中小企業向け
サイバーセキュリティ対策の極意

Ver 2.2a

中小企業向け
サイバーセキュリティ対策の極意

Ver 2.2a

日本で初めてサイバー探偵事務所を開く。ソフト帽とトレンチコートがトレードマーク。日夜懸命に頑張る中小企業の経営者に対して、客観的な態度と視点を持って依頼人に真に役立つ情報を端的に明言する。「東京をサイバー攻撃から守る」という正義感だけが、今日も彼を突き動かす。
今回、その資質を見込まれ、東京都からの依頼でサイバーセキュリティ対策のコンサルタントとして本冊子のガイド役に任命された。

冴羽（さいば） 守（まもる）

※本キャラクターはフィクションです

ケーススタディー　1

なぜ、こんな小さな会社が狙われたの？

1カ月後　会社での会議

これは実際に起きたケースを基に脚色したものだ。この会社は社員10人ほどの小さな会社で、再開時期が未定のままサイトは閉鎖された。個人情報を窃取するサイバー攻撃の対象は、決して大企業や有名な通販サイトだけでなく、顧客情報の収集などインターネットを何らかの形でビジネスに利用している会社は全て標的になっている。サイバー攻撃による被害によって、事業に致命的なダメージを受ける可能性がある。備えあれば憂いなしだ。

ケーススタディー　2

ある日突然、銀行口座の預金残高が消えた！

数日後、銀行の支店長室で

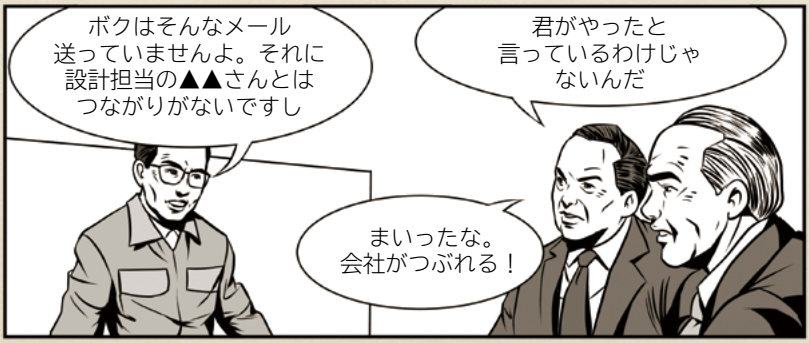
人員不足に悩む中小企業にとって、インターネットバンキングは経理業務の効率化に不可欠なものだが、サイバー攻撃の対象にもなっている。

2019 年は、9 月から被害が急増し、発生件数は 1872 件に上った。年間被害総額も 25 億円超の被害が報告されている。

ケーススタディーにもある通り、インターネットバンキングを利用しているからといって、銀行が代弁してくれるとは限らない。基本的には自己防衛だ。

ケーススタディー　3

取引先企業への踏み台にされた



サイバー攻撃は大企業だけを狙っているわけではない。
このケースでは、標的とされた大企業のセキュリティが堅固だったため、攻撃者はその取引先の中小企業を狙ったのだ。なぜなら、中小企業のセキュリティは大企業に比べて甘く、中小企業のセキュリティを突破すれば、取引のメールなどを介して、大企業のシステム内部へ侵入しやすいからだ。こうして踏み台にされた企業にとっては、ビジネスに与える影響は甚大だ。

ケーススタディー　4

企業データが人質に！日常に潜むサイバー攻撃の魔手

ランサムウェアを使ってパソコンを使用不全にし、身代金要求をするサイバー攻撃が目立つ。そこで中心的役割を果たしたマルウェアの１つに「Emotet（エモテット）」が挙げられる。Emotetは、冒頭のようなやり取りからパソコンや社内システムに忍び込む。そして、感染したパソコンからメール情報やアドレス帳の情報を窃取するほか、ランサムウェアをはじめとする別のマルウェアを呼び込む機能もあり、非常に厄介かつ危険な存在だ。

ケーススタディー　5

メールで届いた入金指示に従ったら詐欺の被害者に！

経営幹部や取引先になりすましたメールを送信し、従業員をだまして不正な口座に入金させることで金銭的な被害をもたらすサイバー攻撃が「ビジネスメール詐欺（Business E-mail Compromise ／ BEC）」だ。攻撃者は、標的となる企業の従業員が業務でやり取りしているメールを、何らかの方法で盗み見したり、ネット上の企業情報などを参考にしたりして、標的となる企業のプロジェクトや人間関係を事前に把握することで、送信メールの信憑性を高める。

ケーススタディー　6

セキュリティは サプライチェーン 全体の責任

中小企業はセキュリティ対策予算や人員が不足しがちで、対策も遅れがちだ。サイバー犯罪者はそこを突く。中小企業を取引のある大企業に攻撃する「入り口」として狙うケースも存在する。そうなれば、被害者であると同時にサイバー犯罪の一端を担ってしまう。取引停止だけでなく、損害賠償を請求されることもあるだろう。「中小企業だから狙われない」という甘い考えは通じない。セキュリティはサプライチェーン全体の問題という点を肝に銘じてほしい。

ケーススタディー　7

サイバー保険に入っていれば……

日々進化するサイバー攻撃の脅威。いつ、どのようなタイミングで狙われるかは分からない。もし攻撃の標的になったら？
そのリスクヘッジに備えるのが「サイバー保険」だ。サイバー事故によって生じた第三者に対する「損害賠償責任」や事故の際に必要となる争訟費用等の損害が補償される。ぜひチェックしてほしい。

はじめに

狙われるのは中小企業

サイバー攻撃の標的は政府・自治体や重要インフラだけではありません。
こうした大規模なサイバー攻撃には、数十万台の端末から一斉攻撃をかける手口があり、それに使用される端末は攻撃者に乗っ取られた端末です。そして比較的セキュリティの甘い中小企業の端末が狙われています。
最近では、大企業は防御が厳重なため、防御の甘い取引先の中小企業を狙い、そこから大企業のシステム内部へ侵入するケースも増えています。

セキュリティ対策はなぜ必要なのか？

インターネットが社会生活の隅々まで普及している今、サイバー攻撃は社会機能や国民生活を脅かす大きな問題となっています。個人も企業もセキュリティに関する正しい知識を身に付け、必要な対策を実践していくことがとても重要になっています。
いったんサイバー攻撃を受けて被害を受けると、金銭の損失はもとより、顧客の喪失、業務の喪失など、経営に直結する重大なリスクが発生します。経営者が責任を問われたり、場合によっては株主代表訴訟の対象にもなったりします。

すぐやろう！　サイバーセキュリティ対策

セキュリティ対策は必要だと分かっていても直接利益を生み出すものではない、難しくてよく分からない、社内に IT のことが分かる人材がいないなどの理由から、手つかずのままにしていませんか？
最優先で実施すべき対策はそんなに難しいものではありません。基本的な対策を実施することで多くの攻撃を防ぐことができます。

備えあれば憂いなし

本書は、サイバー攻撃の最新の手口から、中小企業でも実施できる基本的な対策まで分かりやすくまとめました。

INDEX 目次

中小企業向け　サイバーセキュリティ対策の極意 Ver2.2a

TOP SECRET
MISSION 1

知っておきたいサイバー攻撃の知識

TOP SECRET MISSION 2　すぐやろう！　対サイバー攻撃アクション

TOP SECRET MISSION 3　経営者は事前に何を備えればよいのか？

TOP SECRET MISSION 5 やってみよう！サイバー攻撃対策シミュレーション

TOP SECRET INFORMATION インフォメーション

本書の用語表記について

本冊子では、日ごろ、サイバー攻撃や情報技術（IT）に接することの少ない方々にもご理解いただくために、できる限り専門用語を使わず、分かりやすい用語に統一しています。

① コンピューターに潜り込んで正常な利用を妨げる不正･有害なプログラムは、近年「マルウェア」(malware) と呼ぶようになっていますが、本冊子では主にウイルスと表現しています。
② ネットワークを通じて他のコンピューターへの感染を広める不正なプログラムが「ワーム」(worm)、利用者に気付かれないように有害な動作を行うプログラムが「トロイの木馬」(Trojan horse) と名付けられていますが、本冊子では全てウイルスと表現しています。
③ 集中アクセスによるサービス停止についても、手口としてはボットネットウイルス、DoS 攻撃、DDoS 攻撃など多様ですが、本冊子では主として「集中攻撃」という形で総称しています。
④ ウイルスを発見し駆除するプログラムについても、ウイルス対策ソフトによって定義ファイルやパターンファイルなど呼び方が異なりますが、本冊子では全て定義ファイルと表現しています。
⑤ 本冊子では「サイバーセキュリティ」と「情報セキュリティ」という 2 つの言葉を使っています。「サイバーセキュリティ」は、コンピューターやインターネットの中に広がる仮想空間に関するセキュリティという意味で使用しています。一方、現実に存在する紙媒体に記載された情報などを含むセキュリティの場合は「情報セキュリティ」を使用しています。
⑥ 本冊子で参照した多くの資料では、セキュリティを脅かす事件や事故を総称して「セキュリティインシデント」と表現していますが、本冊子では「サイバー攻撃被害」と表現しています。

詳しくは巻末の「用語解説インデックス」を参照してください。

この冊子の使い方

どんなサイバー攻撃があるのかを知る
→ [01] 知っておきたいサイバー攻撃の知識

被害を予防するための対策を行う
→ [02] すぐやろう！対サイバー攻撃アクション

経営者が備えるべきことを知る
→ [03] 経営者は事前に何を備えればよいのか？

会社としての対応計画を準備する
→ [04] もしもマニュアル

攻撃シーンを想定して実際に行動する
→ [05] やってみよう！サイバー攻撃対策シミュレーション

本書では、これだけは必ず実践してほしい項目に「すぐやろう」マークを付けました。このマークが付いている項目は優先的に確認し、必ず実施しましょう。

今すぐチェックしておくべきこと

攻撃について知っておくべきこと

対策のために行動するべきこと

TOP SECRET

MISSION 1

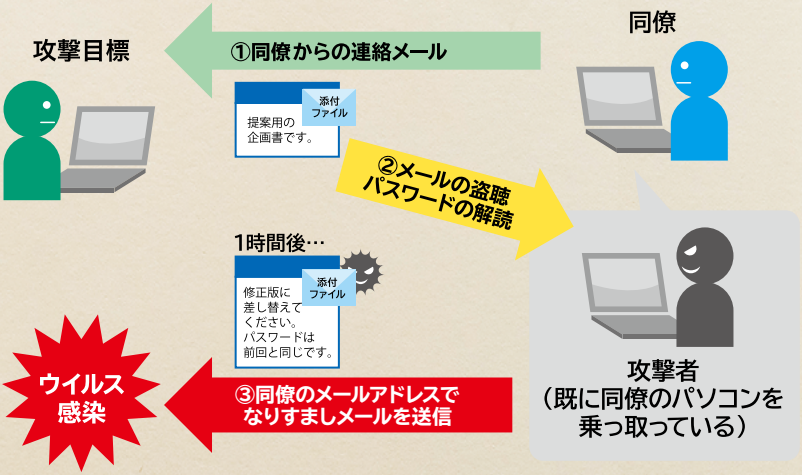
知っておきたい サイバー攻撃の知識

MISSION 1-1 標的型攻撃による情報流出

POINT 1 特定の企業や団体を狙い撃ち！

標的型攻撃とは

標的型攻撃の攻撃者は、特定の個人や企業を狙って、取引先や関係先を装い、仕事に関係しそうな話題の件名や本文のメールを送りつけてきます。メールに添付されているファイルを開いたり、本文の中にあるWebサイトのリンク先にアクセスしたりすると、ウイルスに感染してしまいます。



POINT 2 標的型攻撃による被害

・攻撃者が遠隔操作できるよう、ネットワーク上に組織外部への接続口を勝手に開く
・感染パソコン内の情報を盗み取って外部に送信する
・感染パソコンが会社のネットワークに感染を拡大する
・会社のWebサイトを改ざんする
・盗み取られたパソコン内部の情報が、次の攻撃に悪用される（例：宛先、差出人、件名、本文、署名などへの利用）

こんなメールに注意だ

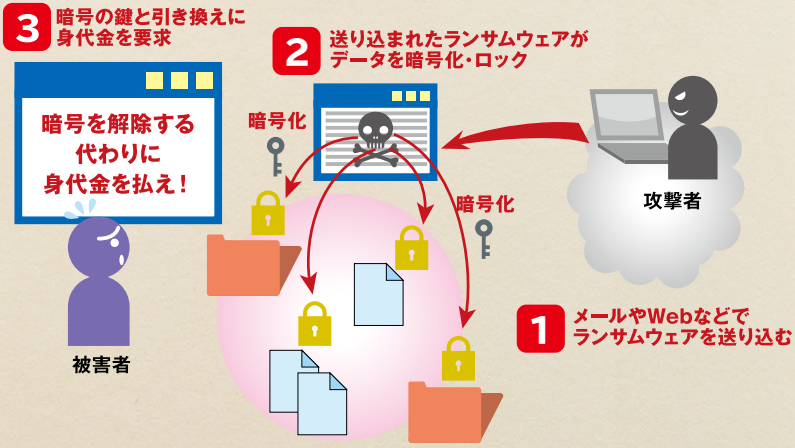
・日本語の言い回しが不自然なメール
・差出人のメールアドレスとメール本文の署名に記載されたメールアドレスが異なるメール
・これまで届いたことがない公的機関からのお知らせ
・心当たりのないメールだが、興味をそそられる内容
・心当たりのない決済や配送通知
・論理的に自分に送られてくることがおかしいメール

MISSION 1-2 ランサムウェアを使った詐欺・恐喝

POINT 1 パソコンやデータを使用不能にして身代金を要求！

ランサムウェアとは

ランサム（ransom）とは身代金のこと。メールに添付されたランサムウェアを不用意に開くと、パソコンのデータが勝手に暗号化されたり、パソコンがロックされたりして使用不能となります。そして、暗号化されたファイルの復元や、ロック解除の引き換えに金銭を要求されます。



POINT 2 侵入手口はメールとWebサイト

ランサムウェアは、メールの添付ファイルやメール本文に記載されているURLのWebサイトなどから侵入します。不用意に添付ファイルを開いたり、覚えのないURLにアクセスしたりしないことが最大の防御です。

POINT 3 世界的脅威として認識されるランサムウェア

ランサムウェアは世界的な脅威となっています。その対抗を目的とした組織として知られるのが、欧州刑事警察機構（ユーロポール）やオランダ警察、セキュリティソフトベンダーなどが立ち上げた「No More Ransom」プロジェクト。2016年7月に組織され、本プロジェクトに参加する各国法執行機関やセキュリティ関連の民間組織等は増え続けて、日本においては情報処理推進機構（IPA）などが参加しています。同プロジェクトは、ランサムウェアで暗号化されたファイルを取り戻すための無料復号ツールを提供する取り組みも継続的に行っています。

対策はバックアップと切り離し保管だ！

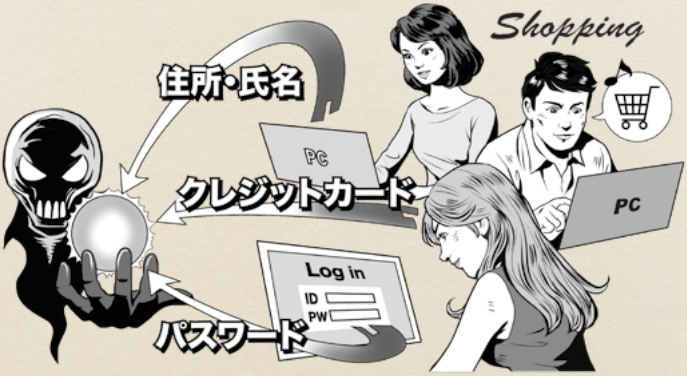
ランサムウェアによって、感染したパソコンだけではなく、共有サーバーや外付けハードディスクに保存されているファイルも暗号化される。ウイルス対策ソフトの導入はもちろん、OS※やソフトウェアを常に最新に保つことに加え、小まめにファイルのバックアップを取得し、パソコンやサーバーから切り離して保管しておくべきだ。

※ Operating System（基本ソフト）

MISSION 1-3 Webサービスからの個人情報の窃取

POINT 1 狙いは個人情報やクレジットカード情報

自社のホームページで、アクセスした顧客の情報を取得するために、個人情報の登録を求める場合があります。また、他社の提供するネットショッピングなどを利用する場合、クレジットカード情報を登録する場合があります。そうしたWebサーバーに登録された個人情報が狙われているのです。



POINT 2 攻撃手口はソフトウェアの脆弱性(ぜいじゃく)※1を狙う

Webサービスに対する攻撃は次の3つです。

・Webサービスでよく使われるソフトウェア※2の脆弱性を狙う

・ブログや電子掲示板などインターネット上で使用されるソフトウェア（Webアプリケーション）の弱点を狙う
・リモート管理用のサービスからの侵入を狙う

※1 セキュリティ上の欠陥（セキュリティホール）
※2 OpenSSL、Apache Struts、WordPressなど

POINT 3 改正割賦販売法への対応で対策が急務に

クレジットカード情報を狙った攻撃増加に伴い、クレジットカードを取り扱う加盟店におけるカード番号等の漏えいや不正使用被害の増加が社会課題となっています。こうした背景から2020年に割賦販売法が改正され、クレジットカード取引におけるセキュリティ対策の強化が事業者側に求められています。対策を怠ると、場合によっては業務改善命令や加盟店登録の取り消しなどの可能性があります。

対策を急ぐべきだ！

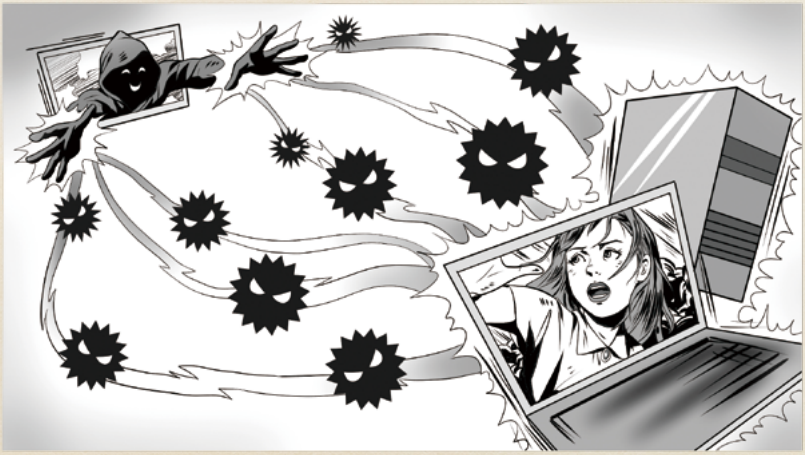
●サービスを提供する場合
- **WebサーバーのOSやソフトウェア、Webアプリケーションを最新の状態にする**
- **Webサイトに対する攻撃を検知・防御するセキュリティソフトの導入と定期的なソフトウェアアップデート**
- **適切なログの取得と継続的な監視**

●サービスを利用する場合
- **同じIDやパスワードを使い回ししない**
- **他社のホームページなどに安易に情報を登録しない**
- **利用をやめたWebサービスは退会する**

MISSION 1-4 集中アクセスによるサービス停止

POINT 1 狙いはサービスの妨害

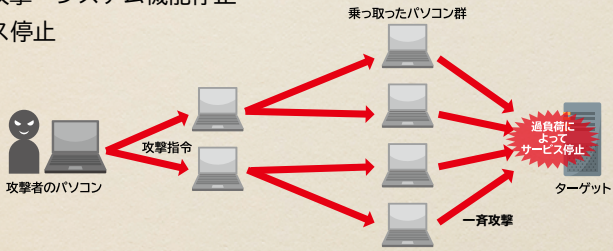
サーバーに処理速度をはるかに上回る大量の要求が集中すると、利用者はそのサーバーにアクセスできない状態になり、最終的にはサーバーがダウンしてしまいます。インターネット回線の容量がオーバーして、接続不能に陥ることもあります。



攻撃者があらかじめ不正に乗っ取った端末から一斉に攻撃を仕掛けます。数万台～数十万台のパソコンを利用した攻撃の事例もあります。最近ではパソコンだけでなく、テレビやネットワークカメラなどインターネットに接続できるデジタル情報家電なども攻撃されています。

POINT 2 攻撃手口は一斉同時集中砲火

1. インターネット経由で攻撃者が脆弱性を攻撃する不正なデータを送信→システム機能停止→サービス停止
2. インターネット経由で攻撃者が大量通信→ネットワークやサーバー処理速度の低下→サービス停止
3. 会社内の端末が感染→社内ネットワークに接続された他端末やサーバーの脆弱性を攻撃→システム機能停止
   →サービス停止



こんな被害が……

被害を受けた組織	発生年月	被害
東京五輪組織委員会	2015年11月	Webサイトにサーバーに大量のアクセスを集中させ機能停止に追い込む「DoS攻撃（ドス攻撃）」を受け、Webサイトが約12時間閲覧不能となる事態に。
世界的SNSや動画配信企業等	2016年10月	マルウェア「Mirai」に感染したIoT機器が踏み台となり、大規模なDDoS攻撃（ディードス攻撃／Dos攻撃よりも悪質な攻撃）が発生。大手SNSや動画配信サービス等が停止。
日本のオンラインゲーム	2017年6月	DDoS攻撃により、プレイヤーがサーバーから切断されたり、ログインしづらくなったりした。
世界的なWebサービス	2019年3月	DDoS攻撃を受け断続的にサービスが停止。
ラグビーワールドカップ組織委員会	2019年9月	大会期間中に組織委員会に対してDDoS攻撃が行われ、職員らにもパスワード等の窃取を目的としたフィッシングメールが送信される事案が発生。

MISSION 1-5 内部不正による情報漏えいと業務停止

POINT 1 内部からも攻撃される！

意図的な情報窃取

個人情報を売買するために、職務で知りえた情報を故意に持ち出すケースです。このケースは情報漏えいというよりも情報窃取です。

うっかりミスや不注意による情報漏えい

自宅で業務を行うために社内規則を守らずに内部情報を持ち出し、紛失してしまったなどのケースです。ほとんどはルールを知りつつ違反しています。

POINT 2 持ち出し手段はUSBメモリーなど

内部情報を持ち出す手段としてはUSBメモリーが一番多く、そのほかではメール、パソコンです。

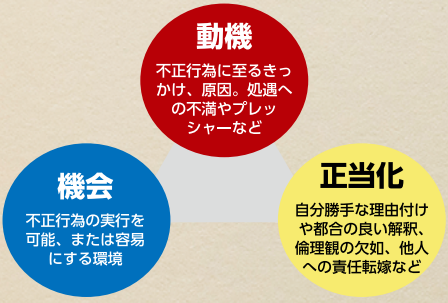
POINT 3 企業の信用が失墜し、賠償が求められる

意図的であれ、うっかりであれ、個人情報の漏えいは企業に重大な打撃を与えます。2018年に起きた情報漏えい事件の1件当たりの平均想定損害賠償額は6億3000万円を超えています（日本ネットワークセキュリティ協会「2018年情報セキュリティインシデントに関する調査報告書」【速報版】）。その一方で、日本損害保険協会による「サイバー保険に関する調査2018」からは、「サイバーリスクへの対応」を経営課題として重要視していない傾向が浮かび上がっています。攻撃手法が多様化・悪質化している現在、早急な対策が必要です。

対策は「動機」「機会」を減らすことだ！

●「動機」を減らす
- **職場環境や処遇に対する不満を解消する**

●「機会」を減らす
- **アクセス権の付与を最小限にするとともに管理を厳格にする**
- **システム操作の記録と監視により管理を強化する**
- **モニタリングや通報制度などにより「必ず見つかる」と思わせる**
- **罰則の強化により「利益にならない」と思わせる**
- **状況に合わせて社内ルールなどの整備・見直しをする**



MISSION 1-6 Webサイトの改ざん

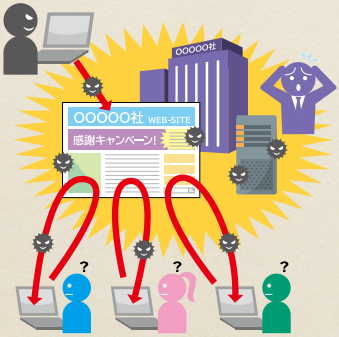
POINT 1 改ざんの目的は2つ

いたずらや主義主張による改ざん

攻撃者がいたずらや主義主張を表示する目的で改ざんするケースです。国際テロ組織の主義主張などが掲載されることもあります。

気付かぬうちにウイルスをばらまくWebサイトに

Webサイトを閲覧しただけでウイルスに感染するように改ざんされるケースです。この場合、Webサイトを改ざんされた企業はウイルス感染に加担した加害者となってしまいます。



POINT 2 ECサイトの脆弱性をついた事案も発生

近年では、ECサイト（インターネットを介した販売サイト）を利用した事業拡大も一般的となりました。しかし、ECサイトを構築するパッケージサービスの脆弱性等を突く形で、Webサイトが改ざんされ、クレジットカード番号等が窃取される被害が起きています。経済産業省によると、2019年までに約14万件のクレジットカード番号等の漏えいが報告されています。

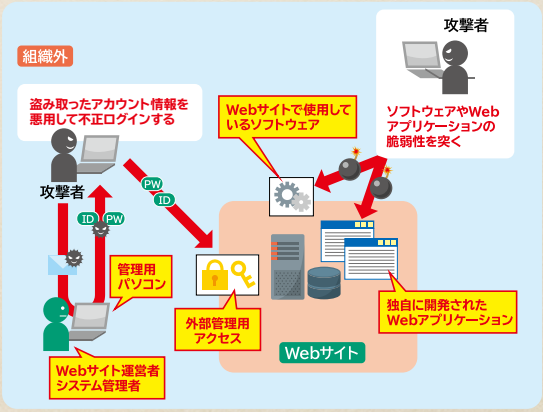
POINT 3 手口は脆弱性攻撃と管理用アカウントの乗っ取り

脆弱性を狙った攻撃による改ざん

Webサーバーに存在する脆弱性を攻撃することにより、改ざんを行います。直接コンテンツの改ざんを行う方法と、秘密の出入り口をつくるなどして遠隔操作で改ざんを行う方法の２つがあります。

管理用アカウントの乗っ取りによる改ざん

管理者のID・パスワードが盗まれ、攻撃者が管理者としてWebサイトを操作して改ざんしてしまうやり方です。正規のWebサイト操作により改ざんが行われるため、被害にほとんど気付きません。



対策を急ぐべきだ！

- サーバーのOSやWebアプリケーションを最新の状態にする
- サーバーに使用しているソフトウェアを更新する
- 管理用アカウントを厳重に管理する
- 改ざんを早期に検知する対策を行う

MISSION 1-7 インターネットバンキングの不正送金

POINT 1 銀行口座が狙われている！

インターネットバンキング不正送金の被害は大手銀行の対策が進み、2016年に被害額はいったん減少したものの、中小企業が利用する金融機関の法人口座の被害などにおいても増加傾向が続いています。警察庁発表によると、2019年に発生したインターネットバンキングの不正送金事案は1872件。被害総額は約25億2100万円（いずれも前年度増）となっており、事態の深刻さがうかがえます。

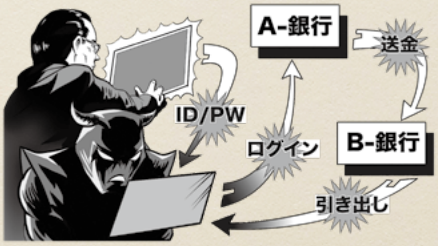
POINT 2 手口はフィッシング詐欺と不正送金ウイルス

フィッシング詐欺

①銀行を装い、「本人認証サービスの確認」といった内容でフィッシングサイト（偽サイト）のURLを送りつける
②偽のログインページにアカウント情報を入力させる

不正送金ウイルス

・攻撃者は改ざんしたWebサイトやメールの添付ファイルなどから不正送金ウイルスを侵入させる
・不正送金ウイルスは、ユーザーがインターネットバンキングを利用する際、本来の画面とよく似た偽のポップアップ画面を表示し、認証情報（ID、パスワードなど）を入力させ、攻撃者に送信する
・攻撃者は、入手した認証情報を利用してインターネットバンキングにログインし、第三者の口座に送金を行う



不正送金を阻止するには

- **金融機関が推奨するセキュリティソフトを導入する**
- **対策ソフトを最新状態に更新し、定期的なウイルススキャンを実施**
- **OSやインストールされているソフトウェアは常に最新の状態を保つ**
- **インターネットバンキングにアクセスした際にいつもと違う画面等が表示された場合、ID・パスワードを入力しない**
- **ID・パスワードを求めるメール等が来ても無視する**
- **ワンタイムパスワードを受信している場合、パソコンではなく、携帯電話やスマートフォンのメールで受信できるように登録する**
- **不正なログインや覚えのない送金等の履歴がないか小まめに確認**

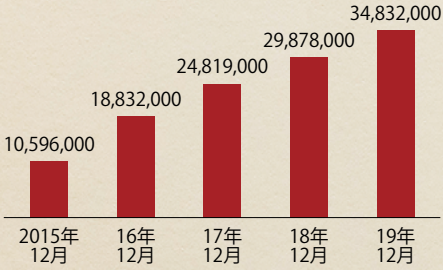
悪意のあるスマホアプリ

不正アプリでスマートフォンは乗っ取られる！

スマートフォンではさまざまなアプリをダウンロードして使用することができますが、中にはインストールされたスマートフォンのデータをのぞき見したり、カメラなどを遠隔で勝手に作動させたりする機能を持つ不正アプリがあります。

Androidの不正アプリが累計3400万個を突破

2010年8月に最初のAndroid不正アプリが検出されて以来、2019年12月時点で3400万個に到達しました（トレンドマイクロ社調べ）。
Androidでは自由にアプリを配布・インストールすることができます。スマートフォンには、電話番号やメールアドレスなどの個人情報をはじめ、クレジットカードや銀行口座の情報を入れている人も多いでしょう。不正なアプリには十分注意してください。



（トレンドマイクロ社調べ）

POINT 2 不正アプリによる被害

・ワンクリック詐欺やフィッシング詐欺により、個人情報などを盗まれたり、アカウントの乗っ取りや不正利用で金銭を奪われたりする
・写真や住所、電話番号などの個人情報を抜き取られて勝手にネット上に掲載されたり、自分のいる場所を追跡してストーキングをされたりして精神的な被害を受ける
・スマートフォン向けのランサムウェアで端末にロックをかけられて身代金を要求される

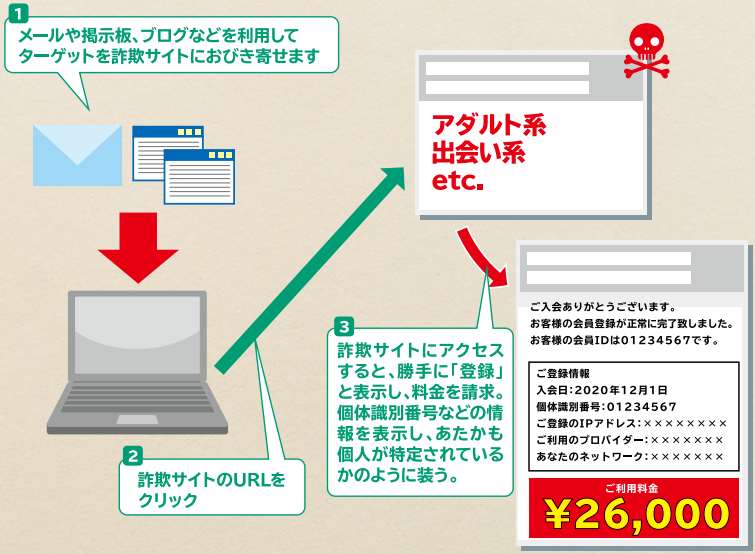
スマートフォンにもセキュリティ対策が必要だ！

スマートフォンのOS・ソフトウェアはアップデートし、ウイルス対策ソフトも導入・更新しよう。また、公式サイト以外からアプリをインストールせず、アカウントやクレジット情報などの入力は慎重に行うことだ。さらに、重要データのバックアップを実施し、盗難・紛失に備えて画面ロックなどを設定し、「GPS（位置情報サービス）」と「端末を探す」機能を有効にしておくとよいだろう。

巧妙・悪質化する ワンクリック詐欺

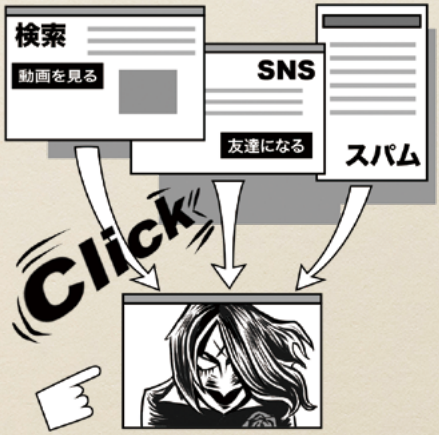
サイトを見ただけで請求！

アダルトサイトや出会い系サイトなどにアクセスさせ、金銭を不当に請求する攻撃です。これまでは利用者のクリックをきっかけにして請求画面が表示されるものでしたが、2016年にはクリックすることなくWebサイトを見ただけで勝手に「登録」させて請求画面が表示される「ゼロクリック詐欺」などが出現しており、今後も注意が必要です。



POINT 2 手口は巧妙化している！

・ワンクリック詐欺に誘導するメールが届く
・パソコンなどに常駐して定期的に料金を要求する画面を表示する
・懸賞サイトや占いサイト、音楽のダウンロードサイトなどを装う
・合法的なコミュニティーサイトで知り合いになり、詐欺サイトに誘う
・個人情報を盗み取り､データを削除するための金銭を要求する
・ウイルス感染の警告画面を表示して、対策ソフトを売りつけたり、パソコンのデータを盗み取ったりする
・相談窓口を装ったサイトで解決料を請求する
・裁判所に訴える、というメールが届く



請求には応じるな！

ワンクリック請求が来ても慌てる必要はない。料金の請求には一切応じず、とにかく無視することが最善の対処法だ。「登録完了」と表示されても、ワンクリックでは契約が成立せず、料金の支払い義務はない。不安な場合は、国民生活センターや消費生活センターなどに相談だ。

MISSION 1-10 Webサービスへの不正ログイン

POINT 1 個人情報の窃取やオンラインショッピングでの不正注文が狙いだ！

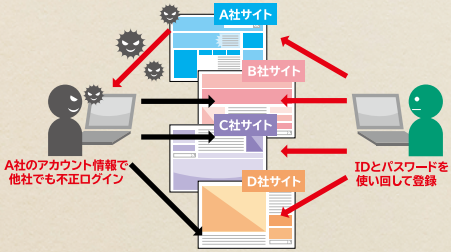
Webサービスから盗み取ったIDとパスワードを悪用し、ほかのサイトに不正ログインして、なりすましを行ったり、不正な注文をしたりする攻撃です。

サービス提供者の被害例

・サービス提供しているサイトから情報を盗み取り、不正な注文やポイントの不正使用を実行
・利用者の個人情報の閲覧、窃取
・登録している利用者にサイトを装ったメールを不正送信

サービス利用者の被害例

・なりすましによるインターネットバンキングでの不正送金やオンラインショッピングでの不正注文



POINT 2 代表的な攻撃手法の特徴

パスワードの推測や情報漏えい型のウイルス

名前や誕生日、IDと同一の文字列、連続した英数字など使われやすい文字列を

攻撃者が入力し、不正ログインされます。以下が主な攻撃手法の一例です。また、情報漏えいを引き起こすタイプのウイルス感染によってもユーザーIDやパスワードが不正利用される確率が高まります。

・パスワードリスト型攻撃
別のWebサービスから窃取したIDやパスワードを使い不正ログイン。

・総当たり攻撃
攻撃者側がツール等を用いて考えられる全てのパターンを試す、文字通り「総当たり」の不正ログイン手法。

・ソーシャルエンジニアリング攻撃
主要な攻撃手法の1つ。例えば、パソコン画面等ののぞき見によってIDやパスワードを窃取する手法です。

不正ログインを防ぐ対策はこれだ！

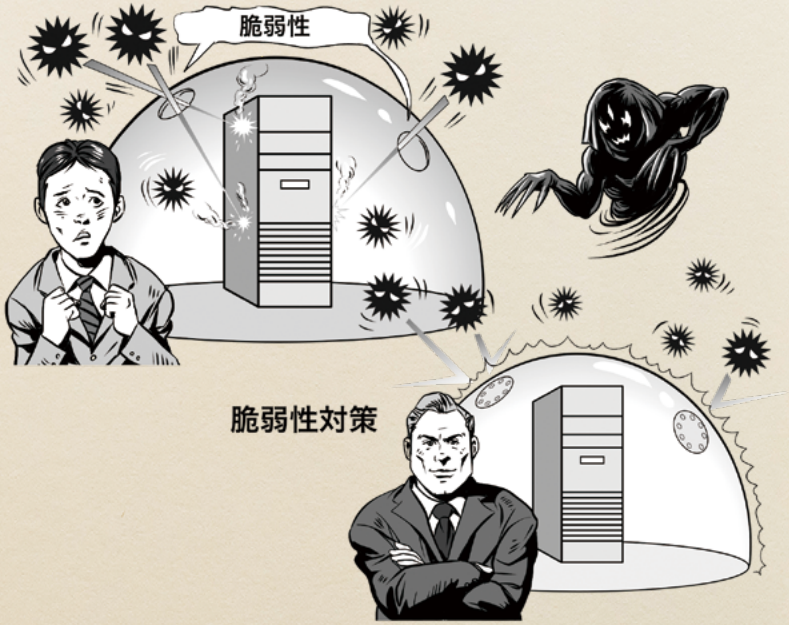
●サービス提供者
- **簡単なパスワード、容易に推測できるパスワードを許可しない**
- **多要素認証を導入（Webとスマートフォンを使ったログインなど）**

●サービス利用者
- **複数のWebサービスで同一パスワードを使い回さない**
- **パスワード管理は他人に知られず、自分でも忘れないよう徹底する**
- **パスワードのほか多要素認証（ログイン時に事前登録されている電話番号との連携を通じた認証など）を採用しているサイトを利用する**
- **離席時のログアウトなどパソコン画面ののぞき見防止策を講じる**
- **パスワードが流出したと疑われるときには速やかに変更する**

公開された脆弱性対策情報の悪用

セキュリティ対策ができていない企業を狙い撃ち

OSやソフトウェアの脆弱性が発見されると、開発したメーカーから更新プログラムが提供されます。攻撃者は、更新プログラムを実施していない利用者を探し出し、攻撃を仕掛けます。



POINT 2 こんな企業が狙われる！

・脆弱性対策情報を知らない
・利用している製品が影響を受けることを知らない
・公開された対策をすぐに実施していない

つまり、OSやソフトウェアをいつも最新の状態にしていない企業がターゲットなのです。

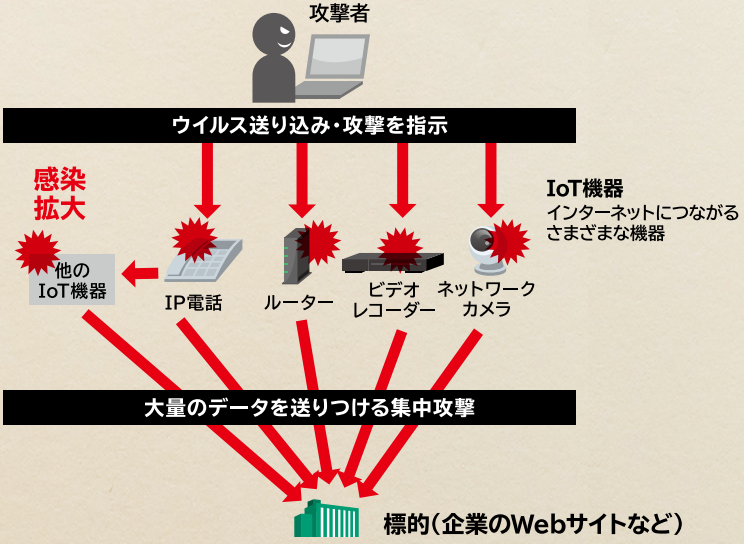
対策はこれだ！

- **社内で使用しているソフトウェアの全てについて、自動更新が設定されているものと設定されていないものを把握する**
- **使っているソフトウェアに関する脆弱性情報を「脆弱性対策情報ポータルサイト」（JVN）などで入手する（P57参照）**
- **使っているソフトウェアに脆弱性が発見された場合に備えて、会社全体のソフトウェアを更新する手順を作成しておく**
- **脆弱性が発見されたら、全てのソフトウェアの更新を確認し、実行する**

MISSION 1-12 IoT機器を踏み台にした攻撃

POINT 1 狙われているのはパソコンやサーバーだけではない！

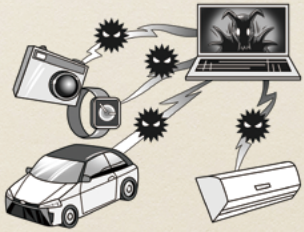
昨今は自動車やネットワークカメラ、情報家電などもインターネットにつながるようになっています（IoT※機器）。攻撃者はインターネット越しにこれらIoT機器の脆弱性や設定不備などを突いて攻撃を行い、不正アクセスやウイルス感染、さらにデータの改ざんや情報漏えい、機器操作などを行います。



※ IoT（Internet of Things）：モノをインターネットにつなげて動作させること

POINT 2 IoT機器向けウイルスの猛威

2016年にはIoT機器向けウイルス「Mirai」による攻撃により、複数の大手ネットサービスが長時間にわたって接続しにくくなるトラブルが発生しました。初期パスワードのまま使用されているネットワークカメラなどのIoT機器が「Mirai」に感染したことが原因でした（P31参照）。



POINT 3 脅威を増すIoT機器へのサイバー攻撃

IoT機器普及につれて、これらを狙ったサイバー攻撃の脅威も増しています。そのため、総務省や情報通信研究機構（NICT）、インターネットプロバイダが連携し、サイバー攻撃に悪用されるおそれのあるIoT機器の調査や注意喚起を行う「NOTICE」という取り組みが行われています。

● NOTICE　https://notice.go.jp/

対策はこれだ！

- **IoT機器を社内ネットワークに接続するリスクとルールを周知させる**
- **IoT機器の管理者を明確にする**
- **インターネットにつながっているIoT機器を把握する**
- **必要がない場合はIoT機器をインターネットに接続しない（または電源を切る）**
- **管理画面にアクセスするためのIDとパスワードを確実に管理する（複雑なものに変更するなど）**
- **制御用ソフトウェアの更新を定期的にチェックし、常に最新の状態にする**

中小企業における サイバー攻撃被害の例

新型コロナ禍も背景に 巧妙化・高度化するサイバー攻撃

2020年に入り、新型コロナウイルス感染拡大防止への対応として注目されたテレワークの拡大などサイバー空間を巡る環境が大きく変化しています。一方、実際の取引先とのメールを装う攻撃の広がりなど、攻撃者の仕掛けるサイバー攻撃の手法も巧妙化・高度化が進んでいます。

中小企業を含んだサプライチェーンが 狙われている

例えば、取引先とのメールを装うEmotetなど高度化した攻撃は、企業のサプライチェーン上においてセキュリティ対策や対策意識の弱い部分をターゲットにします。現実に、Emotetに感染した中小企業の端末やメールアドレスが攻撃者に利用され、取引先への攻撃の起点となり、さらに感染を広げるケースがすでに発生しています。中小企業にとってもサイバー攻撃に対する備えは急務となっているのです。

最近の事例

発生地	主な要因	概要
神奈川県	古いOSの使用	古いOSでしか動作しないソフトウェアを利用するためマルウェア対策ソフト未導入の端末を使用。社内プリンターを利用する際に社内LANに接続し、インターネット接続を介してマルウェアに感染した。
愛知県	私物端末の利用	社内の特定端末から不正な通信先に通信が行われていた。社員の私物端末が会社のWi-Fiに無断接続されていたことに起因。当該端末からの不正送信先は過去にマルウェアやランサムウェア配布に利用されていることが確認されている攻撃者サーバーであった。
埼玉県	私物端末の利用	企業役員の家族が個別に持ち込んだ無線ルーターを介して社内のパソコンがランサムウェアに感染。
岩手県	出張先ホテルのWi-Fi利用	社員が出張先のホテルのWi-Fi環境でなりすましメールを受信。添付のマルウェアを実行したことによってEmotetに感染。このためアドレス情報が抜き取られ、抜き取られた取引先情報等のアドレス宛に攻撃者によってメール送信が行われた。
群馬県	サプライチェーン攻撃	取引先企業のメールサーバーがサイバー攻撃を受けたことにより、メールアドレスが漏えい。複数のアドレスから当該企業に向けてマルウェアが仕込まれたメールが送信された。メール内容は賞与支払いや請求書の支払い等を装うなりすましメールであり、サプライチェーンを通じた攻撃であった。

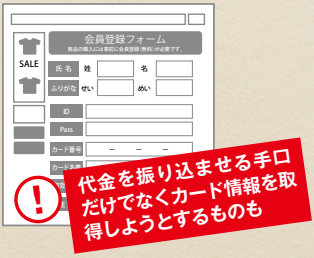
参考：経済産業省「昨今のサイバー攻撃事案を踏まえた注意喚起と報告のお願い」に対する報告結果 及び「中小企業向けサイバーセキュリティ事後対応支援実証事業（いわゆる「サイバ ーセキュリティお助け隊」）」の事業報告を踏まえた昨今の産業を巡るサイバーセキュリティに係る状況の認識と、今後の取組の方向性について」（2020年6月）

MISSION 1-14 なりすましECサイトの被害と回避策

POINT 1 なりすましECサイトに注意！

実在するサイトの外観を装った「なりすましECサイト」。その被害が増加しています。これらは既存のECサイトの模倣などによって消費者を誤認させ、商品代金を騙しとったり、模倣品、海賊版その他購入しようとした品と全く別個の物を送りつけてきたりします。また、こうした手口だけでなく、クレジットカード決済ができるかのように見せかけて消費者側のカード情報等を入力させるサイトも確認されています。

典型事例



その他の特徴としては、「支払い方法が銀行振り込みのみになっている」「問い合わせ先のメールアドレスがフリーメールアドレス」「フォームの崩れやリンク切れなどWebサイトの作り方に粗雑な点が見られる」などが挙げられます。

出典：セーファーインターネット協会／なりすましEC対策協議会「なりすましECサイトに注意！」より

POINT 2 なりすましECサイトの対策を怠ると企業側も大きな不利益を被る可能性が…

なりすましECサイトの被害者は、消費者だけではありません。なりすまされた企業側にも大きな不利益が生じる可能性があります。なりすましECサイトへの対策を放置すると、

・売上減少
・信頼失墜
・被害者からのクレーム・問い合わせ殺到

といった事態が生まれる可能性があります。ECサイトの来訪者への注意喚起など積極的な対策が重要です。

なりすましECサイトを撃退せよ！

なりすましECサイトを撃退するには、積極的なアクションが重要だ。より具体的には、

・来訪者への注意喚起

・迅速な問い合わせ対応

・プロバイダへの削除要請

の3つが考えられる。また、警察に情報提供することで、当該サイトの銀行口座の停止やウイルス対策ソフトやフィルタリング製品への反映がされる場合があり、被害拡大防止が期待できる。

● 一般社団法人セーファーインターネット協会／なりすまし EC サイト対策協議会「なりすましECサイト対策マニュアル」（2015年3月）

https://www.saferinternet.or.jp/wordpress/wp-content/uploads/narisumashi_manual.pdf

ビジネスメール詐欺（BEC）にご注意！

POINT 1 巧妙なBECの罠

ケーススタディー5（P10）でもご紹介した「BEC攻撃」。「取引先から振込先口座変更の指示を電子メールで受信した」などのように、ビジネス関係者を装ったサイバー攻撃が中小企業を狙っています。

POINT 2 BEC被害の事例

BEC攻撃は世界的にも大きな被害を生んでいます。「取引先との請求書の偽装」「経営者などへのなりすまし」「窃取メールアカウントの悪用」「弁護士など社外の権威ある第三者へのなりすまし 」「詐欺の準備行為」の大きく5つのタイプに分類できます。

セキュリティ意識を高め対策を確実に！

- **取引先とメール以外の方法で確認**
- **電信送金に関する社内規程の整備**
- **普段とは異なる表現のメールやフリーメールに注意**
- **不審なメールは組織内外で情報共有**
- **ウイルス・不正アクセス対策はしっかりと**
- **電子署名を活用しよう**

TOP SECRET

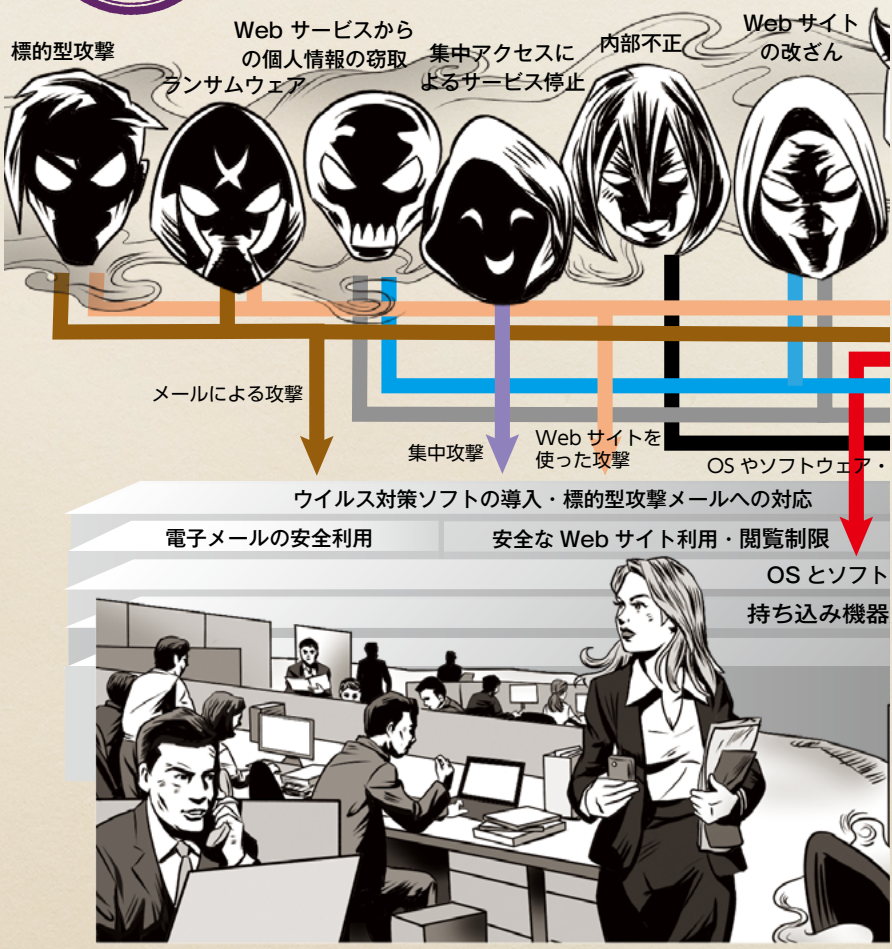
MISSION 2

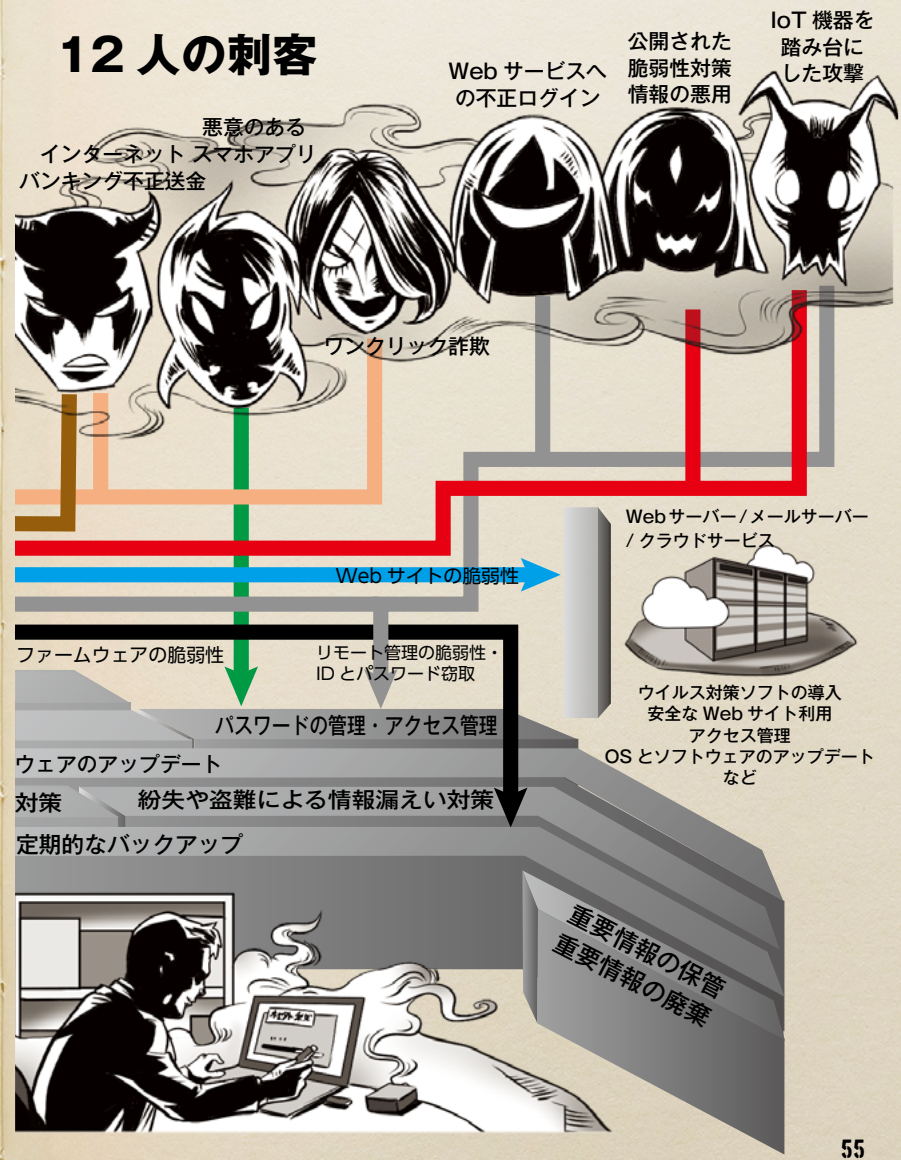
すぐやろう！ 対サイバー攻撃アクション

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 スマホアプリ
バンキング不正送金
ワンクリック詐欺
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
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。

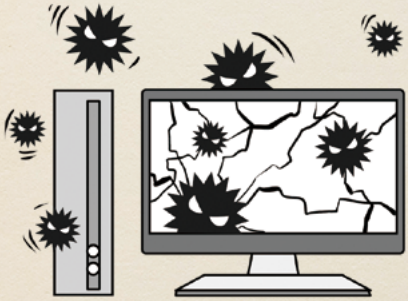
※ Windows7のサポートは2020年1月14日に終了。Windows8.1については2023年1月10日に終了予定。可能な限り早く最新のWindows環境への移行をお勧めします。やむを得ず継続利用する場合には、ベンダーサポートに相談するなどし、適切な対応を図ってください

<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

ウイルス対策ソフト・機器の導入

■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

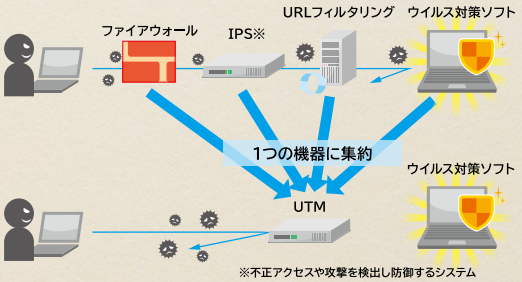
＜個別のパソコンに導入するタイプ＞

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。

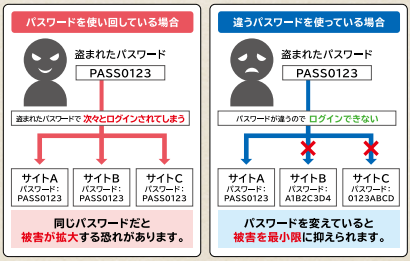
●推測しづらく自分が忘れないパスワードにする。

●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。

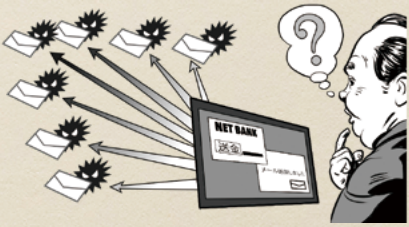
パスワードの使い回しは危険

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

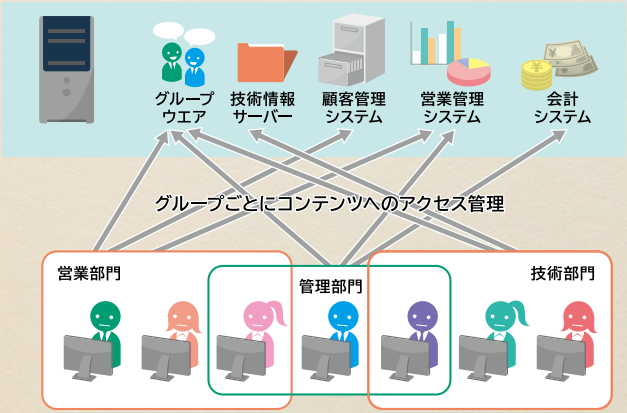
	極秘文書	機密文書	営業データ	技術データ
役　員	○	○	△	△
部　長	△	○	△	△
営業部門	×	×	○	×
技術部門	×	×	×	○

○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＞

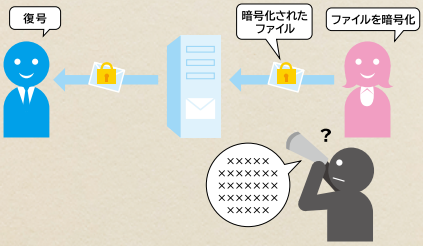
●送信ボタンを押す前に、必ず宛先を再確認する。いったん送信トレイに保存するように設定すれば、送信前に宛先を再確認できる（メールソフトとバージョンによって異なります）。

●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＞

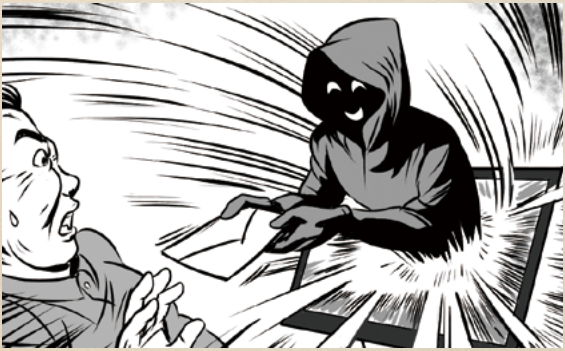
迷惑メールと判断された送信元のIPアドレスを管理する「ブラックリスト」といわれるデータベースがあります。ウイルス対策ソフトの中には、このブラックリストを参照して、このリストに登録されたメールサーバーからのメールは受け取りを拒否する機能を持ったものもあります。もし、あなたの会社が迷惑メールを発信してブラックリストに登録され取引先で受け取り拒否されたら、事業に大きな支障が生じます。

＜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。

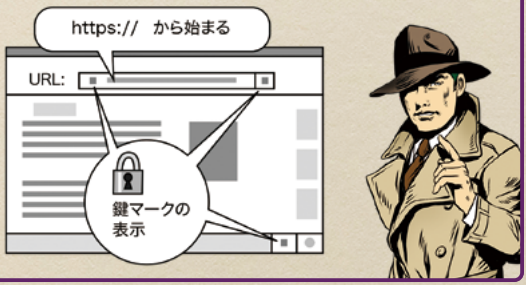
詐欺サイトにご注意を！

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



MISSION 2-13

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

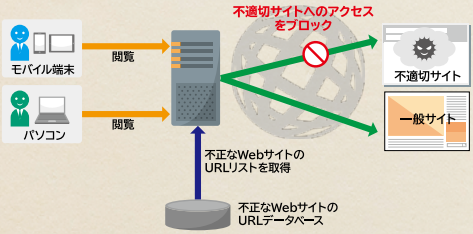
■業務に不要なWebサイトへのアクセスを制限する

<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

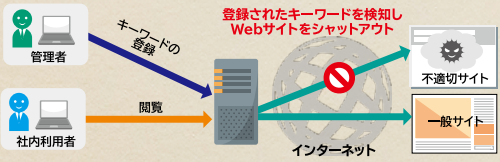
フィッシングサイトやウイルスを配布するような不正なWebサイトのアドレスをURLデータベースから取得し、Web（URL）のフィルタリングを行うことで、アクセスを制限します。



<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。

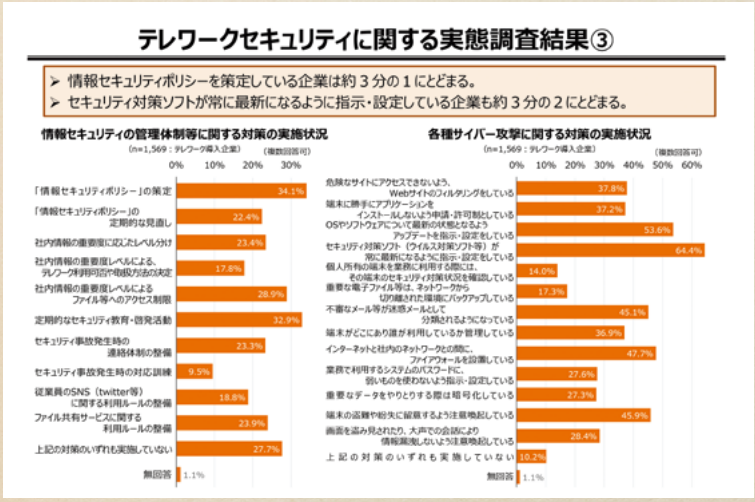


何が防げるの？

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

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。

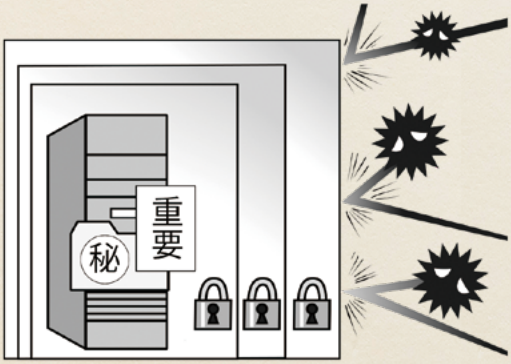
●訪問記録に記入してもらう。
●名刺をもらう。
●知らない人には声をかける。
●訪問した人をオフィスに1人で残さない。

＜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。

TOP SECRET

MISSION 3

経営者は事前に何を備えればよいのか？

MISSION 3-1

サイバーセキュリティ対策は、事業継続を脅かすリスクの1つ

サイバーセキュリティ対策が経営に与える重大な影響

POINT 1 ビジネスの継続のためにはITの活用は不可欠

中小企業にとって、業務の効率化、生産の効率化、人材確保は重要な課題であり、業務、生産工程などの運用コストの削減・効率化のために、ITは大きな柱として活用されています。より一層の業務効率の改善や生産力向上を目指して、モバイル端末の活用や外部クラウドサービスの活用も進んでいます。

POINT 2 ITの活用にはサイバー攻撃などへの備えが必要

ITを活用してどんなに利便性の高いサービスを提供しても、どんなに業務を効率化しても、緊急事態（自然災害、大火災、感染症、テロ、サイバー攻撃など）で事業資産や社会的信用が失われて早期復旧ができない場合は、事業の継続が困難になり、組織の存立さえも脅かされる可能性があります。
サイバー攻撃は事前のセキュリティ対策によって、防御が可能です。

POINT 3 サイバーセキュリティ対策は経営者が自ら実行

サイバーセキュリティリスクは経営に重大な影響を及ぼす可能性がある一方で、投資効果が見えにくいものです。サイバー攻撃のリスクをどの程度受容するのか、セキュリティ投資をどこまでやるのか、経営者がリーダーシップを発揮することが必要不可欠です。

MISSION 3-2

サイバーセキュリティ対策は、事業継続を脅かすリスクの1つ

サイバー攻撃を受けると企業が被る不利益

金銭の損失

顧客の個人情報や取引先などから預かった機密情報を万一漏えいした場合は、多大な損害賠償が発生します。また、インターネットバンキングの不正送金などで直接的な損失を被る企業も増えています。

顧客の喪失

サイバー攻撃を受けた企業は管理責任を問われ、社会的評価は低下し、顧客離れなど大きなダメージを受けることになります。風評被害がいつまでも続き、イメージが回復せず事業の存続が困難になる場合もあります。

業務の喪失

サイバー攻撃を受けると、被害の拡大を防止するため、システムを停止する措置が必要です。その間はメールすら使えなくなり、営業機会を喪失するとともに、社内の業務も停滞してしまいます。

従業員への影響

内部不正が容易に行えるような職場環境は、従業員のモラルを低下させます。また、従業員の個人情報が適切に保護されなければ、従業員から訴訟を起こされることも考えられます。

MISSION 3-3

サイバーセキュリティ対策は、事業継続を脅かすリスクの1つ

経営者に問われる責任

POINT 1 経営者などに問われる法的責任

ITを利活用する際には、顧客の個人情報を収集・活用する、他社への差別化として技術情報を活用するなど、さまざまな重要情報を取り扱います。そのため、企業とその経営者には高い責任が求められます。

企業が個人情報などを適切に管理していなかった場合、経営者や役員、担当者は刑事罰やその他の責任を問われます。場合によっては、経営者が個人として損害賠償責任を負うこともあります。

POINT 2 関係者や社会に対する責任

情報漏えいを引き起こした企業の経営者には、法的責任だけでなく、その情報の提供者や顧客に対して損害賠償や謝罪などが求められます。

また、会社を代表して、社会に対して情報漏えいの原因や再発防止策を明らかにする義務があります。さらに、営業機会の喪失・売上高の減少・企業のイメージダウン・取引先との信頼関係の喪失などを引き起こすことにより、事業に大きなダメージを与え、経営者としての経営責任を果たすことができなくなります。

POINT 3 海外の法律への対応も必要

サイバーセキュリティへの注目は世界中で高まっており、関連法案が世界各国・地域で施行されています。近年はWebなどで個人情報を比較的容易に収集でき、海外との直接取引も容易です。事業展開の中でこうした活動を行っている場合には、諸外国の法律に抵触しないように注意が必要です。

（例）・欧州連合（EU）：EU 一般データ保護規則
（General Data Protection Regulation：GDPR）
・中華人民共和国：中国サイバーセキュリティ法（CS法）
・アメリカ合衆国：「NIST SP800-171」
（米国政府の調達品に関するセキュリティガイドライン）

POINT 4 サイバーセキュリティ対策の情報開示

5G、IoTやAIをはじめとしたICT利活用が社会・経済のあらゆる場面に浸透しつつある中、有効なサイバーセキュリティ対策を講じることは企業の経営課題となっています。加えて、企業の社会的責任を果たし、ステークホルダーからの信頼を得るためには、それらの情報を適切に開示することも重要な視点となっています。

サイバーセキュリティ対策は、事業継続を脅かすリスクの1つ

投資効果（費用対効果）を認識する

サイバーセキュリティ対策にかかる費用の項目

サイバー攻撃に対するセキュリティ対策には、次のような項目があります。これらの項目を実現するためには、当然費用が発生します。

人的対策

・セキュリティポリシー
・各種社内規定、マニュアル
・社員の教育・訓練
・アクセス管理

組織的（管理的）対策

・管理組織の設置・運用
・情報資産の分類・持ち出し管理
・サイバー攻撃対応マニュアルの作成
・事業継続管理

物理的対策

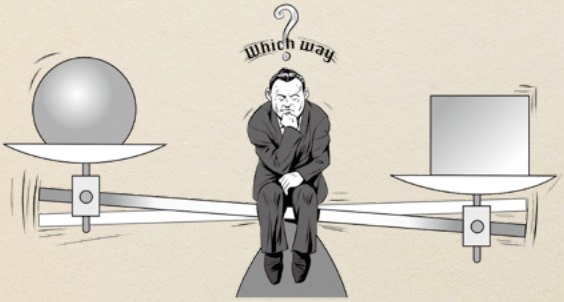
・コンピューターや通信装置の保護
・重要情報の一元管理／入退室管理
・アクセスできる区域の制限
・クリアデスク／クリアスクリーン

技術的対策

・本人認証・アクセス制御／権限管理
・ウイルス対策
・脆弱性対策
・暗号技術／認証技術の利用
・ファイアウォールやコンテンツフィルター

POINT 2 セキュリティ対策の投資効果を考える

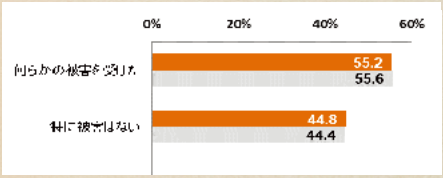
あなたの会社のインターネット接続と業務システムが1週間停止した場合のビジネスへの影響度を考えたことがありますか？　当然その間はメールもやり取りできないため、営業機会はなくなります。また、この時代にメールも送受信できないということで取引先との信頼関係もなくなります。それらの損失を数字に置き換えたものがセキュリティ対策の投資効果です。



コラム セキュリティ対策は経営上の「投資」と位置付ける！

IDC Japanが2020年1月に実施した国内企業878社の情報セキュリティ対策の実態調査結果によると、2020年度の情報セキュリティ投資見込みについて38%の企業が2019年度を上回ると回答しています。総務省「通信利用動向調査（令和元年）」においても55.2%の企業が「何らかの被害を受けた」と回答。対策には相応のコストが必要なものの、近年は中小企業を含むサプライチェーンを狙った攻撃も増えています。こうした観点も鑑み、やむを得ない「経費」でなく、ITを利活用した積極的な経営への「投資」と位置付けることが重要です。

情報通信ネットワークの利用の際に発生した過去1年間のセキュリティ状況の被害



引用：総務省「通信利用動向調査（令和元年）」より

自社のIT活用・セキュリティ対策状況を自己診断する

ITの活用診断

自社のIT活用状況を診断する

IT化において中小企業が注意したいのは、「IT化の範囲を一気に広げ過ぎない」という点です。中小企業が短期間であらゆる業務にITを導入しようとすると、コストの増大だけでなく、スケジュールが煩雑になり結果的に中途半端なクオリティーのシステムになるリスクがあります。下記の診断ツールが利用できます。

IT活用診断ツール

中小企業基盤整備機構：IT経営簡易診断
情報処理推進機構：DX推進指標

IT活用診断のカギは費用対効果

IT導入の目的は、既存ビジネスの効率化や新ビジネス展開などであり、IT化のための投資が、それによって得られる利益を上回っている場合は、投資を削減すべきです（参考「ITガバナンス」P99参照）。

IT化による想定利益＞IT化投資額
（IT導入、運用、セキュリティ対策費）

ITおよびサイバーセキュリティに関する組織の視点6分類

【理想的】

【分類1】ITの利活用を事業戦略上に位置付け、サイバーセキュリティを強く意識し、積極的にITによる革新と高いレベルのセキュリティに挑戦する企業

【もっと積極的】

【分類2】IT・サイバーセキュリティの重要性は理解しているものの、積極的な事業戦略に組み込むところまでは位置付けていない企業

【無駄な投資】

【分類3】過剰なセキュリティ意識により、ITの利活用を著しく制限し、競争力強化に活用させていない企業

【危険】

【分類4】サイバーセキュリティ対策の必要性は理解しているが、必要十分なセキュリティ対策ができていないにもかかわらず、ITの利活用を進めている企業

【分類5】サイバーセキュリティの必要性を理解していない企業や、自らセキュリティ対策を行う上で事業上のリソースの制約が大きい企業

【対象外】

【分類6】ITを利用していない企業

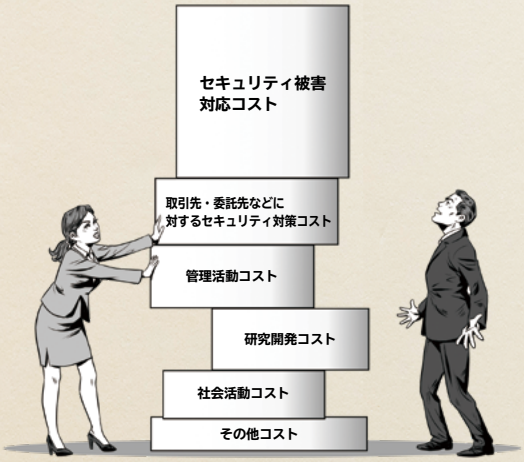
MISSION 3-6

自社のIT活用・セキュリティ対策状況を自己診断する

サイバーセキュリティ投資診断

POINT 1 サイバーセキュリティ投資（コスト）とは

サイバーセキュリティの投資（コスト）としては、P94に示した対策費用以外にも、さまざまなコストがあります。



POINT 2 サイバーセキュリティ対策はどこまでやればよいのか

これで万全というサイバーセキュリティはありません。特に、技術的対策にどれだけ投資してもリスクは残ります。管理的対策や人的対策を優先する方が効果的です。想定被害額を上回るセキュリティ対策費を費やすことは現実的では

ありません。セキュリティ対策費が、セキュリティ侵害による想定被害額を上回っている場合は、対策費を削減すべきです。

セキュリティ侵害による想定被害額（経済的損失、社会的信用）	＞	**セキュリティ対策費**

問題は残ったリスク（残留リスク）によって発生した被害の想定被害額が、支出可能な対策費を上回っている場合は、事業継続が困難になりますので、支出可能な対策費に収まるように残留リスクを下げる対策を講じるか、支出可能な対策費を捻出する必要があります。

セキュリティ侵害発生時に支出可能な対策費	＞	**残留リスクによる想定被害額**

残留リスクをどこまで許容できるかは、まさに経営者の判断です。

コラム「ITガバナンス」と6つの原則

IT活用は今や企業戦略の中で不可欠となっています。この観点から経営層には組織価値を高め、ITシステム戦略の策定や運用に必要となる組織能力である「ITガバナンス」が求められています。その成功には、経営層が次の6原則を実践することが肝要とされています。以下、要約して紹介します。

1. **責任**：役割に責任を負う人は、その遂行権限を持つ
2. **戦略**：情報システム戦略は現在と将来を考慮して、そのニーズを満たす必要がある
3. **取得**：情報システムの導入は短期・長期の両面で効果・リスク・資源のバランスを考慮した意思決定に基づく必要がある
4. **パフォーマンス**：情報システムは現在および将来のニーズを満たす必要がある
5. **適合**：情報システムは関連する全ての法律および規制に適合する必要がある
6. **人間行動**：情報システムのパフォーマンス維持に関わる人間行動を尊重する必要がある

参考：経済産業省「システム管理基準」
https://www.meti.go.jp/policy/netsecurity/downloadfiles/system_kanri_h30.pdf

自社のIT活用・セキュリティ対策状況を自己診断する

情報セキュリティ対策診断

情報セキュリティ対策を診断する

企業（組織）はセキュリティ上の脅威に取り囲まれています。

・個人、顧客、企業（組織）情報を脅威から守る

・会社内の設備を脅威から守る

情報セキュリティ対策は常に新たな脅威に対応する必要があり、継続的に自社の対策状況を診断する必要があります。

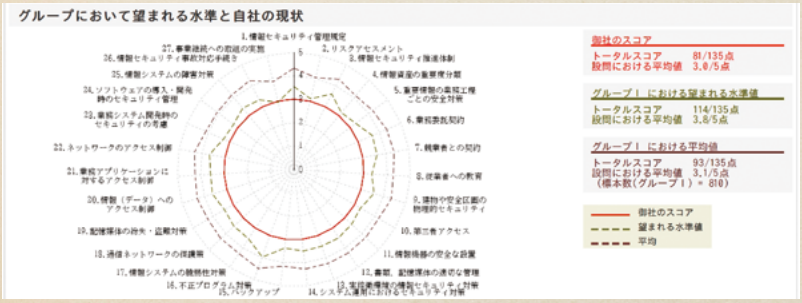
POINT 2 やってみよう！ 情報セキュリティ対策診断

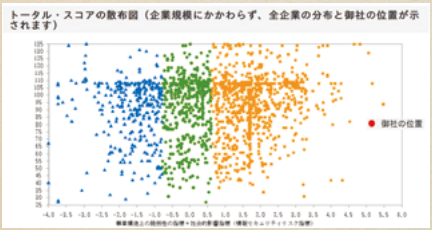
・わが社のセキュリティ対策は大丈夫か？
・セキュリティ対策予算を増額したいが、どこにどう使ったらいいのか分からない
・まだ取り組んでいないセキュリティ対策を考えたい
・自社の情報セキュリティ対策状況はどこが弱点で、どこが強いのか知りたい

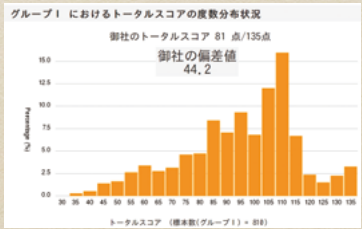
こうした要望に応えて、情報処理推進機構（IPA）では、「情報セキュリティ対策ベンチマーク」を提供しています。

情報セキュリティ対策ベンチマークは、設問に答えるだけで、自社のセキュリティレベルを他社との比較で診断することのできるシステムです。

散布図、レーダーチャート、スコア（点数）などの診断結果が自動的に表示されます。







「情報セキュリティ対策ベンチマーク」（IPA）より転載（一部加工）

MISSION 3-8

ビジネスを継続するために（守りのIT投資とサイバーセキュリティ対策）

業務の効率化、サービスの維持のために

POINT 1 守りのIT投資と攻めのIT投資

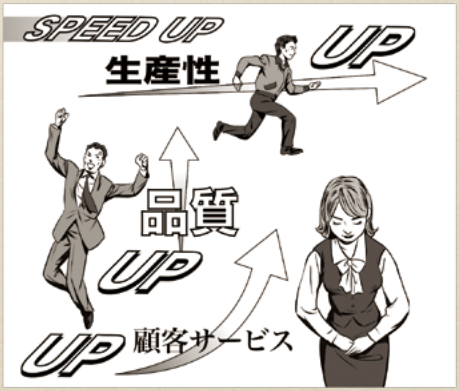
守りのIT投資という言葉を聞いたことがありますか。
従来、IT活用は業務効率化やコスト削減を目的として、定型業務の自動化に集中していました。近年、売り上げ増加を目指したIT投資を「攻めのIT投資」と呼ぶようになり、従来のIT投資を「守りのIT投資」と呼んでいます。

POINT 2 業務の効率化にITを活用

経営者のみなさんが重視している経営課題の1つは、業務効率化やコスト削減です。
改善活動による業務効率化という手法は以前から展開されています。IT活用は、受発注業務や経理業務など、定型・繰り返しが多い業務プロセスを自動化、簡便化することに適しています。

POINT 3 生産性の向上やサービス向上のためにITを活用

ITを活用すれば、コスト削減だけでなく、業務のスピードアップ、品質向上、ミス低減など、生産性の向上にもつながります。また、生産状況の見える化などを通して、工程管理や生産管理など生産性を大幅に向上することも可能です。また、顧客サービスのスピードアップなどを通して、サービス力の向上にもつながります。



MISSION 3-9

経営者が認識すべきサイバーセキュリティ経営3原則

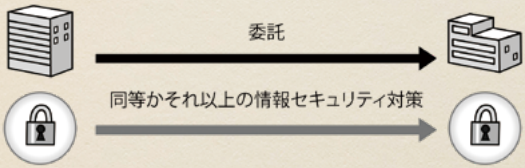
原則1　サイバーセキュリティ対策は経営者のリーダーシップで進める

サイバー攻撃のリスクをどの程度容認するのか、セキュリティ投資をどこまでやるのか、経営者が決めなければサイバーセキュリティ対策はスタートしません。

従業員は安心して業務に集中できる環境を求めますが、利便性が低下し、面倒な作業を伴う対策には積極的に取り組めないこともあります。経営者が自らリーダーシップを発揮しなければ、サイバーセキュリティ対策は進みません。

原則2 委託先のサイバーセキュリティ対策を把握する

子会社で情報漏えいが発生した場合はもちろんのこと、外部委託先に提供した情報がサイバー攻撃により流出してしまうことも経営にとっては大きなリスク要因です。
自社のみならず、系列企業やサプライチェーンのビジネスパートナー、委託先などのサイバーセキュリティ対策に関しても、必要に応じてサイバーセキュリティ対策の報告を求め、不十分な場合は対処を要請します。



原則3 関係者とのサイバーセキュリティに関するコミュニケーションはどんなときにも怠らない

顧客、取引先、委託先、代理店、利用者、株主などからの信頼を高めるには、普段からサイバーセキュリティ対策についての情報開示に努め、関係者との適切なコミュニケーションを図ることが必要です。

ビジネスを継続するために（守りのIT投資とサイバーセキュリティ対策）

経営者がやらなければならない サイバーセキュリティ経営の重要10項目

経済産業省と情報処理推進機構（IPA）がまとめた「サイバーセキュリティ経営ガイドライン Ver 2.0」を基に、経営者が情報セキュリティ全般を統括する「最高情報セキュリティ責任者（CISO）」に指示すべき重要10項目をまとめました。

重要10項目とは

経営者がリーダーシップをとったセキュリティ対策の推進			
	サイバーセキュリティリスクの管理体制構築	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
		2	サイバーセキュリティリスク管理体制の構築
		3	サイバーセキュリティ対策のための資源（予算、人材等）確保
	サイバーセキュリティリスクの特定と対策の実装	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
		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
		6	サイバーセキュリティ対策におけるPDCAサイクルの実施
	インシデント発生に備えた体制構築	7	インシデント発生時の緊急対応体制の整備
		8	インシデントによる被害に備えた復旧体制の整備
サプライチェーンセキュリティ対策の推進		9	ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握
ステークホルダーを含めた関係者とのコミュニケーションの推進		10	情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供

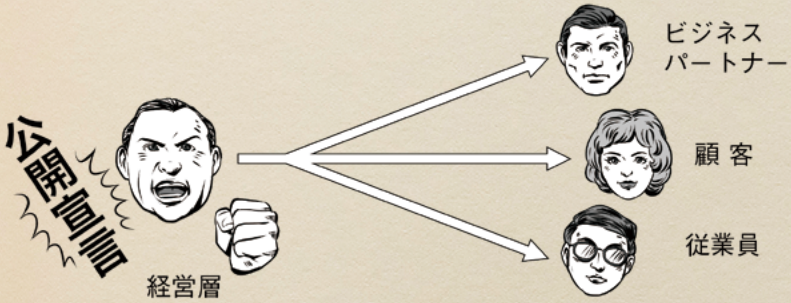
指示1 サイバーセキュリティリスクの認識、組織全体での対応方針の策定

POINT 1 指示すべきことはこれだ

・サイバーセキュリティリスクを経営リスクの1つとして認識し、組織全体での対応方針（セキュリティポリシー）を策定させる

POINT 2 やるべきことはこれだ

・組織全体の対応方針を組織の内外に宣言できるよう、セキュリティポリシーを策定
・セキュリティポリシーを従業員へ周知徹底
・セキュリティポリシーを一般公開することでステークホルダーや社会に対する企業としての姿勢を示す



指示2	サイバーセキュリティリスク管理体制の構築

POINT 1 指示すべきことはこれだ

・サイバーセキュリティ対策を行うため、サイバーセキュリティリスクの管理体制（各関係者の責任の明確化も含む）を構築させる

POINT 2 やるべきことはこれだ

・CISOは、責任範囲を明確にしたサイバーセキュリティリスク管理体制を構築
・取締役、監査役はサイバーセキュリティリスク管理体制を監査
・セキュリティ・バイ・デザインの観点を踏まえて体制を構築
・経営者のリーダーシップの下で体制を構築

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

POINT 1 指示すべきことはこれだ

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

POINT 2 やるべきことはこれだ

・サイバーセキュリティ対策に必要な費用の確保
・セキュリティ対策に必要な人材の確保
・セキュリティ人材育成、キャリアパスを設計検討
・外部の組織が提供するセキュリティ研修等の活用を検討
・各部門においてもセキュリティを意識した業務遂行ができるようにする

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

POINT 1 指示すべきことはこれだ

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

POINT 2 やるべきことはこれだ

・経営戦略の観点から守るべき情報を特定し把握
・守るべき情報に対して、発生しうるサイバーセキュリティリスクを把握
・把握したリスクに対して、実施するサイバーセキュリティ対策を検討（リスクの低減策、回避策、移転策）
・実施できない場合は、残留リスクとしての識別も
・法令上の取り扱いも考慮したリスクの特定と緊急時の情報の保護が行えるような対策も検討
・製品・サービス等においても、セキュリティ・バイ・デザインの観点を踏まえて、対策を考慮

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

POINT 1 指示すべきことはこれだ

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

POINT 2 やるべきことはこれだ

・重要業務を行う端末、ネットワーク、システムまたはサービス（クラウドサービスを含む）には、多層防御を実施
・アクセスログや通信ログ等からサイバー攻撃を監視・検知する仕組みを構築
・従業員に対する教育を行い、適切な対応が行えるよう日頃から備える
・製品・サービス等においても、セキュリティバイデザインの観点を踏まえて、企画・設計段階からサイバーセキュリティ対策を考慮

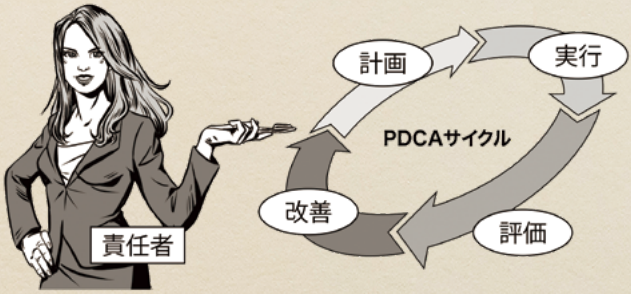
指示6	サイバーセキュリティ対策における PDCAサイクルの実施

POINT 1 指示すべきことはこれだ

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

POINT 2 やるべきことはこれだ

・サイバーセキュリティリスクに継続して対応可能な体制（プロセス）を整備する（PDCAの実施体制の整備）
・サイバーセキュリティリスク管理に関するKPIを定め、組織内の経営リスクに関する委員会においてその状況を経営者に報告する
・新たなサイバーセキュリティリスクの発見等により、追加的に対応が必要な場合には、速やかに対処方針を修正する
・サイバーセキュリティ対策の状況について、情報セキュリティ報告書、CSR報告書等への記載を通じて開示を検討する



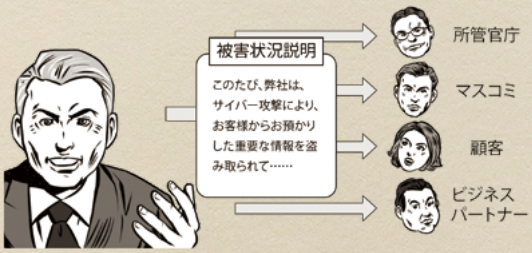
指示7 インシデント発生時の緊急対応体制の整備

POINT 1 指示すべきことはこれだ

・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の組織内の対応体制（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できる体制を整備させる

POINT 2 やるべきことはこれだ

・緊急時において、以下を実施できるような対応体制を構築する
・サイバー攻撃による被害を受けた場合、速やかな各種ログの保全や感染端末の確保等の証拠保全が行える体制を構築する
・インシデント収束後の再発防止策の策定、所管省庁等への報告手順も含めて演習を行う
・緊急連絡網として社外を含む情報開示の通知先一覧を整備し、対応に従事するメンバーに共有しておく
・緊急時に組織内各部署が速やかに協力できるよう予め取り決めをしておく
・関係法令を確認し、法的義務が履行されるよう手続きを確認しておく
・インシデントに関する被害状況、他社への影響等について経営者に報告する



指示8 インシデントによる被害に備えた復旧体制の整備

POINT 1 指示すべきことはこれだ

・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
・BCPとの連携等、組織全体として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、適宜実践的な演習を実施させる

POINT 2 やるべきことはこれだ

・業務停止等に至った場合に、以下を実施できるような復旧体制を構築する
・サイバー攻撃により業務停止に至った場合、関係機関との連携や復旧作業を実施できるよう指示する。また、対応担当者には復旧手順に従った演習を実施させる
・演習内容や組織の関係者の役割を踏まえて検討することが望ましい
・重要な業務をいつまでに復旧すべきかの目標について、組織全体として整合をとる（例えばBCPで定めている目標との整合等）

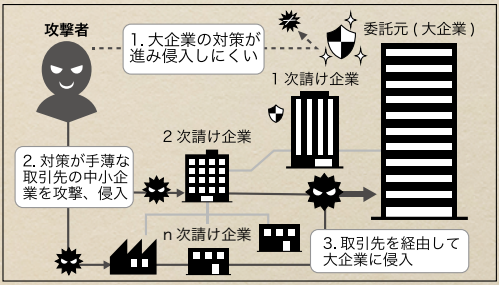
指示9 ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握

POINT 1 指示すべきことはこれだ

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

POINT 2 やるべきことはこれだ

・系列企業やサプライチェーンのビジネスパートナーやシステム管理の委託先等のサイバーセキュリティ対策の内容を明確にした上で契約を交わす
・個人情報や技術情報等の重要な情報を委託先に預ける場合は、情報の安全性の確保が可能であるかどうかを定期的に確認する
・系列企業、サプライチェーンのビジネスパートナーやシステム管理の委託先等がSECURITY_ACTIONを実施していることを確認する
・緊急時に備え、委託先がサイバー保険に加入していることが望ましい



出典：日経コンピュータ 2018年9月27日号より、一部を改変して作成

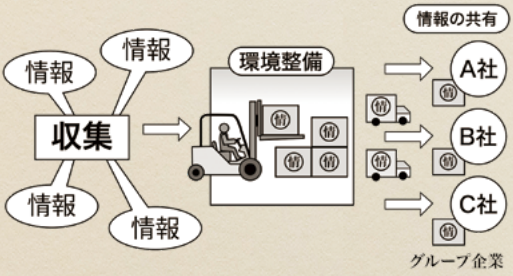
指示10　情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供

POINT 1 指示すべきことはこれだ

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

POINT 2 やるべきことはこれだ

・情報共有を通じたサイバー攻撃の防御につなげていくため、情報を入手するのみならず、積極的に情報を提供する
・IPAやJPCERT/CC等による脆弱性情報などの注意喚起情報を、自社のサイバーセキュリティ対策に生かす
・CSIRT間における情報共有や、日本シーサート協議会等のコミュニティ活動への参加による情報収集
・IPAに対し、告示（コンピュータウイルス対策基準、コンピュータ不正アクセス対策基準）に基づいてウイルス情報や不正アクセス情報の届出をする
・JPCERT/CCにインシデントに関する情報提供を行い、必要に応じて調整を依頼する



◆開示・報告先における注意点

開示・報告先	開示・報告時の留意点
所管官庁	・事前に先方の窓口を確認し、誰が報告するか決めておく
サイバーセキュリティ関係機関（IPA、JPCERT/CC）	・サイバー攻撃の内容、実施していた対策、被害の概要などを報告する ・同種の攻撃手法による二次被害を避けるため、至急報告する
報道機関／マスメディア	・窓口を一本化し、対外的な情報に不整合が起こらないようにする ・世評の影響も踏まえて、法務部門、広報部門などと連携し、適切な公表時期を慎重に判断する ・SNSなどのソーシャルメディアにより、社会的にどのように受け止められているか動向を確認する ・被害の状況に応じて、経営者が記者会見を行うことを想定し、公表する内容を検討する
顧客	・被害者に至急その事実を通知しおわびするとともに、個人情報（顧客情報）漏えいの場合は、詐欺や迷惑行為などの被害に遭わないように注意喚起する ・被害者に連絡する方法（メーリングリストで一斉送信など）を確認・整備しておく
ビジネスパートナー／同業者	・対処に必要な情報を速やかに関係者と共有する（外部委託先や、提携しているクレジットカード会社など） ・同業種を狙った一斉攻撃の可能性があるため、攻撃手法などを同業者間で共有する

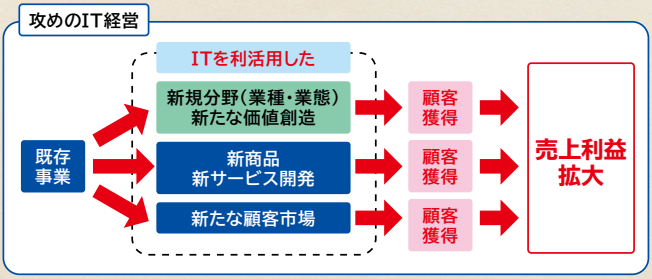
MISSION 3-11

ビジネスを発展させるために(攻めのIT投資とサイバーセキュリティ対策)

次世代技術を活用したビジネス展開

POINT 1 攻めのIT投資とは？

ITを活用して製品・サービス開発に取り組み、ビジネスモデルを変革することや新たな価値を創出することが「攻めのIT経営」です。柔軟かつ大企業に先駆けて IT関連の次世代技術やデジタル情報を活用していくことが中小企業の発展につながります。 デジタル情報や IT技術の進展を受け入れ、それを活用して顧客サービスの強化を図る企業に今大きなビジネスチャンスが訪れています。



「攻めのIT経営中小企業百選」(経済産業省)より

POINT 2 各種の支援策も充実

感染症対策や働き方改革の必要性が高まる中、テレワーク等の実現のためにデジタルツールに関心があっても、導入・定着に至らない中小企業に向けた支援も充実しています。その1つが「中小企業デジタル化応援隊事業」(2020年9月開始)。全国の中小企業とIT専門家をマッチングし、デジタル化・IT化を促進しています。

コラム DX推進はビジネス飛躍のチャンス

これから目指す社会は、「超スマート社会」いわゆる「Society5.0」

政府は、サイバー空間（仮想空間）とフィジカル空間（現実空間）を連携し、すべての物、情報、人を1つにつなぐ「サイバー・フィジカル・システム」（CPS）によって量と質の全体最適を図る社会像として「Society5.0」を提唱し、その考えが「デジタル社会の実現に向けた改革の基本方針」（2020年12月閣議決定）の背景となっています。IoTやビッグデータ、ロボット、AI、5Gなどの技術革新（いわゆる第4次産業革命）により、Society5.0は現実になりつつあります。

DXは、新たな技術を活用したビジネスの変革

新しいITおよびデジタル情報を活用して、ビジネスを変革させるのが「デジタルトランスフォーメーション（DX）」です。DXにより新時代に対応した新たなサービスを創造し、ビジネスを飛躍させることができます。

DX推進のためには、セキュリティも強化

一方、どんなに良いサービスを展開しても、セキュリティ侵害があっては事業が継続できません。ITシステム運用継続計画（IT-BCP）を明確にして、サービス設計の段階から十分なセキュリティ対策を考慮することが重要です。

中小企業のビジネスの拡大・発展に向けて

そのためには、ビジネス、デジタルのスキルとともに、セキュリティ対策のスキルを併せ持った人材が必要です。DXに対応した新たなビジネスの拡大・発展のためには、経営者は、業務や組織、企業風土の変革を含めて、明確なビジョンを持ち、「攻めのIT投資」を牽引する強いリーダーシップが求められます。

引用：内閣府「Society5.0」より

MISSION 3-12

ビジネスを発展させるために(攻めのIT投資とサイバーセキュリティ対策)

IoT、ビッグデータ、AI、ロボットの活用

POINT 1 業務・サービスの効率性を追求

あらゆる機器がインターネットに接続することで、人が行ってきたことをセンサー化し、センサーからの膨大なデータを瞬時に分析できます。その結果を踏まえて業務やサービスを効率的、効果的に行うことが始まっています。IoT(Internet of Things／モノのインターネット)※、ビッグデータ※、AI(Artificial Intelligence／人工知能)※、ロボットの活用は、人手不足に対応した省力化や、自動化のための投資という面でも期待されています。

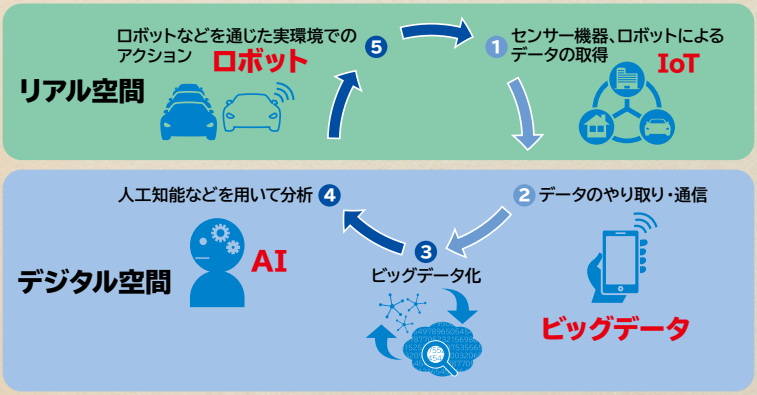
※ IoT、ビッグデータはP122を、AIはP124を参照

コラム IoT、ビッグデータ、AI、ロボットはつながっている

IoT、ビッグデータ、人工知能（AI）、ロボットなどの技術革新によって社会のあらゆる活動、情報がデータ化され、ネットワークによってつながることが可能な時代になりました。これらを組み合わせた機器やサービスが普及するとともに利活用を実現する事例が増えています。リアルタイムに分析を行い、新たなサービスや製品を生み出すことが可能になると、データそのものが創造の源泉になります。

商品やサービスの提供は個々のニーズに合わせてカスタマイズされ、個々のニーズとの効率的なマッチングが可能になります。AIやロボットはますます人間の役割をサポートし、部分的に代替するようになります。こうした状況にどう対応するかは、事業者にとっても重要なテーマです。商品・サービスの開発や生産、さらには流通、アフターサービスなど、事業活動に上手に取り込むことができれば、将来の成長の大きな助けになります。

急速な技術革新により、大量データの取得、分析、実行の循環が可能に



出典：「IoT、AI、ロボットに関する経済産業省の施策について」（経済産業省）より

MISSION 3-13

IoTが果たす役割と効果

POINT 1 IoTは中小企業にとって大きなビジネスチャンス

「5G」に代表される次世代通信技術などによってIoTデバイスは急速に普及し、2024年には10兆円を超える国内市場となる予測もあります。さらに政府が目指す「Society5.0」実現に向けた動きも追い風となり、ビジネスシーンにおいては、IoTがもたらすビッグデータ（蓄積された膨大なデータ）が新たな価値を見いだす資源として注目されています。中小企業にとっても、IoTは、例えば医療・介護、物流、製造業、交通、農業などさまざまな分野での活用が期待でき、大きなビジネスチャンスになるのです。

コラム 中堅・中小企業のIoT活用事例

製造業（東京都墨田区）社員数：50名
各種装置・機械の設計開発等

3DCADをクラウド環境で離れたところから利用可能に

事例ポイント

専門ソフトウェアの導入によって一般的なノートPCで、社内のハイスペックPCを高性能のままにリモート操作可能とした。客先や工場内など遠隔地のどこからでも社内の３DCADソフトをシームレスに利用して設計データの確認や修正が実現できる環境を構築した。

概要

・当該企業は板金加工を中心とした金属加工による部品製造や機械装置設計開発業務に従事。設計開発では3DCAD等のソフトウェアを利用。一般的なオフィスソフトを動作させるPCスペックでは足りずハイスペックな環境が必要であり、場所も設計者の机に限定されている
・設計に関して客先での打ち合わせや工場内確認を行う場合、3DCADのデータ参照が必要であり、設計者の机以外の場所で利用することができない。3DCADデータをプリントアウトした紙媒体を多く用いていた。修正や改編の度に紙とCADを行き来しなければならず膨大な手間が発生していた。修正ミスが起こる可能性も高い状況にあった

効果・メリット

客先や工場内など遠隔地のどこからでも社内の3DCADソフトを利用して設計データの確認や修正を迅速に反映。情報セキュリティ面から見ても、データそのものや紙媒体を持ち運ぶ必要がなくなり、情報漏えいのリスクを最小限に抑えた形で外部での設計対応が可能に。

「中堅・中小製造業のIoT活用事例一覧」（ロボット革命・産業IoTイニシアティブ協議会）より抜粋・要約して作成

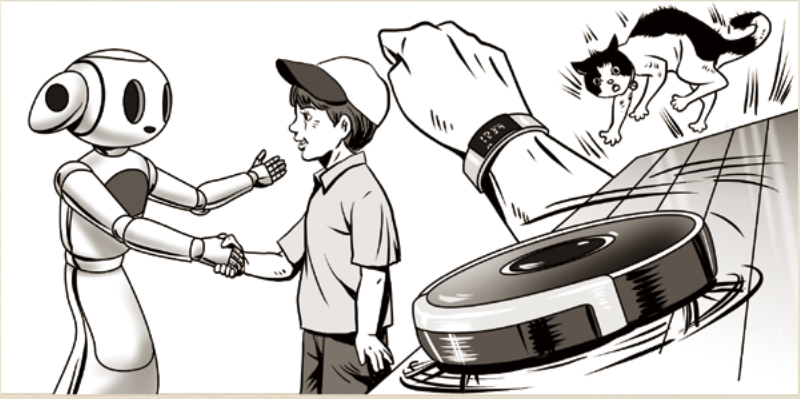
MISSION 3-14

ビジネスを発展させるために(攻めのIT投資とサイバーセキュリティ対策)

人工知能(AI)が果たす役割と効果

POINT 1 急速に進化するAIを活用しよう

インターネットの検索エンジン、スマートフォンの音声検索アプリや音声入力機能、掃除ロボットなどの家電製品、さらに人型ロボットにも人工知能（AI）が搭載されています。身近となったAIを企業経営に活用することによって、経営上のさまざまな課題を解決するのみならず、新しい価値をも生み出します。例えば、大手調査機関では、日本においては2035年にAIによる労働生産性がベースラインで34%向上するという分析も行われています。



コラム 新しい価値を持った業務の創出

AIを含むICTの進化は雇用と働き方にも影響を及ぼします。

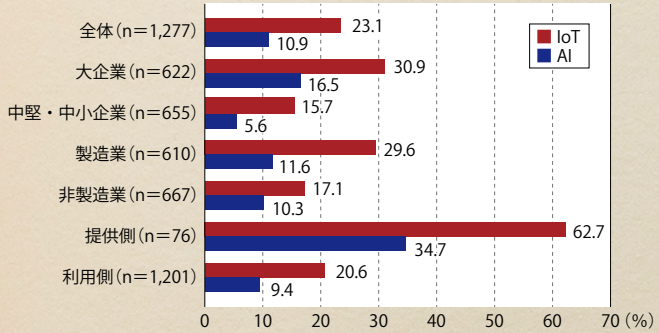
・既存業務の人材不足の解消
・不足している労働力の補完・省力化
・既存の業務効率・生産性の向上（省力化）
・新しい価値を持った業務の創出

などが期待されています。

＜AIの進化で予想されること＞

・労働力不足や過酷労働などの緩和
・農業・漁業の自動化による人手不足問題の緩和
・犯罪の発生予知、事故の未然防止
・個々人の必要に応じたきめ細かいサービスの提供
・医療データの活用などによる課題解決
・職人の知識、ノウハウの体系化による維持と伝承

国内のAIとIoT活用状況



出典：財務省「最先端技術（IoT、AI等）の活用状況」（平成30年11月）を参考に作成

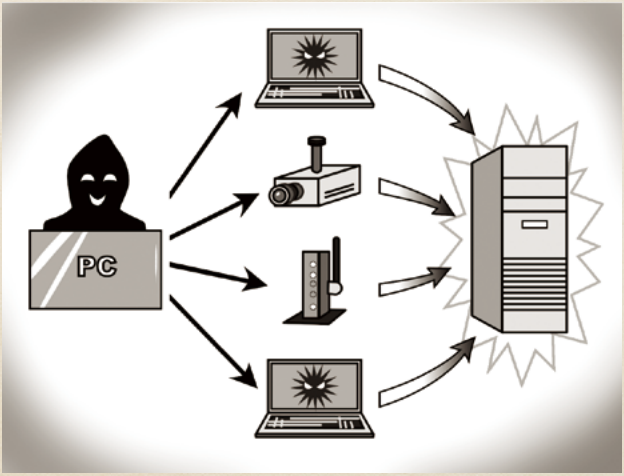
MISSION 3-15

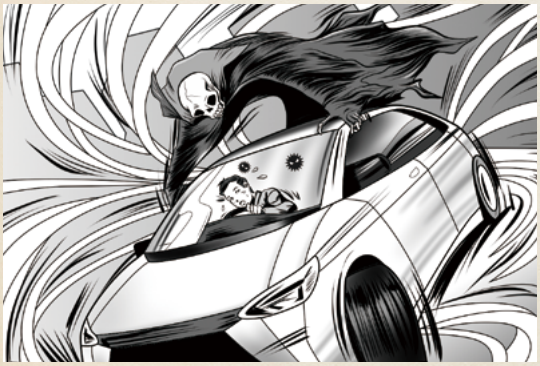
ビジネスを発展させるために(攻めのIT投資とサイバーセキュリティ対策)

IoTを活用する際のサイバーセキュリティ上の留意点

POINT 1 IoTへの脅威

次世代通信技術である5Gの進歩などを背景に、これから飛躍的に活用場面の増加が予想されるIoT機器ですが、一方でセキュリティ対策が十分とはいえないのが現状です。また、5Gが社会浸透していく中では、これまで以上にさまざまなリスクが生まれ、脅威の在り方もさらに多様化・複雑化することが予想されます。そのため、IoT機器をターゲットとしたサイバー攻撃が増大することも懸念されています。利用する際には、それを前提とした対策が欠かせません。(対策はP128参照)





インターネットから自動車の脆弱性を突かれ、ハンドルやエンジンなどが遠隔操作される

ホテルの部屋に設置してある通信機器・設備が不正に遠隔操作される

ペースメーカーや植え込み型除細動器が不正操作される

ビジネスを発展させるために（攻めのIT投資とサイバーセキュリティ対策）

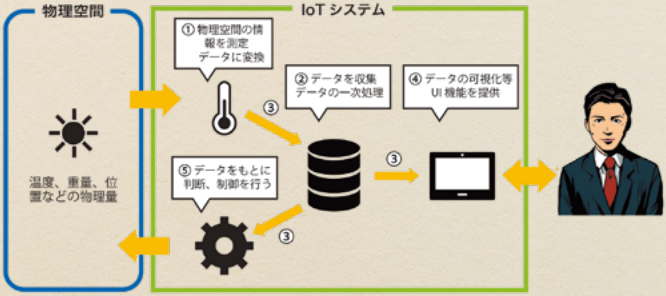
MISSION 3-16 IoTを活用するための基本ルール

POINT 1 IoTのセキュリティは製造サービス提供側とサービス利用者側の双方の意識が大切

製造業を中心にIoTを利活用する動きが加速しています。

IoT機器はインターネットに接続しているネットワーク機器の一種。そのためパソコンと同様にサイバー攻撃のリスクがありますが、セキュリティ面がなおざりにされているものもあります。それらを利用するとサイバー攻撃によってシステムが使えなくなる、あるいは第三者への攻撃の踏み台となるかもしれません。

IoTのセキュリティは、製造サービス提供側とサービス利用者側の双方が注意を払わなくてはならないのです。



出典：JPCERT/CC「IoTセキュリティチェックリスト利用説明書」（2019年6月）より作成

POINT 2

IoT機器やシステム、サービスの提供にあたっての指針

■ 指針1　IoTの性質を考慮した基本方針を定める

IoT機器が原因で情報流出や社会インフラの停止などが起こった場合は、IoT機器やシステム、サービスの提供側の経営責任が問われることもあります。リスクを認識し、内部不正やミスに備えることが必要です。

■ 指針2　IoTのリスクを認識する

他の機器とつながることで、影響が広範囲になるリスクを想定することが大切です。不正操作や、廃棄機器からの情報漏えいリスクも考慮します。

■ 指針3　守るべきものを守る設計を考える

つながる相手や状況に応じてつなぎ方を判断できる設計を検討しましょう。安全安心を実現するために設計が妥当かどうかの評価も必要です。

■ 指針4　ネットワーク上での対策を考える

セキュアなゲートウェイを利用するなど、ネットワーク構成やセキュリティ機能の検討を行いましょう。初期設定もセキュリティに留意し、利用者にも注意喚起を行います。

■ 指針5　安全安心な状態を維持し、情報発信・共有を行う

出荷・リリース後も安全安心な状態を維持できるようソフトウェアをアップデートする手段を確保します。脆弱性について情報発信し、セキュリティに関する重要事項はユーザーへあらかじめ説明しましょう。

参考：IoT推進コンソーシアム「IoTセキュリティガイドラインver1.0」（平成28年7月）より

POINT 3 IoT機器の一般利用者のためのルール

ルール1 問い合わせ窓口やサポートのない機器やサービスの購入・利用を控える

機器やサービスの問い合わせ窓口やサポートがない場合は、不都合が生じたとしても、適切に対処することが困難になります。サービスの購入・利用は控えましょう。

ルール2 初期設定に気を付ける

機器を初めて使用する際には、IDやパスワードの設定を適切に行います。パスワードの設定では、「機器購入時のパスワードを必ず変更する」「他の人とパスワードを共有しない」「他のパスワードを使い回さない」「不要なサービスや機能は有効化しない」に気を付けましょう。また、取扱説明書などの手順に従って、自分でアップデートを実施しましょう。

ルール3 使用しなくなった機器については電源を切る

使用しなくなった機器や不具合が生じた機器をインターネットに接続したまま放置すると、不正利用されるおそれがあります。使用しなくなったWebカメラやルーターなどをそのまま放置せず、電源プラグを抜きましょう。

ルール4 使用しなくなった機器は必ずデータを消す

情報が他の人に漏れることのないよう、機器廃棄・下取りなどのときは、事前にデータを削除しましょう。

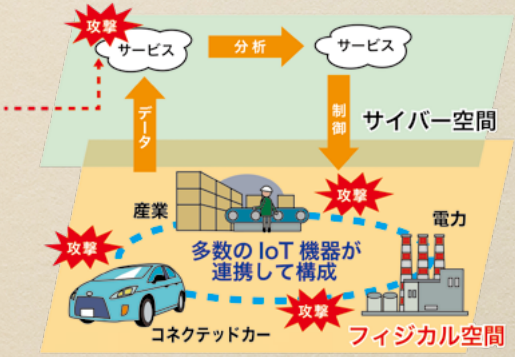
参考：「IoTセキュリティガイドライン」（総務省 経済産業省 平成28 年7月）より

POINT 4 Society5.0とIoT

Society5.0が目指す社会では、IoTによってPCやスマートフォンだけでなく家電製品や車、建物などあらゆるモノがサイバー（仮想）空間とフィジカル（現実）空間で融合されます。このため、IoT機器へのサイバー攻撃が成功すると、フィジカル空間にも影響を与える可能性が高まります。

例えば、IoT製品などに感染するウイルス「Mirai」によりWebサイトが大規模なサイバー攻撃を受けました。さらに重要インフラや生産設備への攻撃による大規模な被害も発生しています。

IoT製品をはじめ、インターネット接続される多様な機器に適切なセキュリティ対策が行われず、インターネット上に晒されアクセス可能な状態にある製品を監視し被害を防止するために、「NOTICE（National Operation Towards IoT Clean Environment）」が行われています（P47参照）。これはサイバー攻撃に悪用されるおそれのあるIoT機器の調査および当該機器の利用者への注意喚起を行うもので、総務省、国立研究開発法人情報通信研究機構（NICT）および一般社団法人ICT-ISAC が主体となって実施されています。



出典：内閣府「IoT社会に対応したサイバー・フィジカル・セキュリティ『サイバー・フィジカル・セキュリティ対策基盤』の研究開発」より作成

MEMO

TOP SECRET

MISSION 4

もしもマニュアル

緊急時対応用マニュアルの作成

サイバー攻撃を受けたときのために、あらかじめ緊急時対応用マニュアルを作成しておきましょう。

作成に当たっては、情報処理推進機構（IPA）が中小企業・小規模事業者向けに提供している「中小企業の情報セキュリティ対策ガイドライン第3版」付録5の「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」を参考にすれば、自社に合った情報セキュリティポリシーを簡単に作成することができます。

緊急時対応用マニュアルは定期的に見直すことも必要です。

POINT 1 マニュアルに記載すべき事項

緊急時対応用マニュアルには次の項目を記載します。

記載すべき項目	記載すべき内容	本書の参照ページ
対応体制	一次対応者、対応責任者、最高責任者を決めます。	P136
サイバー攻撃被害の影響範囲と対応者	サイバー攻撃が発生した場合に対応策を決めるため、サイバー攻撃被害の影響範囲のレベルと対応者を決めます。	P136

記載すべき項目	記載すべき内容	本書の参照ページ
サイバー攻撃被害の連絡および報告体制	サイバー攻撃が発生した場合の連絡・報告手順を決めます。	P137
対応手順	サイバー攻撃被害の内容ごとに、影響範囲のレベルごとの対応手順を決めます。	P137
漏えい・流出発生時の対応	社外秘または極秘情報資産の盗難、流出、紛失の場合の対応を決めます。	P138
改ざん・消失・破壊・サービス停止発生時の対応	情報資産の意図しない改ざん、消失、破壊や情報資産が必要なときに利用できない場合の対応を決めます。	P140
ウイルス感染時の初期対応	悪意のあるソフトウェアに感染した場合の対応を決めます。	P143
届け出および相談 ＜届け出・相談先＞	サイバー攻撃被害対応後に届け出または相談する機関を検討しておきます。	P145
大規模災害などによる事業中断と事業継続管理	大規模災害などの影響により事業が中断した場合に備えて、対応策を決めておきます。	P146

基本事項の決定

対応体制を決める

サイバー攻撃を受けたときに会社として対応する体制を決めます。
対応体制として一次対応者、対応責任者、最高責任者を決めます。

最高責任者	代表取締役
対応責任者	サイバー攻撃対応責任者
一次対応者	発見者または情報システム管理者

サイバー攻撃被害の影響範囲と対応者を決める

サイバー攻撃被害の影響範囲のレベルと対応者を決めます。サイバー攻撃被害が発生した場合、被害レベルを判断して対応を決めます。

被害レベル	影響範囲	対応者
3	顧客、取引先、株主などに影響が及ぶとき 個人情報が漏えいしたとき	最高責任者
2	事業に影響が及ぶとき	対応責任者
1	従業員の業務遂行に影響が及ぶとき	情報システム管理者
0	影響はないが、将来においてサイバー攻撃が発生する可能性がある事象が発見されたとき	情報システム管理者

ACTION 3 サイバー攻撃被害の連絡および報告体制を決める

サイバー攻撃が発生した場合の連絡・報告手順を決めます。

レベル1以上の被害が発生した場合、発見者は以下の連絡網に従い、対応者に速やかに報告し、指示を仰ぐ。

被害レベル	最終対応者	緊急連絡先
3	最高責任者	携帯電話：090-****-**** メールアドレス：president@*****.co.jp
2	対応責任者	携帯電話：090-****-**** メールアドレス：incident@*****.co.jp
1	情報システム管理者	携帯電話：090-****-**** メールアドレス：system@*****.co.jp

ACTION 4 対応手順を決める

サイバー攻撃を認知した際、確認事項や連絡系統を一元化し迅速な対応をするための対応手順を決めます。

区分	サイバー攻撃被害の状況
漏えい・流出	社外秘または極秘情報資産の盗難、流出、紛失
改ざん・消失・破壊 サービス停止	情報資産の意図しない改ざん、消失、破壊 情報資産が必要なときに利用できない
ウイルス感染	悪意のあるソフトウェアに感染

対応手順1

漏えい・流出発生時の対応

被害レベル3の場合

STEP1	発生の報告	漏えいや流出の事実を発見したり、外部から連絡を受けたりした者は即座に対応責任者および最高責任者に報告します。	発見者、一次対応者
STEP2	原因の特定と二次被害の防止	対応責任者は原因を特定するとともに、二次被害が想定される場合には防止策を実行します。	対応責任者
STEP3	被害者対応の準備	個人情報が流出した場合、漏えい・流出した個人情報の本人（被害者）への対応を準備します。	対応責任者
STEP4	問い合わせ対応の準備	被害者本人や関係先からの問い合わせ対応を準備します。	対応責任者
STEP5	報道発表の準備	対応責任者は影響範囲・被害の大きさによって総務部に報道発表の準備を申請します。	対応責任者

STEP6	被害届の提出	対応責任者はサイバー攻撃などの不正アクセスによる被害の場合は都道府県警察本部のサイバー犯罪相談窓口に届け出ます。	対応責任者
STEP7	監督官庁への届け出	対応責任者は個人情報の漏えいの場合には監督官庁に届け出ます。	対応責任者
	対応結果および対策を公表	最高責任者は、社内および影響範囲の全ての組織・人に対応結果および対策を公表します。	最高責任者

被害レベル2の場合

STEP1	発生の報告	発見者は発見次第、システム管理者に報告します。	発見者
STEP2	漏えい先の調査と報告	システム管理者は漏えい先を調査し、対応責任者に報告します。	システム管理者
STEP3	社内への通知	システム管理者は社内関係者に周知します。	システム管理者

対応手順2

改ざん・消失・破壊・サービス停止発生時の対応

被害レベル3の場合

STEP1	発生の報告	発見者は即座に対応責任者および最高責任者に報告します。	発見者
STEP2	原因の特定と応急措置の実施	システム管理者は原因を特定し、応急処置を実行します。	システム管理者
STEP3	社内周知と担当部署への連絡	対応責任者は社内に周知するとともに総務部情報システム担当に連絡します。	対応責任者
STEP4	復旧措置	電子データの場合はシステム管理者がバックアップによる復旧を実行します。	システム管理者
		機器の場合はシステム管理者が修理、復旧、交換などの手続きを行います。	システム管理者
		書類・フィルム原本の場合は情報セキュリティ部門責任者が可能な範囲で修復します。	情報セキュリティ部門責任者
STEP5	原因対策の実施	システム管理者は原因対策を実施します。	システム管理者
	対応結果および対策を公表	最高責任者は、社内および影響範囲の全ての組織・人に対応結果および対策を公表します。	最高責任者

ACTION 2 被害レベル2の場合

STEP1	発生の報告	発見者はシステム管理者に報告します。	発見者
STEP2	原因の特定と応急措置の実施	システム管理者は原因を特定し、応急処置を実行します。	システム管理者
STEP3	社内周知と担当部署への連絡	対応責任者は社内に周知するとともに総務部情報システム担当に連絡します。	対応責任者
STEP4	復旧措置	電子データの場合はシステム管理者がバックアップによる復旧を実行します。	システム管理者
		機器の場合はシステム管理者が修理、復旧、交換などの手続きを行います。	システム管理者
		書類・フィルム原本の場合は情報セキュリティ部門責任者が可能な範囲で修復します。	情報セキュリティ部門責任者
STEP5	原因対策の実施	システム管理者は原因対策を実施します。	システム管理者

ACTION 3 被害レベル1の場合

STEP1	発生の報告	発見者はシステム管理者に報告します。	発見者
STEP2	原因の特定と応急措置の実施	システム管理者は原因を特定し、応急処置を実行します。	システム管理者

STEP3	復旧措置	電子データの場合はシステム管理者がバックアップによる復旧もしくは再作成・入手を実行します。	システム管理者
		機器の場合はシステム管理者が修理、復旧、交換などの手続きを行います。	システム管理者
		書類・フィルム原本の場合は情報セキュリティ部門責任者が可能な範囲で修復します。	情報セキュリティ部門責任者
STEP4	原因対策の実施	システム管理者は原因対策を実施します。	システム管理者

ACTION 4 被害レベル0の場合

発見者は発見次第、発生可能性のあるサイバー攻撃と想定される被害をシステム管理者に報告

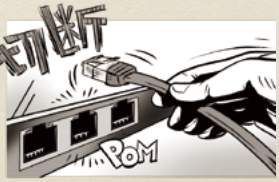
対応手順3

ウイルス感染時の初期対応

従業員が対応可能な場合

従業員は、業務に利用しているパソコン、サーバーまたはスマートフォン、タブレット（以下「コンピューター」といいます）がウイルスに感染した場合には、次の手順を実行します。

STEP1 ネットワークからコンピューターを切断します。



STEP2 システム管理者に連絡します。

STEP3 ウイルス対策ソフトの定義ファイルを最新版に更新します。

STEP4 ウイルス対策ソフトを実行しウイルス名を確認します。

STEP5 ウイルス対策ソフトで駆除可能な場合は駆除します。

STEP6 駆除後再度ウイルス対策ソフトでスキャンし、駆除を確認します。

STEP7 システム管理者に報告します。

ACTION 2 従業員が対応できない場合

従業員自身で対応できないと判断する場合はシステム管理者に問い合わせます。

・ウイルス対策ソフトで駆除できない
・システムファイルが破壊・改ざんされている
・ファイルが改ざん・暗号化・削除されている

対応手順4

届け出および相談

システム管理者は、サイバー攻撃被害への対応後に以下の機関への届け出または相談を検討します。

＜届け出・相談先＞

独立行政法人 情報処理推進機構セキュリティセンター（IPA/ISEC）

ウイルスにかかってしまったり、不正アクセスをされたりした場合は、下記URLを参照してにIPA/ISECに届け出をしてください。
https://www.ipa.go.jp/security/todokede/crack-virus/about.html

IPA/ISECでは、情報セキュリティの相談窓口も開設しています。
https://www.ipa.go.jp/security/anshin/about.html

個人情報保護委員会

個人情報や特定個人情報（マイナンバー）の漏えいなどの事案が発覚した場合は、速やかに下記URLを参照して個人情報保護委員会などに対して報告してください。
https://www.ppc.go.jp/

大規模災害などによる事業中断と事業継続管理

企業にとって、大規模な自然災害をはじめとする緊急事態に備えた事業継続のための計画（BCP）を策定することはとても重要です。

一方、情報システムの活用が進むこれからは、このBCPにプラスして情報システム運用継続計画（IT-BCP）も大切となってきています。

STEP1 環境整備

基本方針を決定し、実施・運用体制を構築する。

STEP2 情報の収集・前提の整理

危機的事象を特定し、特定した事象の顕在化がもたらす被害状況を想定する。

STEP3 分析、課題の抽出

情報システムの復旧優先度を設定し、運用継続に必要なリソースを整理する。

STEP4 計画の策定

事前対策計画、非常時の対応計画、教育訓練計画・維持改善計画を検討する。

STEP5 実施（評価・改善）

平常時にIT-BCPが発動されることはないため、定期的な訓練を通じて組織・個人における習熟度を維持し、計画に問題があれば見直しを図る。

※IT-BCPの策定には「情報システム部門」と「業務部門」等の関連部門間で適切な連携を図り、既存のBCPとの整合性を確保することが大切です
参考：IT-BCP 策定モデル（内閣官房情報セキュリティセンター（NISC））

TOP SECRET

MISSION 5

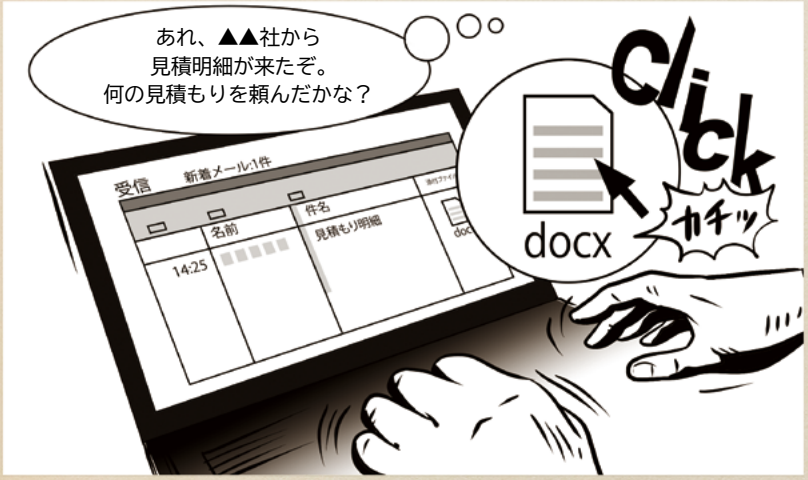
やってみよう! サイバー攻撃対策シミュレーション

SCENE 01

サイバー攻撃前夜

SCENE 02

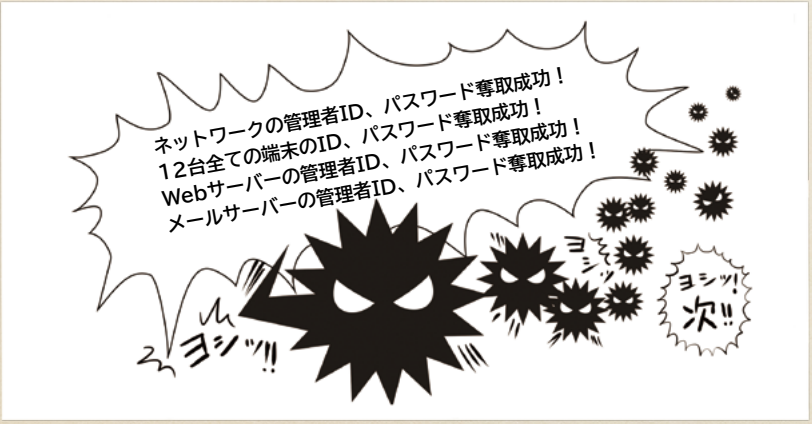
攻撃発生その瞬間



SCENE 03

サイバー攻撃直後

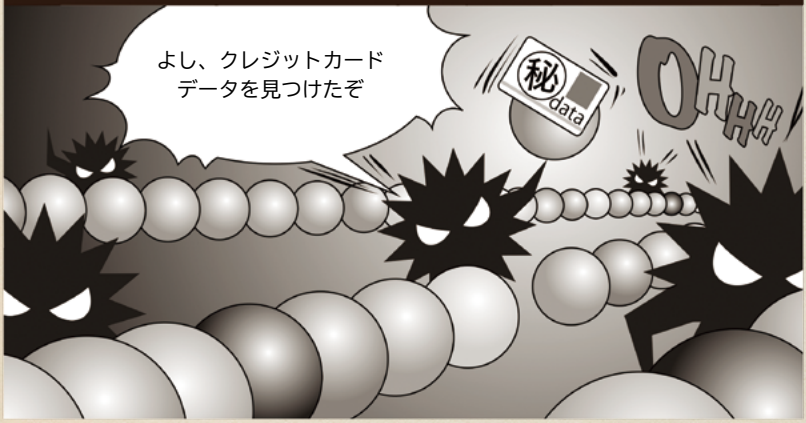
よおし、標的型メールを開いたぞ。
さあ、活動開始だ

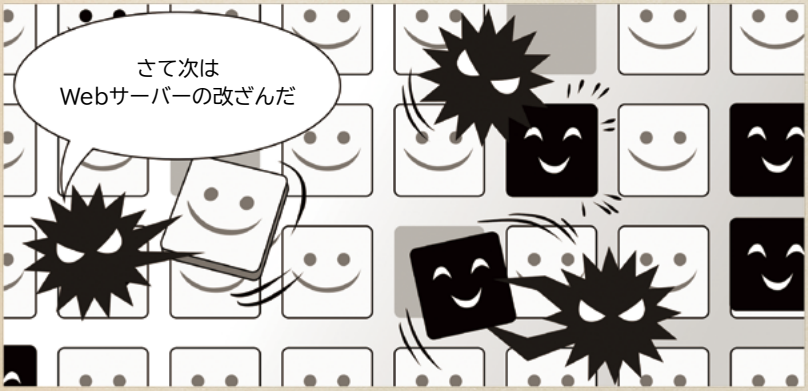


SCENE 04

潜入拡大

クレジットカードの個人情報を取得。クレジットカードを自由に使うためにセキュリティコードなどを盗み取る





顧客への被害の拡大
取引先への被害の拡大

フィッシングサイトでセキュリティコード情報を窃取。
取得した個人情報を使ってキャッシングで現金を引き出す

●●食品卸売株式会社からの請求明細のメールを装い、
標的型メールの攻撃

Mission 5

SCENE 06

サイバー攻撃の発覚

さあ、あなたならどうしますか？

ACTION 1 原因と被害範囲の調査を自社で実施できるかどうかを判断する

標的型攻撃に代表される企業ネットワークに対する外部からの攻撃や、Webアプリケーションの改ざん、不正アクセスなどのサイバー攻撃の発生時に、本格的な調査（フォレンジック〈法的〉調査、ウイルスの不正プログラムの解析、ログの分析など）、復旧支援と再発防止策のアドバイスを支援するセキュリティ会社があります。

ACTION 2 原因と被害範囲の調査を依頼する

SCENE 07

原因が判明 ウイルス感染が原因

さあ、あなたならどうしますか？

ACTION 1 ネットワークからの切断

ACTION 2 感染ウイルス・不正プログラムの駆除

- OSは最新バージョン自動更新をチェック
- アプリケーションも最新の状態に
- データは必ずウイルス対策ソフトで複数チェック

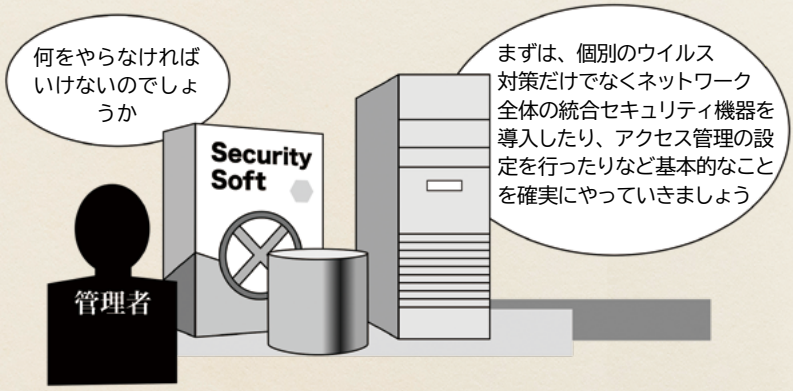
ACTION 3 各機関への連絡・関係先への報告

SCENE 08

再発防止策の作成

さあ、あなたならどうしますか？

ACTION 1 物理的および環境的セキュリティを再検討する



ACTION 2 社員教育など人的セキュリティを強化する

復旧回復

さあ、あなたならどうしますか？

ACTION 1 情報漏えいについての発表

ACTION 2 再発防止の恒久的対策

ACTION 3 不審なログオンや通信の監視

不自然な通信をしているプログラムがないか、外部から不正なログオンが行われていないか、監視します。

大切なのは社内意識の向上！
～感染を狙うメールに注意～

経営者にとってメールの安全な運用は他人事ではない！

コンピューターウイルスやマルウェアは、以下のような経路から感染する。

・USB機器からの感染
・ファイル共有、アプリからの感染
・ウェブ閲覧からの感染　など

これらは、システム設定などにより使用を禁止することで回避できる。しかし、ビジネスツールであるメールを一切禁止することは現実的ではない。加えて、メールを悪用した攻撃の中には人の心理的な隙や行動ミスをついた、システム設定だけでは対応が難しい手口も存在する。

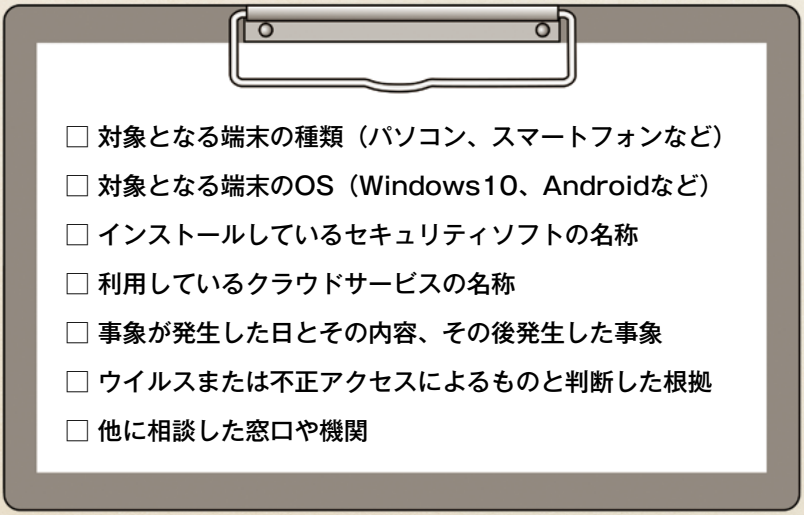
メールを発端とするサイバー攻撃の中には、企業の事業継続に多大な影響を与えるものもある。自社がそのような当事者にならないためにも、定期的な勉強会や訓練を実施するほか、経営者自身も率先して参加するなど、社内全体で危機意識を共有し、個々のリテラシー向上を図っていくことが何より大切だろう。

TOP SECRET
INFORMATION
インフォメーション

もしかしてサイバー攻撃？ここに連絡を！

事前に情報を整理しましょう

サイバー攻撃を受けた可能性がある場合は、事前に次のような情報を整理して緊急連絡先に連絡しましょう。



- □ 対象となる端末の種類（パソコン、スマートフォンなど）
- □ 対象となる端末のOS（Windows10、Androidなど）
- □ インストールしているセキュリティソフトの名称
- □ 利用しているクラウドサービスの名称
- □ 事象が発生した日とその内容、その後発生した事象
- □ ウイルスまたは不正アクセスによるものと判断した根拠
- □ 他に相談した窓口や機関

CHECK 犯罪の可能性がある場合の相談窓口

警視庁 サイバー犯罪対策課

https://www.keishicho.metro.tokyo.jp/sodan/madoguchi/sogo.html
TEL　03-5805-1731
受付時間：平日8:30－17:15

CHECK 一般的な情報セキュリティ相談

独立行政法人 情報処理推進機構（IPA）情報セキュリティ安心相談窓口

https://www.ipa.go.jp/security/anshin/about.html
TEL　03-5978-7509　FAX　03-5978-7518
受付時間：10:00－12:00　13:30－17:00（土日祝日・年末年始を除く）
E-mail　anshin@ipa.go.jp

CHECK 被害の報告・連絡・相談窓口

ウイルスに関する届け出（IPA）
https://www.ipa.go.jp/security/todokede/crack-virus/about.html

不正アクセスに関する届け出（IPA）
https://www.ipa.go.jp/security/todokede/crack-virus/about.html

フィッシング詐欺（フィッシング対策協議会）
https://www.antiphishing.jp/

迷惑メール（日本データ通信協会 迷惑メール相談センター）
https://www.dekyo.or.jp/soudan/

なりすましECサイト（なりすましECサイト対策協議会）
https://www.saferinternet.or.jp/e-commerce/narisumashi/

インシデント報告・届出（JPCERT/CC）
https://www.jpcert.or.jp/form/

インシデント報告・届出（IPA J-CRAT 標的型サイバー攻撃特別相談窓口）
https://www.ipa.go.jp/security/tokubetsu/

法律相談（日本司法支援センター 法テラス）
https://www.houterasu.or.jp/

INFORMATION 6-2 その他の主な報告・連絡・相談窓口等

CHECK 被害が発生している可能性がある場合

違法・有害情報（セーファーインターネット協会）
https://www.safe-line.jp/

違法・有害情報（インターネット違法・有害情報相談センター）
https://www.ihaho.jp/

違法・有害情報（インターネット・ホットラインセンター）
https://www.internethotline.jp/

個人情報（個人情報保護委員会）
https://www.ppc.go.jp/

嫌がらせ・ネットストーカー（管轄の警察署の生活安全課）
Webブラウザーで「警察署一覧」で検索

人権侵害（法務省人権擁護局 みんなの人権110番）
https://www.moj.go.jp/JINKEN/index_soudan.html

CHECK 恒久的対策を行うための情報源

情報セキュリティ対策支援サイト（IPA）
https://security-shien.ipa.go.jp/

セキュリティプレゼンター支援（IPA）
https://security-shien.ipa.go.jp/presenter/

情報セキュリティサービス基準適合サービスリスト（IPA）
https://www.ipa.go.jp/security/service_list.html

サイバーインシデント緊急対応企業一覧（JNSA）
https://www.jnsa.org/emergency_response/

経営とIT化相談窓口（ITコーディネータ協会）
https://www.itc.or.jp/management/diagnosis/

東京都テレワーク推進センター（東京都）
https://tokyo-telework.jp/

テレワーク相談センター（厚生労働省委託事業）
https://www.tw-sodan.jp/

テレワークのセキュリティあんしん相談窓口（LAC）
https://www.lac.co.jp/telework/security.html

ワンストップ総合相談窓口（東京都中小企業振興公社）
https://www.tokyo-kosha.or.jp/support/shien/soudan/

CHECK 東京都による情報源

東京都と警視庁、中小企業支援機関、サイバーセキュリティ対策機関などが連携して開設した、中小企業のための相談窓口です。

https://www.sangyo-rodo.metro.tokyo.lg.jp/chushou/shoko/cyber/soudan/
TEL　03-5320-4773
窓口　東京都産業労働局商工部内 Tcyss事務局（都庁第一本庁舎20階北側）
受付時間：都庁開庁日の9:00～12:00、13:00～17:00

東京中小企業支援 サイバーセキュリティ
https://www.sangyo-rodo.metro.tokyo.lg.jp/chushou/shoko/cyber/

「中小企業向けサイバーセキュリティの極意」ポータルサイト
https://cybersecurity-tokyo.jp/

セキュリティお役立ちリンク

サイバーセキュリティ対策に有用な文献、Webページには下記のようなものがあります。必要に応じて情報を収集しましょう。

●サイバーセキュリティに関する基本文書、白書、解説文書

基本文書（法律・基本計画・各種方針等）	サイバーセキュリティ基本法	総務省
	サイバーセキュリティ戦略	NISC
	サイバーセキュリティ2020	NISC
	セキュリティ関連NIST文書	IPA
各種白書・年次報告書類	情報通信白書	総務省
	AI白書	IPA
	情報セキュリティ白書	IPA
	IT人材白書	IPA

●各実施事項の参考情報

全般	企業経営のためのサイバーセキュリティの考え方	NISC
	サイバーセキュリティ経営ガイドライン	経済産業省
	サイバーフィジカルセキュリティフレームワーク（CPSF）	経済産業省
	サイバーサプライチェーンリスクマネジメント	IPA
	ISMS適合評価制度	JIPDEC
DX関連	Society5.0	内閣府
	サイバーフィジカルシステム（CPS）	JEITA
	DXレポート2 中間取りまとめ（概要）	経済産業省
	DXの推進に関するお役立ちコンテンツ一覧	IPA
テレワーク関連	テレワークで始める働き方改革―テレワークの導入・運用ガイドブック	厚生労働省
	テレワークを実施する際にセキュリティ上留意すべき点について	NISC
	テレワークセキュリティガイドライン第4版	総務省
	テレワーク勤務のサイバーセキュリティ対策！	警視庁

IoT セキュリティ関連	IoTセキュリティガイドライン ver 1.0	総務省
	IoTセキュリティ対応マニュアル産業保安版	経済産業省
	安全なIoTシステムのためのセキュリティに関する一般的枠組	NISC
	IoTセキュリティチェックリスト	JPCERT/CC
	IoT・5Gセキュリティ総合対策プログレスレポート	総務省
人材育成関連	iコンピテンシディクショナリ（iCD）について	IPA
	ITSS+・ITスキル標準（ITSS）・情報システムユーザースキル標準（UISS）関連情報	IPA
	サイバーセキュリティ体制構築・人材確保の手引き	経済産業省
	情報処理技術者試験・情報処理安全確保支援士試験	IPA

●各実施事項の参考情報

内閣サイバーセキュリティセンター（NISC）	
	みんなでしっかりサイバーセキュリティ
	みんなで使おうサイバーセキュリティ・ポータルサイト
	サイバーセキュリティ関係法令_Q&AハンドブックVer1.0
情報処理推進機構（IPA）	
	情報セキュリティ
	ここからセキュリティ
	SECURITY ACTION セキュリティ対策自己宣言
	サイバー情報共有イニシアティブ（J-CSIP）
JPCERTコーディネーションセンター（JPCERT/CC）	
	緊急情報を確認する
	脆弱性対策情報データベース（JVN iPedia）
	JPCERT/CCに依頼する
総務省	
	国民のためのサイバーセキュリティサイト
	国民のためのサイバーセキュリティサイト リンク集
日本サイバー犯罪対策センター（JC3）	
警視庁 情報セキュリティ広場	

中小企業の情報セキュリティ対策ガイドライン

情報セキュリティ対策の進め方

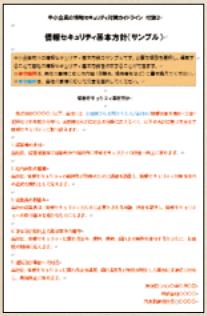
情報技術の進歩・普及に伴い経営効率が向上した一方、重要情報の漏えいや消失、改ざんなど技術特有の不利益が発生する機会も増してきています。
これら不利益が対策の不備により生じた場合、経営者は取引先や従業員などへの社会的・道義的責任に加え、法的責任も追及されるおそれがあります。

近年は企業情報を狙うサイバー脅威も日々巧妙化しています。自社を守るためには、経営者が率先して対策に取り組むことが大切です。

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

情報セキュリティ対策を推進する際に参考にしたいのが、「中小企業の情報セキュリティ対策ガイドライン」（情報処理推進機構〈IPA〉）です。
このガイドラインは情報の安全管理の重要性や企業の保有する機微な情報を各種の脅威から保護するための対策の考え方や段階的に実現するための方策を紹介する目的で作成されたものです。まずはこのガイドラインを参考に、自社に適した対策を実践していくとよいでしょう。

●「中小企業の情報セキュリティ対策ガイドライン」



●付録2
「情報セキュリティ基本方針（サンプル）」

●付録3
「5分でできる！ 情報セキュリティ自社診断」

●付録5
「情報セキュリティ関連規程（サンプル）」

ACTION 1 最低限のルール「情報セキュリティ5か条」

資金や人材が限られる中小企業にとって、最初から全ての対策に取り組むことは容易ではありません。まずは、基本的な対策を取りまとめた「情報セキュリティ５か条」に取り組むことからはじめ、段階的に対策を講じていきましょう。

1 OSやソフトウェアは常に最新の状態にしよう！

Windows OS、Mac OS、Androidなどはいずれも常に最新バージョンに！
Office、Adobe Readerなど利用中のソフトウェアも常に最新バージョンに！

「自動アップデート」は必ずONに！

2 ウイルス対策ソフトを導入しよう！

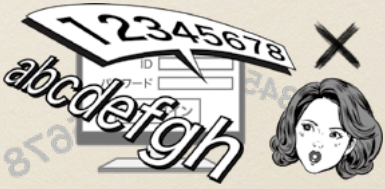
ウイルス定義ファイルは自動更新に設定！
ファイアウォールや脆弱性対策なども可能な統合型セキュリティ対策ソフトを導入！

ウイルス対策ソフトも常に最新に！

3 パスワードを強化しよう！

ID・パスワードは推測や解析、ウェブサービスから流出することで不正ログインに悪用される恐れがある！
「長く」「複雑」「使い回さない」を徹底しよう！

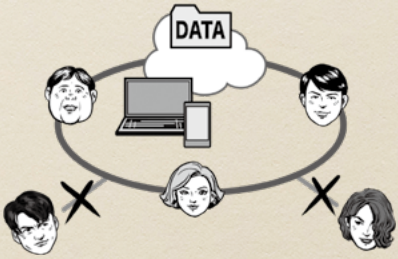
パスワードは使い回さない！



4 共有設定を見直そう！

クラウドサービスの共有を限定的に！
ネットワーク接続の複合機、カメラ、ハードディスク、NASなどの共有を限定的に！
従業員の異動や退職時に設定の変更や削除漏れがないように！

利用者は必要な人だけに！



5 脅威や攻撃の手口を知ろう！

セキュリティ専門機関から常に最新の脅威情報を収集！
利用中のネットバンクやクラウドサービスからの注意喚起を確認！

最新情報で対策を！

ACTION 2 組織的な対策に取り組む

基本的対策の次は組織的な対策です。「中小企業の情報セキュリティ対策ガイドライン」とその付録を参考に自社に適した基本方針を作成し、社内関係者に周知します。また、自社のセキュリティ診断を実施して、取り得る対策を検討していきましょう。

1　情報セキュリティ基本方針の作成と周知

従業員の指針であり、関係者に対して取り組みを表明するための情報セキュリティに関する基本方針を経営者が定め、簡潔な文書にまとめて周知します。
「中小企業の情報セキュリティ対策ガイドライン」と付録2の「情報セキュリティ基本方針（サンプル）」を参考に、経営者と連携して自社に適した基本方針を作成しましょう。

2　実施状況の把握

付録3の「5分でできる！情報セキュリティ自社診断」を利用して、情報セキュリティ対策がどれくらい実施できているかを把握しましょう。

3　対策の決定と周知

「5分でできる！情報セキュリティ自社診断」の結果を基に、解説編を参考にして実施すべき情報セキュリティを検討しましょう。

ACTION 3 本格的に対策に取り組む

情報セキュリティ基本方針を具体的に実現するために、情報セキュリティ責任者を任命して責任分担と連絡体制を整備しましょう。また、情報セキュリティ事故が発生した場合など、緊急時対応体制も整備しておきましょう。

1　管理体制の構築

情報セキュリティ基本方針を具体的に実現するために、情報セキュリティ責任者、情報部門責任者、システム管理者、教育責任者、点検責任者を任命して責任分担と連絡体制を整備しましょう。また、情報セキュリティ事故が発生した場合など、緊急時対応体制も整備しておきましょう。

2　IT利活用方針と情報セキュリティの予算化

クラウドサービスの普及によってIT利活用の方法が多様化したことで、情報セキュリティリスクも多様化しています。自社で利用している情報システムやサービスの台帳を作成したり図式化したりして把握した上で対策を検討し、必要な予算を確保しましょう。

3　情報セキュリティ規程の作成

事業内容や取り扱う情報、職場環境、IT利活用の状況に応じて、「中小企業の情報セキュリティ対策ガイドライン」付録5の「情報セキュリティ関連規程（サンプル）」を参考に、情報セキュリティ規程を作成しましょう。（1）対応するリスクの特定、（2）対策の決定、（3）規程の作成の順に進めます。

4　委託時の対策

業務の一部または全部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サービスを利用したりして、重要な情報を渡したり処理を依頼したりする場合には、委託先に実施してもらう情報セキュリティ対策も決めましょう。取引条件のひとつとして、契約書や覚書に具体的な対策を明記しましょう。

5　点検と改善

「情報セキュリティ5か条」や「5分でできる！情報セキュリティ自社診断」、自社の情報セキュリティ対策に関するルール・規程を基準に、情報セキュリティ対策が、計画通りに実行されているか、見落としている対策はないか、対策がセキュリティ事故防止の役に立っているかを確認しましょう。

ACTION 4 対策をより強固にする

本格的な対策に取り組んでいても、必要な対策を追加して強固にしましょう。

1　情報収集と共有

情報セキュリティに関する脅威や攻撃の手口を知り、社内や取引先、同業者と共有することで対策レベルの向上につなげましょう。

2　ウェブサイトの情報セキュリティ

情報漏えいや改ざんなどの被害が発生する攻撃の対象になりやすいWebサイトの運営形態、構築、運営それぞれの段階に応じた対策を講じましょう。

3　クラウドサービスの情報セキュリティ

クラウドサービスに適した情報セキュリティ対策について、サービスの選定、運用、セキュリティ対策の3段階で検討しましょう。

4　情報セキュリティサービスの活用

コンサルテーションや教育サービス、監査サービスなど、情報セキュリティ対策を強固にする外部のサービスの利用を検討しましょう。

5　技術的対策例と活用

ネットワーク脅威対策やコンテンツセキュリティ対策など、情報セキュリティ対策の向上に資する製品やソフトウェアの導入を検討しましょう。

6　詳細リスク分析の実施

（1）情報資産の洗い出し、（2）リスク値の算定、（3）情報セキュリティ対策の決定の順で、リスクの洗い出しと対策の検討を行いましょう。

中小企業のためのクラウドサービス安全利用手引き

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をクラウドサービスと呼びます。クラウドサービスの利用は、情報システムの構築や管理といった手間が省けるなど、自社での所有・運用と比較して業務の効率化やコストダウンを図れるといったメリットがあります。

利用前の確認

クラウドサービスの利用を検討する際は、情報セキュリティ対策の一部がサービス提供事業者に依存してしまうことや、クラウドサービス固有のリスクがある点についても考慮する必要があります。『クラウドサービス安全利用の手引き』（情報処理推進機構<IPA>）では、サービスを選択するときのポイントについて事例をあげて解説しています。

●中小企業のためのクラウドサービス安全利用の手引き

https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000072150.pdf

パブリッククラウドとプライベートクラウド

クラウドには大きく「パブリッククラウド」と「プライベートクラウド」があり、前者は、企業・個人を問わず必要なときにサーバーやサービス活用が可能です。後者は、企業・組織が専用環境を構築して社内各部署などにサービス提供する形を指します。しかし、各々メリット・デメリットがあり、両者を統合して利用する「ハイブリッドクラウド」の活用が増えつつあります。

CHECK クラウドサービス利用時の確認事項

●選択するときのポイント

1	どの業務で利用するか明確にする	どの業務クラウドサービスで行い、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たか？
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定し、どのようなメリットがあるか確認しましたか？
3	取り扱う情報の重要度を確認する	クラウドサービスで取り扱う情報が漏えい、改ざん、消失したり、サービスが停止したりした場合の影響を確認しましたか？
4	セキュリティのルールと矛盾しないようにする	自社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ませんか？
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ですか？
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は示されていますか？

●運用するときのポイント

7	管理担当者を決める	クラウドサービスの特性を理解した管理担当者を社内に確保していますか？
8	利用者の範囲を決める	クラウドサービスを適切な利用者のみが利用可能となるように管理できていますか？
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について適切に設定・管理は実施できていますか？（共有しない、複雑にするなど）
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・改ざんなどに備えて、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ていますか？

●セキュリティ管理のポイント

11	付帯するセキュリティ対策を確認する	サービスに付帯するセキュリティ対策が具体的に公開されていますか？
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）は提供されていますか？
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、データの取り扱い条件について確認しましたか？
14	適用法令や契約条件を確認する	個人情報保護などを想定し、一般的契約条件の各項目について確認しましたか？
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たか？

No15 クラウドサービスのサーバーは日本国外に設定されている場合もありますが、扱うデータによってサーバーの設置国・地域の法規制が適用されることがあります。No 6、11、12、13はスマートSMEサポーター（認定情報処理支援機関）開示情報で確認できます。
出典：IPA「中小企業のためのクラウドサービス安全利用の手引き」より

IT活用に不可欠なIT人材の確保と育成

セキュリティ人材育成と考え方の変化

企業規模等によっても異なりますが、セキュリティ対策の中心となるのは、セキュリティ統括分野やセキュリティ監視・運用分野等を担うセキュリティ人材です。さらに、ITを利活用して社会を変えるSociety5.0の進展など、時代の変化を受け、本来の業務の中でITを利活用する人材にもセキュリティに関するスキルが求められるようになっています。

求められる「プラス・セキュリティ人材」

企業におけるあらゆる業務でデジタルトランスフォーメーション（DX）が進んでいますが、DXによる利便性はサイバー攻撃にも悪用されやすいため、DXを活用する企業ではセキュリティを意識して必要な対策を総合的に実施することが求められます。

一方、IPAなどによる調査では、そうしたセキュリティ人材の量的・質的不足が大きな課題となっています。セキュリティ対策がセキュリティ人材だけでは対処できなくなっているため、デジタル部門、事業部門、管理部門など、セキュリティ対策が不十分な場合に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も、セキュリティに関する意識を養い、対策の実施に求められる知識・スキルを積極的に身に付けてもらう必要があります。

こうした「プラス・セキュリティ人材」の育成がこれからの企業には求められます。

CHECK「プラス・セキュリティ人材」の育成

「プラス・セキュリティ人材」を育成する際には、経済産業省が定めている、セキュリティ領域のIT人材に求められる個人のIT関連能力を明確化・体系化し、スキルやキャリア（職業）を示した指標である「ITSS+（セキュリティ領域）」を活用し、関連部門でセキュリティ関連タスクを担う人材の特定・育成・配置等を検討するとよいでしょう。

●ITSS+（プラス）・ITスキル標準（ITSS）・情報システムユーザースキル標準（UISS）関連情報
https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/index.html

●サイバーセキュリティ体制構築・人材確保の手引き（経済産業省）
https://www.meti.go.jp/press/2020/09/20200930004/20200930004-1.pdf

情報セキュリティ関連法令

企業の情報セキュリティに関連する国内の法令は、下記のように多岐にわたります。また、海外に子会社や支店、営業所などを有し、日本から海外に商品やサービスを提供している企業や海外から個人データの処理について委託を受けている事業など、業務の内容によっては、EU域内の各国に適用される個人データ保護を規定したEU一般データ保護規則（GDPR：General Data Protection Regulation）などの海外法令への対応も必要になります。

・サイバーセキュリティ基本法
・不正アクセス禁止法
・個人情報保護法
・民法、刑法
・その他のセキュリティ関連法規（電子署名及び認証業務等に関する法律、プロバイダ責任制限法、特定電子メール法）
・知財関連法規（著作権法、産業財産権法、不正競争防止法）
・労働関連・取引関連法規（労働基準法、労働者派遣法、男女雇用機会均等法、公益通報者保護法、労働安全衛生法、下請法、特定商取引法、電子消費者契約法）
・海外法令（GDPR等）
・その他の法律・ガイドライン・技術者倫理
・「非連邦政府組織およびシステムにおける管理対象非機密情報CUIの保護（SP800-171）」

内閣官房内閣サイバーセキュリティセンター（NISC）は、関連法令をQ&A形式で解説する「サイバーセキュリティ関係法令Q&Aハンドブック」を公開しています。自社の業務と照らし合わせながら、効率的・効果的なサイバーセキュリティ対策・法令遵守を実践するとよいでしょう。

●内閣官房内閣サイバーセキュリティセンター（NISC）関係法令等
https://www.nisc.go.jp/law/

情報管理が不適切な場合の処罰など

個人情報などの法的な管理義務がある情報を適切に管理していなかった場合には、企業の経営者や役員、担当者は下記の表に示すような責任を問われ、処罰されることになります。

法令	条項	処罰など
個人情報保護法 個人情報の保護に関する法律	40条 報告及び立入検査	委員会による立入検査、帳簿書類等の物件検査及び質問
	83条 個人情報データベース等不正提供罪	1年以下の懲役又は50万円以下の罰金
	84条 委員会からの命令に違反	6月以下の懲役又は30万円以下の罰金
	85条 委員会への虚偽の報告など	30万円以下の罰金
	87条 両罰規定	従業者等が業務に関し違反行為をした場合、法人に対しても罰金刑
マイナンバー法（番号法） 行政手続における特定の個人を識別するための番号の利用等に関する法律	48条 正当な理由なく特定個人情報ファイルを提供	4年以下の懲役若しくは200万円以下の罰金又は併科
	49条 不正な利益を図る目的で、個人番号を提供又は盗用	3年以下の懲役若しくは150万円以下の罰金又は併科
	50条 情報提供ネットワークシステムに関する秘密を漏えい又は盗用	同上
	51条 人を欺き、人に暴行を加え、人を脅迫し、又は、財物の窃取、施設への侵入、不正アクセス等により個人番号を取得	3年以下の懲役又は150万円以下の罰金
	53条 委員会からの命令に違反	2年以下の懲役又は50万円以下の罰金
	54条 委員会への虚偽の報告など	1年以下の懲役又は50万円以下の罰金
	55条 偽りその他不正の手段により個人番号カード等を取得	6月以下の懲役又は50万円以下の罰金
	57条 両罰規定	従業者等が業務に関し違反行為をした場合、法人に対しても罰金刑

法令	条項	処罰など
不正競争防止法 営業秘密・限定提供データに係る不正行為の防止など	3条 差止請求	利益を侵害された者からの侵害の停止又は予防の請求
	4条 損害賠償請求	利益を侵害した者は損害を賠償する責任
	14条 信頼回復措置請求	信用を害された者からの信用回復措置請求
金融商品取引法 インサイダー取引の規制など	197条の2 刑事罰	5年以下の懲役若しくは500万円以下の罰金又はこれらの併科
	207条1項2号 両罰規定	従業者等が業務に関し違反行為をした場合、法人に対しても罰金刑
	198条の2 没収・追徴	犯罪行為により得た財産の必要的没収・追徴
	175条 課徴金	違反者の経済的利得相当額
民法	709条 不法行為による損害賠償	故意又は過失によって他人の権利又は法律上保護される利益を侵害した者は、これによって生じた損害を賠償する責任を負う

出典：IPA「中小企業の情報セキュリティ対策ガイドライン」より

主な参考文献

ジャンル	タイトル	発行元
サイバーセキュリティ対策全般	中小企業の情報セキュリティ対策ガイドライン　第3版	IPA
	サイバーセキュリティ経営ガイドライン	経済産業省・IPA
	サイバーセキュリティ経営ガイドライン解説書	IPA
	企業経営のためのサイバーセキュリティの考え方の策定について	NISC
	情報セキュリティ５カ条	IPA
	インシデント対応マニュアルの作成について	JPCERT/CC
	中小企業における組織的な情報セキュリティ対策ガイドライン事例集	IPA
	企業(組織)における最低限の情報セキュリティ対策のしおり	IPA
	中小企業における情報セキュリティ対策の実態調査　事例集	IPA
	ISO27002:2014情報セキュリティ管理策の実践（11物理的及び環境的セキュリティ）	JIS
	地方公共団体における情報セキュリティポリシーに関するガイドライン（平成27年3月）	総務省
	情報管理はマネーです	JIPDEC
	サイバーセキュリティ関係法令Q&Aハンドブック	NISC
サイバー攻撃について	情報セキュリティ10大脅威 2021	IPA
	サイバー攻撃ってなに？	NISC
	サイバーセキュリティ 2020	NISC
個別のサイバー攻撃対策	ランサムウェアの脅威と対策	IPA
	IPA テクニカルウォッチ「標的型攻撃メールの例と見分け方」	IPA
	組織における内部不正防止ガイドライン	IPA
	情報漏えい発生時の対応ポイント集	IPA
	IPA 対策のしおり(1) ウイルス対策のしおり	IPA
	IPA 対策のしおり(2) スパイウェア対策のしおり	IPA
	IPA 対策のしおり(3) ボット対策のしおり	IPA
	IPA 対策のしおり(4) 不正アクセス対策のしおり	IPA
	IPA 対策のしおり(5) 情報漏えい対策のしおり	IPA
	IPA 対策のしおり(6) インターネット利用時の危険対策のしおり	IPA
	IPA 対策のしおり(7) 電子メール利用時の危険対策のしおり	IPA
	IPA 対策のしおり(8) スマートフォンのセキュリティ＜危険回避＞対策のしおり	IPA

ジャンル	タイトル	発行元
個別のサイバー攻撃対策	IPA 対策のしおり(9) 初めての情報セキュリティ 対策のしおり	IPA
	IPA 対策のしおり(10) 標的型攻撃メール＜危険回避＞対策のしおり	IPA
	コンピュータセキュリティインシデントへの対応	JPCERT/CC
	高度サイバー攻撃対処のためのリスク評価等のガイドライン付属書	NISC
	「標的型メール攻撃」対策に向けたシステム設計ガイド	IPA
	スマートフォン等の業務利用における情報セキュリティ対策の実施手順策定手引書	NISC
役に立つツール	情報セキュリティハンドブックひな形	IPA
	情報セキュリティポリシーサンプル	IPA
	情報セキュリティ自己診断チェックリスト	NISC
	5分でできる！情報セキュリティ自社診断シート・パンフレット	IPA
	情報セキュリティ対策自己診断テスト ～情報セキュリティ対策ベンチマークVer.5～	IPA
	中小企業のためのクラウドサービス安全利用の手引き	IPA
IoT対策	IoT セキュリティガイドライン	経済産業省
	IoT、AI、ロボットに関する経済産業省の施策について	経済産業省
	2017　攻めのIT経営中小企業百選	経済産業省
	中小ものづくり企業IoT等活用事例集	経済産業省
個人情報	ホームページ「マイナンバー制度とマイナンバーカード」	総務省
	個人情報取扱事業者のみなさん、新たに個人情報取扱事業者となるみなさんへ 「個人情報」の「取扱いのルール」が改正されます！	経済産業省
その他	2020年版中小企業白書	中小企業庁
	令和2年版情報通信白書	総務省
	IT人材白書2020	IPA
	自治体CIO育成研修 集合研修 SLAの考え方	総務省
	情報システムに係る政府調達へのSLA導入ガイドライン	IPA
	ICTの進化が雇用と働き方に及ぼす影響に関する調査研究　平成28年	総務省

IPA：独立行政法人情報処理推進機構
NISC：内閣サイバーセキュリティセンター
JPCERT/CC：一般社団法人JPCERT コーディネーションセンター
JIPDEC：日本情報経済社会推進機構

用語解説インデックス

中小企業向け
サイバーセキュリティ対策の極意 Ver 2.2a

令和4年5月第1刷　令和６年２月第2刷発行
編集・発行　東京都産業労働局商工部経営支援課
新宿区西新宿二丁目8番1号
電話番号　03（5320）4770

印刷　株式会社　シンソークリエイト

登録番号　（5）155

協力
東京中小企業サイバーセキュリティ支援ネットワーク（Tcyss）

※掲載の情報は令和6年2月現在のものです

VEGETABLE OIL INK

リサイクル適性Ⓐ
この印刷物は、印刷用の紙へリサイクルできます

中小企業向け

サイバーセキュリティ対策の極意

Ver 2.2a

東京都