配信予定日：2025 年 7 月 1 日(火) 14:00 頃

カテゴリ：もっと知りたい！ セキュリティ

タグ：＃知識編

過去記事焼き直し：する（過去記事を上書きします）

過去記事：https://cybersecurity-taisaku.metro.tokyo.lg.jp/know_more/05/

クラウドサービスを安全に利用するポイントとは（1/3）

目次

中小企業の経営者や情報システム担当者の皆さん、日々のセキュリティ対策、お疲れさまです。本記事では「クラウドサービスを安全に利用するポイント」について解説します。

近年、働き方改革や新型コロナウイルス感染症対策の影響でテレワークが急増しました。それに伴い、インターネットがあればどこでも仕事ができるクラウドサービスへの移行が進んでいます。今後、ますます普及すると考えられるクラウドサービスを安全に利用するためのポイントについて 3 回に分けて解説します。

１．クラウドサービスとは

インターネットを通じてソフトウェアやハードウェアを利用する情報システムサービスのことを指します。利用者から見えない場所にあるコンピュータを利用することから「クラウド（cloud、雲)」と呼ばれています。

経営管理アプリケーション（財務会計、税務申告、給与計算、労務管理)、業務アプリケーション（顧客管理、販売管理、名刺管理、ホームページ作成、EC サイト)、オフィスアプリケーション（ワープロ、表計算、グループウェア、電子メール、オンラインストレージ）など、さまざまなサービスがあり、利用が急速に進んでいます。代表的なものとして、皆さんにも身近なマイクロソフト社の Microsoft 365 などが挙げられます。

クラウドサービスは、提供される情報システム（ハードウェアやソフトウェア）の範囲によって、次の 3 つの形態に分類されます。

SaaS（Software as a Service の略。 読み方はサース)	会計アプリケーションやオフィスソフト、ファイルサーバーなど、一般に利用されているアプリケーションソフトをウェブサービスとして提供します。
PaaS（Platform as a Service の略。 読み方はパース)	OS やデータベース管理システムなどのミドルウェアを提供します。アプリケーションソフトは別途導入しなければなりません。
IaaS（Infrastructure as a Service の略。 読み方はイアース)	仮想のサーバーやメモリなどのハードウェアやネットワークなどのシステム基盤のみを提供します。

日本の PaaS 市場、IaaS 市場では、大手クラウドサービス（AWS（Amazon)、Azure（Microsoft)、GCP（Google)）の利用率が高く、特に AWS は、PaaS／IaaS 利用企業の半数以上を占めています。[*1]

*1総務省 令和 6 年度 情報通信白書　第 II 部　情報通信分野の現状と課題
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r06/html/nd218200.html

これらのクラウドサービスを提供する組織は「プラットフォーム事業者」「クラウドサービスプロバイダー」などと呼ばれます。一部のサービスでは、プラットフォーム事業者自身が、他の大手事業者が提供する PaaS を利用して業務用アプリケーションを構築し、顧客がそれを利用する、という形で 1 つのクラウドサービスが構築されることもあります。

この場合、複数事業者のサービスで構成されるため、サービス利用者には全体の構成が分かりにくく、サービスを選択するときの判断が複雑になることがあります。

２．クラウドサービスのメリット

クラウドサービスは情報システムを自社で所有・管理する必要がないため、ハードウェアやソフトウェアの導入・保守の費用や負担が軽減されます。
また、利用者はインターネットに接続するパソコンやスマートフォンがあれば、いつでも・どこからでも利用することができる、というメリットがあります。
国の情報システム導入におけるコスト削減や柔軟なリソースの増減などの観点から、「クラウド・バイ・デフォルト原則」や地方公共団体の経費削減や住民サービスの向上を図る「自治体クラウド」など、コンピュータ資源を所有せずに利用するクラウドが主流になりつつあります。

３．クラウドサービスの注意点

クラウドサービスはインターネットを利用するため、いつでも、誰でも、どこからでもアクセス可能である一方、絶えずサイバー攻撃のリスクに晒されています。例えば、動画配信サービスを提供するＡ社がサイバー攻撃をうけ、２ヶ月間のサービスの停止及び２５万件の個人情報の流出が起きた事例があります。原因は、フィッシングなどの攻撃で従業員アカウントが窃取されたためであるといわれています。
そのため、インターネット特有の脅威やリスクを考慮し、サービス提供事業者のセキュリティ対策を把握するとともに、利用者自身でできるセキュリティ対策を実行する必要があります。

４．クラウドサービスを安全に利用するためのポイント

（１） クラウドサービスのセキュリティは、サービス提供事業者と利用者がそれぞれの役割と責任を分担し、必要な対策を実施することで維持・向上します。
以下にクラウドサービスを安全に利用するためのポイントについて解説します。選択するときのポイント

(2)　運用するときのポイント

No.1 どの業務で利用するか明確にする	クラウドサービスでどの業務を行い、どの情報を扱うかを検討し、業務の切り分けや運用ルールを明確にしましょう。
No.2 クラウドサービスの種類を選ぶ	業務に適したクラウドサービスを選び、メリットについて確認しましょう。
No.3 取扱う情報の重要度を確認する	クラウドサービスで取扱う情報が漏えいしたり、改ざんされたり、消失、サービスが停止したときの影響を確認しましょう。
No.4 セキュリティのルールと矛盾しないようにする	セキュリティのルールとクラウドサービス活用との間に矛盾や不一致が生じないようにしましょう。
No.5 クラウド事業者の信頼性を確認する	クラウドサービスを提供する事業者は信頼できる事業者を選択しましょう。
No.6 クラウドサービスの安全・信頼性を確認する	サービスの稼働率、障害発生頻度、障害時の回復目標時間などのサービス品質保証を確認しましょう。
No.7 管理担当者を決める	クラウドサービスの技術的な側面などの特性を理解したうえで、業務に適した運用や設定・操作・ヘルプデスクを行うことができる、管理担当者を社内に確保しましょう。
No.8 利用者の範囲を決める	クラウドサービスを利用する人の範囲を決め、どのような権限を与えるか適切に管理しましょう。
No.9 利用者の認証を厳格に行う	パスワードなどの認証機能を適切に設定・管理しましょう。

No.10 バックアップに責任を持つ	サービス停止やデータの消失・改ざん等に備えて、重要情報を手元に確保して、必要なときに使えるようにしましょう。

（3） セキュリティ管理のポイント

No.11 付帯するセキュリティ対策を確認する	クラウドサービスにおけるセキュリティ対策が具体的に公開されているか確認しましょう。
No.12 利用者サポートの体制を確認する	サービスの使い方がわからないときの支援（ヘルプデスクやFAQ）が提供されているか確認しましょう。
No.13 利用終了時のデータを確保する	サービスの利用が終了したときの、データの取扱い条件について確認しましょう。
No.14 適用法令や契約条件を確認する	個人情報保護など関連法規制の遵守などを規定した利用規約等について確認しましょう。
No.15 データ保存先の地理的所在地を確認する	データがどの国や地域に設置されたサーバーに保存されているか確認しましょう。

なお、本稿は、独立行政法人情報処理推進機構（IPA）が発行している「中小企業の情報セキュリティ対策ガイドライン 第 3.1 版」[*2]を中心に解説しています。

[*2]中小企業の情報セキュリティ対策ガイドライン第 3.1 版
https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf

次回は、クラウドサービスを安全に利用するポイントの続きとして、実際に何をしたら良いのか、例を挙げて解説します。

配信予定日：2025 年 7 月 1 日(火) 14:00 頃
カテゴリ：基礎から学ぶ！ セキュリティ
タグ：＃実用編＃知識編
過去記事焼き直し：する（過去記事を上書きします）
過去記事：https://cybersecurity-taisaku.metro.tokyo.lg.jp/basics/04/

中小企業におけるセキュリティ脅威への対策強化　～不注意による情報漏えいの被害事例から対策を学ぶ～

目次

独立行政法人情報処理推進機構（IPA）が毎年発行している「情報セキュリティ 10 大脅威」の中で、特に中小企業の経営者やシステム担当者が注目すべき点を、2025 年版に基づいて詳細に掘り下げていきます。今回は 10 位に挙げられている「不注意による情報漏えい等」に焦点を当てます。これは長年にわたり頻繁に発生し続けており、この脅威がどのように業務に影響を与え、どのように対策すべきかを解説いたします。

「情報セキュリティ 10 大脅威（2025）」の組織編の一覧は下表のとおりです。※1

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い（2016年以降）
1	ランサム攻撃による被害	2016年	10年連続10回目
2	サプライチェーンや委託先を狙った攻撃	2019年	7年連続7回目
3	システムの脆弱性を突いた攻撃	2016年	5年連続8回目
4	内部不正による情報漏えい等	2016年	10年連続10回目
5	機密情報等を狙った標的型攻撃	2016年	10年連続10回目
6	リモートワーク等の環境や仕組みを狙った攻撃	2021年	5年連続5回目
7	地政学的リスクに起因するサイバー攻撃	2025年	初選出
8	分散型サービス妨害攻撃（DDoS攻撃）	2016年	5年ぶり6回目
9	ビジネスメール詐欺	2018年	8年連続8回目
10	不注意による情報漏えい等	2016年	7年連続8回目

情報セキュリティの落とし穴とされる不注意による情報漏えいは、知らず知らずのうちに発生することが多く、一度起こるとその影響は計り知れないものとなります。

「うちは中小企業だし、不特定多数の一般消費者を相手にするビジネスではないため、大量の個人情報は保有していないから、漏えいして困るような情報はないよ。」

中小企業の経営者の中にはこのような考えから、「自社はサイバーセキュリティによるリスクが低い」と過小評価していることが、事態を悪化させることもあります。

1．「中小企業はセキュリティによるリスクが低い」は本当？

中小企業であっても、日常的に行っている業務の中でセキュリティリスクにつながる情報を取り扱っているのではないでしょうか。

・自社 HP に「問い合わせ」フォームを設けており、入力欄に問い合わせをしてきた人の所属組織や連絡先などを記載する箇所がある
・従業員が名刺交換した相手先の情報を Excel 等で一覧管理し、「顧客リスト」として保有している
・過去に採用試験を受けた方の履歴書を保管している

これらは全て、個人情報や個人データとなります。他にも業務で日常的に取り扱う顧客データや、パートナー企業から預かっている機密情報、従業員の住所や家族構成といった個人情報等、これら全てが潜在的なリスクを孕んでいます。
こうした情報が漏えいした場合、信頼失墜、業務停止、収益の損失、法的責任など重大な結果を招くことになりかねないのです。このため、情報に関するセキュリティ対策は企業規模に関わらず全ての企業にとって必要な対策です。

では、実際に不注意によって情報が漏えいしてしまった具体的な事例をご紹介しながら、要因と対策をみていきましょう。

◆情報漏えいの具体的な事例

事例①　ハードディスクドライブ（HDD）のデータ未削除による個人情報漏えい

委託先従業員が外付け HDD を業務に使用し、顧客情報が含まれるデータを消去せずに廃棄したため、数か月後に上記 HDD を取得した第三者が顧客情報をみることができるようになっていた。※2

事例②　Micorsoft Teams の公開範囲を制限しなかったことによる個人情報漏えい

Micorsoft Teams（リアルタイムのコラボレーションやコミュニケーション、会議、ファイルやアプリの共有を行うことのできるメッセージングアプリケーション。以下 Teams）の公開範囲を制限せずに電子データをアップロードしたため、第三者が閲覧できる状態となっていた。※3

事例②の Teams 設定ミスは、公開範囲が「プライベート」ではなく「パブリック」となっているチームにアップロードしたことが原因であり、人的ミスによる情報漏えいの典型的なケースです。これには、適切なチェック体制の欠如や、業務担当者の情報セキュリティに対する意識の低さが影響しています。

２．情報漏えいの要因は、人的不注意

不注意による情報漏えいはなぜ発生するのでしょうか。先の「情報セキュリティ 10 大脅威」の解説資料には、次のような要因が挙げられています。※4

◇情報リテラシー・モラルの低さ

従業員が扱う情報の機密性や重要性等への理解やモラルが不十分な場合、不用意に外部へ情報漏えいしてしまう可能性があります。例えば、次のようなケースが考えられます。

・重要情報が記載されたメールの宛先を間違う
・重要情報が記載されたメール添付ファイルを取り違える
・重要情報が入った情報端末・記録媒体・紙を紛失する
・重要情報を私的に利用して外部の Web サイト等に公開する

◇情報を取り扱う際の本人の状況

体調不良や多忙等の状況により、情報を取り扱う従業員の注意力が散漫になり、メールの誤送信等のミスによる情報漏えい事故を起こしてしまうことがあります。

◇組織規程および情報を取り扱う手順の不備

外部に情報を持ち出す際の確認手順や作業時の確認手順等に関するプロセスに不備があると、情報漏えい事故を起こしてしまう可能性が出てきます。

３．中小企業による情報漏えいへの対策と対応

それでは、これらの要因を防ぎ、万が一事故が発生した場合の被害を最小限に抑えるためには、どのようにすればよいでしょうか。必要な対策、対応を「情報セキュリティ 10 大脅威」の解説資料をもとに一部加筆、抜粋して掲載します。※4

対策と対応①　情報リテラシー、モラルの向上

従業員が扱う情報の機密性や重要性を理解し、適切に扱うための教育を実施しましょう。
IPA が従業員研修で利用できる様々な研修テキスト例や動画教材を提供しています。
巻末のリンク先よりご高覧ください。※5

対策と対応②　ルール(手順)に基づく運用

情報の取り扱いに関する手順を明確化しましょう。さらに、従業員が確実に確認・実行できるようにすることが大切です。例えば、Web でのアンケートフォームを作成する際などは、権限設定などを確認することをチェックリスト化して、複数人でチェックをするとよいでしょう。

対策と対応③　特定の担当者に業務が集中しない体制の構築

情報管理の責任者を明確化し、複数の従業員で重要な情報についての扱い方について、チェックできる体制を構築しましょう。

対策と対応④　情報の重要度に応じた運用

扱う情報の重要度を分類し、それに合わせた運用（厳格な管理体制の構築）をしましょう。
また、電子データならファイル名の先頭に重要度を記載する等、情報ごとの重要度を媒体に

合わせラベリングをすることにより、情報ごとの重要度がいつでも確認できるようにしましょう。

対策と対応⑤　外部に持ち出す情報や端末の制限

持ち出し可能な情報や端末を制限し、持ち出しの記録を取る、持ち出し前に不必要な情報が格納されていないことを確認する、持ち出しの承認をする責任者を決める、従業員一人だけで持ち出しができないようにするといった対策を実施しましょう。

対策と対応⑥　適切なファイル送受信の運用

重要な情報が入ったファイルを相手に送信するときは、メールに直接ファイルを添付するのではなく、クラウド上のファイルストレージサービスの利用やファイルの暗号化など、安全なファイル送受信方法を検討してください。

セキュリティ対策が取られたファイルストレージでは、登録したファイルを特定の個人だけがアクセスできるように設定することができます。一般的には、ファイルを見せたい相手のメールアドレスなどを登録します。この方法を使うと、メールに直接ファイルを添付するよりも安全性が高いと言われています。

対策と対応⑦ メールの誤送信対策

メールソフトによっては、メール送信前に「このアドレスで本当に良いですか？」と確認を促す画面を表示させる機能や、送信者が送信ボタン押下後に「あ、間違えた！」と思った時に送信を取り消せるよう、送信ボタンを押してから 1 分後にメールを送信する機能、管理者の承認がないと送信できない機能が備わったものがあります。このようなソフトを使うことでメールの誤送信を減らすことができます。

漏えいが発生した（可能性を含む）時には、下記の対応が必要となります。

・早期の状況把握

問題発生時の内部報告体制を整備してください。

いつでも報告体制を確認できるようにしておきましょう。

外部からの連絡窓口を設置し、関係者が分かるようにしておきましょう。

・適切な報告／連絡／相談

問題が発生した場合、速やかに報告し、適切な対応を取れるよう社内・社外の関係組織や公的機関等と連携できるようにしておきましょう。

・インシデント対応体制の整備

問題発生時に迅速かつ的確に対応できる体制を整えます。

具体的な対応については、IPA の「中小企業の情報セキュリティ対策ガイドライン」の 46 ページ（5）セキュリティインシデント対応をご覧ください。※6

ここまで不注意による情報漏えいの事例や影響、対策方法について考えてきましたが、いかがだったでしょうか。
不注意による情報漏えいはどの企業でも起こりやすく、その影響は甚大です。不注意を完全になくすことはできませんが、ルール整備や従業員への教育によるリテラシー及びモラル向上を図ることが、企業の持続可能な発展を支える鍵となるでしょう。

※1 出典：独立行政法人情報処理推進機構（IPA）
https://www.ipa.go.jp/security/10threats/10threats2025.html

※2 出典：SECURITY HOT TOPICS
https://www.itmedia.co.jp/news/articles/2406/14/news130.html

※3 出典：東京都教育委員会
https://www.kyoiku.metro.tokyo.lg.jp/information/press/2024/05/2024053105

※4 出典：独立行政法人情報処理推進機構（IPA）
https://www.ipa.go.jp/security/10threats/eid2eo0000005231-att/katsuyouhou_2025_soshiki.pdf

※5 出典：独立行政法人情報処理推進機構（IPA）
https://www.ipa.go.jp/security/kokokara/study/company.html

※6 出典：独立行政法人情報処理推進機構（IPA）
https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf

配信予定日：2025 年 7 月 9 日(水) 14:00 頃
カテゴリ：もっと知りたい！セキュリティ
タグ：＃知識編
過去記事焼き直し：しない（完全に新規投稿する記事です）
タイトル：
サイバーキルチェーンと MITRE ATT&CK

中小企業の経営者や情報システム担当者の皆さん、日々のセキュリティ対策、お疲れ様です。
本記事では「サイバーキルチェーンと MITRE ATT&CK」について解説します。

●サイバーキルチェーンの概要
サイバーキルチェーンとは、攻撃者の視点から、サイバー攻撃を行う際のプロセスを体系化したものです。企業のセキュリティ担当者や管理者は、サイバー攻撃のプロセスを知ることで、より有効なセキュリティ対策に役立てることが可能となります。
サイバーキルチェーンでは、サイバー攻撃のプロセスを次のように 7 つの段階に分けています。

１．偵察（標的に関する情報収集）
第一段階では、攻撃者はターゲットに関する情報を収集します。情報収集元は、一般に入手可能な公開ウェブサイトやニュース記事、SNS などがあります。なお、このように、一般に公開されている情報を収集、分析して活用する手法のことを OSINT (Open Source Intelligence)と呼びます。また、セキュリティ対策の強化を目的として近年企業等で導入が進んでいる ASM（Attack Surface Management）も OSINT です。ASM については過去記事及び別の回で解説します。

２．武装化（攻撃のためのツールやマルウェア等の作成）
第二段階では、攻撃者は攻撃に用いるツールやコード、マルウェアなどを準備します。第一段階でターゲットとなるサイト等の脆弱性に関する情報があれば、それを悪用して攻撃するプログラム（エクスプロイトコード）などを作成します。

３．デリバリ（メール／ウェブ等で標的にマルウェア等を送り付ける）
第三段階では、攻撃者はターゲットに対し、第二段階で準備したツールやエクスプロイトコード、マルウェア等を送り付けます。主な手段としては、メールのほか、侵害されたウェブサイトに誘導してダウンロードさせる方法などが用いられます。

４．攻撃（送り付けたマルウェア等を実行させる）

第四段階では、攻撃者は第三段階で送り付けたツールやエクスプロイトコード、マルウェア等によってターゲットの脆弱性を悪用し、侵入を試みます。

５．インストール（標的をマルウェア等に感染させる）
第五段階では、攻撃者はターゲットサイトの PC 等にマルウェアや攻撃ツール等をインストールし、攻撃の拠点とします。

６．コマンド＆コントロール（標的と C&C サーバとの通信を確立させる）
第六段階では、攻撃者は、攻撃拠点となる PC 等を遠隔から制御するために、インターネット上の C&C（Command and Control）サーバとの通信を確立させます。

７．目的実行（機密情報や個人情報を盗み出す等，攻撃者が目的を実行する）
最終の第七段階では、攻撃者は機密情報や個人情報を盗み出す、ファイルを暗号化してシステムが正常に動作できなくするなど、目的を実行します。

●MITRE ATT&CK の概要

MITRE ATT&CK（MITRE Adversarial Tactics, Techniques, and Common Knowledge：マイターアタック）とは、米国政府の支援を受けた非営利団体である MITRE 社が運用する、攻撃者の攻撃手法や戦術を分析して作成された、サイバー攻撃の目的や手法を中心としたナレッジベースです。

MITRE ATT&CK では，サイバー攻撃のプロセスを次の 14 の戦術（Tactics）に分け、各 Tactics における攻撃手法を Techniques, Sub-Techniques として分類しています。

表：MITRE ATT&CK における 14 の戦術（Tactics）

No.	Tactics（戦術）	概要
1	Reconnaissance	攻撃対象の情報収集
2	Resource Development	攻撃に必要なリソースの準備
3	Initial Access	初期侵入
4	Execution	悪意あるコードの実行
5	Persistence	確立したリソースの維持
6	Privilege Escalation	特権への昇格
7	Defense Evasion	防御の回避
8	Credential Access	認証情報へのアクセス

9	Discovery	攻撃対象環境の掌握
10	Lateral Movement	横方向への移動
11	Collection	攻撃目標に関するデータの収集
12	Command and Control	C&C サーバとの通信／制御
13	Exfiltration	データの窃取・送信
14	Impact	システムとデータの操作・中断・破壊

サイバーキルチェーンは典型的なサイバー攻撃のプロセス（順序）を表していますが、MITRE ATT&CK は、サイバーキルチェーンのように攻撃のプロセスを表すものではなく、攻撃者が用いる様々な手法等をより詳細に記述したものとなっています。

●参考情報
MITRE ATT&CK
https://attack.mitre.org/

本記事で取り上げている ASM についての詳細を、昨年度の令和 6 年度中小企業サイバーセキュリティ対策事業で記事を配信しています。より知識を得たい方は是非こちらもご参照ください。
https://cybersecurity-taisaku.metro.tokyo.lg.jp/topics/hottopic19/

配信予定日：2025 年 7 月 17 日(木) 14:00 頃
カテゴリ：もっと知りたい！セキュリティ
タグ：＃知識編
過去記事焼き直し：しない（完全に新規投稿する記事です）
タイトル：
ASM と Shodan

内容：
中小企業の経営者や情報システム担当者の皆さん、日々のセキュリティ対策、お疲れ様です。本記事では、近年企業等で導入が進んでいる ASM（Attack Surface Management）と、その実施方法の一つである Shodan（Sentient Hyper-Optimized Data Access Network）の概要について解説します。

●ASM の概要
ASM とは、外部（インターネット）からアクセス可能な機器などサイバー攻撃を受ける可能性のある自組織の IT 資産の情報を攻撃者の視点で調査し、それらに存在する脆弱性を継続的に評価する取り組みであり、「攻撃対象領域管理」などと訳されます。ASM は、専用のツールやセキュリティベンダ等が提供するサービスを活用して実施することが一般的です。

●ASM のプロセス
ASMは、次に示すように、主に 3 つのプロセスから構成されます。

(1) 攻撃対象の発見
最初のプロセスでは、外部からアクセス可能な企業等の IT 資産を発見します。具体的には、次のような手順で攻撃対象となる IP アドレス及びホスト名のリストを得ます。

① 組織名をもとに、公開ウェブサイトや WHOIS を利用し、当該組織が管理者となっているドメイン名を特定します。
② ①で特定したドメイン名に対し、DNS による検索や、ツールなどを活用することで、IP アドレス及びホスト名のリストを取得します。

(2) 攻撃対象の情報収集
（1）で発見した IT 資産の OS やソフトウェア、ソフトウェアのバージョン、開いているポート番号などの情報を収集します。このプロセスでは、情報収集によって調査対象に影響を及ぼさないよう、ウェブページの表示など、通常のアクセスの範囲で行われます。

(3) 攻撃対象のリスク評価

(2) で収集した情報と、公開されている既知の脆弱性情報から脆弱性が存在する可能性を確認し、攻撃面のリスクを評価します。

●ASM 実施による効果

ASM を実施することによる効果として、次が挙げられます。

・情報システムを管理している部門が把握していない自組織の IT 資産とその脆弱性を発見できる。

・情報システムを管理している部門の想定と異なり、公開状態となっている自組織の IT 資産とその脆弱性を発見できる。

●ASM と脆弱性診断の違い

ASM の主な目的は、自組織の IT 資産に存在する脆弱性を発見、評価することであり、脆弱性診断と同じといえますが、次のように、いくつかの観点で異なります。

① 対象とする IT 資産の範囲

ASM は外部からアクセス可能な自組織の全ての IT 資産が対象となり、把握していない IT 資産も含まれます。一方、脆弱性診断では、把握されている IT 資産のみが対象となります。

② 脆弱性の確度

ASM では、発見された IT 資産に含まれている可能性のある脆弱性情報を提示しますが、それはあくまで可能性のレベルであり、脆弱性を特定しているわけではありません。一方、脆弱性診断では、対象となる IT 資産に疑似的な攻撃を行い、その応答を評価して脆弱性を特定します。したがって、ASM に比べ、脆弱性診断の方が脆弱性特定の確度は高いといえます。

表：ASM と脆弱性診断の比較

	対象範囲	脆弱性の特定確度	対象への影響
ASM	外部からアクセス可能な全ての IT 資産	可能性のレベルであり、脆弱性を特定しているわけではないため確度は低い	アクセスパケットがセキュリティ監視機器等に検出されたり、対象の IT 機器の動作に影響を及ぼしたりすることはほとんどない

脆弱性診断	診断対象としてあらかじめ特定したIT資産	疑似的な攻撃を行い、その応答を評価して脆弱性を特定しているため確度は高い	診断のパケットがセキュリティ監視機器等に検出されたり、対象の IT 資産の動作に影響を及ぼしたりする場合がある

このように、ASM と脆弱性診断は、その対象範囲や得られるアウトプットは異なるものであるため、目的に応じて使い分けや併用を検討すべきです。

●Shodan の概要

Shodan は、外部に公開された世界中のサーバやネットワーク機器等の情報を収集・蓄積し、公開している検索エンジンであり、ASM のツールとして活用することができます。Shodan は無償で利用可能ですが、より使い勝手の良い買い切りの有償アカウントや、サブスクリプションによる複数のプランなどもあります。かつては攻撃者が利用するサイトとして認識されていたこともありましたが、現在では ASM の代表的なサービスとして広く活用されています。

●参考情報

ASM（Attack Surface Management）導入ガイダンス～外部から把握出来る情報を用いて自組織の IT 資産を発見し管理する～（経済産業省）
https://www.meti.go.jp/press/2023/05/20230529001/20230529001.html

Shodan
https://www.shodan.io/
※本サービスは民間企業により提供されており、東京都が特定の事業者を推奨するものではありません。

本記事で取り上げている ASM や脆弱性診断は、昨年度の令和 6 年度中小企業サイバーセキュリティ対策事業でも制作しています。観点や内容が異なりますのでより知識を得たい方は是非こちらもご参照ください。
https://cybersecurity-taisaku.metro.tokyo.lg.jp/topics/hottopic19/

配信予定日：2025 年 7 月 17 日(木) 14:00 頃
カテゴリ：ホットトピックス
タグ：＃初級編
過去記事焼き直し：しない（完全に新規投稿する記事です）
タイトル：東京都サイバーセキュリティ対策事業の成り立ちと今後について

内容：
本記事では東京都サイバーセキュリティ対策事業について、各支援内容や活用方法等をご説明させていただきます。令和 7 年度事業にお申込みいただいた方、今後参加を検討している方、是非ご覧ください。

●中小企業の対策レベルに応じた支援メニュー
東京都サイバーセキュリティ対策事業は、セキュリティ対策にこれから着手する企業から、より高度な対策をしたい企業まで、対策度合い（レベル）に応じた支援メニューを用意しています。また、現状を把握し次に何をするべきか整理したい企業のためのメニューも用意しています。

[支援メニューと概要]
レベル１：啓発事業、セミナー・メール訓練・ネットワーク調査等
レベル２：基本対策事業、UTM/EDR の試行導入・規程策定支援等
レベル３：実践力強化プログラム、セミナー・ワークショップ・課題解決支援等
レベル３：インシデント対応強化、CSIRT 構築・IT-BCP 策定支援等
全レベル：フォローアップ、メルマガ・セミナー・セキュリティ対策点検等

各事業の概要を示した図

●東京都が考える情報セキュリティ対策のロードマップ

本事業の前身となる事業は、令和２年まで遡ります。
[参考]https://www.cybersecurity.metro.tokyo.lg.jp/torikumi/291/
当初はセキュリティ対策機器設置や標的型攻撃メール訓練等を行っていましたが、毎年度事業内容をアップデートしています。昨年度から、現在の５つの支援メニューを開始しています。

支援メニューは、中小企業の情報セキュリティ対策のロードマップとなっています。
啓発事業で情報セキュリティ対策の必要性を認知し、基本対策事業でセキュリティ対策機器の導入や規程策定等の一歩目を踏み出し、実践力強化プログラムで継続的なセキュリティ対策をできる人材を育成、インシデント対応強化でサイバー攻撃を受けた際の的確な対応方法や事象の復旧までを行います。これらロードマップの支援メニューと並行してフォローアップを設置しています。フォローアップは、上記支援を受けた方（過去支援企業）を中心に、セキュリティ情報の提供、点検による現状把握と改善をサポートします。

●東京都サイバーセキュリティ対策事業の活用方法

フォローアップのメルマガを除き、支援メニューは毎年度１社１メニューまでご参加いた

だけます。
支援メニューは、企業の状況に応じてうまくご活用いただきたいと考えております。活用方法を例にあげると
・ロードマップに沿って「レベル１→レベル２→レベル３→レベル３」と順番に参加する。
・「レベル１」に参加し以降は自社で１年以内にレベル３相当迄実施する。
・「レベル２」に参加後一旦「フォローアップ」のセキュリティ点検を受けて現状把握をする。
等が考えられます。
なお、本記事を執筆する NTT 東日本株式会社はインシデント対応強化とフォローアップを手掛けておりますが、これら支援メニュー参加者の半数以上は、東京都事業の過去参加企業になっています。昨年度（令和６年度）事業の評価が高かった事、ロードマップとして活用いただいている事が推察されます。

●東京都サイバーセキュリティ対策事業の今後

本事業の来年度の実施については、現時点では未定となっております。
事業の継続や発展には、皆さまの声が重要となっております。皆さまの声をお届けいただく手段として、ご参加いただいている各事業で行われるアンケートに加え、フォローアップのメルマガがございます。メルマガではセキュリティに関する記事だけでなく、アンケートやセキュリティセミナー（開催後アンケート取得）をご案内します。まだ登録されていない方は、是非ご登録いただきますようよろしくお願いいたします。
[フォローアップのメルマガの登録はこちら]
https://cybersecurity-taisaku.metro.tokyo.lg.jp/mail-magazine/

また、令和７年度事業では５つの支援メニューを束ねるポータルサイトの制作・運営も始めています。現在はフォローアップのメルマガで配信する記事の更新情報掲載がメインとなっておりますが、今後、さらに皆さまのお役に立てるよう検討を進めております。
[ポータルサイト]
https://cybersecurity-taisaku.metro.tokyo.lg.jp/

今回は他の記事と異なり、東京都事業の運営側の目線も交え、東京都中小企業サイバーセキュリティ対策事業をご紹介させていただきました。本事業は企業様への専門家派遣に重きを置いており、今後の事業継続や改善に向けた、皆さまの意見を収集しやすいものとなっております。2025 年 7 月 17 日時点、既に参加締め切りを迎えた支援メニューもございますが、支援メニューへのご参加、メルマガ登録、ポータルサイトの活用等で皆さまの情報セキ

ュリティ対策を進めていくとともに、より良い事業となるよう支援メニューにより派遣された専門家やアンケートへご意見いただければ幸いです。

配信予定日：2025 年 7 月 25 日(金) 14:00 頃
カテゴリ：もっと知りたい！セキュリティ
タグ：＃知識編＃インシデント対応強化
過去記事焼き直し：しない（完全に新規投稿する記事です）

【題名】
脅威ベースのペネトレーションテスト「TLPT」の概要と事例

【目次】
●TLPT の概要
●TLPT の主な特徴
　１．本番環境での実施
　２．レッドチームが攻撃を実行
　３．ブルーチームが攻撃の防御、検知、対応等を実施
　４．実際のサイバー攻撃に基づいた脅威シナリオの作成
　５．外部機関による実施
　６．実施結果の検証及び改善
●TLPT の実施事例

【本文】
中小企業の経営者や情報システム担当者の皆さん、日々のセキュリティ対策、お疲れ様です。
本記事では、金融庁等が実施を推奨している TLPT（Threat-Led Penetration Testing：脅威ベースのペネトレーションテスト）について解説します。

●TLPT の概要
TLPT とは、実際のサイバー攻撃の脅威に関する情報を収集・分析した結果（脅威インテリジェンス）を活用し、それを模した手法を駆使することで企業等のサイバーセキュリティ対策の有効性を総合的に評価する手法であり、金融庁が発行する「金融分野におけるサイバーセキュリティに関するガイドライン」等で対応が望ましい事項とされています。
実施方法によりますが、一般的な脆弱性診断とは異なり、サイバー攻撃への耐性だけでなく、その検知や対応力まで含めた組織の「サイバーレジリエンス」のレベルを評価することが可能となります。なお、サイバーレジリエンスについてはまた別な回で解説する予定です。

●TLPT の主な特徴
TLPT は画一的な手法で行うものではなく、実施する企業ごとに最新の脅威動向を踏まえて実施方法を検討し、個別にカスタマイズしたシナリオを用いて行うのが特徴であり、主な

ポイントとして次のようなものがあります。

１．本番環境での実施
TLPT は、現実世界で実際に起きているサイバー攻撃を動的にシミュレーションし、その侵害に対処するための攻撃対応能力を高めることに焦点を当てています。したがって、テストは本番環境で実施されます。

２．レッドチームが攻撃を実行
TLPT では、レッドチームと呼ばれる攻撃を担当するチームが、脅威シナリオをベースに対象組織に攻撃を仕掛けます。レッドチームは本物の攻撃者さながらの攻撃技術を駆使して対象組織のネットワーク内に侵入し、潜伏し続けながら最終的な攻撃目的を達成するために活動します

３．ブルーチームが攻撃の防御、検知、対応等を実施
TLPT では、テストを受ける側の組織はブルーチームとして、レッドチームによるサイバー攻撃に対して現実のサイバー攻撃と同様に、防御、検知、対応等を実施します。ただし、金融庁等ではブルーチームに予告することなく TLPT を実施することを求めています。
TLPT によって一連の攻撃と防御をシミュレーションすることで、サイバー攻撃の各段階においてどのような攻撃を許してしまう可能性があるのか、現状のセキュリティ対策のどこに不備等があるのかを検証することができます。

４．実際のサイバー攻撃に基づいた脅威シナリオの作成
TLPT で用いる脅威シナリオは、レッドチームが収集・分析した脅威インテリジェンスをもとに作成されます。個々の企業や業界の特性等を踏まえ、現実に直面するおそれのあるサイバー攻撃について、攻撃者はどのような集団か、攻撃目的は何か、どのような技術や手法を使用するか等を分析し、リアルかつ具体的なシナリオを作成します。なお、金融庁からは MITRE ATT&CK やサイバーキルチェーン等のフレームワークを活用することが推奨されています。
※MITRE ATT&CK やサイバーキルチェーンについては以下の記事で解説しています。
https://cybersecurity-taisaku.metro.tokyo.lg.jp/know_more/cyberkillchain-mitreattck/

５．外部機関による実施
TLPT は、その客観性と信頼性を確保するため、外部のセキュリティ専門ベンダや機関等による実施が望ましいとされています。

６．実施結果の検証及び改善

テスト実施後は、レッドチームによるサイバー攻撃に対し、ブルーチームがどのような方法やタイミングで防御、検知、対応等できたのか、また、技術面の脆弱性のみならず、人・組織、プロセスにおいてどのような脆弱性や不備、課題等があったのかを検証し、今後の改善につなげていく必要があります。そのため、TLPT の実施目的や結果を企業の経営層が理解し、リスクマネジメントや投資判断に活かすことが求められます。
なお、TLPT において、主に評価・調整・監督等を行う担当はホワイトチームと呼ばれます。

●TLPT の実施事例
次に、国内企業の TLPT 実施事例を一つご紹介します。
こちらの会社（A 社とします）では、外部のセキュリティベンダの協力のもと、下記のような方法で TLPT を実施しました。

・実施対象
　社内情報系ネットワークに接続されている PC
・脅威シナリオ概要
　標的型攻撃メールによるマルウェア感染による情報漏洩
　＜主なプロセス＞
　① 標的型メール開封によるマルウェア感染
　② 情報窃取
　③ 外部への情報漏洩
・攻撃プロセスと A 社 TLPT での実施内容
　A 社では攻撃のプロセスを次のように 6 段階で検討しましたが、全てのプロセスを実施するのは時間やコスト等の制約から難しい状況であったため、No.1 の事前調査プロセスは省略し、太枠線内の No.2 以降のプロセスを実施しました。また、No.3 以降のプロセスについては、前のプロセスの成否によらず実施する等、限られた期間で一定の成果が得られるように工夫をしています。

No	攻撃プロセス	実際の攻撃の例	A 社 TLPT での実施内容
1	事前調査	実際に流出している情報や入手可能な範囲で対象となる組織のアドレス等を事前調査する。	今回は実施せず、**事前に必要な情報を入手する。**

2	攻撃 （初期感染）	No.1 の結果に基づき、下記のプロセスで初期感染を試みる。 ①攻撃メールを送る ②攻撃メール/ファイルを開かせる ③マルウェアをダウンロード/実行させる	No.1 の情報に基づき、下記のプロセスにより初期感染が可能かどうかを確認する。 ①疑似攻撃メールを送付/受信 ②疑似攻撃メール/ファイルを開く ③疑似マルウェアのダウンロード/実行
3	端末乗っ取り	No.2 に成功した場合、マルウェアが C&C（Command and Control）サーバと通信しつつ、初期感染した端末の設定情報収集や攻撃ツールを追加導入し、遠隔操作を試みる。	**No.2 の成否によらず、No.3～5 を実施する。** ①非調査用 PC の設定情報等の収集・遠隔操作 ②ネットワーク内の脆弱性などの調査・探査 ③情報の取得
4	ネットワーク内調査	No.3 に成功した場合、当該端末を攻撃拠点とし、ネットワーク構成や攻撃利用できる脆弱性などのネットワーク内の調査を行う。	
5	侵入拡大	No.4 で取得した情報を基に、遠隔操作により、侵入拡大や目的とする情報の取得を試みる。	
6	情報漏えい	No.5 で取得した情報を外部に転送する。	**No.3～5 の成否によらず、実施する。** ①外部サイトへ PC 上のファイル転送可否を確認

●参考情報

金融分野におけるサイバーセキュリティに関するガイドライン
https://www.fsa.go.jp/news/r6/sonota/20241004/18.pdf

金融庁におけるサイバーセキュリティに関する取組状況
https://www.nisc.go.jp/pdf/council/cs/ciip/dai38/38shiryou0301.pdf

諸外国の「脅威ベースのペネトレーションテスト（TLPT)」に関する報告書
https://www.fsa.go.jp/common/about/research/20180516/TLPT.pdf

配信予定日：2025 年 7 月 25 日(金) 14:00 頃
カテゴリ：もっと知りたい！ セキュリティ
タグ：＃実用編＃知識編＃インシデント対応強化
過去記事焼き直し：する（過去記事を上書きします）
過去記事：https://cybersecurity-taisaku.metro.tokyo.lg.jp/know_more/mottosiritai4/

【題名】
【令和 7 年度版】セキュリティインシデント対応（1/2）

【目次】

【本文】
中小企業の経営者や情報システム担当者の皆さん、日々のセキュリティ対策、お疲れ様です。
本記事では、これまでに「クラウドサービス利用時の注意点」について解説してきました。

今回は実際に何か問題が生じた際に対応が求められるセキュリティインシデントについて、
重要なポイントを分かりやすく、具体的な事例も交えてお伝えします。

１．セキュリティインシデントとは
まず、セキュリティインシデントの定義を確認しましょう。

セキュリティインシデントとは、情報漏えいやシステムの停止などセキュリティに関わる

事故や出来事（事象ともいう）を指します。単に「インシデント」と呼ばれることもあります。

事故は、情報の漏えいや改ざん、破壊・消失、情報システムの停止などが挙げられます。

事象は、事故につながる可能性がある出来事です。メールを誤送信したが情報漏えいにはいたらなかった、あるいは誤送信しそうになったが送信する前に気づいた場合などです。

２．インシデント対応の必要性

インシデントが発生しないように様々な対策を取っていても、予期せぬインシデントが起こる可能性はあります。万が一インシデントが発生した場合には、被害や影響範囲が最小限になるようにし、事業を継続できるようにする必要があります。

３．インシデント発生時の想定被害

インシデントが発生した場合の被害には、直接的な被害と、間接的な被害があります。

【直接的な被害】　攻撃者による不正送金や金銭要求

対応人件費

原因調査や復旧のための外部委託費

復旧までの代替品費

取引先や顧客への謝罪対応費

法的対応のための弁護士費用　など

【間接的な被害】　関係者への被害波及

会社の信用低下

事業停止による機会損失　など

実際にセキュリティインシデント対応を行った際の被害などを集計したデータでは、具体的な被害として最も多いのがデータの破壊（35.7%）、次いで多いのが個人情報の漏えい（35.1%）でした。インシデントに遭うと３割以上の企業で事業運営や信頼性に直結する被害が発生する事が想定されます。
また、約 70%の企業が取引先への影響等の間接的な被害があったと回答しています。サプライチェーン全体でのサイバーセキュリティの不備は、企業自身のみならず取引先にも深刻な影響を及ぼす事が想定されます。※1

４．インシデント対応の目的

インシデントが発生したことで生じる被害とその影響範囲を最小限に抑え、迅速に復旧し、再発を防止することで、企業（組織）の事業が継続できるようにすることが目的です。

５．実際のインシデント対応

ここからは、実際にインシデントが発生した際にどのような対応が必要となるのか具体的なステップを説明していきます。

なお、インシデントの対応は、発生している事象・被害や影響範囲の大きさなどによって変わってきます。このため、インシデント対応時に下記情報をまとめて整理しておくことが大切です。

（１） インシデント対応時に整理すべき情報

インシデントの分類	情報漏えい、ウイルス感染、システム停止など
事業者の名称	事業者の名称（受託案件の場合は委託元）
責任者・担当者	本件に関する責任者及び担当者の所属、氏名
発覚日時	インシデントを認知（発見したり、通報を受けた）した日時
発生日時	調査で判明したインシデントの発生日時
発生事象	表面化している事柄、被害、影響など
対応経過	発生から現時点までの時系列での経過
想定原因	現時点で想定される直接的な原因
被害を受けたシステムの状況	被害を受けたシステムの概要と被害の詳細な状況
システム構成・運用状況	システムの物理的な所在場所 OS やアプリケーションとそれぞれのバージョン構成 システムの構成図

	システムの運用状況 使用しているセキュリティツールやサービスの利用状況

この中で、システム構成・運用状況はインシデントが発生してからでは整理できませんね。普段から整理しておくようにしましょう。

それでは、いまからインシデント発生時の具体的な対応手順と内容を説明します。

（2）インシデント対応時のステップ1・2・3

＜ステップ1＞検知・初動対応
インシデントが疑われる兆候（疑わしい場合を含む）や実際の発生を発見した場合は、すぐに社内の連絡ルールに従って情報セキュリティ責任者に報告します。ネットワークの遮断やシステムの停止を必要に応じて行い、被害の拡大を防ぎます。社外など外部から通報を受けた場合は、通報した人の連絡先を控えておくことも大切です。なお、メール誤送信などの場合は、起こってしまったことを報告しやすい社内風土を作ることも大切です。内部であれ、外部であれ、セキュリティインシデントは人による報告が早期発見につながるからです。※2

責任者への報告を済ませた後は、初動対応へと移ります。
ネットワークの遮断、情報や対象機器の隔離、システムやサービスの停止を必要に応じて行います。このステップの発見時の社内連絡フロー、初動対応の手順は平常時に定めておくことが大切です。

■平常時に定める初動対応手順の例■
「あなたのパソコンはウイルスに感染しています」と警告が出た場合、サポート詐欺（ウイルス感染はない）の可能性、もしくはウイルス感染した可能性があります。全従業者が発生事象の調査や対応を判断する事は困難なため、下記対応を行ってください。※3
【実施事項】
・社内の情報システム部門への連絡
・ネットワークの遮断
【禁止事項】
・画面をクリックしない
・ソフトウェアをインストールしない
・個人情報を入力しない
・電話を掛けない

・指示に従わない

＜ステップ２＞報告・公表
インシデントの影響が広範囲に及ぶ場合、Web サイトやメディアを通じて公表します。
第一報では、公表することで被害の拡大を招かないように、公表する時期や内容などを考慮します。

第二報以降では、被害者や、影響を及ぼした取引先や顧客に対して、インシデントの対応状況や再発防止策等に関して報告します。また、被害者に対する損害の補償等を必要に応じて行います。個人情報漏えいの場合は個人情報保護委員会、業法等で求められる場合は所管の省庁等、犯罪性がある場合は 警察、ウイルス感染や不正アクセスの場合は独立行政法人情報処理推進機構（IPA）へ届け出ます。※2

■報告義務が発生する事項■
下記の要件に該当する場合、個人情報保護委員会への漏えい等報告が義務付けられています。※４
・要配慮個人情報が含まれる個人データの漏えい等（又はそのおそれ）
・不正に利用されることにより財産的被害が生じるおそれがある個人データの漏えい等（又はそのおそれ）
・不正の目的をもって行われたおそれがある当該個人情報取扱事業者に対する行為による個人データ（当該個人情報取扱事業者が取得し、又は取得しようとしている個人情報であって、個人データとして取り扱われることが予定されているものを含む。）の漏えい等（又はそのおそれ）
・個人データに係る本人の数が 1,000 人を超える漏えい等（又はそのおそれ）
・条例要配慮個人情報が含まれる保有個人情報の漏えい等（又はそのおそれ）
その他、取引先との契約条件などに報告義務が課されている場合があります。今一度、情報漏えい等発生時に対応が必要な先を洗い出しておきましょう。

＜ステップ３＞復旧・再発防止策
適切な対応や判断を行うために、5W1H（いつ、どこで、誰が、誰を、何を、なぜ、どうしたのか）の観点で状況を調査し情報を整理します。続いて、訴訟対応等を見越して事実関係を裏付ける情報や証拠を保全し、必要に応じてフォレンジック調査（パソコンのハードディスク、メモリ内データ、サーバーやネットワーク機器のログ等の調査）を行います。フォレンジック調査の後、復旧作業を実施し正しく修復できたことを確認出来たら停止したシステムやサービスを復旧させます。その後、再発防止策を講じ、同様のインシデントが再発しないようにします。例えば、新たなセキュリティツールの導入や従業員の教育強化などを行

います。※2

■フォレンジック調査の種類■
フォレンジック調査を調査対象で分類して説明します。※5

コンピュータフォレンジック ※下記パソコンフォレンジックと比して、サーバー、IoT 機器、スマートフォン等コンピュータ全般を対象とします。	コンピュータ機器を調査する。HDD や SSD などのディスクに対する「ディスクフォレンジック」と、稼働中コンピュータのメモリデータに対する「メモリフォレンジック」に細かく分類される。
ネットワークフォレンジック	パケットキャプチャを用いて、ネットワークログやパケットデータを調査する。
モバイルデバイスフォレンジック	スマホ内の削除済みファイルや履歴データの復元調査にも対応し、携帯の証拠復元フォレンジックとして活用される。
データフォレンジック	削除済みファイルの復元や、改ざんされたデータの解析を行う。データ改ざんの有無を特定する際に利用される。
パソコンフォレンジック	社内のパソコン操作ログやアクセス履歴を対象に、不正アクセスや情報漏えいの痕跡、証拠としてのログ調査をする。

（3）ヒヤリハット事例の活用
「ヒヤリハット」とは、重大な事故には至らなかったものの、注意を怠れば事故に繋がりかねなかった事例を指します。日常業務でのヒヤリハット事例を収集し、共有することで、潜在的なリスクを把握し、予防策を講じることができます。

６．まとめ
セキュリティインシデントへの対策は、事前に発生時の対応手順を定めておくことが大切だとわかっていただけたでしょうか。また、定めた計画や手順どおりに実行できるかを実際にシミュレーションしておくこともとても大切です。また、対応手順は定期的な見直しと改善が重要です。

今回ご紹介したポイントを基に、皆さんの企業でも改めて対策を見直してみてください。
ヒヤリハット事例の収集と対策も忘れずに行いましょう。

なお、本稿は、IPA が発行しいている「中小企業の情報セキュリティ対策ガイドライン 第

3.1 版」を中心に解説しています。セキュリティインシデント対応については、ガイドラインの「付録 8 中小企業のためにセキュリティインシデント対応の手引き」にまとめられていますので、もっと詳しく知りたい方はそちらをご参照ください。

次回は、ランサムウェアに感染した場合を例にして、ステップを踏んだインシデント対応をより具体的に解説します。

※本記事は令和 6 年度中小企業サイバーセキュリティ対策事業で制作された記事を最新情報等で更新したものです。

※1 出典：独立行政法人情報処理推進機構（IPA）
3.5.3　サイバーセキュリティに関する被害の状況
https://www.ipa.go.jp/security/reports/sme/nl10bi000000fbvc-att/sme-chousa-report2024r1.pdf

※2 出典：独立行政法人情報処理推進機構（IPA）
https://www.ipa.go.jp/security/sme/f55m8k0000001wpz-att/outline_guidance_incident.pdf

※3 出典：Cyber Security.com
https://cybersecurity-jp.com/contents/data-security/1465/

※4 出典：個人情報保護委員会
https://www.ppc.go.jp/personalinfo/legal/leakAction/#business

※5 出典：IT トレンド
https://it-trend.jp/forensic/article/forensics_basics

配信予定日：2025 年 7 月 31 日(木) 14:00 頃
カテゴリ：ビジネスヒント
タグ：＃経営課題＃知識編
過去記事焼き直し：しない（完全に新規投稿する記事です）

【題名】
セキュリティ対策における基本的な考え方（１/２）

【目次】
●対策を検討する前にリスクアセスメント（分析・評価）を行う
●守るべきもの（情報、情報システム等）を認識する
●脅威を知る
●脆弱性を知り、対処する
●情報セキュリティの方針、基準を明確にし、手順等を整備する
●セキュリティと利便性のバランスをとる
●インシデントの未然防止に努めつつ，発生時に備えた対処を確実に行う
●実施した対策の有効性について、第三者によるチェックやレビューを実施する

【本文】
中小企業の経営者や情報システム担当者の皆さん、ご認識の通りセキュリティ対策は経営課題です。有効なセキュリティ対策を行うには、そのセオリーとも言える「基本的な考え方」について知っておくことが近道となります。そこで本記事では、セキュリティ対策実施における基本的な考え方について見ていきたいと思います。

●対策を検討する前にリスクアセスメント（分析・評価）を行う
機器導入などのセキュリティ対策を検討する前に、まず自組織の現状を調査し、どこに、どのようなリスクがあるのか、それが顕在化した場合にはどのような影響があるのか等、想定されるリスクについて分析・評価する必要があります。そうすることで、実施する対策の目的や効果が明確となります。
逆に、そうした過程を経ていない場合には、必要な対策に抜けが生じたり、それほど必要性の高くない箇所に過剰な対策を実施したりする可能性が高まるでしょう。

●守るべきもの（情報、情報システム等）を認識する
上記のリスクアセスメントを行う際に行うプロセスの一つとなりますが、自組織の情報資産について認識し、それらの中で何が重要なのか、何を守らねばならないのかを認識する必要があります。情報資産は「組織にとって守るべき価値をもつ情報及びそれを取り扱う一連

の仕組みである情報システム」と定義することができます。一般的には、顧客情報、製品情報、財務情報、経営戦略及び施策、マーケティング情報など、組織が業務を行う上で必要な情報そのものと、それを取り扱うために必要なハードウェア、ソフトウェア、ネットワーク等から構成される情報システムが該当します。

●脅威を知る

組織の重要な情報資産を守るためには、それを脅かすものの存在を認識し、その種類、攻撃者の手口等についても可能な限り詳細に把握する必要があります。また、自組織に対して実際にどのような攻撃が行われているのかを知ることも重要です。

脅威とは、情報資産を脅かし、損失を発生させる直接の原因となるものであり、次のようなものが挙げられます。

表：情報セキュリティにおける脅威

脅威の種類	分類	具体例
環境	災害	地震，落雷，風害，水害
	障害	機器の故障，ソフトウェア障害，ネットワーク障害
人	意図的	不正アクセス，盗聴，情報の改ざん
	偶発的	操作ミス，書類や PC の紛失，物理的な事故

情報資産が存在すれば、そこには常に何らかの脅威が存在します。

内部犯行等、組織内部の脅威については対策によって低減させることができますが、自然災害や組織外部の第三者による攻撃等の脅威をなくすことは不可能です。

●脆弱性を知り、対処する

脆弱性は組織や情報システム等に内在する様々な弱点や欠陥であり、脅威と結び付くことでリスクを顕在化させたり、脅威を増幅させたりする要因となります。脆弱性は自助努力によって取り除いたり、低減させたりすることが可能です。まず組織や情報システム等のどこに、どのような脆弱性が存在するのか、それによってどのようなリスクを顕在化させることになるのかを認識し、適切に対処する必要があります。

脆弱性の種類と例を次の表に挙げます。

表：脆弱性の種類とその具体例

脆弱性の種類	具体例
設備面の脆弱性	・建物の構造上の欠陥 ・設備のメンテナンスの不備 ・入退室管理設備の不備

技術面の脆弱性	・ネットワーク構成における欠陥 ・ソフトウェアのバグ ・アクセス制御システムの不備 ・設定ミス，安易なパスワード ・マルウェア対策の不備
管理面・制度面の脆弱性	・情報セキュリティに関する方針，規程の不備 ・機器や外部記憶媒体管理の不備 ・ユーザ教育，マニュアルの不備 ・インシデント対応計画の不備 ・監視体制，監査の不備

●情報セキュリティの方針、基準を明確にし、手順等を整備する
情報セキュリティに対する組織としての方針、対策実施における基準やルールを明確にすることで、従業員等の意識や認識を合わせるとともに、限られた予算、要員、設備等のリソースを有効に活用します。また、従業員等が対策を確実に実施し、過失による問題の発生を防ぐために、手順書等も整備します。

●セキュリティと利便性のバランスをとる
一般的に、セキュリティと利便性はトレードオフの関係にあるため、利便性を高めれば高めるほどセキュリティは低下します。その逆に、セキュリティを高めれば高めるほど利便性が低下する傾向にあります。利便性の低下は業務効率の低下につながり、従業員等からの不満が高まる可能性もあるため、リスクを十分考慮した上で、セキュリティと利便性のバランスをとることが重要です。また、実施するセキュリティ対策がなぜ必要なのか、それを行わないとどのようなリスクがあるのか等について従業員等に説明し、理解を得ることも重要です。

●インシデントの未然防止に努めつつ，発生時に備えた対処を確実に行う
セキュリティ対策の実施においては、組織や情報システムの脆弱性に対処することで、インシデント（事件、事故）の未然防止に努める必要があります。しかし、どんなに未然防止策を施したとしても、インシデントの発生を完全に防ぐことは不可能です。そのため、未然防止策を施すだけでなく、インシデント発生時に備えた対策を確実に行うことが重要です。

＜インシデント発生に備えた対策の例＞
・インシデントを早期に検知するセキュリティ監視システムの導入及び運用
・インシデント発生時の対応体制や対応手順の整備
・インシデント発生時を想定した対応訓練の実施

・インシデント発生時の対応を支援し、侵害を受けた機器等の調査・分析等を行うセキュリティベンダとの契約締結
・サイバー保険への加入

●実施した対策の有効性について、第三者によるチェックやレビューを実施する
自組織が実施したセキュリティ対策の抜けや不備を発見し、それらを是正・改善するため、第三者によるチェックやレビューを実施します。これは年 1 回程度の頻度で定期的に行うとともに、対象となる組織や情報システムに変化が生じた場合などに随時実施するのが望ましいでしょう。組織の変化とは、取り扱う情報資産や業務内容が変わったり、M&A 等により、他社との統合や合併があったりした場合が該当します。

今回はセキュリティ対策実施における基本的な考え方として、8 つの事項について解説しました。次回も引き続き、他の事項について解説します。

配信予定日：2025 年 7 月 31 日(木) 14:00 頃
カテゴリ：もっと知りたい！ セキュリティ
タグ：＃実用編＃知識編＃インシデント対応強化
過去記事焼き直し：する（過去記事を上書きします）
過去記事：https://cybersecurity-taisaku.metro.tokyo.lg.jp/know_more/mottosiritai5/

【題名】
【令和 7 年度版】セキュリティインシデント対応（2/2）

【目次】

中小企業の経営者や情報システム担当者の皆さん、日々のセキュリティ対策、お疲れ様です。
前回お届けした「セキュリティインシデント対応（1/2)」では、セキュリティインシデントの定義と、実際に発生してしまった時の対応について解説しました。
今回はシリーズ第 2 回として、被害が絶えないランサムウェア攻撃について、インシデントが発生した場合の具体的な対応手順をお伝えいたします。

１．ランサムウェアとは
あらためて、ランサムウェアについて確認しましょう。
ランサムウェアとは、感染したパソコンをロックしたり、ファイルを暗号化して使用できなくする不正プログラムです。ファイルの復元と引き換えに金銭を要求されることから、「ランサムウェア」（ransom（身代金）と software（ソフトウェア）の造語）と言われています。
最近では、サイバー攻撃の一環として「人手によるランサムウェア攻撃」や、情報を窃取しそれを公開すると脅す「二重の脅迫」の被害も報告されています。
また、警察庁が毎年公表している「サイバー空間をめぐる脅威の情勢等について」では、令和 6 年に「ランサムウェアの開発・運営を行う者が、攻撃の実行者にランサムウェア等を提供し、その見返りとして身代金の一部を受け取るもの（RaaS：Ransomware as a Service）による攻撃実行者の裾野の広がりが、対策が比較的手薄な中小企業の被害増加につながっていると考えられる。」とあるように、被害件数は中小企業において年々増加しています。※ 1

２．ランサムウェアに感染したら
ランサムウェアに感染すると、以下のような事象が発生します。

（1）ファイルの拡張子が突然変わったり、開けなくなる。
（2）身代金を要求するメッセージが表示される。
（3）コンピュータの動作が急激に遅くなる。
（4）ウイルス対策ソフトが警告を出す。

ランサムウェアは被害が表面化しやすく、業務に大きな影響を与えます。あらかじめ感染時の兆候を理解し、対応を決めておくことが重要です。そうしないと、実際に感染した際に対応に戸惑い、パニックに陥る可能性があります。
また、確実に復旧するためには、バックアップからの復元が唯一の手段です。「今まで何も起きていないから感染したらそのとき考えよう」とか「専門家に任せれば何とかなるだろう」という考えは通用しません。
ランサムウェアの被害は 10 年以上被害が増加しており、いかなる組織も例外なく被害に遭う可能性があります。感染後の対応も主体的に検討しておきましょう。

３．ランサムウェアに感染した後の対応

検知と連絡受付	パソコンの画面に身代金を要求するようなメッセージが表示された等、前述の事象を発見したときにはランサムウェア感染の可能性があります。 システム管理者、情報セキュリティ管理者等に報告します。
初動対応	感染したパソコンやサーバーの利用を停止し、ネットワークから切り離します。 【切り離し方】 ＜有線接続の場合＞ （1）ネットワークケーブルを抜く ・パソコンやサーバーの背面や側面にある LAN ポート（ケーブルの差し込み口）を見つけます。 ・ネットワークケーブルをこのポートから抜きます。 （2）ネットワーク設定を無効にする Windows 等 OS の設定でネットワーク接続を無効にします。 ＜無線接続（Windows）の場合＞ （1）Wi-Fi を切断する ・タスクバーのネットワークアイコンをクリックして接続済みの SSID の切断をクリックします。
第二報以降	（1）影響を及ぼした取引先や顧客に対して、インシデントに関して報告

	します。 （２）ウイルス感染による影響によって、業法等で報告が求められる場合は所管の省庁へ報告します。 （３）IPA の届出窓口へ届け出ます。※２ ＜IPA 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＞ ■ランサムウェア被害の届出 ランサムウェア攻撃による被害は、ウイルス届出として取り扱われますが、複雑な攻撃の場合があるため専用の届出様式が用意されています。 下記のコンピュータウイルス届出（ランサムウェア被害）様式に則り、判明している範囲で構いませんので、被害の状況や対応した内容等を記入のうえ、届出先にメールでご送付ください。 （様式） コンピュータウイルス・不正アクセス届出様式（Excel 様式） https://www.ipa.go.jp/security/todokede/crack-virus/ug65p9000000nnpa-att/virus_crack_format.xlsx （届出先） 独立行政法人情報処理推進機構 セキュリティセンター コンピュータウイルス届出窓口 E-mail：virus@ipa.go.jp
調査・対応	（１）No More Ransom 等から復号化ツールを入手し、復旧を試みます。 （ウェブサイト「No More Ransom」は、オランダ警察の全国ハイテク犯罪ユニット、ユーロポールの欧州サイバー犯罪センター、Kaspersky、McAfee が主導しています。 ランサムウェアの被害者が犯罪者に不当な支払いをすることなく、暗号化されたデータを取り戻すための支援を目的としています。） ただし、全てのランサムウェアに対応しているわけではありません。※３ （２）データ等のバックアップを行っている場合は、復元（リストア）します。

	ただし、バックアップ装置・媒体をパソコンに常時接続している場合、バックアップファイルも暗号化されている場合もあります。 ＜参考＞適切なバックアップ方法 ■原則的にバックアップに使用する装置・媒体は複数用意し、バックアップ時のみパソコンと接続する、またはバックアップしたファイルのうち1つはオフサイトに保存する。 　また、バックアップの対象がクラウドサービスの場合は、サービスの仕様を確認し、バックアップがサービスに付帯する場合は頻度、保存先、リストア手順について把握しておく。 ■バックアップしたファイルは、定期的に復元（リストア）できるか確認する。 　復元のテストが難しい場合は、いざというときにバックアップ手順を迷わず実施できるようマニュアル等を整備しておく。 （3）復号化ツールでも復旧しない場合、バックアップが復元（リストア）できない場合は、感染した機器やデータの復旧を断念し、再構築します。
復旧	データの復元（リストア）が正しいことを確認できたら、システムを復旧します。

なお、本稿は IPA が発行している「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」を参考に解説しています。

※本記事は令和 6 年度中小企業サイバーセキュリティ対策事業で制作された記事を最新情報等で更新したものです。

※1 出典：警察庁（8 P）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6/R06_cyber_jousei.pdf

※2 出典：独立行政法人情報処理推進機構（IPA）
https://www.ipa.go.jp/security/todokede/index.html

※3 出典：NO MORE RANSOM
https://www.nomoreransom.org/ja/

配信予定日：2025 年 8 月 20 日(木) 14:00 頃
カテゴリ：ビジネスヒント
タグ：＃経営課題＃知識編
過去記事焼き直し：しない（完全に新規投稿する記事です）

【題名】
セキュリティ対策における基本的な考え方（２/２）

【目次】
●最小権限の原則を徹底する
●責務の分離の原則を徹底する
●重要な情報を取り扱うシステムとインターネット接続環境を分離する
●フェールセーフを考慮してシステムを設計・構築する
●システムの構成や機能を単純にする
●システムや設備の重要な機能を分散化する
●二重・三重の対策を施す（多層防御）
●利用者等を一意に識別し、事象の追跡・検証を可能とする

【本文】
前回に続き、本記事では、セキュリティ対策実施における基本的な考え方について見ていきたいと思います。

●最小権限の原則を徹底する
自組織の情報資産にアクセスする人やプロセス、プログラム等に対して、常に必要最小限の権限のみを付与するように徹底します。これを「最小権限の原則」といいます。権限は通常、対象となるシステムを利用する際に使用するユーザ ID 等のアカウントに対して付与されます。
原則に沿わない場合、例えば、ある組織では本来必要がないのにもかかわらず、一般ユーザのアカウントにシステム管理者の権限（特権）を付与していたとします。この場合、サイバー攻撃によって一般ユーザの PC にマルウェアが感染し、アカウントを不正利用したとすれば、攻撃者はシステム管理者として全ての機能が使えるため、より甚大な被害を及ぼすことができてしまいます。また、サイバー攻撃が発生しなくとも、正規のユーザが PC で常時動作しているセキュリティ対策ツールを勝手に停止させたり、無効化したりする可能性もあります。
このように、必要以上の権限を付与することはセキュリティリスクを高めることになりますので、そうならないためには最小権限の原則を徹底していただくことが必要です。

特にシステムの特権アカウントの発行及び管理については細心の注意を払い、付与する権限の有効期間も必要最小限とするように徹底する必要があります。

●責務の分離の原則を徹底する
同一の者に関連する複数の業務を行う権限を与えると、他者のチェック等が入ることなく単独で一連の業務を行うことができるため、当人の確認不足によるミスが発生したり、権限を悪用した不正行為等を発生させたりする原因となります。そうした問題の発生を防ぐためには、一つの業務フローに複数の担当者が関わるよう分離するのが有効であり、これを「責務の分離（職務分離）の原則」といいます。単に分離するだけでなく、各業務の実施状況について、別の担当者や第三者に監視・監査させる等して牽制機能を働かせるとより効果が高まります。

●重要な情報を取り扱うシステムとインターネット接続環境を分離する
企業において、ウェブ、電子メールを中心としたインターネット接続は業務において必須となっていることでしょう。その一方で、そうしたインターネット接続がマルウェア感染の大きな原因となっています。企業の基幹業務システムや個人情報、機密情報を取り扱うシステムとインターネット接続環境が接続されていると、マルウェアによって当該システムにまで被害が及び、情報が流出したり、暗号化されたりする可能性があります（例：従業員のウェブ・電子メール利用により端末がマルウェア感染し、重要システムにまで被害が拡大）。そうしたリスクを低減するには、重要な情報を取り扱うシステムとインターネット接続環境を分離するのが有効です。物理的に分離するのが望ましいのですが、それが難しい場合には、VLAN（Virtual Local Area Network）や VDI（Virtual Desktop Infrastructure）等の技術を活用して論理的に分離します。

●フェールセーフを考慮してシステムを設計・構築する
フェールセーフとは、システムに何らかの障害が発生した場合に安全な方向に向かうように設計・構築しておくことで、被害を最小限にする方法です。例えば、ファイアウォールに障害が発生した場合に全ての通信が通過できてしまうと大変危険であるため、全ての通信をできないように設計することがフェールセーフとなります。

●システムの構成や機能を単純にする
ネットワーク構成、サーバの構成や機能などが単純であるほどセキュリティを確保しやすくなります。例えば、1 台のサーバにウェブ、メール、ドメインコントローラ等の複数の役割を兼ねさせると、設定が複雑になり、障害発生時の原因究明が困難になったり、特定のソフトウェアの障害が他のソフトウェアにも影響を及ぼしたりするなどの問題が発生する可能性が高まります。そのため、システムの構成はできる限り単純にし、1 台のサーバには一

つの機能だけを実装するようにします。

●システムや設備の重要な機能を分散化する
システムや設備の重要な機能を 1 箇所に集中させてしまうと、そこがダウンするとシステム全体が停止状態となってしまうおそれがあります。そうした事態を防ぐためには、システムの重要な機能は適切に分散化させる必要があります。
近年ランサムウェアによって本番データとバックアップデータが全て侵害され、業務復旧に多大な時間を要するインシデントが発生しています。そうしたことから、事業継続において重要な機器やシステムを複数台構成にして冗長化するとともに、バックアップデータを同一ネットワーク上のバックアップサーバ等には保存せず、本番システムからアクセスできないオフサイトや、オフライン媒体に分散して保存するのが有効な対策となります。

●二重・三重の対策を施す（多層防御）
単一の対策ではなく、二重・三重の対策を施すことにより、セキュリティは格段に高まります。例えば、まず公開ウェブサーバの OS、ミドルウェア、アプリケーション等の脆弱性に対処し、堅牢な状態を確保・維持します。その上でファイアウォール、IPS（Intrusion Prevention System）、Web アプリケーションファイアウォール（WAF）を実装し、公開ウェブサーバへの不正アクセスを遮断するのは有効な対策です。また、決済処理を行うシステム等において、まず端末レベルの認証を経た後にユーザの本人認証を行い、最終的な決済処理の直前に再度本人認証を行うのも、二重・三重の対策によってセキュリティを高めている例です。
なお、経済産業省が発行する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の重要 10 項目」の「指示 5：サイバーセキュリティリスクに効果的に対応する仕組みの構築」として、次のような対策例が挙げられています。

＜サイバーセキュリティリスクに効果的に対応する仕組みの構築における対策例＞
① 重要業務を行う端末、ネットワーク、システム又はサービス（クラウドサービスを含む）には、多層防御を実施する。
・必要に応じてスイッチやファイアウォールなどでネットワークセグメントを分離し、別のポリシーで運用する。
・脆弱性診断等の検査を実施して、システム等の脆弱性の検出、及び対処を行う。
・営業秘密や機微性の高い技術情報、個人情報などの重要な情報については暗号化やバックアップなど、情報を保護する仕組みや、改ざん検知の仕組みを導入する。
・ゼロトラストモデルに基づく対策を講じる際には、境界防御の効果が期待できないことを踏まえた認証等の強化を図るとともに、インシデントの予兆の段階で即時の検知と

対処ができるような仕組みや体制を整備する。
・クラウドサービスを利用する際には、クラウドサービスにおいて提供されるセキュリティ機能を考慮した選定を行い、それらの機能を活用するとともに、アクセス制限などの設定やアカウントの管理などが適切に維持・管理されるようにする。

② 自社内で対策実施に必要なスキルを有する人材を確保できない場合は、専門の情報セキュリティサービス等を提供する外部事業者を活用する。
・一定の品質を備えたサービスの選定には、IPA が公表している「情報セキュリティサービス基準適合サービスリスト」を利用することができる。
・サービスを外部委託する場合でも、脆弱性診断や監視サービス等の提供事業者からの報告内容を適切に理解し、対策に反映するスキルを備えた人材が必要となることを認識し、必要な人材の確保・育成に取り組む必要がある。

③ サイバーセキュリティリスクによりシステムが停止した場合に、業務を止めないための計画（BCP）を策定し、バックアップの取得や代替手段の整備等を行う。

④ 従業員に対する教育を定期的に行い、適切な対応が行えるよう日頃から備える。

●利用者等を一意に識別し、事象の追跡・検証を可能とする
組織内やシステムで発生する様々な事象について、それを発生させた主体（利用者、端末、プロセス、プログラム等）を一意に識別・特定し、追跡・検証できるようにします。そのためには、ユーザアカウント等の識別情報を複数人で共用せず、ユーザごとに固有とする必要があります。また、発生した事象をログ等に確実に記録するとともに、ログの改ざん、滅失等が発生しないよう対策を施す必要があります。

ここまで 2 回にわたり、セキュリティ対策実施における基本的な考え方について解説してきました。これらはいずれもセキュリティ対策のセオリーとも言えるものであるため、認識しておいていただきたいと思います。

配信予定日：2025 年 8 月 20 日(水) 14:00 頃
カテゴリ：基礎から学ぶ！ セキュリティ
タグ：＃知識編
過去記事焼き直し：する（過去記事を上書きします）
過去記事：https://cybersecurity-taisaku.metro.tokyo.lg.jp/basics/kisokaramanabu5/

【題名】
【令和 7 年度版】中小企業におけるセキュリティ脅威への対策強化
～ビジネスメール詐欺とは？事例から対策を学ぶ～

【目次】

【本文】
独立行政法人情報処理推進機構（IPA）が毎年発行している「情報セキュリティ 10 大脅威 2025」から、中小企業の経営者やシステム担当者が注目すべき点を掘り下げていきます。

今回は 9 位に挙げられている「**ビジネスメール詐欺**」に焦点を当てます。ビジネスメール詐欺による被害は長年にわたり頻繁に発生し続けており、この脅威がどのように業務に影響を与えるのか、対策はどうすべきかを解説いたします。

引用元：IPA　情報セキュリティ 10 大脅威 2024 解説書
　　IPA　情報セキュリティ 10 大脅威 2025 組織編

１．ビジネスメール詐欺とは
ビジネスメール詐欺とは、悪意のある第三者が**標的とする企業やその取引先の関係者などになりすまして偽のメールを送信し、金銭を騙し取ること**を目的としたサイバー

攻撃です。この攻撃は、企業の従業員を標的にした振り込め詐欺とも言えるもので、ビジネスメール詐欺（Business E-mail Compromise：BEC）と呼ばれています。
特に、企業の金銭の決裁権限を持つ責任者や直接金銭を取り扱う担当者などが攻撃の対象となることが多くなっています。

２．代表的なビジネスメール詐欺

ビジネスメール詐欺の具体的な手法をご紹介します。

（１）取引先からの請求書の偽装

攻撃者が取引先企業や担当者になりすまし、偽の請求書等をメールで送り付け、用意した口座に振り込ませる手口です。
また、ウイルス感染や不正ログイン等により、自社の従業員のメールアカウントが乗っ取られ、攻撃者が自社の従業員になりすまして、取引実績がある別企業の担当者へ偽の請求等を送り付け、用意した口座に金銭を振り込ませることで、取引先が被害に遭うケースもあります。
このような場合、メール本文は巧妙に偽装され、送信元が本物のアカウントであるため、受信したメールが攻撃であることに気付きにくい事が特徴と言えます。

（２）経営者等の権威ある者へのなりすまし

攻撃者が企業の経営者や経営陣・役員等になりすまし、従業員に業務指示を模した内容の電子メールを送信し、用意した口座へ金銭を振り込ませる手口です。
通常の社内メールでの業務指示であるかのように偽装されるため、メールを受け取った従業員は「通常の業務」として何の疑問も抱かないのが、このなりすましの特徴です。
また、弁護士や監査法人、行政庁等の社外の権威ある第三者になりすます場合もあります。

このように、ビジネスメール詐欺の前提として、標的組織の情報の窃取が不可欠であることが分かります。攻撃者は標的組織の経営者や経営幹部、人事担当等の特定任務を担う従業員になりすましたり、または組織内の他の従業員の個人情報を窃取したりしながら、「なりすます相手」を探すわけです。

では、ビジネスメール詐欺の具体的な事例をご紹介しながら、要因と対策をみていきましょう。

（3）ビジネスメール詐欺の事例

【事例 1. ディープフェイクによる映像や音声のなりすまし事例】
医療製品メーカーの株式会社スリー・ディー・マトリックスは、支払口座の変更依頼が書かれた、取引先の名を騙るメールに従い、虚偽の銀行口座に総額 2 億円を振り込んだことを公表しました。その取引先とは創業以来の付き合いがあり、高い信頼関係があったため、同社は振込先口座の変更の理由を直接確認していませんでした。
引用元：IPA　情報セキュリティ 10 大脅威 2024 解説書より抜粋

この事例では、「長年信頼している会社からの依頼」という思い込みが最大の問題といえます。それほど付き合いの深くない取引先であれば、「急に取引口座をなぜ変える必要があるのか」と、ビジネス的な危機感を生むはずですが、長年の信頼がこの感覚を麻痺させていた事がこのなりすましを可能としています。

【事例 2. ディープフェイクによる映像や音声のなりすまし事例】
2024 年 1 月、多国籍企業にて約 37.5 億円が詐取される事件が発生しました。この企業の香港支社の従業員は、英国の本社の CFO を名乗る人物からメールを受信し、そのメールには、ある秘密の取引を本社で開始しており、香港支社の口座を操作しなければならないと書かれていました。さらに従業員は、ビデオ会議の URL が記載されたメールも受信したため、不審に思いつつも会議に参加しました。その会議では、CFO の映像が映し出され、CFO の音声で説明がなされており、また、知り合いの同僚の映像も映し出されていたため、従業員は本物の会議であると信じ込んでしまいました。さらに、香港支社の資金を指定の銀行に振り込むように依頼されました。
従業員は不審に思い、CFO を名乗る人物に質問をしましたが、叱責されたため、最終的に送金手続きをしてしまいました。その後、この従業員は不安に思い、同僚や本物の CFO に確認したところ、取引については知らないと言われたため、警察に通報をしましたが、既に資金は海外に送付されてしまい、会社は資金を取り戻すことができませんでした。
引用元：IPA　情報セキュリティ 10 大脅威 2025 組織編より抜粋

この事例は、メールに加え、高度な技術を用いたビデオ会議による偽造と、役職の立場を利用した催促が特徴的と言えます。被害にあった従業員は不信感を持ちつつも、想定が困難な手法であったことから、通常ではとりえない行動をとってしまったものと思われます。
AI が発達した現代においてはこうした高度な技術を用いた手法もとられうるということを念頭に置く必要があります。

３．ビジネスメール詐欺への対策

では、次にビジネスメール詐欺の対策として、「被害の予防」の観点と「被害を受けた後の対応」を説明していきます。

（１）被害の予防

（IPA「情報セキュリティ 10 大脅威 2025 組織編」より）

IPA の「情報セキュリティ 10 大脅威 2025 組織編」の 9 ページ、表 1.3「情報セキュリティ対策の基本」を実施することや、ビジネスメール詐欺の認識と理解を高めることが重要です。また、下記に挙げる個別の対策も有効と言えます。

◆ガバナンスが適切に機能する業務フローの構築
金銭が絡む手続きをする際は、複数人で審査、承認をする業務フローを構築し、個人の判断や業務命令だけでは完結させないようにする。また、メールだけに依存しない業務フローの構築も重要です。
例えば、振込先口座に変更がある場合は、メール以外の連絡方法（電話等）で直接取引先に確認をする、金融機関にその口座の名義等を確認するなどが上げられます。

◆普段とは異なるメールに注意する
普段とは異なる言い回しや、表現の誤り、送信元のメールドメインに注意しましょう。

◆判断を急がせるメールに注意する
至急の対応を要求する等、担当者に真偽の判断時間を与えないようにする手口も考えられます。真偽を確認するフローを業務フローに盛り込んでおく事も有効です。

◆インシデント対応体制の整備
問題発生時に迅速かつ的確に対応できる体制を整えます。
具体的な対応については、IPA の「中小企業の情報セキュリティ対策ガイドライン 第 3.1 版」の 46 ページからの（5）セキュリティインシデント対応をご覧ください。

（2）被害を受けた後の対応

ビジネスメール詐欺による金銭被害（可能性を含む）を受けた時には、下記の対応が必要となります。

◆適切な報告／連絡／相談

問題が発生した場合、速やかに報告し、適切な対応を取れるよう、社内・社外の関係組織や公的機関等と連携できるようにしておきましょう。

◆メールアカウントの設定を確認する

攻撃者による不正な転送設定やメール振分けの設定等がされていないか確認する。

今回は、ビジネスメール詐欺の事例や影響、対策方法について考えてきましたが、いかがだったでしょうか。

ビジネスメール詐欺による被害はどの企業でも起こる可能性があり、その影響は甚大です。被害を完全になくすことはできませんが、ガバナンスの整備や、メールだけに頼ることがない業務フローの構築等が、企業の持続可能な発展を支える鍵となるでしょう。

＜参考情報＞　他の事例を見る

・ビジネスメール詐欺の事例集を見る（IPA Web サイト）

・5 億円の被害も！日本企業の不正送金・ビジネスメール詐欺被害の事例 4 社（サイバーソリューションズ株式会社 Web サイト）

配信予定日：2025 年 8 月 29 日(金) 14:00 頃
カテゴリ：もっと知りたい！ セキュリティ
タグ：＃知識編＃セキュリティ対策点検
過去記事焼き直し：しない（新規記事です）
記事 URL（新設します）：https://cybersecurity-taisaku.metro.tokyo.lg.jp/know_more/government_initiatives/

日本政府のサイバーセキュリティ施策の概要

目次

中小企業の経営者や情報システム担当者の皆さん、日々のセキュリティ対策、お疲れ様です。
日本国内の企業であれば、その規模や業種等にかかわらず、日本政府が推進しているサイバーセキュリティ施策について、その概要や要点について知っておくことが望ましいですが、関係者でない限り、そうした情報に触れる機会はほとんどないのではないかと思われます。
そこで今回は、日本政府のサイバーセキュリティ施策の概要をご紹介します。

●サイバーセキュリティ基本法の概要
サイバーセキュリティ基本法は、サイバーセキュリティに関する国の施策や戦略を明確に定め、総合的かつ効果的に推進することにより、経済社会の活力向上、持続的発展、国民が安全で安心して暮らせる社会の実現、国際社会の平和及び安全の確保、国の安全保障への寄与などを目的として、2015 年 1 月に施行されました。
同法により、内閣に「サイバーセキュリティ戦略本部」が設置され、同時に内閣官房に「内閣サイバーセキュリティセンター（NISC：National center of Incident readiness and Strategy for Cybersecurity）※」が設置されました。

※2025 年 7 月に内閣官房組織令に基づき「国家サイバー統括室（NCO：National Cybersecurity Office)」に改組

同法では、サイバーセキュリティに関する施策の推進にあたっての基本理念として次の事項を規定しています。

① 情報の自由な流通の確保を基本として、官民の連携により積極的に対応
② 国民一人一人の認識を深め、自発的な対応の促進等、強靱な体制の構築
③ 高度情報通信ネットワークの整備及び IT の活用による活力ある経済社会の構築
④ 国際的な秩序の形成等のために先導的な役割を担い、国際的協調の下に実施
⑤ デジタル社会形成基本法の基本理念に配慮して実施
⑥ 国民の権利を不当に侵害しないよう留意

●サイバーセキュリティ 2025 の概要
上記のサイバーセキュリティ戦略本部より、毎年「サイバーセキュリティ 20xx」と題する文書が公開されています、その最新版は 2025 年 6 月 27 日に公開された「サイバーセキュリティ 2025」であり、日本政府のサイバーセキュリティ施策に関する 2024 年度年次報告及び 2025 年度年次計画となっています。
本書は 230 ページ近くありますが、ここでは第一部の「エグゼクティブ・サマリー」より、そのポイントについて見ていきましょう。

1. サイバー攻撃の動向
2024 年度は、巧妙化・高度化や国家を背景とした攻撃キャンペーン等により、サイバー攻撃が国民生活・経済活動及び安全保障に対し、深刻かつ致命的な被害を生じさせるリスクをはらんでいること、また社会全体に DX が一層浸透したことで、政府機関・重要インフラ等にとどまらず、サイバー攻撃の標的・被害が急速に多様化・複雑化していることが、これまで以上に顕在化しています。2024 年度における主な国内のサイバー攻撃事案は次の通りです。

・某国の関与が疑われるサイバー攻撃グループ「MirrorFace」による安全保障や先端技術に係る機微情報の窃取を目的とした攻撃キャンペーン（2019 年 12 月～）
・他国由来のサイバー攻撃グループ「TraderTraitor」による暗号資産関連事業者からの暗号資産窃取（2024 年 5 月）
・金融機関や地方公共団体等からの委託を受けて情報処理、印刷・発送の受託業務等を行う企業に対し、個人情報を漏えいさせたランサムウェア攻撃（2024 年 5 月）
・出版事業等を行う大手企業に対し、提供するウェブサービスの停止や、書籍の流通事業等に影響を生じさせたランサムウェア攻撃（2024 年 6 月）
・航空会社の国内便・国際便の遅延や、インターネットバンキングへのログイン障害等、複

数の重要インフラ分野に渡って被害を生じさせた DDoS 攻撃（2024 年 12 月～2025 年 1 月）

国外においても、重要インフラ分野等への重大なサイバー攻撃が発生しており、NISC が把握した状況においても、政府機関への不審な通信等の検知・通報件数の急増や、重要インフラのインシデント報告におけるサイバー攻撃の割合が 50%を超えるといった傾向がありました。

2. サイバー攻撃への対応

こうしたサイバー脅威の急速な高まりに対応するため、NISC では次のような施策を行っています。

・政府機関等への ASM, PDNS（プロテクティブ DNS）の導入による横断的監視の強化
・直近に発生した重大インシデントからの教訓・対策や最近の技術動向等を反映した「政府機関等の対策基準策定のためのガイドライン」の一部改定
・政府機関等における生成 AI を含む約款型のサービス等の業務利用に関する注意喚起
・Living Off The Land 戦術等を含む最近のサイバー攻撃に関する注意喚起
・MirrorFace によるサイバー攻撃に関する注意喚起
・DDoS 攻撃への対策に関する注意喚起

3. 新たなサイバーセキュリティ政策の方向性

こうした状況により強力に対応するため、日本のサイバーセキュリティ政策は、能動的サイバー防御の法制化等により、大きな転換点を迎えることとなりました。

サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させるべく、法制度の整備等について検討するため、2024 年 6 月に「サイバー安全保障分野での対応能力の向上に向けた有識者会議」が立ち上げられました。

また、2025 年 5 月には、サイバー対処能力強化法、同整備法が成立するとともに、サイバーセキュリティ戦略本部により、次の事項を柱とする「サイバー空間を巡る脅威に対応するため喫緊に取り組むべき事項」が取りまとめられました。

・新たな司令塔機能の確立
・巧妙化・高度化するサイバー攻撃に対する官民の対策・連携強化
・サイバーセキュリティを支える人的・技術的基盤の整備
・国際連携を通じた我が国のプレゼンス強化

これらのうち、新たに期限を設けて取り組むべきとされた事項は次の通りです。

・インシデントに係る各種報告様式の統一
・IoT 製品に対する「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」の政府機関等における選定基準への反映
・官民共通の「人材フレームワーク」の策定
・脅威ハンティングの実施拡大に向けた行動計画の基本方針の策定
・重要インフラ事業者等が実施すべきサイバーセキュリティ対策に係る基準の策定
・中小企業におけるサイバーセキュリティ対策実施のための環境整備
・耐量子計算機暗号（PQC）への移行の方向性の検討

また、これらを踏まえ、新たなサイバーセキュリティ戦略について、2025 年内を目途に策定することとしています。

「サイバーセキュリティ 2025」の最終ページには、今回紹介したエグゼクティブ・サマリーの内容を 1 枚で表した次の図が掲載されています。

●サイバー対処能力強化法の概要
サイバー対処能力強化法は、2025 年 5 月に成立・公布されたサイバーセキュリティ関連法

です。国家的なサイバー攻撃の脅威が高まっているなか、日本のサイバー安全保障のレベルを欧米主要国並みに引き上げることを目指したものとなっています。
同法のポイントの一つとして、「能動的サイバー防御の導入」があります。これは、攻撃を受ける前にその兆候を検知し、能動的に防御措置を講じることで、ファイアウォールやアンチウイルスといった従来の受動的な防御では困難であった、攻撃者の活動を早期に封じ込める体制を構築するというものです。

このように、日本政府では、ますます高まるサイバー攻撃の脅威に対し、新たな戦略を策定するとともに、多くの施策を進めています。
なお、今回登場した Living Off The Land 戦術については、別の回で解説する予定です。

●参考情報
サイバーセキュリティ 2025（2024 年度年次報告・2025 年度年次計画）（NISC）
https://www.nisc.go.jp/pdf/policy/kihon-s/250627cs2025.pdf

●用語解説
■ASM（Attack Surface Management）
外部からアクセス可能な機器などサイバー攻撃を受ける可能性のある自組織の IT 資産の情報を攻撃者の視点で調査し、それらに存在する脆弱性を継続的に評価する取り組み。
※今年度の東京都事業で取り扱っています。記事配信時点（2025 年 8 月 29 日）で定員に達しています、実施結果は何らかの形で記事にしたいと考えていますのでお楽しみに。
令和 7 年度 中小企業サイバーセキュリティフォローアップ

■PDNS（プロテクティブ DNS）
DNS（ドメインネームシステム）のクエリを分析してサイバー攻撃の脅威を検知し、防御するセキュリティ対策技術。

■Living Off The Land 戦術
マルウェアや攻撃ツールを用いず、標的となっているシステムで利用されている正規の管理ツール、コマンド、機能等を用いて攻撃を行うため、検知が難しいのが特徴。システム内寄生戦術とも呼ばれる。

■セキュリティ要件適合評価及びラベリング制度（JC-STAR）
IoT 製品に対して、独自に定める適合基準（セキュリティ技術要件）に基づき、セキュリティ機能の適合性を評価し、ラベルで可視化する制度。

■耐量子計算機暗号（PQC）

PQC（Post-Quantum Cryptography）は、量子コンピュータを用いた攻撃に対しても安全性を保つことができる暗号方式。量子コンピュータが実用化されると、現在広く普及している公開鍵暗号技術等が危殆化し、暗号化されたデータが解読されてしまう可能性があるが、これに対応するため、PQC に関する調査や研究が行われている。

配信予定日：2025 年 8 月 29 日(金) 14:00 頃
カテゴリ：基礎から学ぶ！ セキュリティ
タグ：＃初級編 ＃基本対策事業 ＃実用編
過去記事焼き直し：する（過去記事を上書きします）
過去記事：https://cybersecurity-taisaku.metro.tokyo.lg.jp/basics/kisokaramanabu3/

【令和 7 年度版】中小企業におけるセキュリティ脅威への対策強化 ～経営者は何をしなければならないのか 前編～

目次

今回から前・後編に渡って中小企業の経営者が「サイバーセキュリティ確保に向けてどのように対応すべきか、具体的には何をしなければいけないのか」についてご紹介します。
独立行政法人情報処理推進機構（IPA）が発行している「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」に基づいて、今回は経営者が「認識すべき 3 原則（前編）」を、次回は「実行すべき重要 7 項目の取組（後編）」を解説していきます。

認識すべき 3 原則

これは、サイバーセキュリティ確保に向けて経営者の行動原則をまとめたものです。経営者が一番初めに悩むことは、「どうやって向き合うのか」つまり、自分の立ち位置や行動についてだと思います。

原則 1「サイバーセキュリティ対策は経営者のリーダーシップで進める」

経営者は、サイバーセキュリティ対策の重要性を認識し、**自らリーダーシップを発揮**して対策を進めます。現場の従業員は業務の利便性が低下したり、面倒な作業を伴う対策には抵抗を感じたりすることがありますが、**経営者が自ら意思決定し、自社の事業に見合った適切な対策を主導**する必要があります。

例えば、新しい事業を開始する場合を考えてみましょう。まず経営者が事業の適合性を判断し、その上で、事業環境を整えて、従業員を教育するでしょう。当然、新たな業務に抵抗する従業員も出るでしょうが、それを含めて事業を推進するのが一般的な経営者の役割と言えます。サイバーセキュリティ対策を新しい事業と置き換えてみれば、特別なものではないとお判りいただけると思います。

とは言っても、通常の事業と異なり、馴染みの薄いサイバーセキュリティを推進するのはハードルが高いものです。そこで、推進するにあたって有効な考え方の一つに、**情報セキュリティガバナンス**のフレームワークがあります。

◇情報セキュリティガバナンスのフレームワーク

経営者が企業戦略としてサイバーセキュリティ向上に取り組むための枠組みです。経営者がリーダーシップを発揮する枠組みでもあり、以下の 4 つの要素から成り立ちます。

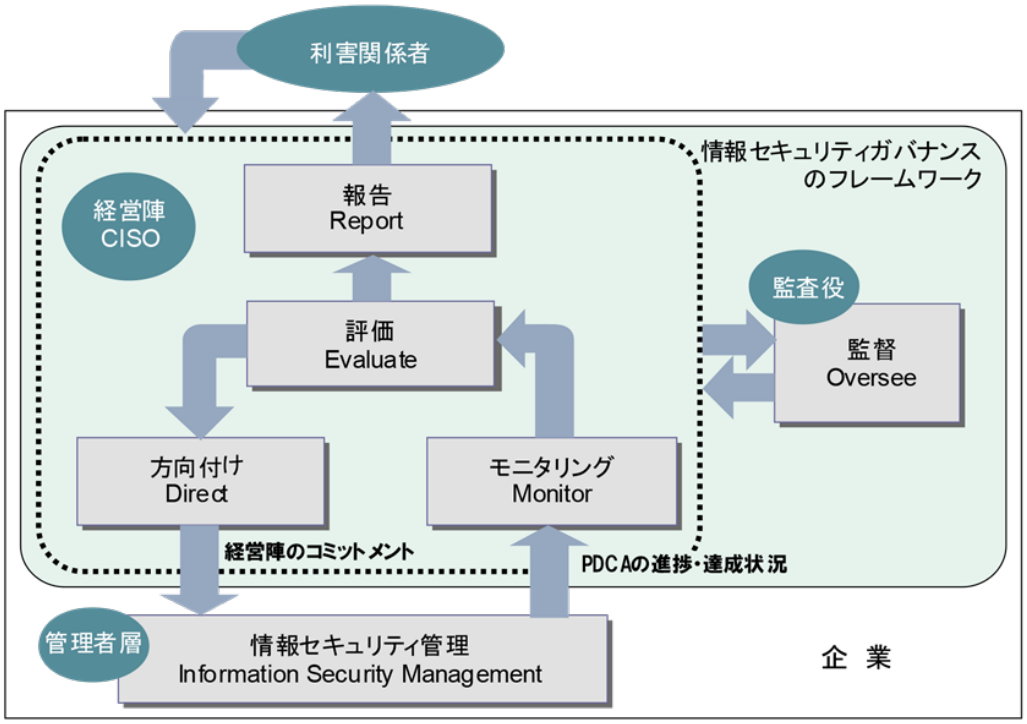
1.方向付け：経営者が懸念する重大事故などを避けるための規則決定

2.情報セキュリティ管理（ISM）：対策の推進や点検の実施

3.モニタリング：対策の進捗や点検による不正行為防止等により状況を監視

4.評価：規則の効果を評価し、見直す

サイバーセキュリティガバナンスのフレームワーク
引用：IPA 「中小企業の情報セキュリティ対策ガイドライン 第 3.1 版」12 ページ
参考：経済産業省 『情報セキュリティガバナンスの概念』
https://www.meti.go.jp/policy/netsecurity/secgov-concept.html



サイバーセキュリティガバナンスのフレームワーク

引用：IPA 「中小企業の情報セキュリティ対策ガイドライン 第 3.1 版」12 ページ

参考：経済産業省 『情報セキュリティガバナンスの概念』

https://www.meti.go.jp/policy/netsecurity/secgov-concept.html

これらの要素を実施することで、サイバーセキュリティガバナンスのフレームワークが整備され、企業全体でセキュリティ意識を高めることができます。

原則 2「委託先のサイバーセキュリティ対策まで考慮する」

業務の委託先に重要な情報を提供する場合、委託先がどのようなサイバーセキュリティ対策(サイバーセキュリティガバナンス)を行っているか考慮する必要があります。委託先に提供した情報が漏えいしたり、改ざんが発生した場合、それが委託先の不備だったとしても、委託元の企業も管理責任を問われることになります。

例えば、最近の事例で自治体が印刷業務を委託している企業でランサムウェア攻撃を受け、自治体が保有する個人情報の漏洩が確認された事件や、大手メーカーの再々委託先企業が仕入れ先情報を不正にダウンロードしていた事件などが発生して

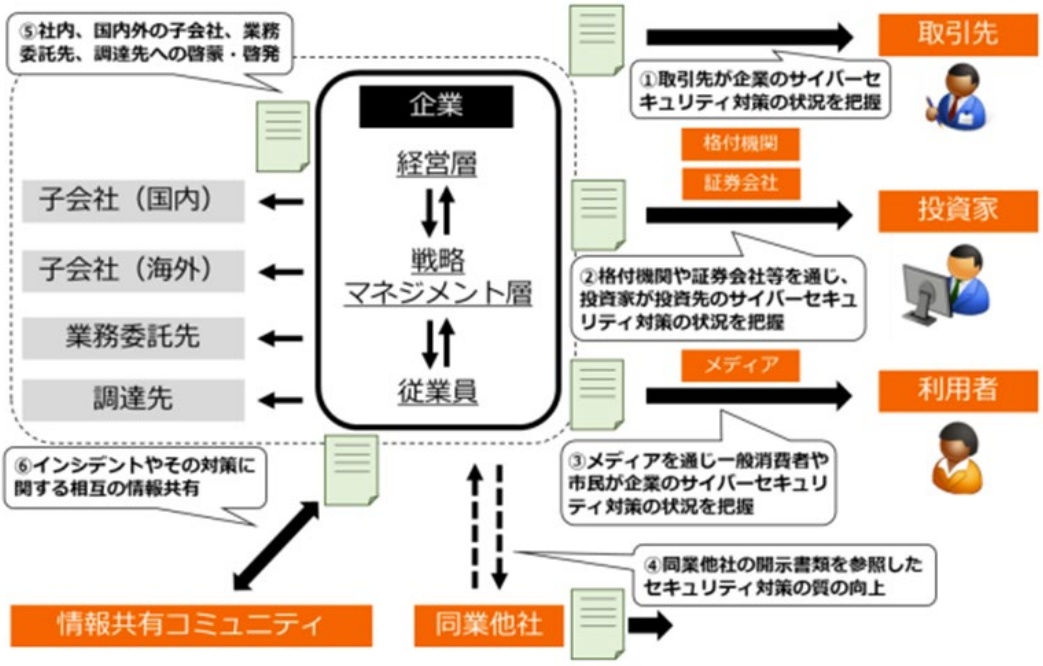
います。
これらの事例から、委託先やビジネスパートナーなどのサイバーセキュリティ対策に関しても、自社同様に十分な注意を払う必要性があることがわかります。また、自社が親会社等から受託している場合には、サプライチェーンの一環として、親会社が求めるサイバーセキュリティ対策が必要となります。

◇セキュリティ対策の格差とサプライチェーン攻撃

全ての企業で十分なセキュリティ対策を講じる必要がありますが、それには、資金面・人材面などの企業体力が不可欠です。
一般的に、中小企業は大企業のような体力を持ち合わせていないため、**大企業と同様の対策を講じることが難しい**場合が生じます。これを、**セキュリティレベルの格差**と呼びます。この格差を利用して、攻撃者はセキュリティレベルの低い企業を経由して重要な情報を狙います。
具体的には、最初にセキュリティ対策が甘い企業の PC を乗っ取り、踏み台にしてサプライチェーン内の別企業の重要な情報を搾取する攻撃を行うのです。

原則３「関係者とは常にサイバーセキュリティに関するコミュニケーションをとる」

業務上の関係者（顧客、取引先、委託先、代理店、利用者、株主など）からのセキュリティに関する信頼を高めるには、普段から自社のサイバーセキュリティ対策や、事故が起きたときの対応について、関係者に明確に説明できるように経営者自身が理解し、整理しておくことが重要です。
そうすることで、万が一インシデントが発生した際にも、適切な対応が取れ、必要以上の不安を与えることなく、信頼関係を維持することができます。



企業をとりまくステークホルダーとサイバーセキュリティ対策の情報開示
引用：総務省「サイバーセキュリティ対策情報開示の手引き」

例えば、第三者認証機関（ISMS/プライバシーマーク）を取得し、自社の HP に公開するなどのアピールも有効です。また、IPA が提供している、「SECURITY ACTION」の宣言も有効な方法と言えます。
「SECURITY ACTION」は中小企業自らが、**サイバーセキュリティ対策に取組むことを自己宣言**する制度です(認証制度ではありません)。自己宣言事業者は SECURITY ACTION サイトへ自社を登録・検索することも可能です。そこに掲載されている取り組み事例を紹介いたします。

◇取り組み事例
企業名：有限会社シブヤ（代表取締役 渋谷勲）
従業員：３名
業　種：製造業（射出成形・金型設計製作等）
取組み段階：二つ星

宣言理由：わが社では WORD、EXCEL などの機密資料以外にも技術情報を含む加工データと呼ばれるものがあり、その保護につながると考えたからです。
また、わが社の情報が盗まれる心配もありますが、それ以上にウイルス感染したデ

ータをお客様に送ってしまうなど、関係者に迷惑をかけることは大問題だと考えていました。これまでセキュリティ対策としてはウイルス対策ソフトを導入している程度でしたが、SECURITY ACTION 宣言には費用がかからないし、一つ星であれば自分たちでも十分取組める内容と思ったため、すぐに申込みました。

一つ星の宣言以降、セキュリティの話題が多く出るようになり、弊社も二つ星を宣言することで、今後ワンランク上の御客様に「弊社はセキュリティ対策に取組んでおり安全です」とアピールできると思い（二つ星を）宣言しました。
（SECURITY ACTION サイト　取組紹介より抜粋）

ここまでサイバーセキュリティ確保に向けた経営者として「認識すべき 3 原則」についてご説明いたしました。 サイバーセキュリティ対策は企業にとって欠かせない重要な要素です。経営者自身がその重要性を理解し、リーダーシップを発揮することで、全社的な取り組みが実現できます。

なお、SECURITY ACTION の取得は、以下の事業で専門家の支援を受けながら取得可能です。

本記事配信時点（2025 年 8 月 29 日）でまだ申し込み可能ですので、お早めにお申し込みください。
令和 7 年度　中小企業サイバーセキュリティ基本対策事業
次回は、「実行すべき重要 7 項目の取組」について、詳しく解説いたします。お楽しみに！

※本記事は令和 6 年度中小企業サイバーセキュリティ対策事業で制作された記事を最新情報等で更新したものです。

配信予定日：2025 年 9 月 5 日(金) 14:00 頃
カテゴリ：基礎から学ぶ！ セキュリティ
タグ：＃初級編 ＃基本対策事業 ＃実用編
過去記事焼き直し：する（過去記事を上書きします）
過去記事：https://cybersecurity-taisaku.metro.tokyo.lg.jp/basics/kisokaramanabu4/

【令和 7 年度版】中小企業におけるセキュリティ脅威への対策強化 ～経営者は何をしなければならないのか 後編～

目次

独立行政法人情報処理推進機構（IPA）が発行している「中小企業の情報セキュリティ対策ガイドライン 第 3.1 版」から、前回に引き続き、経営者として「サイバーセキュリティ確保にどうやって向き合うのか、何をやらなければいけないのか」に焦点を当てています。
前回は「認識すべき 3 原則」についてご説明いたしました。
今回はその続きとなる、「実行すべき重要 7 項目の取組」について説明します。

実行すべき重要 7 項目の取り組み

サイバーセキュリティを確保するために、経営者の役割と取り組みを説明します。
経営者は、重要 7 項目の取組について、自ら実践するか、実際にサイバーセキュリティ対策を実践するうえでの責任者・担当者に対して指示をします。実施する内容によっては、経営者自らが実行しなければならない事もあります。例えば組織全体

の取り組みなどです。

取組１「サイバーセキュリティに関する組織全体の対応方針を定める」
サイバーセキュリティ対策を組織的に実施する意思を、従業員や関係者に明確に示すために、どのような情報をどのように守るかについて、自社に適した**サイバーセキュリティに関する基本方針を定め、明文化して宣言**します。
自社の**経営において最も懸念される事態を明確にする**ことで具体的な対策を促し、組織としての方針を立てやすくなります。
これは、前出の「SECURITY ACTION」の二つ星宣言の必要項目ともなっており、基本的には経営者が自ら実行しなければならないものの一つに挙げられます。

取組２「サイバーセキュリティ対策のための予算や人材などを確保する」
サイバーセキュリティ対策を実施するために、必要な予算と担当者を確保します。これには事故の発生防止だけでなく、**万が一事故が起きてしまった場合の被害の拡大防止や、復旧対応も含みます**。
サイバーセキュリティ対策には高度な技術が必要なため、**専門的な外部サービスの利用やサイバー保険への加入など有効な手段**も検討します。
（前回ご説明した『情報セキュリティガバナンスのフレームワーク』2.ISM の計画）

取組３「必要と考えられる対策を検討させて実行を指示する」
懸念される事態に関連する情報や業務を整理し、損害を受ける可能性（**リスク**）を把握したうえで、責任者・担当者に対策を検討させます。**必要とされる対策には予算を与え、実行を指示**します。
実施する対策は、社内ルールとして文書にまとめておくことで、従業員も実行しやすくなり、取引先などに取り組みを説明する際にも役に立ちます。
実行を指示したサイバーセキュリティ対策がどのように現場で実施されているかについて、月次や四半期ごとなど適切なタイミングで報告させ、進捗や効果を把握します。
（『情報セキュリティガバナンスのフレームワーク』2.ISM の構築と実施）
※取組 1～7 は時系列で手順を書いたものではないため、以降の取組 4～7 も含め、ここで示す必要と考えられる対策として検討しましょう。

取組４「サイバーセキュリティ対策に関する適宜の見直しを指示する」
取組３で指示したサイバーセキュリティ対策について、**実施状況を点検**させ、取組１で定めた**方針に沿って進んでいるかどうか評価**します。
また、業務や顧客の期待の変化なども踏まえて基本方針を適宜見直し、致命的な被

害につながらないよう、**対策の追加や改善を行う**ように、責任者・担当者に指示します。
（『情報セキュリティガバナンスのフレームワーク』4.評価と方向性の見直し）

取組 5「緊急時の対応や復旧のための体制を整備する」
被害範囲や根本原因を速やかに追究して被害の拡大を防ぐ緊急時の対応体制を整備します。
同時に、緊急時の業務復旧に向けた、的確な復旧手順をあらかじめ作成しておくことで、適切な指示を出すことができます。
整備後には予定どおりに機能するかを確認するため、被害発生を想定した模擬訓練を行い、従業員に対する意識づけや適切な対応が可能かを確認します。
経営者のふるまいについても、あらかじめ想定しておけば、冷静で的確な対応が可能になります。
また、この考え方はサイバーセキュリティインシデントにとどまらず、一般的な災害対策でも有効です。

取組 6「委託や外部サービス利用の際にはセキュリティに関する責任を明確にする」
業務の一部を外部に委託する場合は、委託先でも少なくとも自社と同等の対策が行われるようにしなければなりません。そのためには契約書にサイバーセキュリティに関する委託先の責任や実施すべき対策を明記し、合意する必要があります。
IT システム（電子メール、ウェブサーバー、ファイルサーバー、業務アプリケーションなど）に関する技術に詳しい人材がいない場合、自社でシステムを構築・運用するよりも、**外部サービスを利用したほうが、コスト面から有利な場合があります**。ただし、安易に利用することなく、利用規約や付随するサイバーセキュリティ対策などを十分に検討するよう担当者に指示する必要があります。
◇参照：より良い外部サービスが選べる「サイバーセキュリティお助け隊サービス」
「サイバーセキュリティお助け隊サービス」は、中小企業等に対するサイバー攻撃への対処として不可欠なサービスを要件にまとめ、**ワンパッケージで安価に提供するサービス**です。
所定の審査機関により要件を満たすことが確認された民間サービスを「サイバーセキュリティお助け隊サービス」として IPA が登録・公表しています。
サイバーセキュリティ対策のワンパッケージ例
（１）見守り：24 時間 365 日監視挙動や問題のある攻撃を検知し、あなたの PC とネットワークを守ります。

（２）駆付け：問題が発生したときに地域の IT 事業者等が駆付け対応します。（リモート支援の場合あり）
（３）保険：簡易サイバー保険で駆付け支援等のサイバー攻撃による被害対応時に突発的に発生する各種コストが補償されます。
　参考：サイバーセキュリティお助け隊サービスリスト
※『IT 導入補助金』(中小企業・小規模事業者のみなさまが IT ツール導入に活用いただける補助金)で「サイバーセキュリティお助け隊サービス」のサービス利用料の支援が受けられます。
　参考：https://it-shien.smrj.go.jp/applicant/subsidy/security/

取組 7「サイバーセキュリティに関する最新動向を収集する」
情報技術の進歩の速さから、実施を検討すべき対策は目まぐるしく変化します。
自社だけで全てのサイバーセキュリティ情報を把握することは困難です。この場合には、サイバーセキュリティに関する**最新動向を発信している公的機関**などを把握しておき、常時参照することでセキュリティリスクに備えるように担当者に指示します。

また、知り合いや**コミュニティへの参加で情報交換**を積極的に行い、得られた情報について、自社内や委託先などと共有します。
　参考：サイバーセキュリティに関する最新動向を発信している公的機関
　・IPA（独立行政法人情報処理推進機構）
　・NISC（現：NCO（国家サイバー統括室））

2 回に分けてサイバーセキュリティ確保に向けた、経営者としての「認識すべき 3 原則」と「実行すべき重要 7 項目の取組」と「関連するサービスに」ついてご説明しました。委託先を含め、会社規模や目的に合ったサイバーセキュリティ対策組織を作り、常に進化させることが最も重要なことと言えます。
次回もお楽しみに！

※本記事は令和 6 年度中小企業サイバーセキュリティ対策事業で制作された記事を最新情報等で更新したものです。

配信予定日：2025 年 9 月 5 日(金) 14:00 頃
カテゴリ：もっと知りたい！ セキュリティ
タグ：＃知識編＃セキュリティ対策点検
過去記事焼き直し：しない（新規記事です）
記事 URL（新設します）：https://cybersecurity-taisaku.metro.tokyo.lg.jp/know_more/zenkan_chuuigimu/

情報セキュリティ対策における善管注意義務

目次

企業活動においては、ミスや障害、サイバー攻撃等による不測の事態が発生し、契約している業務が予定通りに遂行できなくなったり、機密情報が外部に漏えいしたりするなど、意図せずして顧客や取引先に大きな損害を及ぼしてしまう可能性があります。
状況によっては顧客や取引先との間で訴訟問題にまで発展し、企業経営者等の善管注意義務が問われることにもなりかねません。ということで、今回は情報セキュリティ対策における善管注意義務について見ていきましょう。

●善管注意義務とは
そもそも善管注意義務とは、社会通念上あるいは客観的に見て、当然要求される注意を払う義務とされており、民法の第 644 条では「受任者（委任を受けた者）は、委任の本旨に従い、善良な管理者の注意をもって、委任事務を処理する義務を負う」と規定しています。

つまり、企業であれば、特定の管理者や経営者だけでなく、契約等によって何らかの業務を委任された人に対して求められます。

とはいえ、企業の取締役は法律上（会社法 第 330 条）会社から経営を委任された立場であるため、その責任は重く、善管注意義務を怠って会社に損害を与えた場合、損害賠償責任を負わなければなりません。（会社法 第 423 条）

●情報セキュリティ対策において善管注意義務が問われる例
情報セキュリティ対策において善管注意義務が問われるケースとしては、例えば次のよう

なものが挙げられます。

・ネットワーク機器の既知の重大な脆弱性を突いた攻撃によって社内ネットワークに侵入され、ファイルサーバに保存されていた顧客情報が外部に漏えいした。
・ランサムウェアによる攻撃で大規模なシステム障害が発生し、委託された業務が予定通りに遂行できなくなった。
・会員向け Web サイトに重大な脆弱性があったため、第三者の不正アクセスによって正規会員のポイントが不正利用された。
・クラウド上で顧客に提供している業務管理システムの設定不備により、機密情報が誰でもアクセスできる状態になっていた。
・業務委託先の従業員が USB メモリで顧客の個人情報を不正に持ち出し、紛失した。

●情報セキュリティ対策における善管注意義務違反が認められた判例
過去に情報セキュリティ対策における善管注意義務が法廷の場で問われた判例を示します。

＜原告＞
　インテリア商材の卸小売及び通信販売等を行う会社
＜被告＞
　原告の商材等のウェブ受注システムの開発を受託した会社

＜発生した事象と判例＞
・上記ウェブ受注システムのサーバに不正アクセスがあり、SQL インジェクション（※）と呼ばれる攻撃によって顧客のクレジットカード情報を含む個人情報が流出。
・原告は、被告に対し、「適切なセキュリティ対策を講じていなかった」として、約 1.1 億円の損害賠償を請求。
・東京地裁は、被告がセキュリティリスクを認識していたにもかかわらず、適切な対策を怠ったことから善管注意義務違反があったと認定。

※用語解説：SQL インジェクション
ユーザの入力データをもとに SQL 文を編集してデータベースにクエリを発行し、その結果を表示する仕組みになっているウェブページにおいて、不正な SQL 文を入力することでデータベースを操作したり、データベースに登録された個人情報などを不正に取得したりする攻撃手法。

＜善管注意義務違反とした根拠＞
・経済産業省は「個人情報保護法に基づく個人データの安全管理措置の徹底に係る注意喚

起」において、 IPA（独立行政法人 情報処理推進機構）が紹介する SQL インジェクション対策の措置を重点的に実施することを求める旨の注意喚起をしていた。
・IPA は「大企業・中堅企業の情報システムのセキュリティ対策～脅威と対策」において、ウェブアプリケーションに対する代表的な攻撃手法として SQL インジェクション攻撃を挙げ、その対策をすることが必要である旨を明示していた。

●情報セキュリティにおける善管注意義務の判断基準
上記判例のように、情報セキュリティ対策における善管注意義務においては「その当時の技術水準」に従った対策が行われていたかが問われています。そのため、契約書等で明示的な合意がなくても、「その当時の技術水準」に従った対策を講じることが、法的な義務として求められるでしょう。

「その当時の技術水準」としては、判例にあるように、各省庁や IPA のような公的なセキュリティ機関等が公表している文書、ガイドライン等において対策実施の必要性が説かれていることをもって、それが「当時の技術水準」に該当すると判断される可能性が高いと考えられます。

上記に該当するガイドラインの例として、次のようなものが挙げられます。こうした文書を活用する等して自社のセキュリティ対策実施状況を定期的に点検し、善管注意義務違反とならないよう継続的に改善を図っていただくことをおすすめします。

■中小企業の情報セキュリティ対策ガイドライン（IPA）
https://www.ipa.go.jp/security/guide/sme/about.html

＜概要＞
・中小企業の経営者や実務担当者が、情報セキュリティ対策の必要性を理解し、情報を安全に管理するための具体的な手順等を分かりやすく示したガイドライン
・経営者が認識すべき「3 原則」、経営者がやらなければならない「重要 7 項目の取組」を記載
・すぐに使える「情報セキュリティ基本方針（サンプル）」や「情報セキュリティ関連規程（サンプル）」等のひな形を付録として提供

■サイバーセキュリティ経営ガイドライン（経済産業省、IPA）
https://www.meti.go.jp/policy/netsecurity/mng_guide.html

＜概要＞

・IT に関するシステムやサービス等を供給する企業及び経営戦略上 IT の利活用が不可欠である企業の経営者を対象に、経営者のリーダーシップの下で、サイバーセキュリティ対策を推進するため、経産省と IPA が策定したガイドライン
・サイバー攻撃から企業を守る観点で、経営者が認識する必要のある「3 原則」、及び経営者が情報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）に指示すべき「重要 10 項目」を提示

配信予定日：2025 年 9 月 12 日(金) 14:00 頃
カテゴリ：中小企業サイバーセキュリティ対策事業の知見
タグ：＃知識編＃啓発事業
過去記事焼き直し：しない（新規記事です）
記事 URL（新設します）：https://cybersecurity-taisaku.metro.tokyo.lg.jp/know_more/cyber-taisakutiken1/

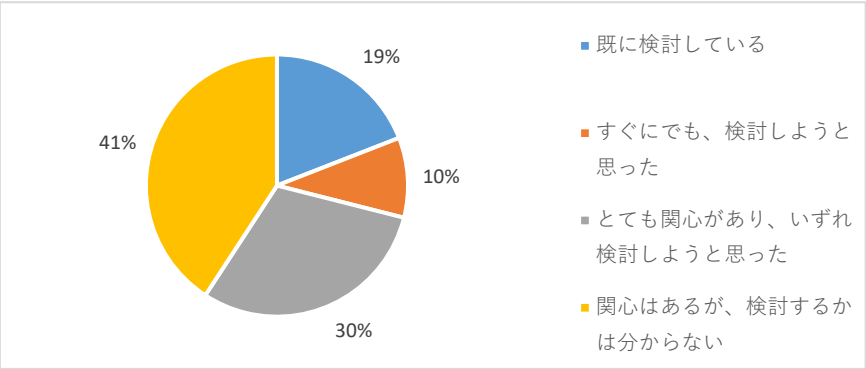
参加して変わった！セキュリティ対策にかける費用

目次

本記事では東京都が独自に調査した情報を発信いたします。
今回は令和 6 年度中小企業サイバーセキュリティ啓発事業からの情報を発信します。

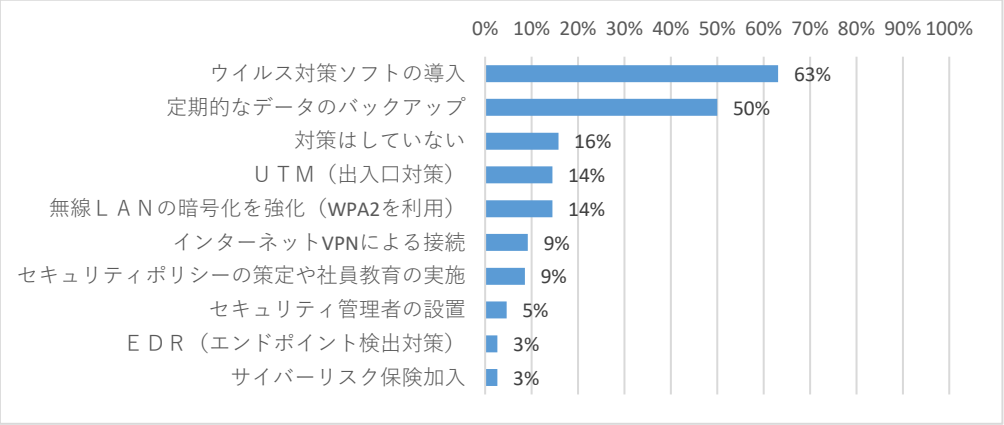
●セキュリティは関心があっても手が出せない
令和 6 年度中小企業サイバーセキュリティ啓発事業では支援対象企業は約 150 社、多種多様な業種の企業様へ支援を行いました。支援開始前に取得したアンケートは以下の結果でした。

セキュリティ対策の検討状況



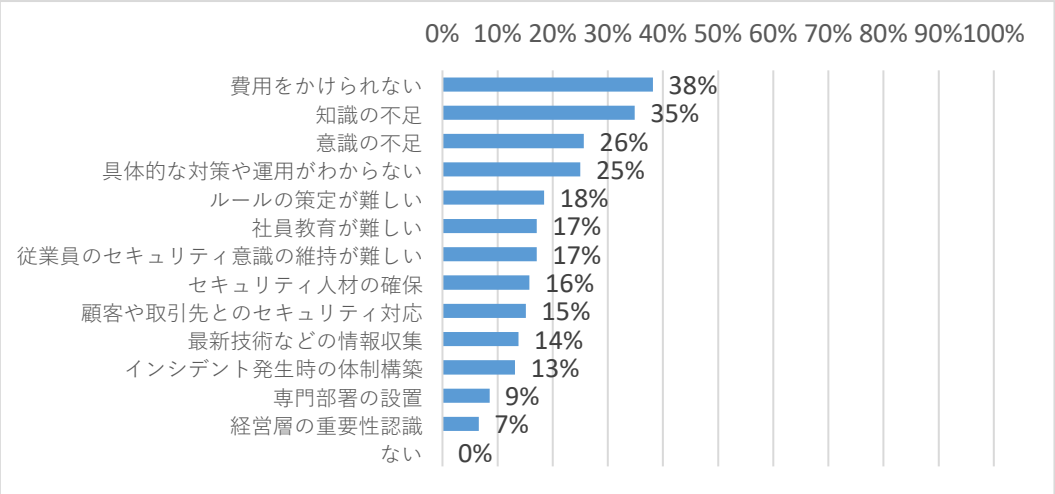
⇒８１％が未検討の状況です。

導入済みのセキュリティ対策



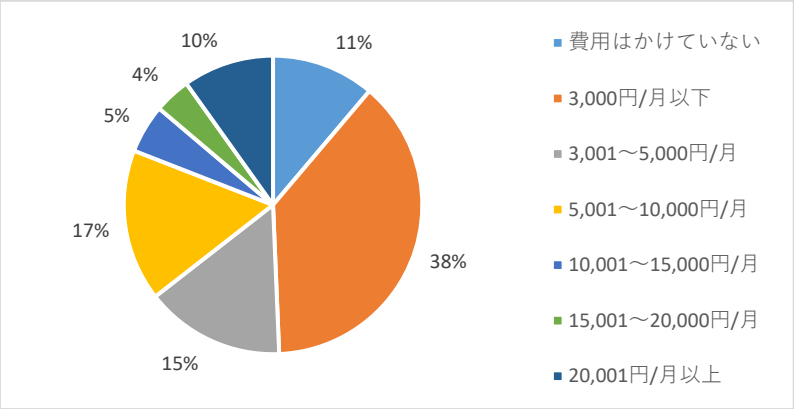
⇒ほぼすべての企業が導入していると思われる「ウイルス対策ソフトの導入」が６３％、「対策はしていない」が１６％という結果でした。ただしこの結果は、次の質問の結果を見ると本当に導入していないとは言い難いです。

セキュリティ対策に関する課題



⇒「知識の不足」が３５％、「具体的な対策や運用がわからない」が２５％ありました。自社の対策状況を正しく把握できておらず、前設問の結果になっている（ウイルス対策ソフトを導入しているかわからない）と推量されます。
最も多い回答である「費用をかけられない」については具体的な金額も聞いています。

セキュリティ対策にかけている費用（月額）



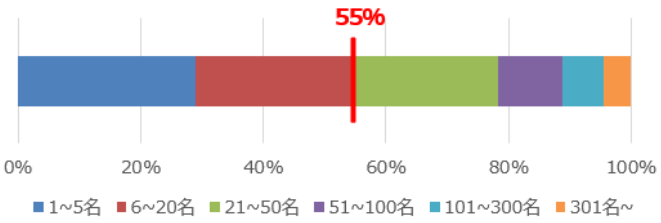
⇒半数の４９％が 3,000 円以下という状況です。この結果をどう見るか、２つの要素で考えていきたいと思います。

A. セキュリティ対策の価格感

独立行政法人情報処理推進機構（IPA）が推進するセキュリティ対策サービスの価格帯を見ると、ネットワーク監視で月額 6,000 円～、端末監視で月額 1 台 750 円～となっています。

B. 調査対象企業の従業員数

半数が従業員 20 名以下でした。



これら A、B の結果をふまえると、セキュリティ対策費用が月額 3,000 円/月と回答した企業の中には、ネットワーク監視はしておらず、端末監視も全員分行っていない企業もあると想定されます。

●東京都が描いたステップアッププログラム

東京都サイバーセキュリティ対策事業は、セキュリティ対策にこれから着手する企業から、より高度な対策をしたい企業まで、対策度合い（レベル）に応じた支援メニューを用意しています。また、現状を把握し次に何をするべきか整理したい企業のためのメニューも用意しています。

[支援メニューと概要]

レベル１：啓発事業、セミナー・メール訓練・ネットワーク調査等

レベル２：基本対策事業、UTM/EDR の試行導入・規程策定支援等

レベル３：実践力強化プログラム、セミナー・ワークショップ・課題解決支援等

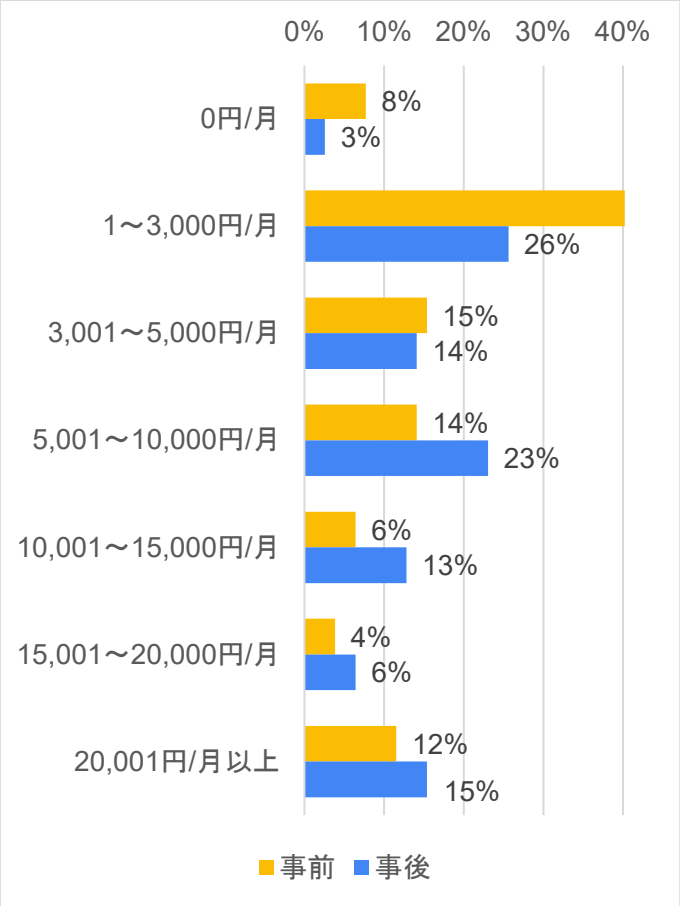
レベル３：インシデント対応強化、CSIRT 構築・IT-BCP 策定支援等

全レベル：フォローアップ、メルマガ・セミナー・セキュリティ対策点検等
※詳細はこちらの記事をご覧ください。

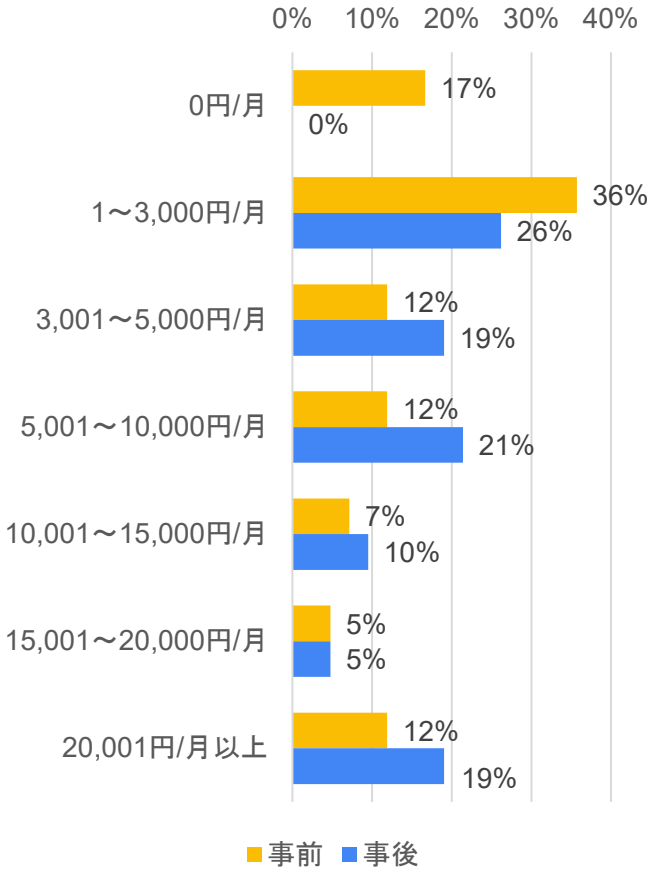
前述までのアンケートを行った啓発事業はレベル１に位置付けられています。名前の通り「啓発」を目的としており、セミナー、標的型攻撃メールの訓練、ネットワーク調査（企業のインターネット接続箇所を中心に調査し構成図を作成する）といった基本的な事項を行っています。

●正直、啓発事業って意味があるのか
昨年度の事業に参加いただいた方には、事後にセキュリティ対策にかける（かけようとしている）費用を聞きました。その結果は以下です。

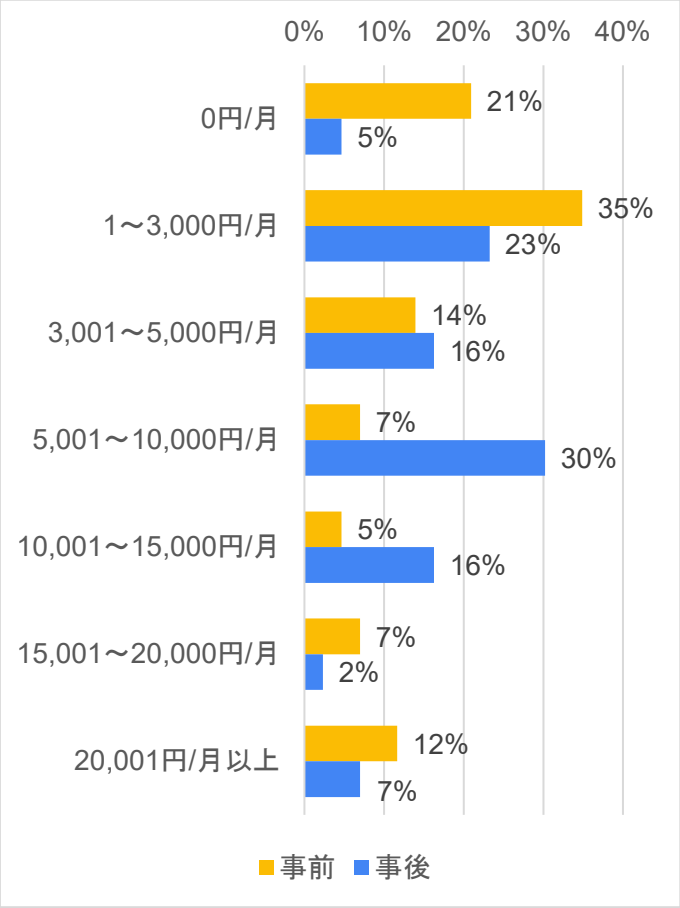
セキュリティ対策にかける費用（セミナー参加前後比較）



セキュリティ対策にかける費用（メール訓練参加前後比較）



セキュリティ対策にかける費用（ネットワーク調査参加前後比較）



セミナー、メール訓練、ネットワーク調査、いずれの取組においても参加した企業はセキュリティ対策にかける費用を増やそうという考えに至ったと考えられます。啓発事業に参加したことで「セキュリティ対策における課題」で最も割合の高かった「費用をかけられない」という状況が好転したと考えられます。

●今後の展望

今年度も啓発事業は行われています。来年度も継続・発展できるよう、東京都、事業者で取り組んでいる最中です。

令和７年度中小企業サイバーセキュリティ啓発事業

※参加募集は締め切っています。

今回は、昨年度の啓発事業での調査結果を題材に、中小企業のセキュリティ対策状況の実態を共有させていただきました。次回以降、他の事業（基本対策事業等）を題材に、得られた知見を記事にさせていただきます。東京都事業は具体的な対策や、専門家派遣を毎年数百社以上に行っています。東京都では支援を通じて得られた知見、見えてきた傾向から、日本の中小企業をサイバー攻撃から守る術を提供していきたいと考えております。皆様からのご

意見・ご感想、本ウェブサイトの下部に記載のあるお問い合わせ先へ是非お寄せください。

配信予定日：2025 年 9 月 12 日(金) 14:00 頃
カテゴリ：もっと知りたい！セキュリティ
タグ：＃知識編
過去記事焼き直し：しない（新規記事です）
記事 URL（新設します）：https://cybersecurity-taisaku.metro.tokyo.lg.jp/know_more/secure-by-design/

セキュリティ・バイ・デザイン概説

目次

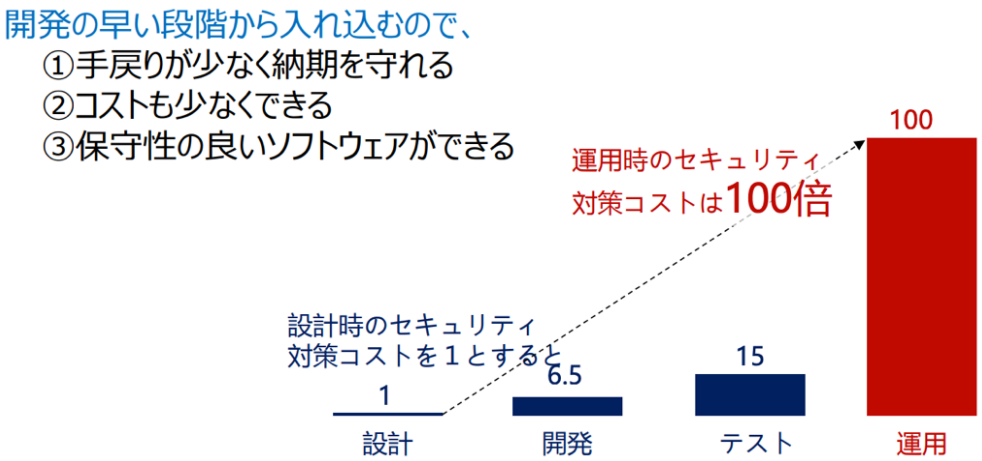
中小企業の経営者や情報システム担当者の皆さん、日々のセキュリティ対策、お疲れ様です。本記事では、情報システムに対して、確実かつ効率的にセキュリティを確保するため、システム開発の企画段階から対策を実装する「セキュリティ・バイ・デザイン」について解説します。

●セキュリティ・バイ・デザインとは
セキュリティ・バイ・デザインは、内閣サイバーセキュリティセンター（NISC：National center of Incident readiness and Strategy for Cybersecurity）※等が十数年前からその必要性について提唱しており、2011 年に NISC が公表した「情報セキュリティを企画・設計段階から確保するための方策に係る検討会報告書」でセキュリティ・バイ・デザインの考え方等が示されています。
また、デジタル庁が 2022 年に発行した「政府情報システムにおけるセキュリティ・バイ・デザインガイドライン」によれば、「情報システムの企画工程から設計工程、開発工程、運用工程まで含めた全てのシステムライフサイクルにおいて、一貫したセキュリティを確保する方策のこと」と定義されています。

※2025 年 7 月に内閣官房組織令に基づき「国家サイバー統括室（NCO：National Cybersecurity Office)」に改組

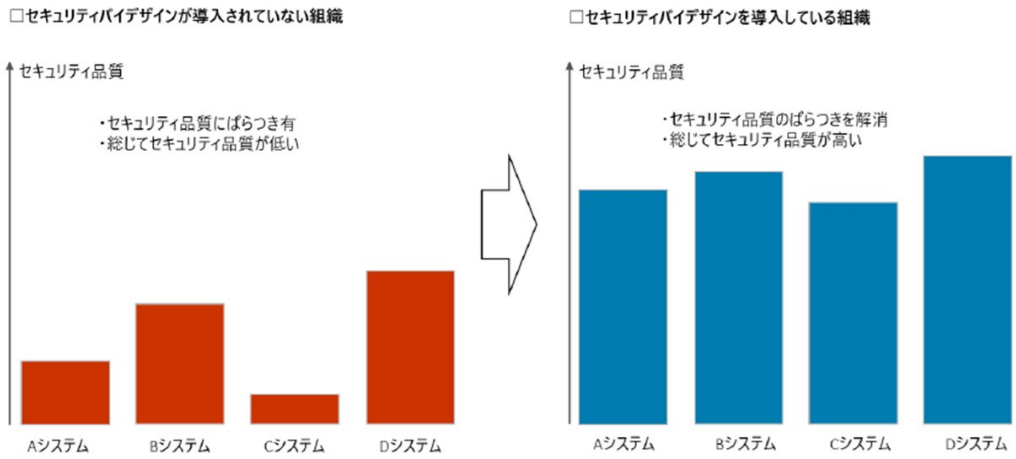
●セキュリティ・バイ・デザイン導入によるメリット
次に、セキュリティ・バイ・デザイン導入によるメリットについて見てみましょう。
主なメリットは二つあり、その一つがコストの低減です。組織にとって適切なシステム開発

プロセス、リスク評価、リスク管理体制等をセキュリティ・バイ・デザインとして導入することで、情報システムの企画工程からセキュリティリスクへの対応方針を定め、システム運用に至るまで一貫したセキュリティ対策の実装が可能となります。これにより、セキュリティ対策の漏れ等による上流工程への手戻りを防止でき、納期の遵守やセキュリティ対策コスト低減が可能となります。



セキュリティ対策の実施タイミングと対策コスト
「セキュリティ・バイ・デザイン導入指南書」より
(https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2022/ngi93u0000002kef-att/000100451.pdf)

二つ目のメリットは、システムのセキュリティ品質の向上です。自組織の管理対象となる全ての情報システムを対象に、システム開発から運用まで標準化されたセキュリティ対策を実施し、対策の妥当性を検証する仕組みを導入することで、システムによるセキュリティ品質のばらつきを解消し、組織全体におけるシステムセキュリティ品質の底上げが可能となります。



セキュリティ・バイ・デザイン導入組織のセキュリティ品質メリット
「政府情報システムにおけるセキュリティ・バイ・デザインガイドライン」より
(https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/7e3e30b9/20240131_resources_standard_guidelines_guidelines_01.pdf)

●セキュリティ・バイ・デザインの基本的な考え方
セキュリティ・バイ・デザイン実施にあたっては、その実効性を高めるため、その根底にある基本的な考え方（原則）を理解しておくことが重要です。ここでは、その六つの原則について見てみましょう。

1．事後ではなく、予防的（未然）にセキュリティ対策を組み込む
セキュリティ・バイ・デザインは、インシデント等の発生を契機に取組むのではなく、予防的（未然）に実施することが求められます。それにより、インシデントの発生する可能性を低減するとともに、インシデント発生時には影響範囲を極小化し、被害を低減する効果が見込まれます。

2．全てのシステムライフサイクルを対象とし、関係者間で責任範囲を明確にする
セキュリティ・バイ・デザインは、特定のシステム開発工程においてのみ実施するのではなく、 全てのシステムライフサイクルを通して、一貫したセキュリティ対策を実施することが求められます。
また、システム開発・運用業務等を委託している関係者間でセキュリティ対策の責任範囲を明確にし、抜け漏れなくセキュリティ対策を実施することが求められます。
過去に発生したインシデントにおいて、特定の工程でしかセキュリティ対策が行われ

ていなかったり、関係者間での責任分界点が不明確であったりしたことが、発生・被害拡大の原因となったケースが数多くあります。

3．システムの初期設定値においてセキュリティが担保された状態を実現する
システムの初期設定値としてセキュリティが担保された状態を実現することが重要です。これにより、システム運用者や利用者によるミス等を極力少なくすることが求められます。
なお、一般的に利用されている ICT 製品において、初期設定では十分なセキュリティが担保されていないことも多くあるため、それを認識の上、設定について十分留意する必要があります。

4．システム特性等に応じ、過不足ないセキュリティ対策を実施する
インターネットで公開するシステム、組織内に限定して利用するシステム、個人情報等の重要情報を扱うシステム等、企業の情報システムには様々なものがあります。
そのため、全てのシステムに画一的なセキュリティ対策を講じるのではなく、システムの特性や重要度等に応じ、過不足なくセキュリティ対策を実施することが求められます。

5．セキュリティリスクの評価、管理を継続的に実施する
セキュリティ対策は一度実施すれば完了というわけではなく、 その後も対策の充足性や残存するリスクの評価を継続的に行い、改善していくことが求められます。これを実現するため、セキュリティリスクを適切に管理するための体制を整備するとともに、リスク管理プロセスを確立し、運用していくことが求められます。

6．利便性を損なうことなくセキュリティを確保することを目指す
一般的に、セキュリティと利便性はトレードオフ（相反）の関係にあるため、利便性を高めれば高めるほどセキュリティは低下し、その逆に、セキュリティを高めれば高めるほど利便性は損なわれる傾向にあります。
しかしながら、セキュリティ・バイ・デザインでは、システムにおける利便性確保とセキュリティ強化を同時に実現し、双方に利益があるポジティブサムを目指すことが求められます。

今回はセキュリティ・バイ・デザインについて、その概要、導入によるメリット、基本的な考え方等について解説しました。次回以降はセキュリティ・バイ・デザインの実施工程と実施内容等について解説します。

配信予定日：2025 年 9 月 19 日(金) 14:00 頃
カテゴリ：中小企業サイバーセキュリティ対策事業の知見
タグ：＃知識編＃基本対策事業
過去記事焼き直し：しない（新規記事です）
記事 URL（新設します）：https://cybersecurity-taisaku.metro.tokyo.lg.jp/know_more/cyber-taisakutiken2/

セキュリティ対策ソフト・ハードを体験して変わる事

目次
●約３か月にわたるソフト・ハードの実体験
●併せて参加可能な情報セキュリティ規定類の策定支援
●体験して変わる事
●今後の展望

本記事では東京都が独自に調査した情報を発信いたします。
今回は令和６年度中小企業サイバーセキュリティ基本対策事業からの情報を発信します。

●約３か月にわたるソフト・ハードの実体験
令和６年度中小企業サイバーセキュリティ基本対策事業では、情報セキュリティ対策ソフトである“EDR”もしくは対策機器（ハード）である“UTM”を約３か月間、参加企業様に導入し、実体験いただくことが可能です。

※EDR／UTM ともにコンピュータウイルス等の対策になります。EDR はパソコン１台１台にインストール、UTM はインターネットの出入り口に装置を取り付けて機能します。詳しくは以下の「３分でわかる！用語解説」を参照願います。
EDR
UTM

EDR はパソコン内の既存のソフトウェアとの競合（相性が悪いと動作に支障をきたすこともある）に注意し、UTM はインターネット通信に影響を与えないよう注意して導入を行います。

EDR／UTM の導入により、コンピュータウイルス等の検知が可能となるのですが、既存の環境に変化が加わるため、誤検知などの問題も発生します。しかし、双方とも通常とは異なる挙動を検知することができるため、業務上不要なウェブサイトの利用を検知したり、会社

が許可していないソフトウェアの利用を検知したりできます。EDR／UTM の導入により、コンピュータウイルス感染のような問題（インシデント）の早期発見や状況把握が可能となります。
東京都では、EDR／UTM をお試し導入する基本対策事業を、インシデント対応の準備段階として位置付けています。詳しくは以下の記事をご覧ください。
東京都サイバーセキュリティ対策事業の成り立ちと今後について

●併せて参加可能な情報セキュリティ規定類の策定支援
基本対策事業では、会社が守るべき情報セキュリティのルール（情報セキュリティ規定類）を、専門家が 4 回訪問して策定する支援も行っています。
４回の訪問で行う事は以下です。また、IPA のひな型を用い、情報セキュリティ規定類を作成するとともに、IPA が創設し推奨する中小企業自らが情報セキュリティ対策に取組むことを自己宣言する制度「SECURITY ACTION 二つ星宣言」も目指します。

	支援の流れ	具体的支援
１回目	リスク洗い出し 情報資産管理 状況の確認	自社診断ツール兼ヒアリングシートを作成し、現在のレベルと問題点を把握。情報資産管理台帳を用いて管理すべき情報資産とその管理状況も把握。
２回目	対策の決定 基本方針の 策定・見直し	基本方針とその作成を補助する情報セキュリティ基本方針策定雛形ツールや、関連規定作成のための情報セキュリティ関連規定雛形ツールについて説明し、それらを用いた検討の実施。また実施計画を作成する課題の具体化と、SECURITY ACTION 二つ星自己宣言の準備。
３回目	関連規定の 策定・見直しに 向けた検討	診断結果FBシートを用いた具体的な対策内容と優先順位を検討。情報セキュリティ関連規定雛形ツールでの基本方針策定の確認と実施計画書作成の支援。SECURITY ACTION 二つ星自己宣言実施への支援。
４回目	関連規定、実施計画書のレビュー（指導まとめ）	策定された関連規定や実施計画書の作成状況の確認・レビューを実施。自社診断ツール兼ヒアリングシートでの再診断を行い、今後の継続的な取組に向け支援。

詳細は本記事ではここまでとさせていただきます。
※詳しくは令和 7 年度中小企業サイバーセキュリティ基本対策事業
セキュリティ対策を始めるにあたり、ソフトやハードの導入に目が行きがちですが、ルールが無いと不正な情報持出し等が発生した時に、“不正”と言い切る理由に欠くことになります。情報セキュリティ規定類の策定は、セキュリティ対策の基本と言えます。

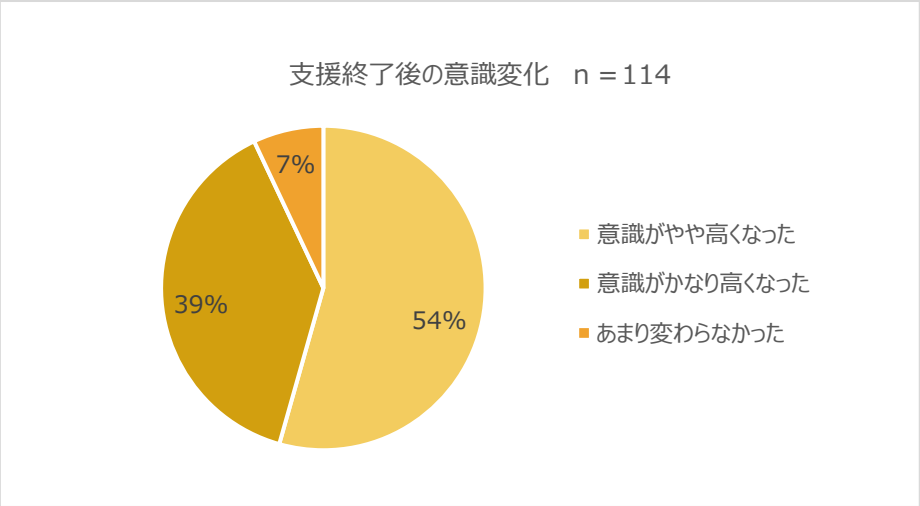
●体験して変わる事
令和 6 年度中小企業サイバーセキュリティ基本対策事業の参加企業へのアンケート結果を紹介していきます。

EDR は 50 社が体験し、うち 48 社にアンケートを取得、88%の企業から満足したとの回答を得ました。半数以上の企業から「レポートで攻撃内容を確認できるのが良かった」との声をいただいています。

UTM は 53 社が体験し、うち 52 社にアンケートを取得、83%の企業から満足したとの回答を得ました。半数以上の企業から「レポートで攻撃内容を確認できるのが良かった」との声をいただいています。
EDR／UTM ともに、レポートで攻撃内容を確認できる点が最も評価されていました。

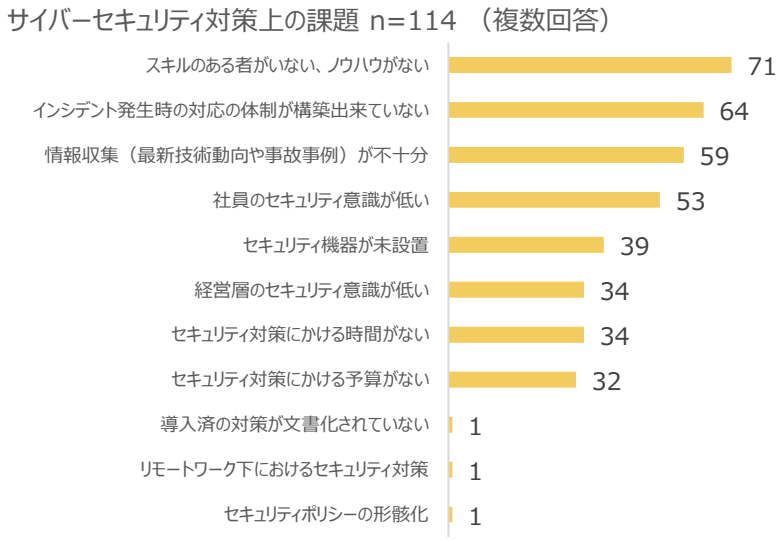
また、情報セキュリティ規定類の策定支援（事業上の名称：情報セキュリティマネジメント指導）については 100 社が参加し、うち 98 社にアンケートを取得、99%の企業から満足したとの回答を得ました。その理由として最も多かったのは約 80%の企業から「自社で対策すべきことが分かったから」との声をいただいています。

これら EDR／UTM、規定類の策定支援を受けた方のうち 114 社にアンケートを取得した結果、以下の回答を得ています。



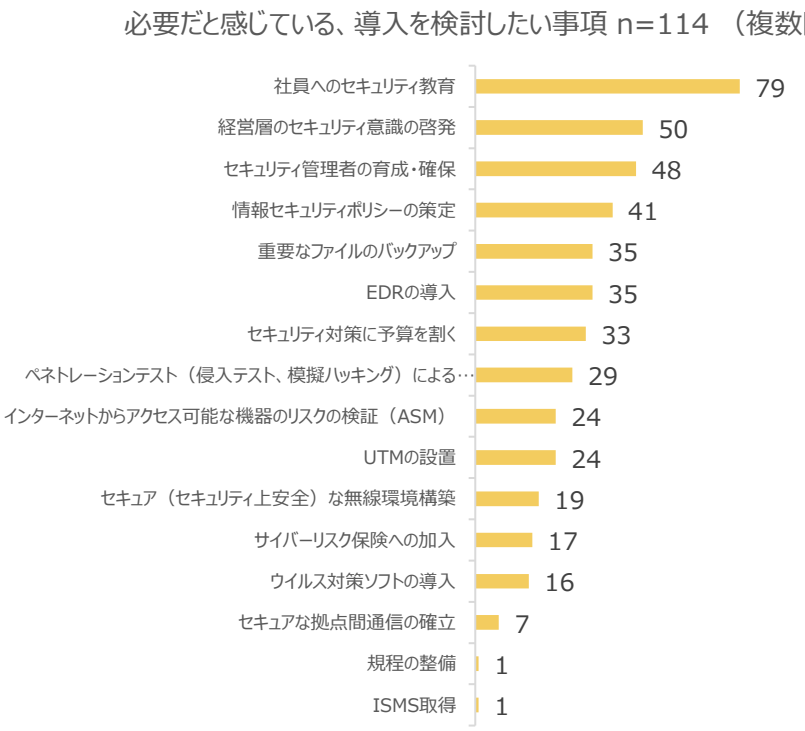
実に 93%の企業の意識が高くなりました。ソフト・ハードや専門家の 4 回指導という実体験を通じることで、意識が高くなる効果がありました。

また、意識したものが具体的に何なのかを示すものとして以下も聞いています。



意識が高まったという事は、それまでは意識をしていなかった（≒知識が無かった）と考えられます。そのため「スキルのある者がいない、ノウハウがない」が最も多かったと推察されます。

体験することで意識が高まりますが、スキルやノウハウを得る・人材に定着することが課題です。もう１問、今後必要だと感じている、導入を検討したい事項についても聞いています。結果は以下です。



「社員へのセキュリティ教育」が必要だと感じている回答が最も多くを占めました。

●今後の展望

今年度も基本対策事業は行われています。来年度も継続・発展できるよう、東京都、事業者で取り組んでいる最中です。

令和 7 年度中小企業サイバーセキュリティ基本対策事業

2025 年 9 月 19 日時点まだ定員に達していませんので、お早めにお申し込みください。

なお、お申込みいただいた時点で定員に達している可能性もございます。詳しくは上記サイトをご確認願います。

前章の「●体験して変わる事」の最後のアンケート設問の結果で最も多かった「社員へのセキュリティ教育」は、実は他の東京都事業でも同様の結果になっています。会社全体へ情報セキュリティ対策を浸透させていく事に、最も課題があると推察しています。その課題への有効打は何か、次回以降の東京都事業の記事も通じ考えていきたいと思います。

今回は、昨年度の基本対策事業で得られた知見を記事にしました。次回以降も、他の事業（実践力強化等）を題材に、得られた知見を記事にさせていただきます。東京都事業は具体的な

対策や、専門家派遣を毎年数百社以上に行っています。東京都では支援を通じて得られた知見、見えてきた傾向から、日本の中小企業をサイバー攻撃から守る術を提供していきたいと考えております。皆様からのご意見・ご感想、本ウェブサイトの下部に記載のあるお問い合わせ先へ是非お寄せください。

配信予定日：2025 年 9 月 19 日(金) 14:00 頃
カテゴリ：基礎から学ぶ！ セキュリティ
タグ：＃初級編 ＃基本対策事業 ＃用語編 ＃知識編
過去記事焼き直し：する（過去記事を上書きします）
過去記事：https://cybersecurity-taisaku.metro.tokyo.lg.jp/basics/kisokaramanabu7/

【令和 7 年度版】中小企業におけるセキュリティ脅威への対策強化 ～ランサムウェアによる攻撃事例から対策を学ぶ（1/2）～

目次

独立行政法人情報処理推進機構（IPA）が毎年発行している「情報セキュリティ 10 大脅威 2025」から、中小企業の経営者やシステム担当者が注目すべき点を掘り下げていきます。
今回は 1 位に挙げられている「ランサムウェアによる攻撃」に焦点を当てます。
2016 年以降 10 年間にわたり 10 大脅威の 1 位を取り続けていることから、最も被害の多い脅威と言えます。
この脅威が業務に与える影響や、どのように対策すべきなのかを 2 回に分けて解説いたします。1 回目の今回は、ランサムウェアの種類と攻撃の特徴について解説いたします。

引用元：IPA 情報セキュリティ 10 大脅威 2025 解説書［組織編］より

１．ランサムウェアとは

ランサムウェア(Ransomware)とは、Ransom(身代金)と Software(ソフトウェア)を組み合わせた造語であり、マルウェア※の一種です。

攻撃者は PC やサーバーをランサムウェアに感染させることで組織の重要なデータを人質に取り、その復旧やシステムの解除を引き換えに金銭、すなわち「身代金」を要求します。

さらに、攻撃者は複数の脅迫を組み合わせることで、攻撃を受けた組織が金銭を支払うことを検討せざるを得ない状況を作り出そうとします。

ランサムウェア攻撃は、組織の規模や業種に関わらず、あらゆる対象に及びます。
ランサムウェアに感染すると、データの暗号化や重要情報の奪取といった被害に遭遇するだけでなく、その調査や復旧に多くの費用と時間が掛かります。

また、業務やサービス提供の停止による経済的損失や、顧客や取引先からの信頼失墜の被害につながるおそれもあります。広く利用されているサービスがランサムウェアに感染すると、社会にも大きな影響を与えることになります。

※マルウェア(malware)とは
malicious（マリシャス：悪意のある）に software（ソフトウェア）の 2 つの単語が組み合わさった造語です。コンピューターウイルスやワーム、トロイの木馬、スパイウェア、など、ユーザーのデバイス(PC、iPad、スマホ等)に不利益をもたらす悪意のあるプログラムやソフトウェアを総称する言葉です。

２．ランサムウェアの代表的な種類

（１）ばらまき型ランサムウェア攻撃

日本では 2015 年頃からランサムウェアの被害が発生しだしました。
当初のランサムウェアはウイルスを添付したメールを、不特定多数の組織に対して無差別に送信する「ばらまき型」でした。
受信したユーザーが添付ファイルを実行することで感染させ、システムのロックや、ファイルを暗号化して使用不能にしたのちに、元に戻すことと引き換えに「身代金」を要求するメッセージ（ランサムノート）を表示させる手法です。

（２）標的型ランサムウェア攻撃

2019 年後半から、海外では「Human-Operated」、日本では「標的型ランサムウェア攻撃」、「侵入型ランサムウェア攻撃」と呼ばれる、特定の組織を狙って攻撃する手法が主流となってきました。
攻撃者が事前に標的組織のネットワークに侵入し、組織の機密情報を窃取して、最終的にランサムウェアを実行し金銭を要求する手法です。

（3）二重脅迫型
標的型ランサムウェア攻撃に「情報の暴露」を加えた二重脅迫の手法です。
データの暗号化に加え、「身代金を支払わなければ、窃取した情報を暴露する」といった二重の脅迫により対象組織を追い詰め、より多額の身代金を払わせようとします。このような脅迫の手法は、「暴露型」または「二重脅迫型」と呼ばれます。

（4）多重脅迫型
被害組織の Web サーバーなどに大量のパケットなどを送りつけて正常なサービス提供ができないよう妨害する DDoS※攻撃の実施や、取引先などの関連組織に情報漏えいを通知するなどの脅迫を行う「多重脅迫」の手法も確認されています。この手法では、対象組織やその周辺に多角的な圧力を加えることで、身代金の要求を迫ります。

※DDoS（ディードス）攻撃とは
Distributed Denial of Service（分散型サービス拒否）攻撃の略称です。Web サーバーなどに対して、複数の場所から大量の通信を発生させることで正常なサービス提供を妨げる攻撃です。

3．標的型ランサムウェアの攻撃
標的型ランサムウェアの攻撃方法は多岐に渡り、以下のようなステップを経ることが一般的です。

（1）侵入
攻撃者はまず、様々な方法を駆使して標的とする組織のネットワーク内部への侵入を図ります。
主な侵入経路には、下記のような感染ルートがあります。

◇脆弱性を悪用しネットワークから感染させる
OS やアプリケーション等のソフトウェアの脆弱性対策が十分でない状態でインターネットに接続されている機器に対して、VPN 等の脆弱性を悪用し、インターネット経由で PC やサーバーをランサムウェアに感染させる。

◇公開サーバーに不正アクセスして感染させる
意図せず外部公開されているポート（リモートデスクトップポート等）に不正アクセスしたり、パスワード管理の不備を利用したりしてランサムウェアに感染させる。

◇メールから感染させる
組織の従業員等へのメールに添付したファイルや、本文中のリンクを開かせることでランサムウェアに感染させる。

◇Web サイトから感染させる
Web サイトの脆弱性等を悪用して、ランサムウェアをダウンロードさせるように改ざんした Web サイトや攻撃者が用意した Web サイトを閲覧させることでランサムウェアに感染させる。

（２）ネットワーク内部で情報収集する
侵入に成功した攻撃者は、続けてネットワーク内の端末を遠隔操作し、多数のアクセス権限の取得を試みます。これは、次のステップとなるデータの窃取やランサムウェア実行の際により大きな効果を得るための準備です。

（３）データの窃取
搾取した組織内の端末やシステムのアクセス権限を利用して、脅迫を行うための情報を収集します。それらの情報は、のちに情報暴露で組織を脅す材料として使われることもあります。奪われた情報は一か所に集められ、攻撃者の管理するサーバーに保管されます。

（４）ランサムウェアの実行・身代金要求
最後に、組織へのランサムウェアの展開と実行を行います。
その際、グループポリシー機能などを使ってランサムウェアを組織内ネットワークに展開し、実行します。ファイルを暗号化した後は、権限を奪取した端末に身代金要求画面を表示させることで脅迫を行います。

ここまでランサムウェアの種類や攻撃方法について考察してきましたが、いかがだったでしょうか。次回は、被害の実例と対策・対応について解説する予定です。

IPA では「ランサムウェア対策特設ページ」を公開しています。

このページでは、ランサムウェアの感染防止や被害低減のために役立つ情報が公開されています。

また、IPA や他機関のランサムウェア関連セキュリティ情報へのリンクも紹介しているので、ぜひ参考にしてください。

ランサムウェアは今も進化をし続けています。適切なセキュリティ情報の入手と、組織全体が正しいランサムウェアの知識を共有する事が発生防止には不可欠といえるでしょう。

４．最後に

東京都では、「令和 7 年度中小企業サイバーセキュリティ基本対策事業」として本記事で取り上げたランサムウェア対策に有効な、セキュリティ機器・ソフトの無償体験（3 か月程度）や、企業のセキュリティ環境を調査し、今後の対策に向けて指導・助言する情報セキュリティマネジメント指導支援を行っています。

令和 7 年度中小企業サイバーセキュリティ基本対策事業

2025 年 9 月 19 日時点まだ定員に達していませんので、お早めにお申し込みください。なお、お申込みいただいた時点で定員に達している可能性もございます。詳しくは上記サイトをご確認願います。

※本記事は令和 6 年度中小企業サイバーセキュリティ対策事業で制作された記事を最新情報等で更新したものです。

配信予定日：2025 年 9 月 26 日（金）14:00 頃
カテゴリ：中小企業サイバーセキュリティ対策事業の知見
タグ：＃知識編＃実践力強化プログラム
過去記事焼き直し：しない（新規記事です）
記事 URL（新設します）：https://cybersecurity-taisaku.metro.tokyo.lg.jp/know_more/cyber-taisakutiken3/

セキュリティのブートキャンプ！限界突破して得られたものは？

目次

本記事では東京都が独自に調査した情報を発信いたします。
今回は令和 6 年度中小企業サイバーセキュリティ社内体制整備事業（後継の令和 7 年度事業が“実践力強化プログラム”という名称のため、以降、同じ名称で統一します）からの情報を発信します。

●突如決まったブートキャンプへの参加
※ここからは、ドラマ風に記事を書かせていただきます。
文章内の登場人物、会社等はすべてフィクションです。
記事内の企業・担当者は実在しておりません。

建設会社勤務の山崎さんはある日、社長に呼び出された。

社長：「山崎さん、これに申し込んで参加して欲しい。」

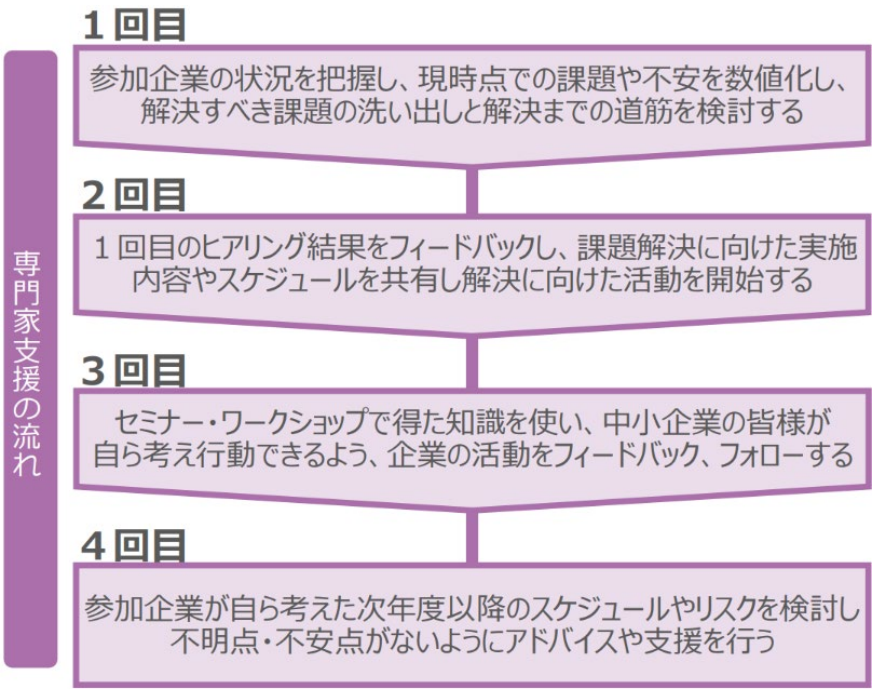
突如社長から言われたのは「令和 6 年度東京都中小企業サイバーセキュリティ実践力強化プログラム」への参加だった。
当社は大手建設会社から発注を受け大規模商業施設等の内装を手掛ける建設会社。
取引先からのセキュリティ対策要請が強まっている事を考慮し、参加を決断した。

説明会に参加して、その内容に驚愕した。
セミナー・ワークショップへ１０回参加しながら、セキュリティの専門家との課題解決に向けた打ち合わせを４回開催。
それを約半年でやりきる。まるでブートキャンプだ。
正直なところ内容を聞いて震えが出てきた。

＜セミナー・ワークショップ１０回の内容＞

日程		会場	セミナー（13時00分～15時00分）	ワークショップ（15時15分～17時30分）
1	7月23日	新宿	サイバーセキュリティを取り巻く背景 中小企業に求められるデジタル化の推進とサイバーセキュリティ対策	自社のIT活用とセキュリティ事情の検討
2	8月6日		これからの企業経営で必要なIT活用とサイバーセキュリティ対策 セキュリティ事象に対応して組織として策定すべき対策基準と具体的な実施 各種ガイドラインを参考にした対策の実施	インシデント事例を活用した対策基準の検討
3	8月20日		ISMSなどのフレームワークの種類と活用法の紹介	情報資産管理台帳作成およびリスクアセスメント（机上演習）
4	9月10日		ISMSの構築と対策基準の策定と実施手順	対策基準の作成（机上演習）
5	9月24日			実施手順の策定（机上演習）
6	10月8日		具体的な構築・運用の実践	実施手順に沿った具体的な対策の検討（机上演習）
7	10月22日			
8	11月19日		組織として実践するためのスキル・知識と人材育成	人材確保の検討
9	12月17日			
10	1月21日		全体総括	振り返りおよび経営者に対する説明事項の検討

＜専門家支援の内容（１回２時間程度の打ち合わせ）＞



確かに、半年で１４回も対応するのは現業をやり切れるか不安がある。しかし、これだけ緻密に計画されたプログラムに参加すれば、確実に成果が出ると胸が高ぶった。

●実践力強化プログラムとは？

実践力強化プログラムは、中小企業がサイバーセキュリティ対策を継続的に実施していくため、社内にサイバーセキュリティ対策の中核的人材を育成することを目的としている。

セミナー・ワークショップを１０回行う中で、最新のサイバー脅威への対処法等を学びながら、他企業との課題解決や事例共有等グループディスカッションを行い、サイバーセキュリティの知見を深めていく。

また、個社に特化した課題解決のため、上記と並行して情報セキュリティの専門家から４回の訪問コンサルを受ける。

東京都の公費負担の事業であり、参加企業側に金銭的な負担は無い。

当社の情報セキュリティ対策は、私が偶然 IT に詳しかった事もあり、基本的なルールの策定や UTM／EDR と言った対策は行ってきた。

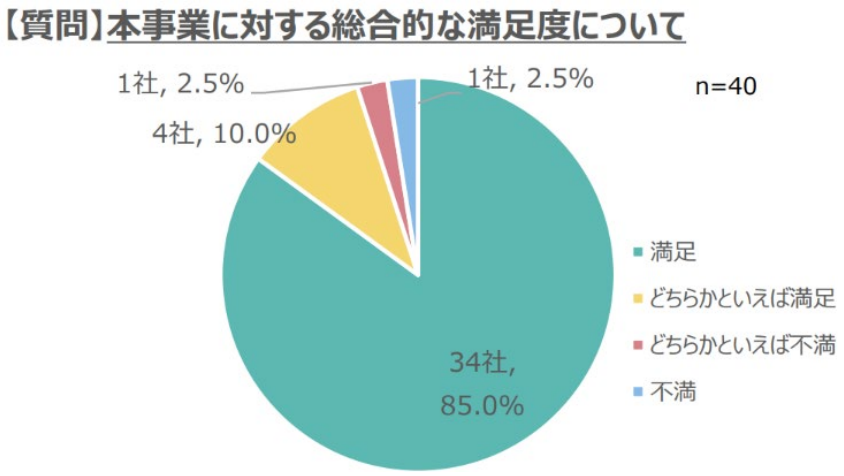
しかし、我流で学んで実施してきたセキュリティ対策には不安があり、正直これ以降何をやればいいのか分からなかった。このような状況も社長は見ており、取引先の要請や、金銭的な負担が無い事が後押しとなり、参加に至った。

※補足：
東京都では、実践力強化プログラムを、基本的なルールの策定や、UTM／EDR 等の導入をしている企業の次の段階として必要な事項と位置付けています。詳しくは以下の記事をご覧ください。
東京都サイバーセキュリティ対策事業の成り立ちと今後について

●限界突破して得られたもの

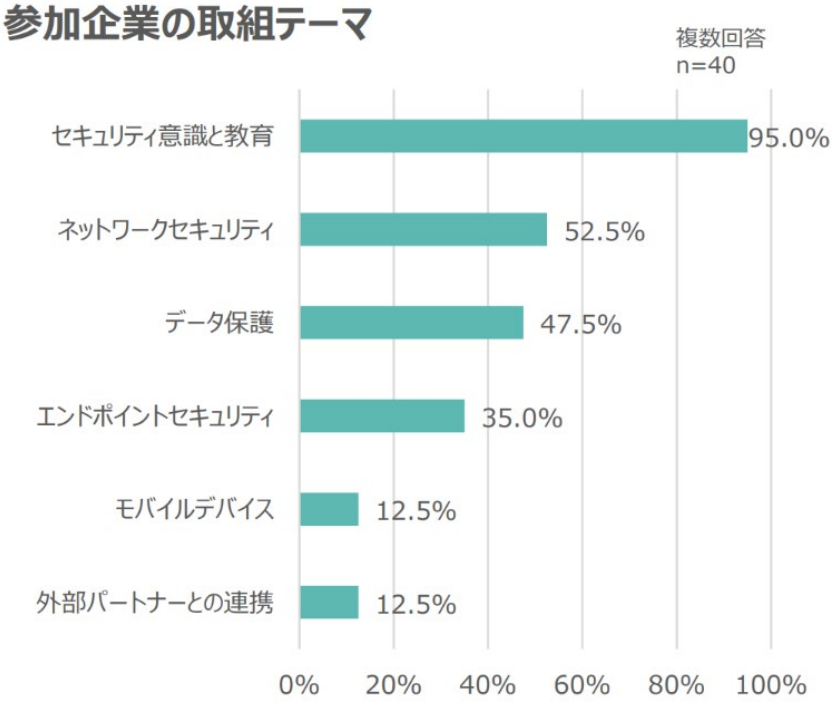
約半年間、１４回の対応が終了した。
課題解決の実施に向け、社長含めた幹部との合意形成も行ったため、自身で表現した「ブートキャンプ」のイメージ通りのキツさだった。しかし、確実な達成感は得られた。

＜参考：令和６年度事業参加企業へのアンケート結果①＞



⇒　95%が満足という結果に。

＜参考：令和６年度事業参加企業へのアンケート結果③＞



⇒セキュリティ意識と教育が最も多かった。

４回の専門家派遣を通じ、当社では以下を行う事とした。
・社員全員、年１回の情報セキュリティ研修を受講する。
・建設現場では、週１回以上朝礼においてセキュリティの注意事項を取り扱う。
・インシデントが発生した際の対応方法を明確に定める。
３点目については、社員教育を進めるもののインシデント発生のゼロ化は困難であるため、実施するに至った。インシデント対応は、東京都事業で支援を受ける事ができるため、来年度はその事業に参加したいと社長へ上申を行った。

※参考：インシデント対応に対する支援
令和７年度東京都中小企業サイバーセキュリティインシデント対応強化
既に定員に達しております、来年度以降も実施されるかは検討中です。

情報セキュリティ対策について漠然とした不安を抱いていたものの、本事業に参加する事で課題が明確になり、今後の取り組みを定める事ができた。現業があるなか、時間の確保等で苦しい状況もあったが、参加して本当に良かったと思う。

●今後の展望

※ここからはドラマ風ではなく、通常の記事の書き方に戻ります。

いかがでしたでしょうか、実践力強化プログラムは参加者目線で書いたほうが内容や効果が伝わると思い、ドラマ風に記事を書かせていただきました。

なお、今年度も実践力強化プログラム事業は行われています。
令和７年度東京都中小企業サイバーセキュリティ実践力強化プログラム
既に定員に達しております、来年度以降も実施されるかは検討中です。

今回は、昨年度の実践力強化プログラム事業で得られた知見を記事にしました。次回以降も、他の事業（インシデント対応強化等）を題材に、得られた知見を記事にさせていただきます。東京都事業は具体的な対策や、専門家派遣を毎年数百社以上に行っています。東京都では支援を通じて得られた知見、見えてきた傾向から日本の中小企業をサイバー攻撃から守る術を提供していきたいと考えております。皆様からのご意見・ご感想は本ウェブサイトの下部に記載のあるお問い合わせ先へ是非お寄せください。

配信予定日：2025 年 9 月 24 日(金) 14:00 頃
カテゴリ：基礎から学ぶ！ セキュリティ
タグ：＃初級編 ＃基本対策事業 ＃用語編 ＃知識編
過去記事焼き直し：する（過去記事を上書きします）
過去記事：https://cybersecurity-taisaku.metro.tokyo.lg.jp/basics/kisokaramanabu8/

【令和 7 年度版】中小企業におけるセキュリティ脅威への対策強化 ～ランサムウェアによる攻撃事例から対策を学ぶ（2/2）～

目次

独立行政法人情報処理推進機構(IPA)が毎年発行している「情報セキュリティ 10 大脅威 2025」から、中小企業の経営者やシステム担当者が注目すべき点を掘り下げていきます。

今回も1位に挙げられている「ランサムウェアによる攻撃」に焦点を当てます。
2回目の今回は、ランサムウェアの被害の実例と対策・対応について解説いたします。

※前回の情報はこちら：中小企業におけるセキュリティ脅威への対策強化～ランサムウェアによる攻撃事例から対策を学ぶ～(1/2)

1. ランサムウェアによる被害の実例

(1)ランサムウェア感染による被害と二次被害

2024 年 6 月、サービス業の K 社はランサムウェア攻撃を含む大規模なサイバー攻撃を受けたと公表しました。複数のサービスが停止したほか、同年 8 月の調査で、約 25 万 4,000 人分の個人情報や企業情報の漏えいが判明しました。フィッシング攻撃等により従業員のアカウント情報が窃取され、社内ネットワークに侵入されたことが原因と推測されています。 また、本事例では、攻撃組織が公開したとされる 情報が SNS 等を通じて拡散されました。この二次被害に対しては、対策チームによる投稿の削除要請および情報開示請求等が行われ、悪質な拡散行為へは刑事訴訟等の準備が進められています。

(2)ノーウェアランサムによる攻撃事例

2024 年 10 月、J 機構は、機構内のセンターがデータ窃取の脅迫を受けたと公表しました。

犯行声明 は国際ハッカー集団「CyberVolk」からで、 搾取データの 5%を公開し、1 万ドルを支払わなければ残りの 95%も公開すると SNS 上で脅迫を受けました。なお、調査によってシステムへの不正侵入やデータ 消失等は確認されず、窃取したとされるデータも公開データでした。

(3)RaaS が利用された国内事例

2024 年 6 月、情報処理業の H 社がランサムウェア攻撃を受けたことを公表しました。攻撃者はサーバーの脆弱性および VPN ルーターの設定不備を悪用して社内ネットワークに侵入し、複数のサーバーに対してデータの暗号化を行いました。10 万件以上の個人情報漏えいの可能性があったが、同年 8 月時点では外部への流出や二次被害は確認されていません。 また、本事例では、RaaS の一種である「Phobos」 を用いた攻撃だったことも確認されています。

2. ランサムウェアの対策と対応

ランサムウェアの対策と対応には、組織的な対応(経営者層/システム管理者/従業員)が必要です。それぞれの組織が役割を分担し合い、かつ総括的に対策や対応をシームレスに行う必要があります。

※印は下記「共通対策」の詳細を参照してください。

(1)経営者層

経営者層では以下の対策と対応が必要となります。

◇組織としての対策・対応体制の確立

・インシデント対応体制を整備し、実際のインシデント時に対応する※

(2)システム管理者や従業員

◇被害の予防対策

・インシデント対応体制を整備し、実際のインシデント時に対応する※

・IPA の「情報セキュリティ 10 大脅威 2025 解説書[組織編]」の 9 ページ、表 1.3「情報セキュリティ対策の基本」を実施する

表 1.3 情報セキュリティ対策の基本

攻撃の糸口	情報セキュリティ対策の基本	目的
ソフトウェアの脆弱性	ソフトウェアの更新	脆弱性を解消して脆弱性を悪用した攻撃によるリスクを低減する
マルウェアに感染	セキュリティソフトの利用	攻撃を検知してブロックする
パスワード窃取	パスワードの管理・認証の強化 ※「認証を適切に運用する」で詳細を解説	パスワード窃取による情報漏えい等のリスクを低減する
設定不備	設定の見直し	誤った設定を悪用した攻撃をされないようにする
誘導（罠にはめる）	脅威・手口を知る	手口から重視すべき対策を理解する

・メールの添付ファイル開封や、メールや SMS のリンク、URL のクリックを安易にしない※
・多要素認証の設定を有効にする
・提供元が不明なソフトウェアを実行しない
・サーバーやクライアント、ネットワークに適切なセキュリティ対策を行う※
・共有サーバー等へのアクセス権の最小化と管理の強化を行う
・公開サーバーへの不正アクセス対策を行う
・適切なバックアップ運用※

◇被害を受けた後の対応
・適切な報告／連絡／相談を行う※
・適切なバックアップ運用を行う※
・復号ツールを活用し、復号化を行う
・インシデント対応体制を整備し、実際のインシデント時に対応する※

（3）身代金の支払いと復旧業者の選定
ランサムウェア被害を受けた場合、原則、身代金は支払わずに復旧を行います。
何故ならば、身代金を支払ってもデータの復元や情報の流出を防げるとは限らないからです。
また、対応を依頼した業者が攻撃者との裏取引で身代金を支払うことでデータ復旧した場合、事実上、自組織が攻撃者に資金提供をしたとみなされるおそれもあります。このため、対応を依頼する業者の選定にも注意が必要です。

※「共通対策」
IPA「情報セキュリティ 10 大脅威 2025 解説書［組織編］」の 37 ページ、表 1.5「複数の脅威に有効な対策集」より

表 1.5 複数の脅威に有効な対策

対策	対象	
	個人	組織
認証を適切に運用する	○	○
情報リテラシー、モラルを向上させる	○	○
添付ファイルの開封やリンク・URL のクリックを安易にしない	○	○
適切な報告／連絡／相談を行う	○	○
インシデント対応体制を整備し対応する	−	○
サーバーや PC、ネットワークに適切なセキュリティ対策を行う	○	○
適切なバックアップ運用を行う	○	○

① 認証の適切な運用

推測可能なパスワードの設定や不適切な管理をすると、攻撃者に不正ログインされやすくなってしまいます。そのためには適切な設定や運用が必要となります。

② 情報リテラシー、モラルを向上

故意に不正をはたらくことは論外ですが、中には意図せず情報モラルに反することを行ったり、組織のためによかれと考えて規則に反してしまう場合もあります。
どのような場合にも自身の行為には責任が伴う事を認識する必要があります。

③ 添付ファイル開封、リンクや URL の安易なクリックの抑止

様々なサービスからの連絡がメールで行われたり、SMS からのお知らせを受け取ることがあります。しかし、本物を騙った偽の連絡であると、それに起因として個人情報を盗まれたり、金銭被害に繋がったりするおそれがあります。

④ 適切な報告／連絡／相談

◇【システム管理者や従業員】

被害を受けたときは適切な人や機関への相談が必要です。不安に感じたときや被害に遭ったときは慌てず、まずは落ち着いて、対応する事が望ましいと言えます。

◇【組織】
組織内で適切な報告や連絡が無いと被害の拡大だけでなく、外部からは隠蔽とみなされ、さらなる信頼の失墜につながります。経営者や上司、責任者は部下や担当者が包み隠さず躊躇なくエスカレーションできる風土や関係性を築くことも重要です。

⑤ インシデント対応体制を整備し対応する
セキュリティインシデントが発生した際、誰がどのように、何から行えばよいのか？これを理解して、あらかじめ対応する仕組みを整えているのといないのとでは、同じ事象の問題が起きたとしても受ける被害の大きさは全く異なります。適切な体制構築が必要です。

⑥ サーバーやクライアント、ネットワークに適切なセキュリティ対策を行う
脅威はサーバーやクライアント、ネットワークに関連したものが多いのが特徴です。ただし、組織としてのポリシーの制定や要員確保、事前検証、手順の確立、そしてそれを維持し続ける予算の確保と仕組みが必要であり、検討事項が多い事も特徴と言えます。

⑦ 適切なバックアップ運用
データの破損の原因は、記憶装置の故障やランサムウェア等のサイバー攻撃だけではなく、運用時の操作ミスによる消去や誤った更新と、多岐に渡ります。データ復旧には人手と時間を要しますが、適切なバックアップを取得しておくことで、この被害を軽減することが可能です。

IPA の「情報セキュリティ10大脅威 2025」の 36 ページから始まる「共通対策」ではさらに詳しい具体的な対応をご紹介しています。こちらもご参照ください。

ここまでランサムウェアの攻撃事例や対策・対処について考察してきましたが、いかがだったでしょうか。
前回の繰り返しですが、IPA では「ランサムウェア対策特設ページ」を公開しています。
このページでは、ランサムウェアの感染防止や被害低減のために役立つ情報が公開されています。

また、IPA や他機関のランサムウェア関連セキュリティ情報へのリンクも紹介しているので、ぜひ参考にしてください。
ランサムウェアは今も進化をし続けています。
正しいランサムウェアの知識を共有し、事前にできる対策をできるだけ打つことによって、ランサムウェアの発生を防止する事が可能となり、組織として重要な情報や業務継続性を保証することができます。

3. 最後に

東京都ではセキュリティ対策をこれから始めたい企業や事業継続に向けたさらなる強化を図りたい企業向けに、セキュリティ専門家による各種の支援を行っています。すでに募集を締め切っている支援もありますが、下記支援はまだ参加者募集中です。ぜひご確認ください。

基本対策事業 URL：https://kihontaisaku.metro.tokyo.lg.jp/

※本記事は令和 6 年度中小企業サイバーセキュリティ対策事業で制作された記事を最新情報等で更新したものです。

配信予定日：2025 年 10 月 3 日(金) 14:00 頃
カテゴリ：もっと知りたい！セキュリティ
タグ：＃知識編
過去記事焼き直し：しない（新規記事です）
記事 URL（新設します）：https://cybersecurity-taisaku.metro.tokyo.lg.jp/know_more/secure-by-design2/

セキュリティ・バイ・デザイン概説 2

目次

中小企業の経営者や情報システム担当者の皆さん、日々のセキュリティ対策、お疲れ様です。前回に続き、本記事では、情報システムに対して、確実かつ効率的にセキュリティを確保するため、システム開発の企画段階から対策を実装する「セキュリティ・バイ・デザイン」について解説します。

●セキュリティ・バイ・デザインの工程概要
前回解説したように、セキュリティ・バイ・デザインは、デジタル庁のガイドラインによれば、「情報システムの企画工程から設計工程、開発工程、運用工程まで含めた全てのシステムライフサイクルにおいて、一貫したセキュリティを確保する方策のこと」と定義されています。また、同ガイドラインは、デジタル庁「デジタル・ガバメント推進標準ガイドライン」のセキュリティ編と位置付けています。そのため、「デジタル・ガバメント推進標準ガイドライン」のシステム開発・運用工程におけるセキュリティ・バイ・デザインの工程と概要を次に示します。

#	システム開発・運用工程	セキュリティ・バイ・デザイン工程	概要
1	サービス・業務企画	セキュリティリスク分析	・想定脅威にかかるセキュリティリスク分析の実施 ・セキュリティ対応方針の決定

2	要件定義	セキュリティ要件定義	・機能面、非機能面でのセキュリティ要件の定義
3	調達	セキュア調達	・セキュリティ調達仕様の策定、責任範囲の明確化 ・安全な委託先、安全な プロダクトの選定
4	設計・開発	セキュリティ設計	・機能面と非機能面でのセキュリティ設計 ・セキュリティ運用設計
5		セキュリティ実装	・セキュリティ機能の実装 ・アプリケーションのセキュアコーディング ・プラットフォームのセキュリティ設定の実施（堅牢化、要塞化）
6		セキュリティテスト	・セキュリティ機能のテスト ・脆弱性診断
7	サービス・業務の運営と改善	セキュリティ運用準備	・セキュリティ運用体制の確立 ・セキュリティ運用手順の整備
8	運用及び保守	セキュリティ運用	・平時のセキュリティ運用 ・有事のセキュリティ運用

セキュリティ・バイ・デザインの実施工程と概要
「政府情報システムにおけるセキュリティ・バイ・デザインガイドライン」より
(https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/7e3e30b9/20240131_resources_standard_guidelines_guidelines_01.pdf)

これ以降は、セキュリティ・バイ・デザインの各工程において求められること（要求事項)、実施内容、セキュリティ対策の考え方について見ていきましょう。

●セキュリティリスク分析工程における要求事項及び実施内容
セキュリティ・バイ・デザインの最初の工程はセキュリティリスク分析です。

この工程における要求事項は次の通りです。

・システムにおけるセキュリティ脅威が特定されていること
・当該脅威にかかる発生可能性、システムへの影響度を踏まえて、リスク分析が実施されていること
・リスク分析結果に基づき、セキュリティ対応方針を検討し、リスク対応優先度や遵守すべきセキュリティ標準（セキュリティ　ベースライン）対応リソース等を決定していること

一般的に、システム開発の初期段階でリスク分析を行われているケースは少ないと思われますが、セキュリティ・バイ・デザインでは、要件定義の前段階であるサービス・業務企画段階でリスク分析を行うことを求めています。

また、上記の要求事項を踏まえた実施内容としては次の事項が挙げられています。

・システムで取扱う重要情報、アクター、実施業務、他システムとの連携方法等、システムで取扱う重要情報のフローやライフサイクルが分かる内容を記載したシステムプロファイルの作成
・システムプロファイルに基づくセキュリティ脅威の特定
・セキュリティ脅威の発生可能性、システムへの影響度を踏まえたリスク分析の実施
・リスク分析結果を踏まえたセキュリティ対応方針の決定（リスク対応優先度、遵守すべきセキュリティ標準、検証方法、対応リソース等）

なお、セキュリティリスク分析において活用できるフレームワークとして、EBIOS（Expression of Needs and Identification of Security Objectives）があります。EBIOS は、フランスの国家情報システムセキュリティ庁（ANSSI）が提唱するリスク分析手法であり、次の 5 つの Workshop で構成されています。

Workshop1：スコープとセキュリティベースライン（Scope and security baseline）
Workshop2：脅威の特定（Risk Origins）
Workshop3：戦略的シナリオ（Strategic Scenarios）
Workshop4：攻撃手順シナリオ（Operating Scenarios）
Workshop5：リスクへの対策（Risk Treatment）

●セキュリティリスク分析工程におけるセキュリティ対策の考え方
システム開発においては、システムの特性や重要度に応じた適切なセキュリティ対応方針が示されていないことから、セキュリティ対策が不十分であったり、場合によっては過剰なセキュリティ対策が実施されたりすることもあります。
そうした状況に陥るのを防ぎ、適切なレベルのセキュリティ対策を実施するため、対象となるシステムにおいて想定される脅威とその発生可能性、システムへの影響度等を踏まえ、リスク分析を実施します。
その結果から、システムの特性や重要度等に見合った適切なセキュリティ対応方針を検討し、想定されるセキュリティ脅威に伴うリスクへの対策や遵守すべきセキュリティ標準（ベースライン）等を決定します。また、開発工程や運用工程における第三者によるチェックやレビュー（脆弱性診断、セキュリティレビュー等）の実施方針、そのために必要となるリソース等についても検討・決定します。

●セキュリティ要件定義工程における要求事項及び実施内容
セキュリティリスク分析工程に続くのがセキュリティ要件定義工程です。

この工程における要求事項は、セキュリティリスク分析結果、セキュリティ対応方針に従い、システムで満たすべきセキュリティの状態が定義されていることです。
その実施内容として、①システムに実装する要件、②アプリケーション開発におけるセキュリティ要件、③セキュリティ管理における要件の項目例を挙げます。

①　システムに実装する要件
システムに実装するセキュリティ要件としては、次のようなものがあり、これらについて、システム基盤（ネットワーク、ハードウェア、OS、ミドルウェア等）において実装する要件と、アプリケーションに実装する要件を明確にする必要があります。

・識別及び認証
・アクセス制御
・データ保護（暗号化等）
・セキュリティ監視
・マルウェア対策

・サービス妨害攻撃対策

② アプリケーション開発におけるセキュリティ要件
アプリケーション開発におけるセキュリティ要件としては、次のようなものがあります。

・アプリケーションの特性、使用言語等に応じたセキュリティ要件（対処が必要な脆弱性等）
・セキュリティテスト方式に関する要件
・開発環境におけるセキュリティ対策要件（本番環境との隔離、アクセス制御、ライブラリ管理等）

③ セキュリティ管理における要件
セキュリティ管理におけるセキュリティ要件としては、次のようなものがあります。

・アイデンティティ管理（ID 管理）
・パッチ管理
・パフォーマンス管理
・構成管理
・変更管理
・ログ管理
・インシデント管理
・問題管理
・鍵管理

●セキュリティ要件定義工程におけるセキュリティ対策の考え方
サイバー攻撃が行われる前提で、多層のセキュリティ対策を実施し、仮に一つのセキュリティ対策が突破されたとしても、別のセキュリティ対策により被害を極小化することを目的とした考え方（多層防御）に基づいて、セキュリティ要件を定義することが重要です。
OS やミドルウェア、ネットワーク、アプリケーションの各コンポーネント等においては、多層のセキュリティ対策を実施することにより、攻撃者にとって攻撃コストの高いシステムを実現することが有効です。
また、攻撃や事故の発生自体を防止する防御に類するセキュリティ対策に偏らず、インシデントやその兆候を速やかに検知し、その後のインシデント対応、サービス復旧のための対策も含め、多層的にセキュリティ対策を実装することが求められます。

今回はセキュリティ・バイ・デザインの実施工程概要と、セキュリティリスク分析工程、セ

キュリティ要件定義工程における要求事項、実施内容、セキュリティ対策の考え方等について解説しました。次回以降も同様に、セキュリティリスク分析、セキュリティ要件定義に続く各工程について順次解説します。

●参考情報

デジタル・ガバメント推進標準ガイドライン
(https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/d4e68a9b/20250619_resources_standard_guidelines_guideline_01.pdf)

セキュリティ・バイ・デザイン導入指南書
(https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2022/ngi93u0000002kef-att/000100451.pdf)

配信予定日：2025 年 10 月 3 日（金）14:00 頃
カテゴリ：中小企業サイバーセキュリティ対策事業の知見
タグ：＃知識編＃インシデント対応強化
過去記事焼き直し：しない（新規記事です）
記事 URL（新設します）：https://cybersecurity-taisaku.metro.tokyo.lg.jp/know_more/cyber-taisakutiken4/

意味あるの？インシデント対応強化の効果

目次

本記事では東京都が独自に調査した情報を発信いたします。
今回は令和 6 年度中小企業サイバーセキュリティ特別支援事業（後継の令和 7 年度事業が“インシデント対応強化”という名称のため、以降、同じ名称で統一します）からの情報を発信します。

●インシデント対応強化の目標

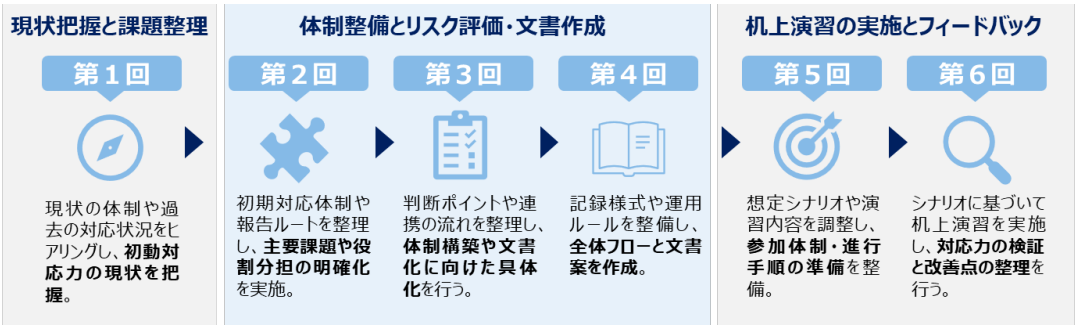
「不審なメールの添付を開いてから、パソコンがおかしくなった。」
様々な状況からスタートするセキュリティの事故（インシデント）対応。初動が遅れると大変なことになることは、過去の記事で紹介しています。
＜過去の記事＞
【令和 7 年度版】セキュリティインシデント対応
上記記事では具体的な対処策も示していますが、東京都ではインシデント対応強化という支援を行っています。

２つのコースから選択可能です。インシデント対応方法を“ヒト”を主軸に整理する“CSIRT 構築コース”と、システム等の“モノ”を主軸に整理する“IT-BCP 策定コース”があり、それぞれ以下を目標としています。

支援コース	達成目標

CSIRT 構築コース	インシデント発生時に備えて、準備から初動対応までの一連の対応を行う組織（機能）を構築することを目指す
IT-BCP 策定コース	インシデント発生時に、IT-BCP を発動し、業務再開から IT システムが復旧するまでの計画を策定することを目指す

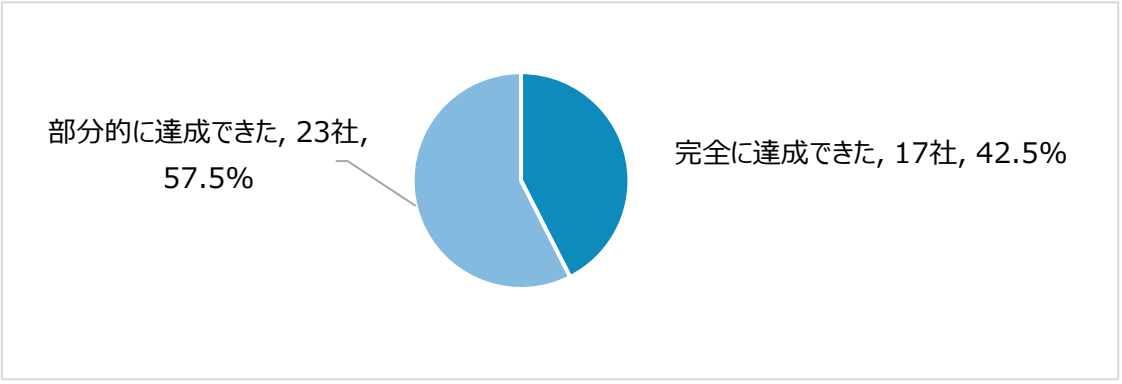
支援は、専門家が合計 6 回、参加企業に訪問して行います。各回の内容は以下です。



●目標は達成できるのか

令和 6 年度のインシデント対応強化に参加した企業（合計４０社）が具体的に目標を達成できたのか、参加後のアンケート結果を紹介していきます。

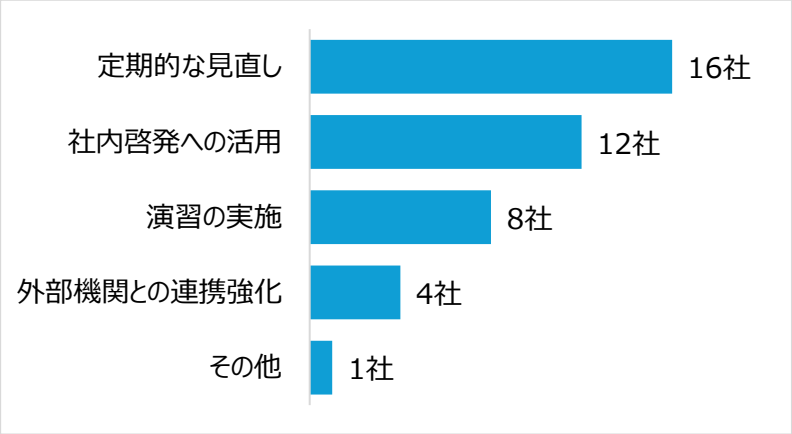
■目標達成状況



完全に達成できた企業が 42.5%、部分的に達成できた企業が 57.5%でした。達成による効果を測るため、もう一歩踏み込んで質問を行いました。

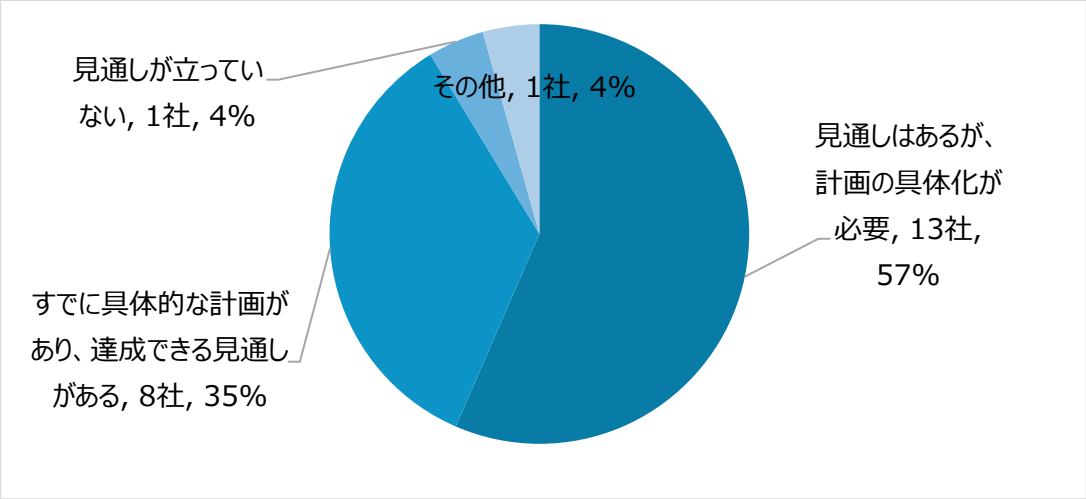
■作成した CSIRT もしくは IT-BCP を今後どのように運用していくか

※完全に達成できた 17 社に対し質問、複数回答可能



ほぼ全社の 16 社が定期的な見直しをしていくとの回答です。専門家支援以後、企業が自走し取り組むに至った点は、本事業の効果があったと考えられます。

■目標を達成する見通しはあるか
※部分的に達成できた 23 社に対し質問



「部分的に達成できた」と回答した 23 社のうち、ほぼ全社の 21 社が「目標を達成できる見通しがある」との回答でした。専門家支援中に完全に達成まで至らなかったのは悔やまれますが、見通しがあり、こちらも企業が自走し取り組むに至っている状況で、本事業の効果があったものと考えられます。

●今後の見通し
今年度もインシデント対応強化は行われています。
令和 7 年度東京都中小企業サイバーセキュリティインシデント対応強化
既に定員に達しております、来年度以降も実施されるかは検討中です。

今回は、昨年度のインシデント対応強化で得られた知見を記事にしました。次回以降も、他の事業（フォローアップ等）を題材に、得られた知見を記事にさせていただきます。東京都事業は具体的な対策や、専門家派遣を毎年数百社以上に行っています。東京都では支援を通じて得られた知見、見えてきた傾向から日本の中小企業をサイバー攻撃から守る術を提供していきたいと考えております。皆様からのご意見・ご感想は本ウェブサイトの下部に記載のあるお問い合わせ先へ是非お寄せください。

配信予定日：2025 年 10 月 3 日(金) 14:00 頃
カテゴリ：技術的セキュリティ対策（1/2）
タグ：＃実用編＃知識編＃技術的セキュリティ対策
過去記事焼き直し：する（過去記事を上書きします）
過去記事：https://cybersecurity-taisaku.metro.tokyo.lg.jp/know_more/mottosiritai9/

技術的セキュリティ対策（1/2）

目次

中小企業の経営者や情報システム担当者の皆さん、日々のセキュリティ対策、お疲れ様です。

セキュリティ対策に必要な考え方として、「組織・人的対策」「物理的対策」「技術的対策」という３つの分類があります。
「組織・人的対策」は、守秘義務契約などのセキュリティに対しての社内ルールを設定する対策です。ルールを設定するだけではなく、実現するための社内教育も重要となります。
「物理的対策」は、入退室・施錠管理や盗難・災害といった物理的要因に対する対策を指します。
そして「技術的対策」は、ハードウェア・ソフトウェアやネットワークなどの技術的な対策を行うことです。今回は、この技術的対策について解説します。

１．技術的対策の重要性

IT を活用するうえでセキュリティを向上するには組織・人的対策、物理的対策だけでは限界があり、環境に応じた技術的対策が必要です。
ところが技術的対策は一般の人には難解なため、おろそかになりがちです。これはサイバー攻撃者が効率的に成果を挙げるために都合がよく、その結果、サイバー攻撃による被害が後を絶ちません。

２．技術的対策例と活用

技術的対策のために必要な製品、ソフトウェア、サービスは様々なものが提供されています。

攻撃手法は日々多様化、複雑化しているため、技術的対策も随時、対策の見直しや更新を行い、最新の状態にしていくことが必要となります。
以下に代表的な技術的対策を挙げるので、自社の環境に合わせて導入を検討し、活用してください。

（1）ネットワーク脅威・端末対策

ネットワークの境界付近に配置して通信の処理や監視を行い、不正な通信の制御と管理を行うことで対策を実施します。

●ファイアウォール

通信をさせるかどうかを判断し、許可または拒否する技術です。
例えば、インターネットと社内 LAN との間に設置して、外部からの不正なアクセスが社内のネットワークに侵入するのを防ぎます。

●IDS（Intrusion Detection System：侵入検知システム）

システムやネットワークに対する不正なアクセスなどを検知して、管理者に通知する技術です。
例えば、インターネットとファイアウォールの間に設置することで、不正アクセスと思われる通信を検知して管理者に通知できます。

●IPS（Intrusion Prevention System：侵入防御システム）

システムやネットワークに対する不正なアクセスなどを検知して、自動的に遮断する技術です。
例えば、インターネットとファイアウォールの間に設置することで、不正アクセスと思われる通信を検知して管理者に通知するとともに、通信を遮断できます。

●UTM（Unified Threat Management：統合脅威管理）

ファイアウォールや IDS・IPS、メールフィルタリング、URL フィルタリングなど複数の異なるセキュリティ機能を一つのハードウェアに統合して、社内ネットワークとインターネットの脅威であるウイルスの侵入や不正アクセス、サイバー攻撃などを検知し、防御するツールです。
※UTM についてはこちらの記事で解説しています。「UTM」【3 分でわかる！用語解説＃ 3】

●EDR（Endpoint Detection and Response）

ネットワークに接続されたパソコンやサーバー、スマートフォンなどの端末機器に侵入したウイルスやランサムウェアなどのサイバー攻撃を検出し、管理者に通知する技術です。最

新の EDR 製品では、AI による異常検知や自動隔離機能が強化されており、テレワーク端末や BYOD（私物端末）にも対応可能なクラウド型 EDR の導入が推奨されています。
※EDR についてはこちらの記事で解説しています。「EDR」【3 分でわかる！用語解説＃２】

●WAF（Web Application Firewall）
ウェブアプリケーションの脆弱性を悪用した攻撃から、ウェブアプリケーションを保護する技術です。
例えば、ファイアウォールや IDS・IPS とウェブサーバーの間に設置することで、ウェブアプリケーションがやり取りするデータを監視して攻撃を検出できます。

●VPN（Virtual Private Network）
インターネットのような公衆ネットワーク上で、保護された仮想的な専用線環境を構築する技術です。
例えば、テレワーク勤務者が職場との間で機密性の高い電子データをやり取りする際に、VPN を利用することで暗号化による安全な通信が可能になります。
また、VPN に加え「ゼロトラスト」モデルの導入が推奨されています。VPN だけでは不十分な場合があるため、端末の状態やユーザーの認証情報をもとにアクセスを制御するゼロトラスト型の仕組みについてもご検討ください。
※VPN、ゼロトラストについてはこちらの記事で解説しています。「VPN とゼロトラスト」【3 分でわかる！用語解説＃４】

（２）コンテンツセキュリティ対策
プログラム実行や電子メール送受信、ウェブ閲覧などを、その内容（コンテンツ）によって制御することで対策を実施します。

●ウイルス対策
ウイルスを検知・駆除することで、ウイルスに感染するのを防ぐための対策です。
例えば、利用するパソコンにウイルス対策ソフトをインストールしてウイルス定義ファイルを最新の状態にすることで、既知のウイルスを検知できます。これに加え、ふるまい検知（未知のマルウェアを検出する技術）を備えた製品の導入が推奨されています。クラウド型のウイルス対策ソフトはテレワーク環境でも有効です。

●メールフィルタリング
メールの送受信を監視して、指定した条件によって特定の処理を実行する技術です。
例えば、メールサーバーにフィルタリング機能を設定することで、迷惑メールやウイルスが添付されたメールをブロックできます。

●URL フィルタリング

ウェブサイトへのアクセスや閲覧について、そのアドレスや内容が所定の条件に合致もしくは違反する場合に、アクセスの停止や警告などを行う技術です。

例えば、URL フィルタリング機能を持つ機器を導入することにより、業務に関係がないウェブサイトの閲覧を禁止し、不正サイトへアクセスしてしまうリスクを減らすことができます。

（3）アクセス管理

情報システムの利用者を、認可及び制限する機能を提供します。

●アクセス制御

利用者や情報機器がデータなどにアクセスすることができる権限や認可を制御する技術です。

例えば、業務で使用するクラウドサービスなどを事務所のみで利用可能とするアクセス制御を行うことで、事務所外からデータへの不正アクセスのリスクを軽減できます。

●多要素認証

サービス利用時に行う利用者認証を、3つの要素（（1）知っているもの、（2）持っているもの、（3）本人自身に関するもの）のうち、2つ以上の要素を用いて行う技術です。

例えば、スマートフォンアプリによるワンタイムパスワードや、生体認証などを組み合わせることで、より強固な認証が可能です。

●特権 ID 管理

情報システムの特権（コンピュータを管理するために与えられた最上位の権限）の利用申請や権限付与、操作ログなどを管理する技術で、アクセス権限の最小化を意識した管理が重要です。

例えば、サイバー攻撃や内部不正などによる、特権の不正利用を防止し、リスクを軽減することができます。

（4）システムセキュリティ管理

組織が保有する IT 資産について、一元的な管理や脆弱性を検出する機能を提供します。

●IT 資産管理

パソコンやサーバーなどのハードウェアやソフトウェアの保有状況・構成情報を取りまとめて管理する技術です。

例えば、クラウド型 IT 資産管理ツールを導入することで、社外の端末やテレワーク環境でもセキュリティパッチの適用状況を把握することができ、脆弱性に対する攻撃のリスクを軽減することができます。

●脆弱性検査

サーバーやアプリケーションに対してスキャニングを行い、脆弱性などがないか検査を行います。

例えば、サービス提供前のウェブアプリケーションに対して、脆弱性検査を行うことで、既知の脆弱性の有無を点検することができます。

脆弱性がある場合は、脆弱性があるサーバーやアプリケーションに対し、脆弱性修正パッチの適用や安全な設定などの対策を速やかに実施することで、攻撃のリスクを軽減することができます。

●ログ管理

サーバーなどに誰がログインしたか、どのデータに対してアクセスがあったかは、サーバー上にログファイルとして記録されます。

ログファイルの内容はサーバーなどの運用期間に応じて増えていくので、一定期間（例えば１週間、3 か月、1 年などの期間）で自動的に削除されるように設定されているのが一般的です。

サイバー攻撃があった場合、このログファイルに書かれている内容をもとに、情報漏えいが生じたかどうかを分析するので、ログファイルをどのように管理するかの方針を、組織として定めておくことは重要です。

一方で、ログファイルの内容を十分に理解するには専門的な知識が必要となるため、こうした管理を容易にするためのツール類も提供されています。

なお、本稿は、独立行政法人情報処理推進機構（IPA）が公表している「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」を参考に解説しています。

次回は、データの暗号化、安全消去に関する技術的対策について解説します。

※本記事は令和 6 年度中小企業サイバーセキュリティ対策事業で制作された記事を最新情報等で更新したものです。

配信予定日：2025 年 10 月 10 日(金) 14:00 頃
カテゴリ：もっと知りたい！セキュリティ
タグ：＃知識編
過去記事焼き直し：しない（新規記事です）
記事 URL（新設します）：https://cybersecurity-taisaku.metro.tokyo.lg.jp/know_more/secure-by-design3/

セキュリティ・バイ・デザイン概説 3

目次

中小企業の経営者や情報システム担当者の皆さん、日々のセキュリティ対策、お疲れ様です。本記事では、前回に続き、セキュリティ・バイ・デザインのセキュア調達工程、セキュリティ設計工程における要求事項、実施内容、セキュリティ対策の考え方等について解説します。

●セキュア調達工程における要求事項及び実施内容
セキュリティ要件定義工程に続くのがセキュア調達工程です。

この工程における要求事項は次の通りです。

・委託先とのセキュリティ対応の責任範囲を明確にした上で、必要なシステムにおけるセキュリティ要件やサプライチェーンリスク対策を含めた網羅的なセキュリティ仕様を策定していること
・クラウドサービスを利用する際はサービス形態（SaaS、IaaS、PaaS 等）を踏まえて責任範囲を特定し、責任共有モデルに基づく義務を果たす能力と内部統制について透明性の高いサービスを選定すること
・システムのセキュリティ仕様を実装できる能力を有し、求めるセキュリティ管理基準を満たし、セキュリティリテラシーおよび意識が高い、安全な委託先が選定されていること

・システムで利用する機器、ミドルウェア、ライブラリ等については、それら自身がセキュリティ・バイ・デザインやセキュリティ・バイ・デフォルト等の安全な開発手法を取り入れており、不正侵入の経路となるバックドア等が含まれていない、サービス提供期間中継続的なサポートを受けられる安全なものを選定すること

今日多くの企業において、システム開発・運用業務を外部に委託したり、一部の業務でクラウドサービス等を利用したりしていることでしょう。その際に、セキュリティを十分考慮した調達が行われていないと、委託先の対策不備やクラウドサービスの設定不備に起因する情報漏洩等のセキュリティインシデントが発生するリスクが高まります。この工程は、そうしたリスクを低減する上で大変重要です。
なお、セキュリティ・バイ・デフォルトとは、セキュリティ機能や設定を最初から（デフォルトで）ソフトウェアやハードウェアに組み込んだ状態にすべきである、という原則です。

そして、上記の要求事項を踏まえた実施内容として次の事項が挙げられています。

・セキュリティ要件に基づいて、調達仕様におけるセキュリティ仕様策定
・セキュリティ仕様に関する、委託先との責任範囲の明確化
・委託先に求めるセキュリティ管理基準の策定
・セキュリティ仕様を満たす能力を有した安全な委託先の選定
・不正侵入の経路となるバックドア等が含まれていない、継続的なサポートを受けられる安全なプロダクトの選定

●セキュア調達工程におけるセキュリティ対策の考え方
委託先の能力不足や管理不足が原因によるセキュリティインシデントが多発していることから、システムのセキュリティ要件に基づくセキュリティ仕様を策定した上で、当該仕様を実装可能な、十分な能力を有した委託先を選定します。もちろん選定するだけでなく、委託先に求める具体的なセキュリティ管理基準等を策定し、委託先を管理、監督することも必要です。
また、導入したソフトウェアや機器の脆弱性が原因によるセキュリティインシデントも多発していることから、製品調達においてもセキュリティを十分考慮する必要があります。

●セキュリティ設計工程における要求事項及び実施内容
セキュア調達工程に続くのがセキュリティ設計工程です。

この工程における要求事項は次の通りです。

・セキュリティ要件を満たすように実装方針を具体化し、システムにおける機能面と非機能面でのセキュリティ設計が実施されていること
・堅牢化（攻撃対象領域が少なく、多層多重で守られている）されていること
・サイバーレジリエントな設計が実施されていること
・サービスデザインの観点から、システムの利用者や運用者等による人的ミスを引き起こす可能性が十分に低減された仕様になっていること

これらの要求事項を踏まえた実施内容として次の事項が挙げられています。

・アプリケーションセキュリティ
・OS セキュリティ
・ミドルウェアセキュリティ
・ネットワークセキュリティ
・クラウドセキュリティ
・物理セキュリティ
・セキュリティ運用（平時、有事）

●セキュリティ設計工程におけるセキュリティ対策の考え方

① 攻撃対象領域の管理及び防御
セキュリティ設計においては、攻撃対象となる領域（Attack Surface）を極力減らす設計を行い、防御することが重要です。そのため、ASM（Attack Surface Management）を導入してシステムにおける攻撃対象領域を把握するとともに、脆弱性管理（情報収集、対処要否の判断、迅速なパッチ適用等の対処等）を行います。また、攻撃者による脆弱性や設定ミスの悪用を防止するため、システムにおいて不要な機能やサービスは無効化し、セキュリティに関する設定を強化します。

② 管理者アカウントの保護
権限管理に起因するインシデント被害を極小化するため、発行するアカウントに対して過剰なアクセス権限は付与しないようにすることが重要です。特に管理者アカウントが悪用

された場合には被害が大きくなるため、利用者を必要最小限とし、システムへのアクセスにおいては多要素認証等を用いて十分に保護します。また、管理者アカウントの利用者を特定可能な仕組みを導入し、追跡可能な状態にします。

③ サイバーレジリエンスを高める設計の実施

サイバー攻撃がますます大規模化、高度化するなか、インシデントが発生する前提に立ち、防御力だけでなく、回復力（サイバーレジリエンス）を高める設計が重要です。システムアーキテクチャの設計においては、求められるセキュリティレベルが異なるネットワークの分離やアクセス権の必要最小権限付与等、インシデント発生時のシステムへの被害を極小化するための設計が求められます。また、セキュリティ運用においては、ネットワーク機器やサーバ等の各種ログ、セキュリティ製品のアラート等を収集して分析し、インシデントの発生やその予兆を速やかに検知するための独立した監視環境を用意することも重要です。そして、発生したインシデントに対応し、速やかな業務復旧を可能とするための体制や運用プロセスの整備、重要データやシステムの安全なバックアップシステムの構築等が求められます。

④ 人的ミスへの対応策の検討

人的ミスを誘発する可能性のあるシステム仕様については、ユーザインタフェースやデザイン等を改善することで事故発生防止を図ります。また、そうしたシステム仕様の改善に加え、システム利用者や運用者等のリテラシーを高めるための取組みとして、教育コンテンツを事前に提供する等の対策を講じることも有効です。

今回はセキュリティ・バイ・デザインのセキュア調達工程とセキュリティ設計工程における要求事項、実施内容、セキュリティ対策の考え方等について解説しました。次回は残る 4 つの実施工程と実施内容、実施における留意事項について解説します。

●参考情報

政府情報システムにおけるセキュリティ・バイ・デザインガイドライン
(https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/7e3e30b9/20240131_resources_standard_guidelines_guidelines_01.pdf)

配信予定日：2025 年 10 月 10 日（金）14:00 頃
カテゴリ：中小企業サイバーセキュリティ対策事業の知見
タグ：＃知識編＃インシデント対応強化
過去記事焼き直し：しない（新規記事です）
記事 URL（新設します）：https://cybersecurity-taisaku.metro.tokyo.lg.jp/know_more/cyber-taisakutiken5/

ライトな支援あります！セキュリティ対策点検

目次

本記事では東京都が独自に調査した情報を発信いたします。
今回は令和 6 年度中小企業サイバーセキュリティフォローアップ事業からの情報を発信します。

●レベルアップと併設されたライトな支援とは

東京都では中小企業のセキュリティ対策度合い（レベル）に応じた支援を用意しています。

[支援メニューと概要]
レベル 1 ：啓発事業、セミナー・メール訓練・ネットワーク調査等
レベル 2 ：基本対策事業、UTM/EDR の試行導入・規程策定支援等
レベル 3 ：実践力強化プログラム、セミナー・ワークショップ・課題解決支援等
レベル 3 ：インシデント対応強化、CSIRT 構築・IT-BCP 策定支援等
全レベル：フォローアップ、メルマガ・セミナー・セキュリティ対策点検等
※詳細は過去の記事をご覧ください。
東京都サイバーセキュリティ対策事業の成り立ちと今後について

支援メニューごとに参加企業が来る・もしくは専門家の訪問を受ける、回数を書くと以下です。

[支援メニューごとの打ち合わせ等回数]
レベル１：啓発事業、１～５回
レベル２：基本対策事業、２～６回
レベル３：実践力強化プログラム、１４回
レベル３：インシデント対応強化、６回
全レベル：フォローアップ、１～３回

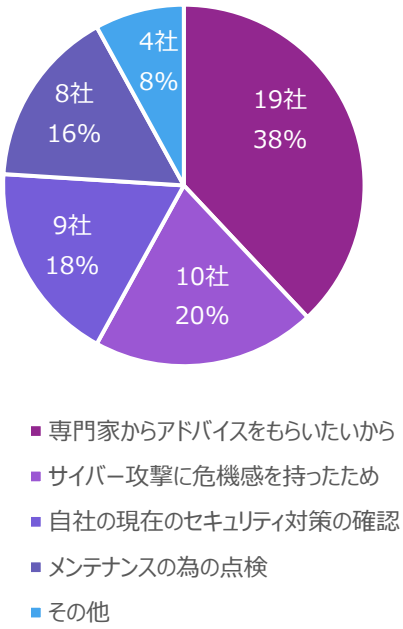
最も回数の多い実践力強化プログラムは、過去の記事で「ブートキャンプ」と表現した通り、ハードなトレーニングと言えます。
一方で、最も訪問回数の少ないフォローアップは、レベル１～３の支援に併設された、ライトな支援となっています。

フォローアップの内容は
（１） メルマガ
（２） セミナー（オンライン）
（３） セキュリティ対策点検（専門家派遣１～３回）
となっています。

次項でセキュリティ対策点検にフォーカスして参加企業の反応等アンケート結果を紹介していきます。

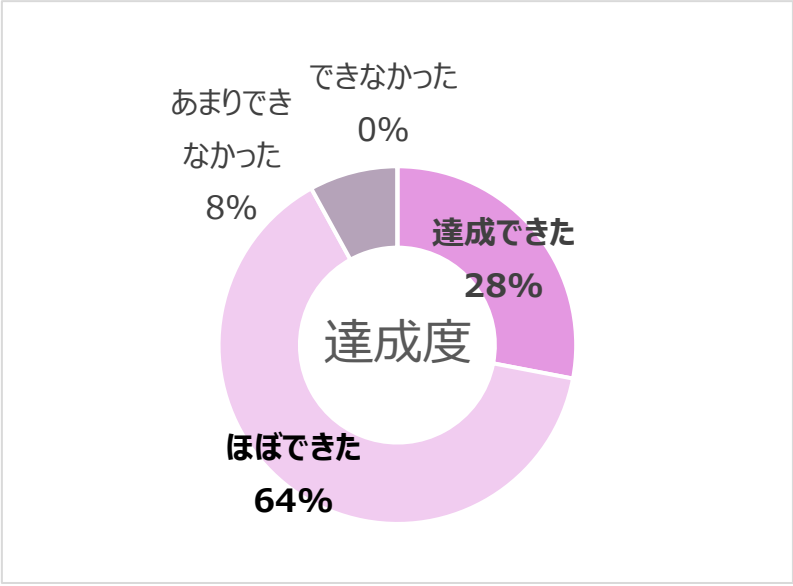
●参加企業が考えていること
令和６年度のフォローアップ事業のセキュリティ対策点検には５０社が参加しました。アンケート結果を紹介していきます。

■参加目的



各企業の参加目的として最も多かったのは「専門家からアドバイスをもらいたいから」、ついで「サイバー攻撃に危機感を持ったため」に。
「その他」には、「経営層へセキュリティ対策の理解を深めてもらいたい」などがありました。

■参加目的の達成度合い



参加目的に対して、9割超が一定以上の達成を実感していました。
東京都事業の他支援と比して“ライトな支援”ですが、目的を達成できる支援であることがわかります。

●今後の見通し
今年度もセキュリティ対策点検は行われています。
令和７年度東京都中小企業サイバーセキュリティフォローアップ
既に定員に達しております、来年度以降も実施されるかは検討中です。

令和６年度の参加企業へのアンケートでは、今後支援として求める内容も聞きました。

■支援に求める内容（複数回答、有効回答数 47 社）

１位	セキュリティ対策に役立つ情報の提供	36 社
２位	自社システムのセキュリティ診断	27 社
３位	セキュリティインシデントの対応実習	14 社

情報提供のニーズは高く、回答の約８割を占め、次いでセキュリティ診断が約６割を占めています。
上記の声を受け、令和７年度事業ではセキュリティ対策に関するメルマガ配信とシステムのセキュリティ診断として「ASM」と「プラットフォーム脆弱性診断」を行っています。参加企業の目的達成度合い９割を超えている支援ですが、毎年度改善を図っています。

今回の記事により、東京都の５つの支援（啓発、基本対策、実践力強化、インシデント対応強化、フォローアップ）における東京都独自ノウハウを紹介させていただきました。内容を絞って記事にしているため、まだまだご紹介したい内容があります。次回以降の記事もご期待ください。

東京都事業は具体的な対策や、専門家派遣を毎年数百社以上に行っています。東京都では支援を通じて得られた知見、見えてきた傾向から日本の中小企業をサイバー攻撃から守る術を提供していきたいと考えております。皆様からのご意見・ご感想は本ウェブサイトの下部に記載のあるお問い合わせ先へ是非お寄せください。

配信予定日：2025 年 10 月 10 日(金) 14:00 頃
カテゴリ：技術的セキュリティ対策（2/2）
タグ：＃実用編＃知識編＃技術的セキュリティ対策
過去記事焼き直し：する（過去記事を上書きします）
過去記事：https://cybersecurity-taisaku.metro.tokyo.lg.jp/know_more/mottosiritai10/

技術的セキュリティ対策（2/2）

目次

中小企業の経営者や情報システム担当者の皆さん、日々のセキュリティ対策、お疲れ様です。本シリーズ２回目となる今回は、技術的セキュリティ対策のうち身近でありながら誤解も多いデータの暗号化、安全消去について解説します。

なお、前回は技術的対策に必要となるセキュリティソフトウェアやサービスとその活用法について解説しているので、そちらもぜひご覧ください。
（前回の記事はこちら）技術的セキュリティ対策（1/2）

１．データの暗号化

昨今、コンピュータとインターネットの利用は、業務でもプライベートでも不可欠になりました。インターネットは誰でも利用可能なネットワークのため、暗号化は、盗聴・改ざん・漏えいなどを防止し、セキュリティとプライバシーを守るために必須の技術です。

そのような背景から、コンピュータとインターネットの普及に伴い、「逆さ読み」などの古典暗号から、数学を応用した現代暗号が生み出されました。現代暗号の技術には様々な方法があり、それぞれ異なる目的やセキュリティ要件に応じて使用されています。
ここではパソコンなどに保存するデータの暗号化と、インターネットを利用するときの通信の暗号化について解説します。

●データ暗号化

特定の法則に基づいてデータを変換し、第三者に内容を知られないようにする技術。
例えば、サーバー、パソコン、電子媒体をディスクまたはファイル単位で暗号化することで、メール送信時の添付ファイルの盗聴、社外からの不正アクセスによるデータの持ち出し、パソコンや電子媒体の紛失や盗難などによる情報漏えいのリスクを低減することができます。
さらに、端末の紛失・盗難対策としてディスク全体の暗号化が推奨されています。BitLocker（Windows）や FileVault（Mac）などの OS 標準機能を活用し、自動暗号化と復号キーの安全な管理を行うことが重要です。

代表的なものに、暗号をかける人と、暗号を解く人が共通の同じ鍵を持つことを前提とした「共通鍵暗号（対称鍵暗号）」の技術で AES（Advanced Encryption Standard：現代の標準的な対称鍵暗号で高いセキュリティを提供します）があります。
Microsoft Office（Word、Excel、PowerPoint など）のパスワード使用による暗号化には、AES が使用されています。

●通信暗号化
特定の法則に基づいて通信を変換し、第三者に傍受・盗聴されないようにする技術。
通信を暗号化する場合、授受する 2 者間で鍵を共有しなければなりません。しかし、秘密である鍵をインターネット経由で送ると、通信経路上、第三者に傍受され、解読されてしまうリスクがあります。
では、場所を隔てた 2 者間で、インターネットを使って安全に鍵を共有するには、どうしたらよいのでしょうか？この問題は「公開鍵暗号」の発明によって解決されました。

「公開鍵暗号」は、秘密の鍵を 2 者間で共有しなければならない「共通鍵暗号」の本質を覆す画期的な発明でした。
「公開鍵暗号」では暗号化する鍵と復号する鍵とが異なり、暗号化する人は復号する鍵を知らなくても暗号化することができます。そこで暗号化する人は、相手が持っている「暗号化しかできない鍵」を公開してもらい、暗号化して相手に送ります。このとき通信経路で鍵が傍受されても、「暗号化しかできない鍵」なので解読されることはありません。受け取った相手は、自分だけが持っている「復号しかできない鍵」を使って元に戻します。

インターネット経由でデータの通信を行うとき、データを保護するために用いられる暗号化や認証のための技術規格のうち、最も普及しているものの 1 つが、この「公開鍵暗号」の技術である TLS*です。一般的なウェブブラウザはすべて TLS に対応しているので、改めて導入する必要がないメリットがあり、世界的に広く利用されています。なお、TLS 1.2 以降の使用が必須とされており、TLS 1.0/1.1 は非推奨です。

*過去に SSL（Secure Sockets Layer）として規格化され、現在は TLS（Transport Layer Security）という名前で国際標準となっていますが、TLS のことを今でも SSL と呼んでいる場合もあります。

２．データの破棄

情報システムを使わなくなった場合、システム内にデータを保存したまま放置したり、廃棄したりすると、それが情報漏えいの原因となるため、速やかにデータの消去を行う必要があります。

またクラウドサービスの場合も、不要となったデータをクラウド上に保存したままにするのは、情報漏えいのリスクを不必要に高めることにつながります。

電子的なデータは、人には直接見えない形で、磁気パターンや電気的、または光学的な形で記録されています。これらは目に見えない「ビットとバイト」の集まりにすぎず、コンピュータを使わないと読解することができません。そのため、データが保存されている場所や形は直感的に理解しづらく、二度と復元できないように破棄・消去するには、正しい方法で行う必要があります。

よく使う Windows の削除やフォーマットでは、データが完全に消去されません。

これらの操作では、データそのものはディスク上に残っており、ファイルの参照情報、図書に例えると目次だけが削除され、本文は削除されていない状態です。そのため、復元ツールを使用すると、消去したデータが復元できてしまいます。

以下に電磁記録媒体の種類別に完全な破棄・消去の方法を説明します。

（１）HDD（ハードディスクドライブ）・CD 等の光ディスク

●上書き

データを上書きして消去する方法です。複数回実施することで、データの復元難易度を高めることができます。ただし、複数回実施しても最新の技術や強力なリカバリツールにより完全な消去が保証されるわけではありません。光ディスクは DVD-RW、BD-RE など書き換え可能ディスクが対象になります。専用のツールが流通していますので、それらを使用して複数回の上書き消去を行うことで復元リスクを低減できます。

●消磁

磁気を使ってデータを消去する方法です。専用の機器が必要であり、全てのハードディスクで使用できるわけではありません。また、HDD の磁気ヘッドを完全に消去するため、再利用はできません。光ディスクは対象外です。

●物理破壊
物理的に破壊することでデータを確実に消去します。破壊は、ハンマーでの打撃や、専用のシュレッダーで行います。光ディスクに傷をつける場合は、データを記録するための薄い金属の「反射層」を破壊する必要がありますが、記録面（銀色や青い部分）は厚い樹脂で保護されているため、傷が浅いと「反射層」に達しません。ラベル面（記録面の裏）に傷をつけたほうが「反射層」に達しやすく確実に破壊することができます。なお、環境負荷や廃棄物処理の観点から、専門業者による処理が望ましいとされています。

（２）SSD（ソリッドステートドライブ）
SSD とは、記憶媒体にフラッシュメモリを用いる外部記憶装置です。HDD と比べデータ読み書き速度が速く、小型で軽量なためスマートフォン、モバイル機器や USB メモリなどに使われています。SSD のデータ消去は、データを管理する方式が HDD とは異なるため上書きでは完全な消去が難しいことがあります。

●暗号化消去
データが保存されている領域を暗号化し、その暗号化キーを破棄する方法です。これにより、データが実質的に読み取れなくなります。暗号化消去は、ドライブ内の全データを迅速に消去する方法ですが、暗号化の管理が適切に行われていることが前提です。機器に暗号化機能がない場合は、専用のツールを使用します。

●工場出荷時リセット
SSD のファームウェアが提供するリセット機能を使って、データを消去する方法です。
ただし、すべての SSD がこの方法に対応しているわけではありません。

●物理破壊
SSD を物理的に破壊することでデータを確実に消去します。
（３）クラウドサービス
クラウドサービスのデータ消去はプロバイダーに依存するので、サービス契約に基づく明確な消去手順を確認することが重要です。
データ消去後の残存データ（例えば、バックアップやキャッシュ）の管理についても考慮が必要です。

●サービスプロバイダーによる消去
クラウドサービスのプロバイダーは、消去を実施することができますが、契約やサービスレベルアグリーメント（SLA）に従ってデータが適切に消去されることを確認する必要があり

ます。

●消去要求
ユーザーは、クラウドサービスの管理コンソールやサポートを通じてデータ消去を要求することができます。これには、アカウントの削除や特定のデータセットの消去が含まれます。

●暗号化 クラウドサービスに保存されているデータを暗号化することで、情報漏えいのリスクを低減できます。暗号化されたデータが物理的に消去されなくても、暗号化キーの削除により復元できなくなります。

なお、本稿は、独立行政法人情報処理推進機構（IPA）が公表している「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」を参考に解説しています。

次回は、監査・点検の効果的な実施方法について解説します。

配信予定日：2025 年 10 月 17 日(金) 14:00 頃
カテゴリ：もっと知りたい！セキュリティ
タグ：＃知識編
過去記事焼き直し：しない（新規記事です）
記事 URL（新設します）：https://cybersecurity-taisaku.metro.tokyo.lg.jp/know_more/secure-by-design4/

セキュリティ・バイ・デザイン概説 4

目次

中小企業の経営者や情報システム担当者の皆さん、日々のセキュリティ対策、お疲れ様です。セキュリティ・バイ・デザイン概説の最終回となる本記事では、セキュリティ実装以降の各工程における要求事項、実施内容、セキュリティ対策の考え方のほか、実施における留意点等について解説します。

●セキュリティ実装工程における要求事項及び実施内容
セキュリティ設計工程に続くのがセキュリティ実装工程であり、セキュリティ設計の内容をシステムに実装する工程です。

この工程における要求事項及び実施内容は次の通りです。

・セキュリティ設計に基づいて、セキュリティ機能の実装
・セキュリティ設計方針に基づくアプリケーションのセキュアコーディング
• セキュリティ設計に基づくプラットフォームのセキュリティ設定の実施（堅牢化、要塞化）

●セキュリティ実装工程におけるセキュリティ対策の考え方
セキュリティ関連のコーディングやセキュリティ設定は、テンプレートや自動化機能を用いることでミスやばらつきを防止することが推奨されます。同様にアプリケーション開発においては、セキュアコーディングをサポートする開発用ツールやフレームワークを活用することが有効です。また、各種プラットフォーム向けに最適化されたセキュリティベンチマーク（ベストプラクティス）やセキュリティ設定が組み込まれたシステムイメージ、IaCテンプレート等を使用することも推奨されます。

●セキュリティテスト工程における要求事項及び実施内容
セキュリティ実装工程に続くのがセキュリティテスト工程です。

この工程における要求事項及び実施内容は次の通りです。

・セキュリティ機能テストの実施（単体テスト、結合テスト、システムテスト等）
・対象となるシステムに応じた脆弱性診断の実施（下記例）
　Web アプリケーション脆弱性診断
　プラットフォーム脆弱性診断
　スマートフォンアプリケーション診断
・実際の脅威に基づく高度なセキュリティ診断（TLPT 等）
・機能テストで検出されたバグの是正対応
・脆弱性診断、TLPT 等で検出された脆弱性に対する是正対応

●セキュリティテスト工程におけるセキュリティ対策の考え方
攻撃対象となる領域（Attack Surface）に対して漏れなく脆弱性診断が実施されるように、システムの環境や特性に応じた適切なスコープで脆弱性診断を実施します。また、重要度の高いシステムにおいては、表層的な脆弱性診断のみでは不十分であるため、専門家による高度な診断を追加で実施する等、リスクレベルに応じた脆弱性診断を実施することが重要です。

●セキュリティ運用準備工程における要求事項及び実施内容
セキュリティテスト工程に続くのがセキュリティ運用準備工程です。

この工程における要求事項及び実施内容は次の通りです。

・セキュリティ運用体制の確立
・下表の項目に対応したセキュリティ運用手順の整備

平時の運用	有事の運用
構成管理、変更管理	インシデント対応
セキュリティ製品のアラート、システムログ等を活用したセキュリティ監視、検知	
脅威情報の収集、対象システムへの影響分析	
CVSS 等に基づく、リスクに応じた脆弱性対応	
定期的な脆弱性診断の実施	

・システム運用において人的ミスが発生する可能性のある箇所の洗い出し、是正
・有事を想定したセキュリティ運用訓練の実施

●セキュリティ運用準備工程におけるセキュリティ対策の考え方
事前にインシデント対応手順等を整備していたとしても、実際にインシデントが発生すると、想定通りには対応が進まず、多くの時間を要して被害が拡大するケースが多くあります。そのため、インシデント発生を想定した訓練を実施し、実運用上の課題を特定し、体制や手順の見直しを行うことで、インシデント対応の実行性を担保する取組みが推奨されます。また、訓練実施後には関係者に結果をフィードバックすることで、セキュリティ意識の向上やインシデント対応手順の理解を促進する効果も見込まれます。

●セキュリティ運用工程における要求事項及び実施内容
セキュリティ運用準備工程に続くセキュリティ・バイ・デザインの最終工程がセキュリティ運用工程です。

この工程における要求事項及び実施内容は次の通りです。

・前工程で整備した運用体制、手順等によるセキュリティ運用の実施
・セキュリティ運用を行う要員の教育及び訓練の実施、重要な情報を取り扱う要員のスクリーニング（要員のスキルや行動特性等を考慮）

●セキュリティ運用工程におけるセキュリティ対策の考え方

① SBOM 等によるソフトウェアの構成管理
アプリケーションで使用するライブラリやミドルウェア等に深刻な脆弱性が発見された場合に、それが対象システムに含まれるかどうかを迅速に判断できるよう、SBOM 等を利用してソフトウェアの構成管理を行います。

② 定常的な脅威情報/脆弱性情報の収集及び対応
セキュリティ脅威や脆弱性に対処するため、定常的に脅威情報や脆弱性情報を収集し、被害の発生が想定される脆弱性に対しては、緊急にセキュリティパッチを適用する、セキュリティパッチが適用できないケースは暫定対処策を講じる、システムの機能を制限する等、対応方針を決定します。

③ サイバーレジリエンスを高めるセキュリティ運用
インシデントやその兆候の早期検知、速やかなインシデント対応や業務復旧を実践することで、インシデント発生時のシステム被害やサービスへの影響を極小化します。また、インシデント対応やサービス復旧の実行性を維持するため、定期的にインシデント対応手順やサービス復旧手順を見直し、インシデント対応訓練を実施します。
実際にセキュリティインシデントが発生した場合には、根本的な発生原因を究明して再発防止策を講じるとともに、対応において想定通りに進まなかった部分等について継続的に改善を行うことで、インシデント対応レベルの向上を図ります。
こうした取り組みが組織のサイバーレジリエンス（回復力）を高めることにつながります。

●セキュリティ・バイ・デザイン実施における留意事項
これまで 4 回にわたり、セキュリティ・バイ・デザイン導入のメリットや基本的な考え方、各工程における要求事項、実施内容、セキュリティ対策の考え方等について解説してきまし

た。このシリーズのまとめとして、セキュリティ・バイ・デザイン実施における留意事項を挙げておきます。

・セキュリティ・バイ・デザインの工程間で整合のとれていないセキュリティ対策が実施された場合、システムのセキュリティ品質を確保することが困難になるため、工程間で一貫した、整合性が確保されたセキュリティ対策を実施するよう留意する必要がある。

・セキュリティ・バイ・デザインの実施内容の全てを同時に実現することは困難であるため、自組織の開発プロセスやルール、考慮すべきリスク等を踏まえ、重要かつ実施可能な箇所から運用を開始し、課題の改善と内容の拡充を図りながら成熟度を向上していくことが推奨される。

・セキュリティ・バイ・デザインは一過性の取り組みではなく、脅威の動向やシステム環境の変化等を踏まえ、再実施の要否、再実施方法等を検討し、継続的にセキュリティリスクの低減を図っていくことが求められる。

●用語解説

IaC（Infrastructure as Code）

IT インフラの構成をコード化し、構築、変更、削除等を自動化する手法であり、その設定ファイルを IaC テンプレートと呼びます。

TLPT（Threat-Led Penetration Testing）

実際のサイバー攻撃の脅威に関する情報を収集・分析した結果（脅威インテリジェンス）を活用し、それを模した手法を駆使することで企業等のサイバーセキュリティ対策の有効性を総合的に評価する手法です。

CVSS（Common Vulnerability Scoring System）

脆弱性の深刻さを評価する仕組みであり、ベンダに依存しない共通の評価方法を提供しています。

SBOM（Software Bill of Materials）

ソフトウェアを構成する各部品（コンポーネント）の名称、ビルド情報、ライセンス情報、互いの依存関係、どのような構成となっているか等を示すリスト。SBOM により、ソフトウェアの構成情報を詳細に把握することができるため、脆弱性情報の即時の特定等が可能となります。

●参考情報

政府情報システムにおけるセキュリティ・バイ・デザインガイドライン
(https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/7e3e30b9/20240131_resources_standard_guidelines_guidelines_01.pdf)

配信予定日：2025 年 10 月 17 日(金) 14:00 頃
カテゴリ：基礎から学ぶ！ セキュリティ
タグ：＃実用編＃知識編
過去記事焼き直し：する（過去記事を上書きします）
過去記事： https://cybersecurity-taisaku.metro.tokyo.lg.jp/basics/kisokaramanabu9/

【令和７年度版】中小企業におけるセキュリティ脅威への対策強化　～サプライチェーンの弱点を悪用した攻撃から対策を学ぶ～

独立行政法人 情報処理推進機構（IPA）が毎年発行している「情報セキュリティ 10 大脅威 2025」から、中小企業の経営者やシステム担当者が注目すべき点を掘り下げていきます。

今回は２位に挙げられている「サプライチェーンの弱点を悪用した攻撃」を事例とともに深掘りします。

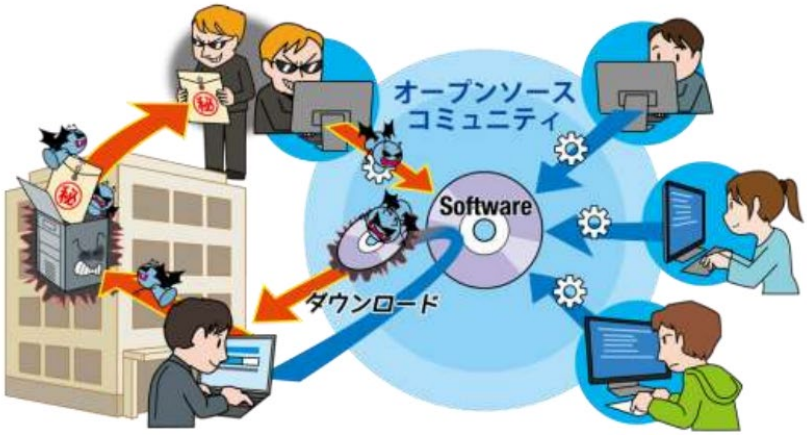
１．サプライチェーンとは

サプライチェーンとは、商品の企画、開発、調達、製造、在庫管理、物流など、製造から販売までの一連のプロセス及び、その商品やサービスが最終消費者に届くまでに関わる全ての組織や活動のネットワークを指します。
サプライヤー、製造業社、流通業者などがこれにあたります。

また、ソフトウェア開発のライフサイクル*に関与する全てのモノ（ライブラリ、各種ツール等）や人の繋がりを、ソフトウェアサプライチェーンと呼びます。
*ソフトウェア開発のライフサイクル：ソフトウェアが企画・仕様、設計から実装、テスト、運用、及びメンテナンス・監視までたどる、一連のライフサイクルのこと

このような「ビジネス上の繋がり」や「ソフトウェアの繋がり」を悪用した攻撃をサプライチェーン攻撃と呼びます。

この脅威が業務にもたらす影響や、取るべき対策について解説いたします。



引用元：IPA　情報セキュリティ 10 大脅威 2025 解説書［組織編］より

2．狙われるサプライチェーンの弱点

標的とする組織が強固なセキュリティ対策を行っていて直接攻撃が困難な場合、攻撃者は、そのサプライチェーンの脆弱な部分を探し出して攻撃を行います。

大手企業と繋がりのある中小企業の中には、セキュリティへの対策が十分でない企業も多くあります。攻撃者はその脆弱な企業を足掛かりとして間接的、及び段階的に標的とする組織を狙います。

攻撃者の侵入を許してしまった場合、機密情報の漏えいや信用の失墜等、様々な被害が発生します。

また、自組織のセキュリティ対策が十分ではなく、攻撃を受けた上で足掛かりとされると、サプライチェーン上の取引相手に損害を与えてしまい、取引相手を失ったり、損害賠償を求められたりするおそれが想定されます。

3．主な攻撃手口

サプライチェーンを狙った攻撃はさまざまな手口で行われます。以下に代表的なサプライチェーンの弱点を悪用した攻撃例を紹介いたします。

（1）取引先や委託先が保有する機密情報を狙った攻撃

標的とする組織よりもセキュリティが脆弱な取引先や委託先、国内外の子会社等を攻撃し、その攻撃を受けた組織が保有する標的組織の機密情報等を窃取する手法です。

標的とする組織では機密情報扱いであり、堅牢なセキュリティのもと管理されているとしても、セキュリティが脆弱なサプライチェーン上の組織でも同じように厳密に管理されているとは限らず、そこが狙われてしまうのです。

（2）ソフトウェアサプライチェーン攻撃

標的組織と取引のある、または調達するであろうソフトウェアやサービスを改ざんして、ソフトウェアそのものやアップデートプログラムなどに不正コードを混入させ、標的組織に侵入するための足掛かりとする攻撃手法です。

標的組織がそのソフトウェアを導入したり、更新する際にウイルス感染を引き起こすのです。

（3）サービスサプライチェーン攻撃

はじめに企業システムの運用、監視等を請け負う事業者（MSP：マネージドサービスプロバイダー）等を攻撃し、足掛かりとする攻撃手法。

MSP が利用する資産管理ソフトウェア等にウイルスを仕込み、MSP の複数顧客にウイルスを感染させる手口もあります。

4．サプライチェーンの弱点を悪用した具体的な攻撃事例

【事例 1 ：業務委託先業者からの顧客情報漏えい】

2024 年 5 月、情報処理業の I 社は VPN 経由の不正アクセスを受け、端末やサーバー等がランサムウェア攻撃を受けたことを公表しました。また同年 6 月には、攻撃者が窃取したとされる情報のダウンロード用 URL が攻撃者グループのリークサイトに掲載されました。この攻撃によって、I 社に業務を委託した組織からは 情報漏えいに関するお知らせが多数公表され、自治体だけでも約 50 万件以上の個人情報の漏えいが判明しています。また、業務委託元の 1 組織からは損害賠償請求を行う予定も報告されています。

引用元：IPA　情報セキュリティ 10 大脅威 2025 解説書［組織編］より抜粋

この事例は、「2．主な攻撃手口」の「（1）取引先や委託先が保有する機密情報を狙った攻撃」の具体的な内容になります。

機密情報を保有する委託先が攻撃者に狙われた訳ですが、委託元も「委託しても情報漏えいの責任は委託元に残る場合がある」ことに意識を持ち、セキュリティの可視化と継続的な確認体制の構築が必要であると言えます。

【事例 2 ：提携先企業に不正アクセス、顧客情報漏えい】

2024 年 3 月、Linux 環境で広く利用されている「XZ Utils」という可逆圧縮ツールに悪意のあるコードが仕込まれたことが確認されました。この悪意あるコードは共同開発者によって挿入されており、特定の条件下でリモートからシステム全体へ不正アクセスできるおそれがありました。

引用元：IPA　情報セキュリティ 10 大脅威 2025 解説書［組織編］より抜粋

この事例は、「２．主な攻撃手口」の「（３）サービスサプライチェーン攻撃」の具体例です。
オープンソースソフトウェアの利便性とリスクの両面を改めて認識させるものであり、今後のオープンソースソフトウェア活用においては、技術的な対策だけでなく、信頼性の評価と継続的な監視体制の構築が求められます。

５．サプライチェーンの弱点を悪用した攻撃への対策
サプライチェーンの弱点を悪用した攻撃への対策は組織で実施する必要があります。
以下に「経営層の観点」「自組織の観点」「関わる組織の観点」で説明していきます。

（１）経営層の対応と対処
◇被害の予防
・インシデント対応体制を整備し対応する※

（２）自組織の対応と対処
◇被害の予防
・情報管理規則の徹底
調達先や業務委託先等、契約時に取引先の規則を確認します。

・セキュリティ評価サービス（SRS）*1 を用いた自組織のセキュリティ対策状況の把握
*1 セキュリティ評価サービス（Security Rating Services）：攻撃者と同様の手法を用いた擬似的な攻撃を行うことにより潜在的な脆弱性を評価し改善するための助言を行うサービス

・信頼できる委託先、取引先、サービスの選定
商流に関わる組織、サービスの信頼性評価*2（ISMAP*3 など）、品質基準を検討し、複数候補を検討します。
*2 サービスの信頼性評価：システムやソフトウェアが一定の条件下で正常に稼働し、安定的にサービスを提供しつづけることができるかどうかを測るための指標
*3 ISMAP：政府が活用しているクラウドサービスのセキュリティレベルを評価する制度

・契約内容の確認
組織間の取引や委託契約における情報セキュリティ上の責任範囲を明確化し、合意を得ます。また、賠償に関する契約条項を盛り込みます。

・委託先組織の管理
委託元組織が委託先組織のセキュリティ対策状況と情報資産の管理の実態を定期的に確認できる契約とすることが重要です。また、業務委託自体が適切であるかも検討します。

・納品物の検証
納品物に組み込まれているソフトウェアの把握と脆弱性対策を実施します。ソフトウェアの把握や管理においてはソフトウェア部品表（SBOM）*4 の導入を検討します。
*4 ソフトウェア部品表（Software Bill Of Materials）：ソフトウェアアプリケーションを構築するためのライブラリ、コードパッケージ、サードパーティ製コンポーネントなどのライセンス情報・バージョン・修正適用状況・依存関係等をすべて記載したもの。

◇被害を受けた後の対応
・インシデント対応体制を整備し対応する※
・被害への補償組織としての体制の確立

（３）関わる組織の対応と対処
自組織に関わる組織の対応は共に実施する必要があります。

◇被害の予防
・取引先や委託先との連絡プロセスの確立
・取引先や委託先の情報セキュリティ対応の確認、監査
・情報セキュリティの認証取得 ISMS、プライバシーマーク、SOC2 等を取得し、定期的に見直して必要な運用を維持する。
・公的機関等が公開している資料の活用

◇被害を受けた後の対応
・適切な報告／連絡／相談を行う※

「※」の詳細については、IPA の「情報セキュリティ１０大脅威 2025」の 36 ページからの「共通対策」をご参照ください。
また、前回の「中小企業におけるセキュリティ脅威への対策強化～ランサムウェアによる攻撃事例から対策を学ぶ～（2/2）」でも、詳細を解説していますので、併せてご参照ください。

ここまでサプライチェーンの弱点を悪用した攻撃の事例や影響、対策方法について考えてきましたが、いかがだったでしょうか。
今回取り上げた事例や対策から分かるように、サプライチェーンを狙った攻撃の影響は自組織の外部へも及びます。
サプライチェーンは企業活動と切り離すことは困難です。
セキュリティへの取り組みは各企業を超えてサプライチェーン全体で実施することで、企業活動を支える基盤を強化することが可能です。
そのため、サプライチェーン全体で的確なセキュリティ対策を行うことは、企業の持続可能な発展を支える鍵となるとも言えます。

※本記事は令和 6 年度中小企業サイバーセキュリティ対策事業で制作された記事を最新情報等で更新したものです。

配信予定日：2025 年 10 月 17 日(金) 14:00 頃
カテゴリ：基礎から学ぶ！ セキュリティ
タグ：＃実用編＃知識編
過去記事焼き直し：する（過去記事を上書きします）
過去記事：https://cybersecurity-taisaku.metro.tokyo.lg.jp/basics/kisokaramanabu10/

中小企業におけるセキュリティ脅威への対策強化　～内部不正による情報漏えい等の被害から対策を学ぶ～

目次

独立行政法人 情報処理推進機構（IPA）が毎年発行している「情報セキュリティ 10 大脅威 2025」から、中小企業の経営者やシステム担当者が注目すべき点を掘り下げていきます。
今回は 4 位に挙げられている「**内部不正による情報漏えい等の被害**」を深掘りします。
従業員や元従業員等の組織関係者による機密情報の持ち出しや、社内情報の削除等の不正行為が発生しています。
また、組織内の情報管理の規則を守らずに情報を持ち出し、紛失や情報漏えいにつながるケースもあります。
組織関係者による不正行為は、組織の社会的信用の失墜や、損害賠償や業務停滞等による経済的損失を招きます。
また、不正に取得された情報を使用した組織や個人も責任を問われる場合があります。この脅威がどのように業務に影響を与えるのか、対策はどうすべきなのかを解説します。

引用元：IPA　情報セキュリティ 10 大脅威 2025 解説書

１．内部不正による情報漏えい等の被害による脅威

悪意を持った組織関係者が、金銭受領、転職先での悪用、組織への私怨等を動機として、組織が保有する技術情報や顧客情報等の重要情報の持ち出しや第三者への提供、不特定多数が閲覧できる場所への公開、情報の削除や改ざん等の不正行為を行うことがあります。

また、自宅等の社外で作業するために組織の情報管理の規則を守らず情報を外部へ持ち出し、情報漏えいするケースもあります。

不正に取り扱われた情報の重要性や被害規模によっては、組織の社会的信用の失墜や、顧客等への損害賠償、損失補填、復旧作業等による経済的損失が発生し、組織の競争力の大幅な低下につながります。

その結果、組織経営の根幹を揺るがすおそれがあります。

また、自組織に持ち込まれた情報が不正に取得されたものであることを知りつつ使用した場合、刑事罰の対象になることもあります。

２．主な攻撃手口

以下に代表的な内部不正による情報漏えい手口を紹介します。

（１）アクセス権限の悪用

付与された権限を悪用し、組織の重要情報を窃取したり不正に操作を行うケースです。

必要以上に高いアクセス権限が付与されている場合、より重要度の高い情報が狙われ、被害が大きくなるおそれがあります。

また、複数人で端末を共用している場合、他人のアカウントで不正アクセスされるリスクも生じます。

（２）在職中に割り当てられたアカウントの悪用（離職後のアカウント利用）

離職者が在職中に使用していたアカウントが削除されていない場合、それを使用して組織の情報に不正にアクセスを続ける事が出来てしまいます。
これにより重要情報を容易に持ち出す事が可能となります。

（３）内部情報の不正な持ち出し（物理的な持ち出し）

組織の情報を、USB メモリーや HDD 等の外部記憶媒体、メール、クラウドストレージ、スマホカメラ、紙媒体等を利用し、外部に不正に持ち出すケース。こうした行為は予防措置の欠如によって、発見が遅れる事が多々あります。

３．内部不正による情報漏えいの具体的な事例

【事例１：顧客情報を転職先に持ち出し、営業活動に使用】

2024 年 8 月、不動産業 T 社は同業他社に転職した元従業員の個人情報の不正持ち出しを発表しました。不動産登記簿に記載されていた氏名、マンション名、部屋番号等、2 万 5,406 件がもちだされ、転職先で DM（ダイレクトメール）送付に利用されていました。同社は刑事告訴を視野に管轄警察署に相談を行ったということです。

参照元：IPA　情報セキュリティ 10 大脅威 2025 解説書

この事例は、「２．主な攻撃手口」の「（３）内部情報の不正な持ち出し」の具体的な内容になります。

【事例２：委託先企業が仕入先情報を不正ダウンロード】

2024 年 2 月、機械メーカーD 社は委託先作業者が私用で仕入先情報をダウンロードし、漏えいの可能性があると公表した。システム開発案件での再委託先による事案で、約 2 万 2,000 件の担当者氏名、連絡先、振込先情報が含まれていたとのことです。

参照元：IPA　情報セキュリティ 10 大脅威 2025 解説書

この事例は、「２．主な攻撃手口」の「（１）アクセス権限の悪用」の具体的な内容になります。

委託先への情報提供範囲は必要最小限にとどめることが重要です。また、委託先へ提供するデータの暗号化、アクセスログの取得・監視といった対策も有効です。

４．内部不正による情報漏えい等への対策

本対策は主に「システム管理者の観点」で説明していきます。

システム管理者の対応と対処

◇被害の予防

・基本方針の策定

「不正のトライアングル」を意識して基本方針を策定し、情報取扱ポリシーの作成、内部不正者に対する懲戒処分等を規定した就業規則等や、委託先との契約内容を整備します *1。

なお、組織内での対策推進は、経営層の積極的な関与が不可欠です。

内部不正対策の責任は経営者にあり、最高責任者である経営者が総括責任者の任命並びに管理体制および実施策の承認を行い、組織横断的な管理体制を構築する必要がある為です。

*1 内部不正を想定した従業員規約等は下記の経産省発行の秘密情報の保護ハンドブックのP175 ページ以降の「参考資料２　各種契約書等の参考例」、また、情報管理も企業力を合わせてご参照ください。

・資産の把握、対応体制の整備

情報資産を把握し、その重要度をランク付けした上で重要情報の管理者を定めます。

・重要情報の管理、保護

重要情報の利用者 ID およびアクセス権の登録・変更・削除に関する手順を定めて運用します。

従業員の異動や離職に伴う不要な利用者 ID 等は直ちに削除します。

また、それらの適切な管理、定期的な監査を実施します。さらに、利用者 ID の共用禁止等の処置を検討します。DLP（情報漏えい対策）等のツールの導入も併せて検討します。

・物理的管理の実施

重要情報の格納場所や重要情報を扱う執務室への入退室を管理します。

USB メモリー、スマートフォン、プリンター等の外部媒体は利用制限を行い、持ち出しや持ち込み等の履歴を管理します。

また、記録媒体の廃棄を行う際には、適切なデータ消去の運用 *2 を実施します。

消去できない場合は媒体の物理的な破壊も検討する必要があります。

また、リース品はデータ消去/初期化してから返却します。

*2 適切なデータ消去：

Windows11 の場合、「完全に削除する」又は「ゴミ箱を空にする」を実行したり、クリックフォーマットをしたりしても、ハードディスクや USB メモリー上にはデータが残っており、復元ツール等を利用すると復元できてしまいます。

ハードディスクや USB メモリーの完全なデータ消去は、時間がかかりますがフルフォーマット(Windows の場合にはクイックフォーマットのチェックを外して実行)で可能です。

・情報リテラシー、モラルを向上させる※

従業員向けに情報セキュリティ対策研修・情報事故対応演習等を実施します。従業員の入れ替わりや時間の経過に伴うリテラシーの低下に応じ、適宜実施していくことが必要になります。

・人的管理およびコンプライアンス教育の徹底

必要に応じ、従業員に秘密保持義務を課す誓約書に署名させます。 また、定期的な職務の変更、職場の異動を実施します。

被害の予防に対する対策の状況は、IPA 発行の組織における内部不正防止ガイドラインの102 ページ「付録Ⅱ：内部不正簡易チェックシート」を使ってチェックする事ができます。

◇被害の早期発見

・システム操作履歴の監視

重要情報へのアクセス履歴や利用者の操作履歴等のログ、証跡を記録し、監視する事で早期

検知に努めます。また、監視していることを従業員に周知することで不正の予防が可能です。さらに、特定時期の監視の強化 退職予定者の退職前後のシステム操作の監視を強化することで早期発見につながることがあります。

◇被害を受けた後の対応

・適切な報告／連絡／相談を行う※
・インシデント対応体制を整備し対応する※
・内部不正者に対する適切な処罰の実施

「※」の詳細については、IPA の「情報セキュリティ１０大脅威 2025」の 36 ページの「共通対策」をご参照ください。

ここまで内部不正による情報漏えい等の事例や影響、対策方法について考えてきましたが、いかがだったでしょうか。
内部不正による情報漏えい等は、従業員又は元従業員が行うため通常のセキュリティ対策だけでは十分ではないことがお分かりいただけたかと思います。
内部不正による情報漏えいは、システム的な管理／監視と人的管理およびコンプライアンス教育の両輪で行い、これを防止する事は、企業の持続可能な発展を支える鍵となるとも言えます。

５．事例

事例を見る

・弊社元従業員による個人情報の不正な持ち出しに関するご報告とお詫び(不動産業Ｔ社)
・仕入先様情報の漏洩可能性に関するお詫びとお知らせについて（機械メーカーD 社）

※本記事は令和 6 年度中小企業サイバーセキュリティ対策事業で制作された記事を最新情報等で更新したものです。

配信予定日：2025 年 10 月 24 日（金）14:00 頃
カテゴリ：中小企業サイバーセキュリティ対策事業の知見
タグ：＃知識編
過去記事焼き直し：しない（新規記事です）
記事 URL（新設します）：https://cybersecurity-taisaku.metro.tokyo.lg.jp/know_more/cyber-taisakutiken6/

東京都事業から見えた中小企業セキュリティ対策の実態と求められる事

目次

本記事では東京都の中小企業サイバーセキュリティ対策事業を通じて見えた、中小企業のセキュリティ対策の実態と求められる事をご紹介いたします。

●標的型攻撃メールは効率的？
昨今は中小企業であってもサイバー攻撃の被害を受けると言われていますが、東京都事業ではそれが身近にわかるデータとして

「標的型攻撃メールは 5 割以上の中小企業が開封する」

事を確認しています。
令和 6 年度中小企業サイバーセキュリティ啓発事業において 762 名、52 社に対し標的型攻撃メール訓練を行いました。結果は以下です。

単位	対象数	開封数	開封率
個人	762	155	20%
企業	52	29	56%

1 社最大 20 名が参加し、当該企業で 1 名でも開封した場合は、企業が開封したとカウントしています。

個人の結果は 20%でしたが、企業は 56%と半数以上の企業が標的型攻撃メールを開封しています。攻撃者目線で見ると、標的型攻撃メールを複数企業にばら撒くことで、半数以上の企業でウイルス感染などを引き起こす事が期待できます。昨今のパソコンの性能や、AI の進化も考えると、攻撃者にとって標的型攻撃メールは効率的な手法だと推察されます。

●“兼任体制”が当たり前の中小企業
そのような危機にさらされている中小企業側の体制はどうかと言うと、多くのリソースをかけられない実態があります。東京都中小企業サイバーセキュリティ対策事業の専門家派遣を通じて得た所感ですが、情報セキュリティ担当を担う方は以下のケースが多いです。

＜情報セキュリティ対策を担う方＞
従業員 20 名以下の企業：社長や役員が兼務
従業員 20 名から 100 名：総務部が兼務
従業員 100 名以上：専任者（情報システム部署内メンバーであることが多い）

中小企業庁の集計によると中小企業は約 336 万社、そのうち 285 万社は従業員 20 名以下です。
https://www.chusho.meti.go.jp/koukai/chousa/chu_kigyocnt/index.html
多くの企業では「誰かがついでにやっている」状態にあります。セキュリティに関して“漠然とした不安”を抱えながらも、専任と比して知識・経験が得難く、具体的な対策に踏み切れない状況にあると推察されます。

※なお、本件に関する統計的なデータもご紹介します。IPA が実施した調査では専門部署のある中小企業は 9.3%との事です（以下、P.69 参照）。
https://www.ipa.go.jp/security/reports/sme/nl10bi000000fbvc-att/sme-chousa-report2024r1.pdf

●やっていないのではなく、できる範囲で最適化
誤解してはいけないのは、中小企業は「何もしていない」わけではないということです。具体的な事例をいくつかご紹介いたします。

・取引先から求められるセキュリティチェック項目に対し、必須事項だけ対応して乗り切っている。

・パソコンは MAC も Windows も混在している状況であり、ウイルス対策等の集中管理が困難なため、会社情報はクラウド上にしか保存しないよう指導している。

・外部からの不正アクセスの可能性を減らすため、会社の外から中への通信となるリモートアクセスは行っていない。

いずれの事例も、支援させていただいている中小企業ご担当者様が自ら調べて取り組まれた事項です。事業実態に即し限られたリソースでできる事に取り組まれています。

●求められるのは「正しい評価」と「次の一歩」
残念ながら、冒頭の標的型攻撃メールのように、サイバー攻撃はどの企業に対しても行われています。これを完璧に防ぐには高水準のセキュリティ対策が必要です。しかし、中小企業のリソースが限られる状況です。中小企業に求められているのは、完璧な対策ではなく「今できることを正しく評価し、次の一歩を見定める」ことだと考えています。

東京都事業の専門家派遣支援には、単に足りない部分を指摘するのではなく、現状の取り組みが妥当かを見極めたうえで、優先度を明確に示す伴走型の支援が求められています。セキュリティは“やれば終わり”ではなく、日々の業務とともに育てていくもの。中小企業が自らのペースで無理なく続けられる対策こそが、現場に根付く“リアルなセキュリティ”の姿だと考えています。今後も東京都中小企業サイバーセキュリティ対策事業にご注目ください。皆様からのご意見・ご感想は本ウェブサイトの下部に記載のあるお問い合わせ先へ是非お寄せください。

配信予定日：2025 年 10 月 24 日(金) 14:00 頃
カテゴリ：もっと知りたい！セキュリティ
タグ：＃知識編
過去記事焼き直し：しない（新規記事です）
記事 URL（新設します）：https://cybersecurity-taisaku.metro.tokyo.lg.jp/know_more/living-off-the-land/

検知が困難な Living off the Land 戦術を用いた攻撃

目次

中小企業の経営者や情報システム担当者の皆さん、日々のセキュリティ対策、お疲れ様です。
今回は「日本政府のサイバーセキュリティ施策の概要」の中で少し触れた「Living off the Land 戦術」について解説します。

●Living off the Land 戦術とは
2024 年 6 月 25 日に JPCERT コーディネーションセンター（JPCERT/CC）、内閣サイバーセキュリティセンター（NISC）※1 より、「Operation Blotless 攻撃キャンペーン」に関する注意喚起がありました。
この「Operation Blotless 攻撃キャンペーン」では、Living off the Land（LotL：システム内寄生型、もしくは環境寄生型）戦術などと呼ばれる手法が用いられており、日本の組織もターゲットとなっているとのことです。LotL によるサイバー攻撃は、マルウェアを用いるのではなく、システム内に組み込まれている正規の管理ツールやコマンド、機能等を用いて認証情報の窃取、システム情報の収集等を行います。そのため、一般的に導入されているセキュリティツールでは検知が困難であることが特徴です。なお、この手法を過去に実際に用いた APT※2 攻撃グループとして「Volt Typhoon」の存在が知られています。

※1 2025 年 7 月に内閣官房組織令に基づき「国家サイバー統括室（NCO：National Cybersecurity Office）」に改組。

※2 APT（Advanced Persistent Threat：持続的標的型攻撃）とは、高度で持続的な手法を用

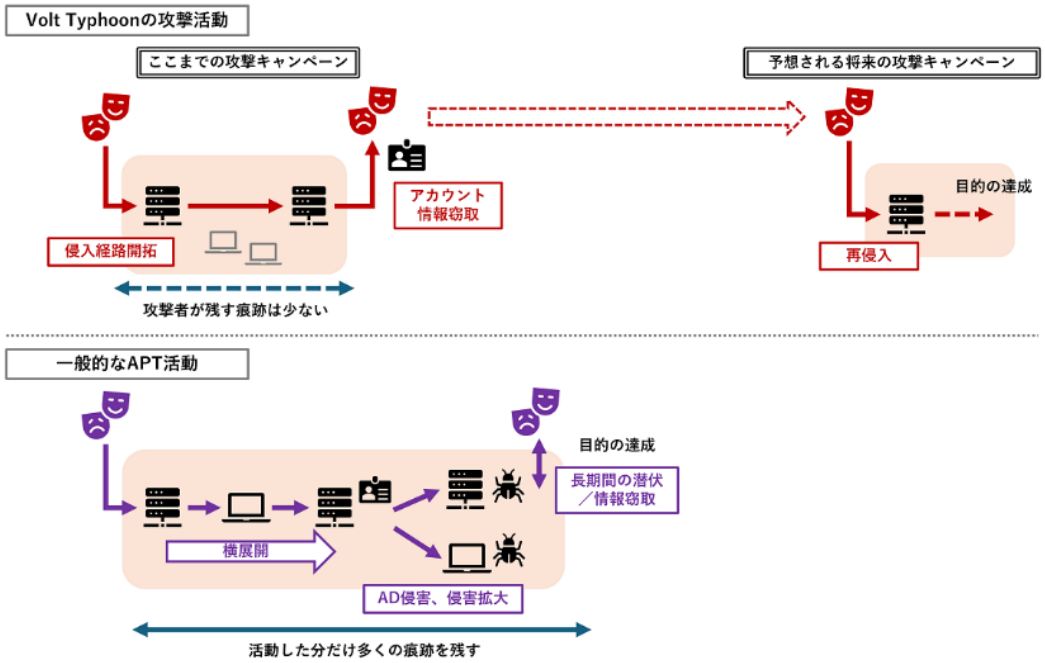
いて行われるサイバー攻撃を意味します。

●攻撃グループ「Volt Typhoon」による攻撃の特徴

「Volt Typhoon」とは、某国家が主導する攻撃グループであり、主に米国における通信、エネルギー、運輸、水道といった重要インフラ企業をターゲットしています。「Volt Typhoon」の活動目的は、上記のような重要インフラ企業等への本格的な侵入に備え、「侵入方法を開拓」することであり、そのために Active Directory（AD）サーバに保存されている認証情報（NTDS※3 ファイル）を窃取することのようです。また、攻撃が短期間に行われていることも特徴で、長期間にわたる潜伏・情報収集等は行われていないとのことです。

※3 NT Directory Services の略で、Active Directory サーバのデータベースファイルです。

LotL を用いた Volt Typhoon の攻撃活動と一般的な APT 活動の比較



（https://www.jpcert.or.jp/at/2024/at240013.html）

●LotL を用いた攻撃活動による侵害有無調査が困難な理由

(1) 調査に必要な Active Directory の各種ログの少なさ

上記のように、LotL では、Active Directory がターゲットとなるため、同サーバを中心とした調査が必要となりますが、一般的に、Active Directory では、調査に必要なログが出力されておらず、長期間の保存もされていないケースが多くあります。そのため、仮に侵害され

ていたことがわかったとしても、その調査に必要なログが残っていない可能性があります。

(2) 初期侵入経路となった機器のログの少なさ
LotL では、初期侵入経路として VPN（Virtual Private Network）製品の脆弱性を悪用した攻撃が多用されています。一般的に、そうしたネットワーク機器では各種ログを調査可能な状態で長期間保存していないことが多いため、仮に侵害されていたことがわかったとしても、調査が困難となる可能性があります。

(3) 侵害箇所が限定的
LotL では、他のサイバー攻撃の事例のように、多数の端末やサーバへの横展開や AD サーバそのものへの侵害等がなく攻撃の痕跡が残る箇所が少ないのが特徴です。そのため、侵害調査できる箇所が限定的となります。

●侵害調査として推奨される対応（短期的）
これまでに観測されている攻撃事例や JPCERT/CC が対応した事例等踏まえると、侵害有無調査を行う場合、短期的な対応として次のような事項が推奨されます。

(1) Active Directory データベースファイルの持ち出し試行の確認
(2) Windows イベントログの削除試行の確認
(3) Active Directory での PowerShell の実行内容の調査
(4) Web サーバやネットワーク機器などへの Webshell※4 の設置有無調査
(5) 過去の攻撃で使用されたリバースプロキシツールの設置有無調査
(6) VPN 機器等におけるログ調査や管理者アカウントの使用状況調査

※4 攻撃者がシステムへのバックドアとして使用するために設置する不正なスクリプト

●侵害調査として推奨される対応（中長期的）
今後の攻撃に備えて、短期的な対応に加え、次のような対応が推奨されます。

(1) 攻撃の侵入経路になり得るインターネットに接続されたネットワーク機器（VPN 等）の設定や運用の点検
(2) Active Directory の各種ログ保存設定の見直し、侵害兆候に関するアラート設定等の導入
(3) 不要な管理者アカウントや権限の削除

配信予定日：2025 年 10 月 24 日(金) 14:00 頃
カテゴリ：基礎から学ぶ！ セキュリティ
タグ：＃初級編＃実用編＃知識編
過去記事焼き直し：する（過去記事を上書きします）
過去記事： https://cybersecurity-taisaku.metro.tokyo.lg.jp/basics/kisokaramanabu11/

タイトル：
中小企業におけるセキュリティ脅威への対策強化　～標的型攻撃による機密情報の窃取から対策を学ぶ～

目次：

独立行政法人情報処理推進機構（IPA）が毎年発行している「情報セキュリティ 10 大脅威 2025」から、中小企業の経営者やシステム担当者が注目すべき点を掘り下げていきます。
今回は 5 位に挙げられている「**標的型攻撃による機密情報の窃取**」を深掘りします。
標的型攻撃とは、特定の組織（企業、官公庁、民間団体等）を狙う攻撃のことです。機密情報等の窃取や業務妨害を目的としています。
攻撃者は、社会の動向や慣習の変化に合わせて攻撃手口を変えます。また、標的とする組織の状況に応じた巧妙な攻撃手法で目的を果たそうとします。
この脅威がどのように業務に影響を与えるのか、対策はどうすべきなのかを解説いたします。

引用元：IPA　情報セキュリティ 10 大脅威 2025 解説書

１．標的型攻撃による機密情報の窃取の脅威

特定の組織や企業に狙いを定め、機密情報等の窃取や業務妨害を目的とした標的型攻撃が確認されています。

この種の攻撃は、明確な目的を持ち、PC やサーバーをウイルスに感染させたり、不正にアクセスすることで組織内部に侵入し、情報窃取や破壊活動等を行います。

これらの攻撃は一時的なもので終わることは少なく、組織内に長期間潜伏して活動を行うケースがあります。

窃取された機密情報が悪用された場合、企業の事業継続や国家の安全保障に重大な影響を及ぼすおそれがあります。

さらに、データ削除やシステム破壊により企業活動が妨害されたり、その企業のサプライチェーンに属する関連組織が攻撃の踏み台にされるおそれもあります。

組織の規模や業種に関わらず標的となる可能性があることが特徴と言えます。

２．代表的な攻撃例

以下に、代表的な標的型攻撃による機密情報の窃取例を紹介します。

（１）フィッシングメールによる感染

攻撃者は、業務や取引に見せかけた巧妙な偽装メールを送信し、そのメールの添付ファイルや本文のリンクにマルウェアを仕込みます。受信者がファイルを開封したり、リンクにアクセスすると、PC がマルウェア感染する仕組みです。

メールの件名や本文、添付ファイル名は業務や取引に関連するように偽装されているため、偽物と気づきにくいのが特徴です。さらに、実在する組織名が使われる場合もあるため、注

意が必要です。
また、通常の業務メールのやり取りを装い、複数回のやり取りを経て油断させる手口もあります。顧客や取引先とのやり取りの中であっても、気軽にリンクを開く、ファイルを開くといった行為は危険を伴うものだという意識を持つ必要があります。

（２）脆弱性を突いた不正アクセス

攻撃者は、標的組織が利用するクラウドサービスや Web サーバー、VPN 装置等の脆弱性を悪用して不正アクセスを行い、組織内部へ侵入します。
この侵入が成功し、正規の認証情報等を窃取できた場合は、次回から正規の経路で組織のシステムへ再侵入することもあります。

（３）改ざんされた Web サイトを利用した攻撃（水飲み場型攻撃）

攻撃者は、標的とする組織が頻繁に利用する Web サイトを調査し、予め改ざんしておきます。
そして、標的組織の従業員や職員がその Web サイトにアクセスすることで、偽装したマルウェアをインストールさせ PC を感染させます。これにより、標的組織は通常の業務活動を行っている際にウイルスに感染し、その結果として情報が盗まれることとなります。この攻撃手法は「水飲み場型攻撃」とも呼ばれ、無意識の間に感染が進行するため、非常に巧妙な手口です。

３．標的型攻撃による機密情報の窃取事例

【事例１：マルウェア感染による情報漏えい】

2024 年 3 月、IT ベンダーF 社にて情報漏えいが発生しました。原因はマルウェアによるものと見られ、業務用 PC1 台の感染に端を発し、最終的に 49 台の業務用 PC に感染が拡大しました。このマルウェアは様々な偽装を行って検知されにくくするなど高度な手法を用いていたため、発見が非常に困難でした。また、通信ログや操作ログを確認したところ、ファイルが社外に持ち出されたおそれがあり、その一部に個人情報や顧客の業務に関連する情報が含まれていたことも判明しています。ただし、情報が悪用されたという報告は受けていないとのことでした。
参照元：IPA　情報セキュリティ 10 大脅威 2025 解説書

【事例２：日本の暗号資産関連事業者へのサイバー攻撃】

2024 年 5 月、某国当局の下部組織の一部とされるサイバー攻撃グループが、D 社から約 482 億円相当の暗号資産を窃取しました。サイバー攻撃グループ はリクルーターを装い、暗号資産ウォレットソフトウェアを開発する 企業の従業員に、採用前試験を装い悪意あるスクリプトを送付し、その従業員の PC の情報を窃取しました。その後、この従業員になりすまし、システムに不正アクセスした上で、D 社の暗号資産を盗み出していたとのことです。
参照元：IPA　情報セキュリティ 10 大脅威 2025 解説書

このように、PC1 台のマルウェア感染から被害が広がったもの、悪質なスクリプト送付による不正アクセスやなりすましなど、さまざまな手法による標的型攻撃が実際に起こっています。

４．標的型攻撃への対策

標的型攻撃による機密情報の窃取への対策を、「経営者の観点」「セキュリティ管理者・システム管理者の観点」「従業員・職員の観点」で説明します。

（１）経営者の観点

◇組織としての体制の確立

・インシデント対応体制を整備し、実際のインシデント時に対応します。※

（２）セキュリティ管理者・システム管理者の観点

◇被害の予防および被害に備えた対策

・情報の管理と運用規則策定
　情報は暗号化するなどの管理や運用の規則を定めて運用します。
・サイバー攻撃に関する継続的な情報収集
・情報リテラシー、モラルを向上させます※
・インシデント対応の定期的な訓練を実施
　関係者やセキュリティ業者、専門家と迅速に連携する対応方法や連絡方法を整備します。
・サーバーやクライアント、ネットワークに適切なセキュリティ対策を行います。※
・アプリケーション許可リストの整備
・取引先のセキュリティ対策実施状況の確認
　サプライチェーンや委託先を狙った攻撃への対策状況を確認します。
・海外拠点等も含めたセキュリティ対策の向上

◇被害の早期検知

・サーバーやクライアント、ネットワークに適切なセキュリティ対策を行います※

◇被害を受けた後の対応

・インシデント対応体制を整備し、実際のインシデント時に対応します※

（３）従業員・職員の観点

◇被害の予防および被害に備えた対策（通常、組織全体で実施）

・IPA の「情報セキュリティ 10 大脅威 2025 解説書」の 9 ページ、表 1.4「情報セキュリティ対策の基本」＋αを実施

表 1.4 情報セキュリティ対策の基本+α

備える対象	情報セキュリティ対策の基本＋α	目的
クラウドの選定	選定前の事前調査	クラウドサービスのガイドラインに沿った運営をしている業者やそのサービスを選定する[3]
インシデント全般	責任範囲の明確化（理解）	クラウドサービスを契約する際は、インシデント発生時に誰（どの組織）がどこまでインシデント対応する責任があるのかを明確化（理解）する
クラウドの停止	代替案の準備	業務が停止しないように代替策を準備する
クラウドの仕様変更	設定の見直し	更新情報は常に確認し、仕様変更により意図せず変更された設定は適切な設定に修正する（設定不備により発生する情報漏えいや攻撃を防止する。）

・メールの添付ファイル開封、メールや SMS のリンク、URL のクリックを安易にしない※

◇被害を受けた後の対応

・インシデント対応体制を整備し、実際のインシデント時に対応します※

「※」の詳細については、IPA の「情報セキュリティ 10 大脅威 2025 解説書」の 36 ページの「共通対策」をご参照ください。

ここまで標的型攻撃による機密情報の窃取について考えてきましたが、いかがだったでしょうか。

ネットワーク内部へ不正アクセスされた場合、情報の漏えいや改ざん、他組織への攻撃の踏み台（中継）になるおそれがあるため、日々の確認や平時の備えが大切なことがおわかりいただけたかと思います。

標的型攻撃による機密情報の窃取は、業種や企業の大小に関わらず発生します。

「自社は狙われないから大丈夫」と考えるのではなく、常にこのような脅威が存在することを認識することが重要です。この認識がセキュリティ意識の向上につながり、企業の持続可能な発展を支える鍵となります。

５．事例

事例を見る

１．個人情報を含む情報漏えいのおそれについて（IT ベンダーF 社）

２．D社ビットコインの不正流出、某国グループが関与＝警察庁（ロイター）

※本記事は令和 6 年度中小企業サイバーセキュリティ対策事業で制作された記事を最新情報等で更新したものです。

配信予定日：2025 年 10 月 31 日(金) 14:00 頃
カテゴリ：3 分でわかる!用語解説
タグ：＃初級編＃用語編＃知識編
過去記事焼き直し：しない（新規記事です）
記事 URL（新設します）：https://cybersecurity-taisaku.metro.tokyo.lg.jp/glossary/yogokaisetu21/

「クリックフィックス」

目次

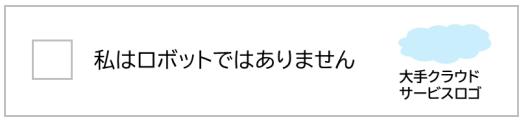
サイバーセキュリティの基本を理解するためには、いくつか重要なセキュリティ用語を知っておくことが必要です。
これらの言葉や概念を正確に理解することで、企業が直面するリスクを最小限に抑え、適切な対策を講じることができます。
本記事では、中小企業が特に知っておくべきセキュリティ用語について解説しています。

今回のテーマは、「クリックフィックス」です。

●クリックフィックスとは
ウェブサイトを閲覧する際、次の画面に進むための操作に見せかけ、マルウェアに感染させるソーシャルエンジニアリングのひとつの手口です。

ソーシャルエンジニアリングとは「人間の心理的な隙や信頼を悪用して、情報や行動を引き出す手口」です。著名なものとしてはフィッシングメールがあります。

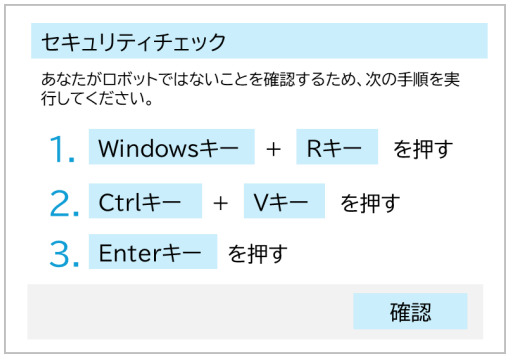
●クリックフィックスの手口
以下のような画面を見たことがないでしょうか。



この画面はウェブサイトを閲覧している際、次の画面に進むために表示される認証画面で

す。
正規の認証画面は、人間と自動化（ボット）を区別して悪意ある自動処理を防ぐ目的で利用されています。例えば問い合わせや投票といった入力操作を自動的に大量に行われることを防ぎます。しかし、あたかも正規の認証画面のように偽り、利用者をマルウェアに感染させようとする偽の認証画面の存在が確認されています。

偽の認証画面をチェックしてしまうと、次のような画面が表示されます。



上記の通りに操作をすると、パソコンがマルウェアに感染してしまいます。

手順１は、Windows において「ファイル名を指定して実行」のダイアログが開く操作です。
手順２は、クリップボードの内容（※）が「ファイル名を指定して実行」ダイアログに貼り付けされます。
手順３は、貼り付けされたものが実行されます。

「※」の部分が重要です。実は上記画面を表示した際に、クリップボード（テキストを選択し右クリックしてメニューからコピーを選択した際等に、一時的に選択した内容を保存する機能）にスクリプトが格納されています。このスクリプトは、マルウェアをダウンロードしたり実行したりするためのコンピュータを動作させる命令文です。
一連の操作は、パソコンの操作者本人が行うものであるため、セキュリティ対策ソフト等の機能を回避する可能性があります。

利用者が「疑問はない」、「次の画面が表示される時間を優先し疑うことをやめる」、「大手企業のロゴなので信頼できる」と考えることにより、画面に表示された通りの操作をしてしまう。そうした人間の心理的な隙や信頼を利用した手口です。

●クリックフィックスへの対処方法
従業員向けにクリックフィックスについての教育をしましょう。
クリックフィックスは、ウェブサイト閲覧時に正規に行われていることを巧妙に真似てい

るため、今後も様々なパターンが登場する可能性があります。しかし、主な手口や偽画面を知る事や、キー入力を指示された際に疑う事、疑った際は報告・確認する事を学ぶ事は有効です。例えば、クリックフィックスの最新の手口をインターネット検索で調べて紹介し、特定のキーを入力するような画面が表示されたら情報システム担当者へ報告し確認するよう周知するとよいでしょう。

技術的対策としては、EDR のようなパソコンの意図しない処理を検知する事が有効です。EDR については過去の記事を参照してください。
https://cybersecurity-taisaku.metro.tokyo.lg.jp/glossary/yougokaisetu2/
なお、東京都中小企業サイバーセキュリティ基本対策事業では EDR のお試し導入を行っております。今年度は定員に達しましたが、来年度事業が行われる可能性があります。事業開始は東京都産業労働局の公式 X や中小企業向けサイバーセキュリティ対策の極意のページに掲載されますのでフォローやブックマークへの登録をお願いいたします。

●まとめ
クリックフィックスは、ウェブサイトを閲覧する従業員に対し、人間の心理的な隙や信頼を悪用してパソコンをマルウェアに感染させるなどの被害を与える手口です。
マルウェアに感染させる手口はメールによる感染が認知されていますが、今回のようなウェブサイトによる感染もあります。クリックフィックスは巧妙で、ウェブサイト上の様々なものをコピーして偽画面を作れてしまいます、今回例示した認証画面だけでなく、「９つの画像から橋の画像を選ぶ」「リモート会議ツールの不具合解消を騙るポップアップ」なども確認されています。最新の情報を収集しつつ、従業員教育や技術的対策の導入を進める事が重要です。

参考
トレンドマイクロ「ClickFix（クリックフィックス）とは？多様な攻撃に悪用されるソーシャルエンジニアリングの手口」
https://www.trendmicro.com/ja_jp/jp-security/25/i/securitytrend-20250905-01.html
当記事内の画像（クリックフィックス手口で利用される偽画面）は、上記サイトを参考に簡略化したイメージを作成し掲載しています。

配信予定日：2025 年 10 月 31 日(金) 14:00 頃
カテゴリ：基礎から学ぶ!セキュリティ
タグ：＃知識編＃用語編＃実用編
過去記事焼き直し：する
記事 URL：https://cybersecurity-taisaku.metro.tokyo.lg.jp/basics/kisokaramanabu12/

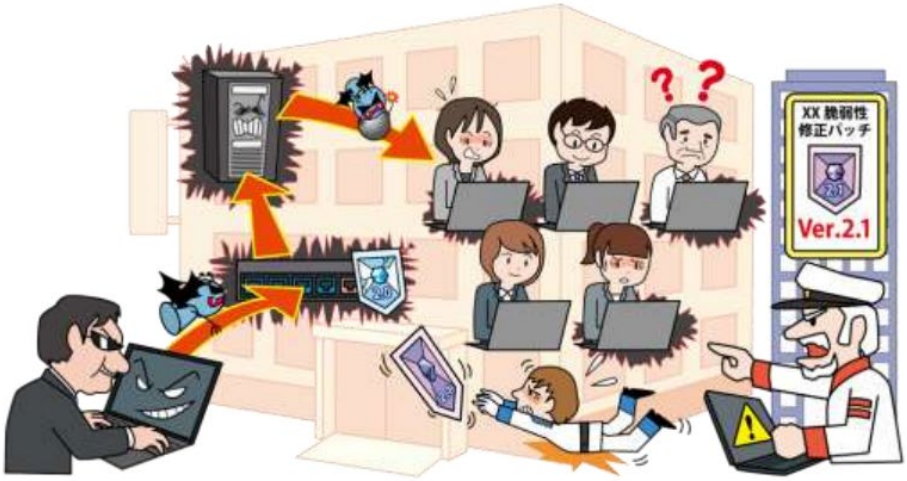
タイトル
【令和７年度版】中小企業におけるセキュリティ脅威への対策強化　～修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）から対策を学ぶ～

目次

独立行政法人情報処理推進機構（IPA）が毎年発行している「情報セキュリティ 10 大脅威 2025」から、中小企業の経営者やシステム担当者が注目すべき点を掘り下げていきます。

今回は３位に挙げられている「システムの脆弱性を突いた攻撃」の中から「ゼロデイ攻撃」について事例とともに深掘りします。(2024 年の５位「修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃)」と、７位「脆弱性対策情報の公開に伴う悪用増加」が統合され、３位にランクインしました)

１．ゼロデイ攻撃とは
ゼロデイ攻撃とは、システムやソフトウェアの脆弱性に対して、開発ベンダー等が認知もしくは修正プログラムを提供する前に行われる攻撃です。
ゼロデイ攻撃が行われた場合、ウイルス感染や情報漏えい等の直接の被害に留まらず、事業やサービスが停止するなど、多くのシステムやユーザーに影響が及ぶことがあります。
そのため企業には、脆弱性対策情報が公開された場合、早急な対応が求められます。



引用元：IPA　情報セキュリティ 10 大脅威 2025 解説書より

２．ゼロデイ攻撃による脅威

OSやアプリケーション等のソフトウェアの脆弱性が発見されると、開発ベンダー等が調査・分析し、修正プログラム（パッチ）や対策情報を公開します。

しかし、脆弱性対策情報の公開前に攻撃者が脆弱性の存在を知った場合、当該ソフトウェアの脆弱性を悪用したゼロデイ攻撃を仕掛けるおそれがあります。

ゼロデイ攻撃が行われると、ウイルス感染や情報漏えい、Web ページやファイルの改ざん等の被害が発生し、事業やサービスが停止する可能性があります。

また、多くのシステムやユーザーに利用されているソフトウェアの脆弱性がゼロデイ攻撃に悪用された場合、被害が広範囲に及び、社会が混乱状態に陥るおそれもあります。

未知の脆弱性を悪用した攻撃を受けた場合は、被害者が攻撃されたことに気付かないケースもあります。

仮に攻撃に気付いたとしても、脆弱性の対策情報が公開されていないために、適切な対応を取れないことが想定されます。

ユーザー側がパッチを未適用状態の N デイ脆弱性*1 を悪用するケースとは異なり、脆弱性対策情報が公開されてはいるものの、ゼロデイ攻撃への対策を行うことは非常に困難です。

*1 N デイ脆弱性：

すでに公開されている脆弱性で、ベンダーや開発者等がパッチを提供もしくは作成中でユーザーは実装を待っている状態のもの。次回で詳しくご説明します。

３．代表的な攻撃例

ソフトウェアの脆弱性の悪用

開発ベンダー等が脆弱性対策情報を公開する前に、攻撃者はその脆弱性を悪用して攻撃します。

悪用の手口は、脆弱性によって異なります。例えば、通信プロトコルの脆弱性を悪用した

DDoS 攻撃（分散型サービス妨害攻撃）*2、アプリケーションの脆弱性を悪用した簡易プログラム（スクリプト）の実行、OS の脆弱性を悪用した特権アカウントの作成等があります。

***2 DDoS（Distributed Denial of Service）攻撃：**

攻撃対象となる Web サーバーなどに対し、複数のコンピューターから大量のパケットを送りつけることで、正常なサービス提供を妨げる行為を指します。

４．ゼロデイ攻撃の事例

【事例１：P 社製機器の OS の脆弱性を悪用したゼロデイ攻撃】

2024 年 4 月 12 日（米国時間）、P 社は同社製品 OS の某機能において、認証されていない遠隔の第三者によって、root 権限で任意のコード実行ができる脆弱性があることを公表、この脆弱性を悪用したゼロデイ攻撃も確認されました。この脆弱性は、深刻度（CVSS v3.0）のベーススコアが最大の 10.0 と評価され、脆弱性を悪用した攻撃が国内外で確認されました。他方、IPA、JPCERT/CC からは、侵害調査 の推奨等の注意喚起が行われました。

参照元：IPA　情報セキュリティ 10 大脅威 2025 解説書

【事例２：C 社製品へのゼロデイ攻撃】

2023 年 10 月、C 社は同社製品にリモートから認証がなくとも特権アカウントを作成できる脆弱性があり、9 月中旬よりゼロデイ攻撃が行われていたと公表しました。

同社は、顧客のサポート中に本脆弱性を確認しており、本製品の利用者に対して開発ベンダー等が推奨する対策を講じるとともに、侵害を受けていないか確認するように呼びかけています。

これらは典型的なゼロデイ攻撃の事例です。ほとんどの場合、脆弱性による攻撃の被害が出てからでないと、脆弱性の存在に気が付かず対策が打てないことがお判りになるかと思います。

５．ゼロデイ攻撃への対策

ゼロデイ攻撃への対策を、「経営者の観点」「管理者の観点」で説明します。

（１）経営者の観点

◇被害の予防

・インシデント対応体制を整備し、実際のインシデント時に対応します※

（２）管理者（セキュリティ担当者・システム管理者）の観点

◇被害の予防

・IPA の「情報セキュリティ 10 大脅威 2025 解説書(組織編)」の 9 ページ、表 1.4「情報セキュリティ対策の基本」＋α を実施

表 1.4 情報セキュリティ対策の基本+α

備える対象	情報セキュリティ対策の基本＋α	目的
クラウドの選定	選定前の事前調査	クラウドサービスのガイドラインに沿った運営をしている業者やそのサービスを選定する[3]
インシデント全般	責任範囲の明確化（理解）	クラウドサービスを契約する際は、インシデント発生時に誰（どの組織）がどこまでインシデント対応する責任があるのかを明確化（理解）する
クラウドの停止	代替案の準備	業務が停止しないように代替策を準備する
クラウドの仕様変更	設定の見直し	更新情報は常に確認し、仕様変更により意図せず変更された設定は適切な設定に修正する（設定不備により発生する情報漏えいや攻撃を防止する。）

・資産の把握、対応体制の整備
・セキュリティのサポートが充実しているソフトウェアやバージョンを使用します
・修正プログラムや回避策の提供が迅速である製品や開発ベンダーを利用し、サポート対象のソフトウェアを使用します
・利用するソフトウェアの脆弱性情報の収集と周知、対策状況の管理
・サーバーやクライアント、ネットワークに適切なセキュリティ対策を行います※
◇被害の早期検知
・サーバーやクライアント、ネットワークに適切なセキュリティ対策を行います※
◇修正プログラムのリリース前の対応
・回避策や緩和策の適用
・当該ソフトウェアの一時的な使用停止。場合によってはサービスの停止も検討します
◇修正プログラムリリース後の対応
・修正プログラムの適用。必要に応じて回避策、緩和策を無効化します
◇被害を受けた後の対応
・影響調査および原因の追究、対策の強化
・適切な報告／連絡／相談を行います※
「※」の詳細については、IPA の「情報セキュリティ 10 大脅威 2025 解説書」の 36 ページの「共通対策」をご参照ください。

ここまでゼロデイ攻撃について考えてきましたが、いかがだったでしょうか。
ゼロデイ攻撃は基幹となる重要ソフトウェアの未解決な脆弱性を狙う攻撃のため、利用者側で完全に防ぐことは困難です。

自社で使用しているソフトウェアの修正プログラムが各端末で適用されているのか、定期的に確認を行い、適切なセキュリティ対策を導入しましょう。たとえ攻撃を受けたとしても対処できるよう、事前の準備が重要になると言えます。
常にこのような脅威への準備を万全にすることが、企業の持続可能な発展を支える鍵となります。

６．事例

事例を見る

1. P 社製 OS コマンドインジェクションの脆弱性に関する注意喚起
2. 「IOS XE」の深刻なゼロデイ脆弱性 - JPCERT/CC も攻撃被害を確認（Security NEXT）

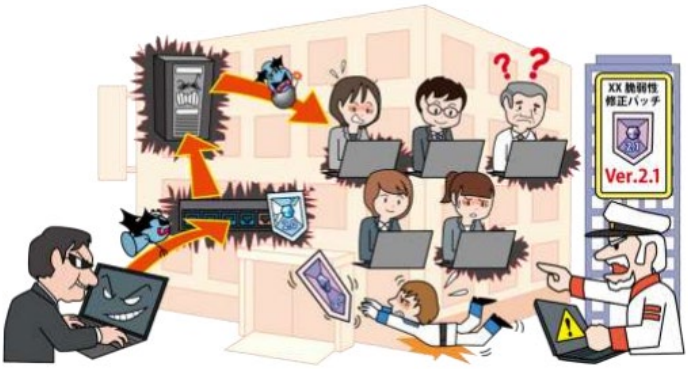
※本記事は令和 6 年度中小企業サイバーセキュリティ対策事業で制作された記事を最新情報等で更新したものです。

配信予定日：2025 年 10 月 31 日(金) 14:00 頃
カテゴリ：基礎から学ぶ！セキュリティ
タグ：＃実用編＃用語編＃知識編
過去記事焼き直し：する（過去記事を上書きします）
過去記事：https://cybersecurity-taisaku.metro.tokyo.lg.jp/basics/kisokaramanabu13/

【令和 7 年度版】中小企業におけるセキュリティ脅威への対策強化　～システムの脆弱性を突いた攻撃への対策を学ぶ～

目次

独立行政法人情報処理推進機構（IPA）が毎年発行している「情報セキュリティ 10 大脅威 2025」から、中小企業の経営者やシステム担当者が注目すべき点を掘り下げていきます。
今回は 3 位に挙げられている「システムの脆弱性を突いた攻撃」に焦点を当てます。(2024 年の 5 位「修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）」と、7 位「脆弱性対策情報の公開に伴う悪用増加」が統合され、3 位にランクインしました）
ソフトウェアやハードウェアの脆弱性対策情報の公開には、利用者に対して脆弱性の脅威やその対策方法を知らせるという利点があります。
しかし一方で、その公開された情報は悪意ある攻撃者にとっても貴重な攻撃の手がかりとなり得るのです。
攻撃者はその情報を悪用し、脆弱性対策を講じていない当該製品を使用したシステムを狙って攻撃を行う恐れがあります。
近年では、ゼロデイ／N デイ攻撃（それぞれの定義については後述します）の境界が曖昧になり、脆弱性情報の公開後すぐに悪用される傾向が強まっているため、細心の注意を払って、最新の情報を入手する必要があると言えます。



引用元：IPA　情報セキュリティ 10 大脅威 2025 解説書より

１．脆弱性対策情報の公開に伴う悪用増加による脅威

一般的に、OS やアプリケーション等のソフトウェアに脆弱性が発見された場合、開発ベンダーが脆弱性の修正プログラム（パッチ）を作成します。

その後、ベンダーはセキュリティ対応機関等と連携するか、または自身で脆弱性対策情報として脆弱性の内容とパッチや対策方法、暫定対策情報を一般に公開し、当該ソフトウェアの利用者へセキュリティ脅威への対策を促します。

一方攻撃者は、公開された脆弱性対策情報を基に攻撃コード等をいち早く作成し、パッチ適用等のセキュリティ対策を実施する前のソフトウェアに対して、脆弱性を悪用した攻撃を行います。（N デイ攻撃）

これによるマルウェア感染や情報漏えい、Web ページやファイルの改ざん等の被害の発生が確認されています。

特にネットワーク機器(VPN 機器)やコンテンツ管理システム(プラグインを含む CMS) 等、広く利用されている製品の脆弱性の場合には、脆弱性情報が公開されると瞬く間に多くの攻撃の対象となる危険性があります。

昨今、脆弱性が発見されてからそれを悪用した攻撃が発生するまでの時間が短くなっており、より迅速な対応が求められています。

２．代表的な攻撃例

（１）公開される前の脆弱性を悪用（ゼロデイ攻撃）

開発ベンダー等が脆弱性対策情報を公開する前に、攻撃者が脆弱性を悪用して行う攻撃をゼロデイ攻撃と呼びます。悪用の手口は、脆弱性毎に様々ですが、例えば、ネットワーク機器の脆弱性を悪用した遠隔での任意のコード実行が挙げられます。

（２）製品利用者が対策する前の脆弱性を悪用（N デイ攻撃）

パッチや回避策が公開され、そのパッチの適用や回避策を講じるまでの期間の

脆弱性を N デイ脆弱性と呼び、これに対するサイバー攻撃をNデイ攻撃と呼びます。ソフトウェアの脆弱性管理が不適切な場合、未対策の期間が長くなり、被害に遭うリスクも大きくなります。
加えて、その脆弱性が確かであることを示す実証コード（PoC）※が公開されることもあり、このコードが攻撃に悪用されることも少なくありません。
※PoC(Proof of Concept)：脆弱性が新たに発見された場合に、プログラムに潜む問題点を明確にする（＝実証する）ために用意されたコードを意味します。
（ゼロデイ攻撃の詳細はこちらの記事「中小企業におけるセキュリティ脅威への対策強化　～修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）から対策を学ぶ～」を参照してください）

（２）公開されている攻撃ツールの使用
公開された脆弱性に対する攻撃ツールは短期間で作成され、ダークウェブ上で取引されたり、攻撃サービスとして提供されたりすることがあります。
また、誰でも利用可能なオープンソースのツールに脆弱性を利用する機能が実装され、それを悪用されることもあります。

３．脆弱性悪用の具体的事例
【事例１：P社製 PAN-OS の機能の脆弱性を悪用したゼロデイ攻撃】
2024 年 4 月 12 日（米国時間）、P社は、PAN-OS の GlobalProtect 機能において、認証されていない遠隔の第三者によって、root 権限で任意のコード実行ができる脆弱性があることを公表しました。また、この脆弱性を悪用したゼロデイ攻撃も確認されています。この脆弱性は、深刻度
（CVSS v3.0）のベーススコアが最大の 10.0 と評価され、脆弱性を悪用した攻撃が国内外で確認されました。他方、IPA、JPCERT/CC からは、侵害調査の推奨等の注意喚起も行われました。

【事例２：Windows 上の PHP の脆弱性を悪用した攻撃】
2024 年 6 月、Windows 上で動作する CGI モードの PHP に OS コマンドインジェクションの脆弱性があることが報じられました。この脆弱性は、既存の脆弱性（CVE-2012-1823）に対する保護を回避できるというものです。この脆弱性が悪用され、webshell が設置されるといった被害や、ランサムウェア「TellYouThePass」の感染活動に悪用されたことも確認されています。
また、IPA からは、修正プログラムの適用等の注意喚起が行われました。

【事例３：太陽光発電施設の遠隔監視機器に対する攻撃】

2024 年 5 月、C 社製の太陽光発電施設向け遠隔監視機器がサイバー攻撃を受け、不正送金の踏み台として悪用されたことを一部の報道機関が報じました。この攻撃との関係性は不明ですが、C社製品に関する脆弱性の一部(CVE-2022-29303 等）については、米国サイバーセキュリティ・インフラストラクチャセキュリティ庁の「既知の悪用された脆弱性カタログ」（KEV）に掲載されています。なお、コンテックからは、複数回の注意喚起（アップデートの推奨等）が行われていました。

これらは脆弱性を悪用した、ゼロデイ攻撃、N デイ攻撃の事例です。
脆弱性対策ができていない場合、マルウェア感染等に留まらず、事業やサービスの停止等に端を発し、甚大な被害に至ることもあります。近年は脆弱性が発見されてから、それを悪用した攻撃が発生するまでの時間が短くなっているため、脆弱性対策情報が公開された場合、早急な対策の実施が求められます。

４．脆弱性対策情報の公開に伴う悪用への対策
脆弱性対策情報の公開に伴う悪用への対策を、「経営者の観点」「管理者（セキュリティ担当者・システム管理者）の観点」で説明します。
（１）経営者の観点
◇被害の予防
・インシデント対応体制を整備し、対応します※
・パッチ適用や回避策を講じるための予算を確保します
（２）管理者（セキュリティ担当者・システム管理者）の観点
◇被害の予防
・IPA の「情報セキュリティ 10 大脅威 2025 解説書」の 9 ページ、表 1.3「情報セキュリティ対策の基本」を実施します

表 1.3 情報セキュリティ対策の基本

攻撃の糸口	情報セキュリティ対策の基本	目的
ソフトウェアの脆弱性	ソフトウェアの更新	脆弱性を解消して脆弱性を悪用した攻撃によるリスクを低減する
マルウェアに感染	セキュリティソフトの利用	攻撃を検知してブロックする
パスワード窃取	パスワードの管理・認証の強化 ※「認証を適切に運用する」で詳細を解説	パスワード窃取による情報漏えい等のリスクを低減する
設定不備	設定の見直し	誤った設定を悪用した攻撃をされないようにする
誘導（罠にはめる）	脅威・手口を知る	手口から重視すべき対策を理解する

・セキュリティのサポートが充実しているソフトウェアやバージョンを使うようにします。（パッチや回避策の提供が迅速である製品を利用し、サポート対象のソフトウェアを使う）
・最新の脆弱性情報の収集、対策状況の管理、パッチマネジメントを行います
・サーバーや PC、ネットワークに適切なセキュリティ対策を行います
◇被害の早期検知
・サーバーやクライアント、ネットワークに適切なセキュリティ対策を行います※
◇被害を受けた後の対応
・整備した対応体制に基づき対応します
・影響調査および原因の追究、対策を強化します
・適切な報告／連絡／相談を行います※
・インシデント対応体制を整備し対応します※

「※」の詳細については、IPA の「情報セキュリティ１０大脅威 2025」の 36 ページ以降の「共通対策」をご参照ください。
また、インシデント対応体制を整備し対応するための方策については、「もっと知りたい！セキュリティ」の「セキュリティインシデント対応（1/2）」および「セキュリティインシデント対応（2/2）」でも解説しています。こちらも併せて参照してください。

ここまで脆弱性対策情報の公開に伴う悪用増加について考えてきましたが、いかがだったでしょうか。
ゼロデイ／N デイ攻撃の境界が曖昧になり、脆弱性情報の公開後すぐに悪用される傾向が強まっているため、利用者側で速やかに適切な対応策を講じることが求められています。
自社で使用しているソフトウェアの修正プログラムが各端末で適用されているかを定期的に確認し、適切なセキュリティ対策を日々継続する事が重要になると言えます。
これらの対策を行うことで、脆弱性を狙ったセキュリティ脅威に対してより強靭な防御を構築し、業務を安全に日々継続できることが、企業の持続可能な発展を支える鍵となります。

５．事例
事例を見る
１．Cisco ASA および FTD における複数の脆弱性（CVE-2025-20333、CVE-2025-20362）

に関する注意喚起（JPCSERT/CC）

２．NetScaler ADC および NetScaler Gateway の脆弱性について（CVE-2025-7775 等）| 情報セキュリティ | IPA 独立行政法人 情報処理推進機構（IPA）

３．Apple 0-Day 脆弱性 CVE-2025-43300 が FIX：ゼロクリック RCE の PoC も公開 – IoT OT Security News（IoT OT Security News）

４．CVE-2025-0411：ウクライナの組織を標的としたゼロデイ攻撃キャンペーンとホモグリフ攻撃 | トレンドマイクロ | トレンドマイクロ（JP）（TREND MICRO）

※本記事は令和 6 年度中小企業サイバーセキュリティ対策事業で制作された記事を最新情報等で更新したものです。

配信予定日：2025 年 11 月 7 日(金) 14:00 頃
カテゴリ：もっと知りたい！ セキュリティ
タグ：＃知識編
過去記事焼き直し：しない（新規記事です）
記事 URL（新設します）：https://cybersecurity-taisaku.metro.tokyo.lg.jp/know_more/zeijyakusei-kanri-sikumi/

脆弱性を識別・評価・管理する仕組み

目次

中小企業の経営者や情報システム担当者の皆さん、日々のセキュリティ対策、お疲れ様です。サイバー攻撃により被害を受けるリスクを最小化するためには、組織や情報システム等のどこに、どのような脆弱性が存在するのか、それによってどのようなリスクを顕在化させることになるのかを認識し、適切に対処する必要があります。今回は、組織で利用する IT 製品等の脆弱性を認識してその影響度等を評価し、管理する上で知っておいていただきたい基準や仕組み等について解説します。

●組織における脆弱性の例
「セキュリティ対策における基本的な考え方」の回で解説したように、脆弱性は組織や情報システム等に内在する様々な弱点や欠陥ですが、自助努力によって取り除いたり、低減させたりすることが可能です。一般的に、組織における脆弱性には次のようなものがあります。

組織における脆弱性の種類とその具体例

脆弱性の種類	具体例
設備面の脆弱性	・建物の構造上の欠陥 ・設備のメンテナンスの不備 ・入退室管理設備の不備

技術面の脆弱性	・ネットワーク構成における欠陥 ・ソフトウェアのバグ ・アクセス制御システムの不備 ・設定ミス，安易なパスワード ・マルウェア対策の不備
管理面・制度面の脆弱性	・情報セキュリティに関する方針，規程の不備 ・機器や外部記憶媒体管理の不備 ・ユーザ教育，マニュアルの不備 ・インシデント対応計画の不備 ・監視体制，監査の不備

OS やソフトウェアのリリース後に設計ミスやプログラミングミスなどによる欠陥（バグ）が発見されることがありますが、それらの多くが脆弱性となります。市販されているソフトウェア等であれば、脆弱性の影響度や緊急度に応じて開発元が脆弱性を修正するためのプログラム（パッチ）を提供しますが、利用している側の組織がパッチを適用しなければ脆弱性は存在したままとなります。
これ以降は組織で利用する IT 製品における脆弱性管理において、有用な基準や手法等について取り上げます。

●SCAP を構成する 6 つの標準仕様
OS やミドルウェア、ネットワーク機器等の脆弱性については、自社の IT 環境に関係のある情報をいち早く収集し、その緊急度や影響度等を考慮しながら適切に対処することが求められます。
米国の国立標準技術研究所（NIST：National Institute of Standards and Technology）では、情報セキュリティ対策の自動化と標準化を目指して、脆弱性の管理、測定、評価等を自動化するための基準として、セキュリティ設定共通化手順（SCAP：Security Content Automation Protocol）を策定しています。
SCAP は、次の 6 つの標準仕様から構成されています。

SCAP の 6 つの標準仕様

略称	名称	主な用途
CVE	Common Vulnerabilities and Exposures (共通脆弱性識別子)	脆弱性を識別する

CCE	Common Configuration Enumeration (共通セキュリティ設定一覧)	セキュリティ設定を識別する
CPE	Common Platform Enumeration (共通プラットフォーム一覧)	製品を識別する
CVSS	Common Vulnerability Scoring System (共通脆弱性評価システム)	脆弱性の深刻度を評価する
XCCDF	eXtensible Configuration Checklist Description Format (セキュリティ設定チェックリスト記述形式)	チェックリストを記述する
OVAL	Open Vulnerability and Assessment Language (セキュリティ検査言語)	脆弱性やセキュリティ設定をチェックする

●JVN の概要

日本では、組織の脆弱性管理を支援するポータルサイトとして JVN（Japan Vulnerability Notes）があります。

JVN は、国内で使用されている各種製品等の脆弱性関連情報とその対策情報を提供するポータルサイトであり、独立行政法人 情報処理推進機構 （IPA）と JPCERT コーディネーションセンター（JPCERT/CC）とが共同で運営・管理しています。

JVN では、脆弱性関連情報だけでなく、製品開発者との調整を通じ、対策方法や対応状況等の情報も提供しているのが特徴です。

JVN では、脆弱性を識別するための識別子として前述の CVE を採用しています。CVE は個別の製品に含まれる脆弱性を対象としており、米国政府の支援を受けた非営利団体の MITRE 社が採番し管理しています。なお、MITRE 社は「サイバーキルチェーンと MITRE ATT&CK」の回でもご紹介しています。

●CVSS の概要

SCAP の一つである CVSS は、IT 製品の脆弱性に対する製品ベンダー等に依存しないオープンで汎用的な評価手法です。現状では CVSS のバージョン 3 が広く普及していますが、最新版は 2023 年 11 月にリリースされたバージョン 4 です。

CVSS バージョン 3 では、脆弱性を評価するために次の三つの基準を用いています。

①基本評価基準（Base Metrics）

基本評価基準は、脆弱性そのものの特性を評価します。IT 製品の機密性、完全性、可用性に対する影響を、どこから攻撃が可能かといった攻撃元区分や，攻撃する際に必要な特権レベルなどの基準で評価し、CVSS 基本値（Base Score）を算出します。

②現状評価基準（Temporal Metrics）
現状評価基準は、脆弱性の現状の深刻度を評価します。当該脆弱性に対する攻撃コードの出現有無や、対策情報が利用可能であるかといった基準で評価し、CVSS 現状値（Temporal Score）を算出します。

③環境評価基準（Environmental Metrics）
環境評価基準は、IT 製品の実際の利用環境も加味した上で、最終的な脆弱性の深刻度を評価します。当該脆弱性を突いた攻撃による被害の大きさや、対象製品の組織における使用状況といった基準で評価し、CVSS 環境値（Environmental Score）を算出します。

●EPSS と KEV の概要
CVSS とは異なる脆弱性評価の仕組みとして、EPSS（Exploit Prediction Scoring System）や KEV（Known Exploited Vulnerabilities catalog）があり、近年 CVSS に加え、脆弱性管理に活用する組織が増えてきています。
EPSS は、機械学習によって当該脆弱性が今後 30 日以内に悪用される可能性を予測した指標であり、EPSS を開発・運営する FIRST（Forum of Incident Response and Security Teams）のサイトで公開されています。なお、FIRST は、世界中の CSIRT（Computer Security Incident Response Team）コミュニティが情報交換やインシデント対応における協力関係を構築する目的で 1990 年に設立された国際的なフォーラムであり、CVSS の管理も行っています。
KEV は、既知の悪用された脆弱性のリストであり、実際に悪用されたことが確認された脆弱性を米国の CISA（Cybersecurity and Infrastructure Security Agency）が公開しています。

その他、ソフトウェアの脆弱性管理等に活用できるツールとして SBOM（Software Bill Of Materials）があります。SBOM はソフトウェアを構成する各部品（コンポーネント）の名称，ビルド情報，ライセンス情報，互いの依存関係，どのような構成となっているか等を示すリストです。SBOM により，ソフトウェアの構成情報を詳細に把握することができるため，脆弱性情報の即時の特定等が可能となります。

配信予定日：2025 年 11 月 7 日(金) 14:00 頃
カテゴリ：もっと知りたい！ セキュリティ
タグ：＃インシデント対応強化＃知識編
過去記事焼き直し：しない（新規記事です）
記事 URL（新設します）：https://cybersecurity-taisaku.metro.tokyo.lg.jp/know_more/incident-sosikitaisei1/

セキュリティインシデントに備えた組織体制（１／３）

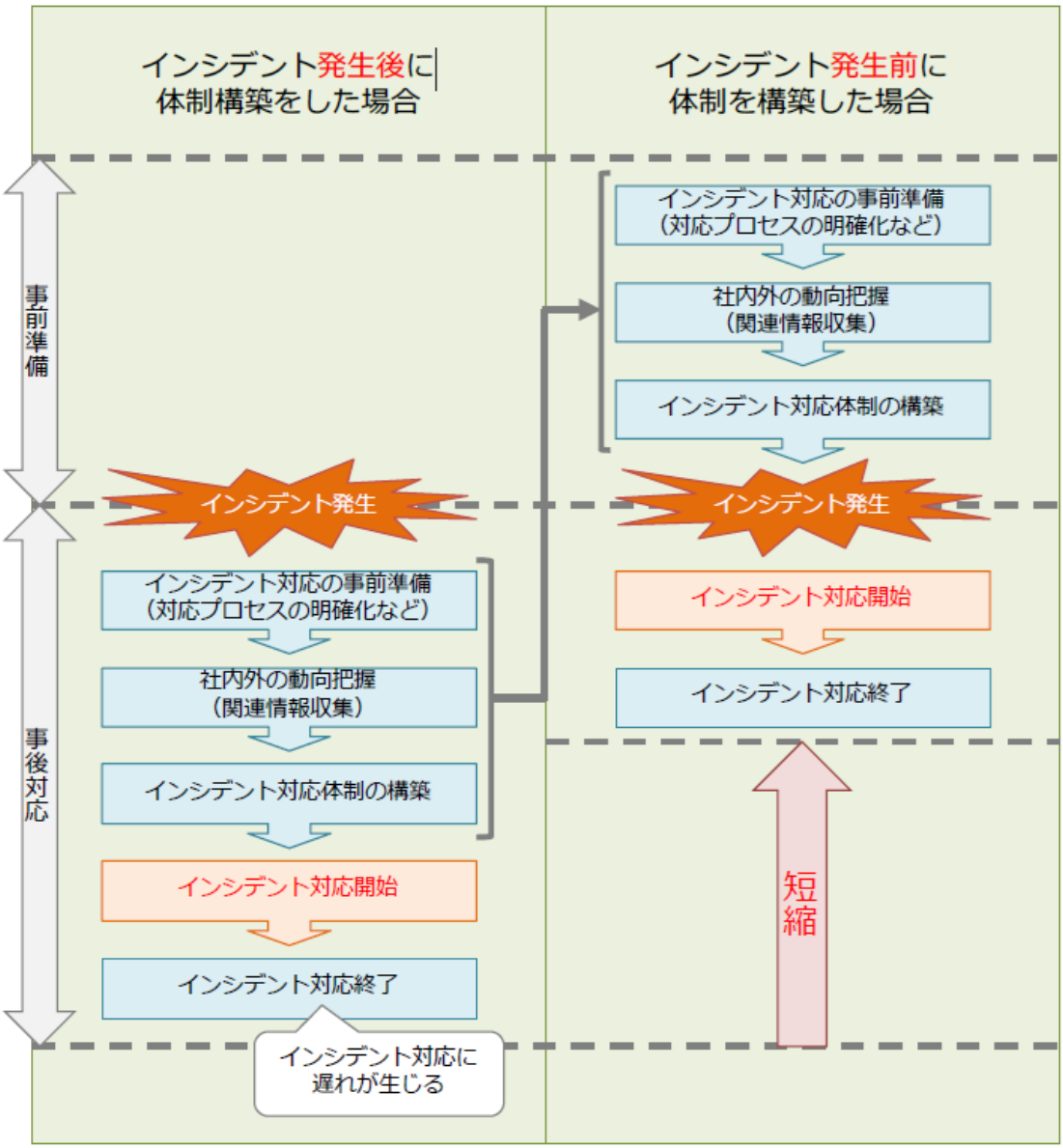
目次

中小企業の経営者や情報システム担当者の皆さん、日々のセキュリティ対策、お疲れ様です。本記事では、セキュリティインシデントに備えた組織体制として、多くの企業で設置・運用が進んでいる CSIRT（シーサート）の役割や期待される効果等について解説します。

●CSIRT の概要

近年、ランサムウェアをはじめとしたサイバー攻撃の脅威が増大しており、企業の業務継続が困難になったり、機密情報や個人情報が流出したりするリスクがますます高まっています。そうしたリスクに対応するため、CSIRT（Computer Security Incident Response Team）を設置・運用する組織が増えています。
なお、広義の CSIRT には、国際連携を行う CSIRT や、CSIRT 間の情報連携を行う「コーディネーションセンター」等も含まれますが、ここでは特定の組織で活動する「組織内 CSIRT」を前提として解説します。
CSIRT には、インシデント発生時にその対応を主導し、情報を集約して顧客、株主、経営者、監督官庁等に適時報告するとともに、現場組織等に適時対応を指示すること等が求められます。
もしインシデント発生後に CSIRT のような体制を構築したとすれば、対応を開始するまでに多くの時間を要し、復旧するまでに多くの損害が発生してしまうことでしょう。一方、インシデント発生前に CSIRT 体制が構築できていれば、発生したインシデントに迅速かつ適切に対応し、その損害や影響を最小化することが可能となります。
JPCERT コーディネーションセンター（JPCERT/CC）が公開している「CSIRT ガイド」には、それをわかりやすく表した次の図が掲載されています。

インシデント発生後に体制構築した場合と発生前に構築した場合の比較イメージ



(https://www.jpcert.or.jp/csirt_material/files/guide_ver1.0_20211130.pdf)

また、CSIRT にはインシデント発生時の対応だけでなく、平常時の活動として、セキュリティに関する最新情報を収集したり、外部のセキュリティベンダーや関連機関、ISAC（Information Sharing and Analysis Center）等の業界団体、他の CSIRT 等と連携して情報を共有したりすることにより、インシデント発生に備えた対応を行うことなども重要な役割です。加えて、インシデント収束後には再発防止のための対応なども求められます。

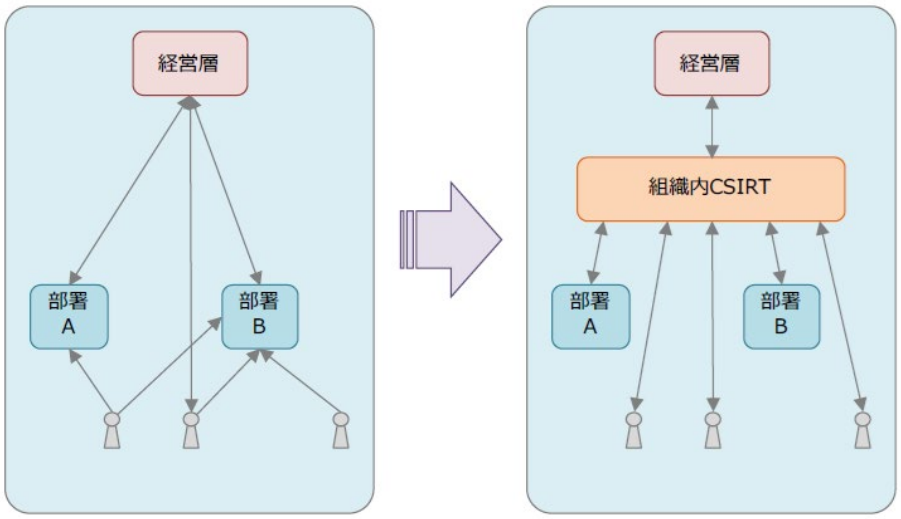
また、CSIRT の一機能、もしくは関連組織として、SOC（Security Operation Center）を設置したり、セキュリティ専門ベンダー等が運営する外部の SOC と契約したりするケースも多くあります。SOC の主な役割は、各種セキュリティ製品からのアラートや、サーバ、ネ

ットワーク機器等のログ分析を行ってインシデントの発生やその兆候等を早期に検知し、CSIRT に適時報告（エスカレーション）することです。

●CSIRT 構築・運用による効果
CSIRT を構築・運用することにより、次のような効果が期待されます。

（1）インシデントに関する情報の一元管理
もし CSIRT が存在しないとすれば、組織内でインシデントが発生した場合、その情報が各部署から個々に経営層に報告/伝達されることになるため、それを経営層が整理して状況を把握しなければならなくなります。また、対応に関する指示についても経営層から各部署に個別に行う必要があります。
一方、CSIRT が設置されていれば、インシデントに関する情報の集約を行うとともに、組織内の関係者に適切に報告/伝達する機能を担うことにより、それに基づいた効果的な対応を行うことが可能となります。

CSIRT を構築・運用することによる効果のイメージ①

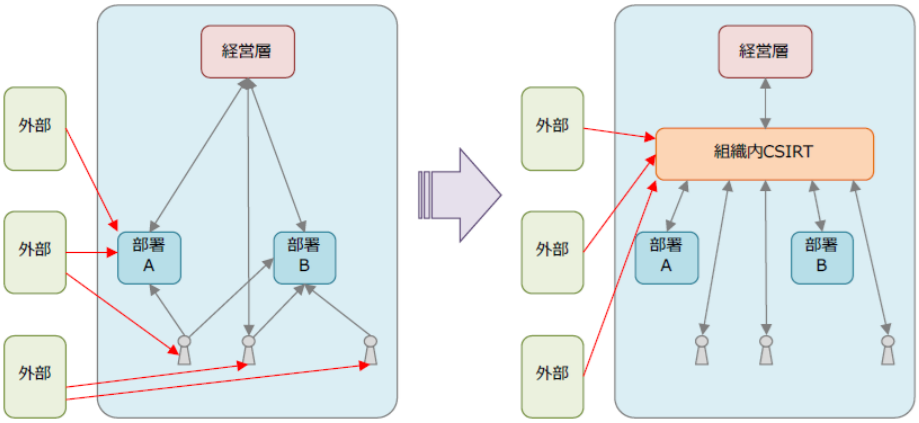


(https://www.jpcert.or.jp/csirt_material/files/guide_ver1.0_20211130.pdf)

（2）インシデントに関する組織内外との統一された窓口
もし CSIRT が存在しないとすれば、自組織で発生したインシデントについて問合せを受ける窓口が不明確であることから、様々な部署や担当者に顧客や取引先から連絡が入ることが考えられます。その結果、連絡を受けた部署や担当者間の連携や関連付けが難しくなり、インシデントへの対応が混乱し、遅れる可能性があります。
CSIRT がインシデントの報告や問合せについての社内外に向けた統一の窓口として機能す

ることで、情報を集約し、それらの関連付けを行うことで、効果的な対応に繋げるとともに、社内外に発するメッセージを統一化することが可能となります。

CSIRT を構築・運用することによる効果のイメージ②



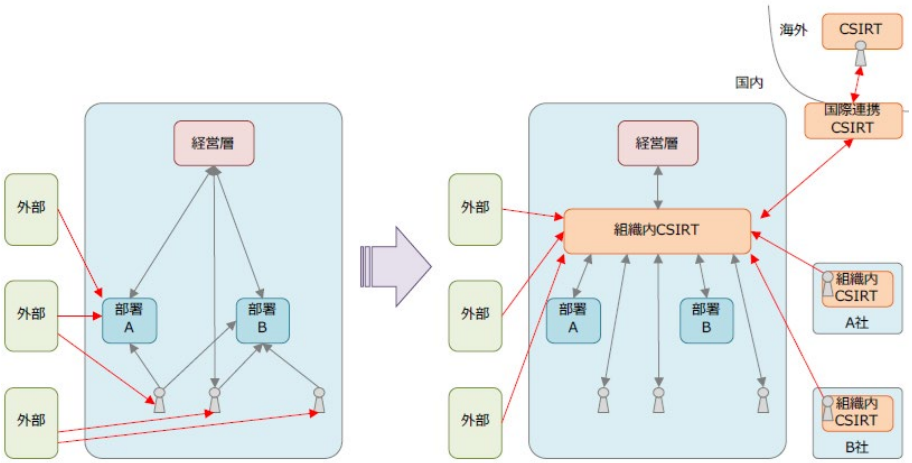
(https://www.jpcert.or.jp/csirt_material/files/guide_ver1.0_20211130.pdf)

（3）インシデント対応に関係する外部組織との信頼関係の構築

インシデントに関する情報を他の組織と共有することで、自組織のインシデント対応に役立てることができます。とはいえ、通常インシデントに関する情報には、その組織にとって機微な情報が含まれているため、外部と共有するのは難しい場合が多いでしょう。それを可能にするには、共有する組織間で信頼関係が築かれていることが前提となります。

もし CSIRT が存在しなければ、他の組織と情報交換するのは各部署の担当者となるため、提供した情報が果たして相手の組織内で適切に扱われるかどうか確信を持てず、信頼関係を築くことはより困難になります。一方 CSIRT があれば、外部に対する「信頼の窓口」として機能することで、組織間の信頼関係を築くことができる可能性が高まります。

CSIRT を構築・運用することによる効果のイメージ③



(https://www.jpcert.or.jp/csirt_material/files/guide_ver1.0_20211130.pdf)

今回はセキュリティインシデントに備えた組織体制として、CSIRT の役割や、構築・運用することによる効果について解説しました。次回以降は CSIRT を核としたインシデント発生時の対応における留意点等について解説します。

配信予定日：2025 年 11 月 7 日(金) 14:00 頃
カテゴリ：もっと知りたい！ セキュリティ
タグ：＃知識編＃実用編
過去記事焼き直し：する（過去記事を上書きします）
過去記事：https://cybersecurity-taisaku.metro.tokyo.lg.jp/know_more/mottosiritai11/

【令和 7 年度版】情報セキュリティの見直しと強化（監査と点検）（1/3）

目次

中小企業の経営者や情報システム担当者の皆さん、日々のセキュリティ対策、お疲れ様です。

本記事では、組織における情報セキュリティ対策への取り組みを評価し、改善へと導くための監査・点検の重要性とその実施方法について説明します。

１．情報セキュリティ対策の重要性と監査・点検の必要性

今日のデジタル社会では、情報セキュリティインシデントが企業に甚大な影響を及ぼすことがあります。特にサイバー攻撃は手口が巧妙化し増加し続けています。このような中で、個人情報や機密情報の保護は企業活動において不可欠です。情報漏えいやシステムダウン等の事態が発生すれば、企業の信頼を失墜させかねません。従って、情報セキュリティ対策は経営戦略の重要な一部であり、定期的な監査と点検によってその有効性を評価し続けることが必要です。

２．監査と点検の役割と違い

「監査」と「点検」という言葉は、情報セキュリティだけでなく、様々な分野で使われています。
「監査」には、会計監査、業務監査、監査役監査などがあります。
「点検」には、自動車の日常点検と定期点検、ガス設備定期保安点検、消防用設備等の点検などがあり、経験がある人も多いのではないでしょうか。

監査と点検は、どちらも何かしらの基準と実際の状態や状況を比較し、そのギャップを確認する行為です。
それぞれの違いについて、明確な定義はありませんが※1、一般的には以下のように区分されています。

用語	範囲	実施主体	特徴
監査	組織全体または特定部門	監査担当者や外部専門家	独立性・客観性を重視
点検	特定の業務や設備	業務や設備の担当者	問題の早期発見･予防を重視

監査は対象業務に従事していない他部署や取引先など、独立した立場の監査担当者によって実施されるものに対し、点検は担当者自身が実施します。
従って、客観的かつ専門的な確認を行う場合には監査が適しており、適時簡易に確認する場合には点検が適しています。
状況に応じて使い分けることで効果的な取り組みとなります。

※1 経済産業省「情報セキュリティ監査基準」では次のように説明しています。
情報セキュリティ監査は、独立かつ専門的な立場から、組織体の情報セキュリティの状況を検証又は評価して、情報セキュリティの適切性を保証し、情報セキュリティの改善に役立つ的確な助言を与えるもの

３．効果的な情報セキュリティ監査・点検の実施方法

情報セキュリティ対策の監査と点検を効果的に進めるためには、以下の事項を確認することがポイントです。

・セキュリティルールの徹底
一般に必要とされる情報セキュリティ対策や組織内で策定されたセキュリティルールを基準とし、これらの対策やルールがしっかりと周知・実行されているか確認します。

・潜在的なリスクの特定
現行のシステムや業務プロセスにおける潜在的なリスクや対策の欠落･漏れ等がないか確認します。不十分な点があれば、必要な改善策を講じます。

・事故防止対策の有効性の検証
現行の対策がセキュリティ事故の防止に役に立っているかを検証し、必要に応じて改善策や

新たな対策の導入を検討します。

監査・点検には、以下の方法があります。

質問(インタビュー)	従業員や委託先の管理者などに直接質問して回答してもらう
閲覧(レビュー)	関連する文書や記録、パソコンの設定画面など対策を実行した証拠となるものを確認する
観察(視察)	点検の対象となる職場に出向き、従業員が規程や標準規格などに従った行動をしていることを確認する
技術診断	専用ソフトウェアなどを使ってコンピュータやネットワークのセキュリティ対策が実行されているかを確認する
チェックリスト	チェックリストや質問書を配付して回答してもらう

ここでは例として、監査・点検の基準に独立行政法人情報処理推進機構（IPA）の公表資料「情報セキュリティ５か条※2」を用いた進め方を解説します。

※2「情報セキュリティ５か条」
https://www.ipa.go.jp/security/sme/f55m8k0000001wb3-att/000055516.pdf

４．監査・点検の進め方の例

「情報セキュリティ５か条」を監査・点検の基準に用いて「質問（インタビュー)」「閲覧（レビュー)」を行う場合、以下のステップに沿って進めていきます。

（１)「情報セキュリティ５か条」を基準にする。

1. OS やソフトウェアは常に最新の状態にしよう！
2. ウイルス対策ソフトを導入しよう！
3. パスワードを強化しよう！
4. 共有設定を見直そう！
5. 脅威や攻撃の手口を知ろう！

（２）5 か条のうち 「1. OS やソフトウェアは常に最新の状態にしよう！ 」に示された対策例の実施状況を確認する。

1. OS やソフトウェアは常に最新の状態にしよう！

対策例	・Windows Update（WindowsOS の場合）、ソフトウェア・アップデート（macOS の場合）などベンダの提供するサービスを実行する。 ・Adobe Reader、ブラウザなど利用中のソフトウェアを最新版にする。 ・テレワークで利用するパソコン等のソフトウェアやルーター等のファームウェアを最新版にする。 ・利用中のソフトウェアに脆弱性が存在しないか、MyJVN バージョンチェッカ※で確認する。 ※パソコンにインストールされているソフトウェア製品が最新かどうかを簡単な操作で確認できるツール　https://jvndb.jvn.jp/apis/myjvn/?

【手順１】
従業員に、パソコンの Windows Update 画面を開いてもらい、以下を確認する。
・「最新の状態です」または「更新プログラムを利用できます」「利用可能な更新があります」のいずれが表示されているか。
・その他のオプション「利用可能になったらすぐに最新の更新プログラムを入手する」がオンになっているか。

【手順２】
「更新プログラムを利用できます」「利用可能な更新があります」と表示された場合、または「利用可能になったらすぐに最新の更新プログラムを入手する」がオフの場合は、最新の状態にしていない理由を訊ねる。

【手順３】
回答から「セキュリティ事故防止のために役に立っているか？」を判断し、必要に応じて、助言や改善を依頼する。

回答例	**改善依頼・助言例**
・アップデートが始まると、完了するまでパソコンが使えなくなることがあるので更新プログラムの入手をオフにした。 ・アップデートのリリース時に、たまたまネットワークに接続していなかったのでアップデートを後回しにしてパソコンを使っていた。	・更新プログラムの入手をオンにしてアップデートを業務時間外に設定してもらう。 ・アップデートしてからパソコンを使うようにしてもらう。

回答例	改善依頼・助言例
・OS をアップデートすると利用している業務システムの動作が保証されないので更新プログラムの入手をオフにしている。 ・サポートが終了した OS で動く業務システムを使っているため、アップデートすることができない。	・業務システムが最新版の OS に対応しているかメーカーに問い合せてもらう。 ・対応している場合は業務システムもアップデートしてもらう ・対応していない場合は以下を遵守してもらう ① インターネットに接続しない。 ② 外付け HDD や USB メモリ等の外部メディアに接続する場合には必ずパターンファイルを更新したウイルス検知ソフトでスキャンしてから接続する。

５．情報セキュリティ監査・点検の基準

情報セキュリティの監査・点検を実施するには、判断の根拠となる基準が必要です。
情報セキュリティ監査・点検の基準として利用できる資料は、公的機関が無償で提供しているものがあります。
社内の環境や取り組みレベルに合わせて、活用してください。

＜IPA＞
『情報セキュリティ 5 か条』
https://www.ipa.go.jp/security/sme/f55m8k0000001wb3-att/000055516.pdf
『5 分でできる！情報セキュリティ自社診断』
https://www.ipa.go.jp/security/sme/f55m8k0000001waj-att/000055848.pdf

＜東京都＞
『中小企業向けサイバーセキュリティ対策の極意』MISSION2 すぐやろう！対サイバー攻撃アクション
https://www.cybersecurity.metro.tokyo.lg.jp/security/docs/CyberSecurity.Ver.3.0.pdf

＜経済産業省＞
『情報セキュリティ管理基準』
https://www.meti.go.jp/policy/netsecurity/is-kansa/IS_Management_Standard_R7.pdf

＜内閣サイバーセキュリティセンター＞

『政府機関等のサイバーセキュリティ対策のための統一基準』（令和 7 年度版）
https://www.nisc.go.jp/pdf/policy/general/kijyunr7.pdf

なお、本稿は、IPA が発行している「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」を参考に解説しています。

次回は、「監査・点検結果をどのように活かすか？」について解説します。

配信予定日：2025 年 11 月 14 日(金) 14:00 頃
カテゴリ：基礎から学ぶ！ セキュリティ
タグ：＃初級編 ＃基本対策事業 ＃実用編
過去記事焼き直し：しない（新規記事です）
記事 URL（新設します）：https://cybersecurity-taisaku.metro.tokyo.lg.jp/basics/kisokaramanabu21/

EPP と EDR の違いとは？セキュリティ対策の役割分担

目次

●EPP と EDR はどちらも端末を守る仕組み

EPP（Endpoint Protection Platform）と EDR（Endpoint Detection and Response）は、どちらも端末を守る仕組みですが、EPP は「侵入を防ぐ」、EDR は「侵入された後に検知・対応する」ことを目的としています。

●基本的な違い

項目	EPP	EDR
主目的	感染の予防	侵入後の検知・封じ込め
監視対象	ファイル・通信・メール等	端末内のプロセス・挙動・通信履歴
検知手法	シグネチャ、ヒューリスティック等	挙動分析、ログ相関分析等
防御範囲	既知のマルウェア中心	未知・標的型攻撃中心
対応手段	検出・駆除・隔離	攻撃経路追跡・端末隔離・分析報告
運用形態	自動防御中心	分析・監視中心 （監視センター（SOC）等による人手での対応）
詳細	3 分でわかる!用語解説「ウイルス対策ソフト（EPP)」	3 分でわかる!用語解説「EDR」

●それぞれの役割

（1）EPP：感染を防ぐ防御

EPP は端末上でファイルや通信を監視し、既知のマルウェアを検知してブロックします。
AI やクラウド照会機能を備え、未知の脅威にも一定の防御力を持ちます。
ただし、ゼロデイ脆弱性を突く攻撃（ゼロデイ攻撃）などでは、EPP だけで防ぎきれない場合があります。
※ゼロデイ攻撃についてはこちらで解説しています。

（2）EDR：侵入後の監視・対応

EDR は端末内で発生する全挙動（プロセス起動、通信、ファイル操作など）を監視し、不審な動きがあれば即座に検知します。
また、攻撃経路や影響範囲を可視化し、必要に応じて端末をネットワークから隔離します。

●EPP と EDR の連携による多層防御

両者を組み合わせることで、侵入防止と侵入後対応の二重の防御を実現します。
【攻撃の流れ】
外部攻撃 → EPP がブロック → 防ぎきれない攻撃が侵入 → EDR が挙動検知 → 端末隔離 → 監視センター（SOC）等が分析・報告

●まとめと補足

EPP は防御の第一線、EDR は侵入後対応の要。
両者を正しく組み合わせることで、「防ぐ」「見つける」「止める」の三段階を実現できます。

なお、EPP、EDR には様々な製品が存在します。製品ごとに機能も様々で、EPP と EDR 両方の機能を有する製品も存在するようです。製品の比較は各販売会社に確認いただきたいのですが、比較する上での観点について別の記事で紹介したいと思います。

配信予定日：2025 年 11 月 14 日(金) 14:00 頃
カテゴリ：3 分でわかる!用語解説
タグ：＃初級編＃用語編＃知識編
過去記事焼き直し：しない（新規記事です）
記事 URL（新設します）：https://cybersecurity-taisaku.metro.tokyo.lg.jp/glossary/yogokaisetu22/

「ウイルス対策ソフト（EPP)」

目次

サイバーセキュリティの基本を理解するためには、いくつか重要なセキュリティ用語を知っておくことが必要です。
これらの言葉や概念を正確に理解することで、企業が直面するリスクを最小限に抑え、適切な対策を講じることができます。
本記事では、中小企業が特に知っておくべきセキュリティ用語について解説しています。

今回のテーマは「ウイルス対策ソフト（EPP)」です。

●EPP とは
いわゆる「ウイルス対策ソフト」と呼ばれる製品の多くは、専門的には EPP（Endpoint Protection Platform）と呼ばれます。
EPP とは、パソコンやスマートフォンなどのエンドポイント（端末）を守るための総合防御ソフトのことです。
EPP の主な目的は、ウイルスやマルウェアが侵入する前に防ぐこと、すなわち「予防」にあります。
感染後の調査や封じ込めを担当する EDR とは異なり、EPP は「入口防御の要」として位置づけられます。

●EPP の主な役割と目的
EPP が担うのは、主に次の 4 つの役割です。
1. マルウェア検知

ウイルス・トロイの木馬・ランサムウェアなどを検出

2. 駆除・隔離

感染ファイルを自動的に削除または隔離

3. リアルタイム保護

常にシステムを監視し、危険を即座にブロック

4. 自動アップデート

新種ウイルスへの対応データを自動で更新

EPP は、利用者が意識せずとも端末を常に安全な状態に保つ常駐型の防御機能といえます。

●EPP の主な検知方式

EPP は 1 つの技術だけで動いているわけではなく、複数の検知エンジンを組み合わせて既知・未知の脅威を見つけます。

（1）シグネチャ検知（パターンマッチング方式）

過去に判明しているウイルスの特徴的なコード列（シグネチャ）をもとに照合して検出する最も基本的な方式です。

長所：精度が高く誤検知が少ない

短所：新種のウイルスには対応できない

（2）ヒューリスティック分析

未知のウイルスを見つけるために、コードの構造や挙動を解析して怪しい動きを判断する手法です。

長所：未知のマルウェアもある程度検出可能

短所：正常なプログラムを誤検知するリスクあり

（3）挙動（ビヘイビア）分析

プログラムの実行中の動作を監視し、不審な行動（自己複製、暗号化、外部通信など）を検知します。

長所：実際の攻撃行動を検出できる

短所：リソース負荷が高く、リアルタイム処理に限界がある場合もあります。

（4）機械学習（AI 検知）

AI が大量のマルウェアサンプルを学習し、「正常／異常」を自動判別する方式です。

長所：ゼロデイ攻撃にも強く、更新頻度に依存しにくい

短所：学習モデルに依存し、誤検知が起こることもあります。

※ゼロデイ攻撃についてはこちらで解説しています。

（5）クラウド検知

最新の脅威情報をクラウド上のデータベースに照会して判定します。

長所：シグネチャ更新が不要で最新状態を維持できる

短所：オフライン環境では利用が制限される

●まとめ

EPP はエンドポイントに最初の防御壁を築くための重要な仕組みです。

しかし、完璧ではありません。未知の攻撃や標的型攻撃では、感染後の追跡や封じ込めが必要になります。

したがって、EDR や SOC（監視センター）との連携が欠かせません。

EPP は「侵入を防ぐ」、EDR は「侵入されても止める」。

この役割分担を理解しておくことが、現代のサイバー対策の第一歩です。

※EDR についてはこちらで解説しています。

配信予定日：2025 年 11 月 14 日(金) 14:00 頃
カテゴリ：もっと知りたい！ セキュリティ
タグ：＃インシデント対応強化＃知識編
過去記事焼き直し：しない（新規記事です）
記事 URL（新設します）：https://cybersecurity-taisaku.metro.tokyo.lg.jp/know_more/incident-sosikitaisei2/

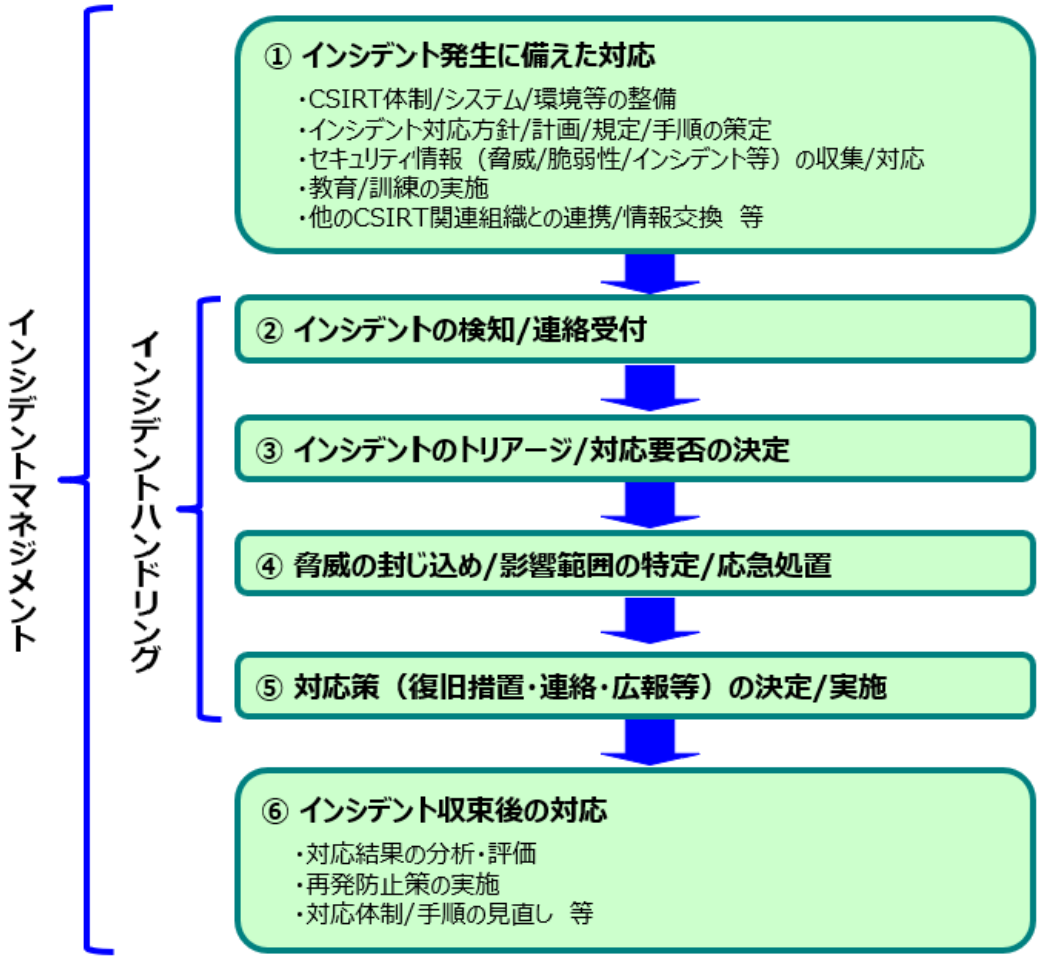
セキュリティインシデントに備えた組織体制（２／３）

目次
●インシデントマネジメント及びインシデントハンドリングの概要
●インシデントマネジメントにおける留意点
●用語解説

中小企業の経営者や情報システム担当者の皆さん、日々のセキュリティ対策、お疲れ様です。今回はセキュリティインシデントに備えた組織体制である CSIRT(シーサート：Computer Security Incident Response Team)を核とした、インシデント発生時の対応における留意点等について解説します。

●インシデントマネジメント及びインシデントハンドリングの概要
前回解説したように、CSIRT には、インシデント発生時に対応を主導し、情報を集約して関係者に適時報告したり、現場組織等に適時対応を指示したりするほか、平常時の活動として、インシデント発生に備えた各種の対応等が求められます。CSIRT が核となって行うこうした一連の業務をまとめて「インシデントマネジメント」もしくは「インシデント管理」、インシデントを検知してから収束させるまでの対応を「インシデントハンドリング」と呼びます。CSIRT を核とした一般的なインシデントマネジメントの流れを次の図に示します。

インシデントマネジメント/インシデントハンドリングの流れ



●インシデントマネジメントにおける留意点

以降はインシデントマネジメント/インシデントハンドリングの流れに沿って、それぞれ留意すべき事項について解説します。

① インシデント発生に備えた対応

インシデント発生に備えた対応として、体制や対応手順の整備、インシデントを早期に検知し、被害を最小化するためのシステム導入等が必要です。その具体例を次に挙げます。

・インシデント対応体制（CSIRT）の整備
・CSIRT の活動範囲、対象とするインシデントの明確化
・インシデント対応計画（中長期計画、年度計画など）、規程類の策定
・想定されるインシデントに対する個別の対応手順、連絡体制の整備
・インシデント発生に備えた設備、機器（代替設備、代替機器、交換部品、バックアップデータなど）の整備

・セキュリティベンダとの契約（セキュリティ監視サービス、インシデント対応サービス等）
・インシデントの検知・対応に必要なシステム（IPS、IDS、SIEM 等）の導入・構築
・セキュリティ情報（脅威動向、脆弱性、インシデント事例等）の収集及び対応（周知、影響度分析、パッチ適用、対策強化等）
・インシデント発生に備えた教育・訓練の実施
・他の CSIRT 関連組織（JPCERT/CC、日本シーサート協議会、他社の CSIRT 等）との連携・情報交換
・サイバー保険の契約

近年サイバー攻撃により製品の製造やサービスの提供に多大な支障を及ぼすインシデントが多発しているように、セキュリティ対策/対応の不備が企業の事業継続や存続にかかわる重大な問題にまで発展する可能性があります。したがって、セキュリティ対策やインシデント対応の検討・強化にあたっては、権限を有する経営層が関与するのが望ましいでしょう。

② インシデントの検知・連絡受付
・ネットワーク機器のログ、サーバのログ、EPP、EDR、IDS、IPS、SIEM 等からインシデントを検知
・顧客、取引先、自組織の従業員、その他社外の第三者などからの連絡（通報）によってインシデントを検知

上記のように、ログやセキュリティ機器によるインシデント検知の仕組みと、人による検知の仕組みの両方が必要です。この二つの仕組みによるインシデント検知の例を次に示します。

ログやセキュリティ機器によるインシデント検知の例
・認証サーバのログからの不審なログイン失敗／成功の検知
・EPP や EDR からのアラートによるマルウェアの検知
・IDS，IPS，SIEM からのアラートによるサイバー攻撃の検知
・ファイアウォールやプロキシサーバのログからの不審な通信の検知

社員や顧客などからの連絡・通報などによるインシデント検知の例
・PC を紛失した社員からの連絡による検知
・システムダウンや動作異常を発見した社員からの連絡による検知
・取引先や顧客からの連絡によるマルウェア拡散の検知
・第三者からの通報による情報漏えいの検知

これらのほか、SNS やインターネット上の匿名掲示板、攻撃者が開設しているウェブサイト等によって情報漏えいの事実を知るというケースもあります。そのため、インシデントを早期に検知するためには、日ごろからネット上でやり取りされている情報等にも注意する必要があります。

③ インシデントのトリアージ・対応要否の決定
・インシデントを検知した SOC（Security Operation Center）のアナリスト、あるいはインシデントの連絡を受けた窓口担当は、インシデントの内容、状況等を CSIRT の担当者、組織の管理者等に適時報告（エスカレーション）する
・CSIRT はインシデントの内容を確認の上、あらかじめ定められた判断基準に従ってトリアージ（優先度を決定して選別）し、対応の要否や方法を決定する

インシデント発生時にはその状況等を速やかにエスカレーションするとともに、当面の対応方針等を決定する必要があります。軽微なものまで含め、CSIRT がすべてのインシデントに対応することはできないため、トリアージの判断基準を可能な限り詳細に定めておく必要があります。

今回はインシデント発生に備えた対応から検知、トリアージ等における留意点について解説しました。次回はそれ以降の対応について解説します。

●用語解説
IPS（Intrusion Prevention System）
ネットワーク上で攻撃や不正アクセスをリアルタイムに検知し、防御する機能を持つ機器。

IDS（Intrusion Detection System）
ネットワーク上で攻撃や不正アクセスをリアルタイムに検知し、通知する機能を持つ製品/サービス。

SIEM（Security Information and Event Management）
ネットワーク上でサーバやネットワーク機器等のログを収集し、それらを相関分析してサイバー攻撃等を検知・通知する製品/サービス。

EPP（Endpoint Protection Platform）

ウイルス定義ファイルによるパターンマッチングを主とした一般的なウイルス対策製品。
※詳しくは 3 分でわかる!用語解説「ウイルス対策ソフト（EPP)」

EDR（Endpoint Detection & Response）
パソコン、サーバなどのエンドポイント環境で発生している様々な事象を分析することによってマルウェアの侵入やその後の振る舞いなどを検知し、対処する製品/サービス。
※詳しくは 3 分でわかる!用語解説「EDR」

配信予定日：2025 年 11 月 21 日(金) 14:00 頃
カテゴリ：もっと知りたい！ セキュリティ
タグ：＃インシデント対応強化＃知識編
過去記事焼き直し：しない（新規記事です）
記事 URL（新設します）：https://cybersecurity-taisaku.metro.tokyo.lg.jp/know_more/incident-sosikitaisei3/

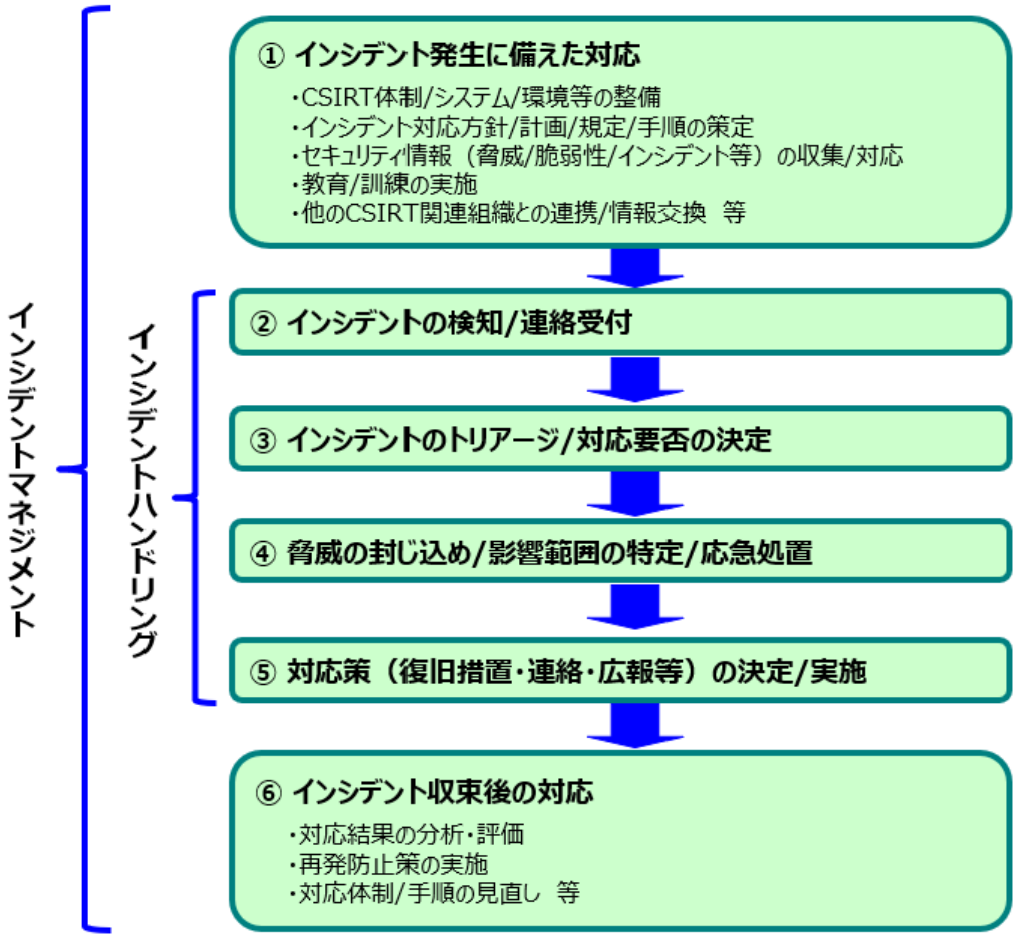
セキュリティインシデントに備えた組織体制（３／３）

目次
●インシデントマネジメントにおける留意点
●サイバーレジリエンスと OODA

中小企業の経営者や情報システム担当者の皆さん、日々のセキュリティ対策、お疲れ様です。
前回に続き、セキュリティインシデントに備えた組織体制である CSIRT(シーサート：Computer Security Incident Response Team)を核とした、インシデント発生時の対応における留意点について解説します。

●インシデントマネジメントにおける留意点
前回は下図の①～③について解説しました。今回は④以降について解説します。

インシデントマネジメント/インシデントハンドリングの流れ（前回より再掲）



④ 脅威の封じ込め／影響範囲の特定／応急処置

・CSIRT は、対応を要するインシデントについて、検知されたマルウェア等の脅威を封じ込める策を最優先で行うとともに、被害の拡大を回避するために必要な処置を行うようシステム管理者等に指示する

・CSIRT は、SOC（Security Operation Center）のアナリスト、システム管理者、契約しているセキュリティベンダー等と連携し、インシデントの影響範囲を特定するとともに、暫定的な復旧処置（応急処置）を行う

・インシデント対応の内容について確実に記録を残す

一連のインシデント対応において発生している事象の正確な確認と被害の最小化、証拠となるログ等の確保を行う必要があります。

サイバー攻撃によるインシデントの場合には、被害を受けたと思われる機器をネットワークから切り離すとともに、インシデントの内容や原因を分析するため、関連するログやストレージ（ハードディスク等の記録装置）の内容を別な媒体に物理的にコピーする等して、イ

ンシデントの痕跡や証跡を保全します。

⑤対応策（復旧措置・連絡・広報等）の決定／実施
・CSIRT は、インシデントの内容やレベルに応じ、セキュリティベンダーにデジタルフォレンジックスを依頼するとともに、復旧のための対応策を検討し、決定する
・インシデントの内容や影響度、対応状況などについて、顧客をはじめ、社内外の関係者に適時説明する
・決定した対応策に必要な各種リソースを確保し、実施する
・対応策の内容について、必要に応じて社内外の関係者に説明する
・インシデントの収束が確認されたら、顧客や社内外の関係者に対し、その旨を連絡・公表する

インシデントの原因究明には多くの時間を要する可能性があるため、原因究明よりも復旧のための対応策を優先します。発生したインシデントが顧客や取引先等に影響を及ぼしている場合には、その関係者に適時説明するとともに、監督官庁や個人情報保護委員会等に状況を報告する必要もあります。
そのほか、ホームページを通じたインシデントの説明、問合せ窓口の設置、正式な調査結果報告等の対応を迅速に行うことも求められます。したがって、CSIRT はインシデントの正確な情報を集約し、経営者や関係部門の責任者などに対して適時伝える必要があります。
インシデントを公表することにより、顧客や関係者からの問合せが殺到することも想定されるため、そうした場合の説明内容や FAQ 等を明確にして社内に周知しておきます。
また、インシデントの復旧後に同様の事象が再発しないよう、当面の間はシステムの状態を細心の注意を払って監視し、わずかでも異常が見つかった場合には、直ちに対応できる体制を整えておく必要があります。

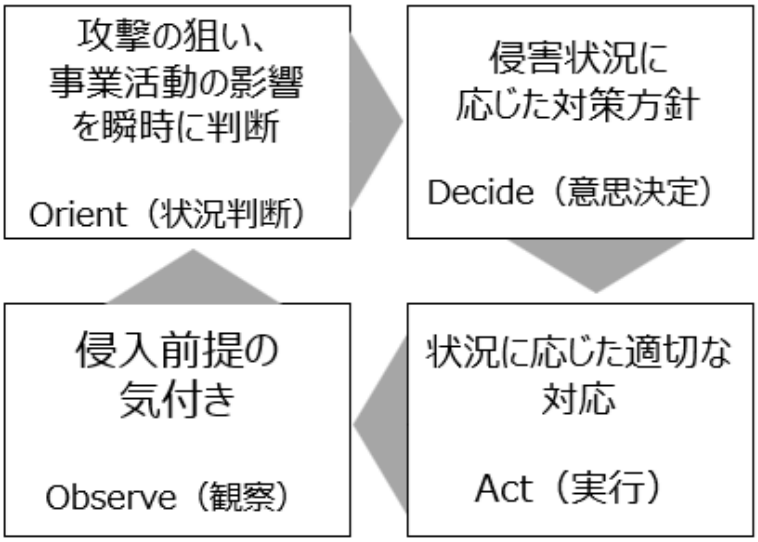
⑥インシデント収束後の対応
・一連のインシデント対応の結果について関係者で評価し、問題点を洗い出すとともに、改善策を検討・決定する（SLA，体制，手順，検知システム，対応方法の見直し等）
・インシデントの再発を防止するための対策（即時実施すべきもの、中長期的な取組みを要するもの等）を検討・決定する
・インシデントの評価結果に基づき、必要な各種リソースを確保し、改善策、再発防止策を実施する
・新たに必要となった各種リソース（要員、設備、システム、サービス等）を確保・整備する
・顧客との契約内容（SLA、責任範囲など）について見直す
・インシデント対応体制、対応手順について見直す

・見直した内容に基づき、要員の教育・訓練を実施する

インシデントの判断基準や手順に不備や誤りなどがなかったか、対応者のスキルレベルに対して十分であったか、状況判断が適切に行われ、余分な時間を費やすことはなかったか等、様々な観点から評価し、問題箇所を確認します。
インシデントの発生原因が自組織の IT 環境にあったのか、あるいは業務内容や従事している人間の問題であったのか等により、見直すべき点は異なってきます。IT を取り扱う要員の認識不足や注意不足、連絡体制の不備等による問題であった場合には、IT 管理体制をはじめ、業務内容や手順、要員の教育方法等の抜本的な見直しが必要となります。

●サイバーレジリエンスと OODA
インシデントマネジメントにおいては、組織のレジリエンス（resilience）を高めることが重要です。レジリエンスとは「回復力」や「復元力」を意味する用語であり、サイバー攻撃によるインシデント発生時に、その影響を最小化し、元の状態に回復させる組織の能力がサイバーレジリエンスです。
サイバーレジリエンスを高めるためには、OODA（ウーダ）ループによる取組みが重要とされています。OODA ループとは、次に示すように、観察（Observe）、状況判断（Orient）、意思決定（Decide）、実行（Act）を繰り返すことです。

OODA ループの例



OODA と似たものとして、PDCA（Plan-Do-Check-Act）があります。PDCA は計画に基づいて、1 年など長期的なスパンで取り組むのに対し、OODA は対象を常に観察し、その状況に応じて素早く臨機応変に対応する（高速でループを回す）ことを前提としています。

そうすることで、突発的なセキュリティインシデントに迅速に対応し、サイバーレジリエンスを向上させることが可能となります。

配信予定日：2025 年 11 月 21 日(金) 14:00 頃
カテゴリ：基礎から学ぶ！ セキュリティ
タグ：＃初級編＃実用編
過去記事焼き直し：しない（新規記事です）
記事 URL（新設します）：https://cybersecurity-taisaku.metro.tokyo.lg.jp/basics/imakikitai1/

いまさら聞けない！よくあるネットワーク構成図

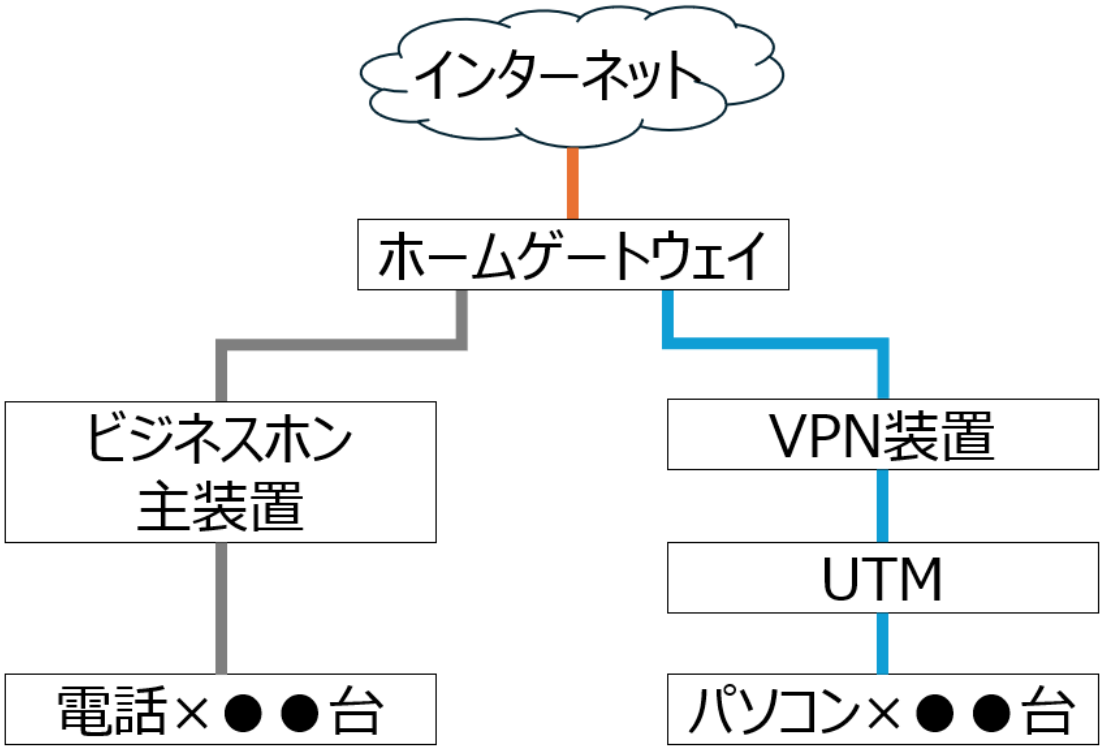
目次

東京都サイバーセキュリティ対策事業を通じ、情報セキュリティ対策はわかりづらいというお悩みをいただきます。解決策の一つとして「情報セキュリティに限らずＩＴの基本的な事項を知る」事があります。
いまさら聞けない！シリーズとして、今後連載をしていきたいと思います。今回は中小企業でよくあるネットワーク構成図をご紹介いたします。

※なお、本記事は分かりやすさを重視し、技術的な事項は大幅に要約して説明をいたします。技術的に正しい事項を理解する必要がある場合は、別途、専門書等でご確認をお願いいたします。

●ネットワーク構成図

通信に関わる機器や配線を図化したものをネットワーク構成図と言います。以下は中小企業でよくある構成のネットワーク構成図です。



●各機器の主な機能や役割

機器名	主な機能や役割
ホームゲートウェイ	インターネット側から企業側へ引き込まれる光ファイバーの線を、電話線（図のグレーの線）や、ネットワークの線（図の青の線）に変換する装置です。
ビジネスホン主装置	1つの電話番号を複数の電話機で利用可能にするための装置です。
VPN 装置	社外（インターネット側）から社内へ暗号化して通信するための装置です。 ※詳細は別記事「VPN とゼロトラスト」を参照。
UTM	不正な通信を監視し、制御する装置です。 ※詳細は別記事「UTM」を参照。

●別パターンも結局は同じ

上記で示したのはよくある構成（よくあるパターン）ですが、別のパターンをいくつか挙げると以下があります。

① ビジネスホン主装置は、ホームゲートウェイではなく電柱から企業側へ引き込まれた電話線と接続されている。
② VPN 装置と UTM が、１台の機器になっている。
③ UTM が無い。

それぞれ、どういう状況なのかイメージがつきますでしょうか。①～③が、よくあるネットワーク構成図と異なるポイントを書くと以下になります。

① 電話とネット（光ファイバー）の線が一緒か別々か
② VPN と UTM が別々の機器か１台の機器か
③ UTM があるかないか

このようなポイントを考えていけば、皆様の会社のネットワーク構成図が、よくあるネットワーク構成図とどう異なるのか理解できます。
また、実際の機器や配線を追い、どの機器がどのような機能を持ち、どこと接続しているかを調べていくことで、正しいネットワーク構成図を作成することができます。

●ネットワーク構成図は役に立つ
ネットワーク構成図を作成し、管理することで以下の効果が期待できます。
・保有資産の把握
・不具合発生時の対応（被疑箇所や影響範囲の特定、復旧作業）
・新たな機器の導入や既存機器の撤去時の検討
IT 機器や配線を特定の企業に任せている（購入や保守委託をしている）場合は、当該企業でネットワーク構成図を作成してくれることがあります（別途費用がかかる場合もありますのでご確認をお願いいたします)。しかし、様々な企業から IT 機器を購入している場合は、ネットワーク構成図は各社の情報システム管理者等で作成する必要があります。作成していない企業は、本件を機に作成してはいかがでしょうか。

配信予定日：2025 年 11 月 21 日(金) 14:00 頃
カテゴリ：3 分でわかる!用語解説
タグ：＃初級編＃用語編＃知識編
過去記事焼き直し：しない（新規記事です）
記事 URL（新設します）：https://cybersecurity-taisaku.metro.tokyo.lg.jp/glossary/yogokaisetu23/

「PPAP」

目次

サイバーセキュリティの基本を理解するためには、いくつか重要なセキュリティ用語を知っておくことが必要です。
これらの言葉や概念を正確に理解することで、企業が直面するリスクを最小限に抑え、適切な対策を講じることができます。
本記事では、中小企業が特に知っておくべきセキュリティ用語について解説しています。

今回のテーマは「PPAP」です。

●PPAP とは
電子メールの添付ファイルを送信する際、パスワード付きファイル（ZIP ファイル等）を添付するメールと、そのパスワードを記載したメールを別送信する方法を、PPAP（Password 付き ZIP ファイル＋Password 別送）と呼びます。企業で広く使われているメール添付ファイルのセキュリティ手法ですが、現在は廃止が進んでいます。その理由と代替策を紹介します。

●PPAP 廃止の理由（PPAP の問題点）
PPAP 廃止の主な理由として以下があります。
１．盗聴・誤送信に弱い
ファイルとパスワードを同じメール経路で送るため、メールを盗聴された場合に添付ファイルを簡単に閲覧されてしまう。また、メール誤送信時はパスワードまで送ってしまうケースが多い。
２．ウイルスチェックができない

パスワード付き ZIP は暗号化されているため、セキュリティソフトが中身をスキャンできず、マルウェア感染の温床になる。
３．ファイルが利用されたか記録が残らない
誤送信があった場合、当該ファイルが誤送信先で利用されたかわからない。
４．パスワードを突破される
パスワード付きZIPファイルにパスワードを総当たりされ､ファイルを解凍されてしまう。
５．メール利用者の手間
パスワード化してメールを２つ作成して送信するため、添付ファイルなしのメールと比して手間がかかる。

●代替策
PPAP の問題点を解決するには、安全で、ログが残り、誤送信対策にも強い方式を利用する必要があります。具体的にはメール送信者及び受信者がデータをアップロード／ダウンロードできるクラウドストレージや、セキュアファイル転送サービスを利用する方法があります。
この方法を採用すれば、以下のメリットがあります。
・誤送信した場合はクラウドストレージ上のファイルを削除すればよい。
・誰がいつ開いたか、アクセスログが残る。
・ダウンロード有効期限を設定する､パスワードを設定する等､アクセス制御ができる。
・大容量ファイルも送ることができる。
・ウイルススキャンが可能。
しかし､受信者側の企業の情報セキュリティルールにより､クラウドストレージやセキュアファイル転送サービスの利用が禁止されているケースがあるため、ファイル送信時には相手側に確認を取る必要があります。

また､上記方法は導入における手間や費用が掛かる場合があります｡PPAP を行っている環境においてすぐにできる代替策として、パスワードを電話等別手段で相手に送る方法があります｡しかし､電話は複雑なパスワード文字列を通知することが難しいため､頻繁にファイルを送る相手には会議の場でパスワードを通知し一定期間利用する方法もあります。
（例：月１回の定例会議でその月に利用するパスワードを通知する）

配信予定日：2025 年 11 月 28 日(金) 14:00 頃
カテゴリ：ビジネスヒント
タグ：＃知識編＃経営課題
過去記事焼き直し：しない（新規記事です）
記事 URL（新設します）：https://cybersecurity-taisaku.metro.tokyo.lg.jp/tip/security-hyoukaseido1/

サプライチェーン強化に向けたセキュリティ対策評価制度（１／２）

目次

IPA（独立行政法人 情報処理推進機構）が公開している「情報セキュリティの 10 大脅威 2025[組織]※」で「サプライチェーンや委託先を狙った攻撃」が第 2 位になっているように、近年サプライチェーンにおける重大なセキュリティインシデントが多発しており、製品の製造や流通等にも大きな影響を及ぼしています。そんな中、経済産業省では、2025 年 4 月に「サプライチェーン強化に向けたセキュリティ対策評価制度構築に向けた中間取りまとめ」（以下「中間取りまとめ資料」と表記します）を公表しました。今回は、この取組みの概要について解説します。

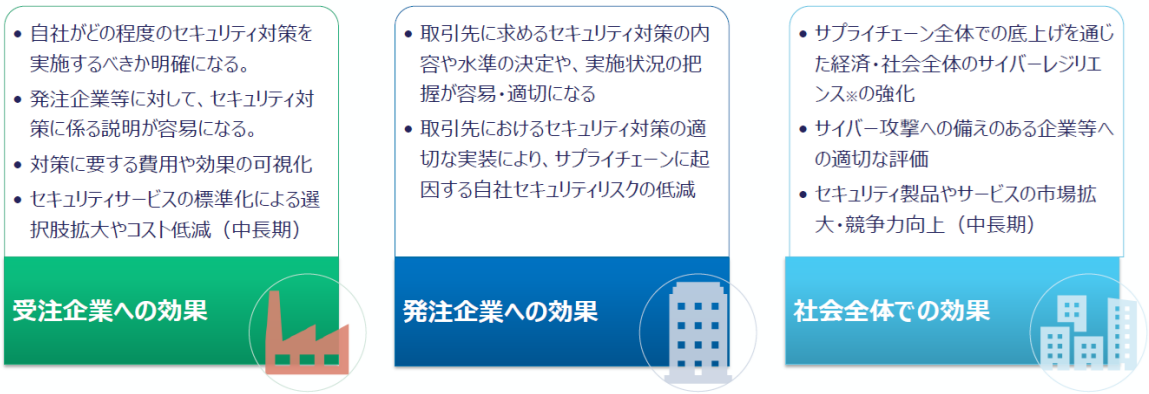
※2024 年に発生した社会的に影響が大きかったと考えられる情報セキュリティにおける事案から、約 200 名の有識者からなる「10 大脅威選考会」が脅威候補に対して審議・投票を行い、決定したもの。組織向けと個人向けの 2 つの観点で 10 個ずつ示されており、組織向けのみ脅威の大きさによるランク付けがされている。
(https://www.ipa.go.jp/security/10threats/10threats2025.html)

●取組みの背景
上記のような状況の中、企業の取引においてサイバーセキュリティ対策の担保が求められています。その際、業務等を受注する側の企業は異なる取引先から様々な対策水準を要求されていますが、発注する側の企業では各企業等の対策状況を客観的に判断することが難しいといった課題があります。
こうした課題に対応するため、経済産業省では、「サプライチェーン強化に向けたセキュリティ対策評価制度」（以下「本制度」と表記します）の実現に向け、その目的や位置付け、

要求項目・評価基準の内容、制度の普及のために必要な施策等について有識者や産業界と検討を進めています。その検討内容を「中間取りまとめ」として 2025 年 4 月に公表しました。なお、本制度は、サプライチェーンにおける重要性を踏まえた上で満たすべき各企業の対策を提示しつつ、その対策状況を可視化する仕組みです。

●本制度の趣旨・目的
サプライチェーンにおける取引先へのサイバー攻撃を起因としたセキュリティリスクや、製品/サービスの提供途絶、取引ネットワークを通じた不正侵入等のリスクに対し、本制度に基づくマークの取得を通じ、適切なセキュリティ対策の実施を促し、サプライチェーン全体でのセキュリティ対策水準の向上を図ることを目的としています。
具体的には、2 社間の取引契約等において、発注企業が、受注側に求める適切な段階（★3～★5）を提示し、示された対策を促すとともに実施状況を確認することを想定しています。

●本制度によって期待される効果
本制度によって期待される効果として、中間取りまとめ資料に次の図が示されています。



「サプライチェーン強化に向けたセキュリティ対策評価制度構築に向けた中間取りまとめ」より
(https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_supply_chain/pdf/20250414_2.pdf)

図にあるように、本制度により、発注者・受注者双方にとって、適切なセキュリティ対策の決定や対策状況の説明が容易となるほか、取引先のセキュリティ対策が適切に実装されることで、発注企業のサプライチェーンリスクの低減、経済・社会全体でのサイバーレジリエンス※の強化等が期待されます。

※サイバーレジリエンス(Cyber resiliency)
サイバー資源を使用する、またはサイバー資源によって実現するシステムに対する不利な

状況、ストレス、攻撃、侵害を予測し、それらに耐え、回復し、適応する能力。

●本制度における段階の考え方
本制度における★3～★5 の各段階の考え方として、中間取りまとめ資料に次の表が示されています。

	★3	★4	★5
想定される脅威	• 広く認知された脆弱性等を悪用する一般的なサイバー攻撃	• 供給停止等によりサプライチェーンに大きな影響をもたらす企業への攻撃 • 機密情報等、情報漏えいにより大きな影響をもたらす資産への攻撃	• 未知の攻撃も含めた、高度なサイバー攻撃
対策の基本的な考え方	• 全てのサプライチェーン企業が最低限実装すべきセキュリティ対策として、基礎的な組織的対策とシステム防御策を中心に実施	• サプライチェーン企業等が標準的に目指すべきセキュリティ対策として、組織ガバナンス・取引先管理、システム防御・検知、インシデント対応等包括的な対策を実施	• サプライチェーン企業等が到達点として目指すべき対策として、国際規格等におけるリスクベースの考え方に基づき、自組織に必要な改善プロセスを整備した上で、システムに対しては現時点でのベストプラクティスに基づく対策を実施
脅威に対する達成水準（イメージ）	• 組織内の役割と責任が定義されている。 • 一般的なサイバー脅威への対処を念頭に、自社 IT 基盤への初期侵入、侵害拡大等への対策が講じられている。 • インシデント発生時に、取引先を含む社内	• セキュリティ対策が組織的な仕組みに基づいて実施され、継続的に改善している。 • 取引先のシステムやデータを含む内外への被害拡大や攻撃者による目的遂行のリスクを低減する対策が講じられている。	• 組織において国際規格等に基づくマネジメントシステムが確立されている。 • リスクを適宜適切に把握した上で、インシデントに対して迅速に検知・対応するなど、ベストプラクティスに基づくサイバーレジリエン

	外関係各所への報告・共有に必要な最低限の手順が定義、実施されている。	• 事業継続に向けた取組や取引先の対策状況の把握など、自社の位置づけに適合したサプライチェーン強靭化策が講じられている。	ス確保策が講じられている。 • 取引先等への指導や共同での訓練の実施など、自社サプライチェーン全体のセキュリティ水準向上に資する対策が講じられている。
評価スキーム	自己評価 　社内等の専門家による評価を想定	第三者評価 　第三者評価を原則とするが、評価コストの負担を抑える観点から詳細は今後検討	第三者評価

「サプライチェーン強化に向けたセキュリティ対策評価制度構築に向けた中間取りまとめ」より
(https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_supply_chain/pdf/20250414_2.pdf)

★3については、一般的なサイバー脅威に対処しうる水準を目指すものとして規定しています。
★4については、初期侵入の防御に留まらず、内外への被害拡大防止・目的遂行のリスク低減によって取引先のデータやシステム保護に寄与する点や、サプライチェーンにおける自社の役割に適合した事業継続を推進している点を明確化したものとなっています。
★5については、より高度なサイバー攻撃への対応として、自組織のリスクを適切に把握・マネジメントした上で、システムに対する具体的な対策としては既存のガイドライン等も踏まえた上で現時点でのベストプラクティスに基づく対策を実行する形を想定しています。

次回は、本制度における評価スキームや実施に向けたスケジュール等について解説します。

配信予定日：2025 年 11 月 28 日(金) 14:00 頃
カテゴリ：ビジネスヒント
タグ：＃知識編＃経営課題＃インシデント対応強化
過去記事焼き直し：しない（新規記事です）
記事 URL（新設します）：https://cybersecurity-taisaku.metro.tokyo.lg.jp/tip/incident-taikendan1/

ランサムウェアに感染したら？インシデント体験から学ぶ

目次

ランサムウェアに感染して製品の流通が停止した等、昨今は様々なインシデントがメディアで報道され、被害を受けた企業はウェブサイトで経緯等を公開しています。
しかしながら、インシデント対応の詳細な経緯が公開されることはあまりありません。企業イメージに傷がつく、公開の必要性がない等、理由は様々と思いますが、失敗から学べることは多々あります。
今回は、過去のインシデント事例をフィクションとして修正し、失敗から学べるインシデント対応のポイントとして記事にしたいと思います。

●ある企業で発生したインシデント
A 社は従業員 300 名、大手機械メーカーの部品を製造している。情報セキュリティ対策は、大手機械メーカーからの依頼もあり、進んでいる状況（※）。
※東京都中小企業サイバーセキュリティ対策事業だと「レベル 3：インシデント対応強化」に取り組み始めているレベル。
参考：東京都サイバーセキュリティ対策事業の成り立ちと今後について
この企業において、ランサムウェアに感染し 1 か月以上外部とインターネット通信ができなくなりました。その対応経緯を次項で紹介します。

●インシデント対応の経緯
[発覚当日]
・社内ファイルサーバにアクセスできないとの申告があり調査開始。
・システム管理者がサーバを確認したところ、ランサムウェアと思える挙動をしていた（サーバ内に暗号化されたファイルが複数存在）。

・ウイルスによる外部へのデータ流出を懸念し、会社全体でインターネット接続を不可とした。
・システム管理者だけでは対応ができず、急遽セキュリティ企業へ調査業務を見積額不明なまま委託。
・取引先へ電話で連絡、一部取引先からは詳細な報告を求められる。以降、この対応稼働捻出もあり担当者は深夜まで勤務。
・機械部品の製造はインターネットを利用しないのでできなくはないが、受発注管理が手作業となり生産効率が激減。
[３日後]
・サーバの調査の結果、原因はランサムウェアと断定。しかし、サーバにランサムウェアが流入した経路が不明。
・従業員のパソコンやメールサーバが汚染され社外にウイルスを拡散する可能性があるため、インターネット接続は復旧させないこととした。
・パソコンが必要な業務については、新規にパソコンを購入し徐々に復旧。
[１週間後]
・原因となるウイルスを特定し、ウイルスを駆除するソフトを用意し、全端末のウイルスチェックを開始。
・この時点でもパソコンが必要な業務の一部しか復旧できておらず、生産効率は従来の半分にも満たない。
・万が一の状況を考慮し、全端末ウイルスチェックが終わった後も１か月程度様子を見る事とした。
[１か月後]
・インターネット接続を復旧し、従来の IT 環境を復旧した。

●インシデント対応の補足・考察
上記の例では、発覚当日にインターネット接続を不可としたことで、ウイルスによる外部へのデータ流出・メールによる社外へのウイルス拡散防止という事態に対処できた点は評価できます。しかしながら「生産効率が激減した」という点もあり、インシデント発生を想定した準備ができていなかったと考えられます。例えば、あらかじめ代替手段を整理しておけば、１週間後においても「生産効率が従来の半分にも満たない」状況は回避できます。
また、これ以外にもいくつか改善できるポイントがあります。
・原因を特定する方法の整理
　⇒見積額不明なまま委託しなくて済む可能性がある。
・取引先への報告タイミングや報告内容のルール化
　⇒特定の担当者への対応稼働の偏り（深夜まで勤務）が無くなる。

実際のインシデント対応時は、少ない情報に対し、限られた稼働・リソースで対応していく必要があります。あらかじめ備えておくことで、インシデント被害を抑える事が出来ます。東京都中小企業サイバーセキュリティ対策事業では「インシデント対応強化」という事業で、インシデント対応を想定した準備を支援しています。今年度の参加企業募集は終了しましたが、来年度も事業が行われる可能性があります。東京都産業労働局のウェブサイトや公式X等を適宜ご確認ください。（ブックマークやフォローをお勧めします）

参考：令和７年度中小企業サイバーセキュリティ社内体制整備事業　インシデント対応強化
参考：東京都産業労働局ウェブサイト「中小企業向けサイバーセキュリティ対策の極意」
参考：東京都産業労働局公式X「東京都　産業・仕事」

配信予定日：2025 年 11 月 28 日(金) 14:00 頃
カテゴリ：基礎から学ぶ！ セキュリティ
タグ：＃初級編＃実用編
過去記事焼き直し：しない（新規記事です）
記事 URL（新設します）：https://cybersecurity-taisaku.metro.tokyo.lg.jp/basics/imakikitai2/

いまさら聞けない！ルータの役割

目次

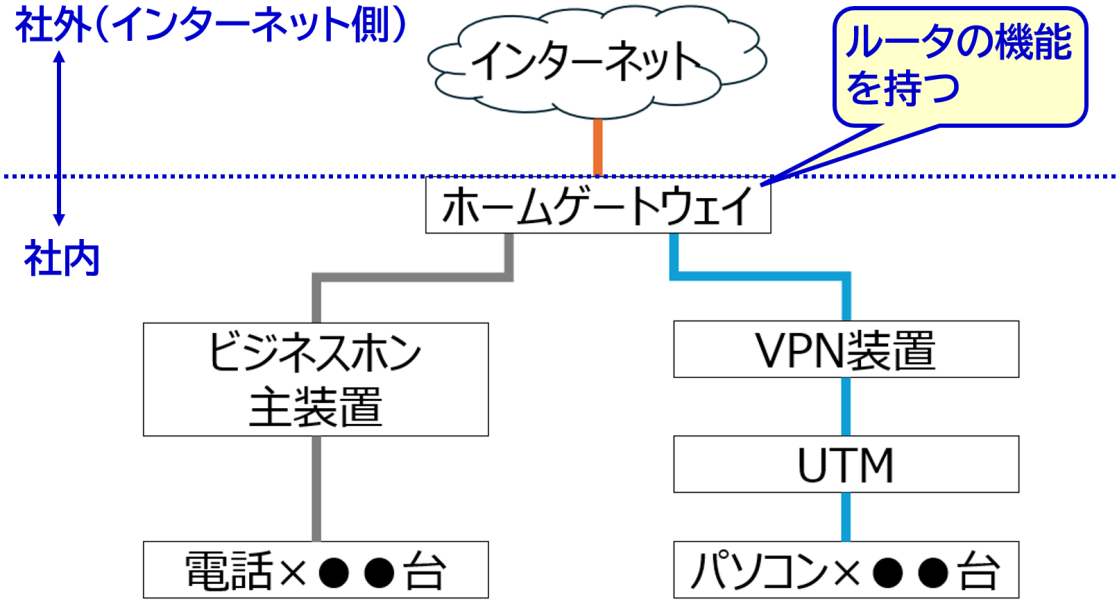
東京都サイバーセキュリティ対策事業を通じ、情報セキュリティ対策はわかりづらいというお悩みをいただきます。解決策の一つとして「情報セキュリティに限らずＩＴの基本的な事項を知る」事があります。
今回はルータの役割をご紹介いたします。

※なお、本記事は分かりやすさを重視し、技術的な事項は大幅に要約して説明をいたします。技術的に正しい事項を理解する必要がある場合は、別途、専門書等でご確認をお願いいたします。

●ルータとは
「ネットワーク同士をつなぎ、最適な道順でデータを届ける装置」です。技術的に様々な機能を有していますが、中小企業や SOHO（≒家庭）でよくある利用方法から、ルータの機能を解説していきます。

●ルータの設置場所
上記で言う「ネットワーク同士」とは、「社外：インターネット側のネットワーク」と「社内：企業側のネットワーク」を指します。企業の内外の境界部分にルータは設置されます。
実は前回の記事で紹介した、ホームゲートウェイがルータの機能を持っています。
※前回記事：いまさら聞けない！よくあるネットワーク構成図
前回記事の構成図で示すと、ルータの位置は以下の通り、ホームゲートウェイの位置になり

ます。



なお、前回記事ではよくあるネットワーク構成を簡単に理解するため、ホームゲートウェイのルータ機能については触れませんでした。今回もルータの役割を簡単に理解するため、重要な機能に絞り、解説していきたいと思います。

●ルータの主な役割１：インターネットプロバイダとの接続

各企業では、社外の電柱から引き込まれる光ファイバーや、貸しビルから提供される物理的な線をホームゲートウェイに接続していると思います。しかし、インターネットを利用するには社外と社内の物理的な接続に加え、社外側でのインターネット接続処理が必要です。このインターネット接続処理をしてくれるのが、インターネットプロバイダ（ISP：Internet Service Provider）です。

接続処理について具体的に説明します。社外にはインターネットプロバイダの装置があり、その装置に対して社内のルータから ID/PW 等で接続を行い、インターネットが利用できるようになります。この機能が、ルータの主な役割の１つです。

●ルータの主な役割２：IP アドレスの変換

インターネット上の様々なウェブサイトと、それを利用する様々な企業を接続するため、各個を IP アドレスという数値で識別しています。インターネット利用上のルールとして、IP アドレスは社外（インターネット側のネットワーク）と、社内（企業側のネットワーク）で明確に異なるものを利用する必要があり、この IP アドレスの変換を行う機能も、ルータの主な役割の１つです。

●セキュリティ観点での役割

ルータのセキュリティ観点での主な役割を解説します。
社内から社外への通信のみを許可する動作をすることで、社外からの不正な通信を防ぎます。社内パソコンから社外ウェブサイトへの通信を例に説明します。

パソコン（社内 IP アドレスA）がウェブサイト（社外 IP アドレスα）へ通信要求
　↓
ルータが社内 IP アドレス A を社外で使える社外 IP アドレスβに変換
　↓
ウェブサイトが社外 IP アドレスβにウェブサイトのデータを通信
　↓
ルータがデータの送り先を社外 IP アドレスβから社内 IP アドレス A に変換
　↓
パソコンでウェブサイトが表示される

ルータは、上記の通信の流れしか行わない、言い換えると「ルータは社内から社外への通信要求以外には応じない」という動きをすることで、ハッカー等社外からの不正な通信をブロックできます。

しかし、「ルータ側から不正侵入された」という話を聞いた方もいると思います、実際にそのような事例はあります。原因は、ルータの脆弱性や、VPN 機能の脆弱性や設定誤り等、様々あります。
VPN に関する事例は以下の記事をご確認ください。
中小企業におけるセキュリティ脅威への対策強化　～テレワーク時代の新しい働き方に潜むリスクと対策を学ぶ～
中小企業におけるセキュリティ脅威への対策強化　～システムの脆弱性を突いた攻撃への対策を学ぶ～

上記記事を深く理解する助けとなるＩＴの基本的な事項についても、今後記事にしたいと思います。

配信予定日：2025 年 12 月 5 日(金) 14:00 頃
カテゴリ：基礎から学ぶ！　セキュリティ
タグ：＃初級編＃実用編
過去記事焼き直し：しない（新規記事です）
記事 URL（新設します）：https://cybersecurity-taisaku.metro.tokyo.lg.jp/basics/imakikitai3/

いまさら聞けない！ネットで安全に買い物できる理由その 1

目次

東京都サイバーセキュリティ対策事業を通じ、情報セキュリティ対策はわかりづらいというお悩みをいただきます。解決策の一つとして**「情報セキュリティに限らずＩＴの基本的な事項を知る」**事があります。

今回はネットで安全に買い物ができる理由その 1 をご紹介いたします。

※なお、本記事は分かりやすさを重視し、技術的な事項は大幅に要約して説明をいたします。技術的に正しい事項を理解する必要がある場合は、別途、専門書等でご確認をお願いいたします。

●鍵マークがあれば安心
インターネット上で買い物をする際、個人情報やクレジットカード番号などを入力してもなぜ安全なのか、皆さんはどう考えているでしょうか。鍵マークがあれば安心、という言葉を聞いたことがある人もいると思います。
[鍵マークが出ている例（Microsoft Edge ブラウザ）]

[鍵マークが出ていない例（Microsoft Edge ブラウザ）]

上記の表示から考えると鍵マークが出ていれば「セキュリティ保護“あり”」なのだと理解している方が多いと思います。
しかし、実は冷静に考えると、すごい事が起きています。

●鍵配送問題

遠くにいる相手に情報を送る（通信する）には、通信途中で盗聴を防ぐため暗号化が使われます。暗号化の簡単な例を挙げます

UPLZP

これは暗号化されています。暗号化ルールは「アルファベット順から 1 文字ずらす（A→B、B→C・・・Y→Z、Z→A)」です。

事前に遠くにいる相手に暗号化ルールを伝え、相手は暗号化ルールの逆手順を行えばよい事がわかります。暗号化した情報を元に戻すことを復号化と言います、復号化を行うと上記は

TOKYO

となります。しかし、この暗号化ルールはシンプルで盗聴者に見抜かれそうです。それを防ぐには暗号化ルールを複雑する方法があります。例えば、あいうえお順にする、ある辞書のページ数にする（例えば“121”と書くと辞書の 121 ページに書かれた最初のアルファベット文字に変換する)、お互いしか知らない独自の変換表を使う、日時によって変換ルールを変更する等、暗号化ルールを複雑にする方法はたくさんあります。

ここまでの話を読んで課題に気付いた方はいるでしょうか。この暗号化ルール（以後、“鍵”と記載）は相手にあらかじめ伝えなくてはいけません。鍵を通信すると盗聴されますし、鍵を暗号化して通信すると相手が復号化できないです。このような課題を鍵配送問題と言います。

鍵配送問題は特に軍事上の通信で課題となっていました。「鍵を安全に相手に渡すのは、パソコンが上手くやっといてくれている」と思う方がいると思いますが、その通りです。現代の技術で解決済みです。

●公開鍵暗号方式

鍵配送問題を解決する手段として「公開鍵暗号方式」が 1977 年に発明され、インターネット上の安全な通信のため利用されています。仕組みをわかりやすく説明するため、例え話で説明します。
公開鍵暗号方式とは「南京錠を電子的に実現したもの」と考えるとわかりやすいです。南京

錠は、誰でも開錠状態から施錠できる「錠前」と、開錠のための「鍵」で出来ています。

錠前（開錠状態）⇒誰でも手で施錠できる。

錠前（施錠状態）

錠前の鍵　⇒錠前を開錠状態にできる。

南京錠を例にインターネット上の安全な通信の流れを説明すると以下になります。

① オンラインショッピング事業者は、錠前を世界中に配る（公開する）。
② 利用者は錠前を用いて個人情報やクレジットカード番号を暗号化し、オンラインショッピング側に通信する。
③ オンラインショッピング事業者は、自分しか保有していない錠前の鍵を使い、暗号化を解く（錠前を開錠する）。

ここで言う錠前を電子的に再現したものを「公開鍵」と言い、錠前を開錠できる鍵を「秘密鍵」と言います。
公開鍵はロック（暗号化）専用の鍵、秘密鍵は開錠専用の鍵と言えます。公開鍵から秘密鍵を特定することは技術的に困難です。

●暗号方式のいいとこ取りをした TLS

実際のインターネット上の通信では、様々な暗号方式の特性を使い分けた TLS（Transport Layer Security）という仕組みを利用しています。
公開鍵暗号方式は鍵配送問題を解決できますが、実はコンピュータの処理が大変です（時間がかかります）。そのため、暗号化ルール（鍵）だけを公開鍵暗号方式で相手に送り、その後の通信は処理が楽な共通鍵暗号方式（暗号化も復号化も同じ鍵を利用する方式）で行います。

これが TLS の仕組みなのですが、TLS では加えて「ハッシュ関数」という技術も用いています。技術的にかなり難しいので本記事では説明を割愛させていただきます。

今回はネットで安全に買い物できる理由を説明しました。しかし実は、今回の説明だけでは“安全”を説明するには不十分です。次回は「通信先が本当にその本人（実在する企業）なのか確認する技術」について説明したいと思います。

配信予定日：2025 年 12 月 5 日(金) 14:00 頃
カテゴリ：ビジネスヒント
タグ：＃知識編＃経営課題
過去記事焼き直し：しない（新規記事です）
記事 URL（新設します）：https://cybersecurity-taisaku.metro.tokyo.lg.jp/tip/security-hyoukaseido2/

サプライチェーン強化に向けたセキュリティ対策評価制度（２／２）

目次

前回は経済産業省が 2025 年 4 月に公表した「サプライチェーン強化に向けたセキュリティ対策評価制度構築に向けた中間取りまとめ」の概要として、本制度の趣旨・目的、期待される効果、★3～★5 の各段階の考え方等について解説しました。今回は本制度における評価スキームや実施に向けたスケジュール等ついて解説します。

●本制度のサプライヤー企業（取引先）への適用における考え方
サプライヤー企業への適用にあたっては、次の 3 つのサプライチェーンリスクに照らし、対象となる取引先を★4 または★3 の段階を適用する考え方がモデル分岐図として提示されています。

(1) 発注者の重要な機密情報（※）が取引先 IT 基盤で取扱われるか
(2) 取引先の事業中断により、自社業務に許容できない遅延が生じるか
(3) 取引先環境から発注者の内部システムへのアクセスが可能か

※当該情報を漏洩した場合における、社会的信用低下や損害賠償等の訴訟リスクなどビジネスへの影響が大きいもの。

(1)～(3)のいずれかが「YES」であれば、対象となる取引先に★4 の段階を適用することとしています。なお、★4 では対策の強度が不足している場合には、適用要件をさらに上乗せすることも想定します。

また、(2)の判断においては、次のような観点の例が示されています。

・製品・サービス供給の中断による自社への影響範囲
・同業他社からの調達可否
・在庫確保の困難さ

(1)～(3)が全て「NO」であれば、対象となる取引先にひとまず★3 の段階を適用しますが、次のような追加要素も加味し、★4 の段階を適用するべきかを検討・調整することとしています。

・直近で当該取引先または同業他社等でインシデントが観測される等、リスク増大が懸念されるか
・再委託先に自社にとって重要な事業者が含まれるか

●本制度の再委託先への適用における考え方

再委託先への本制度の適用においては、元の発注者ではなく、直接の取引先（委託先）による判断で実施することとしています。

その際、直接の取引先（委託先）が★4 の適用対象の場合、★4 の要求事項に「重要な取引先におけるセキュリティ対策状況の把握」があるため、重要な機密情報が提供されている再委託先等にも相応の要件を適用することが期待されます。

●本制度における評価スキーム

本制度における★3、★4 の評価スキームとして、次のように示されています。★5 については、「今後検討する（TBD：to be determined)」とのことです。

	★3	★4	★5
評価実施主体	適合性評価の対象となる組織自身 （自己評価）	認定機関から認定を受けた評価機関 （第三者評価）	TBD
有効期間	1 年	3 年	
維持に必要な手続き	有効期限を更新するため、要求事項の遵守状況について年次で自己評価 （専門家の助言プロセス有り）	・有効期間内は、1 年ごとに自己評価を実施（評価機関に提出） ・有効期限を更新する際（3 年に 1 回）は第三者評価が必要	

資格の取消し等	取得組織において虚偽報告、情報隠蔽等の不正行為が確認された場合、評価機関または認定機関から資格の一時停止または取消しを行う場合がある	

「サプライチェーン強化に向けたセキュリティ対策評価制度構築に向けた中間取りまとめ」より
(https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_supply_chain/pdf/20250414_2.pdf)

＜★3（自己評価）における評価プロセス＞
① 取得希望組織は、★3 要求事項に基づき自己評価を記入（必要に応じ、社内外の資格者※の助言を得る）
② 社内外の資格者は、記入内容を評価、要求事項に対する合否を判断
③ 取得希望組織または社内外の資格者は、登録機関に評価結果を提出
④ 登録機関は、申請内容に問題が認められない場合には台帳に登録・公開

※資格者として、情報処理安全確保支援士、セキュリティプレゼンター（IPA のセキュリティ対策資料等を活用して中小企業等に対して情報セキュリティの普及啓発を行う人材）、IT コーディネータ等、必要な知見・知識を持つ者の活用を検討。社内に資格者がいない場合は、社外に評価を依頼することを想定。

＜★4（第三者評価）における評価プロセス＞
① 認定機関が、評価機関・技術検証事業者を認定
② 取得希望組織は、★4 要求事項に基づき回答を準備
③ 取得希望組織は、評価機関または技術検証事業者に、検証・評価を依頼
④ 評価機関または技術検証事業者は、検証・評価を実施
⑤ 評価結果を取得希望組織に通知し、認定機関に提出
⑥ 認定機関は、「合格」とされた組織を台帳に登録し、公開

●本制度が効果的と想定される業界等
本制度が効果的と想定される業界として、次の 3 つを挙げており、優先的に制度活用を促進していくとしています。

(1) サプライチェーン発注者層
政府機関、重要インフラ事業者、主要製造業等、重要な機密情報を有し、高いセキュリティレベルが求められる業界

(2) 多様な業界から業務を受ける中間層

BPO（Business Process Outsourcing）事業者、製品・部品製造業等、重要な機密情報・重要な業務の委託を受け、様々な業界からセキュリティ要請を受けている業界・事業

(3) サプライチェーンを下支えするエンド層

情報管理や事業継続において重要な役割を果たす業界・事業者であり、BtoB を行う中小企業全般

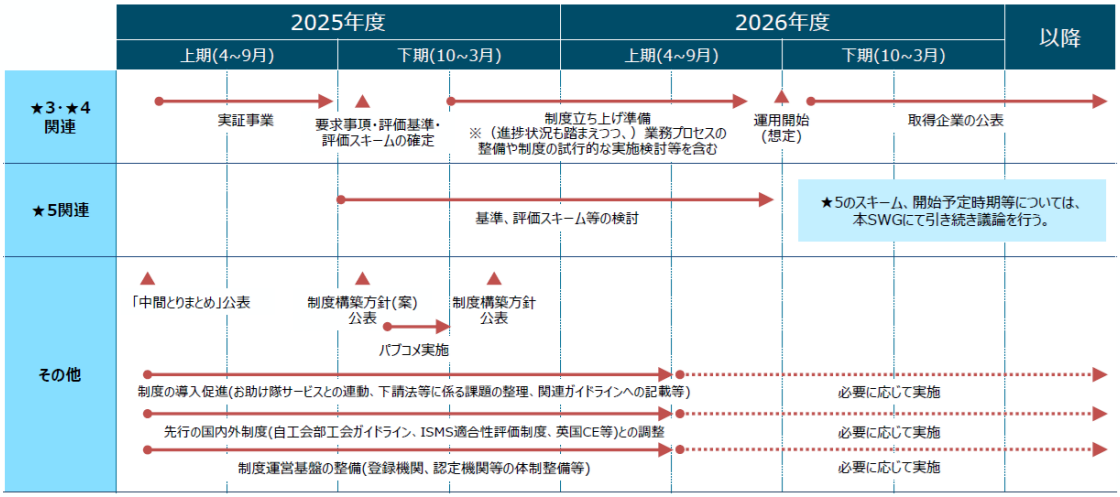
上記のうち(3)については、特に次のような事業者が対象となり、セキュリティ対策を進めるために、★3、★4 の活用が期待されています。

・比較的規模の大きな事業者（101 人以上）
・インシデントを経験した事業者
・既に対策に取り組んでいる事業者（SECURITY ACTION※宣言者） 等

※中小企業自らが情報セキュリティ対策に取組むことを自己宣言する制度であり、安全・安心な IT 社会を実現するために創設された。取組み目標に応じて「★一つ星」と「★★二つ星」がある。

●本制度の進め方及びスケジュール

次の図に示すように、2026 年度の本制度開始を目指し、今後は実証事業による制度案の検討と並行して、制度運営基盤の整備や利用促進等を進めていく予定です。



「サプライチェーン強化に向けたセキュリティ対策評価制度構築に向けた中間取りまとめ」より
(https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_supply_

chain/pdf/20250414_2.pdf)

配信予定日：2025 年 12 月 5 日(金) 14:00 頃
カテゴリ：ビジネスヒント
タグ：＃知識編＃経営課題＃インシデント対応強化
過去記事焼き直し：しない（新規記事です）
記事 URL（新設します）：https://cybersecurity-taisaku.metro.tokyo.lg.jp/tip/incident-taikendan2/

顧客の重要書類を紛失したら？インシデント体験から学ぶ

目次

ランサムウェアに感染して製品の流通が停止した等、昨今は様々なインシデントがメディアで報道され、被害を受けた企業はウェブサイトで経緯等を公開しています。
しかしながら、インシデント対応の詳細な経緯が公開されることはあまりありません。企業イメージに傷がつく、公開の必要性がない等、理由は様々と思いますが、失敗から学べることは多々あります。
今回は、過去のインシデント事例をフィクションとして修正し、失敗から学べるインシデント対応のポイントとして記事にしたいと思います。

●ある企業で発生したインシデント
A 社は従業員 200 名、主な事業は物件のリノベーションで、大手不動産会社から業務を請け負っています。情報セキュリティ対策は個人情報を保有する機会があまりないことから重視していなかったため、これからという状況です（※）。
※東京都中小企業サイバーセキュリティ対策事業だと「レベル 1：啓発事業」に取り組み始めているレベル。
参考：東京都サイバーセキュリティ対策事業の成り立ちと今後について
この企業において、個人情報を含む書類を紛失しました。その対応経緯を次項で紹介します。

●インシデント対応の経緯
[発覚当日]
・A 社から業務委託している工事会社の社員が、リノベーション物件の情報を記載した書類を紛失した。本来あってはならない事だが、その情報には前居住者の氏名等の個人情報も含まれていた。

・最後に書類を見たのが 2 日前であるが、どこで紛失したのか見当がつかない状況。
・紛失した情報は 7 名分の氏名、連絡先等と特定。
・業務委託元の大手不動産会社へ一次報告、詳細な報告を求められる。
・A 社社員は業務委託先の従業員とともに、2 日間の行動場所で書類を探す。
[1 日後]
・ 大手不動産会社へ報告、その後、以下を要求された。
  - 情報セキュリティポリシーの策定
  - 社員教育の実施
  - 業務委託先へ情報取扱いに関する契約、教育を実施
[3 日後～5 日後]
・紛失した情報の 7 名に対し個別にお詫び（菓子折り持参訪問）
・大手不動産会社へ詳細報告。
[1 か月後]
・情報セキュリティポリシーの策定（施行は半年後）

●インシデント対応の補足・考察
上記の例では、工事業者には不要な情報である個人情報を渡していたことで、個人情報漏えい事案となってしまいました。しかし元をたどると、個人情報は保有していないという思い込みや、情報管理をするための土台となる情報セキュリティポリシーが無かった事から発生したものと推察されます。
仮に情報セキュリティポリシーがあれば
・情報の授受管理
  ⇒工事業者には不要な情報である個人情報を渡すことは無かった。
・社員教育や業務委託先管理
  ⇒事業を行う全てのメンバーが情報取り扱いを意識することで、様々な局面で書類に不要な個人情報が記載されていることを指摘できた。また、書類の紛失も防げた。
と言ったことが期待できました。
東京都中小企業サイバーセキュリティ対策事業では「基本対策事業」という事業で、情報セキュリティポリシーの策定支援を行っています。今年度の参加企業募集は終了しましたが、来年度も事業が行われる可能性があります。東京都産業労働局のウェブサイトや公式 X 等を適宜ご確認ください。（ブックマークやフォローをお勧めします）

参考：令和 7 年度中小企業サイバーセキュリティ基本対策事業

配信予定日：2025 年 12 月 12 日(金) 14:00 頃
カテゴリ：基礎から学ぶ！ セキュリティ
タグ：＃初級編＃実用編
過去記事焼き直し：しない（新規記事です）
記事 URL（新設します）：https://cybersecurity-taisaku.metro.tokyo.lg.jp/basics/imakikitai4/

いまさら聞けない！ネットで安全に買い物できる理由その２

目次

東京都サイバーセキュリティ対策事業を通じ、情報セキュリティ対策はわかりづらいというお悩みをいただきます。解決策の一つとして**「情報セキュリティに限らずＩＴの基本的な事項を知る」**事があります。

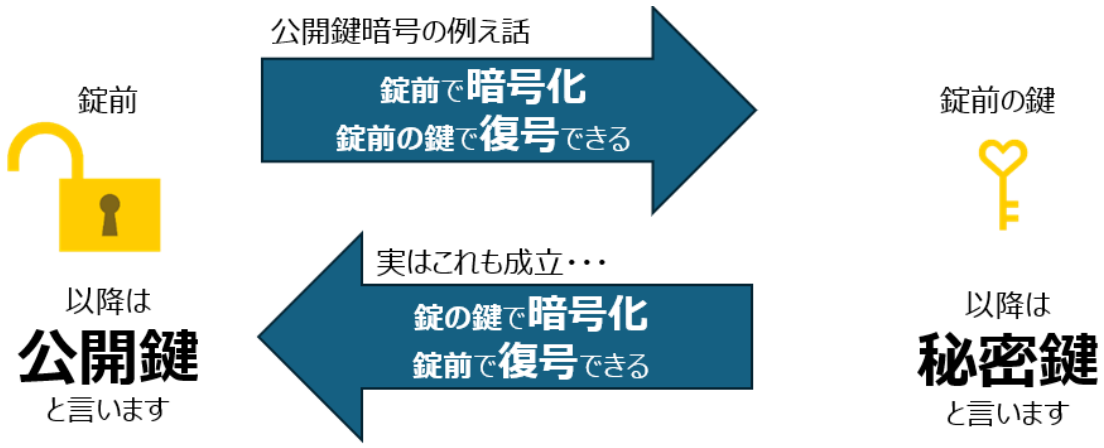
今回はネットで安全に買い物ができる理由その２をご紹介いたします。

※なお、本記事は分かりやすさを重視し、技術的な事項は大幅に要約して説明をいたします。技術的に正しい事項を理解する必要がある場合は、別途、専門書等でご確認をお願いいたします。

●通信先の相手は本物なのか
前回の記事「いまさら聞けない！ネットで安全に買い物できる理由その１」では遠くの相手と暗号化して通信する方法を説明しました。しかし、そもそも遠くの相手が本当に本人（例：オンラインショップ大手企業Ａ社）なのかを確認する必要があります。

これを解決する技術として「電子署名」があります。電子署名は、公開鍵暗号方式を逆手順で使う事で、通信先の相手が本物である事を証明する事が出来ます。

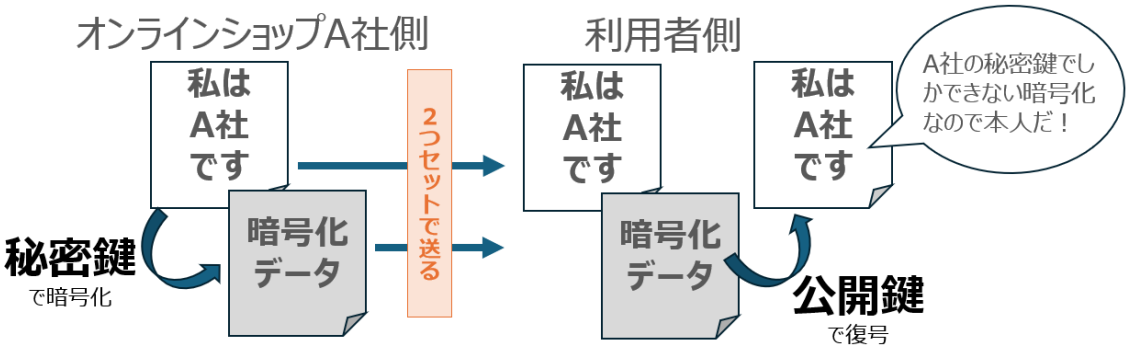
●電子署名を理解するために
　公開鍵暗号方式をわかりやすく理解いただくため「錠前」と「錠前の鍵」で説明しました。しかし電子署名を理解する上では、この例え話を変更する必要があります。実は「錠前の鍵で暗号化すると、錠前で復号できる」という使い方も可能です。



●電子署名で身分を証明

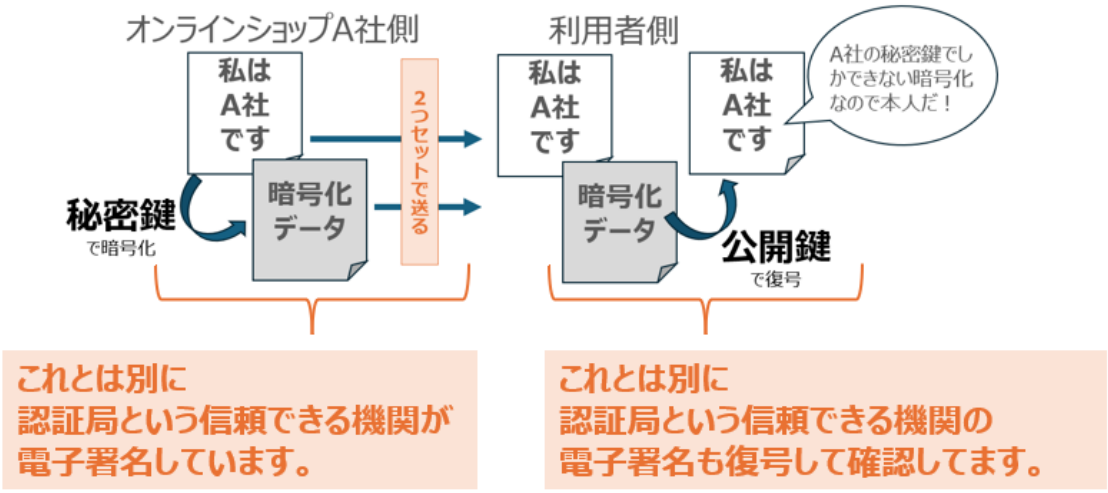
オンラインショップＡ社側は、自分の身分証を秘密鍵で暗号化し、身分証と暗号化データをセットで送信します。

利用者側は暗号化データを公開鍵で復号して突合します。



復号すると「私はＡ社です」というデータになる暗号化データはＡ社の秘密鍵でしか作成できないので、これは確かにＡ社が作成したものだとわかります。

しかしこれでも身分を証明するには不十分です、なりすましを防ぐために電子的な身分証を証明する認証局という機関（企業）があります。この認証局が、Ａ社の身分証に対して電子署名をしています。



認証局は基本的に皆さんがウェブサイトを閲覧する際にブラウザに記録されており、オンラインショップＡ社の身分証に電子署名している認証局が、ブラウザに記録されている認証局と異なる場合は以下のようなエラーが表示されます（ブラウザの種類や状況により様々な表示があります）。

認証局に電子署名をしてもらうには費用が掛かります。そのため、ウェブサーバの検証環境では認証局の電子署名をせずに検証を行う事があり、上記のようなエラーを見る事があります。インターネット上でも上記のようなエラーを見かける事がありますが、実はブラウザに記録されている認証局と異なる以外に、身分証の有効期限が切れている時もエラーになります。

ネットで安全に買い物できる理由、いかがでしたでしょうか？わかりやすく概略を理解いただくため技術的な要素は簡略化しましたが「ハッシュ関数」「SSL 証明

書」「SSL/TLS」「ECDSA」等様々な技術を用いてインターネットを安全に利用できるようにしています（今回は説明を割愛させていただきました）。

配信予定日：2025 年 12 月 12 日(金) 14:00 頃
カテゴリ：ビジネスヒント
タグ：＃知識編＃経営課題＃インシデント対応強化
過去記事焼き直し：しない（新規記事です）
記事 URL（新設します）：https://cybersecurity-taisaku.metro.tokyo.lg.jp/tip/yuryojirei1/

自分ごとにする方法！優良事例から学ぶ

目次

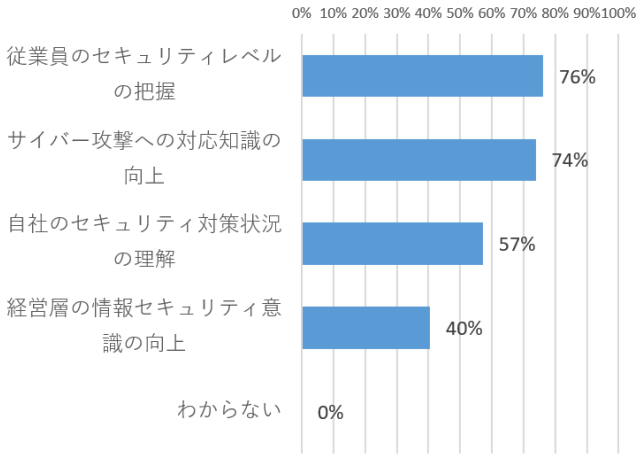
中小企業の経営者や情報システム担当者のお話を聞くと、よく出る悩みが「従業員の情報セキュリティ対策意識の向上」です。
今回は、情報セキュリティ教育に関する優良事例をご紹介します。

●標的型攻撃メール訓練の有効性
従業員の情報セキュリティ対策意識を向上するため、集合研修、e ラーニング、標的型攻撃メール訓練（以後、メール訓練と記載）を行っている企業は多いと思います。
メール訓練は、本物の不審メールを模したメールを体験することで学べるため、従業員一人一人が自分ごととして捉えるきっかけとなることを期待して実施する企業が多いです。

なお、東京都では「令和７年度サイバーセキュリティ啓発事業」の中でメール訓練を受ける事が出来ます。来年度の事業は現時点では未定ですが、継続される場合は東京都の「中小企業向けサイバーセキュリティ対策の極意ポータルサイト」に掲載されますので、適宜ご確認ください。

上記事業の令和６年度実施時に約５０社に参加いただきアンケートを取得しましたが、従業員のセキュリティレベルの把握、サイバー攻撃への対応知識の向上といった効果があったようです。

■ 標的型攻撃メール訓練の効果



一方で、メール訓練を毎年実施している企業からは、慣れてきた、開封が 0 にならない、特定の人が開封し続けている、という声を聞くことがあります。企業により課題は様々ですが、問題の 1 つとして「開封した人へのケア」があると思います。

●標的型攻撃メール訓練の効果を上げるには
具体的な取り組み事例を 2 つ紹介したいと思います。

1．再訓練
開封した人には個別に教育資料を配布し、再度メール訓練を行います。実際に行った企業様では再訓練により開封する人はほぼいないとの事です。さらにその後の毎年同社が行っているメール訓練でも開封をしないとの事です。

2．報告書作成
開封した人にはインシデント対応報告書を作成してもらいます。
報告書は例えば以下のようなフォーマットを使います。
＜例＞IPA 中小企業のためのセキュリティインシデント対応の手引き

インシデント対応時に整理しておくべき事項	
インシデントの分類	情報漏えい、ウィルス感染、システム停止など
事業者	事業者の名称 ※自社の受託案件に関連したインシデントの場合は委託元含む関係事業者の名称
責任者・担当者	本件に関する責任者および担当者の所属、氏名
発覚日時	インシデントを認知した日時
発生日時	調査で判明したインシデントの発生日時
発生事象	表面化している事柄、被害、影響など
対応経過	発生から現時点までの時系列での経過
想定される原因	現時点で想定される直接的な原因
被害を受けたシステムの状況	被害を受けたシステムの概要・詳細
システム構成・運用状況	システムの物理的所在地やOS、アプリケーションとバージョン構成 ※可能であれば簡単な構成図等も併記 システムの運用状況やセキュリティツール・サービスの利用状況等

※上記は情報システム担当者向けの項目もありますが、あえて考えて書いてもらっているとの事です。

●注意したい事項

上記の取組は、開封者への罰則のように映る方もいると思います。実際、開封者が職場内で悪いことをしたように映るケースはあります。確かに、開封した人は不審メールに引っかかってしまうような行動をしています。しかし、上記の取組をしている企業であっても毎年誰かが開封し 0 にはできない状況です。ある時点に行った訓練メールを開封しなかった人が、未来永劫開封しないとは言い切れません（過信は禁物です）。開封者を責め、未開封者を過信させるような状況にならないよう、経営者や情報システム担当者は最適な情報セキュリティ教育を企画推進することが求められます。

配信予定日：2025 年 12 月 12 日(金) 14:00 頃
カテゴリ：ビジネスヒント
タグ：＃知識編＃経営課題
過去記事焼き直し：しない（新規記事です）
記事 URL（新設します）：https://cybersecurity-taisaku.metro.tokyo.lg.jp/tip/security-guide1/

サイバーセキュリティ経営ガイドライン概説（１／４）

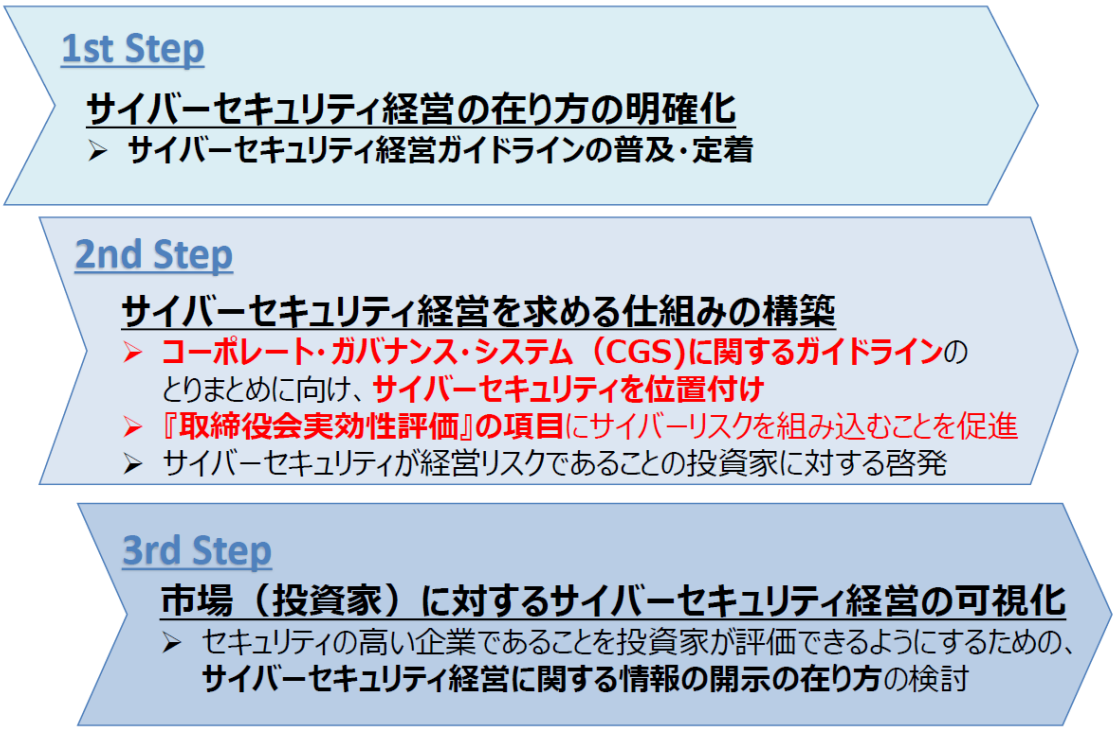
目次

サイバー攻撃の脅威は日々高まり続けており、セキュリティ対策に不備や欠陥があれば、自社のみならず、顧客や取引先にまで大きな被害を及ぼすことにもなりかねません。そうした事態に陥らないため、経営者には適切な経営資源を確保し、対策を施すことが求められます。今回は、経営者が自社の対策状況を知り、強化する上で活用すべきサイバーセキュリティ経営ガイドラインの概要について解説します。

●経済産業省によるサイバーセキュリティ強化への取組み
経済産業省では、従前から「産業サイバーセキュリティ強化へ向けたアクションプラン」を掲げており、その中の一つに「サイバーセキュリティ経営強化」があります。その実現に向け、次の 3 つの施策を推進してきました。

① 経営者向け：サイバーセキュリティ経営を促す仕組みの構築
② 現場の実務者向け：具体的な対策の導入を促す事例集と可視化ツールの整備
③ 中小企業向け：サイバー保険等と連携した『サイバーセキュリティお助け隊』の創設

そして、①の経営者向けの施策を推進するために策定されたのが、今回のテーマである「サイバーセキュリティ経営ガイドライン」なのです。なお、経済産業省では①の実現に向け、図に示す 3 つの Step で進めてきました。



経済産業省「産業サイバーセキュリティ強化へ向けたアクションプラン」より
（https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/002_03_00.pdf）

●サイバーセキュリティ経営ガイドラインとは

サイバーセキュリティ経営ガイドライン（以下「ガイドライン」と表記）は、大企業及び中小企業（小規模事業者を除く）のうち、IT に関するシステムやサービスなどを供給する企業及び経営戦略上 IT の利活用が不可欠である企業の経営者を対象に、経営者のリーダーシップの下で、サイバーセキュリティ対策を推進するため、経済産業省と独立行政法人 情報処理推進機構（IPA）が策定したガイドラインです。

近年サイバー攻撃はますます悪質・巧妙化しており、セキュリティ対策が不十分な企業を探しては脅し、金銭を奪うことを目的としたビジネスと化している感すらあります。たとえ身代金を支払わなかったとしても、サイバー攻撃によって顧客の個人情報や取引先と NDA(秘密保持契約）を締結している情報が外部に流出するようなことになれば、社外にまで大きく被害を広げ、その後の事業継続や取引に多大な影響を及ぼすことにもなりかねません。

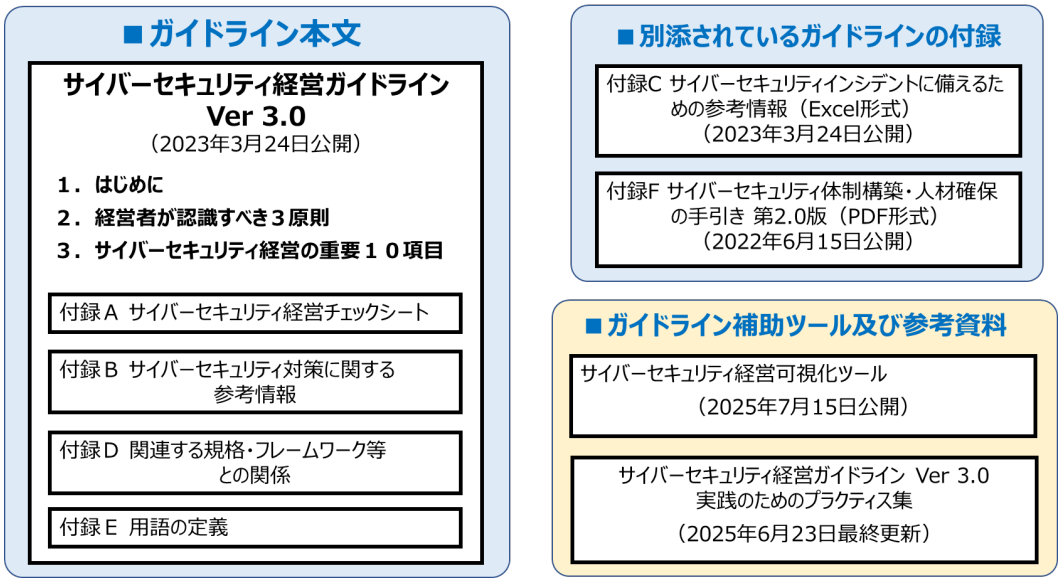
そのような事態に陥らないためには、企業の経営者がサイバー攻撃の脅威とリスクを認識した上で、人材や資金等の経営資源を確保し、インシデントの予防・検知・対処・回復といった観点から自社に必要な対策を見極め、実施していく必要があります。

とはいえ、現実にはどこから手を付ければ良いのか、自社のセキュリティ対策は適切に行われているのか、どこに不備があるのかよくわからないということも多いでしょう。そのような疑問や不安を低減・解消するための一助となるのがこのガイドラインです。

●ガイドラインの全体構成

ガイドラインは、図に示すように、本文と各種付録に加え、ガイドラインを補助するツールや実践するための参考資料等から構成されています。

ガイドライン本文は、2015 年 12 月に初版である Ver1.0 が公表された後、随時改訂が行われており，2023 年 3 月に Ver3.0 が公表されました。



サイバーセキュリティ経営ガイドラインの全体構成

●経営者が認識すべき 3 原則

ガイドラインでは「経営者が認識すべき 3 原則」として、ガイドライン本文の項番 2 で次が挙げられています。

（1）経営者は、サイバーセキュリティリスクが自社のリスクマネジメントにおける重要課題であることを認識し、自らのリーダーシップのもとで対策を進めることが必要

（経営者はリーダーシップをとってサイバー攻撃のリスクと企業への影響を考慮したサイバーセキュリティ対策を推進するとともに、企業の事業継続のためのセキュリティ投資を実施すべきである）

（2）サイバーセキュリティ確保に関する責務を全うするには、自社のみならず、国内外の拠点、ビジネスパートナーや委託先等、サプライチェーン全体にわたるサイバーセキュリティ対策への目配りが必要

（自社のサイバーセキュリティ対策にとどまらず、在来形の部品調達などの形態や規模にとどまらないクラウドサービスの利用等のデジタル環境を介した外部とのつながりの全て

を含むサプライチェーン全体を意識し、総合的なサイバーセキュリティ対策を実施すべきである）

（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対策を実施するためには、関係者との積極的なコミュニケーションが必要
（平時から社外の利害関係者（株主、顧客等）はもとより、社内の関係者（CIO 等セキュリティ担当者、事業担当責任者等）に事業継続に加えてサイバーセキュリティ対策に関する情報開示を行うことなどで信頼関係を醸成し、インシデント発生時にもコミュニケーションが円滑に進むよう備えるべきである。）

企業が効果的なサイバーセキュリティ対策を行うには、適切な人材や予算の確保等、適切な経営資源の確保やリーダーシップが必要であり、そのためには経営者の積極的な関与が不可欠です。
近年は、企業グループの子会社や取引先企業等を攻撃し、部品の供給やグループの本業であるサービスの提供に影響を及ぼすサプライチェーン攻撃の脅威も高まっています。そのため、自社にとどまらず、企業グループの子会社、取引先等も含めたサプライチェーンとしてのサイバーセキュリティリスクを認識し、対策を強化していく必要があります。
また、サイバー攻撃によって被害が発生した場合であっても、必要以上に関係者に不安を感じさせたり、不信感を持たれたりすることがないよう、日ごろからサイバーセキュリティ対策の実施状況等について情報開示する等、コミュニケーションを密にすることも重要です。

次回は、ガイドラインの「サイバーセキュリティ経営の重要１０項目」について解説します。

●参考情報
サイバーセキュリティ経営ガイドラインと支援ツール
(https://www.meti.go.jp/policy/netsecurity/mng_guide.html)

配信予定日：2025 年 12 月 24 日(水) 14:00 頃
カテゴリ：もっと知りたい！ セキュリティ
タグ：＃インシデント対応強化＃知識編
過去記事焼き直し：しない（新規記事です）
記事 URL（新設します）：https://cybersecurity-taisaku.metro.tokyo.lg.jp/know_more/log-forensic1/

ログ分析とデジタルフォレンジックス（１／２）

目次
●ログ分析の概要
●ログ分析による効果と分析例
●ログ分析における留意点

中小企業の経営者や情報システム担当者の皆さん、日々のセキュリティ対策、お疲れ様です。今回は、サーバやネットワーク機器、セキュリティ機器等の各種ログの概要やログ分析の必要性や実施例等について解説します。

●ログ分析の概要
IT システムから出力される各種ログは、OS、アプリケーション、通信機器などが、その稼働状態、処理の実行状況、障害・異常の発生状況等を示す記録です。出力されたログを分析し、その結果に基づいて対応することで、サイバー攻撃の発生を検知して早期に対処したり、将来的に発生する可能性のあるインシデントを未然に防いだりすることも可能となります。一般的な IT 環境における主にログを表に示します。ただし、実際に出力されるログの種類や内容についてはログの出力元であるサーバやセキュリティ製品の設定によります。

主なログの種類と概要

主なログの種類		概　要
OS が出力するログ	UNIX システムログ	Linux に代表される UNIX 系 OS が出力するログであり、ログイン、プロセスの起動／終了、コマンド実行等が記録される
	Windows イベントログ/PowerShell ログ	Windows 系 OS が出力するログ。アプリケーションの起動・停止、ログイン、ネットワークへの接続、システム設定の変更等、各種イベントの発生状況や PowerShell の実行履歴等が記録される

一般的なサーバソフトウェアが出力するログ	Web サーバアクセスログ	Web サーバが出力するログであり, 各クライアントからのアクセス履歴が記録される
	プロキシサーバログ	プロキシサーバが出力するログであり、内部ネットワークからインターネット上の Web サイトへのアクセス履歴等が記録される
	DNS クエリログ	DNS(Domain Name System)サーバが出力するログであり、名前解決要求の履歴が記録される
	ファイルサーバログ	ファイルサーバが出力するログであり、サーバ内のフォルダやファイルへのアクセス履歴、操作履歴等が記録される
	ディレクトリサーバ/認証サーバログ	Windows 環境における Active Directory 等のディレクトリサーバや認証サーバが出力するログであり、ログインの成功、失敗、権限昇格等の履歴が記録される
	DB ログ	DBMS(Database Management System)が出力するログであり、DB へのアクセス履歴、操作履歴等が記録される
セキュリティ関連製品が出力するログ	ファイアウォールログ	ファイアウォールが出力するログであり、通信パケットの接続許可（Accept)、破棄（Drop)、接続拒否通知及び破棄（Reject）の履歴やファイアウォールの稼働状況等が記録される
	IDS/IPS ログ	IDS(Intrusion Detection System：侵入検知システム)/IPS(Intrusion Prevention System：侵入防御システム)が出力するログであり、検知／遮断した攻撃や不審なアクセスの履歴が記録される
	AV ログ	AV(Anti-Virus)ソフトが出力するログであり、マルウェアの検知、駆除等の履歴が記録される。各 PC で出力されたログは AV 管理サーバに集約される仕組みになっている製品が多い
	EDR ログ	EDR(Endpoint Detection and Response)製品が出力するログであり、PC、サーバ等のエンドポイントで発生している事象（プロセス生成、ファイル操作、レジストリ更新、ネットワーク接続等）が記録される
	VPN ログ	VPN(Virtual Private Network)機能を提供する機器が出力するログであり、当該機器へ接続した端末の IP アドレス、認証の成功／失敗の履歴等が記録される
その他	クラウドサービスログ	各種クラウドサービスで出力されるログであり、アクセス履歴、ログインの成功、失敗、操作の履歴等が記録される

●ログ分析による効果と分析例

ログの分析により、次のような事象を早期に発見することが可能となります。仮に早期発見ができなくとも、ログはセキュリティインシデントが発生した場合に状況の調査や原因究明を行うための重要な証拠データとなるため、適切に出力・保存する必要があります。

① 内部ネットワークからインターネットへの不審なファイルの送信

・プロキシサーバのログから、業務時間外等にサイズの大きなファイルを送っている通信を抽出し、その通信を行っていた PC 等の操作内容と突合し、正当なものであるかどうかを確認する。

・ファイアウォールのログから、内部ネットワークからインターネットへの通信で Drop, Reject されているものを抽出し、それらが正規の利用者によるものであるかを確認する。

・クラウド上の外部ストレージサービスのログから、大量もしくはサイズの大きなファイルを送っている端末/ユーザを抽出し、正当なものであるかを確認する。

② 内部に侵入したマルウェア等による不審な通信

・プロキシサーバのログから、一定間隔で特定のサイトに同じサイズのファイルを連続して送っている通信等を抽出し、その通信を行っていた PC 等の操作内容と突合し、正当なものであるかどうかを確認する。

・Active Directory サーバのログから、ドメイン管理者の権限でアクセスしている不審な通信や、連続したログイン失敗、ログの削除等の履歴を抽出し、それらが正当なものであるかを確認する。

・DNS クエリログの内容（リクエスト内容や頻度等）から、マルウェアによる不審な通信が疑われるものを抽出し、正当なものであるかを確認する。

・ファイルサーバのログから、業務時間外等に頻繁にファイルにアクセスしている端末/ユーザを抽出し、それらが正当なものであるかどうかを確認する。

③ システム管理者の認識していない設定変更

・サーバの OS ログから、システム管理者の権限で実行された操作履歴や PowerShell の実行履歴等を抽出し、それらが正当なものであるかを確認する。

④ インターネットからの不正アクセスやその試み

・IDS/IPS のログやアラートから、不審なコマンドの実行やサイバー攻撃が疑われる通信を確認する。

・VPN のログから、海外から連続してログインに失敗している IP アドレスや、長時間接続しているユーザ等を抽出し、それらが正当なものであるかを確認する。

●ログ分析における留意点

ログはあくまでもシステムの振る舞いに関する記録であるため、不審な振る舞いをしていたユーザ ID や IP アドレスが特定できても、それを行っていた人間を特定することはできません。したがって、他人のユーザ ID 等を用いたなりすましによる不正アクセスなどを発見するのは困難です。そうした行為を発見するには、日頃から次のような情報を集めておき、ログの内容と比較するのが有効です。

・各ユーザの平均的なシステムの利用時間や利用時間帯
・各ユーザが通常使用している IP アドレス及びアプリケーション

今回は主なログの種類やログ分析の実施例等について解説しました。次回はログの運用管理における留意点やデジタルフォレンジックスの概要等について解説します。

配信予定日：2025 年 12 月 24 日(水) 14:00 頃
カテゴリ：基礎から学ぶ！ セキュリティ
タグ：＃初級編＃実用編
過去記事焼き直し：しない（新規記事です）
記事 URL（新設します）：https://cybersecurity-taisaku.metro.tokyo.lg.jp/basics/tlsgaisetu/

セキュアな通信を実現する TLS 概説

目次
●SSL の概要と常時 HTTPS 化の進行
●TLS の概要
●SSL/TLS のセキュリティ問題
●TLS1.3 におけるハンドシェイク手順

中小企業の経営者や情報システム担当者の皆さん、日々のセキュリティ対策、お疲れ様です。今回は、セキュアな通信を実現する代表的な技術として普及している TLS（Transport Layer Security）の概要や仕組みについて解説します。

●SSL の概要と常時 HTTPS 化の進行
TLS について解説する前に、その前身となった SSL（Secure Sockets Layer）について解説します。SSL は、かつての米国 Netscape Communications 社（現在は他社に吸収合併）が開発した認証と暗号化を行うための方式であり、主に Web ブラウザと Web サーバ間でデータを安全にやり取りするための業界標準プロトコルとして使用されていました。
その後 SSL は、2000 年頃から標準化が行われ、TLS に移行されましたが、”SSL”という名称が広く普及しているため、現在でも実際の技術は TLS であっても、”SSL”と呼ばれていることもあり、”SSL/TLS”と併記する場合もあります。
なお、TLS によって確立されるセキュアな通信経路上で HTTP（Hypertext Transfer Protocol）通信を行う仕組みが「HTTP over TLS」であり、URI スキーム「https」で表されます。多くの場合、ブラウザで Web サイトにアクセスすると、URL の先頭が”https://・・”となっていると思いますが、このとき、「HTTP over TLS」によってセキュアな通信が確立しています。
近年 Web サイト全体を HTTPS 化すること（常時 HTTPS 化）が進んでおり、株式会社フィードテイラーの調査によれば、国内上場企業における常時 SSL 化（HTTPS 化）は、2025 年 10 月の時点で 95%近くにまでなっているようです。

「常時 SSL 化 調査レポート 上場企業サイト対応状況」
(https://www.feedtailor.jp/report_aossl/)

●TLS の概要
TLS は、その名の通り、通信規約（プロトコル）の機能階層のうち、「トランスポート層」という層における暗号化プロトコルを中心とした技術で、SSL のバージョン 3.0 に基づいて標準化が行われました。その主な機能としては、デジタル証明書（Web サイトやクライアント PC 等の信頼性を証明するための電子的な身分証明書）によるサーバ、クライアント間の相互認証と通信データの暗号化を行います。なお、一般的な Web サイトではクライアントの認証は省略しており、サーバの認証と通信データの暗号化を主に行っています。
また、TLS は Web 通信で用いる HTTP だけでなく、メール送信に用いる SMTP（Simple Mail Transfer Protocol)、ファイル転送に用いる FTP（File Transfer Protocol）等、多くのプロトコルで使用することが可能です。

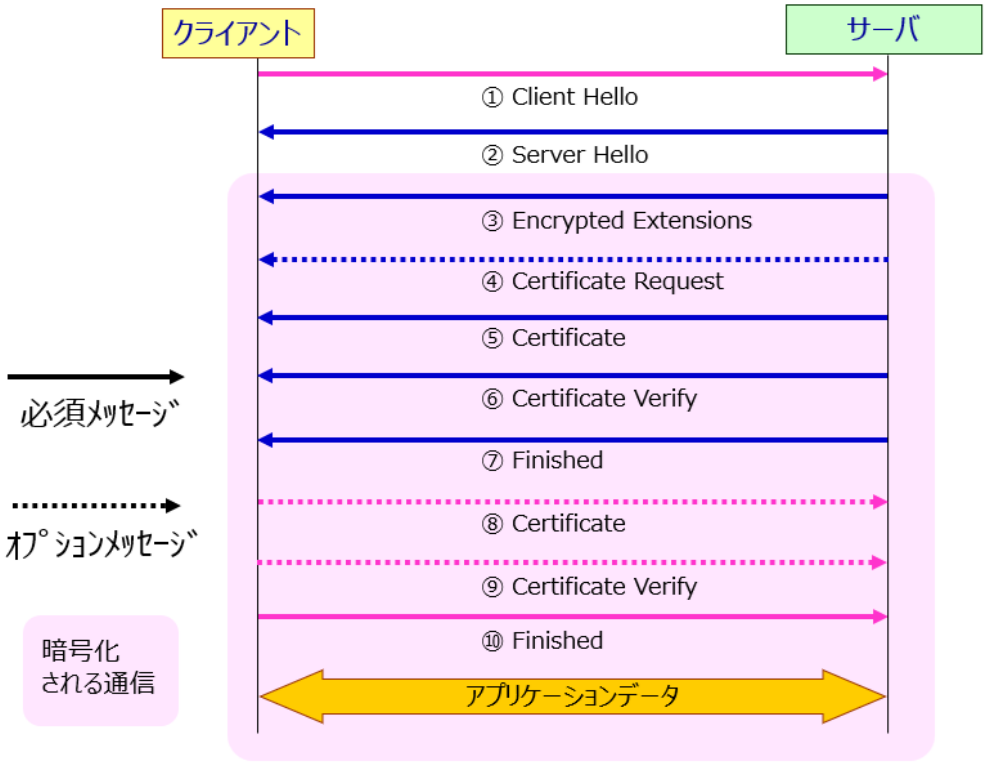
●SSL/TLS のセキュリティ問題
近年以下に示すように、SSL と TLS に複数の重大な脆弱性が発見されたため、現在では SSL の全バージョン及び TLS の初期バージョンについては使用が推奨されていません。そのため SSL/TLS については、TLS の最新バージョンである 1.3 を使用することが推奨されます。

＜SSL/TLS で発見された主な脆弱性＞
■SSL3.0 及び TLS1.0, TLS1.1 の「POODLE」脆弱性
SSL3.0 において、攻撃によって暗号化された通信が解読されてしまう脆弱性が存在することが 2014 年 10 月に公表されました。この脆弱性は POODLE（Padding Oracle On Downgraded Legacy Encryption）と名付けられています。その後、この脆弱性が TLS 1.0 , TLS 1.1 においても存在することが報告されました。

■SSL/TLS の「FREAK」脆弱性
SSL/TLS において、米国からの輸出規制により導入された弱い暗号技術をサポートしていたことに起因する脆弱性が存在することが 2015 年 3 月に公表されました。
この脆弱性は「FREAK：Factoring attack on RSA-EXPORT Keys」と名付けられており、一般的に利用されているブラウザ等に広く影響があることが判明しました（現在はいずれも脆弱性を修正したバージョンが提供されています)。
FREAK の脆弱性が悪用されると、攻撃によってバージョンの古い脆弱な暗号技術の使用が強制され、暗号化された通信が解読されてしまう可能性があります。このような攻撃をダウングレード攻撃と呼びます。

●TLS1.3 におけるハンドシェイク手順

ここから、TLS1.3 におけるセキュアな通信の確立（ハンドシェイク）手順について解説します。TLS1.3 におけるハンドシェイク手順は次の図のようになっています。



TLS1.3 におけるハンドシェイク手順

① Client Hello

クライアントが利用可能な暗号スイート（暗号アルゴリズムの組み合わせ）、鍵の合意に必要なクライアント側の情報、TLS バージョン等をサーバに送信し、通信の開始を通知します。

② Server Hello

サーバが、クライアントから送られてきた一覧の中から実際に使用する（合意した）暗号スイート、鍵合意に必要なサーバ側の情報、TLS バージョン等をクライアントに通知します。TLS1.3 では、この時点でクライアントとサーバ間での鍵合意が成立するため、これ以降の通信が暗号化されます。

③ Encrypted Extensions

サーバからの補足情報として、アプリケーション層で使用するプロトコルに関する情報（ALPN：Application-Layer Protocol Negotiation）等が送られます。

④ Certificate Request（クライアント認証を行う場合のみ）
サーバがクライアントに対し、デジタル証明書の提示を要求します。その際、サーバが信頼している認証機関の情報等も提示します。前述の通り、一般的な Web サイトではクライアントの認証は省略しているため、この工程はスキップされます。

⑤ Certificate
サーバが、自身のデジタル証明書をクライアントに送信します。

⑥ Certificate Verify
サーバが、自身のデジタル証明書の秘密鍵を用いて、ここまでの通信内容のダイジェスト（ハッシュ値※）からデジタル署名を生成し、検証情報として送信します。これを受信したクライアントは、⑤で受け取ったサーバのデジタル証明書に含まれる公開鍵を使い、デジタル署名を検証します。

※ハッシュ値
元のデータから固定長の値を出力する関数（ハッシュ関数）を用いて求めたもの。ハッシュ値により、大きなサイズのデータの一致や不一致を容易に照合することができます。

⑦ Finished
サーバがハンドシェイクの終了をクライアントに通知します。

⑧ Certificate（クライアント認証を行う場合のみ）
クライアントが、自身のデジタル証明書をサーバに送信します。一般的な Web サイトではこの工程はスキップされます。

⑨ Certificate Verify（クライアント認証を行う場合のみ）
クライアントのデジタル証明書の秘密鍵を用いて、ここまでの通信内容のダイジェストからデジタル署名を生成し、検証情報として送信します。これを受信したサーバは、⑧で受け取ったクライアントのデジタル証明書に含まれる公開鍵を使い、デジタル署名を検証します。一般的な Web サイトではこの工程はスキップされます。

⑩ Finished
クライアントがハンドシェイクの終了をサーバに通知します。以降はアプリケーションデー

タの通信が行われます。

TLS1.2 までのハンドシェイク手順では、クライアントとサーバ間で 2 往復のやり取りが必要であり、その最終段階で暗号化が開始される仕組みでした。TLS1.3 からこの仕組みが大幅に改善され、暗号化に必要な情報を一度に受け渡し、早い段階で暗号化通信を開始できるようになりました。

配信予定日：2025 年 12 月 24 日(水) 14:00 頃
カテゴリ：ビジネスヒント
タグ：＃知識編＃経営課題
過去記事焼き直し：しない（新規記事です）
記事 URL（新設します）：https://cybersecurity-taisaku.metro.tokyo.lg.jp/tip/security-guide2/

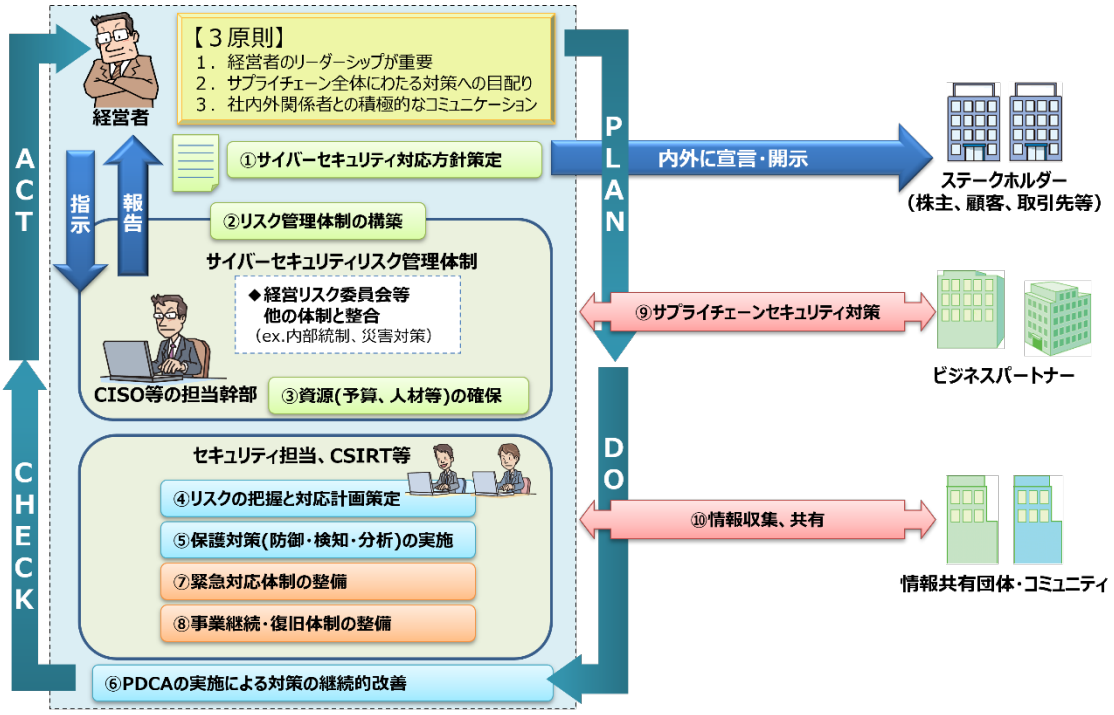
サイバーセキュリティ経営ガイドライン概説（２／４）

目次

前回は経済産業省によるサイバーセキュリティ強化への取組みの概要や、サイバーセキュリティ経営ガイドライン（以下「ガイドライン」と表記）の構成と「経営者が認識すべき３原則」について解説しました。今回は、「サイバーセキュリティ経営の重要１０項目」について解説します。

●サイバーセキュリティ経営の重要 10 項目の概要
ガイドラインでは、経営者は、CISO（Chief Information Security Officer）等に対して、重要１０項目を指示し、実施させる必要があるとしています。単に指示すればよいというわけではなく、経営者が自らの役割として実施方針の検討、予算や人材の割当、実施状況の確認や問題の把握と対応等を通じてリーダーシップを発揮することが求められます。
なお、自組織での対応が困難、もしくは専門事業者による実施が適切と判断される項目については、外部委託による実施も検討することとしています。

経済産業省では、ガイドラインの全体像を次の図で示しています。図中の①～⑩が、サイバーセキュリティ経営の重要 10 項目であり、ガイドラインの本文では「指示 1 ～指示 10」として解説されています。



サイバーセキュリティ経営ガイドラインの全体像
（https://www.meti.go.jp/policy/netsecurity/mng_guide.html）

●指示 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者が責任を負うべき経営リスクの一つとして認識し，組織全体としての対応方針（セキュリティポリシー）を策定させる。
・策定した対応方針を対外的な宣言として公表させる。

<解説>
企業として対応方針を明確にすることで、従業員等の意識や認識を合わせることが可能となり、また対外的に宣言することで、株主や顧客、取引先等の信頼性を高め、ブランド価値向上につながることにもつながります。

●指示 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リスクの管理に関する各関係者の役割と責任を明確にした上で、リスク管理体制を構築させる。

・サイバーセキュリティリスクの管理体制の構築にあたっては、組織内のガバナンスや内部統制、その他のリスク管理のための体制との整合を取らせる。

＜解説＞
サイバーセキュリティリスク管理体制が整備されていないと、責任の所在があいまいとなり、リスクに対応した適切な対策が講じられず、インシデントが発生する可能性が高まるとともに、発生時には被害が拡大することにもつながります。

●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
・サイバーセキュリティに関する残存リスクを許容範囲以下に抑制するための方策を検討させ、その実施に必要となる資源（予算、人材等）を確保した上で、具体的な対策に取り組ませる。
・全ての役職員に自らの業務遂行にあたってセキュリティを意識させ、それぞれのサイバーセキュリティ対策に関するスキル向上のための人材育成施策を実施させる。

＜解説＞
サイバーセキュリティ対策のための適切な予算の確保が出来ていないと、必要な対策の実施や人材の確保が困難となるほか、信頼できる外部のセキュリティベンダへの業務委託なども困難となります。

●指示 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
・事業に用いるデジタル環境、サービス及び情報を特定させ、それらに対するサイバー攻撃（過失や内部不正を含む）の脅威や影響度から、自組織や自ら提供する製品・サービスにおけるサイバーセキュリティリスクを識別させる。
・サイバー保険の活用や守るべき情報やデジタル基盤の保護に関する専門ベンダへの委託を含めたリスク対応計画を策定させ、対応後の残留リスクを識別させる。

＜解説＞
自組織のサイバーセキュリティリスクのアセスメントを行うことなく、他社の事例やベンダからの提案等をそのまま取り入れて実態にそぐわない対策を実施したとすれば、未対策のリスクによる事業の中断や機密情報の漏えい等、経営上許容できない大きな損失が発生する可能性があります。

●指示 5：サイバーセキュリティリスクに効果的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として、防御・検知・分析の各機能を実現する仕組みを構築させる。

・構築した仕組みについて、事業環境やリスクの変化に対応するための見直しを実施させる。

＜解説＞
サイバー攻撃を防御するための対策を行うだけでなく、攻撃をいち早く検知・分析し、それに基づく適切な対応がとれるようにしておく必要があります。

●指示 6：PDCA サイクルによるサイバーセキュリティ対策の継続的改善

・リスクの変化に対応し、組織や事業におけるリスク対応を継続的に改善させるため、サイバーセキュリティリスクの特徴を踏まえた PDCA サイクルを運用させる。
・経営者は対策の状況を定期的に報告させること等を通じて問題の早期発見に努め、問題の兆候を認識した場合は改善させる。
・株主やステークホルダーからの信頼を高めるため、改善状況を適切に開示させる。

＜解説＞
サイバーセキュリティ対策の実施状況等について経営者が定期的な報告等を受けておらず、自組織のリスクや問題を把握できていないと、適切な対策が実施されず、サイバー攻撃を受ける可能性が高まります。

●指示 7：インシデント発生時の緊急対応体制の整備
・影響範囲や損害の特定，被害拡大防止を図るための初動対応，再発防止策の検討を速やかに実施するため、制御系を含むサプライチェーン全体のインシデントに対応可能な体制（CSIRT 等）を整備させる。
・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ができる体制を整備させる。
・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る。

＜解説＞
インシデントの未然防止策をどれほど実施したとしても、その発生を完全に防ぐことはできないため、発生時に備えた体制整備や対策を確実に行うとともに、定期的な演習等によって対応力を強化・維持していくことが重要です。

●指示 8：インシデントによる被害に備えた事業継続・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る。

・制御系も含めた BCP との連携等，組織全体として有効かつ整合のとれた復旧目標計画を定めさせる。
・業務停止等からの復旧対応について，対象を IT 系・社内・インシデントに限定せず、サプライチェーンも含めた実践的な演習を実施させる。

＜解説＞
近年業務のデジタル環境への依存度がますます高まるなか、組織としての事業継続の観点から、業務の復旧プロセスと整合性のとれたデジタル環境の復旧計画と体制を整備する必要があります。

●指示 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状況把握及び対策
・サプライチェーン全体にわたって適切なサイバーセキュリティ対策が講じられるよう、国内外の拠点、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対策状況の把握を行わせる。
・ビジネスパートナー等との契約において、サイバーセキュリティリスクへの対応に関して担うべき役割と責任範囲を明確化するとともに、対策の導入支援や共同実施等、サプライチェーン全体での方策の実効性を高めるための適切な方策を検討させる。

＜解説＞
サプライチェーンを構成する自組織の国内外拠点、系列企業、ビジネスパートナー等において適切なサイバーセキュリティ対策が行われていないと、その一端を担う企業等が攻撃を受け、自組織やサプライチェーン全体に影響が及ぶ可能性があります。

●指示 10：サイバーセキュリティに関する情報の収集，共有及び開示の促進
・有益な情報を得るには自ら適切な情報提供を行う必要があるとの自覚のもと、サイバー攻撃や対策に関する情報共有を行う関係の構築及び被害の報告・公表への備えをさせる。
・入手した情報を有効活用するための環境整備をさせる。

＜解説＞
情報共有活動に参加することにより、他の組織が解析した攻撃手法等の情報を活用し、自組織で同様の被害が発生するのを未然に防止することが可能となります。

以上が「サイバーセキュリティ経営の重要１０項目」です。組織の実情やセキュリティ対策実施状況によって優先度は異なりますが、昨今のサイバー攻撃やインシデント事例等に照

らすと、いずれも重要な内容であることがおわかりいただけたかと思います。

次回以降は、ガイドラインの各種付録や補助ツール、参考資料をはじめ、ガイドラインの活用方法や実践方法等について解説します。

●参考情報
サイバーセキュリティ経営ガイドライン Ver 3.0
(https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide_v3.0.pdf)

配信予定日：2026 年 1 月 9 日(金) 14:00 頃
カテゴリ：もっと知りたい！ セキュリティ
タグ：＃知識編
過去記事焼き直し：しない（新規記事です）
記事 URL（新設します）:https://cybersecurity-taisaku.metro.tokyo.lg.jp/know_more/zero-sase/

ゼロトラストと SASE

目次
●ゼロトラストの概要
●NIST ZTA の概要
●ゼロトラストにおける 7 原則
●ゼロトラストの実現方式
●SASE の概要
●SASE を構成する主な技術やサービスと関連技術

中小企業の経営者や情報システム担当者の皆さん、日々のセキュリティ対策、お疲れ様です。
今回は、近年注目されているセキュリティモデルである「ゼロトラスト」と、クラウド環境におけるネットワークセキュリティモデルである「SASE（Secure Access Service Edge）」について解説します。

●ゼロトラストの概要
ゼロトラストは、2010 年に米国 Forrester Research 社の John Kindervag 氏が提唱したセキュリティの概念モデルであり、「ゼロトラストモデル」「ゼロトラストセキュリティ」とも呼ばれています。
ゼロトラストを直訳すると「何も信頼しない」となります。セキュリティモデルであるゼロトラストは、組織の IT 環境を構成する各種機器やアプリケーション、ネットワーク、端末、ユーザ等は「いずれも安全ではない可能性がある」という考え方に基づいてセキュリティ対策を行うというものです。そのためには、ユーザがサーバやアプリケーション等に対して何らかのリクエストを発行するごとに、端末やユーザの信頼性を都度確認するといった対応が必要となります。
これに対し、従来からのセキュリティの考え方は、組織の内部ネットワークは「トラスト（信頼できる）」で、組織外のインターネットなどは「アントラスト（信頼できない）」であるため、その境界をファイアウォールや VPN（Virtual Private Network）機器等で防御するというものであり、「境界防御モデル」と呼ばれています。

このモデルは、オンプレミスによる情報システムが大半で、端末もユーザも、その大半が社内ネットワークの内側にいるような場合にはある程度有効です。しかし、昨今のクラウドサービスやテレワークの急速な普及により、組織の IT 環境を構成するアプリケーションや端末などは各所に分散しており、境界防御モデルでは対応が困難になってきています。ゼロトラストは、そのように分散化が進んだ IT 環境において有効なセキュリティモデルとして注目されています。

●NIST ZTA の概要

NIST（National Institute of Standards and Technology：米国国立標準技術研究所）は、ゼロトラストに基づいた企業におけるサイバーセキュリティアーキテクチャのガイド文書として「SP 800-207：Zero Trust Architecture（ZTA）」を 2020 年 8 月に公開しています。ZTA は、サイバー攻撃によるデータ侵害を防止し、ラテラルムーブメント（横方向への感染拡大）を制限するよう設計されており、ゼロトラストにおける 7 原則、論理コンポーネント、導入する際のアプローチ方法やユースケース等が示されています。

Zero Trust Architecture（NIST）
(https://www.nist.gov/publications/zero-trust-architecture)

●ゼロトラストにおける 7 原則

NIST ZTA では、ゼロトラストモデルを実現するには次の 7 つの原則を満たす必要があるとしています。

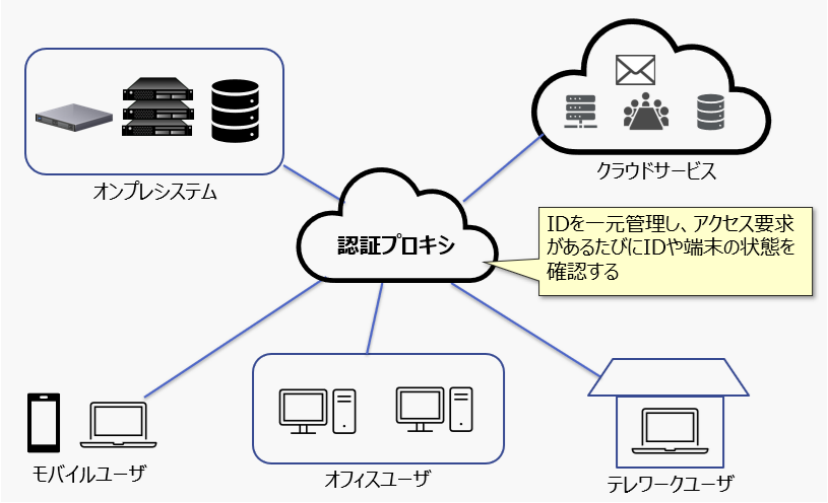
① すべてのデータソースと情報処理サービスをリソースと見なす
② ネットワークの場所に関係なくすべての通信を保護する
③ 組織の個々のリソースへのアクセスはセッションごとに付与する
④ リソースへのアクセスは動的なポリシーによって決定する
⑤ 組織が所有及び関連するすべての資産のセキュリティを監視・測定する
⑥ すべてのリソースへの認証と認可は動的であり、アクセスが許可される前に厳格に実施する
⑦ 資産とネットワーク及び通信の状態に関する情報を可能な限り収集し、それを用いてセキュリティの改善を図る

●ゼロトラストの実現方式

NIST ZTA では、ゼロトラストの実現方式として次の三つを挙げています。

■ID ガバナンス拡張方式

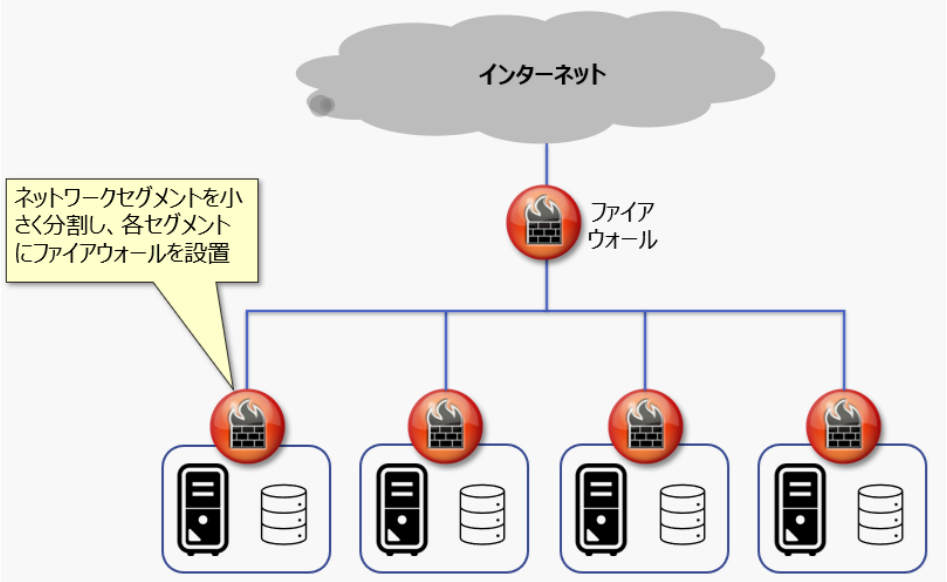
この方式では、クラウド上の認証プロキシが ID を一元管理します。ユーザがデータやアプリケーションにアクセスする際、クラウド上の認証プロキシを必ず経由させる構成とし、アクセス要求があるたびに ID や端末の状態を確認します。



ID ガバナンス拡張方式のイメージ

なお、ユーザ認証、シングルサインオン、ID 管理、ID 連携等の機能をクラウド上で提供するサービスは IDaaS（Identity as a Service）と呼ばれます。

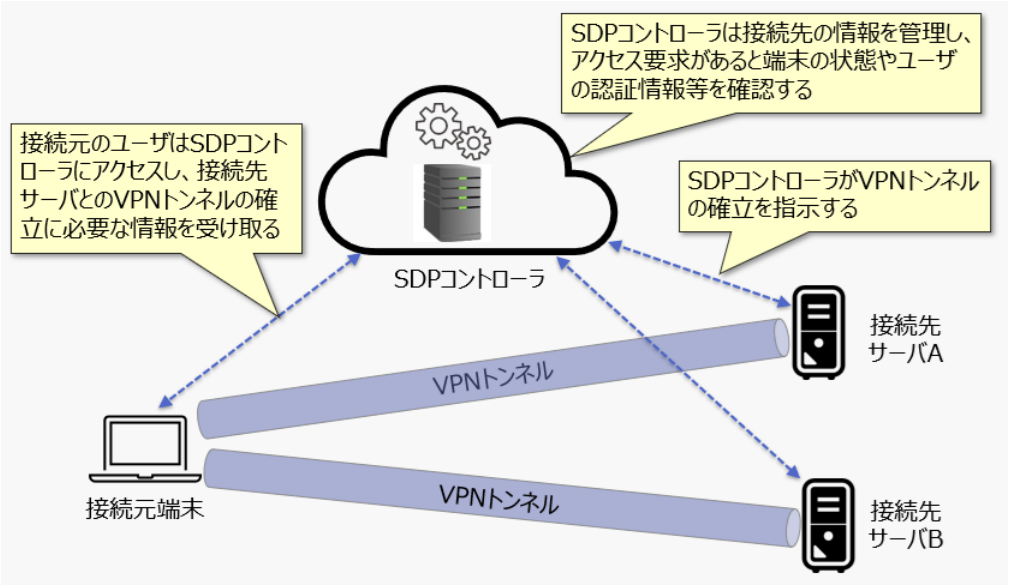
■マイクロセグメンテーション方式
この方式では、サービスやアプリケーションごとにネットワークセグメントを小さく分割し、セグメント間の通信をファイアウォール等で確認します。



マイクロセグメンテーション方式のイメージ

■ソフトウェア定義境界（SDP）方式
SDP（Software Defined Perimeter）コントローラがネットワークレベルで接続を管理する方式で、次のようにして接続を行います。

・接続元のユーザはまず SDP コントローラにアクセスする
・SDP コントローラが端末の状態やユーザの認証情報などを確認する
・SDP コントローラが接続に必要な情報を送り、VPN トンネル（安全な通信路）の確立を指示する
・接続元の端末と接続先のサーバが VPN トンネルを確立する



ソフトウェア定義境界方式のイメージ

SDP は、端末とサーバなどの接続をソフトウェアで集中的に管理・制御し、アクセス制御に関する設定を動的に変更してセキュアなネットワークを実現する技術です。動的に接続先が決まるため、通信経路を隠蔽し、攻撃者による不正アクセスや通信データの盗聴等を防ぐことができます。
主に SDP によって実現されるゼロトラスト志向の接続方式や、それを実装したサービス等は ZTNA（Zero Trust Network Access）とも呼ばれます。ZTNA は米国ガートナーが提唱したコンセプトであり、従来の VPN に代わるセキュアな接続方式として注目されています。

●SASE の概要

SASE（Secure Access Service Edge）は、米国ガートナーが 2019 年に提唱したクラウド環境におけるネットワークセキュリティモデルであり、「サシー」「サッシー」などと呼ばれます。SASE は、前出の ZTNA をはじめ、クラウド環境において必要となる各種ネットワークサービスとセキュリティサービスを統合し、包括的なサービスとして提供することをコンセプトとしています。

●SASE を構成する主な技術やサービスと関連技術

SASE は数多くの技術やサービスによって構成されます。SASE の末尾 E（Edge）とは、各種クラウドサービスやオフィス環境、テレワーク環境等がインターネットに接続する場所（アクセスポイント）にあるデバイスを意味しています。SASE は、オフィスやテレワーク等、利用者のシステム利用環境に依存しない各種ネットワークサービスとセキュリティサービスを提供します。

SASE を構成する主な技術やサービス

略称	概要
SD-WAN	Software Defined - WAN。物理的な WAN 上に、ソフトウェアによって構築された仮想的な WAN。SD-WAN は、遠隔地にある拠点間のネットワークであってもソフトウェアによって一元管理できるため、ネットワークの運用管理を柔軟かつ効率的に行うことが可能。
SWG	Secure Web Gateway。セキュアな Web アクセスを実現するクラウド上のプロキシサービスであり、コンテンツフィルタリング、アプリケーションフィルタリング、アンチウイルス、サンドボックス等の機能を提供する。
FWaaS	Firewall as a Service。クラウド上で提供される SaaS 型の Firewall サービスであり、設定されたルールに基づいて Edge やデバイス間のアクセス制御を行う。
ZTNA	Zero Trust Network Access。ゼロトラスト志向のセキュアなネットワーク接続サービスであり、従来の VPN に代わるものと位置付けられている。主に SDP によって実現される。
RBI	Remote Browser Isolation。Web ブラウザの機能を PC に代わってクラウド上で実行し、その結果を PC に画面転送するサービス。ブラウザを PC から分離（アイソレーション）することで、Web アクセスによって PC がマルウェアに感染するリスクを大きく低減することができる。
CASB	Cloud Access Security Broker（キャスビー）。2012 年に米国ガートナーが提唱したクラウド環境におけるセキュリティ対策のコンセプトであり、可視化、コントロール、データ保護、脅威防御等の機能から成る。

CSPM	Cloud Security Posture Management。クラウドサービス利用における設定ミス、構成不備、管理面の不備等によるセキュリティインシデントの発生リスクを低減することを目的とした状態監視機能や管理機能。
DLP	Data Loss Prevention。組織の機密データが外部に流出したり、持ち出されたりするのを防止するためのツールやサービス。監視対象とする機密データを判別するための条件や特徴、キーワードを登録しておくことで、該当するデータの流出や持ち出しを検知し、保護することが可能となる。
UEBA	User and Entity Behavior Analytics。ユーザ等の行動や活動内容を各種ログや監視ツール等を用いて解析することで、通常とは異なる行動や不正行為と疑われる事象を発見する。

配信予定日：2026 年 1 月 9 日(金) 14:00 頃
カテゴリ：もっと知りたい！ セキュリティ
タグ：＃知識編＃インシデント対応強化
過去記事焼き直し：しない（新規記事です）
記事 URL（新設します）: https://cybersecurity-taisaku.metro.tokyo.lg.jp/know_more/log-forensic2/

ログ分析・管理とデジタルフォレンジックス（2/2）

目次
●ログの運用管理上の留意点
●デジタルフォレンジックスの概要
●デジタルフォレンジックスにおける調査手順
●ログ分析サービスにおける実施手順
●用語解説

中小企業の経営者や情報システム担当者の皆さん、日々のセキュリティ対策、お疲れ様です。
前回はログの概要やログ分析について解説しました。
今回は、ログの運用管理における留意点やデジタルフォレンジックスの概要等について解説します。

●ログの運用管理上の留意点
ログの運用管理にあたっては、次の点に留意する必要があります。

① ログ取得、保存、管理に関するポリシーの策定及び設定
システムの標準的な設定では十分なログが出力されなかったり、逆に不要なログが大量に出力されたりする場合もあります。例えばファイアウォールでは、通信の遮断（Drop, Reject）ログのみを出力し、許可（Accept）ログについては大量になるため記録していないことも多くあります。しかし、内部に侵入したマルウェアの不正な通信を検知するためには、インターネット側に出ていく通信（アウトバウンド通信）の許可ログを取得しておく必要があります。このように、目的に応じて取得すべきログや、その保存期間、管理方法等のポリシーを策定し、対象となる機器に設定を施します。

② ログを安全に保存できるシステムの構築
攻撃者により、サーバや PC 等に保存されたログの改ざん、消去等が行われる可能性があります。また、設定によりますが、ストレージ等の容量不足から長期間にわたってログを保存

することが困難な場合も多くあります。なお、多くの場合、設定した容量の上限に達するとログは上書きされます。
そのため、十分なストレージ容量を備えたログ管理専用のシステムを構築する等して、ログを必要な期間にわたって安全に保存（保全）できる仕組みが必要となります。

③ 必要な情報を記録するためのシステム面での工夫
例えば、3 層構造の Web システムでは、DBMS（Database Management System）にアクセスしているのは常に Web アプリケーションサーバであるため、DBMS でログを残しても、個々の利用者については識別できないこともあります。このような場合には、アプリケーションを変更し、ユーザ情報を DBMS に引き渡すようにする必要があります。

④ ログの運用管理要員の確保及び手順書等の整備
ログの分析及び運用管理を行うための要員を確保するとともに、手順書等を整備し、そのための教育や訓練を実施しておく必要があります。

⑤ SIEM 等を活用したログの管理及び分析
インシデントを早期に検知するためには、ログを保存しておくだけでなく、前回解説したように、目的に応じて分析する必要があります。とはいえ、各サーバやネットワーク機器等に分散しているログを個々に分析するのは非効率であり、それらの相関を見ることも困難です。そのため、各種のログを効率的に収集し、分析するため、ログ管理専用システムや SIEM（Security Information and Event Management：セキュリティ情報イベント管理製品）と呼ばれるシステムを導入するケースが増えています。これらのシステムは、ログの正規化、集約化、相関分析、アラート通知などの機能を有しています。組織内に CSIRT（Computer Security Incident Response Team）や SOC（Security Operation Center）を設置している場合には、SOC 担当者がログ管理専用システムや SIEM を運用し、必要に応じて結果を CSIRT に報告します。

●デジタルフォレンジックスの概要
フォレンジックス（「フォレンジック」ともいいます）とは、本来事件や事故の証拠を収集し、裁判で立証する行為を意味します。デジタルフォレンジックス（「コンピュータフォレンジックス」ともいいます）とは、データの改ざんや不正アクセス等、コンピュータに関する犯罪の法的な証拠性を明らかにするために、原因究明に必要な機器やデータ、ログなどを保全したり、収集・分析したりすることです。広義には、セキュリティインシデント発生時に、関連する各種ログや侵害を受けた機器等を調査する行為全般をフォレンジックと呼びます。

●デジタルフォレンジックスにおける調査手順
デジタルフォレンジックスは、通常次のような手順で行います。

・対象となる PC やサーバを隔離する等して保全する
・対象 PC やサーバのキャッシュやメモリの内容を取得する
・対象 PC やサーバのディスクイメージを取得する
・ディスクイメージを調査用のディスク上にコピーする
・取得したデータの調査を実施する

ディスクイメージとは、調査対象である PC やサーバのハードディスク等のストレージの中身を物理的に完全にコピーしたものです。
なお、デジタルフォレンジックスで証拠を収集する際には、揮発性の高いものから順に進める必要があります。「RFC 3227：証拠収集とアーカイビングのためのガイドライン」によれば、揮発性の順序について、次のように例示されており、上のものほど揮発性が高く、収集の優先度も高くなります。

・レジスタ、キャッシュ
・ルーティングテーブル、ARP キャッシュ、プロセステーブル、メモリ等
・テンポラリファイルシステム
・ディスク
・当該システムと関連する遠隔ロギングと監視データ
・物理的設定、ネットワークトポロジ（接続形態）
・アーカイブ用メディア（CD, DVD 等）

●ログ分析サービスにおける実施手順
セキュリティベンダ等が提供しているログ分析サービスは、NDA（Non-Disclosure Agreement：秘密保持契約）締結後、通常次のような流れで実施されます。

① 事前調整（分析を依頼する組織とセキュリティベンダ間で実施）
・分析を依頼する理由、目的、緊急度等の確認
・対象となるシステム、ネットワーク構成等の確認
・分析対象ログの確定
・分析対象期間の確定
・分析日程、実施期間等の調整

② ログの収集・送付（分析を依頼する組織にて実施）

・分析対象ログを収集し、セキュリティベンダに送付

③ 付加情報の提供（分析を依頼する組織にて実施）
・分析する上で参考となる情報として、ネットワーク構成図、セキュリティ製品の設定内容（ファイアウォールのアクセス制御設定等)、IT 資産管理台帳等をセキュリティベンダに提供（可能な範囲で）

④ ログ分析（セキュリティベンダにて実施）
・分析の目的等を踏まえて対象ログを分析
・分析途中で報告すべき事象等が確認された場合には随時報告

⑤ 分析結果報告書の作成及び報告会の実施（セキュリティベンダにて実施）
・分析結果をとりまとめ、報告書を作成
・分析を依頼した組織の関係者への報告会を実施
・報告会では、分析の結果確認された事象や問題点を説明するとともに、その対応策等について助言（デジタルフォレンジックス等、更なる詳細調査が必要となる場合もある）

⑥ 分析結果及び助言等を踏まえた対応（例）
・デジタルフォレンジックス等による追加調査の実施
・セキュリティ機器等の設定見直し
・新たなセキュリティ対策製品やサービスの導入
など

●用語解説

■ARP キャッシュ

ARP（Address Resolution Protocol）は、IP アドレスから MAC アドレス（Ethernet の物理アドレス）を得るために使われるプロトコル。ARP キャッシュには、 IP アドレスと MAC アドレスを紐づけた情報が一時的に保存される。

配信予定日：2026 年 1 月 9 日(金) 14:00 頃
カテゴリ：ビジネスヒント
タグ：＃知識編＃経営課題
過去記事焼き直し：しない（新規記事です）
記事 URL（新設します）：https://cybersecurity-taisaku.metro.tokyo.lg.jp/tip/security-guide3/

サイバーセキュリティ経営ガイドライン概説（3/4）

目次

前回までサイバーセキュリティ経営ガイドライン（以下「ガイドライン」と表記）の構成や「経営者が認識すべき 3 原則」「サイバーセキュリティ経営の重要 10 項目」等について解説しました。ガイドラインには、自組織の実情を可視化するツールや参考資料等も数多く提供されています。今回は、それらの主な内容やポイント、活用方法等について解説します。

※前回までの記事
・サイバーセキュリティ経営ガイドライン概説（１／４）
・サイバーセキュリティ経営ガイドライン概説（２／４）

●ガイドラインの活用に向けて
ガイドラインにはサイバーセキュリティ対策を強化する上で参考となる事項が記載されていますが、熟読して内容を理解したとしても、それを実践し、自組織にサイバーセキュリティ経営を根付かせるのはそう容易ではありません。ガイドラインが求めている事項を実践する上で有効なのが、各種付録や補助ツール、参考資料類の活用です。ここでは、目的に応じた活用方法を紹介します。

●組織のサイバーセキュリティ対策の実施状況を知るには
ガイドライン実践の第一歩として、自組織の対策実施状況を把握することが挙げられます。この目的には、次の付録や補助ツール等が活用できます。

① ガイドライン付録Ａ サイバーセキュリティ経営チェックシート
② サイバーセキュリティ経営可視化ツール（Excel 版、Ver2.1）

ここからは、これらの内容や活用方法について見てみましょう。

①の「付録 A サイバーセキュリティ経営チェックシート」は、「経営者が認識すべき 3 原則」と「サイバーセキュリティ経営の重要 10 項目」の実践状況についてセルフチェックするためのシートです。「サイバーセキュリティ経営の重要 10 項目」のチェックシートの一部を次に示します。なお、各項目の右側にある括弧内の記号は NIST（米国国立標準技術研究所）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を示すもので、該当する項目には同フレームワークのサブカテゴリの識別子が記載されています。

指示 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

□	経営者が、サイバーセキュリティリスクを経営者が負うべき経営リスクの 1 つとして認識している	(－)
□	経営者が、組織全体としてのサイバーセキュリティリスクを考慮したサイバーセキュリティの基本方針を策定し、宣言している	(ID.GV-1)
□	法令・契約やガイドライン等の要求事項を把握し、基本方針等に反映している	(ID-GV-3) (DE.DP-2)

指示 2　サイバーセキュリティリスク管理体制の構築

□	組織の基本方針に基づき、CISO 等からなるサイバーセキュリティリスク管理体制を構築している	(ID-GV)
□	サイバーセキュリティリスクの管理に関する各関係者の役割と責任を明確にしている	(ID.GV-2)
□	組織内のガバナンスや内部統制、事業継続に関するリスク管理体制とサイバーセキュリティリスク管理体制の関係を明確にしている	(ID-GV-4)

「サイバーセキュリティ経営ガイドライン Ver 3.0　付録 A サイバーセキュリティ経営チェックシート」より
(https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide_v3.0.pdf)

サイバーセキュリティ経営チェックシートは PDF 形式ですが、コピー＆ペーストが可能であるため、編集可能な形式に変換することで、実際にチェックシートとして使用することが可能です。とはいえ、チェック結果の集計・可視化等は別途行う必要があるため、それほど使い勝手が良いとは言えません。
一方、次に紹介する②は IPA（独立行政法人 情報処理推進機構）のサイトでツールとして提供されており、実践状況をチェックするだけでなく、結果の集計や可視化まで行うことが可能です。

●サイバーセキュリティ経営可視化ツール

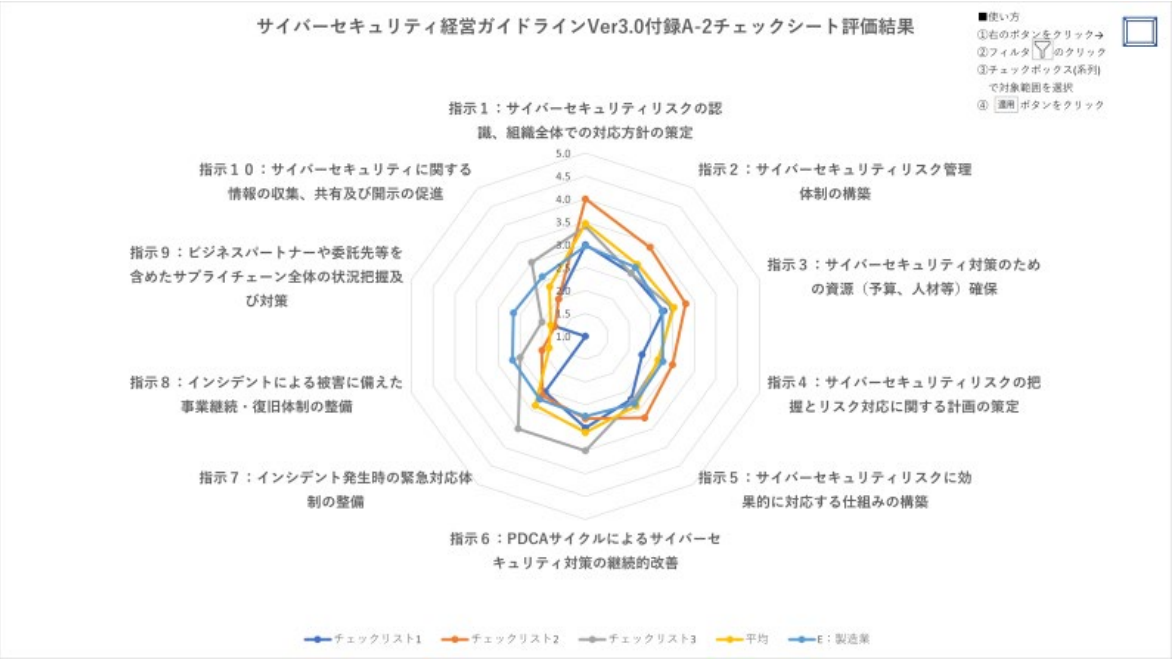
②の「サイバーセキュリティ経営可視化ツール（Excel 版、Ver2.1)」は、「使い方ガイド」「チェックリスト 1」「チェックリスト 2」「チェックリスト 3」「可視化結果」シートから構成されています。これらの中で、「チェックリスト（1〜3)」は、付録 A と同様に「サイバーセキュリティ経営の重要１０項目」の実践状況について自己点検するためのチェック項目集です。回答方式には成熟度モデルを採用しており、40 個の設問について 5 段階の選択式となっているほか、回答のヒントとして、用語の例、判断基準の例、参考情報等も示されています。

	サイバーセキュリティ経営ガイドライン Ver 3.0			可視化ツール						
指示	付録A-2のチェック項目			選択肢		回答欄（該当する箇所を選択）	重要	スコア	平均	回答のヒント
1 指示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	1	1-1	経営者が、サイバーセキュリティリスクを経営者が負うべき経営リスクの1つとして認識している	1	認識していない又は部分的である	○	□	0	0.00	【用語の説明】 ・経営者：取締役がいる会社の場合は取締役、いない会社・組織の場合は相当する権限を持った経営層 ・経営会議：取締役会設置会社の場合は取締役会、取締役会非設置会社やその他組織の場合は相当する会議体（経営戦略会議、社長会議、役員会議等、経営者が出席する会議） ・サイバーセキュリティリスク：対象は、制御システム等を有する部門のサイバーセキュリティも含む 【判断基準の例】 ・経営者が、ニュースや部下の報告等から昨今のサイバー攻撃の動向と自社への影響をある程度理解しているが、経営会議の資料等の形にしていなければレベル２ ・経営会議の議題に入っているが、資料は付録、CISO等の実施責任者の報告を垂れ流すだけ等であればレベル３以下（経営者が自分で考え、自分の言葉で語っているかがポイント。） ・経営会議の議題に入っており、かつ経営者が自分の考え、自分の言葉で議論していればレベル４ ・経営会議で議論されたことが現場に展開され、その結果がまた経営会議に報告・議論されるというプロセスが回っていればレベル５
				2	認識しているが、文書化等はできていない	○				
				3	認識しており、文書化されているが、対策は部下に任せている	○				
				4	認識しており、定期的に経営会議等で議論している	○				
				5	認識しており、経営会議等での議論を踏まえて継続的に改善している	○				
	2	1-2	経営者が、組織全体としてのサイバーセキュリティリスクを考慮したサイバーセキュリティの基本方針を策定し、宣言している	1	できていない又は部分的である	○	□	0		【用語の説明】 ・サイバーセキュリティの基本方針：セキュリティポリシーと同義 【判断基準の例】 ・基本方針が文書化されているが、その内容を経営者が把握・承認していなければレベル２ ・基本方針の内容が経営者に承認され、社外に公表されていればレベル３ ・自社の主な事業や業務プロセスにおけるサイバーセキュリティリスクの評価を行い、基本方針に変更の必要がないか等定期的に確認していればレベル4 ・サイバー攻撃の動向をウォッチしながら、基本方針に変更の必要がないか等適宜改訂していればレベル５。
				2	基本方針が策定され、文書化されている	○				
				3	基本方針が経営者により承認され、公表されている	○				
				4	サイバーセキュリティリスクの評価結果が基本方針に反映されている	○				
				5	基本方針が適宜改訂されている	○				

IPA「サイバーセキュリティ経営可視化ツールのチェックリスト」より（抜粋）
(https://www.ipa.go.jp/security/economics/checktool.html)

このツールは組織単体としてのチェック結果を可視化するだけでなく、グループ企業等における各社の状況を可視化し、比較できるようになっています。

グループ企業であれば、同じ Excel ファイル内に企業毎のチェックリストを作成し、それぞれ回答を記入します。その後、可視化結果シートで比較したい企業を選択すると、次のように各社の回答結果がレーダーチャート上に表示されます。



IPA「サイバーセキュリティ経営可視化ツール」より
(https://www.ipa.go.jp/security/economics/checktool.html)

このように、グループ企業等も含めた組織の実情を可視化することで、取り組むべき課題を把握し、改善に向けた対応策を検討することが可能となります。

次回は、「サイバーセキュリティ経営ガイドライン Ver 3.0 実践のためのプラクティス集」と「付録 F　サイバーセキュリティ体制構築・人材確保の手引き」について解説します。

配信予定日：2026 年 1 月 16 日(金) 14:00 頃
カテゴリ：基礎から学ぶ！ セキュリティ
タグ：＃知識編＃初級編
過去記事焼き直し：しない（新規記事です）
記事 URL（新設します）：https://cybersecurity-taisaku.metro.tokyo.lg.jp/basics/attack-damage1/

攻撃や被害が減らない理由（1/2）

目次
●攻撃されやすいサービス仕様やシステム仕様
●脆弱な Web サイトやソフトウェア等の存在
●用語解説

中小企業の経営者や情報システム担当者の皆さん、日々のセキュリティ対策、お疲れ様です。本記事では、昨今企業等におけるサイバー攻撃や、その被害が増加し続ける主な理由として考えられる事項を挙げ、解説します。

●攻撃されやすいサービス仕様やシステム仕様
まず、各種 IT サービスを提供している側の理由となりますが、サービスの仕様やシステムの仕様にセキュリティ面の不備等があり、攻撃者にそれを悪用されているということが挙げられます。その具体例を次に示します。

(1) アカウント（ID）の登録時等に十分な本人確認を行っていない
アカウントの登録時等に十分な本人確認を行っていないと、第三者のなりすましにより不正にアカウントを取得され、悪用されるリスクが高まります。
一時期、電子マネー決済サービス等に他人の銀行口座を勝手に紐づけ、不正に預金を引き出すといった事件が多発しましたが、その主な原因となったのが、メールアドレスのみで電子マネー口座が開設可能である等、本人確認が十分に行われていなかったことでした。

(2) パスワードの最低文字数が少なく、使用できる文字種も少ない
脆弱なパスワードが設定されていると、推測や総当たり攻撃等により、第三者に破られてしまう可能性が高まります。

(3) 多要素認証や二段階認証を実装していない

上記(2)に加え、多要素認証や二段階認証を実装していないと、第三者によってアカウントが不正利用されるリスクが格段に高まります。

(4) ログイン試行回数の制限がない

ログイン試行回数の制限がないと、何通りものパスワードを試すことができますので、推測やブルートフォース攻撃等により、パスワードが破られる可能性が増大します。

(5) メールアドレスをユーザ ID にしている

現状こうしたサービスは数多くありますが、結果として同じユーザ ID を様々なサービスで使いまわすことになり、またメールアドレスは第三者であっても比較的入手が容易であることから、不正なログインの試行に使われるリスクが高まります。

(6) ユーザ ID が数字のみ

金融系のサービスで口座番号がユーザ ID になっているケースのように、数字のみのユーザ ID は現在でも広く使われています。口座番号等であれば、正規の番号体系や書式がわかれば、他人のユーザ ID を推測することも比較的容易に可能です。

(7) システムで使用するアカウントに必要以上の権限を付与している

「セキュリティ対策における基本的な考え方」の回で解説したように、一般ユーザのアカウントにシステム管理者の権限（特権）を付与していた場合、サイバー攻撃によって一般ユーザの PC にマルウェアが感染し、アカウントを不正利用したとすれば、攻撃者はシステム管理者として全ての機能が使えるため、より甚大な被害を及ぼすことができてしまいます。

(8) 使用できる端末の制限がない

例えば広く利用されている LINE では、従来はアカウント登録を行った端末（スマートフォン等）でしか利用できない制限がありました。最近のアップデートにより、アカウント登録を行った端末（メイン端末）の他に、サブ端末として最大 3 台まで登録できるようになりましたが、サブ端末には一定の機能制限があります。一方、こうした端末の制限なく利用できるサービスも数多くあります。両者を比較すると、端末の制限がない方がユーザの利便性は高くなりますが、その反面、第三者にアカウントを不正利用されるリスクは高まります。

(9) 商品購入、送金等の重要な処理を行う際に再認証する必要がない

近年普及している 3D セキュアのように、重要な処理を行う前に再度ユーザ認証等を行うことにより、アカウント乗っ取り等による不正な処理が行われるリスクを低減するこ

とができます。一方そうした仕組みがないと、不正な処理が行われるリスクは高まります。

(10)新たな端末からの利用、口座情報やメールアドレスの変更等があっても通知されない
自分のアカウントに新たな端末からログインがあった場合にメール等で通知があれば、自分以外による不正なログインがあったとしてもそれを知ることができます。また、重要な登録情報の変更があった場合にも通知があれば、第三者による不正な変更等を知ることができます。一方、そうした通知が行われないサービスは、攻撃者にとっては非常に都合の良いものとなります。

●脆弱な Web サイトやソフトウェア等の存在
Web サイトによる新たなサービスや、新たなソフトウェア、アプリケーション（アプリ）等が次から次へとリリースされていますが、そうしたサイトやアプリ等には依然として深刻な脆弱性が存在していることが珍しくありません。

次のグラフは、IPA（独立行政法人 情報処理推進機構）が定期的に公表している「情報セキュリティ早期警戒パートナーシップ」における脆弱性関連情報の届出件数の年ごとの推移です。同パートナーシップは、IPA が受付機関、JPCERT コーディネーションセンター（JPCERT/CC）が調整機関となり、脆弱性関連情報の発見者、ソフトウェアの製品開発者、Web サイト運営者と協力をしながら、脆弱性に対処することを目的とした一連の活動です。

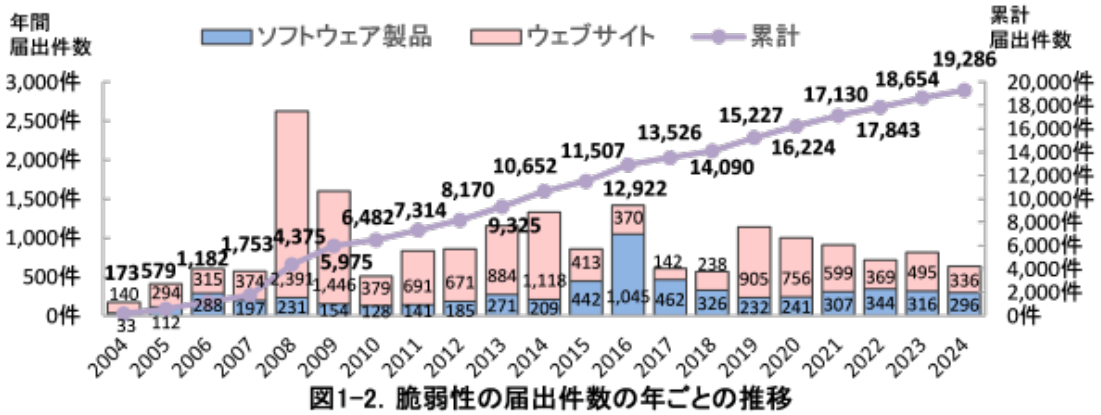


図1-2. 脆弱性の届出件数の年ごとの推移

ソフトウェア等の脆弱性関連情報に関する届出状況
(https://www.ipa.go.jp/security/reports/vuln/software/2024q4.html)

このように、件数は年によって増減がありますが、毎年 500 件を超える脆弱性関連情報の届出があります。もちろん届出されたものはごく一部であり、企業等が脆弱性診断によって

発見して対処したものや、いまだに発見されないままの脆弱性が無数にあるのが実態です。そうした脆弱なWebサイトやアプリ等がなくならない理由として、次のような状況が考えられます。

(1) 時間・予算の制約

Webサイトやアプリでサービスを提供する側が、短期間での開発/リリースを強く要望していながら、予算も限られており、その中でサイトやアプリを開発する側がなんとかそれを実現しようとしているケースです。このような場合、時間や予算の制約からセキュリティ対策はほとんど考慮されず、多くの脆弱性が内在したままリリースされることになります。

(2) セキュリティに関する要件や基準が不明確

Webサイトやアプリでサービスを提供する側が、発注/業務委託時に当該サービスにおけるセキュリティ面の要件や対策実施における基準等を示すことなく、全て開発者側に委ねているケースです。このような場合、セキュリティ対策は開発者が独自に判断し、自助努力で行われることになりますので、結果として十分な対策が行われない可能性も高まります。

(3) Webサイトやアプリを開発する側のスキルや経験が不足

Web サイトやアプリでサービスを提供する側が, 発注/業務委託時に当該サービスにおけるセキュリティ面の要件や対策実施における基準等を示したとしても、それを受託するベンダ等にセキュリティに関するスキルや経験がなければ、不十分な対策しか施されず、多くの脆弱性が内在する可能性があります。

今回は、サイバー攻撃や、その被害が増加し続ける理由として、攻撃されやすいサービス仕様やシステム仕様、脆弱なWebサイトやアプリ等の存在について解説しました。次回も引き続き、サイバー攻撃の被害が増加し続ける理由について解説します。

●用語解説

ブルートフォース攻撃

パスワードを破ることを目的とした攻撃手法の一つで、特定の文字数、文字種で設定され得る全ての組合せを試す方式。総当たり攻撃とも呼ばれる。

3D セキュア

ネットショッピング等でクレジットカード決済を行う際に、クレジットカード発行会社にあらかじめ登録したパスワード等、本人しか分からない情報を入力させることにより、なりすましによるクレジットカードの不正使用を防止する方式。

配信予定日：2026 年 1 月 16 日(金) 14:00 頃
カテゴリ：基礎から学ぶ！ セキュリティ
タグ：＃初級編 ＃実用編 ＃知識編
過去記事焼き直し：する（過去記事を上書きします）
過去記事：https://cybersecurity-taisaku.metro.tokyo.lg.jp/basics/kisokaramanabu15/

【令和 7 年度版】中小企業におけるセキュリティ脅威への対策強化　～情報セキュリティ対策の進め方『できるところから始めよう』～

目次

中小企業において、情報セキュリティの脅威はますます無視できない問題となっています。独立行政法人情報処理推進機構（IPA）が発行している「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」の「第 2 部実践編」では、具体的な対策方法と中小企業の経営者やシステム担当者がこれにどう取り組むべきかを詳しく解説しています。

情報セキュリティ対策に組織全体で取り組むには、実行すべき対策を決めて、従業員に周知する必要があります。
しかし、こうした作業を行うには情報セキュリティに関する知識や経験が必要となるため、それらの知識や経験に長けた人材がいないと対策が進まなくなることも考えられます。

このような背景から、IPA のガイドラインでは規模の小さな企業や、これまで十分な情報セキュリティ対策を実施してこなかった企業などを対象に、すぐに取り組める対策を示し、段階的に発展させていく計画を紹介しています。この「すぐに取り組める対策」が、多くの企業にとって無理なく、自社の状況に応じた対策を開始する道筋となります。

今回は、『できるところから始めよう』と題し、すぐに始められる情報セキュリティ対策に

焦点を当てて進めていきます。

1. 情報セキュリティに対する中小企業の現状と課題

サイバー攻撃が日常的に発生する状況下において、昨今では、情報セキュリティ対策が強固な大企業だけではなく、中小企業も攻撃の標的にされています。
同一のサプライチェーンを構成する中小企業を経由して、目的企業を攻撃する事例も多数報じられています。
中小企業であっても、サイバー攻撃により取引先企業の機密情報が漏えいするリスクや、次なる攻撃の足掛かりとされる可能性があることを念頭に置き、適切な対策を実施することが重要です。

IPA の「2024 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」報告書によると、情報セキュリティ対策に『投資していない』と回答した企業は約 62%と 2021 年度の 33.1%と比べて大幅に増加しています。

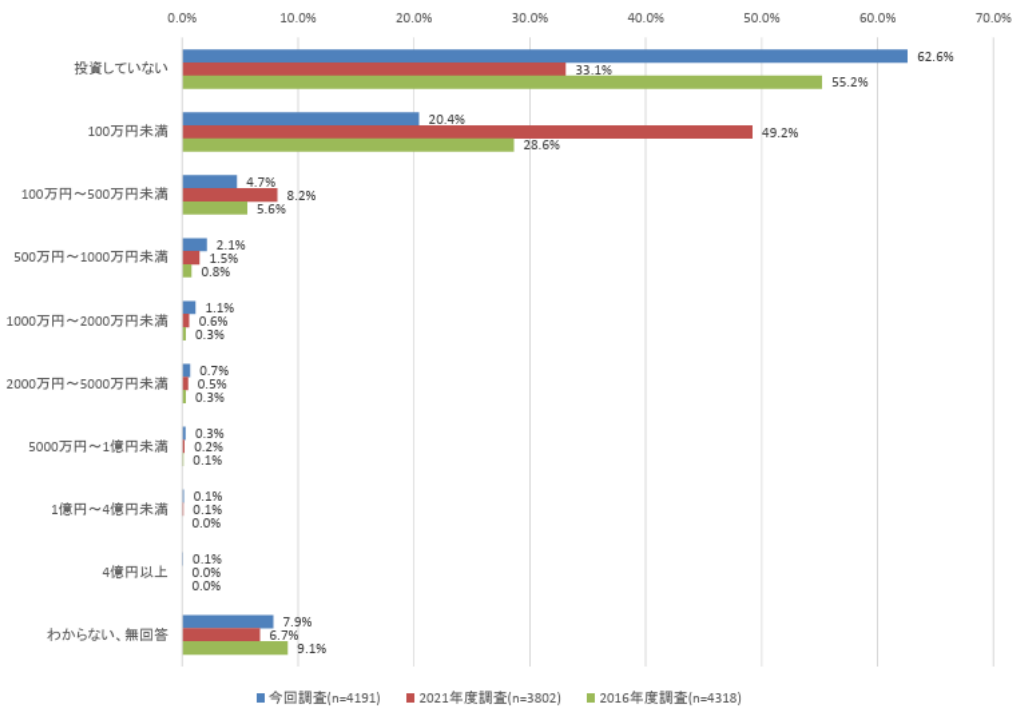


図 1．直近過去 3 期の情報セキュリティ投資額（前回調査との比較）（n=4191）
（引用:「2024 年度中小企業における情報セキュリティ対策に関する実態調査」報告書 P.178）

投資を行わなかった理由として、「必要性を感じない」(44%)、「費用対効果が不明」(24%)、「コストが高い」（21%）が上位を占めていますが、近年は「人材不足」も大きな課題とな

っています。
なお、「必要性を感じていない」理由として中小企業(101 名以上)では「既に十分な対策がとられているから」が最も多く 62%、小規模企業者では「重要情報を保有していないため」が 38%と最も多く、次いで「他社とのネットワーク接続が無いため」が 32%となっています（下図参照)。

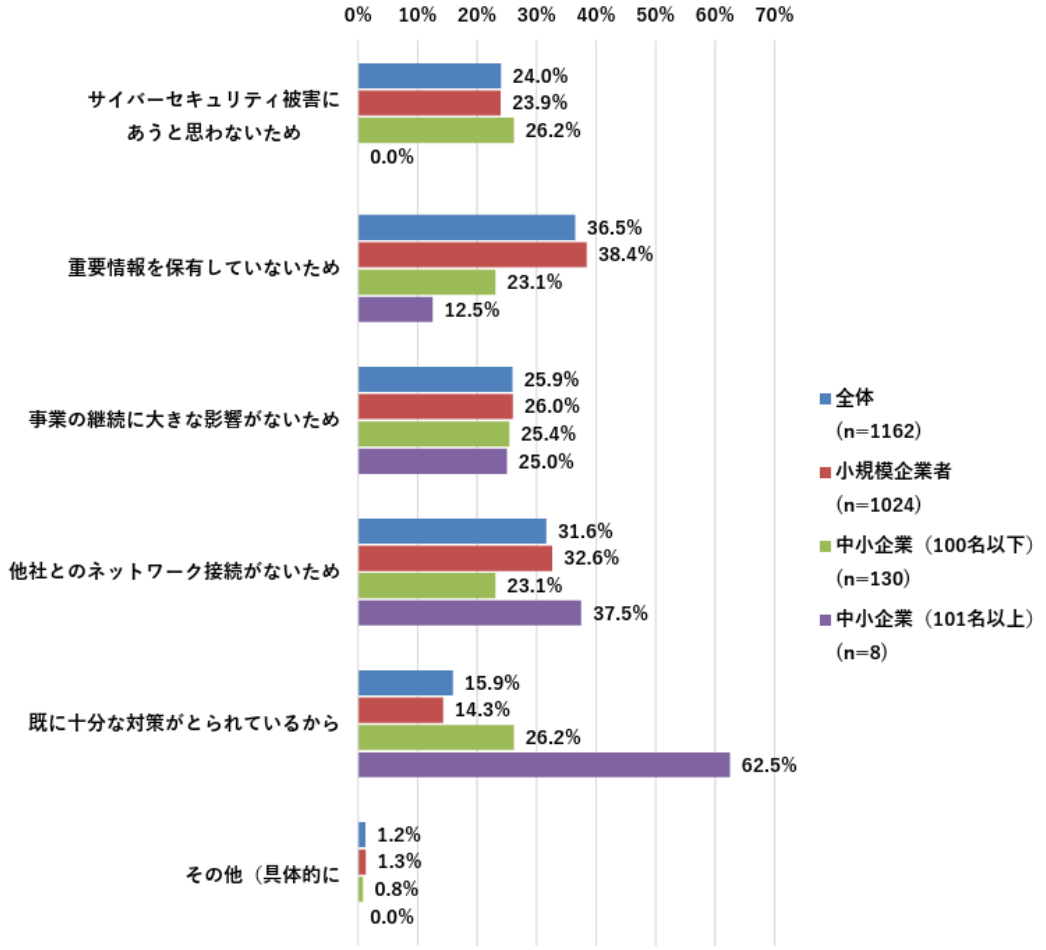


図 2. 情報セキュリティ対策投資に「必要性を感じていない」と回答した理由（企業規模別）（n=1162）
(引用:「2024 年度中小企業における情報セキュリティ対策に関する実態調査」報告書 P.113)

2. 情報セキュリティ 5 か条から始めるセキュリティ対策

多くの中小企業にとって、情報セキュリティは「守るべき秘密情報はない」などの物理的理由や、「費用対効果が見えない」「自社は攻撃の対象にならない」という心理的理由から対策が後手に回りがちです。また一方で、必要性は十分に認識しているが、大掛かりでかつ精巧な対策は大変で、なかなか始められないという声も聞きます。

インターネットの普及に伴い、攻撃者の手口は年々巧妙かつ悪質になっており、中小企業も無関係ではいられません。
「情報セキュリティ５か条」では企業の規模に関わらず、重要な基本対策が５項目にまとめられています。必ず実行しましょう。

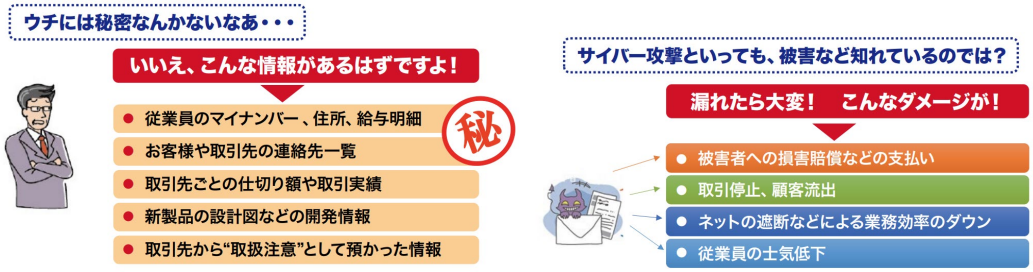


図３．中小企業の思い込み
（引用：情報セキュリティ５か条）

（1）OS やソフトウェアは常に最新の状態にしよう！

OS やソフトウェアを古い状態で放置していると、セキュリティ上の脆弱性を抱えたままになり、それを悪用した攻撃によりウイルス感染するリスクが高まります。お使いの OS やソフトウェアに修正プログラムを適用するなど、常に最新の状態にしましょう。

【対策例】

・Windows Update（Windows OS の場合）、ソフトウェア・アップデート（macOS の場合）などベンダが提供するサービスを実行する。OS ソフトウェアの自動更新を有効化する。
・Adobe Acrobat Reader やブラウザなど、利用中のソフトウェアを最新版にする。
・テレワークで利用するパソコンのソフトウェアや、Wi-Fi ルーターのファームウェアを最新版にする。
・クラウドサービスの脆弱性管理を徹底する。
・利用中のソフトウェアに脆弱性が存在しないか、「MyJVN バージョンチェッカ※」や「脆弱性対策情報データベース※」で確認する。
※MyJVN バージョンチェッカは、パソコンにインストールされているソフトウェア製品が最新かどうかを簡単な操作で確認できるツールです。
※脆弱性対策情報データベースは、国内外問わず日々公開される脆弱性対策情報を収集、蓄積することを目的とした IPA が提供するデータベースです。

（2）ウイルス対策ソフトを導入しよう！

近年、ファイルの暗号化や、パスワードを盗み、遠隔操作を行うウイルスが増加しています。ウイルス対策ソフトを導入し、ウイルス定義ファイル（パターンファイル）を自動更新設定

にすることで、新たな脅威にも対応できるようにするとともに、EDR や XDR など高度な対策が推奨されています。

【対策例】
・ウイルス定義ファイルが自動更新されるように設定する。
・統合型のセキュリティ対策ソフトの導入を検討する。
・OS に標準搭載されているセキュリティ機能（Windows Defender 等）を有効活用する。
・テレワークで利用するパソコン等の端末にウイルス対策ソフトを導入し、ウイルス定義ファイルを最新の状態にする。

（3）パスワードを強化しよう！
パスワードの解析や流出による不正アクセスの被害は依然として多発しています。
強固なパスワードを設定するために、パスワードは「長く」し、多要素認証（MFA）の必須化などを組み合わせましょう。

【対策例】
・パスワードは 12 文字以上で「できるだけ長く」する。
・名前、電話番号、誕生日、簡単な英単語などは使わず、推測できないようにする。
・同じ ID・パスワードを複数のサービスで「使い回さない」。
・テレワークで VPN やクラウドサービスを利用する際、多段階認証や多要素認証を必須化する。
・長文のパスフレーズ（単語ではなく文章のような長い文字列）推奨

（4）共有設定を見直そう！
データ保管などのクラウドストレージやネットワーク接続した複合機の設定を誤ったために、無関係な人に情報を見られてしまうといった情報漏えいのケースが増えています。データ共有時の設定を確認し、適切な権限を持った人だけがデータにアクセスできるようにしましょう。

【対策例】
・ウェブサービス、クラウドストレージ、ネットワーク接続の複合機・カメラ、ハードディスク（NAS：Network Attached Storage）などの共有範囲を限定する。
・従業員の異動や退職時には速やかに設定を変更（削除）する。
・テレワークで使用するパソコン等は他者と共有しない。共有せざるを得ない場合は、別途ユーザーアカウントを作成する。
・外出先でフリーWi-Fi は極力使わない。やむを得ず利用する場合には、「セキュリティ保護あり」のアクセスポイントを利用する。また、パソコンのファイル共有をオフにする。

（5）脅威や攻撃の手口を知ろう！

攻撃者が取引先や関係者を装い、ウイルスを仕込んだメールを送ってきたり、正規のウェブサイトに似せた偽サイト（フィッシングサイト）を立ち上げて ID・パスワードを盗もうとしたりする巧妙な手口が増えています。常に最新の脅威や攻撃の手口の動向を追って、対策をとりましょう。

【対策例】

・IPA など、セキュリティ専門機関のウェブサイトやメールマガジンで最新の脅威や攻撃の手口を知る。

・利用中のインターネットバンキングやクラウドサービスなどが提供する注意喚起を確認する。

・管理者が従業員に適宜注意喚起し、セキュリティに関する懸念があった場合は、速やかに報告するよう従業員教育を実施する。

3. 効果的な取組事例

【業種共通の対策】

2024 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において、効果的な取組事例が紹介されており、業界共通の対策として以下が紹介されています。

（1） **SECURITY ACTION 二つ星の対策実施によるサイバーインシデント被害低減の効果**

・SECURITY ACTION 二つ星の対策(「5 分でできる！情報セキュリティ自社診断」の診断項目）を多く実施している企業ほど、サイバーインシデント被害が少なく、被害額も少ないと回答していることが明らかになっています。診断項目の実施により、サイバーインシデント被害（発生率・被害額）の低減が期待されます。

（2） **第三者評価制度（ISMS 認証、P マーク）の取得による取引先からの信頼獲得の効果**

・第三者評価制度（ISMS 認証、P マーク）を取得している企業では、取引先からのサイバーセキュリティ要請に応じたことが取引につながった大きな要因であると考えている企業の割合が、取得していない企業に比べ約 2 倍となりました。これは、サイバーセキュリティ対策に関する第三者評価制度の取得が、取引上の信頼を得るための重要な要素であることを示しています。

（3） **サイバーセキュリティ体制の整備による取引先からの信頼獲得の効果**

・普段からサイバーセキュリティ体制が整備されている企業では、取引先からのサイバーセキュリティ要請に応じたことが取引につながった大きな要因であると考えている割合が、未整備の企業の約 2 倍になりました。これは、サイバーセキュリティ体制の整備が取引上の信頼を得るための重要な要素であることを示しています。

（４） **取引における自社の事業へのリスク認識を持つことによる取引先からの信頼獲得の効果**

・他社との取引におけるリスク認識がある企業では、取引先からのサイバーセキュリティ要請に応じたことが取引につながった大きな要因であると考えている企業が、リスク認識がない企業の約２倍となりました。これは、サイバーセキュリティ対策を実施する上で、取引におけるリスク認識をもつことが、取引上の信頼を得るための重要な要素であることを示しています。

（引用：2024 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～業種ごとの効果的な取組事例集～より一部抜粋）

4. SECURITY ACTION「★一つ星」取得のすすめ

SECURITY ACTION は、中小企業が自主的に情報セキュリティ対策に取り組む姿勢を自己宣言する制度です。安全・安心な IT 社会を実現するために創設されました。

「★一つ星」を宣言するには、情報セキュリティ５か条に従って状況のチェックと対策に取り組みます。なお、「★一つ星」は、これから情報セキュリティ５か条に取り組むことを宣言するものであり、対策実施前でも申込みは可能で、情報セキュリティ対策に取り組んだことのない企業でも、すぐに始めることができます。

規模や業種を問わず共通する基本的な対策を実行することで、顧客や取引先との信頼関係の構築に大いに役立ちます。さらに、デジタル化やサイバーセキュリティ対策などを支援する公的支援制度の要件になるなど、情報セキュリティのはじめの一歩として、とても有益な制度です。

（SECURITY ACTION 自己宣言の申込方法はこちら）

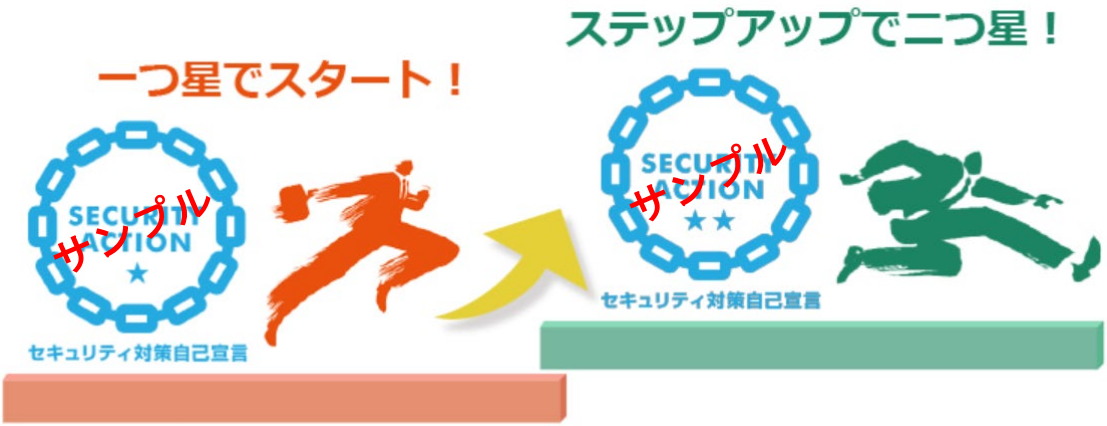


図４.SECURITY ACTION「★一つ星」「★★二つ星」ロゴマーク（サンプル）

ここまで情報セキュリティ５か条の内容と、これを実践する宣言である SECURITY ACTION「★一つ星」についてご紹介いたしましたが、いかがだったでしょうか。

まだまだ情報セキュリティに対して、「投資していない」「必要性を感じない」と考える中小企業が多いのは統計から見ても明らかです。
しかし、大きな費用をかけることなく、まずは「できるところから始める」ことを意識し、アクションを起こすことが重要です。

まずはスモールステップで構わないので、情報セキュリティ 5 か条を足掛かりに情報セキュリティ対策に取り組みましょう。
その姿勢が企業の持続可能な発展を支える鍵となると考えます。

5. 取り組む際の参考資料

ここまでの解説で取り上げたガイドラインでは、「できるところから始める」の解説に加えて、具体的にはどのように取り組んだら良いのか、さらに進めるためにはどうしたら良いのかなど発展的な取り組み方法について紹介しています。
ぜひ、理解を深めたい、次のステップに進みたいと思った際の参考にしてください。

1.中小企業の情報セキュリティ対策ガイドライン(IPA)
2.付録 1：情報セキュリティ 5 か条（IPA）
3.2024 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（IPA）
4.SECURITY ACTION（IPA）

配信予定日：2026 年 1 月 16 日(金) 14:00 頃
カテゴリ：ビジネスヒント
タグ：＃知識編＃経営課題
過去記事焼き直し：しない（新規記事です）
記事 URL（新設します）：https://cybersecurity-taisaku.metro.tokyo.lg.jp/tip/security-guide4/

サイバーセキュリティ経営ガイドライン概説（4/4）

目次
●サイバーセキュリティ経営の重要 10 項目の実践事例を知るには
●プラクティス集の主な内容
●サイバーセキュリティ体制の強化を図るには

最終回の今回は、前回に続き、サイバーセキュリティ経営ガイドライン（以下「ガイドライン」と表記）の効果的な活用方法について解説します。

●サイバーセキュリティ経営の重要 10 項目の実践事例を知るには
サイバーセキュリティ経営可視化ツール等によって自組織の現状や課題を把握したら、次はガイドラインの要求事項を実践する具体的な方法を検討したり、予算や体制整備を図ったりする必要があるでしょう。このような段階において参考となるのが「サイバーセキュリティ経営ガイドライン Ver 3.0 実践のためのプラクティス集 第 4 版」（以下「プラクティス集」と表記）です。
このプラクティス集についても可視化ツールと同様に IPA のサイトで提供されています。
対象としている主な読者は「情報セキュリティの取組みはある程度進めてきたが、サイバー攻撃対策やインシデント対応は強化が必要。それに向けた体制づくりや対策は何から始めるべきか」と考えている経営者や CISO 等、セキュリティ担当者です。
そうした方々が、例えば図に示すようなタイミングや場面において活用することを想定しています。

No	利用するタイミング	具体的な利用場面
1	新たにサイバーセキュリティ部門を設置・所管することになった場合や、CISO等に着任した場合など	どこからサイバーセキュリティの取組に着手してよいかわからない際に、はじめの一歩として実践事例や参考情報を活用する
2	経営環境の変化（デジタルトランスフォーメーションへの取組着手など）により、サイバーセキュリティ対策の重要性が増し、対策を検討する場合など	経営ガイドラインに紐づく実践事例を参考に、サイバーセキュリティ対策の検討に役立てる
3	インシデントが発生し、サイバーセキュリティ対策を強化しなければならない場合など	取組や工夫の例を参考にインシデントの再発防止に向けた対策の実施に役立てる
4	セキュリティ担当者へ教育を実施する場合や、外部の事業者としてサイバーセキュリティ対策を支援する場合など	人材育成の担当者が教材として活用する、また企業のサイバーセキュリティ対策支援に役立てる

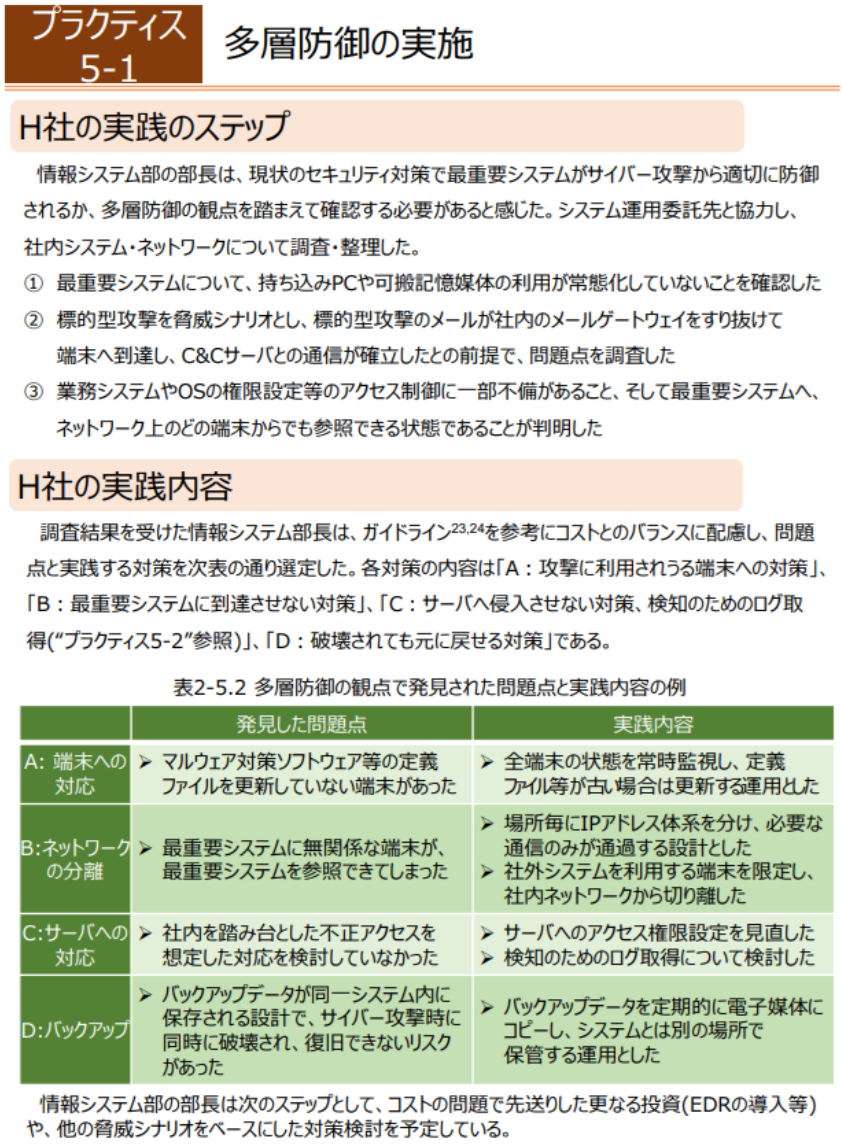
プラクティス集を利用するタイミングや場面の例
（https://www.ipa.go.jp/security/economics/hjuojm00000044dc-att/cms_practice_v4_1.pdf ）

●プラクティス集の主な内容

それでは、プラクティス集の主な内容について見ていきましょう。

第２章では、企業での事例に基づいたガイドライン「サイバーセキュリティ経営の重要 10 項目」の実践手順、実践内容、取り組む際の考え方、ヒント等が示されています。

例えば、「指示 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」では、従業員500名規模の製造業Ｈ社の事例に基づき、同社のシステム環境の概要を説明した上で、次のように「多層防御の実施」がプラクティスとして紹介されています。



プラクティス 5-1 多層防御の実施

H社の実践のステップ

情報システム部の部長は、現状のセキュリティ対策で最重要システムがサイバー攻撃から適切に防御されるか、多層防御の観点を踏まえて確認する必要があると感じた。システム運用委託先と協力し、社内システム・ネットワークについて調査・整理した。

① 最重要システムについて、持ち込みPCや可搬記憶媒体の利用が常態化していないことを確認した
② 標的型攻撃を脅威シナリオとし、標的型攻撃のメールが社内のメールゲートウェイをすり抜けて端末へ到達し、C&Cサーバとの通信が確立したとの前提で、問題点を調査した
③ 業務システムやOSの権限設定等のアクセス制御に一部不備があること、そして最重要システムへ、ネットワーク上のどの端末からでも参照できる状態であることが判明した

H社の実践内容

調査結果を受けた情報システム部長は、ガイドライン[23,24]を参考にコストとのバランスに配慮し、問題点と実践する対策を次表の通り選定した。各対策の内容は「A：攻撃に利用されうる端末への対策」、「B：最重要システムに到達させない対策」、「C：サーバへ侵入させない対策、検知のためのログ取得(“プラクティス5-2”参照)」、「D：破壊されても元に戻せる対策」である。

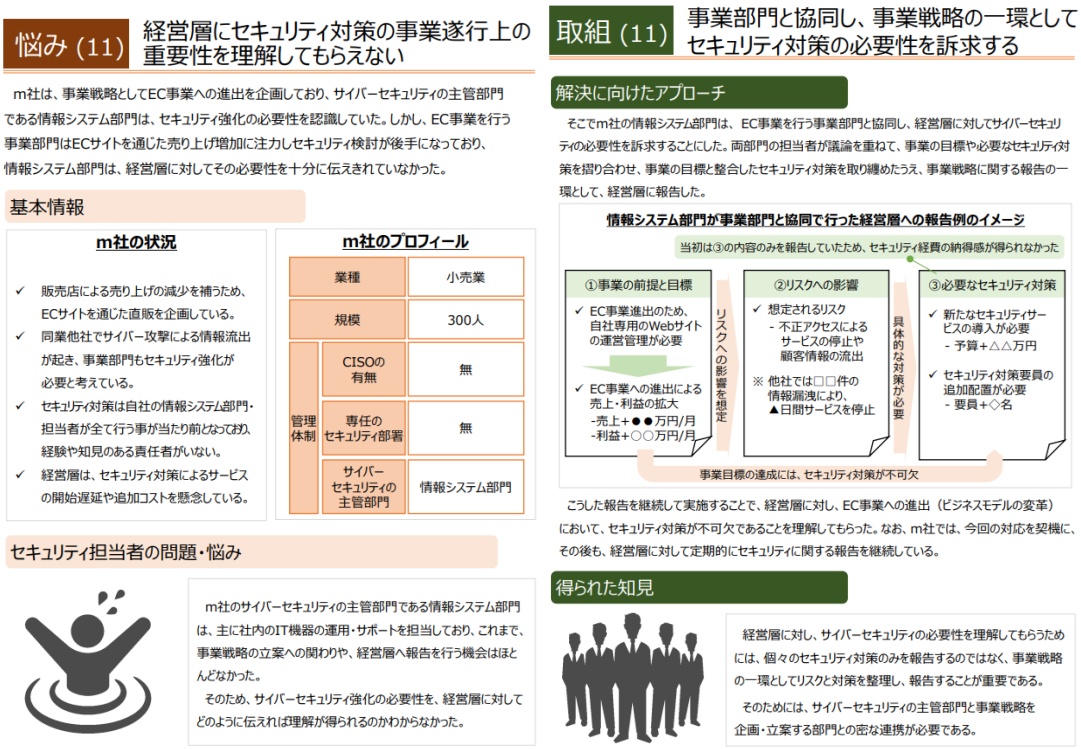
表2-5.2 多層防御の観点で発見された問題点と実践内容の例

	発見した問題点	実践内容
A: 端末への対応	➢ マルウェア対策ソフトウェア等の定義ファイルを更新していない端末があった	➢ 全端末の状態を常時監視し、定義ファイル等が古い場合は更新する運用とした
B:ネットワークの分離	➢ 最重要システムに無関係な端末が、最重要システムを参照できてしまった	➢ 場所毎にIPアドレス体系を分け、必要な通信のみが通過する設計とした ➢ 社外システムを利用する端末を限定し、社内ネットワークから切り離した
C:サーバへの対応	➢ 社内を踏み台とした不正アクセスを想定した対応を検討していなかった	➢ サーバへのアクセス権限設定を見直した ➢ 検知のためのログ取得について検討した
D:バックアップ	➢ バックアップデータが同一システム内に保存される設計で、サイバー攻撃時に同時に破壊され、復旧できないリスクがあった	➢ バックアップデータを定期的に電子媒体にコピーし、システムとは別の場所で保管する運用とした

情報システム部の部長は次のステップとして、コストの問題で先送りした更なる投資(EDRの導入等)や、他の脅威シナリオをベースにした対策検討を予定している。

H 社の事例に基づく指示 5 のプラクティス
(https://www.ipa.go.jp/security/economics/hjuojm00000044dc-att/cms_practice_v4_1.pdf)

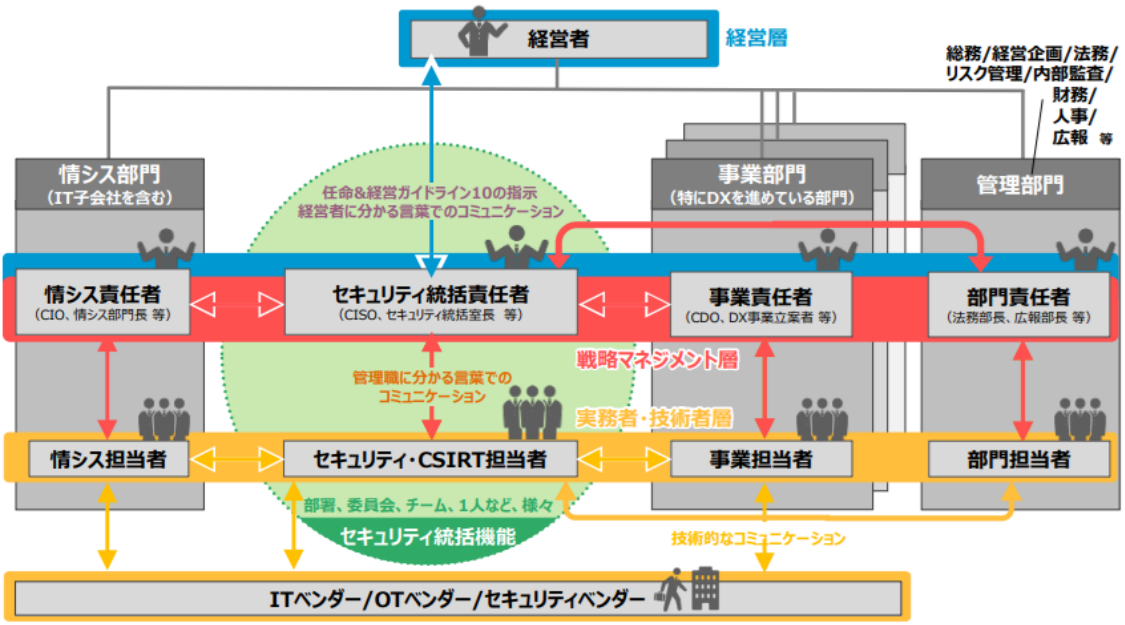
続く第 3 章では、サイバーセキュリティ対策をこれから実践するセキュリティ担当者が対策を推進する上での悩みを 18 個挙げ、それを解決するために取り組んだ際の実践手順、内容、取り組む際の考え方、得られた知見等が事例で示されています。
例えば、悩み(11)では、従業員 300 名規模の小売業 m 社の「経営者にセキュリティ対策の事業遂行上の重要性を理解してもらえない」という状況を取り上げ、その解決に向けたアプローチや、そこから得られた知見がプラクティスとして紹介されています。



m 社の悩みとその解決への取組事例に基づくプラクティス
(https://www.ipa.go.jp/security/economics/hjuojm00000044dc-att/cms_practice_v4_1.pdf)

●サイバーセキュリティ体制の強化を図るには
ガイドラインの要求事項を実践する上で、サイバーセキュリティ体制の強化は多くの組織で重要な課題となる可能性が高いでしょう。この課題に取り組む上で参考となるのが、ガイドラインの別添資料として提供されている「付録 F　サイバーセキュリティ体制構築・人材確保の手引き 第 2.0 版」（以下「手引き」と表記）です。
この手引きは、ガイドライン「サイバーセキュリティ経営の重要１０項目」の「指示２　サイバーセキュリティリスク管理体制の構築」と「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」について具体的な検討を行う場合の参考となることを目的として作成されました。

前半の「サイバーセキュリティリスクの管理体制の構築」では、企業におけるリスクマネジメント活動の一部として、セキュリティ対策及びセキュリティインシデント対応について、CISO や経営層を補佐してセキュリティ対策を組織横断的に統括する「セキュリティ統括機能」を設置するのが有効であり、その形態として「専門組織型」「委員会型」等があると解説しています。



セキュリティ統括機能のイメージ
(https://www.meti.go.jp/policy/netsecurity/tebikihontai2.pdf)

後半の「サイバーセキュリティ関連タスクを担う人材の活用」では、不足するセキュリティ人材を確保する方法、セキュリティ統括人材及びセキュリティ担当者の確保のポイント等のほか、「プラス・セキュリティ」の重要性について解説しています。
「プラス・セキュリティ」とは、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と定義しています。「プラス・セキュリティ」は、本来あらゆる業務において必要ですが、セキュリティ対策業務として明示的に位置づけられてはいないものの、対策が不十分な場合にはセキュリティ上の問題が生じるような業務を担っている人材にとっては特に重要です。
その他、具体的なセキュリティ人材の教育プログラムや有効な試験・資格等、組織がサイバーセキュリティ体制の強化を図る上で参考となる情報が数多く掲載されています。

今回ご紹介したガイドラインをはじめ、各種付録や補助ツール、参考資料等は、業種や規模を問わず、多くの組織にとって有用なものと考えます。既に様々なセキュリティ施策を実施し、サイバーセキュリティ強化に取り組んでいる組織の方は、その充足度や残課題等の確認に、これから取り組もうとしている組織の方は、その第一歩を踏み出すために活用いただいてはいかがでしょうか。

配信予定日：2026 年 1 月 23 日(金) 14:00 頃
カテゴリ：基礎から学ぶ！ セキュリティ
タグ：＃実用編 ＃知識編
過去記事焼き直し：する（過去記事を上書きします）
過去記事：https://cybersecurity-taisaku.metro.tokyo.lg.jp/basics/kisokaramanabu16/

【令和 7 年度版】中小企業におけるセキュリティ脅威への対策強化　～情報セキュリティ対策の進め方 『組織的な取り組みを開始しよう』～

目次

中小企業において、情報セキュリティの脅威はますます無視できない問題となっています。
独立行政法人情報処理推進機構（IPA）が発行している「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」の「第 2 部実践編」では、具体的な対策方法と中小企業の経営者やシステム担当者がこれにどう取り組むべきかを詳しく解説しています。

情報セキュリティ対策に組織全体で取り組むには、実行すべき対策を決めて、従業員に周知する必要があります。
しかし、こうした作業を行うには情報セキュリティに関する知識や経験が必要となるため、それらの知識や経験に長けた人材がいないと対策が進まなくなることも考えられます。

このような背景から、IPA のガイドラインでは規模の小さな企業や、これまで十分な情報セキュリティ対策を実施してこなかった企業などを対象に、すぐに取り組める対策を示し、段階的に発展させていく計画を紹介しています。この「すぐに取り組める対策」が、多くの企業にとって無理なく、自社の状況に応じた対策を開始する道筋となります。

今回は、『組織的な取り組みを開始しよう』と題し、すぐに始められる情報セキュリティ対策に焦点を当てて進めていきます。

１．情報セキュリティに対する中小企業の現状

IPA が作成した、「2024 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」報告書によると、情報セキュリティに関する組織体制について、「組織的には行っていない（各自の対応）」と回答した企業の割合が、規模が小さい企業ほど多く見られました。
小規模企業者では 84.5%、100 人以下の中小企業では 47.6%、101 人以上の中小企業では 13.6%が、情報セキュリティ対策を組織的に行っていないと回答しています。
つまり、100 人以下の中小企業・小規模企業者の半数以上が「組織的に行わず、各自に任せている」状況にあると言えます。

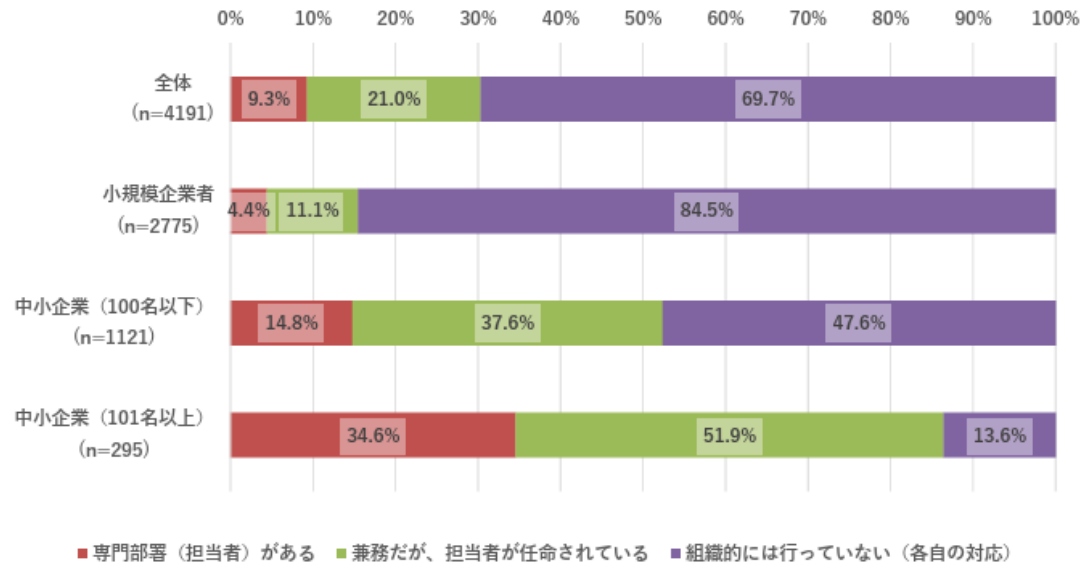


図 1．情報セキュリティに係る組織体制(企業規模別)
(引用：「2024 年度中小企業における情報セキュリティ対策に関する実態調査」報告書 P.115)

「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」の「第 1 部経営者編」では、情報セキュリティ対策は経営者こそが中心的な役割を果たすべきだと示されており、リーダーシップを発揮して推進することが求められています。
これは、情報セキュリティ対策を従業員「各自に任せる」のではなく、「組織的に実施すること」を求めていると言えます。

２．組織的な取り組みを開始する

次に、具体的に「組織的な取り組み」をどのように進めるかについて見ていきましょう。

（1）情報セキュリティ基本方針の作成意義

情報セキュリティ対策を組織に浸透させるためには、経営者主導のもとで情報セキュリティに

関する基本方針を定めることが重要です。そして、この基本方針を、従業員や関係者に効果的に伝えるためには、簡潔な文書で表現しましょう。
基本方針には決まった書式や形式はありませんが、IPA が提供している「情報セキュリティ基本方針（サンプル）」（付録２）などを参考にするとよいでしょう。
自社の事業の特徴や顧客のニーズを踏まえて、経営者と連携しつつ、自社に適した基本方針を作成することが大切です。

また、策定した基本方針は従業員に対するセキュリティ行動指針としてだけではなく、関係者に対して自社のセキュリティへの取り組み姿勢を表明するものでもあります。
作成した文書は、従業員や顧客などの関係者に周知し、透明性のある取り組みを積極的にアピールすることが望まれます。

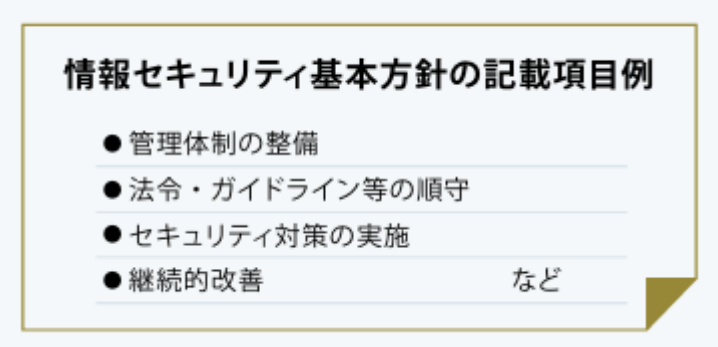


図２．情報セキュリティ基本方針例
（引用：中小企業の情報セキュリティ対策ガイドライン）

（２）自社のセキュリティ状況の把握

「５分でできる！情報セキュリティ自社診断」（付録３）を利用して、情報セキュリティ対策が現状でどの程度実施されているか把握することができます。
自社診断は、下記の表（図 3）に示されている 25 項目の設問に答えるだけで、情報セキュリティ対策の実施状況を把握できるツールです。現状把握のために、積極的に活用しましょう。

具体的な使い方は以下のとおりです。

【手順１】
経営者または情報システム担当や部門長など実施状況が分かる人が「５分でできる！情報セキュリティ自社診断」の診断編に記入します。

【手順２】
事業所が複数ある、部署数が多いなど、一人で記入することが難しい場合には、事業所や部署

ごとに記入し、責任者・担当者が集計します。

【手順３】
実施状況が分からない場合は、各従業員に質問して、回答を総合して記入します。

【手順４】
チェック欄の該当するもの１つに○を付けて、「実施している…４点」「一部実施している…２点」「実施していない…０点」「わからない…－１点」で採点します。

【手順５】
全項目の合計点で、組織全体のセキュリティ対策の実施状況と、回答が「わからない」になっている項目を把握します。

診断項目	No	診断内容	チェック			
			実施している	一部実施している	実施していない	わからない
Part 1 基本的対策	1	パソコンやスマホなど情報機器の OS やソフトウェアは常に最新の状態にしていますか？	4	2	0	−1
	2	パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイル※1 は最新の状態にしていますか？	4	2	0	−1
	3	パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？	4	2	0	−1
	4	重要情報※2 に対する適切なアクセス制限を行っていますか？	4	2	0	−1
	5	新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？	4	2	0	−1
Part 2 従業員としての対策	6	電子メールの添付ファイルや本文中の URL リンクを介したウイルス感染に気をつけていますか？	4	2	0	−1
	7	電子メールや FAX の宛先の送信ミスを防ぐ取り組みを実施していますか？	4	2	0	−1
	8	重要情報は電子メール本文に書くのではなく、添付するファイルに書いてパスワードなどで保護していますか？	4	2	0	−1
	9	無線 LAN を安全に使うために適切な暗号化方式を設定するなどの対策をしていますか？	4	2	0	−1
	10	インターネットを介したウイルス感染やSNSへの書き込みなどのトラブルへの対策をしていますか？	4	2	0	−1
	11	パソコンやサーバーのウイルス感染、故障や誤操作による重要情報の消失に備えてバックアップを取得していますか？	4	2	0	−1
	12	紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は机上に放置せず、書庫などに安全に保管していますか？	4	2	0	−1
	13	重要情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の対策をしていますか？	4	2	0	−1
	14	離席時にパソコン画面の覗き見や勝手な操作ができないようにしていますか？	4	2	0	−1
	15	関係者以外の事務所への立ち入りを制限していますか？	4	2	0	−1
	16	退社時にノートパソコンや備品を施錠保管するなど盗難防止対策をしていますか？	4	2	0	−1
	17	事務所が無人になる時の施錠忘れ対策を実施していますか？	4	2	0	−1
	18	重要情報が記載された書類や重要なデータが保存された媒体を破棄する時は、復元できないようにしていますか？	4	2	0	−1
Part 3 組織としての対策	19	従業員に守秘義務を理解してもらい、業務上知り得た情報を外部に漏らさないなどのルールを守らせていますか？	4	2	0	−1
	20	従業員にセキュリティに関する教育や注意喚起を行なっていますか？	4	2	0	−1
	21	個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしていますか？	4	2	0	−1
	22	重要情報の授受を伴う取引先との契約書には、秘密保持条項を規定していますか？	4	2	0	−1
	23	クラウドサービスやウェブサイトの運用等で利用する外部サービスは、安全・信頼性を把握して選定していますか？	4	2	0	−1
	24	セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成するなど準備をしていますか？	4	2	0	−1
	25	情報セキュリティ対策（上記１～24 など）をルール化し、従業員に明示していますか？	4	2	0	−1

図３．自社診断のための２５項目

（引用：5 分でできる！情報セキュリティ自社診断）

（3）対策の決定と周知

診断結果をもとに、自社で実行すべき情報セキュリティ対策を検討しましょう。その際、参考資料として「5 分でできる！情報セキュリティ自社診断」の解説編を利用することで、簡単かつ効率的に対策を検討できます。

この資料には、コストを抑えつつ効果が期待できる具体的な対策例が示されているため、診断

結果に基づき、自社に適した施策を検討する手助けとなります。

具体的な使い方は以下のとおりです。

- 対策の検討と決定は、責任者・担当者と経営者が行います。
- 診断項目ごとに対策を実施しない場合に考えられる被害・事故や、防止するための対策例が示されているので、参考にして検討します。
- 検討する際には従業員の意見を聞き、職場環境や業務に適した対策を決定します。

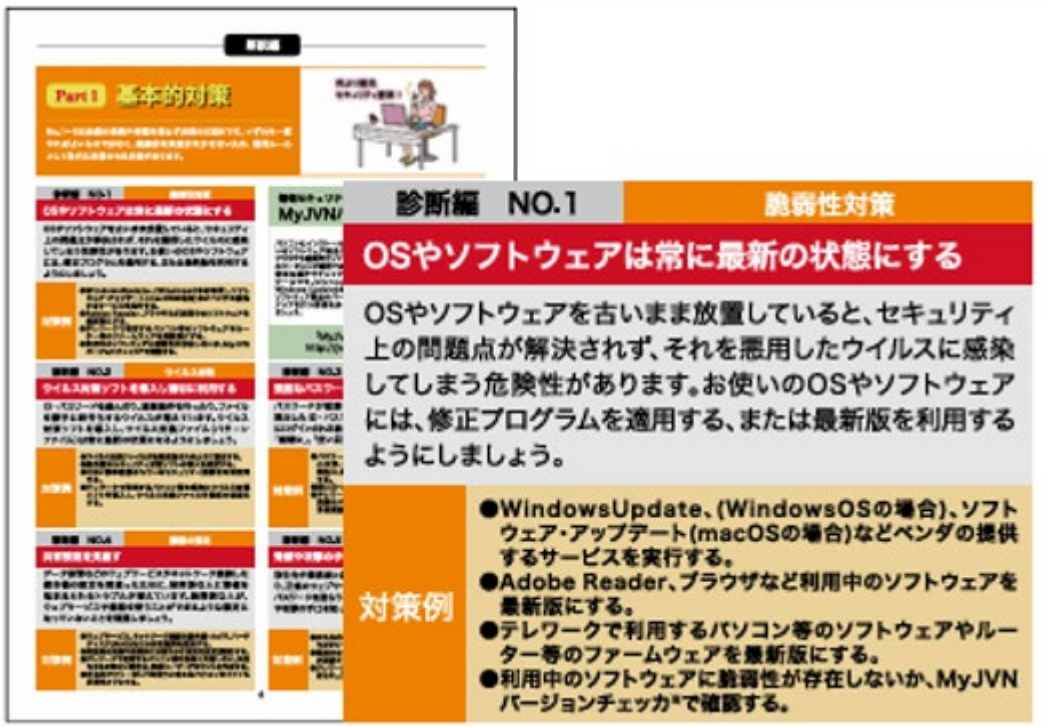


図４.「５分でできる！情報セキュリティ自社診断」解説編
（引用：５分でできる！情報セキュリティ自社診断）

（４）情報セキュリティハンドブックの作成と周知

対策が決定した後、その内容を従業員一人ひとりが実践できる形で定めた「情報セキュリティハンドブック」を作成し、周知します。
このハンドブックの作成には「情報セキュリティハンドブック（ひな形）」（付録４）を活用します。情報セキュリティハンドブック（ひな形）は、「５分でできる！情報セキュリティ自社診断」の対策例と連動しており、具体的な対策が明確化されています。

作成したハンドブックは単なる資料として従業員に配布するにとどまらず、必要に応じて説明

会を実施しましょう。従業員が内容を十分に理解し、日常業務に反映できるよう徹底します。

作成方法と運用の流れは以下のとおりです。

- 情報セキュリティハンドブックは、責任者・担当者が作成します。
- ひな形に記載された例文を編集して、決定した対策を社内ルールとして明文化します。（図 5.情報セキュリティハンドブック（ひな形）のカスタマイズ例を参照）
- 完成した情報セキュリティハンドブックを全従業員に配付し、必要に応じて説明する機会を設けるなどして、情報セキュリティ対策を徹底します。

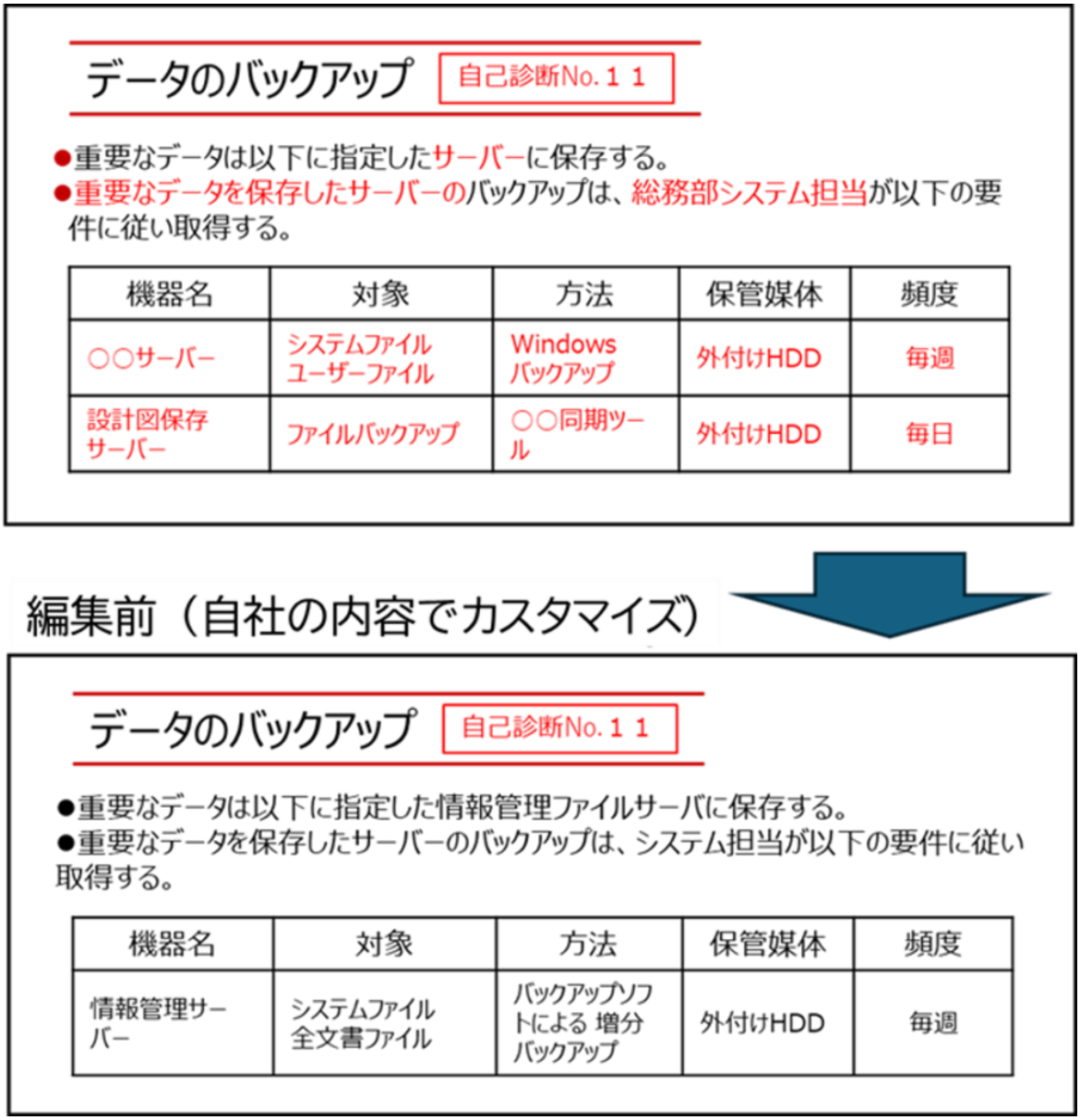


図５．情報セキュリティハンドブック（ひな形）のカスタマイズ例

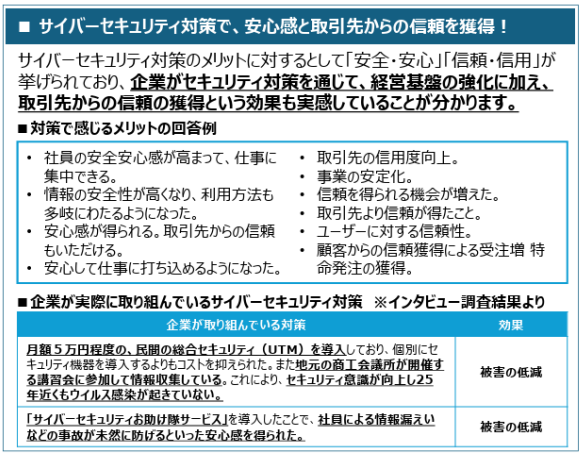
（参考：情報セキュリティハンドブック（ひな形））

３．効果的な取組事例

2024 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において、効果的な取組事例が紹介されており、業種ごとの対策として以下が紹介されています。

（１） 製造業

・約５割がサイバーセキュリティ体制を組織的に整備し、経営基盤の強化と取引先からの信頼を獲得しています。また約５割強がサイバーセキュリティ教育を実施し、約４分の１の企業が SECURITY ACTION 二つ星の対策を実施（「5 分でできる！情報セキュリティ自己診断」の得点が 70 点以上）し、社内のサイバーセキュリティ対策を向上させサイバーインシデント被害の低減の効果を得ています。



■ サイバーセキュリティ対策で、安心感と取引先からの信頼を獲得！

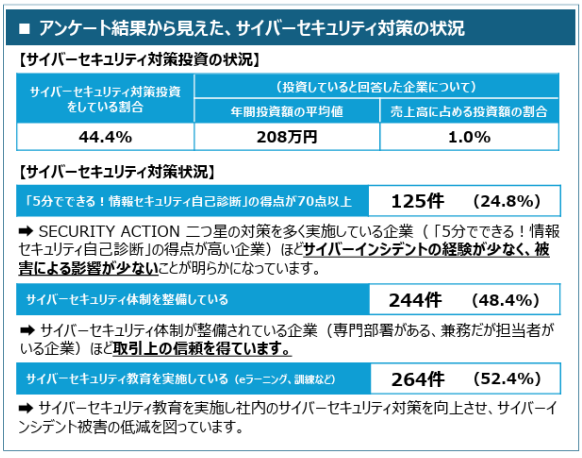
サイバーセキュリティ対策のメリットに対するとして「安全・安心」「信頼・信用」が挙げられており、**企業がセキュリティ対策を通じて、経営基盤の強化に加え、取引先からの信頼の獲得という効果も実感していることが分かります。**

■対策で感じるメリットの回答例

- 社員の安全安心感が高まって、仕事に集中できる。
- 情報の安全性が高くなり、利用方法も多岐にわたるようになった。
- 安心感が得られる。取引先からの信頼もいただける。
- 安心して仕事に打ち込めるようになった。
- 取引先の信用度向上。
- 事業の安定化。
- 信頼を得られる機会が増えた。
- 取引先より信頼が得たこと。
- ユーザーに対する信頼性。
- 顧客からの信頼獲得による受注増 特命発注の獲得。

■企業が実際に取り組んでいるサイバーセキュリティ対策 ※インタビュー調査結果より

企業が取り組んでいる対策	効果
月額５万円程度の、民間の総合セキュリティ（UTM）を導入しており、個別にセキュリティ機器を導入するよりもコストを抑えられた。また地元の商工会議所が開催する講習会に参加して情報収集している。これにより、セキュリティ意識が向上し25年近くもウイルス感染が起きていない。	被害の低減
「サイバーセキュリティお助け隊サービス」を導入したことで、社員による情報漏えいなどの事故が未然に防げるといった安心感を得られた。	被害の低減



■ アンケート結果から見えた、サイバーセキュリティ対策の状況

【サイバーセキュリティ対策投資の状況】

サイバーセキュリティ対策投資をしている割合	（投資していると回答した企業について）	
	年間投資額の平均値	売上高に占める投資額の割合
44.4%	208万円	1.0%

【サイバーセキュリティ対策状況】

「5分でできる！情報セキュリティ自己診断」の得点が70点以上	125件 （24.8%）

➡ SECURITY ACTION 二つ星の対策を多く実施している企業（「5分でできる！情報セキュリティ自己診断」の得点が高い企業）ほど**サイバーインシデントの経験が少なく、被害による影響が少ない**ことが明らかになっています。

サイバーセキュリティ体制を整備している	244件 （48.4%）

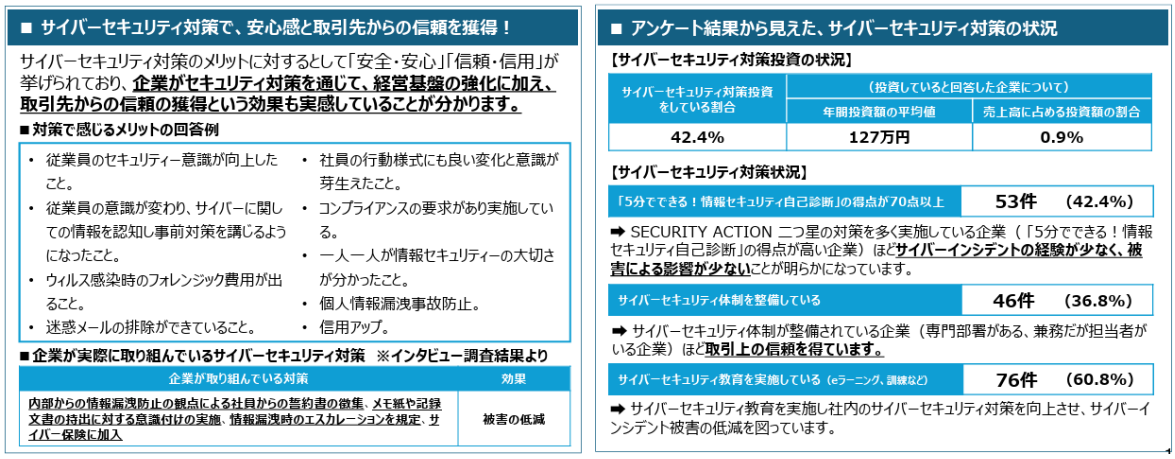
➡ サイバーセキュリティ体制が整備されている企業（専門部署がある、兼務だが担当者がいる企業）ほど**取引上の信頼を得ています。**

サイバーセキュリティ教育を実施している（eラーニング、訓練など）	264件 （52.4%）

➡ サイバーセキュリティ教育を実施し社内のサイバーセキュリティ対策を向上させ、サイバーインシデント被害の低減を図っています。

（２） 金融業・保険業

・約３割強がサイバーセキュリティ体制を組織的に整備し、経営基盤の強化と取引先からの信頼を獲得しています。また約６割がサイバーセキュリティ教育を実施し、約４割強の企業が SECURITY ACTION 二つ星の対策を実施（「5 分でできる！情報セキュリティ自己診断」の得点が 70 点以上）し、社内のサイバーセキュリティ対策を向上させサイバーインシデント被害の低減の効果を得ています。



■ サイバーセキュリティ対策で、安心感と取引先からの信頼を獲得！

サイバーセキュリティ対策のメリットに対するとして「安全・安心」「信頼・信用」が挙げられており、**企業がセキュリティ対策を通じて、経営基盤の強化に加え、取引先からの信頼の獲得という効果も実感していることが分かります。**

■対策で感じるメリットの回答例

- 従業員のセキュリティー意識が向上したこと。
- 従業員の意識が変わり、サイバーに関しての情報を認知し事前対策を講じるようになったこと。
- ウィルス感染時のフォレンジック費用が出ること。
- 迷惑メールの排除ができていること。
- 社員の行動様式にも良い変化と意識が芽生えたこと。
- コンプライアンスの要求があり実施している。
- 一人一人が情報セキュリティーの大切さが分かったこと。
- 個人情報漏洩事故防止。
- 信用アップ。

■企業が実際に取り組んでいるサイバーセキュリティ対策　※インタビュー調査結果より

企業が取り組んでいる対策	効果
内部からの情報漏洩防止の観点による社員からの誓約書の徴集、メモ紙や記録文書の持出に対する意識付けの実施、情報漏洩時のエスカレーションを規定、サイバー保険に加入	被害の低減

■ アンケート結果から見えた、サイバーセキュリティ対策の状況

【サイバーセキュリティ対策投資の状況】

サイバーセキュリティ対策投資をしている割合	（投資していると回答した企業について）	
	年間投資額の平均値	売上高に占める投資額の割合
42.4%	127万円	0.9%

【サイバーセキュリティ対策状況】

「5分でできる！情報セキュリティ自己診断」の得点が70点以上	53件	(42.4%)

➡ SECURITY ACTION 二つ星の対策を多く実施している企業（「5分でできる！情報セキュリティ自己診断」の得点が高い企業）ほど**サイバーインシデントの経験が少なく、被害による影響が少ない**ことが明らかになっています。

サイバーセキュリティ体制を整備している	46件	(36.8%)

➡ サイバーセキュリティ体制が整備されている企業（専門部署がある、兼務だが担当者がいる企業）ほど**取引上の信頼を得ています。**

サイバーセキュリティ教育を実施している（eラーニング、訓練など）	76件	(60.8%)

➡ サイバーセキュリティ教育を実施し社内のサイバーセキュリティ対策を向上させ、サイバーインシデント被害の低減を図っています。

（引用：2024 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～業種ごとの効果的な取組事例集～より一部抜粋）

4．SECURITY ACTION「★★二つ星」宣言のすすめ

「SECURITY ACTION」は、中小企業が自主的に情報セキュリティ対策に取り組む姿勢を自己宣言する制度です。安全・安心な IT 社会を実現するために創設されました。

「★★二つ星」を宣言するためには、いくつかのプロセスを経る必要があります。
まずは、「中小企業の情報セキュリティ対策ガイドライン」に付属している、付録 3「5 分でできる！情報セキュリティ自社診断」を活用し、自社のセキュリティ状況を評価します。
その後、同ガイドラインの付録 2「情報セキュリティ基本方針（サンプル）」を参考に自社の情報セキュリティ基本方針を策定します。
この基本方針は社内だけでなく外部にも公開する必要があります。外部への公開により、「組織的な取り組みを開始する」を実施したことの宣言になります。

外部公開の方法としては、自社ウェブサイトへの掲載や会社案内やパンフレットへの掲載などが選択できます。また、「★一つ星」宣言から「★★二つ星」へのステップアップだけではなく、準備が整えば「★★二つ星」からの宣言も可能です。
SECURITY ACTION 自己宣言の申込方法はこちらを参照してください。

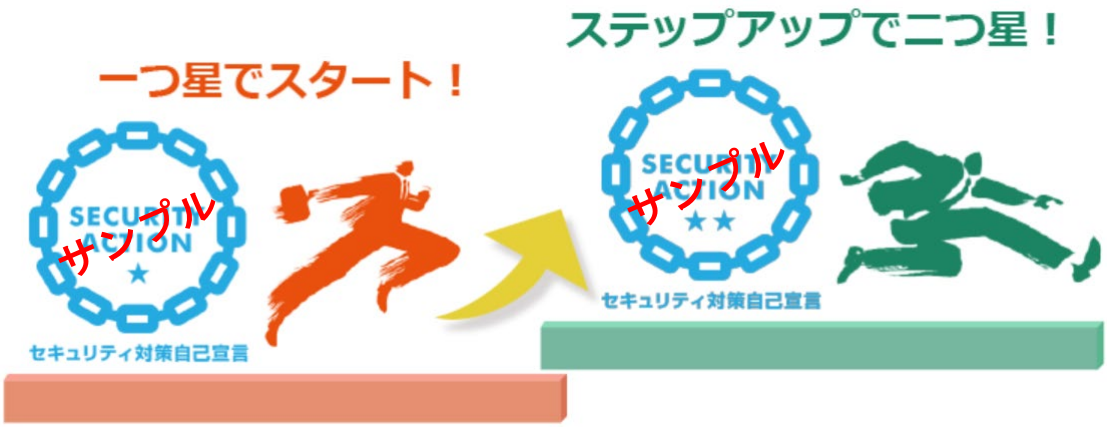


図 6 . SECURITY ACTION「★一つ星」「★★二つ星」ロゴマーク（サンプル）

５．最後に

ここまで「組織的な取り組みを開始する」ためのプロセスと、それを実行した証としての SECURITY ACTION「★★二つ星」についてご紹介いたしましたが、いかがだったでしょうか。

「情報セキュリティ対策を組織的に始めたいが、何から始めればよいかわからない」「具体的な手段が分からない」とお考えの中小企業が多いのは統計からみても明らかです。

この「SECURITY ACTION」の自己宣言プロセスは決して難しくありません。
初めて取り組む企業でも詳細な手順を IPA の公式サイトで確認できるので、情報セキュリティの取り組みを加速させたい中小企業にとって有益な第一歩となるでしょう。

まずはこのような取り組みを組織的に開始することが、自社の安全性確保と信頼性向上に繋がり、企業の持続可能な発展を支える鍵となると考えます。
今回の内容が実践への第一歩を踏み出す手助けとなることを願っています。

６．取り組む際の参考資料

ここまでの解説で取り上げたガイドラインでは、「組織的な取り組みを開始する」の解説に加えて、具体的にはどのように取り組んだら良いのか、さらに進めるためにはどうしたら良いのかなど発展的な取り組み方法について紹介しています。

ぜひ、理解を深めたい、次のステップに進みたいと思った際の参考にしてください。

１．中小企業の情報セキュリティ対策ガイドライン（IPA）

2．付録 1：情報セキュリティ 5 か条（IPA）
3．付録 2：情報セキュリティ基本方針（サンプル）（Word ファイル、IPA）
4．付録 3：5 分でできる！情報セキュリティ自社診断（IPA）
5．付録 4 ：情報セキュリティハンドブック（ひな形）（PowerPoint ファイル、IPA）
6．2024 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（IPA））
7．SECURITY ACTION（IPA）

配信予定日：2026 年 1 月 23 日(金) 14:00 頃
カテゴリ：基礎から学ぶ！ セキュリティ
タグ：＃実用編 ＃知識編
過去記事焼き直し：する（過去記事を上書きします）
過去記事：https://cybersecurity-taisaku.metro.tokyo.lg.jp/basics/kisokaramanabu17/

【令和 7 年度版】中小企業におけるセキュリティ脅威への対策強化　～情報セキュリティ対策の進め方『体制・DX・予算から（1/3)』～

目次

独立行政法人情報処理推進機構（IPA）が発行している「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」の「第 2 部実践編」では、具体的な対策方法と中小企業の経営者やシステム担当者がこれにどう取り組むべきかを詳しく解説しています。

情報セキュリティ対策に組織全体で取り組むには、実行すべき対策を決めて、従業員に周知する必要があります。しかし、こうした作業を行うには情報セキュリティに関する知識や経験が必要となるため、それらの知識や経験に長けた人材がいないと対策が進まなくなることも考えられます。

このような背景から、IPA のガイドラインでは規模の小さな企業や、これまで十分な情報セキュリティ対策を実施してこなかった企業などを対象に、すぐに取り組める対策を示し、段階的に発展させていく計画を紹介しています。この「すぐに取り組める対策」が、多くの企業にとって無理なく、自社の状況に応じた対策を開始する道筋となります。

今回は、『本格的に取り組みをはじめよう』というテーマで、３回に分けて具体的な取り組みの方法をご紹介します。1 回目となる今回は、管理体制の構築、デジタルトランスフォーメーション（DX)、そしてセキュリティ対策費用の予算化の重要性に焦点を当てます。

１．情報セキュリティに対する中小企業の現状

IPA が作成した、「2024 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」報告書によると、情報セキュリティに関する管理体制を構築していない企業は規模が小さ

いほど多い傾向にあります。

具体的には、「組織的に対応していない」企業の割合は、小規模企業者で 84.5%、100 人以下の中小企業では 47.6%、101 人以上の中小企業では 13.6%となっています。
つまり、100 人以下の中小企業の約半数は「組織的に行っておらず各自の対応に任せている」状況です。

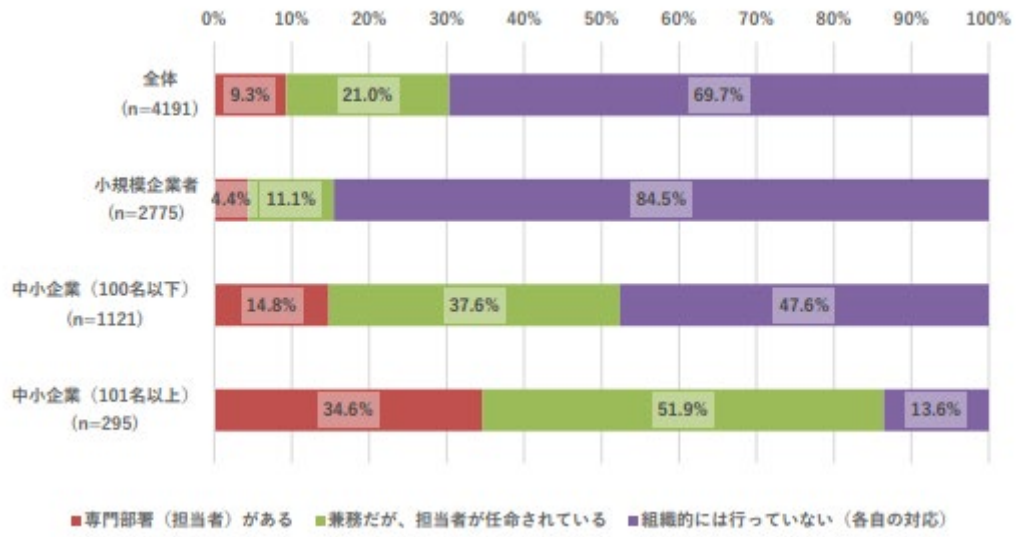


図１．社内の情報セキュリティ対策の体制（企業規模別）
（引用：「2024 年度 中小企業における情報セキュリティ対策に関する実態調査」報告書）

同じ報告書では、デジタルトランスフォーメーション（DX※）の推進と情報セキュリティの予算化の実施状況も報告されています。

※DX（Digital Transformation）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。

IT（DX）投資額について最も多かった回答は「投資していない」で、全体の 59.7%を占めました。次に「１百万円未満」が 20.7%、「１百万円から５百万円未満」が 5.3%という結果になっています。
さらに情報セキュリティ対策のデータでも、「投資していない」企業が全体の 62.6%でトップとなり、次に「１百万円未満」が 20.4%と相当数存在しています。これに対し、「１百万円から５百万円未満」と回答した企業はわずか 4.7%に留まっています。
この結果から、IT（DX）投資および情報セキュリティ対策投資のいずれも低迷していることが分かります。

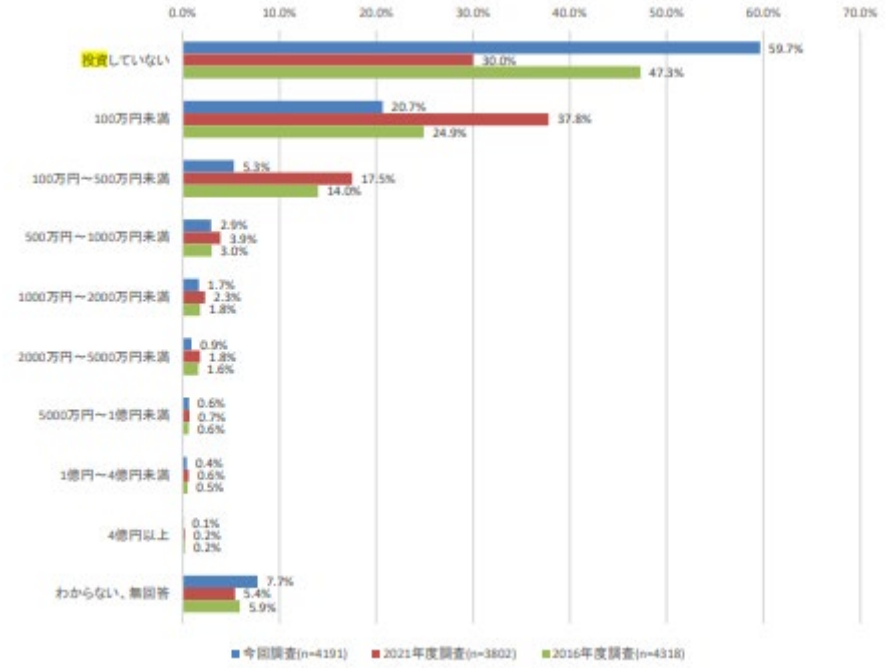


図 2 -1. IT 投資額

（引用：「2024 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」報告書）

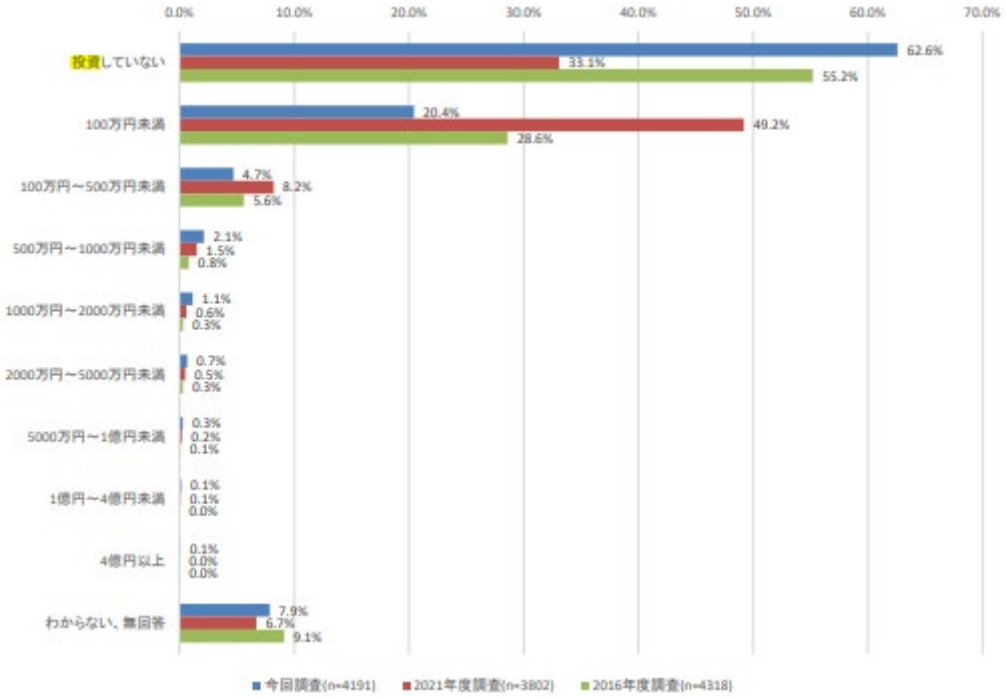


図 2 -2. 情報セキュリティ投資額

（引用：「2024 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」報告書）

これは、デジタルトランスフォーメーション（DX）の推進や情報セキュリティ対策の取り

組みに課題があることを示唆しています。

２．本格的に取り組みを開始する

自社に適した対策を実行して効果をあげるには、まず、自社が抱える情報セキュリティ上のリスク（事故が発生したとき経営や事業に深刻な損害をもたらす危険性を指します。以下、「リスク」と記載。）を明確に把握することが重要です。

このプロセスでは、経営者が懸念する情報セキュリティ上の重大事故や業務停止などのリスクを洗い出し、それに基づき自社にとって最大の損失を招く可能性がある事故を未然に防ぐための対策を検討します。

具体的な対策内容を整理し、詳細に書面化することで全社的に共有できる明確な基盤を構築します。この書面化した対策を「規定」と呼びます。

３．管理体制の構築

それでは具体的に「管理体制の構築」について見ていきたいと思います。

（１）責任分担と連絡体制の整備

前回取り上げた「組織的な取り組みを開始しよう」において策定・共有された情報セキュリティ基本方針を具体的に実現するために、情報セキュリティ対策を推進する管理体制を決めます（表１）。

情報セキュリティ責任者を中心に、各部門の責任者を通じて、全従業員への情報が的確に伝達される経路を確立しましょう。また、万が一セキュリティ事故や問題が発生した場合には、発生時の状況が迅速に情報セキュリティ責任者に報告されるよう、連絡フローを整えることが重要です。

すでに個人情報保護管理体制（例えば、特定個人情報の事務取扱担当者や苦情対応窓口）などが決まっている場合は、それら既存の管理体制との整合を図りましょう。

役職名	役割と責任
情報セキュリティ責任者	情報セキュリティに関する責任者です。情報セキュリティ対策などの決定権限を有するとともに、全責任を負います。
情報セキュリティ部門責任者	各部門における情報セキュリティの運用管理責任者です。各部門における情報セキュリティ対策の実施などの責任と権限を有します。
システム管理者	社内の情報システムに必要な情報セキュリティ対策の検討・導入を行います。
教育責任者	情報セキュリティ対策を推進するために従業員への教育を企画・実施します。
点検責任者	情報セキュリティ対策が適切に実施されているか点検します。

表１．情報セキュリティ管理のための役割と責任分担例

（引用：中小企業の情報セキュリティ対策ガイドライン）

なお、上記の情報セキュリティ責任者やシステム管理者がそれぞれの役割を果たすためには、情報セキュリティに関する知識や経験が必要です。

こうした知識の習得や経験は一朝一夕では難しいため、中長期の視点を持ちながら、人材育成を計画的に進めていくことを考えましょう。

また、小規模な企業においては、表１の例に忠実である必要はなく、組織の規模や事情に応じた現実的な体制（役割分担）を独自に設計することも大切です。
例えば、経営者自らが情報セキュリティ責任者を兼務することや、防犯や防火などの安全管理責任者を置かれている場合には、この責任者が情報セキュリティ責任者を兼ねることもあります。
しかし、特定の人物一人が情報セキュリティ対策の全てを担う体制は望ましいものではありません。その人物が不在になった場合や、業務負担が大きすぎる場合に問題が生じる可能性が高まります。
そのため、特に情報セキュリティ責任者と点検責任者（監査責任者）は、兼務しないようにしましょう。

この観点から、最低でも２名以上のメンバーによる組織体制が必要と考えられ、実務を担うシステム管理者を加えた３名体制が、一般的な最小限の構成人数といえます。複数人で役割と責任を分担することで、業務を効率的に分散させるとともに、確かな管理体制を整備することが可能になります。

（２）緊急時対応体制の整備
事業や顧客に重大な影響を及ぼすインシデントが発生した際、速やかに適切な対応を取るためには、事前に明確な体制を決めておくことが不可欠です（表２）。

対応を誤ったり、遅れてしまうと、被害が予想以上に拡大し、復旧が難航するなど、深刻な事態を招く可能性があります。
そうならないためには、危機管理の観点から、誰が何を行うのか、その役割や具体的な手順を明確に決めておく必要があります。

さらに、組織内外の緊急連絡先や伝達ルートを整備し、あらかじめ周知しておくことも重要です。加えて、緊急時の対応を想定した訓練やシミュレーションを定期的に実施し、実際に決めたとおりに対応できるのか確認します。

また、関係者やIT製品のメーカー、保守ベンダー等への連絡先をまとめておくことも欠かせません。
業務システムの障害が発生した際には、メールや連絡先を確認するためのウェブ閲覧もできなくなる可能性があるため、連絡方法について代替手段も確認しておきましょう。

役職名	役割と責任
情報セキュリティ責任者 （例：代表取締役）	事故の影響を判断し、対応について意思決定します。
情報セキュリティ部門責任者 （例：管理部長、営業部長）	・事故の原因を調べて情報セキュリティ責任者に報告します。 ・情報セキュリティ責任者の判断・意思決定に基づき適切な処置を行います。 ・事故の原因や被害が情報システムに関係する場合はシステム管理者と連携して適切な処置を行います。
システム管理者 （例：管理部長兼務）	事故の原因や被害が情報システムに関係する場合は情報セキュリティ部門責任者と連携して適切な処置を行います。
事故・異常を発見した従業員	事故や異常の内容を情報セキュリティ部門責任者に報告します。

表２．緊急時対応対策の役割と責任
（引用：中小企業の情報セキュリティ対策ガイドライン）

４．DX の推進と情報セキュリティの予算化

デジタルトランスフォーメーション（DX）の推進

近年のビジネス環境において、中小企業であっても競争力維持・強化のために、デジタルトランスフォーメーション（DX）を進めていくことが求められています。

DX を推進する過程では、クラウドサービスなどデジタル技術やインターネットの活用が多様化する一方で、それに伴うセキュリティリスクも複雑化しています。
それらのリスクに適切に対応するため、セキュリティ管理の充実が最優先事項です。より有効なセキュリティ対策のために、自社の情報システムやネットワーク構造を可視化して対策を検討するとともに、予算を確保する必要があります。

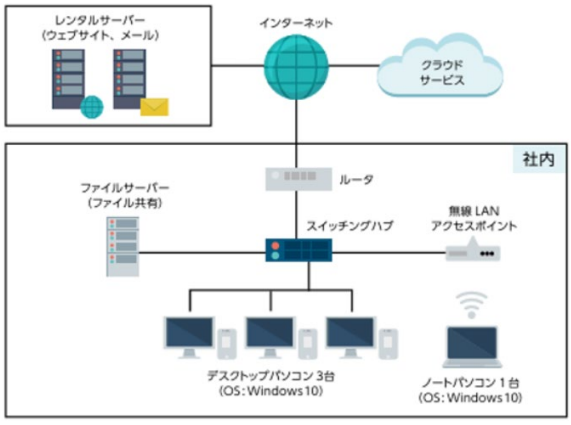


図３．情報システムとインターネットとの接続状況の図
引用：中小企業の情報セキュリティ対策ガイドライン

情報セキュリティの予算化

情報セキュリティに関わる予算の確保は、企業経営の中でしばしば難題となりがちです。
その理由は主に、情報セキュリティへの投資は企業の売上や利益に直結しないため、経営層にその投資対効果が見えづらい点にあります。そのため、セキュリティ予算を上申する際に、

どのように説明すべきかを悩んでいる担当者が多いのも事実です。
その原因としては、次のようなことが挙げられます。

（1）経営者が、セキュリティ投資を「利益を生み出すもの」ではなく、単なる「コスト（費用)」と捉えている
（2）セキュリティ関連の用語や概念が難解で、具体的なリスクやインパクトが理解されづらい
（3）自社のセキュリティリスクが顕著化していない

このように、経営層の理解が不足しているとセキュリティ対策の重要性を説明することが困難です。
このような課題を克服し、情報セキュリティ予算の必要性をしっかりと伝えるためには、「5分でできる！情報セキュリティ自社診断」などのツールを活用し、セキュリティリスクマネジメントの重要性を強調することが有効です。
費用ではなく、リスクが発生することにより売り上げや利益が減少したり、社会的信用が失墜したりすることを防ぐために必要な投資であることを認識してもらうことが重要です。

５．最後に

ここまで「管理体制の構築」と「デジタルトランスフォーメーション（DX）の推進」「情報セキュリティの予算化」の重要性について紹介いたしましたが、いかがだったでしょうか。
管理体制の構築というと大げさな感じがしますが、最低限の体制として、管理者と点検者、さらに実務者（システム管理者）の 3 名が揃っていれば、適切な体制を構築することが可能です。もちろん定期的な見直しは必要ですが、組織体制を整え、積極的に IT 投資を始めることが、企業の持続的成長と発展に不可欠です。これらの取り組みは、単なるコストではなく、企業を守り、競争力を高めるための重要な投資であることを認識してください。

また、DX が売上や利益を拡大するための投資であるのと同様に、情報セキュリティもまた企業の事業継続、さらには社会的信用を守るための投資であることもおわかりいただけたかと思います。
まずは、組織的な体制作りと積極的な IT 投資を開始することが、企業の持続的な成長と発展を支える鍵となると考えます。

６．取り組む際の参考資料

ここまでの解説で取り上げたガイドラインでは、「本格的に取り組む」方法に加え、具体的にどのように取り組むべきか、さらに進めるためにはどうしたら良いのかなど発展的な取り組み方法について紹介しています。

ぜひ、理解を深めたい、次のステップに進みたいと思った際の参考にしてください。

1．中小企業の情報セキュリティ対策ガイドライン（IPA）
2．付録 3：5 分でできる！情報セキュリティ自社診断（IPA）
3．付録 4 ：情報セキュリティハンドブック（ひな形）（IPA）
4．「2024 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」報告書（IPA）

配信予定日：2026 年 1 月 23 日(金) 14:00 頃
カテゴリ：基礎から学ぶ！ セキュリティ
タグ：＃知識編＃初級編
過去記事焼き直し：しない（新規記事です）
記事 URL（新設します）：https://cybersecurity-taisaku.metro.tokyo.lg.jp/basics/attack-damage2/

攻撃や被害が減らない理由（2/2）

目次
●サーバ製品やネットワーク機器等の重大な脆弱性の存在
●ユーザ ID/パスワード等のクレデンシャル情報の大量流出
●業務形態の変化と脆弱なネットワーク
●サイバー攻撃が高収益なビジネスとして確立し、分業化も進む

中小企業の経営者や情報システム担当者の皆さん、日々のセキュリティ対策、お疲れ様です。
前回に続き、本記事では、昨今企業等におけるサイバー攻撃や、その被害が増加し続ける主な理由として考えられる事項を挙げ、解説します。

●サーバ製品やネットワーク機器等の重大な脆弱性の存在
多くの企業等で利用されているサーバ製品やネットワーク機器等にも重大な脆弱性が続々と見つかっており、攻撃者のターゲットとなっています。
JPCERT コーディネーションセンター（JPCERT/CC）では、そうした重大な脆弱性に関する情報を公開し、注意喚起を行っています。その一部を次の表に示します。

JPCERT/CC によって注意喚起された重大な脆弱性（一部抜粋）

公開日	内容
2025-12-03	Array Networks Array AG シリーズにおけるコマンドインジェクションの脆弱性に関する注意喚起
2025-09-26	Cisco ASA および FTD における複数の脆弱性（CVE-2025-20333、CVE-2025-20362）に関する注意喚起
2025-08-27	Citrix Netscaler ADC および Gateway の脆弱性（CVE-2025-7775）に関する注意喚起
2025-04-04	Ivanti Connect Secure などにおける脆弱性（CVE-2025-22457）に関する注意喚起
2025-01-15	Fortinet 製 FortiOS および FortiProxy における認証回避の脆弱性（CVE-

	2024-55591）に関する注意喚起
2025-01-09	Ivanti Connect Secure などにおける脆弱性（CVE-2025-0282）に関する注意喚起
2024-11-19	Palo Alto Networks 製 PAN-OS の管理インタフェースにおける複数の脆弱性（CVE-2024-0012、CVE-2024-9474）に関する注意喚起
2024-10-24	Fortinet 製 FortiManager における重要な機能に対する認証の欠如の脆弱性（CVE-2024-47575）等に関する注意喚起
2024-04-13	Palo Alto Networks 社製 PAN-OS GlobalProtect の OS コマンドインジェクションの脆弱性（CVE-2024-3400）に関する注意喚起
2024-02-15	Fortinet 製 FortiOS の境域外書き込みの脆弱性（CVE-2024-21762）に関する注意喚起
2024-01-11	Ivanti Connect Secure および Ivanti Policy Secure（旧: Pulse Connect Secure）の脆弱性（CVE-2023-46805 および CVE-2024-21887）に関する注意喚起

(https://www.jpcert.or.jp/)

こうした情報は当然のことながら攻撃者も収集しているので、該当する製品等を自社で使用していたとすれば、一刻も早く対処しないと攻撃を受けてしまう可能性があります。それを防ぐためには、「脆弱性を識別・評価・管理する仕組み」の回で解説したような脆弱性情報に基づく対処の仕組みを組織内で確立し、運用していただくことが望まれます。

●ユーザ ID/パスワード等のクレデンシャル情報の大量流出

次に挙げられるのが、後を絶たないユーザ ID、パスワード等のクレデンシャル情報（認証に用いられる情報の総称）の大量流出です。

例えば、かなり前のことですが、2018 年には、日経ビジネス社が国内の複数の大手グループ企業の社員情報が大量に流出していることを報じました。情報はリスト化され、当初は海外の闇サイトで販売されていましたが、その後公開サイトで無料提供されました。

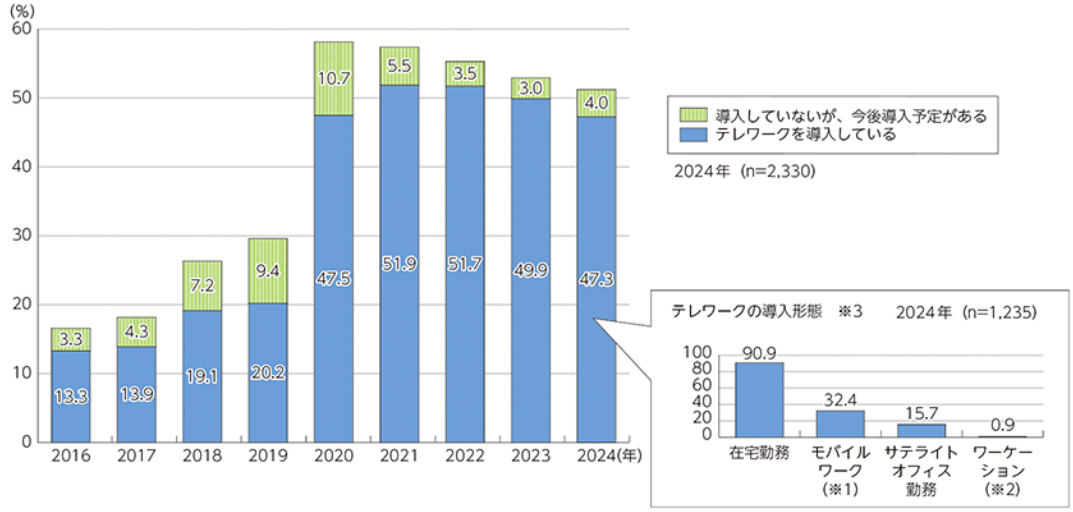
(https://cybersecurity-jp.com/news/26848)

このとき流出していたのは約 16 億件ものクレデンシャル情報です。これらは過去 10 年ほどの期間に流出した「メールアドレス・パスワード」「ユーザ ID・パスワード」「電話番号・パスワード」のいずれかが対になっているものであり、既に無効となっているものもありますが、有効でそのままログイン可能なものも数多く含まれていたようです。

一度流出した情報は削除や回収は不可能であり、永続的にネット上に存在することになります。そして、このような流出は後を絶たず続いており、それらを入手して悪用する不正アクセスを助長しています。

●業務形態の変化と脆弱なネットワーク

新型コロナ禍により、多くの企業にテレワークが浸透しました。その後元の勤務形態に戻った企業もあるものの、依然としてテレワークを主としていたり、推奨していたりする企業も数多くあります。それ自体は業務の効率化や勤務形態の多様化に寄与していることから歓迎すべき点ですが、その反面サイバー攻撃を増長させる要因となっていることも否めません。



※1 営業活動などで外出中に作業する場合。移動中の交通機関やカフェでメールや日報作成などの業務を行う形態も含む。
※2 テレワークなどを活用し、普段の職場や自宅とは異なる場所で仕事をしつつ、自分の時間も過ごすこと。
※3 導入形態は無回答を含む形で集計。

テレワーク導入率の推移（総務省：令和 7 年版 情報通信白書）
(https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r07/html/nd21b220.html)

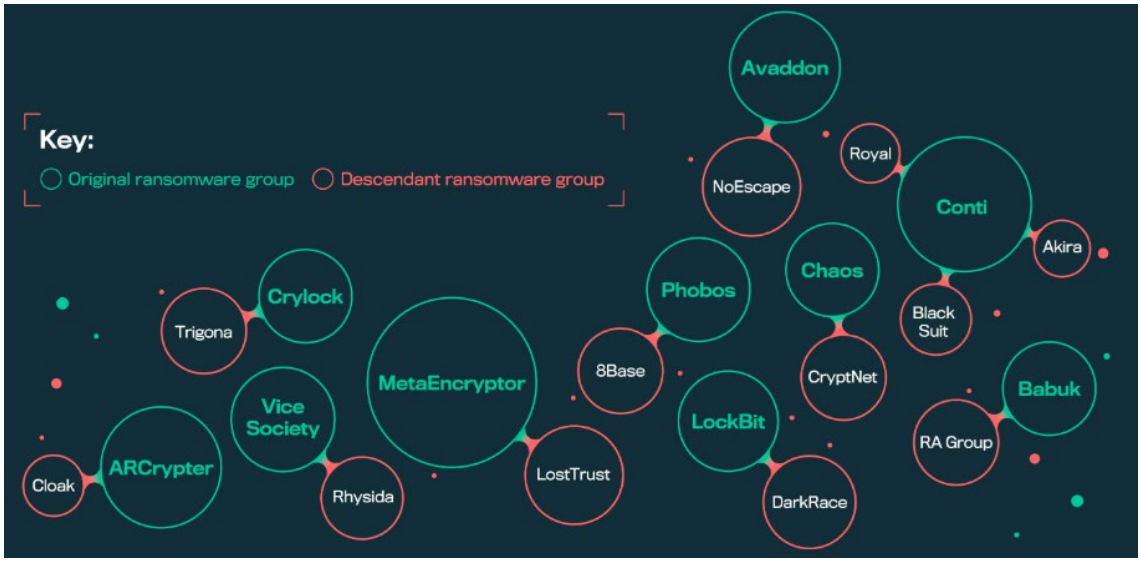
従前サイバー攻撃対策は、インターネット等、外部のネットワークとの境界にあるファイアウォールや VPN（Virtual Private Network）機器等による、いわゆる「境界防御」が中心でした。境界防御では、サイバー攻撃の脅威を境界で遮断することが前提であるため、組織の内部ネットワークやサーバ、PC 等のエンドポイント環境では十分な対策が行われていないという状況となっています。そのため、一旦マルウェア等が感染/侵入すると、短時間で内部ネットワーク全体に被害が拡大するおそれがあります。

また、テレワークの普及により、システム管理業務をはじめ、多くの業務がリモートで行われています。そのため、遠隔操作用のツール等が稼働する機器も増加し、結果として攻撃されやすい状況になっている面もあります。

●サイバー攻撃が高収益なビジネスとして確立し、分業化も進む

ランサムウェアによる攻撃の多くは、攻撃ツールの開発者、身代金の管理者、攻撃実行者が分かれており、RaaS（Ransomware as a Service）としてサービス提供者が 30～40%を受け

取り、残りを攻撃実行者が受け取るといったビジネスモデルが確立しています。
昨今攻撃グループが乱立している状況からしても、世界中に身代金を支払う組織が数多くあり、サイバー攻撃を行う者たちにとって、ランサムウェアは大変都合の良い金銭獲得手段となってしまっているのが実情でしょう。
WithSecure 社が発表したリサーチによれば、近年グループ内での対立によってメンバーが離脱し、攻撃用のソースコードを流用して新たなグループを立ち上げているような状況もあり、その結果攻撃グループが増加し続けているようです。以下の図の緑の円がオリジナル（元の）ランサムウェア攻撃グループであり、赤い円がそこから派生したグループを表しています。



ランサムウェア攻撃グループが派生している状況の例
(https://www.withsecure.com/en/expertise/topicals/ransomware)

このようにビジネスモデルが確立し、分業化が進んだことで、開発を担当する者は豊富な資金を元手に、より強力なツールを開発することに専念できる状況となっています。その結果、ランサムウェアの高機能化が進み、近年では Windows だけでなく、Linux を攻撃対象としたランサムウェアも数多く存在しています。そうした高機能なランサムウェアは、仮想マシンの脆弱性を悪用して乗っ取り、仮想イメージそのものが暗号化されてしまう可能性があるほか、NAS（Network Attached Storage）を攻撃して暗号化し、被害を拡大させる可能性もあります。

前回、今回と企業等におけるサイバー攻撃や、その被害が増加し続ける主な理由として考えられる事項について解説してきました。それらの中には自助努力ではどうにもならないこ

ともありますが、脆弱性への対処については取組み次第で状況を改善できるはずです。

配信予定日：2026 年 1 月 30 日(金) 14:00 頃
カテゴリ：ビジネスヒント
タグ：＃知識編
過去記事焼き直し：しない（新規記事です）
記事 URL（新設します）：https://cybersecurity-taisaku.metro.tokyo.lg.jp/tip/security-ikusei/

組織に求められるセキュリティ人材の確保と育成

目次
●サイバーセキュリティ体制構築・人材確保の手引き
●組織に求められるプラス・セキュリティ人材とは
●プラス・セキュリティ人材の育成方法
●キャリアデザインを含めた人材育成計画の検討
●セキュリティプレゼンター制度の概要
●用語解説

サイバーセキュリティに関する知見や経験を有する人材の確保や、従業員に対するセキュリティ教育、意識向上等は、多くの企業において重要な課題となっています。今回は、そうしたセキュリティ人材の確保や育成に関して参考となるガイド文書や制度等について解説します。

●サイバーセキュリティ体制構築・人材確保の手引き
組織のサイバーセキュリティ体制の強化を進める上で参考となるのが、サイバーセキュリティ経営ガイドラインの「付録 F　サイバーセキュリティ体制構築・人材確保の手引き 第 2.0 版」（以下「本手引き」と表記）です。
「サイバーセキュリティ経営ガイドライン概説」の第 4 回でも解説しているように、本手引きは、同ガイドラインにおいて示されている重要１０項目のうち、次の２項目について具体的な検討を行う場合の参考としていただくことを目的として提供されています。

指示２　サイバーセキュリティリスク管理体制の構築
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

これらのうち、指示 3 における検討のポイントとして次の内容が示されており、特に「プラス・セキュリティ」の取組みの重要性が強調されています。

3.1 **セキュリティを主たる業務とする人材の確保**	① 外部委託を積極活用していても、サイバーセキュリティリスクの把握と対策を推進する自社要員を割り当てる必要があり、当該人材には役割に応じた知識・スキルが求められる。 ② サイバーセキュリティに関する専門性を有する人材は不足状態にあり、確保には工夫が求められる。
3.2 **「プラス・セキュリティ」の取組推進**	① 事業部門、管理部門等においてそれぞれの業務に従事する人材が、DX等のデジタル活用を進めるなかでセキュリティを意識し、業務遂行に伴う適切なセキュリティ対策の実施やセキュリティ人材との円滑なコミュニケーションに必要な能力を育成する「プラス・セキュリティ」の取組が欠かせない。 ②「プラス・セキュリティ」を担う人材に自らの役割と責任の自覚を促すための意識付けを行う。
3.3 **教育プログラム・試験・資格等の活用と人材育成計画の検討**	① 各分野に求められる知識・スキルを踏まえ、教育プログラムや試験・資格の活用を検討する。 ② 自社に必要な人材の配置計画をもとに、キャリアデザインを含めた育成計画を検討する。

「サイバーセキュリティ体制構築・人材確保の手引き」（第 2.0 版）概要版より
(https://www.meti.go.jp/policy/netsecurity/tebikigaiyou2.pdf)

●組織に求められるプラス・セキュリティ人材とは
本手引きでは、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」と定義しています。そして、「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が「プラス・セキュリティ人材」です。

なお、本手引きでは、プラス・セキュリティやプラス・セキュリティ人材について正しく理解するため、次のように補足しています。

①　「プラス・セキュリティ」人材という人材を別に確保する必要はない
通常業務に従事する人材が、サイバーセキュリティの知識やスキルを習得することが「プラス・セキュリティ」の取組みに相当します。同様に、「プラス・セキュリティ」知識がこれまでのサイバーセキュリティ知識とは別に存在するわけではありません。

②　「プラス・セキュリティ」は、DX に取り組んでいなくても必要
DX への取組みの有無に関わりなく IT を活用して事業を行うすべての企業等で必要です。

③　「プラス・セキュリティ」の取組は技術系以外でも必要
サイバーセキュリティに関する知識の中には、情報の保護方法と法律との関係、ステークホルダーからの信頼感醸成のための情報提供のあり方等、法務や広報のような技術系以外の業務に従事する人材が活用することで有効に機能するものもあります。

④　「プラス・セキュリティ」で求められる知識・スキルには高度なものもある
「プラス」の語感から付加的な印象を受けるかもしれませんが、「プラス・セキュリティ」の対象となる業務で求められるセキュリティの知識・スキルと、サイバーセキュリティの専

門業務で用いられる知識・スキルとの間でレベルに明確な違いがあるわけではありません。どちらの業務においても、平易なものから高度なものまで幅広く活用します。

●プラス・セキュリティ人材の育成方法
プラス・セキュリティ人材の育成には、サイバーセキュリティに関する知識・スキル・経験を習得するための教育機会の提供や人材の育成・配置を行うことが必要です。その主なポイントを次に示します。

(1) 各分野に求められる知識・スキルを踏まえ、教育プログラムや試験・資格を活用
(2) 本人の希望を踏まえた上で、キャリアデザインを含めた育成計画を策定・実行

例えば、国家サイバー統括室（NCO：National Cybersecurity Office）では、次のようなプラス・セキュリティ人材の教育カリキュラムの例を公開しています。

	A. 経営層向け	B. 部課長級向け
目標	● サイバーセキュリティが自社のコーポレートリスクに与える影響の把握 ● 影響を踏まえた自社のセキュリティ体制構築・投資の決定・指示 ● インシデント発生時の適切な経営判断・指示	● サイバーリスクが自部署に与える影響理解 ● 自部署で実施されている対策の現状理解 ● 上記の経営層への報告 社内外とのコミュニケーション
時間設定	7.5時間（集合講習3時間＋オンデマンド4.5時間（うち必須3時間））	11時間（集合講習4.5時間＋オンデマンド6.5時間（うち必須5.5時間））
留意点	● 経営会議及び対外対応として実際に起こり得るケースから逆算。 ● 各コマのインプット項目では、部課長級向けから内容を限定・変更。	● 部署内会議やベンダー管理で実際に起こり得るケースから逆算。 ● 既存のスキル等フレームワーク（SP800-181等）と紐付けを実施。
1.基礎知識	①デジタルインフラの基本（30分）◇ ②デジタル技術の基盤とリスク（30分）◇ ③デジタル環境のコストと運用責任（30分）◇	①デジタルインフラ入門（20分）◇ ②サイバーセキュリティに関する用語の意味（20分）◇ ③デジタル環境の管理や責任に関するキーワード（20分）◇ ①デジタルインフラの要点（30分）◆ ②デジタル技術の基盤とリスク（30分）◆ ③デジタル環境のコストと運用責任（30分）◆
2.脅威と対策	①サイバー攻撃手法とそのトレンド（30分）◆ ②脅威への対策（30分）◆ ③事例紹介（実際のサイバー攻撃事例の紹介、サイバー攻撃のデモンストレーション等）（30分）★	①サイバー攻撃手法とそのトレンド（30分）◆ ②脅威への対策（30分）◆ ③事例紹介（実際のサイバー攻撃事例の紹介、サイバー攻撃のデモンストレーション等）（30分）★ ④演習1：脅威と対策における“悪い見本”から学ぶ（60分）★
3.投資	①コーポレートリスクとしてのサイバーセキュリティ（コンプライアンスを含む）（30分）◆ ②体制構築・人材確保（30分）◆ ③演習1：各種対策の費用、損失想定、確率値から必要な投資を検討（70分）★	①サイバーセキュリティのリスクマネジメントの特徴（30分）◆ ②対策における費用と損失の考え方（30分）◆ ③リスクマネジメントのケーススタディ（30分）★ ④演習2：自部署リスクとその対応策を洗い出し、リスク管理部門等へ説明（60分）★
4.SHとの関係	①インシデント対応における経営層の役割（30分）◆ ②通常時の備えと情報開示の在り方（30分）◆ ③インシデント対応と情報開示の事例から学ぶ（30分）★ ④演習2：インシデント発生時の模擬記者会見（50分）★	①インシデント対応プロセスとその準備（30分）◆ ②通常時の備えとインシデント情報の取扱上のポイント（30分）◆ ③インシデント対応と情報開示の事例から学ぶ（30分）★ ④演習3：インシデント発生時の社内外連絡（60分）★
5.関係法令	–	①サイバーセキュリティに関する国内法令とその読み方（20分）◆ ②サイバーセキュリティに関する基準・規格等（20分）◆ ③サイバーセキュリティに関するガイドライン等（20分）◆

★：集合講習での開催が推奨されるもの（受講必須）
◆：オンライン・オンデマンド形式での実施を想定（受講**必須**）
◇：オンライン・オンデマンド形式での実施を想定（受講**任意**）

NCO「プラス・セキュリティ知識補充講座 カリキュラム例」より
(https://security-portal.nisc.go.jp/dx/pdf/plussecurity_curriculum.pdf)

また、各分野の人材が必要な知識・スキルを身に着けるため及びこれを評価する一つの方法として、試験・資格の活用が有効です。本手引きでは、巻末資料２に活用可能な試験・資格の例が数多く挙げられていますが、それらのうち、IPA で実施しているセキュリティに関す

る２種類の資格・試験制度の概要を次に示します。

試験・資格名称	対象者等
情報処理安全確保支援士試験	サイバーセキュリティに関する専門的な知識・技能を活用して企業や組織における安全な情報システムの企画・設計・開発・運用を支援し、また、サイバーセキュリティ対策の調査・分析・評価を行い、その結果に基づき必要な指導・助言を行う人材
情報セキュリティマネジメント試験	情報システムの利用部門にあって、情報セキュリティリーダとして、部門の業務遂行に必要な情報セキュリティ対策や組織が定めた情報セキュリティ諸規程（情報セキュリティポリシを含む組織内諸規程）の目的・内容を適切に理解し、情報及び情報システムを安全に活用するために、情報セキュリティが確保された状況を実現し、維持・改善する人材

「サイバーセキュリティ体制構築・人材確保の手引き」（第 2.0 版）より
(https://www.meti.go.jp/policy/netsecurity/tebikihontai2.pdf)

●キャリアデザインを含めた人材育成計画の検討
「プラス・セキュリティ」を必要とする部署においては、自部署の業務にはサイバーセキュリティに関してどのようなリスクがあって、どのように対応する必要があるかについて、業務の分析を行ったり、必要に応じて社内のサイバーセキュリティ対策の関係者と協議したりする人材を育成する必要があります。
このような人材を育成するには、サイバーセキュリティ対策において、どのような点を意識し、自らの業務に照らしてどのような対策をとる必要があるのかを考えるといった経験が有用です。とはいえ、そうした経験を自部署内のみで経験することは困難な場合があるため、本人の希望を踏まえた上で、セキュリティ担当部署との兼務、もしくは異動により実践経験を積んだり、セキュリティ委員会やリスクマネジメント委員会等のメンバーとして経験を積んだりすることが考えられます。

●セキュリティプレゼンター制度の概要
自組織でセキュリティ人材を確保・育成することが困難な場合等には、IPA のセキュリティプレゼンター制度を活用することも有用です。セキュリティプレゼンターとは、情報セキュリティに関する知識とスキル・技術を持ち、IPA のセキュリティ対策資料等を活用して、中小企業等に対して情報セキュリティの普及啓発を行う人材であり、2025 年 11 月の時点で全国から約 1,800 名が登録されています。

IPA「セキュリティプレゼンター一覧」
(https://www.ipa.go.jp/security/sme/presenter/eid2eo0000002r6h-att/presenter_list.pdf)

セキュリティプレゼンターには、情報処理安全確保支援士、システム監査技術者（情報処理技術者試験）、CISA（公認情報システム監査人）等の情報セキュリティ関連資格保有者の他、中小企業診断士、IT コーディネータ、社会保険労務士、税理士などの資格保有者もおり、様々な視点からの支援活動を行っています。

IPA「セキュリティプレゼンター制度について」
(https://www.ipa.go.jp/security/sme/presenter/index.html)

●用語解説
DX（Digital Transformation）
企業がデータとデジタル技術を活用することで、製品やサービス、ビジネスモデルなどを変革するとともに、業務や組織、企業文化・風土を変革することで、競争優位性を高めようとする一連の取組み。

配信予定日：2026 年 1 月 30 日(金) 14:00 頃
カテゴリ：基礎から学ぶ！ セキュリティ
タグ：＃実用編 ＃知識編
過去記事焼き直し：する（過去記事を上書きします）
過去記事：https://cybersecurity-taisaku.metro.tokyo.lg.jp/basics/kisokaramanabu18/

【令和 7 年度版】中小企業におけるセキュリティ脅威への対策強化　～情報セキュリティ対策の進め方『情報セキュリティ規程から（2/3)』～

目次

独立行政法人情報処理推進機構（IPA）が発行している「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」の「第 2 部実践編」では、具体的な対策方法と中小企業の経営者やシステム担当者がこれにどう取り組むべきかを詳しく解説しています。
情報セキュリティ対策に組織全体で取り組むには、実行すべき対策を決めて、従業員に周知する必要があります。
しかし、こうした作業を行うには情報セキュリティに関する知識や経験が必要となるため、それらの知識や経験に長けた人材がいないと対策が進まなくなることも考えられます。
このような背景から、IPA のガイドラインでは規模の小さな企業や、これまで十分な情報セキュリティ対策を実施してこなかった企業などを対象に、すぐに取り組める対策を示し、段階的に発展させていく計画を紹介しています。この「すぐに取り組める対策」が、多くの企業にとって無理なく、自社の状況に応じた対策を開始する道筋となります。
前回から『本格的に取り組みをはじめよう』というテーマで、3 回に分けて具体的な取り組み方法をご紹介しています。2 回目となる今回は、情報セキュリティ規程に焦点を当て進めていきます。

１．情報セキュリティに対する中小企業の現状

近年、企業や組織を狙ったサイバー攻撃は、頻度や規模を増し日常的に発生する社会的な脅威となっています。最近では、情報セキュリティ対策が強固な大企業ではなく、同一のサプライチェーンを構成する中小企業などの取引先を経由して、攻撃が行われる事例も報じられています。

特に中小企業の場合、セキュリティ対応の不備を悪用され、取引先の機密情報の漏えいや攻撃者が次なる標的へと進むための「踏み台」とされる危険性があります。中小企業は、次の攻撃の足掛かりにされる可能性があることを念頭に置き、適切な情報セキュリティ対策を実施することが重要です。

IPA が作成した、2024 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-報告書-では、中小企業の情報管理に関する実態が浮き彫りになりました。

報告書によると、「情報セキュリティ対策をルール化し、従業員に明示している企業」はわずか 18.1%、一部実施している企業を含めた場合も 39.2%にとどまっていることが判明しました。つまり、少なくとも中小企業の約 60%が正式な文書ポリシーを導入できていない現状を示しております。

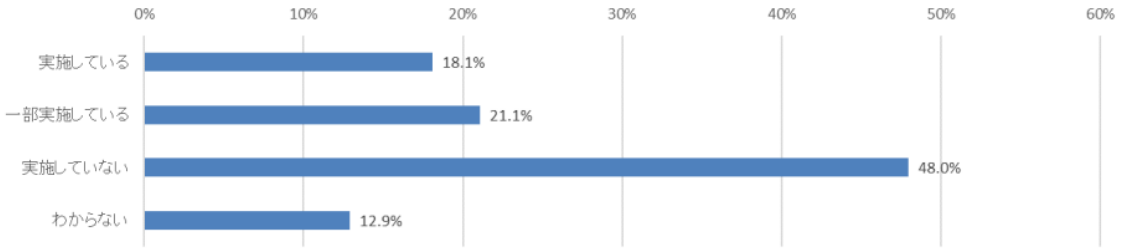


図１．情報セキュリティ対策の状況

（“情報セキュリティ対策をルール化し、従業員に明示しているか“に関する回答）

引用：「2024 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」報告書

セキュリティポリシーは、企業の情報資産を守るために定められたルールやガイドラインです。この規程がなければ、情報を安全に保護し、従業員が安心して情報を取り扱う環境を整えることができません。

セキュリティポリシーを欠いたまま情報セキュリティ対策を進めると、全体的な安全性に欠ける場当たり的な対応に陥る可能性があります。

中小企業がサイバー攻撃の被害を最小限に抑え、さらに安心してビジネス活動を推進するためには、技術的なセキュリティツールの導入以上に、組織の基盤となるルールづくりやガイドラインの整備を進めることが求められます。

２．情報セキュリティ規程の作成

企業が直面するリスクは、その事業内容をはじめ、扱う情報の種類や職場環境、IT インフラの利用状況などによって大きく異なります。汎用的な規程をそのまま使用しても、自社の特性やニーズに適さないことが考えられます。ここでは、自社に適した情報セキュリティ規程を効果的に作成するためのポイントを紹介します。

（１）リスクの洗い出し

まず、情報セキュリティ上のリスクを特定することが必要です。

経営者が懸念する重大なセキュリティ事故を念頭に置きつつ検討を進めます。この時、以下

のような状況を併せて考えることで、対応すべきリスクを把握します。

- 外部要因
  関連する業務や情報に係る法律や規制、情報セキュリティ事故の傾向、取引先からの情報セキュリティに関する要求事項など
- 内部要因
  自社の経営方針や情報セキュリティ方針、管理体制、現行の情報システムの利用状況など

（引用：中小企業の情報セキュリティ対策ガイドライン）

（2）優先的に対応するリスクと対策の決定

全てのリスクに対応しようとすると、高額な費用が必要となったり、業務の非効率化につながるおそれがあります。

そのため、いつ事故が起きてもおかしくない、あるいは事故が起きると大きな被害になるなど、影響が甚大なリスクを優先して対策を実施します。

逆に事故の発生確率が低い、または発生しても被害が軽微なものについては、現状のままにするなど、合理的に対応します。

（引用：中小企業の情報セキュリティ対策ガイドライン）

（3）実践的な規程の作成プロセス

「優先的に対応するリスクと対策の決定」で決めた対策内容を文書化した規程を作成します。

経験が不足している場合、一から作成するのは難しいかもしれません。そのため、中小企業の情報セキュリティ対策ガイドラインに掲載されている「付録５：情報セキュリティ関連規程（サンプル）」（概要は表１）を活用すると良いでしょう。このサンプルを参考に、自社に適した規程にするために修正を加えれば、効率的に規程を完成させることが可能です。

- サンプル使用時のポイント
  サンプル文中の赤字や青字で記載された箇所を自社の実情に即した表現や内容に書き換えることで規定を完成できます。
  サンプルに明記されていなくても必要な対策や有効な対策があれば、追記します。

	名　称	概　要
1	組織的対策	情報セキュリティのための管理体制の構築や点検、情報共有などのルールを定めます。
2	人的対策	取締役及び従業員の責務や教育、人材育成などのルールを定めます。
3	情報資産管理	情報資産の管理や持ち出し方法、バックアップ、破棄などのルールを定めます。
4	アクセス制御及び認証	情報資産に対するアクセス制御方針や認証のルールを定めます。
5	物理的対策	セキュリティを保つべきオフィス、部屋及び施設などの領域設定や領域内での注意事項などのルールを定めます。
6	IT 機器利用	IT 機器やソフトウェアの利用などのルールを定めます。
7	IT 基盤運用管理	サーバーやネットワーク等の IT インフラに関するルールを定めます。
8	システム開発及び保守	独自に開発及び保守を行う情報システムに関するルールを定めます。
9	委託管理	業務委託にあたっての選定や契約、評価のルールを定めます。委託先チェックリストのサンプルが付属します。
10	情報セキュリティインシデント対応ならびに事業継続管理	情報セキュリティに関する事故対応や事業継続管理などのルールを定めます。
11	テレワークにおける対策	テレワークのセキュリティ対策についてルールを定めます。

表 1. 情報セキュリティ関連規程(サンプル)の概要

（引用：中小企業の情報セキュリティ対策ガイドライン）

さらに、情報セキュリティ対策は以下の 3 つのカテゴリに分類することで整理しやすくな

ります。

【人的対策】

従業員教育やガイドライン・規程など「人」に係る対策

サンプル例では、「組織的対策」「人的対策」「情報資産管理」「アクセス制御及び認証」「委託管理」「テレワークにおける対策」「情報セキュリティインシデント対応ならびに事業継続性管理」が該当します。

【物理的対策】

IT 機器や施設など、主に情報を管理している実体があるもの(PC や設備など)に係る対策

サンプル例では、「物理的対策」「IT 機器利用」「IT 基盤運用管理」が該当します。

【技術的対策】

プログラム(セキュリティソフトなど)やネットワーク(ネットワーク監視など)に係る技術的な対策

サンプル例では、「IT 機器利用」「IT 基盤運用管理」「システム開発及び保守」が該当します。

これらの観点を組み合わせることで、自社に最適な情報セキュリティ規程を策定し、実際の運用面で有効性を発揮することが期待されます。

ここまで「本格的に取り組む」の「情報セキュリティ規程」についてご紹介いたしましたが、いかがだったでしょうか。

規程の作成は一見すると複雑で、ハードルが高いと感じるかもしれません。

しかし、まずは初めの一歩としてサンプルを参考にしながら自社の状況に合わせてカスタマイズすることで、スムーズに進めることができるでしょう。

情報セキュリティ規程は、いわばセキュリティ対策の「バイブル」です。この規程が欠けていると、個々のセキュリティ対策が一貫性を欠いた場当たり的なものになってしまう可能性が高いため、非常に重要です。

また、この規程は単に文章として存在するだけではなく、情報セキュリティ担当者が社内の意識向上を図るための説明をする際の根拠にもなります。

規程を用いることで「なぜこの対策が必要なのか」説得力を持って説明することができ、社内全体のセキュリティ意識の統一を目指す一助となるでしょう。

まずは、脅威への基本的な考え方を整理し、それを文書化して定めることが必要不可欠です。

この取り組みは単なるセキュリティ対策だけではなく、長期的には企業の信頼性や競争力を強化し、持続的な企業活動を支える基盤になると考えます。

３．取り組む際の参考資料

ここまでの解説で取り上げたガイドラインでは、「本格的に取り組む」方法に加え、具体的にどのように取り組むべきか、さらに進めるためにはどうしたら良いのかなど発展的な取り組み方法について紹介しています。

ぜひ、理解を深めたい、次のステップに進みたいと思った際の参考にしてください。

1．中小企業の情報セキュリティ対策ガイドライン（IPA）

2．付録 5：情報セキュリティ関連規程（サンプル）（IPA）

3．「2024 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」報告書（IPA）

配信予定日：2026 年 1 月 30 日(金) 14:00 頃
カテゴリ：ビジネスヒント
タグ：＃知識編
過去記事焼き直し：しない（新規記事です）
記事 URL（新設します）：https://cybersecurity-taisaku.metro.tokyo.lg.jp/tip/system-guide/

重要情報を扱うシステムの要求策定ガイド概説

目次

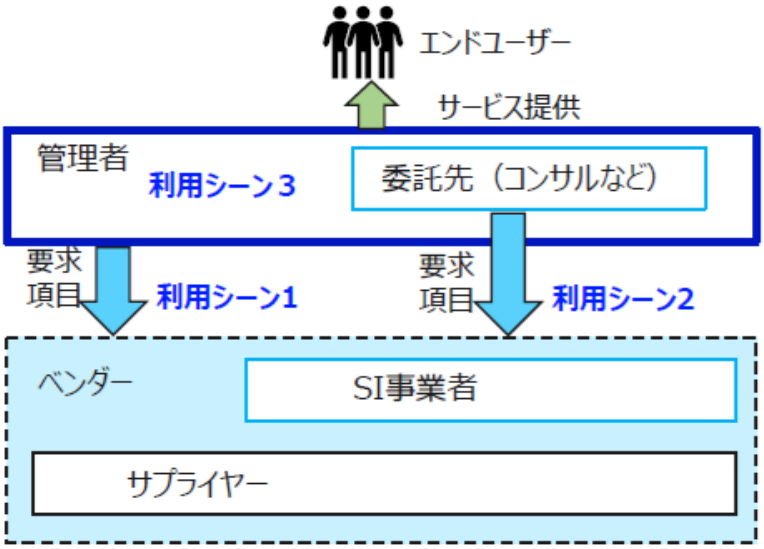
IPA（独立行政法人 情報処理推進機構）では、経済産業省からの要請を受け、重要情報を扱うシステムにおけるサービスの安定供給にあたり、そのシステムのオーナーである管理者が、必要な対策を策定することを可能とするべく「重要情報を扱うシステムの要求策定ガイド」（以下「本ガイド」と表記します）を 2023 年 7 月に公開しました。今回は本ガイドの概要について解説します。

●本ガイド策定の背景
ビジネス環境や技術環境がめまぐるしく変化する今日では、変化への対応力等「利便性」を備えたクラウドサービス等への要求も高まっています。そこで IPA は、重要情報を扱うシステムの構築・調達・運用時に、管理者が「自律性」と「利便性」の双方を両立したシステムの要求仕様を策定できるよう本ガイドを定めました。

●本ガイドの利用シーンとステークホルダー
本ガイドにおいて重要情報とは、国民生活や経済活動の基盤となるサービスで使われる情報のうち、その情報に不正なアクセスがなされた場合、その情報の改ざん・破損があった場合、またはその情報の滅失・紛失または利用が不可能であった場合に、サービス提供に支障が生じ、国家および国民の安全や秩序などを損なう恐れや、経済活動に与える影響が特に大きいものおよびそれに準ずるものと定義されています。そうした情報を扱うのは、主に政府関連機関や地方公共団体、重要インフラに該当する企業等であると考えますが、本ガイドは、そこまでの重要情報を扱っていなくとも、情報システムの調達等においてセキュリティ要件を策定する上で大変参考となる内容となっています。

まず、本ガイドの利用シーンとして、次の 3 つが想定されています。

利用シーン 1 ：管理者自らが調達仕様書を策定する場合
利用シーン 2 ：委託先が調達仕様書を策定する場合
利用シーン 3 ：管理者自らが構築、運用を行う場合



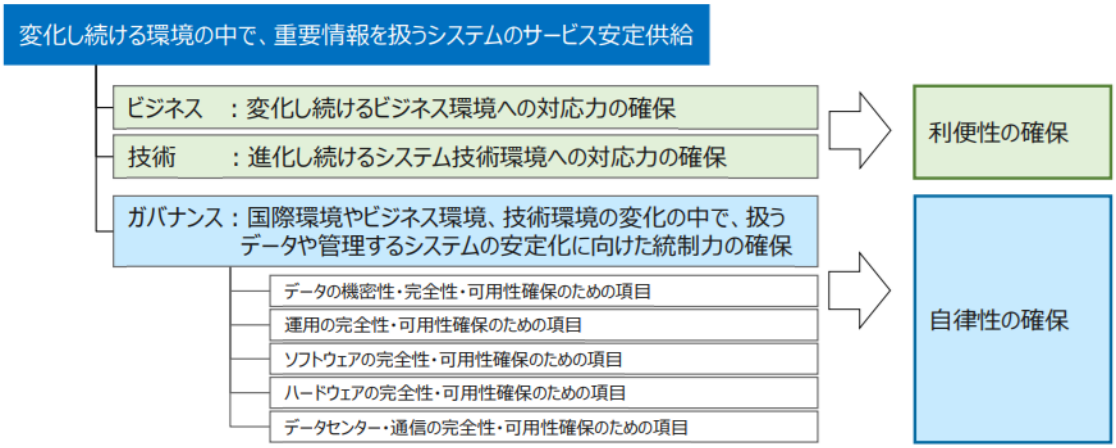
「重要情報を扱うシステムの要求策定ガイド Ver.1.0」より
(https://www.ipa.go.jp/digital/kaihatsu/t6hhco0000006s3t-att/system-youkyu-guide.pdf)

続いて、本ガイドにおける管理者、SI 事業者等のステークホルダーの役割を次のように定義しています。

＜本ガイドにおけるステークホルダーとその役割＞
■エンドユーザー
重要情報を扱うシステムを利用して業務を遂行する
■管理者
重要情報を扱うシステムで提供するサービスのあるべき姿を定め、システムの調達および運用の責任をもつ
■SI 事業者（ベンダー）
管理者が示す要求項目に基づいてシステムを設計、構築、運用するサービスを提供する
■サプライヤー（ベンダー）
クラウドサービスおよびシステムの構成要素（ハードウェア、ソフトウェア、データセンター・通信など）を提供する

●要求項目の整理における考え方

本ガイドでは、変化し続ける環境の中で、様々なリスクを想定し、重要情報を扱うシステムのサービス安定供給を継続するために、「利便性」をビジネスと技術の観点で、「自律性」をガバナンスの観点で要求項目を整理しています。



「重要情報を扱うシステムの要求策定ガイド Ver.1.0」より
(https://www.ipa.go.jp/digital/kaihatsu/t6hhco0000006s3t-att/system-youkyu-guide.pdf)

●要求項目の策定ステップ
管理者は、以下のステップを通して要求項目を策定します。

(1) システムの特性評価

システムの特性を次の 9 つの項目で評価し、優先すべき「享受したい内容」を見極めます。9 つの項目は「自律性」確保と「利便性」確保の 2 つに大別され、自律性の観点では「データの漏洩・改ざんなどの防止」を優先すべきか、「データの利用不可・システム停止などの防止」を優先すべきか、または両方なのかを見極めます。また、利便性の観点では変化し続ける「ビジネス環境への対応」と「技術環境への対応」のどちらを優先すべきか、または両方なのかを見極めます。

＜システムの特性を評価する項目＞

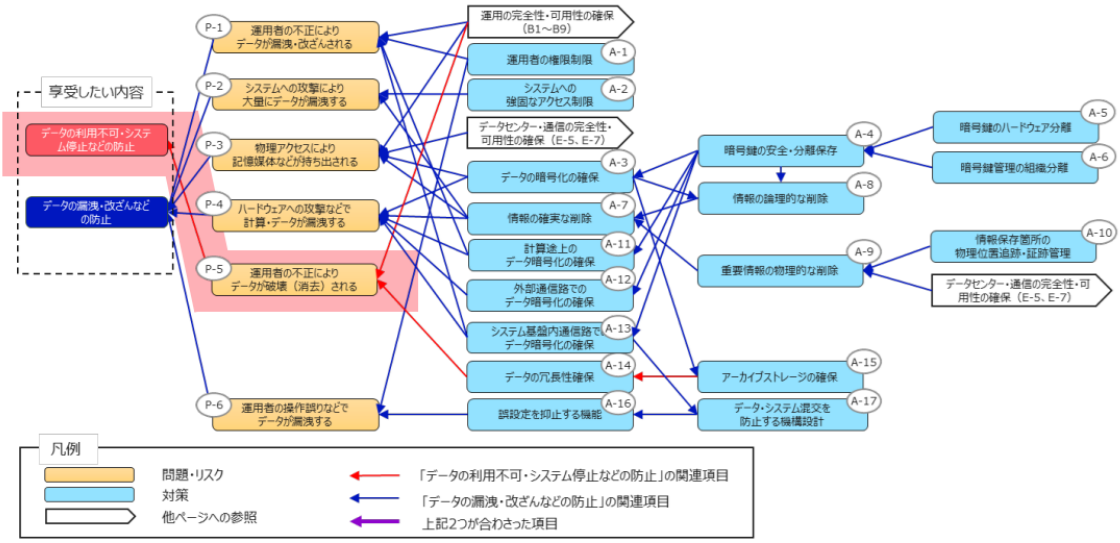
① データの内容・種類（自律性）
② データ数（自律性）
③ 漏洩・改ざん後、取返しがつく/つかない（自律性）
④ データの利用不可・システムの停止などによる影響（自律性）
⑤ 即時的な代替手段の有無（自律性）
⑥ 新機能のリリース頻度（利便性）
⑦ 業務のピーク特性（利便性）
⑧ 先進標準技術への追随（利便性）

⑨ ポータビリティの確保（利便性）

(2) 問題・リスク／利便性要素の選定

続いて、(1)で整理した「享受したい内容」をもとに、自律性の観点では「問題・リスク」を、利便性の観点では「利便性の要素」を、次に示すように樹形図を使って明確にしていきます。

このステップでは、どの問題・リスクに対策を講じるか・講じないか（問題・リスクを許容するか）、または、どの利便性の要素を享受するか、しないかを見極めることがポイントとなります。



「重要情報を扱うシステムの要求策定ガイド Ver.1.0」より
(https://www.ipa.go.jp/digital/kaihatsu/t6hhco0000006s3t-att/system-youkyu-guide.pdf)

(3) 必要な対策の選定

最後に、(2)で明確化された「問題・リスク」「利便性の要素」に紐づく「対策」を選定します。本ガイドでは、「対策」ごとの目的と詳細内容（要求項目）を表で一覧として示しており、目的を理解しながら要求項目を選定できるようになっています。例えば、「自律性確保のための要求項目一覧（データ）」として、次のような要求項目が示されています。（一部抜粋）

No.	データの機密性・完全性・可用性確保のための対策	対策の目的	対策の詳細内容（要求項目）
A-1	運用者の権限制限	運用者の不正もしくは操作誤りなどでデータが漏洩・改ざんされないようにする。	• 非常時復旧などに関わる必要最低限の人を除き、通常サービスのためにシステム基盤を操作する運用者に、重要情報を扱うシステムの業務データに直接アクセスできる手段を用意しないこと。
A-2	システムへの強固なアクセス制限	インターネットなどからシステム基盤内のベンダーの運用操作領域に侵入されることによるデータの漏洩がないようにする。	• システム基盤のうちベンダーの運用操作に関わるインタフェースは通常のアクセス経路から独立した通信経路とし、インターネットなどから操作されないこと。
A-3	データの暗号化の確保	物理アクセスによる記憶媒体などの持ち出しおよびファイル転送などによるデータの持ち出しをされてもデータの漏洩を防止する。	• システム基盤内のストレージについて、暗号化の機能が提供されること。
A-4	暗号鍵の安全・分離保存	暗号鍵をデータと別保管することで、データと暗号鍵を同時に奪われることを防止する。	• システム基盤に保管されるデータの暗号鍵に運用者が通常の手段でアクセスできないこと。 • システム基盤に保管されるデータの暗号鍵を重要情報を扱うシステムの管理者が指定または生成可能であること。
A-5	暗号鍵のハードウェア分離	暗号鍵とデータをハードウェア的に分離しシステム基盤に侵入されても復号のための鍵が持ち出されないことで、データの漏洩を防止する。	• システム基盤に保管されるデータの暗号鍵を、暗号化対象のデータおよびそれに対する処理を行う計算基盤からハードウェア的に分離した機器に格納し、短期的な利用を除きデータと同一のハードウェアに置かないこと。
A-6	暗号鍵管理の組織分離	運用者による組織的な取組でもデータを読み取らせないようにする。（データと鍵の管理を別組織にすることで1組織では解読できない仕組み）	• 一定の規格に基づく暗号鍵管理装置を重要情報を扱うシステムの管理者が持ち込んでシステム基盤に接続し、暗号化に用いることなどの仕組みによって、鍵管理の組織分離を実現すること。
A-7	情報の確実な削除	利用終了後のデータの漏洩・不正利用を防止する。	• 明示的に処理不要と指定されたデータを除き、システム基盤内のストレージに格納された全てのデータが利用終了時に確実に削除される仕組みを確立すること。

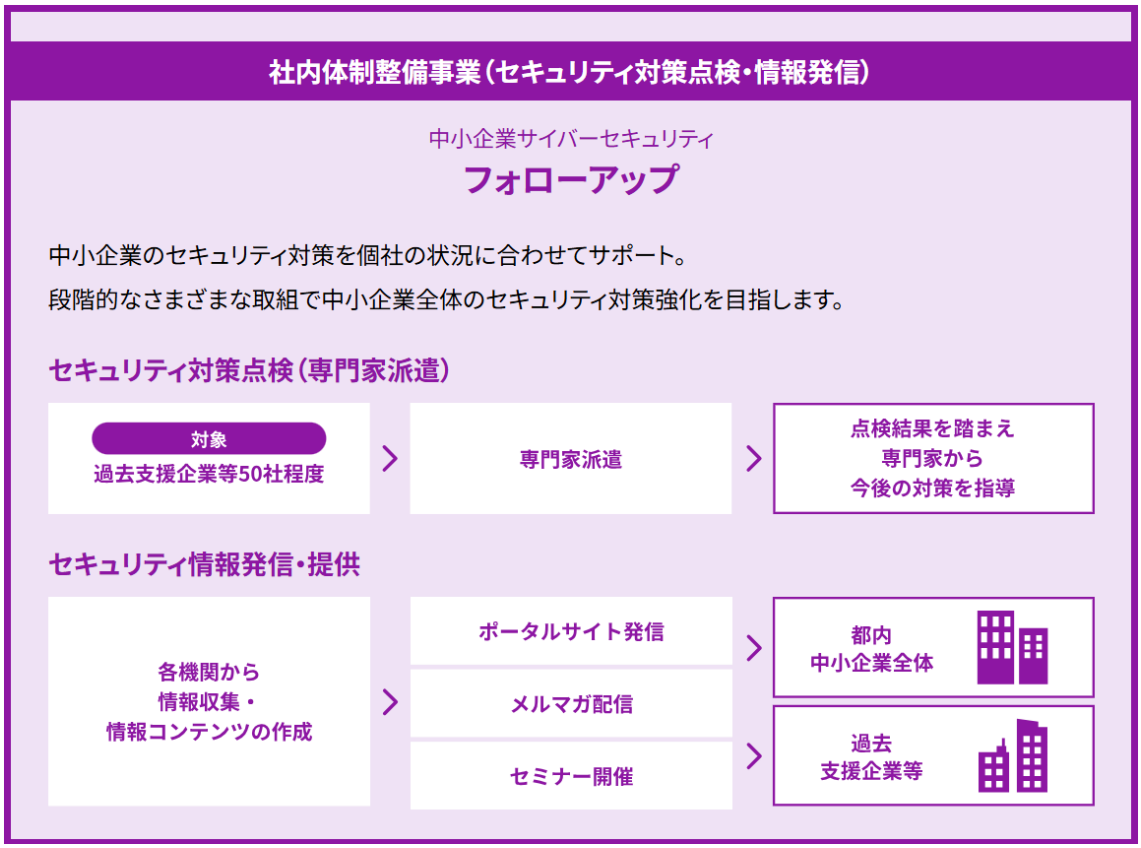
「重要情報を扱うシステムの要求策定ガイド Ver.1.0」より
(https://www.ipa.go.jp/digital/kaihatsu/t6hhco0000006s3t-att/system-youkyu-guide.pdf)

配信予定日：2026 年 2 月 6 日(金) 14:00 頃
カテゴリ：参加者の声
タグ：＃実用編
過去記事焼き直し：しない（新規記事です）
過去記事：https://cybersecurity-taisaku.metro.tokyo.lg.jp/questionnaire/r7tenken/

参加者の声（令和 7 年度セキュリティ対策点検 1 回コース）

目次

１．事業概要



当事業は都内中小企業がセキュリティ対策の継続的な実践や、定期的な見直しが出来るようサポートする事業です。「セキュリティ対策点検(専門家派遣)」と、「セキュリティ情報発信・提供」の 2 つの支援を実施いたしました。
支援内容詳細については、下記をご確認ください。

フォローアップ事業 TOP
https://cybersecurity-taisaku.metro.tokyo.lg.jp/follow-up/
記事「ライトな支援あります！セキュリティ対策点検」
https://cybersecurity-taisaku.metro.tokyo.lg.jp/know_more/cyber-taisakutiken5/

セキュリティ対策点検(専門家派遣)は、ASM、プラットフォーム脆弱性診断、約 50 項目のヒアリングシートを用いて専門家がお伺いしてセキュリティ対策状況の棚卸しや今後の取り組みをアドバイスします。
専門家の派遣回数 1 回コースと 3 回コースがあります。今回は令和 7 年度の事業においてセキュリティ対策点検 1 回コースを受けていただいた企業様 2 社にヒアリングした内容を紹介させていただきます。

２．ヒアリングより（セキュリティ対策点検１回コース）

A 社（主要発注元の取引停止を防ぐため、情報セキュリティ対策を優先事項として取り組む）

セキュリティ対策状況：
セキュリティインシデントが主要発注元の取引停止に直結する恐れがあり、情報セキュリティ対策は優先事項として取り組んでいる。これまで規程や体制の整備を実施し、今後はシステムによる対策を検討している。

参加の背景：
体制強化のため情報セキュリティ委員会を設置し規程整備を進めた頃、都の支援事業の存在を知り参加。レベル別の支援メニューを活かし、令和 6 年度基本対策事業、令和 7 年度セキュリティ対策点検に参加。

参加しての変化：
技術的な診断およびヒアリングベースの診断を用い、有識者の意見を聞くことで今後必要なセキュリティ対策が明確になった。システム導入は予算が必要であり、予算化に向け取り組みを進めている。

今後実施していきたい対策：
製造業では今後、経済産業省のサプライチェーン強化に向けたセキュリティ対策評価制度★4 が求められるため、取得に必要なセキュリティ対策システムの導入を実施していきたい。

B 社（情報システム部署経験者を採用し情報セキュリティ対策を強化）

セキュリティ対策状況：

飲食店という業態であり比較的情報セキュリティ対策は求められない環境であったが、上場を目指すにあたり証券会社から情報セキュリティ対策を指摘されたこともあり、情報セキュリティ対策に取り組み始め、ルールや教育から着手している。

参加の背景：

体系立てた情報セキュリティ知識を得るため令和 6 年度実践力強化プログラムに参加し、今年度は社内の現状を調査して必要な対策を明確化したかったためセキュリティ対策点検に参加。

参加しての変化：

情報セキュリティ対策状況を体系的に確認し、今後の改善点が明確になった。

今後実施していきたい対策：

社内体制強化のため情報セキュリティ委員会を設置し、インシデント対応力を強化するため CSIRT の設置を行いたい。

個社の様々な事情に配慮し企業名は伏せさせていただきました。皆様の情報セキュリティ対策のお役に立てれば幸いです。

次回はセキュリティ対策点検 3 回コースを受けていただいた企業様の声を掲載したいと思います。

配信予定日：2026 年 2 月 6 日(金) 14:00 頃
カテゴリ：基礎から学ぶ！ セキュリティ
タグ：＃知識編 ＃実用編
過去記事焼き直し：する（過去記事を上書きします）
過去記事：https://cybersecurity-taisaku.metro.tokyo.lg.jp/basics/kisokaramanabu19/

【令和 7 年度版】中小企業におけるセキュリティ脅威への対策強化　～情報セキュリティ対策の進め方 『本格的に取り組もう（3/3)』～

目次

独立行政法人情報処理推進機構（IPA）が発行している「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」の「第２部実践編」では、具体的な対策方法と中小企業の経営者やシステム担当者がどう取り組むべきかを詳しく解説しています。

今回は、『本格的に取り組みをはじめよう』というテーマの３回シリーズの最終回をお届けします。この回では、「４.本格的に取り組む」 の「（４）委託時の対策」と「（５）点検と改善」に焦点を当て、進めていきます。

１．委託時の対策

（１）委託と受託の関係

ビジネスを展開する企業において、全ての業務を自社で完結させることは現実的ではありません。そのため、多くの企業は特定の業務を外部へ依頼する手段として「委託」を選択しています。
「委託」は、外注や委任、準委任、アウトソーシングなど、多様な形態を含み、他の企業や専門機関に特定の業務を行ってもらう手法です。

一方「受託」とは、他者からの依頼を受け、業務を引き受けることを指します。また、業務の成果物を確約する「請負」を意味することもあります。
どのような企業でも事業を円滑に進めるうえで、全ての業務を自社で行うことは難しいため、委託している業務があり、それを引き受ける受託企業があることでビジネスは成り立っています。また、業務を委託するときには、委託元と委託先との間で業務上必要な情報のやり取りが生じます。
製造業で、外部の工場に部品の製造を委託する場合は、詳細な設計図が、税理士に決算書の作成を委託する際には、売上伝票や出金伝票が提供され、運送会社に商品配送を委託する場合には、顧客の住所・氏名などの個人情報が授受されます。
こういったプロセスで、重要な情報や個人情報が委託先に提供されますが、もし委託先が適切なセキュリティ対策を講じていなければ、情報漏えいや改ざんなどのリスクが生じる恐れが高まります。
さらに、こうした事故が委託先で発生した場合であっても、委託元の管理責任が問われることもあります。
また、委託先がサイバー攻撃を受け、システム停止やウイルス感染が発生すると、受発注や製品出荷の停止を引き起こし、自社のビジネスに大きな影響を与える可能性があります。
近年、グローバル化やデジタル化が進んだ結果、委託や受託の関係が複雑化しています。
具体的には、部品の製造を受託した企業が、原材料を海外から調達し、部品加工をさらに他社に委託・再委託するケースや、完成部品の運送を別の配送業者に委託することなどが行われています。
このような調達や製造、販売などの一連の流れは「サプライチェーン」と呼ばれていますが、サプライチェーンの中で情報セキュリティ対策が不十分な企業があると、その企業がサイバー攻撃を受けることで、サプライチェーン内の他の企業にも影響を与える可能性があります。このため、業務を受託する側の中小企業であってもサプライチェーンを構成する一員であることを自覚し、情報セキュリティ対策に取組むことが求められています。

（2）委託や受託時の対策とその状況

近年、社内業務の一部または全てを外部に委託したり、レンタルサーバーやクラウドサービスなどの外部の IT サービスを利用することが一般的になっています。
重要な企業情報を外部に託したり、処理を依頼する場合には、委託先にも情報セキュリティ対策を実施してもらう必要があります。

IPA が作成した、「2024 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」(以降「実態調査」と略す)によると、販売先（発注元企業）からの情報セキュリティに関する要請を受けた経験があるかについて、「いいえ」が 79.9%と高く、「はい」の 12.2%を大きく上回っています。

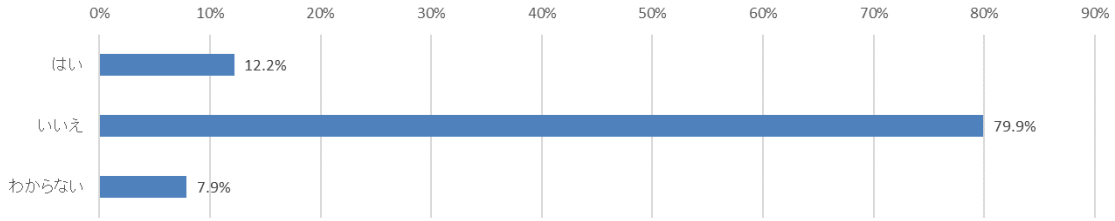
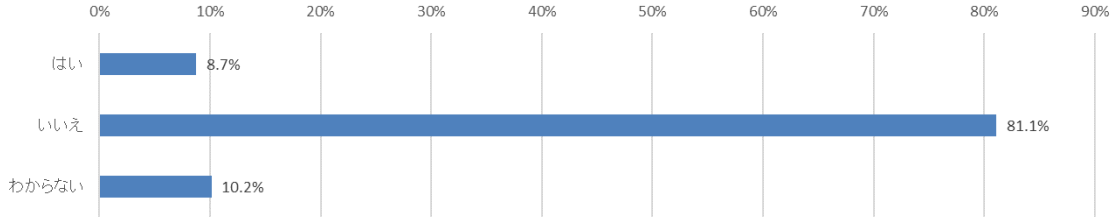


図 1　販売先（発注元企業）から情報セキュリティに関する要請を受けた経験　（引用：「2024 年度 中小企業における情報セキュリティ対策に関する実態調査」報告書）

また、仕入先（委託・協力企業）に対してセキュリティ対策の要請をしたことがあるかについても、「いいえ」が 81.1%と高く、「はい」の 8.7%を大きく上回っています。



これは、「自社のセキュリティが十分であれば問題ない」、あるいは「特に要求されていないので、情報セキュリティに特別な配慮は不要」といった誤った認識を招く原因となっています。

直接指示することが難しい外部委託先に情報セキュリティ対策を実施してもらうためには、取引契約の中であらかじめ具体的な対策を契約書や覚書などに盛り込むことが大切です。
もし、個別に契約や覚書を交わすことが難しい場合は、委託先のサービス規約や情報セキュリティに関わる対応方針を確認したうえで選定することが求められます。
実態調査によると、販売先（発注元企業）からの情報セキュリティに関する要請の具体的な内容について「秘密保持」の割合が 79.6%と最も高く、次いで「情報セキュリティに関する契約内容に違反した場合の措置」が 36.4%、「サイバーインシデントが発生した場合の対応」が 30.5%となっています。

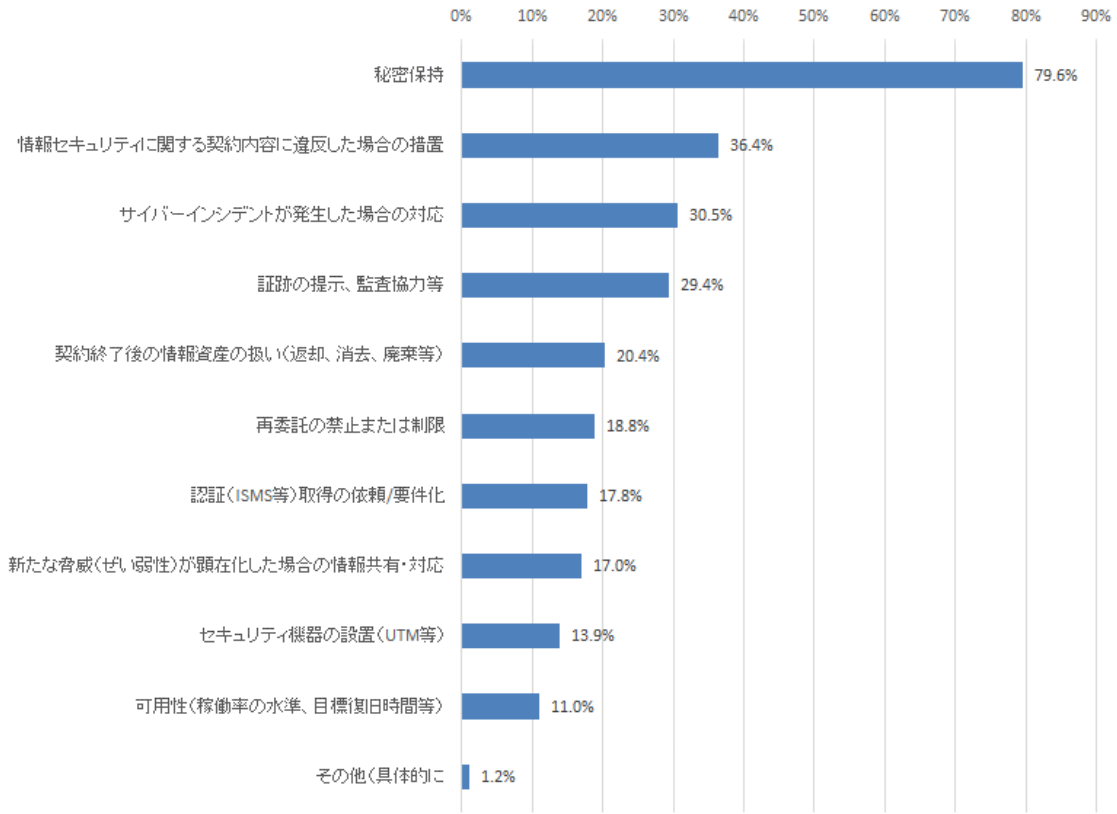


図２　販売先（発注元企業）からの情報セキュリティに関する要請の具体的な内容
（引用：「2024 年度 中小企業における情報セキュリティ対策に関する実態調査」報告書）

これらのデータから、委託先・受託先との間での秘密情報の扱いに対する意識、リスク管理の意識は高まっているものの、具体的な情報セキュリティ対策に関して意識しているのは企業の３割程度に過ぎないことがわかります。

（３）個人情報を取り扱う業務の委託や受託

個人情報保護法では、個人データ※1の取り扱いを委託する場合は、委託先にも情報セキュリティ対策を実施するように監督することが義務付けられています。
委託元は、委託先の状況を把握し、対策が確実に実施されるよう責任を持つ必要があります。

1

もし委託先の対策が不十分で事故が起きた場合、委託元は管理責任を問われ、委託先は委託元の信頼を失うことになります。
重要な情報や個人情報など、セキュリティ事故の影響が大きい情報を取り扱う場合は、委託元は委託先に求めるセキュリティ対策要件を明確に伝え、受託側はそれらを理解、実行することが重要です。

これらを踏まえ、取り扱う情報の種類や委託する業務に適した情報セキュリティ対策を、委託先にも実施してもらいます。機密情報や個人情報を取り扱う際には、「情報セキュリティ関連規程（サンプル）」（付録 5）の「9 委託管理」を参考にして、委託先の選定、契約締結をしてください。
さらに、情報セキュリティ対策が継続して実施されているか、新たな対策が必要になったときに対応しているかを随時確認し、委託先の情報セキュリティ対策を維持するよう責任を持って管理します。
※個人情報保護法では「個人情報」、「要配慮個人情報」、「個人情報データベース等」「個人データ」、「保有個人データ」、「個人関連情報」、「仮名加工情報」、「匿名加工情報」等の語を使い分けており、個人情報取扱事業者等に課される義務はそれぞれ異なるので、注意が必要です。

２．点検と改善

情報セキュリティの点検とは、計画した情報セキュリティ対策が適切に実行されているか、見落としがないか、その対策がセキュリティ事故の防止に役立っているかを確認することです。
点検結果を経営者に報告し、経営者が意図するセキュリティ対策が実現できているかを確認し評価をすることが重要です。経営者の評価を得ることで、場合によってはリスクの特定に戻り、対策を見直すことで取り組みの精度を高めることができます。
具体的な点検や改善の取組みについては、過去の記事「情報セキュリティの見直しと強化（監査と点検）(1/3)」に詳細が説明されているので、そちらも併せてご参照ください。

ここまで「４.本格的に取り組む」の「（４）委託時の対策」と「（５）点検と改善」についてご紹介いたしました。業務をスムーズに遂行する上で、受託と委託の関係が不可欠であること、そして、これらの関係性が生じる際には、情報セキュリティの重要性を考慮する必要があることを理解していただけたでしょうか。
情報セキュリティへの取り組みを疎かにしないよう、定期的な点検と改善を行うことが重要であり、その取り組みが企業の持続可能な発展を支える鍵となります。

今回をもって、中小企業の情報セキュリティ対策ガイドラインの「第２部実践編」の解説は終了となります。今後も定期的に点検を行い、セキュリティ対策を強化していきましょう。

３．取り組む際の参考資料

ここまでの解説で取り上げたガイドラインでは、「本格的に取り組む」方法に加え、具体的にどのように取り組むべきか、さらに進めるためにはどうしたら良いのかなど発展的な取り組み方法について紹介しています。

ぜひ、理解を深めたい、次のステップに進みたいと思った際の参考にしてください。

１．中小企業の情報セキュリティ対策ガイドライン（IPA）

２．付録５：情報セキュリティ関連規程（サンプル）（IPA）

３．「2024 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」報告書（IPA）

配信予定日：2026 年 2 月 6 日(金) 14:00 頃
カテゴリ：基礎から学ぶ！ セキュリティ
タグ：＃知識編 ＃実用編
過去記事焼き直し：する（過去記事を上書きします）
過去記事：https://cybersecurity-taisaku.metro.tokyo.lg.jp/basics/kisokaramanabu20/

【令和 7 年度版】中小企業におけるセキュリティ脅威への対策強化　～よくある質問への回答～

目次

これまで、独立行政法人情報処理推進機構（IPA）が発行する「情報セキュリティ１０大脅威 2025」や「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」を基に、中小企業の経営者やシステム担当者が行うべき情報セキュリティ対策について掘り下げてきました。

今回は、セミナーやメルマガのアンケートでたびたび寄せられる質問に焦点を当てて解説します。

- 経営層に求められるリーダーシップの具体的アクション【組織・人的対策】
- 社員教育の進め方　【組織・人的対策】
- 情報資産の扱い方・管理方法　【技術的対策】

１．経営層に求められるリーダーシップの具体的アクション

情報セキュリティにおいて最も重要な要素は、定着化であると言っても過言ではありません。とはいえ、この定着化の実現は、最も困難な要素でもあります。
経営層の方からよく聞く声として、次のようなものがあります。

・規程を作ったが、どう徹底させればよいかわからない
・現場が面倒くさがって、なかなか実行してくれない
・社員の IT リテラシーが低く、理解が進まない
・社内教育は実施しているが、浸透しない

これらを解決するためには、次の４つのアクションが重要です。

・経営層の積極的な参画
・セキュリティ規程の見直し
・従業員に自分事として感じさせる
・定期点検の有効活用

「セキュリティ規程の見直し」と「定期点検の有効活用」は、以前の記事で解説したので、今回は「経営層の積極的な参画」と「従業員に自分事として感じさせる」という観点で進めていきます。

（１）経営層の積極的な参画

情報セキュリティ対策を疎かにすると、経営に大きな影響を与え、最悪の場合、経営破綻や法的・道義的責任を問われることもあります。外部への影響だけでなく、企業と従業員を守るためも、情報セキュリティ対策は組織全体で取り組む必要があり、その際、経営層の関与は不可欠です。
経営層の積極的な関与なしに、情報セキュリティ対策は成り立たないといえます。
経営層には情報セキュリティ対策を組織的に実施する意思を、従業員や関係者に宣言し（情報セキュリティ基本方針の作成と公開)、具体的な対策を「企業や組織を守るためだけでなく従業員を守るための取り組みでもある」ことを説明することが求められます。また、その後も継続的に対策に取り組む姿勢を見せることが重要です。

（２） 経営層が果たすべき具体的なリーダーシップ

経営層には、サイバーセキュリティ経営ガイドライン Ver3.0 に記載されているサイバーセキュリティ※対策におけるリーダーシップと同等のことが求められます。経営者は、以下の１０項目について、サイバーセキュリティ対策を実施する上での責任者や担当部署 CISO、サイバーセキュリティ担当者等）への指示を通じて組織に適した形で確実に実施させる必要があります。
指示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

指示２：サイバーセキュリティリスク管理体制の構築
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
指示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
指示５：サイバーセキュリティリスクに効果的に 対応する仕組みの構築
指示６：PDCA サイクルによるサイバーセキュリティ対策の継続的改善
指示７：インシデント発生時の緊急対応体制の整備
指示８：インシデントによる被害に備えた事業継続・ 復旧体制の整備
指示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状況把握及び対策
指示１０：サイバーセキュリティに関する情報の収集、共有及び開示の促進

この際「任せきり」や「依頼しっぱなし」にならないよう、組織のリスクマネジメントの責任を担う経営者が自らの役割として実施方針の検討、予算や人材の割当、実施状況の確認や問題の把握と対応等を通じてリーダーシップを発揮することが重要となります。

※サイバーセキュリティと情報セキュリティとの違い
セキュリティ対策の基本的な考え方は同じと言えるが、サイバーセキュリティは情報セキュリティの３要素である、「機密性」「完全性」「可用性」に「安全性」(テロや戦争などの物理的な機器の破壊を想定)が加わり、かつ、デジタルデータを対象としている。また、情報セキュリティでは対象となっていた紙媒体が対象外となっていることが大きな違いといえる。

２．教育の進め方

情報セキュリティ教育は、以下の点を考慮して教育計画を年度単位で立案します。

・情報セキュリティ関連規程の説明（特に入社時や規程改訂時）
・最新の脅威に関する注意喚起（随時）
・関連法令の理解（特に公布・施行時）
・個人情報の取り扱いに関する留意事項

計画の立案においては IPA「講習能力養成セミナー」が動画公開されておりますので、適宜参考にするのが良いでしょう。

また、情報セキュリティ教育で重視すべきポイントは次の３点です。

・基礎知識の提供
・脅威の具体的理解
・自ら対策を考える能力の育成

学習並びに研修資料作成にあたっては、独立行政法人情報処理推進機構（IPA）が提供しているコンテンツを利用するとよいでしょう。

（１）基礎知識の提供

「5 分でできる！情報セキュリティポイント学習」など、簡単に学べるコンテンツを活用し、従業員が日常の中で実践的に学べるようにします。このコンテンツは、主に中小企業で働く方を対象に、職場の日常の１コマを取り入れた１テーマ５分程度の無料コンテンツです。

従業員向けコース(4 テーマ)は、親しみやすい内容で、セキュリティに関する様々な事例を疑似体験しながら、適切な対処法を学ぶことができます。

（２）脅威の具体的理解

「情報セキュリティ１０大脅威 2025」や「映像で知る情報セキュリティ」などを活用します。

情報セキュリティ１０大脅威 2025 は、組織編と個人編の２系統で構成されています。これらの学習を通じて自社や自身を脅かす可能性のある脅威について学び、自分自身の身の回りに起こり得ることと捉えてもらい、具体的なリスクについて理解を深めます。

また、映像教材を利用すれば、ドラマ仕立てで情報セキュリティ上の様々な脅威と対策を学ぶことができます。

（３）自ら考える能力の育成

危険予知訓練（KYT：危険のＫ、予知のＹ、訓練(トレーニング)のＴをとったもの）を通じて、組織や職場に潜むリスクを発見し、対応策を考える力を養います。ＫＹＴの基礎手法である「ＫＹＴ基礎４ラウンド法」では、危険の潜むイラストを使ったシミュレーションにより、リスクを予測し、対策を検討する能力を身につけることができます。

イラストの例を図１に示します。

図１　危険が潜むイラスト例

引用元：令和６年度 東京都中小企業サイバーセキュリティフォローアップ事業
第１回セミナー「社内へのサイバーセキュリティ対策の浸透」より抜粋

ラウンド	危険予知訓練の4ラウンド	危険予知訓練の進め方
1R	どんな危険がひそんでいるか	イラストシートの状況の中にひそむ危険を発見し、危険要因とその要因がひきおこす現象を想定して出し合い、チームのみんなで共有する。
2R	これが危険のポイント	発見した危険のうち、これが重要だと思われる危険を把握して○印、さらにみんなの合意でしぼりこみ、◎印とアンダーラインをつけ「危険のポイント」とし、指差し唱和で確認する
3R	あなたならどうする	◎印をつけた危険のポイントを解決するにはどうしたらよいかを考え、具体的な対策案を出し合う
4R	私達はこうする	対策の中からみんなの合意でしぼりこみ、※印をつけ「重点実施項目」とし、それを実践するための「チーム行動目標」を設定し、指差し唱和で確認する

図２　ＫＹＴ基礎４ラウンド法による危険予知訓練の進め方

引用元：厚生労働省 職場のあんぜんサイト から抜粋引用

これらを組み合わせることで、従業員が自分事としてとらえられるように学習していきます。

具体的な進め方の詳細は下記のサイトをご確認ください。

・職場のあんぜんサイト：危険予知訓練（ＫＹＴ）　（厚生労働省）

３．資産の扱い方・管理方法

ここでは、情報セキュリティにおける資産の洗い出し方法と管理するためのリスク分析の方法を解説します。

情報資産の把握方法については、こちらの記事でも紹介しています。あわせてご覧ください。

・コスト意識から投資意識へ～セキュリティ対策に関わる費用と効果～

（１）資産管理台帳の作成

業務で利用する電子データや書類を洗い出し、情報資産管理台帳に記入します。

その際、業務の流れ（業務フロー）に沿って情報資産を整理すると、業務全体を俯瞰でき、どのように情報を生成し、保持し、破棄しているかといったライフサイクルが見えるので効果的です。

例えば、「受注データ」は、注文受付で発生し、販売管理システムで管理され、期間が過ぎると、注文書破棄のタイミングで消滅します。

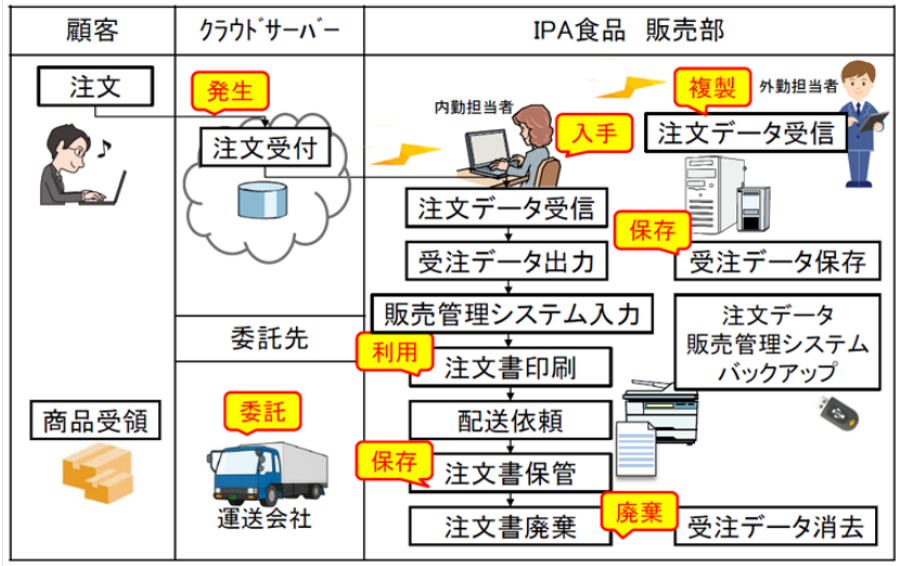


図３　業務の流れとデータのライフサイクル例

　引用元［IPA］セキュリティプレゼンターカンファレンス 2017　資料を基に作成

また、資産の粒度は、細かすぎると管理が大変になり、逆に粗いと以降の資産のリスク評価、管理が難しくなります。

例えば、「設計書」などと大きい単位で洗い出しを行い、顧客単位に分ける必要はありません。下記の「台帳記入例」シートのリストアップ例が資産粒度の目安となります。

この作業を通じて、業務フローに沿った形で情報の管理が可能となります。

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		
						個人情報	要配慮個人情報	特定個人情報
人事	社員名簿	社員基本情報	人事部	人事部	事務所PC	有		
人事	社員名簿	社員基本情報	人事部	人事部	書類	有		
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	
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
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			
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			
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		
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		

引用元：中小企業の情報セキュリティ対策ガイドライン第 3.1 版を基に作成

（2）資産の評価

次に、それぞれの情報資産ごとに情報セキュリティの 3 要素（機密性・完全性・可用性）に対する評価を行い、その影響度を明確にします。法律や契約などの要件も確認しつつ、企業独自の基準で判断します。

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		
						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
人事	社員名簿	社員基本情報	人事部	人事部	事務所PC	有			3	1	1
人事	社員名簿	社員基本情報	人事部	人事部	書類	有			3	3	3
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		3	3	2
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	3	3	2
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				2	2	2
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				2	2	2
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			3	3	3
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			3	3	3

図 5　評価基準を追記した資産管理台帳記入例

引用元：中小企業の情報セキュリティ対策ガイドライン第 3.1 版を基に作成

基準作成においては、外部影響等を十分考慮し、「顧客情報を含む場合は機密性３とする」「外部に直接損害を与える可能性があるものは完全性３とする」「３時間以上の停止が許容されないものは可用性３とする」など、可能な限り客観的な基準とし、業務の変容、情報資産の活用方法の変容などに際し、客観的な見直しができるようにしましょう。

（３）資産の管理

３要素の評価から重要度を決定し、発生頻度なども考慮した上で、リスク値を算出します。
リスク値の大きさに基づき、適切な対応策を検討して管理します。

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			3	1	1	3		2023/4/1	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	6 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			3	3	3	3		2023/4/1	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	3 リスク小
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		3	3	2	3	5年	2023/4/1	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	3 リスク小
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	3	3	2	3	7年	2023/4/1	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	6 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				2	2	2	2		2023/4/1	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 リスク小
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				2	2	2	2		2023/4/1	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 リスク小
共通	電子メールデータ	重要度は現在のため最高値で評価	担当者	総務部	事務所PC	有			3	3	3	3		2023/4/1	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	6 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			3	3	3	3		2023/4/1	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	6 リスク大
営業	顧客リスト	得意先（直近５年間に実績があるもの）	営業部	営業部	社内サーバー	有			3	3	3	3		2023/4/1	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	6 リスク大
営業	顧客リスト	得意先（直近５年間に実績があるもの）	営業部	営業部	可搬電子媒体	有			3	2	2	3		2023/4/1	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	3 リスク小
営業	顧客リスト	得意先（直近５年間に実績があるもの）	営業部	営業部	モバイル機器	有			3	2	2	3		2023/4/1	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	6 リスク大
営業	受注伝票	受注伝票（過去10年分）	営業部	営業部	社内サーバー				2	2	2	2		2023/4/1	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 リスク中
営業	受注伝票	受注伝票（過去10年分）	営業部	営業部	書類				2	2	2	2		2023/4/1	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 リスク小
営業	受注契約書	受注契約書原本（過去10年分）	営業部	営業部	書類				2	3	2	3		2023/4/1	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	3 リスク小
															3:通常の状態で脅威が発生する	2:部分的に対策を実施している		可能性：	

利用方法　台帳記入例　重要度定義　情報資産管理台帳　脅威の状況　対策状況チェック　診断結果

図６　リスク値まで決定した資産管理台帳記入例
　引用元：中小企業の情報セキュリティ対策ガイドライン第 3.1 版を基に作成

情報セキュリティ管理を成功に導くためには、経営層と従業員が共にセキュリティの重要性を理解し、「自分事」と認識して積極的に関与することが大切です。
また、管理においては各情報資産にはどのような情報が含まれており、資産の形態からどういった脅威が存在し、それらの脅威の発生頻度を考慮の上、脅威からいかに守るかを整理することが重要となります。

情報資産の管理に必要な手順からもわかる通り、情報セキュリティにおいては、社員一人一人の協力が必要となります。そのためには、経営層がリーダーシップを発揮し、組織的として社員一人一人が「自分事」という認識を持ち、自ら積極的に行動す

る風土を形成することが重要となります。その際に重要となる教育において、本資料で紹介した各種参考先、ノウハウを是非ご活用いただけますと幸いです。

４．関連文書

今回の記事でご紹介した情報のリンク先を以下に記載しています。
ぜひ、理解を深めたい、次のステップに進みたいと思った際の参考にしてください。

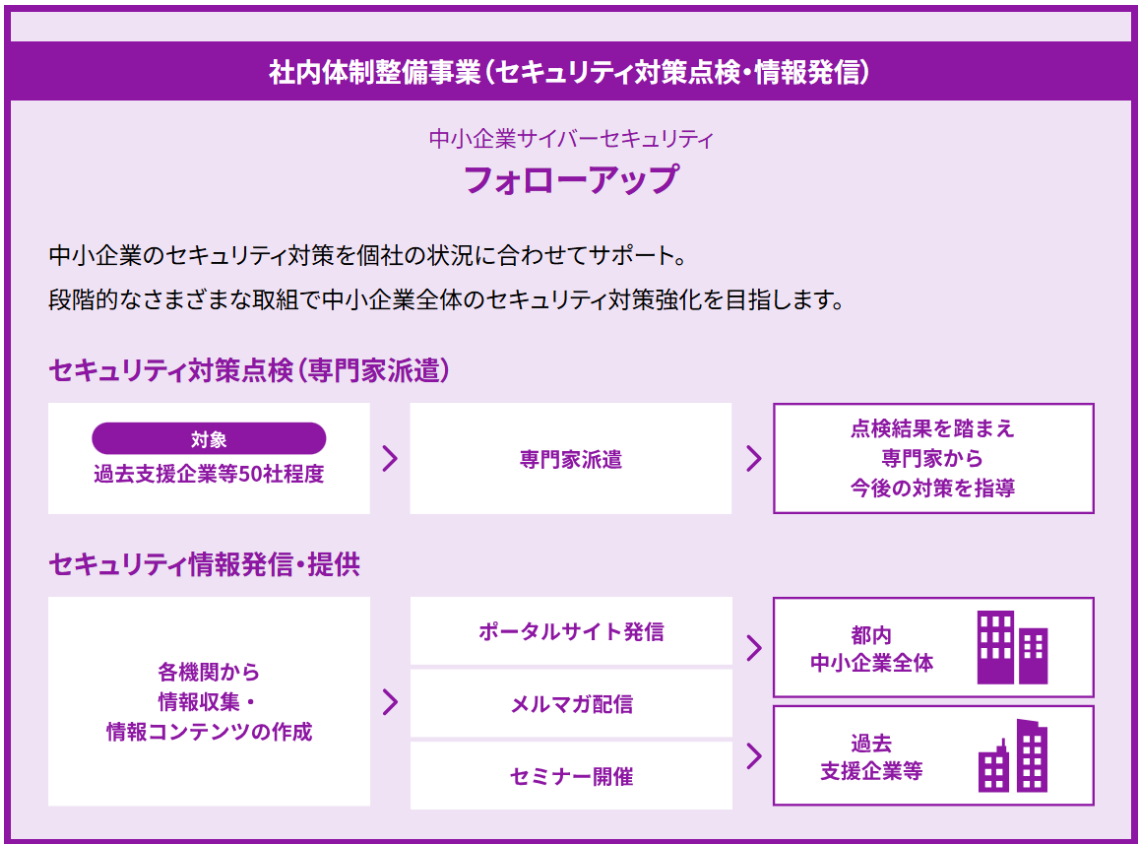
1. 情報セキュリティ１０大脅威 2025（IPA）
2. 中小企業の情報セキュリティ対策ガイドライン（IPA）
3. サイバーセキュリティ経営ガイドライン Ver3.0（IPA）
4. 講習能力養成セミナー（IPA）
5. 5 分でできる！情報セキュリティポイント学習（IPA）
6. 映像で知る情報セキュリティ（IPA）
7. 職場の安全サイト（厚生労働省）

配信予定日：2026 年 2 月 13 日(金) 14:00 頃
カテゴリ：参加者の声
タグ：＃実用編
過去記事焼き直し：しない（新規記事です）
過去記事：https://cybersecurity-taisaku.metro.tokyo.lg.jp/questionnaire/r7tenken3/

参加者の声（令和 7 年度セキュリティ対策点検 3 回コース）

目次

１．事業概要



当事業は都内中小企業がセキュリティ対策の継続的な実践や、定期的な見直しが出来るようサポートする事業です。「セキュリティ対策点検(専門家派遣)」と、「セキュリティ情報発信・提供」の 2 つの支援を実施いたしました。
支援内容詳細については、下記をご確認ください。

フォローアップ事業 TOP
https://cybersecurity-taisaku.metro.tokyo.lg.jp/follow-up/
記事「ライトな支援あります！セキュリティ対策点検」
https://cybersecurity-taisaku.metro.tokyo.lg.jp/know_more/cyber-taisakutiken5/

セキュリティ対策点検(専門家派遣)は、ASM、プラットフォーム脆弱性診断、約 50 項目のヒアリングシートを用いて専門家がお伺いしてセキュリティ対策状況の棚卸しや今後の取り組みをアドバイスします。
専門家の派遣回数 1 回コースと 3 回コースがあります。今回は令和 7 年度の事業においてセキュリティ対策点検 3 回コースを受けていただいた企業様 2 社にヒアリングした内容を紹介させていただきます。

２．ヒアリングより（セキュリティ対策点検３回コース）
C 社（キャリア社員の採用により体制を強化、先んじて業界ガイドラインに対応）

セキュリティ対策状況：
金融・IT 分野のキャリア社員を採用し情報セキュリティ体制を強化。メンバーの知見を活かし、業界ガイドライン対応を計画的かつ早期に実現している。

参加の背景：
対策は進めているものの、情報セキュリティ分野のプロにより、自社対策状況を評価し、課題の棚卸をしたく参加した。

参加しての変化：
ASM の実施により、体制強化以前の一人情シス時代の IT 資産が発見された。ヒアリングだけでなく、技術的な診断も重要だと認識しました。

今後実施していきたい対策：
インシデント対応の備えとして、経営層と年 1 回インシデントシナリオの読み合わせをしていますが、今後はより難易度の高いインシデント対応演習を行いたい。

D 社（お客様情報を預かり事業を行うため、セキュリティ対策は最重要事項）
セキュリティ対策状況：

金融のお客様から調査業務を請け負っており、セキュリティ対策は最重要事項として取り組んでいる。これまでにルールの整備を行ってきた。

参加の背景：
システム関連の対策状況に不安があり、技術的な診断（プラットフォーム脆弱性診断、ASM）や専門家に相談できる支援を受けたかったため、事業に参加した。

参加しての変化：
システム関連については、認証やアクセス権限の設定等、課題を具体的に示してもらえたので良かった。ルール関連についてはインシデント対応に課題があると感じた。

今後実施していきたい対策：
システム関連の課題は、数年後に予定している基幹システム更改と併せて解決していく。インシデント対応は東京都事業等をうまく活用して進めていきたい。

個社の様々な事情に配慮し企業名は伏せさせていただきました。皆様の情報セキュリティ対策のお役に立てれば幸いです。
次回はインシデント対応強化の CSIRT コースを受けていただいた企業様の声を掲載したいと思います。

配信予定日：2026 年 2 月 13 日(金) 14:00 頃
カテゴリ：基礎から学ぶ！セキュリティ
タグ：＃初級編＃実用編
過去記事焼き直し：しない（新規記事です）
記事 URL（新設します）：https://cybersecurity-taisaku.metro.tokyo.lg.jp/basics/imakikitai5/

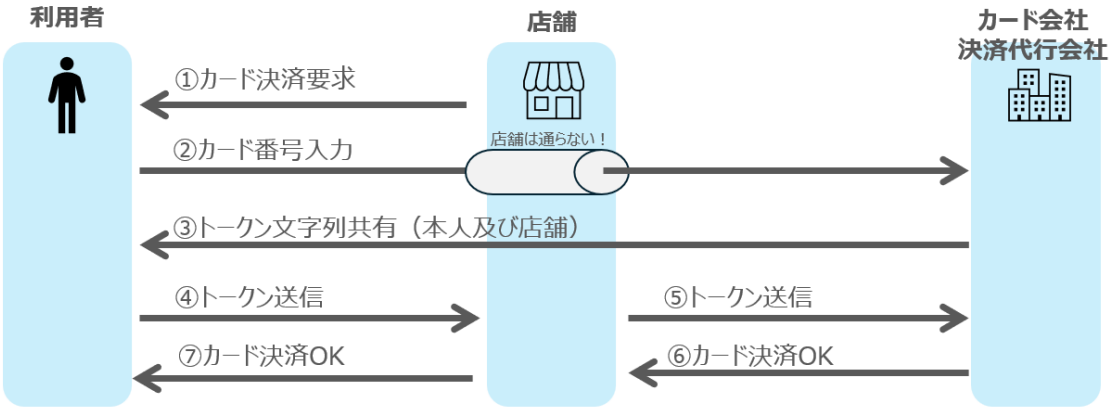
いまさら聞けない！組織や社会による対策

目次

サイバー攻撃の被害報道を見かけるたびに恐怖や不安を感じる方もいると思いますが、皆様の会社以外の組織や社会により情報セキュリティ対策が行われるケースもあります。
今回は組織や社会により行われたセキュリティ対策を 3 つご紹介いたします。

※なお、本記事は分かりやすさを重視し、技術的な事項は大幅に要約して説明をいたします。技術的に正しい事項を理解する必要がある場合は、別途、専門書等でご確認をお願いいたします。

●「クレジットカード番号は漏えいしていません。」の理由
企業がサイバー攻撃を受けたニュースを見ると「なお、クレジットカード情報は漏えいしていません」という記載を目にすると思います。その理由は、企業にはクレジットカード番号ではなく、トークンという別の文字列を保存して本人確認をしているため、カード番号の漏洩が発生しづらいです。
図解すると以下です。クレジットカード番号の情報は、利用者とカード会社(決済代行会社)の間でやり取りされ、店舗に残るのはトークンのみとなります。



なお、すべてのカード決済がこの方式を採用しているわけではありません、心配な場合は店舗（企業）に確認しましょう。

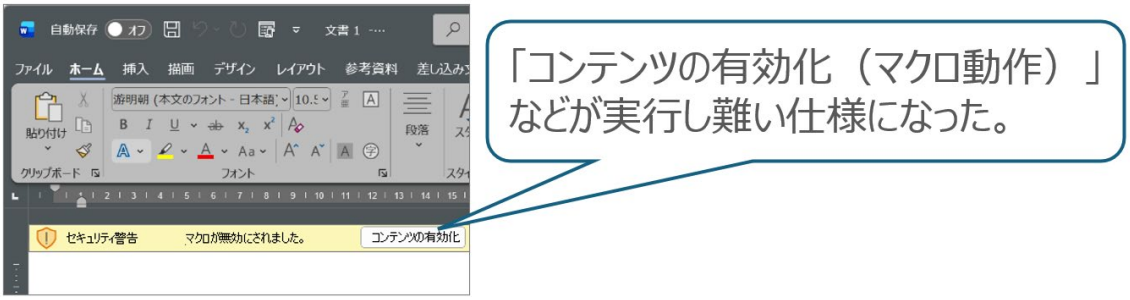
●Wi-Fi では安全性が無い通信方式は禁止されている

Wi-Fi の通信方式は年々改良が進み、適宜安全性に対する問題を確認しており、最新の Wi-Fi ルータでは WEP・WPA は禁止されている。
（業界団体は、WEP・WPA 機能を搭載した製品を認証しません。）

方式名	安全性	理由等
WEP (1999年頃～)	×	通信データを盗聴し（簡単にできる）、分析されると暗号化された通信の中身を見れてしまう
WPA (2003年頃～)	×	WEPの改良版、既に攻撃手法が確立
WPA２ (2004年頃～)	○	パスワード攻撃（辞書攻撃等）に弱いので、パスワードは長く更新を推奨
WPA３ (2018年頃～)	◎	パスワード攻撃にも強い

●Emotet の企業努力による排除

2020 年や 2022 年に大流行した「Emotet」というウイルスは、メールに添付されているオフィスファイルのマクロ（作業を自動処理する等ができるプログラム）を悪用して感染していました。
対策として、Microsoft 社が 2022 年以降に「インターネットから取得した Office ファイルのマクロを、デフォルトでブロック」したことにより、大幅に被害が減りました。



しかし上記の仕様を回避するため「ドキュメントを閲覧するのに特定の操作が必要」というような主旨の内容のメッセージが表示され、マクロを実行させようとする手口もあるようです。

参考：IPA「Emotet（エモテット）関連情報」

配信予定日：2026 年 2 月 13 日(金) 14:00 頃
カテゴリ：3 分でわかる!用語解説
タグ：＃初級編＃用語編＃知識編
過去記事焼き直し：しない（新規記事です）
記事 URL（新設します）：https://cybersecurity-taisaku.metro.tokyo.lg.jp/glossary/yogokaisetu24/

「ソーシャルエンジニアリング」

目次

サイバーセキュリティの基本を理解するためには、いくつか重要なセキュリティ用語を知っておくことが必要です。
これらの言葉や概念を正確に理解することで、企業が直面するリスクを最小限に抑え、適切な対策を講じることができます。
本記事では、中小企業が特に知っておくべきセキュリティ用語について解説しています。

今回のテーマは「ソーシャルエンジニアリング」です。

●ソーシャルエンジニアリングとは
ソーシャルエンジニアリングとは、技術的な手法ではなく、人の心理的な隙や行動のミスにつけ込み、ID やパスワードなどの重要な機密情報を盗み出したり、不正な操作をさせたりする詐欺的・心理的操作的な攻撃手法です。

●ソーシャルエンジニアリングの手口
ソーシャルエンジニアリングには以下の手口があります。
1. なりすまし
   IT 担当者や上司、取引先などを装って電話やメールで情報を聞き出す（フィッシング、ビッシング（電話を利用）など)。
2. 盗み見（ショルダーハッキング）
   パスワード入力画面をのぞき見する。
3. ゴミ箱漁り（トラッシング）
   捨てられた書類から機密情報を回収する。

4. 無意識の操作誘導
　偽のウェブサイトに誘導し、ID・パスワードを入力させる。

●ソーシャルエンジニアリングが増える？
ソーシャルエンジニアリングは、IT システムから見ると正規のユーザの操作に見えます。

・なりすましされた操作
・正規のユーザ操作を背中越しに盗み見
・正規のユーザが印刷した書類をゴミ箱漁り
・フィッシングメール等で偽のログイン用ウェブサイトに誘導し正規のユーザの ID・パスワードを盗む。

そのため、ソーシャルエンジニアリングは技術的な防御が難しく、標的型攻撃などで利用されます。近年は様々な情報セキュリティ対策システムの導入が行われているため、ソーシャルエンジニアリングが増える事は十分に考えられます。引き続き注意をしていきましょう。

配信予定日：2026 年 2 月 20 日(金) 14:00 頃
カテゴリ：基礎から学ぶ！セキュリティ
タグ：＃知識編　＃実用編
過去記事焼き直し：しない（新規記事です）
過去記事：https://cybersecurity-taisaku.metro.tokyo.lg.jp/basics/kisokaramanabu22/

2026 年は「AI の利用をめぐるサイバーリスク」にも注意！

目次

独立行政法人情報処理推進機構（IPA）が「情報セキュリティ 10 大脅威 2026」を発表しました。「組織」向けの脅威として「AI の利用をめぐるサイバーリスク」が 3 位にランクインし、毎年決定している 10 大脅威として初選出されました。

情報セキュリティ 10 大脅威 2026[組織]

順位	「組織」向け脅威	初選出年	10 大脅威での取り扱い（2016 年以降）
1	ランサム攻撃による被害	2016 年	11 年連続 11 回目
2	サプライチェーンや委託先を狙った攻撃	2019 年	8 年連続 8 回目
3	AI の利用をめぐるサイバーリスク	2026 年	初選出
4	システムの脆弱性を悪用した攻撃	2016 年	6 年連続 9 回目
5	機密情報を狙った標的型攻撃	2016 年	11 年連続 11 回目
6	地政学的リスクに起因するサイバー攻撃（情報戦を含む）	2025 年	2 年連続 2 回目
7	内部不正による情報漏えい等	2016 年	11 年連続 11 回目
8	リモートワーク等の環境や仕組みを狙った攻撃	2021 年	6 年連続 6 回目
9	DDoS 攻撃（分散型サービス妨害攻撃）	2016 年	2 年連続 7 回目
10	ビジネスメール詐欺	2018 年	9 年連続 9 回目

<出典>

IPA「情報セキュリティ 10 大脅威 2026」
https://www.ipa.go.jp/security/10threats/index.html
詳しい解説は 2026 年 2 月下旬以降に順次公開予定

今回は AI に関連したサイバーリスクについて 2 点紹介したいと思います。

１．生成 AI の利用による情報漏えいリスク

発生が多いと想定されるリスクは、生成 AI の利用による情報漏えいリスクです。生成 AI に入力した情報は、社外システムにより学習・ログ保存・分析される可能性があります。

[漏えいの例①]
・顧客情報を貼り付けて要約させる
・未公開の提案書、設計書を投入
・プログラムのソースコードを丸ごと入力

上記は機密情報を直接入力する例ですが、以下のような直接入力ではないものの機密情報を推論できるケースもあります。

[漏えいの例②]
・社内構成を断片的に質問
・業務内容を連続質問

１つ１つの質問ではどの企業か特定できずとも、複数の質問をつなぎ合わせると、どの企業か特定できる可能性があります。「これぐらいならば聞いても大丈夫だろう」が積み重なると情報漏えいする事になります。

このようなリスクを防ぐには、「生成 AI への入力＝社外のシステムへの情報の入力（漏えいリスク）」という認識を持つ事と、「学習機能を OFF にする等、漏えいリスク対策を行って生成 AI を利用する」事が必要です。

２．生成 AI の悪用によるサイバー攻撃巧妙化のリスク

2025 年末から各企業の社長や役員を騙る不審なメールが多数確認されています。

[不審なメールの例]

上記は一例であり、様々な内容が確認されています。短期間に大量に様々な内容のメールが送信されている事から、生成 AI の悪用が想定されます。
本件については東京都のセキュリティセミナー第 4 回で詳しく解説していますので、是非アーカイブ動画をご覧ください。

アーカイブ動画掲載先
https://cybersecurity-taisaku.metro.tokyo.lg.jp/seminar/
※2026 年 2 月 20 日時点、メルマガ登録者限定公開となっております。下記よりメールマガジンの登録をお願いいたします。
https://cybersecurity-taisaku.metro.tokyo.lg.jp/mail-magazine/

今回は AI に関連したサイバーリスクを 2 点紹介しましたが、あくまで一部のリスクとなります。他のリスクとしては例えば誤情報（ハルシネーション）や著作権・法的リスクがあります。今後も最新情報を調べるようにしましょう。

配信予定日：2026 年 2 月 20 日(金) 14:00 頃
カテゴリ：参加者の声
タグ：＃実用編
過去記事焼き直し：しない（新規記事です）
過去記事：https://cybersecurity-taisaku.metro.tokyo.lg.jp/questionnaire/r7incidentcsirt/

参加者の声（令和 7 年度インシデント対応強化 CSIRT 構築コース）

目次

１．事業概要

当事業では、攻撃が発生した際に迅速に検知し、的確な対応を行うことで、サプライチェーンへの影響を最小限に抑えるためのセキュリティインシデント対応力の強化をサポートします。「CSIRT 構築コース」と、「IT-BCP 策定コース」の 2 つの支援を実施いたしました。

支援実施の流れ(CSIRT 構築コース)

支援内容詳細については、下記をご確認ください。
インシデント対応強化事業 TOP
https://incident-taiou.metro.tokyo.lg.jp/
記事「意味あるの？インシデント対応強化の効果」
https://cybersecurity-taisaku.metro.tokyo.lg.jp/know_more/cyber-taisakutiken4/

CSIRT 構築コースでは、インシデントが発生した場合に備えて、準備から初動対応までの一連の対応を行う組織（機能）を構築します。今回は令和 7 年度の事業において CSIRT 構築コースを受けていただいた企業様 3 社にヒアリングした内容を紹介させていただきます。

２．ヒアリングより（インシデント対応強化 CSIRT 構築コース）

E 社（情報セキュリティ対策を事業課題と捉え積極的に取り組み）

セキュリティ対策状況：
取引先の要請、経営層の意識の高さ、過去のインシデント事案を受け、ポリシー策定やセキュリティ対策システム導入を積極的に実施し、同業他社と比較して対策が進んでいる状況。

参加の背景：
昨今のランサムウェア被害を見て、自社が適切なインシデント対応をできるか不安になっていた。具体的な対策を進めるため東京都事業に参加することとした。

参加しての変化：
「インシデントは全社で対応する事項」という認識ができた。加えてバックアップやログ管理等、情報セキュリティ対策の課題が明確になった。

今後実施していきたい対策：
システム関連の対応強化（バックアップ・リストアテスト、ログの取得・分析・検知の仕組み強化、ゼロトラストソリューションの導入）、経済産業省等情報セキュリティ関連の認証への対応。

F 社（経営層の意識が高く、情報セキュリティ対策を推進）

セキュリティ対策状況：
経営層の意識が高く、情報セキュリティ対策を推進している。過去に基本対策事業に参加して EDR の導入及びポリシー策定を進めてきた。

参加の背景：

昨今の社会情勢を受けサイバーセキュリティ対策の必要性を感じているが、飲料業界であり情報セキュリティに詳しいものがいないため、プロによる支援が欲しいため参加を申し込んだ。

参加しての変化：
ランサムウェア対策のドキュメントを作成し様々な考慮が必要と感じた。演習では証拠保全という考え方があることを認識した。

今後実施していきたい対策：
現行バックアップシステムは災害対策を目的としており、ランサムウェア対策ができる方式に切り替え予定。IT-BCP に関するドキュメントの見直し。

G 社（クラウドサービス事業者として信頼性を示すため情報セキュリティ対策を強化）

セキュリティ対策状況：
お客様の課題解決に資するクラウドサービス開発を手掛ける。信頼性を示すため情報セキュリティ対策は事業の優先事項と位置づけ、ISMS 認証を取得。

参加の背景：
独力で ISMS 認証取得や各種システム導入を進めてきたが、インシデント発生時に適切な対応ができるか不安があったため、令和 7 年度インシデント対応強化に参加し、外部専門家のアドバイスも受け解決を図ることとした。

参加しての変化：
演習でインシデント発生を体験することで、メンバーの社内システムの理解度合いや、リスク対処の考え方に違いがあることが分かった。インシデント対応ルールの習熟がより求められると感じた。

今後実施していきたい対策：
システム運用面の適正化（多要素認証の設定、管理者権限の適正運用、バックアップ・復旧手順の作成)、インシデント対応習熟のため演習の定期的な実施。

個社の様々な事情に配慮し企業名は伏せさせていただきました。皆様の情報セキュリティ対策のお役に立てれば幸いです。

次回はインシデント対応強化の IT-BCP 策定コースを受けていただいた企業様の声を掲載したいと思います。

配信予定日：2026 年 2 月 27 日(金) 14:00 頃
カテゴリ：もっと知りたい！セキュリティ
タグ：＃知識編　＃中小企業サイバーセキュリティ対策事業の知見
過去記事焼き直し：しない（新規記事です）
記事 URL：https://cybersecurity-taisaku.metro.tokyo.lg.jp/know_more/cyber-taisakutiken7/

セキュリティセミナーで分かった！中小企業の注目コンテンツ

目次

東京都中小企業サイバーセキュリティフォローアップ事業では、メルマガに登録いただいている方を対象に全４回のオンラインセキュリティセミナーを開催いたしました。
今回は、各回で取得したアンケート結果から、各回でどのコンテンツが人気だったのかを解説していきたいと思います。

■セキュリティセミナーの開催日時・タイトル

開催日	開催回	タイトル
2025/12/10	第１回	いまさら聞けない、サイバー攻撃対策手段 ～基本的な情報セキュリティ対策を紹介～
2025/12/23	第２回	2025 年のサイバーセキュリティ事案を振り返る ～最新の被害事例を紹介～
2026/1/15	第３回	2026 年をいい年に、各社優良事例から今後の取り組みを導く ～各社の情報セキュリティ対策事例を紹介～
2026/1/27	第４回	生成 AI、地政学リスク、量子暗号、今後のセキュリティリスクを考える ～最新の脅威や対策を紹介～

開催日はリアルタイムでの配信日です、後日アーカイブを配信しております。
※アーカイブは 2026/2/27 時点、メルマガ会員限定公開になっております。
メルマガ登録　※令和 7 年度の最終配信は 2026/3/6 14:00 を予定しております。
アーカイブ掲載先　※メルマガに記載の ID/PW 認証が必要です。

全ての開催回において 13:00-14:30 に配信を行い、最後にアンケートを取得させていただきました。セミナーアンケートでは満足度を問うことが多いのですが、当事業ではセミナー内容の具体的に何が印象に残ったか聞いています。

１．第１回の人気コンテンツ
第１回はウイルス対策ソフト（EPP）など、基本的な情報セキュリティ対策を紹介しました。最も人気があったコンテンツは

「EPP と EDR の違い」

でした。確かにこの内容、企業様からよく聞かれます。
本件はセミナー以外にも記事にしておりますので是非ご覧ください。
EPP と EDR の違いとは？セキュリティ対策の役割分担

２．第２回の人気コンテンツ
第２回は 2025 年に報道されたサイバー攻撃被害事例を紹介し、攻撃者の手口についても解説しました。最も人気があったコンテンツは

「アスクル株式会社が公開したサイバー攻撃の詳細な手口」

でした。同社はサイバー攻撃被害を確認した 2025 年 10 月 19 日の第 1 報から、本記事の配信日 2026 年 2 月 27 日までに原因や復旧状況等を第 18 報まで公開しています。セミナーではその中でも攻撃の詳細な手口を解説させていただきました。
同社の情報公開は攻撃の手口以外にも、復旧の優先度等参考になる情報があります。
アスクル株式会社コーポレートサイト
※ニュースリリースを参照

３．第３回の人気コンテンツ
第３回は各企業が取り組んでいる情報セキュリティ対策の優良事例を多数紹介しました。最も人気があったコンテンツは

「情報セキュリティ対策テクニック全般」

でした。本セミナーは大きく４つの構成で出来ており
・IT の利用を制御することでの情報セキュリティ対策
・業務フローの作成は情報セキュリティ対策に有効

・中小企業はどこまで情報セキュリティ対策を実施すべきか
・情報セキュリティ対策テクニック（組織・人的・物理・技術）
４点目はさらに１１項目ほどの小項目でテクニックを紹介していますが、全般的に評価をいただいた結果となりました。
しかしながら、この第３回のセミナーは全４回の中で最もリアルタイム／アーカイブともに視聴数が少ない状況です。東京都事業等で様々な企業様に訪問して教えていただいたノウハウを多数紹介しており、他にはあまりないコンテンツと思います。セミナーのアーカイブを是非ご覧ください。

４．第４回の人気コンテンツ
第４回はセキュリティ分野における生成 AI や量子暗号等、最新技術から数年先の技術まで幅広く紹介しました。
最も人気があったコンテンツは

「2025 年末～2026 年始にかけて実在の社長を装った LINE メッセージによる送金指示による特殊詐欺(ビジネスメール詐欺)が発生」

でした。本件は生成 AI 悪用により行われている疑いがあり、どのように悪用されているか解説しています。また、特殊詐欺とサイバー攻撃が紐づいた象徴的な事例とも言えます。特殊詐欺については東京都や警視庁・警察庁のウェブサイトで様々な情報を発信していますので是非ご覧ください。
東京都 特殊詐欺被害防止 特設サイト
警視庁 特殊詐欺
警察庁 SOS47 特殊詐欺対策ページ

配信予定日：2026 年 2 月 27 日(金) 14:00 頃
カテゴリ：参加者の声
タグ：＃実用編
過去記事焼き直し：しない（新規記事です）
記事 URL：https://cybersecurity-taisaku.metro.tokyo.lg.jp/questionnaire/r7incidentitbcp/

参加者の声（令和 7 年度インシデント対応強化 IT-BCP 策定コース）

目次

１．事業概要

当事業では、攻撃が発生した際に迅速に検知し、的確な対応を行うことで、サプライチェーンへの影響を最小限に抑えるためのセキュリティインシデント対応力の強化をサポートします。「CSIRT 構築コース」と、「IT-BCP 策定コース」の 2 つの支援を実施いたしました。

支援実施の流れ(IT-BCP 策定コース)

支援内容詳細については、下記をご確認ください。
インシデント対応強化事業 TOP
https://incident-taiou.metro.tokyo.lg.jp/
記事「意味あるの？インシデント対応強化の効果」
https://cybersecurity-taisaku.metro.tokyo.lg.jp/know_more/cyber-taisakutiken4/

IT-BCP 策定コースでは、インシデントが発生した場合に備えて、準備から初動対応までの一連の対応ルール（主にシステムや業務の復旧に向けた行動）を策定します。今回は令和 7 年度の事業において IT-BCP 策定コースを受けていただいた企業様 3 社にヒアリングした内容を紹介させていただきます。

２．ヒアリングより（インシデント対応強化 IT-BCP 策定コース）

E 社（情報セキュリティ対策を事業課題と捉え積極的に取り組み）

セキュリティ対策状況：
取引先の要請、経営層の意識の高さ、過去のインシデント事案を受け、ポリシー策定やセキュリティ対策システム導入を積極的に実施し、同業他社と比較して対策が進んでいる状況。

参加の背景：
昨今のランサムウェア被害を見て、自社が適切なインシデント対応をできるか不安になっていた。具体的な対策を進めるため東京都事業に参加することとした。

参加しての変化：
「インシデントは全社で対応する事項」という認識ができた。加えてバックアップやログ管理等、情報セキュリティ対策の課題が明確になった。

今後実施していきたい対策：
システム関連の対応強化（バックアップ・リストアテスト、ログの取得・分析・検知の仕組み強化、ゼロトラストソリューションの導入）、経済産業省等情報セキュリティ関連の認証への対応。

F 社（経営層の意識が高く、情報セキュリティ対策を推進）

セキュリティ対策状況：
経営層の意識が高く、情報セキュリティ対策を推進している。過去に基本対策事業に参加して EDR の導入及びポリシー策定を進めてきた。

参加の背景：

昨今の社会情勢を受けサイバーセキュリティ対策の必要性を感じているが、飲料業界であり情報セキュリティに詳しいものがいないため、プロによる支援が欲しいため参加を申し込んだ。

参加しての変化：
ランサムウェア対策のドキュメントを作成し様々な考慮が必要と感じた。演習では証拠保全という考え方があることを認識した。

今後実施していきたい対策：
現行バックアップシステムは災害対策を目的としており、ランサムウェア対策ができる方式に切り替え予定。IT-BCP に関するドキュメントの見直し。

G 社（クラウドサービス事業者として信頼性を示すため情報セキュリティ対策を強化）

セキュリティ対策状況：
お客様の課題解決に資するクラウドサービス開発を手掛ける。信頼性を示すため情報セキュリティ対策は事業の優先事項と位置づけ、ISMS 認証を取得。

参加の背景：
独力で ISMS 認証取得や各種システム導入を進めてきたが、インシデント発生時に適切な対応ができるか不安があったため、令和 7 年度インシデント対応強化に参加し、外部専門家のアドバイスも受け解決を図ることとした。

参加しての変化：
演習でインシデント発生を体験することで、メンバーの社内システムの理解度合いや、リスク対処の考え方に違いがあることが分かった。インシデント対応ルールの習熟がより求められると感じた。

今後実施していきたい対策：
システム運用面の適正化（多要素認証の設定、管理者権限の適正運用、バックアップ・復旧手順の作成)、インシデント対応習熟のため演習の定期的な実施。

個社の様々な事情に配慮し企業名は伏せさせていただきました。皆様の情報セキュリティ対策のお役に立てれば幸いです。

今回で参加企業様の声の特集は終了となります。過去記事は以下になります、まだご覧になられてない方は是非ご一読ください。

参加者の声（令和７年度セキュリティ対策点検１回コース）

参加者の声（令和７年度セキュリティ対策点検３回コース）

参加者の声（令和７年度インシデント対応強化 CSIRT 構築コース）