを取ることになります。すなわち、社外ユーザーにとって価値がある情報のやり取りも行われます。資産価値としては非常に高い位置付けとなりました。

次に行ったことは脆弱性の把握です。これには2つの観点があります。一つは、サービス提供会社に関する脆弱性です。「利用するシステムの脆弱性の把握をどのようにしているのか？」「従業員のセキュリティ意識はどうか？」などを確認していきました。確認には質問票を作成し、サービス提供事業者へ記載してもらいました。もう一つは自社の利用における脆弱性です。パスワード管理の方法や外部利用者の認証方法などを検討していきました。

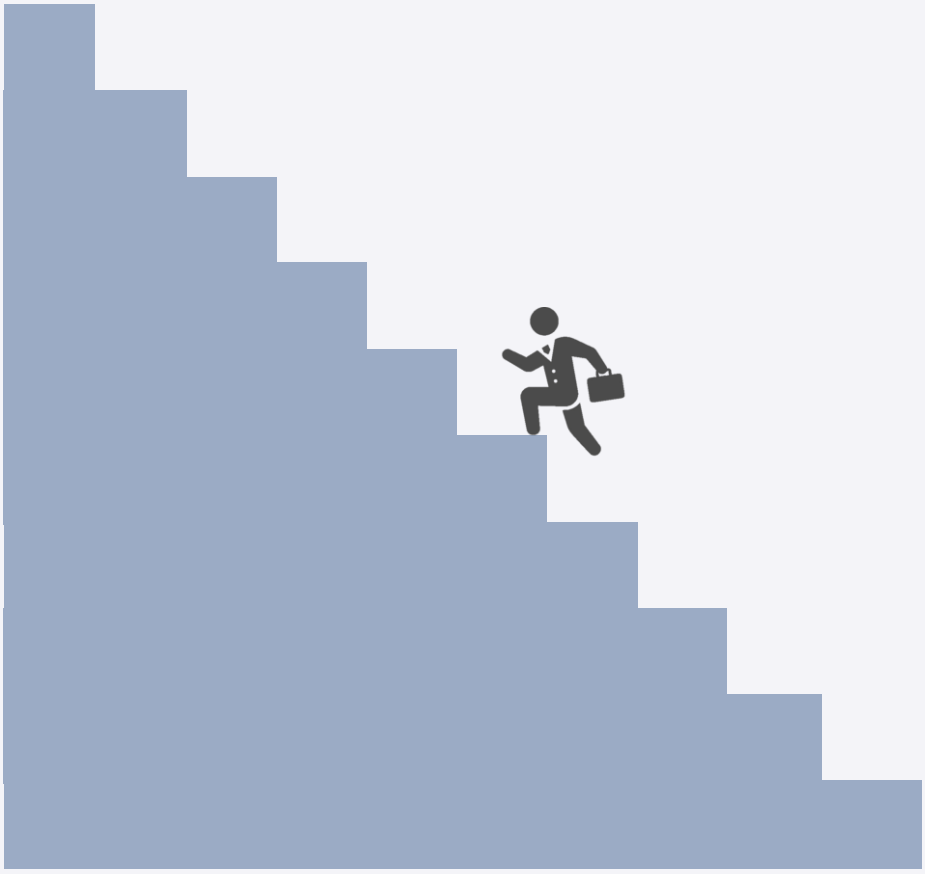
そして脅威分析です。STRIDE分析などに基づきシステムの状況を確認し、ATTACKツリーで利用方法における脅威について検討を行いました。システム面については、最近のスタンダードな対策は取られており、問題は使い方でした。特になりすましの脅威については完全には排除できないことも想定されました。社外利用者はなかなかルールの統一が難しかったからです。

今回のリスクアセスメントの結果、目的達成に必要な条件などを考慮し運用ルールの細かい設計を行いました。最終的には利用に伴う利用規程を定め、参加者が安全な利用を行えるような対策を施しています。

リスクの対応をしっかりしていくことは、予算を適切に運用することや優先度の高いところから対応をしていくことにつながる。まずは自社にとっての脅威や脆弱性を考えていこう。そういえば以前、自社にとっての最悪なケースはどのようなものかというワークをセミナー中にやった気がする。今回のATTACKツリーを使って最悪なシーンを想定して脅威を把握してみよう。脆弱性は運用フローの見直しや保守会社とも連携をとっていこう。そうすればリスクについてより理解ができ、対策が取れているのか、取れていないのかがわかってくるはずだ。

対策から考えるのではなく、対策を打つべき要因から考えられるようになれば、事業計画を進める上でも各ポイントで対応ができるようになる。そうすれば、長期的にもその時々で最適な対策を取れるようになるだろう。

リスクを知る
やるべきことを知る



コラム
～リスクを正しく評価する～

リスクアセスメントでは、脅威や脆弱性といったさまざまな情報をもとに考えていきます。情報漏れがないか、検討漏れがないかなど常に気を使う作業です。リスクアセスメントをするためには、業務フローなども把握していきます。運用の脆弱性を確認するためです。業務フローなどはベースラインアプローチで全体像を把握していきます。全体像が把握でき、危険そうなポイントや重要な資産に関係するポイントは形式的なアプローチでより詳細を把握していきます。

詳細の把握ができたら、詳細リスク分析で各資産について脅威や脆弱性を把握していきます。個人情報などを含む資産は詳細リスク分析を行うことが多いです。詳細リスク分析を行う過程で脆弱性の可能性がありそうな場合には、関係者へ話を聞くなどし資産の扱い方を確認することもあります。

これらのリスクアセスメントはセキュリティ担当者一人で行うのではなく、関係者を巻き込んで行うと良いです。正しく業務内容を理解し、資産を把握し、脅威や脆弱性を網羅します。関係者が集まって検討することでより精度の高いものが出来上がります。また、時々は専門家の意見を聞くことで脅威の情報がアップデートされ、より精度が上がっていきます。

あとがき

リスクアセスメント、リスクマネジメントはセキュリティ担当としては是非とも身につけたいスキル・知識の一つです。対策を考えて実行することも重要ですが、本当にその対策が有効なのか、これから取り組む施策にどのような対策が必要なのかを考えることにつながります。セキュリティ対策をどこまでやれば良いのかわからないという話もよく聞きますが、これらもリスクアセスメントを適切に行うことで判断がつくようになります。勿論、初めは本当にこれでいいのかと悩むこともあると思いますが、セキュリティ担当者として、判断をして行ってください。ただ、一人でその責任を背負いこむのではなく、経営層や関係者が積極的にフォローすることが重要になります。全員で会社のリスクに対して取り組みましょう。

令和4年度

中小企業サイバーセキュリティ対策継続支援事業

第6回

セミナー開催日：令和4年10月25日

リスクに対応？
予算は？いつまでに？
どうやって？

　自分の会社にもリスクがあることはわかったけど、どのように対応をしていけばいいのだろう？リスクがあるのだから無くしていけばいいのかもしれないが・・・
リスクがあるのは、事業を行う中でいろいろな取り組みをしているからだ。リスクを全てなくそうとすると、業務ができなくなってしまうのではないだろうか？

　事業をしていく中では、リスクを取ってでもやらないといけないこともあるだろう。とはいえ、安全にやらないといけない。そうすると、リスクを無くすのではなく、リスクを減らしていく対応方法を検討することも重要そうだ。

　いざ進めるためにも、予算や人員の確保をしないといけない。把握したリスクすべてに予算を獲得することは難しい。対応方法の検討は難しそうだ・・・

Day6

1.リスクへの対応

リスク対応の施策

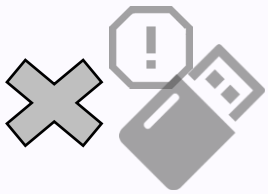
リスク対応は大きく４つに分けられます。細かい対策をする前に、各リスクに対して、どのような方針で考えるのかを決めておくと対策立案がスムーズになります。前回のポイントを振り返りながら、もう少し詳しく見ていきましょう。

①リスク回避

仕事のやり方を変える、情報システムの利用方法を変えるなどして、想定されるリスクそのものをなくします。

【例】

- 個人情報を利用後はすぐに消去し保持しない
- インターネットバンキング専用のパソコンを設置し、メールやウェブ閲覧は利用しない



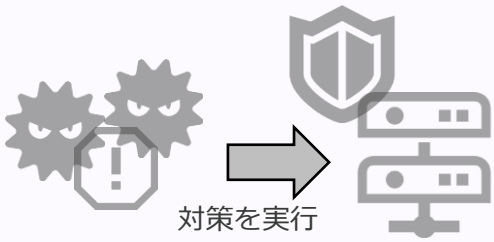
リスクがあるものは持たない

②リスク低減

自社で実行できる情報セキュリティ対策を導入ないし強化することで、脆弱性を改善し、事故が起きる可能性を下げます。

【例】

- 社用携帯にストラップを常時接続し、服につけておく
- 外部記憶媒体を利用の際は特定の端末のみ許可する



対策を実行

③リスク転嫁

自社よりも有効な対策を行っている、あるいは保証能力がある他社のサービスを利用することで自社の負担を下げます。

【例】

- 決済業務を外部の決済代行サービスに変更する
- 保険商品に加入する

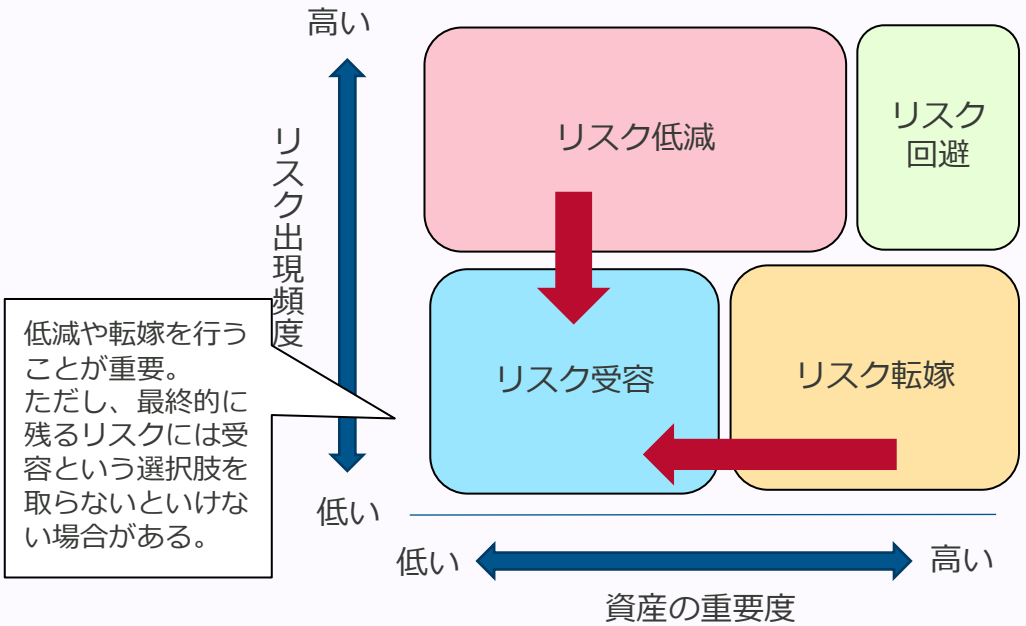
他社へリスクを負担してもらう

他社

④リスク受容

事故が発生しても受容できる、あるいは対策に係る費用が損害額を上回る場合などは対策を講じず、現状を維持します。

リスクを受け入れる



資産の重要度は、情報資産の価値・事故の影響の大きさを示すもので、機密性、完全性、可用性から算定します。　なお、資産の重要度は、セミナー第4回6ページに記載があります。

Day6
1.リスクへの対応

リスク回避の検討ポイント

リスク回避は、リスク発生原因を除去することにより、発生させなくするための方法です。リスクが無くなることによりセキュリティ事故などが起こらなくなります。

リスク回避の特徴は以下の通りです。

リスク回避の特徴と例

リスク発生原因を除去することが最大の特徴です。リスクそのものがなければ、情報漏えいなどのセキュリティ事故が起きる可能性をゼロにできるかもしれません。しかしながら、現実的には、リスクを回避してばかりでは事業運営に支障をきたします。

リスク回避の例

社用携帯電話としてスマートフォンを支給する場合、スマートフォンの紛失による情報漏えいのリスクがあります。社用携帯電話の配布をやめてしまえば、このリスクを回避することができます。

紛失可能性のあるスマートフォンは配布しない

リスク回避が推奨される事例としては以下のようなものがあります。また、この事例に当たらない場合でも、リスク分析の結果、想定されるリスク顕在時の損失が高すぎるような場合には回避を取る場合もあります。

資産の重要度が高い × 出現頻度が高い → リスク回避を検討

※事業の影響度や今後の展望を考えた場合には容易にリスク回避を取れない場合もあります。その際は、低減や転嫁を考えましょう。

こんな事例も

リスク回避とは、リスクの発生原因を除去することです。リスクがなければリスクが発生しないため、セキュリティ事故は起こらない、何か事故が起こっても影響は発生しないという考えになります。

ある会社では、取引先にリスク回避の対応を取られてしまい、ビジネスチャンスを逃してしまいました。取引先が求めるセキュリティレベルに達していないという評価となってしまったため、契約をすることは危険だという判断をされてしまったのです。セキュリティに対する意識はあったものの、セキュリティの取り組みを後回しにし、対策などをしっかりとできていなかったことが原因です。

この件をきっかけとして、この会社ではセキュリティの強化に努めました。担当者を任命し、社内のセキュリティ担当組織も立ち上げました。危険だと言われた項目について検討を行い、対策を行いました。現在では、セキュリティ水準も高くなってきており、取引も再開されました。

セキュリティ対策を疎かにしてしまうと、取引先からリスク回避という考えのもと取引自体を見直しされてしまう可能性も十分あります。

Day6
1.リスクへの対応

リスク低減の検討ポイント

リスク低減は、発生確率や頻度、損害、損失などを減らす対策をすることです。セキュリティの取り組みは、リスク低減となることが多いです。

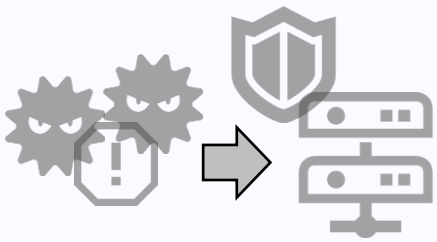
リスク低減の特徴は以下の通りです。

リスク低減の特徴と例

リスクが発生する可能性や損失する損害額を減らしていくことが特徴です。セキュリティ対策としての技術的な対策や、セキュリティ規程の作成等を組み合わせます。

リスク低減の例

火災に備えて消火器を設置することで、損失の可能性を低減します。地震に備えて拠点を複数設置することも損害の可能性を低減する対策といえます。ウイルス対策ソフトなどの導入もリスク低減の一つです。



リスク低減が推奨される事例としては以下のようなものがあります。リスク低減では、事故を起こさないという発想だけでなく、損害を少なくするという視点も重要です。そのセキュリティ対策はどのリスクに働きかけ、発生確率を低減するのか、損害を小さくするのかなどを検討することが重要です。

資産の重要度が低い × 出現頻度が高い → リスク低減を検討

こんな事例も

ある会社では、情報流出に対してリスク低減を進めています。情報流出のリスクの一つに、メールを起因としたウイルス感染がありました。これに対応するため、メールの利用ルール（組織的対策）を定め、従業員へ教育（人的対策）を行います。さらに、端末にウイルス対策ソフトを導入（技術的対策）するとともに、メールの無害化サービスを導入し、メールを起因としたウイルス感染の発生回数を減らしました。メール無害化サービスでは、添付ファイルを無害化したり、メールに含まれるURLを無害化するなどの特徴があります。

別の会社では、リスクの発生回数を減らすための対応が充実してきたため、損害を小さくするための対応を進めています。情報の保管の仕方を工夫し、インシデントが発生した場合でも影響を受ける範囲を最小限にとどめています。さらに、何か問題があった場合にもすぐ検知できるように取り組んでおり、影響を受ける時間も最小限になるように努めています。

情報流出に対して、発生確率を減らすとともに損害を受ける範囲や時間を減らしていくことで情報流出のリスクを低減しています。

リスク低減の種類

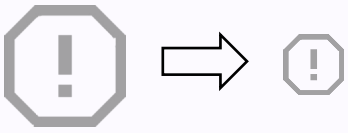
リスク低減といってもリスクに対してやみくもに対策をするべきではありません。対象のリスクにおいて、どのような方法で対策をすることがよいのかを検討する必要があります。

Point① 発生損失・発生可能性のリスク低減

発生損失低減

リスクが発生したとしても、少ない損失で済むようにリスク低減を行う

リスクが顕在化した際に損失が少なく済むように対応することです。物理的には、消火器やスプリンクラーを設置して火災に備える、技術的には、データや通信を暗号化して情報漏えいを防止する、などがあげられます。

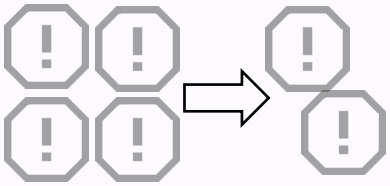


会社に存在するリスク
発生損失低減

発生可能性低減

リスクの発生回数を減らすようにリスク低減を行う

リスクが顕在化しないように発生回数を減らす対応をすることです。物理的にはスマートフォン紛失対策のストラップ装着、技術的にはウイルス対策ソフトの導入に代表されるような、セキュリティ製品の設置などがあげられます。



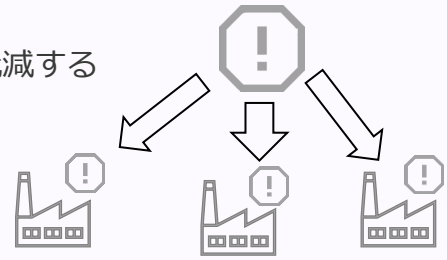
会社に存在するリスク
発生回数低減

Point② 分離・集中のリスク低減

分離

リスクを分離することにより、損失や発生可能性を低減する

リスクが顕在化しても、影響範囲を少なくできるように分離する手法です。影響範囲は少なくできるものの、それぞれに対策を立てる必要があるなど、対策費用や対策実施までに時間がかかる可能性があります。

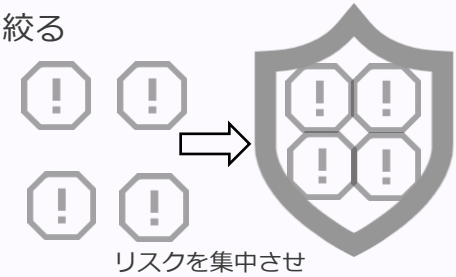


会社に存在するリスクを分離する

集中

リスクを一箇所に集め、対策実行や管理のポイントを絞る

リスクをまとめる手法です。インターネットとの接続点を一箇所にまとめるなども集中の事例です。集中させた箇所に対して十分な対策をすることで、対策にかかる負担を減らすことが可能になります。ただし、この一箇所の対策がおろそかになると、事故の危険性が高まります。



リスクを集中させ
守るポイント絞る

Day6

1.リスクへの対応

セキュリティ対策の種類

リスク低減では各種対策を実行していきます。対策を考える際には、第3回のセミナーで紹介した技術、人、組織、物理を意識して対策を検討していきます。

組織的対策

企業や組織が適切な情報セキュリティを維持できるように、行うべき対策です。企業の変化などに合わせて、変化が求められます。定期的な見直しなどを行い、ルールの整備や管理体制などを整えていくことが重要です。

主な対応内容
- セキュリティ運用指針の策定、計画立案
- 規程やルールの見直し
- セキュリティ管理体制の構築

人的対策

従業員がセキュリティ事故を起こさないように、ルールの浸透やセキュリティ管理の重要性を理解する対策です。企業では常に人の入れ替わりが発生します。入社時に研修を行うことが一般的ですが、定期的に意識を啓発していくことが重要です。また、ルールが変わった場合などは、ルールを浸透させていくためにも、教育やトレーニングを行うことが重要になります。

対応内容
- ルールや規約の内容を浸透させる啓発活動
- 攻撃に備えたトレーニング活動

技術的対策

ネットワークやサーバ、PCなどの機器、保存されているデータを守るための対策です。デジタル化が進む今日においては、技術的対策が求められる状況が増えています。セキュリティ担当者としては自社のシステム等を理解し、技術的な対策の検討も求められます。

対応内容
- PCのウイルス対策ソフトなど社内システムの導入
- クラウドなどの利用にあたってのセキュリティの導入

物理的対策

紙やUSB、パソコンなどの紛失から情報流出を防ぐための対策です。紙などの情報ももちろんですが、ペーパーレス化などに伴い、デジタルデバイスを利用する状況も増えています。デジタルデバイスでは扱う情報量が増えているため、紛失などを起こさないように、物理的な対策が特に重要となります。

対応内容
- 情報持ち出しの禁止通達
- 個人情報の持ち出しに対する記録の取得
- 監視カメラを設置

テキスト第3回より再掲

Day6

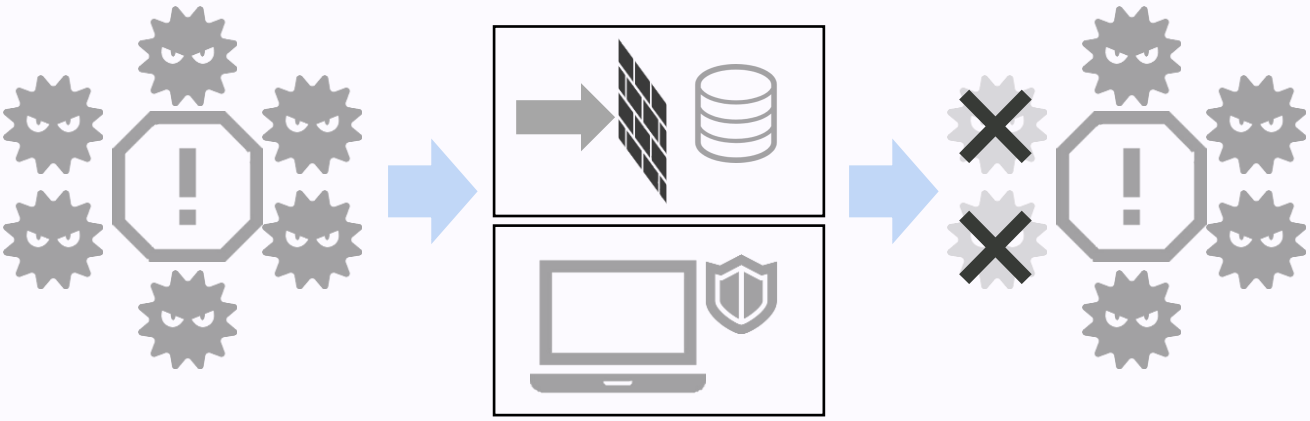
1.リスクへの対応

セキュリティ対策の実行

リスク低減を行う際には、リスクに対して対策を検討し実行していく必要があります。リスク分析とセキュリティ対策の実行はセットで考えていきましょう。対策は一つの方法を繰り返すだけでなく、複数の方法を組み合わせることも有効です。

Point① 1種類の対策を複数個組み合わせて低減を実施

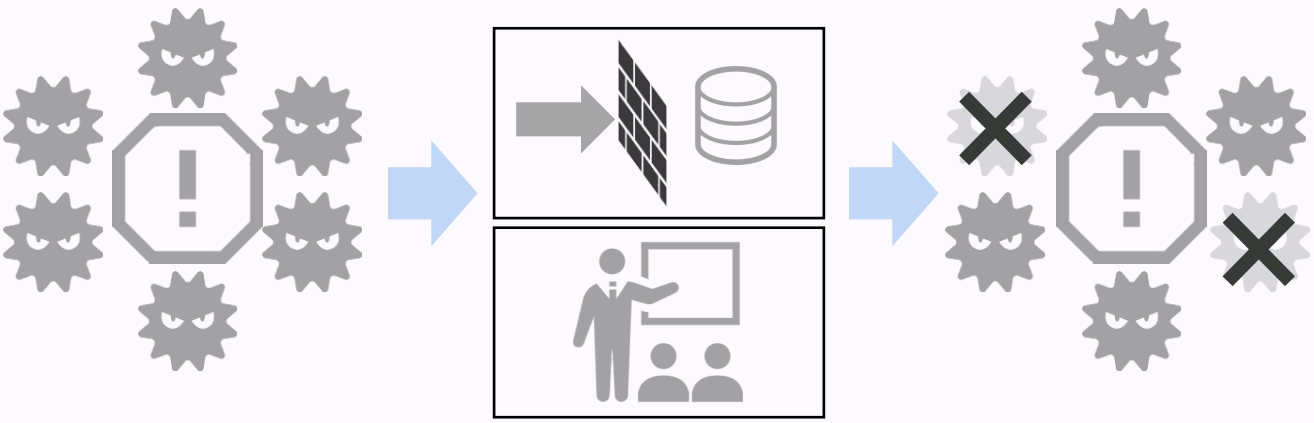
リスク分析の結果、リスクに対して対応を行う必要があります。今回はリスク低減を行うため、技術的な対策を複数行う対応方法を実施しました。



リスク分析の結果　　複数の技術的対策を組み合わせる　　セキュリティ対策の結果

Point② 複数種類の対策を組み合わせて低減を実施

リスク分析の結果、リスクに対して対応を行う必要があります。リスク低減を行うために、技術的な対策と人的対策を組み合わせます。適切な対策を組み合わすことでより効果的なリスク低減が可能となります。



リスク分析の結果　　技術的対策 人的対策 を組み合わせる　　セキュリティ対策の結果

Day6

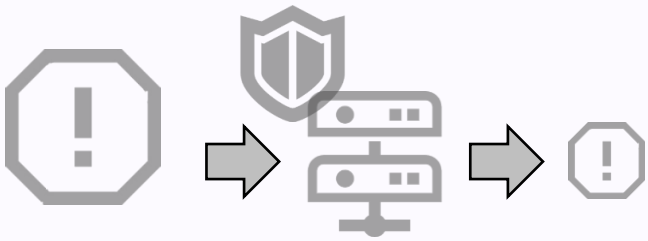
1.リスクへの対応

残留リスクの考え方

リスク低減をどんなに行っても、リスクをゼロにすることはできません。最低限のリスクは存在することになります。どうしても残ってしまうリスクを残留リスクと呼びます。

Point① 残留リスクとは

残留リスクとは、対策を講じた後にも残っているリスクです。また、対策が講じられず、残ってしまうリスクも残留リスクと呼ばれる場合もあります。



リスク低減後も残ったリスク

Point② 残留リスクへの対応

残留リスクが存在する場合、残ったリスクが組織にどの程度の影響を及ぼすかを検討する必要があります。リスク分析を改めて行うなどの対応が必要です。残留リスクがある場合には、大きく2つの対応パターンがあります。

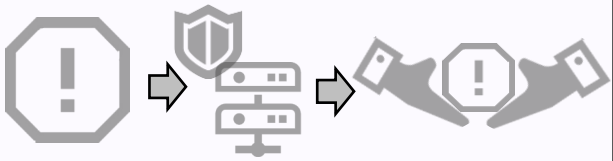
追加のリスク低減の対策を実施

リスクに対して対策を行った結果、まだ対策が必要な場合には、さらに低減の対策を実施します。例えば、技術的な対策で添付ファイルの監視を行ったが、従業員がファイルを開く可能性があるので、教育を行うなど、複数の対策を組み合わせていきます。

リスクが受容できるレベルまで対策を繰り返し行う

リスク受容し、対策を終了する

リスク低減の取り組みをどんなにしてもリスクは残りますが、そのリスクが受容できるレベルと判断し、受け入れるという選択をすることができます。ただし、受容できるかどうかは会社によって違いが出ます。各社に合わせたリスク分析が重要です。



リスクが受容できるレベルまで対策ができているので、これ以上の対策は行わない

こんな事例も

ある会社では、残留リスクに対しての検討が疎かになっていました。すでにリスク対応しているという意識があったため、追加の対応が必要とは夢にも思っていなかったとのことです。支援に入り、残留リスクに対して検討を行ったところ、リスクが顕在化した場合の影響は事業継続を圧迫する可能性があるほどでした。急いで追加の対策を立案・実行する運びとなりました。

リスクに対して対策をしているということが重要ではなく、リスクが受容できるレベルまで対策が取られていることが本来のあるべき姿と担当者は感じたそうです。

ミニワーク
～考えてみよう～

ミニワークテーマ

自社のリスクを振り返ってみよう。

自社の状況を振り返ってみましょう。自社にとって対策の有無に関わらずリスクだと考えるものをあげてみましょう。

Day6
1.リスクへの対応

リスク転嫁の検討ポイント

リスク転嫁は、リスクによるマイナスの影響を第三者へ移転することです。別の表現として、リスク移転という言い方もありますが、同じ意味です。

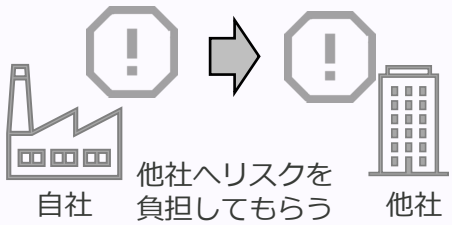
リスク転嫁の特徴は以下の通りです。

リスク転嫁の特徴と例

リスクを第三者に負担してもらうことが最大の特徴です。だからといって事故が起こっていいというわけではありません。

リスク転嫁の例

典型的な例は、保険への加入です。費用を払うことでリスクが顕在化し問題が発生した際には、損失した被害額を保険会社に引き受けさせることができます。



リスク転嫁が推奨される事例としては以下のようなものがあります。リスク転嫁では、他社へリスクを負担してもらうことになります。また、リスクは変わる可能性があります。定期的なリスクの見直しを行い、保証の範囲などを適切に検討していくことが重要です。

資産の重要度が高い × 出現頻度が低い → リスク転嫁を検討

こんな事例も

リスク転嫁としての代表は保険サービスです。セキュリティ事故が発生した場合には莫大な費用がかかるため、発生した被害に対しての金額を保険金で賄い、事業継続に対しての影響を最小限にとどめることが期待できます。

ある会社では、事故原因調査・コールセンター設置・見舞金の支払い・法律相談・再発防止策の策定を補償内容としたサイバー保険に加入しています。保険により、サイバー事故に起因して一定期間内に生じた各種費用が補償されます。毎年リスク分析を行う中で、保険の内容も見直しており、万が一に備えています。

セキュリティ事故に伴う費用の換算

項目		費用（想定）
業務継続費用	対策組織業務に係る人件費（1か月分）	500万円
	損害賠償費用（訴訟参加費＝0.1%）	36万円
	弁護士費用・裁判費用	30万円
見舞い品費用	見舞い品代＋送料他（2万人分）	1400万円
謝罪訪問費	謝罪訪問に掛かる費用（10人分）	110万円
広報費用	謝罪広告費	なし
	情報公開ページ作成費用（2回）	10万円
臨時的な対策費用	コールセンター設置費用（1ヶ月分）	500万円
	問い合わせ窓口常駐人員（1ヶ月分）	200万円
合計		2786万円

第5回テキストより再掲

Day6
1.リスクへの対応

リスク受容の検討ポイント

リスク受容は、存在するリスクや残留リスクを受け入れるという考えです。どんなにリスク低減を行っても、最終的に残留リスクが発生します。その際にはリスクを受容していくという判断をする場合があります。

リスク受容の特徴は以下の通りです。

リスク受容の特徴と例

リスクを受け入れて特段の対策をしないという考えです。しかしながら、対策が技術的に困難な場合や対策費用が膨大にかかるリスクを受容せざるを得ない場合、漏えい発生時の損失など、リスクが現実化した場合の被害規模の把握が重要です。

リスク受容の例

社用携帯電話としてスマートフォンを支給する場合、紛失による情報漏えいのリスクがあります。しかし、社用携帯電話が利用できないと業務に及ぼす影響が大きいため、従業員に使用時のルールを徹底的に教育した上で、スマートフォンの支給を続けることにしました。

リスクを受け入れる

リスク受容はリスク低減のセキュリティ対策を実行した結果、最後に残る軽微なリスクを受け入れることです。例えば、リスクが顕在化した際に対応する費用よりも低減のための対策を実行する方が費用が掛かる場合などはリスク受容をするケースが多いです。

資産の重要度が低い × 出現頻度が低い → リスク受容を検討

こんな事例も

Emotetの感染リスクは多くの企業で対策などを検討しているのではないでしょうか？しかし、Emotetの感染を完全に排除するために現状の感染経路を考えると、メールを利用しないということになります。

しかしながら、メールは今も外部とコミュニケーションを取るために必要な主流なツールの一つです。メールを廃止するとなると、自社だけでなく取引先や顧客の理解を得る必要があります。メール以外のコミュニケーションツールを導入してもらうなど、準備や金銭的な負担も考えられます。コミュニケーションツールの導入が困難という理由で断念しなければならない事業や、取引先が存在するかもしれません。

このように、極端なリスクの対応は現実的ではない場合があります。企業にとってリスクは回避できるかもしれませんが、大きな機会損失に繋がるかもしれません。そのためには、リスク受容の考えを適切に意識した対応が重要になります。メールを使わないということではなく、メールを適切に利用できるように、従業員の教育を行いリスクの発生可能性を下げるなども意識した対応が望まれます。

Day6

1.リスクへの対応

リスク受容の判断

リスク受容をする際には、自社における基準を定め、運用していくことが望ましいです。基準には、リスク分析の数値や損害想定額などを活用していきます。また、リスク回避と合わせた判断をすることも重要です。

Point① リスクを算出する計算式の結果で受容する

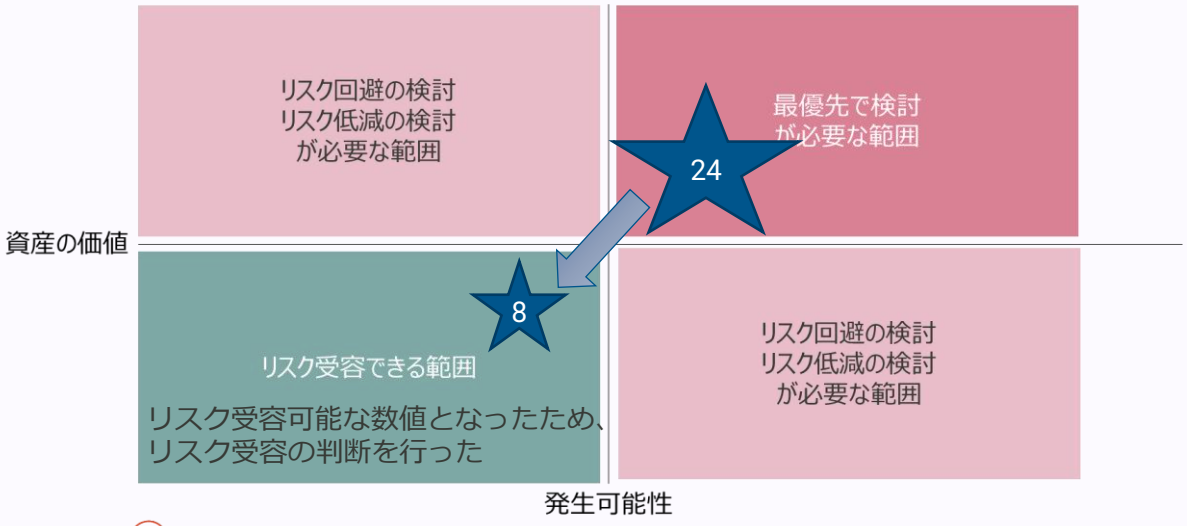
今回の例では、リスクの受容できる数値を17と定めます。リスクを算出する計算式：リスク＝資産価値 × 脅威 × 脆弱性 × 発生可能性をもとに、リスク低減を行う前の数値を算出します。

リスク＝資産価値(2) × 脅威有(2) × 脆弱性有(2) × 発生可能性は高い(3) ＝ 24

24では受容できる数値17を大きく超えているので、リスク低減を行いました。対策として発生可能性を低くし、社内への適用を行います。その結果発生可能性は3 → 1 となりました。

リスク＝資産価値(2) × 脅威有(2) × 脆弱性有(2) × 発生可能性は高い(1) ＝ 8

8へと数値が下がったことにより、リスク受容数値17を下回りました。残留リスクの確認を行い、リスクの受容という選択肢が合理的であり、リスクが顕在化した場合に事業影響が小さいことを確認し、最終的に受容しました。



Point② 被害損害額の予想から受容する

今回の例では、リスク受容できる数値を被害損害額の予想から算出します。年次損失予測を求めることで、リスクを受容できるかを判断します。今回の閾値では年間200万円を下回ればリスク受容するとします。

1年間の被害損害額の算出の計算
1人当たりの資産価値 ＝ 3万円
流出可能性人数： 5万人 × 0.01 = 500人
事故1回あたり対応費用 ：500人 × 3万円 ＝ 1500万円
1年間の発生確率：1 ÷ 10 ＝ 10%
年次損失予測： 1500万円 × 10% ＝ 150万円

計算の結果、1年間の損失予想は150万円でした。閾値である200万円を下回る結果となったため、リスク受容の判断を行うこととなりました。

Day6

1.リスクへの対応

リスク受容は事故０を保証するものではない

リスク受容というのは、リスクそのものがなくなるわけではありません。低減を行った結果、顕在化しても大きな影響がないという場合にリスクを受け入れたということです。そのため、受容したリスクは定期的に確認することが重要です。

Point① リスクは存在する

リスク受容では、リスクそのものは存在します。各リスクの特徴をとらえたうえで、慎重に受容する必要があります。

影響度が低いリスク

リスクが顕在化しても損失などの影響が少ないリスクです。1回あたりの顕在化時の影響は小さくとも、発生回数が多くなると受容しきれない場合があります。

出現頻度が低いリスク

リスクの顕在化の可能性が少ないリスクです。ただし、リスクが顕在化をした場合に大きな損害が発生する場合があります。リスク転嫁と合わせて考えることが重要です。

リスク低減等が技術的に困難なリスクや対策費用が膨大にかかるリスク

リスク低減などを試みても実施が難しい、しかしながら事業観点から回避もできない状況で起こるリスク受容です。リスク顕在化の可能性や影響も大きい場合、1回のリスクの顕在化、インシデントの発生が企業存続を脅かす可能性があります。

Point② 定期的なリスク分析が重要

リスク受容を行ったリスクについては、定期的な見直しが重要です。リスク分析直後は受容できるリスクでも、新たな脆弱性の発見や攻撃手口による脅威の変化などにより、受容できないリスクとなる場合があります。

影響度が低いリスク

発生回数をモニタリングし、発生回数が閾値を超えるようならば発生回数を減らす対策を立案することが求められます。

出現頻度が低いリスク

1回の顕在化で大きな影響を及ぼす可能性がある場合、脆弱性や脅威、発生回数など、網羅的に分析を行い、影響度を下げる工夫を考えることが求められます。

リスク低減等が技術的に困難なリスクや対策費用が膨大にかかるリスク

現在のリスク分析による影響度などの把握を行うとともに、低減や転嫁の検討や回避の検討を行うことが求められます。

ミニワーク
～考えてみよう～

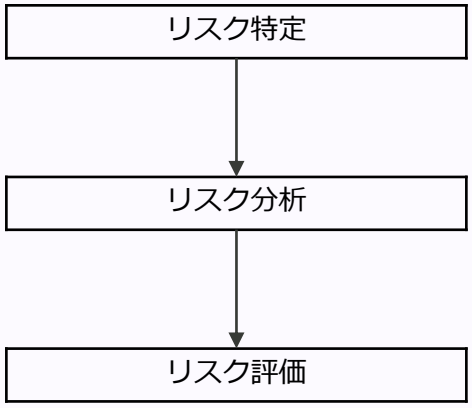
ミニワークテーマ

対策ができていないリスクや受容できるまでになっていない
（対策が十分でないと感じる）リスクを考えてみましょう

ISO/JISからみるリスク管理

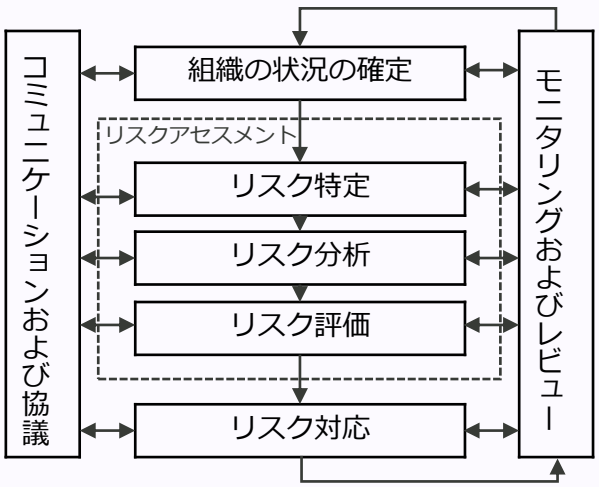
ISOの中でも代表的なISO27001/JISQ27001の中にもリスクアセスメントが定められています。また、リスクマネジメント規格（ISO31000/JISQ31000）というものがあり、それぞれに違いがあります。

ISO27001で定める
リスクアセスメントプロセス



ISO27001では、「機密性」「完全性」「可用性」の3つの特性を損なうリスクに対してリスクアセスメントを行います。これらのプロセスを実施する方法として、詳細リスク分析、ベースラインアプローチ、非形式的アプローチがあります。

ISO31000で定める
リスクマネジメントプロセス



ISO31000では、リスクマネジメントの枠組みを定めています。その中のリスクマネジメントプロセスは、リスクを認識し、対処していく過程のことを言います。

ISO27001は情報セキュリティマネジメントシステムとして、リスクが顕在化した場合の対応や事業継続を意識した取り組みも含まれます。 ISO31000では、リスクに対応するための事前の活動が中心という違いがあります。それぞれの違いを理解し、利用します。特に、ISO31000は認証を目的とした規格ではないため、リスクマネジメントの仕組みが確立されているかを確認し、常に改善を行っていく活動が重要です。

ISO31010/ JISQ31010から見るリスクアセスメント技法

ISO31010はリスクアセスメント上のポイントや実施する上での技法についてまとめられた文書です。実際にリスクアセスメントを行う際に助けとなる技法についてまとめられています。

リスクアセスメント技法（一部抜粋）			
ブレーンストーミング	予備的ハザード分析	環境リスクアセスメント	故障モード・影響解析並びに故障モード・影響及び致命度解析
構造化又は半構造化インタビュー	HAZOPスタディーズ	構造化“What-if”技法	
デルファイ法	ハザード分析及び必須管理点	シナリオ分析	
チェックリスト		事業影響度分析	FTA（故障の木解析）

※ ISO/IEC規格は国際標準化機構（ISO）によって作成された規格です。JIS規格はISO/IEC規格と整合性を保ち日本産業規格（JIS)より発行された日本の国家規格です。本ページで紹介したJIS規格は日本産業標準調査会(https://www.jisc.go.jp/index.html)から閲覧できます。なお、閲覧にあたってはアカウント登録が必要です。

Day6
2.リスクへの対策

対策にかける費用の検討

セキュリティの対策をどこまでお金をかけて実施するのかと悩まれている担当者の方は多いのではないでしょうか？リスクを低減するために対策を行っていきますが、かけられる予算は無限ではありません。効果的に予算を投資していくことが重要です。

Point① セキュリティ対策予算の確保

必要な予算を確保しておくことは、サイバーセキュリティリスク管理において重要です。サイバーセキュリティ経営ガイドライン内でも、「サイバーセキュリティ経営の重要１０項目」の中の「指示３ サイバーセキュリティ対策のための資源（予算、人材等）確保」が定められています。

対策を怠った場合のシナリオ
- 適切な予算確保が出来ていない場合、組織内でのサイバーセキュリティ対策の実施や人材の確保が困難となるほか、信頼できる外部のベンダへの委託が困難となる恐れがある。
- 適切な処遇の維持、改善ができないと、有能なサイバーセキュリティ人材を自社にとどめておくことができない。

対策例
- 必要なサイバーセキュリティ対策を明確にし、それに要する費用を確保する。
- 従業員向けやセキュリティ担当者向けなどの研修等のための予算を確保し、継続的に役割に応じたセキュリティ教育を実施する。
- サイバーセキュリティ人材を組織内で雇用することが困難な場合は、専門ベンダの活用を検討する。
- 組織内の IT 人材育成の戦略の中で、外部人材の採用も含めた社内のセキュリティ人材育成 、キャリアパスを設計検討する。
- 自組織においてセキュリティ人材の育成が困難な場合は、外部の組織が提供するセキュリティ研修等の活用などを検討する。

出典：経済産業省
サイバーセキュリティ経営ガイドライン Ver2.0
https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide2.0.pdf

Point② 費用を明確にする

サイバーセキュリティリスク管理体制を構築、維持するためには予算を確保しますが、大きく以下の３種類に分類されます。

- 事前対策費用（対策のための製品の調達費用、人材育成費用等）
- 対策運用費用（監視や予防の業務に要する費用、製品の保守費用等）
- 事後対策費用（インシデント対応費用、再発防止対策費用等）

サイバーセキュリティ対策に関する予算や人員計画は、経営会議など経営層の意思決定の場で承認されるべきことです。ビジネスへの影響を踏まえたサイバーセキュリティ対策の検討結果を CISO 等が経営会議などの場に提示し、実施する対策の内容、時期、費用等が適切かどうかといった項目を検討し、経営層の承認を得る必要があります。

出典：IPA（独立行政法人情報処理推進機構）
サイバーセキュリティ経営ガイドライン 解説書 Ver.1.0
https://www.ipa.go.jp/files/000056148.pdf

Day6
2.リスクへの対策

予算の獲得と計画性

セキュリティの対策をすべて無償ですることはできません。技術的な対策を立案する場合には予算を確保し実装する必要があります。限られた資源の中で予算を獲得し、計画を立ててセキュリティ対策を行うことが重要です。

Point① 年間計画と予算獲得

予算策定を年間計画で行う場合には、1年間の取り組みをある程度想定しておく必要があります。特に、機器の導入や入れ替えなどが発生する場合には、数年での計画と予算の調整が必要になる場合もあります。

無償	有償
ルール見直し・作成	機器導入
社内講師によるトレーニング	外部講師・コンテンツによるトレーニング
内部監査	外部監査

想定スケジュール					
リスク分析 →		対策立案 →	予算執行 外部講師 トレーニング ★	ルール見直し →	予算執行 外部監査 ★

これらスケジュールから、必要な予算は外部講師招聘のための予算と、外部監査を受けるための予算を獲得していくこととなります。また、年間計画が立案されているため、実行がしやすくなるというメリットもあります。

Point② スポット対応と予算獲得

セキュリティの対応には顕在化リスクに対して対応する場合があり、その場合は計画通りの執行とならない場合があります。

スポット対応となりやすい予算
インシデントの発生に伴う対応費用
インシデント原因根絶のための対策費用
新たな脅威出現による対応費用

スポットで予算獲得が必要な場合には、経営会議などでの承認が求められるケースが多いです。また、緊急事態での予算獲得となるため、しっかりと吟味できないケースとなります。ゆとりを持った対応を目指すのであれば、予算計画の中に事後対策費用などを初めから計画しておくとスムーズです。

Day6

2.リスクへの対策

今ある設備での対策検討

セキュリティは経営にも直結する問題であり、多くの企業が取り組みを行っています。セキュリティ製品も数多く市場に出回っており、各種サービスもセキュリティ機能が充実しています。新規サービスを導入する前に、導入済のサービスで実現できることはどのようなものがあるかを検討することも重要です。

Point① サービスを把握し使いこなす

現在のクラウドサービスの多くはセキュリティ機能が充実しています。サービスの中には、認証方法としてID・パスワード認証と合わせて2要素認証を有効にする設定などがあります。また、ネットワーク機器などではログ保存やレポート機能を有しているものがあるため、検知の仕組みとして活用することもできます。

中小企業サイバーセキュリティ対策継続支援事業参加者コミュニティで利用しているSNSでは、2段階認証(2要素認証と同等の認証方法)とログイン通知のアラートを受け取るという機能が設定できます。これにより、不正ログイン防止と不正ログインがあった場合の早期検知が可能になります。

Point② 従業員の皆様の理解も必要

急な設定変更は利用者である従業員の皆さんが混乱し、業務に支障が出る場合があります。従業員の方がスムーズに対応できるように取り組んでいくことも重要です。以下のような対応をしながら、十分な移行期間を設けて取り組んでいき、徐々に文化として根付かせていくことが重要です。

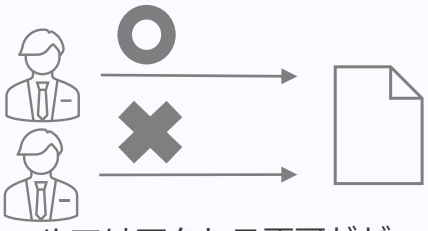
Day6
2.リスクへの対策

危険な運用でカバー

セキュリティ対策を検討すると、人の行動や日々の業務の中で気を付けるという運用面でセキュリティ強化を進めることがあります。最終的に必要な場合もありますが、運用面でカバーすることをなるべく少なくできるようにセキュリティ対策を検討してみましょう。

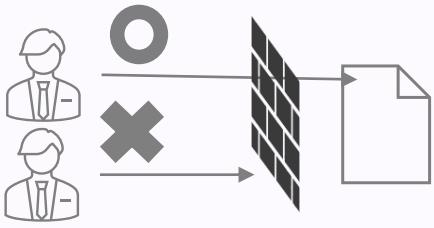
Point① 人の脆弱性を考慮して対策を

運用でセキュリティを担保しようとした場合には、ミスや誤操作といったことを考慮する必要があります。人の介在が多くなると、ルール違反やルール忘れなどが発生しやすくなり、セキュリティ事故につながります。



ルールではアクセス不可だが、
実際はアクセスできてしまう

あるデータへのアクセスを、ルールによって人の行動を制御することで制限します。この場合、本来アクセスしてはいけない人も技術的にはアクセスできてしまいます。誤操作によりファイルにアクセスしてしまうと、見てはいけない情報を見ることになったりと情報漏えいにつながります。



技術的に通信を止め、
アクセスできなくする

あるデータへのアクセス制御を、技術的な対策で実現します。ルールを知らない人や間違ってアクセスしてしまった場合にも、制御する機器が自動でアクセスを止めてくれるため、権限がない情報にアクセスするという危険性がなくなります。

こんな事例も

ある会社では、セキュリティ対策のほとんどを日々の業務による運用によりカバーしていました。この会社では、USBなどの外部記憶媒体の利用は社内のセキュリティ規程で利用を禁止しています。これはセキュリティ担当者も知っていることです。本来であるならば、PC導入の初期設定の段階で検討を行い、システム側で対応を検討しておくべきでした。例えば、 PCのシステム制御でUSBを認識しないようにするなどの対応ができます。しかし、そういった検討をせず導入してしまったため、USBを接続すれば認識し、外部記憶媒体として利用できる状態になっていました。運用面だけで接続を禁止した状態であるため、従業員の教育をより強化するなど注意していました。

しかし、ある社員が外部記憶媒体を認識できることに気づきました。この結果、家でも業務をするために情報を持ち出すといったことが頻発し、情報流出の危険性が高まりました。いよいよ追加の対策が必要となり、現在ではシステム側でのUSB利用禁止となりました。

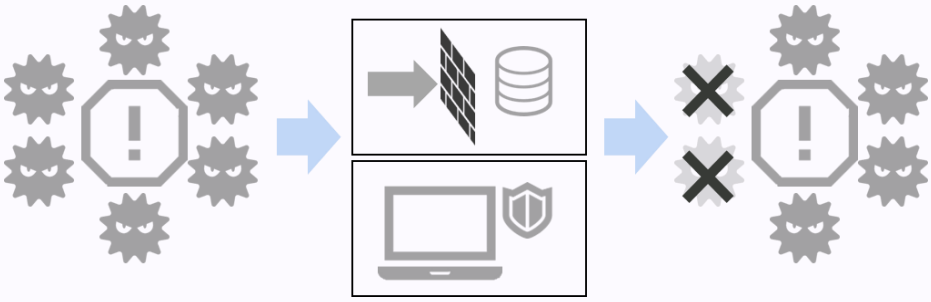
運用面で取り組むセキュリティが最小限となるよう心がけ、利用するシステム側でセキュリティを高めておくことが重要と感じる事例でした。

効果を測定するために

セキュリティ対策にかける予算は、短期的に測定する費用対効果ではなく、長期的に効果を測定する投資対効果で考えていく必要もあります。効果を測定していくためには、指標が必要になります。これら指標は対策の検討からすでに意識をしておくことが重要です。これら指標をもとに、効果あるセキュリティ対策を行いましょう。

Point① 対策の立案時に効果測定も意識する

リスクを低減するためにセキュリティの対策案を検討します。低減するために、組織や人、技術や物理的な対策を考え導入を進めます。



リスク低減を技術的な対策を用いて実装すると、リスク発生の可能性を減らすことができます。想定される効果として、6つの顕在化のきっかけが2つ消失し、33%程度の低減効果があると言えます。

実際の場合、「攻撃と思われる通信」が1か月で会社に届く頻度などをUTMを導入する前に計測しておきます。導入する機器のチューニングを行いながら「攻撃と思われる通信」をどの程度防ぐことができるかを検討することで、低減効果を予測することができます。今回の場合は効果測定の方法として、「攻撃と思われる通信」をどの程度防ぐことができるかを数値とし、効果測定のためには「全体の通信量」や「攻撃と思われる通信量」を集めるといった作業が発生し、事前に通信量の計り方を検討しておくことが重要になります。

Point② 効果測定の指標

効果測定の取り方は様々な方法があります。投資対効果としては損害時にかかる費用を算出しておき比較することも重要になります。

対策の種類	効果測定
組織	セキュリティ事故の統計など 例：ヒヤリハットの件数の推移、事故の件数の推移
人	アンケート調査など 例：規程の認知度、ルールの認知度
技術	ログ統計や通信量の把握など 例：攻撃可能性の通信制御回数など
物理	紛失などの統計など 例：PCなどの紛失回数など

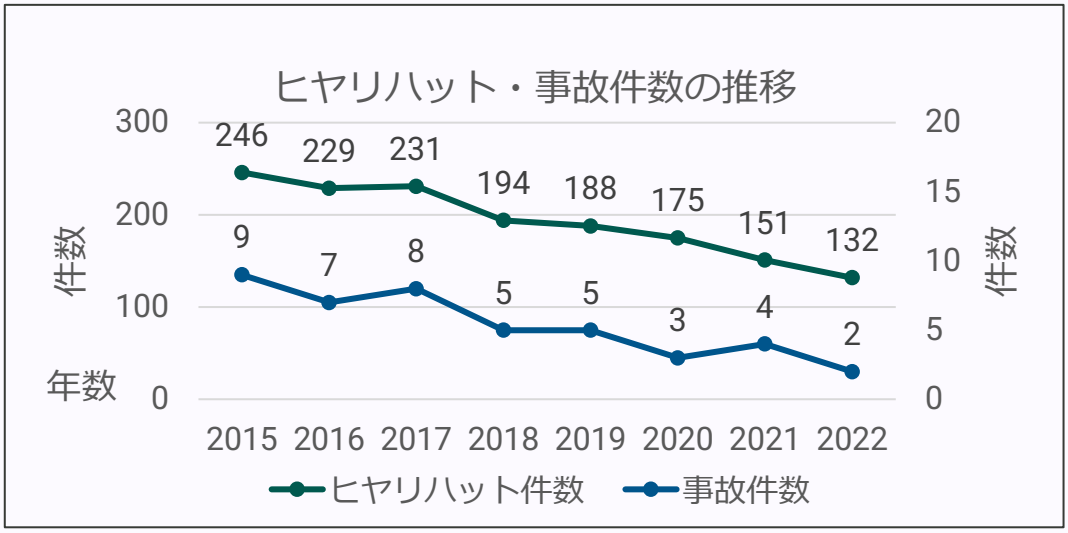
例えば、過去との比較をしていくことで、対策が効果的に働いているかを確認することができます。また、過去との差分を比較することで基準となる数値を導き出し、効果を測定していくという方法もあります。

Day6
2.リスクへの対策

効果を測定するために

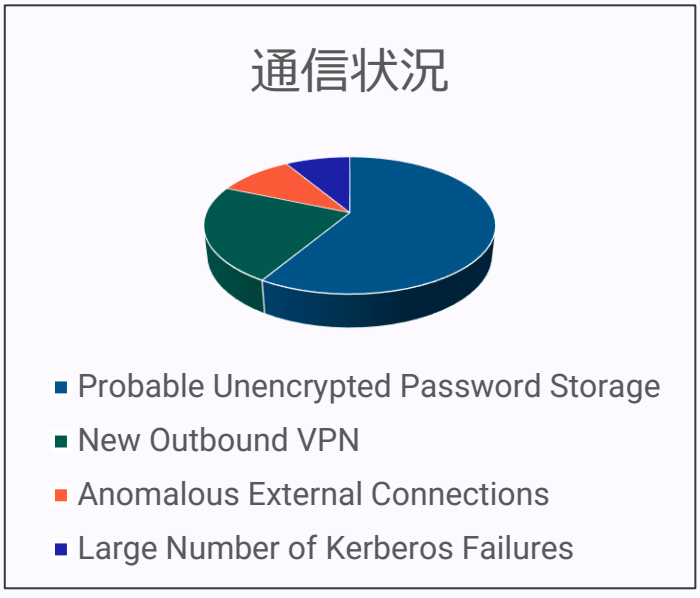
長期的に効果を測定する投資対効果では、レポートなど定期的なアウトプットを用意し、効果を可視化していく必要があります。
セキュリティ機器が自動でレポートを作成するような機器も多く存在します。また、セキュリティ事故の件数などを観測することも対策に対しての効果を見ることにつながります。

Point③ ヒヤリハット・事故件数の収集



従業員からのヒヤリハットや事故件数を観測していくことで、セキュリティの取り組みなどの浸透度や事故発生の会社の状況を把握することができます。

Point④ セキュリティ製品のレポート機能活用



※画像はイメージです。

セキュリティ機器は通信の制御をするだけでなく、レポートを抽出する機能があります。攻撃の可能性がある通信の検知状況、通信制御をどの程度実施したかを把握することができます。

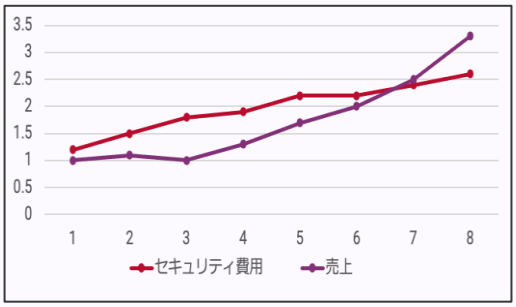
通信制御をしていること自体で効果が出ていると考えることもできますが、機器導入前の数値を把握できていると、機器を導入した際の効果をより把握することにつながります。
機器の入れ替えなどの際には、現状を把握し、目指す効果を検討し、比較する数値を定めておくことを意識してはいかがでしょう。

セキュリティが利益につながる事例
～セキュリティをコストとしない～

セキュリティの取り組みが売上につながる

セキュリティの重要性や必要性は多くの企業で認識されてきています。セキュリティの強化は経営課題ととらえ、設備投資を行っている企業も多いのではないでしょうか？

ある企業では、セキュリティをより強化していくためにネットワークを制御するセキュリティ製品の導入を決めました。セキュリティ担当者は予算獲得にあたり、セキュリティ機器を入れることによる効果を考える必要性があります。以下の観点から経営層の説得にあたりました。



セキュリティへの投資が売上に影響する場合も

ある企業の経営層にむけた説明のポイント

・他社との比較

ユーザーの声などがセキュリティベンダのホームページに記載されています。同業、同規模会社などの情報を集めました。

・現在の脅威状況

自社の分析や社員へのヒアリングを行ったところ、スパムメールと思しきメールなどが会社にも届いていることがわかりました。現在は大きな事故等にはなっていませんが、今後も事故が起きないとは限りません。セキュリティ製品を入れることで事前に対策を打つこととしました。

・企業アピール

セキュリティがしっかりしているということは、会社運営のアピール材料になります。サプライチェーンに代表されるように、企業間の連携を行う中でセキュリティがしっかりしているということは重要な要素です。機会損失を未然に防ぐことにつながります。

利用者一覧
同業他社
同規模会社

脅威状況

一番苦労した点は、現在の状況を把握することでした。情報を取得していなかったため、比較するデータがありませんでした。そのため、まずは現状のデータ取得に力を入れました。データ取得が事前にできたことで、セキュリティ製品の導入を終えた後に取得したデータと比較をすることができるようになりました。

導入効果を求める声が出始めた際には、金銭的な面で費用を回収することは難しく、事故の件数の減少や従業員の理解度、比較したデータの結果が効果となりました。

最近では、セキュリティ強化の取り組みから効果が生まれています。企業とのパートナー連携ではセキュリティ不備を指摘されることが段々と少なくなり、対応にかける時間が短縮されました。スムーズな連携からビジネスチャンスを生み出し、機会損失を減らす効果も出始めています。また、デジタルを活用したサービス展開を視野に入れていく中で、社内で取り組んできたセキュリティのノウハウや知識を活かすこともできるようになりました。特に、効果測定のデータがサービス提供をする際のデータとして活用されています。現在は、セキュリティレベルが高いサービスをお客様に提供でき、社内のセキュリティとサービスのセキュリティの相乗効果を生み出しています。

サービスのセキュリティの事例
～新規サービス企画とセキュリティ～

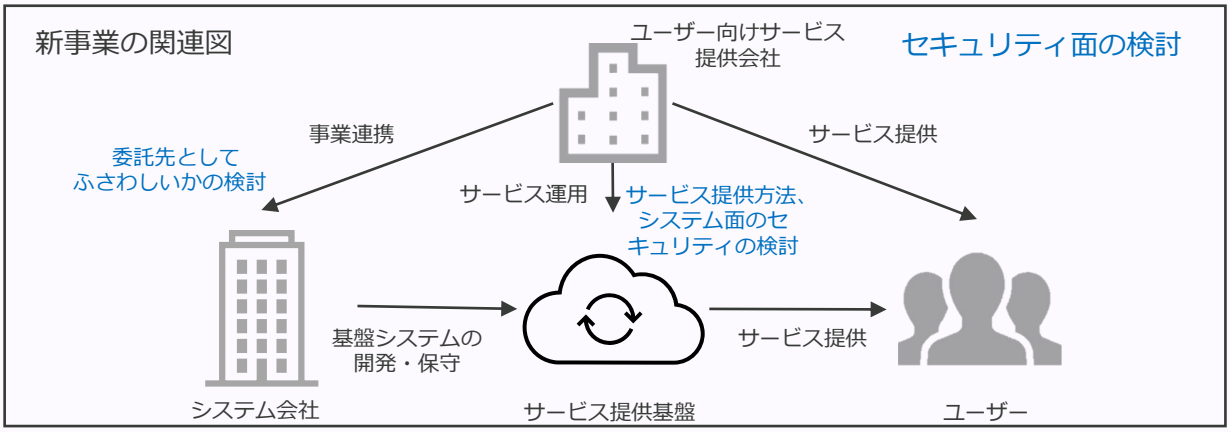
事業継続のためリスクへ対応する

DXに代表されるように、新たなビジネスモデルを創出していく事業企画を進めることが多くなりました。今までになかった取り組みですので、事業を企画する際には、多くのことを検討しないといけません。この検討にはセキュリティも含まれます。

セキュリティというと社内の情報を守るといったイメージが強いですが、これからのセキュリティ担当は、事業への関与を高め、自社サービスに対してのセキュリティも考えていく必要があります。

ある企業では、システム会社と連携し新システムを構築し、ユーザーへサービスを提供する企画を進めています。

事業企画では、セキュリティ担当者も加わり議論が進められます。セキュリティ担当者の観点としては、この事業を継続していくためのリスクを把握し、適切に対処していくことでした。



委託先に対するセキュリティ担当者の対応	
委託先組織に対する確認	セキュリティのトレーニングは最低年1回は実施している
	個人情報に関する責任者を定めている
委託先開発環境の確認	開発環境と本番環境は分割している
	特権アカウントは厳重に管理されている
	本番環境へのアクセスは制限されている

サービス運用に対するセキュリティ担当者の対応	
運用ルール検討	ユーザー問い合わせ対応の認証方法
	OS・アプリケーションなどのバージョンアップ対応手順
システム検討	ログイン失敗回数の許容範囲
	認証失敗時の画面表示文言の検討
	取得ログやログへのアクセス権

※記載の内容はサンプルです。

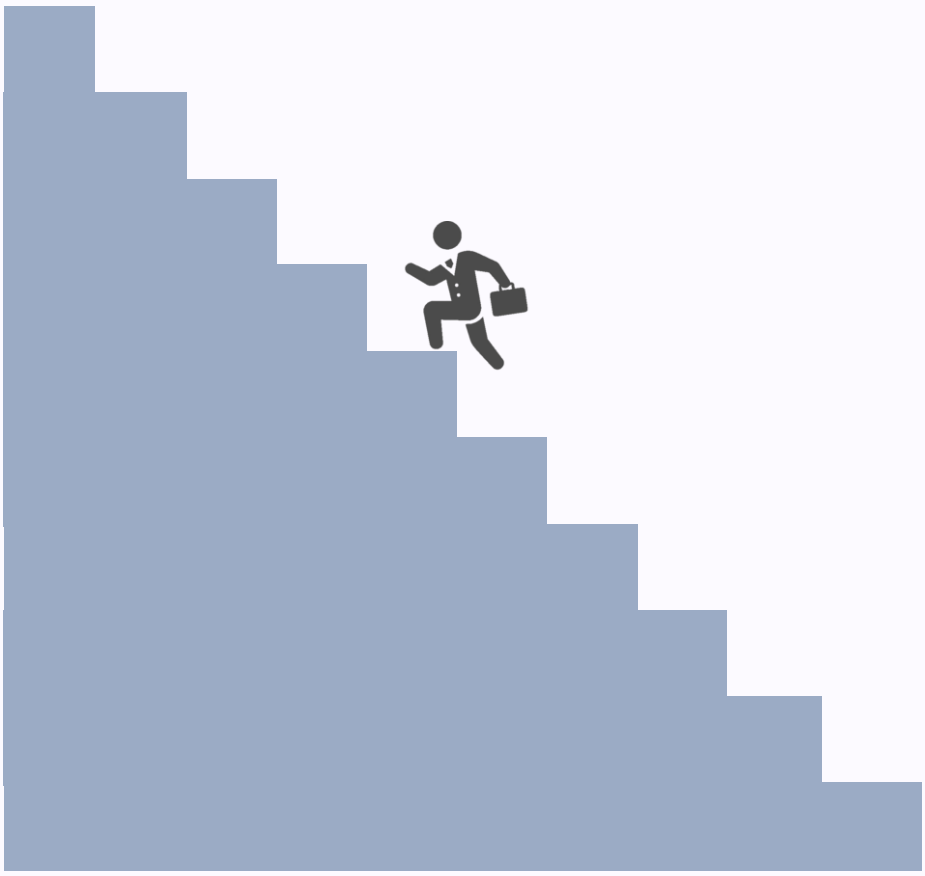
セキュリティ担当者は事業設計から関わることで、リスクの対応をより早い段階で行うことができます。より早い段階だからこそ、回避や低減など多くの選択肢から手段を検討でき、事業継続のための適切な対応につながります。

今まで漠然とセキュリティ対策をしてきたけれども、場当たり的な対応が多かったように感じる。そして、低減ばかり考えていたけれど、回避・低減・転嫁・受容など、リスクに対していろいろなアプローチの方法があることがわかった。リスク分析を改めて見直し、どの対応が適切か考えてみよう。どうしても対応できないリスクについては、回避をするという考え方も大切だと感じた。

自社が抱えるリスクに対して、ずっと自分たちだけで対応しなければいけないと思っていたけれど、保守会社にリスクを転嫁するという選択を考えてみてもいいかもしれない。サイバー保険などの加入を検討してもよいだろう。

対策をするには予算は重要だ。今まで、セキュリティ対策にはどのくらいの予算が必要なのかわからなかったが、前回のセミナーで習ったALEなどを活用して、予算を確保できるように努めよう。

リスクに向き合う
リスクに対応する



コラム
～セキュリティは投資かコストか？～

　セキュリティ強化をしていくためには少なからず費用がかかります。一時的にかかる機器購入などの費用だけでなく、保守などのような月々かかる費用もあります。よくセキュリティは投資かコストかという議論を耳にします。日本の場合、社内業務のデジタル化を進めてきたという歴史的な経緯もあり、圧倒的にコストと捉える風潮がありました。

　しかしながら近年はDXなどの時代の流れもあり、事業系のIT活用が積極的に行われています。お客様にクラウドを利用してサービスを提供するなどが活発化されている今日では、セキュリティは投資と考える人が増えているのでは無いでしょうか？セキュリティ事故の発生は多くの顧客に被害を与える可能性があります。また、最悪の場合には倒産してしまう可能性もあります。事業分野におけるセキュリティをより意識する今日では、セキュリティ強化にかけた費用が投資となってお客様から選ばれるようになります。

　社内のセキュリティにおいては費用を回収することはなかなか難しいことも事実です。しかし、社内セキュリティの取り組みで得たリスク分析の実施方法やルールの作り方、対応策の実現方法などは事業分野におけるセキュリティでも充分活かせるのでは無いでしょうか？

あとがき

　セキュリティの対策を立てていく際には、予算をどのように獲得していけば良いのか、対策はどこまでやれば良いのかという不安が少なからず出てきます。特に、予算獲得できなかった場合に、リスクが残り続けることは、担当者として心労も絶えないのではないでしょうか？対策をすれば、従業員から効率が落ちたという声を聞くこともあり、複雑な気持ちになるセキュリティ担当者もいるのではないでしょうか？
　セキュリティの取り組みを一人で行っていると色々な方面からの意見に悩むことは多いと思います。社内外で相談や共有をできる人を見つけ、セキュリティ対策に臨めるようにしていけると良いと思っています。セキュリティという分野は広いですが、横のつながりも強い分野であるとも感じます。ぜひ、外との繋がりを大切にしてください。

令和4年度

中小企業サイバーセキュリティ対策継続支援事業

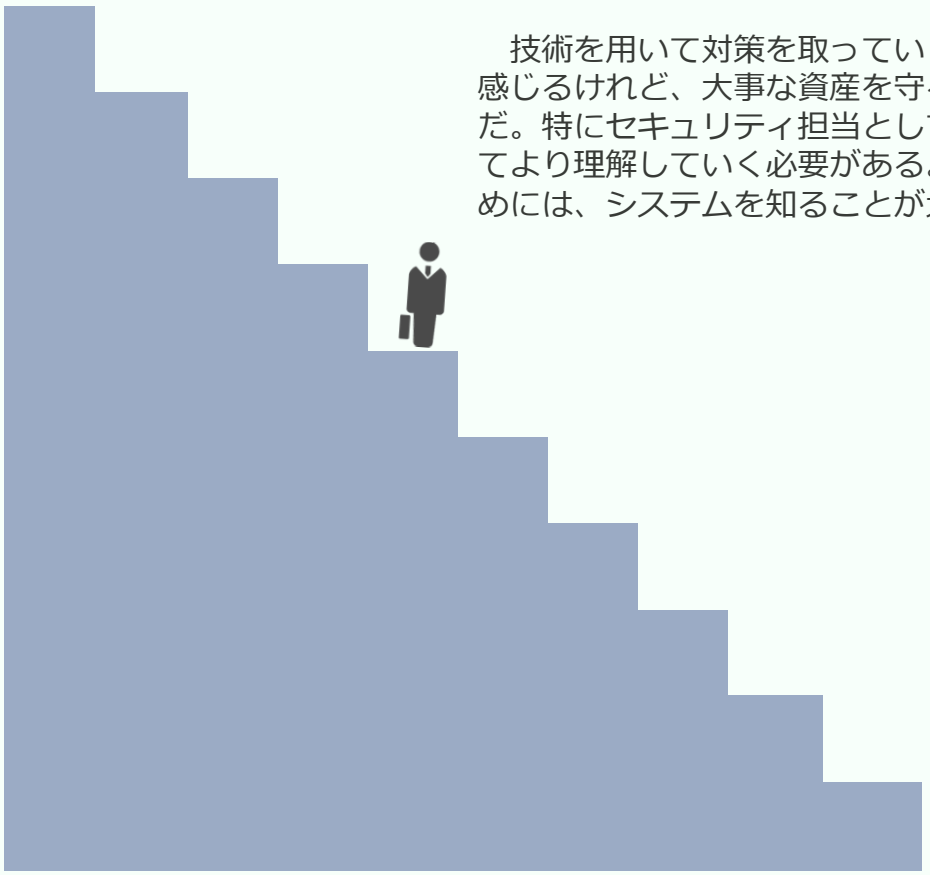
第7回

セミナー開催日：令和4年11月15日

技術を味方に
技術を活かし
技術に頼る

　リスク分析や対応の検討を行い、何を守っていくのか、どのような方針で対応していくのかという点は意識ができるようになってきた。しかし、実際にはどうやって資産を守っていけばよいのだろうか？人に対して教育をして、みんなで注意することで資産を守っていくことは必要だと思う。とは言うものの、できることならば人の負担を減らして対策を取れるようになっていきたい。

　人のミスをゼロにすることは難しいため、技術的な対策を取っていくのが良いらしい。特に現在ではデジタル化が推進されているので、使っているシステムを守るためにも技術を用いたセキュリティは理解しておかないといけない。さらに、セキュリティを強化するためのシステムもあるため、それらも使いこなす必要がある。



　技術を用いて対策を取っていくというのは難しいと感じるけれど、大事な資産を守るためには必要なことだ。特にセキュリティ担当としては、システムについてより理解していく必要がある。手段を選んでいくためには、システムを知ることが大切だ。

アップデートと ウイルス対策ソフトの導入

OSやソフトウェアは定期的にアップデートを行う必要があります。セキュリティ担当としては、企業が保有する情報機器のセキュリティ機能とその設定を把握し適切に管理する必要があります。

Point① 機器やOS、ソフトウェアの状態を常に把握しておく

代表的な機器の内部構成	代表的な機器の内部構成（ホストOS型）	代表的な機器の内部構成（ハイパーバイザー型）
ソフトウェア アプリケーション	ソフトウェア アプリケーション	ソフトウェア アプリケーション
ミドルウェア	ミドルウェア	ミドルウェア
	ゲストOS	ゲストOS
	仮想化ソフト	仮想化ソフト
ホストOS	ホストOS	
ハードウェア	ハードウェア	ハードウェア

セキュリティの重要ポイントとして、OSやソフトウェアのアップデートがあげられています。セキュリティ担当としては、これらをもれなく適切に行うことが重要となります。

管理名称	記載事項の例
機器名称	ホスト名、呼称 など
OSバージョン	Windows 11 など
管理責任者	A部署 ○○ など
ミドルウェアバージョン	Apache Tomcat 10.15.7 など
保守期間	2021年1月 ～ 2022年12月

また、昨今は仮想化が主流となっているため、バージョンアップについても注意が必要となります。

バージョンアップにおけるポイント

1. 機器や各種バージョンを把握し、アップデートやサポート終了情報を把握する
2. バージョンアップをする環境を把握し、相互関係性と動作確認を検証する
3. バージョンアップをして動作保証ができない場合には代替案を検討しておく

Point② ウイルス対策ソフトの導入

セキュリティ対策ソフトには、個人用の製品と法人用の製品が多くのベンダから提供されています。従業員数にもよりますが、法人用ソフトには管理者機能がついており、端末管理がしやすくなるという特徴があります。

メリットの例	デメリットの例
ライセンス管理の効率化	パソコンの動作が遅くなる場合がある
セキュリティルールを統一できる	高機能なため高コストになる可能性がある
管理者の情報管理が一元化できる	PCの今後の購入で選択肢が減る場合がある
運用が一元化できる	ー

Day7

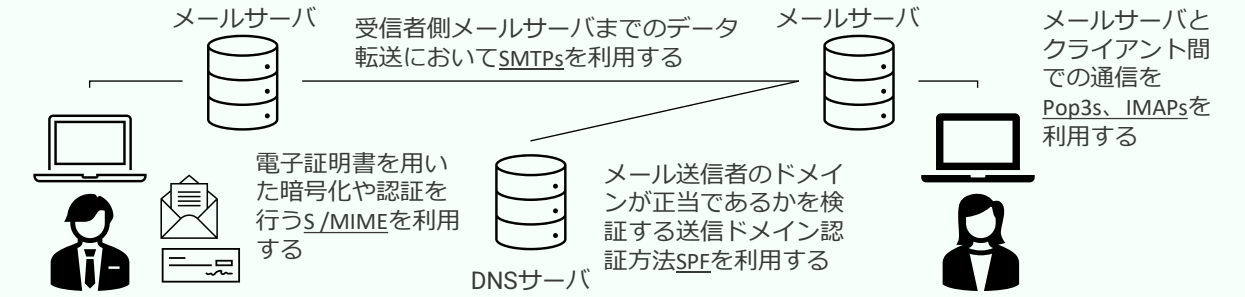
1.技術的対策の基本事項

電子メールの安全利用

電子メールは多くのビジネスシーンで利用されている反面、攻撃に利用される可能性が高くなります。電子メールを安全に利用することは、ウイルス感染などの危険性を減らすことにつながります。

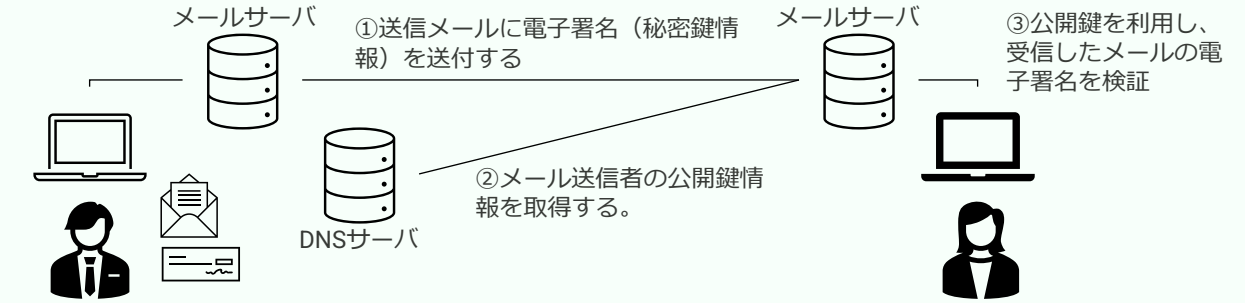
Point① メールシステムのセキュリティを強化する

メールの仕組みにおける強化の例

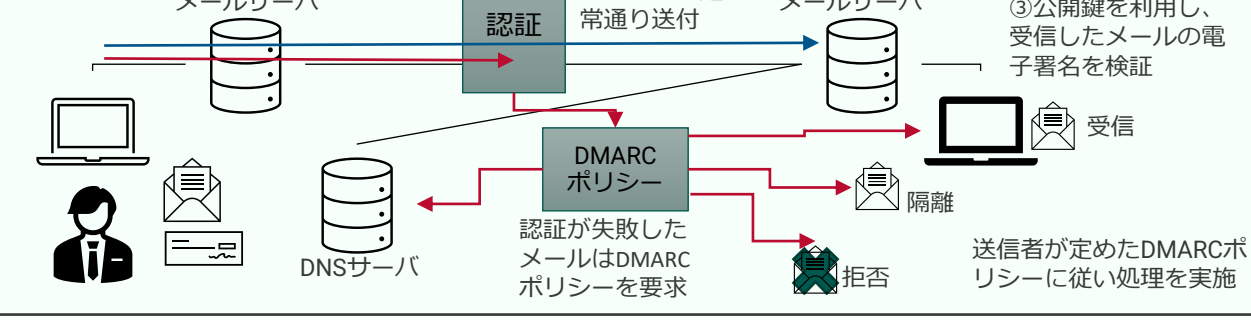


SMTPs：メールサーバ間の通信で利用するSMTPと通信をTLSで暗号化
Pop3s，IMAPs：受信用のメールサーバとクライアントの間の通信で利用するプロトコルをTLSで暗号化
SPF：メール受信時に送信元のドメインが詐称されていないか、IPアドレスを利用して確認し、なりすましを防ぐ
S /MIME：認証局が発行した電子証明書を使用し、送信メールの暗号化、電子署名付きメールを送信する

DKIMを用いた認証



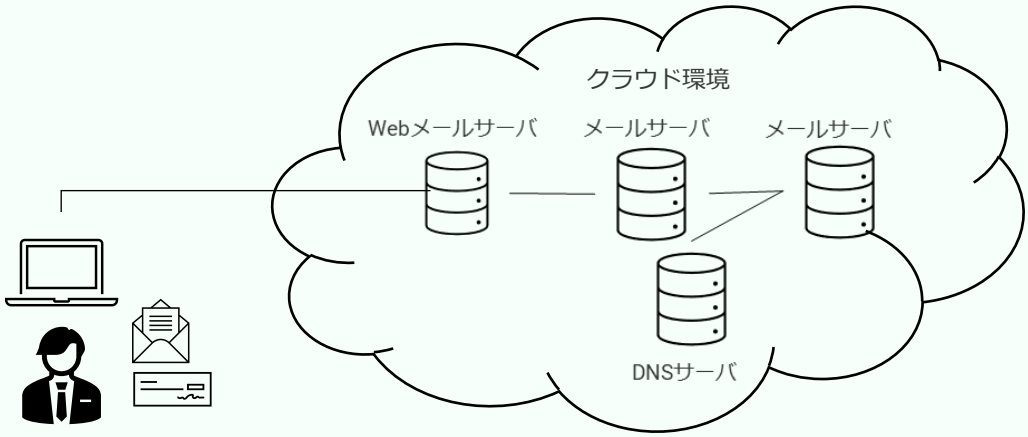
DMARCを用いた認証



DKIM：メール受信時に送信元のドメインが詐称されていないか、電子署名を利用してメール送信元が詐称されていないかどうかを確認する
DMARC：メール送信側が前もって、メール受信側の認証失敗時の動きを「DMARCポリシー」として設定し、認証失敗時に受信メールをどう扱うか判断する

電子メールの安全利用

Point② クラウドメール（Webメール）の利用も検討



クラウドメール（Webメール）を使うと、メールサーバなど自社で保有、管理する手間が大幅に削減できます。また、インターネットにつながる環境であればWebブラウザからもメールの閲覧・送受信が可能となります。

One point

メールには、メールヘッダーと呼ばれる情報が存在します。「To」(宛先)、「From」(送信元)、「Subject」(題名)など、電子メールの送信に必要な情報が含まれています。メールヘッダーを見ていくと、IPアドレス偽装、類似ドメイン、不正な返信などの情報が確認できる場合があります。経由してきたサーバは「Received」の部分で見ることができます。通常「Received」がいくつかある場合は、下から上へという流れでメールが送られています(青字箇所)。また「送信者」の部分が改竄される場合は「From」の部分が改竄され、通常は「From」の部分と同じであるはずの「Return-Path」の部分のメールアドレスと異なったものになります(赤字箇所)。

ただし、フリーメールを使って送信される場合やアカウントが乗っ取られてメールが送られてくるような場合には、メールヘッダーに異常が見られないというケースもあり、添付ファイルやURLの確認といった作業が必要となります。

メールヘッダーの例

Return-Path: <AAAA@AA-BBBB.co.jp>
Received: from mail2.kk-apex.co.jp (mail2 AAAA@AA-BBBB.co.jp[210.xxx.xxx.227])
by xxxxx.xxx.co.jp (8.9.3/8.9.3)
with SMTP id JAA0711234 for <kxxx.@xxx.co.jp>; Wed, ** Mar 20XX 09:13:09 +0900
Received: from ws1.DD-DDDDDDD.co.jp ([210.xxx.xxx.226])
by mail2. DD-DDDDDDD.co.jp (NAVGW 2.5.2.9)
with SMTP id M**** for < kxxx.@xxx.co.jp>; Wed, ** Mar 20XX 09:32:21 +0900
Received: from pc01([192.xxx.xxx.55])
by ws1. AAAA@AA-BBBB.co.jp(8.11.6/3.7Wpl2)
with ESMTP id h2J0Cw028698; Wed, 19 Mar 2003 09:12:58 +0900
From: “KKKK KKKK” <KK@kkkkk.co.jp>
To: “’DDD DDDD’” <DD@ddddd.co.jp>
Subject:メールヘッダー
Date: Wed, ** Mar 20XX 09:10:33 +0900
Message-ID: <000501c2edab$f5be11a0$3701a8c0@ws1.AA-AAAAA.co.jp>
MIME-Version: 1.0
Content-Type: text/plain; charset="iso-2022-jp"
Content-Transfer-Encoding: 8bit

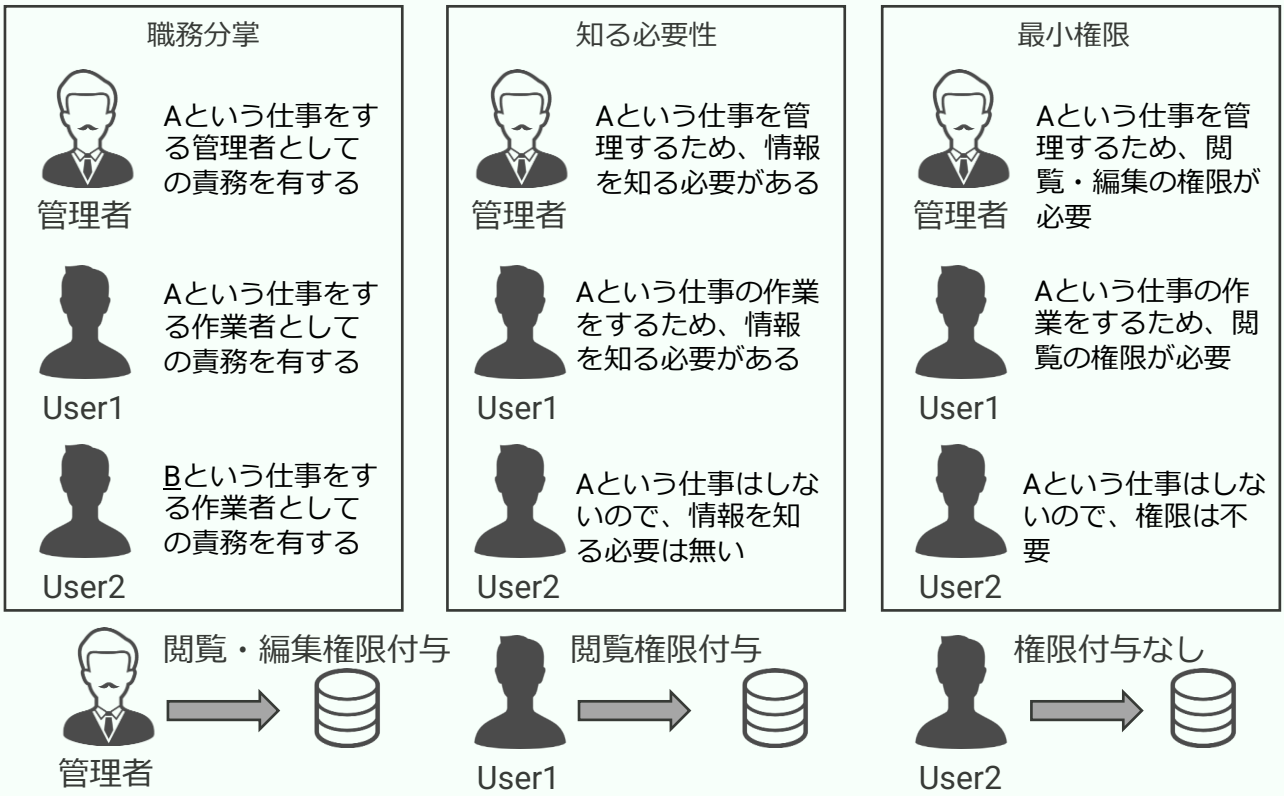
本メールヘッダーはサンプルです。

アカウント管理

デジタル化が進む今日においては、アカウントは個人を特定する情報であり、適切に管理する必要があります。アカウントは誰にでも与えるのではなく、必要な人に必要な分だけ与えることで情報へのアクセスや流出の可能性を減らすことにつながります。職務分掌や知る必要性は、規程で定める役割や業務分掌などと対応付けた管理を行います。

Point① 適切な権限付与の実施

アカウントを利用する際には、どのような役割（ロールと表現される場合もあります）を用意しどのような人（例えば役職、職務担当者など）に付与するかを検討する必要があります。



代表的なアカウントの種類と役割の例		
アカウントの種類	**役割**	**できること**
特権アカウント	管理担当者に付与されるアカウント	• アカウント作成・削除・停止 • 役割とアカウントの紐付け • 設定追加・変更・削除など
ユーザーアカウント1	役職者（部長職）に付与されるアカウント	• 部門所属者への部門内フォルダへのアクセス権付与 • ファイル作成・変更・削除
ユーザーアカウント2	一般ユーザーに貸与されるアカウント	• 許可されたファイル・フォルダのアクセス • ファイルの作成・変更・削除
監査アカウント	監査担当者に貸与されるアカウント	• ログの閲覧

アカウント管理

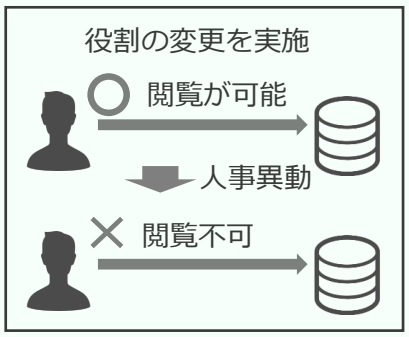
Point② 特権アカウントと一般アカウントの管理

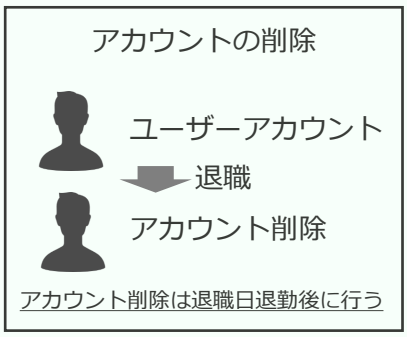
特権アカウントと一般アカウントでは用途とできることが異なります。管理者が主に利用する特権アカウントが流出すると、大きな影響が出るので管理には一層の注意が必要です。

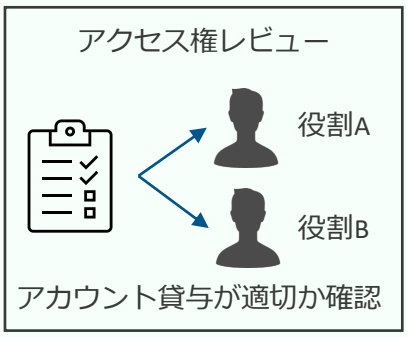
	特権アカウント	一般アカウント
利用者	✓ 情報システムセキュリティ責任者 ✓ 従業員	✓ 一般社員
アカウント	✓ 推奨：推測困難であるもの <禁止アカウント名> WindowsOS：administrator、admin LinuxOS：root ✓ 1つの特権アカウント名を2名以上で共用しない ✓ Guest用アカウントは無効化する	✓ 従業員番号 ✓ 従業員コード
認証	<パスワードに使う文字> ✓ 12文字以上 <パスワードの管理> ✓ ロックアウトの閾値は3回、時間は6時間に設定する	<パスワードに使う文字> ✓ 10文字以上 <パスワードの管理> ✓ ロックアウトの閾値は5回、時間は1時間に設定する
利用時の注意点	✓ 作業申請を出し、承認された作業のみでアカウントを利用する ✓ 利用時は常に2名以上で作業を行い、ダブルチェックできる体制で利用する	✓ 個人の責任により管理し、業務で利用する
その他	✓ 保守業者等へ貸し出す際には、専用の特権アカウントを提供する。また作業後はアカウントの削除、またはパスワードの変更を行う。	✓ 第3者へ貸し出す際はユニークなアカウントと必要な権限のみ付与し、作業終了後は削除する

Point③ 人事異動や退職のアクセス権の変更を後回しにしない

アカウントは人事異動や退職により変更が発生します。特に退職後はアカウント削除などを実施することが求められます。







Day7

1.技術的対策の基本事項

認証管理

本人の認証において現在広く利用されているのが、パスワードによる認証です。最近では、パスワードと他の要素を組み合わせて２要素認証などが推奨されています。セキュリティの担当者としては、識別・認証・認可の違いや認証方法の違いを理解し、各システムにおける重要度などを加味した認証の仕組みを検討することが重要です。

識別・認証・認可の違い

ユーザーがログインを行う過程には、以下のような意味合いがあります。

識別
ユーザーID等を用いて、自身が誰であるかを表す

認証
パスワード等を用いて許可された本人であることを表す

認可
認証された者が行うことのできる操作の範囲を決定する

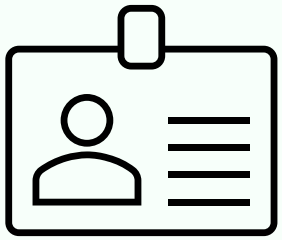
認証方法の違い

認証の目的は、本人しか知り得ない・持ち得ない情報をもとに本人であることを特定することです。

知識による認証

知識による認証の代表例はパスワードです。自分が覚えていること、知っていることで本人を特定します。

持ち物による認証



持ち物による認証の代表例はICカードや鍵などです。持っているということで本人を特定します。

生体による認証

生体による認証の代表例は指紋や虹彩などです。自身の体の一部を利用して本人を特定します。

生体認証の情報が流出した際には指紋を変えることはできませんが、パスワードであればすぐに変更することが可能です。３つの認証方法に基本的には優劣はありません。利用するシステムやシステムで利活用・保存される資産などにおいて決定することが望ましいと言えます。また、これらの認証方法を複数組み合わせた認証方法を多要素認証と呼びます。多要素認証も様々な内容がありますので、検討が必要です。

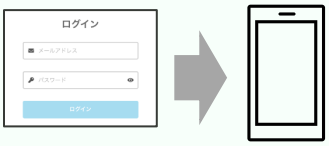
Day7

1.技術的対策の基本事項

認証管理

Point① システム利用時の適切な認証を

安全な環境が無くなっている今日、認証は自身を証明するものであり、セキュリティ担当者としては、認証情報が真正性を担保するものになります。利用するシステムの重要度に合わせた認証方法を検討しましょう。

社内へのVPN接続	グループウェア	VPN接続後アクセスできるファイルサーバ
		
外部からのアクセスとなるため、常に2要素認証で認証を行う	初回のみ2段階認証を求めるが、同日中に同じ場所からのアクセスは、パスワードのみで認証を行う	アクセス制限がすでにかけられているので、パスワードのみで認証を行う

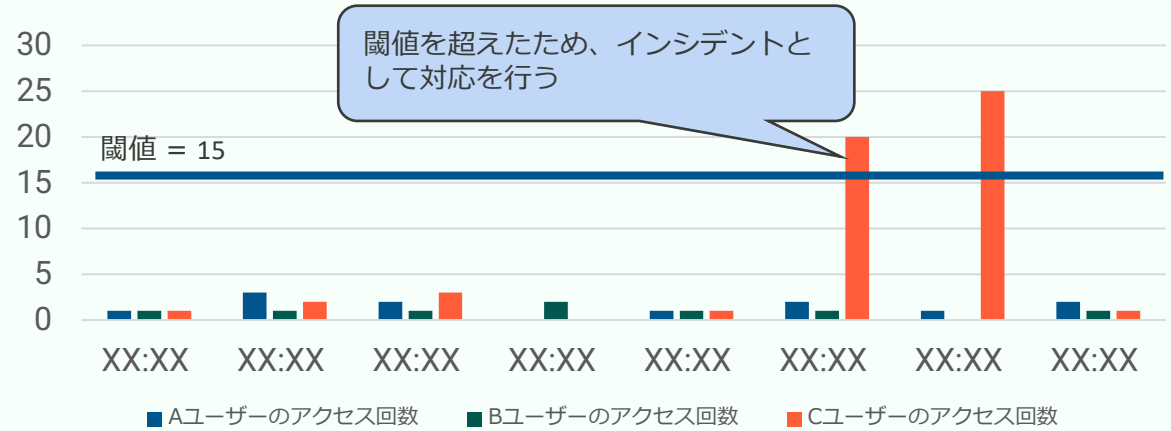
Point② 認証ログを管理し適切な利用を

一般的にログインという行為には、識別と認証が確認されて成功となります。そのため、認証ログを適切に確認し管理することで外部からの攻撃の可能性などに気づくことになります。

認証ログの一元管理	認証ログの個人確認
認証ログとは、ログイン試行の成功・失敗のログです。例えばログイン試行が一定期間内に大量に発生することは、リスト型攻撃が発生している可能性があり、対処が必要です。	最近では、日常的にログインされる場所以外から発生した時に、メール通知されます。これに気づくことにより直ちにセッションの切断や認証方法の変更の対応をすることで、被害の影響を小さくすることが可能になります。

Point③ 閾値を決めて対応の基準に

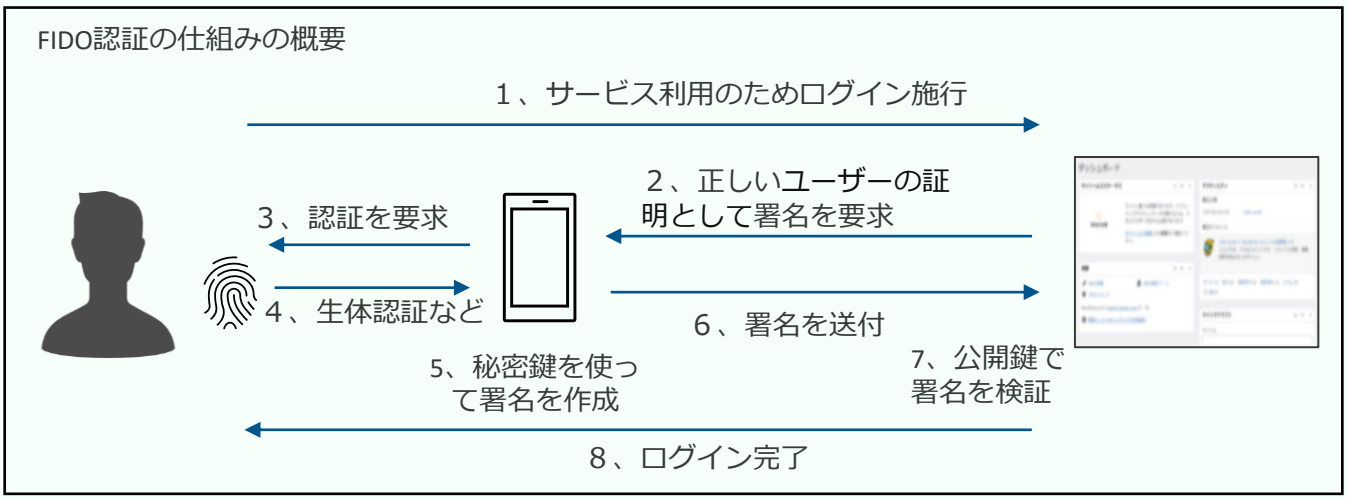
閾値とは、境界となる基準の値です。例えばリスト型攻撃・DDoS攻撃は何を持って攻撃と判断し対応するのか基準を決めておくことで、インシデント対応がスムーズになります。



認証管理

Point④ パスワード認証に代わる認証技術

パスワードに代わる認証手段として期待される認証技術としてFIDO（ファイド）というものがあります。



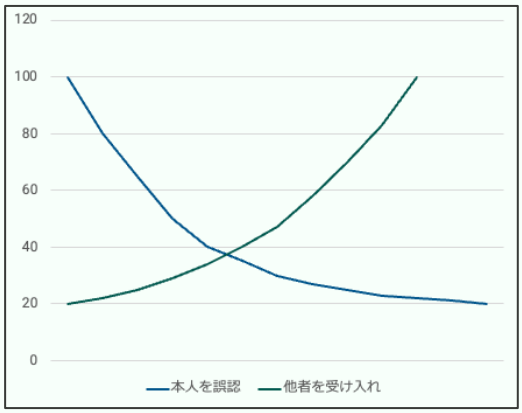
パスワードのような情報をサービスを提供する側で保持をしないことが最大の特徴となります。FIDOでは秘密鍵と公開鍵を利用して署名を検証することで認証を行います。署名を作成するための作業として、デバイスで生体認証などを行ないますが、この生体属性情報をサービスログインの認証では利用しないため、サービス提供事業者側に情報を保有する必要がなくなるというメリットがあります。また、利用者側も情報を提供する必要がなくなります。また、端末を紛失したとしても、署名を作成するための作業となるデバイスでの生体認証に失敗するため、署名作成が行えず、安全性が高い認証方式と言われています。

これらが利用できるシステムでは、パスワードよりも積極的に利用することが推奨されます。ただし、現状ではパスワードと並行した運用となっているケースもあります。サービス仕様をよく理解したうえで利用していきましょう。

One point

最近では、スマートフォンの普及に伴い、生体属性を利用するシーンも多くなりました。生体属性の場合には、「本人が誤って拒否される場合」「他人を誤って受け入れてしまう場合」が存在します。一致率を高く設定しすぎると本人を拒否する率が高まり、低く設定しすぎると他人を受け入れてしまう可能性が高まります。

これらの特性を理解し、対象のシステムでどのような認証方法を利用するかを考えましょう。



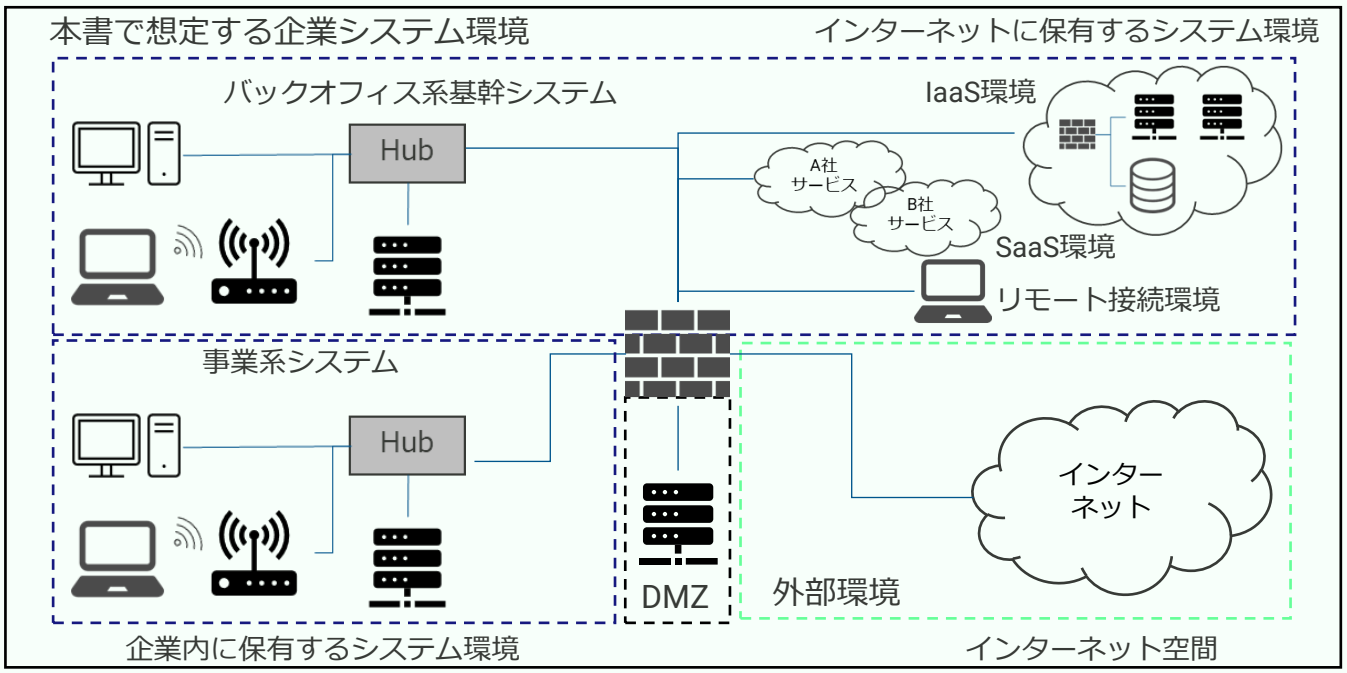
ミニワーク
～考えてみよう～

ミニワークテーマ

アカウント管理方法について、自社で行っている良いと思う取り組みや、改善したいと思う取り組みを考えよう

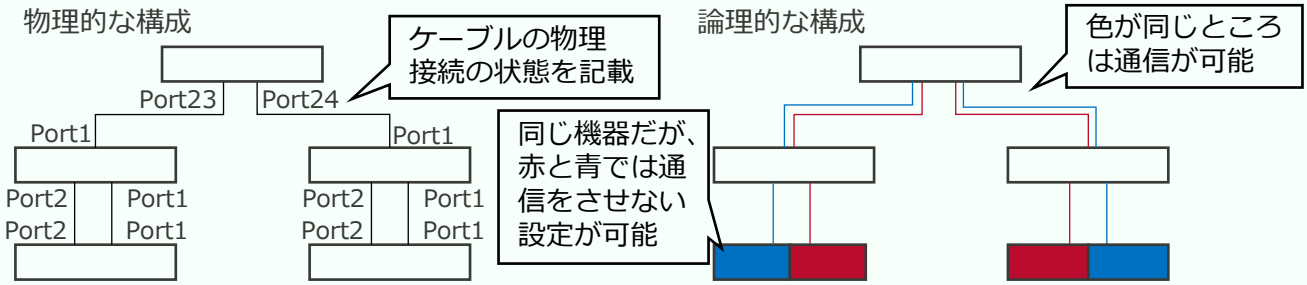
ネットワーク構成を検討する

会社のインフラ環境はバックオフィス系業務を行う基幹システムや事業系システムなど複雑化しています。特に最近ではクラウドと自社の建物内に存在するシステムが混在する環境のため、セキュリティの適用範囲が広範囲になります。



Point① システム構成を正しく理解する

システム構成やネットワーク構成を正しく作成し、管理することはセキュリティを向上させるために非常に重要です。構成を正しく把握できていないと、攻撃の影響範囲の推測ができず、被害が大きくなる可能性があります。



物理・論理ネットワークを正しく理解する

ネットワーク構成図は、物理的な配線形態を表す物理構成図と、ネットワークの論理的な接続を表す論理構成図に分かれます。通信の可否の状況を確認する際は、論理ネットワークについても確認を行いましょう。

冗長性を確保し可用性を高める

冗長とは、障害が発生することに備えて、予備の設備などを平常時から運用しておくことです。ただし、予備の設備のメンテナンスをおろそかにすると、切り替わったタイミングでセキュリティ機能が弱まるため注意が必要です。

影響範囲を特定し対応計画を検討する

拠点間をVPNなどで接続する場合には、論理ネットワーク上は一つのネットワークに所属していることになります。影響範囲を正しく理解し対策をしましょう。

Day7
2.インフラセキュリティ

ネットワークで防御を行う

現在の多くのサービスはネットワークが主に利用されます。ネットワークで防御を行い、攻撃を検知していくことが求められます。

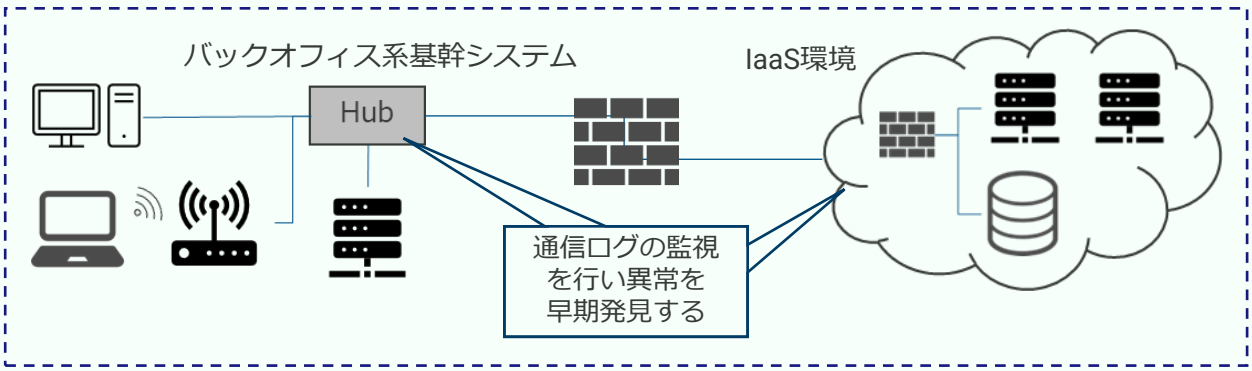
Point① それぞれの機器の特徴を活かし防御を行う

Firewall	IDS /IPS	WAF
主に、IPアドレスやポートを判断材料として不正と思われる通信やアクセスを防ぎます。インターネットとの境目に設置されることが多い製品です。	IDSは不正侵入検知を行います。IPSではこれに加えて防御を行えます。IPS・IDSは通信の中身（パケット）の内容を監視し不正アクセスを検知します。バッファオーバーフロー攻撃など攻撃コードを送りつける通信を検知できます。	Web アプリケーションに対する攻撃を防ぐことに特化しています。SQL インジェクションやクロスサイトスクリプティングなどWeb特有の通信に対して、検知・防御できます。

※UTM(Unified Threat Management：統合脅威管理)とは・・・
ファイアウォール、アンチウイルス、IPS/IDSなど複数のセキュリティ対策機能を１つのハードウェアに統合した製品をさします。そのため、UTMを利用していると聞いた際には、どのような機能が含まれた製品であり、何の機能を有効にしているか確認する必要があります。
セキュリティ強化の一環として、「UTMを導入している」から「UTMを導入し、〇〇と△△の機能を利用している 」と説明できるようにしていきましょう。

Point② ネットワークを監視し攻撃を把握する

近年では攻撃も巧みになり、防御だけではなく検知の強化も重要になってきています。誰が、どの端末から、どのデータに対してアクセスしているかなどを把握する仕組みを用いることが重要です。特にインターネットの境であるUTMでは、インターネットへの通信ログは取得できますが、社内やクラウド環境内のログを取得することはできません。これらに対応した検知の仕組みを導入することも重要です。



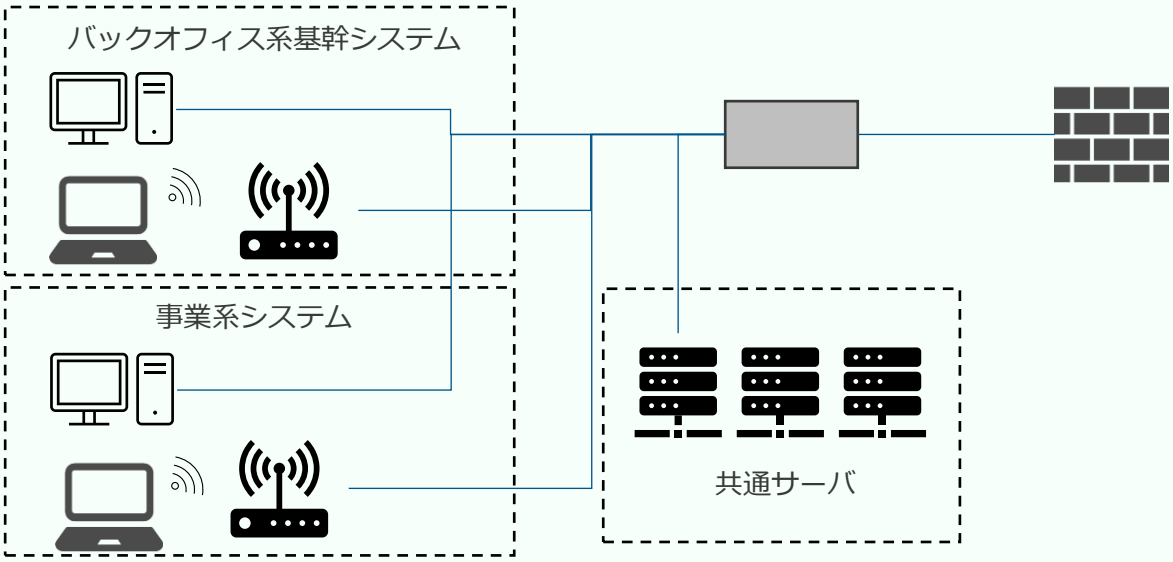
攻撃を検知するためには、ファイルへのアクセス・移動、機器の設定変更などを検知することが重要です。また、可用性の観点から、各機器が正常に動いているかを把握することも重要です。通信の監視と合わせて各機器の異常を早期に発見できるようにしましょう。

LAN分割による対策

ネットワークセキュリティにおいてLAN分割という選択が可能です。人事や総務などを有するバックオフィス系基幹ネットワークとサービス開発・提供を行う事業系ネットワークを同じルールにすることには限界があります。LANを分割しそれぞれに適したルールを設けることで、DXを加速させそれぞれのLANに合わせた対策をとることができるようになります。

Point① それぞれの機能に分けたLAN分割

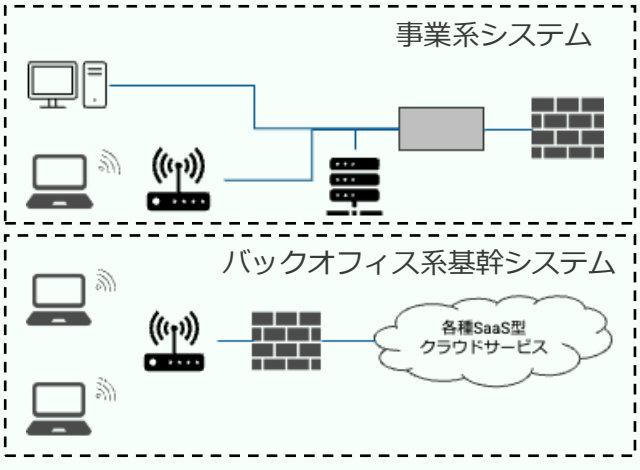
LAN環境を分割することにより、影響範囲を各LANの中に抑える効果があります。また、それぞれのルールで運用ができるため、DXなどを加速させることが期待できます。



バックオフィス系基幹システムと事業系システムをあえて相互に通信できないようにすることで、問題発生時の影響を最小限にとどめることができます。また、ファイアウォールで各LANに対する通信ポリシーを設定することで、それぞれのLANに最適なセキュリティを整えることにつながります。

こんな事例も

従業員30名程度のある会社では、セキュリティの一環として、社内業務従事者環境と事業部門従事者環境を物理的に分断して利用しています。それぞれの特性を考慮した結果このような形になりましたが、業務における大きな影響は出ていません。また、社内業務従事者環境と事業部門従事者環境のファイルのやり取りなどはクラウドを利用しています。クラウド利用の浸透にもつながり、結果的に利便性の向上にもつながりました。



ミニワーク
～考えてみよう～

ミニワークテーマ

FWやUTMなどで現在行っている自社のセキュリティ対策にはどのようなものがあるか考えてみましょう。

Day7
2.インフラセキュリティ

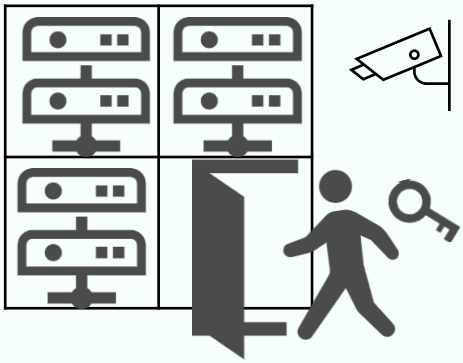
サーバ防御

サーバとは、サービスや機能を提供する側のコンピュータの総称です。現在のサーバは仮想化されていることも多く、管理が複雑になっています。また、最近ではサーバがクラウド環境に配置されているということも珍しくありません。

Point① サーバを安全に管理する

自社の建物内にサーバがある場合には、サーバ本体だけでなく、設置場所のサーバルームやサーバを設置するラックなどにも配慮することが求められます。

サーバの設置場所としては、外部の人間や権限のない社員、職員が容易にサーバに近づけないような情報セキュリティ上の問題がない場所であるかどうかを検討します。特にサーバルーム（またはサーバラック）は、防犯カメラの設置や生体認証の導入など、他の執務エリアよりもセキュリティ対策を強化することも重要です。また入退室（または開閉）の記録をとり、管理することもセキュリティを高めるためには重要となります。入退室や利用のルールを定め文書化していくことがセキュリティ担当としては求められます。



Point② サーバ構成の特性を理解し管理する

最近では、自社の建物内にサーバを置かず、IaaS（Infrastructure as a Service）を利用しサーバを構築するケースも増えています。設置する環境や利用するクラウドサービスの特性を理解し、提供ベンダとの責任分界点を明確にしてセキュリティ対策にあたることが求められます。

<table>
<tr><th>構成</th><th>オンプレミス</th><th>IaaS
（Infrastructure as a Service）</th><th>PaaS
（Platform as a Service）</th><th>SaaS
（Software as a Service）</th></tr>
<tr><td>データ・ユーザー情報</td><td rowspan="7">ユーザー</td><td rowspan="6">ユーザー</td><td rowspan="2">ユーザー</td><td>ユーザー</td></tr>
<tr><td>ソフトウェア
アプリケーション</td><td rowspan="6">事業者</td></tr>
<tr><td>ミドルウェア</td><td rowspan="5">事業者</td></tr>
<tr><td>OS</td></tr>
<tr><td>仮想化ソフト</td></tr>
<tr><td>OS</td></tr>
<tr><td>ハードウェア</td><td>事業者</td></tr>
</table>

オンプレミス型の場合にはハードウェアから管理をする必要があります。IaaSの場合、クラウドとはいえOS管理やミドルウェアの管理が必要です。クラウド事業者の対応範囲を明確にし、保守業者としっかり会話をしセキュリティ対策を進めることが重要になります。また、近年ではクラウドの設定ミスにより情報が公開されてしまうという事件も多くなっています。データを格納しているフォルダの公開設定の間違いや、データの保存先の間違いなどはユーザー責任となりますので、注意しましょう。また、SaaS型の場合でもデータやユーザー情報はユーザー側で管理します。そして、事業者の管理が多い場合、事業者の作業ミスなどの影響を受ける可能性がありますので、リスクとして認識し、業者選定などは慎重に行う必要があります。

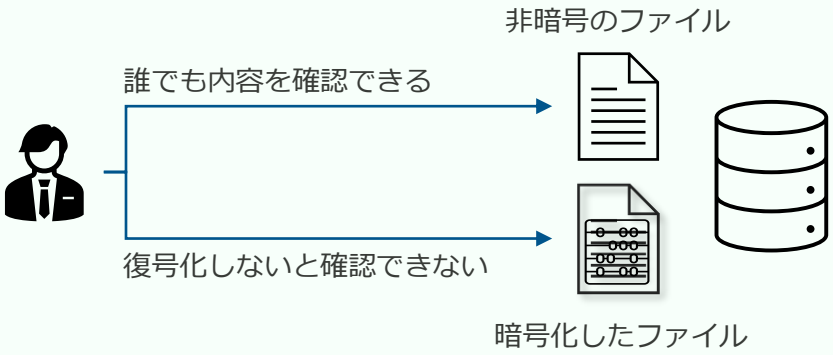
Day7
2.インフラセキュリティ

データ保護

資産の多くがデータ化されている今日において、データ保護は重要なセキュリティ対策となります。

Point① 情報を暗号化して管理する習慣を

企業が保有する情報を常に暗号化しておけば情報漏えいの対策として有効です。ウイルス感染などに伴う、社内のサーバやデータへの不正アクセス、悪意のある社員による持ち出しがあったとしても、暗号化された情報を読み取ることはほぼ不可能になります。ただし、鍵となる情報がわからなくなると所有者ですら読み取ることができないため注意が必要です。



Point② データ損失防止（DLP）の活用も検討

データ損失防止（DLP）は、データの流出や破壊を検出して防止するための対策です。機密情報を自動的に特定し、社外への送信や印刷出力をブロックすることが可能になります。

代表的な機能

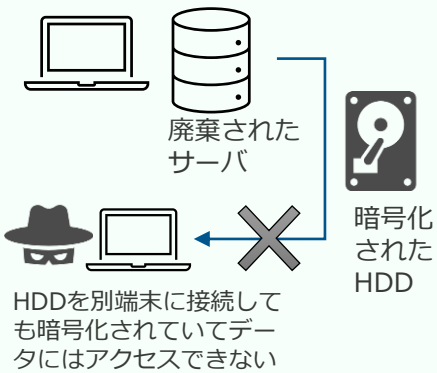
- 印刷制限機能
  → データのコピー、印刷、画面キャプチャなどの操作を制限します。
- コンテンツ監視機能
  → 機密情報を特定し、操作をリアルタイムに監視します。
- メールセキュリティ機能
  → 機密情報を特定し、本文あるいは添付による転送を強制的に禁止します。

One point

パソコンでもデータ保護を行うことが重要です。最近のパソコンにはストレージを暗号化する機能が標準で備わっています。

PCを紛失した場合、同じ型のパソコンでストレージを読み取ることができてしまう可能性があります。この対策として、HDDを暗号化することで情報流出を防ぐことが可能となります。

この機能はあくまで別端末にHDDが接続された際に有効になるため、通常利用しているときに利便性が下がることはありません。



バックアップの取得

情報資産が攻撃にあわないように防御をすること、攻撃にあっても気づけるように検知をすることはもちろん重要です。しかし、攻撃にあわないという保証ができない今日では、バックアップをとり、復旧できるようにしておくことも重要です。

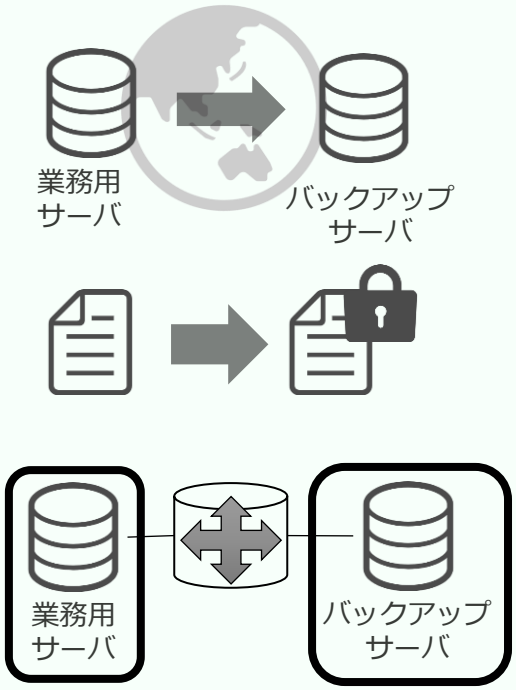
Point① バックアップを取得する

バックアップと言っても考慮する点は多岐にわたります。

■物理的な隔離
オフラインバックアップであれば、バックアップ媒体を遠隔地に輸送して保管します。オンラインバックアップでは遠隔地にあるストレージにバックアップを実施します。これらの方法は特に災害リスクへの対策となります。

■自動暗号化保存
バックアップ先にクラウドサービスを利用する場合に、バックアップ先からの情報漏えいリスクを防ぎます。復号化に必要な鍵は安全に保管する必要があるのはもちろんです。

■ネットワーク上の隔離
オンラインでバックアップを実施する場合は、サイバー攻撃リスクを考慮して、バックアップ先はネットワーク的に分離できることが重要です。安易に同一ネットワーク上にバックアップシステムを接続すると、共倒れのリスクが高まります。

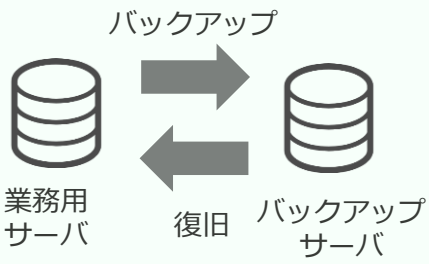


出典：総務省
バックアップの推奨
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/business/business_admin_10.html

バックアップの保存期間を長期にすれば古い情報まで保存できますが、ストレージの費用が高くなります。目的や事業特性を意識した、バランスを整えた設計が必要になります。

Point② バックアップから復旧する

バックアップは、もしもの時に復旧できなければ意味がありません。バックアップしたものから復旧できることが重要になります。もしもの時に復旧手順がわからないということがないようにする必要があります。
復旧手順の確認は手順書の確認だけでなく、実際に復旧トレーニングまでできると確実です。セキュリティ担当としてのトレーニングに加え、万が一の時に備えておくことが重要です。



Day7
2.インフラセキュリティ

ログの取得と説明責任

攻撃にいち早く気づき、被害状況や影響範囲の調査などの事後対応を効果的に行うためには、ログの取得と保管が重要になります。情報システム内で何が起こっていたかを後から追跡調査を行い、事故の原因究明や、対策を導き出すことにつながります。

Point① ログを取得する

ログの具体的な例としては次のものが挙げられます。

通信ログ	取得ポイント	ログの種類
ファイアウォールを通過または拒否された通信ログ	ファイアウォール	通信
IDSやIPSが監視した通信のログ	IDS・IPS	通信
DHCPサーバがパソコンにIPアドレスを割り当てたログ	DHCPサーバ	システム
ファイルサーバへのアクセスのログ	ファイルサーバ	アクセス
ファイルの参照や、編集などの成功や失敗のログ	ファイルサーバ	システム
情報システムへのログイン、ログアウトなど認証のログ	情報システム	システム
Webサーバへのアクセスのログ	Webサーバ	アクセス
Webプロキシサーバが中継した通信のログ	Webプロキシサーバ	通信
パソコンの監査のログ	パソコン	システム

ログには、誰と誰がいつどのような内容の通信を行ったか、という情報が記録されています。また、企業秘密に関する情報や、電子メールの内容、利用者が入力した個人情報などがそのまま含まれている場合もあります。ログは機密情報であるということを理解し、取り扱いには十分な注意が必要です。

出典：総務省
「ログの適切な取得と保管」をもとに作成
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/business/business_admin_22.html

ログ保存期間に注意

ログ保存期間が短いと調査可能期間も短くなります。数ヶ月程度は保存されている状態にしましょう。

ログの保存先に注意

ログは取得機器ではなく、別サーバに保存することで、対象機器に不正アクセスがあった際に、証拠隠滅をされる可能性が下がります。

ログの操作に注意

ログの消去等が誰でもできてしまうと、不正アクセスの際に証拠が隠滅されてしまう可能性があります。アカウント権限に注意しましょう。

Point② 説明責任を果たす

説明責任とは、「担当や権限を持つことに対して、詳細な説明を行うこと」です。セキュリティ担当者の場合は経営層に自社のセキュリティ状態を説明するようなケースが想定されます。また、セキュリティ責任者の場合には、セキュリティ事故発生時など、経緯や被害内容・再発防止対策などを顧客や関係者に知らせる説明責任があります。

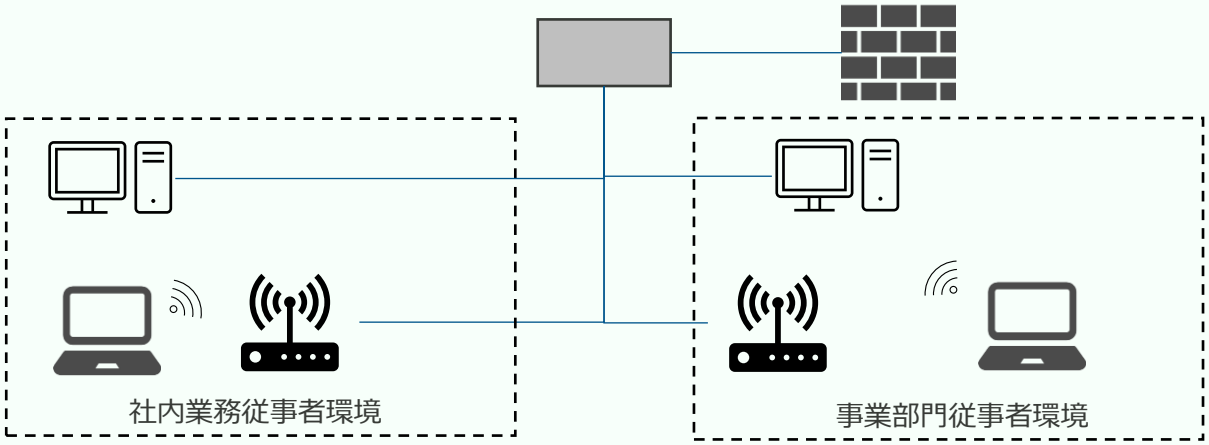
正しく説明責任を果たすためには普段からログを取得し、システムの記録を残しておく必要があります。経緯を把握するためには、どこからウイルスが侵入したのか？（メールの記録やFWの通信ログなど）、ウイルス実行によりシステム上でどのような動作があったのか？（パソコンのシステムログなど）、どのデータにアクセスされたのか？（データのアクセス操作ログなど）といったことを知る必要があります。それぞれの記録としてログを取っておくことで、セキュリティ事故などの時に報告書に正しく記載でき、関係者が納得する説明をすることができます。

Day7

3.技術的対策の先進事項

システムの役割に応じた技術的な対策

DXが進む中で、セキュリティは社内に限定するものではなくなりました。事業部門がサービス提供用のシステムを持つことも多くなり、事業システムと社内システム双方のセキュリティを考える必要性が出ています。

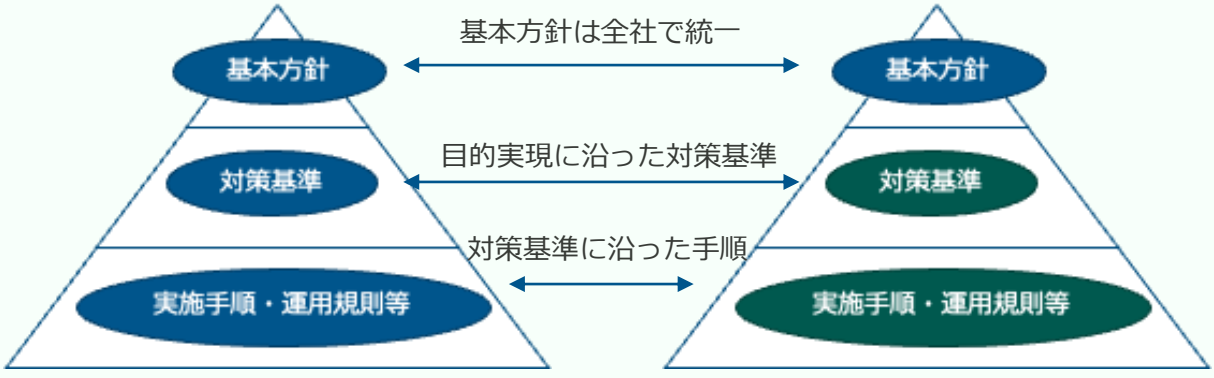


主に人事や総務、経理といったバックオフィス部門が利用する環境。社内のセキュリティ規程やルールが適用される。

主にお客様へサービスを提供するための環境。社内の規程を適用するが、サービス提供にあたって社内規程では不都合が出やすい。

社内業務環境に適用されている社内規程の例	社内規程を事業部門環境に適用した場合に発生する問題点の例
社内からのリモートアクセスを行う通信の禁止	サービス適用のためのサーバをメンテナンスするためにリモートアクセスを許可する必要がある
許可のないクラウド利用の禁止	お客様とのやり取りにおいて、お客様の都合に合わせたクラウドでのファイルのやり取りをする必要がある
許可のないソフトウェアの利用の禁止	開発をするために、ソフトウェアやアプリケーションをインストールする必要がある

事業部門のDX化が進んでいくと、社内規程を事業部門環境に適用していくことが難しくなるケースがあります。この場合、事業部門環境に即した規程を定め運用していくことが必要です。



Day7

3.技術的対策の先進事項

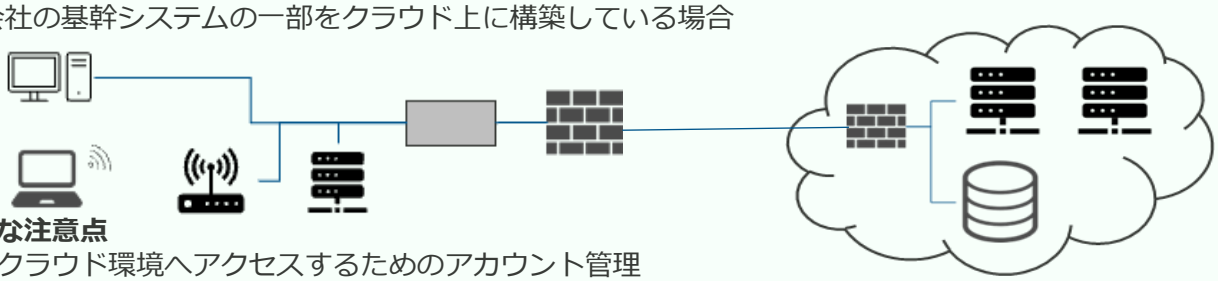
クラウドサービス利用時のセキュリティ対策

近年はクラウドを中心とした社内インフラの構築やサービスの利用が増えています。今までの社内を前提としたセキュリティ対策から変化が必要です。

Point① クラウドの特性に合わせて対策を行う

クラウドサービスの利用といっても大きく２つのパターンに分かれます。それぞれの特性を意識して、対策を検討しましょう。

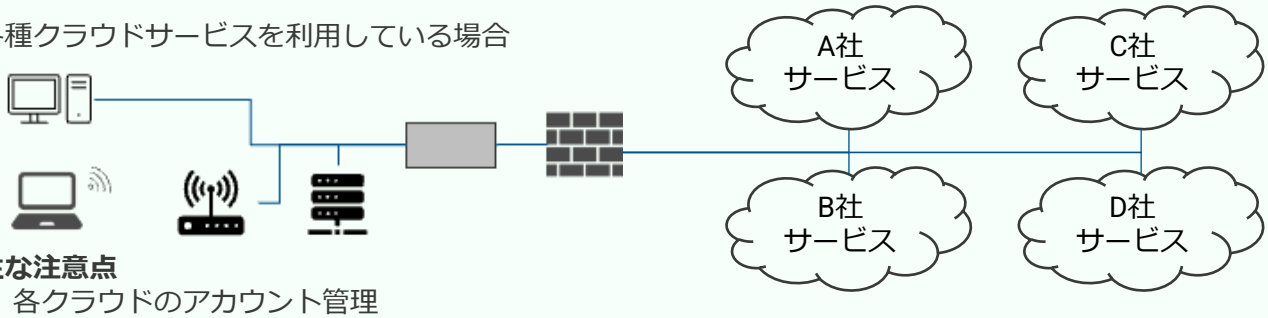
◆会社の基幹システムの一部をクラウド上に構築している場合



主な注意点

・クラウド環境へアクセスするためのアカウント管理
・構築したサーバやシステムの管理・OSやアプリケーションの脆弱性の管理
・公開範囲などの設定管理・保守業者の管理

◆各種クラウドサービスを利用している場合

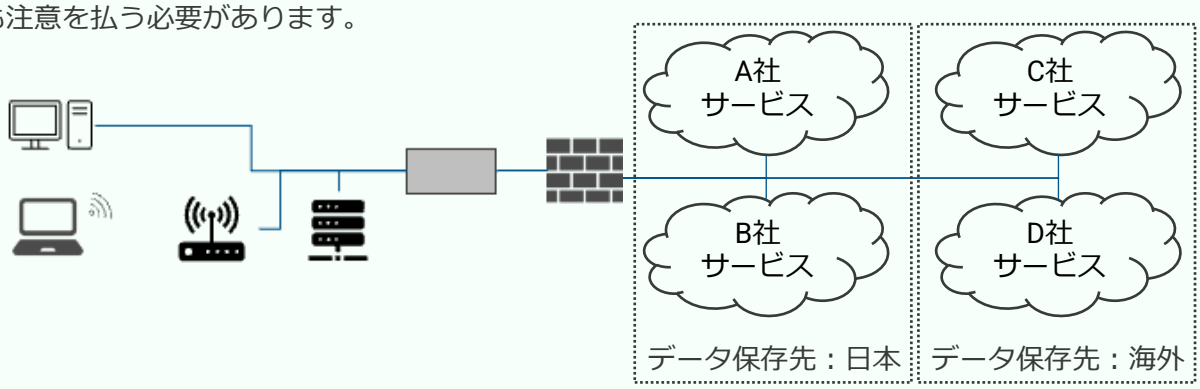


主な注意点

- 各クラウドのアカウント管理
- クラウドサービス事業者の委託管理

Point② データの保存先を確認する

主にSaaS型のクラウドサービスを利用している場合には、データがどこに保存されるかについても注意を払う必要があります。

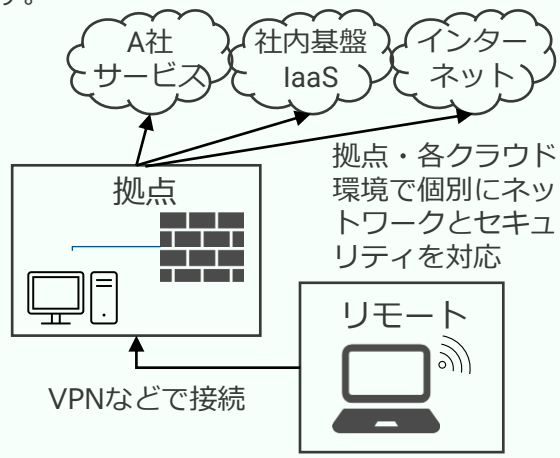


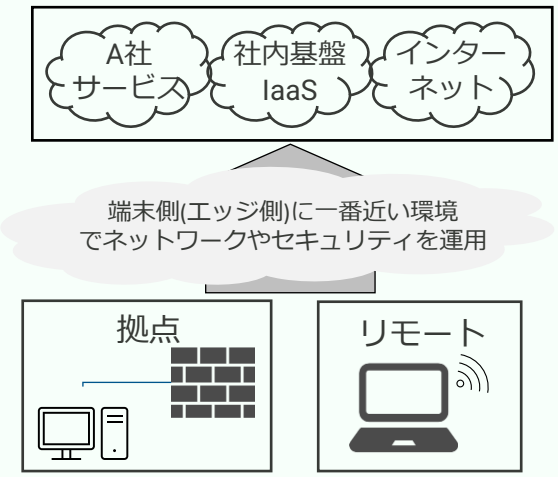
クラウドサービスを提供する事業者の中には、海外にデータセンターを保有している場合があります。この場合、設置先の国の法制度が適用されることになり、予期せぬトラブルに発展する可能性があります。また、業務従事者のセキュリティ意識なども変わる可能性があるため、国内のみで利用するような場合には、国内にデータセンターがある事業者を選ぶと安心です。

クラウドサービス利用時のセキュリティ対策

Point③ 包括的に一元管理し運用の最適化を

拠点環境とクラウド環境は併用され、働く場所は多様化しています。自社集約して処理するのではなく、端末側(エッジ側)に一番近い環境でネットワークやセキュリティを処理するという考え方が提唱されています。





端末側(エッジ側)に一番近い環境でネットワークやセキュリティを運用することで、従来個別に対応していたものが一元的に管理されます。そのため、運用負荷が減る効果が期待できます。

機能が包括的に提供され一元管理しやすい	通信遅延の低減	セキュリティルールの維持
ネットワークやセキュリティの機能が端末側(エッジ側)に一番近い環境に集約されます。拠点や各システムでネットワークやセキュリティの管理が軽減されます。	ネットワーク遅延などが発生しないようにネットワーク管理を行う必要がある中、端末側(エッジ側)に一番近い環境の中で最適な帯域や通信経路を確保できます。	それぞれの環境でセキュリティルールを導入する必要性がないため、統一されたセキュリティルールが適用され、セキュリティの維持向上の効果が期待できます。

機能	特徴
セキュリティ制御を行うための代表的な機能とその特徴	
SWG （Secure Web Gateway）	URLフィルタやアプリケーションフィルタ、アンチウイルス、サンドボックスなどの機能を提供するサービス。
CASB （Cloud Access Security Broker）	各種クラウドサービスへの通信の可視化、データ流出等の阻止、監視や制御、送受信するデータの暗号化を実現する。
ZTNA （Zero Trust Network Access）	すべてのアクセスや通信を脅威とみなす考えのもと、ユーザーの端末やアイデンティティ管理を行い、アクセスの許可を行う。
FWaaS （Firewall as a Service）	ファイアウォールの機能を提供するクラウド型のサービス。
ネットワーク制御を行うための代表的な機能とその特徴	
SD-WAN （Software Defined Wide Area Network）	拠点や社外のネットワークを最適化し場所を問わず快適な通信を実現する。

Day7

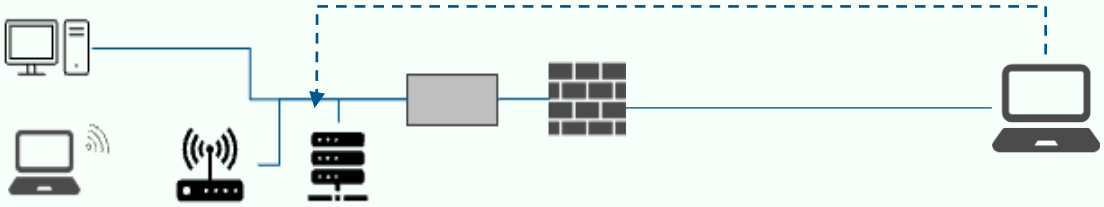
3.技術的対策の先進事項

リモートワーク時のセキュリティ対策

リモートワークを実施する場合、リモートワークの規程作り、リモートワークを行うための環境作りが必要です。本ページでは、リモートワークを行うために必要な環境について説明を行います。

Point①
アクセス制限や端末の管理を強化する

リモートワークでは、社外に端末や情報資産が持ち出されることを前提にしたセキュリティ強化が求められます。そのため、管理方法をより強化した運用が必要です。

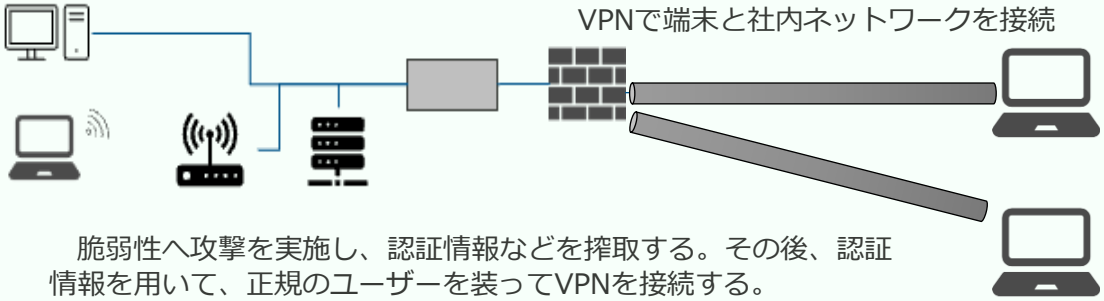


アクセス制限のポイント	主な認証ポイント
パソコン	パソコンへのログイン時
ファイアウォール	VPNなどの利用時
ファイルサーバ	サーバアクセス時
データ	データアクセス時

One point

VPNとは、送信側と受信側がそれぞれ通信の処理を行うことで、第３者には通信が見えない仮想的なトンネルを形成して通信する仕組みです。この技術により、社外にいながらも、あたかも社内にいるかのように業務をすることができます。

しかし、VPNでも脆弱性が報告されており、適切に対処しないと、VPNのIDやパスワードが流出し、第３者が不正にVPN接続をしてしまうという危険性が報告されています。もし、VPNのIDやパスワードが流出した場合、社内へのアクセスが可能となり、社内に保管されている資産が漏えいするなどの危険性があります。



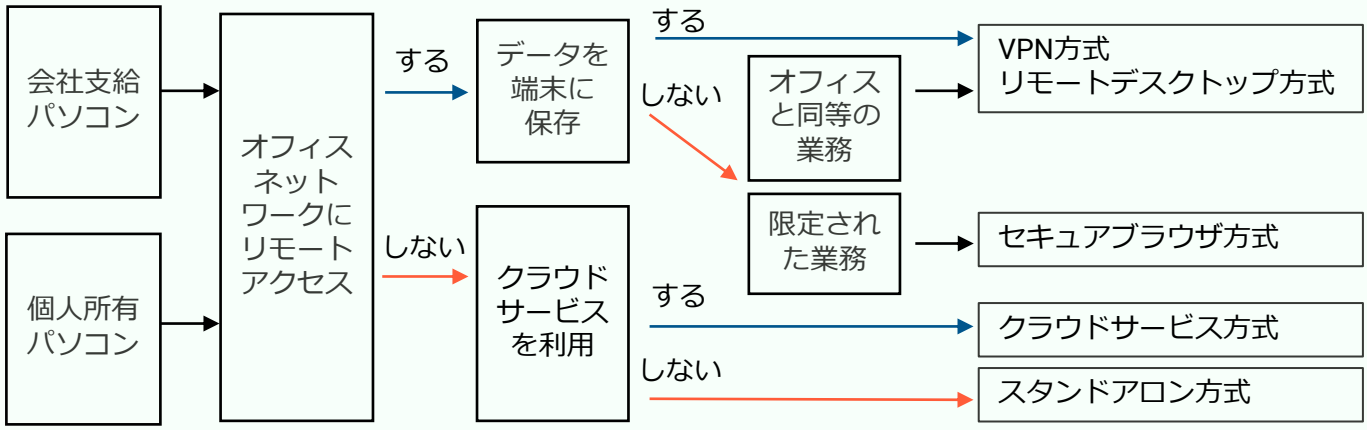
脆弱性へ攻撃を実施し、認証情報などを搾取する。その後、認証情報を用いて、正規のユーザーを装ってVPNを接続する。

リモートワーク時のセキュリティ対策

Point② リモートワークセキュリティの状態を確認する

リモートワーク時に気をつけるべきセキュリティは多岐にわたります。また、リモートワークをどのような方法で実現するかにより、各社気をつけるセキュリティのポイントが異なる点にも注意が必要です。利用している方式を把握し、セキュリティ対策を実施しましょう。チェックリストは、中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）を確認しましょう。

該当するテレワーク方式の確認



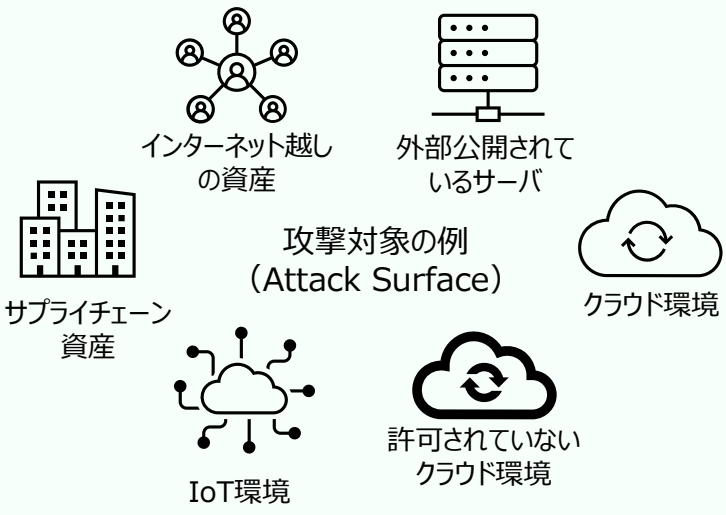
出典：総務省
「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）」をもとに作成
https://www.soumu.go.jp/main_content/000816096.pdf

Point③ 攻撃の可能性がある範囲を明確にする

リモートワークを行う場合には、クラウドの利用やパソコン・資産の持ち出しなどが発生します。また、認識されていないサーバやクラウドなどが利用されているケースも考えられ、脆弱性や意図せず空いているポートを狙った攻撃の可能性を明確にすることの重要性は一層高まっています。

Attack Surfaceは、攻撃対象領域と言われるもので、攻撃を受けうる可能性（脆弱性を含む）があるネットワークやサーバ、クラウド、ホスト、システムなどを指します。 Attack Surfaceを把握し、それらに対処していく取り組みのことをAttack Surface Management（ASM）と呼びます。

近年では、インターネットに面した脆弱なシステム自体が攻撃対象となることも多くなっています。攻撃対象領域を把握し、攻撃に利用されないように対処をしていくことで、クラウドの利用をはじめリモートワークをより安全に実施することが可能となります。



要件定義からセキュリティ担当が関わる事例

セキュリティと運用はバランス良く。セキュリティはより上流から考える。

事業運営をしていると、既存のシステムではなかなか実現が難しいという事があります。その場合、自社専用のシステムやアプリケーションを構築します。現在では、クラウド上に開発を行うことも珍しくありません。

基幹システムのリプレースを行った2つの会社の事例を紹介します。両社とも、構築を担当する会社と何度もミーティングを重ね、必要な機能や付随機能について検討をしてきました。

A社
セキュリティ担当が開発の企画の段階から積極的に関わりシステム開発を進めました。システムを利用する部門から、開発への参加はありませんでした。

機能要件	顧客管理
	顧客情報更新・修正
	顧客へのメール送信
	検索機能
非機能要件	認証機能
	稼働率99.9%以上
	ログ取得
	タイムアウト機能

B社
セキュリティ担当は積極的には関わらず、システムを利用する部門の担当者を中心に進めていきました。

機能要件	顧客管理
	顧客情報更新・修正
	顧客へのメール送信
	検索機能
非機能要件	レスポンスタイム
	稼働率99.9%以上
	画面操作性
	視認性

A社ではセキュリティ担当が積極的に関わったため、セキュリティ機能が充実したシステムになりました。対してB社では、担当部門が中心となったため、利用者が利用しやすいシステムになりました。どちらの会社も特徴はあるものの業務をする上で必要な機能を持ったシステムを開発する事ができました。しかし、どちらの会社もシステムを使っていくと問題も出てきました。

A社の問題点
画面が見づらく、操作がしづらい
A社が実施した改善策
一部システムの改修を実施

B社の問題点
情報漏えいリスクが高い
B社が実施した改善策
セキュリティ機能の充実化 運用におけるセキュリティ対策の実施

それぞれの会社で良い点悪い点がありました。この２つの会社はどうすればよかったのでしょうか？今回の２社の事例から、システム開発ではセキュリティ担当と利用者の両者がしっかりと意見交換しながら進めていく事が望ましいという事がわかります。最近では、セキュリティバイデザインという考え方があり、企画・設計のフェーズからセキュリティ対策を組み込んでいく事が良いとされています。また、セキュリティ担当としては、企画の段階から積極的な関わりをしていくとともに、ユーザーの声を聞くことが大切です。しかし、守る所はセキュリティを優先するという強い意志も重要になってきます。何を守るのか、どうやって守るのかを意識し対応をしていきましょう。

Day7
3.技術的対策の先進事項

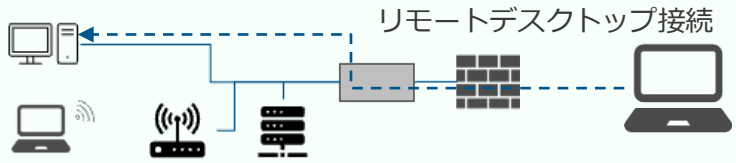
変化に対応する技術的対策の事例

在宅ワークの環境を整える。

働き方改革という言葉をよく聞くようになりました。業務時間の短縮や生産性の向上など多くの視点で語られていると感じます。特に、コロナの影響により、急ピッチでテレワークのシステムを整えたという会社も多いのではないでしょうか？
ある会社では、コロナの流行がきっかけとなり、本格的な在宅業務へと舵を切りました。最初は在宅ワークをするだけで精一杯でしたが、数年来の改善で業務効率も出社している時と遜色無くなっています。

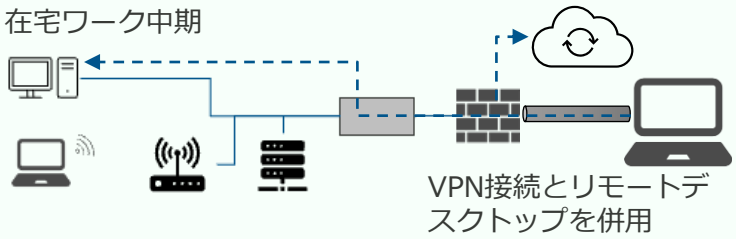
在宅ワークの環境変化（概要図）

在宅ワーク初期



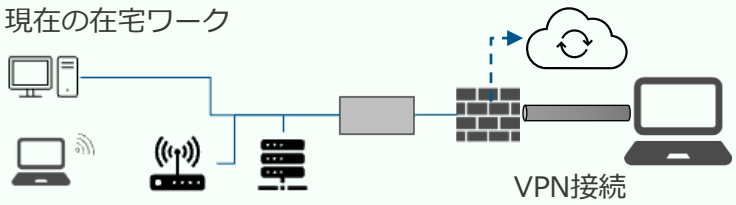
社内のパソコンにリモートデスクトップをする事で作業をしていました。業務はできていましたが、社内接続するための端末が直接インターネット接続できたため、情報漏えいのリスクがありました。

在宅ワーク中期



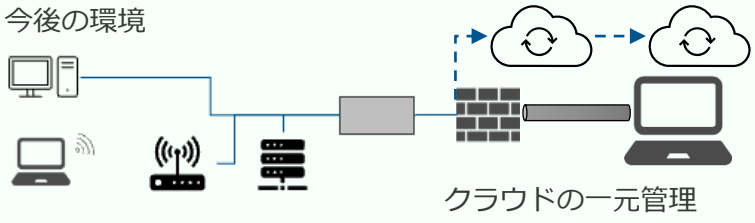
社内へのアクセスにVPNを利用し、通信の安全性を高めました。またクラウドサービスへは社内からアクセスすることでファイル共有やコミュニケーションを管理しやすくしました。ただし、クラウドへのアクセスが技術的には個人端末からできてしまうことや、シャドーITの可能性を無くすことはできませんでした。

現在の在宅ワーク



リモートデスクトップ方式を廃止して、PCがインターネットに繋がったら自動でVPN接続を要求し、インターネットへの接続を制限しました。クラウドへもアクセス制限をかけ、個人端末の利用禁止も技術的に行えるようになりました。

今後の環境



今後は、増大したクラウドサービスの一元管理を目指した、SASEなどのサービス導入を検討しています。利便性とセキュリティの両方を高めていく予定です。

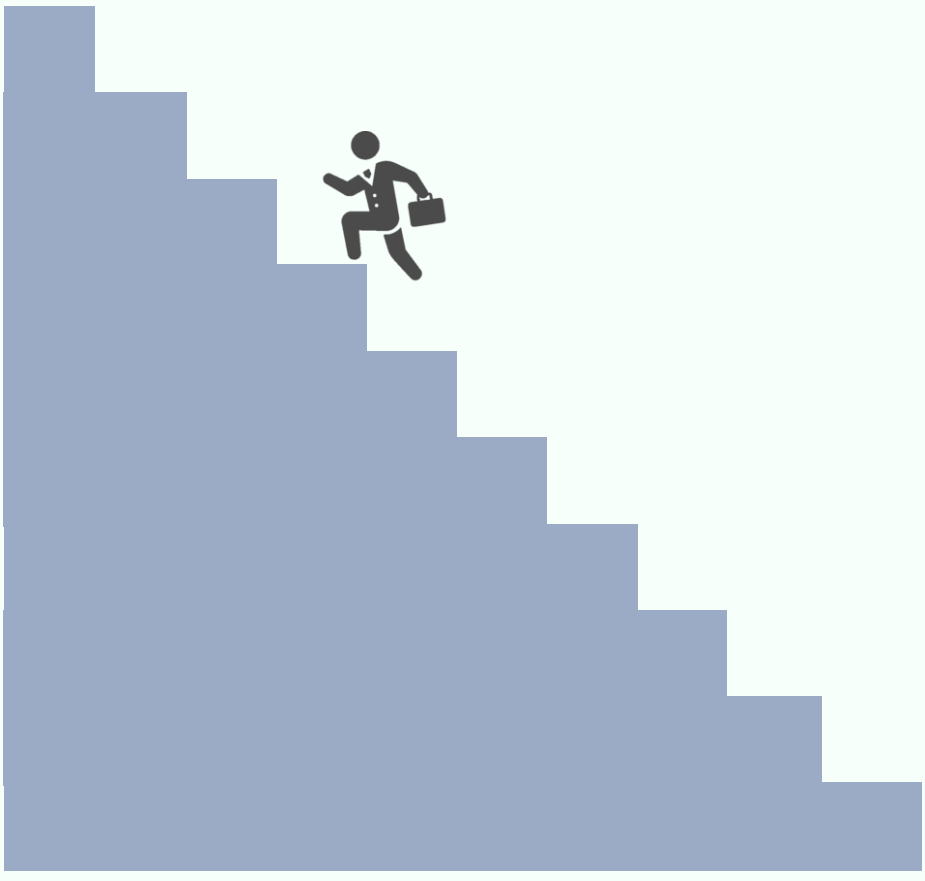
在宅ワークの環境を最初から理想の形とすることはなかなか難しいものです。しかし、生産性を高め、働き方に選択肢を持たせるためには必要なことです。日々変わるデジタル環境において、それらを実現するためにセキュリティを考えることが大切であり、決して否定するためのセキュリティにならないように意識することが重要です。

技術的な対策について学んできた。セキュリティ担当として技術の理解は必要不可欠だと感じた。現状は自分で機器を設定することはないけれども、緊急対応などが必要になったら、機器操作などをするケースもあるかもしれない。

今までは保守会社に任せきりだったけれど、本来ならば自分たちで決めるべきところが決められていないケースもあるのではないか？要件定義において、要件を詰めるようなことも明確にはしてこなかった。そういえば、自分の会社のネットワークはどのような構成になっているのだろう・・・？全て自社で用意する必要性はないだろうが、外部を使う基準や自分達のやりたいことなどを自分達で伝えられないといけない。

まずはネットワーク構成図を最新のものに更新していこう。現状の機器を最大限に使いこなしながら、セキュリティ強化を目指していくのもいいだろう。足りない機能などについては新しい機器の導入なども必要かもしれないが、その際には要件をしっかり詰めて導入をしよう。自分の会社のことなのだから、自分たちで現状を把握し、見直していくことが重要だ。

技術的対策を使いこなす



コラム
～時代と共に変化する認証～

現在多くのシステムで認証の仕組みを導入しています。認証の中でスタンダードとなっているものがパスワードです。しかし、最近ではパスワードでの認証も限界を迎えています。そのため、多要素認証が広く利用されるようになりました。多要素認証と言ってもその方法は多岐にわたります。

パスワードを入力した後にSMSで毎回ワンタイムパスワードが送られてくるシステムもあれば、端末を登録しておけばワンタイムパスワードが不要なシステムもあります。また、パスワードではなく、パスフレーズというものも存在します。単語を複数組み合わせ、フレーズにして文字数を多くすることで、セキュリティを強化するものです。

知識属性以外でも生体認証もスマートフォンを中心に利用が広がっています。利用するシステムの重要性に基づいて、どのような認証をしていくか検討することは、セキュリティ担当の大切な仕事と言えます。

最近、普段と違う所からのログイン時にだけワンタイムパスワードを求められるといったことはありませんか？システムのアクセスログなどを分析し、ユーザーの行動パターンやアクセス端末など普段と違う場合に追加の認証を求めるものです。普段と違う場合のみ追加認証が必要なので、認証の手間を軽減することにつながります。認証が強化されると、覚えるパスワードが増えたり、一手間増える煩わしさを感じるかもしれません。利用者の負担軽減も意識しながら認証の仕組みは考えられています。

あとがき

現在主流となっているクラウドもここ10年程度で出現した技術です。ITやデジタルを取り巻く環境はこの10年程度で大きく変わりました。小学生の時、Windows95が学校に導入された1990年代当時から20数年が経ち、今ではプログラミングが授業で行われる時代となりました。それに合わせてインターネットを使った犯罪や事故も増え、セキュリティの必要性も高まっています。非常に大きな変化の中で技術的な対策を進めて行くことは、学び続ける姿勢や、学び直しといった日々の学習も重要になります。

今後も新しい技術が登場し、新しいリスクが登場してくることはほぼ間違いないのではないでしょうか？その中で新しいセキュリティ対策の方法も登場し、対策をとって行く必要があります。技術的な対策を使いこなしながらセキュリティ強化に取り組んでいけるように、活動をしていきましょう。

令和4年度

中小企業サイバーセキュリティ対策継続支援事業

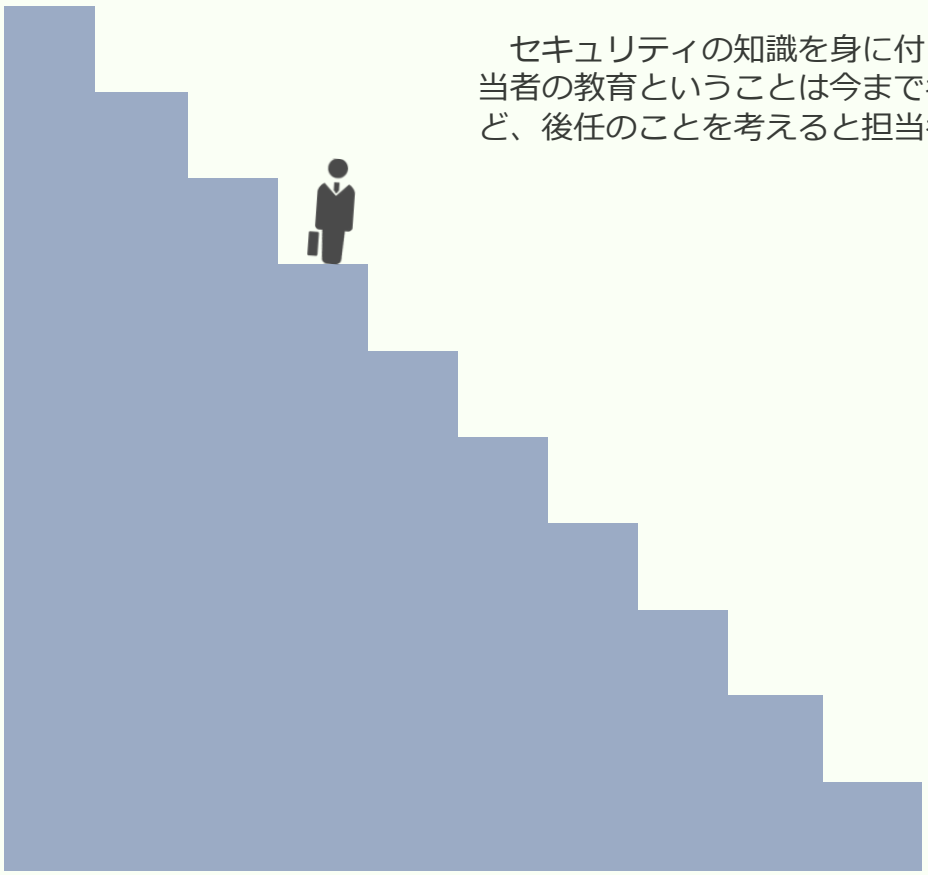
第８回

セミナー開催日：令和4年12月6日

組織の成熟度を上げる
ルール作りを

技術的な対策をしっかりしていく必要性は分かった。とはいえ、最終的には人へのセキュリティ対策をしっかりとしていかないといけない。そのためには、セキュリティ規程に代表されるようなルールを整備するべきだ。

ルールはあるけれども・・・いつ作ったんだっけ？というものもある。現在の状態と合わないことは間違いないだろう。守るべきルールがそもそも正しくないのであれば、正しく守られるわけがない・・・ルールを見直して、正しい教育をしていくことで、組織の成熟度を上げていかないといけない。そもそも自分たち担当者もしっかりと成長していかないと組織も成長していかない。



セキュリティの知識を身に付けることも重要だ。担当者の教育ということは今まで考えていなかったけれど、後任のことを考えると担当者教育も考えていこう。

Day8

1.組織・人の対応を強化する

セキュリティ規程
ルールの見直し

セキュリティ規程が作成された次の対応として、ルールの見直しをしていく必要があります。特に、デジタル化の対応が進む今日において、変化スピードが上がっており、ルールの見直しが後手に回らないようにしましょう。

Point① 現状のルールと現在の業務状況の差分を確認

すでにある規程を見直す際には規程の文言だけを見るのではなく、デジタル化の実態や現状業務との矛盾についても検討をする必要があります。

規程修正の例		
規程の文面	現状	修正案
社外のファイルストレージを利用してはならない	クラウド環境の利用を推奨している	会社が定めたクラウド環境、ファイルストレージ以外を利用してはならない
ファイルをEメール添付する際は、パスワード付きZipを利用する	クラウドを利用したファイル共有を行う	ファイルを外部と共有する際は、会社が定めたファイル共有ツールを利用する
在職中に得た情報を退職時に持ち出してはならない	業務利用で個人所有端末を利用している	在職中に得た情報は退職時に返却および削除を行い、機密保持契約書を取り交わす

まずは、規程の文面と現状の業務について差分や矛盾があるところを洗い出してみましょう。また、業務の変化において規程の中で定義されていないというケースもあります。これらも洗い出して追加をしていきましょう。また、不要なものは削除するという対応も必要です。

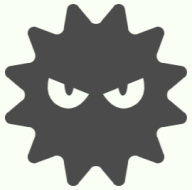
また、規程に矛盾がでるとそれ自体が脆弱性となります。内部不正の要因となる機会となるため、注意が必要です。

Point② 新たな脅威の出現や従業員からの要望で見直しも重要

規程の運用を開始した後にも、社員や職員の要求や社会状況の変化、新たな脅威の発生などに応じて、定期的な見直しが必要です。定期的な見直しのためには、情報収集を行うことが必要です。さらに、従業員がルールを守っているかの情報収集をし、見直しに活かしていきます。

社会状況の変化

法改正やセキュリティの認識が改められた時などに見直しを行います。



新たな攻撃手法の出現

パスワードの解析性能の向上や攻撃手法の確立により見直しを行います。

社員・職員の要望

生産性の観点や働き方の観点から従業員の要望を取り入れ見直しを行います。

出典：総務省
「国民のためのサイバーセキュリティサイト」をもとに作成
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/business/business_executive_04-6.html

Day8

1.組織・人の対応を強化する

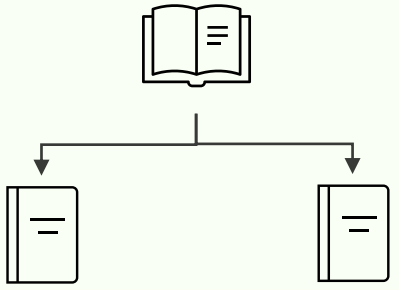
セキュリティ規程
ルールの作成・更新

セキュリティの規程は誰が守るべきルールなのかはっきりすると、わかりやすくなります。自分に関係ないと思っていた規程の一部分にだけ遵守するルールがあると見落としにつながり、ひいては事故につながる可能性があります。

Point① 規程を分割して対象者を明確にする

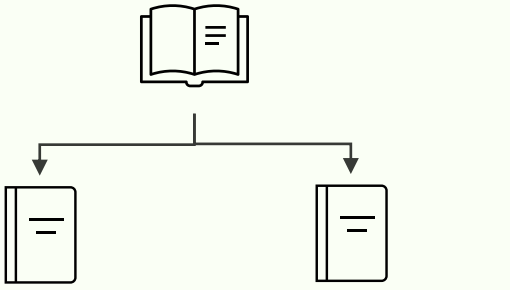
一つの規程に多くの対象者が存在すると、どの文章に対して守ればいいのか理解しづらいです。対象者ごとに規程を分けるという選択肢もあります。

①対象者ごとに分ける



対象者ごとに規程を分けることが可能です。この場合、読み手は自分に関係する点だけの理解に集中することができます。

②環境ごとに分ける



環境で分けることも可能です。環境によりセキュリティルールを変えなければならない場合などに有効です。

Point② 必要な規程を作成する

セキュリティ規程を作成しても、これが足りないといったことは起こり得ます。必要な規程を網羅して、足りないものは作成していくことが重要です。

規程の例		
規程名	概要	主な対象者
インシデント対応規程	インシデント時の手順や方針をまとめた規程	インシデント対応責任者 情報システム関係者
システム管理規程	システムの管理・更新についてまとめた規程	システム管理者、責任者 情報システム関係者
外部委託先管理規程	外部委託先に対しての管理方法や確認方法をまとめた規程	委託先管理者
監査規程	監査に伴う規程。内部監査を含んで記載する場合もあり	監査担当者

ただし、文書の数が多くなると文書管理の手間が増え、文書をまとめると一つの文書当たりの分量が増えて読みづらいということが発生します。自社にとってどちらが有益なやり方かを検討する必要があります。

Day8

1.組織・人の対応を強化する

セキュリティ強化に向けた体制作り

セキュリティを担当者自身の力で進めることは困難です。第1回のセミナーで紹介した通り、関係者を巻き込み、役割を明確にしていくことが重要です。

Point① 役割と責任

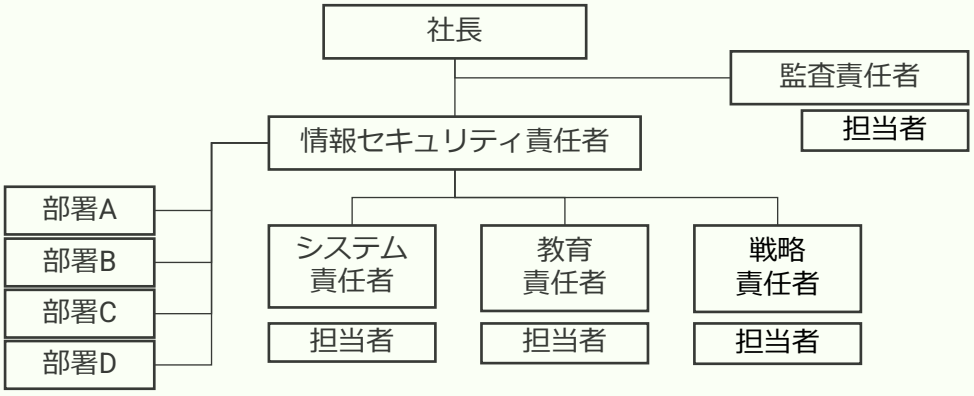
情報セキュリティ組織体制で大切なことは形式ではなく、誰が「責任者」なのかを明確にして運用することです。以下の例だけでなく、各組織に合わせて責任者・担当者を任命することも必要です。

役割と責任の例	
役割	主な活動
情報セキュリティ責任者	• 社内の情報セキュリティを統括する。 • セキュリティの推進、体制の構築（リソースの手配、予算の確保）をする。 • ビジネスの視点でセキュリティ対策や事故発生時の影響を検討する。 • 組織の方針や規程について承認をする。または、承認者へ権限譲渡をする。
戦略責任者・担当	• 自社の事業計画に合わせたセキュリティ戦略を策定する。 • リスク分析や資産管理を通してセキュリティ対応策を考え、実行し、評価する。 • セキュリティ上の課題を発見し対処する。
教育責任者・担当	• 教育計画や目標・スケジュールを策定する。 • 研修テキスト・教材・テストの選定を行う。 • 講師として従業員への教育を行う。
監査責任者・担当	• 社内の情報セキュリティマネジメントや各種対策が効果的に実行できているかを監査する。 • できていない場合には指摘をし、是正措置のヒントを与える。
システム責任者・担当	• セキュリティ機器類の導入計画や設計を行う。 • 現在導入されている機器の有効性の評価を行う。 • システム周りの保守や監視を行う。

Point② 情報セキュリティ組織

少人数組織の場合、経営者が情報セキュリティ責任者を兼ねる場合もあります。 また、防犯や防火などの安全管理責任者が兼ねるという方法もあります。

組織が100名を超える規模の場合には、決めた方針のとおりに情報セキュリティの取り組みが行われているかを確認するため、監査責任者を立てます。監査を外部の専門家に依頼することもできます。また、これらに合わせて、個人情報保護責任者やインシデント対応責任者などを配置する組織もあります。



ミニワーク
～考えてみよう～

ミニワークテーマ

自社が目指すべき人員体制・組織体制はありますか？
まだ、目指すべき人員体制・組織体制がない場合、担当者として、どのような人員体制・組織体制を目指したいですか？

Day8

1.組織・人の対応を強化する

セキュリティ関連規程と指針・指標・マニュアル

規程や指針・指標・マニュアルについての違いを理解することで、必要な資料は何かを確認することができます。また不足している資料を作成する際は、資料の目的を明確にした上で作成することが重要です。

セキュリティ関連規程	指針・指標	マニュアル（手順書）
決まりやルールのことです。やるべきこと、やってはいけないことが明確に記載されています。	指針・指標のことです。目指すべきゴールが示され、ゴールにたどり着くまでの流れや方向性、遵守すべき項目について記載されています。	物事を確実に実施するために参照するものです。マニュアル通りに実施することで、その従業員の経験に関係なく基本的に同じ結果を得ることができます。

Point① 作成の目的を明確にし提示する

■規程
会社の裁量で決められる会社内のルール全般を提示します。

■指針・指標
テーマに対して今後どうしていけば良いのか、というような未来の方向性や見通し、事象に対する対応方針等を提示します。

■マニュアル
事象に対して行うべき具体的な方策や手順、過去の事例を提示します。

Point② 内容の具体性

■規程
ルールを明示し、ルールを守らなかった場合の罰則などについて提示します。

■指針・指標
ゴールまでの大まかな流れや行動範囲など、抽象的な内容を記載し、読み手に「どう行動すべきか」を考えさせます。

■マニュアル
「誰が・いつ・どこで・何を・なぜ・どのように」といった5W1Hで指図するような具体的な内容を記載し、読み手を問わず誰でも同じ行動がとれるよう記載します。

Point③ 読み終わった後の行動

■規程
読了後の理想は「守るべきルールを把握している状態」です。ルールの記載のため、具体的な方法や行動は読み手が考えることになり、読み手によって、行動が変わる場合があります。

■指針・指標
読了後の理想は「守るべき規程・ルールを守っている状態」です。ただし、記載されるのはあくまでも大まかな流れや行動範囲となるため、具体的な方法は読み手が考えることになり、読み手によって、行動が変わる場合があります。

■マニュアル
読了後の理想は「指示した通りに行動している状態」です。そのため、行動後に得られる結果は読み手が誰であってもほぼ同じものとなります。また、記録をして次のアクションに活かせるようにすることも求められます。

Day8

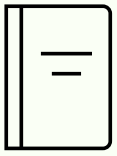
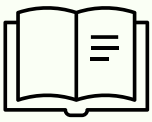
1.組織・人の対応を強化する

規程の理解度アップに向けて

規程は作成して終わりではありません。従業員の方や対象者として定められた方が正しく理解し、行動する必要があります。

Point① セキュリティ関連規程と指針・指標・マニュアルを使い分ける

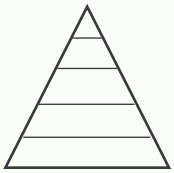
規程は文章で書かれていることが多く、読み手にとって読みやすいものとは言いづらいものです。さらに、セキュリティ意識なども読み手の理解度に影響します。規程・指針・指標・マニュアルの特性や従業員の理解度を考慮する必要があります。

セキュリティ関連規程	指針・指標	マニュアル（手順書）
		
作成・更新された事を周知し、保存場所を明確にする。勉強会などで読み合わせを行う。	変更された規程をより理解するために勉強会などのテキストとして利用する。	常に目の届くところ、すぐ読めるところにおいておき、不明点等があれば参考にして行動する。

Point② 文書の識別と管理

組織が必要と判断する文書化した情報を識別し、適切に管理することが重要です。文書には階層が存在し、適した管理方法、承認方法が求められます。

文章の階層化



1次文書：文書体系の最高位に位置づけられる文書：情報セキュリティ方針
2次文書：会社のルールなどを定めた規程等の文書：規程等
3次文書：具体的な作業の手順などを表した文書：マニュアル等
4次文書：計画書や管理台帳などの文書：計画書や管理台帳等
5次文書：記録を記載した文書：入退館記録等

階層	作成	審査	承認
1次文書	担当部門(情報セキュリティ組織・チームなど)	文書管理責任者	経営層
2次文書	担当部門(情報セキュリティ組織・チームなど)	文書管理責任者	経営層 情報セキュリティ責任者
3次文書	各部門	主幹部門長	文書管理責任者
4次文書	上位文書の定めに従う		
5次文書			

なお、それぞれの文書には、タイトル・作成日・更新日・作成者・承認者・文書番号・様式番号などを入れ識別します。また、表紙に入れるだけではなく、ヘッダー情報として入れると文書内すべてに記載がされます。

Day8

1.組織・人の対応を強化する

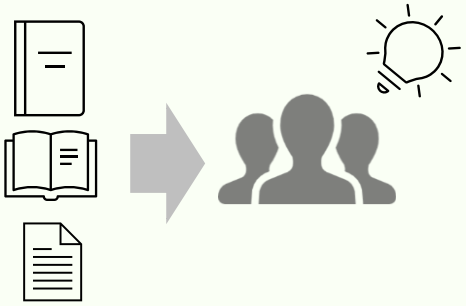
情報セキュリティの意識向上、教育及び訓練

組織のセキュリティを向上させ、人の脆弱性を無くしていくための対策が教育です。情報セキュリティ教育の責任者や教育担当者（教育の実施者）を定め責任を明確にしつつ、従業員の理解度を上げていくことが重要です。

Point① なぜ教育を行うのか？

情報セキュリティ教育の目的のひとつに、情報セキュリティ基本方針や情報セキュリティ規程を周知し、理解してもらうことがあります。特に、入社時などは理解ができていないため、しっかりと教育を行うことが重要です。

情報セキュリティ対策を適切に実践するためには、情報セキュリティ規程に書かれている内容を理解するとともに、何のために情報セキュリティ対策が必要かという理解がないと、セキュリティ対策に対するモチベーションが高まりません。そこで、情報セキュリティ対策における脅威と対策についても併せて教育します。

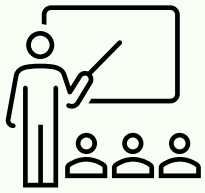


規程・指針・指標・マニュアルを理解し行動できるようにする

Point② 教育方法を選択し理解を深める

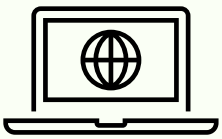
教育の提供はいろいろな方法が選択できます。目的や勤務状況や形態、学ぶべき内容などにより使い分けていきましょう。

集合学習



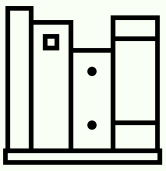
従業員が集まって教育を受ける形態です。全員が同じ内容を受講するため、内容の齟齬が出づらく、一体感を高め、意識を向上しやすくなります。

E-learning



現在のリモートワークなどに対応した形態です。個人のペースで進めながらも、受講進捗を把握したり、実施状況がわかりやすいという効果もあります。

個人学習



規程を読む、資料を読むなどの形態です。一体感が出ず、個人のもともとの意識により理解度が影響されます。自由な時間でできるため、意識がある人にとっては有益です。

毎回同じ教育方法では飽きてしまう場合もあります。受講者が興味を引き、積極的な受講となるような仕掛けをしていくことも重要です。

Day8

1.組織・人の対応を強化する

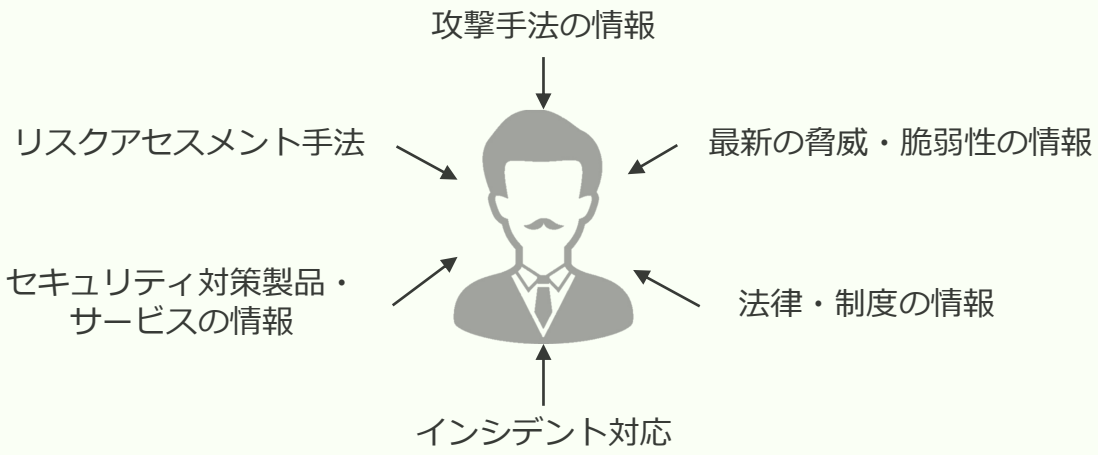
情報セキュリティの意識向上、教育及び訓練

情報セキュリティの意識を向上させ、教育及び訓練の対象となるのは、従業員だけではありません。セキュリティ担当者や各責任者こそ積極的にセキュリティ教育や訓練を受けていく必要があります。

Point③ セキュリティ担当者の成長

組織のセキュリティ向上には中心となるセキュリティ担当者の成長が欠かせません。セキュリティ担当者が率先して教育や訓練を受け、従業員へ還元していくことが重要です。

日々インプットしていく情報の例



One point

IPA（独立行政法人情報処理推進機構）が公開している情報セキュリティ対策支援サイトは、情報セキュリティ対策を「知りたい」「学びたい」「始めたい」「強化したい」方々と、 それを後押しする方々の活動をサポートします。このサイトではそれぞれの役割（経営者、対策実践者、従業員、啓発者／教職員、一般／学生）に合わせて、情報セキュリティ対策を進めることができます。

<内容>
・情報セキュリティ診断
・5分でできる！ポイント学習
・SECURITY ACTION自己宣言者サイト
など

出典： IPA（独立行政法人情報処理推進機構）
情報セキュリティ対策支援サイト
https://security-shien.ipa.go.jp/

こんな事例も

セキュリティ担当者も日々情報のアップデートやトレーニングが重要です。

ある会社では、避難訓練や防災訓練と同じように、インシデント対応訓練を行っています。被害を少なくするための行動を手順書化するだけでなく、有事の際にも慌てないで、対応できることを目指しています。9月1日に防災の日として防災訓練をするように、内閣サイバーセキュリティセンターが設定しているサイバーセキュリティ月間（2月1日から3月18日）の中でインシデント対応訓練を行っています。

訓練を行うことで、自分たちに足りていない知識やスキルもわかってきたため、外部に委託する箇所や自分たちが教育を受ける箇所も明確になり、成長のための行動をとっています。

Day8
1.組織・人の対応を強化する

雇用におけるセキュリティの注意事項

従業員による故意の情報漏えいを防ぐために、秘密保持義務を記載する場合があります。セキュリティ規程ではなく、就業規則に記載される場合もありますが、雇用時にセキュリティの役割や責務を認識させ、ルールを守らせることが重要です。

Point① 秘密情報管理に関する就業規則の例

従業員が遵守する規程に禁止事項等を明確に定め、雇用時に認識してもらうことが重要です。

第○条（服務規律）
1. 従業員は、職場の秩序を保持し、業務の正常な運営を守るため、職務を遂行するにあたり、次の各号に定める事項を守らなければならない。
   ✓ 会社の施設、設備、製品、材料、電子化情報等を大切に取り扱い保管するとともに、会社の許可なく私用に使用しないこと。
2. 従業員は、入退場に関し、次の各号に定める事項を守らなければならない。
   ✓ 警備員から所持品の検査を求められたときは、応じること。
   ✓ 会社の許可なく、書類や社品を会社外に持ち出さないこと。
3. 従業員は、従業員証を常時携帯し、入場のとき又は求められたときは、直ちに提示しなければならない。

第○条（遵守事項）
1. 従業員は、次の各号に定める事項を守らなければならない。
   ✓ 会社の内外を問わず、在職中、又は退職若しくは解雇によりその資格を失った後も、会社の秘密情報を、不正に開示したり、不正に使用したりしないこと。
   ✓ 従業員は、在職中及び退職後【六ヶ月間／一年間／二年間】、会社と競合する他社に就職し、また競合する事業を営まないこと。
   ✓ 退職時に、会社から貸与されたパソコンや携帯電話等、会社から交付を受けた資料（紙、電子データ及びそれらが保存されている一切の媒体を含む）を全て会社に返却すること。

Point② 秘密保持契約書を締結する

採用時やプロジェクトへの参画時に特定の情報の閲覧や保有を行うために、秘密保持契約書（機密保持契約書と表現する場合もあり）を取り交わします。

秘密保持契約書の例	
タイミング	目的
入社時	入社にあたり会社の機密情報にアクセス・閲覧するために取り交わしを行う。
プロジェクト参画時	プロジェクト特有の情報や顧客情報にアクセス・閲覧するために取り交わしを行う。
退職時	会社退職時に会社の情報の返却や破棄を明言し、会社で知り得た情報を口外しないことを目的に取り交わしを行う。

経済産業省が公開している『各種契約書等の参考例』では、各種契約書の参考文面が紹介されています。

出典：経済産業省
「各種契約書等の参考例」をもとに作成
https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/reference2.pdf

Day8

1.組織・人の対応を強化する

懲戒の対応について

従業員がルールに違反した場合には、企業秩序維持のため懲戒を検討しなければならないことがあります。懲戒や適用のルールを明確にしておくことも重要です。また、法律で定められた罰則もあり、組織内にとどまらない場合もあります。

Point① 情報管理が不適切な場合の処罰

企業が個人情報などの法的な管理義務がある情報を適切に管理していなかった場合、経営者や役員、担当者は刑事罰その他の責任を問われることになります。

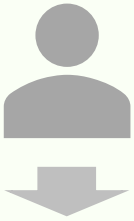
法令	条項	処罰など
個人情報保護法	当該個人情報取扱事業者等その他の関係者に対して報告徴収・立入検査を実施（法第143条）	委員会による立入検査
	報告徴収に対して虚偽の報告をした（法第177条）	刑事罰（50万円以下の罰金）が科される可能性
	委員会からの命令に違反（法第145条第４項）	刑事罰（１年以下の懲役又は100万円以下の罰金）
	第三者の不正な利益を図る目的で提供又は盗用（法第174条）	刑事罰（１年以下の懲役又は50万円以下の罰金）

出典：個人情報保護委員会
「個人情報取扱事業者等が個人情報保護法に違反した場合、どのような措置が採られるのですか。」 をもとに作成
https://www.ppc.go.jp/all_faq_index/faq1-q11-1/

Point② 懲戒処分を定めつつ、報告がしやすい環境を

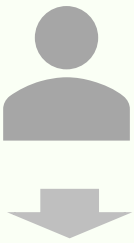
故意による犯罪などの場合は別として、一度のルール違反で厳しい処罰を行うと、正しい報告をせず、隠すことを考えるようになります。報告がしやすい環境を用意しつつ、正しい行動をしている人を称えることも重要です。

故意による犯罪



即時の処罰の実行

ルール誤認識による違反



注意喚起・指導

ルール違反などの理由がルール誤認識であるなどの場合、注意喚起や指導を行い、改善を促します。もし、指導を行っても改善がされず、繰り返される場合には処分を検討していきます。

ミニワーク
～考えてみよう～

ミニワークテーマ

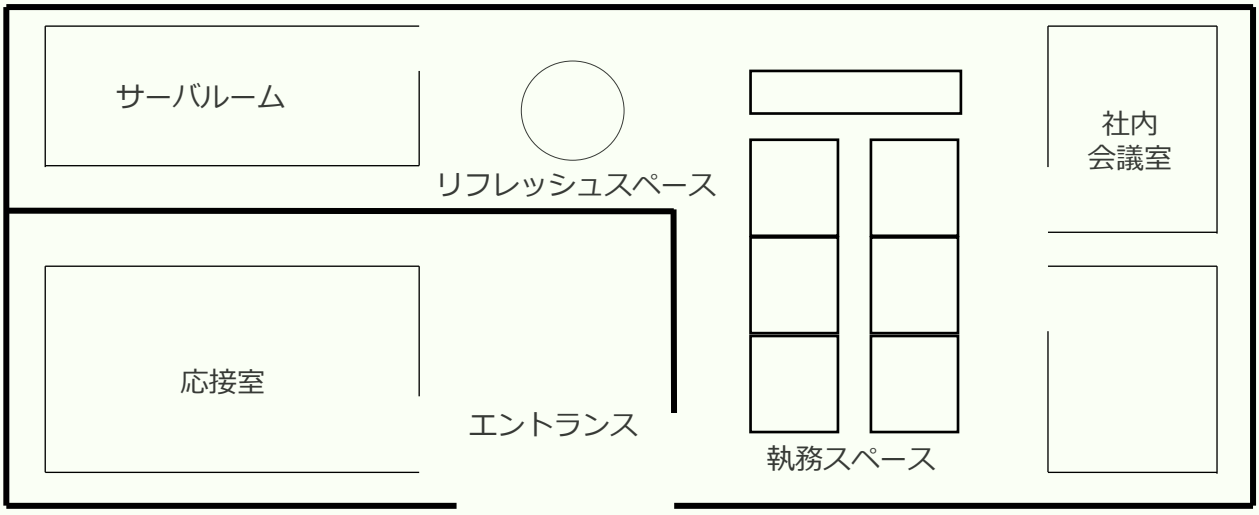
現在施行している規程や指針・指標、マニュアルはどのようなものがありますか？また、いつ頃作成されましたか？
最後に更新したのはいつ頃ですか？

物理セキュリティ

物理セキュリティでは、建物への侵入や各機器を守るために必要な対策を検討し実行します。

Point① フロア区分を定める

オフィス内では、社員が活動する場や外部の人が出入りする場とセキュリティルールを区分する必要性があります。



企業における部屋・スペースの例		
部屋名	区分	主な用途
サーバルーム	機密エリア	サーバや電子機器など社内インフラを構成する機器を設置する。入退室などを厳重に管理する必要がある。
社内会議室	執務エリア	主に社内で会議を行う。従業員のみが入退室できるエリア。
執務スペース	執務エリア	主に従業員が業務・執務を行う。従業員のみが入退室できるエリア。
リフレッシュスペース	執務エリア	主に従業員がリフレッシュをする。自動販売機の補充などにより外部の者が入室することも想定する必要がある。
応接室	受付エリア	主に外部の人と打ち合わせなどを行うスペース。外部の人が入室する前提で部屋を管理し、入退室を管理する。
エントランス	受付エリア	基本的には誰でも入退室が可能なエリア。受付を行うなど、来客情報などを管理する必要がある。

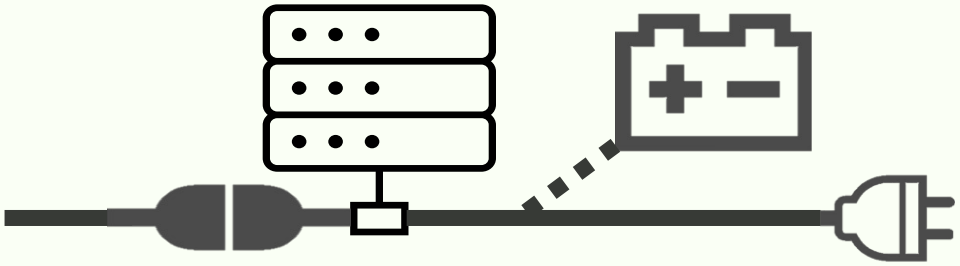
各エリアを明確にし、入退室の記録を取ることが重要です。例えば、従業員にはICカードを貸与し、執務スペースへの出入りにはICカードによる記録を取るといった方法があります。また、ICカードを持たない来客者は、入退室記録簿などに記名をしてもらうことで管理をすることができます。来客者の行動範囲を明確化するため、立ち合いなどのルールを定めておくことが重要です。

物理セキュリティ

Point② 機器自体の安定稼働を守る

物理セキュリティでは、機器自体に対してセキュリティ対策を行います。盗難などの対策だけでなく、電源などについても意識する必要があります。

UPS（Uninterruptible Power Supply）
停電などの際に機器を安全にシャットダウンする時間を稼ぐ装置を導入する。

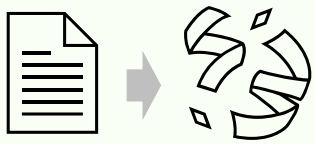


つながるLANケーブルが抜けないように注意する。執務スペースエリアなどで利用する場合、抜けやすくなるので注意が必要。

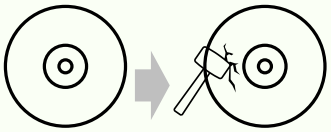
電源ケーブルが抜かれないようにケーブルロックなどを利用する。
サーバラック内の電源から通電することで、施錠管理できる。

Point③ 資産の廃棄に注意

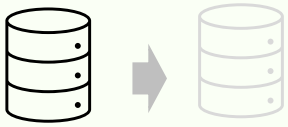
入退室管理システムにおいて、その役目を終えてシステムを構成していた機器を廃棄する際にも、情報セキュリティの観点で考慮しなければならない事項があります。



紙ベースの資産では、シュレッダーなど読み取りができない形で廃棄します。



外部記憶媒体では、データの削除や物理的な破壊で破棄を行います。



サーバなどストレージでは、データの削除を行い、破棄を行います。

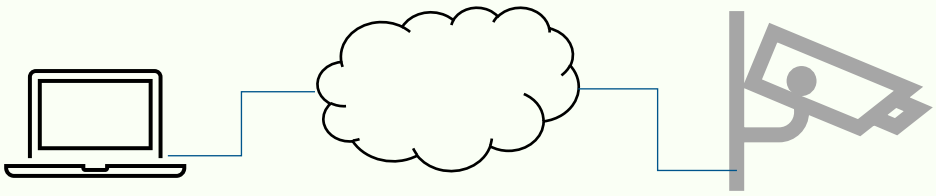
One Point

入退室管理システムでは、システムを構成する一部の機器において利用者に紐づいたID やログを保存しています。システムによっては ID に加えて個人を識別する情報を保持しているかもしれません。組織のセキュリティポリシーに照らし合わせて、それらの情報が漏えいすると問題となる場合は、リース、レンタルの返却や廃棄処理を外部委託する際の処置について調達仕様で要件化（復元不能な電磁フォーマットや物理的破壊を行い消去証明書を提出する、などと記載）しておくべきです。一般的には管理サーバ、制御装置及び鍵管理盤など IP ネットワークに接続された機器に ID やログは保持されます。あらかじめシステム内のどの機器に漏えいしては困る情報が保存されるのかを確認し、廃棄処理の対象とする機器をリストアップしておきましょう。

物理セキュリティ

Point④ 物理セキュリティ対策を保護する

監視カメラなども物理セキュリティに該当します。最近の監視カメラはインターネット接続されているため、物理セキュリティを高めるための監視カメラを、技術的対策等で保護するといった処置が求められます。



監視カメラの映像をネットワークを通じて視聴ができる

物理的な対策として、監視カメラを設置し入退室を監視

監視カメラを導入すると、人の出入りや作業などが記録されるため検知能力が高まります。また、抑止の効果が働くため、セキュリティの向上が期待できます。

しかし、ネットワークを利用する端末が増えることになり、認証やアクセス制御を適切に行わないと監視カメラがウイルスに感染する事態が発生します。ウイルス感染により、DDoS攻撃に加担するようなBotとなり、加害者の一端となってしまう可能性があります。

Point⑤ 物理セキュリティと論理セキュリティを組み合わせる

技術的対策、組織的・人的・物理的対策と説明をしてきました。物理セキュリティに対して、組織・人・技術を論理セキュリティと表現する場合があります。また、４つの対策を各々実施するのではなく、組み合わせて実施することでより強固なセキュリティ対策となります。Point④のように物理セキュリティへ取り組んだことにより資産が増え、増えた資産に対してセキュリティ対策が求められるというケースもあります。リスクアセスメントを実施し、リスクへの対応を行っていくことが求められます。

フロアレイアウトと論理セキュリティの組み合わせ		
フロアレイアウト		論理セキュリティ
サーバルーム	機密エリア	許可された人だけが入退室可能。また、入退室を共連れで行わないようにルールを定め、記録を取得。
社内会議室	執務エリア	従業員が所有するICカードで出入りが可能。共連れでの入退室も可能であり、執務エリアでは社員証の着用がルール化されている。
執務スペース		
リフレッシュスペース		
応接室	受付エリア	来客者が入れるように施錠等はせず、受付としてインターホンや呼び出し用の電話を置いておく。監視カメラを設置し入退室が記録できるようにする。
エントランス		

Day8

3.組織の成熟度を高める

組織の成熟度の考え方

セキュリティを強化するためには、組織の成熟度を高めていく必要があります。成熟度とは、理想と現実のギャップを埋めるために、段階に応じた改善や改革を行っていくための指標です。ただし、成熟度は従業員の入れ替わりやルールの変更などにより変動するということを理解し、取り組むことが重要です。

Point① 強いセキュリティ組織とは

セキュリティの成熟度が上がっている状態とはどのようなものでしょうか？それは、決められたルールが守られ行動できている状態、それぞれの役割を認識し実行できている状態です。

経営層

- 社内の情報セキュリティを統括し、セキュリティの推進、体制の構築をする。
- ビジネスの視点でセキュリティ対策や事故発生時の影響を検討する。
- 組織の方針や規程について承認をする。または、承認者へ権限譲渡をする。

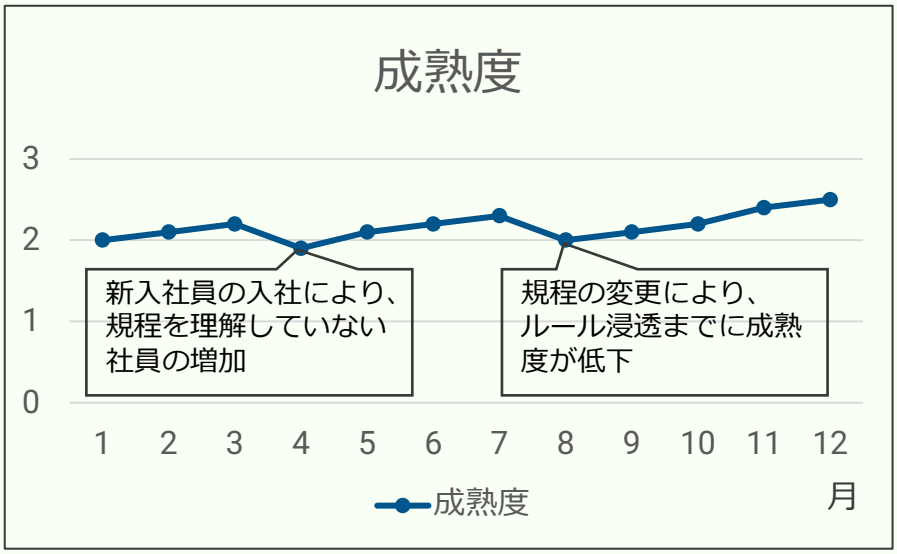
セキュリティ
戦略担当

- 自社の事業計画に合わせたセキュリティ戦略を策定する。
- リスク分析や資産管理を通してセキュリティ対応策を考え、実行し、評価する。
- セキュリティ上の課題を発見し対処する。

セキュリティ
システム担当

- セキュリティ機器類の導入計画や設計を行う。
- 現在導入されている機器の有効性の評価を行う。
- システム周りの保守や監視を行う。

Point② 成熟度は下がることもあることを認識



セキュリティの成熟度は従業員の入れ替わりや規程などの変更により、下がるケースがあります。下がることを考慮しながらも、PDCAのサイクルを回しながら長期の視点で、現状理解と目指すべき理想の姿のギャップを埋めていく活動が求められます。

また、セキュリティに関する事項をたまにしか行わない場合も、徐々に成熟度が下がるケースがあります。定期的な情報共有等を継続して行くことが重要です。

組織の成熟度の考え方

Point③ 自分たちが目指すべき姿と現状のギャップを把握

成熟度を考えるためにも、自分達が何を目指しているのかを定めることは重要です。理想の状態と現状のギャップ、優先度などを考慮した対応をして行くことが重要です。第3回に紹介したサイバーセキュリティフレームワークでは、プロファイルという考えがあります。

フレームワークプロファイル (プロファイル / Profile)

プロファイルは自組織のビジネス上の要求事項、リスクの許容度、割り当て可能なリソース等から目標となるプロファイルを作成し、ギャップ分析を行うことで優先順位付けされた改善計画を立てることができます。プロファイルの雛形はありませんが、コアのサブカテゴリーに関して、現在の状態（AsIs）と目指す目標の状態（ToBe）のギャップを洗い出し、費用対効果や優先順位を決めていくことができます。

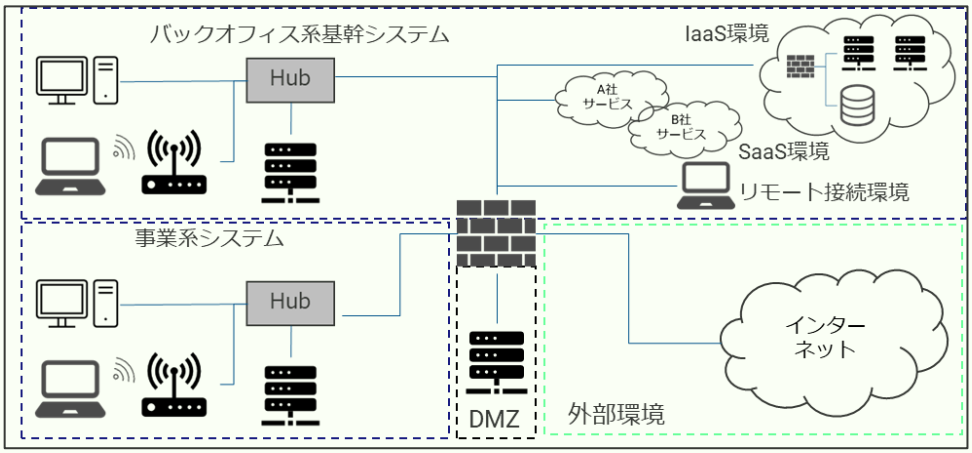
出典：IPA（独立行政法人情報処理推進機構）
「重要インフラのサイバーセキュリティを改善するためのフレームワーク」をもとに作成
https://www.ipa.go.jp/files/000071204.pdf

現状
基幹ネットワークにおいて、攻撃の予兆を知る術がなく、従業員からの報告や外部からの報告で攻撃の可能性を知る状態になっている

理想の状態
基幹ネットワーク、事業ネットワーク、クラウド環境において、ログにより攻撃の予兆が把握でき、予兆があった際は、担当へメールが配信される状態

Point④ 範囲や測定方法を明確にする

現状や理想の状態を把握する際に、適用される範囲や測定方法を定めておかないと正しく状態を把握することが難しくなります。組織の成熟度を把握するためにも、計画の段階で定義しておくことが重要です。



適用範囲と測定方法の例			
識別	ID.AM	資産管理	自組織内の物理デバイスとシステムが、目録作成されている。

現状：バックオフィス系基幹システム：物理デバイスとシステムの目録が作成されている
事業系システム：目録作成ができていない
確認方法：目視による物品確認 および 環境確認
あるべき姿：全環境の物理デバイスとシステムの目録が作成されている
確認方法：MDM（または同等の機能を有するもの）でのシステム一元管理

Day8

3.組織の成熟度を高める

組織の成熟度を上げる セキュリティチームの運営

セキュリティを強化するためには、セキュリティの担当者や対応チームの成長が不可欠です。セキュリティ担当者やチームの状態の把握やスキルアップを行うための運営が求められます。

Point① 個人が求められるレベルを明確にし成長する

個人の能力のレベル定義をする際は、ITSS（ITスキル標準）などを活用すると便利です。個人の能力や実績に基づいた、7段階のレベルが設定されています。セキュリティ担当としてまずは、レベル4・5が存在するチームを目指していくとよいのではないでしょうか？

Lv	レベル感（ITSS（ITスキル標準）より抜粋）
7	市場全体から見ても先進的なサービスの開拓や市場をリードした経験と実績を有しており、世界で通用するレベル。
6	社内だけでなく市場においても経験と実績を有しており、国内のハイエンドプレーヤとして通用するレベル。
5	社内において自他共に経験と実績を有しており、企業内のハイエンドプレーヤとして通用するレベル。
4	自らのスキルを活用することによって、独力で業務上の課題の発見と解決をリードする。また、プロフェッショナルとして求められる経験の知識化とその応用（後進育成）に貢献できるレベル。
3	スキルの専門分野確立を目指し、プロフェッショナルとなるために必要な応用的知識・技能を有し、要求された作業を全て独力で遂行するレベル。
2	上位者の指導の下に、要求された作業を担当するレベル。
1	情報技術に携わる者に、最低限必要な基礎知識を有しているレベル。

出典：IPA（独立行政法人情報処理推進機構）
「IT人材の育成」をもとに作成
https://www.ipa.go.jp/jinzai/itss/itss1.html

Point② 組織や役割に必要な能力を明確にし成長する

成熟度を上げるためには、個人の能力だけでなく組織としての役割や必要な能力を明確にする必要があります。担当の能力が必要な能力に達していない場合には教育なども検討します。

セキュリティチーム(組織)の主な役割の例		
セキュリティ戦略		
法令対応	基本方針の策定	体制策定
実務		
セキュリティ関連規程・指針・指標策定	情報共有・情報連携	インシデント管理
支援		
新規技術・サービス導入	データ管理	
実務支援		
セキュリティ戦略 / 予算措置	セキュリティバイデザイン	選定基準
運用保守基準 / 品質管理	アセスメント / 監査	サプライチェーンリスク管理

出典：経済産業省
「サイバーセキュリティ体制構築・人材確保の手引き」をもとに作成
https://www.meti.go.jp/policy/netsecurity/tebikihontai2.pdf

Point①とPoint②を一緒に考え、セキュリティ組織・チームとしての役割とそれを実行する人の能力を考えたチーム体制を維持し、不足する場合には、チーム運営の中で補っていく必要があります。

組織の成熟度を上げる
セキュリティチームの運営

Point③ 役割とタスクを定め、責任範囲を明確にする

セキュリティの業務において役割やタスクを定義し、責任範囲を明確にしていきます。また、タスクが整理されると、自社で実施すべきか、外部委託すべきかという検討も必要になります。それらが決まると、責任と体制が決まってきます。

経営層

タスクの例
- サイバーセキュリティ意識啓発
- 対策方針の指示
- セキュリティポリシー、予算、対策実施事項の承認

セキュリティ
戦略担当

タスクの例
- サイバーセキュリティ教育
- サイバーセキュリティリスクアセスメント
- セキュリティポリシー・指針・指標の策定・管理・周知
- 警察・官公庁等対応

セキュリティ
システム担当

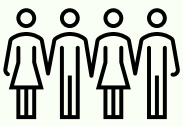
タスクの例
- セキュリティ製品、サービスの導入、運用
- セキュリティ監視・検知・対応
- インシデントレスポンス、連絡受付

出典：経済産業省
サイバーセキュリティ体制構築・人材確保の手引き
https://www.meti.go.jp/policy/netsecurity/tebikihontai2.pdf

Point④ 会社に適したセキュリティ機能のチーム(体制)検討

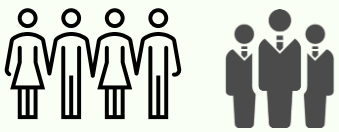
セキュリティチームは会社の規模やセキュリティ業務のタスクにより変化をします。自社に適した体制はどのようなものかを検討し、適したチームを構築していきましょう。該当ページも参考にし、体制を決めていきましょう。

社内人員のチーム体制



社内の人員を集めてチームを構築します。専任だけでなく、兼務の人材を集める場合もあります。

外部連携したチーム体制



社内の人員と専門分野では外部の力も借りたチームを構築します。

外部中心のチーム体制

社内では責任者のみを配置し、他は外部へ委託をしてチームを構築します。

セキュリティのチームの体制を整えるときは、外部と連携をしたチーム体制を作ることが多いです。しかし、判断を強いられる場合には社内の責任者が決断する必要性があります。体制と責任範囲を明確にしましょう。

Day8

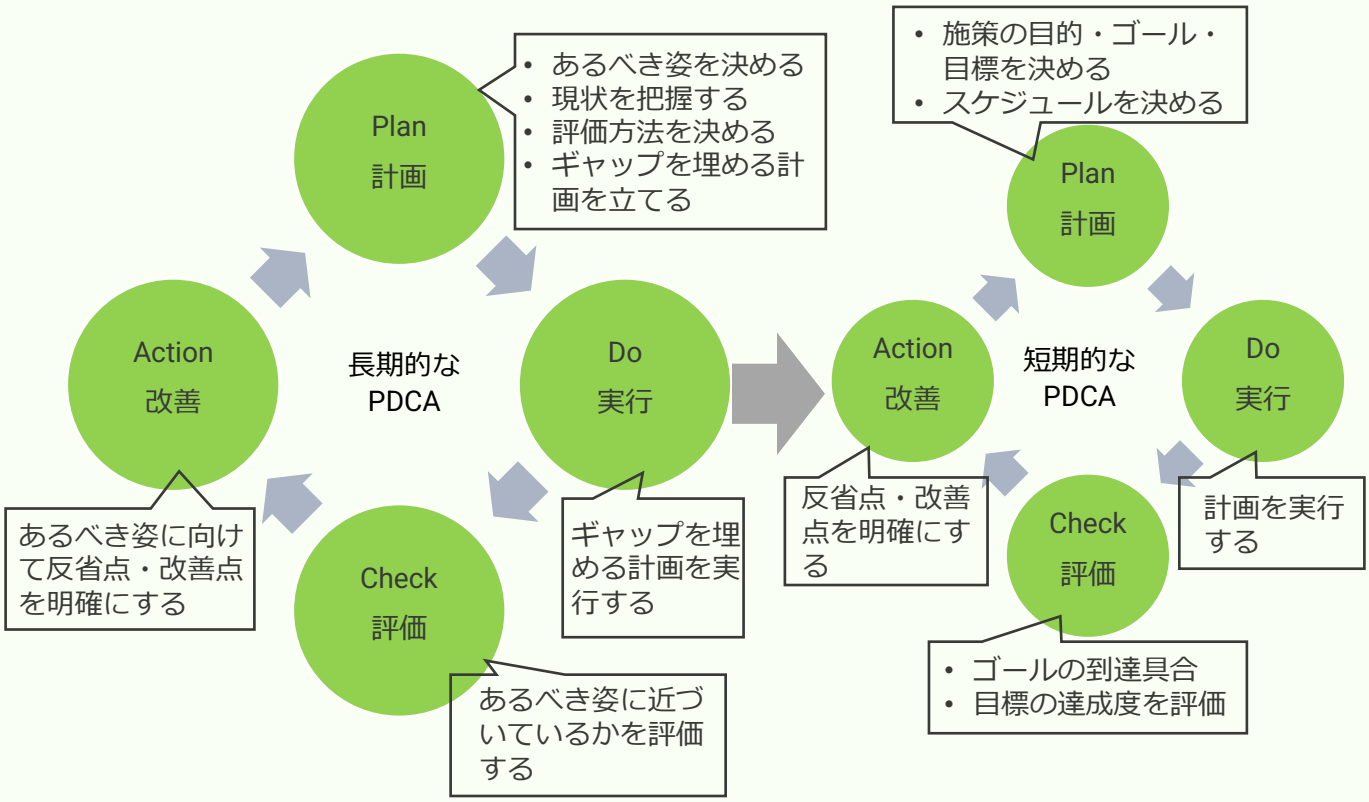
3.組織の成熟度を高める

組織の成熟度を上げる活動

組織の成熟度を上げて行くためには、PDCAを実施しながら、理想の状態に近づけていくことが重要です。

Point① PDCAを回しながら成熟度を上げる

PDCAを回しながら成熟度を上げていきます。この時に、長期的な計画と短期的な計画を組み合わせながら考えていくと、あるべき姿に向けたPDCAとなってきます。



長期的な視点でのPDCAでは、あるべき姿と現状のギャップを把握し、ギャップ解消を目指した活動を実施します。ギャップ解消の活動となる各施策は、短期的なPDCAサイクルを行うことで精度があがり、より効果的なギャップ解消の取り組みとなります。

One Point

「サイバーセキュリティ経営ガイドライン解説書Ver.1.0 」ではPDCAについて以下のような表記があります。

フレームワーク（PDCA）のサイクル

情報セキュリティマネジメントシステムでは、PDCA のサイクルは、通常１年間とするケースが多く、この１年ごとのサイクルは、企業や組織における年度計画の見直しとタイミングが同じであるため、馴染み易いサイクルです。一方、昨今の環境変化は短期間に発生する場合もあり、未知のサイバー攻撃への対応などを考慮すると、さらに短いサイクルで見直しを実施することも検討します。

出典：IPA（独立行政法人情報処理推進機構）
サイバーセキュリティ経営ガイドライン解説書Ver.1.0
https://www.ipa.go.jp/files/000056148.pdf

Day8

3.組織の成熟度を高める

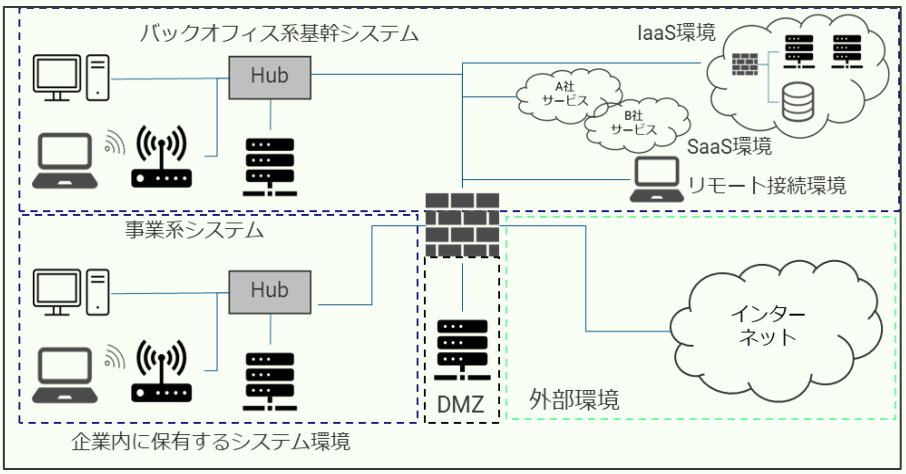
組織の成熟度を上げる計画

組織の成熟度を上げて行くためには、何をして行くのかを示す計画が非常に重要です。ありたい姿を定めると共に、評価方法や適用範囲などを検討していきます。

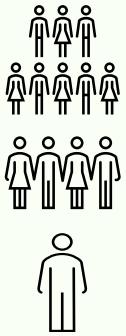
Point① 適用範囲を明確にする

セキュリティの取り組みをどこに適用して行くのかを考えます。基本的には全社となりますが、それぞれのネットワークの役割などにより多少の違いが発生する場合があります。また、従業員や委託社員などの違いも明確にします。

適用範囲（場所・システム環境）の事例



適用範囲（人）の事例



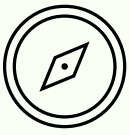
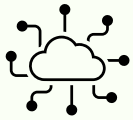
従業員

契約社員

嘱託職員

Point② 会社の目指す姿を実現するために必要なセキュリティ像（ありたい姿）を明確にする

ありたい姿は、経営理念や会社の事業計画に即したものでなければいけません。広い視点で考えながら、事業計画を実現するために必要な姿、ありたい姿を考えていきます。

会社が目指すビジョン	ビジョン実現のための戦略	戦略を安全に実現するセキュリティのあるべき姿
		
会社が目指すビジョン、成し遂げたいこと、提供したい価値を把握する。	ビジョン実現のために取りうる戦略を把握する。	戦略を安全に実行するために必要となるセキュリティのあるべき姿を定める。

あるべき姿を決める際には、役職や業務内容などが違う人が集まって決めていくことが理想です。経営者のありたい姿は売上向上や円滑な事業運営、セキュリティ担当者のありたい姿は従業員のセキュリティ理解向上など粒度に差が生まれます。会社の目指すビジョンを実現するために必要なセキュリティ像は、立場や役職などが違う関係者で集まり決めていきます。

あるべき姿をPoint③で紹介するCSFのカテゴリー・サブカテゴリーで整理することで、現状とのギャップを把握しやすくなります。また、優先度をつけることで取り組みの判断に迷わなくなります。

組織の成熟度を上げる計画

Point③ とるべきセキュリティ対策のポイントを決める

会社として何に気を付ければよいのか、どのあたりをポイントとして取り組むべきかを考えるときには、フレームワークを活用すると便利です。今回は、第3回のテキストで紹介した、NIST CSF (Cybersecurity Framework) を用いて成熟度について説明します。

気を付けるポイントをカテゴリーごとに説明しているのが、コアです。コアは、業種や業態を問わず、各組織で共通となるサイバーセキュリティ対策を示しています。第3回のテキストで紹介した通り、5つの機能と23のカテゴリーで構成されます。さらに、各カテゴリーには複数のサブカテゴリー（計108項目）が紐づいており、サイバーセキュリティ対策として取り組むべき具体的な対策項目の参考とすることができます。

フレームワークコア (コア / Core)			
機能	識別子	カテゴリー	サブカテゴリー（一例のみ記載）
識別	ID.AM	資産管理	自組織内の物理デバイスとシステムが、目録作成されている。
	ID.BE	ビジネス環境	サプライチェーンにおける自組織の役割が、識別され、周知されている。
	ID.GV	ガバナンス	組織のサイバーセキュリティポリシーが、定められ、周知されている。
	ID.RA	リスクアセスメント	資産の脆弱性が、識別され、文書化されている。
	ID.RM	リスクアセスメント管理戦略	リスクマネジメントプロセスが、組織の利害関係者によって定められ、管理され、承認されている。
	ID.SC	サプライチェーン リスクマネジメント	サイバーサプライチェーンのリスクマネジメントプロセスが、組織の利害関係者によって、識別され、定められ、評価され、管理され、承認されている。
防御	PR.AC	アクセス制御	認可されたデバイス、ユーザー、プロセスのアイデンティティと証明書が、発行、管理、検証、取消し、監査されている。
	PR.AT	意識向上およびトレーニング	すべてのユーザーに対し情報が周知され、トレーニングが実施されている。
	PR.DS	データセキュリティ	保存されているデータが、保護されている。
	PR.IP	情報を保護するための プロセスおよび手順	情報技術/産業用制御システムのベースラインとなる構成は、セキュリティ原則（例：最低限の機能性の概念）を組み入れて、定められ、維持されている。
	PR.MA	保守	組織の資産の保守と修理は、承認・管理されたツールを用いて実施され、ログが記録されている。
	PR.PT	保護技術	監査記録/ログ記録の対象が、ポリシーに従って決定され、文書化され、実装され、その記録をレビューされている。

Day8
3.組織の成熟度を高める

組織の成熟度を上げる計画

フレームワークコア (コア / Core)			
機能	識別子	カテゴリー	サブカテゴリー（一例のみ記載）
検知	DE.AE	異常とイベント	ネットワーク運用のベースラインと、ユーザーとシステムで期待されるデータフローが、定められ、管理されている。
	DE.CM	セキュリティの継続的なモニタリング	ネットワークは、サイバーセキュリティの潜在的なイベントを検知できるようにモニタリングされている。
	DE.DP	検知プロセス	検知に関する役割と責任は、説明責任を果たせるように明確に定義されている。
対応	RS.RP	対応計画の作成	対応計画が、インシデントの発生中または発生後に実行されている。
	RS.CO	コミュニケーション	人員は、対応が必要になった時の自身の役割と行動の順序を認識している。
	RS.AN	分析	検知システムからの通知は、調査されている。
	RS.MI	低減	インシデントを封じ込めている。
	RS.IM	改善	学んだ教訓を対応計画に取り入れている。
復旧	RC.RP	復旧計画の作成	イベントの発生中または発生後に復旧計画を実施している。
	RC.IM	改善	復旧計画は、学んだ教訓を取り入れている。
	RC.CO	コミュニケーション	広報活動が管理されている。

NISTはフレームワークコアを公開しており、無料でダウンロードすることが可能です。

重要インフラのサイバーセキュリティを改善するためのフレームワーク　1.1版
　原文　https://www.nist.gov/document/2018-04-16frameworkv11core1xlsx
　和訳　https://www.ipa.go.jp/files/000071205.xlsx

　これらの各カテゴリー、サブカテゴリーに対して、適用範囲や適用する関係者、取り組み方法、評価方法を決めておくことで、現状を把握しやすくなります。また、Point④で紹介するティアの判定基準を定めることで、現状をより理解できます。

One Point

　「サイバーセキュリティ経営ガイドライン」ではサイバーセキュリティ経営チェックシートが付録として掲載されています。チェック項目には、NISTが提供するサイバーセキュリティフレームワークとの対応関係が提示されています。いきなりCSFは難しそうと感じる方は、サイバーセキュリティ経営チェックシートも活用しながら、ありたい姿と現状のチェックをしてみましょう。ただし、項目数としては、CSFの方が多くなりますので、自社で不足する項目は、CSFを参考にして追加しましょう。

出典：経済産業省
サイバーセキュリティ経営ガイドライン Ver 2.0
https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide2.0.pdf

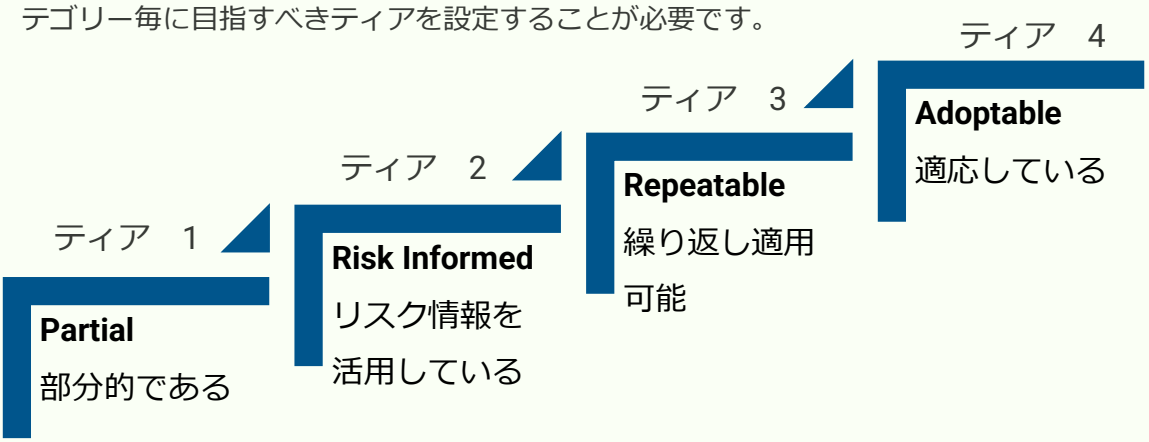
組織の成熟度を上げる計画

Point④ 現状を把握する

カテゴリー・サブカテゴリーの項目に従い、現状を把握していきます。現状を把握する際には、同じくCSFの要素である、フレームワークインプリメンテーションティア (ティア / Tier)を利用していきます。

● フレームワークインプリメンテーションティア (ティア / Tier)

ティアは、組織のセキュリティリスク管理がどの程度実践できているかをティア 1 (部分的)からティア 4 (適応)で示すことで、自組織の現状を把握し、優先的に取り組むべき施策や追加リソースの割り当てなどの決定を行うにあたっての指標とすることができます。必ずしもティア4を目指すことが正解ではなく、自組織のビジネス特性や情報資産の実態などに応じて、コアカテゴリー毎に目指すべきティアを設定することが必要です。



また、「何をもってティアの各4段階に到達しているかを判断するのか」というティアの具体的な定義は、各組織内で議論し、関係者間でのレベルの解釈のすり合わせおよび共通認識が必要となります。具体的な定義を決める際には、Point①で説明した適用範囲などの考えを利用します。また、取り組みの進捗度なども評価基準となります。以下に事例を示します。

評価対象のコア・カテゴリー・サブカテゴリー			
識別	ID.AM	資産管理	自組織内の物理デバイスとシステムが、目録作成されている。

適用範囲と取り組み・評価方法の例			
適用場所	適用する関係者	取り組み方法	評価方法
A、B、C ネットワーク	全従業員	物理デバイス、システムの一覧をエクセルにて作成する	物理デバイスとシステムと一覧の目視確認

評価基準の例			
ティア 1	ティア 2	ティア 3	ティア 4
未着手の適用場所がある状態。	全適用場所において目録が作成されているが評価がされていない。	全適用場所において目録と実態の評価が定期的にされている。	目録と実態の評価が定期的にされているだけでなく、より良い管理に向けた施策が継続的に実行できている。

108のサブカテゴリーにおいて評価基準等を決めてから現状を把握すると計画に時間がかかるというデメリットが生じます。PDCAを回して行く中で評価基準も見直していくことで、スピード感も意識した取り組みとなります。

組織の成熟度を上げる計画

Point⑤ あるべき姿と現状のギャップを洗い出す

現状とあるべき姿を比較し、ギャップの把握を行います。このギャップを解消して行くことであるべきセキュリティの姿に近づくことになります。以下の例は、カテゴリーに対しての実施ですが、サブカテゴリーであるべき姿と現状のギャップが把握できるとより詳細な状況を把握することができます。

フレームワークコア (コア / Core)					
機能	カテゴリー（一部のみ表示）	ティア（ ：理想、 ：現状）			
		1	2	3	4
識別	資産管理				
	ビジネス環境				
防御	アクセス制御				
	意識向上およびトレーニング				
検知	異常とイベント				
	セキュリティの継続的なモニタリング				
対応	対応計画の作成				
	コミュニケーション				
復旧	復旧計画の作成				
	改善				

Point⑥ 優先度をつけギャップ解消に向けた計画を立案する

ギャップに対して改善のための対応を進めていきます。ギャップが複数ある場合には、優先度をつけた対応が求められます。

ギャップの大きさ	重要な項目	実行のしやすさ
あるべき姿に近づくため、ギャップの大きさから優先順位を決めて取り組みます。	各カテゴリー・サブカテゴリーの中でも、重要な項目を優先的に取り組みます。	予算や環境、スキルなどまずはやりやすいところから取り組みます。

ギャップ解消は短期では全て解消しないことがほとんどです。長期的な視点で予算なども意識しながら計画を立案する必要があります。

長期計画	予算	体制
中期計画や年間計画として、いつまでに何をやるかの計画を検討します。	活動にはお金が必要です。予算を意識し、必要であれば予算確保を行います。	実行にあたり、体制が不足するようであれば、体制強化の働きかけを行います。

Day8

3.組織の成熟度を高める

組織の成熟度を上げる行動

計画が定まったら、次は実際に行動をしていきます。PDCAのDoの部分です。理想実現に向けて、現状と理想のギャップにアプローチした取り組みになっていることが重要です。また、短期的なPDCAを実践することも有効です。

Point① 取り組みを明確にし計画を立てる

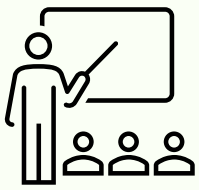
取り組みを実施するにあたり、まずはなぜその取り組みを行い、どのように評価をするのかを決めていきます。そして取り組みを実行し、評価をします。

◆アプローチするギャップ

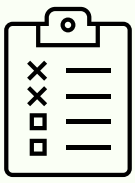
フレームワークコア (コア / Core)					
機能	カテゴリー（一部のみ表示）	ティア（■：理想、■：現状）			
		1	2	3	4
防御	意識向上およびトレーニング	■	■	■	■
		■			

この取り組みは組織を成熟させるために、どこに関係した取り組みなのかを明確にします。

◆取り組み終了後の目標と評価方法

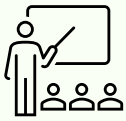


出席100%



テスト80%以上

◆主な取り組み内容と取り組み方法



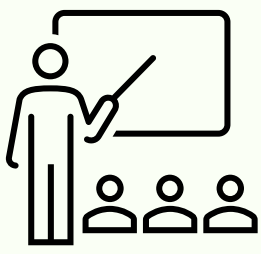
勉強会準備
コンテンツ検討
勉強会の開催

テスト作成
テスト実施
採点
フィードバック

行ったことに満足するのではなく、この取り組みを実施したことでどのような結果になったのかを把握します。そのためには、目標や評価方法を決めて、実施方法を検討します。

Point② 取り組みを実行する

取り組みの計画が立ったら実際に実行していきます。例えば、トレーニング講師などをセキュリティ担当者が実施する場合、目標をより効果的に達成するために、セキュリティ担当者が講師スキルを求められる場合もあり、研鑽が必要です。



求められるミッション
- 教育計画や目標・スケジュールを策定する。
- 研修テキスト・教材・テストの選定を行う。
- 講師として従業員への教育を行う。

求められるスキルやノウハウ
- 講師としてのコミュニケーションスキル・ノウハウ
- 指導方法や評価のスキル・ノウハウ
- 情報収集スキル

Day8

3.組織の成熟度を高める

組織の成熟度を確認

取り組みを実行した結果どのような変化があり、あるべき姿に近づいているのかを確認します。計画で定めた評価方法に基づき、現状の確認を行います。

Point① 現状の姿を確認する

計画でも確認したように現状を把握していきます。（本書P222参照）ありたい姿と改めて比較をすることで、ギャップを埋める活動となっているか、ありたい姿に近づいているかを確認します。

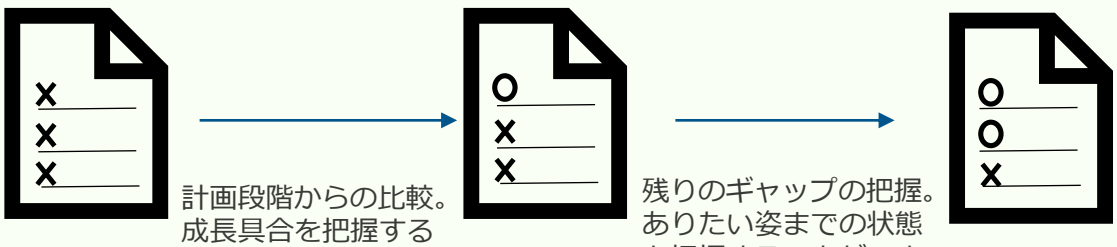
フレームワークコア (コア / Core)						
機能	カテゴリー（一部のみ表示）		ティア（ : 理想、 : 現状）			
			1	2	3	4
識別	資産管理	ありたい姿				
		計画時				
		評価時				

計画で確認方法まで定められていると評価がスムーズです。取り組みや施策によっては効果が出るまでに時間がかかるケースがあります。半面、評価までの期間が長い場合、うまくいっていない場合のリカバリーに遅れが生じるケースがあります。自社にあった適切なタイミングを見定め、評価を行っていきましょう。例えば、四半期ごとですと、年4回の評価ができ、約3か月の期間で評価ができます。

計画と評価のスパンの例											
4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
★			★			★			★		★
計画立案			1回目評価			2回目評価			3回目評価		4回目評価

Point② 比較をする

評価において、改めて現状の把握を行います。比較のパターンとしては、ありたい姿との比較を中心に考えます。また、計画時と比較をすることで、自分たちの成長を可視化することができます。成熟度を意識しつつも、成長度も把握することで取り組みの進捗などモチベーションアップにつながります。

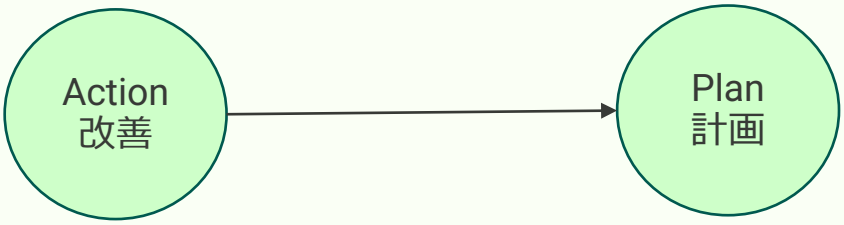


組織の成熟度の見直し

現状の確認後には、見直しや改善・是正を行います。ありたい姿を実現するためには、このままの計画でよいのか、ありたい姿に到達した後にどのような対応を検討していくのかを考えます。

Point① 改善・是正を検討する

あるべき姿を目指し、実行において取り組みを行い、評価を行います。評価により残っているギャップが把握されます。現在の対応をそのまま進めてよいのか、他の方法などに改めていくのかを判断します。



立てた計画に対して計画通りに進んでいる → 次の実行（Do）の準備を進める

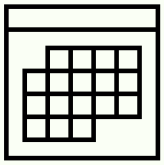
立てた計画に対して遅れが出ている → リカバリー計画の策定を進める

立てた計画に対して予定以上に進んでいる → 推進計画の策定を進める

Point② 計画変更に対応する

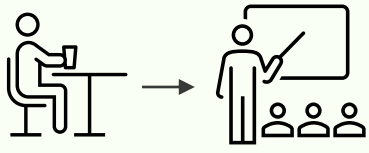
計画通りに進まない場合には計画変更を検討せざるを得なくなる場合があります。ただし、あるべき姿や評価指標が変わるわけではありません。何を変更して計画に対応するのかを考える必要があります。

スケジュールの変更



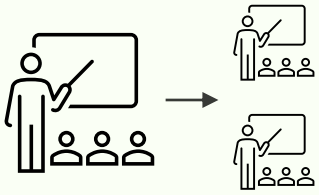
あるべき姿に到達するまでのスケジュールを調整します。この場合、現状とあるべき姿にギャップがある状態が予定より長くなります。長くなることが問題ないのか、影響はないのかをしっかりと検討する必要があります。

実行内容の変更



実行（Do）において、思った以上の効果が出なかった場合や成長度が遅いとなった場合には手段を変えるという選択肢があります。改めて実行（Do）の短期的な計画から始めるため、準備等に時間がかかる場合があります。

実行回数の変更



想定される効果に対して回数を重ねることで達成できると判断される場合は、実行回数を増やします。実行（Do）の回数が当初予定より増えるため、想定以上の稼働となり、セキュリティ担当が兼務をしている場合、他業務に影響が出る可能性があります。

ミニワーク
～考えてみよう～

ミニワークテーマ

自社のセキュリティの成熟度を上げるために、現在のセキュリティ担当者・チームが取り組んでいることは何でしょうか？

Day8

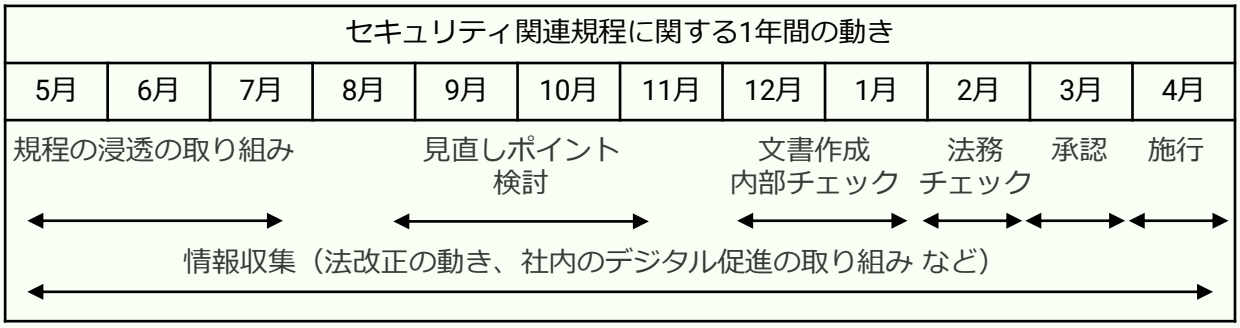
4.事例紹介

セキュリティ関連規程更新の具体例 ～自社のありたい姿を規程にする～

A社ではセキュリティに関係するものだけでも20ほどの規程があります。それらの規程はセキュリティを担当するチームが管理をしています。セキュリティチームでは適切な管理を行うため、日々さまざまな取り組みを行なっています。

管理をしているセキュリティ関連規程や指針・指標の一覧	
基本方針	個人情報保護規程
基本規程	人材管理規程
監査規程	文書管理規程
ネットワーク管理･利用規程	物理管理規程
システム管理・変更規程	リスク管理規程
システム利用規程	外部委託先管理規程
SNS利用規程	インシデント対応規程

セキュリティチームでは一年間の計画を立て、規程の更新や作成を行なっています。4月から年度が変わるため、4月の施行に合わせて、逆算したスケジュールで実施しています。



基本的な更新のルールは、事業計画やデジタル戦略を意識し、法令などを確認し検討します。見直す必要があるポイントなどを確認し、最終的に規程の文言修正を行います。そして、法務または顧問弁護士のチェックをし、経営会議で承認されて、施行となります。経営計画の変更や法令の改定が行われた際は、規程の大幅変更も行う場合があり、その時は非常に忙しくなるタイミングです。

2022年4月に施行された個人情報保護法の改定では、2020年6月の公布後から変更ポイントの整理を開始しました。匿名加工情報や仮名加工情報の利用有無や第三者提供の実施有無など、事業計画との擦り合わせを行いながら変更する場合の文言なども確認していきます。時には顧問弁護士の方のアドバイスを聞きながら対応を行いました。2022年4月1日付で改正された個人情報保護法に紐づく規程が作成されています。

そして、規程は変更しなくともマニュアルや手順が変更になるといったケースも存在します。規程に準拠はしているが、システムが変わりやり方が変わるなどの場合にはマニュアルの変更のみ行います。関連部署とのコミュニケーションをしっかりととることにより、いち早く情報をキャッチアップした対応が重要となります。また、リスク分析の結果、対策を強化する場合にもマニュアル変更が必要になります。最近だと2要素認証導入に伴う改訂などの事例をよく聞きます。この場合には、マニュアルの更新と合わせて従業員への周知を徹底し、事業影響を少なくする施策も検討する必要があります。

Day8

4.事例紹介

組織の成熟度を上げる事例 ～KPIを定めPDCAを評価～

B社では、組織の成熟度を上げるためPDCAサイクルを実施しています。セキュリティチームでは、事業年度の初めに計画として目標や評価指標を定めます。これをKPIとして置いています。B社では、セキュリティを「自社の事業運営を安全に円滑に行うために実施する」と定義し、それを実現する要因の一つとして成熟度を大切にしています。この成熟度はさらに2つの要素に分割されます。一つは会社全体の成熟です。適用範囲を会社の全環境、全従業員としています。もう一つは、セキュリティチームの成熟です。セキュリティを取り組むにあたって、担当チームが成熟していくことは重要な要素だと考えています。

B社の目標事例			
目標	KGI	KSF	KPI
安定した事業運営を行うため、組織がセキュリティの取り組みを理解し、実践している状態を維持する。	従業員のセキュリティの理解度90%以上の維持	従業員向けの取り組み	1、トレーニング開催回数 2、テキスト作成本数 3、理解度把握の取り組み件数
		セキュリティチーム向けの取り組み	1、トレーニング受講件数 2、勉強会開催件数 3、資格取得人員数

この目標を達成して行くことは、組織の成熟度を上げることにつながっているとB社では考え、PDCAを意識しています。セキュリティ担当チームではこの目標を実行するためにKSFで定めた「従業員向けの取り組み」と「セキュリティチーム向けの取り組み」のバランスを意識し取り組みを行っています。KGI達成のためには「従業員向けの取り組み」のみをしていれば良いようにも思われます。それだけでなく、従業員向けの取り組みを主導して行く立場にあるセキュリティチームが成長できる施策を行うことも、目標達成のためには重要な要素であるとB社では考えています。

Plan
1年間の目標・KGI・KSF・KPIを設計し、アクションプランの検討を行う

Do
実行スケジュールをたてアクションプランを実行する

Check
KPIの達成状況を確認し、KSF・KGIの達成状況の確認と進捗について評価する

Action
評価の結果を受けてアクションプランの見直し・検討を行う。必要に応じて目標の変更を行う場合もある。

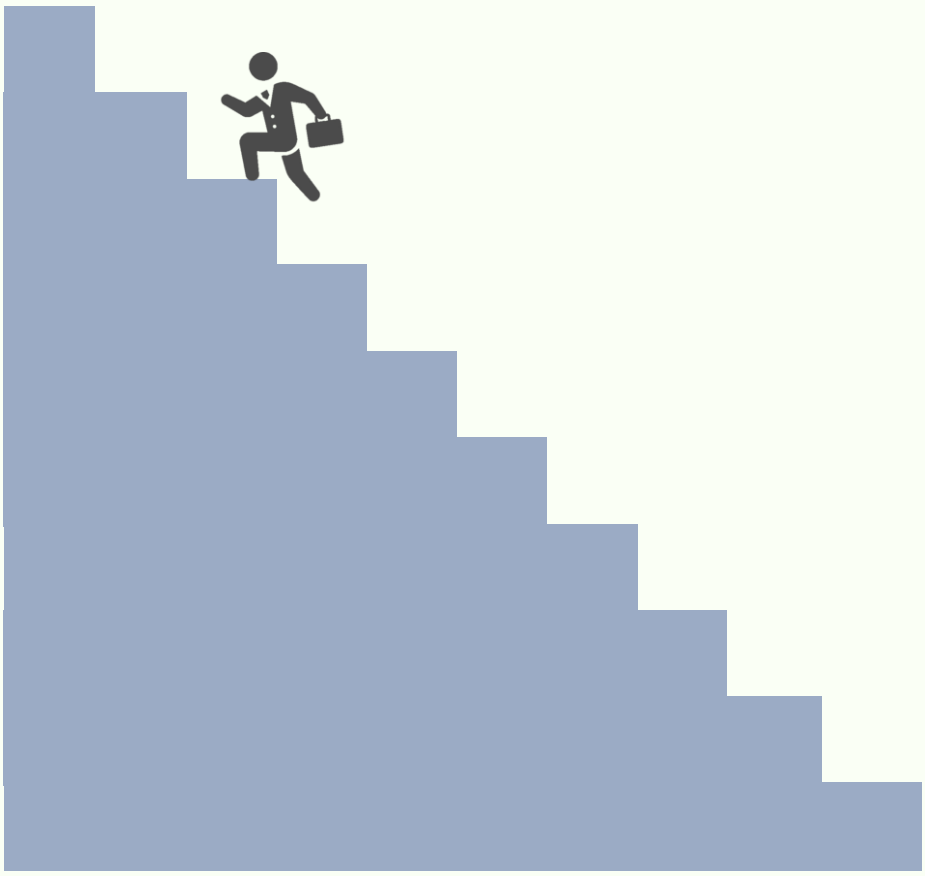
KPIと連動した取り組みとなっているため、セキュリティチームも日々の業務の中で実施する意義が分かりやすく、モチベーションが高く維持されています。また、B社の特徴として、事業貢献も意識しており、セキュリティだけ行っていればいいというわけではないという点が挙げられます。PDCAの評価において、事業貢献が無い、事業部門からの評判が悪いといった場合、改善をする必要があります。セキュリティの目的が明確になっており、事業との連携を意識しつつも、セキュリティチームが成熟し、評価される仕組みが整えられています。

組織的な対応や人への対応を今までも行ってきたつもりだったけど、作って終わりにはしていなかっただろうか？見やすい工夫やわかりやすく理解してもらいやすい取り組みはしてきただろうか？自社の規程はどうなっていたか。さっそく確認してみよう！

セキュリティ対策の理解度を高めていくことは組織の成熟度を上げていくことにもつながる。もちろん自分自身の成長は組織の成熟度を上げるためには重要だ。

まずは、自分たちの状態を把握することから始めてみよう。組織の状態や個人の状態も確認しないといけない。そこから、組織を成熟させるための計画を立てて、実行し、評価し、改善をするサイクルを回していこう。

組織の成熟度を上げる。組織を強くする。



コラム
～組織の成熟度を上げていくために～

組織の成熟度を上げていくために特に重要だと感じることは、人材育成の仕組みだと思います。特に、セキュリティチームの成熟度の場合、後任育成の仕組みが整っているかが重要です。レベルの高い担当者がチームに参加し、所属しているときにはセキュリティチームも会社全体も高い成熟の状態を目指しやすくなります。

これは、担当者を中心としたPDCAが行われており、適時対応や評価、改善活動が行われているからです。担当者が退職した事を起因に、セキュリティの成熟度がどんどん低下していくという事例は非常によく聞きます。専門職と言っても過言では無いセキュリティ担当者の急な不在により、PDCAがうまく回らなくなるからです。セキュリティチームが機能しなくなることで、全社的な成熟度も下がり始めるという結果につながります。

これらに対応していくためには、早い段階で後任となる人材の育成を行なっていく事が重要です。現在、セキュリティ人材の不足は顕著であり、市場価値も高まっています。なかなか採用することができないという声も聞きます。後任候補を見つけ育成をしていきながら成熟度を上げていく事が重要です。セキュリティに限らずですが、担当者任せにせず組織として対応していく姿勢をとっていく事が、組織力を一段高めた成熟した状態となるのかもしれません。

あとがき

セキュリティの勉強をして個人のレベルを上げて行くことは本人の努力の賜物です。しかし、個人がどんなにレベルアップ・スキルアップをしてもそれが組織に還元されるかは、別の話だと感じています。組織の成熟度を上げるためには、会社や経営層の理解も必要です。従業員の皆さんの協力も必要になってきます。成熟度を上げるためには組織一丸となった対応をするところからスタートを切る必要があります。

レベルアップ・スキルアップをしたセキュリティの担当者が活躍し、評価されることも重要です。せっかく育ったセキュリティ担当者が退職してしまった、辞めてしまったという話もよく聞きます。いなくなってから価値に気がついても後の祭りです。セキュリティを担当する方が活躍し成長し評価されるような環境を作ることも成熟の証なのかもしれません。

令和4年度

中小企業サイバーセキュリティ対策継続支援事業

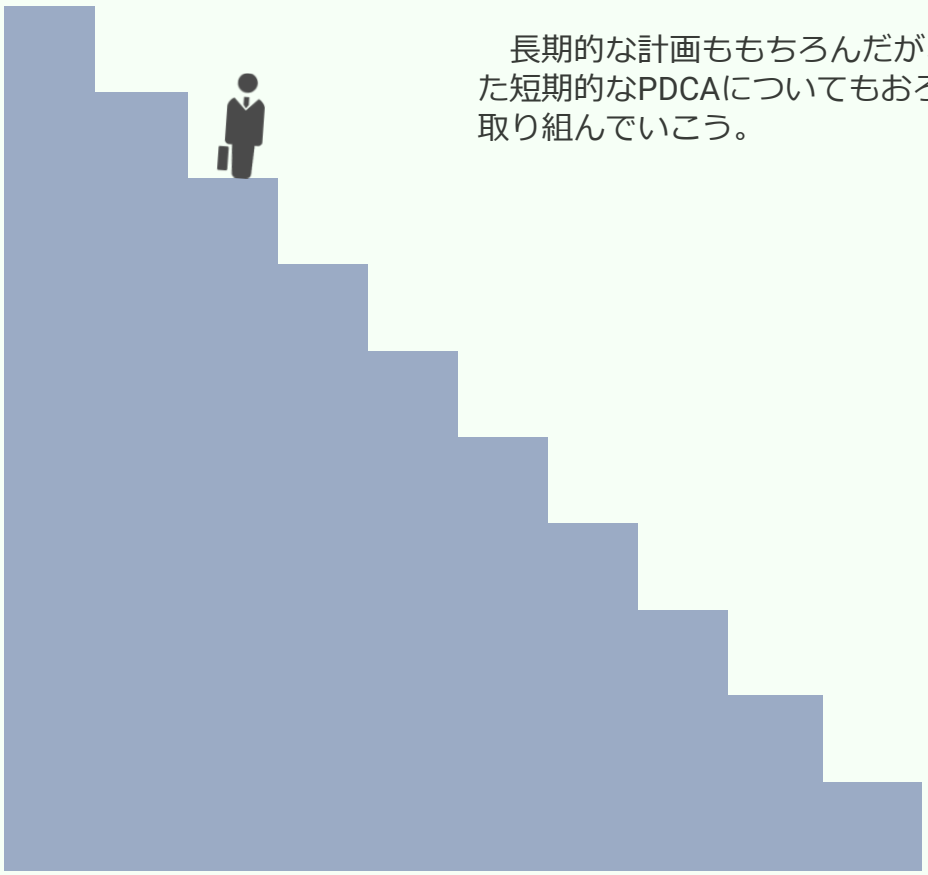
第９回

セミナー開催日：令和4年12月20日

動き出す
取り組む

資産を洗い出し、リスクを検討することができた。対応方針も決まり、リスクへの対応を行い始めている。この対応の質をいかに上げていくかが今後重要になりそうだ。

今までは、がむしゃらに取り組んできたように思う。PDCAという言葉は知っていたけれども、しっかりできていたかというとそんなことはないだろう。実際、いままで行ってきた教育も過去の習慣に従っていたというありさまだ。せっかくリスク検討もしてきたので、できることならばリスク対応に結びついた取り組みをしていきたい。



長期的な計画ももちろんだが、日々の動きを意識した短期的なPDCAについてもおろそかにしないように取り組んでいこう。

Day9

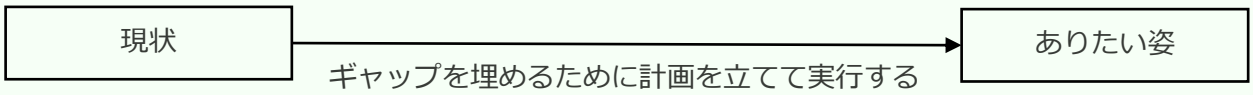
1.計画を作成する必要性とは

なぜ計画を作成するのか？

セキュリティの対策を計画していますか？行き当たりばったりで対策をしようとすると、対策が不十分になってしまうことがあります。きちんと計画を立ててセキュリティ対策を行いましょう。

Point① ありたい姿を実現するための計画策定

ありたい姿と現状のギャップをどのように埋めるかを考えていくことが計画です。計画策定することで道筋ははっきりするため、「次に何をすれば良いのか？」ということが少なくなります。



計画時に意識すること	
ゴール（ありたい姿）	体制（誰がこの計画を実行するか？）
目的（なぜこの計画を実行するか？）	予算（いくら投資して実行するか？）
対応するリスク（どのリスクが関係するか？）	スケジュール（いつまでに実行するか？）

計画を関係者で定期的に振り返り、「目的に沿った対応ができているか？」、「進捗に遅れはないか？」、「予算が上振れしていないか？」を確認することも重要です。

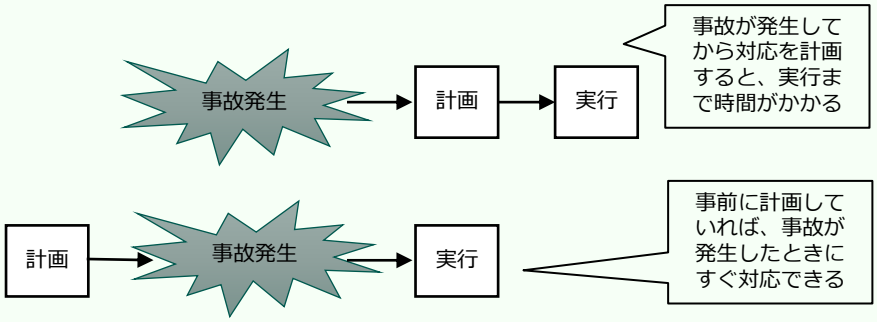
WBS（Work Breakdown Structure）などを活用する

WBSは、プロジェクト全体を詳細な作業に分割する手法です。プロジェクトのゴールを実現するために、必要な成果を階層的に詳細化し、必要な作業を配置していきます。

WBSのイメージ	
成果A	
作業A-1	
作業A-2	
作業A-2-1	
作業A-2-2	

Point② 不測の事態を想定して早めに計画

不測の事態というのは事業を運営していると必ずどこかで起こり得ます。これらを想定した計画に事業継続計画があります。そして、セキュリティ事故も不測の事態の一つです。事故が起こってから何をするのかを考えると対応が後手に回ります。事故を想定した計画を事前に作成することで、実行のスタートが早くなります。



Day9

1.計画を作成する必要性とは

方針と今後の目標を定める

セキュリティ基本方針を作成している企業は増えました。セキュリティ担当者はこの方針に従い、方針で謳われている内容を自社にとって最適な形で実施するために行動することが求められます。

Point① なぜセキュリティ対策を行うのか？

会社でセキュリティ対策を行う理由を明確に答えられますか？基本方針でよく見かける文章は、『株式会社○○○○（以下、当社）は、お客様からお預かりした（または当社の）情報資産を事故・災害・犯罪などの脅威から守り、お客様ならびに社会の信頼に応えるべく、以下の方針に基づき全社で情報セキュリティに取り組みます。』という内容です。

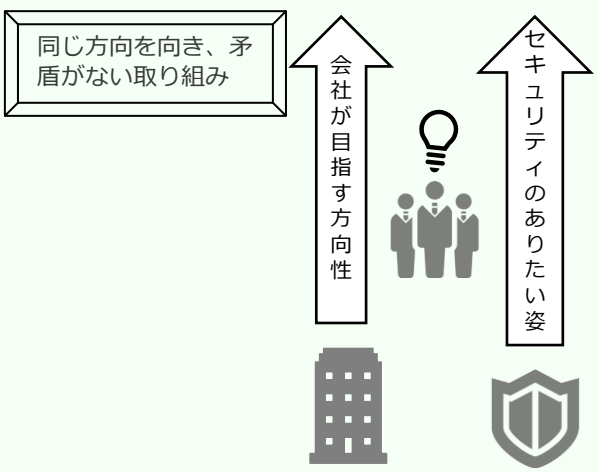
これらの文章を噛み砕いていくと、以下の取り組みが必要なことがわかります。

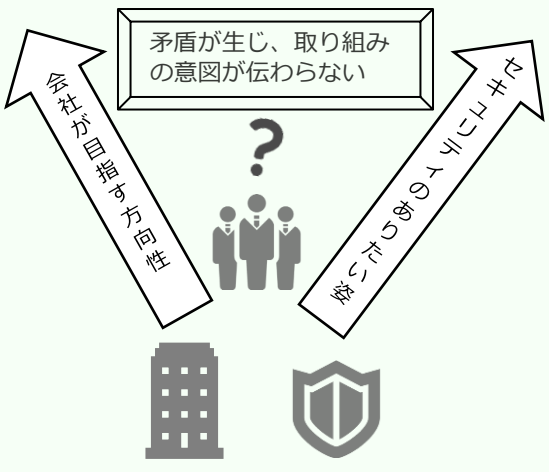
方針で謳われている求められる取り組みの例	
お客様からお預かりした（または当社の）情報	資産管理を行い、情報資産を把握する
事故・災害・犯罪などの脅威から守り	脅威・脆弱性の把握、リスク分析、対応方針の検討
お客様ならびに社会の信頼に応える	セキュリティ対策の実行

上記取り組みを実現するためには、以下の対応が必要となります。

取り組みを実現するために必要な対応の例	
体制の構築	役割を定義し、セキュリティにおける責任を明確にする
教育	従業員の教育、セキュリティ担当者への教育を行う
事故等への対応	セキュリティ事故を検知し、対応・復旧が行えるように準備をする
PDCAの循環	成熟度の向上のため、永続的に計画・実行・評価・改善を行う

では、これらは何のために実施しているのでしょうか？「事業を成長させるため」、「お客様に安心してもらうため」、「従業員が安全に働けるため」など各社により違いがあることでしょう。方針と一言で言わず、何のために実施しているのかを明確にしておくことで、各判断をする際に、悩むことが少なくなります。





会社が目指す方向とセキュリティの目指すありたい姿は、同じ方向である必要があります。これにより、リスクに対して自社に必要な適切な対策・対応をとることができます。方向性が合わないと、矛盾が生じ従業員が混乱することになります。

ミニワーク
～考えてみよう～

ミニワークテーマ

自社の現在の目標は何ですか？
なぜセキュリティを強化するのでしょう？

Day9

1.計画を作成する必要性とは

短期的なPDCAを行うための現状確認

組織の成熟度を上げるPDCAの中でも現状確認の重要性を説明しました。企業の全体像を把握し長期の計画を作る中ではCSFを用いた現状確認を行いました。Do（実行）の中で行う短期のPDCAでも現状を把握するところから考えることは重要です。

Point① アンケート調査による現状把握

従業員が普段どのように業務で情報資産を取り扱っているかなど、セキュリティ担当者の目からは見えない点を把握していきます。

アンケートの質問例
セキュリティの基本方針はどこに掲載されていますか？
セキュリティ規程やガイドラインはどこに保存されていますか？
ヒヤリハットや事故およびその疑惑がある場合にどこに連絡しますか？
会社のネットワークを業務以外に利用していませんか？
会社が定めるIT環境以外を業務で利用していませんか？

このようなアンケートを最初に取得することにより、従業員の理解が弱い点に対してアプローチしやすくなります。

また、Check（評価）でも同じようにアンケートをとることで、活動後にどのような変化があったかを把握することができます。そして、定期的（例えば月に１度）に実施することで、従業員が気をつけるべき点を繰り返し意識づけすることができます。

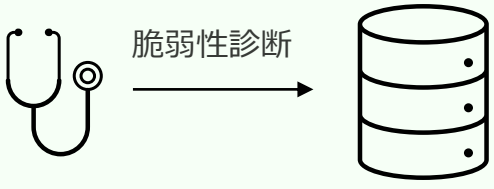
Point② テストによる理解度把握

従業員の理解度を測るためには、テストをするということも有効です。テストで点数が悪い点を重点的に補強することができます。JNSA（日本ネットワークセキュリティ協会)では情報セキュリティ理解度チェックを運営しています。これらを活用しセキュリティのテストを行うことも有効です。

出典：JNSA（日本ネットワークセキュリティ協会）
情報セキュリティ理解度チェック
https://slb.jnsa.org/slbm/

Point③ 脆弱性診断によるシステムの現状把握

脆弱性診断というサービスを活用することで、自社のシステムの弱点を調査してくれます。診断を受けて、自社システムの状態を把握することができ、システムの改修などを計画しやすくなります。



OSのバージョンが古く脆弱性などがあることを指摘

Day9

2.内部監査への対応

内部監査を計画する

ISO/IEC 27001（JIS Q 27001:2014）の要求事項では、「内部監査においては、ISMS の取組みが組織の規定した要求事項に従って実施されているか、 JIS Q 27001:2014 の要求事項に適合しているか、有効に実施され継続的に維持されているかを評価します。」と記載されています。 1年に一度程度で実施していくことで、あるべき姿への到達度やセキュリティの浸透度、ルールが守られているかを把握できます。

Point① 監査の特徴を理解し計画する

監査では「保証型」や「助言型」、「内部」や「外部」といった特徴が存在します。

保証型の監査	助言型の監査
組織が構築した情報セキュリティマネジメントの整備・運用状況が、監査結果を利用する者（委託元など）の期待する水準にあるか否かについて、独立かつ専門的な立場の監査人が、一定の基準に照らし、保証意見を表明する監査形態	組織が構築した情報セキュリティマネジメントの整備・運用状況について、独立かつ専門的な立場の監査人が、一定の基準に照らして不十分な点を検出し、必要に応じて検出事項に対応した改善提言を表明する監査形態

第一者監査（内部監査）	第二者監査（外部監査）	第三者監査（外部監査）
従業員または代理人（コンサル・専門家）が行う監査	利害関係のある団体またはその代理人により行われる監査	外部の独立した組織（審査会社など）が行う監査

出典：IPA（独立行政法人情報処理推進機構）
「セキュリティ評価の視点と他の評価方法との比較」をもとに作成
https://www.ipa.go.jp/security/benchmark/benchmark-hyouka.html
日本工業規格
「JIS Q 19011：2019 マネジメントシステム監査のための指針」をもとに作成

Point② 監査範囲（対象）と監査項目を選定する

監査の対象と項目を選定します。監査の目的や監査対象部門・業務が決まったら、目的を達成するためにどのような項目を確認すれば良いのかを検討します。

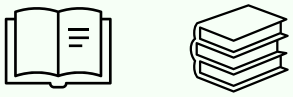
監査項目の例			
監査項目	監査基準	監査方法	対象組織（部門）
体制、権限、責任	情報セキュリティポリシー、規程	レビュー ヒアリング	セキュリティチーム
関係資料をレビューしセキュリティ責任者へのインタビューを行う。情報セキュリティ対策に係る権限、責任、連絡体制が文書の定める通りになっており、承認されているかを確認する。			
情報資産の保管	資産管理台帳	ヒアリング 視察	○○部門
資産管理台帳で定める資産の場所を対象業務部門へヒアリングを行い、実際に存在するかを確認する。また、その際に、資産管理台帳に記載がない資産たり得るものが存在しないかを確認する。			

この他にも、フロアレイアウトやシステムに関する項目も必要となる場合があります。ただし、監査項目の選定は悩むケースも多くなるため、初めはIPA（独立行政法人情報処理推進機構）が発表している、チェックリストや情報セキュリティ対策ベンチマーク（https://www.ipa.go.jp/security/benchmark/index.html）など外部のチェックリストを利用することも有効です。

内部監査を計画する

Point③ 監査方法を選定する

監査の方法を選定します。目的を達成するためにどのような方法を行っていくことが良いかを検討します。

査閲（レビュー）	質問（ヒアリング）
文書や記録等の監査資料を入手し、内容を確認する 	担当者等に質問し、状況を確認する 
観察（視察）	**チェックリスト**
業務を行っている場所や状況を見て確認する 	チェックリストへの回答から実態を確認する 

出典：一般財団法人 日本情報経済社会推進協会
「ISMSユーザーズガイド（情報セキュリティマネジメントシステム）」をもとに作成
日本工業規格
「JIS Q 19011：2019 マネジメントシステム監査のための指針」をもとに作成

Point④ 監査人を選定する

監査を行う人は、監査対象業務や部署と因果関係が無い人が望ましいです。また、以下のような資質を持つ人が監査をするとより効果が高い監査を行うことができます。自組織内にこのような人材がいない場合には、代理人として、コンサルタントや専門家が実施するという方法もあります。費用は掛かりますが、細かい点に気付き、是正策まで相談することが可能です。

監査人の要件	留意すること
独立・公正・誠実	• 監査人は、監査を客観的に実施するために、監査対象から独立している。監査の目的によっては、被監査主体と身分、密接な利害関係を有することがあってはならない。 • 監査人は、監査の実施にあたり、偏向を排し、常に公正かつ客観的に監査判断を行わなければならない。 • 監査人は、職業倫理に従い、正直に、かつ責任感をもって行わなければならない。
専門能力	• 監査人は、適切な教育と実務経験を通じて、専門職としての知識及び技能を保持しなければならない。
業務上の義務	• 監査人は、相当な注意をもって業務を実施しなければならない。 • 監査人は、監査の業務上知り得た秘密を正当な理由なく他に開示し、自らの利益のために利用してはならない。
品質管理	• 監査人は、監査結果の適正性を確保するために、適切な品質管理を行わなければならない

出典：一般財団法人 日本情報経済社会推進協会
「ISMSユーザーズガイド（情報セキュリティマネジメントシステム）」をもとに作成
日本工業規格
「JIS Q 19011：2019 マネジメントシステム監査のための指針」をもとに作成

Day9

2.内部監査への対応

内部監査を計画する

Point⑤ 監査の計画を作成する

監査を行う際の計画を作成します。監査計画では主に以下のような項目について検討を行います。

監査計画書の記載項目の例		
項目	内容	記載の例
監査目的	監査を実施する目的	セキュリティ規程の遵守の確認
監査テーマ	監査の具体的なテーマや重点監査事項	規程の理解度と実施方法を確認
監査範囲	監査対象の業務、情報システム等の範囲	○○に関する業務
被監査部門	監査の対象となる部門	○○部門
監査方法	監査で適用する監査技法	ヒアリング、文書調査
監査実施日程 または期間	監査の計画から報告までの日程 または実施期間	yyyy/mm/dd ~ yyyy/mm/dd
監査実施・ 管理体制	監査責任者・担当者	責任者：○○、担当：○○
監査項目	監査で確認する大項目	評価項目を作成し実施
適用基準	監査で適用する基準等	セキュリティ規程

通常では、これらの項目をまとめて、監査計画書を作成します。目的が慣例化しないようにすることに注意し、経営計画やリスクアセスメントの結果、年間計画を考慮した目的とすることが重要です。特にリスクアセスメントの結果を受けリスク対応を進めていく中で、計画通りに対応できているか、対策はリスクに有効に働いているかを把握する必要があります。

出典：一般財団法人 日本情報経済社会推進協会
「ISMSユーザーズガイド（情報セキュリティマネジメントシステム）」をもとに作成
日本工業規格
「JIS Q 19011：2019 マネジメントシステム監査のための指針」をもとに作成

Point⑥ 承認を得る

監査計画書として監査の内容が決まったら、承認を得て実施しましょう。セキュリティ責任者だけでなく、必要に応じて経営層の承認が必要な場合があります。経営層がセキュリティの必要性を理解していないと承認が得づらかったり、対象部門が協力してくれないといった問題が発生します。日頃のコミュニケーションが重要となります。

Point⑦ システムを確認する場合の注意点

対象として情報システムを確認する場合には、特に注意が必要です。技術にも理解がある人が実施する必要がありますが、情報システム部門を確認する場合には専門的な知識がないと適切な確認にならない場合があるからです。このような場合には内部だけで対応しようとせず、外部機関の利用を検討してください。

項目の例			
監査項目	基準	方法	対象組織（部門）
システムの監視	システム構成図 ネットワーク管理規程	レビュー ヒアリング、視察	情報システム部門
システム構成図をレビューし監視対象機器を確認、取得しているログの種類・保存期間のヒアリングを行い、視察にて実際ログが取得・保存されているかを確認する。			

このような場合には、各機器の役割や構成図を読み解く力、ログの違いや意味などを確認する人が理解しておく必要があります。また、保存されているログがレビューやヒアリングで聞いたログと一致していることを確認する必要があります。これらも技術的な理解が求められます。

Day9

2.内部監査への対応

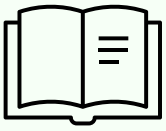
内部監査を実施する

計画の承認を得たら次は監査を実行していきます。定められた期間で定められた部署・業務を監査します。監査対応では、資料の確認なども行うため、対象部署には事前に連絡をし、資料などを用意しておいてもらうとスムーズです。

Point① 監査証拠をもとにした監査を実施

監査では、複数の資料や関連規程をもとに「何を行うのか」、「どのような方法で行っているのか？」、「本当に行っているのか？」などを確認していきます。

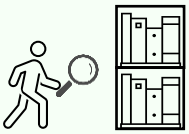
情報資産の管理についての監査の例



規程では、「資産管理台帳を作成し、対象の資産は定められた方法で管理する」という文面があるため、今回の監査で実施できているか確認する。

資産管理台帳があることを確認する。次に、資産管理台帳で記載されている資産の一覧を確認する。

インタビューで資産についてのヒアリングを行い、資産管理台帳に記載の通り管理されているか、日頃の運用の実態はどうなっているかを確認する。



実際に管理されている場所まで赴き、管理方法と管理の実態があっているかを確認する。

管理の記録を確認し、実際に管理が正しく行われていることの証拠とする。証拠は厳重に管理する。

Point② 監査の証拠となり得るかを慎重に判断する

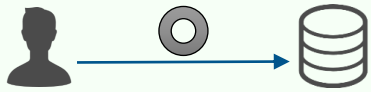
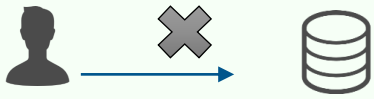
監査人が入手した資料・記録がそのまま証拠となるわけではありません。資料や記録の入手方法や入手時の状況等を加味して、証拠となり得るかを判断します。

資産管理台帳と資産が一致しない場合	定められた方法と実際の方法に乖離がある場合	記録と実態に乖離がある場合
このような場合は、資産管理台帳は資料として不十分という結果となり、指摘の対象となります。	このような場合は、手順に不備があります。手順を定めた資料は不十分となり、指摘の対象となります。	このような場合は、記録が不十分となります。正しく記録がされていないため、指摘の対象となります。

内部監査を実施する

Point③ システムの設定を確認する

文書や業務実態だけでなく、システムやシステムの運用についても確認を行う必要があります。システムを確認する際は、会社の基幹システムや事業を行うためのシステムなどについて、効率性・信頼性・安全性を客観的な視点に基づき評価する必要があります。

システムの確認の例	
アクセスが可能な場合	
	①アクセスを許可された人がアクセスすることができる。 ②アクセスのために認証の機能が有効になっている。 ③アクセスログが定められた期間記録されている。
アクセス不可の場合	
	①アクセスを許可されていない人はアクセスすることができない。 ②アクセスが試みられたログが定められた期間記録されている。

システムの確認では、実際に機器の設定や保存されているログが規程の定める通りになっているかを確認します。また、運用面として、作業方法などについても確認する場合があります。

機器の設定などが規程通りとなっていることを確認する

<主に確認すること>
- パスワードの強度が規程通りである。
- アクセス制御が規程通りである。
- ログの保存期間が規程通りである。
- リモートアクセスのタイムアウトが規程通りである。
- 保存期間を超えたログが保存されていない。
- アカウントは管理台帳に定める通りであり、用途不明なものは存在しない。

運用面が規程通りとなっていることを確認する

<主に確認すること>
- 作業をする際には承認された手順書を用いて作業が行われている。
- 作業をする際には複数名体制で実施している。
- 外部のものが作業をする際は、必要な権限のみを付与したアカウントを貸与して作業が行われている。
- 作業時のログを記録し、規程で定められた期間保存されている。

One Point

情報セキュリティに関する監査とは別に、システム監査というものがあります。システム監査基準では、「システム監査とは、専門性と客観性を備えたシステム監査人が、一定の基準に基づいて情報システムを総合的に点検・評価・検証をして、監査報告の利用者に情報システムのガバナンス、マネジメント、コントロールの適切性等に対する保証を与える、又は改善のための助言を行う監査の一類型である」と定めています。ただし、システム監査の目的は、「組織体の経営活動と業務活動の効果的かつ効率的な遂行および変革」、「組織体の目標達成に寄与」、「利害関係者に対する説明責任を果たすこと」とされており、必ずしもセキュリティに特化しているわけではありません。

出典：経済産業省
「システム監査基準」をもとに作成
https://www.meti.go.jp/policy/netsecurity/downloadfiles/system_kansa_h30.pdf

Day9

2.内部監査への対応

内部監査の結果をまとめる

監査終了後には、監査報告書を作成します。監査報告書を作成するに当たり、監査項目と監査した結果を吟味し、判断をする必要があります。監査報告書ではこれらを取りまとめます。

Point① 監査結果を分析する

監査報告書を取りまとめる際に、監査の結果について検討を行います。業務の実態や集めた証拠、証拠の有効性を総合的に判断して、監査項目に対して適切な状態かを判断します。

1. 関連書類の閲覧及び査閲、担当者へのヒアリング、現場への往査及び視察、システムテストへの立会、テストデータによる検証及び跡付け、脆弱性スキャン、システム侵入テストなどの方法を通じて入手された監査書類について、入手源泉及び入手時の状況等を勘案して、監査証拠として採用するか否か、それが有する信用性及び証明力の程度を慎重に判断

2. 入手した監査証拠の必要性と十分性の判断に当たって、監査対象者（部門）から提出された資料、監査人自ら入手した資料、監査人自ら行ったテスト結果等を総合的に勘案して、相互に矛盾があるか否か、異常性を示す兆候があるか否かを評価

3. 採用している対策・取り組みが適切であるか否かの判断は、リスクに応じたものでなければならないため、監査人が入手した監査証拠の評価に当たっては、リスクアセスメントの結果との関連づけを考慮

Point② 監査報告書の作成

監査報告書では、以下のような項目について取りまとめを行います。詳細な監査結果や補足資料等がある場合は、監査報告書の添付資料とする場合もあります。

項目	内容
監査実施者	監査を実施した責任者・担当者
監査目的	監査を行う目的
監査実施期間	監査の計画から報告までの期間
監査対象	監査の対象とした部門や業務
監査方法	監査で適用した監査技法
適用基準	監査で適用した基準等
監査項目	監査で確認した大項目
監査結果概要（総括）	監査結果の総括
検出事項	監査で検出された事項（評価できる事項を含む）
指摘事項	監査結果に基づき、問題点として指摘する事項
改善提言	指摘事項を踏まえて、改善すべき事項（緊急改善事項、一般的改善事項）
特記事項	その他記載すべき事項

指摘事項及び改善提言が多い場合には、別紙としてまとめます。指摘事項及び改善提言では、それぞれ重要性が高いものから記載し、指摘事項と改善提言の対応関係が明らかとなるよう工夫されることが望ましいです。また、改善提言を行う場合には、緊急性のある改善提言を要緊急改善提言とし、その他の改善提言と分けて記載することが有益です。

出典：一般財団法人 日本情報経済社会推進協会
「ISMSユーザーズガイド（情報セキュリティマネジメントシステム）」をもとに作成
日本工業規格
「JIS Q 19011：2019 マネジメントシステム監査のための指針」をもとに作成

Day9

2.内部監査への対応

改善を行う

監査結果の取りまとめと並行して、指摘事項がある場合には、改善を行う必要があります。また、PDCAの観点では、改善実施後あらためて確認を行うと効果が高まります。

Point① 結果の報告をする

監査報告書がまとまったら、依頼者に対して報告会などを開催し、監査の結果を報告します。それだけでなく、監査対象部門や対象業務従事者に対しても報告会を開催し、監査結果を説明することもセキュリティ意識を高めるためには有益です。報告会では、次の事項を意識し説明します。

監査証拠の取得方法	監査の方法	監査後の活動
監査の証拠として得た情報は、違法な方法で取得した情報ではなく、正当な入手方法により入手したサンプルであること。	監査報告書に従い、一連の監査の流れや目的・監査手段・期間などを明確にする。	監査の結果を受けた指摘事項と改善方法を説明し、今後どのような是正策を行うのかを説明する。

指摘事項の説明だけではなく、監査対象部門において、優れた実践活動が認められる場合は、報告会で評価することが望ましいです。

出典：一般財団法人 日本情報経済社会推進協会
「ISMSユーザーズガイド（情報セキュリティマネジメントシステム）」をもとに作成
日本工業規格
「JIS Q 19011：2019 マネジメントシステム監査のための指針」をもとに作成

Point② 指摘事項に対して対応する

指摘事項があった場合には、改善を行う必要があります。助言型監査の場合には、監査担当者が指摘事項に対応した改善案を提示し報告書や報告会で共有します。また、改善策を監査対象部門で検討し実施するという方法があります。ただしこの場合には、対策が有効であるかを有識者が確認する必要があります。

指摘事項と改善提言の例	
指摘事項例	改善提言例
権限、責任、連絡体制の項目において、連絡体制に部署異動した人が記載されていたため、権限を有する適切な人員に連絡が取れない。	連絡体制図を見直し、更新を行う。
資産管理台帳には、鍵のかかるキャビネット保管となっていた資料が鍵がかからないキャビネットに保管されているため、保管場所の変更が必要。	鍵のかかるキャビネットを用意し、施錠をした上で保管する。また、併せて鍵の保管等についてもルールを明確にする。
システムへの作業承認が得られておらず、作業の手順が不明瞭なまま設定変更作業が行われている。	作業手順を明確にし、手順書通りの作業を行うことをルールに定める。また、承認履歴を確実に残し、作業ログの保管を行い、定期的に実施状況の確認を行うルールへ変更する。

ミニワーク
～考えてみよう～

ミニワークテーマ

内部監査を進めるための計画書を考えてみましょう。
もし、自社で内部監査を行うとしたらどのような計画を立てれば良いか、下の監査計画の空欄を埋めながら考えましょう。

監査計画書の記載項目の例		
項目	内容	計画案
監査目的	監査を実施する目的	
監査テーマ	監査の具体的なテーマや重点監査事項	
監査範囲	監査対象の業務、情報システム等の範囲	
被監査部門	監査の対象となる部門	
監査方法	監査で適用する監査技法	
監査実施日程 または期間	監査の計画から報告までの日程 または実施期間	
監査実施・ 管理体制	監査責任者・担当者	
監査項目	監査で確認する大項目	
適用基準	監査で適用する基準等	

Day9

3.教育への対応

教育計画を作成する

セキュリティの重要な取り組みの一つに、教育があります。各種対策を行なっても、日々の業務の中で人による間違いや認識違いといったことが起こり得ます。これらを起こさないために、セキュリティ対策への理解を深め、組織の人員の意識を高めることが求められます。

Point① 教育タイミングの検討

教育を行う際には、どのタイミングで行うかが重要なポイントです。効果的に理解度を上げていくためにも、適切なタイミングはいつなのかを考えましょう。また、繁忙期を避けるなど、参加しやすいタイミングを考慮することも必要です。

教育タイミングの例	
タイミング	実施内容
入社時	新卒・中途に関わらず社員が入社した際に行います。一般的には会社のルールや業務内容の説明などと一緒に行うケースが多いです。入社時研修では適度な緊張感もあり、基本ルールを習得させるには最適です。細かい点は配属後でも良いですが、会社全体の「やらなければならないこと」と「やってはいけないこと」を明確に指導します。
部署・業務異動時	部署や業務が変わると取り扱う情報資産も変わることがあります。情報資産ごとにその価値と取り扱いルールを徹底させるため、部署異動や業務変化が発生した際には教育が必要です。この場合は部門内での教育とすることもできます。外部とやり取りをすることが多い部署・業務の場合、応対の仕方や問い合わせへの受け答え方なども指導します。
昇進 役割変更時	今までと立場が変わるので、セキュリティに対して求められる責任が変化します。 役割や責任と権限などがどのように変わったのかを理解させるために指導します。
期初、期末 四半期毎など	会社の区切りの時期は目標などの基本姿勢を再認識させるのに最適です。期初にはスローガンや目標・計画などを元に教育を行い、期末であれば振り返りを行います。
定例・定期	日常において日々意識をつけるため、定例会や定期勉強会などを行います。ただし、毎回同じ内容を繰り返すと形骸化するため、内容の変更など行いながら実施します。

Point② 教育内容の検討

何を教育するのが良いかを検討します。これはリスクアセスメントなどの結果、内部監査やヒヤリハットなどの状態から教育内容の検討を行う必要があります。

教育内容の例	
方針や関係規程の周知を目的とした教育	脅威と対策に関する教育
• 求められる役割とその役割で行うべき対応 • 資産管理台帳を元にした資産の取り扱い方 • 機密情報や個人情報の取り扱い注意事項 • 情報やパソコンの持ち出し方および注意事項 • ソフトウェアインストールのルールや注意事項 • 遵守事項、禁止事項、推奨事項の理解 • 守らなかった場合の対応について	• ウイルス感染した場合の影響などの理解 • 感染経路など注意点の理解 • メール利用時の注意事項 **インシデントや緊急時の対応に関する教育** • 事故発生時のフローの理解 • 事故発生時の対応訓練

教育計画を作成する

Point③ 教育対象者を定める

教育を誰に対して行うかは内容と合わせて考える必要があります。教育が必要な人は誰なのかを明確にして実施することで効果が高まります。

全社員	特定の社員	セキュリティ担当者
会社のルールなどを教育するときは全社員が対象となります。また、目標や振り返りなども全社員が理解できるように取り組みましょう。	入社や異動・昇格では特定社員のみが対象となります。対象者の属性を整理し誰に対して行うのかを明確にする必要があります。	セキュリティ担当者としてセキュリティの理解を上げるための教育を実施します。チーム内の勉強会や外部のセミナー受講などを行います。

Point④ 適切な教育方法を検討する

教育内容、教育対象者が決まったら教育方法を検討します。求める理解度や受講のしやすさなどを考慮して検討します。

方針や関係規程の周知を目的とした教育	脅威と対策に関する教育	インシデントや緊急時の対応に関する教育
講義やe-learningで教育を行います。また、時間が取れない場合には、規程を読むという方法もあります。理解度を把握するためにはテストなどを行います。	講義やe-learningという方法だけでなく、デモンストレーションなど実際に確認・体験する方法も有効です。実際に体験することで理解度が上がり、意識が向上します。	インシデント対応の模擬訓練などが効果的です。標的型メール訓練では開封時にエスカレーションまで実施するなどをします。セキュリティ担当者が初動対応まで実施するとより効果が得られます。

Point⑤ 教育の計画を作成する

教育を行う際の計画では主に以下のような項目について検討を行います。

教育計画書の記載項目の例		
項目	内容	記載の例
目的	教育をする目的 長期的なPDCAに影響	メールからのウイルス感染リスクを軽減する
目標	数値で置けるような目標 短期的なPDCAに影響	開封率10%以下 開封者のエスカレーション100%
スケジュール	教育の実施期間	yyyy/mm/dd ~ yyyy/mm/dd
講師の調整	講義形式などの場合の講師	今回は講師なし
コンテンツ・内容	主な研修の内容	標的型メール訓練サービスを利用
開催方法	開催方法	yyyy/mm/ddに訓練メール配信
評価方法	到達度の評価方法	開封に伴うシステムログ、エスカレーション記録

計画書は責任者、経営層により承認されて実行します。また、今回の例のように予算が必要な場合には余裕を持って計画を作成しましょう。

Day9

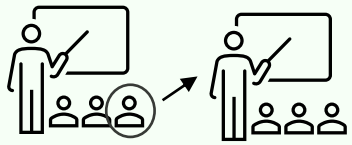
3.教育への対応

従業員のセキュリティレベルを高める

従業員のセキュリティを高めるためには、教育や訓練をすることが重要です。まとめて実施するようなケースもあれば、日々の情報共有からセキュリティの意識を高めることも可能です。

Point① 研修の方法を工夫し効果を高める

教育の方法は計画書作成の段階で検討されます。効果を高めるため、最善の方法を検討する必要があります。その中で工夫し、より高い効果を狙います。

セキュリティ教育の例
セキュリティ担当者が全従業員に教育を行うのではなく、一部の受講者（部門管理者など）に行います。講義を受講した人が部門内で講義を行うことで、部門管理者の理解を高めるとともに、部門特有のセキュリティなどに特化した話ができ、理解度が高まりやすくなります。  受講者が部門に持ち帰り講師を行う

Point② テストを行い理解度を把握する

セキュリティ教育の理解度を把握する方法として、テストが広く利用されています。集合型、e-learningなどでは、教育して終わりではなく、テストをするなどして理解度を把握しましょう。

理解度テストの例	
テスト問題の例	回答方法の例
自社のヒヤリハット件数で一番多いのは誤送信である。	○ or ×方式での回答
事故の可能性がある際の正しい連絡先はどこか？	選択問題（４択程度）
なぜセキュリティに取り組むのか？	記述式回答にて回答

テストには、現状を把握する目的で行うテストと教育の理解度を把握するために行われるテストの２種類が存在します。どちらの目的でテストを行うかを意識し、問題を設定することが重要です。現状を把握する目的で行うテストでは、全般的に広く出題することや世間とのレベルの乖離などを把握するため、市販の問題を利用することも有効です。反面、教育の理解度を把握する場合には、教育内容に即した問題を出題する必要があり、自社で作成する方が目的に沿っていると言えます。

Point③ プラスセキュリティ人材を育成する

セキュリティ担当者だけでなく、デジタル部門や事業部門・管理部門等においてセキュリティを意識し、業務遂行に伴うセキュリティ対策の実施に必要な能力を備える人材の確保や育成も重要です。DXなどを進めるに当たり、事業部門でシステム開発やリスクアセスメントを行うような人材の場合、セキュリティに関する意識を養い、対策の実施に求められる知識・スキルを積極的に身につけてもらう必要があります。自らの業務遂行にあたってセキュリティを意識し、必要かつ十分なセキュリティ対策を実現できる能力を身につけること、あるいは身につけている状態のことを、「プラスセキュリティ」と定義されています。

従業員のリテラシーを高めるだけでなく、主たる業務を持ちながらセキュリティの取り組みに協力し、スキルや知識を持った「プラスセキュリティ」人材を育成していくことも重要です。

出典：経済産業省
「サイバーセキュリティ体制構築・人材確保の手引き」をもとに作成
https://www.meti.go.jp/policy/netsecurity/tebikihontai2.pdf

従業員のセキュリティレベルを高める

Point④ セキュリティ担当者が教育を行う

従業員の教育を行う場合には、セキュリティ担当者が講師として教育を行うケースも珍しくありません。より効果的に従業員を教育するためにはどのような点に気をつければ良いのでしょうか？

STEP 1

■ 教育の目的と目標の明確化

- 教育・訓練の対象範囲を設定する
- どのような課題を解決するための教育なのかを具体的に示す
- 何が実現すれば今回の教育が成功したと言えるかを定める

STEP 2

■ 教育実施方法の明確化

- 教育内容・利用コンテンツ・テキストを具体的に示す
- 時間配分と時間内で行うことを具体的に示す

STEP１・２は主に計画書で定めておく内容です。ただし、STEP２の利用コンテンツやテキストなどは計画後に定めても問題はありません。また、時間配分等はテキストなどが決まった後に考えていきます。

STEP 3

■ 教育の周知

- 教育内容・方法に合わせて対象者に周知する
- 参加できない場合のフォローを案内する
- 参加率を上げるために、リマインドなどの工夫をする

教育の場があることを周知します。シフトなどで業務調整が必要な場合には１ヶ月程度前から周知しておくことが望ましいと言えます。

STEP 4

■ 教育の実施

- 計画に基づき実施する
- 聞かせるだけでなく、考えさせる工夫をする
  計画はSTEP２で決めておきますが、実際に講義形式で行う場合には、時間いっぱい聞いてもらうだけでは知識として定着しません。周りの人と会話をしてもらう、グループワークをするなど、声に出す・体験する・考えるといった動きを講義内に盛り込むことで理解度が上がります。

- テストとアンケートをする
  理解度を図るためのテストを行うだけでなく、講師の話し方、テキストの内容などについてアンケートを取得すると、次回のコンテンツに対しての検討材料となります。

教育を行います。従業員が多い場合には複数回に分けて行い参加率を高めます。従業員が従業員に教育をする場合には、受講者に緊張感を持ってもらうことが重要です。教育前に経営層から一言もらうなどの方法があります。

STEP 5

■ 不参加者へのフォロー

- フォローアップで教育を行う
- 個人対応してもらいテストを実施する

不参加者が出ることも想定して計画を考えることが重要です。特に連続して不参加の人は個別フォローするなどの対応をしましょう。

Day9

3.教育への対応

担当者のセキュリティスキルを高める

会社のセキュリティの取り組みを推進するセキュリティ担当者がスキルを高め成長していくことは、非常に重要な施策となります。セキュリティ担当者こそ積極的にセキュリティ教育に参加していきましょう。

Point① 担当者に求められるスキルや知識を把握する

担当者の役割として、求められるスキルや知識を把握しましょう。サイバーセキュリティ体制構築・人材確保の手引きでは、各分野に求められる知識・スキルの概観をまとめています。また、巻末には、活用可能な試験・資格の例も記載されています。資格取得を目指すこともスキルを高めます。

【注釈】
※1「◎」は主導できるレベル（情報処理安全確保支援士試験レベル）、「○」はコミュニケーションが取れるレベル（情報セキュリティマネジメント試験レベル）を想定。
※2 企業等によって、「◎」、「○」の付し方の変更や、知識・スキル項目の追加・削除・詳細化が必要。
※3 分野に固有のタスクを実施するための知識・スキルについては含まれていない。

	分野	セキュリティ関連知識・スキル（大項目）		
		セキュリティマネジメント	システムセキュリティ	セキュリティオペレーション
戦略マネジメント層	経営リスクマネジメント	○		
	法務			
	システム監査			
	事業ドメイン（戦略・企画）			
	セキュリティ統括	◎	○	○
	セキュリティ監査			
	デジタルシステムストラテジー			
実務者・技術者層	デジタルシステムアーキテクチャ	○	◎	○
	デジタルプロダクト開発			
	脆弱性診断・ペネトレーションテスト	○	◎	◎
	セキュリティ監視・運用			
	セキュリティ調査分析・研究開発			
	デジタルプロダクト運用		○	○
	事業ドメイン（生産現場・店舗管理）			○

区分については以下を想定し、知識・スキルの詳細については各シラバスが参考になります。
「◎」；主導できるレベル（情報処理安全確保支援士試験レベル）
https://www.jitec.ipa.go.jp/1_13download/syllabus_sc_ver2_0.pdf
「○」；コミュニケーションを取れるレベル（情報セキュリティマネジメント試験レベル）
https://www.jitec.ipa.go.jp/1_13download/syllabus_sg_ver3_3.pdf

出典：経済産業省
「サイバーセキュリティ体制構築・人材確保の手引き」をもとに作成
https://www.meti.go.jp/policy/netsecurity/tebikihontai2.pdf

Point② 担当者自身の得意・不得意を理解する

セキュリティの業務は非常に幅広く、全てを完璧に行うということは非現実的です。自分の得意不得意を意識し、不得意な点をどのようにカバーし対応していくのかを考えることが重要です。

得意・不得意を把握する

普段の業務の中で把握	診断やテストで把握	フィードバックで把握
好き/嫌い/得意/苦手という気持ちがあると思います。これらを整理し、得意不得意を整理していきます。	市販の能力診断やテストを行い把握します。数値やグラフで把握できるものも多いため、視覚的に確認ができます。	フィードバックで把握します。上長との面談などを通して、自身の強みや弱みを把握することができます。

スキルアップを目指し取り組む

得意な点を伸ばす	できることの幅を広げる	不得意な点を勉強
得意な点に磨きをかけ、スキルを向上させます。関係する知識なども高めることが期待できます。	まだやったことが無い業務に挑戦することでスキルアップを図ります。	不得意な点を克服し、成長に繋げていきます。

担当者のセキュリティスキルを高める

Point③ メンバー・後任を育成する

セキュリティ関連の業務を責任者の立場で取り組む場合には、セキュリティ組織・チームが永続的に活動できるようにすることも重要です。メンバーや担当者の育成や次世代を担う人材の育成にも力を入れる必要があります。

計画
短期的なPDCAとして、人材育成計画を作成します。（組織の成熟度とセットで考える場合には、長期的なPDCAの一環として考える場合もあります。）計画では、組織・チームの強みや弱み、自社で行う業務・役割、求められるスキル、現在のメンバー・担当者の能力を把握し計画を取りまとめます。
実行
計画に基づき育成の取り組みを実行します。セキュリティ組織・チーム内での勉強会や外部セミナーの受講、研修への参加などを行っていきます。参加がしやすい雰囲気作りや業務調整も必要です。また、初めて経験する業務に挑戦させるという方法もあります。業務経験を積むことで担当者としての成長を促します。
評価
参加者がどの程度成長しているかを定期的に評価します。業務と連動させる場合には四半期ごとなどに面談等を行うことで評価することも有効です。セミナー参加などをする場合には参加レポートを書くなどしアウトプットを行う、勉強会などで講師を担当するなどの方法から評価を行うこともできます。
改善
担当者の成長具合に合わせて業務内容などを見直していきます。また、必要であればキャリアの希望などもしっかりと把握をすることが望ましいです。本人の希望するキャリアや業務を担当することでモチベーションが上がり、成長スピードも高まります。

One Point

セキュリティの業務に携わる人員を育てたら辞めてしまった、というエピソードを聞くことがあります。辞めた理由としては、セキュリティ業務の経験を活かした転職であったり、セキュリティ以外の業務をしたいといった理由があります。せっかく育ったセキュリティ担当者がいなくなるというのは、育成していた側からすると虚無感にも似た感情を抱くのではないでしょうか？

兼務で行っている場合には、しっかりと評価をする仕組みが必要となる場合があります。例えば、給与や賞与への反映なども検討します。また、兼務であるために本来の業務が疎かになることに対して、不利な評価をされないようにすることも重要です。

専任の組織やチームで取り組んでいる場合には、評価制度などは整っているケースが多いように感じています。しかしながら、専任であるがゆえにキャリアパスの幅が狭いことや日々の業務内容が変わらずに、将来に不安を感じるといった話もよく聞きます。組織が成熟していく中で、できることを増やしていくことも重要です。

転職などが一般的となっている今日において、人材の流出を防ぐことは現実的ではありません。常に人を育てていく環境、正しい評価ができる仕組みを作っていくことが重要です。

Day9

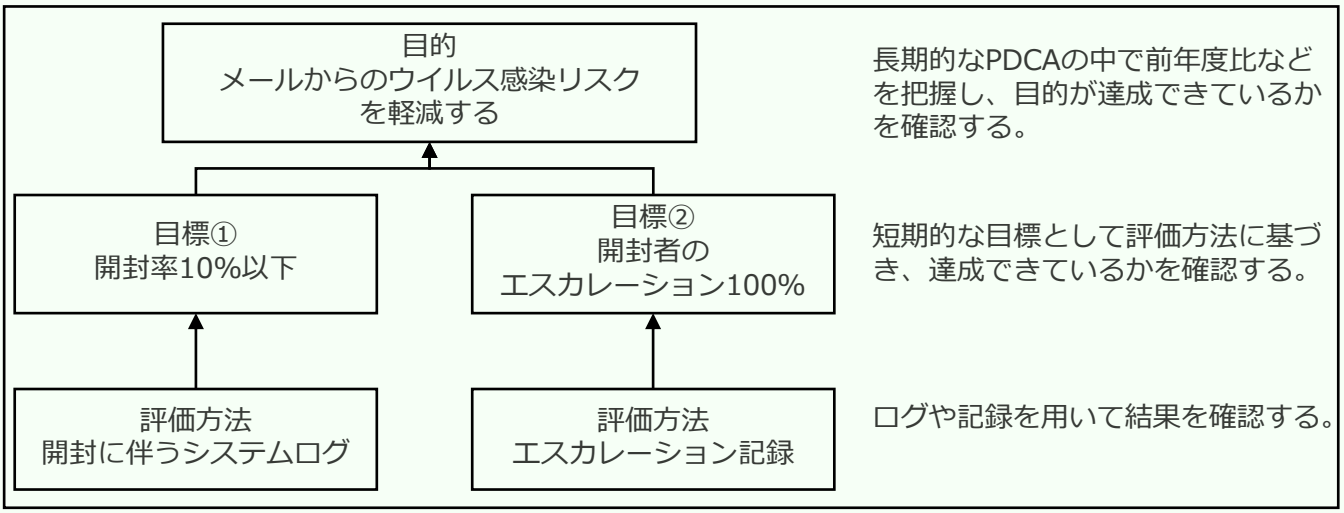
3.教育への対応

継続的な教育に向けて

継続的に成長をしていくためには、振り返りは欠かせない行動です。計画から実行の結果を振り返り、発生した問題点や良かった点と向き合うことで、次の取り組みをより良くします。

Point① 計画に対しての振り返りを行う

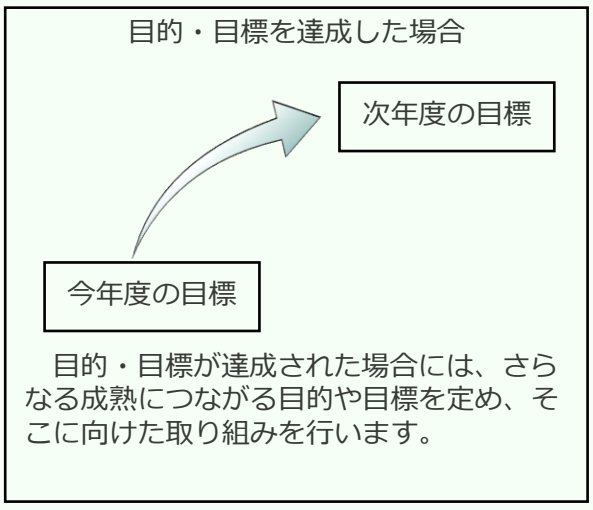
計画の振り返りを行う際に重要なことは、目的が達成できたかです。計画では、目的を達成するために必要な目標をたて、目標達成をどのような方法で評価するかを定めています。教育終了後、必要な記録を集めて評価を行います。



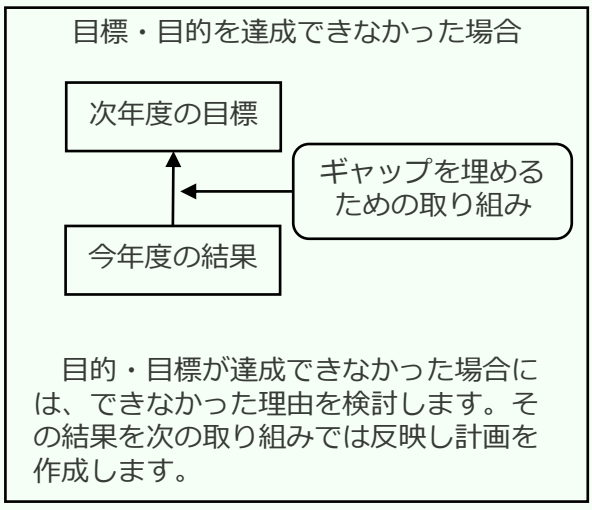
目的や目標の達成がどの程度できたかを数値で置くことは重要です。それだけでなく、良かったこと、うまくいったことも把握することで取り組みが前向きな活動となります。

Point② 評価を次の計画に反映する

評価は次の結果に反映します。目標や目的が達成できた場合には次の到達点を目指して、うまくいかなかった場合にはその理由を考えて検討を行います。



目的・目標が達成された場合には、さらなる成熟につながる目的や目標を定め、そこに向けた取り組みを行います。



目的・目標が達成できなかった場合には、できなかった理由を検討します。その結果を次の取り組みでは反映し計画を作成します。

規程が変わったような場合には、全従業員へ説明が必要です。このような場合に欠席者がでるようなら、個別に時間を調整するなどし、確実に実施します。

ミニワーク
～考えてみよう～

ミニワークテーマ

今年の計画はどのようなものでしたか？
現時点でどのような評価を行いますか？

Day9

4.年間計画への対応

年間計画を作成する

内部監査や教育について説明を行ってきました。これらを定期的に繰り返していくことでPDCAが循環し、成熟度向上につながります。取り組みをより有意義にするためには、年間計画などを作成し、実施していくことが重要となります。

Point① 年間計画で意識すること

情報セキュリティを向上させるために必要な要素を洗い出し、計画を立てていきます。年間である一定期間だけ意識するものもあれば、毎日意識をするべき項目もあります。

1年間の運用の中で実施していくべき事項	
実施項目	主な内容
組織の状況を理解する	自社の資源（ヒト、モノ、カネ）や、その他の課題・リスク、顧客や株主などから求められているものといった、自分たちの組織について理解する。 参考テキスト：第1回、第8回（主に、組織の成熟度を高める）
リスクアセスメント	資産管理台帳を更新し、潜在するリスクやリスクが顕在化した時の影響の洗い出しを行う。 参考テキスト：第4回、第5回
リスク対応計画	重要な情報資産など対応が必要なものを洗い出し、リスク対応計画を策定し管理する。 参考テキスト：第6回、第7回、第8回（主に、組織・人・物理対策）
目的目標を管理する	運用のゴールとして設定する目標を決めて、スケジュールごとなどで達成までの活動を追って管理できるようにする。 参考テキスト：第2回、第8回（主に、組織の成熟度を高める）
教育	定期的な教育の実施などで自社のルールを浸透させ、従業員に理解させる。 併せてセキュリティの担当者の教育を行う。 参考テキスト：第9回
内部監査	規程で定める通りに運用ができているか、漏れている運用はないか、もっと改善すべきことはないかを自社で確認する。 リスクアセスメントの結果、対応計画が進んでいるかを確認する。 参考テキスト：第9回
改善	日頃の活動や内部監査を受けて改善点が出てきた場合には、対応を行い、再発防止に努める。 参考テキスト：第9回

ISMS認証では上記に加えて、マネジメントレビュー（活動の結果や関係者からのフィードバックを組織のトップへ行い、適切に運用されているか判断を仰ぐこと）や事業継続計画（何らかの事態が発生した際に企業活動を継続・復旧するための計画）なども含まれます。

こんな事例も

年間計画を初めて作る際に、何から行うか悩んでしまうという人は多いのではないでしょうか？PDCAのサイクルで計画を意識するあまり、計画に必要な情報が不足するという問題が立ちはだかります。計画作成に必要な情報を集めるため、Check（評価）を最初にするという企業も存在します。最初に自社の評価をすることで、実態を把握してから計画を立て始めます。公開されているチェックシートを利用したり、社内にある文書類を確認したりと簡単な評価から行い、計画を作成していきます。2年目（PDCA２周目）からは計画、実行、評価、改善のサイクルの中で計画を見直し理想の姿に近づいていきます。

Day9

4.年間計画への対応

年間計画を作成する

Point② 自社にあった年間計画を作成する

年間計画を作成する際には、自社の会計年度や繁忙期との調整、入社や人事異動のタイミングなどを考慮しないと、忙しくてできなかったなどの結果に陥ります。

年間計画の例①												
項目	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
全般	★新入社員入社、人事異動					★繁忙期		★次期予算確定				
組織の状況理解	★資源の確認、必要な資源の用意											
リスクアセスメント	★資産管理台帳更新、リスクアセスメント											
リスク対応計画	★リスク対応方針検討　★対策の導入											
目的目標管理	★年間計画始動					★次期計画検討・予算獲得				★次期計画作成		
教育	★新入社員教育	★担当教育		★従業員教育計画		★従業員教育		★新入社員教育計画				
内部監査							★内部監査計画	★内部監査				
改善	日々必要な改善を実施											
日々の取り組み	チェックリストの運用、ログ等の記録の確認、ヒヤリハットへの対応、情報収集　など											

年間計画の例①は、4月に新入社員が入社し人事異動等が多くなるパターンを記載しました。繁忙期は上期と下期が分かれる9月頃となります。そのため、参加率を高めたい教育などは繁忙期後に実施します。同じ理由で協力が必要となる内部監査も繁忙期を外して実施します。ただし、次期年間計画作成を年明けから始めたいため、年内で内部監査を終えられるように調整しています。この計画の改善点としては、予算確定と次期計画作成の時期があっていないことです。先に予算が決まるため、予算ありきの計画になりがちです。計画に応じて後にあらためて予算を振り分けることや、追加予算獲得が必要となります。

年間計画の例②												
項目	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
全般	★繁忙期											★繁忙期
組織の状況理解	★資源の確認、必要な資源の用意											
リスクアセスメント	★資産管理台帳更新、リスクアセスメント											
リスク対応計画	★リスク対応方針検討　★対策の導入											
目的目標管理	★年間計画始動								★次期計画作成	★必要予算確定		
教育	★担当教育							★従業員教育計画	★従業員教育			
内部監査	★内部監査計画　★内部監査											
改善	日々必要な改善を実施											
日々の取り組み	チェックリストの運用、ログ等の記録の確認、ヒヤリハットへの対応、情報収集　など											

年間計画の例②は、毎年新入社員が入ってこないため、新入社員教育は年間計画には盛り込んでいません。また、3月から4月が繁忙期となるため、スタートも繁忙期終了後からとなりますが、従業員教育を繁忙期前に行い、意識を高める工夫をしています。今回の例では予算執行は都度承認を得ることとし、計画を作成し、必要な予算を確認ができるようになりました。必要な予算を事前に獲得しておく例①と比べると実態に合わせた計画を推進できますが、予算執行の承認が取れないと計画が実行できないという弱点があります。

Day9

4.年間計画への対応

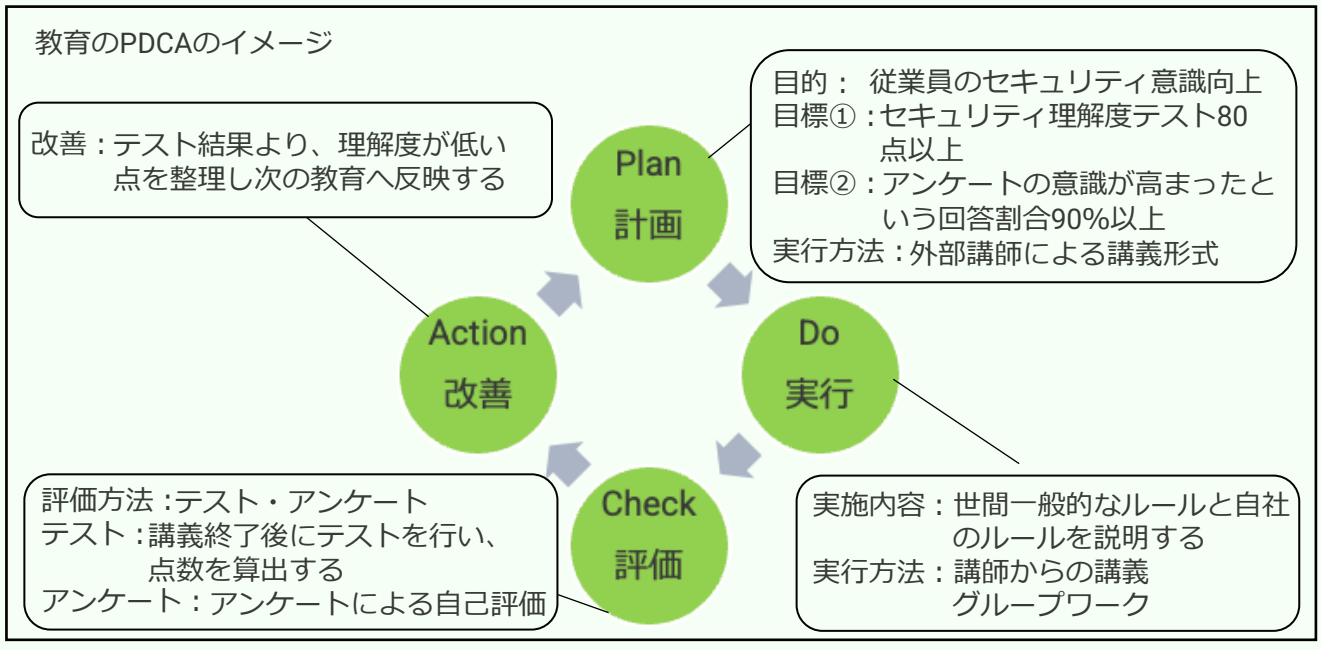
成り行き任せから計画的PDCAへ

「セキュリティは重要だと思っている。基本方針などはIPAのサンプルをもとに作った。でも、次に何をやれば良いのかわからない。」という企業は多いのではないでしょうか？A社では、セキュリティを考える中で、「こんな製品が流行っているらしい」、「無償でこんな教育が受けられるらしい」という情報の中からできることを選んでセキュリティ対策を進めてきました。

初めは製品を入れたり、ルールを作ってみたりと、セキュリティの意識や対策も前に進んでいるように感じていました。実際、従業員もセキュリティの意識が高まり、セキュリティ事故を起こさないようにしようとする行動などもできていたように感じます。初めは良かったのですが、段々と次に何をすればよいのか悩むことも多くなり、従業員の意識も低下しているように担当者は感じていました。

どうすればよいか考えたセキュリティの担当者は、行き当たりばったりで取り組んでいたセキュリティを、PDCAを意識したセキュリティの取り組みへ変革していくことにしました。とはいうものの、長期的なPDCAを考えられるほど担当者のレベルも成熟していなかったため、最初に短期的なPDCAから取り組みました。特に従業員の意識低下という問題を強く感じていたため、まずは教育面から短期のPDCAを回してみることにしました。

従業員の意識はどのようにしたら上がるのか？この問いに対して、答えとなるような教育計画を作成することから始めました。実際の教育では外部から講師を招聘する事で、普段とは違う雰囲気の中で従業員に緊張感を持たせます。また、普段は聞いて終わりのところをグループワークなどを行い、声に出す、他の人の意見を聞くなど、刺激を受ける工夫を行いました。



最後にテストとアンケートを行う事で理解度や満足度の測定も行いました。これらの結果は次の教育計画に反映させていく予定です。そして、外部講師からのフィードバックも受けました。今までは教育をして終わっていたものが、担当者としても次につながる結果を得て終えることができました。

教育のPDCAを行なった事で長期的なPDCAのイメージも付き、今後は他の実行でも同じように取り組んでいく予定とのことです。

Day9

4.年間計画への対応

計画通り実行するためには

計画を作成して実行していきたいのに思うように実行できなかった、ということはありませんか？ある会社でも、計画は作るけれども計画通りに進まないという悩みを抱えていました。

A社では、セキュリティの年間計画はセキュリティ担当者と上位役職者が作成し運用まで行うこととなっています。2人ともセキュリティ専任というわけでなく、兼務のため他にも業務がありました。計画が思い通りにいかない理由の1つ目として、セキュリティ関連業務にかける稼働時間が想定通り確保できないということがあげられました。元々の業務に加えて、飛び込みの業務や急な依頼による対応などが頻発します。売上に直結しないセキュリティ関係の業務はどうしても後回しになっていました。

計画が思い通りにいかない理由1
セキュリティ関連業務にかける稼働時間が想定通り確保できない

計画通りに進まない2つ目の理由は、予算獲得がなかなかできない点です。計画を作成し実行しようにもお金がかかる取り組みに承認がされず、計画倒れになることが多々ありました。担当者としては、経営層のセキュリティ理解が課題であると捉えています。この2つ目の問題は1つ目の問題とも関連がありました。もし予算があれば、自分たちではできないけれども、外部にお願いし計画通りにできたという取り組みも存在したからです。

計画が思い通りにいかない理由2
予算獲得がなかなかできない

計画通りにいかない直接的な要因は2つの理由と担当者は話しますが、自分たちが成長できるような取り組みも計画していればよかったと振り返ります。そもそも計画を実行する自分たちの能力が変わらないとできることは増えません。また、予算を得ようにも適切な説明ができなかった時もあるとのことでした。自分たち担当者こそ積極的に勉強することで本気度が会社にも伝わるのではないかとA社の担当者は話します。

計画が思い通りにいかない理由1
セキュリティ関連業務にかける稼働時間が想定通り確保できない

計画が思い通りにいかない理由2
予算獲得がなかなかできない

<改善案>

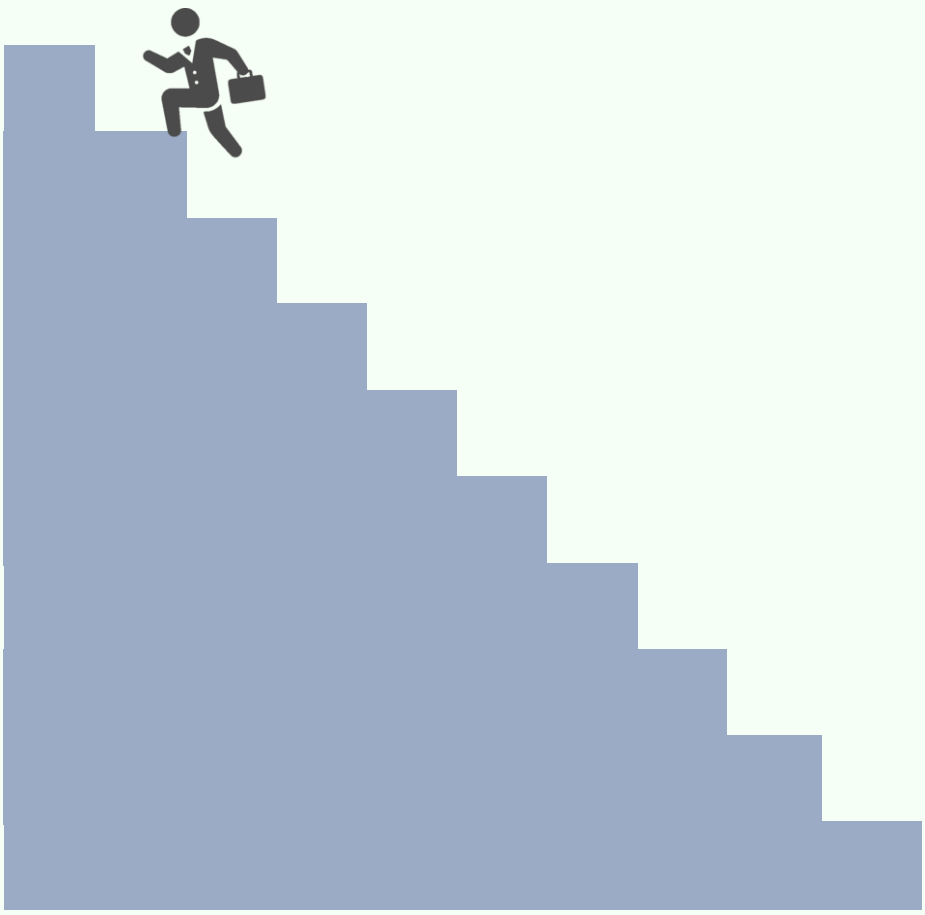
- 自分達が成長することで、セキュリティ業務にかける稼働の質を上げることができたのではないか？
- 説明や根拠が乏しく、予算獲得の必要性が伝わらなかったのではないか？
- 自分達の取り組みのあり方を変えることで、予算の必要性が伝わったのではないか？

今回の担当者のように、自身の反省点を振り返り改善していくことは重要です。しかし、それだけでなく、業務メンバーの理解を得ること、経営層が必要性と重要性を理解すること、会社全体が計画を推進していく必要性を理解することが大切ではないでしょうか？

今までは課題があってがむしゃらに解決することだけを考えていた。だからこそ、場当たり的な対応になってしまった部分があることは間違いない。これからは一つ一つ目標をもって取り組んでいくこと、振り返りを行っていくことを意識していこう。
積み重ねていくことでセキュリティも向上していく。PDCAを意識しながらも、Doの部分は日頃の取り組みとなる。先を見据えながら、日々しっかりと対策に取り組んでいくことが重要だ。

まずは、各取り組みに対して計画を立てよう。そして、計画倒れにならないように実行をしよう。

計画を作る
実行する



コラム
～計画とリソースのあり方～

セキュリティの取り組みでは、短期的なPDCAを実践する場合も計画から行います。計画を立てている企業の計画案を見ると、大きく3種類のパターンがあるように感じます。

1つ目は、過去の踏襲から計画を作成しているパターンです。前年度と比べてもほとんど変化がありません。専門組織が無く、業務評価などもされない場合このような傾向が強いように感じます。

2つ目はリソースの観点からできる計画を立てているパターンです。予算や体制が先に来て、その中でできることを行おうとしています。取り組む意欲はあるものの、満足いく取り組みができないため、セキュリティ担当者のモチベーションが下がっているケースもこのパターンでは多いです。

3つ目は評価を受け、長期的なPDCAの中で検討された目的や目標に則った計画を立て取り組んでいるパターンです。セキュリティのPDCAを行う理想的な形といえます。

リソースにも限りがあるため全て計画通りにいかない場合はもちろんあることでしょう。それでもまずはリスク分析に則った計画を作成し、経営層や予算管理部門としっかりと議論をしていくことが会社にとっても重要ではないでしょうか？

あとがき

「段取り八分の仕事二分」とは、事前の段取りを予め終わらせておくことで、その仕事は八割完了しているという意味の格言です。セキュリティに限らず仕事の多くは計画をしっかりと作り込み、あとは実行するだけの状態になっていることが理想ではないでしょうか？

ただし、長期的な計画では時々目的を見失う場合もあります。定期的な振り返りは自分達が何を目指しているのか？最善と思われる方法が取れているのか？を関係者で振り返りながら議論をしていくことが重要です。また、中からだと気付けないこともあるため、外から自分達の取り組みがどう見えているのかを確認するという方法もあります。外野からさまざまな声が上がることもありますが、一意見として適切な意見のみを吸い上げ、リスク分析に即して取り組みを進めていく姿勢こそ、セキュリティ担当者には求められるのかもしれません。

令和4年度

中小企業サイバーセキュリティ対策継続支援事業

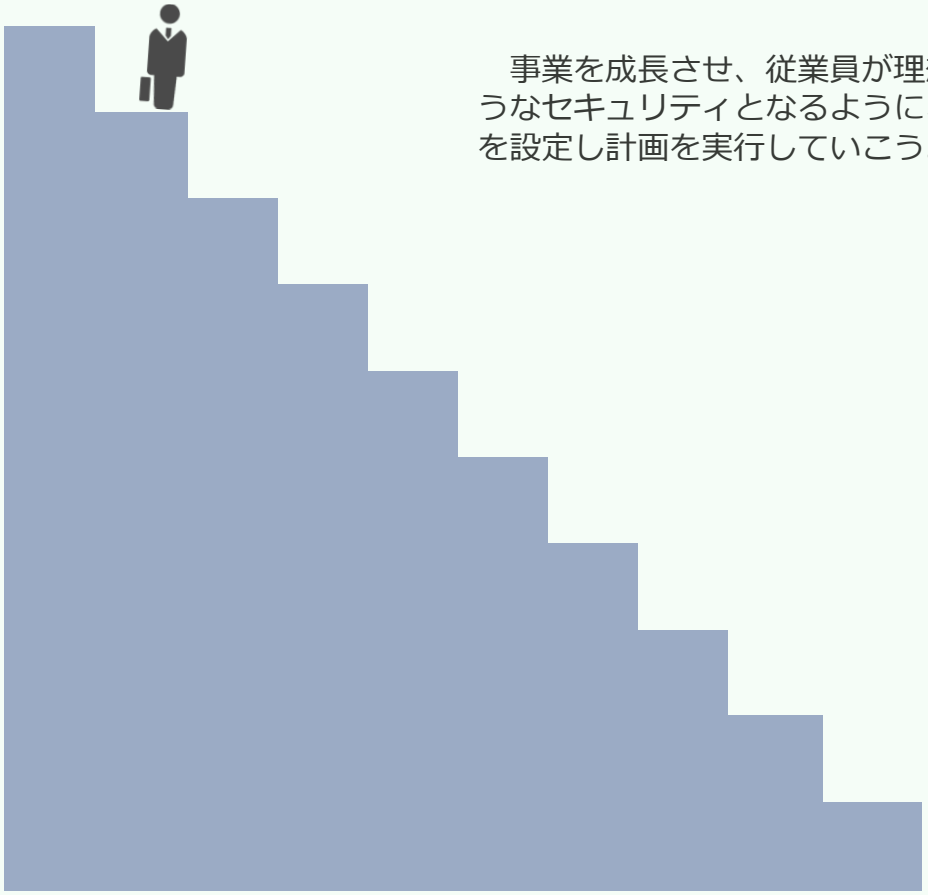
第１０回

セミナー開催日：令和5年1月24日

セキュリティはこれからも進化する

資産を管理し、リスクアセスメントを行い、対応方針を検討し、対策を行っていくことをしっかりと継続していくことが重要だ。特にこれからは防御の仕組みと合わせて、検知の取り組みをしっかりと行っていく必要がある。日々の業務の中でなかなかセキュリティに注力する運用はできていなかった。これからは、一人で抱え込むのではなく、周りの人にも協力してもらいながら取り組んでいこう。

セミナーを聞いていて、セキュリティは本当に細かいところまで考えていく必要があると感じている。セキュリティ担当者の仕事はたくさんある。業務はしっかりと行っていくとしても、稼働が多くなり業務過多になってしまうのは良くない。役目はしっかりと果たしつつ、働き方についても考えていく必要がありそうだ。セキュリティは奉仕の精神だけではできない。



事業を成長させ、従業員が理想の働き方ができるようなセキュリティとなるように、長期的な視点で目標を設定し計画を実行していこう。

Day10

1.事業戦略とセキュリティ

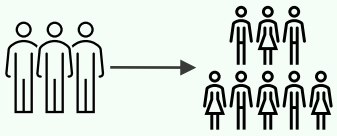
事業計画とセキュリティの関係性

セキュリティの取り組みは事業計画や事業戦略と合わせて考える必要があります。経営層としっかりとコミュニケーションをとり、事業を促進するセキュリティにしていきましょう。

Point① 事業に沿って先を見据えて検討する

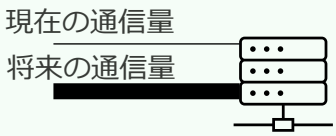
セキュリティは事業計画に沿って対応します。また、ITやセキュリティの投資では数年先まで見通して検討することが重要です。

従業員数の変化



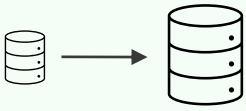
現在の従業員数でセキュリティの計画を立てていると、パソコンの数やアカウント、ライセンス数などが足りないといった事態に陥ります。このような事態になり、暫定的な対応が必要になると、イレギュラーな状態となり、セキュリティ対策が網羅されない可能性があります。

通信量の変化



利用するクラウドサービス、クラウドの利用状況などにより、通信量が変化します。今後、よりクラウド利用が進む場合には、想定される通信量にUTMなどの製品が耐えられるか検討し、導入する必要があります。もし、通信量に耐えられないと、ネットワーク遅延といった影響が発生します。

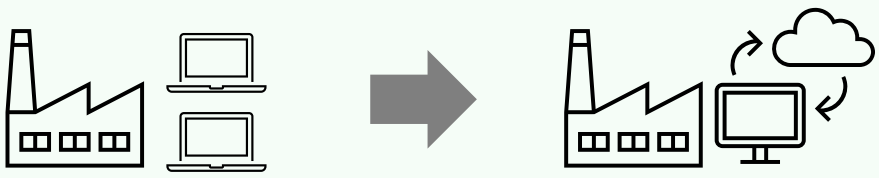
保存容量の変化



検知の観点からログを収集するにあたり、どのくらいの期間保存するかは、サーバなどの容量に関係します。通信量や従業員数の増加により、発生するログが多くなると、想定していた期間ログが残らないといった問題が発生する可能性があります。

Point② 攻めのIT投資を活かすセキュリティへ

既存のビジネスの変革や新たなビジネスの創出による利益拡大を目指してIT投資していくことが今後重要になります。社内に目を向けたセキュリティだけではなく、お客様へ提供する製品やサービスについてもセキュリティの考え方は必要となります。



事業系の環境はインターネットに繋がらないようにすることでセキュリティ対策としていた

新たなビジネスの創出のため、データをクラウド管理し、データ分析を行い、お客様へ新たな価値を届ける

価値創造やビジネス創造を行う際には、デジタルを活用することが多くなっています。そのため、価値創造やビジネス創造の場ではセキュリティ対策の検討や実行が重要となり、今後セキュリティ担当者の活躍の場は今以上に広がります。

Day10

1.事業戦略とセキュリティ

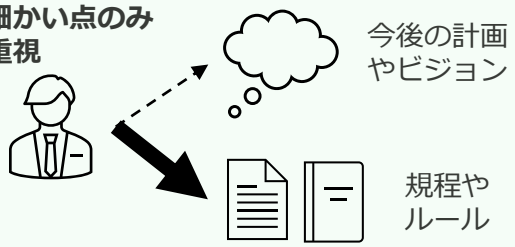
長期的な視野で規程を見直す

企業を取り巻く環境は、市場環境、顧客ニーズ、取引先との関係等により、日々変化しています。市場やニーズに対応するためには社内体制の変更などを行う必要があります。企業は、環境変化に対応する中で、セキュリティレベルを維持管理します。

Point① 視野を広く持って意識する

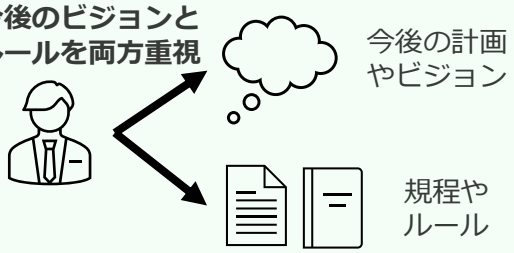
セキュリティの業務は非常に細かな点まで管理します。そのため、細部に注意が行きがちです。規程の改修やセキュリティ対策の取り組み計画を考える際には長期的な視野、視点を持つことも重要です。

細かい点のみ重視



細かい点に意識が行き過ぎると、なぜそのルールが必要なのか、何を目指しているのかといった目的意識が欠如してしまいます。その結果、達成すべき計画やビジョンを阻害してしまう可能性があります。また、対策手段にこだわってしまうと本当に必要な対策がとれないといった状態に陥ります。

今後のビジョンとルールを両方重視



今後の計画やビジョンを正しく把握・認識し、それが実現可能なルールとなっていることを確認します。目的に対して、ずれが生じていないかなど定期的に確認することで、事業計画を阻害しないルールづくりにつながります。

Point② DXを意識したセキュリティへ

DXを進めていくことは、戦略として多くの企業で検討されているのではないでしょうか？実際にDXを推進していくとなると、取り組むべきことは多岐にわたります。セキュリティ担当者としては、DXを推進していくにあたって必要なセキュリティを担っていくことが大切です。

データ活用

DXなどを進める中で、データを分析し、活用することは重要な取り組みの一つです。集めたデータを保管するだけではなく、分析などを安全に行うセキュリティ対策の検討が大切です。

諸外国の法律も意識

新しい価値創造やビジネスのあり方を考えると、海外を意識して対応を検討する必要があります。商圏とする国の法律や規定などに準拠してセキュリティ対策や取り組みを実現することが求められます。

IoTやOTにも目をむける

自社のビジネス環境によっては、IoTやOTの環境に対してのセキュリティを考えていく必要があります。各環境の特徴や利用方法などを意識して規程やルールを定めていくことが求められます。

DXを検討していく際には、ビジネス企画とセキュリティのルール作り、対策の実行が並行して行われます。そのため、双方向でコミュニケーションをとり、認識を合わせながら進めていくことが求められます。

Day10

1.事業戦略とセキュリティ

事業計画に合わせたセキュリティへ

事業計画を検討する際に重要な要素となるのがDXです。今後のセキュリティの取り組みは、DXと一緒に進める必要があり、セキュリティ担当者としても、DXを意識した対応が求められると言えます。

Point① デジタル化からDXへ

DXを進めるといっても、一足飛びにDXまで行き着くわけではありません。デジタイゼーション、デジタライゼーション、デジタルトランスフォーメーションと進んでいきます。それぞれのフェーズに合わせつつ、一歩先を行くセキュリティ対策、ルールを検討しましょう。

デジタイゼーション	デジタライゼーション	デジタル トランスフォーメーション
物理データのデジタル化に代表されます。紙媒体からデータとしての保管というように手段の代替としてのIT活用を進めます。 この場合、物理対策が中心だったセキュリティ対応から、資産のあり方が変わってきます。そのため、資産管理のルールを変更していく必要があります。	業務フロー・プロセスのデジタル化に代表されます。手続きのオンライン化や製品やサービスをデジタルにより顧客へ届けるための仕組みなどが該当します。フローやプロセスといった一連の流れや取り組みが変化していくため、セキュリティ対策も幅広く見直し、取り組む必要があります。	基幹事業のデジタル化と変革に代表されます。自社のノウハウを商用サービス化するなど、新規事業の推進や新規市場への参入も行われます。今までの事業体系と異なるため、事業に関わるセキュリティの対策や取り組みについて、検討する必要があります。

「データとデジタル技術を活用して、顧客や社会のニーズを基に、製品やサービス、ビジネスモデルの変革」を目指し、新しい価値創造を行っていきます。価値提供に伴って、顧客へのサービス提供のあり方が変化し、ITを活用したサービス提供へ切り替わる場合があります。これからは、自社の資産を守るというセキュリティだけでなく、サービスとして提供するためのセキュリティについて検討する可能性も十分あり得ます。

こんな事例も

ある会社では、今までの事業経験から数多くの有益なデータと研究結果を保有していました。DXを意識するようになり、保有しているデータや研究結果を顧客向けのビジネスに活用できるのではないかと考えていました。クラウドを利用したSaaS型のサービスを開発することで、お客様にも自社のノウハウを提供することができるとわかり、早速サービス化を検討しました。

ここで一つハードルとなったのが、セキュリティの問題です。今までは、契約するシステムの認証方法などを意識して選定すれば良かったのですが、今回は自分たちがサービスを提供するためのシステムです。どのようなセキュリティ機能を実装すれば良いのか検討もできない事態になりました。そこで、顧客が利用するサービス導入に伴うセキュリティチェック項目を意識しつつ、開発者と相談しながら実装していきました。自分達のサービスにおけるセキュリティ基準を明確にしつつ、機能を盛り込んでいくことは、社内のセキュリティ以上に大変であると感じる瞬間でした。

現在はサービス開発時に必要なセキュリティ機能も文書化し、機能拡張にも力を入れています。

Day10

1.事業戦略とセキュリティ

セキュリティ担当者の理想の働き方のために

セキュリティ担当者の仕事は幅広く、扱う情報も機微情報が多くなります。また、セキュリティ担当者は何か問題が発生した際の連絡先となっているケースも多いため、休み中であろうと連絡が来たら対応しないといけないという話もよく聞きます。

point① セキュリティ業務の中で見直していきたいこと

セキュリティの仕事は慈善事業ではありません。継続して対応できるような担当者の働き方や体制を改善し、長期的に対応できるようにしていく必要があります。

設定変更やログ監視のために出社する必要がある

会社のシステムによっては、機器の設定変更やログの確認のために出社が必要となる場合があります。

勤務時間が長くなり、終業時間が深夜になってしまう

攻撃者はいつ、どんな手段で攻撃してくるかわかりません。深夜の攻撃に毎日対応していくと体を壊してしまうかもしれません。

責任が重くなり、ストレスを感じてしまう

サイバー攻撃によって、会社が被る損害は大きいです。そのため、セキュリティ担当者はストレスを抱え込んでしまう可能性もあります。

負担軽減策①
リモートでアクセスできるシステムを作る

機器の設定変更やログの監視ができるように、環境を整えましょう。ただし、セキュリティ事故が発生した場合には、社内へのアクセスができないといったことも想定されます。また、リモートアクセスが可能ゆえのセキュリティリスクも存在します。それぞれにしっかりと対策を行い、会社が目指す働き方をセキュリティ担当者が実践できるようにしましょう。

負担軽減策②
外部に委託する

セキュリティ業務の一部または全部を外部に委託したり、外部サービスを利用するという方法もあります。外部のパートナーや専門家をうまく利用することで、自身の担当する業務を減らし、稼働調整をしやすくすることが期待できます。ただし、委託先管理といった新しい業務が発生してくる点に注意が必要です。

負担軽減策③
責任を分散させる

セキュリティ業務を1人で抱えるのではなく、体制と役割をしっかりと作りましょう。他の従業員がセキュリティ担当者の不在時にも事故や関係各所への連絡に対応できるようにすることが大切です。役割分担し責任を分散することで負荷を軽減させる方法もあります。また、メンタルヘルスなどのサポートを活用するといった方法を検討してもよいかもしれません。

こんな事例も

ある会社ではすべてのセキュリティ対応を一人で行っていました。何か問題があった場合には、休みの日に連絡がいくことも度々発生しています。この会社のセキュリティ担当者はまじめな気質で、対応を頑張っていました。ただし、休みの日が休みで無くなったり、日ごろの対応の疲れや、必要性等が理解されない苦しみは日々感じていました。体調不良でも連絡が来るようなこの環境にだんだんと不満も現れ、転職を考えるようにもなりました。セキュリティ担当者がよりよく働けるためには、経営者の理解やサポート体制が重要であり、理解やサポートが無いとセキュリティ担当者に進んでなりたがる人はいないのではないかと語っています。

ミニワーク
～考えてみよう～

ミニワークテーマ

自身の理想の働き方を考えてみましょう。
また、それを実現するために必要なことは何かを
考えましょう。

Day10

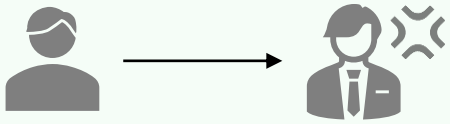
2.日々の運用

セキュリティの日々の運用

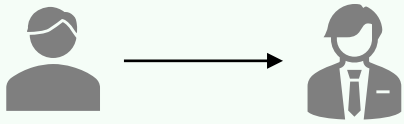
教育や監査といった大きな取り組みも重要ですが、それにもまして、日々の取り組みがセキュリティでは大切であり重要です。これから自走していくにあたり、日々の運用を大切にしていきましょう。

Point① エスカレーションに対応する

セキュリティ事故はいつ起こるか分かりません。従業員のミスなどでセキュリティ事故が発生したときにも、上司にエスカレーション（相談）しやすい環境を整えることが大切です。早いエスカレーションが事故の被害を抑えることにつながります。



業務が忙しいなどを理由にエスカレーションに対してイライラしていると、エスカレーション自体してはいけないといった雰囲気になってしまいます。これにより、初動対応が遅れたり、自社のヒヤリハットが正しく集計できない可能性が高まります。



小さなエスカレーションに対しても真摯に対応します。事故などへの気付きが速くなり、初動対応がスムーズです。また周囲の協力が円滑になり、取り組み自体が関係者の協力を得ながら進めることができます。

報告されたエスカレーションはしっかりと記録をとりましょう。期間を決めて分析することで、自社ではどのようなヒヤリハット、事故が発生しているのかを把握することができます。これは次の対策立案や教育などを考える際の重要なデータとなります。

Point② 情報収集と共有をする

最新の脅威や脆弱性、攻撃の手口を知ることはセキュリティ担当者として日々行っていきましょう。組織の対策レベルの向上につながります。また、その情報を関係者（従業員、パートナー企業など）と共有し、サプライチェーン全体のセキュリティ向上を目指しましょう。

①情報収集の方法

情報収集で重要なことは、情報が自然と集まる方法を用意することです。信頼できる情報収集先をブックマークすることやRSSリーダーを利用する方法があります。

例えば、セキュリティの専門機関やセキュリティベンダのメールマガジンやソーシャルメディアへの登録、セミナーに定期的に参加することも有効です。

②情報共有の枠組み

近年、取引先や同業者を経由したサイバー攻撃が増加しています。そこで、収集した情報は社内の関係者だけでなく、取引先や同業者に対しても共有することで、対策の向上が期待できます。最近ではISAC(アイザック)といった業界内での情報共有・連携の取り組み推進を図る組織で、セキュリティに取り組む業界も存在します。

<参考情報>

情報収集の方法には、以下のようなサイトが利用できます。

■ここからセキュリティ！
https://www.ipa.go.jp/security/kokokara/

■IPAセキュリティセンター
https://www.ipa.go.jp/security/

■IPAサイバーセキュリティ注意喚起サービス「icat for JSON」
https://www.ipa.go.jp/security/vuln/icat.html

■JPCERT/CC
https://www.jpcert.or.jp/

■警察庁@police
https://www.npa.go.jp/cyberpolice/

■日本シーサート協議会
https://www.nca.gr.jp/

セキュリティの日々の運用

Point③ 外部組織と連携する

セキュリティの対応を自社だけで行うと非常に大きな労力がかかるだけでなく、情報量も不足しがちとなります。うまく外部組織と連携を図ることが重要です。

●一般的な情報セキュリティ相談

情報処理推進機構(IPA) 情報セキュリティ安心相談窓口
https://www.ipa.go.jp/security/anshin/
TEL：03-5978-7509　FAX：03-5978-7518
mail：anshin@ipa.go.jp
受付時間：10:00～12:00
　　13:30～17:00(土日祝日・年末年始を除く)

中小企業サイバーセキュリティ相談窓口
【電話相談窓口】03-5320-4773
【相談フォーム】 ：https://www.shinsei.elg-front.jp/tokyo2/uketsuke/form.do?id=1461031266630
【窓口でのご相談】 東京都産業労働局商工部内 Tcyss事務局
(東京都新宿区西新宿2丁目8番1号都庁第一本庁舎20階北側)

●犯罪の可能性がある場合の相談窓口

サイバー犯罪相談窓口
https://www.keishicho.metro.tokyo.lg.jp/sodan/madoguchi/sogo.html
電話：03-5805-1731
受付時間：8:30～17:15（平日のみ）

●被害の報告・連絡・相談窓口

コンピュータウイルス・不正アクセスに関する届出 (IPA)
https://www.ipa.go.jp/security/outline/todokede-j.html

フィッシング詐欺
(フィッシング対策協議会)
https://www.antiphishing.jp/

迷惑メール
(日本データ通信協会 迷惑メール相談センター)
https://www.dekyo.or.jp/soudan/

なりすましECサイト
(なりすましECサイト対策協議会)
https://www.saferinternet.or.jp/e-commerce/narisumashi/

インシデント報告・届出
(JPCERT/CC)
https://form.jpcert.or.jp/

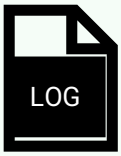
インシデント報告・届出
(IPA J-CRAT 標的型サイバー攻撃特別相談窓口)
https://www.ipa.go.jp/security/tokubetsu/index.html

個人情報保護委員会
https://www.ppc.go.jp/personalinfo/legal/leakAction/

Point④ 異常を検知し対応する

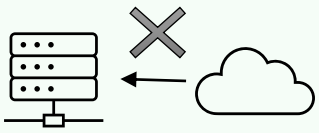
近年のセキュリティでは防御だけでなく、検知の仕組みも重要です。ただ検知するだけでなく、対応有無の判断など、次の行動に進めるように取り組みましょう。

ログの取得



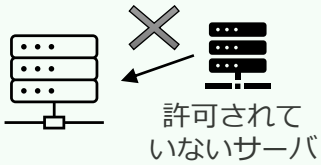
サーバへの通信が正しいものなのか？また、サーバからの通信が正しいものなのか？のログを取得し、異常と判断される場合には早急に対応します。

外部からの通信制御



外部からの不正な通信があった場合には、即断の対処が必要な場合があります。この場合、通信の発生だけでなくログイン可否についてもログを確認しましょう。

機器の管理



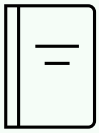
機器の管理も重要です。許可されていないサーバや端末が、ネットワークに繋がった際に検出できるようにしましょう。

通信ログや機器からのログを管理することは、セキュリティの日々の運用の中でも重要です。攻撃に気付き、初動対応を素早く行うことで、セキュリティ事故の被害を最小限に抑えることに繋がります。
また、日々のログを管理し分析することで、攻撃傾向や業務における危険な利用の可能性、ルールを逸脱した利用など多くのことに気付くことができます。これらに対して対策していくことで、よりセキュリティの取り組みが向上します。

セキュリティの日々の運用

Point⑤ 活動を記録に残す

セキュリティの取り組みをして終わりにしてはいけません。しっかりと記録に残し、蓄積し、振り返り・分析することが重要です。

記録をつける	議事録をつける	履歴を残す
		
入退室の記録、貸出記録などを取得します。物理的な紛失などに気付き、人の行動を確認しやすくなります。	セキュリティ組織のミーティング記録などを残します。意思決定プロセスなどを記録することで、セキュリティの取り組みに対して決定理由などが後世に残ります。	エスカレーションや問い合わせの履歴を残します。自社の課題や従業員が起こしやすいセキュリティ事故などの傾向がわかり、対策を検討する材料になります。

資産管理からリスクアセスメントにより対策は立案されるべきではありますが、記録を残しながら対応を進めていくことにより、データによる判断が可能となります。一般的な脆弱性や脅威だけでなく、記録からわかる自社特有のリスクを正しく把握することで、より実態にあったセキュリティ対策につながります。

～Note～

Day10

2.日々の運用

システムや機器を管理する

セキュリティの日々の運用では、利用しているシステムや機器の管理をしっかりとしていくことが重要となります。システムが正しく動いていない場合、セキュリティ事故につながる可能性があります。

Point① 実態に合わせてチューニングを行う

機器の設定は一度すれば終わりというわけではありません。定期的に見直しをしたり、必要に応じて設定の追加といった対応を行う必要があります。

URLやIPアドレスなどで通信をチューニング

フィッシングサイトや攻撃に利用されていると思われるIPアドレスなどは通信機器などでブロックします。ブロックすることによって、誤操作やウイルス感染からの異常な通信を通信機器で止めることが可能となります。

通信ポリシーのチューニング

業務実態や案件状況などにより通信機器に設定している通信ポリシーをチューニングします。

ファイルのアップロードの設定など必要な人のみが通信できるようにすることで、業務とのバランスをとりながら、セキュリティを高めることにつながります。

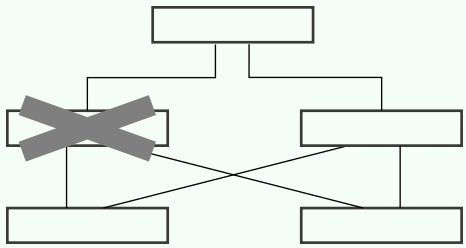
ログ出力のチューニング

検知の観点からログを出力し確認する癖をつけましょう。現在のリスクに対して必要なログはどのようなものかを意識し、本当に必要なログを取り、内容を確認できるようにしましょう。

機器の管理や設定は保守業者が全て行っているというセキュリティ担当者もいるかもしれません。しかし、細かいチューニングを保守業者にお願いすると時間や費用がかかってしまいます。初期設定等や保守自体は業者にお願いしつつも、細かいチューニングは担当者自身でできるようにすることも大切です。

Point② 機器の状態を管理し適切なセキュリティ維持を

物理的に機器が存在している限り故障といった機器が動かなくなるというケースは存在します。機器の状態を適切に管理し、機能が有効になっていると確認することもセキュリティの日々の運用としては重要です。



冗長化をしていたつもりが、実は機器が故障していることがあります。通信には影響がない場合、気付くのが遅れることが考えられます。機器の状態を把握し、異常にいち早く気付くことが重要です。

証明書には有効期限があるため、有効期限が切れると失効状態となり、通信ができないといった不具合が発生します。

機器の管理等を正しく把握し運用することで、事象に対して、攻撃なのか故障なのかといった判断を素早くすることができ、初動対応が早くなります。

システムや機器を管理する

Point③ EOSやEOSLの情報を把握する

製品やサービスは無期限に使えるわけではありません。提供企業は新しい製品やサービスを提供していく中で、古い製品やサービスを終了します。終了するとソフトウェアがバージョンアップされなくなり、脆弱性等が解消されなくなります。

サービスや製品の終了とサポートの終了などの日時を把握することはセキュリティ担当者として重要な取り組みとなります。EOSやEOSLなどの情報を把握し、前もって対応を検討しておく必要があります。

EOS（ End of Sale ）：製品・サービスの販売終了
EOSL（End of Service Life）：保守／サポート期間終了

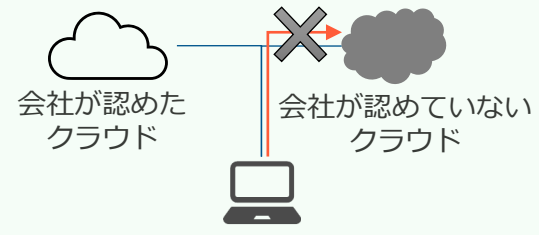
なお、サポート終了をEOS（End of Support）と呼んだり、技術的なサポート終了の場合には、EOE（End of Engineering）と呼んだりする場合もあります。

管理名称	記載事項の例
アプリケーション・ソフトウェア名称	Zoom、DropBoxなど
バージョン情報	10.15.7
管理責任者	A部署 ○○ など
利用用途	オンライン会議で利用
利用機器・利用者	ホスト名、ユーザー名
EOSL予定日	yyyy/mm/dd

機器管理表では、EOSやEOSLの情報を記録に残せるようにしておき、余裕を持った入れ替え計画を立案し実行することが大切です。EOSLを迎えてから計画を立てると実際に次の製品やサービス導入までに時間がかかり、脆弱性を保有したまま日々の運用を行うこととなります。

Point④ シャドーITや不許可端末の接続を把握し対応する

利用許可がされていない端末やクラウドサービスにいち早く気付くことも重要となります。通信ログや各種機器からのログの確認、構成図などから把握し、対応していきます。



会社が認めていないクラウド環境へアクセスが発生するようならば、通信をさせないような対策を取る必要があります。このような場合には通信ログを監視しアクセス状況を把握することが重要です。

個人所有の端末を会社の無線LANに接続するといった場合があります。接続を許可しない場合には、IPアドレスの管理や無線LAN接続のログ監視など接続状況を把握し管理することが求められます。

シャドーITや不許可端末の接続は、大きなセキュリティ事故にもつながりやすい事案です。気づきを早くし、素早く対応できるように取り組みましょう。

Day10

2.日々の運用

ログを管理する

異常やセキュリティ事故に気付く、認証等の状況を把握するといった検知の重要性が上がるにつれて、ログを取得し解析・分析することは非常に重要な取り組みとなっています。

Point① ログを取得し解析する

日々の事業運営の中では、システムや通信から大量のログが取得されます。これらのログを解析することで、攻撃の予兆や不正な通信の発生をいち早く確認します。

インターネットから機器へ不正アクセスしようとする異常な通信ログのイメージ

```
Nov ** 0*: 0*: 0* Hostname in.telnetd[7421]: connect from 115.XXX.XXX.167 (115.XXX.XXX.167)
Nov ** 0*: 0*: 0* Hostname telnetd[5848]: ttloop: peer died: EOF
Nov ** 0*: 0*: 0* Hostname in.telnetd[17991]: connect from 121.XXX.XXX.179 (121.XXX.XXX.179)
Nov ** 0*: 0*: 0* Hostname telnetd[7421]: ttloop: peer died: EOF
Nov ** 0*: 0*: 0* Hostname in.telnetd[17999]: connect from 115.XXX.XXX.167 (115.XXX.XXX.167)
```

本来であれば、通信が来るはずがないところから受信しています。頻度が多いようならば、接続元のIPアドレスで制御することなどを検討します。

ログイン履歴のログのイメージ

```
Hostname pts/1      122.XXX.XX.50     Wed Oct ** 10:53 - 10:54  (00:01)
Hostname pts/0      122. XXX.XX.50     Wed Oct ** 07:24 - 07:47  (00:22)
Hostname pts/0      119. XXX.XX.154  Tue  Jun ** 09:24 - 10:04  (00:39)
Hostname pts/0      122. XXX.XX.50     Wed Jun ** 10:23 - 11:24  (01:00)
Hostname pts/0      118. XXX.XX.1      Wed Mar ** 07:34 - 07:51  (00:17)
Hostname pts/0      118. XXX.XX.1      Fri Mar ** 08:23 - 08:26  (00:02)
```

ログインした時間に覚えがない、本来であればアクセスするような時間ではないといった場合には、第３者によるアクセスといった可能性が考えられます。

Point② ログ取得時の注意事項

ログは取っているだけでは意味がありません。解析や分析を行うことが重要となります。しかし、ログを解析するような際は、取得時から注意しておくことがあります。

時刻を同期する

ログを取得すると時刻が一緒に取得されます。複数の機器からログを取得する場合、すべての時刻を同じにしておくことで解析の質が高まります。NTPサーバと時刻を同期させることで、すべての機器が同じ時間を刻むようになります。

異常を特定する

ログは各機器が出力しますが、攻撃とみなされる通信やウイルスの起動などを除いては正常・異常の判断を人がする必要があります。取得するログから何がわかるのか、どのような結果なら異常なのか考えておくと対応がスムーズです。

取得する場所を考える

ログはサーバやパソコン本体だけでなく、ソフトウェアやアプリケーションでも取得できます。管理すべきログはどこで取れるのか、どのようなログが取れるのかを把握し、取得ポイントや取得方法を決めて運用をすることが大切です。

ログ取得は大切ですが、やみくもに取れば良いというわけではありません。保存先の容量も有限であり、取得数が多いと管理も大変になります。また、解析においてもどのログを対象として良いのかといった悩みが生じる場合もあります。事前に見るべきログ、取るべきログを定めて運用していくことが望ましいと言えます。また、それぞれの機器やソフトウェアで取得すると管理に時間がかかります。統合ログ監視といった製品を利用すると一元管理されるため、解析等がしやすくなります。

ログを管理する

Point③ ログや記録を組み合わせて判断する

「異常」の定義は各社により様々です。ログとログを組み合わせてわかる異常もあれば、ログと記録を組み合わせてわかる異常もあります。また、インシデント対応の時などは、複合的にログや記録を見ながら、状況を把握していきます。

■ログを組み合わせて状態を把握する

遠隔操作を狙った通信と認証可否のログ

```
Nov 19 06:32:11 Host sshd[19369]: Connection closed by authenticating user name122.XXX.XXX.50 port 59704 [preauth]
Nov 19 06:31:30 Host sshd[19369]: Failed password for name from 122.XXX.XXX.50 port 59704 ssh2
Nov 19 06:31:37 Host sshd[19369]: Failed password for name from 122.XXX.XXX.50 port 59704 ssh2
Nov 19 06:32:11 Host sshd[19369]: Failed password for name from 122.XXX.XXX.50 port 59704 ssh2
Nov 19 06:32:11 Host sshd[19369]: Connection closed by authenticating user name122.XXX.XXX.50 port 59704 [preauth]
Nov 19 06:32:23 Host sshd[19394]: Failed password for name from 122.XXX.XXX.50 port 59733 ssh2
Nov 19 06:33:05 Host sshd[19394]: Failed password for name from 122.XXX.XXX.50 port 59733 ssh2
Nov 19 06:33:23 Host sshd[19394]: Failed password for name from 122.XXX.XXX.50 port 59733 ssh2
Nov 19 06:33:23 Host sshd[19394]: Connection closed by authenticating user name122.XXX.XXX.50 port 59733 [preauth]
Nov 19 06:33:33 Host sshd[19416]: Accepted password for name from 122.XXX.XXX.50 port 59767 ssh2
Nov 19 06:37:58 Host sshd[19488]: Disconnected from user name122.XXX.XXX.50 port 59767
```

ログイン履歴のログ

```
Hostname pts/0      122.XXX.XX.50   Sat Nov 19 06:33 - 06:37  (00:04)
Hostname pts/1      122. XXX.XX.50    Wed Oct ** 10:53 - 10:54  (00:01)
Hostname pts/0      122. XXX.XX.50    Wed Oct ** 07:24 - 07:47  (00:22)
Hostname pts/0      119. XXX.XX.154  Tue  Jun ** 09:24 - 10:04  (00:39)
Hostname pts/0      122. XXX.XX.50    Wed Jun ** 10:23 - 11:24  (01:00)
Hostname pts/0      118. XXX.XX.1     Wed Mar ** 07:34 - 07:51  (00:17)
Hostname pts/0      118. XXX.XX.1     Fri Mar ** 08:23 - 08:26  (00:02)
```

遠隔操作を狙った通信と認証可否のログを見ると、6:33分にAcceptedのログが出力しており、遠隔操作を可能とするアカウントへの認証が成功したことが伺えます。これを裏付けるように、ログイン履歴のログでは、6:33分から6:37分にログイン履歴が存在しています。遠隔操作を狙った通信と認証可否のログを見ると、 6:37分Disconnectedという接続が切断されたログが伺えます。

■記録とログを組み合わせて異常を発見する

上記のログでは、 6:33分から6:37分にログインがなされたということがわかりました。このログの結果と記録を合わせて解析することで異常なのかを判断します。

作業申請書

作業日：M月D日
作業時間：6:30～6:40
作業内容：メンテナンス
作業者：〇〇
承認者：■■

例えば、機器へのアクセスがあった時間帯に左記のような作業申請書が出ていたとします。このような場合には、計画された作業としてログイン履歴は異常ではないと判断することができます。

もし、このような申請書や記録がなく、ログイン履歴が存在するような場合には、不正アクセスの可能性として捉え、より本格的な調査を行う必要が出てきます。

■ログが存在しないことも異常と考える

ログを確認したけれども、ログが全く存在していないというケースも考えられます。このような場合には、「ログが取得されていない」、「ログ取得は有効となっているが出力されていない」、「ログが何らかの理由により消された」ということが考えられます。ログが消されたような場合には、何者かが不正アクセスした可能性もあるため、至急の調査が必要です。ログが消されたということを検知するためには、日頃からログを確認しておく必要があります。

Day10

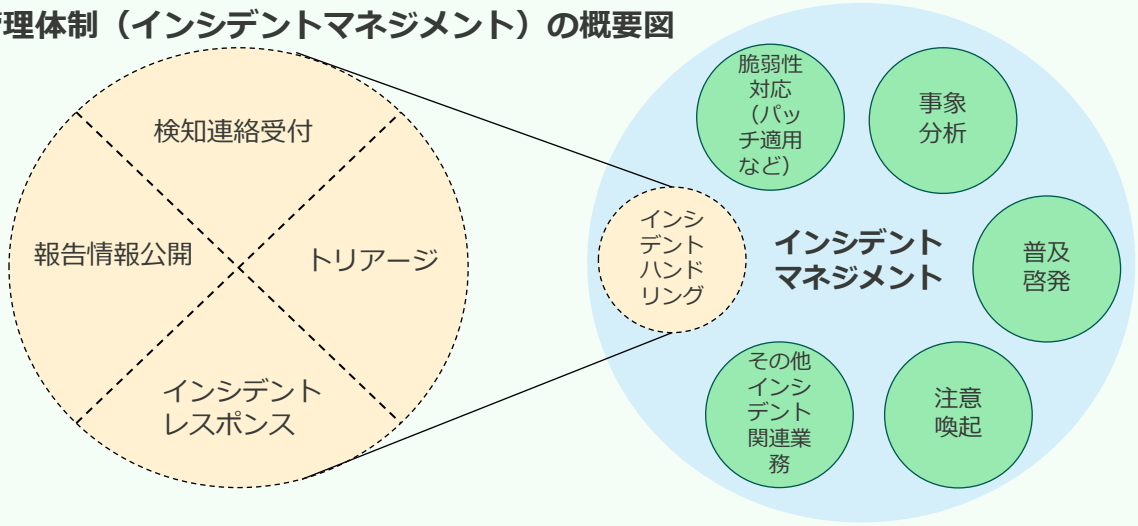
2.日々の運用

異常に対応する

システムの管理やログの取得・解析の目的は、異常な状態に気付くことにあります。異常な状態を放置せず対応していくこともセキュリティの運用の中では重要な取り組みです。

JPCERT/CC では、危機管理体制と緊急対応に求められる機能を以下のように示しています。
企業経営や事業活動及び企業ブランドに重大な損失をもたらす事態、または社会一般に重大な影響を及ぼすと予想される事態を「危機」と考え、万一危機が発生した場合に損失を極小化するための活動と位置付けています。危機管理体制（インシデントマネジメント）には、次のような機能が必要になります。

危機管理体制（インシデントマネジメント）の概要図



出典：一般社団法人 JPCERT コーディネーションセンター
経営リスクと情報セキュリティ ～ CSIRT：緊急対応体制が必要な理由 ～
https://www.jpcert.or.jp/csirt_material/files/csirt_for_management_layer_20211130.pdf

Point① 状況を把握する

異常に対応するためには、まずは気付くということが重要です。異常な状態をどのように気付くか整理し準備をしておきましょう。

社内からの報告	ログの検出	社外からの連絡
従業員からの報告により異常に気付きます。アンチウイルスソフトが反応した、パソコンの動作がおかしい、通信ができないといったケースでは、従業員からの報告により気付くことになります。	サーバやファイルへの不正なアクセス、インターネットへのファイルアップロード、といった場合にはログから検出します。本来であれば起こり得ないことをログにより発見することができます。	保守業者からの連絡や取引先からの連絡により異常に気付きます。不正なメールが取引先に届いたことにより、自社のウイルス感染に気付くといったケースが該当します。

出典：一般社団法人 JPCERT コーディネーションセンター
「インシデントハンドリングマニュアル」をもとに作成
https://www.jpcert.or.jp/csirt_material/files/manual_ver1.0_20211130.pdf

異常に対応する

Point② 優先順位付け(トリアージ)をする

トリアージで必要なのは「冷静な判断」です。インシデントでないものをインシデントと見なして取り返しの付かない行動を起こしてしまったり、自組織とは無関係のインシデントに対応してしまったりすると、本来は秘匿すべき情報を無関係の第３者に開示してしまうといった「インシデント」を引き起こしてしまう可能性もあります。「勘違い」に基づいた活動は、それ自体がインシデントを引き起こす原因になってしまうのです。

誤検知・勘違いの可能性は？	オペレータの誤操作の可能性は？	自組織で対応すべきインシデントか？
システムの誤検知や報告者の勘違いということは少なくありません。	作業中の誤操作などを検知し、異常と判断されるケースもあります。	報告や連絡を受けた場合でも、自組織が全く関係がないという可能性もあります。

Point③ インシデントに対応する

自組織で対応すべきインシデントと判断された場合は、インシデントの対応を進めます。

自組織で対応する	外部と連携し対応する
セキュリティ担当者やIT部門で対応が可能な場合には、対応計画を策定し、実施します。対応計画の策定や実施に際しては、必要に応じて外部の専門機関や関係している可能性のあるサイト(関係者)に対して、対応の支援を依頼したり、必要な情報を提供してもらったりします。	自組織での技術的な対応が困難な場合(例えば外注先でなければ対応ができないような問題など)は、契約している保守業者などと連携して対応を行います。また、経営層と連携し、対応計画を策定し実施します。外部と連携はするものの、対応における判断は自社でする必要があります。

Point④ 報告・情報公開を検討する

インシデントが発生した際には、必要に応じて関係者へ報告・情報公開する必要があります。

顧客・お客様へ	監督官庁へ	組織内部へ
インシデントの概要や対策などを報告します。	所属業界を管轄する監督官庁へ報告を行います。	従業員へ状況や対応策について報告・共有を行います。

出典：一般社団法人 JPCERT コーディネーションセンター
「インシデントハンドリングマニュアル」をもとに作成
https://www.jpcert.or.jp/csirt_material/files/manual_ver1.0_20211130.pdf

Point⑤ 暫定と恒久を意識する

インシデントが長期化しサービスの提供ができない場合、売上が無く会社の継続が困難になる可能性が発生します。このような場合や恒久的な対応や対策の実装まで時間がかかるというような場合には、暫定的な対応や対策を行い、サービスを再開させる必要があります。

ただし、暫定的な対応や対策で終了してしまうと同じインシデントが発生する可能性があるため、最終的には恒久的な対応や対策を行います。恒久的な対応や対策では、インシデント発生原因などをしっかりと解析・分析した上で考える必要があります。

Day10

2.日々の運用

経営層へレポートする

セキュリティの取り組みを始めた当初は、課題や問題が顕著であり、それらの進捗を報告していくこととなります。しかしながら、取り組みが順調に進むとだんだんと報告する内容が減っていくというケースもあります。

Point① ログの傾向やヒヤリハットを報告する

ログの傾向やヒヤリハットの集計、その他各記録などの状況を報告します。これらの報告により、攻撃の兆候や事故の可能性を関係者で共有することができます。

報告の例

週次での報告	月次での報告
週次での報告は主にセキュリティ組織・チーム内で行います。チーム内で共有することにより、今後の対策などを議論することにつながります。また、必要であれば、セキュリティ組織・チームの活動を見直し、より良い対応としていきます。	週次報告でまとめたものを経営陣へ報告します。例えば、経営会議でその１ヶ月のセキュリティ組織・チームの活動内容の報告と合わせて、その月に発生したヒヤリハットや異常ログの状況などを共有します。

Point② 年間計画の進捗や計画・結果を報告する

週次や月次では活動をメインとした報告を中心としました。四半期や年次といった場合には、年間計画の進捗や各施策の計画・結果を報告します。

報告の例

施策の報告	計画進捗の報告
短期的なPDCAを実施するような場合には、取り組みを行う計画の内容や実施時期を報告します。実行が終了した場合には、その結果を報告します。	年間計画に対して現在の進捗を報告します。取り組みに対しての進捗や課題などが報告の対象となります。もし計画に対して、遅れ等がある場合には合わせてリカバリープランなどを報告します。

Point③ インシデント発生や対応状況を報告する

セキュリティ事故が発生すると、通常時以上にコミュニケーションをしっかりとり、状況を細かく報告する必要があります。

具体的には、インシデントに関して「いつ(時期など)」、「どこで(影響範囲など)」、「だれが(被害者数などの状況)」、「何を(流出した情報など)」、を明確にして整理していきます。開示・報告は、できるだけ早く行うことが望ましいですが、インシデントや被害の状況に応じて、初期発生時、被害状況把握時、インシデント収束時等の段階に応じたタイミングでの報告を検討していきます。もし、適切な開示がされなかった場合、社会的責任を果たせないことで、関係者からの信頼を失い、企業価値が大きく低下する恐れがあります。

ミニワーク
～考えてみよう～

ミニワークテーマ

ログを分析してみよう。

通信をした端末はどのパソコンでしょう。
PC名を調べましょう。

通信ログ
date=2022-11-29 time=19:04:58 logid=0000000013 type=traffic subtype=forward level=notice vd=root srcip=10.10.10.121 srcport=1037 srcintf="lan5" dstip=200.200.200.100 dstport=81 dstintf="wan1" poluuid=eabf262c-3188-51e8-c989-47909acfaa8a sessionid=202929 proto=6 action=close policyid=1 policytype=policy dstcountry="Brazil" srccountry="Reserved" trandisp=snat transip=100.100.100.1 transport=61453 service="tcp/81" duration=381 sentbyte=27503 rcvdbyte=434578 sentpkt=126 rcvdpkt=393 appcat="unscanned"

DHCPサーバログ	

lease 10.10.10.121 {
starts 4 2022/11/28 18:32:49;
ends 4 2022/11/28 19:32:49;
hardware ethernet 70:8b:cd:9d:b7:84;
 	
lease 10.10.10.120{
starts 2 2022/11/29 16:56:32;
ends 2 2022/11/29 17:56:32;
hardware ethernet 08:00:27:7d:6f:cd;
	lease 10.10.10.121 {
	starts 2 2022/11/29 18:56:32;
	ends 2 2022/11/29 19:56:32;
	hardware ethernet 08:00:27:4b:2b:21;
	
	lease 10.10.10.123 {
	starts 5 2022/11/29 19:01:39;
	ends 5 2022/11/29 19:01:39;
	hardware ethernet 08:00:27:ac:06:ad;

アドレス管理表		
PC名	IPアドレス	MACアドレス
PC_00	DHCP	70:8b:cd:9d:b7:84
PC_1	DHCP	08:00:27:fc:f6:cb
PC_2	DHCP	08:00:27:e4:cd:4f
PC_3	DHCP	08:00:27:4b:2b:21
PC_100	192.168.23.10	08:00:27:58:ca:11
PC_200	192.168.23.20	08:00:27:0a:93:97

Day10

3.これからの活動

企業を成長させるための セキュリティへ

セキュリティの維持向上の先には企業を成長させることにつながることが大切になります。DXを進めていくにあたって、セキュリティの求められる点も変わる可能性があります。

Point① 今必要なセキュリティは何か？

基本的な方針は変わらないものの、サービス関係や事業関係では、求められるセキュリティの要素が変わります。そのため、自身が取り組んでいるセキュリティは何かを意識した、目的ベースの思考が重要となります。

社内関係のセキュリティ	サービス関係のセキュリティ	事業関係のセキュリティ
基幹系システムなどを中心として、主に従業員が守るルールを定め、従業員教育などを行います。安定した会社運営などに寄与するセキュリティです。	自社がお客様に提供するサービスに関するセキュリティについて検討を行います。顧客の情報を保護するためにどのようなセキュリティが必要かを考え実装します。DXを考えると、このようなセキュリティも今後重要になってきます。	主に事業部門に特化したセキュリティルールなどを定めていきます。サービスを提供するための開発環境などをセキュアに保ち、安全な開発を行えるようにします。社内セキュリティのルールをそのまま適用しようとすると、事業運営に支障が出るような場合重要となります。

担当するサイバーセキュリティ関連タスクの例

• 予算やリソースの確保 • リスクアセスメント • ポリシー・ガイドライン策定・管理 • サイバーセキュリティ教育 • 社内相談対応 • インシデントハンドリング • BCP対応 ・内部犯行対策 • 法令等遵守対応 • 監視・検知・初動対応・原因究明 • インシデントレスポンス	• 脆弱性診断の実施 • ペネトレーションテストの実施 • 脅威情報の収集・分析 • デジタルフォレンジック • セキュリティ技術開発 • セキュアシステム要件定義 • セキュアアーキテクチャ設計 • セキュアソフトウェア方式設計 • テスト設計 • 基本・詳細設計 • セキュアプログラミング • パッチ開発・テスト・品質保証	• 事業戦略立案 • 企画、要件定義 • 仕様書作成 • プロジェクトマネジメント • 構成管理、運用設定 • 脆弱性情報の収集、脆弱性対応 • セキュリティツールの導入・運用 • 教育・管理 • 設備管理・保全

特にサービスのセキュリティを考えることとなった場合には、開発などの専門的な知識が求められます。数ある要素の中から選択するということが必要です。

出典：経済産業省
「サイバーセキュリティ体制構築・人材確保の手引き」をもとに作成
https://www.meti.go.jp/policy/netsecurity/tebikihontai2.pdf

Day10

3.これからの活動

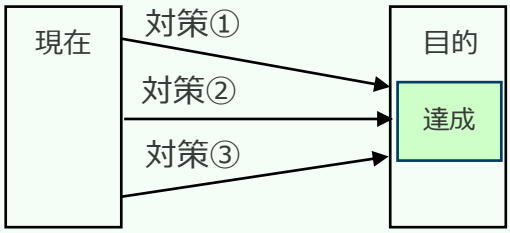
企業を成長させるための セキュリティへ

Point② 企業を成長させるセキュリティ思考を

セキュリティを強化したことにより、事業部門がやりづらくなり良い製品が作れなくなってしまったというようなことはあってはいけません。守るところはしっかりと取り組みつつも、事業が成長できるセキュリティを意識しましょう。その時に大切になる考えが、目的思考です。

目的思考の場合

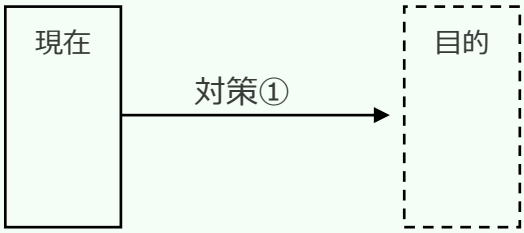
目的を達成するためにセキュリティへの取り組みを行います。そのため、さまざまな手段を検討でき、自社にあったセキュリティ対策を進められるようになります。目的を達成するため、企業の成長戦略に即した動きをすることができます。



多くの手段から最適な
手段を選ぶことができる

手段思考の場合

手段思考に陥ってしまうと、何の目的でその手段を取っているのかがわからず、形骸化されたセキュリティとなってしまいます。この手段で対応をしなければならないという思考に陥ると、業務のやりづらさなどが発生し、企業成長を止めてしまう可能性が生まれます。



手段に固執してしまい
目的が希薄になる

目的思考を行うことが重要ですが、この場合選択できる手段をどれだけ考えられるかという点が重要になります。仮に、目的思考でも手段が一つしか思いつかないといった場合だと、本当に最適な手段と言えるのかわからなくなります。セキュリティ担当者としては目的を達成するための手段を知っていること、考えられることが大切です。そのためにも、他社の事例を聞くセミナーなどへの参加はセキュリティ担当者として必要な行動と言えます。

こんな事例も

ある会社では、社内の作業効率を上げるためにITの活用などを進めており、セキュリティも意識していました。IPAや関係省庁の情報を参考にし、わかる範囲のセキュリティを行っていました。ただし、自分たちで考えて検討したというよりも、サンプルや具体例を参考としつつできる範囲で実施してきたという形です。そのため、なぜこの対策を行うのかといった目的を考えることはしてきませんでした。

一連のセキュリティの取り組みが終わると、次に何をすれば良いのかがわからなくなりました。なぜなら、セキュリティに取り組むことが目的となっていたため、取り組みがひと段落すると目的を見失ってしまったからです。そのことに気づいた担当者は、セキュリティは何のために行っているのかを考えるようにしました。これにより、一段高い視点で目的が考えられるようになりました。そこから改めて必要なセキュリティを考えると、まだまだやらなくてはいけない事が出てきました。しかし、次の問題点は手段の選択肢が少ないという事でした。担当者としてもレベルアップをしないといけないと感じた瞬間でした。

手段を考える際には、保守業者や専門家にもアドバイスをもらいつつ、さまざまな事例を聞いて、目的にあった手段を検討しています。

Day10

3.これからの活動

セキュリティ担当者として成長するために

セキュリティ担当者として、成長していくことが大切です。スキルを磨くだけであれば、業務経験を積み、資格を取得することなどを考えれば良いかもしれません。しかし、セキュリティ担当者として成長を重ねるためには日々の積み重ねも大切です。

Point① 情報を収集し自分のものとする

セキュリティ担当者として成長するためには、セキュリティに関する情報を収集し、定着させていくことが重要です。業務だけをしていた場合には、業務に関係する情報は手に入ります。しかし、攻撃など第３者が存在するセキュリティにおいては、幅広く関心を持ち、情報を集めていくことが大切となります。

セミナー参加	展示会参加	勉強会の参加
警視庁に代表されるように、セキュリティ関連のセミナーは広く行われています。最近ではオンラインで行われるセミナーも増えていますので、自身に関係がある内容・テーマのセミナーに参加し情報を収集します。	製品やサービスを導入する際には、展示会などに参加する方法もあります。実際のサービスを見て体験して、自社にあった製品やサービスを選択します。説明を聞くことで理解も深まります。	有志で開催される勉強会へ参加するということも一つの方法です。気になるテーマや必要なテーマを選びます。最近はオンラインで開催されている勉強会も増えており、参加しやすくなっています。

Point② 他社から学ぶ

脆弱性の発見やセキュリティ事故の発生など、日々多くのセキュリティに関するニュースが流れています。対岸の火事ではありません。他社で起こっていることが自社でも起こらないとは言えない状態です。他社で起こったセキュリティ事故が自社でも起こる可能性があるか、起こらないようにするにはどのような対応をするか、起こった場合にはどのような対応をするかを日々考えることは、セキュリティ担当者としての成長を促します。

他社で発生したセキュリティ事故

↓

事故の概要を把握する

↓

自社での発生可能性の検討	発生防止策の検討	事故発生時の対応の検討
同じような事故が自社で起こる可能性があるかを考えます。自社の環境や攻撃の特徴を整理しさまざまな可能性を考慮していくことで、担当者としての見識が深まることが期待できます。	他社で発生したセキュリティ事故を自社で起こさないためにどのような取り組みが有効か考えます。組織・人・技術・物理と検討していくことで、対応策を幅広く検討でき、見識が深まることが期待できます。	もし同じような事故が発生した場合にはどのような対応が必要か検討します。連絡を取る関係機関や顧客対応などを考えていくことで、セキュリティ事故の模擬訓練ともなります。

Day10

3.これからの活動

セキュリティ担当者として成長するために

Point③ コミュニティへ参加する

コミュニティへ参加することで、情報の交換や事例の収集などがしやすくなります。また、信頼できる相手からの情報であり、わからないことも聞きやすいという特徴があります。

情報獲得	事例共有	人材交流
コミュニティ内では、有識者からの情報発信などが行われているものも多く、セキュリティの知識やスキルアップにも繋がります。自社のセキュリティ対策のヒントにつながる情報を得ることも期待できます。	交流会では、自社のセキュリティ対策などの事例を共有し合うなど、双方向でコミュニケーションをとることができます。これにより、インプットだけでなくアウトプットによる知識の定着が期待でき、成長に繋がります。	セキュリティのスキル・知識だけでなく、悩みや経験など人材交流も可能です。同じ境遇を持つ人材と交流することで視野が広がります。社内では言えないことを言うことで、モチベーション維持にも繋がります。

中小企業サイバーセキュリティ対策継続支援事業のFacebookもコミュニティです。参加者同志のコミュニティページではありますが、セミナーやワークショップのように連絡を取り合いわからないことを質問したり、関係者同士で事例などを共有することができると参加者に有意義な活動となります。ぜひ有効に活用し、コミュニティへ参加するメリットや意義を見出してください。

One Point

最近では、SNSを使って情報収集をするセキュリティ担当者は多くなりました。Facebookはもちろんのこと、TwitterやLINEグループなどを利用している担当者もいます。公的機関のSNSだけで無く、有志団体が行っているSNSからも有益な情報を得ることができます。また、有志団体のSNSでは質問することが可能な双方向コミュニケーションが取れることも多いです。ただし、顔が見えないSNSですので、利用時には相応の注意が必要です。まずは、公的機関のSNSをフォローし情報収集をしてみてはいかがでしょうか？

代表的なSNSアカウント

情報処理推進機構(IPA)（Twitter IPA公式アカウント）
https://www.ipa.go.jp/about/socialmedia/twitter.html

警視庁（警視庁サイバーセキュリティ対策本部）
https://twitter.com/mpd_cybersec

内閣サイバー(注意・警戒情報)
https://twitter.com/nisc_forecast

Day10

3.これからの活動

次の一歩へ

やることはわかってきたけれども、実際これからできるのだろうか、という不安もあると思います。また、セキュリティ事故が起こったらどうしようという不安もあることでしょう。やることを整理し、準備して進めていきましょう。

Point① 基本を意識し取り組んでいく

全10回のカリキュラムでは、スタンダードなセキュリティの対応フローに則り説明してきました。STEP1～５の長期的なPDCAを意識しつつ、STEP４では短期的なPDCAを進め、セキュリティの取り組みを推進させていきましょう。

STEP 1

■ 役割を意識し体制を整える

- 自分が担う役割を意識する
- 取り組む体制を整備する
- 必要なリソース（予算や工数）を確保する

テキスト第1回

STEP 2

■ デジタル化方針やDX、会社の方針を理解する

- 方針を把握し即したセキュリティを意識する
- DXやデジタル化には積極的に関わりを持つ

テキスト第2回

STEP 3

■ 資産を整理し、リスクを把握する

- 資産管理台帳を整備する
- 脅威や脆弱性を把握し自社への影響を把握する
- リスクに対しての対応方針を検討する

テキスト：第４回～第6回

STEP 4

■ リスクに対応する

- 組織・人・技術・物理対策の導入を計画する
- 計画を実行し実行結果を評価する
- 振り返りを行い、次の取り組みを検討する

テキスト：第7回～第9回

STEP 5

■ STEP１～４の評価・振り返りをする

- 現状できていない点はどのあたりかを把握する
- 次の施策のために何が必要かを検討する

日々取り組むこと

■ システムの状態を把握する

- システムの動作状況を確認する
- ログを取得、確認する
- 異常を検知する

■ ヒヤリハット・事故に対応する

- エスカレーションや相談に対応し、解決を図る
- トリアージを行う
- 事故対応を行う

■ 記録をつける、確認する

- 入退室や作業、貸与物の貸し出しなどの記録を確認する
- エスカレーションの内容、対応、結果を記録する
- 長期・短期PDCAの活動記録をつける

■ 情報収集を行う

- 脅威や脆弱性の情報を収集する
- 関連する法律やガイドラインなどの情報を収集する
- セミナーや勉強会の開催情報を収集する

■ 共有・報告・連携を行う

- 関係者、組織・チーム内で状況を共有する
- 経営層へ報告する
- 外部機関と連携をする

次の一歩へ

Point② 悩んだ時は

セキュリティの取り組みを進めていく中で、全く悩みがないということはありません。そんな時は基本に立ち返りつつ、目的を意識して臨んでいきましょう。

何に取り組めばいいのかわからない

まずは基本に立ち返り考えていきましょう。やるべきことは数多くあります。ひとつひとつ確認をしながら、何から取り組むべきか考えましょう。

1. 資産管理、リスクアセスメントを行い、リスクに対して取り組みを検討する
2. サイバーセキュリティフレームワークを使い不足するポイントを検討する
3. 会社が目指すビジョンやデジタル戦略から取り組みを検討する

どのような手段を取ればいいかわからない

実際に手段を考えるためには、事例や製品・サービスを知っている必要があります。

1. 事例や具体例などを収集し、自社で利用できそうな手段を導入する
2. コミュニティなどに所属し相談する
3. 保守業者や専門家など外部の有識者に頼る

対応できる人がいない、時間がない

人ではなく、組織として対応できるように考えていきましょう。組織の成熟度を意識し、人が入れ替わることを前提として取り組みましょう。

1. 役割と責任、体制図を定め関係者を巻き込んだ活動をする
2. 会社としてセキュリティの取り組みに理解を持ち、セキュリティ担当者が動きやすい環境を作っていく
3. 保守業者や専門家など外部の有識者に頼る

効果があるのか、効果が出ているのかわからない

効果をどのように測定するかは計画の段階で決めておきましょう。セキュリティ事故が起きないことを効果とすることもできますが、各取り組みに対して、どのような結果が出ており、評価できるかを意識しましょう。

1. 過去との差分を確認し効果を把握する。監査やチェックリストを活用し現在の状態を把握し、過去の記録と比較をすることで効果を測定する
2. ログを取得しログの記録を持って効果を把握する。不正な通信を止めたログや外部からの攻撃可能性のある通信がどの程度セキュリティ機器で制御されているかを把握する
3. PDCAのサイクルの活動記録や年間計画の達成度で測定する。目標を定め進捗や達成度を示し、日々の活動の効果を測定する

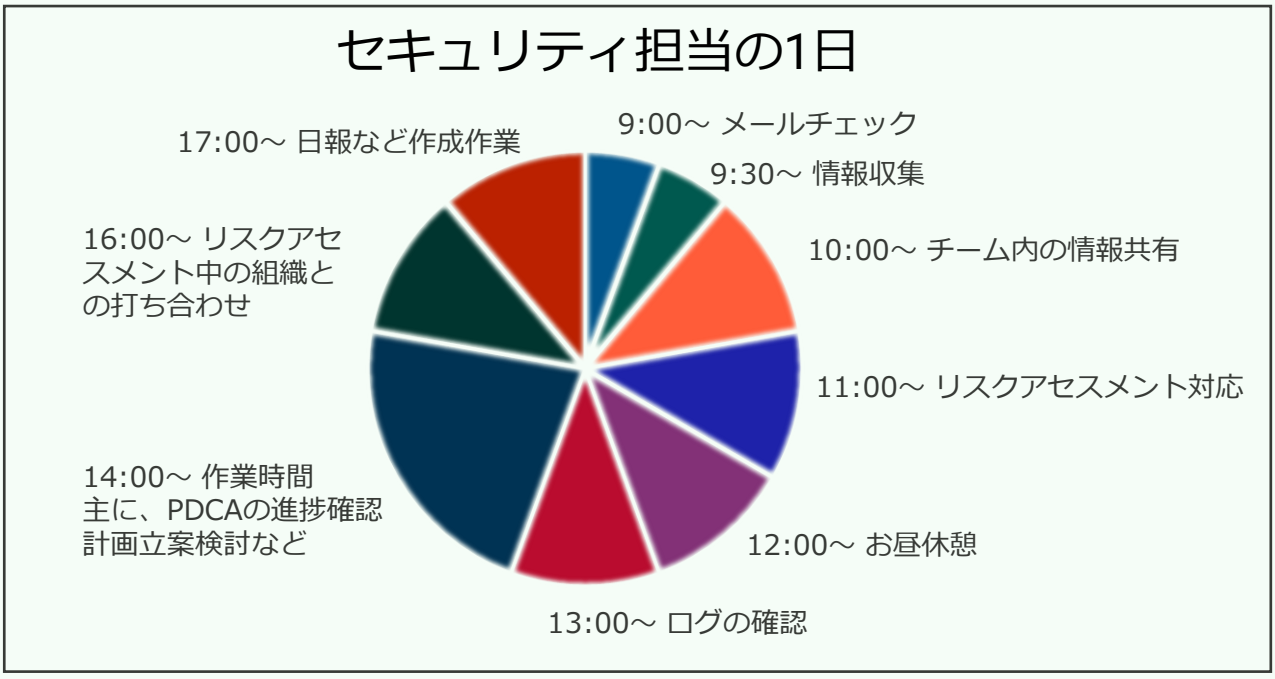
Day10

3.これからの活動

セキュリティ担当者の1日

ある会社のセキュリティ担当者の仕事は、情報収集から始まります。主にセキュリティ関係のニュースを確認し、新たな脆弱性や企業の事故報告の発表などを見ていきます。新たな脆弱性が発見された時は、自社で対応が必要かCVSSを用いて確認します。1日の内、30分くらいこの情報収集に時間を充てています。

セキュリティ担当者の仕事は主に社内のセキュリティの維持向上です。そのため、現在取り組んでいる短期的なPDCAを対応していくことが日々の業務の中心となっています。今は、リスクアセスメントを進めており、実行フェーズとして資産管理台帳の更新を関係部署と調整して進めています。資産管理台帳を作成する際の質問に答えることが最近は多いです。資産管理台帳の更新はもう少しで終わりそうなところまで進んでいます。この後は、資産管理台帳に記載されている内容と、実際の資産が合っているのかを確認していく予定です。流石に全ての部署で全ての資産を確認していくことは難しいので、対応部署が悩むような資産や記載がおかしいような資産について確認する計画を作っています。



午後の業務はログの確認から始めます。異常なログはアラートとして発報されるようになっていますが、能動的に調べる癖をつけることで、アラートに上がらない危険性に気付けることがあります。以前は従業員のルール違反を発見し、注意喚起を行いました。事故を未然に防ぐためには必要な作業だと思っています。

1番大変なのは、事故対応が発生した時です。誤送信や紛失事故では対象者に指示を出し、対応してもらいます。誤送信などは、本人に自覚があれば対応を収束させますが、身に覚えがないような場合には本格的な事故対応となり、全ての予定をキャンセルして、対応にあたります。基本的にはインシデント対応規程や手順書に沿って対応していきますが、内容によっては自分で考えて対応しないといけないため、知識やスキルの必要性を1番感じるタイミングです。

最近ではDXの流れから、サービスに対してのセキュリティを考える機会が増えてきました。いままでは社内セキュリティだけでしたが、事業についてやサービスを買ってくれるお客様、売り上げなども考えないといけないため、今まで以上に意識しないといけないことが増えました。そのため、セキュリティの知識をアップデートしようと努力しています。

Day10

3.これからの活動

セキュリティ担当者としての成長

ある会社のセキュリティ担当者は、担当者に任命されて5年が経とうとしています。任命当初は何をすればよいのか全くわからなかった担当者ですが、今では経営層にもレポートする立派な担当者として、社内に欠かせない人材となっています。もともと、セキュリティの勉強をしていたわけでなく、人事異動により、担当となりました。担当になったからにはと、日々の業務や勉強を通して、セキュリティの知識をつけてきました。

1年目の目標

- セキュリティ関連の書籍を月1冊読む

まずは知識をつけることが大切だと感じた担当者は本を読むなどして、セキュリティとは何か、どのような業務があるのか、自分に求められているものは何かを考えました。特に意識したことは、自分に求められていることは何かです。セキュリティの業務は幅広く、全てを行うことは不可能だと思った担当者は自分に必要なスキル、知識を身につけることから始めました。

2年目の目標

- 情報セキュリティマネジメント試験に挑戦
- 発表されるレポートなどを読む
- ニュースから情報を集める

だんだんと知識がついてきたと感じた２年目は、情報セキュリティマネジメント試験に挑戦しました。試験では体系立てた勉強ができるため、本を読んでつけた知識を整理することができました。試験と合わせて、発表されるレポートなども読むようになりました。IPAが発表する資料などを読み、最近の事例に広く触れることができるようになりました。また、ニュースも見るようになり、企業の被害の状況などもわかってきました。最近では、もし自社で同じような攻撃が起こったらと考え、模擬訓練をしています。

3年目の目標

- セミナー参加

３年目には外部のセミナーにも参加しました。初めてセミナーに参加した時のドキドキは今も覚えているそうです。緊張で話を覚えていないこともあるそうですが、セミナーで話が分かった喜びも感じ、セキュリティの業務の楽しさも感じ始めました。

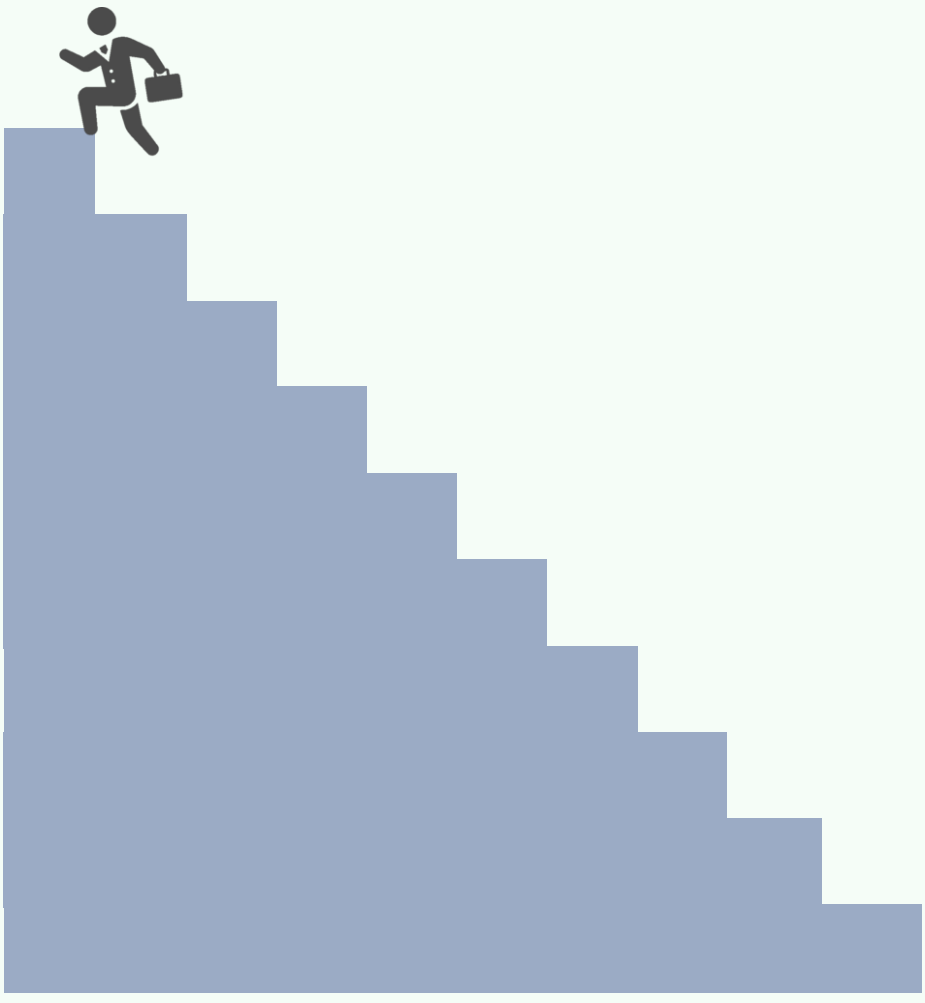
以降はニュースや資料を読みつつ、気になった書籍を読むようにし、知識のアップデートをはかっていきます。セキュリティ関連の業務を行う中でわからないことは調べながら進められるようにもなってきたため、業務をすることが1番の勉強になっています。新しい役割も任され、さらに知識をつけないといけない点はありますが、日々充実して業務にあたれています。

この会社の担当者は、セキュリティの仕事に就いたことを前向きな形で捉え、日々意識しながら業務してきました。だんだんと知識がついてくることを楽しさと捉えながら取り組んでいくことが成長の近道なのかもしれません。

この1年間セミナーや支援を受けてセキュリティの考え方や取り組むべきことがわかってきた。ただ、これからは一人で実施していくと思うと不安な気持ちもある。困ったら、周りに助けを求めることも必要だろう。社内の協力者と連携をとりながらセキュリティの取り組みを進めていこう。

会社は今後デジタル化やDX化を進めていくことだろう。実現すべきビジョンを実現するためにもセキュリティは重要だ。しっかりと自分の会社に必要なセキュリティを考えて取り組んでいこう。まずは次年度の計画を作り、実行していこう。ここからが本当のスタートだ。

セキュリティで会社を成長させる！



コラム
～セキュリティを担当してよかったこと～

セキュリティの業務は基本的に大変なことが多いです。セキュリティを強化した結果、一手間増えたと事業部門から小言が出る場合もあります。「もし、セキュリティ事故が発生したら自分が悪いの？」というプレッシャーを感じることもあるかもしれません。セキュリティ担当者となることは不運なことなのでしょうか？

セキュリティを担当してよかったことを各企業の担当者に聞くと、普段の業務では得られない経験という答えが返ってきます。社内で有識者がいないため、一から考え実施した経験は人生においても転機となったという回答もありました。また、人がいないからこそ頼られるという経験は人の役に立っているというやりがいにも繋がっているという回答もあります。

他にも、普段出会わない人たちとの出会いと回答した担当者もいます。事業部門ではライバル企業でも、セキュリティでは協力しあえることで、同業界関係者とコミュニティが広がったそうです。

セキュリティ担当者として、価値や楽しみを見出し取り組めることが、自身の成長や価値を高めていくのかもしれません。

あとがき

全10回が終了しました。ありがとうございました。10回目は日々の業務や働き方について記載を行ってきました。セキュリティの業務は担当者のボランティア精神ではできません。しっかりと計画を練って取り組んでいくことが大切です。全10回を通して、何を考え、どのような取り組みを進めていけばよいのかをまとめてきました。これからは取り組みをどのような手段で実行していけばよいのかなど悩むことはあると思います。手段は無限大です。だからこそ、効果がある手段を選定し実行していく必要があります。これからはこの実行手段に着目し各社の情報を集めるなどし、幅広い手段を活用できるように意識をしてみてください。いろいろな意見を聞くことで、自社にあった手段が見つかるはずです。会社の継続的な成長の為、セキュリティからより良い効果を出せるように期待しています。

令和4年度
中小企業サイバーセキュリティ対策継続支援事業