

TOP SECRET

MISSION 2

すぐやろう! 対サイ
バー攻撃アクション



INDEX

Mission 1

Mission 2

Mission 3

Mission 4

Mission 5

info

今やろう! 5+2の備えと社内使用パソコンへの対策



サイバー攻撃に対して 何ができるか

標的型攻撃

Web サービスから
の個人情報の窃取

集中アクセスに
よるサービス停止

内部不正

Web サイト
の改ざん

ランサムウェア

メールによる攻撃

集中攻撃

Web サイトを
使った攻撃

OS やソフトウェア・

ウイルス対策ソフトの導入・標的型攻撃メールへの対応

電子メールの安全利用

安全な Web サイト利用・閲覧制限

OS とソフト

持ち込み機器



12 人の刺客

INDEX

Mission

Mission 2

Mission 3

Mission 4

Mission 5

Info

IoT 機器を
踏み台に
した攻撃公開された
脆弱性対策
情報の悪用Web サービスへ
の不正ログイン

フィッシング詐欺

悪意のある
インターネット
バンキング不正送金

Web サイトの脆弱性

Webサーバー/メールサーバー
/クラウドサービス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
などリモート管理の脆弱性・
ID とパスワード窃取

パスワードの管理・アクセス管理

ファームウェアの脆弱性

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

すぐやろう



- 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。

※ 2017年4月11日にWindows Vistaのサポートが終了。2020年1月14日にはWindows 7のサポートが終了予定



<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。



特にInternet ExplorerやMicrosoft Office製品、Java、Adobe Flash Player・Adobe Readerといった多くの人が使っている製品のセキュリティホールが攻撃の対象となっています。



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。



INDEX
Mission 1
Mission 2
Mission 3
Mission 4
Mission 5
Info

今やろう! 5+2の備えと社内使用パソコンへの対策



ウイルス対策ソフト・ 機器の導入

すぐやろう

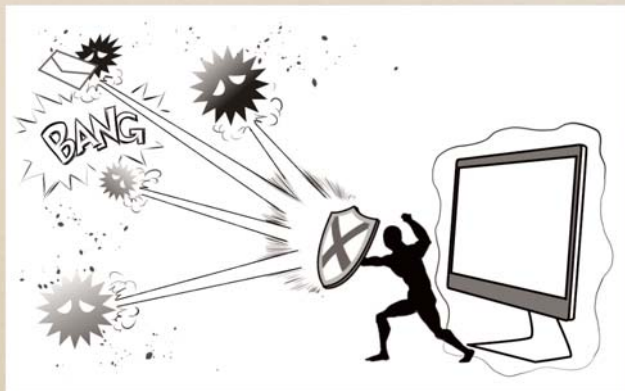


- ウイルス対策ソフトウェア（セキュリティソフト）がインストールされているか、また最新バージョンになっているかを確認する

<個別のパソコンに導入するタイプ>

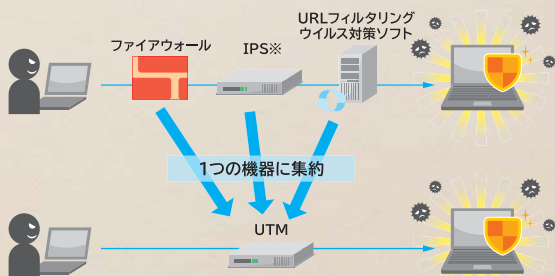
個別のパソコンに導入するウイルス対策ソフトウェアには自動的に更新する機能が付いています。最近のウイルス対策ソフトウェアは脆弱性スキャンやWeb脅威対策、URLフィルターなど多くのセキュリティ機能が付いています。

※ 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。



※不正アクセスや攻撃を検出し防御するシステム

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、毎日このプログラムの更新だ。

メールの添付ファイル、ダウンロードしたファイル、USBメモリやCD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ことだ。





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

すぐやろう



■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

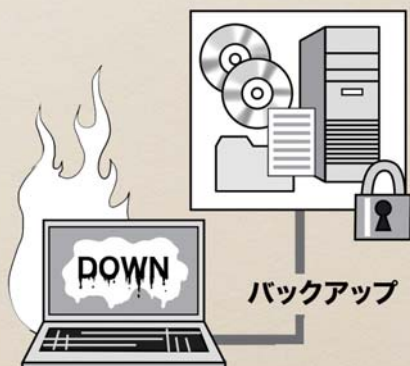


定期的バックアップの重要性

ビジネスで利用するデータは削除誤りなどの人的ミス、ハードウェア障害、ソフトウェア障害など、さまざまな要因によって壊れる危険があります。このような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。

「システムのバックアップ」を取っておくと、システムを早急に復旧させることができます。

こうした定期的なバックアップは、サイバー攻撃によるデータの改ざんや破壊、ウイルス感染にも有効です。



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オススメだ。





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

すぐやろう



- 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＞

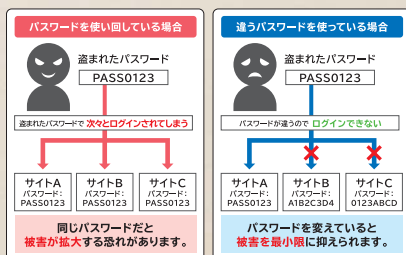
他人に推測されやすいパスワード（ニックネームや誕生日など）は使わない。

- 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

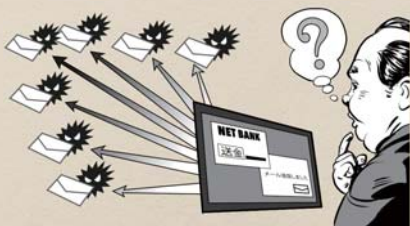
パソコン本体はもちろん、メールやSNS、各種アプリや会員サイトなどのWebサービスを使うときに必要となるのがID（アカウント）とパスワード。1つのパスワードを使い回している場合、それが流出すると、ほかのサービスも乗っ取られてしまう可能性が高くなります。



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。



2段階認証でより安全に

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。





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

すぐやろう



- 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（情報資産管理台帳の作成はP130参照）。
- 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。

アクセス管理の例

	極密文書	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

※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

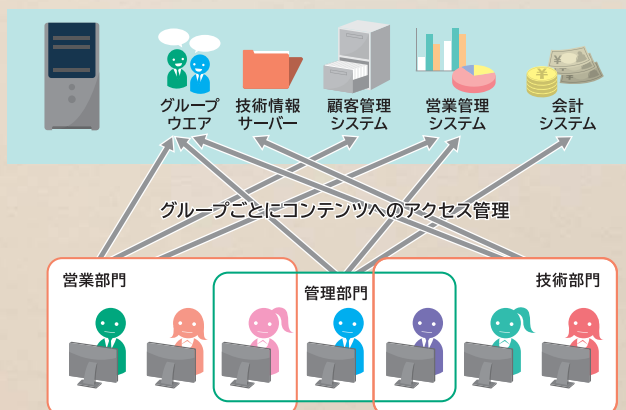
※2 情報および処理方法が正確であること、かつ完全であること

※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

何か「防げる」の？

例えば「社外秘」の情報はこれらにアクセスできる利用者也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設定するということです。それ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できるようになるので、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

すぐやろう



- 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。
- 携行時の注意
 - ・ 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

持ち出したパソコンを街なかのWi-Fiなど社外のネットワーク環境に何のセキュリティ対策もしないで接続すると、ウイルスに感染したり、情報を盗み取られたりする可能性があるので注意だ。





今やろう！ 5+2の備えと社内使用パソコンへの対策



持ち込み機器対策


すぐやろう



■ 私物の機器類を会社に持ち込む際にはセキュリティと使い方のルール（例）を設ける

<持ち込み機器の使い方ルール>

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 	<ul style="list-style-type: none"> ・ 基本的に社内へ無断で持ち込まない ・ 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が指定したものを導入する ・ 社内LANへの接続を禁止する ・ データや情報を持ち出す場合はそのルール（P58参照）に準拠する ・ 家族や友人への貸与を禁止する
スマートフォン タブレット端末 携帯電話など 	<ul style="list-style-type: none"> ・ 会社で指定したアプリケーション以外には使わない ・ 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が指定したものを導入する ・ 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	<ul style="list-style-type: none"> ・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	<ul style="list-style-type: none"> ・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させることだ。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

すぐやろう



- 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

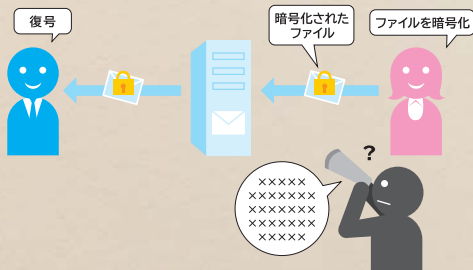
<誤送信対策>

- 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することができる（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することができます。

- 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）。



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。



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

すぐやろう



- 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	<input type="checkbox"/> OSやアプリケーションの脆弱性の解消 <input type="checkbox"/> スпамメールのフィルタリング <input type="checkbox"/> 従業員教育 <ul style="list-style-type: none"> ・ 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	<input type="checkbox"/> ウイルス対策ソフトによる各機器の感染チェック <input type="checkbox"/> 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	<input type="checkbox"/> 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。



(画像はトレンドマイクロ社提供)

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。

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P19参照





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

※ P51参照

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か疑わしいと思ったら、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

すぐやろう



- 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※に保存しない

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

<フィッシング"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。

詐欺サイトはこれで見分ける！

フィッシングサイトなどを見分ける方法がある。

通常、インターネットバンキングへのログイン画面やクレジットカード番号などの重要な情報の入力画面では、入力した情報を盗み見られないために暗号化技術（SSL）が使用されている。しかし詐欺サイトではこのSSLを使っていないことがほとんどだ。

SSLかどうかの判断は、URLで分かる。通常は「http://」から始まるが、SSLの場合「https://」で始まる。また、WebブラウザのURL表示部分（アドレスバー）や運営組織名が緑色の表示になり、鍵マークが表示される。SSLを使っているサイトは、サイト運営組織が実在していることを証明する電子証明書※を発行している。

※ 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



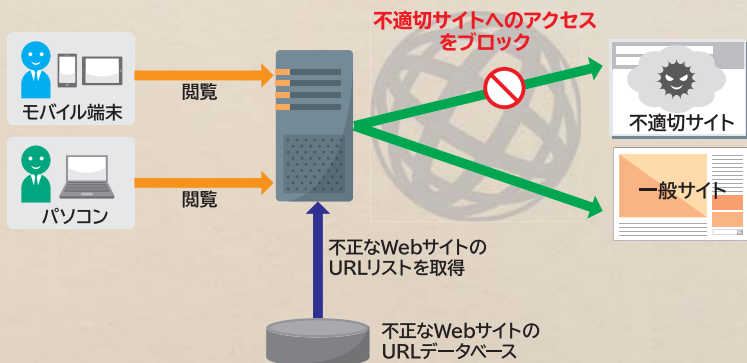
■ 業務に不要なWebサイトへのアクセスを制限する

<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

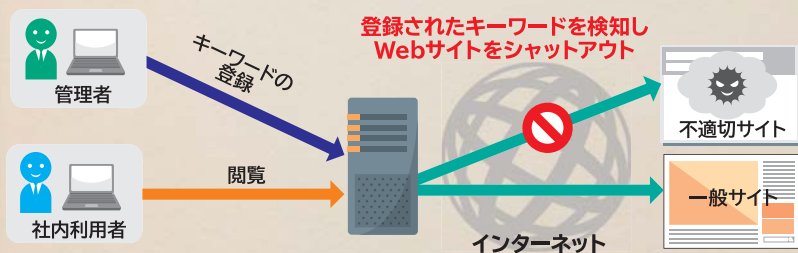
フィッシングサイトやウイルスを配布するような不正なWebサイトのアドレスをURLデータベースから取得し、Web（URL）のフィルタリングを行うことで、アクセスを制限します。



＜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。



中小企業の規制は緩い！

キーマンズネットが2017年に実施した「企業におけるWebサイト閲覧の規制状況」についての調査で、「私的利用を許可していない」と回答した企業を従業員規模で分けて見ると「100名以下」が26.7%、「101～1,000名以下」が66.2%、「1,001名以上」が77.9%と、従業員規模が大きいほどインターネットの私的利用を許可しない傾向にある。



今やろう!

重要情報の洗い出し

すぐやろう



■ 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

顧客名簿

氏名	
年齢	
住所	
TEL	

購買履歴

月	日
月	日
月	日
月	日

基本データ

No.236

住所

氏名

連絡先

●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傳票
- 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

すぐやろう



- 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。



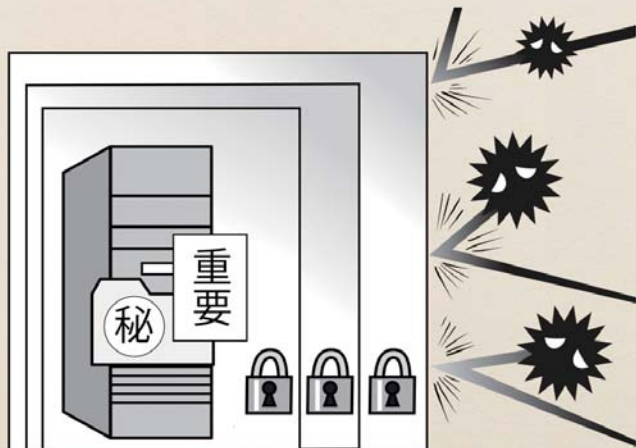
＜クリアデスク・クリアスクリーンの徹底＞

- 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P58参照。

＜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	<ul style="list-style-type: none"> ・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
外付け ハードディスク	<ul style="list-style-type: none"> ・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	<ul style="list-style-type: none"> ・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	<ul style="list-style-type: none"> ・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	<ul style="list-style-type: none"> ・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

おまけクイズ



パソコンに保存してある重要情報（データ）が故障やサイバー攻撃などで失われないように、日ごろから注意すべき行動として最も適切なものはどれですか。

- ①他のパソコンにデータをもう1つ複製（バックアップ）している
- ②メーカーの有償修理サポートを切らさないよう注意している
- ③情報はハードディスクやDVDなどに切り離して保存している



ヒント

パソコンが故障した場合、パソコン上に保存している情報は失われることが想定されます。パソコンが故障することで起こるリスクに対しては、重要情報を適切に保存しておくことが有効です。ただ、ランサムウェアのようなサイバー攻撃を受けた場合、ネットワークでつながっているパソコンや共有サーバー、外付けハードディスクなどにも被害が及びます。メーカーサポートは故障自体の修繕には有効ですが、有償サポートの場合でも多くの場合、パソコンの中のデータまでは保証してもらえません。

「情報セキュリティ自己診断チェックリスト」（内閣官房情報セキュリティセンター）より編集・構成

答え ③