中小企業向け
サイバーセキュリティ対策の極意

あなたの会社も
狙われている。

中小企業向け
サイバーセキュリティ対策の極意

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も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。
平成 27 年度には、1 件当たり 9,100 万円という被害も発生し、全体で 30 億円余り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、銀行が弁償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。

はじめに

約400倍

情報通信研究機構（NICT）サイバーセキュリティ研究所サイバーセキュリティ研究室が2016年の1年間で観測したサイバー攻撃に関連する通信量は約1,281億パケット※でした。観測を始めた2005年は約3.1億パケットでしたから、11年間で413倍に増加しています。

※通信の伝送単位

2020年東京が狙われている

2020年には東京2020オリンピック・パラリンピックが開催されます。
2016年に開催されたリオデジャネイロオリンピックでは、テロと同様にサイバー攻撃が大きなリスクとして懸念され、2,300万件のアタックをブロックしたと報告されています。また、オリンピックの中核施設に隣接した変電所を運営している電力会社Light社が期間中に受けた攻撃は、1,300万件に達しました。
東京2020大会でも同様のサイバー攻撃が予想されます。

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ります。

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

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 4 もしもマニュアル

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、本冊子では全て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「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

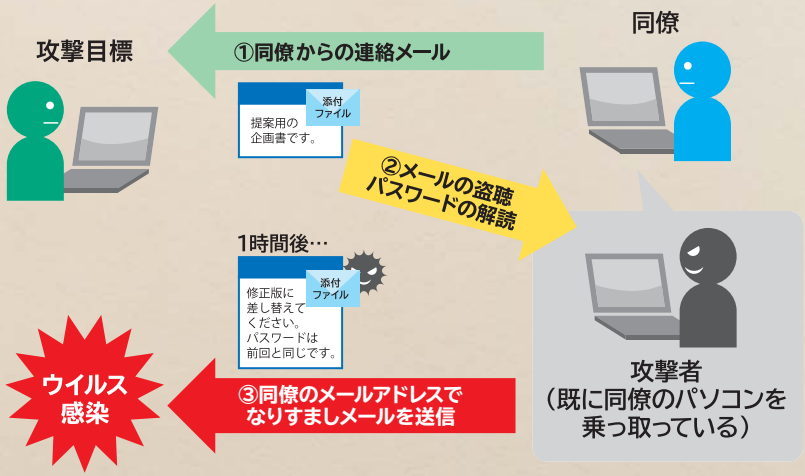
知っておきたい サイバー攻撃の知識

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

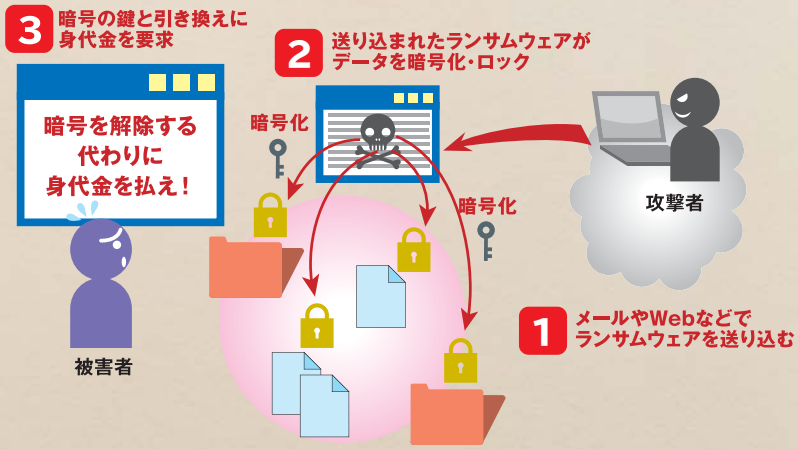
・日本語の言い回しが不自然なメール
・差出人のメールアドレスとメール本文の署名に記載されたメールアドレスが異なるメール
・これまで届いたことがない公的機関からのお知らせ
・心当たりのないメールだが、興味をそそられる内容
・心当たりのない決済や配送通知
・論理的に自分に送られてくることがおかしいメール

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。

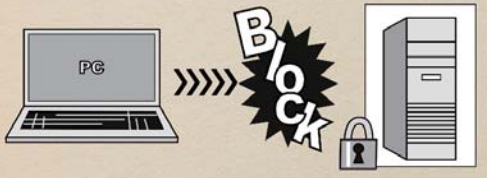


POINT 2 侵入手口はメールとWebサイト

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。

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。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※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

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
・適切なログの取得と継続的な監視

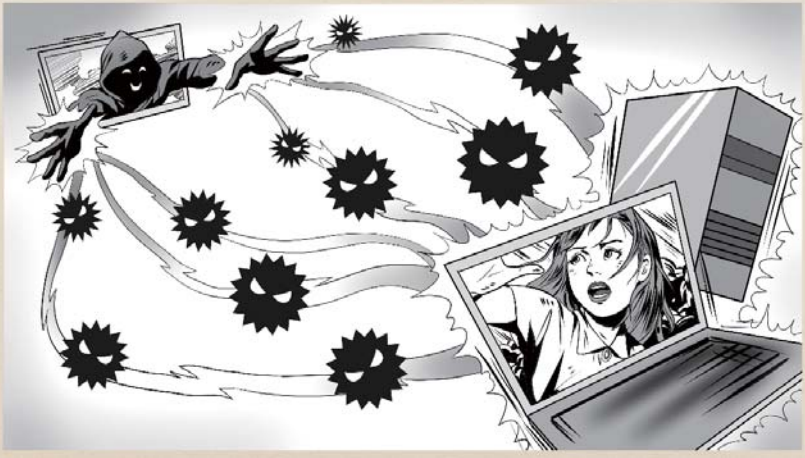
●サービスを利用する場合

・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

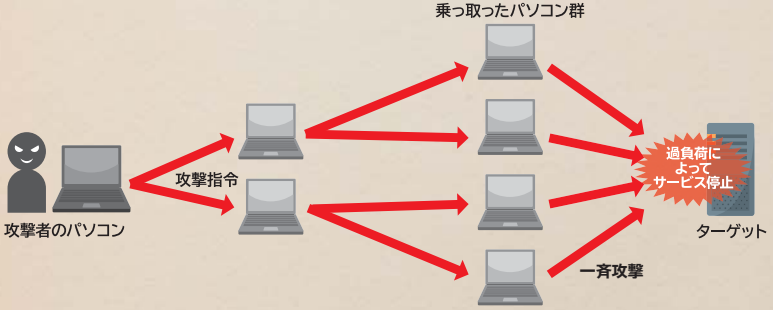
サーバーに処理速度をはるかに上回る大量の要求が集中すると、利用者はそのサーバーにアクセスできない状態になり、最終的にはサーバーがダウンしてしまいます。
インターネット回線の容量がオーバーして、接続不能に陥ることもあります。



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利用されています。

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
日本政府	2005年 2～9月	中国における反日デモに呼応した集中攻撃。
オンラインゲーム会社	2009年6月	集中攻撃を受け、一時サービス停止に追い込まれた。
掲示板サイト	2010年3月	韓国などの一般利用者からサイトへ攻撃。
金融機関	2015年6月	インターネットの取引画面に接続できない状態となった。攻撃停止と引き換えに、ビットコインによる支払いを要求された。
厚生労働省	2015年11月	Webサイトが集中攻撃を受け、安全確認の期間も含め約3日間Webサイトが停止。

内部不正による情報漏えいと業務停止

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。

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。

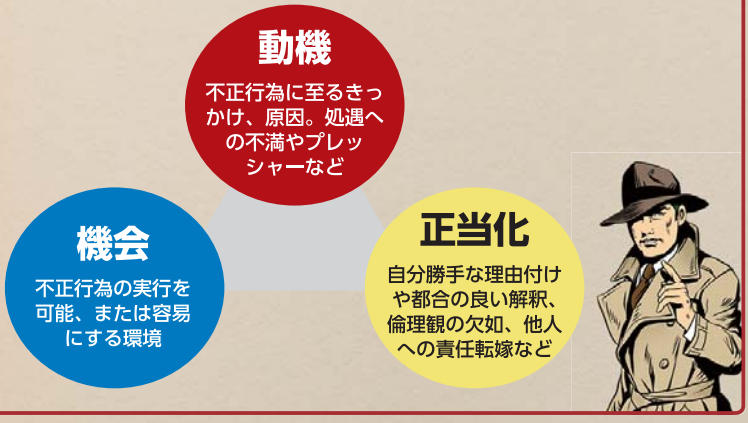
POINT 3 企業の信用が失墜し、賠償が求められる

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。2016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6億円を超えています。

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

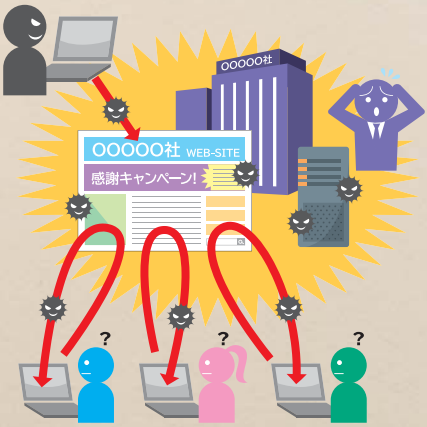
POINT 1 改ざんの目的は2つ

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。



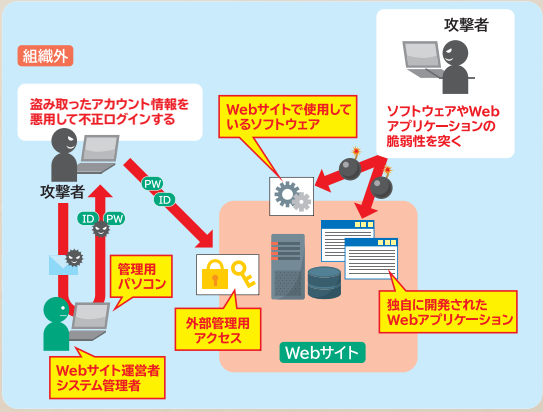
POINT 2 手口は脆弱性攻撃と管理用アカウントの乗っ取り

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年には被害額は減少したものの、中小企業が利用する金融機関の法人口座の被害が増えています。

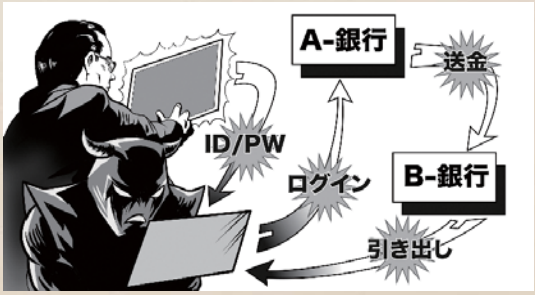
POINT 2 手口はフィッシング詐欺と不正送金ウイルス

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

- **ワンタイムパスワードなど金融機関が推奨する最新のセキュリティ対策を導入する**
- **金融機関が推奨するセキュリティソフトを導入する**
- **ログイン画面のURLを必ずチェックする**
- **ログイン画面に鍵マークが表示されていることを確認する**
- **ログイン画面でポップアップ画面が表示されることはない**
- **出入金履歴を小まめに確認する**
- **金融機関がメールによってクレジットカード番号やネットバンキングの第2暗証番号の入力、パスワード変更を求めることはない**

MISSION 1-8

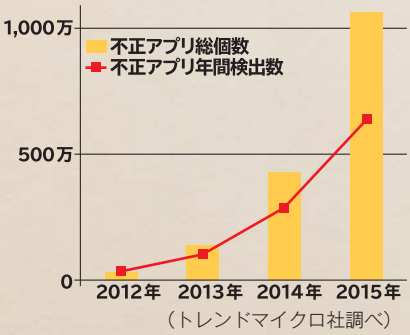
悪意のあるスマホアプリ

POINT 1 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1,000万個を突破

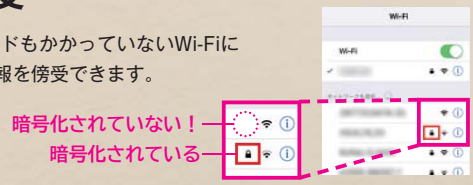
2010年8月に最初のAndroid不正アプリが検出されて以来、5年を待たずして1,000万個に到達しました。特に2015年には、わずか1年の間に630万個が新たに登場しました。（トレンドマイクロ社調べ）Androidでは自由にアプリを配布・インストールすることができます。不正なアプリに十分注意してください。



（トレンドマイクロ社調べ）

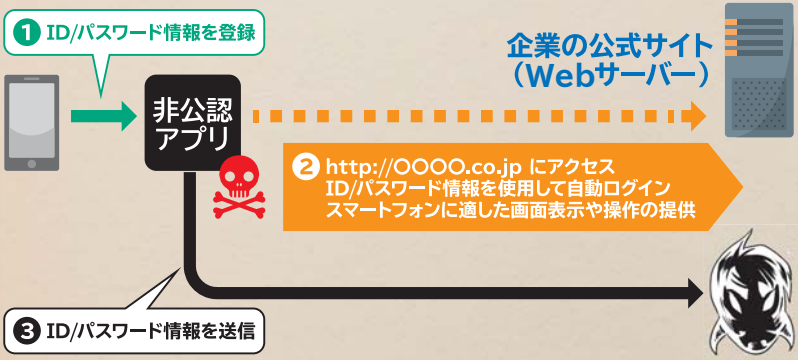
Wi-Fiを使って傍受

暗号化がされておらず、パスワードもかかっていないWi-Fiに接続すると、他者が簡単に通信情報を傍受できます。この状態でパスワードを入力すると簡単に盗まれてしまいます。



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！

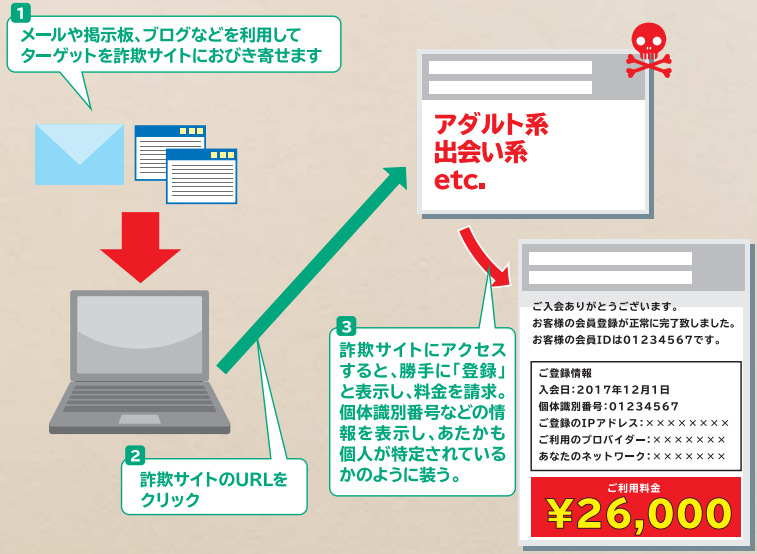
・スマートフォンのOS・ソフトウェアはアップデートする
・ウイルス対策ソフトを導入・更新する
・公式サイト以外からアプリをインストールしない
・重要なデータのバックアップを取る

MISSION 1-9

巧妙・悪質化するワンクリック詐欺

POINT 1 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」が出現しています。



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！

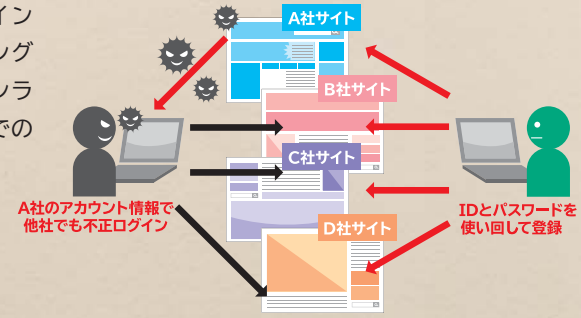
Webサービスから盗み取ったIDとパスワードを悪用し、ほかのサイトに不正ログインして、なりすましを行ったり、不正な注文をしたりする攻撃です。

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



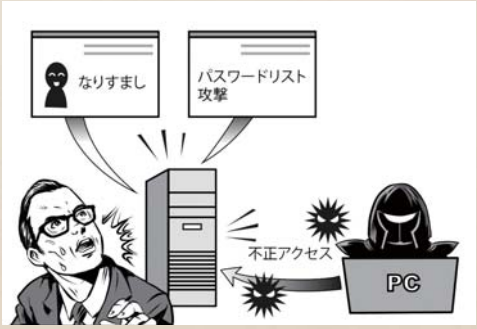
POINT 2 手口はパスワードの推測とリスト攻撃だ！

パスワードの推測

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。

パスワードリスト攻撃

別のWebサービスから窃取したIDやパスワードを使って不正ログインされます。



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**
- **多要素認証を導入する**

●サービス利用者

- **パスワードを複数のWebサービスで使い回さない**
- **パスワード管理ソフトを利用する**
- **パスワードのほか複数の認証方法を採用しているサイトを利用する**
- **利用をやめたWebサービスは退会する**

MISSION 1-11

公開された脆弱性対策情報の悪用

POINT 1 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！

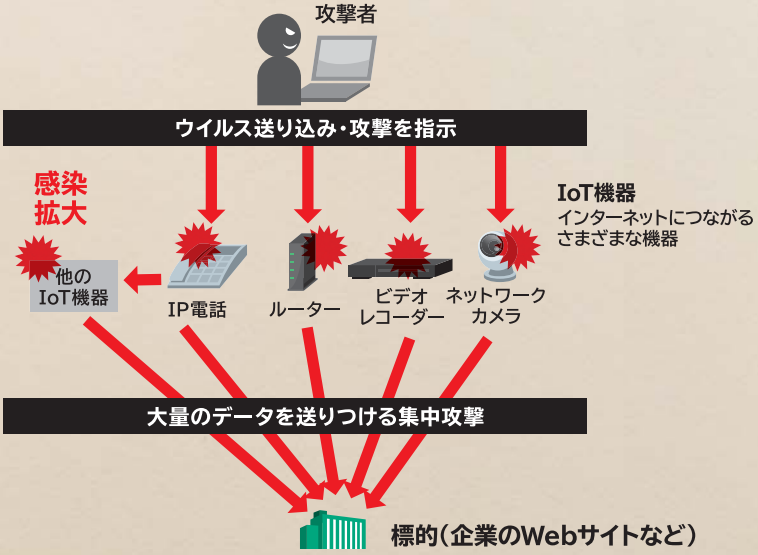
- **社内で使用しているソフトウェアの全てについて、自動更新が設定されているものと設定されていないものを把握する**
- **使っているソフトウェアに関する脆弱性情報を入手する（P49参照）**
- **使っているソフトウェアに脆弱性が発見された場合に備えて、会社全体のソフトウェアを更新する手順を作成しておく**
- **脆弱性が発見されたら、全てのソフトウェアの更新を確認し、実行する**

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！

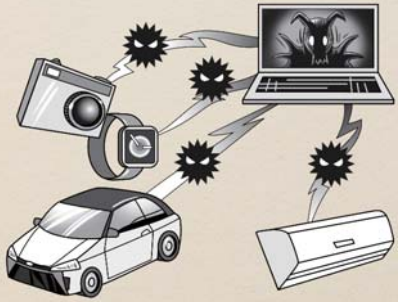
昨今は自動車やネットワークカメラ、情報家電などもインターネットにつながるようになっています（IoT※機器）。攻撃者はインターネット越しにこれらIoT機器の脆弱性や設定不備などを突いて攻撃を行い、不正アクセスやウイルス感染、さらにデータの改ざんや情報漏えい、機器操作などを行います。



※ 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。



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**
- **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**
- **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

最近の事例

業種（都道府県） 従業員規模	概　　要
製造業（東京） 51～100名	自動車部品加工製造。ランサムウェアと思われるウイルスに感染し、パソコンが使用不能になった。
製造業（栃木） 51～100名	加工食品の製造および卸売。2013年、役員のパソコンがウイルス感染し、過去の電子メールが勝手に大量発信され、自社および取引先の重要な情報が漏えい、信用が失墜。
製造業（神奈川） 6～20名	経営者宛てのメールに添付されているファイルを開いてしまった結果、ランサムウェアに感染。バックアップなどを行っていたが、個人の写真などのデータは参照できなくなった。
製造業（静岡） 51～100名	従業員がメールに添付されていたファイルを開き、ウイルス感染により自社の基幹システムが書き換わる障害が発生。復旧するまでの1週間ほど、基幹システムの一部が使用できなくなった。
卸売業（福岡） 6～20名	2010年、1台のパソコンがウイルスに感染、急きょアプリケーションの停止とネットワークからの切り離しを行ったが、完全な復旧までに2カ月を要した。
小売業（福島） 6～20名	2015年、普段使用しているパソコン画面が突然動かなくなった。地元のシステム会社にメンテナンスを依頼し確認をしてもらったところ、ウイルスに感染していることが分かった。

不動産業（埼玉） 6～20名	2017年1月、パソコンがランサムウェアに感染。感染していないデータのみをウイルスチェック可能なハードディスクに1つずつ確認しながら移行した。感染したパソコンは廃棄。
不動産業（京都） 21～50名	2016年、役員がメールの添付ファイルを開封し、1台の社内LAN 端末パソコンがランサムウェアに感染、共有サーバー内にアクセスできなくなった。再稼働には1週間以上の時間を要した。
不動産業（高知） 51～100名	業務上多くの顧客情報を保有しているが、社内のパソコンがメールを通じてウイルスに感染して対応に苦労した。何が起きているかが理解できず、外部の専門家に対処してもらった。
サービス業（栃木） 6～20名	2015年ごろ、関係者しか立ち入ることのできない設備の写真が、業務と直接関係がない非公式な文書に掲載されて委託元に送付された。調査の結果、退職した従業員の不正によるものと判明。
サービス業（神奈川） 21～50名	産業廃棄物業者。2015 年ごろ、ウイルスへの感染により、基幹システムのスローダウンやレスポンス低下などが慢性化、大きな被害はなかったものの、業務効率の低下が定常的に発生。また派遣従業員が退職する際、顧客情報データを持ち出したことが操作履歴を分析した結果、発覚した。
情報通信業（東京） 101～300名	2011年、顧客情報の入ったパソコンの紛失事故が発生した。情報漏えいなどの実害はなかったが、顧客に紛失の事実を伝え、その後信用を失うこととなった。

「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　2017年7月」情報処理推進機構（IPA）より抜粋編集

おさらいクイズ

Q ワンクリック詐欺に対して注意すべき行動として間違っているのは、次のうちどれですか。

①画像やリンクをクリックしたときに、こちらが意図しない入会完了画面や料金請求画面が表示された場合は、消費生活センターや警察などに相談する。

②意図しない入会完了画面や料金請求画面が表示されたときには、画面に表示されている問い合わせ先に電話やメールで連絡して入会を取り消す。

③信頼できるホームページかどうか、「ホームページの信頼性評価」などの機能が付いているウイルス対策ソフトを使って判断する。

ヒント

URLをクリックしただけで、意図しない入会完了画面や料金請求画面が表示され、それを信用してお金を振り込んでしまうワンクリック詐欺。これらの画面が表示されたら、無視することが適切な対策の1つです。トラブルが発生した場合には、身近な人や各種相談窓口に相談しましょう。ウイルス対策ソフトの中には、そのWebサイトが信頼できるかどうかを表示する機能を持つものもあります。Webサイトを閲覧するにはこのような機能を活用するのも有効です。架空の請求画面に表示されている問い合わせ先に連絡してしまうと、連絡に使った電話番号やメールアドレスにも請求が来るようになり、事態が悪化することもあります。

「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 ②

TOP SECRET

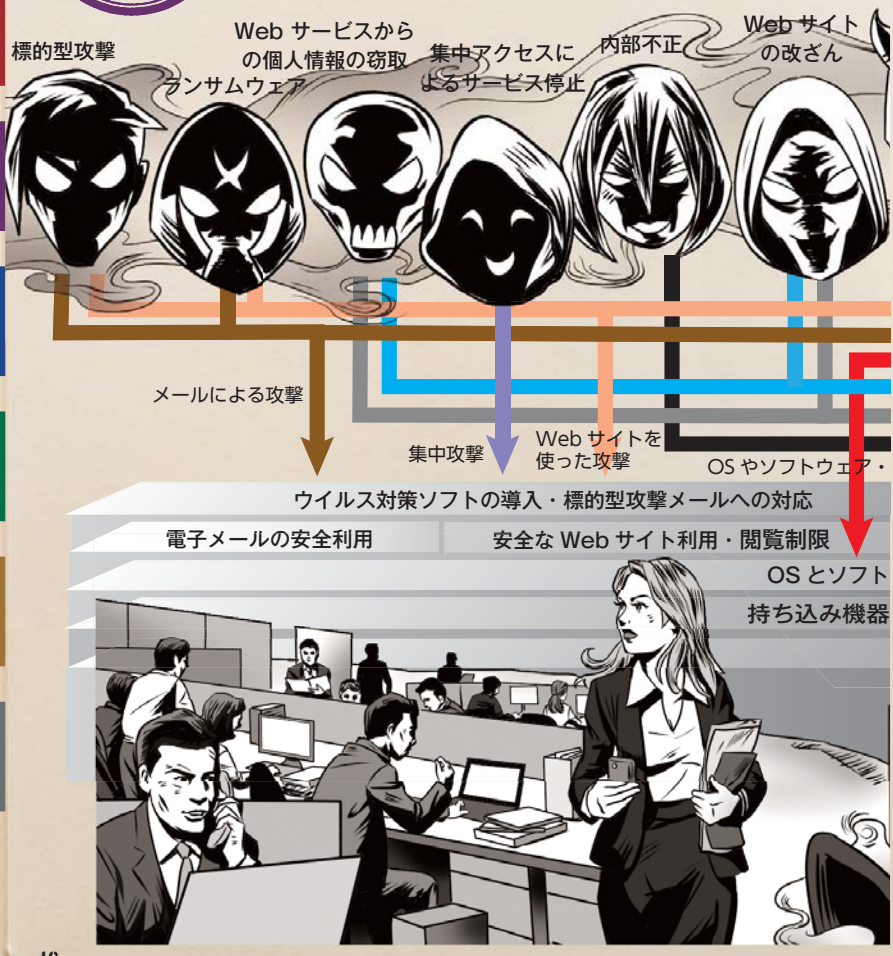
MISSION 2

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

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

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。

MISSION 2-3

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

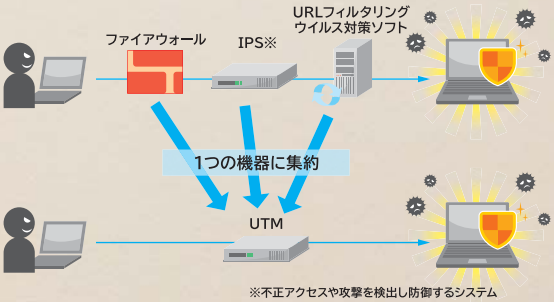
＜個別のパソコンに導入するタイプ＞

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。



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メモリーや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。

MISSION 2-4

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＞

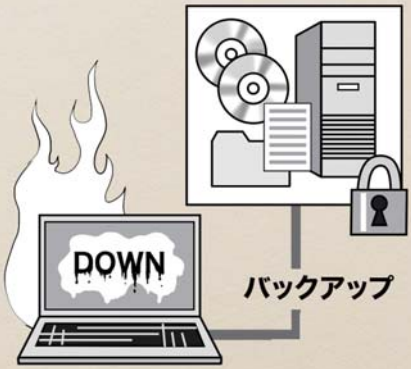
- ハードディスク（HDD）やDVDなどの外部記憶媒体に保存
- 重要情報はネットワークと切り離して保存
- 保管方法を決めておく（保管場所や保管媒体など）
- バックアップ媒体のセキュリティ対策も同時に実施
- 必要に応じて1つ前のデータも保存

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お薦めだ。

MISSION 2-5

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

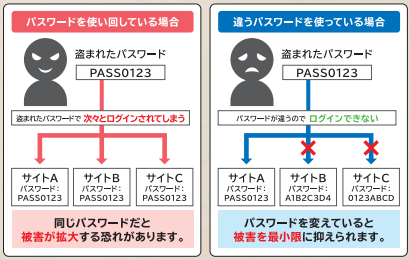
＜パスワードの強化＞

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。

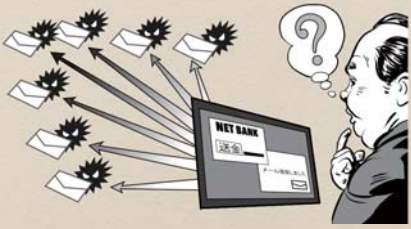
パスワードの使い回しは危険

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

■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。

※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

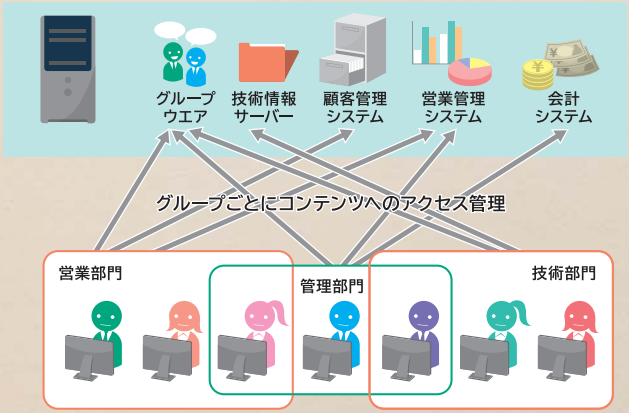
	極秘文書	機密文書	営業データ	技術データ
役　員	○	○	△	△
部　長	△	○	△	△
営業部門	×	×	○	×
技術部門	×	×	×	○

○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」の情報はこれらに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。

MISSION 2-7

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

■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 	・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** 	・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	・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。

MISSION 2-9

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

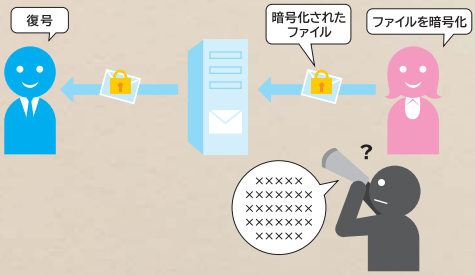
■誤送信しないように宛先や内容、添付ファイルの確認をする
■原則としてファイルを添付しない
■万一必要な場合は、添付ファイルを暗号化する

＜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

■ 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

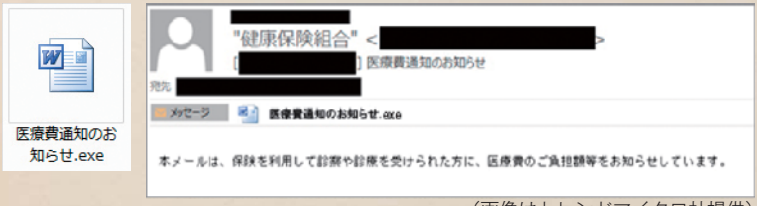
潜伏期間対策	
ウイルスの早期発見	□ウイルス対策ソフトによる各機器の感染チェック □不審な通信などの監視

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。



（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

MISSION 2-11

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。

MISSION 2-12

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ー※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ブラウザーの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

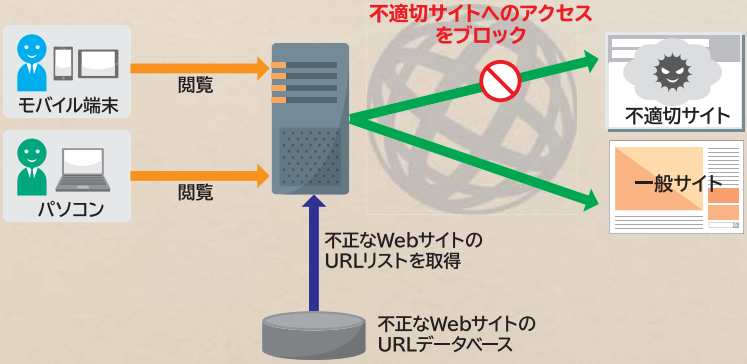
■業務に不要なWebサイトへのアクセスを制限する

<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。

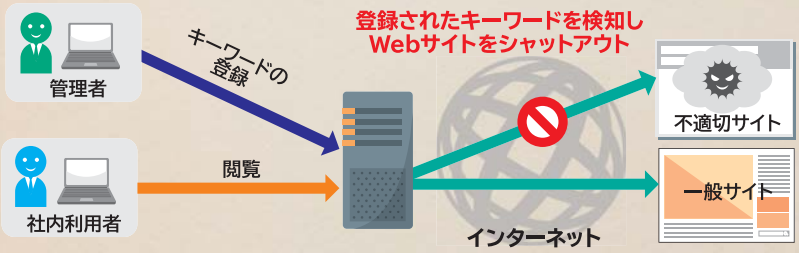
●商用サービスとURLデータベースを使った規制

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。

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

■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	・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	・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

おさらいクイズ

Q 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

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、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ことから、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を利活用することは、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ることになります。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。

情報管理が不適切な場合に問われる法律

個人情報保護法
民法第709条（不法行為による損害賠償）
建設業法
マイナンバー法
不正競争防止法
金融商品取引法

詳細な罰則規定などはP184参照

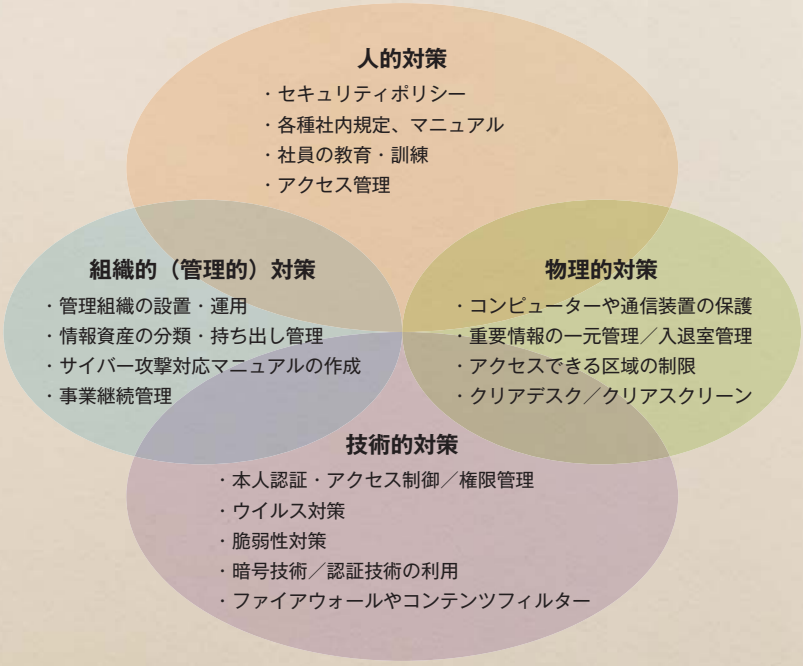
MISSION 3-4

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

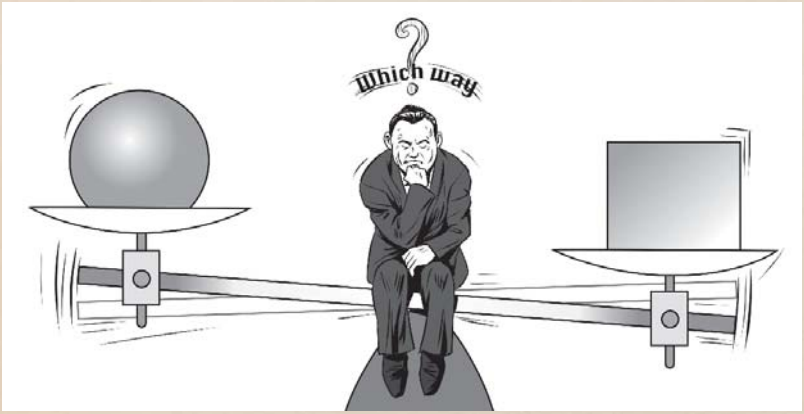
POINT 1 サイバーセキュリティ対策にかかる費用の項目

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。

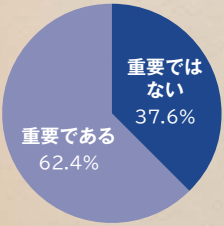


POINT 2 セキュリティ対策の投資効果を考える

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 IT投資が重要でないと考える会社はまだ４割近く



中小企業庁が実施した「中小企業の成長と投資行動に関するアンケート調査」によると、IT投資を重要ではないと考えている中小企業がまだ37.6%もあります。

※ ここでは、「最重要である」、「重要である」の回答項を「重要である」とし、「あまり重要ではない」、「重要ではない」の回答項目を「重要ではない」として集計しています。（「中小企業白書2016」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

経済産業省：攻めのIT活用指針
全国商工会連合会：簡易事業診断（IT活用編）

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。

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

【対象外】

【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

【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、P86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。

MISSION 3-7

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

POINT 1 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。

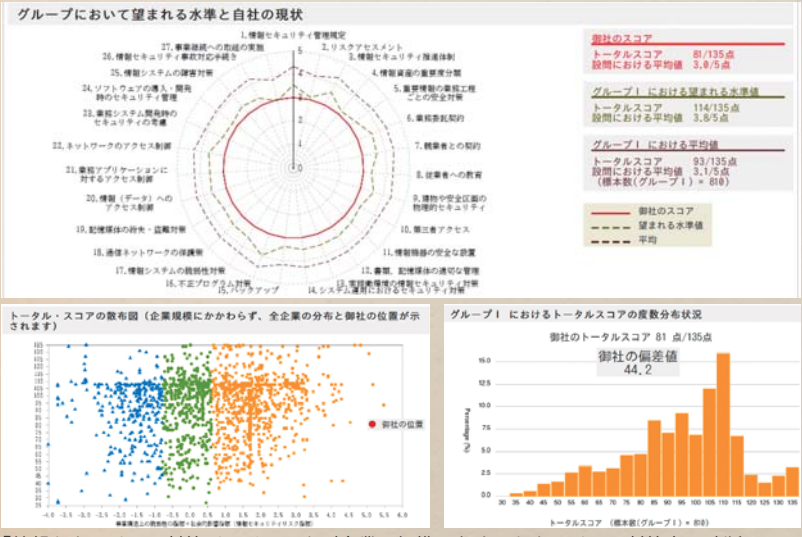
POINT 2 やってみよう！情報セキュリティ対策診断

・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（企業・組織のためのセキュリティ対策自己診断ツールVer.4.x）」（情報処理推進機構セキュリティセンター）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

経営者の皆さんが重視している経営課題の一つは、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

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

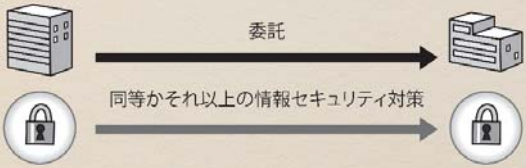
サイバー攻撃のリスクをどの程度容認するのか、セキュリティ投資をどこまでやるのか、経営者が決めなければサイバーセキュリティ対策はスタートしません。

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

重要10項目とは

リーダーシップの表明と体制の構築	1	サイバーセキュリティリスクの認識、組織全体での対応の策定
	2	サイバーセキュリティ管理体制の構築
リスク管理の枠組み決定	3	リスクの把握と対応計画の策定
	4	PDCAサイクルの実施と対策状況の開示
	5	系列企業・ビジネスパートナーの対策実施および状況把握
攻撃を防ぐための事前の対策	6	予算確保・人材配置および育成
	7	ITシステム管理の外部委託
	8	情報収集と情報共有
攻撃を受けた場合に備えた準備	9	緊急時対応体制の整備とトレーニングの実施
	10	被害発覚後の必要な情報の把握、開示体制の整備

重要項目 1	サイバーセキュリティリスクの認識、組織全体での対応の策定

POINT 1 なぜ重要か？

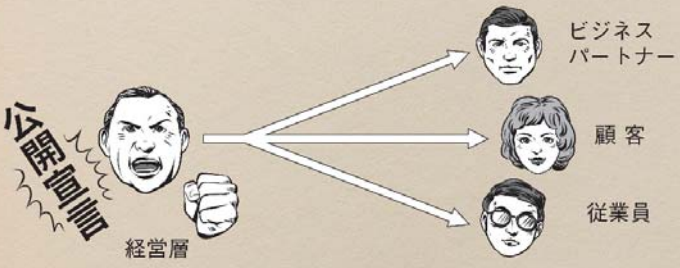
経営者がサイバー攻撃を経営リスクとして対処することを宣言することにより、全ての従業員にサイバーセキュリティ対策の重要性を周知させることができます。経営者のサイバーセキュリティ対策宣言は、顧客、取引先、株主などの信頼性を高め、ブランド価値向上につながります。

POINT 2 やるべきことはこれだ！

1. セキュリティポリシーを作成する。
   セキュリティポリシーの作成には、情報処理推進機構（IPA）から、自社の事情に応じた内容に書き換えて作成することができるサンプルが提供されています。
2. セキュリティポリシーを、顧客、取引先、株主などに宣言する。

情報セキュリティポリシー作成手順　P128

情報セキュリティポリシーサンプルを使った作成手順P180~183



重要項目 2

サイバーセキュリティ管理体制の構築

POINT 1 なぜ重要か？

仮にサイバー攻撃を受け、事業の継続性に支障が生じるようなシステム停止の判断が必要な局面で、サイバーセキュリティ管理体制を構築していない場合、経営者の判断を仰ぐしかないため、迅速に適切な対応ができない上に、責任の所在が不明確になります。

POINT 2 やるべきことはこれだ！

1. 組織内に経営者レベルの権限を持った責任者を任命する。
2. 責任者を中心としたサイバーセキュリティ管理体制を構築する。
3. サイバーセキュリティ管理体制において各関係者の責任を明確にする。

重要項目 3

リスクの把握と対応計画の策定

POINT 1 なぜ重要か？

企業の守るべき資産（個人情報や重要技術など）を把握していないと、直面するリスクを的確に把握できません。過度なリスク対策は、日常的なITの利活用を妨げ、事業活動に支障をきたす恐れがあります。また、企業として容認できない残留リスクが残る場合、想定外の損失を被る恐れがあります。

POINT 2 やるべきことはこれだ！

1. 企業の守るべき資産（個人情報や重要技術など）を決める。
2. サイバー攻撃の手口や脅威、被害状況を把握する。
3. サイバーセキュリティリスクが事業に及ぼす影響を想定し、リスクを把握する。
4. サイバーセキュリティリスクの影響の度合いに応じてリスク対策の目標や計画を策定する。また、許容できるリスクとして対策を講じないと判断したものを残留リスクとする。

重要項目 4

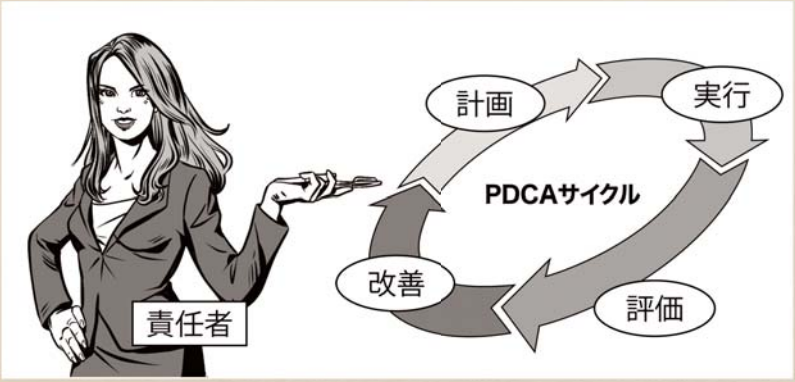
PDCAサイクルの実施と対策状況の開示

POINT 1 なぜ重要か？

PDCAサイクルを実施しないと、環境の変化に合わせて、絶えずサイバーセキュリティ対策の見直しと改善を進めることができません。適切なセキュリティ対策の状況開示が行われなかった場合、ステークホルダーの不安感や不信感を引き起こすことになり、企業価値が損なわれる恐れがあります。

POINT 2 やるべきことはこれだ！

1. サイバー攻撃のリスクに対応したPDCAを実施できる体制を整備する。
2. 常に自社のサイバーセキュリティ対策の状況を把握し、必要に応じて経営者が改善のための指示をする。
3. セキュリティ上の新たなリスクがあった場合は、必要な情報を適切に開示する。



重要項目 5	系列企業・ビジネスパートナーの対策実施および状況把握

POINT 1 なぜ重要か？

系列企業やサプライチェーンのビジネスパートナーにおいて適切なサイバーセキュリティ対策が行われていないと、これらの企業を踏み台にして自社が攻撃されることもあります。その結果、他社の二次被害の誘因となる恐れや、加害者になる恐れもあります。また、緊急時の原因特定などの際に、これらの企業からの協力を得られないことにより事業継続に支障が生じます。

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といったビジネスパートナーを含めたサイバーセキュリティ対策について、内容を契約書、報告書などで確認し状況を把握します。

重要項目 6

予算確保・人材配置および育成

POINT 1 なぜ重要か？

適切な予算が確保できていない場合、会社内でのサイバーセキュリティ対策の実施や人材の確保が困難となるほか、信頼できる外部専門会社への委託が困難となる恐れがあります。

POINT 2 やるべきことはこれだ！

1. サイバーセキュリティ対策を実施するために必要な予算を確保する。
2. 必要となる人材の確保や、継続的な社員教育を実施する。

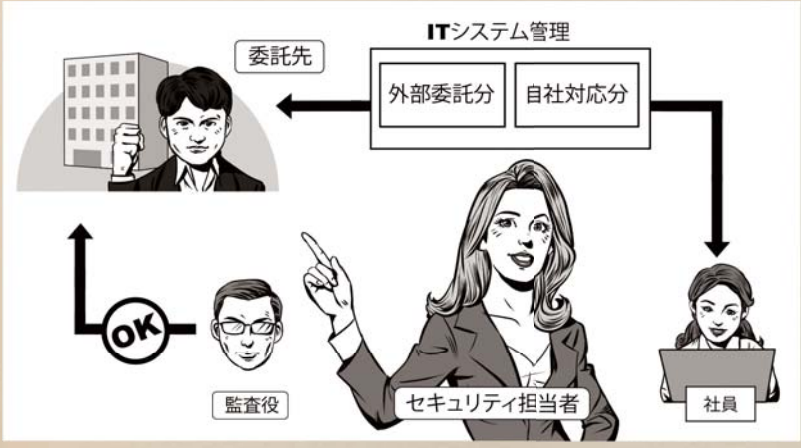
重要項目 7	ITシステム管理の外部委託

POINT 1 なぜ重要か？

ITシステムなどの運用について、自社に技術的な能力が欠ける場合はシステム管理を十分に行えず、システムの脆弱性を突いた攻撃を受ける恐れが高まります。

POINT 2 やるべきことはこれだ！

1. 自社で実施すべき対策を把握する。
2. 自社で対策できるリソースがない場合は必要に応じて外部への業務委託を検討する。
3. 外部委託先のセキュリティレベルについて、安全が確保できるように定期的に確認する。



重要項目 8

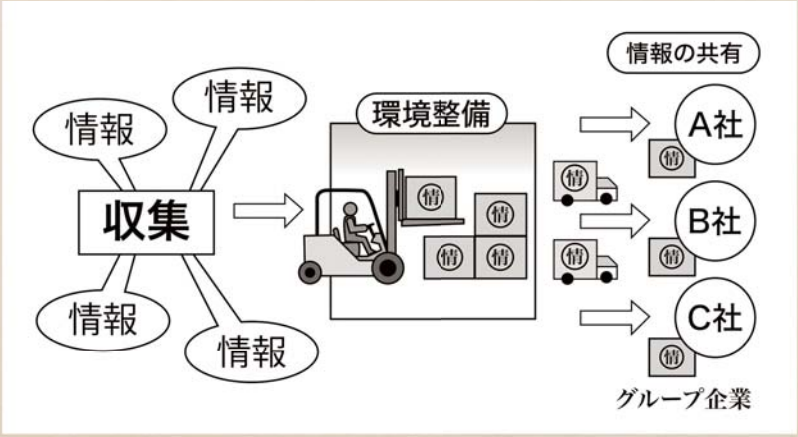
情報収集と情報共有

POINT 1 なぜ重要か？

サイバー攻撃の手法や脅威などを効率的に収集するだけでなく、自社で発見した脆弱性情報や自社に対する攻撃に関する情報を公的機関に提供したり、関連会社などの企業内グループで共有したりすることで、同様の被害が社会全体に広がることを未然に防止できます。

POINT 2 やるべきことはこれだ！

1. 情報処理推進機構（IPA）やJPCERT コーディネーションセンターなどの情報を収集して活用する。
2. 情報を収集するだけでなく、自社の情報も積極的に提供する。（P165参照）



重要項目 9	緊急時対応体制の整備とトレーニングの実施

POINT 1 なぜ重要か？

緊急時の対応体制（社内の専門部署、緊急連絡先や初動対応マニュアル）が整備されていないと、速やかな原因特定、応急処置を取ることができません。
サイバー攻撃を受けた場合は、平時とは異なる状況での判断を求められますので、さまざまなケースを想定した訓練や演習を繰り返し実施する必要があります。

POINT 2 やるべきことはこれだ！

1. 緊急連絡先や初動対応マニュアルなどを整備して対応体制をつくっておく。
2. 緊急時の対応手順の確認やトレーニングを定期的に実施する。

重要項目 10	被害発覚後の必要な情報の把握、開示体制の整備

POINT 1 なぜ重要か？

被害発覚後の対応で重要なことは、被害の拡大防止や二次被害の回避です。速やかに通知や注意喚起が行われない場合、顧客や取引先などへ被害が及ぶ恐れがあり、損害賠償請求など責任を問われる可能性があります。場合によっては法的責任を負うことにもなります。組織内情報管理の責任者である経営者が感染被害を発表しないと、ステークホルダーに対し、組織としての責任を果たしたことにはなりません。

POINT 2 やるべきことはこれだ！

1. サイバー攻撃の被害があった場合に備え、通知・報告するべき機関や関係先、またその内容を整理してマニュアル化しておく。
2. サイバー攻撃の被害について、経営者が顧客や取引先に報告・公表できるように準備しておく。

◆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 コーディネーションセンター)	・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。 (P165以降を参照)
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。

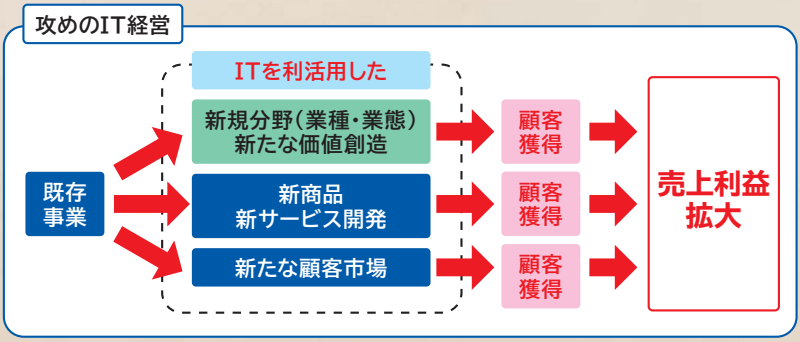
MISSION 3-11

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。
積極的かつ柔軟にIT技術を受け入れて「攻めのIT経営」で事業を発展させ、より一層顧客サービスの強化を図るためには、攻めのIT投資が必要です。



「攻めのIT経営中小企業百選」（経済産業省）より

コラム「攻めのIT経営中小企業百選」

経済産業省では、平成26年度から新たに、攻めの分野でのIT利活用に積極的に取り組み、成果を上げている中小企業を「攻めのIT経営中小企業百選」として、これまで100社の中小企業を選定しています。

◆東京の企業の例（2016年選定）

株式会社旭フーズ（卸売業）	商品在庫情報の見える化で競争力強化
芝園開発株式会社（サービス業）	IT活用による駐輪場管理ノウハウで、自治体向けビジネスを拡大
ジー・オー・ピー株式会社（サービス業）	仮設機材使用量の山積み表自動作成で、提案型営業の強化と業績拡大
株式会社ダンクソフト（情報通信業）	サテライトオフィス構築支援事業で、働き方改革を提案
株式会社築地太田（卸売業）	Tsukiji OFM Systemを活用し、海外輸出も積極拡大
プラスエンジニアリング株式会社（製造業）	年間15,000種類の多品種少量・特殊形状部品加工を一元管理する自社開発業務システム
株式会社星製作所（製造業）	デジタル経営戦略とWeb自動見積もりによる営業力強化
株式会社美萩工芸（製造業）	営業支援システムなどの活用で大幅な効率化を図る
株式会社ユウトハンズ（印刷業・情報通信業）	文書管理システムの自社導入実績を元に、印刷業から新事業へ進出

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※、ビッグデータ※、AI※、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P114を、AIはP116を参照

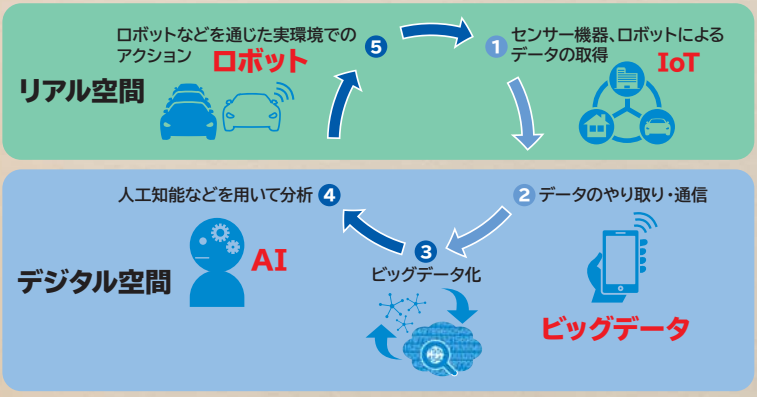
コラム IoT、ビッグデータ、AI、ロボットはつながっている

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



「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

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

2020年にはIoT機器が530億台に達すると予測されています。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が大きなビジネスチャンスになるのです。

コラム　ものづくり企業　IoT活用事例

製造業（東京都青梅市）社員数：160名
自動車用金属加工部品、医療向け部品製造

スマートフォンを活用した「見える化システム」を自社開発。
自社の現場発ノウハウを、日本の中小製造業の発展に役立ててもらうために、システムの外販を決定

事例ポイント

社内のエンジニアが「欲しいもの」「必要なもの」をシステム化し、スマートフォンなどを活用して、リアルタイムで「経営と現場の見える化」を実現

概要

- 出退勤、生産指示、在庫管理、工程不良管理、生産実績管理、品質管理、状況分析などをリアルタイムで棚卸しできる仕組み。経営と現場に「気付き」をもたらすために、独自のシステムを開発
- 生産管理を中心としたWeb版の統合管理システムに、スマートフォンなどを活用した機械の稼働データを取得するための情報収集装置を組み合わせて「経営と現場の見える化」を実現
- IoTを利用した統合情報管理システムを中小製造業でも手が届く価格帯で実現することを目指し、IT関連企業と連携して、外販に向けた取り組みを開始


スマートフォンを活用した情報収集装置

効果・メリット

現場に行かなければ分からなかった現在の作業状況を、遠隔からリアルタイムで管理可能。また作業者が入力したデータや、機械の稼働データに基づいた経営改善にも活用可能

「中小ものづくり企業IoT等活用事例集」（経済産業省 関東経済産業局 2017年）より抜粋・要約、写真転載（関東経済産業局 地域経済部 情報政策課）

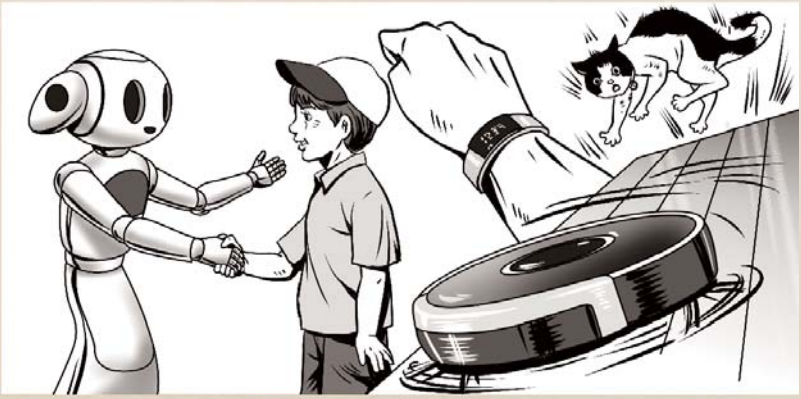
MISSION 3-14

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：Artificial Intelligence）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。



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。

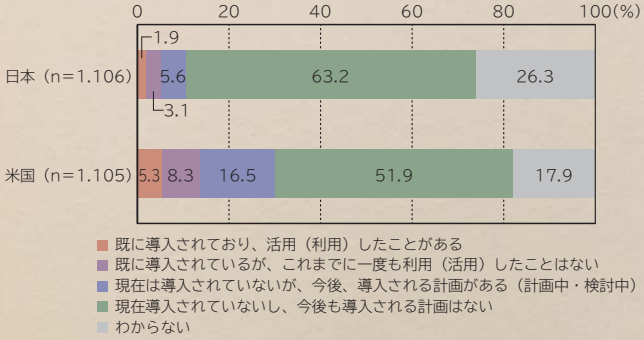
・既存業務の人材不足の解消
・不足している労働力の補完・省力化
・既存の業務効率・生産性の向上（省力化）
・新しい価値を持った業務の創出

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

最近のAI導入状況



総務省「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）より作成

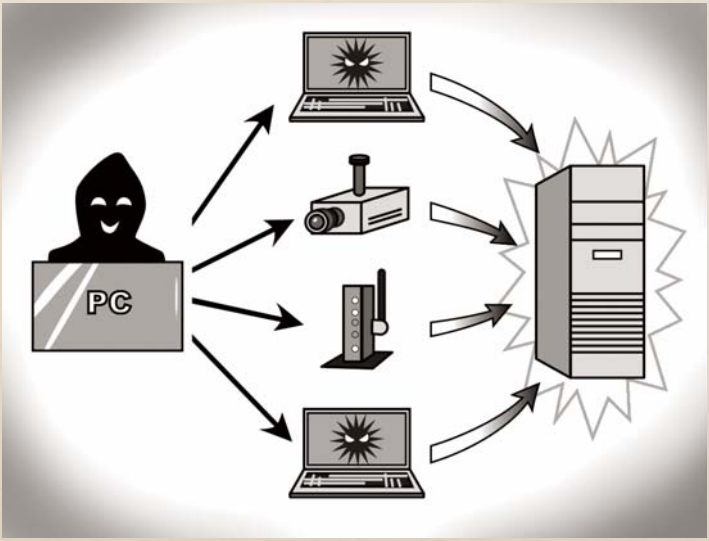
MISSION 3-15

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

これから飛躍的な増加が予想される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。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P120参照）



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

MISSION 3-16

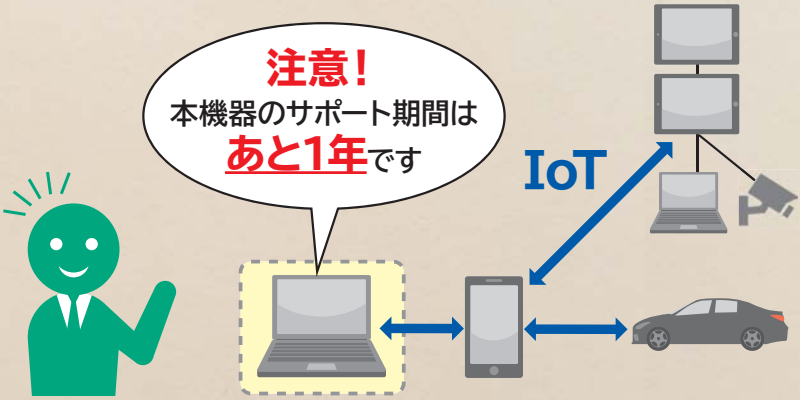
ビジネスを発展させるために（攻めのIT投資とサイバーセキュリティ対策）

IoTを活用する一般利用者のための基本ルール

POINT 1 リスクの大半は簡単な注意で回避可能

IoT機器もパソコンなどと同様、サイバーセキュリティ対策を怠ってはいけません。インターネットを経由して遠隔操作され会社の重要情報が漏えいする、機器が悪用されて犯罪に巻き込まれるなど、サイバー脅威にさらされる危険性をはらんでいるからです。

こうした脅威から会社を守るために、基本的なルールを確認しましょう。



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ので、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」など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、不正利用される恐れがあります。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。

「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

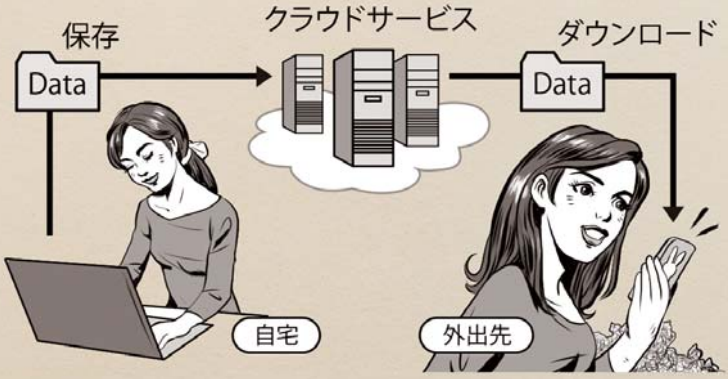
コラム クラウドサービスの活用

クラウドサービスとは

クラウドサービスは、従来は利用者が手元のパソコンなどにインストールして利用していたデータやソフトウェアを、事業者がネットワーク経由でサービスとして提供するものです。インターネットに接続できる環境であればすぐに導入できます。

<メリット>

・自社サーバーや情報処理ソフトウェアを保有する必要がなく、初期コストを抑えられる。
・常に最新のサービスを利用できる。
・メンテナンスする必要がなく運用コストが安い。
・サービスの利用範囲を必要に応じて変更できる。
・導入や維持について社内担当者の負担が軽減される。
・出張先や自宅からも利用できる。



クラウドサービス利用時の留意点

クラウドサービスでも、ネットワークを介して攻撃を受ける可能性や人為的な操作ミス、意図的な情報漏えいなど、情報セキュリティ面でのリスクは、自社でサーバーを保有する場合と同じようにあります。
自社の情報資源をクラウド事業者に委ねる以上は、十分なセキュリティ対策を備えたクラウドサービスを選んで利用することが重要です。

＜デメリット＞

・障害などによりデータが消失する可能性がある。
・サイバー攻撃に対するセキュリティ対策のレベルは事業者に委ねられている。
・アカウント情報が第三者の手に渡ってしまった場合、簡単に情報漏えいしてしまう。
・基本的にパッケージ化されたシステムが提供されるため、自由にカスタマイズしにくい。

セキュリティホールを減らす網羅的・体系的な対策の策定方法

新・5分でできる自社診断シート

すぐに活用しよう!

「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＞）には＜新・5分でできる！情報セキュリティ自社診断＞があります。25の設問に答えるだけで自社のセキュリティレベルを把握することができる自社診断シートと、その解説が付いています。

●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/keihatsu/sme/guideline/index.html
よりダウンロードできます。

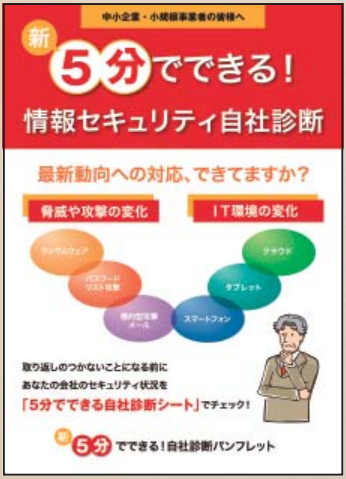
＜新・5分でできる！情報セキュリティ自社診断＞の構成

Part 1 基本的対策	OSやソフトウェアのアップデート、ウイルス対策ソフト、パスワード、アクセス制限などの基本的対策についての設問
Part 2 従業員としての対策	メールの受送信や重要情報の取り扱い、パソコン対策などについて、全ての従業員が注意しなければならないことについての設問
Part 3 組織としての対策	情報セキュリティ対策について、従業員に対する意識付けやルール、事故が発生した場合など会社が行う対策についての設問

<新・５分でできる自社診断シート>　（部分抜粋）

診断項目	No	診断内容	チェック 実施している	チェック 一部実施している	チェック 実施していない	チェック わからない	自社診断パンフレットと対応しています
Part 1 基本的対策	1	Windows Update※1を行うなどのように、常にOSやソフトウェアを安全な状態にしていますか？	4	2	0	0	P3 No.1「脆弱性対策」を参照
	2	パソコンにはウイルス対策ソフトを入れてウイルス定義ファイル※2を自動更新するなどのように、パソコンをウイルスから守るための対策を行っていますか？	4	2	0	0	P3 No.2「ウイルス対策」を参照
	3	パスワードは自分の名前、電話番号、誕生日など推測されやすいものを避けて複数のウエブサービスで使い回しをしないなどのように、強固なパスワードを設定していますか？	4	2	0	0	P3 No.3「パスワード管理」を参照
	4	ネットワーク接続の複合機やハードディスクの共有設定を必要な人だけに限定するなどのように、重要情報に対する適切なアクセス制限を行っていますか？	4	2	0	0	P3 No.4「機器の設定」を参照
	5	利用中のウェブサービス※3や製品メーカーが発信するセキュリティ注意喚起を確認して社内共有するなどのように、新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？	4	2	0	0	P3 No.5「情報収集」を参照
Part 2 従業員としての対策	6	受信した不審な電子メールの添付ファイルを安易に開いたりメール文中のリンクを安易に参照したりしないようにするなど、電子メールを介したウイルス感染に気をつけていますか？	4	2	0	0	P4 No.6「電子メールのルール」を参照
	7	電子メールを送る時には宛先に送信アドレスを確認するなどのように、宛先の誤送信を防ぐ仕組みを徹底していますか？	4	2	0	0	P4 No.7「電子メールのルール」を参照
	8	重要情報をメールで送る時は重要情報を添付ファイルに書いてパスワード保護するなどのように、重要情報の保護をしていますか？	4	2	0	0	P4 No.8「電子メールのルール」を参照
	9	無線LANを利用する時は強固な暗号化を必ず利用するなどのように、無線LANを安全に使うための対策をしていますか？	4	2	0	0	P4 No.9「無線LANのルール」を参照
	10	業務端末でのウェブサイトの閲覧やSNSへの書き込みに関するルールを決めておくなどのように、インターネットを介したトラブルへの対策をしていますか？	4	2	0	0	P4 No.10「ウェブ利用のルール」を参照
	11	重要情報のバックアップを定期的に行うなどのように、故障や誤操作などに備えて重要情報が消失しないような対策をしていますか？	4	2	0	0	P4 No.11「バックアップのルール」を参照
	12	重要情報を紙の上に放置せず書棚に保管し施錠するなどのように、重要情報の紛失や漏えいを防止する対策をしていますか？	4	2	0	0	P5 No.12「保管のルール」を参照
	13	重要情報を社外へ持ち出す時はパスワード保護や暗号化して肌身離さないなどのように、盗難や紛失の対策をしていますか？	4	2	0	0	P5 No.13「持ち出しのルール」を参照
	14	離席時にコンピュータのロック機能を利用するなどのように、他人に使われないようにしていますか？	4	2	0	0	P5 No.14「離席時の安全管理」を参照
	15	事務所で見知らぬ人を見かけたら声をかけるなどのように、無許可の人の立ち入りがないようにしていますか？	4	2	0	0	P5 No.15「事務所の安全管理」を参照
	16	退社時に机の上のノートパソコンや備品を引き出しに片付けて施錠するなどのように、盗難防止対策をしていますか？	4	2	0	0	P5 No.16「事務所の

<解説パンフレット>



MISSION 3-18

セキュリティホールを減らす網羅的・体系的な対策の策定方法

情報セキュリティハンドブック ひな形（従業員向け）

ACTION 1 すぐに活用しよう!

「情報セキュリティハンドブック（ひな形）」を使えば、従業員に自社のセキュリティルールを確認してもらうためのハンドブックが簡単に作成できます。赤い文字色で記載例があらかじめ記載されています。自社のルールに合わせて赤字を中心に修正し、また必要に応じて項目を加筆して効率よく使うことができます。

●情報セキュリティハンドブック（ひな形）
https://www.ipa.go.jp/files/000055529.pptxよりダウンロードできます。

＜内容構成＞
- 全社基本ルール
- 仕事中のルール
- 全社共通のルール
- 従業員のみなさんへ

＜情報セキュリティハンドブックひな形（従業員向け）＞（部分抜粋）

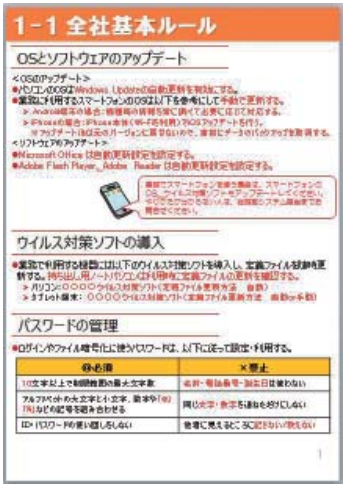

Ver 1.2

情報セキュリティ
ハンドブック
（ひな形）

ハンドブックの使い方

本ハンドブック（ひな形）は、従業員に配付し自社のセキュリティルールを確認してもらうためのものです。5分でできる！情報セキュリティ自社診断に活用しています。赤字で記載した箇所は記載例になりますので、自社のルールにあわせて赤字を黒に修正し、また必要に応じて項目を追加して、ご利用ください。

株式会社●●●●


1-1 全社基本ルール

OSとソフトウェアのアップデート

＜OSのアップデート＞
●パソコンのOSはWindows Updateの自動更新を有効にする。
●業務に利用するスマートフォンのOSは以下を参考にして手動で更新する。
- Android端末の場合：機種毎の説明を参照して必要に応じて対応する。
- iPhoneの場合：iPhone本体（Wi-Fi利用）からOSアップデートを行う。
※アップデートは日本のバージョンに変更はいやで、事前にデータのバックアップを実施する。

＜ソフトウェアのアップデート＞
●Microsoft Office は自動更新設定を設定する。
●Adobe Flash Player、Adobe Reader は自動更新設定を設定する。

重要なスマートフォン端末の場合は、スマートフォンのOS、ウイルス対策ソフトウェアをアップデートしてください。やり方がわからない人は、情報部のスタッフ担当者まで問合せください。

ウイルス対策ソフトの導入

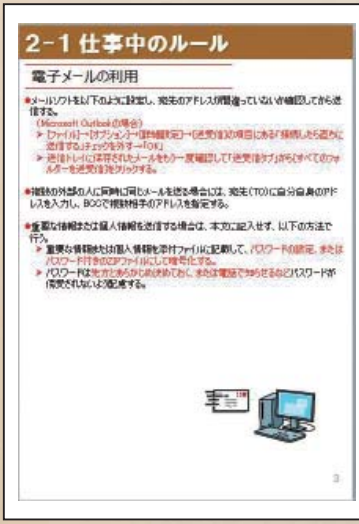
●業務で利用する機器には以下のウイルス対策ソフトを導入し、定義ファイル（辞書）を更新する。特に出入用ノートパソコンは利用毎に定義ファイルの更新を確認する。
- パソコン：○○○○ウイルス対策ソフト（定義ファイル更新方法：自動）
- タブレット端末：○○○○ウイルス対策ソフト（定義ファイル更新方法：自動or手動）

パスワードの管理

●ログインやファイル暗号化に使うパスワードは、以下に従って設定・利用する。

条件	×禁止
10文字以上で8種類数の最大文字数	名前・電話番号・誕生日は使わない
アルファベットの大文字と小文字、数字や「@」「%」などの記号を組み合わせる	同じ文字・数字を連続を使わない
ID・パスワードの使い回しをしない	他者に見えるように記録しない・残さない

1


2-1 仕事中のルール

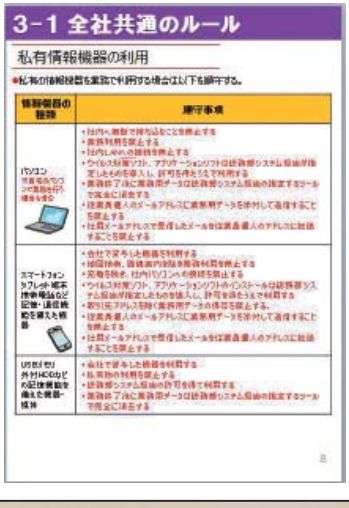
電子メールの利用

●メールソフトを以下のように設定し、宛先のアドレス間違っていないか確認してから送信する。
（Microsoft Outlookの場合）
- 「ファイル」→「オプション」→「詳細設定」→「送信時の項目にある「接続したら直ちに送信する」にチェックを外す→「OK」
- 送信トレイに正常されたメールをもう一度確認して「送受信タブ」から「すべてのフォルダーを送受信」をクリックする。

●複数の外部の人に同時に同じメールを送る場合には、宛先（TO）に自分自身のアドレスを入力し、BCCで複数相手のアドレスを指定する。

●重要な情報または個人情報を送信する場合は、本文に記入せず、以下の方法で行う。
- 重要な情報または個人情報を添付ファイルに記載して、パスワードの設定、または、パスワード付きのZIPファイルにして暗号化する。
- パスワードは先方にあらかじめ決めておく、または電話でお知らせするなどパスワードが流出されないよう配慮する。

3


3-1 全社共通のルール

私有情報機器の利用

●私有の情報機器を業務で利用する場合は以下を順守する。

情報機器の種類	順守事項
パソコン（自宅やカフェで業務を行う場合を含む）	• 社内LAN接続で持ち込むことを禁止する • 業務利用を禁止する • 社内LANへの接続を禁止する • ウイルス対策ソフト、アプリケーションソフトは会社情報システム部が指定したものを導入し、許可を得ようえで利用する • 業務終了後に業務用データは会社情報システム部への指定するツールで完全に消去する • 会社貸与者以外の業務用データの保存を禁止する。 • 従業員者本人のメールアドレスに業務用データを添付して送信することを禁止する • 社員メールアドレスで受信したメールを従業員者本人のアドレスに転送することを禁止する
スマートフォン タブレット端末 携帯電話など記憶・通信機能を備えた機器	• 会社で貸与した機器を利用する • 個人情報、会社業務情報を業務利用を禁止する • 充電を除き、社内パソコンへの接続を禁止する • ウイルス対策ソフト、アプリケーションソフトのインストールは会社情報システム部が指定したものを導入し、許可を得ようえで利用する • 紛失した際、遠隔で業務用データの消去を禁止する。 • 従業員者本人のメールアドレスに業務用データを添付して送信することを禁止する • 社員メールアドレスで受信したメールを従業員者本人のアドレスに転送することを禁止する
USBメモリ、外付けHDDなどの記憶機能を備えた機器・媒体	• 会社で貸与した機器を利用する • 私用物の利用を禁止する • 会社情報システム部からの許可を得て利用する • 業務終了後に業務用データは会社情報システム部からの指定するツールで完全に消去する

8

MISSION 3-19

セキュリティホールを減らす網羅的・体系的な対策の策定方法

情報セキュリティポリシーの明文化

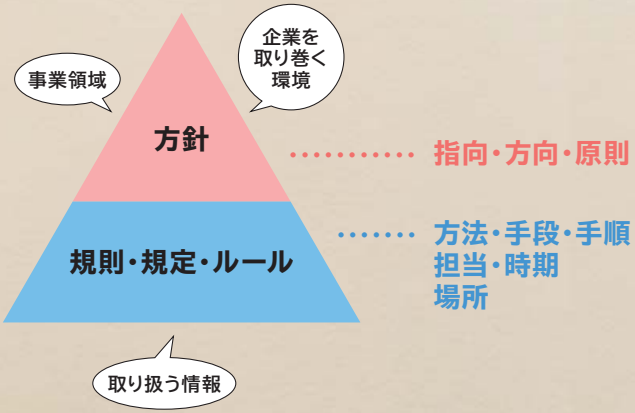
ACTION 1 すぐに活用しよう!

情報セキュリティポリシーをゼロからつくり上げるのは、多くの中小企業にとって難しい作業です。

情報処理推進機構（IPA）では、中小企業・小規模事業者向けに、情報セキュリティポリシー作成ツールを提供しています。自社のリスクを分析し、状況に合わせて情報セキュリティポリシーサンプルを編集すれば、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。

まず、こうしたツールを活用して、自社の情報セキュリティポリシーを策定し、スキルの向上とともに追加変更していきます。

情報セキュリティポリシーサンプルを使った作成手順P180~183



ポリシーの策定には「わが社の情報セキュリティポリシー（付録）」を使い、以下の手順で行います。

手順 1

情報資産管理台帳を作成する

自社で保有している情報を＜ツールA リスク分析シート＞の「情報資産管理台帳」シートへ記入例に従い書き出し、それぞれの重要度を判定してください。

重要度2　事故が起きると事業に深刻な影響がある
重要度1　事故が起きると事業に重大な影響がある
重要度0　事故が起きても事業に影響はない

手順 2

リスク値の算定

＜ツールA リスク分析シート＞の「脅威の状況」シートで想定される脅威を指定し、「対策状況チェック」シートで自社の対策状況を指定すると情報資産ごとのリスク値が計算されて対策が必要な情報資産が分かります。

リスク値4 ～ 6	大	重点的に対策を実施
リスク値1 ～ 3	中	対策を実施
リスク値　0	小	現状維持

手順 3

情報セキュリティ対策を決定

＜ツールA リスク分析シート＞の「対策状況チェック」シートで自社の対策状況を以下から選択すると、「診断結果」シートに診断結果と自社で策定すべく情報セキュリティポリシーが表示されます。

1：実施している　　・・・対策を実施済みの場合
2：一部実施している　　・・・対策を実施しているが、十分でない場合
3：実施してない／わからない　・・・対策を実施していないか、関連情報がない場合
4：自社には該当しない　　・・・当該項目に該当する業務を行っていない場合

手順 4

情報セキュリティポリシーを策定

手順3で表示された情報セキュリティポリシーを＜ツールB 情報セキュリティポリシーサンプル＞の中から選択し、自社の状況に合わせて編集すれば、自社専用の情報セキュリティポリシーが完成します。
なお必要に応じて、さらに項目を追加していただいてもかまいません。

重要度は機密性、完全性、可用性それぞれの観点での評価値から3段階で判定します。
また、被害発生可能性は、情報の内容ごとの脅威の発生頻度×脆弱性への対応状況により3段階で算定し、「リスク値＝重要度×被害発生可能性」でリスク値を診断します（手順2）。これで対策の必要な情報資産が分かります。
さらに、現段階での対策実施状況により、策定すべき情報セキュリティ対策が表示される仕組みです（手順3）。

セキュリティホールを減らす網羅的・体系的な対策の策定方法

情報資産管理台帳の作成

どのような情報資産があるか洗い出して重要度を判断する

情報セキュリティポリシーの策定に当たっては、組織の事業継続のためにセキュリティを確保すべき情報資産としてどのようなものがあるかをリストアップします。個々の情報の重要度を判断するため、情報資産管理台帳を作成し、自社の情報資産を洗い出します。

<ツールA「リスク分析シート」情報資産管理台帳　記入例>

情報資産管理台帳

業務分類	情報資産名称	備考	利用者範囲	管理部署	媒体・保存先	個人情報の種類		
						個人情報	要配慮個人情報	マイナンバー
営業	製品カタログ	現役製品カタログ一式	営業部	営業部	書類			
営業	製品カタログ	現役製品カタログ一式	営業部	営業部	可搬電子媒体			
営業	キャンペーン応募者リスト	20xx年のキャンペーン応募者情報	営業部	営業部	社内サーバー	有		
調達	委託先リスト	外部委託先(直近5年間に実績があるもの)	総務部	総務部	社内サーバー			
調達	発注伝票	発注伝票(過去10年分)	総務部	総務部	社内サーバー			
調達	発注伝票	発注伝票(過去10年分)	総務部	総務部	書類			
技術	製品設計図	現役製品の設計図	開発部	開発部	社内サーバー			
❶技術	❷製品設計図	❸現役製品の設計図	❹開発部	❺開発部	❻書類	❼		

ACTION 2 情報資産管理台帳の作成

情報処理推進機構（IPA）では、中小企業・小規模事業者向けに、情報資産管理台帳作成ツールを提供しています。

作成ツールのテンプレートを活用すると効率的に情報資産管理台帳を作成できます。作成ツールでは、情報資産の機密性※や完全性※、可用性※それぞれの評価値を記入し重要度を判定します。

さらに、「脅威の状況」「対策状況チェック」の2枚のシートでリスク値を診断します。

組織的対策や人的対策など11項目について対策状況チェックの診断結果が表示されます。

※ 機密性、完全性、可用性についてはP72参照。

	評価値				保存期限	登録日	現状から想定されるリスク（入力不要・自動表示）					
	機密性	完全性	可用性	重要度			脅威の発生頻度（「脅威の状況」シートで設定）	脆弱性（「対策状況チェック」シートで設定）	被害発生可能性		リスク値	
	0	1	1	1		2016/7/1	2:特定の状況で発生する（年に数回程度）	2:部分的に脆弱性未対策	1	可能性：低	1	リスク中
	0	1	1	1		2016/7/1	2:特定の状況で発生する（年に数回程度）	2:部分的に脆弱性未対策	1	可能性：低	1	リスク中
	2	1	0	2		2016/7/1	3:通常の状態で発生する（いつ発生してもおかしくない）	2:部分的に脆弱性未対策	2	可能性：中	4	リスク大
	0	1	1	1		2016/7/1	3:通常の状態で発生する（いつ発生してもおかしくない）	2:部分的に脆弱性未対策	2	可能性：中	2	リスク中
	1	0	0	1		2016/7/1	3:通常の状態で発生する（いつ発生してもおかしくない）	2:部分的に脆弱性未対策	2	可能性：中	2	リスク中
	1	0	0	1		2016/7/1	2:特定の状況で発生する（年に数回程度）	2:部分的に脆弱性未対策	1	可能性：低	1	リスク中
	2	2	2	2		2016/7/1	3:通常の状態で発生する（いつ発生してもおかしくない）	2:部分的に脆弱性未対策	2	可能性：中	4	リスク大
	2	2	2	2		2016/7/1	2:特定の状況で発生する（年に数回程度）	2:部分的に脆弱性未対策	1	可能性：低	2	リスク中

おさらいクイズ

Q1 **サイバーセキュリティ対策について、誤りがあるものは次のうちどれですか。**

①まずは事業推進のため社内のIT化を一気に行うことを優先し、サイバーセキュリティ対策は収益が上がってから取り組みたい。

②サイバー攻撃を受けた際の被害想定額が支出可能な対策費を上回ってしまったので、残留リスクを下げる対策を講じる。

③経営者は経営に専念し、サイバーセキュリティ対策は現場の従業員に任せておいた方がよりよい対策ができると思う。

④系列企業やビジネスパートナーが対策を実施しているかどうかを確認したり把握したりする必要性は全くない。

⑤全従業員を対象に必要な知識を習得してもらうべくセミナーを開催した。

⑥攻撃を受けて情報漏えいした可能性が疑われたが、明確な証拠がなかったので、特に何もしなかった。

Q2 **IoTセキュリティガイドラインに定められているIoT機器を使用する際の基本ルールとして、正しいものは次のうちどれですか。**

①問い合わせ窓口やサポートサービスのない機器の使用は控える。
②初期設定のID・パスワードはそのまま使う。
③使用しなくなった機器の電源プラグは抜く。
④パスワードは誰でも分かりやすいものにする。
⑤アップデートを実施する。

答え 1. ①③④⑥　2. ①③⑤

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」付録3の作成ツール「情報セキュリティポリシーサンプル」の「11.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」を活用すれば、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。

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。	136ページ
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。	136ページ

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。	137ページ
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。	137ページ
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。	138ページ
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の対応を決めます。	140ページ
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の対応を決めます。	143ページ
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。	145ページ
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。	146ページ
想定されるリスク	事業の中断が想定される大規模災害などを検討します。	146ページ
復旧責任者および関連連絡先	想定する大規模災害等が発生し、事業が中断した際の復旧責任者の役割および関係者連絡先について確認します。	147ページ
事業継続計画	被害対象に応じて復旧から事業再開までの計画を立案します。	147ページ

P136～147に記載例を示します。

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 対応責任者
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	一次対応者
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	一次対応者

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	一次対応者	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

ACTION 2 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します。

MISSION 4-5

対応手順3

ウイルス感染時の初期対応

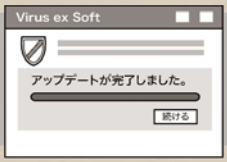
ACTION 1 従業員が対応可能な場合

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。

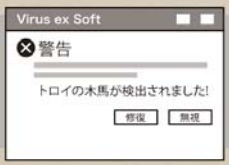
STEP1 ネットワークからコンピューターを切断します。

STEP2 システム管理者に連絡します。

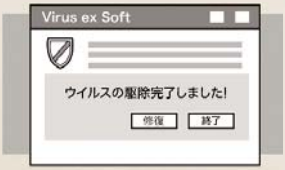
STEP3 ウイルス対策ソフトの定義ファイルを最新版に更新します。



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）

ウイルスの届け出

郵送、FAX、E-mail、Webにて受け付けしています。
届け出の際は、Webサイトにある届出様式を使用してください。
Web：https://www.ipa.go.jp/security/outline/todokede-j.html
FAX：03-5978-7518
E-mail：virus@ipa.go.jp
※郵送先については、Webサイトにてご確認ください。

不正アクセスに関する届け出

FAX、E-mailにて受け付けしています。
届け出の際は、Webサイトにある届出様式を使用してください。
Web：https://www.ipa.go.jp/security/ciadr/index.html
FAX：03-5978-7518
E-mail：crack@ipa.go.jp

相談

情報セキュリティ安心相談窓口
主に電話、E-mailにてご相談を受け付けしています。
電話：03-5978-7509
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
※詳細については、Webサイトをご覧ください。
https://www.ipa.go.jp/security/anshin/index.html

大規模災害などによる事業中断と事業継続管理

会社のITシステムが直面するリスクには、サイバー攻撃などの人為的なリスクのほかに、大規模災害や停電など環境的なリスクもあります。こうしたリスクによって、ITシステムが使えなくなり、長期の事業中断を余儀なくされるケースもあります。企業の経営者は、こうした環境リスクの影響により、会社の事業が中断した場合に備えておく必要があります。

想定されるリスクをリストアップする

ITシステムが重大な被害を受け、事業を中断しなければならないリスクをリストアップします。

- 大型地震の発生に伴う設備の倒壊・損壊（電源設備や空調機など）
- 通信会社の事故による回線の途絶
- 落雷による一部地域の停電

ACTION 2 復旧責任者および関連連絡先

リストアップしたリスクに基づいて被害対象となる設備と復旧の責任者、関係者の連絡先を整理しておきます。

被害対象	復旧責任者	関係者連絡先
電源設備 空調機	総務部長	○○電力△△支店 (株)○○設備
(○○システム) ハードウェア ソフトウェア ネットワーク機器 回線サービス バックアップクラウド サーバー	対応責任者 システム管理者	(株)○○システム開発 (株)△△ネットワーク サービス (株)◇◇マネージド サーバー
顧客	営業部長	営業部取引先リスト参照
従業員人的被害	総務部長	従業員名簿参照

ACTION 3 事業継続計画

対応責任者は、想定する大規模災害などの被害が発生し、事業が中断した際の復旧責任者の役割認識および関係者連絡先について、有効に機能するか検証します。

復旧責任者は、被害対象に応じて復旧から事業再開までの計画を立案します。

ワークショップ 自社でやろう サイバー攻撃への対応リアクション

ある日、JPCERT コーディネーションセンターという団体から次のような連絡を受けました。

「あなたの会社から官公庁に対するサイバー攻撃が行われています。」

担当者から連絡を受けたあなた（経営者）はどうしますか。

1. そんなことはないだろうと考え、そのまま事業を継続する。
2. 事業を継続しながら、原因を探すよう指示する。
3. いったん全てのネットワークを遮断し、原因を探すよう指示する。

正解はもちろん3です。

1は論外です。もしかすると損害賠償を請求されることにもなりかねません。できれば2と考えたいところですが、どの端末が汚染されているのか分からない状況では事業を継続しながらでは不十分です。

ではどのような原因が考えられますか。

1. レンタルサーバーを利用しているWebサーバーが乗っ取られ、他社のネットワークの弱点を探すための不正な動作をしている。
2. 会社内の端末の1つがウイルスに感染して、ウイルスが入ったメールを官公庁や他の企業に送り続けている。
3. 会社内の端末の1つがウイルスに感染して、会社内にある従業員のメールアドレスやマイナンバーなどの個人情報、取引先情報などをひそかに送り続けている。

正解は全てです。

他の会社や官公庁に対するサイバー攻撃の拠点になっているということは、あなたの会社の端末が乗っ取られていて、誰にも分からないように外部からコントロールされているということですから、全ての原因が考えられます。

TOP SECRET

MISSION 5

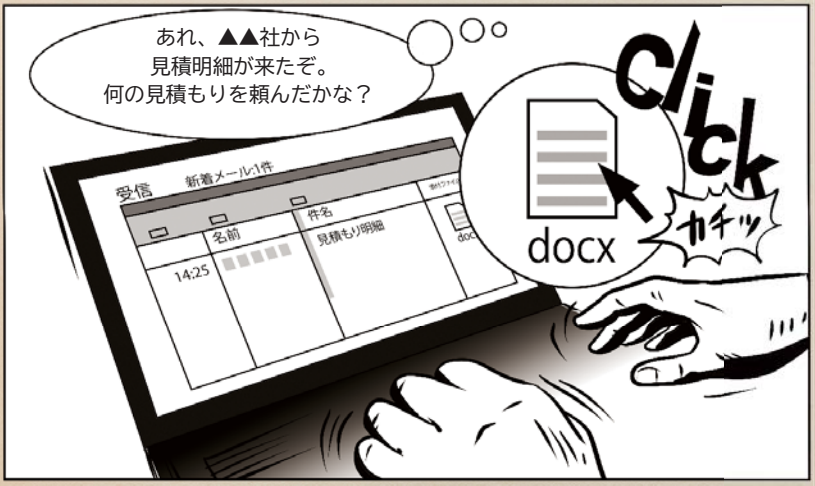
やってみよう! サイバー攻撃対策シミュレーション

SCENE 01

サイバー攻撃前夜

SCENE 02

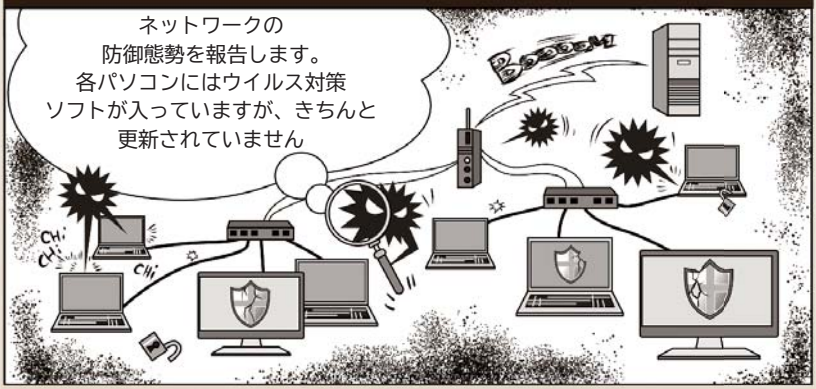
攻撃発生その瞬間

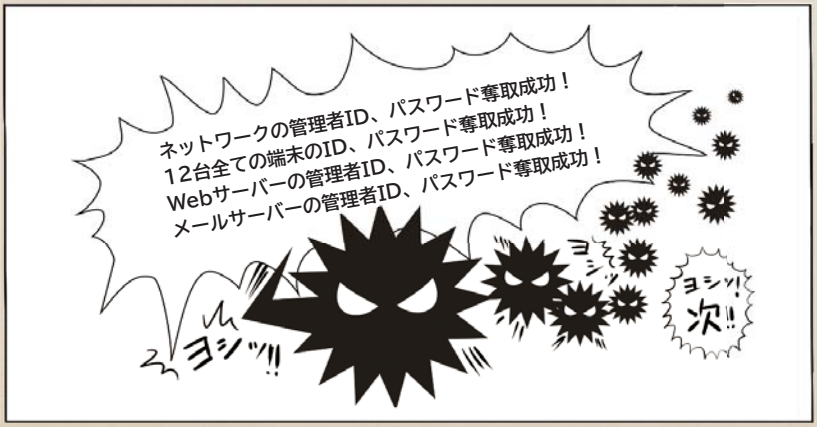


SCENE 03

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

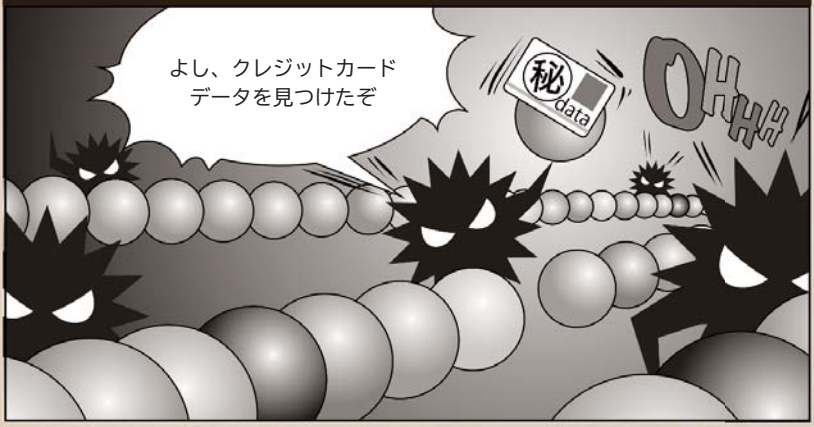


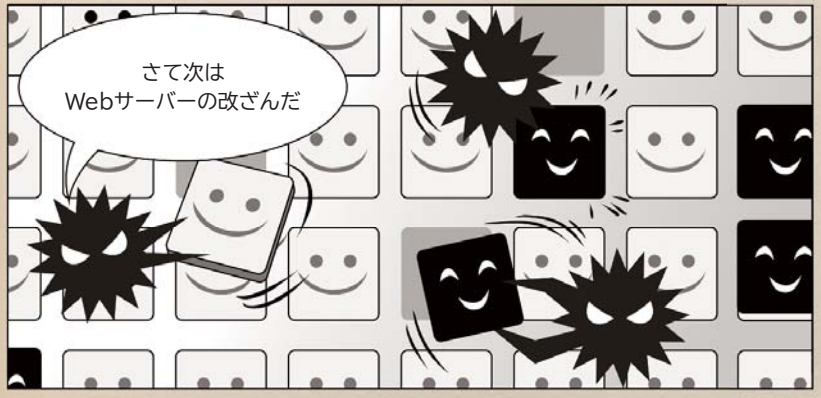


SCENE 04

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





SCENE 05

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

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

SCENE 09

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

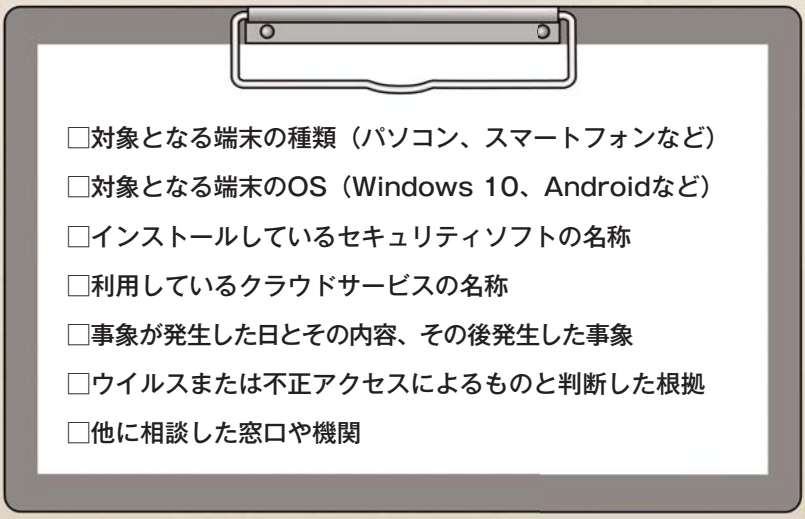
不自然な通信をしているプログラムがないか、外部から不正なログオンが行われていないか、監視します。

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のでは？と思ったら、次ページの緊急連絡先に連絡するに当たって、事前に次のような情報を整理しておきましょう。



□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（Windows 10、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 緊急連絡先

警視庁 サイバー犯罪対策課　03-3431-8109
受付時間：平日8:30－17:15
専門の警察官が、サイバー犯罪に関わる相談や情報提供を電話で受け付けています。
http://www.keishicho.metro.tokyo.jp/sodan/madoguchi/sogo.html

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）情報セキュリティ安心相談窓口
03-5978-7509　E-mail　anshin@ipa.go.jp
受付時間：10:00－12:00　13:30－17:00　土日祝日・年末年始を除く
ウイルスおよび不正アクセスの技術的な相談に対してアドバイスが受けられる、IPAの窓口です。
https://www.ipa.go.jp/security/anshin/index.html

CHECK ウイルスおよび不正アクセス被害の届け出

ウイルスを発見または感染した場合、あるいは不正アクセス被害に遭った場合、被害の拡大と再発防止に役立てるため、情報処理推進機構（IPA）では情報提供を受け付けています。それぞれ以下のサイトから届け出をしましょう。

ウイルスに関する届け出
https://www.ipa.go.jp/security/outline/todokede-j.html

不正アクセスに関する届け出
https://www.ipa.go.jp/security/ciadr/index.html

やられる前に、しっかり予防を！

サイバー攻撃から会社を守るための情報源

☑ソフトウェアの脆弱性と対策情報を知りたい
☑情報流出、フィッシングサイト、不正侵入など被害を最小限に抑えたい
☑脅威発生状況の把握、手口の分析、再発防止のための助言が欲しい

一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）
https://www.jpcert.or.jp/

☑インターネットを利用した金融犯罪や情報流出の情報が欲しい
☑eコマースに対する脅威、ウイルスの脅威への対策を考えたい
☑サイバー犯罪の被害が懸念される警戒情報を知りたい

一般財団法人 日本サイバー犯罪対策センター（JC3）
https://www.jc3.or.jp/

☑さまざまなサイバー脅威情報、脆弱性情報、攻撃予兆情報を収集し共有したい
☑信頼できる企業同士で、お互いに問題解決したい

日本シーサート協議会
http://www.nca.gr.jp/

☑フィッシングサイト、ワンクリック詐欺、クレジットカード不正使用などインターネット取引におけるトラブルの相談に乗ってほしい

消費者庁 消費者ホットライン
188（全国共通）
http://www.caa.go.jp/region/shohisha_hotline.html

☑迷惑メールに関して相談に乗ってほしい
☑迷惑メールの情報や特定電子メール法に基づく対策を知りたい

一般財団法人 日本データ通信協会（JADAC） 迷惑メール相談センター
03-5974-0068
http://www.dekyo.or.jp/soudan/index.html

☑フィッシング詐欺情報と注意事項を知りたい
☑フィッシングの動向分析・技術的対策・法的対策を知りたい

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

☑「中小企業の情報セキュリティ対策ガイドライン」対応製品やサービスを知りたい
☑マイナンバー対応について、あらゆる情報が欲しい
☑情報セキュリティに関する調査・研究情報が知りたい
☑情報セキュリティに関するセミナーやイベントに参加したい

特定非営利活動法人 日本ネットワークセキュリティ協会
http://www.jnsa.org/

☑なりすましECサイト（電子商取引）の被害状況や対処法を知りたい

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
https://www.saferinternet.or.jp/narisumashi/

☑どうしたら脆弱性対策ができるのか知りたい
☑ソフトウェア製品の脆弱性や対策情報を知りたい
☑必要な脆弱性対策情報を効率よく入手したい

警察庁 サイバー犯罪対策プロジェクト 脆弱性の対策には
http://www.npa.go.jp/cyber/kanminboard/siryou/sec_hole/vuln_solution.html

CHECK

主な情報セキュリティベンダー

株式会社アンラボ（主な製品）AhnLab MDS
http://jp.ahnlab.com/site/main.do
株式会社カスペルスキー（主な製品）Kaspersky Endpoint Security for Business
http://www.kaspersky.co.jp/
株式会社シマンテック（主な製品）Symantec Endpoint Encryption
https://www.symantec.com/ja/jp/
ソフォス株式会社（主な製品）Endpoint Protection
https://www.sophos.com/ja-jp.aspx
ソースネクスト株式会社（主な製品）ZERO スーパーセキュリティ
http://www.sourcenext.com/
トレンドマイクロ株式会社（主な製品)ウイルスバスター ビジネスセキュリティサービス
http://jp.trendmicro.com/
エフセキュア株式会社（主な製品）プロテクション サービス ビジネス
https://www.f-secure.com/
マカフィー株式会社（主な製品）McAfee Endpoint Protection for SMB
http://www.mcafee.com/japan/

情報処理推進機構（IPA ）「主なワクチンベンダーのWebサイト等一覧」より

CHECK

Tcyss相談窓口
（東京中小企業サイバーセキュリティ支援ネットワーク）

サイバー攻撃に遭った！
会社の情報が流出してしまった…
セキュリティ対策って、どうすればいい？
そんなときのために、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。

困ったら、まずはお電話を **03-5320-4773**※

窓口での受付は　**東京都産業労働局商工部内（都庁第一本庁舎30階北側）**※

※電話、窓口とも受付時間は都庁開庁日の9:00～12:00、13:00～17:00

Webサイトからは　**東京都電子申請　中小企業サイバーセキュリティ対策相談**
http://www.sangyo-rodo.metro.tokyo.jp/chushou/shoko/cyber/

情報セキュリティ5カ条

最低限のルール「情報セキュリティ5カ条」

情報セキュリティ対策に詳しくなくても、まずはここから！

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！

パスワードは英数字記号含めて10文字以上に！
名前、電話番号、誕生日、簡単な英単語などは使わない！
同じID・パスワードをいろいろなWebサービスで使い回さない！

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！

情報セキュリティ用語解説

CHECK 個人情報

特定の個人を識別できる場合は全て「個人情報」という扱いを受けることになります。
たとえ姓（名字）だけでは誰かを特定できないとしても、その姓（名字）に「○□△会社に勤務」「東京都○△区○△町△番地在住」などのプロフィール情報が加われば、その人が誰であるかを特定できますので、個人情報となります。つまり、ほとんどの情報が個人情報だといっても過言ではありません。

CHECK 改正個人情報保護法

2015年9月に改正され、2017年5月30日に全面施行された「個人情報保護法」で、保有する個人情報が5,000人以下の中小企業も新たに「個人情報取扱事業者」と定められました。つまり、個人情報をベースに活動する者全てが同法の義務を負うことになったのです。
そのポイントをまとめると、次のようになります。
①身体的特徴も個人情報です。
②人種、信条、病歴など差別や偏見を生む可能性のある個人情報を取得するときは、必ず本人の同意を得なければなりません。
③個人情報を本人以外の第三者に渡すときは、あらかじめ本人の同意を得なければなりません（ただし、生命、身体、財産の保護が必要なときには不要）。
④個人情報データベースに含まれる個人情報を第三者に提供する場合も本人の同意を得なければなりません。さらに、個人情報保護委員会への届け出も必

要です。また、提供者は提供年月日や情報の受領者氏名などを記録し保存することも義務付けられています。

⑤特定の個人を識別できないように個人情報を加工し、そこから個人情報を復元できないようにしてビッグデータなどに利用することができるようになりました。

CHECK プライバシーマーク

こんなマークを見たことはありませんか。
これはプライバシーマークといいます。
「個人情報」をルールや手続きに従って安全に取り扱い、管理することのできる会社だけが使うことができるマークです。

プライバシーマークを取得するためには、審査に合格する必要があります。審査では、その会社が「個人情報」をどのように取り扱い、管理しているかを審査されます※。

通信販売など大量の個人情報を取り扱う会社は、このマークを取得しましょう。

※ 基準はJIS Q 15001をベースとして、「個人情報保護法」「個人情報保護法に関するガイドライン」「地方自治体による個人情報関連の条例」「業界団体の個人情報関連のガイドライン」などを審査に取り入れています

CHECK 不正競争防止法改正と営業秘密の保護強化

不正競争防止法は、公正な競争を妨げる行為を禁止し、適正な競争を活性化させて、公正な市場を守るための法律です。

同法は2015年に改正されましたが、ここで「営業秘密の保護強化」が図られました。

ポイントは次の通りです。

①処罰の対象が拡大

- 営業秘密を不正に開示した者からその秘密を取得して開示した者、さらにそれを取得して開示した者というように、2次3次と不正に関わった者は、全て処罰されます。
- 不正取得や不正開示が未遂だったとしても、処罰されます。
- 他人の営業秘密を不正に使用して生産したり輸出入したりすると、処罰されます。
- 海外のサーバーに保管された営業秘密を海外で不正使用しても、処罰されます。

②罰則の強化

- 罰金刑の上限が引き上げられました。
- 営業秘密侵害で得た犯罪収益は、裁判所の判断で没収されることもあります。

③民事救済の実効性を向上

- 損害賠償請求の際、民事訴訟法上は原則原告が「侵害した者（被告）が違法に取得した技術を使った」ことを立証しなければなりませんが、この改正により被告がそれを実証することとし、原告の立証負担を軽くしました（立証責任の転換）。
- 営業秘密の不正使用に対する差し止め請求の期間制限が10年から20年に延長されました。

CHECK 外部委託契約とSLA（Service Level Agreement）

こんな経験や疑問はありませんか？

・サービスを委託したが、お互いに食い違いが生じてトラブルになった。

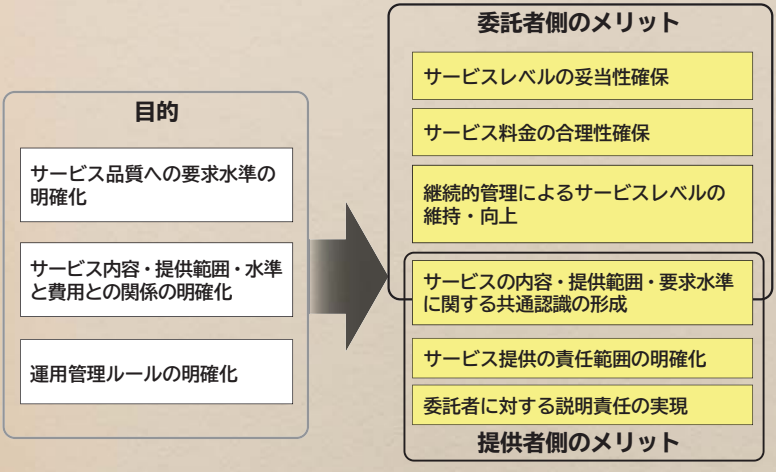
・委託されたサービスの品質と費用が見合っているのか不明瞭。

・人材コストが上がり、サービスの提供が続けられるか不安。

サービスの委託者と提供者との間で役割分担や責任の所在があいまいなままだったり、委託業務の量的変化や人材コストの変化などが影響するサービス提供の継続性について、あらかじめ契約に明示されていなかったりすると、双方にトラブルが生じます。

このような問題を解消するために、①サービス品質への要求水準の明確化②サービス内容・提供範囲・水準と費用との関係の明確化③運用管理ルールの明確化を図り、文書化します。それがSLAです。

これにより、以下のように委託者・提供者双方にメリットが生じます。



「情報システムに係る政府調達への SLA導入ガイドライン」（経済産業省）より

CHECK マイナンバーのセキュリティ考慮事項

事業者は従業員の源泉徴収票作成時にマイナンバーを取り扱いますが、マイナンバーを含む個人情報（「特定個人情報」といいます）は、個人情報保護法とは取り扱いが異なり、さらに厳格に保護されなければならないので、要注意です。
マイナンバーはマイナンバー法でルールが定められています。次のポイントを守ってください。

1　社員番号への使用は禁止

マイナンバーはマイナンバー法で規定された社会保障、税、災害対策に関する事務以外に使用できません。たとえ本人の同意があったとしても、社員番号に使うというようなことはできません。

2　漏えい防止対策を確実に

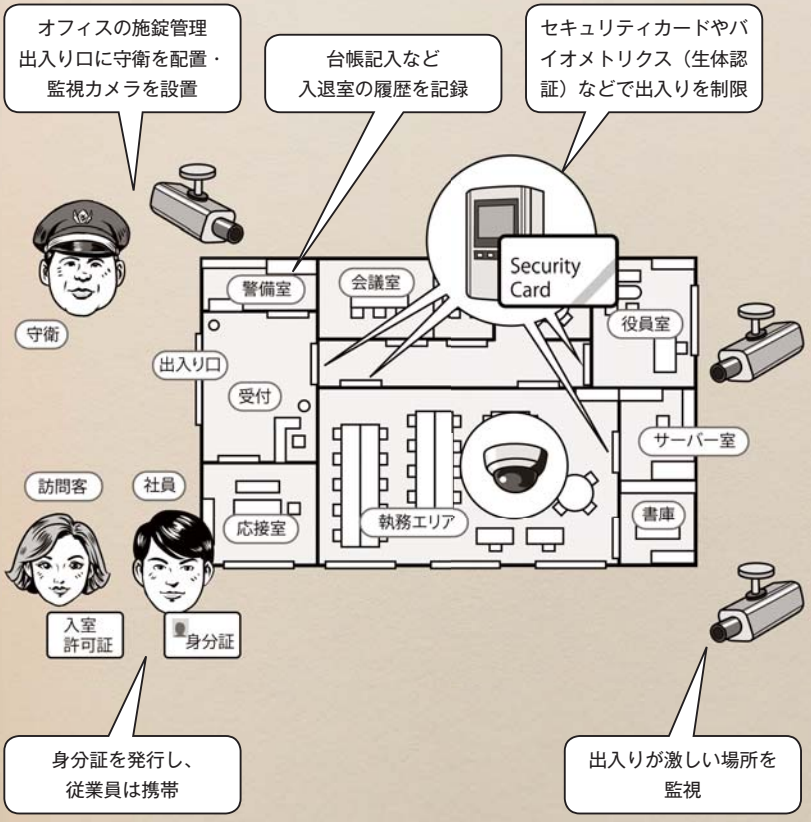
漏えいを防止するためマイナンバーの保管は厳重に行ってください。
もし、税理士や社会保険労務士などに外部委託する場合には、①委託先との契約には秘密保持義務や情報の持ち出し禁止などを盛り込み、適切に監督すること②再委託をする場合は委託元の許諾を得ること③不正アクセスを防止する対策を取ることが求められます。

3　不要になったら即廃棄

マイナンバー法で規定された場合を除き、特定個人情報を収集または保管してはいけません。
不要になったら、マイナンバーをできるだけ速やかに廃棄するか削除しなければなりません。
ただし、マイナンバーを復元できない程度にマスキングしたり削除したりした上で、他の個人情報の保管を継続することはできます。

CHECK 物理（環境）的セキュリティ

企業には正社員のほか派遣社員、アルバイト、パートなどの従業員、さらにはさまざまな訪問客がオフィスを出入りします。そのため、オフィスへの入退管理を強化し、容易に情報や情報機器に触れられることのないような対策が必要です。以下の図のような、オフィスの施錠管理や入退室管理、監視カメラの設置といった対策が物理（環境）的セキュリティです。



セキュリティお役立ちリンク

情報処理推進機構（IPA）情報セキュリティ	http://www.ipa.go.jp/security/index.html
脆弱性対策	http://www.ipa.go.jp/security/vuln/index.html
情報セキュリティ対策	http://www.ipa.go.jp/security/measures/index.html
情報セキュリティ啓発	http://www.ipa.go.jp/security/keihatsu/features.html
届け出・相談・情報提供	http://www.ipa.go.jp/security/outline/todoke-top-j.html
JPCERT コーディネーションセンター（JPCERT/CC）	https://www.jpcert.or.jp/
緊急情報を確認する	https://www.jpcert.or.jp/menu_alertsandadvisories.html
JPCERT/CCに依頼する	https://www.jpcert.or.jp/menu_reporttojpcert.html
公開資料を見る	http://www.jpcert.or.jp/menu_documents.html
JVN脆弱性対策情報データベースMyJVNバージョンチェッカ	http://jvndb.jvn.jp/apis/myjvn/#VCCHECK
警視庁　情報セキュリティ広場	http://www.keishicho.metro.tokyo.jp/kurashi/cyber/index.html
注目情報	http://www.keishicho.metro.tokyo.jp/kurashi/cyber/joho/index.html
セキュリティ対策	http://www.keishicho.metro.tokyo.jp/kurashi/cyber/security/index.html
インターネット上における犯罪に関する情報提供	http://www.keishicho.metro.tokyo.jp/kurashi/cyber/Internet_crime.html
サイバー犯罪に関する情報提供	https://www.keishicho.metro.tokyo.jp/anket/jiken_cyber.html

警察庁　サイバー犯罪 対策プロジェクト　官民ボード	http://www.npa.go.jp/cyber/kanminboard/seikabutsu.html
内閣サイバーセキュリティセンター	https://www.nisc.go.jp/security-site/office/index.html
総務省　国民のための 情報セキュリティサイト	http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/
国民生活センター インターネットトラブル	http://www.kokusen.go.jp/topics/internet.html
東京くらしWEB 架空請求対策（STOP！架空請求！）	http://www.shouhiseikatu.metro.tokyo.jp/torihiki/taisaku/
日本サイバー犯罪対策センター （JC3）　情報提供	https://www.jc3.or.jp/info/index.html
日本産業協会　迷惑メール情報提供	http://www.nissankyo.or.jp/spam/index.html
日本データ通信協会 迷惑メール相談センター	http://www.dekyo.or.jp/soudan/index.html
インターネットホットライン 連絡協議会	http://www.iajapan.org/hotline/
JNSAソリューションガイド	http://www.jnsa.org/JNSASolutionGuide/IndexAction.do
ここからセキュリティ！	http://www.ipa.go.jp/security/kokokara/
インターネットを楽しむために	https://www.jaipa.or.jp/elt/
個人情報保護委員会 中小企業サポートページ （個人情報保護法）	https://www.ppc.go.jp/personal/chusho_support/
日本ネットワークセキュリティ協会 マイナンバー対応のための 情報ポータル（企業向け）	http://www.jnsa.org/mynumber/index.html

情報セキュリティポリシーサンプル

わが社の情報セキュリティポリシーを策定する

情報処理推進機構（IPA）のWebサイト（https://www.ipa.go.jp/security/keihatsu/sme/guideline/index.html）から「中小企業の情報セキュリティ対策ガイドライン」付録3のツールをダウンロードし、以下の手順に沿って自社に合った情報セキュリティポリシーを策定してみましょう。

1　情報資産管理台帳を作成します

⑴＜ツールA＞リスク分析シート内の「情報資産管理台帳」シートに、社員名簿や給与データなど自社で保有している情報を記入例に従って入力します。
⑵それぞれの情報について機密性や完全性などの評価値を決めると、重要度が判定されます。

2　リスク値を算定します

⑴＜ツールA＞内の「脅威の状況」シートで、書類やパソコンなど保存先ごとに想定される脅威を指定すると、「情報資産管理台帳」に反映されます。
⑵「対策状況チェック」シートで、組織的セキュリティ対策やマイナンバー対応などの対策状況を指定します。情報資産ごとのリスク値が自動計算され、脆弱性と被害発生の可能性が「情報資産管理台帳」に反映されます。

3　情報セキュリティ対策を決定します

これまでの判定結果が＜ツールA＞内の「診断結果」シートに反映されます。そこに自社で策定すべく情報セキュリティポリシーが表示されます。

4　情報セキュリティポリシーを策定します

⑴＜ツールA＞内の「診断結果」シートに表示された情報セキュリティポリシーを＜ツールB＞情報セキュリティポリシーサンプル（下表）の中から選択します。

⑵自社の状況に合わせて項目を追加するなど、自社専用の情報セキュリティポリシーを編集します。

＜ツールB＞「情報セキュリティポリシーサンプル」表紙より

本ツールは、中小企業向けの情報セキュリティポリシーのサンプルです。ツールAの結果をもとに自社に必要なサンプルを選択し、自社で実施する対策に編集することで自社の情報セキュリティポリシーを作成することができます。
※赤字箇所は、自社の事情に応じた内容（役職名、担当者名など）に書き換えて下さい。
※青字箇所は、自社の事情に応じた文言を選択して下さい。

目　次

以下はサンプル項目のうちの1つです。
必要に応じて項目を追加したり文言を追加したりすれば、自社に合ったオリジナルの情報セキュリティポリシーが完成します。

5	アクセス制御及び認証	改訂日	20yy.mm.dd
適用範囲	情報資産の利用者及び情報処理施設		

1. アクセス制御方針
社外秘又は極秘の情報資産を扱う情報システム又はサービスに対するアクセス制御は以下の方針に基づいて運用する。対象となるシステム等は「9.1 アクセス制御対象情報システム及びアクセス制御方法」に記載する。
●「情報資産管理台帳」の利用者範囲に基づき、利用者の業務・職務に応じた必要最低限のアクセス権を付与する。
●特定の情報資産へのアクセス権が、同一人物に集中することで発生し得る不正行為等を考慮し、複数名に分散してアクセス権を付与する。

2. 利用者の認証
社外秘又は極秘の情報資産を扱う社内情報システムは、以下の方針に基づいて利用者の認証を行う。認証方法等は「9.2 利用者認証方法」を参照のこと。
●利用者の認証に用いるアカウントは、利用者1名につき1つを発行する。
●複数の利用者が共有するアカウントの発行を禁止する。

3. 利用者アカウントの登録
利用者の認証に用いるアカウントは、代表取締役又は情報セキュリティ責任者の承認に基づき登録する。アカウント名の設定条件は「9.3 利用者アカウント・パスワードの条件」を参照のこと。

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

5. パスワードの設定
利用者の認証に用いるパスワードは、以下に注意して設定する。パスワードの設定条件は、「9.3 利用者アカウント・パスワードの条件」を参照のこと。
●十分な強度のあるパスワードを用いる。
●他者に知られないようにする。

6. 従業員以外の者に対する利用者アカウントの発行
当社の取締役又は従業員以外の者にアカウントを発行する場合は、代表取締役又は情報セキ

文中の赤字の部分を自社の事情に応じた内容に書き換えます。

6	物理的対策	改訂日	20yy.mm.dd
適用範囲	情報処理設備が設置される領域		

1. セキュリティ領域の設定

当社内で扱う情報資産の重要度に応じて社内の領域を区分する。区分した領域内では以下を実施する。

レベル 1 領域	本社受付・応接スペース・商談室・倉庫
利用者	従業員、社外関係者、部外者が立ち入り可
施錠	最終退室者による施錠
設置可能情報機器	ディスプレイ、プロジェクター、ホワイトボード
制限事項	未使用時に社外秘又は極秘の情報資産の放置禁止
部外者管理	従業員の許可を受けて入室可能
管理記録	ー
侵入検知	ー
来客用名札	着用不要
火災対策	火災検知器、消化器設置

レベル 2 領域	本社執務室・社長室・書庫・工場・営業所
利用者	従業員以外の入室は従業員の許可又はエスコートが必要
施錠	最終退室者による施錠及び警備会社への通報装置作動
設置可能情報機器	ディスプレイ、プロジェクター、ホワイトボード、パソコン、複合機、電話機
制限事項	情報機器・設備の無断操作禁止・無断持出し禁止
部外者管理	従業員/受付守衛/総務部受付の許可を受けて入室可能
管理記録	入退室を所定様式に記録
侵入検知	センサーによる警備会社通報
来客用名札	要着用
火災対策	スプリンクラー、消化器設置

レベル 3 領域	サーバールーム
利用者	予め登録された者
施錠	常時施錠及び警備会社への通報装置作動、鍵の管理責任者

文中の青字の部分は自社の事情に応じた文言を選択します。

CHECK 情報管理が不適切な場合の処罰など

情報の種類	根拠法による規定		処罰など
個人情報 （マイナンバーを含む）	個人情報保護法	1）虚偽申告・命令違反	６カ月以下の懲役または30万円以下の罰金、業務停止命令
		2）データベース提供罪	１年以下の懲役または50万円以下の罰金
	民法（不法行為による損害賠償、709条）		損害賠償
	建設業法		役員または使用人が懲役刑に処せられた場合は営業停止処分
	マイナンバー法 （個人および法人に対して）		秘密を漏らし、または盗用した者は、３年以下の懲役もしくは150万円以下の罰金 行為者を雇用する法人に対しても罰金
他社から預かった 秘密情報 （外部非公開のデータなど）	不正競争防止法の営業秘密 不正取得・利用行為など		損害賠償、信頼回復措置
自社の秘密情報 （非公開のノウハウなど）	不正競争防止法の営業秘密 不正取得・利用行為など		善管注意義務違反に対する関係者からの損害賠償請求（経営者に対する民事訴訟）
上場会社の株価に影響を与える可能性のある重要な未公開の内部情報	金融商品取引法		内部情報をもとに取引が行われた場合、罰金または課徴金の可能性

「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2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
サイバー攻撃について	情報セキュリティ10大脅威 2017	IPA
	サイバー攻撃ってなに？	NISC
	サイバーセキュリティ 2017	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.3～	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	2016年版中小企業白書	中小企業庁
	平成28年版情報通信白書	総務省
	IT人材白書2017	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

MEMO

中小企業向け
サイバーセキュリティ対策の極意

平成29年11月発行
編集・発行　東京都産業労働局商工部調整課
新宿区西新宿二丁目8番1号
電話番号　03（5320）4770

印刷

印刷物規格表　第1類
印刷番号　（29）17

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）

※掲載の情報は平成29年8月現在のものです。

中小企業向け
サイバーセキュリティ対策の極意

東京都