沖縄県内企業を取り巻く
サイバー犯罪の状況について

沖縄県警察本部生活安全部
サイバー犯罪対策課
指導係

はじめに知っていただきたいこと

- サイバー犯罪は、どこか遠い国や映画の中の話ではありません。
  - 県内でも発生しており、大きな被害を受けた企業も少なくありません。

- 被害を防ぐために、安全対策（情報セキュリティ対策）を取る必要があります。
  - 情報セキュリティ対策を取らなければ、被害に遭うのは時間の問題です。
  - 必要な情報セキュリティ対策にコストをかける必要があります。

本日、お話する内容

1 情報セキュリティについて

2 サイバー犯罪の現状

3 事例紹介

- ランサムウェアによる二重恐喝（ダブルエクストーション）

4 大切な基本の対策

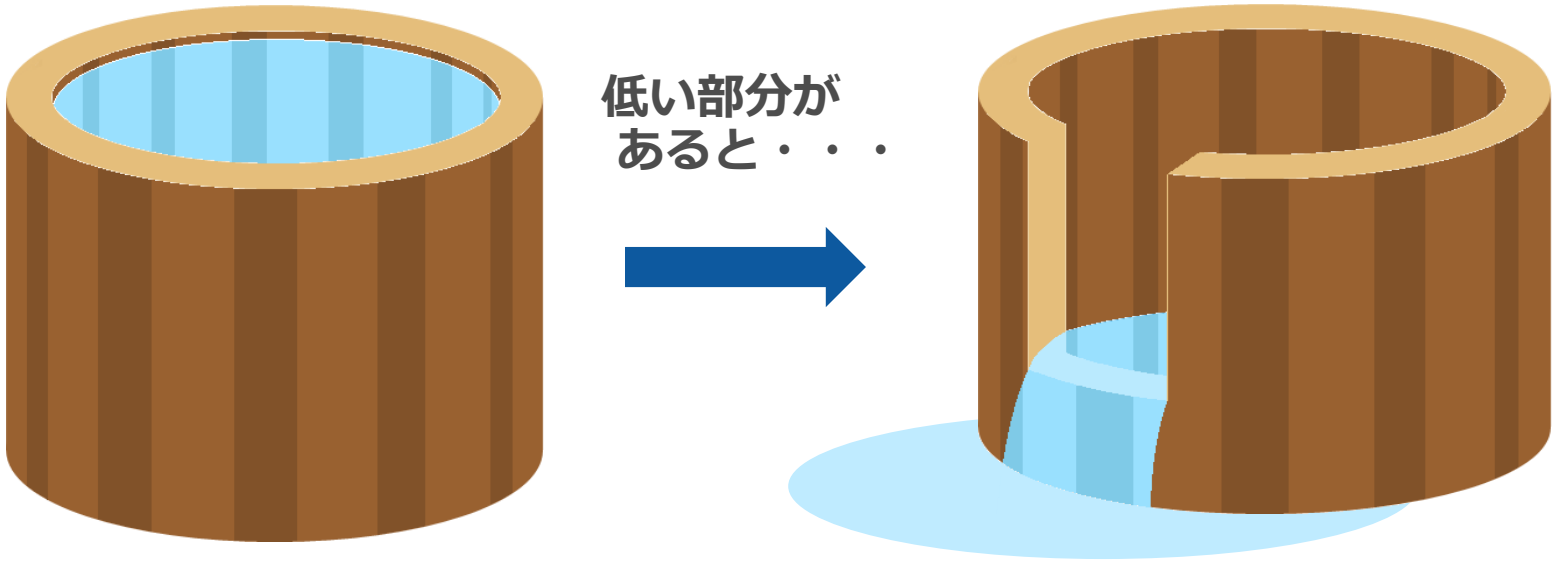
情報セキュリティについて

情報セキュリティ対策は誰が行うのか？

- 経営者？コンピュータ・情報セキュリティ管理者？一般社員？
- 情報セキュリティ対策はコンピュータ管理者や情報セキュリティ管理者などの技術者がするものと思い込んでいませんか？

情報セキュリティ対策は経営者以下
全社員で取り組むものです！

組織のセキュリティ水準はどこで決まるか？



「桶の理論」
組織のセキュリティ水準 ＝ 最も低い部分の水準

全体のセキュリティを高めるには「底上げ」が必要

【参考】IPA情報セキュリティ10大脅威 2024

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い(2016年以降)
１位	ランサムウェアによる被害	2016年	９年連続９回目
２位	サプライチェーンの弱点を悪用した攻撃	2019年	６年連続６回目
３位	内部不正による情報漏えい等の被害	2016年	９年連続９回目
４位	標的型攻撃による機密情報の窃取	2016年	９年連続９回目
５位	修正プログラムの公開前を狙う攻撃（ゼロディ攻撃）	2022年	３年連続３回目
６位	不注意による情報漏えい等の被害	2016年	６年連続７回目
７位	脆弱性対策の公開に伴う悪用被害	2016年	４年連続７回目
８位	ビジネスメール詐欺による金銭被害	2018年	７年連続７回目
９位	テレワーク等のニューノーマルな働き方を狙った攻撃	2021年	４年連続４回目
10位	犯罪のビジネス化（アンダーグラウンドサービス）	2017年	２年連続４回目

選ばれる脅威は毎年ほとんど変わらない！

出典：情報セキュリティ10大脅威 2024

サイバー犯罪の現状

サイバー犯罪とは

情報技術や通信機能を利用した犯罪
インターネットを利用した犯罪

不正アクセス禁止法違反

ネットワーク上で他人のアカウント（ID､パスワード等）を無断で使用する など

コンピュータ･電磁的記録対象犯罪等

データを改ざんする
ウイルスに感染させて情報を窃取する など

ネットワーク利用犯罪

インターネット上で児童ポルノを公開する
保護者の同意を得ず深夜にSNSで青少年を呼び出す など

サイバー犯罪の特徴

匿名性が高い

IDやハンドル名が使われることが多く、相手方を確認する手段がほとんどないため、「なりすまし」されやすい。

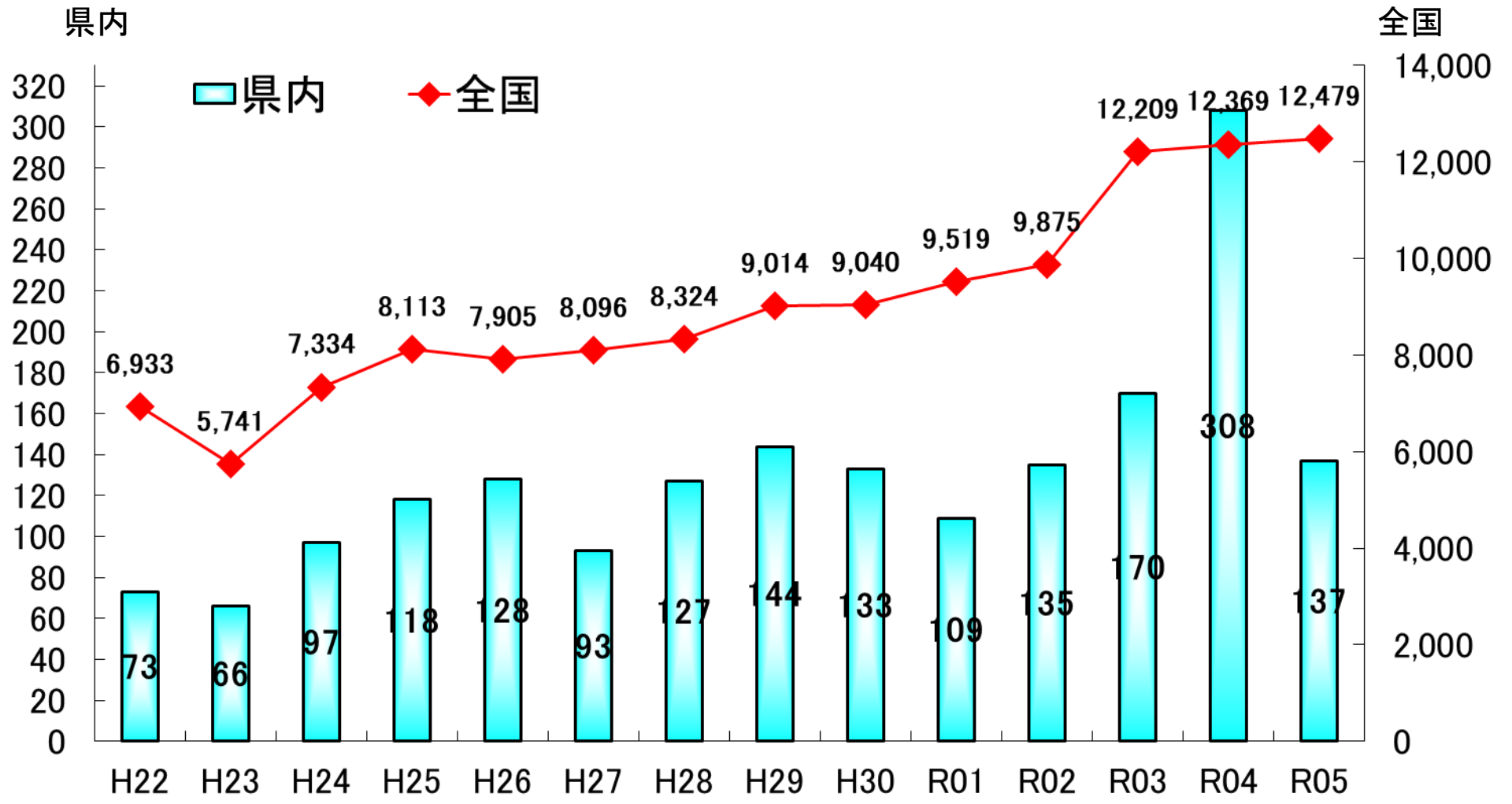
痕跡が残りにくい

使用履歴などを正しく記録する仕組みや設定がなされていれば、大きな手掛かりとなる。

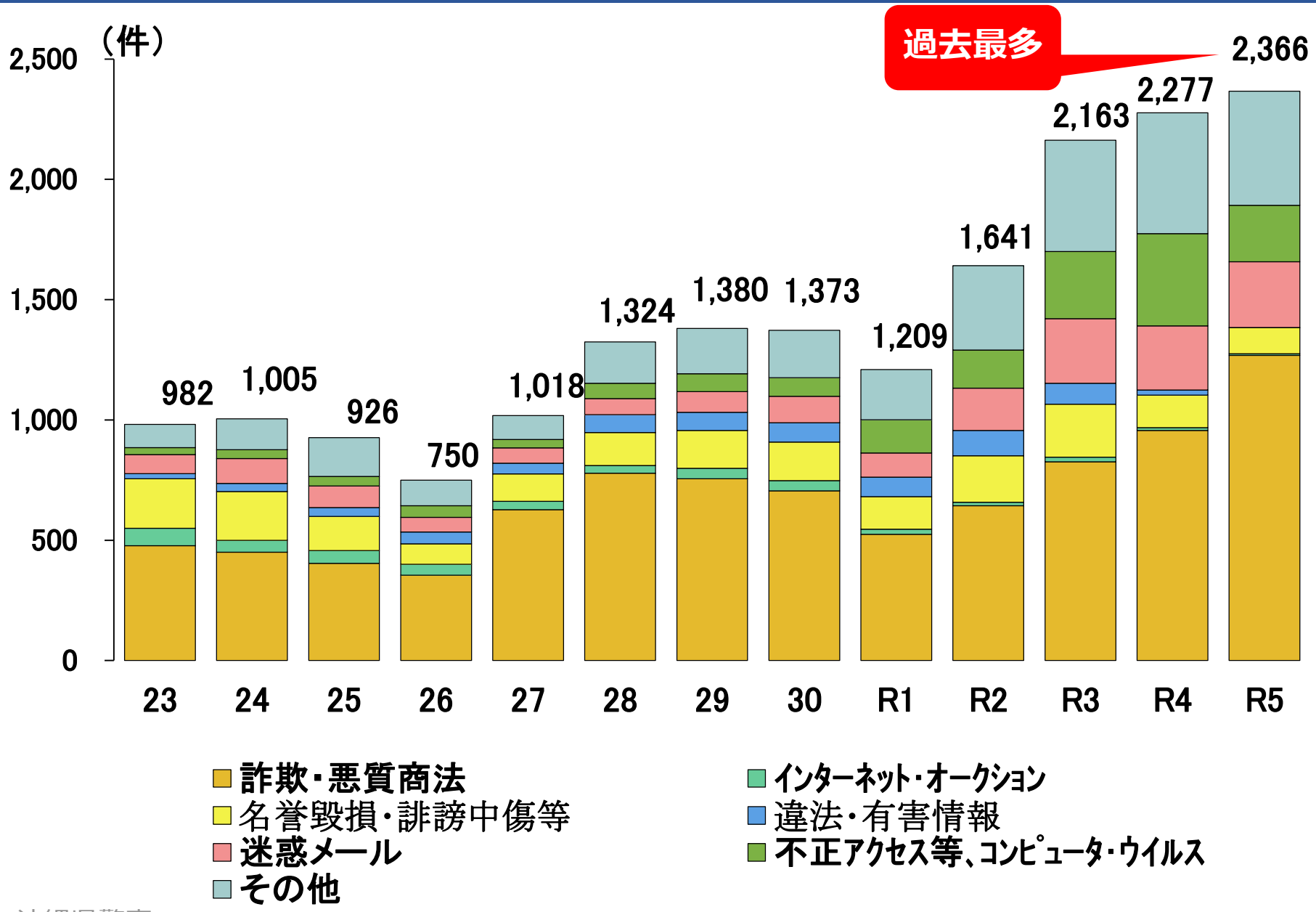
場所や時間の制約が少なく、不特定多数に被害が及びやすい

サイバー空間に国境はなく、どこでも、いつでも、誰でも被害者になり得る。

サイバー犯罪の検挙件数の推移



サイバー犯罪等に関する相談件数の推移／県内

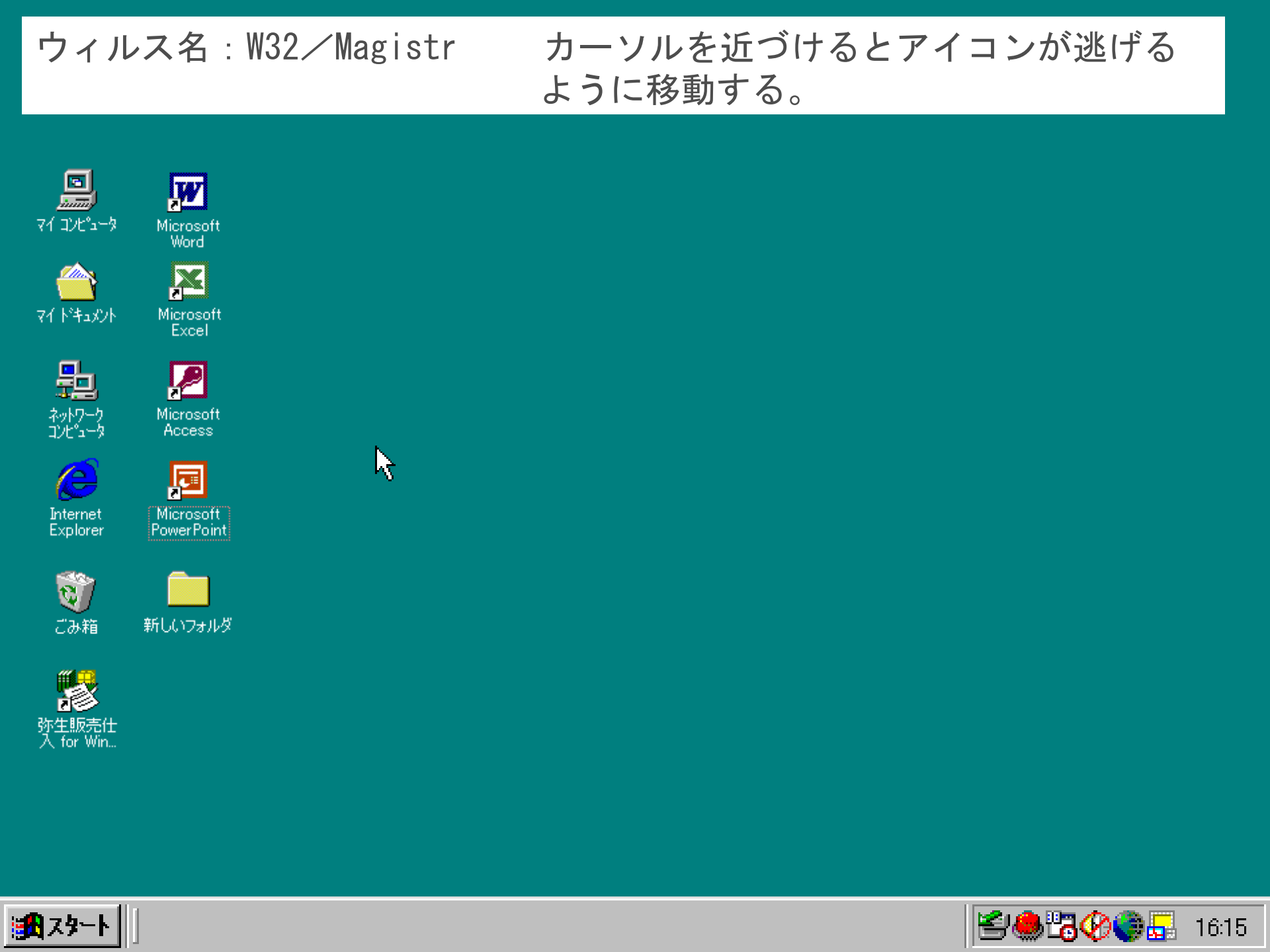


ランサムウェアによる二重恐喝（ダブルエクストーション）

ウィルス名：W32／Hybris　　渦巻きを画面に表示して作業の邪魔をする。

マイ ドキュメント
Microsoft Excel
Internet Explorer
Microsoft PowerPoint
ネットワーク コンピュータ
Microsoft Word
ごみ箱
弥生販売仕入 for Win...
新しいフォルダ
A 般
CAPS
KANA
スタート
16:15

ウィルス名：W32／Magistr　　カーソルを近づけるとアイコンが逃げるように移動する。



ランサムウェアによる二重恐喝（ダブルエクストーション）

従来のランサムウェア（Ransom【身代金】）

感染させたパソコンのファイルを勝手に暗号化するなどパソコンに制限をかけ、その制限の解除と引き換えに仮想通貨（暗号資産）等を要求するウイルス

被疑者

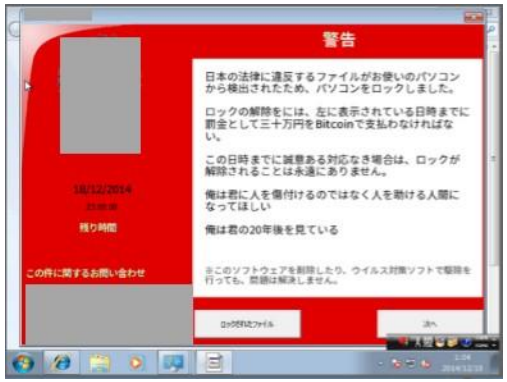
ブログサイト

① ソフトウェアの更新プログラムを偽装してアップロード

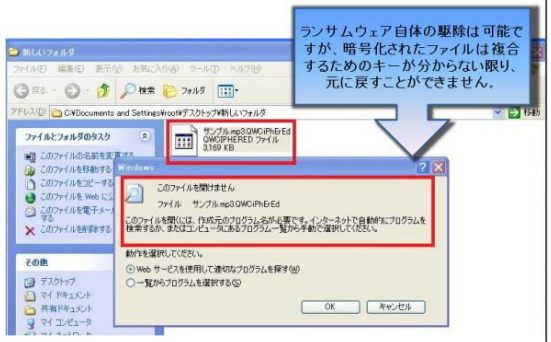
② 閲覧

③「ランサムウェア」のダウンロード

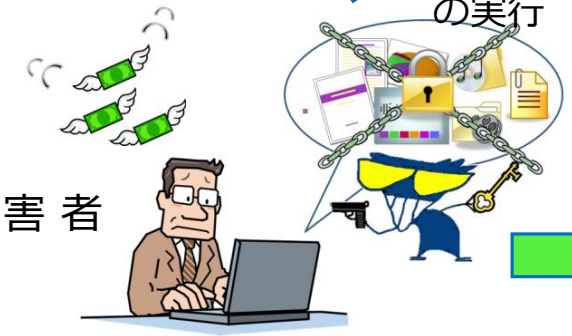
④「ランサムウェア」の実行



・警告画面の表示と暗号資産等の要求



・ファイルの暗号化



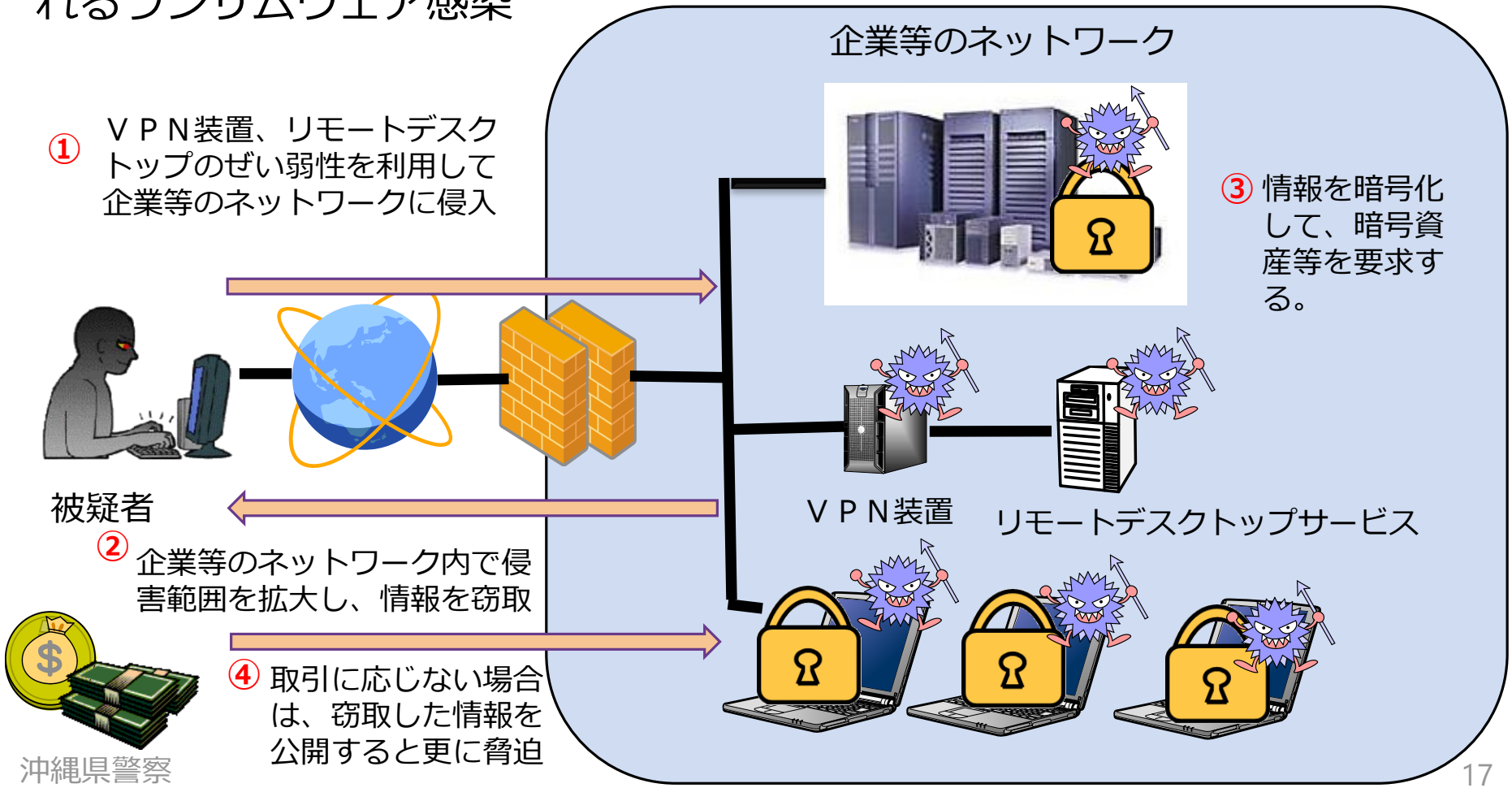
被害者

仮想通貨等の支払い

ランサムウェアによる二重恐喝（ダブルエクストーション）

二重恐喝（ダブルエクストーション）

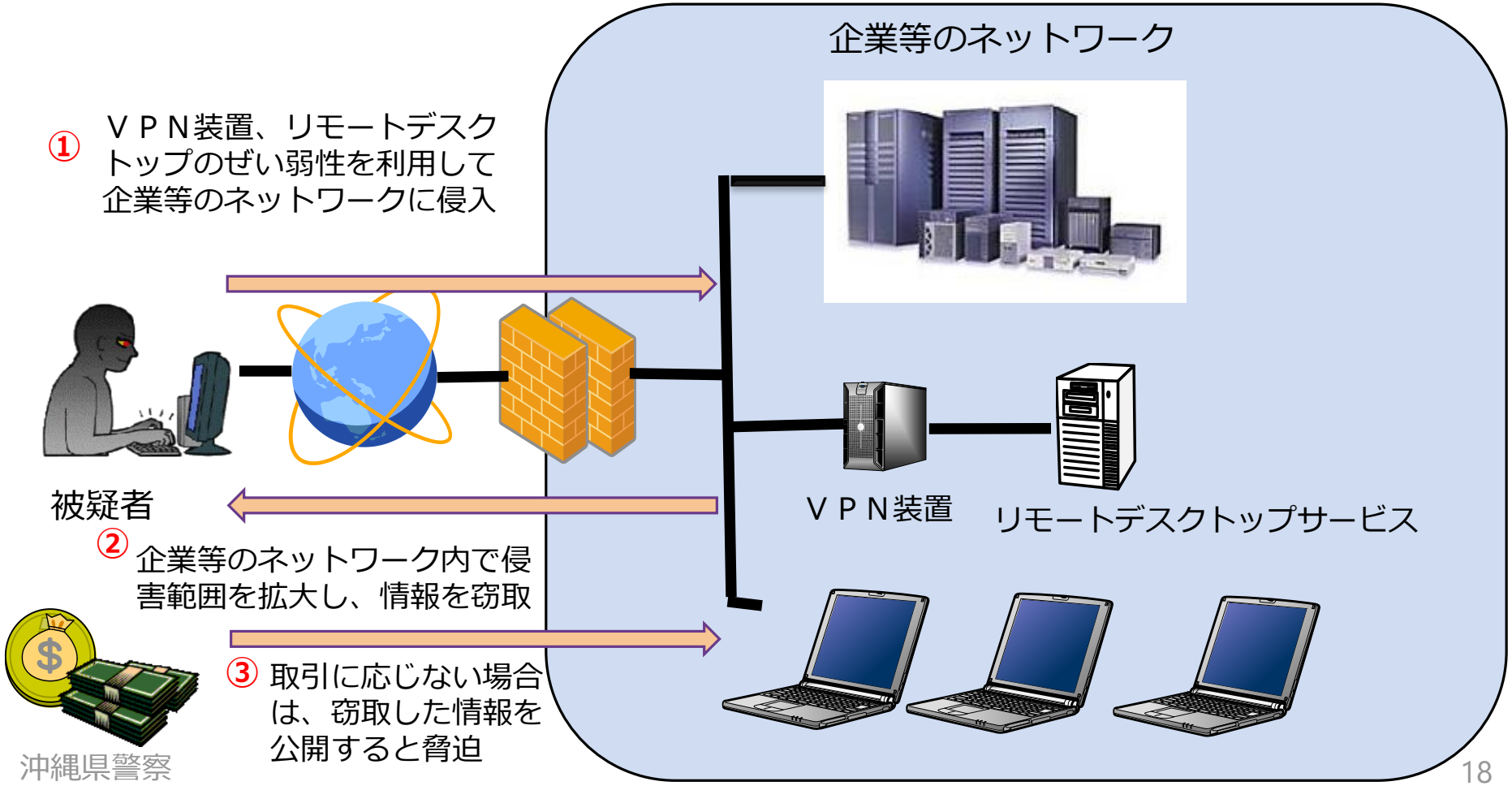
企業等を標的として、情報を窃取した上で暗号化を行い、当該情報を公開しないことと引き換えに取引に応じるように脅迫する二重恐喝とみられるランサムウェア感染



ランサムウェアによる二重恐喝（ダブルエクストーション）

ノーウェアランサム

データを暗号化する（ランサムウェアを用いる）ことなくデータを窃取し対価を要求する手口



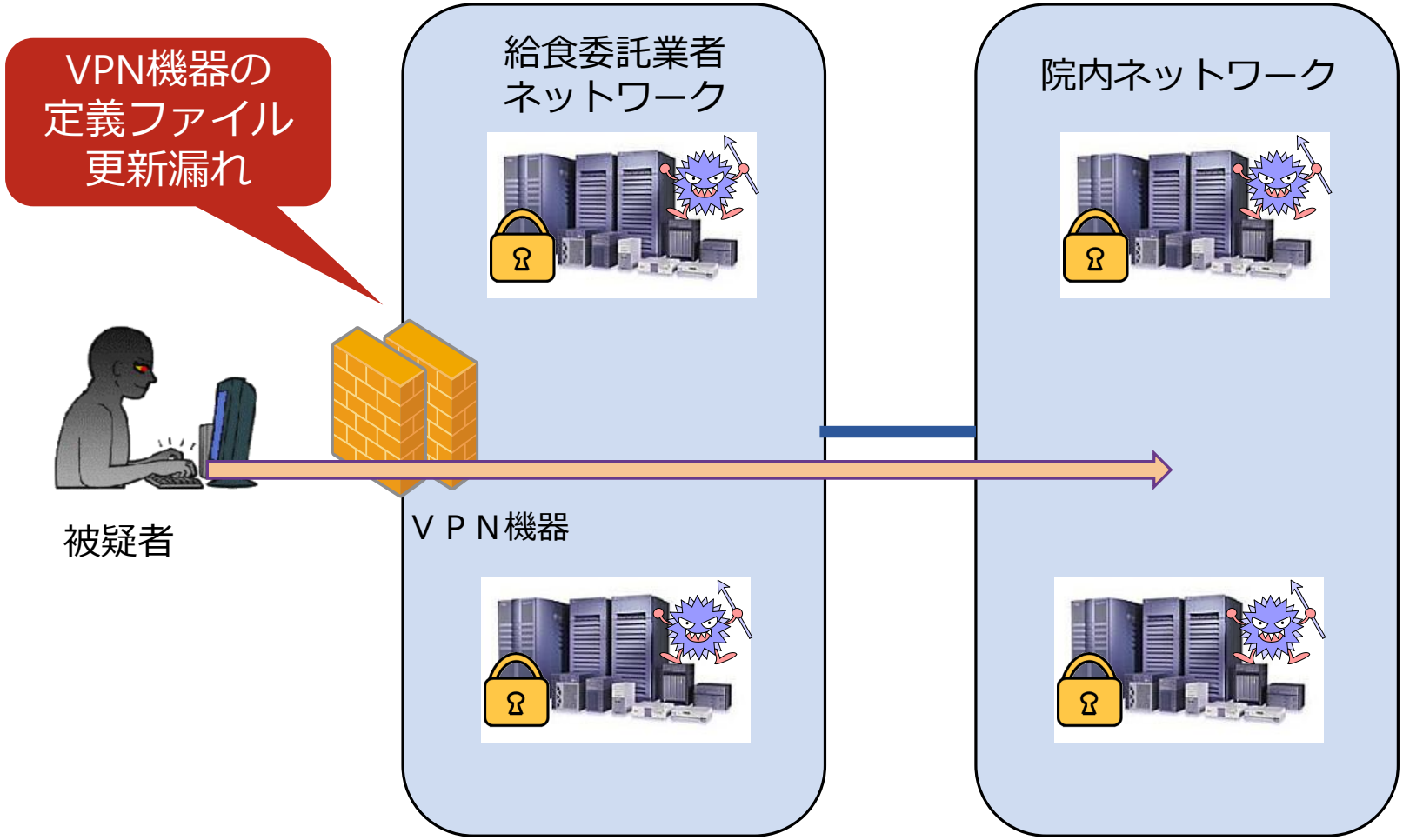
ランサムウェア感染事案

琉球新報

令和５年７月６日

ランサムウェア感染事案

大阪急性期・総合医療センターの例（2022年10月30日）



サプライチェーンのVPN機器のぜい弱性が放置されていた

ランサムウェア感染事案（県内）

令和４年10月16日
琉球新報

令和４年10月16日
沖縄タイムス

ランサムウェア感染事案（県内）

VPN機器

未更新！

機器の更新作業

図書館

？

運用会社　　リース会社

令和５年２月９日
琉球新報

ランサムウェアへの対策

身代金型ウイルスの主な感染経路
- **メール（添付ファイル、本文に記されたアドレス）**
- **不正なウェブサイトを閲覧**
- **ネットワークを経由して脆弱性を攻撃**

- ＯＳ、ソフトウェアを最新状態に保つ
- ウイルス対策ソフトを正しく使用する
- 安易にメールの添付ファイルを開いたり、メール本文のリンクをクリックしない
- 大切なデータをこまめにバックアップする
- 身代金は支払わない

ランサムウェアへの対策

- 警察庁において、ランサムウェアによって暗号化された被害データを復号するツールを開発
  - 被害に遭ってしまったら相談・通報をお願いします
- 『No More Ransom』というサイトで復号ツールが公開されていることがあります

大切な基本の対策

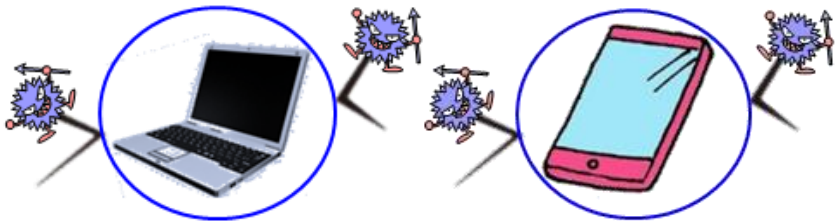
基本的なセキュリティ対策

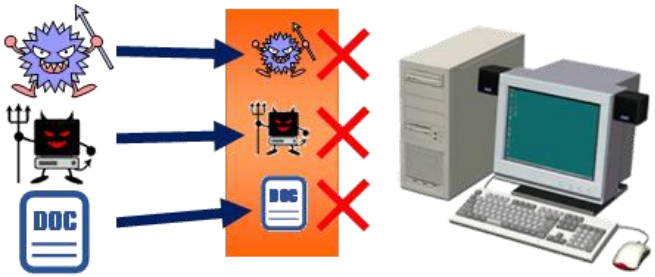
ＯＳ、ソフトウェアを**最新状態**に保つ

- Windows 7 / 8 を使っていませんか？
- Windows Update は正常に行われていますか？
- 古いブラウザ、メールソフトなどを使っていませんか？

セキュリティソフトを**最新状態**で使用する

- ライセンスは有効ですか？
- 最新のバージョンを使っていますか？
- セキュリティソフトの定義ファイルは最新ですか？





Internet Explorerのサポート終了について

Internet Explorerのサポート終了

- **2022年６月16日**にInternet Explorerの<u>サポートが終了</u>しました。
- EdgeのIEモードは、2029年までは<u>サポートが継続される予定</u>です。
- IEでの利用を前提とした業務アプリケーション等は早めの対応を検討しましょう。

MyJVNバージョンチェッカ for .NET

Windowsパソコンに入っているソフトウェアが
最新版であるかを**確認**できる**無料のツール**

対応ソフト

- Adobe Reader
- Adobe Flash Player
- JRE（Java実行環境）
- Firefox、Chrome
- Thunderbird
- iTunes
- QuickTime
- Lhaplus　など

MyJVNバージョンチェッカ for .NET 入手先

https://jvndb.jvn.jp/apis/myjvn/vccheckdotnet.html

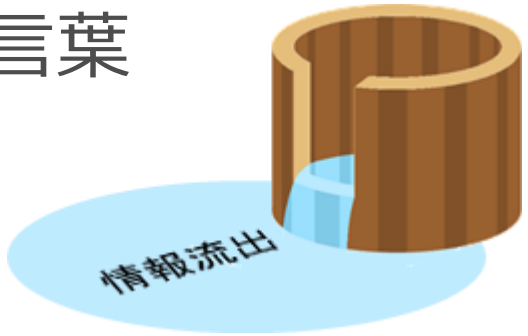
定期的なバックアップ等について

ランサムウェア等に備えたバックアップ

- ランサムウェアにより、バックアップデータも暗号化されてしまうという事例が確認されています。
- 不測の事態に備えて、バックアップはなるべくこまめに取得し、ネットワークから切り離して保管しましょう。
- バックアップデータによるシステム復旧手順を確認しておきましょう。

パスワードの重要性

- “適切ではない”パスワードの例
  - 生年月日、電話番号、辞書にある言葉
  - 同じパスワードの使い回し



- 適切なパスワードの作り方（例）

① 覚えやすい言葉を選ぶ　「ハイサイおじさん」

② ローマ字にする　haisaiojisan

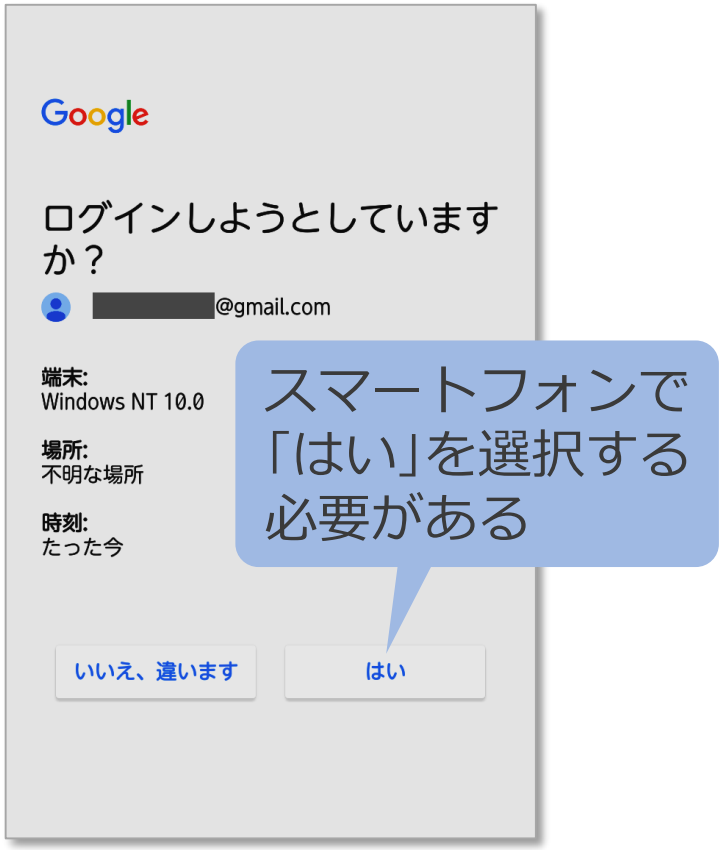
③ 大文字、数字、記号を入れる（基本パスワードの完成）　Haisa!oji3

④ サービス名にちなんだ文字を加える　〔Yahoo!なら〕 YAHaisa!oji3

２段階認証を有効にして安全性を高める

Gmailにパスワード認証でログインとしたら･･･

スマートフォン認証も必要（スマートフォン側）



県警サイバー犯罪対策課公式SNS（X・LINE）

サイバー犯罪や
サイバーセキュリティに
関する情報を
随時発信しています！

X

https://twitter.com/opp_cyber/

LINE

https://lin.ee/1UTWGD3

参考　IPA情報セキュリティ安心相談窓口等

- 情報セキュリティに関する技術的な相談に対して電話やメールでアドバイスを提供

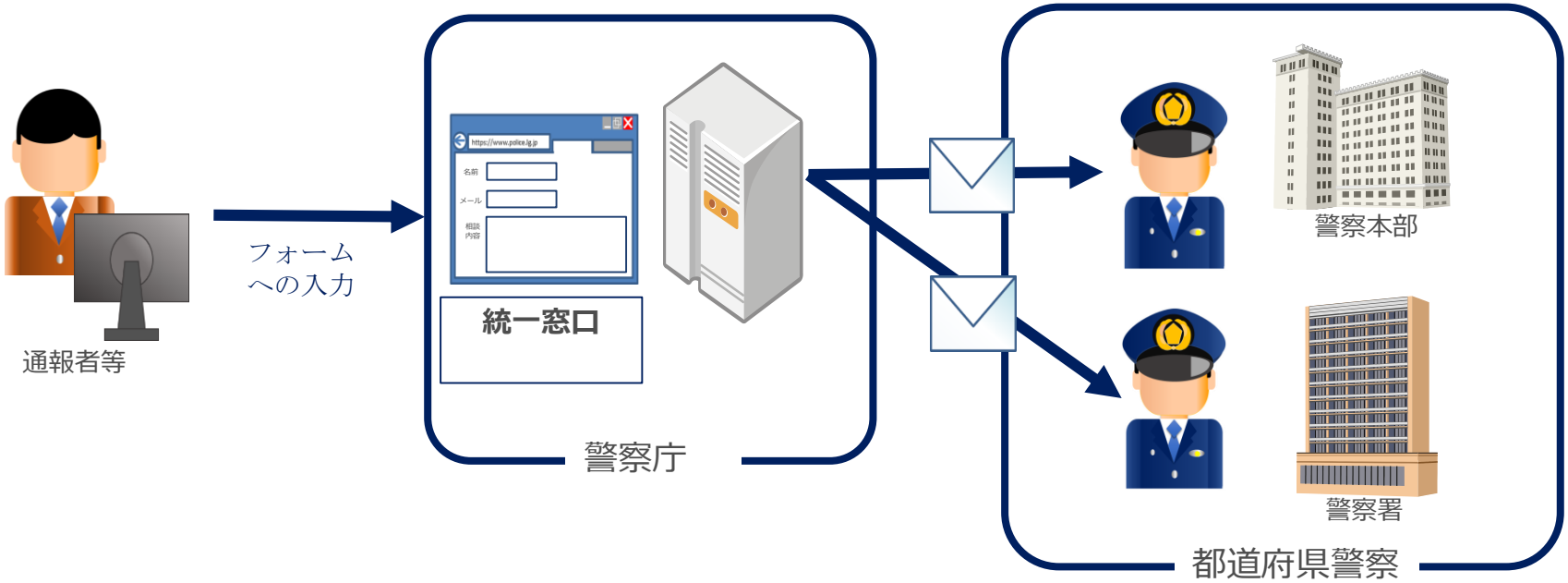
  電話番号：**０３－５９７８－７５０９**
  平日10:00-12:00 および 13:30-17:00

  メール：**anshin@ipa.go.jp**

- 映像で知る情報セキュリティ
  - Youtube「**IPAチャンネル**」でいつでも視聴可能
- ５分でできる！ポイント学習
  - インターネット接続環境があれば、いつでもどこでも学習可能な、eラーニングシステム

サイバー事案に関する通報等のオンライン窓口

- 警察庁ウェブサイトにおいて、サイバー事案に関する通報等の全国統一のオンライン受付窓口が設置されました。



- 爆破予告、殺人予告、自殺予告等の人命に関わる事案は最寄りの警察署へ通報又は110番通報！

警察の情報発信・相談窓口を活用してください

警察の相談窓口

- 警察本部警察安全相談窓口

  TEL 098-863-9110
  （又はプッシュ回線等から
  #9110）

- 各警察署の警察安全相談窓口

ご清聴ありがとうございました