県内企業を取り巻く
サイバー犯罪の状況について

令和３年１１月１１日

沖縄県警察本部生活安全部サイバー犯罪対策課
課長補佐（サイバー犯罪対策担当）　赤嶺智

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 サイバー犯罪の現状

2 事例紹介

- インターネットバンキングを狙った偽メール
- 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）

3 大切な基本の対策

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

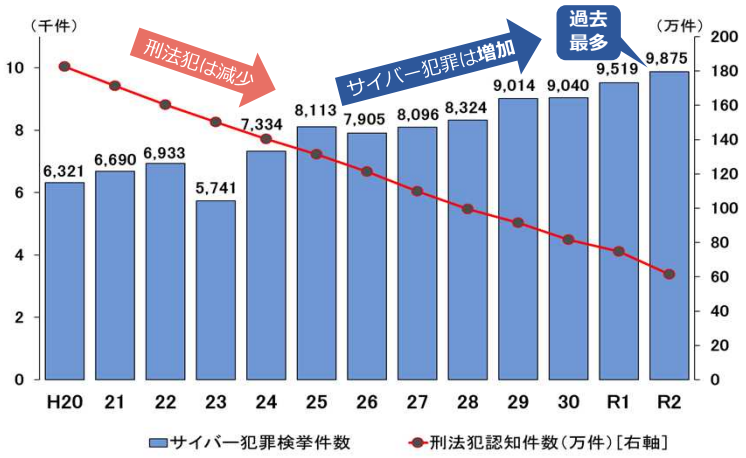
サイバー犯罪の特徴

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。

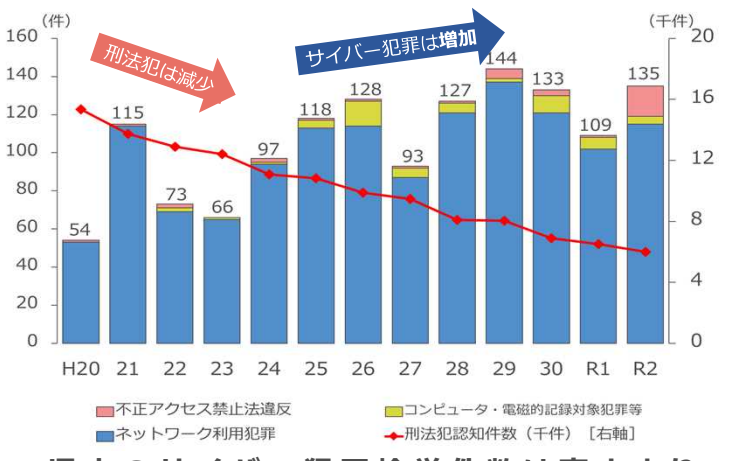
場所や時間の制約が少なく、不特定多数に被害が及びやすい
サイバー空間に国境はなく、どこでも、いつでも、誰でも被害者になり得る。

サイバー犯罪検挙件数の推移／全国



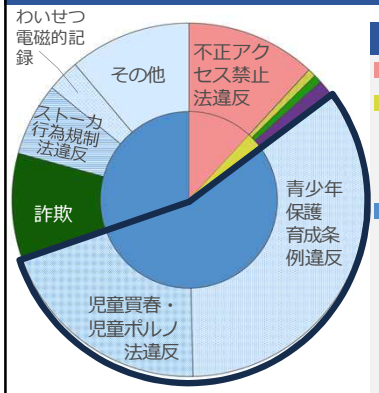
犯罪の発生場所は実空間からサイバー空間へ

サイバー犯罪検挙件数の推移／県内



県内のサイバー犯罪検挙件数は高止まり

サイバー犯罪検挙の内訳／県内 Ｒ２年

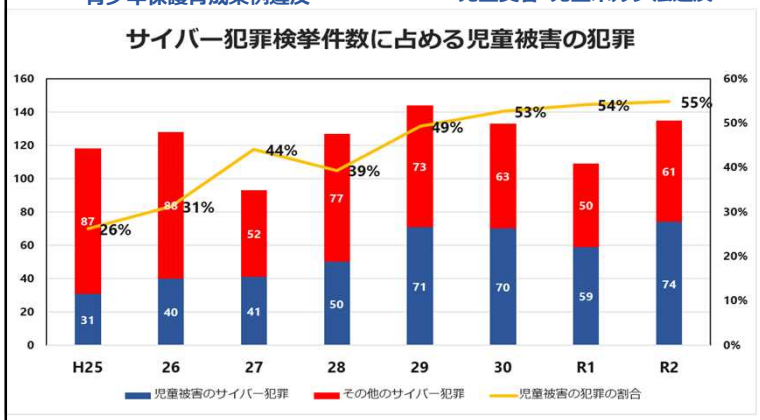


罪種	件	内訳
不正アクセス禁止法違反	16	
コンピュータ・電磁的記録対象犯罪等	4	
私電磁的記録不正作出		1
電子計算機損壊等業務妨害		1
電子計算機使用詐欺		2
ネットワーク利用犯罪	115	
青少年保護育成条例違反		47
児童買春・児童ポルノ法違反		27
詐欺		13
ストーカ行為規制法違反		9
わいせつ図画公然陳列・頒布		4
その他		14
合計	135件	

54.8%

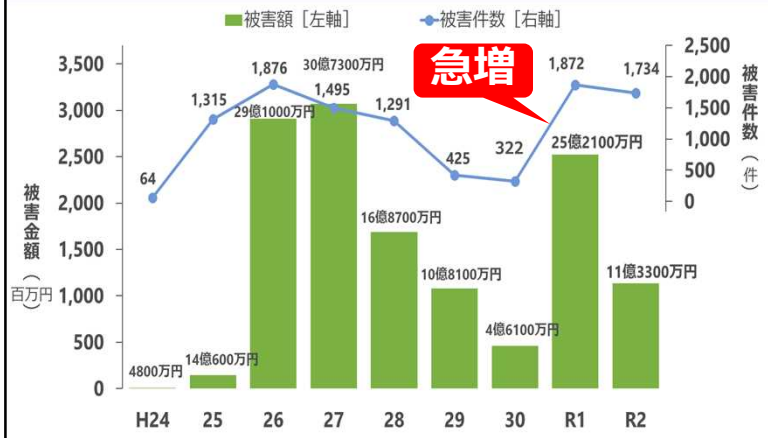
児童が被害者となる罪種が54.8%を占める

児童が被害者となる罪種が件数を押し上げ



児童が被害者となる罪種の占める割合が増加

インターネットバンキング不正送金被害の推移／全国



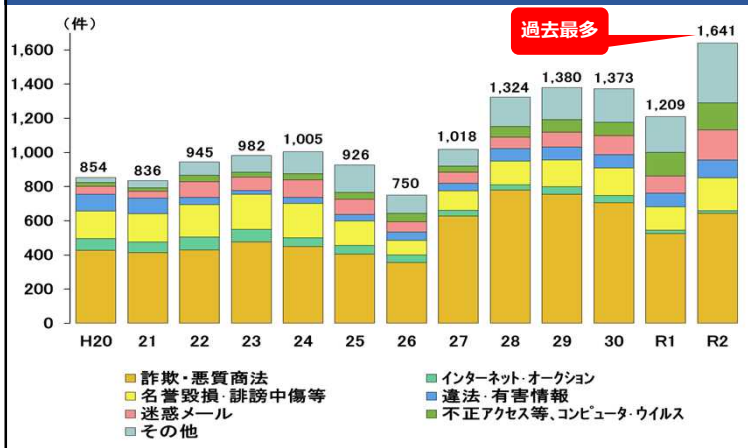
減少傾向にあったが、令和元年9月から急増！！

インターネットバンキング不正送金被害の推移／県内

全国の傾向と同様に令和元年９月以降急増！！

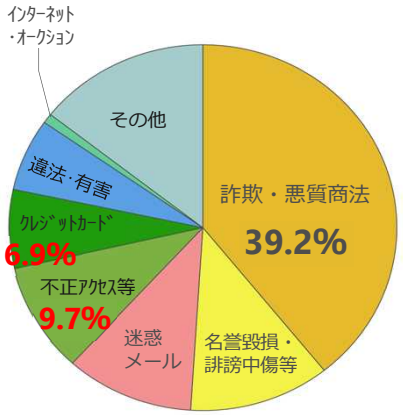
サイバー犯罪等に関する相談

サイバー犯罪等に関する相談件数の推移／県内



平成２８年以降、県内の相談件数は高水準で推移
Ｒ２年は、インターネット・オークションに関する相談を除く全ての区分で増加

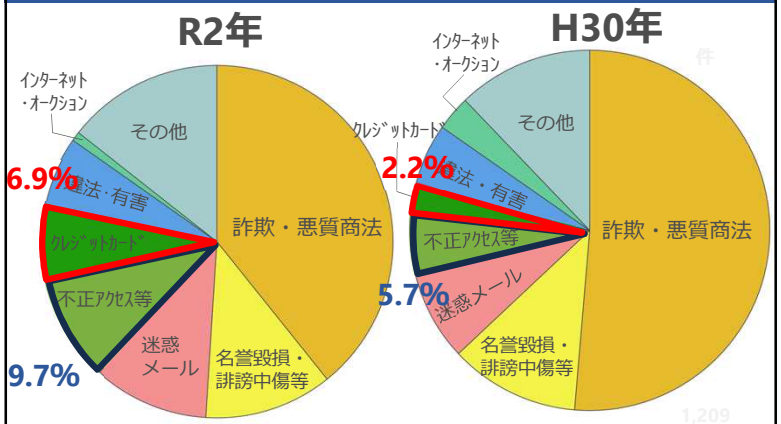
サイバー犯罪等に関する相談の内訳／県内Ｒ２年



項　　目	件
詐欺・悪質商法	644
名誉毀損・誹謗中傷等	138
迷惑メール	135
不正アクセス等、コンピュータ・ウイルス	101
クレジットカード番号窃取等	114
違法・有害情報	105
インターネット・オークション	14
その他	236
合計	1,641

詐欺・悪質商法に関する相談が約３９％を占める

サイバー犯罪等に関する相談の内訳／県内Ｒ２年



より悪質な不正アクセス等・コンピュータ・ウイルスや
クレジットカード番号窃取等の相談の割合が増加！！

サイバー犯罪等に関する相談件数から見る情勢の分析

詐欺・悪質商法
ｲﾝﾀｰﾈｯﾄ・ｵｰｸｼｮﾝ
} 減少

迷惑メール → 増加傾向

名誉毀損・誹謗中傷等 → 減少傾向から横ばいへ

不正ｱｸｾｽ等、ｺﾝﾋﾟｭｰﾀｳｲﾙｽ → 令和元年以降高止まり

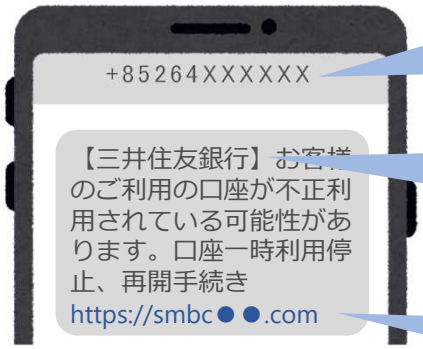
ｸﾚｼﾞｯﾄｶｰﾄﾞ番号窃取等 → 増加傾向

●これまでの詐欺・悪質商法（架空請求、不当請求、詐欺サイト等）から被害が大きく、悪質化したものとなっている。

インターネットバンキングを狙った偽メール

インターネットバンキングを狙った偽メール１

令和元年９月以降全国でSMSを用いたフィッシングの被害が多発



海外からの**ショートメッセージ／SMS**
本事例では、香港から

三菱UFJ銀行、みずほ銀行、ゆうちょ銀行、イオン銀行等、様々な金融機関を偽ったSMSが確認されている。

正規の事業者を連想させるリンクは危険な**偽サイト！**

メールに書かれたリンク先はフィッシングサイト！

インターネットバンキングを狙った偽メール１

他の事例（ゆうちょ銀行）では・・・

１　フィッシングサイトへの情報入力

ＳＭＳにより誘導された本物そっくりのフィッシングサイトで、インターネットバンキングに必要な情報（ＩＤ、パスワード、合い言葉）を入力

２　金融機関から自動音声による確認コードの通知

携帯電話に金融機関から電話があり、自動音声による確認コードが通知された。

３　フィッシングサイトへの確認コードの入力

１のフィッシングサイトに確認コードを入力する欄があり、同欄に金融機関から電話にて通知を受けたコードを入力

インターネットバンキングを狙った偽メール１

どうなったか（結果）

1　ハードウェアトークンによるワンタイムパスワードを設定していたが解除された。

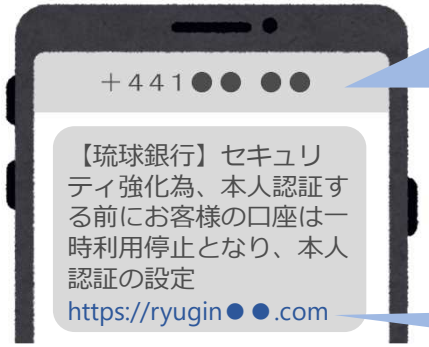
2　被疑者側でインターネットバンキングの認証アプリを登録され、送金時の認証を被疑者側が自由にできる状態となった。

3　限度額まで不正送金された。

犯罪の手口は、日々巧妙化している。

インターネットバンキングを狙った偽メール２

県内金融機関を装った偽メール！！



海外からの**ショートメッセージ／SMS**（当初は海外であったが、現在は、国内の携帯電話も存在）

琉球銀行を連想させるURL

インターネットバンキングを狙った偽メール２

県内金融機関を装った偽メール！！

海外からの**ショートメッセージ／SMS**（当初は海外であったが、現在は、国内の携帯電話も存在）

琉球銀行を連想させるURL

令和元年12月から令和２年12月に偽メールが送付！！

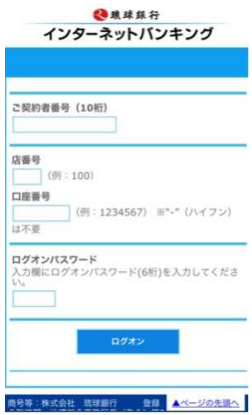
インターネットバンキングを狙った偽メール２

本物

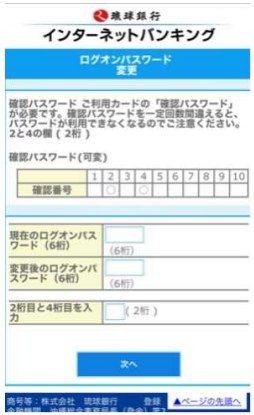
偽サイト

タップすると表示される偽サイト

インターネットバンキングを狙った偽メール２



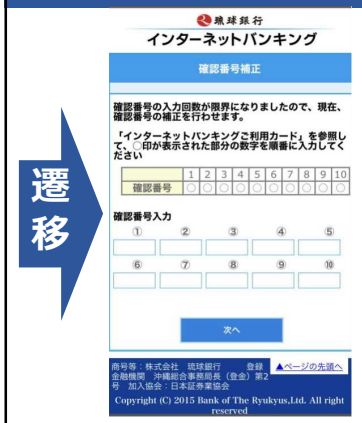
遷移



偽サイトに契約者番号、店番号、口座番号等を入力する。

現在のログオンパスワード等を入力する。

インターネットバンキングを狙った偽メール



遷移

遷移

求められる確認番号を入力する。

インターネットバンキングで送金操作の際に必要な全ての情報が犯罪者に渡る。

インターネットバンキングを狙った偽メール２

今回の県内金融機関の偽メールの被害

（令和元年12月、令和２年２月、６月、12月）は

被害件数 ３９件

(12月７件、2月７件、６月1件、12月２３件、県外１件を含む。)

被害額　3,034万5,700円

昨年の県内の被害総額（４１件）は・・

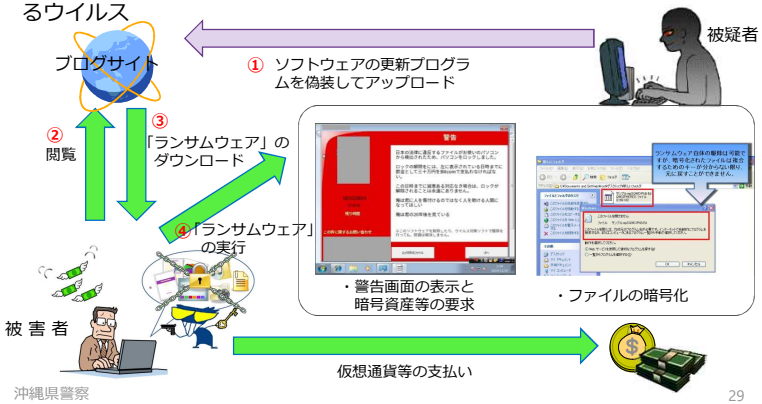
被害総額　約3,６１４万円

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）

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】）

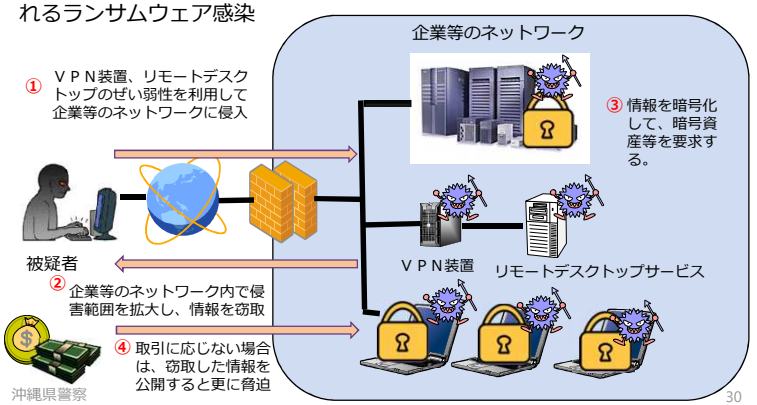
感染させたパソコンのファイルを勝手に暗号化するなどパソコンに制限をかけ、その制限の解除と引き換えに仮想通貨（暗号資産）等を要求するウイルス



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



大切な基本の対策

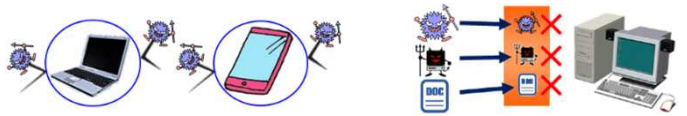
基本的なセキュリティ対策

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のサポートが終了します。**
- **EdgeのIEモードは、少なくとも2025年10月14日まではサポートが継続されます。**
- **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。**
- **Windows 8.1のInternet Explorerは使用可能ですが、2023年１月10日にはサポートが終了します。**

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

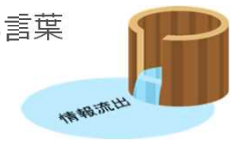
ランサムウェア等に備えたバックアップ

- **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!0ji3
④ サービス名にちなんだ文字を加える	〔Yahoo!なら〕 YAHaisa!0ji3

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）

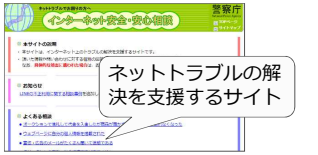
【参考】県警サイバー犯罪対策課公式SNS（Twitter・LINE）

●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。

【Twitter】
https://twitter.com/opp_cyber/
【LINE】
https://lin.ee/1UTWGD3

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



警察庁 インターネット安全・安心相談
https://www.npa.go.jp/cybersafety/

沖縄県警察 サイバー犯罪対策
http://www.police.pref.okinawa.jp/

ご静聴ありがとうございました