TOP SECRET

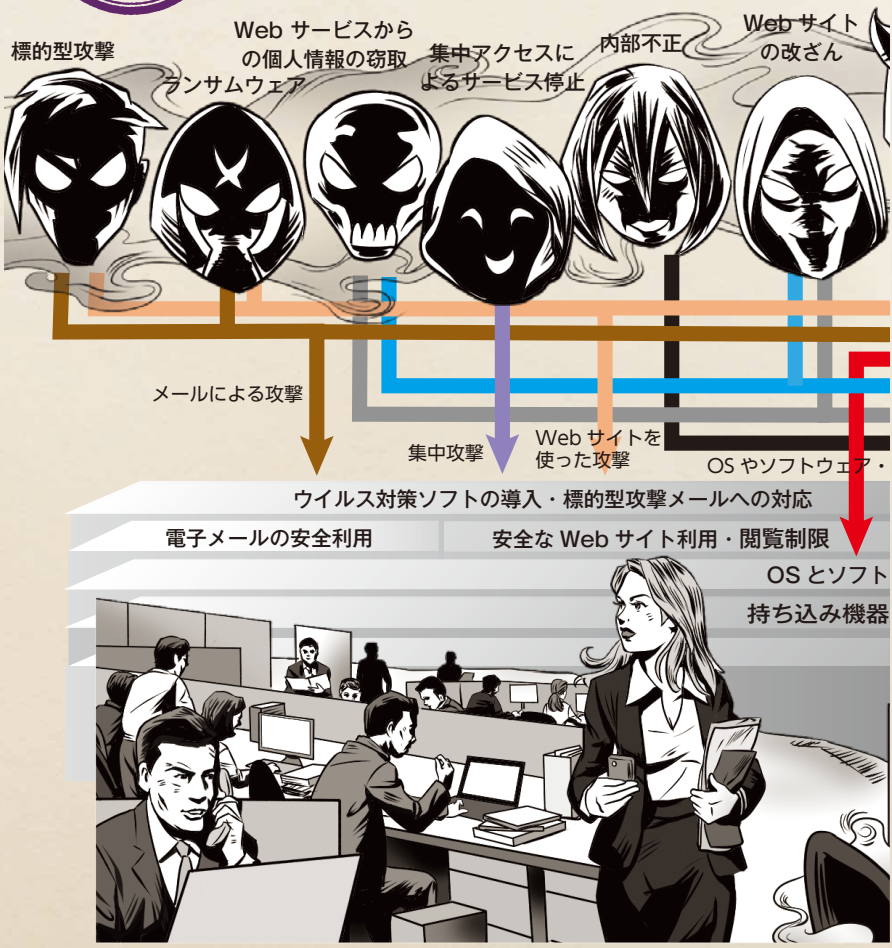
MISSION 2

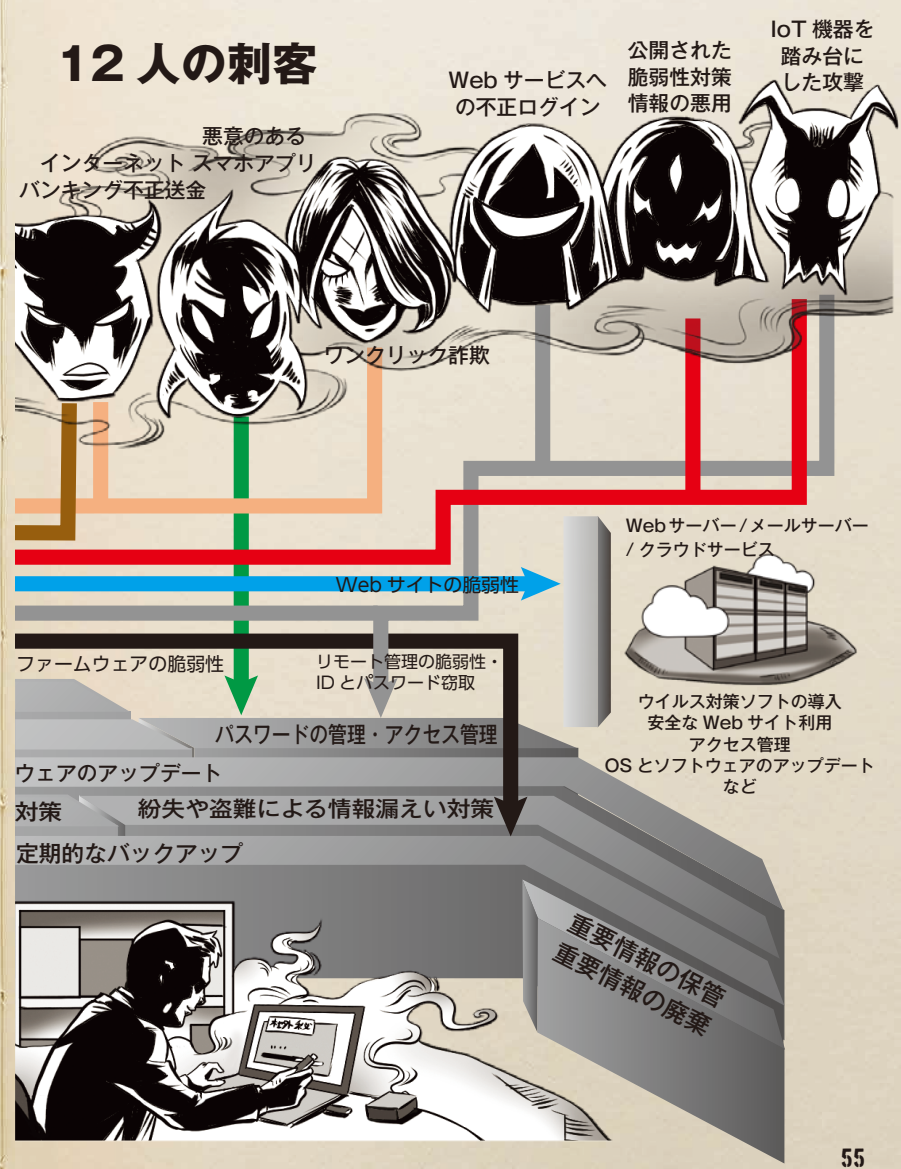
すぐやろう！ 対サイバー攻撃アクション

今やろう！ 5+2の備えと社内使用パソコンへの対策

MISSION 2-1

サイバー攻撃に対して何ができるか




12 人の刺客
悪意のある
インターネット バンキング不正送金
スマホアプリ
Web サービスへ
の不正ログイン
公開された
脆弱性対策
情報の悪用
IoT 機器を
踏み台に
した攻撃
ワンクリック詐欺
Web サーバー / メールサーバー
/ クラウドサービス
Web サイトの脆弱性
ファームウェアの脆弱性
リモート管理の脆弱性・
ID とパスワード窃取
ウイルス対策ソフトの導入
安全な Web サイト利用
アクセス管理
OS とソフトウェアのアップデート
など
パスワードの管理・アクセス管理
ウェアのアップデート
対策
紛失や盗難による情報漏えい対策
定期的なバックアップ
重要情報の保管
重要情報の廃棄

今やろう！ 5+2の備えと社内使用パソコンへの対策

OSとソフトウェアのアップデート

■パソコンのOSは可能な限り自動更新にする
■インストールしているソフトウェアは、常に最新の状態にする

<OSのアップデート>

●パソコンのOSは可能な限り最新の状態を保つようにする。自動更新が利用できる場合は、自動更新機能を有効にする。
●サポートが終了した古いOSは使わない※。
●業務に利用するスマートフォンのOSは機種ごとの情報を常に調べて手動で更新する。

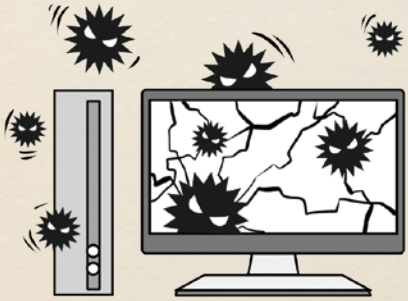
※ Windows7のサポートは2020年1月14日に終了。Windows8.1については2023年1月10日に終了予定。可能な限り早く最新のWindows環境への移行をお勧めします。やむを得ず継続利用する場合には、ベンダーサポートに相談するなどし、適切な対応を図ってください

<ソフトウェアのアップデート>

●全てのソフトウェアを最新版にする。
●自動更新機能がある場合は必ず設定する。
●自動更新が設定できないものについては、定期的に脆弱性情報をチェックする。

セキュリティ上の脆弱性が攻撃対象に！

OSは、日々新たなセキュリティ上の脆弱性が発見されています。サイバー攻撃はこの脆弱性を利用してウイルスを潜入・繁殖・拡散させます。



また、OSだけでなく、Microsoft Office製品やAdobe Acrobat Readerなど、多くの人が使用している製品のセキュリティホールも攻撃の対象となっています。OSもソフトウェアも常に最新版にしておくことが大切です。

※ Adobe Flash Playerは2020年12月31日でサポートが終了しました。直ちにアンインストールすることが、メーカーから強く推奨されています

脆弱性情報はここから入手

JPCERT コーディネーションセンターが運営・提供している脆弱性に関するメーリングリストやJVN（脆弱性対策情報ポータルサイト）などから、自分が使っているソフトウェアに関する脆弱性情報を入手だ。

今やろう！ 5+2の備えと社内使用パソコンへの対策

MISSION 2-3 ウイルス対策ソフト・機器の導入

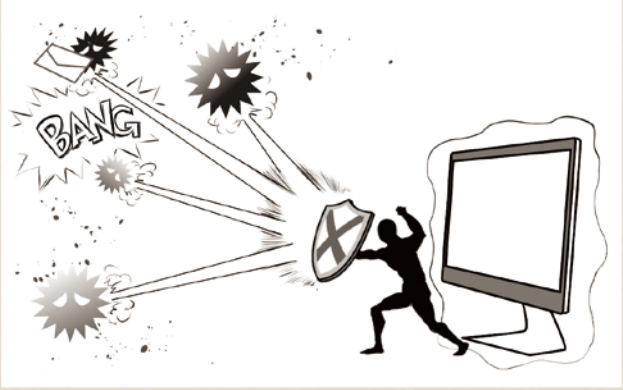
すぐやろう

■ウイルス対策ソフトウェア（セキュリティソフト）がインストールされているか、また最新バージョンになっているかを確認する

＜個別のパソコンに導入するタイプ＞

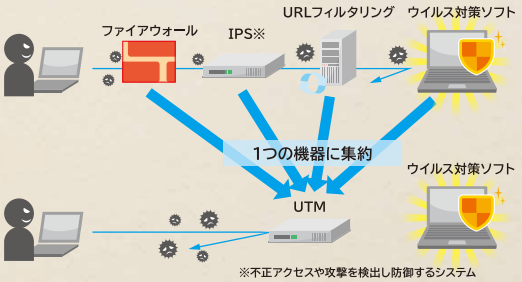
個別のパソコンに導入するウイルス対策ソフトウェアには自動的に更新する機能が付いています。最近のウイルス対策ソフトウェアは脆弱性スキャンやWeb脅威対策、URLフィルターなど多くのセキュリティ機能が付いています。

※ パソコンを購入した際に、ウイルス対策ソフトの試用版がインストールされている場合がありますが、一定期間を過ぎると、利用できなくなったり、更新できなくなったりするものがあります



<ネットワークの出入り口に設置するタイプ>

オフィスのネットワークとインターネット網との間の出入り口部分に、統合型セキュリティ機器（UTM）を導入することで、二重にセキュリティを強め外部への情報漏えいや被害拡大を防ぐことができます。UTMは複数のセキュリティ機能を1つのハードウェアに統合し、集中的に管理します。



ウイルス対策ソフトは必ず最新のものに

ウイルスは毎日たくさんの新種が登場している。そのために、ウイルス対策ソフトを新しいウイルスに対応できる状態に保つ必要がある。ウイルス対策ソフトには、ウイルスを発見して駆除するプログラムを自動的に更新する機能が付いている。この機能を利用するか、更新プログラムがないか毎日チェックするかのどちらかだ。メールの添付ファイル、ダウンロードしたファイル、USBメモリーやCD・DVDなどの外部記憶媒体に格納されたファイルも、必ずウイルスチェックを行ってから使うほうがよい。

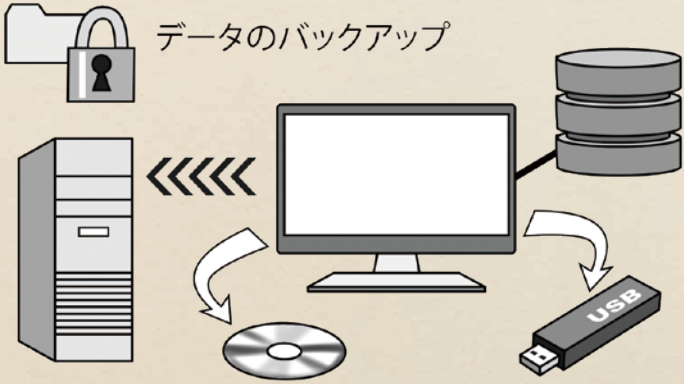
今やろう！ 5+2の備えと社内使用パソコンへの対策

定期的なバックアップ

■重要データは、定期的に別媒体へバックアップを取って保存する

<バックアップの方法>

●ハードディスク（HDD）やDVDなどの外部記憶媒体に保存。
●重要情報はネットワークと切り離して保存。
●保管方法を決めておく（保管場所や保管媒体など）。
●バックアップ媒体のセキュリティ対策も同時に実施。
●必要に応じて1つ前のデータも保存。



定期的バックアップの重要性

ビジネスで利用するデータは、削除誤りなどの人的ミスやハードウェア障害、ソフトウェア障害など多様な要因によって破損する危険があります。これらのリスクから業務データを守るためには、定期的なバックアップが不可欠です。

重要なデータのバックアップがあれば、万が一データが消失してしまっても、速やかにビジネスを復旧させることができます。

バックアップには、使っているPCが壊れたときのために重要なデータを外付けのHDDなどにバックアップする方法や、クラウドへバックアップする方法があります。クラウドの場合、保管するデータセンターの場所が会社から遠いところにあったり、複数のデータセンターで相互にバックアップしていたりと、社内で保管するより安心な場合もあります。

クラウドの活用に際しては、管理担当者の選定や利用範囲と権限の明確化、利用者が使うパスワードなどの認証機能を適切に設定・管理するなどの点に留意が必須です。

Windowsのバックアップ機能を活用だ！

定期的バックアップのために市販のバックアップソフトウェアを使う方法もあるが、Windowsには自動バックアップ機能が付いている。一度設定すれば指定したフォルダーを定期的にバックアップしてくれる。保管場所としてはネットワークから切り離すことができる外付けのハードディスクがお薦めだ。

今やろう！ 5+2の備えと社内使用パソコンへの対策

パスワードの管理

■パスワードを強化する
■ID・パスワードを盗まれないようにする

<パスワードの強化>

他人に推測されやすいパスワード（ニックネームや誕生日など）は使わない。

●長いパスワード（推奨は10桁以上）にする。

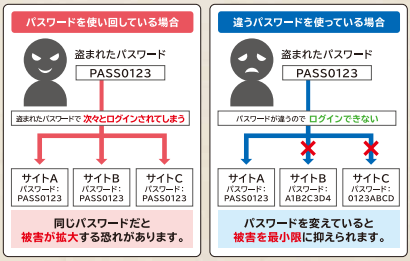
●推測しづらく自分が忘れないパスワードにする。

●他人の目に触れるような場所に、パスワードを残さない。

●いろいろなWebサービスで同じID・パスワードを使い回さない。

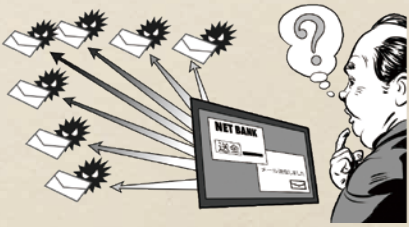
パスワードの使い回しは危険

パソコン本体はもちろん、メールやSNS、各種アプリや会員サイトなどのWebサービスを使うときに必要となるのがID（アカウント）とパスワード。1つのパスワードを使い回している場合、それが流出すると、ほかのサービスも乗っ取られてしまう可能性が高くなります。



対策を講じないと……

IDやパスワードを盗まれて不正にログインされることで、会社にも個人にもさまざまな被害が発生します。



- 自分が利用しているインターネットバンキングから知らない口座に振り込まれた
- ショッピングサイトで勝手に高額な買い物をされた
- 知らないうちに迷惑メールを大量に送信させられた

など、他人に迷惑をかけることになるケースもあります。

多要素認証でより安全に

通常はIDとパスワードを使って本人であることを確認するが、さらにもう1つ別のパスワードで認証する方法がさまざまなオンラインサービスで使われている。また複数の要素を使って認証する多要素認証も多く使われている（P43を参照）。

今やろう！ 5+2の備えと社内使用パソコンへの対策

アクセス管理

■データや社内ネットワークへのアクセスについて利用者の制限やIDの管理を行う
■職務や業務、役割によってもIT機器や情報に対してアクセスの管理・制限を行う

<ネットワークなどへのアクセス管理>

●社内のパソコンやIT機器、ネットワークなどへアクセスする場合、職務を実施するために必要な情報に限定したり利用者を制限したりする。
●職務の変更や人事異動があったら、利用者のアクセス権限を見直す。

<情報へのアクセス管理>

●会社の重要情報を機密性※1、完全性※2、可用性※3の観点から評価し、情報資産の重要度を仕分ける。
●情報ごとにアクセス権を設定する。
●アクセス権の設定ではID・パスワードの使い回しを禁止する。

※1 アクセスを許可された者だけが必要な情報にアクセスできること
※2 情報および処理方法が正確であること、かつ完全であること
※3 認可された利用者が必要なときに情報および関連する資産にアクセスできること

アクセス管理の例

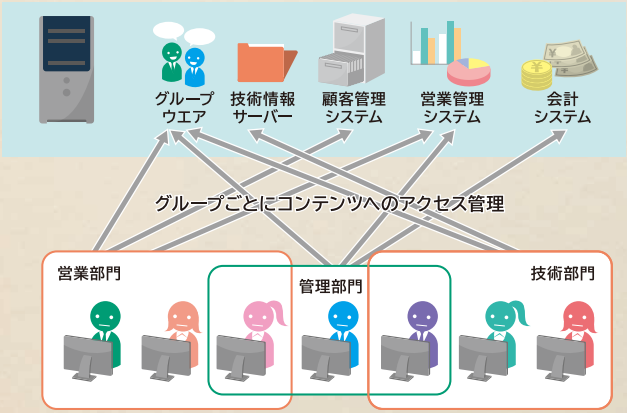
	極秘文書	機密文書	営業データ	技術データ
役　員	○	○	△	△
部　長	△	○	△	△
営業部門	×	×	○	×
技術部門	×	×	×	○

○は読み書き可
△は閲覧のみ可
×は閲覧・編集とも不可

何が防げるの？

例えば「社外秘」の情報はアクセスできる利用者も制限する必要があります。つまり、この情報を利用できるのは誰かを決め、それ以外の人は利用不可とするのがアクセス権の設定です。

ネットワーク上の共有フォルダーやWebページにアクセス権を設定すると、特定のユーザーだけが利用するので、重要なデータを保護できます。



無線LANのアクセスに注意だ

社内で無線LAN（Wi-Fi）を使う会社が飛躍的に増えている。しかし「簡単に接続できる」「社内の人しか使わないから」といった理由で、接続時のパスワードを設定していない企業も少なくない。無線LANが社内ネットワークに直結している場合、誰でも簡単に侵入できる可能性がある。無線LANには必ずパスワードを設定し、接続できる権限を持った人間と端末を決めておくべきだ。

今やろう！ 5+2の備えと社内使用パソコンへの対策

紛失や盗難による情報漏えい対策

■原則は情報の持ち出し禁止
■パソコンやUSBメモリーなどの記憶媒体やデータを外部に持ち出す場合、盗難・紛失などに備えて、パスワード設定や暗号化などの対策を実施する

<情報持ち出しの対策>

●パソコンや記憶媒体を持ち出す場合の規定を設ける。
●利用者の認証（ID・パスワード設定、USBキーやICカード認証、指紋認証など）を行う。
●保存されているデータに対して、重要度に応じてHDD暗号化、パスワード設定などの技術的対策を実施する。
●紛失情報が何かを正確に把握するため、持ち出し情報の一覧を作り、管理を行う。
●ノートパソコンまたはタブレット端末に保存するデータは最小限にする。
●電子媒体はケースに入れ、USBメモリーはタグ、ストラップ、鈴などを付ける。
●不要な場所に持ち出さない。
●携帯時には注意する。
・電車内では肌身離さず、網棚に置かない
・自動車内には保管しない
・他者からのぞき見されない状態で扱う

紛失・盗難対策の基本はパスワード

パソコンやモバイル端末などの情報が収められた機器は、起動の際にパスワードをかけたり、ファイルそのものにもパスワードを設定したりするなどの対策を事前に行っておくことで、盗難・紛失時に情報を簡単に見られないようにすることができます。

街なかのフリーWi-Fiに注意だ

公共施設をはじめ街なかには多くのAP（アクセスポイント）が設置されている。だが、APすべてが万全のセキュリティ対策を講じているとは限らない。中には利便性を追求し最低限の対策に留めるAPも存在し、使い方によっては通信内容を盗まれる可能性がある。

また必ずしも『暗号化＝安心』というわけではない。例えば「偽AP」だ。この場合、暗号化に関係なく通信内容が盗まれる。

便利なフリーWi-Fiだが利用する際、少なくとも次の点は確認だ。

- **接続するフリーWi-FiのAP名の確認**
- **接続後、ID・パスワード等の入力画面になった場合、URLが「https://」で始まっているか**
- **ブラウザーに鍵マークが表示されているか**

特にテレワーク等、機微な情報を扱う際は不特定のAPは避けるべきだ。

今やろう！ 5+2の備えと社内使用パソコンへの対策

テレワーク等での持ち出し・持ち込み機器対策

■テレワーク等で機器を社外に持ち出す際や私物機器類を会社に持ち込む場合には、セキュリティと使い方のルール（例）を設ける

＜使い方ルール＞

情報機器の種類	順守事項
パソコン ※自宅のパソコンで業務を行う場合も含む 	・データや情報を持ち出す場合は会社ルール（P66参照）に準拠する ・ウイルス対策ソフトおよびアプリケーションなどは会社指定のものを導入 ・情報セキュリティ事故の発生に備えて担当者への連絡体制を確認する ・作業開始前に端末のOSやソフトウェアが最新か確認 ・機密情報を送信する際には暗号化する ・テレワークなどで会社機器を社外に持ち出す場合、フリーWi-Fiなどには接続しない ・基本的に私物機器は社内に無断で持ち込まない ・私物機器は社内LANへの接続を禁止する ・家族や友人への会社機器の貸与を禁止する

スマートフォン タブレット端末 携帯電話など 	・会社で指定したアプリケーション以外は使わない ・社内パソコンに接続する前には必ずウイルス対策ソフトでチェックする ・ウイルス対策ソフトなどは会社指定のものを導入 ・業務情報と私的な情報を混在させない ・家族や友人への貸与を禁止する
USBメモリー 外付けHDD	・社内パソコンに接続する前には必ずウイルス対策ソフトでチェックする
共通	・個人のメールアドレスに業務用データを添付して送信しない ・社用メールアドレスで受信したメールを個人のアドレスに転送することを禁止する

私物端末による脅威とは

●感染した私物端末が不正プログラムなどで遠隔操作される。
●私物端末でデータを持ち出される。
●感染した私物端末から社内のネットワークに感染が広がる。
●感染した私物端末のテザリング機能を利用して外部への通信が行われ、情報が漏えいする。

持ち込み機器にもウイルス対策ソフトを

私物の機器は原則として持ち込み禁止にするのが安全だが、実際には私物端末を業務に利用するニーズも増えている。その場合は持ち込みを許可する端末に必ずウイルス対策ソフトをインストールする。ソフトによっては、USBメモリーなどを差し込んだら自動的にチェックを求める機能が付いているものもある。

今やろう！ 電子メールへの備え

電子メールの安全利用

- ■誤送信しないように宛先や内容、添付ファイルの確認をする
- ■原則としてファイルを添付しない
- ■万一必要な場合は、添付ファイルを暗号化する

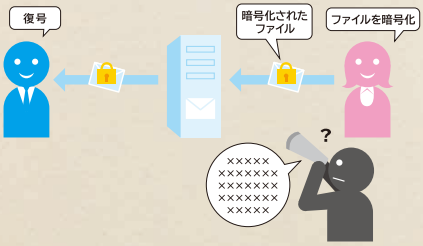
＜誤送信対策＞

- ●送信ボタンを押す前に、必ず宛先を再確認する。いったん送信トレイに保存するように設定すれば、送信前に宛先を再確認できる（メールソフトとバージョンによって異なります）。
- ●大量のアドレスへ同報メールを送るときなどはそれぞれの受信者にアドレスが分からないようにBCCを使う。

＜添付ファイルの暗号化＞

メールを安全に送受信するために添付ファイルを簡単に暗号化できます。

- ●アプリケーションソフトにある暗号化機能を利用する。
- ●圧縮・解凍ソフトの暗号化機能を利用する（パスワードを設定する）。



なお、パスワード付きZIPファイルなどをメール添付で送り、後からパスワードを別のメールで送ることは、「Emotetなどのマルウェアに悪用される」「受信者の作業負荷を高める」といった理由で、禁止する動きが広がっています。

＜電子メールのなりすまし対策＞

ビジネスツールとして広く普及する電子メール。しかし、近年は「なりすまし」や標的型攻撃も登場しています。その対策手段の1つが「送信ドメイン認証技術」の導入です。この中には、送信元のメールサーバーのIPアドレスを認証に用いる「SPF」と、暗号化技術を用いて認証する電子署名方式の「DKIM」の2方式があり、さらに両者の結果を利用する「DMARC」があります。

対策を講じないと…

送信設定間違いによる重要情報の漏えい事故や、同報メールの送信方法の誤りによるメールアドレスの漏えい事故につながる可能性があります。誤送信対策をする一方で、受信対策、すなわち迷惑メール対策もしっかり行いましょう。下記のサイトが参考になります。

● 迷惑メール相談センター
https://www.dekyo.or.jp/soudan/

添付ファイルはなるべく減らす！

電子メールを使ったサイバー攻撃の多くは、添付ファイルに仕込まれたウイルスや不正プログラムによるものだ。
だからビジネス上のやり取りでは添付ファイルを減らすことが、防御の第一歩だ。
ファイルを送るにはWeb上で提供されている無料転送サービスも使うことができる。
添付ファイルを減らすことは、メールサーバーや通信回線の負荷の軽減にもつながる。

今やろう！ 電子メールへの備え

標的型攻撃メールへの対応

■不審な電子メールは開かない
■標的型攻撃メールを見分ける

入り口対策	
ウイルスの侵入防御	□OSやアプリケーションの脆弱性の解消 □スパムメールのフィルタリング □従業員教育 ・不審なメールを開かない ・ウイルス対策ソフトを適切に導入

潜伏期間対策	
ウイルスの早期発見	□ウイルス対策ソフトによる各機器の感染チェック □不審な通信などの監視

出口対策	
外部への 情報漏えい防止	□統合型セキュリティ機器（UTM）によるデータ送信のチェック

巧妙な標的型攻撃メールの事例

これは、とある会社の社員に届いたメールです。その会社が加盟する健康保険組合からの「医療費通知のお知らせ」というメールだったので、添付されていた「医療費通知のお知らせ」というファイルを開きました。クリックした途端に不正プログラムが動きだし、遠隔操作ツールが実行されてしまいました。添付ファイルはワードのアイコンになっていましたが、拡張子は「doc」でも「docx」でもなく、「医療費通知のお知らせ.exe」という不正プログラムだったのです。

これは実際にあった事例です。同じように、取引先を偽装して、「請求明細」や「明細書」というタイトルの不正プログラムが送られてきた事例もあります。

※警察庁発表によると2019年には、確認された標的型攻撃メールは5300を超える

こんな添付ファイルに注意だ

- **件名に「緊急」など、ことさらに添付ファイルの開封を促すメール**
- **日ごろメールでやり取りすることのない種類のファイルが添付されているメール**
- **IDやパスワードなどの入力を要求する添付ファイルやURLが記載されたメール**

メールについての注意点はP24参照

今やろう！ 電子メールへの備え

迷惑メール発信への対応

すぐやろう

■ ウイルス対策ソフトで迷惑メールをブロック
■ 統合型セキュリティ機器（UTM）※で迷惑メールの送信をチェック

※ P58参照

最近ではスマートフォンなどへの迷惑メールが日常茶飯事となっているため、その危険性があまり言われなくなっていますが、迷惑メールはサイバー攻撃の予兆の1つであることを認識しましょう。

＜迷惑メールの発信は受け取り拒否につながる＞

迷惑メールと判断された送信元のIPアドレスを管理する「ブラックリスト」といわれるデータベースがあります。ウイルス対策ソフトの中には、このブラックリストを参照して、このリストに登録されたメールサーバーからのメールは受け取りを拒否する機能を持ったものもあります。もし、あなたの会社が迷惑メールを発信してブラックリストに登録され取引先で受け取り拒否されたら、事業に大きな支障が生じます。

＜万が一ブラックリストに登録されてしまったら＞

取引先で受け取り拒否されたら、拒否した理由が記されたメールが送られてきます。そこに参照したブラックリスト名とURLが記載されています。
ブラックリストを登録・管理している団体のWebサイトに行き、送信元IPアドレスを入力し、リストから削除するための手順を確認してください。ただし、ブラックリストを管理している団体のほとんどは海外の団体ですから、削除依頼は英語で行う必要があります。

迷惑メールを発信していないかをチェック！

もし、あなたの会社のメールサーバーが迷惑メール発信の踏み台にされていると疑わしく思ったら、すぐにメールサーバーの通信量を調べよう。迷惑メールの踏み台となっている場合は、毎日数十万通のメールを発信しているはずだ。

今やろう！ インターネット利用への備え

安全なWebサイト利用

■不用意に信頼できないサイトへアクセスしないようにする
■パスワードをブラウザー※に保存しない

※ Microsoft EdgeやGoogle Chromeなどのインターネット閲覧ソフト

<フィッシング詐欺サイト>

●メールの送信者欄（Fromアドレス）は偽装できるため、なりすましメールに注意する。
●必要に応じて、金融機関が推奨するセキュリティソフトなどの導入も検討する。
●カード番号や暗証番号を入力するような依頼がメールで来ることはなく、もしそのようなメールが金融機関などから届いた場合は、送信元に電話で問い合わせたり、ホームページを見たりして真偽を確認する。

<ワンクリック詐欺（不正請求）につながるサイト>

●信頼できないサイトにはアクセスしない。
●アクセスしても安易なダウンロードはしない。
●ウイルス対策ソフトなどの警告画面が表示された場合は次に進まない。

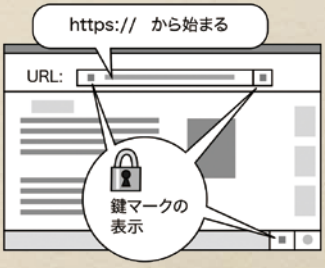
詐欺サイトにご注意を！

フィッシングサイトなどの詐欺サイトが巧妙化している。正式なものと「URLが1文字だけ」違うといった騙されやすいサイトもあるので要注意だ。検索などで調べた場合でも、該当のサイト名やURLスペルが合っているかをよく確かめよう。

同時に鍵マークがURL表示窓に出ているかも確認しよう。この鍵マークをクリックするとサイト運営組織の実在を証明する電子証明書※の内容を確認することができる。しかし、鍵マークがあっても詐欺サイトの可能性がある。

また、詐欺サイトへの誘導にはメールやSMSも使われる。メールやSMSに記載されたURLや電話番号を安易にクリックしてはいけない。メールソフトやWebブラウザーにフィッシングサイト判別機能があればこれらを活用するのも1つの手だ。

※ 信頼できる第三者（認証局）が本人であることを証明するインターネットにおける証明書で、「運転免許証」や「印鑑証明書」のようなもの



今やろう！ インターネット利用への備え

閲覧制限

すぐやろう

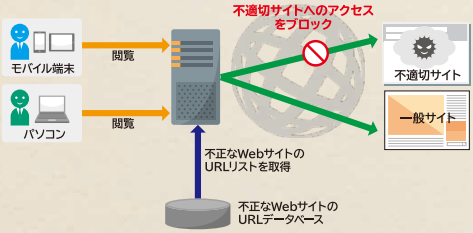
■業務に不要なWebサイトへのアクセスを制限する

<URLフィルタリング>

特定のURLアドレスを持つWebサイトとのアクセスを制限します。アクセス制限には次のような方法があります。

●商用サービスとURLデータベースを使った規制

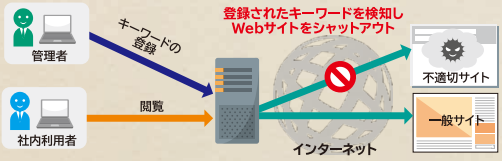
フィッシングサイトやウイルスを配布するような不正なWebサイトのアドレスをURLデータベースから取得し、Web（URL）のフィルタリングを行うことで、アクセスを制限します。



<キーワードによる規制>

●キーワードによる規制

ブラウザーに対し入力するキーワードを管理者が事前に規制します。

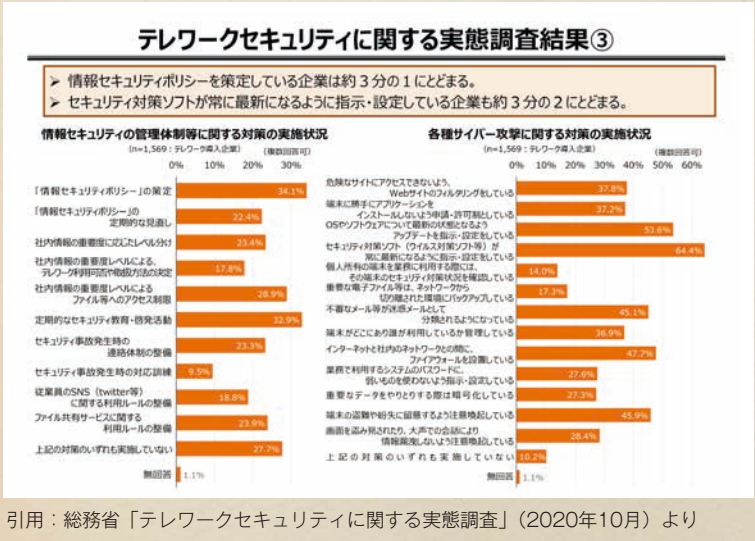


何が防げるの？

インターネットの業務外利用を制限することによって、安全でないWebサイトの利用や不正プログラムのダウンロードを防ぐことができます。

閲覧制限への対策は比較的手薄!?

2020年の新型コロナ禍に際して、感染拡大防止の観点から多くの企業でテレワークが導入された。しかし、総務省が実施した「テレワークセキュリティに関する実態調査」（2020年10月）からは、テレワーク導入に際しての経営課題がセキュリティの確保にある点が分かる。また、同調査の「各種サイバー攻撃に関する対策の実施状況」からは、Webサイトのフィルタリングなどの閲覧制限対策が比較的手薄になっている姿も浮かび上がる。



引用：総務省「テレワークセキュリティに関する実態調査」（2020年10月）より

今やろう！

重要情報の洗い出し

■機密性、完全性、可用性の観点から重要度を評価する

<情報セキュリティの三大要件>

適切な情報管理を行うために3つの観点から重要度を評価し、重要度の高いものを優先して対策を行いましょう。

	説明	対策の例
機密性	アクセスを許可された者だけが情報にアクセスできる	情報漏えい防止、アクセス権の設定
完全性	情報と処理方法が正確でかつ完全である	改ざん防止・検出
可用性	許可された利用者が必要なときに情報と関連資産にアクセスできる	電源対策、システムの二重化

●個人情報とは

①氏名　②住所　③電話番号
④メールアドレス　⑤生年月日
⑥性別　など

●これも個人情報（紙媒体／データベース）

①各種会員の申込書
②顧客の氏名が表記される売上伝票
③顧客氏名や会員コードが入っているもの
④アンケートなど氏名を記入させるもの
⑤特定の個人を識別できるメールアドレス情報
⑥防犯・監視カメラに記録された本人と判別できる映像　など

企業の各部門で保有している情報資産の例

経営企画部門	**経営戦略に関する情報資産** 経営計画、目標、戦略、新規事業計画、M＆A計画など
総務・人事部門	**管理に関する情報資産** 従業員個人情報、マイナンバー、人事評価など
法務・知的財産部門	**知的財産などに関する情報資産** 各種契約情報、公開前の知的財産情報、共同研究情報、係争関連情報など
情報システム部門	**情報システムに関する情報資産** 社内システム情報（ユーザーID、権限情報）、システム構築情報、セキュリティ情報など
営業部門	**顧客・営業に関する情報資産** 顧客個人情報、売買契約情報、販売協力・協業先情報、仕入先情報、仕入価格情報など
研究開発部門	**研究開発技術に関する情報資産** 共同研究情報、研究者情報、素材情報、図面情報、製造技術情報、技術ノウハウなど

「サイバーセキュリティ経営ガイドライン解説書」（情報処理推進機構）より作成

今やろう！

重要情報の保管

- ■オフィスへの入退室を管理する
- ■クリアデスク・クリアスクリーンを徹底する
- ■重要情報を一元管理する
- ■保管室への入退室を管理する
- ■重要書類の持ち出しを管理する
- ■重要情報廃棄の基本ルールを徹底する

<オフィス全体の入退室管理>

最終退室者は以下を行います。

●全員のパソコンがシャットダウンされ、プリンターなど周辺機器の電源が切られているか確認する。

●全ての出入り口の施錠を確認する。

●退室時刻と退室者氏名を管理簿に記録する。

＜入退室管理（訪問者）＞

オフィスに見知らぬ人がいることは、セキュリティ上問題があります。整理整頓が行き届いていたとしても、見ず知らずの人に勝手に情報を盗み見されたり、持ち出されたりすることもあるかもしれません。

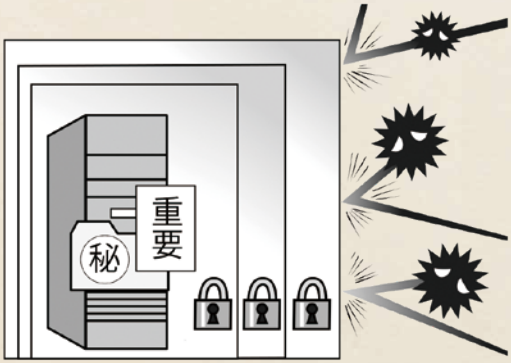
●訪問記録に記入してもらう。
●名刺をもらう。
●知らない人には声をかける。
●訪問した人をオフィスに1人で残さない。

＜クリアデスク・クリアスクリーンの徹底＞

●重要書類、スマートフォン、重要な情報を保存したUSBメモリーやCDなどの電子媒体を業務以外のときは机上に放置せず、クリアデスクを徹底する。
●離席時にはパソコンの画面をロックし、クリアスクリーンを徹底する。
・スクリーンセーバーの起動時間を10分以内に設定し、パスワードを設定
・スリープモードの起動時間を10分以内に設定し、解除時のパスワード保護を設定
・離席時には［Windows］+［L］キーを押してパソコンをロック（Windowsの場合）

＜重要情報の一元管理＞

机の上に放置した情報は、誰かに持ち去られたり、盗み見られたりする危険にさらされています。関係者以外が見たり、触れたりすることができないように、重要情報は放置せず、一元管理する必要があります。保管場所を定め、作業に必要な場合のみ持ち出し、終了後に戻すようにしましょう。



＜保管室への入退室管理＞

●保管室への入退室者を制限する。
●施錠忘れを防ぐために入退室者と時間の記録を残す。
●机の上をチェックする。
●パソコン（モニターも）や機器の電源をチェックする。
●消灯をチェックする。
●施錠をチェックする。

＜重要書類の持ち出し＞

ルールについてはP66参照。

<スタンドアロンのパソコンによる管理>

ネットワークを経由した感染と情報流出を防ぐために、最重要情報についてはネットワークに接続をしていないスタンドアロンのパソコンで管理し常時ネットワークには接続しない。

<重要情報廃棄の基本ルール>

媒体	廃棄方法
サーバー・パソコン ※リース物件返却・売却含む	・システム担当がハードディスクを取り出し破壊 ・システム担当がデータ抹消ツールにより完全消去 ・専門のデータ消去サービスを利用する。ただし、依頼先の会社の信頼度も考慮して業者を選定する
外付け ハードディスク	・システム担当が破壊 ・システム担当がデータ抹消ツールにより完全消去
CD・DVDなどの ディスク	・利用者がシュレッダーで細断 ・利用者がディスクの両面にカッターなどでキズを入れる
USBメモリー	・システム担当がデータ抹消ツールにより完全消去
重要書類	・利用者がシュレッダーで細断 ・大量の場合はシステム担当が溶解処分を専門業者に依頼し、廃棄証明書を取得

これらの方法を企業・組織の情報資産の重要度に応じて組み合わせ、最適な方法をとることが重要です。次ページでは、情報資産の廃棄に関連して発生した近年の重大事案をご紹介します。

廃棄資産の転売で行政情報流出の危機に

2019年11月、個人情報を含む神奈川県の大量の行政データが蓄積されたハードディスク（HDD）が転売される事案が明らかになった。

これは、リース契約満了によって県が返却したHDDのデータ消去（物理破壊）を委託された企業の社員がデータ消去の不十分な状態で一部を持ち出し、ネットオークションで販売したために発生した。

この事案を受け、神奈川県庁は同年12月16日に再発防止検討チームを発足。外部に出たHDDは21日までに全て回収し、2020年1月27日に情報流出防止策を決定した。同月、総務省も「県情報を保存するために使用した情報機器からの情報流出防止策」を発出。原因特定とデータ抹消措置の作業完了まで県職員が立ち会い確認するなどの今後の再発に向けた具体的な防止策を明らかにした。