Blue Planet-works
Safety for the Connected World

医療機関におけるサイバーセキュリティ対策

～職員が知っておくべきサイバーセキュリティの世界～

株式会社Blue Planet-works

セキュリティアドバイザー 鴫原祐輔

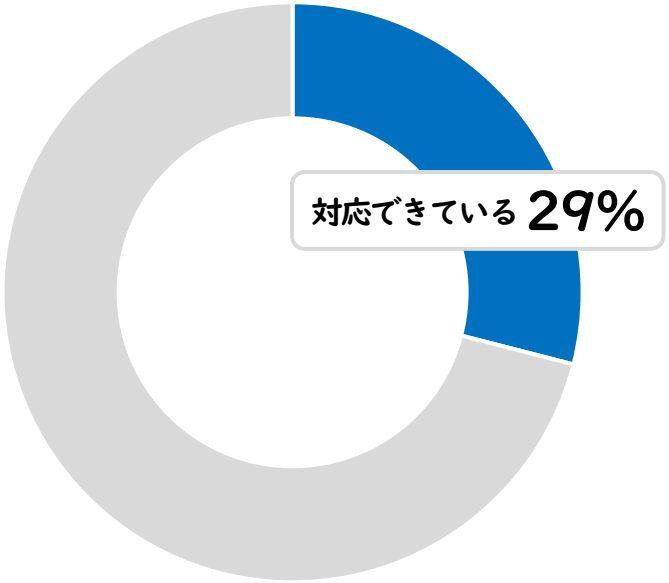
サイバーセキュリティ研修を受ける意味

- 組織の一員であることを自覚する -

国内医療機関におけるサイバーセキュリティ対策の実情

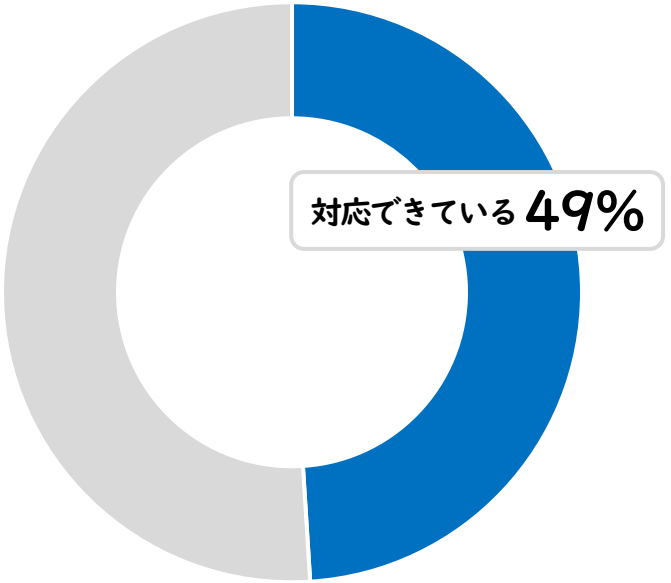
Blue Planet-works
Safety for the Connected World

人的セキュリティへの対応状況



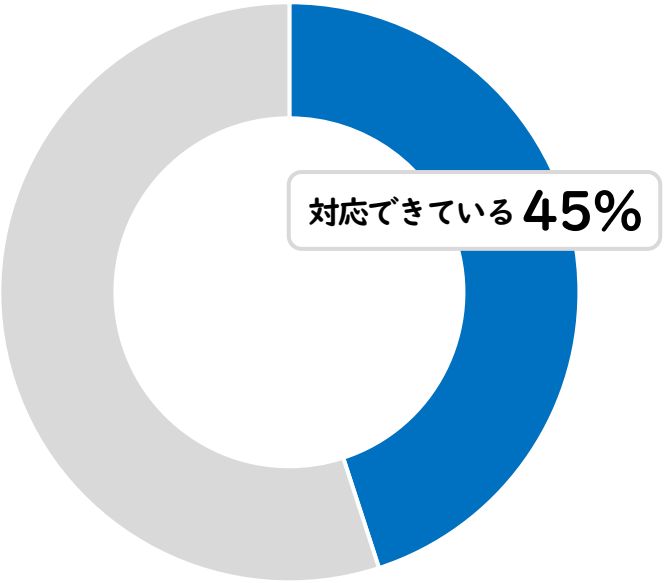
セキュリティ事故を回避するために必要な教育やルールの制定ができているか。

技術的な脆弱性への対応状況



セキュリティ事故を引き起こす可能性がある技術的な問題点に対処しているか。

セキュリティ事故への対応準備



セキュリティ事故発生時における被害最小化に必要な体制が整備されているか。

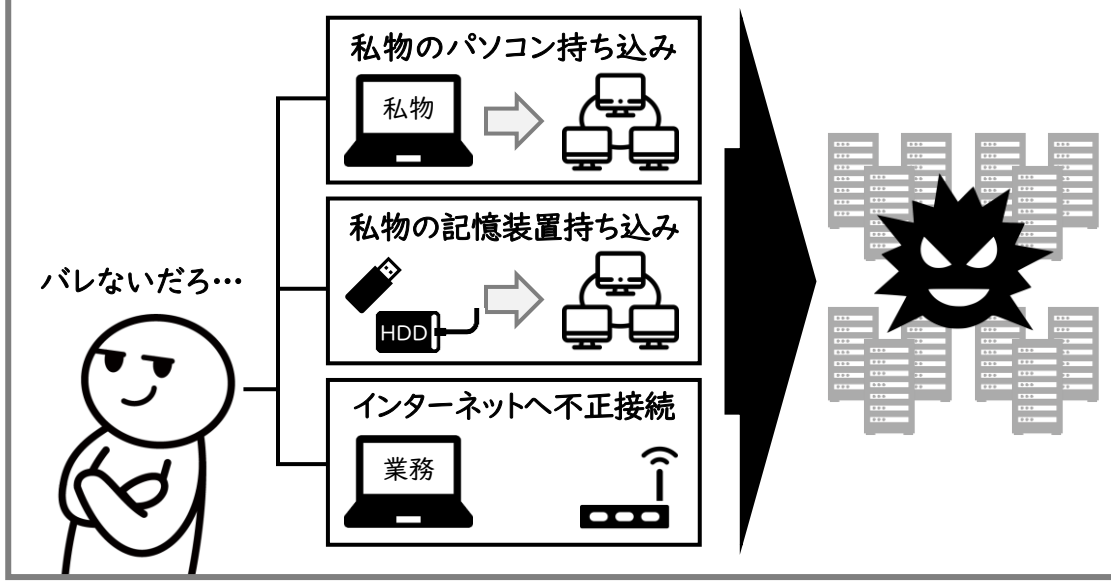
出典：医療ISAC「国内病院に対するセキュリティアンケート調査の結果と考察」

国内医療機関におけるサイバーセキュリティ事故例

Blue Planet-works
Safety for the Connected World

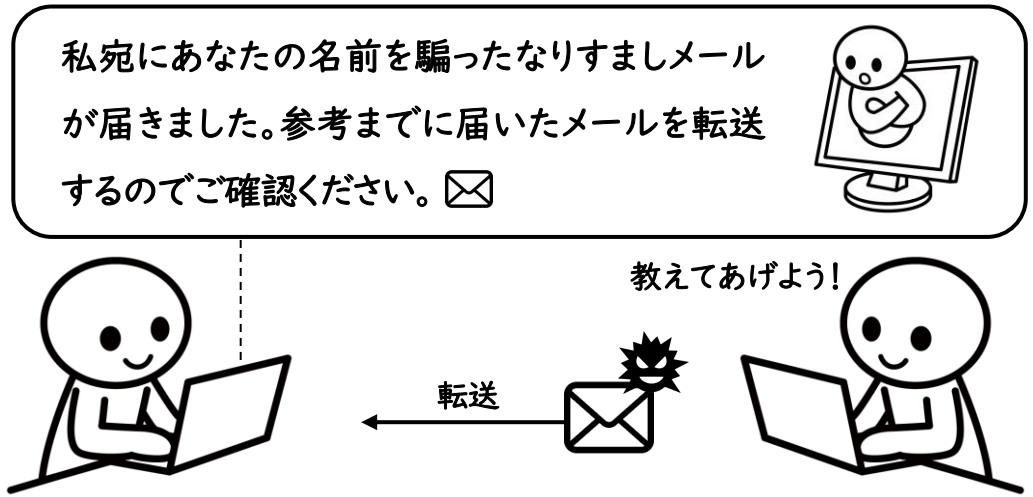
医療機関 A

2018年10月、院内関係者の「ルール違反」によって外部からランサムウェアが持ち込まれ、インターネットに接続されていない電子カルテを含む診療部門のシステム（4台）、診療部門端末（2台）、看護部門で利用するシステム（1台）などが使用不能に陥った。証拠不全で侵入経路の特定に至らず。

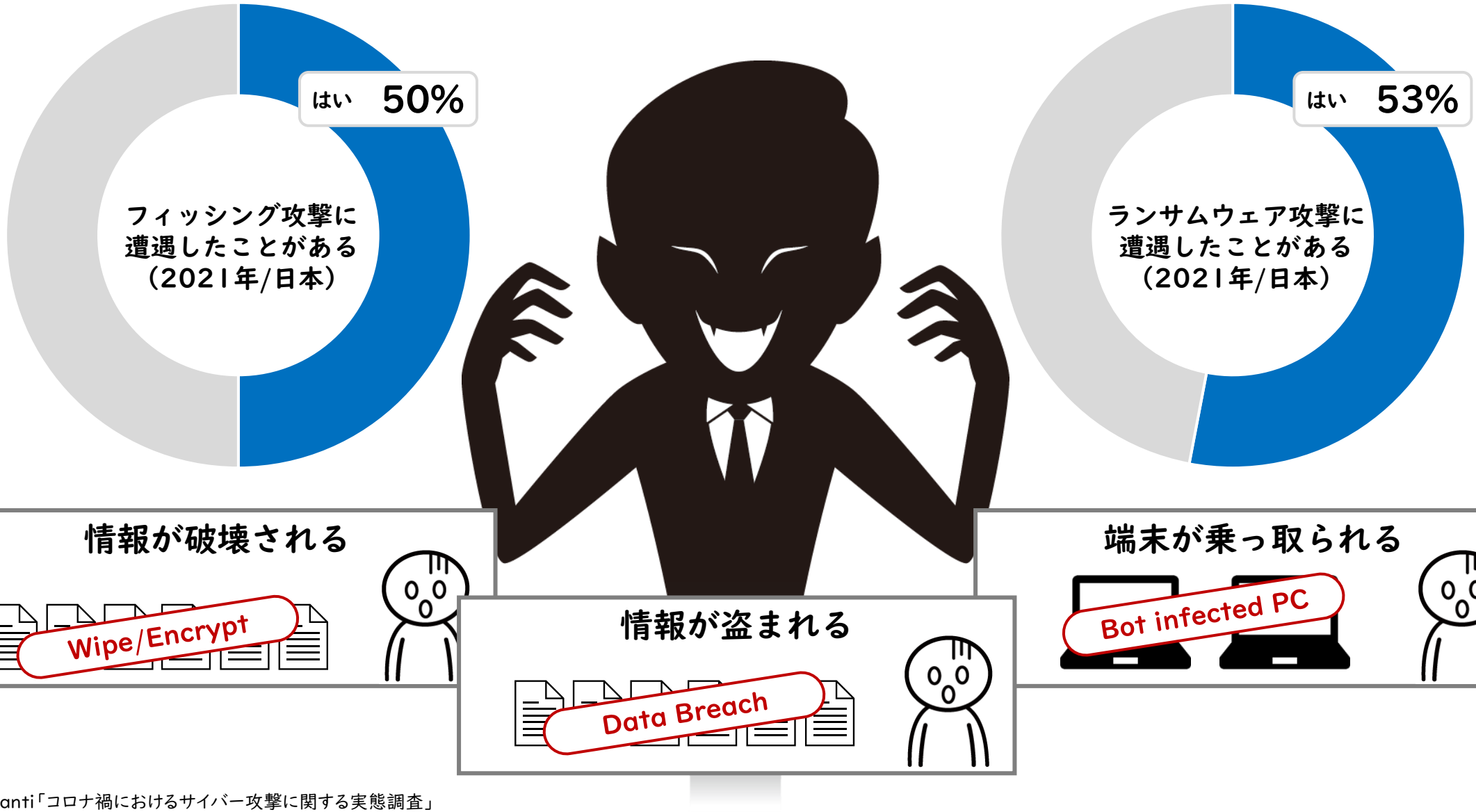


医療機関 B

2020年2月、医療機関Bに在籍する職員を騙る「なりすましメール」が関係のある別組織に送られた。この「なりすましメール」を受信した人物が注意喚起のために騙られた職員に当該メールを転送したところ、当該職員が誤ってメールに添付されていたファイルを起動してしまいマルウェアに感染する。



サイバー攻撃は身近なところにある



出典：Ivanti「コロナ禍におけるサイバー攻撃に関する実態調査」

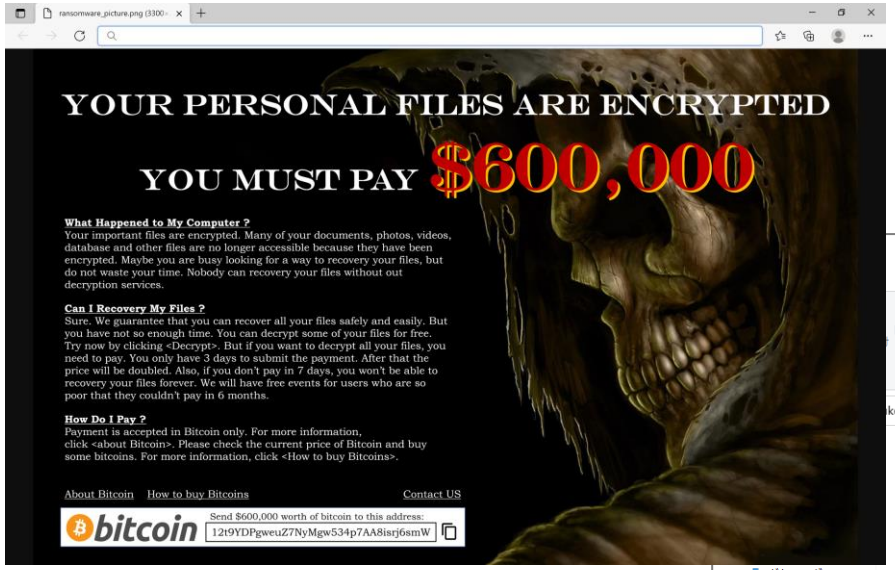
サイバー攻撃による事故の発生は想像以上に大きな影響を伴う #1

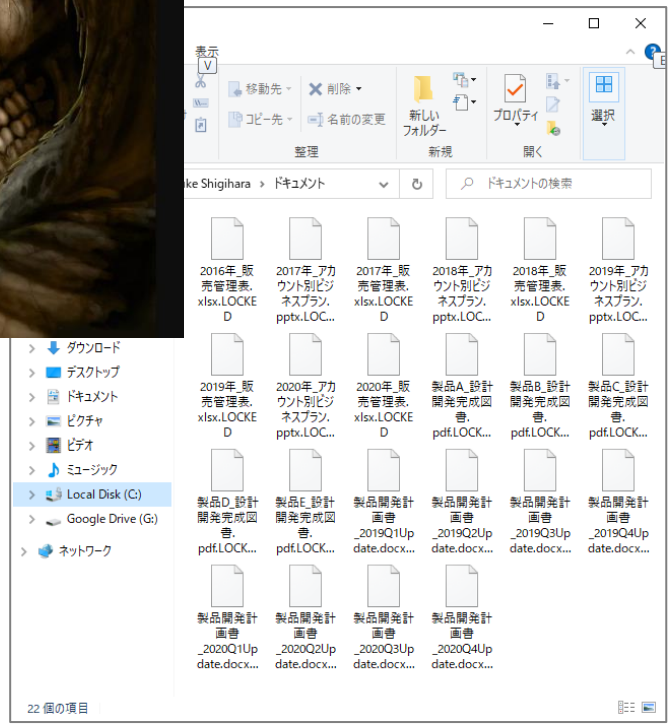
Blue Planet-works
Safety for the Connected World

情報が破壊される

攻撃者によって侵入された端末やそれを踏み台にして侵攻した他端末内のデータが暗号化されて使用不能に陥る。近年では攻撃者が業務に影響が出るシステムを狙って攻撃を仕掛けたり、復旧できないようにバックアップデータまで侵害するケースが数多く報告されている。

2021年10月に発生した徳島県つるぎ町の町立半田病院におけるランサムウェア感染事案では約2ヶ月の間、全13の診療科で電子カルテや診療請求業務に関連するシステムが機能不全に陥った。





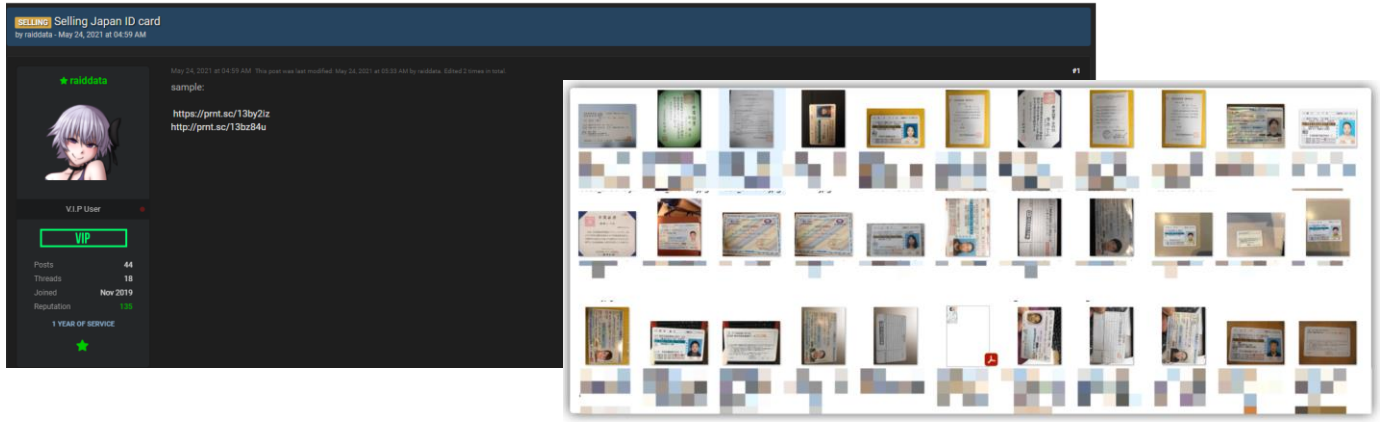
サイバー攻撃による事故の発生は想像以上に大きな影響を伴う #2

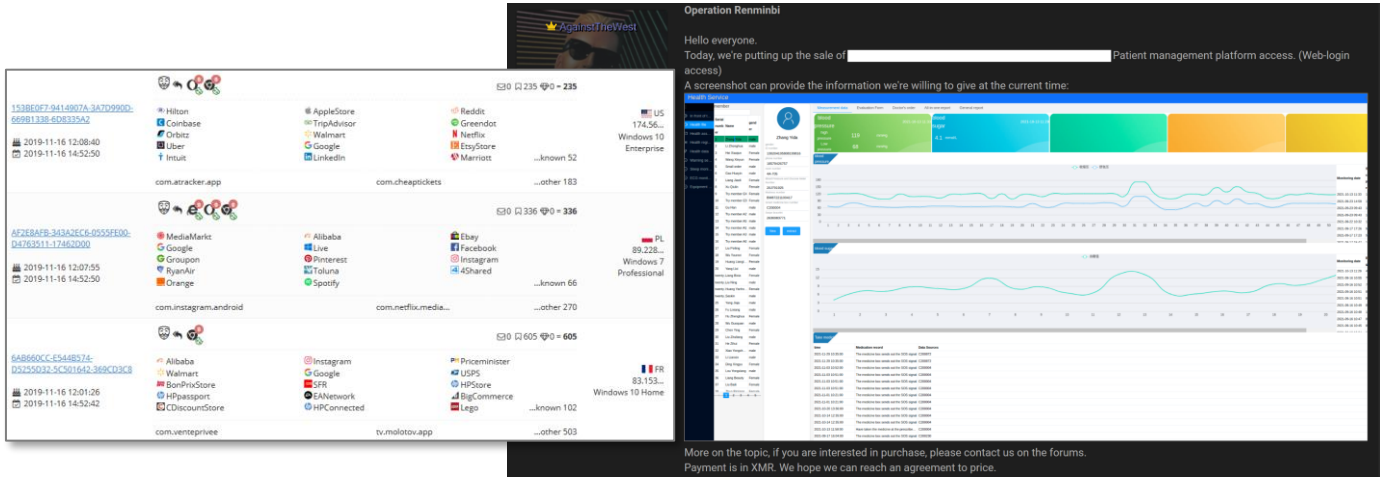
Blue Planet-works
Safety for the Connected World

情報が盗まれる/端末が乗っ取られる

攻撃者によって持ち出された情報はダークウェブ上で不当に公開されたり、第三者に対して売買される。二次的、三次的な被害へとつながっていくリスクがある。

また、乗っ取られた端末は「bot（ボット）」としてダークウェブ上で販売されることがある。端末内に保存されているデータや認証情報の全てが第三者に渡るリスクがある。第三者が端末を不正操作可能になるため、端末内に保存されたデータやクラウド上の情報に対する改ざんも容易に可能となってしまう。

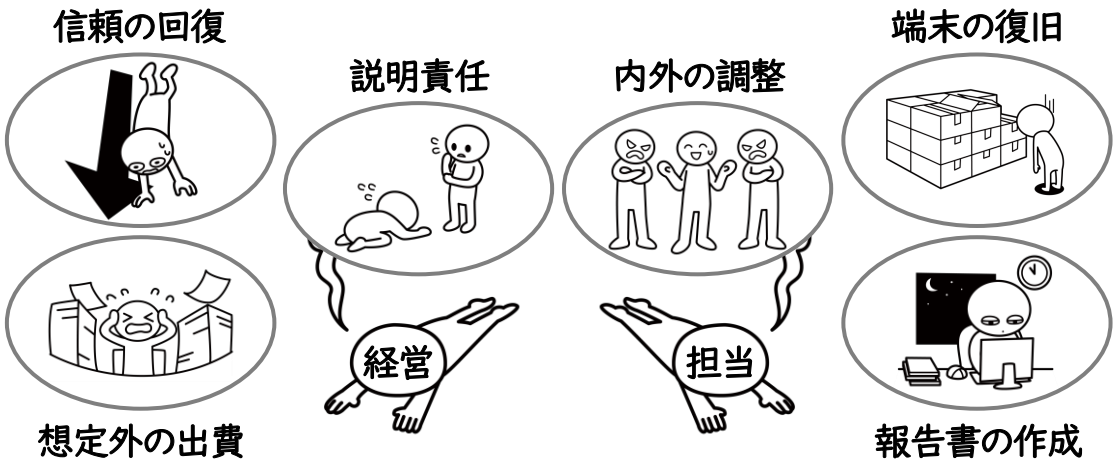




平時の状態に戻るためには多大な労力とコストを支払うことになる

Blue Planet-works
Safety for the Connected World

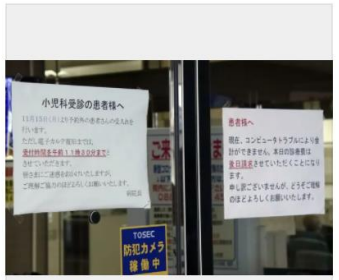
業務の正常化には多大な労力とコストを費やす



身代金払わず2億円でカルテ構築　徳島サイバー被害の病院

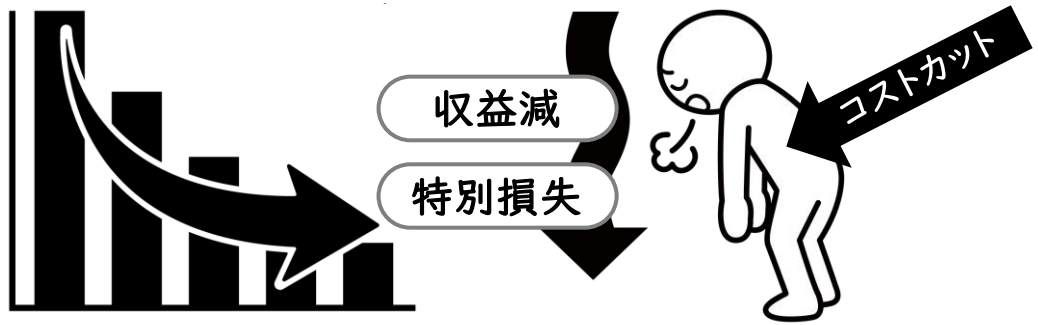
2021/11/25(木) 19:39 配信 31

KYODO



サイバー攻撃を受け患者約8万5千人分の電子カルテが閲覧できなくなった徳島県つるぎ町の町立半田病院が、犯人が復元の代わりに要求している「身代金」を支払わない方針を決めたことが25日分かった。約2億円をかけ新システムに切り替えカルテを再構築する。

復旧後も組織の健全性維持に大きな影響が生じる



インシデントによって生じた影響は、その後も継続的に組織へ影響を与える可能性がある。過去、国内での被害事例として「企業A：情報漏洩により4年先までの経営計画の見直しが発生」「企業B：情報漏洩により顧客離れが発生して赤字化、失った信頼の回復に3年を要する」「企業C：セキュリティ事故により受注していた業務の取り消しが発生」といったものがある。

出典：Yahoo!Japanニュース https://news.yahoo.co.jp/articles/a003af66094 1bb2a3a8f42705ad0ebc864c1 1 1a0

サイバー攻撃が成立する決定要因の多くは「人」である

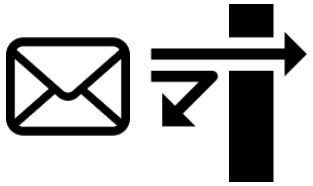
Blue Planet-works
Safety for the Connected World

組織として強固なセキュリティ対策を施していたとしても ユーザーの行動が攻撃の成否を決める

情報システム部門が検討を重ねて様々な対策を実施してリスクを軽減

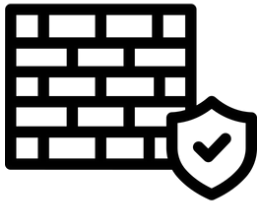
Endpoint Security
（端末のセキュリティ）

Mail Security
（メールのセキュリティ）



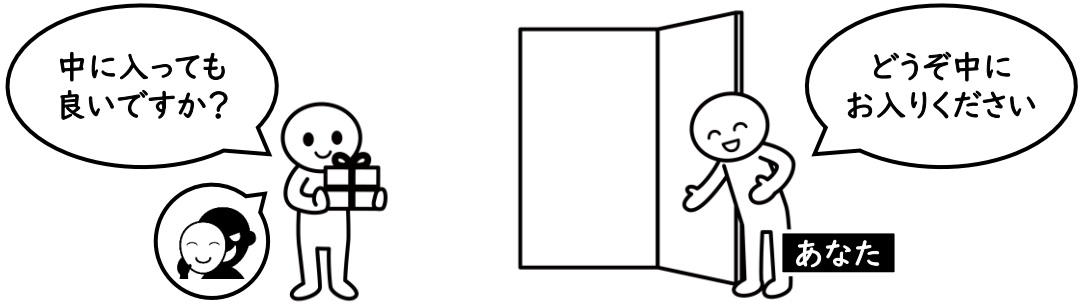
Web Security
（ウェブアクセスのセキュリティ）

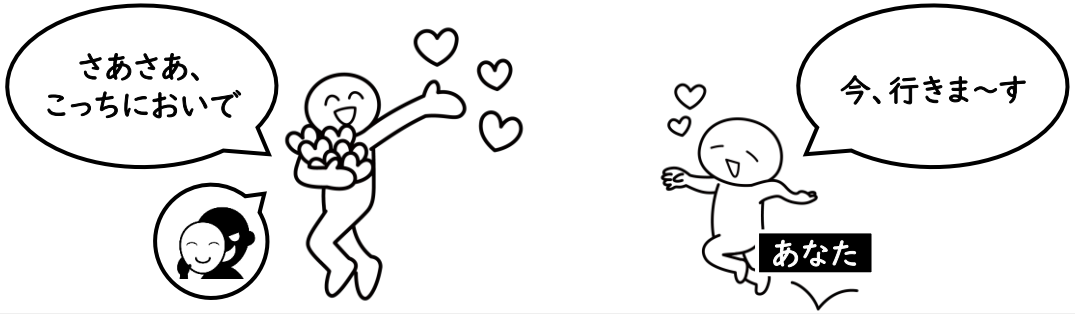
Network Security
（ネットワーク通信のセキュリティ）



ID Security
（ID/Passwordのセキュリティ）

しかしながら・・・





セキュリティ事故の多くはユーザー自身が脅威を招き入れたり・誘いに乗ってしまうことで顕在化する

ウェブサイトに潜む脅威

- 職員が知っておくべきサイバーセキュリティの世界＜ウェブ編＞ -

見た目上の区別が困難になっているフィッシングサイト

Blue Planet-works
Safety for the Connected World

サイトデザインはオリジナルサイトから流用

フィッシングサイトで利用されるページデザインはオリジナルサイトのデザインをそのまま流用するため、ページ内におけるデザインの差異で真偽の判断を下すことは難しいと言えます。

URLが違う

POINT

個人情報や機密情報を入力する様なサイトはあらかじめ「お気に入り」に登録するか検索エンジンからアクセスしましょう。

ブラウザの通知機能を悪用したフィッシングサイトへの誘導

Blue Planet-works
Safety for the Connected World

ユーザーを不安に陥れてフィッシングサイトへのリンクを押させる

検索結果から何気なくウェブサイトにアクセスすると、突然、ブラウザの「通知」を許可するように誘導するページが表示されます。この時、「許可」ボタンを押してしまうとブラウザ起動時にユーザーの不安を煽る通知が表示されるようになります。

ユーザーの実在性確認と称したページ

ブラウザの設定が追加され勝手に通知を送りつけることができるようになる。

通知を許可すると怪しい通知が起動
（複数の種類がある）

POINT

原則、許可しない。誤って許可しても慌てずにIPAのサイト※に掲載された手順でブラウザから設定を削除しましょう。

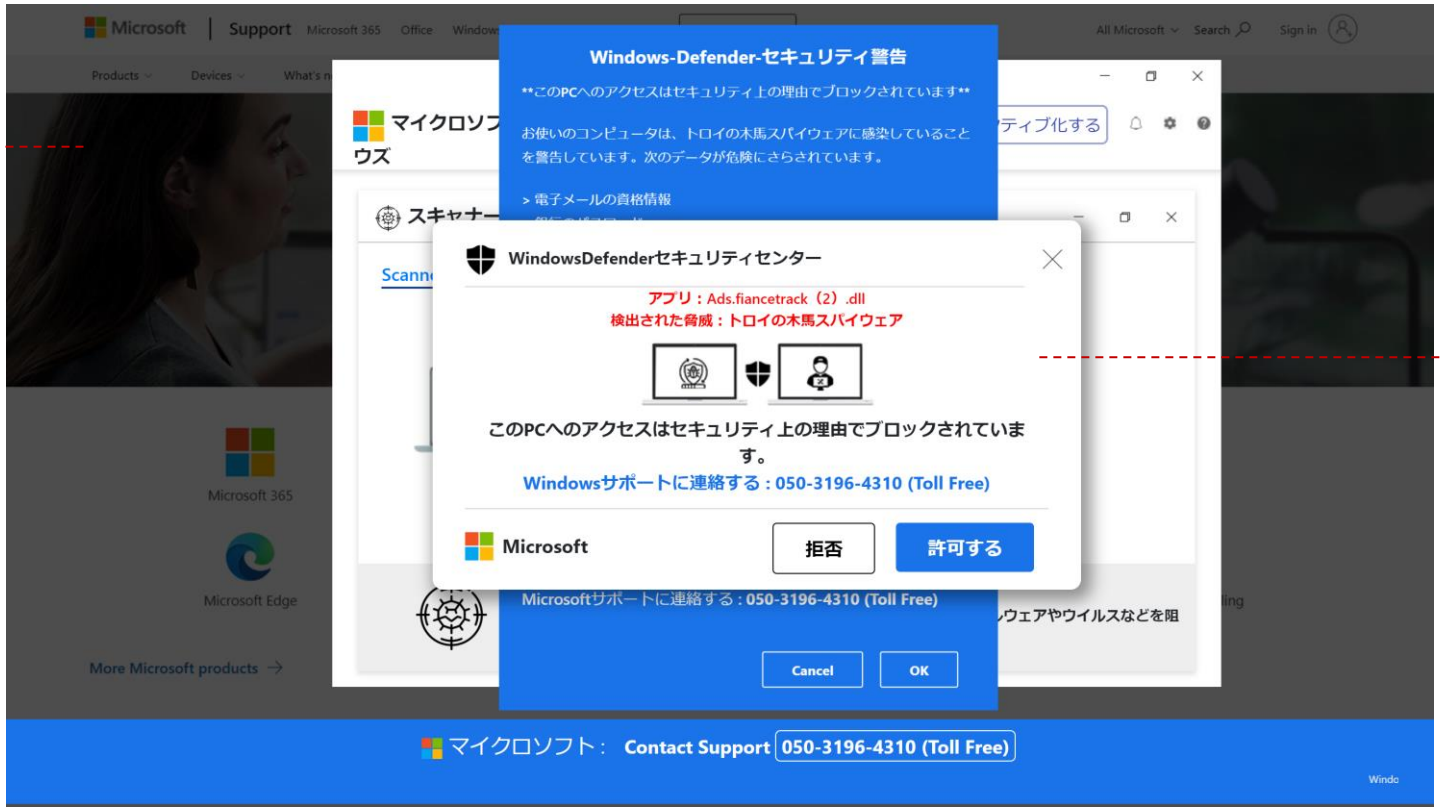
※https://www.ipa.go.jp/security/anshin/mgdayori20210309.html

テクニカルサポート詐欺

Windows Defenderのアラートを装った詐欺

テクニカルサポート詐欺と呼ばれており、何らかの不具合が発生しているように見せかけて救済するために金銭を要求する。アラートウィンドウを閉じられないようにすることでユーザーの不安をさらに煽る。

背景にマイクロソフトの
ウェブサイトを表示



クリックすると
全画面表示になる

POINT

速やかに当該ページを閉じましょう。指示された電話番号にかけてはいけません。

タイポスクワッティング（Typosquatting）を使った攻撃

Blue Planet-works
Safety for the Connected World

テクニック	概要	例
ドット（.）の入力漏れを狙う	ウェブサーバーを表す「www」の後に入力される「.」を省略した形でドメイン名を取得する。	正：www.google.com 誤：wwwgoogle.com
特定文字の抜け落ちを狙う	ドメイン名で利用される企業名や特定の単語から一文字抜け落ちた形でドメイン名を取得する。	正：www.facebook.com 誤：www.facebok.com
特定文字の重複を狙う	ドメイン名で利用される企業名や特定の単語から一文字増やした形でドメイン名を取得する。	正：www.twitter.com 誤：www.twiitter.com
特定持ちの入力順の間違いを狙う	ドメイン名で利用される企業名や特定の単語から文字の入力順を変更した形でドメイン名を取得する。	正：www.youtube.com 誤：www.yuotube.com
見た目が似た文字との打ち間違いを狙う	ドメイン名で利用される企業名や特定の単語で見た目が似ている文字を置き換えた形でドメイン名を取得する。	正：www.apple.com 誤：www.app l e.com
トップレベルドメインの入力間違いを狙う	.comや.co.jpといったドメイン名の属性を示すトップレベルドメインの入力間違いを狙った形でドメイン名を取得する。	正：www.takaoka-med.org 誤：www.takaoka-med.jp

POINT

ウェブサイトへのアクセス時には余分な単語や欠落している単語、間違ったスペル、接尾辞等がないかどうかを確認する。

ウェブサイトに潜む脅威と遭遇した場合の基本的な対処方法

Blue Planet-works
Safety for the Connected World

確認	セルフチェックポイント
□	**クリックする前にリンク先を確認** リンクをクリックする場合や自分で入力する場合でも余分な単語や欠落している単語、間違ったスペル、接尾辞等がないかどうかを確認する。
□	**アドレスバーに表示されるURLの確認** 見た目上は普段見慣れたウェブサイトであってもアドレスバーに表示されるURLがアクセス先のドメイン名等を持ったものであるか確認する。
□	**何らかの変更を要求される場合は連絡元を確認** 突然、何らかの変更要求を受けた場合、連絡元のウェブサイト等で公開されている注意喚起情報等を確認する。また、メールであれば件名で検索すると良い。
□	**「お気に入り」や「検索エンジン」からアクセス** 個人情報や機密情報の入力を求められる場合、メール内のリンク等からではなく、あらかじめ「お気に入り」登録したリンクや検索エンジンからアクセスし直す。

確認	セルフチェックポイント
□	**バナー広告に何を警告されても無視** 不安を煽るようなバナー広告が表示されても基本は無視する。Windowsのアラートを偽装するものもあるが、自分で対処せずに情報システム部門等に相談する。
□	**怪しいバナー広告は触らない** 画面に表示されるバナー広告内にある「×」「いいえ」「No」等の拒否する選択肢があっても、まともに機能する保証はないのでページを閉じる。
□	**画面が遷移しても慌てない** 何かの拍子でページが遷移してしまうことがあっても、反応せず慌てずにページを閉じる。ユーザー情報を取得した等のメッセージがあっても無視する。
□	**「許可」してしまったら報告** ブラウザの設定を変更する通知ウィンドウを誤って触ってしまい、何らかの設定を「許可」してしまった場合は速やかに情報システム部門に相談する。

POINT

自分で判断ができない時は必ず情報システム担当部門や専門知識を持った人に相談する。

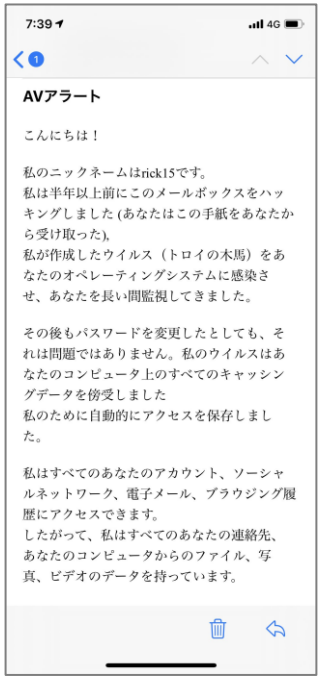
セクストーション詐欺

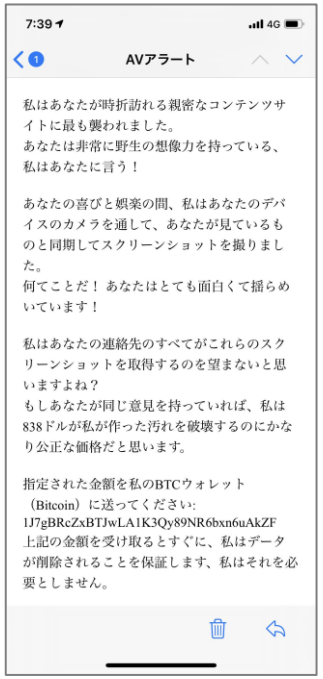
セクストーション詐欺

アダルトサイトを閲覧していた証拠を持っていると脅し金銭を要求してくる詐欺メールです。他にも端末にマルウェアを仕掛けたので保存されているあらゆる情報を窃取し、ユーザーを監視していると脅してくるものもあります。

既に、貴方の個人情報、データ、写真、ウェブ閲覧履歴を僕のサーバーにダウンロードし保存してあります。
貴方のメッセンジャー、SNS、メール、チャット履歴、連絡先一覧の全てにも僕はアクセス済みです。
僕のウイルスはドライバレベルで動作し署名を継続的に更新するため、ウイルス対策ソフトウェアでは検知されません。
同様に、この手紙がなぜウイルス対策のソフトウェアに検出されなかったのかの理由も、今ではご理解いただけていると思います・・・
貴方の情報を収集している間に、貴方はアダルトサイトの大ファンだということを発見しました。
ポルノサイトを訪問して、とてつもない快楽に耐えながら、興奮するような動画を閲覧するのが本当にお好きなようですね。
偶然にも、貴方の卑猥なシーンを録画することに成功したので、貴方の自慰行為と絶頂に達する姿を見せるような動画数本をモンタージュにしました。
もし嘘だと思うのであれば、僕のマウスを数回クリックするだけで、全ての動画が貴方の友人、同僚や親戚とシェアできることを実現いたしましょう。
僕的には、パブリックアクセスにしてしまっても問題はありません。
貴方の好きな動画の趣向を考慮しても、そんな動画を公にされたくはないはずです。（僕の言いたいことは分かるでしょう）
公になったら、本当の大惨事になるかもしれませんね。

なので、ここで取引をしましょう。
17万円（送金時の為替レートに応じたビットコイン相当額）を僕に送金してください。
送金を受け取ると、この卑猥な動画は全て削除しましょう。
その後は、お互いのことは綺麗さっぱり忘れてしまい、貴方のデバイスにある有害なソフトウェアの機能を停止して削除することを約束します。
僕は言ったことは守ります。
僕が貴方のプロフィールとトラフィックをしばらくチェックしていることを考えると、これは公正な取引であり、かなり安価なはずです。
ビットコインの購入、送金方法が分からない場合は、どのサーチエンジンで検索しても方法は知ることができます。

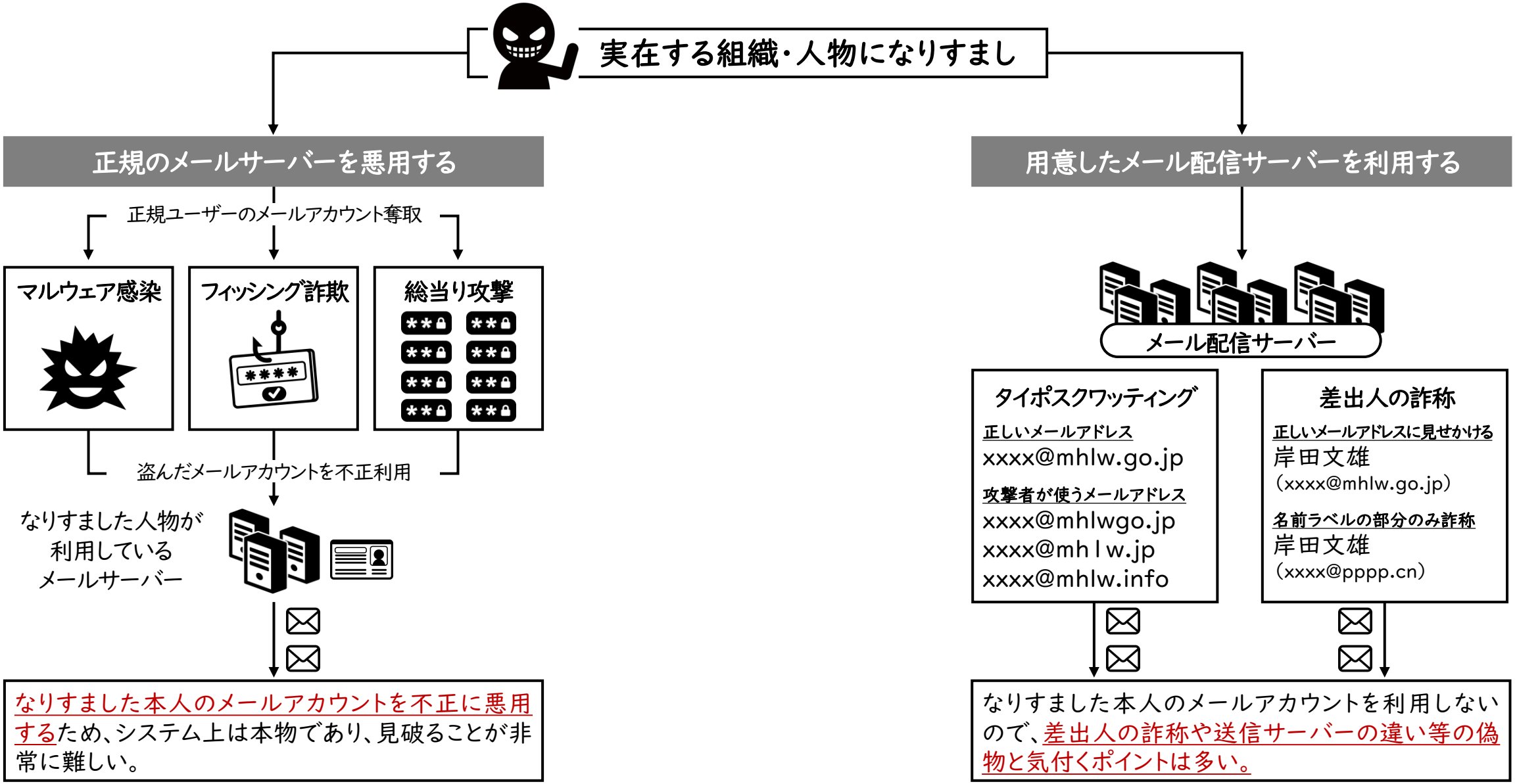




POINT

基本的には無視する。クラウドサービスなどのパスワードは念の為、変更しておく。

実在する組織・人物になりすます「ビジネスメール詐欺（BEC）」とは



ビジネスメール詐欺：情報システム担当者になりすまし

注：被害者の方の証言に基づき作成しています。

送信者：情報システム担当（xxxxxxx@pppp.net）
件　名：あなたのパソコンで故障を検出しました
添　付：なし

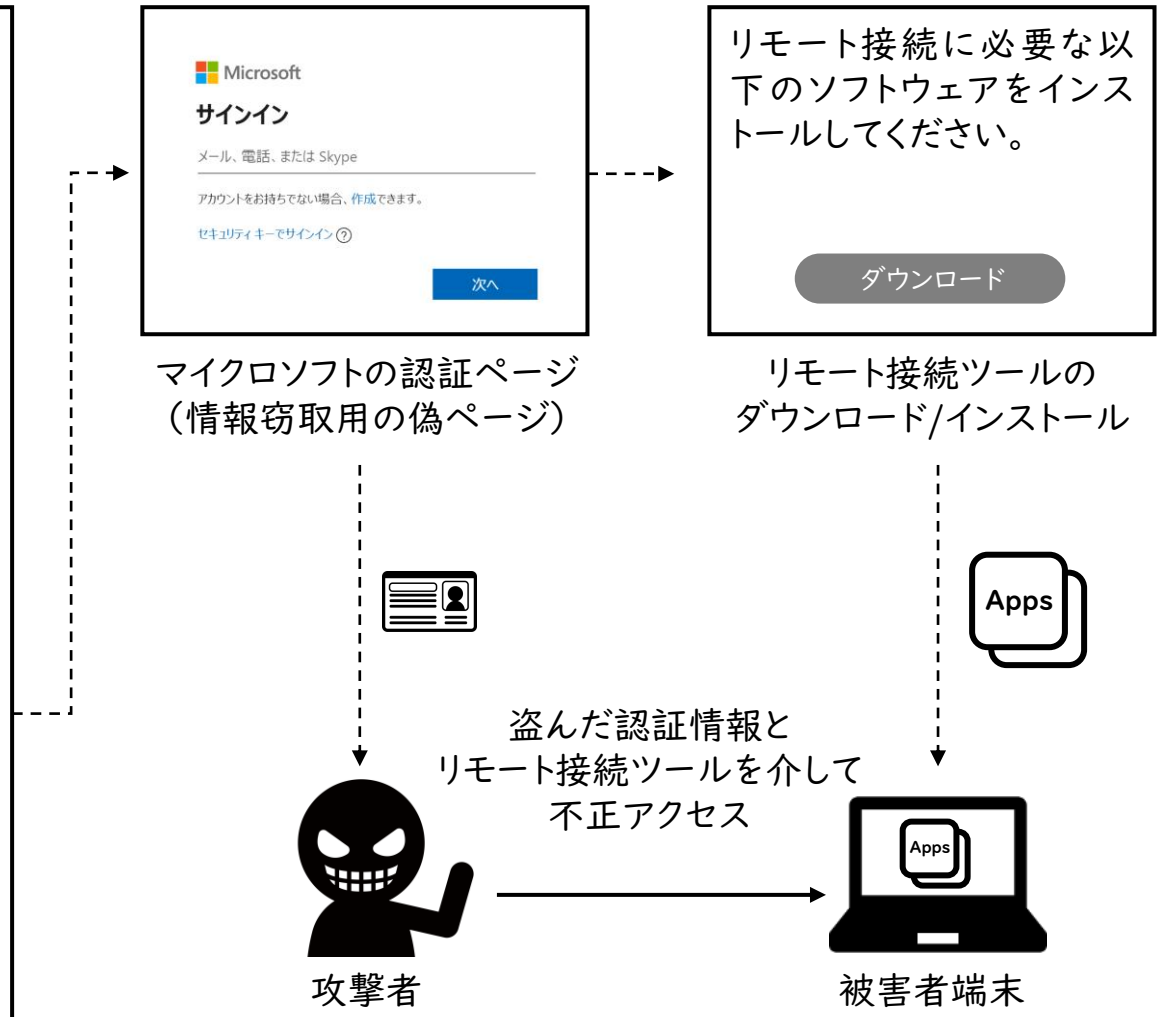
あなたが利用している端末でハードウェア障害を検知しました。

型番：L-117847-P15-V
エラーコード：E-12548

リモート接続にて状況の確認と問題の解決を試みます。
以下より接続に必要なユーザー情報の登録をしてください。

https://support-customer-xxxxxx.info/UYfQtQUa8T-cpyD_zHcl-uVZd3u4h5h-wsyAPWUdK8-yk=?d=YrEo1M50KcfTv_%2Fallfx%2Fja%2Fsupport2Fsa_symc%2F123283672783

情報システム担当



ビジネスメール詐欺：役員や上司になりすまし+二重拡張子

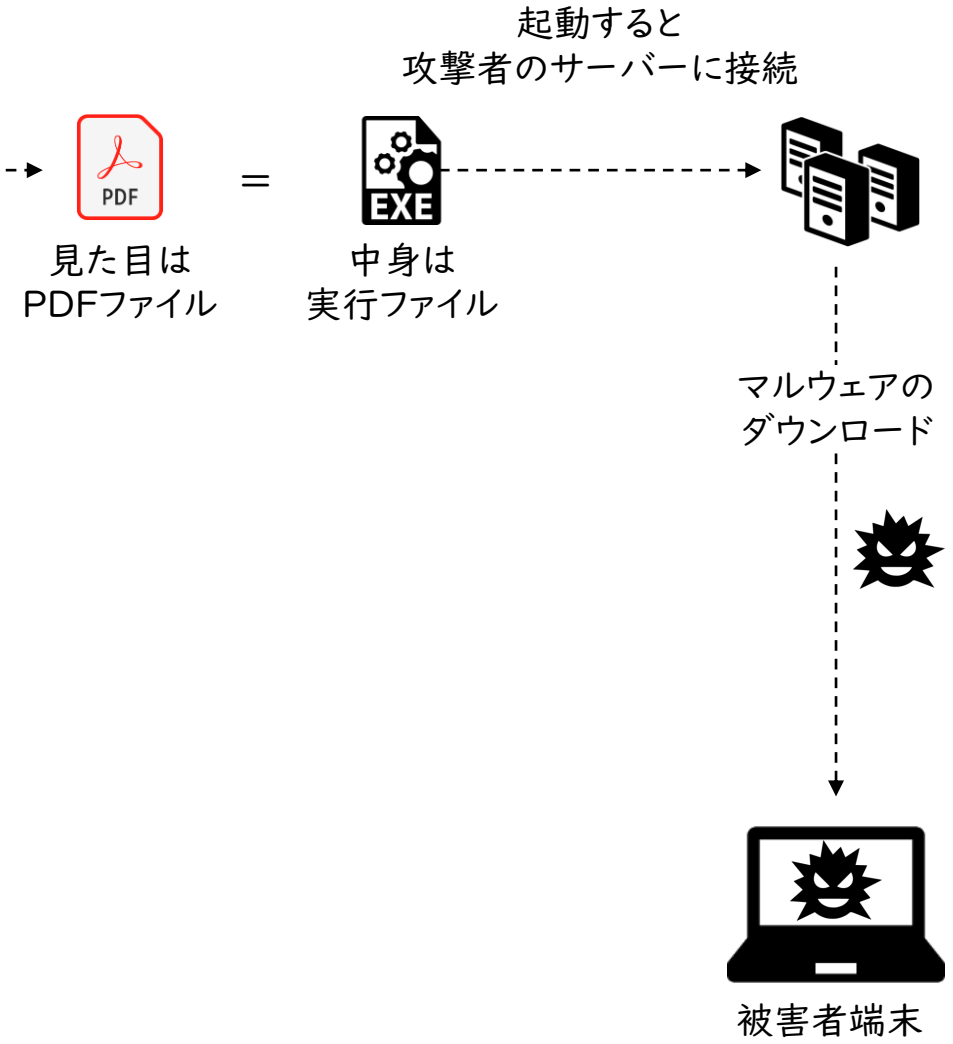
注：被害者の方の証言に基づき作成しています。

送信者：役員・上司の名前（xxxxxxx@pppp.net）
件　名：本日の会議資料送付
添　付：会議資料.pdf.exe

各位

本日の会議で使う資料です。
事前に確認してください。

〇〇（役員・上司の苗字）



ビジネスメール詐欺：取引先等になりすまし+外部サイト悪用

注：被害者の方の証言に基づき作成しています。

送信者：外部組織に在籍する人物の名前（xxxxxxx@pppp.net）
件　名：本日の会議資料送付
添　付：なし

ご確認をお願いします。

https://xxxxxxxx.co.jp/005105087147441 2_xxxxxxxx.html

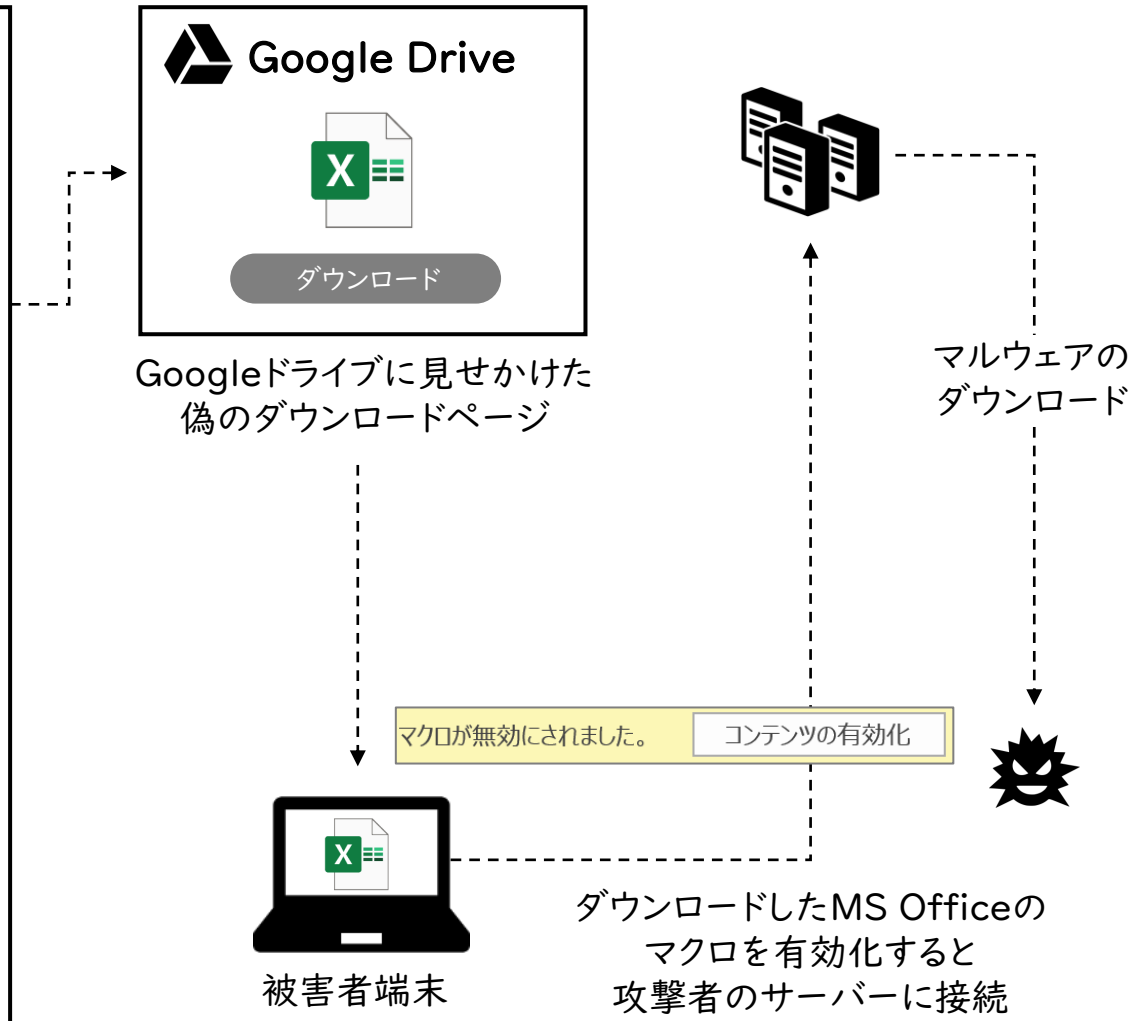
騙られている人物の
所属する組織のドメイン名

騙られている人物の
所属する組織名

宜しく御願い致します。

[メールアドレスに記載の人物の名前]
XXXXXXX@xxxxxxxx.co.jp

騙られている人物の名前と
本物のメールアドレス



ビジネスメール詐欺：取引先等になりすまし+不正送金

注：被害者の方の証言に基づき作成しています。

送信者：取引先のメールアドレス（finance@xxx.co.jp）
件　名：取引口座変更のお願い
添　付：なし

取引先番号：xxxxxxxx-xxx

弊社では以下のとおり、2021年〇月〇日より
取引における振込先先の口座を変更させていただきます。

突然のご連絡となりますが、
次回よりご対応よろしくお願いします。

振込先金融機関：〇〇銀行〇〇支店
振込先口座番号：（普通）XXXXXXX

株式会社〇〇〇〇 購買部 〇〇（担当者名）

当事者間しか知り得ない取引時に使用する固有のID

取引先の購買部には実在しない人物

メールに潜む脅威と遭遇した場合の基本的な対処方法

Blue Planet-works
Safety for the Connected World

確認	セルフチェックポイント
□	**差出人のメールアドレスを確認する。** 本文中で名乗っている人物と差出人のメールアドレスの整合性が取れていることを確認する。特に@より後ろの部分が名乗っている組織のドメイン名かどうかは必ず確認する。
□	**本文の内容確認** 本文に記載された内容が自分に関係のある内容であるか確認する。見知った相手であっても、脈略のない内容であれば疑ってかかる。
□	**本文内の文脈や文法間違いの確認** 攻撃者の多くは機械翻訳を利用する場合が多く、使用する単語や全体の文脈におかしいポイントが存在していることが多い。
□	**変更・提出などを要求される場合は本人に確認** 重要事項の変更や何らかの機密情報を要求される場合、メールとは異なる手段で相手側に事実確認をする等、双方にて事実確認をする場合の手順を決めておく。

確認	セルフチェックポイント
□	**添付ファイルは拡張子を確認** 攻撃者が使う手口として表示されるアイコンを偽装した「二重拡張子」を用いることが多いため、添付ファイルは実行前に必ず拡張子を確認する。（例：pdf.exe）
□	**添付ファイルの絶対にマクロは有効化しない** ExcelやWordといったドキュメントファイルが添付されていた場合、例えそれが誰から送られたものであろうと「コンテンツの有効化」は絶対にしない。
□	**本文内にある外部サイトへのリンクを確認** 本文内に外部リンクをクリックするように誘導している場合、視認できるリンク先と実際のリンク先が一致しているかカーソルを合わせる等して確認をする。
□	**クラウドストレージのダウンロードリンクは事前確認** ファイルの受け渡し等でクラウドストレージを利用する場合、相手方が当該クラウドストレージを利用していることを事前に確認する。

POINT

自分で判断ができない時は必ず情報システム担当部門や専門知識を持った人に相談する。

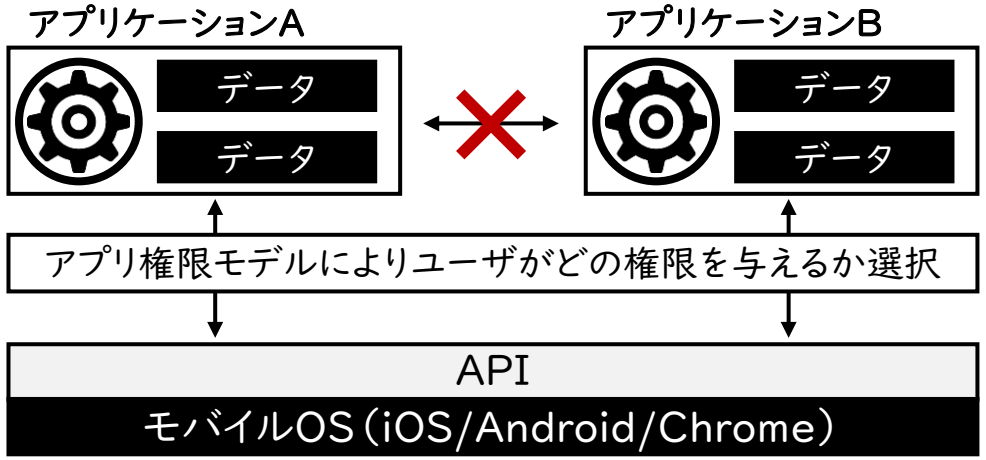
スマートフォンやタブレット利用に潜む脅威

- 職員が知っておくべきサイバーセキュリティの世界＜iOS/Android編＞ -

モバイルOS搭載機を危険に晒すのは何か

Blue Planet-works
Safety for the Connected World

iOS及びAndroid（Chrome含む）は「アプリケーションサンドボックス」という設計様式を採用しており、特定のアプリケーションが管理者（ユーザー）の許可なく、他のアプリケーションやシステム領域にアクセスすることはできない仕組みになっている。Windowsで採用されているオープンファイルシステム（特定のアプリケーションは他のアプリケーションやシステム領域にアクセスできる）の失敗を踏まえて安全な設計が施されている。



モバイルOS搭載機を危険に晒すユーザーの行動

信頼できないアプリをインストールする

不必要な権限を要求したり提供元が不明なアプリを気にせずインストールすることで侵害リスクを高める。

信頼できないWi-Fiに接続する

提供元や安全性が不確実なWi-Fiへ接続することでやり取りするデータの侵害リスクを高める。

信頼できないリンクをクリックする

SMSやSNSといった日常的に接するコミュニケーションツールを介して危険を呼び込む。

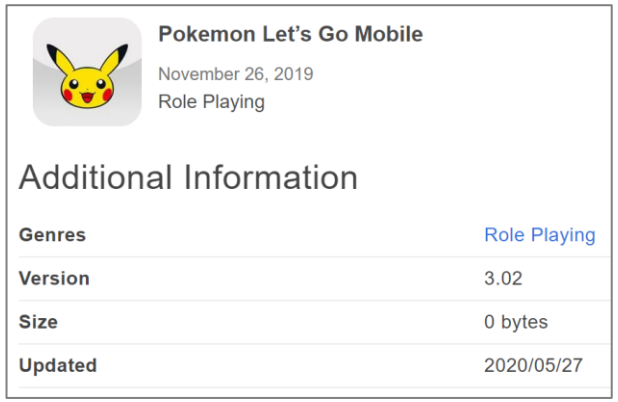
信頼できないものを受け入れる設定をする

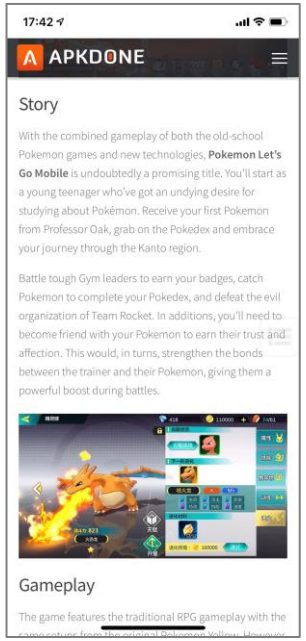
公式アプリストア以外からのインストールや発行元不明のプロファイルを受け入れる脆弱な設定をする。

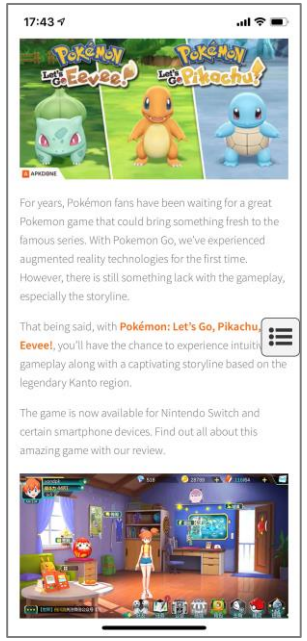
人気コンテンツを悪用したスパイウェア

Android　Chrome

Blue Planet-works
Safety for the Connected World







Android OS（Chrome OS含む）向けに配信されている「Pokemon Let's Go Mobile」は人気ゲーム「ポケットモンスター」のキャラクターやゲームシステムを無断利用して開発されたスパイウェアです。

誤ってインストールした際に開発者側に渡ってしまう権限

- ユーザーに許可なく写真撮影及び動画撮影を行うこと
- ユーザーに許可なく録音を行うこと
- ユーザーに許可なくカレンダーの編集
- ユーザーに許可なくメール及びSMSを送信
- ユーザーに許可なく保存されたデータの取得及び削除
- ユーザーに許可なく保存されたパスワード等の取得
- ユーザーに許可なく連絡先情報の読み取り
- ユーザーに許可なくシステム設定の変更
- 端末情報及び位置情報の取得

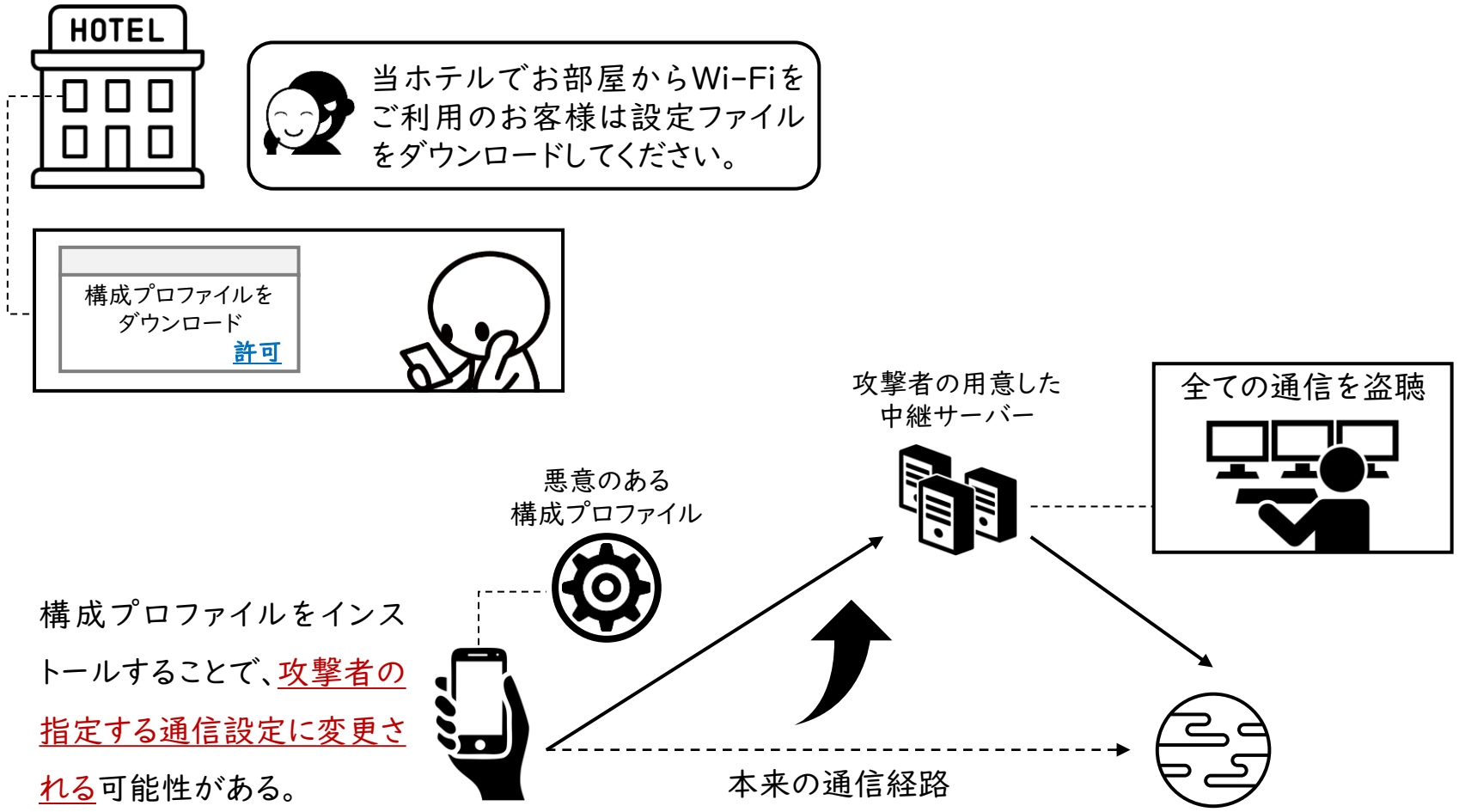
POINT

自身で安全性の判断ができないならばストア以外のウェブサイトからアプリケーションをインストールするのはやめる。

悪意ある構成プロファイルを利用した通信の盗聴

iOS

iOS上の構成プロファイル
（例：NTT Docomo）



POINT

出所が不明なものや信頼できない構成プロファイルを不用意にセットアップしない。

Wi-Fiに潜む危険性

Windows　Mac　iOS　Android　Chrome

Blue Planet-works
Safety for the Connected World

スターバックスコーヒーが提供するWi-Fiはどれ？

① **STARBUCKS_WiFi**
セキュリティ保護あり

② **at_STARBUCKS_Wi2**
セキュリティ保護あり

③ **STARBUCKS_Free_WiFi**
セキュリティ保護なし

マクドナルドが提供するWi-Fiはどれ？

① **00_MCD-FREE-WIFI**
セキュリティ保護あり

② **MCD-FREE-WIFI**
セキュリティ保護あり

③ **MCD-FREE-WiFi**
セキュリティ保護あり

接続

BPw-Sales-WiFi
セキュリティ保護あり

スマートフォンやタブレットは一度接続したことがあるWi-Fiに対しては次回以降は自動的に接続する設定がある。

接続したことのあるネットワークに自動的に接続します。接続したことのあるネットワークが見つからない場合は、手動でネットワークを選択する必要があります。

自動接続

BPw-Sales-WiFi
セキュリティ保護なし

POINT

安全性が確認できない公衆Wi-Fiに接続する場合はVPN等の通信を暗号化する仕組みを活用する。

スミッシング（SMSフィッシング）による攻撃

iOS　Android

Blue Planet-works
Safety for the Connected World

スミッシングとはスマートフォン等で利用されるショートメッセージサービス（SMS）を悪用した詐欺行為として使われている。電話番号を指定するだけで送りつけることが可能で、従来のビジネスメールの様なセキュリティフィルタが適用されていないため着弾率が極めて高い。記載されたURLをクリックすると情報を盗み取るものや不正プログラムは配布するものなど多岐にわたる。

スマートフォンのSMSに突然届く「不在通知」などに記載されているURLをクリックするとどうなるのか・・・

Windows端末からアクセスすると「メンテナンス中」の表示がされるだけで何も起きない。PCユーザーはおそらく攻撃の対象に含まれていないと思われる。

スミッシング（SMSフィッシング）による攻撃

iOS

Blue Planet-works
Safety for the Connected World

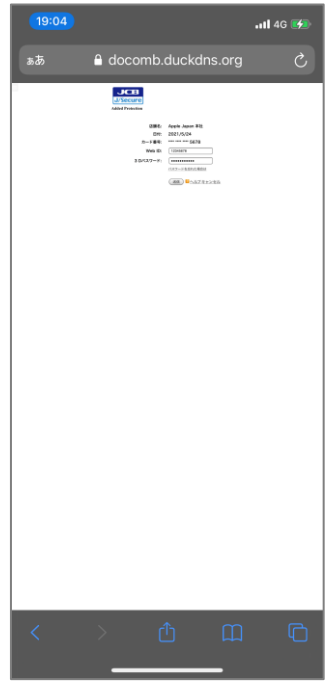
商品を配達したという内容だったのに、なぜかApple IDの認証ページが表示される。（偽物）

適当なIDとパスワードを入力して次に進める。

アカウントがロックされていると警告されて解除を要求される。

個人情報の入力画面が表示されるので、適当な情報を入力して次に進める。

今度はクレジットカードの情報を求められるので適当な情報を入力して次に進める。



JCBの「J/Secure」の認証情報を入力する様に求められるので適当な情報を入力して次に進める。

ロックが解除されたことを表現したかったのか本物のApple IDの認証ページにリダイレクトされる。

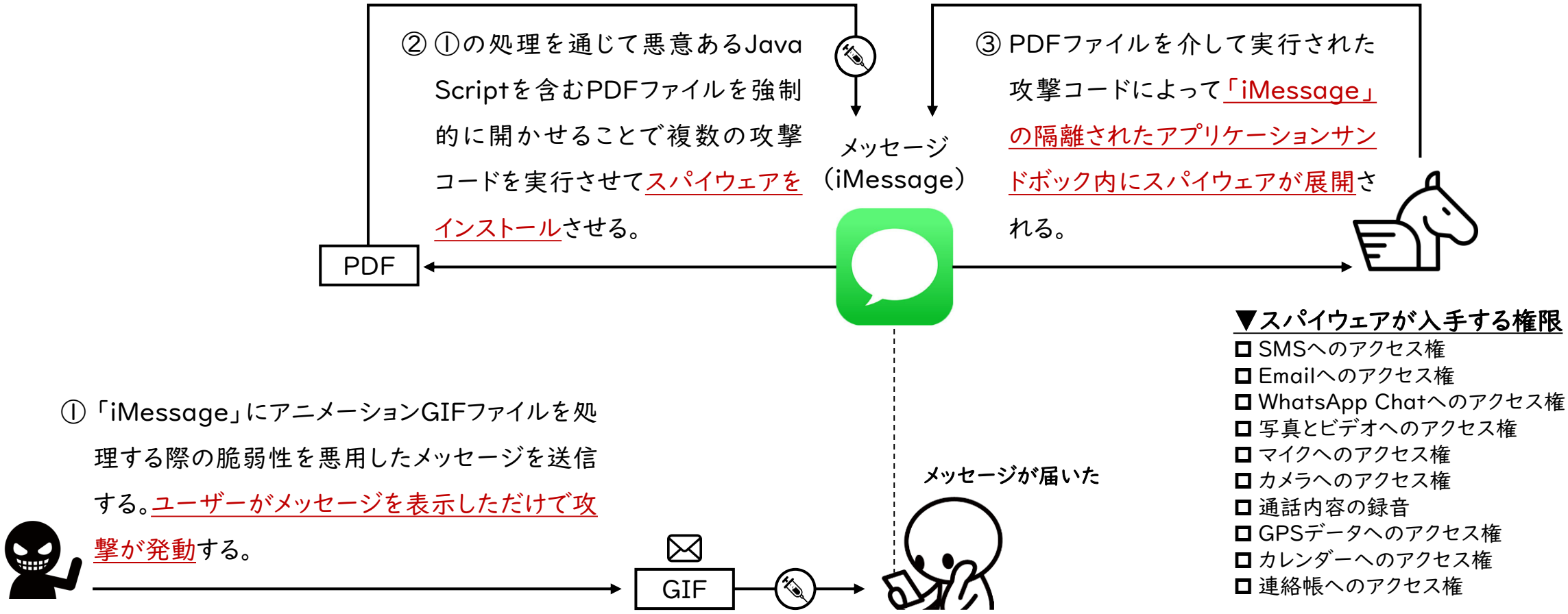
スミッシング（SMSフィッシング）による攻撃

Android　Chrome

Blue Planet-works
Safety for the Connected World

リンク先に表示されるたのは佐川急便のウェブサイトをコピーしたフィッシングサイトであり、アクセスと同時に警告ウィンドウが表示されAPK（Android Application Package）ファイルを保存するように促してくる。様々な種類が存在していると思われるが、このAPKファイルをインストールするとSMSフィッシングをばら撒く踏み台として使われてしまう。他にもいろいろと情報は抜かれてしまう。

リンクをクリックするといった操作を必要とせず「表示する」という行為のみで攻撃を成立させる手法が存在する



注：FORCEDENTRYを利用した攻撃は2021年1月にリリースされたiOS14にてセキュリティサンドボックス「BlastDoor」が実装されたことで解消された。

スマートフォンやタブレットに潜む脅威と遭遇した場合の基本的な対処方法

Blue Planet-works
Safety for the Connected World

確認	セルフチェックポイント
□	**公衆のWi-Fi環境を利用する場合のVPN接続の利用** 提供元が不確かであったり、業務に関する情報をやり取りする場合はWi-Fi接続時にVPN接続等の通信内容を保護する仕組みを利用して盗聴対策を施す。
□	**不必要なアプリケーションをインストールしない** App StoreやGoogle Play以外からアプリケーションは原則としてインストールしない。業務上、外部サイトからのインストールを要求されたら情報システム部門に相談する。
□	**不必要に権限を付与しない** 業務に必要なアプリケーションであっても利用する機能とは関係がないのに不必要な権限許可要求をされる場合があるので、許可すべきかどうかを十分に検討する。
□	**アプリケーションをインストールする時は規約を確認** アプリケーションをインストールする場合には事前に利用規約に目を通し、自身の端末情報や個人情報等がどのように扱われるのかを確認しておく。

確認	セルフチェックポイント
□	**SMSで届く連絡には注意を払う** 携帯キャリアや宅配事業者を名乗ったSMSについては内容に関係なく疑う。当該事業者がSMSを利用した通知サービスを実施しているかは事前に確認する。
□	**可能な限り生体認証の仕組みと連動させる** アプリケーションへのログインや設定変更等、重要な情報を取り扱う場合にはスマートフォンやタブレットに実装されている生体認証（指紋や顔認証）を活用する。
□	**OSとアプリケーションは常に最新の状態にしておく** OSやアプリケーションの脆弱性を悪用してユーザーに気づかれずに攻撃を展開する手法も存在しているため、常に最新の状態を維持することを心がける。
□	**端末間のデータ共有機能は使用する時だけ有効に** iOSのAirDropに代表される端末間でデータを共有する仕組みは第三者から不必要な接続や端末情報を読み取られる可能性もあり、使用する時だけ機能を有効化する。

POINT

自分で判断ができない時は必ず情報システム担当部門や専門知識を持った人に相談する。

まとめ

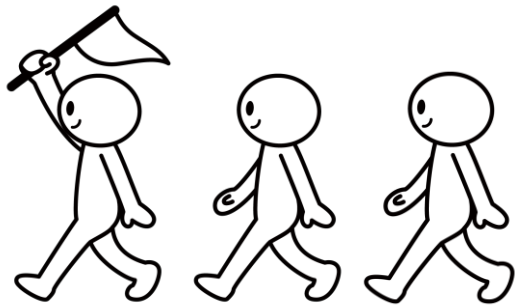
- セキュリティインシデントを引き起こす当事者にならないために -

いつ遭遇するともわからない脅威に対して
適切な対応が取れるように日頃から「セキュリティ」を意識する

例えば、我々は「地震」という「脅威」に対して何をしているのか・・・

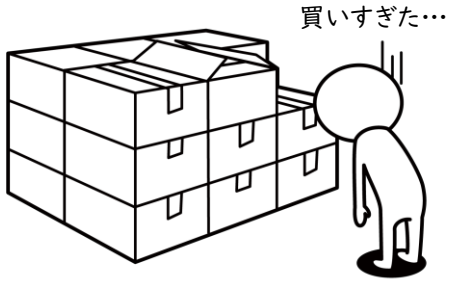
訓練

いざという時に備えて実践的な訓練を繰り返し行うことで意識の向上やスキルアップを図る。



準備

有事に備えて必需品を備蓄したり、脆弱な場所に対して補強を施し、災害時のリスクを低減する。

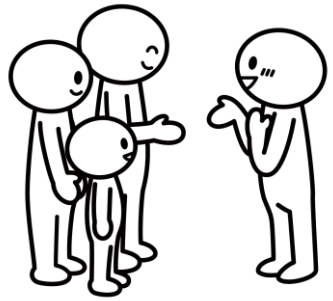


収集

過去の経験や最新の情報を入手して危険予測を行う。収集した内容に基づいて次の行動を決める。

連携

有事の際にはお互いが助け合い、必要に応じて専門家に助けを要請し、問題に対処していく。



Blue Planet-works
Safety for the Connected World

ありがとうございました。