TOP SECRET

MISSION 1

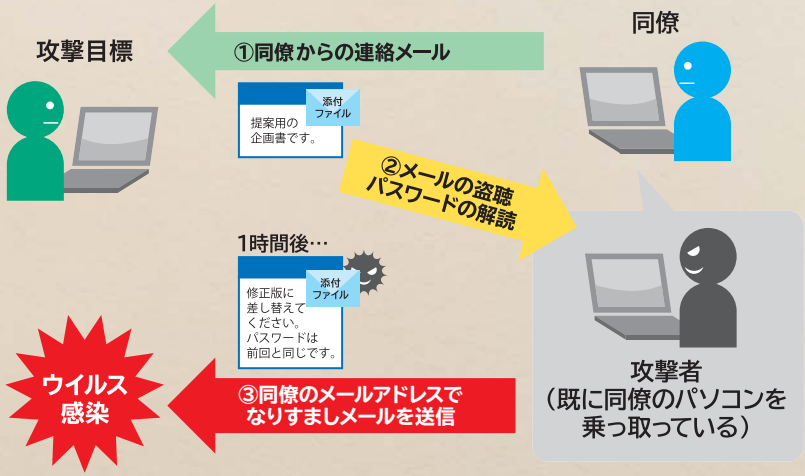
知っておきたい サイバー攻撃の知識

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

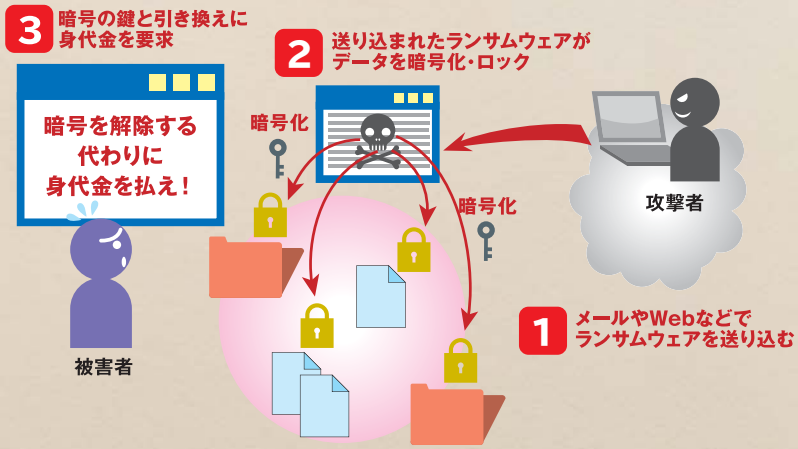
・日本語の言い回しが不自然なメール
・差出人のメールアドレスとメール本文の署名に記載されたメールアドレスが異なるメール
・これまで届いたことがない公的機関からのお知らせ
・心当たりのないメールだが、興味をそそられる内容
・心当たりのない決済や配送通知
・論理的に自分に送られてくることがおかしいメール

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。

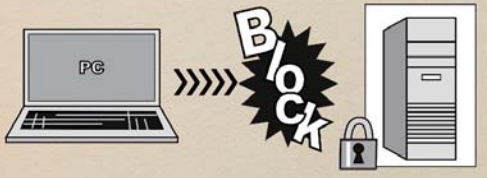


POINT 2 侵入手口はメールとWebサイト

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

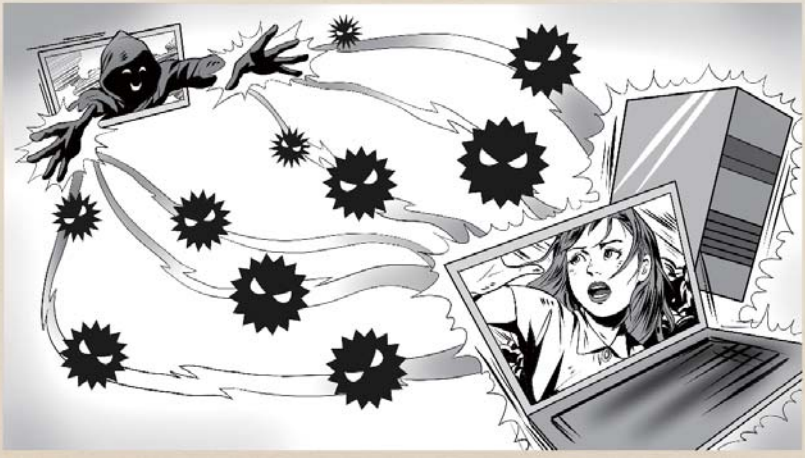
●サービスを利用する場合

・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

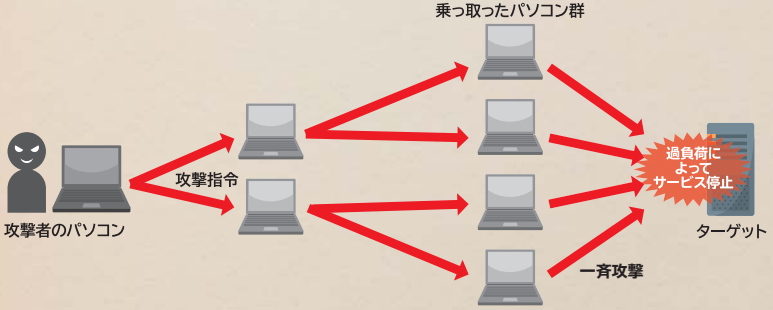
サーバーに処理速度をはるかに上回る大量の要求が集中すると、利用者はそのサーバーにアクセスできない状態になり、最終的にはサーバーがダウンしてしまいます。
インターネット回線の容量がオーバーして、接続不能に陥ることもあります。



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。

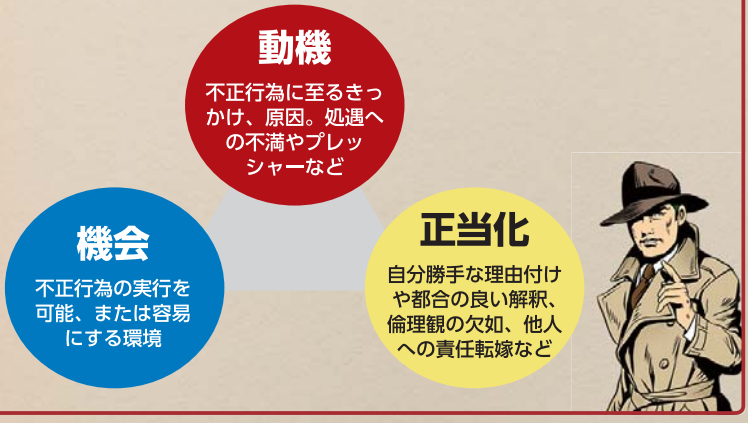
POINT 3 企業の信用が失墜し、賠償が求められる

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

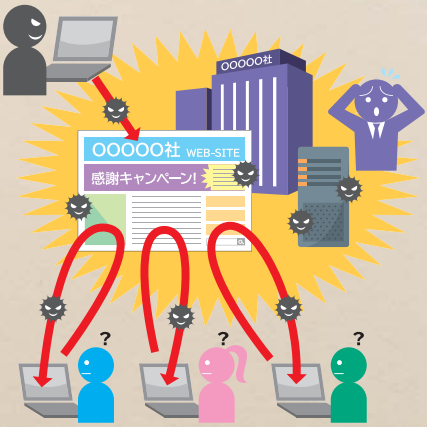
POINT 1 改ざんの目的は2つ

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。



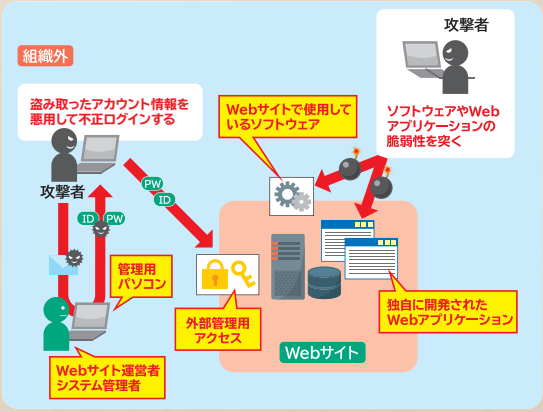
POINT 2 手口は脆弱性攻撃と管理用アカウントの乗っ取り

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。

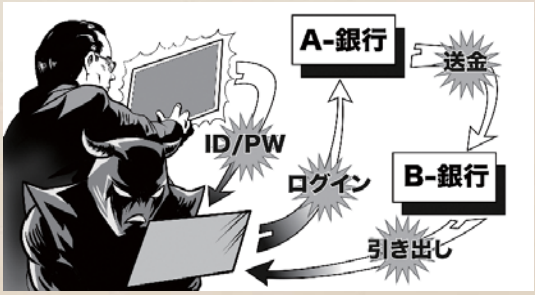
POINT 2 手口はフィッシング詐欺と不正送金ウイルス

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

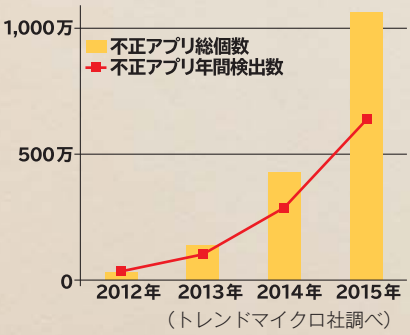
悪意のあるスマホアプリ

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

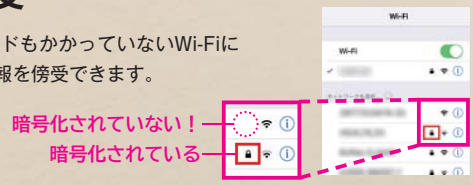
2010年8月に最初のAndroid不正アプリが検出されて以来、5年を待たずして1,000万個に到達しました。特に2015年には、わずか1年の間に630万個が新たに登場しました。（トレンドマイクロ社調べ）Androidでは自由にアプリを配布・インストールすることができます。不正なアプリに十分注意してください。



（トレンドマイクロ社調べ）

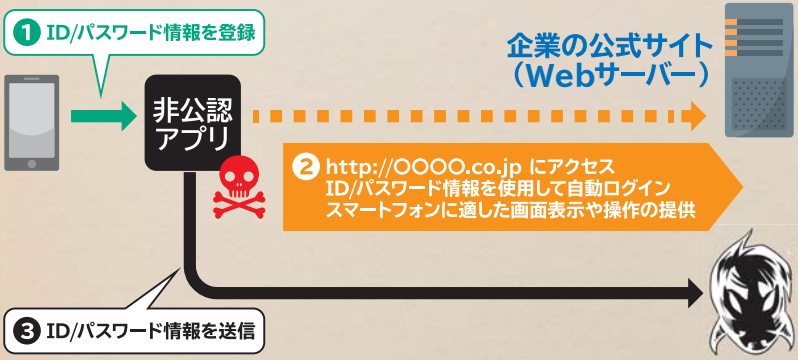
Wi-Fiを使って傍受

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！

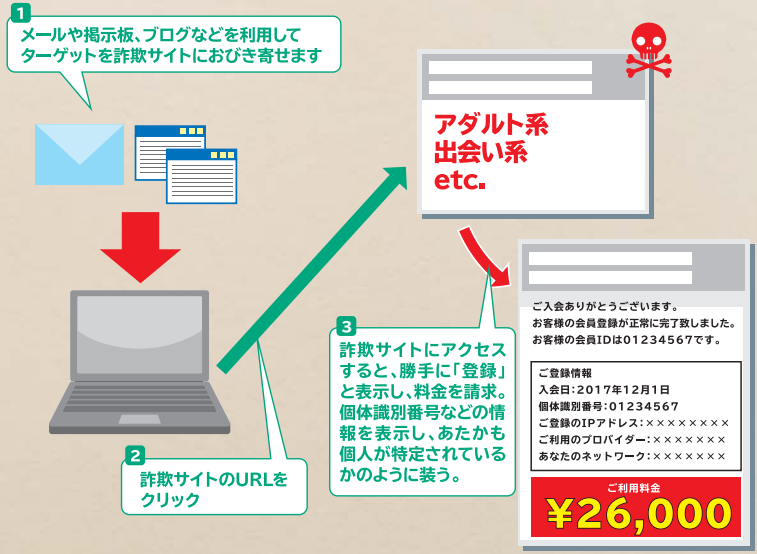
・スマートフォンのOS・ソフトウェアはアップデートする
・ウイルス対策ソフトを導入・更新する
・公式サイト以外からアプリをインストールしない
・重要なデータのバックアップを取る

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！

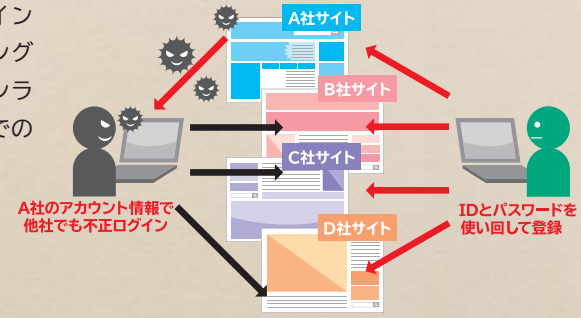
Webサービスから盗み取ったIDとパスワードを悪用し、ほかのサイトに不正ログインして、なりすましを行ったり、不正な注文をしたりする攻撃です。

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



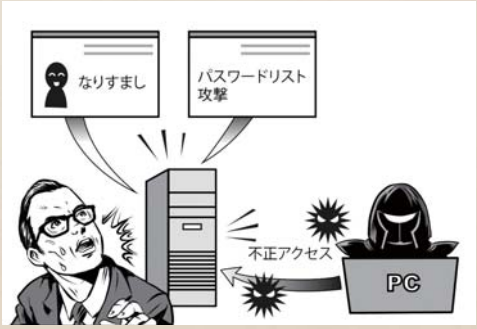
POINT 2 手口はパスワードの推測とリスト攻撃だ！

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！

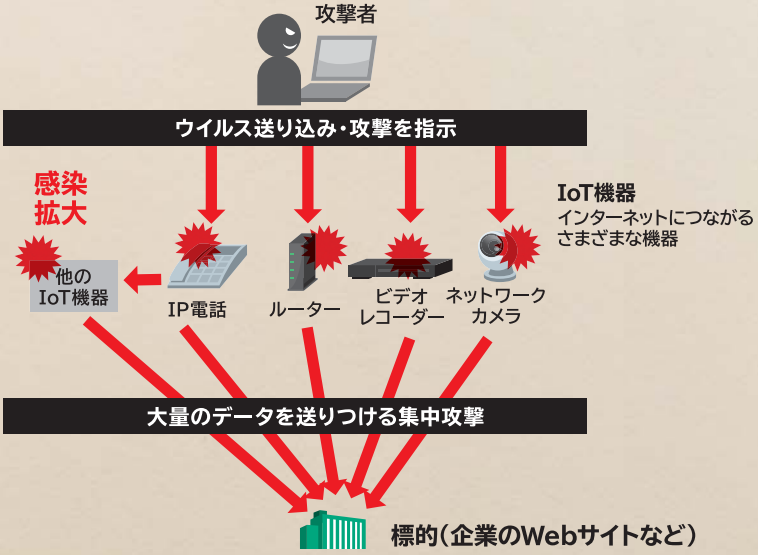
- **社内で使用しているソフトウェアの全てについて、自動更新が設定されているものと設定されていないものを把握する**
- **使っているソフトウェアに関する脆弱性情報を入手する（P49参照）**
- **使っているソフトウェアに脆弱性が発見された場合に備えて、会社全体のソフトウェアを更新する手順を作成しておく**
- **脆弱性が発見されたら、全てのソフトウェアの更新を確認し、実行する**

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！

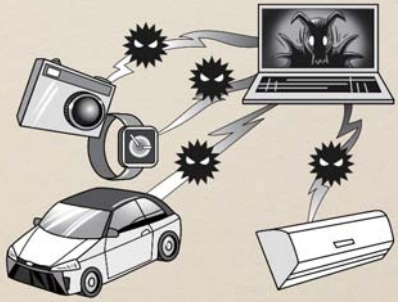
昨今は自動車やネットワークカメラ、情報家電などもインターネットにつながるようになっています（IoT※機器）。攻撃者はインターネット越しにこれらIoT機器の脆弱性や設定不備などを突いて攻撃を行い、不正アクセスやウイルス感染、さらにデータの改ざんや情報漏えい、機器操作などを行います。



※ 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