TOP SECRET

MISSION 1

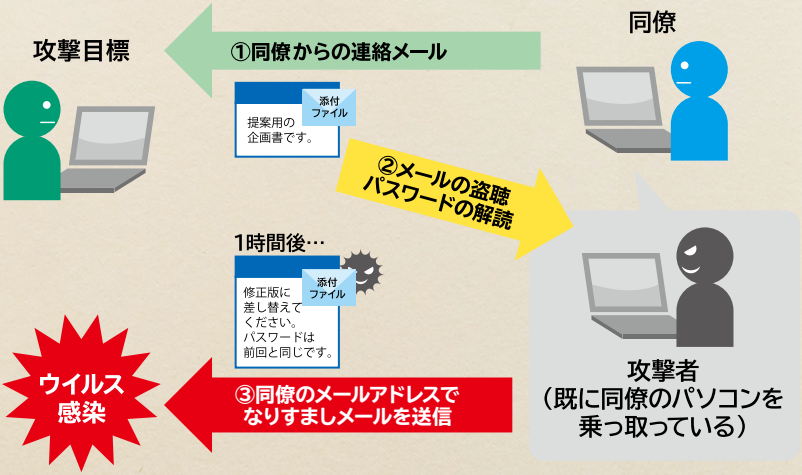
知っておきたい サイバー攻撃の知識

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

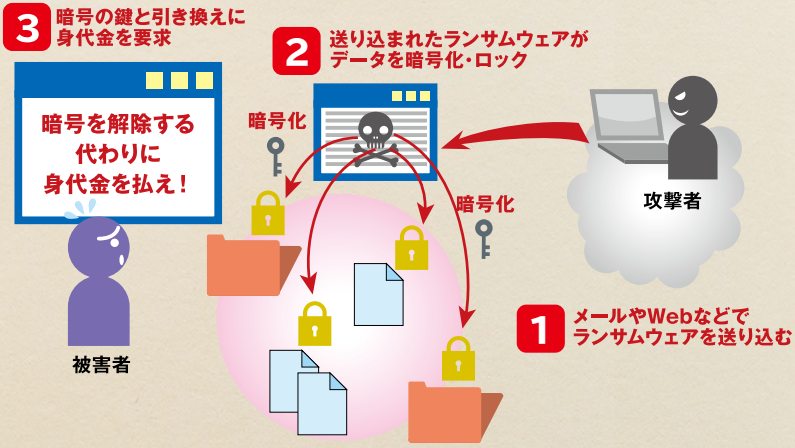
・日本語の言い回しが不自然なメール
・差出人のメールアドレスとメール本文の署名に記載されたメールアドレスが異なるメール
・これまで届いたことがない公的機関からのお知らせ
・心当たりのないメールだが、興味をそそられる内容
・心当たりのない決済や配送通知
・論理的に自分に送られてくることがおかしいメール

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！

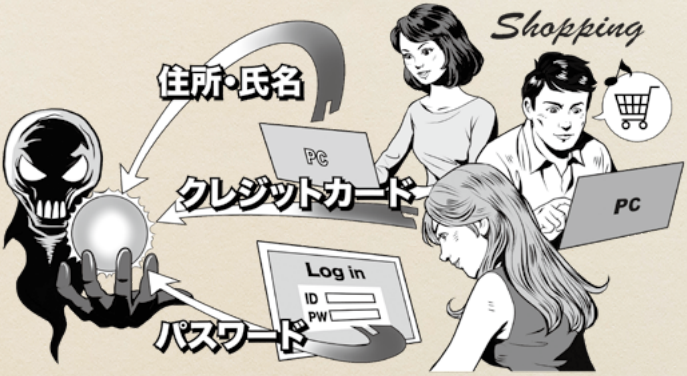
ランサムウェアによって、感染したパソコンだけではなく、共有サーバーや外付けハードディスクに保存されているファイルも暗号化される。ウイルス対策ソフトの導入はもちろん、OS※やソフトウェアを常に最新に保つことに加え、小まめにファイルのバックアップを取得し、パソコンやサーバーから切り離して保管しておくべきだ。

※ 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！

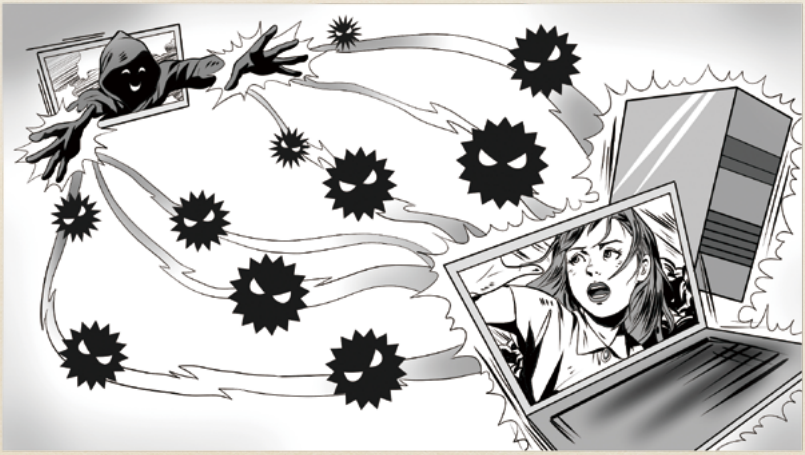
●サービスを提供する場合
- **WebサーバーのOSやソフトウェア、Webアプリケーションを最新の状態にする**
- **Webサイトに対する攻撃を検知・防御するセキュリティソフトの導入と定期的なソフトウェアアップデート**
- **適切なログの取得と継続的な監視**

●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

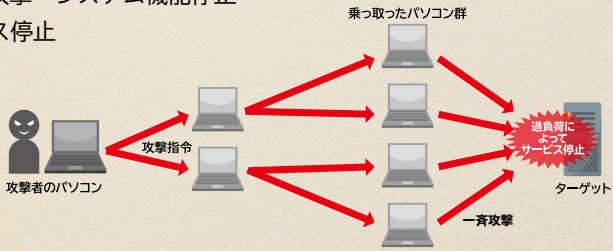
サーバーに処理速度をはるかに上回る大量の要求が集中すると、利用者はそのサーバーにアクセスできない状態になり、最終的にはサーバーがダウンしてしまいます。インターネット回線の容量がオーバーして、接続不能に陥ることもあります。



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。

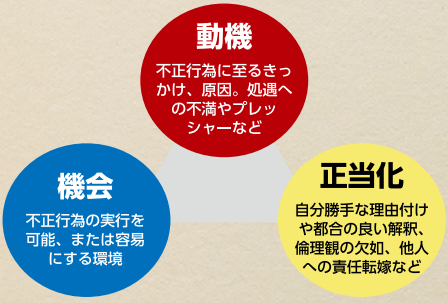
POINT 3 企業の信用が失墜し、賠償が求められる

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

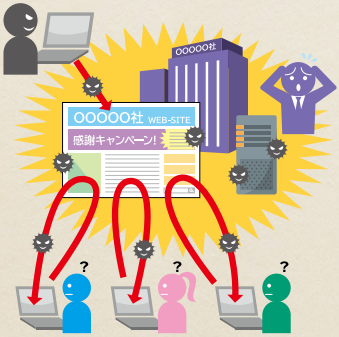
POINT 1 改ざんの目的は2つ

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。

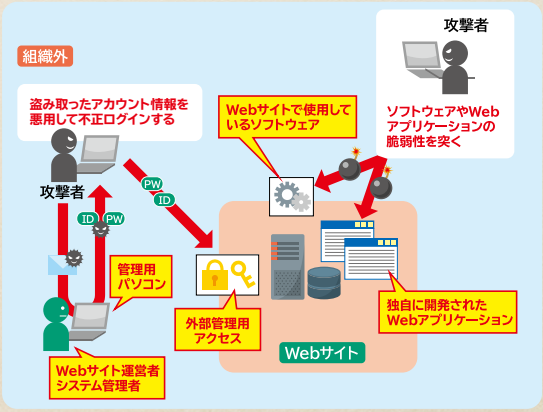
POINT 3 手口は脆弱性攻撃と管理用アカウントの乗っ取り

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。

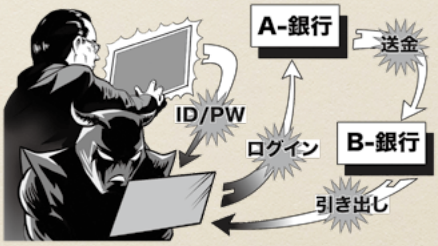
POINT 2 手口はフィッシング詐欺と不正送金ウイルス

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**

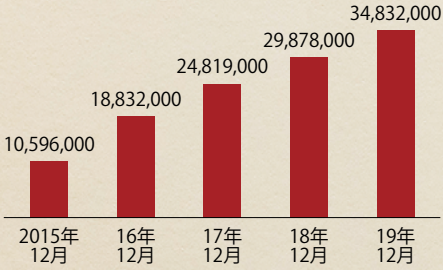
悪意のあるスマホアプリ

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

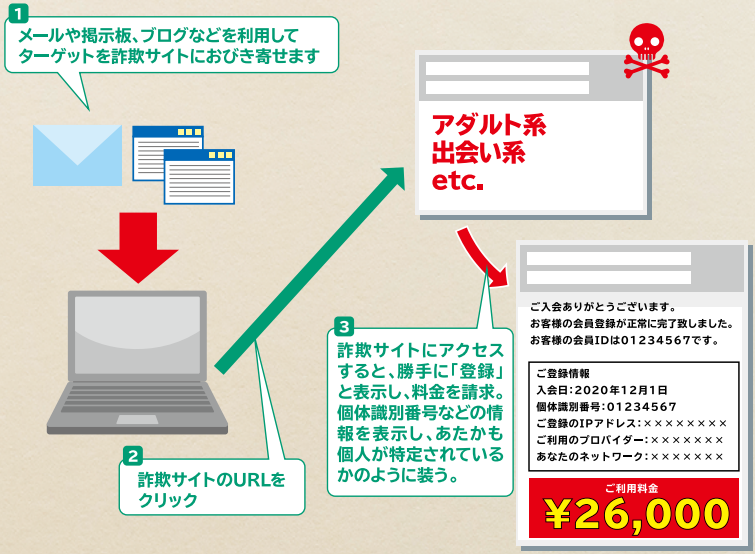
スマートフォンにもセキュリティ対策が必要だ！

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

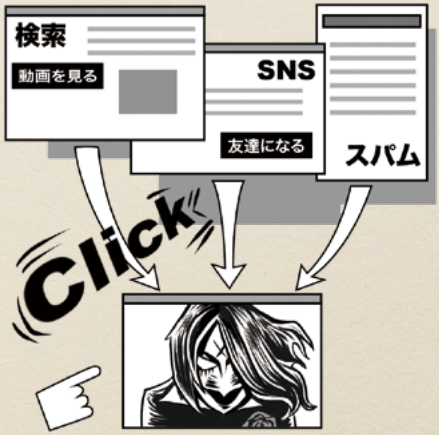
サイトを見ただけで請求！

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！

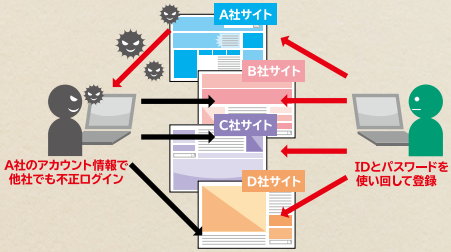
Webサービスから盗み取ったIDとパスワードを悪用し、ほかのサイトに不正ログインして、なりすましを行ったり、不正な注文をしたりする攻撃です。

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！

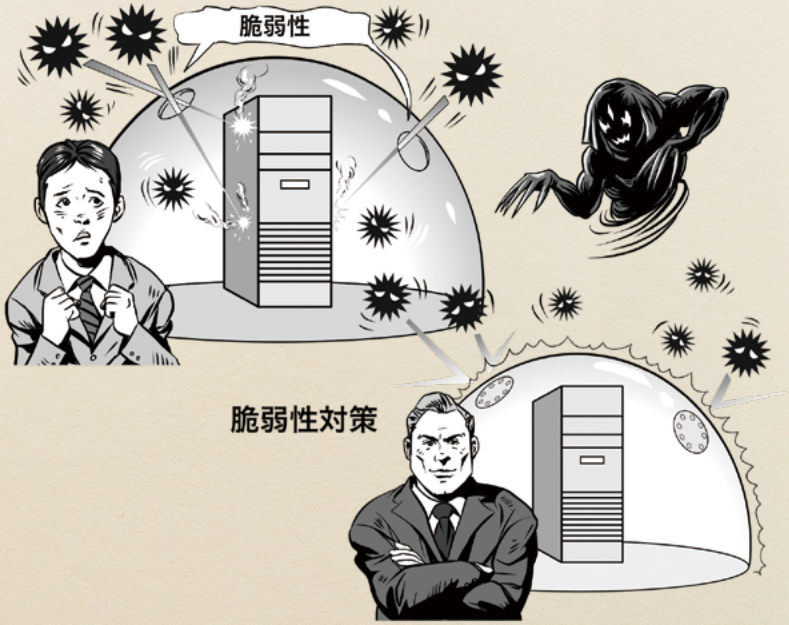
●サービス提供者
- **簡単なパスワード、容易に推測できるパスワードを許可しない**
- **多要素認証を導入（Webとスマートフォンを使ったログインなど）**

●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。

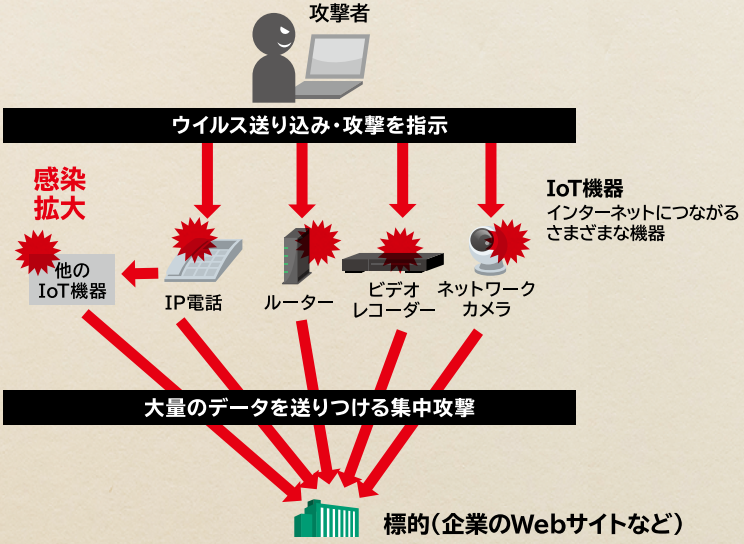
対策はこれだ！

- **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！

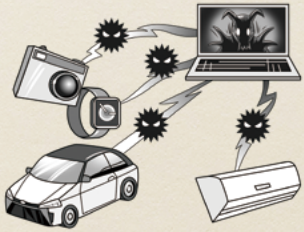
昨今は自動車やネットワークカメラ、情報家電などもインターネットにつながるようになっています（IoT※機器）。攻撃者はインターネット越しにこれらIoT機器の脆弱性や設定不備などを突いて攻撃を行い、不正アクセスやウイルス感染、さらにデータの改ざんや情報漏えい、機器操作などを行います。



※ 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。

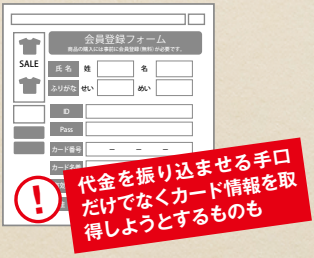
参考：経済産業省「昨今のサイバー攻撃事案を踏まえた注意喚起と報告のお願い」に対する報告結果 及び「中小企業向けサイバーセキュリティ事後対応支援実証事業（いわゆる「サイバ ーセキュリティお助け隊」）」の事業報告を踏まえた昨今の産業を巡るサイバーセキュリティに係る状況の認識と、今後の取組の方向性について」（2020年6月）

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**