秋田県警察サイバー防犯ボランティアイメージキャラクター

紅（あか）っち　　蒼（あお）っち

サイバー犯罪の現状と対策について

令和７年11月27日

秋田県警察本部サイバー犯罪対策課

本日の講話内容

1　サイバー犯罪の現状

2　事例から考える最新の手口

3　セキュリティ対策

1　サイバー犯罪の現状

2　事例から考える最新の手口

3　セキュリティ対策

１　サイバー犯罪の現状

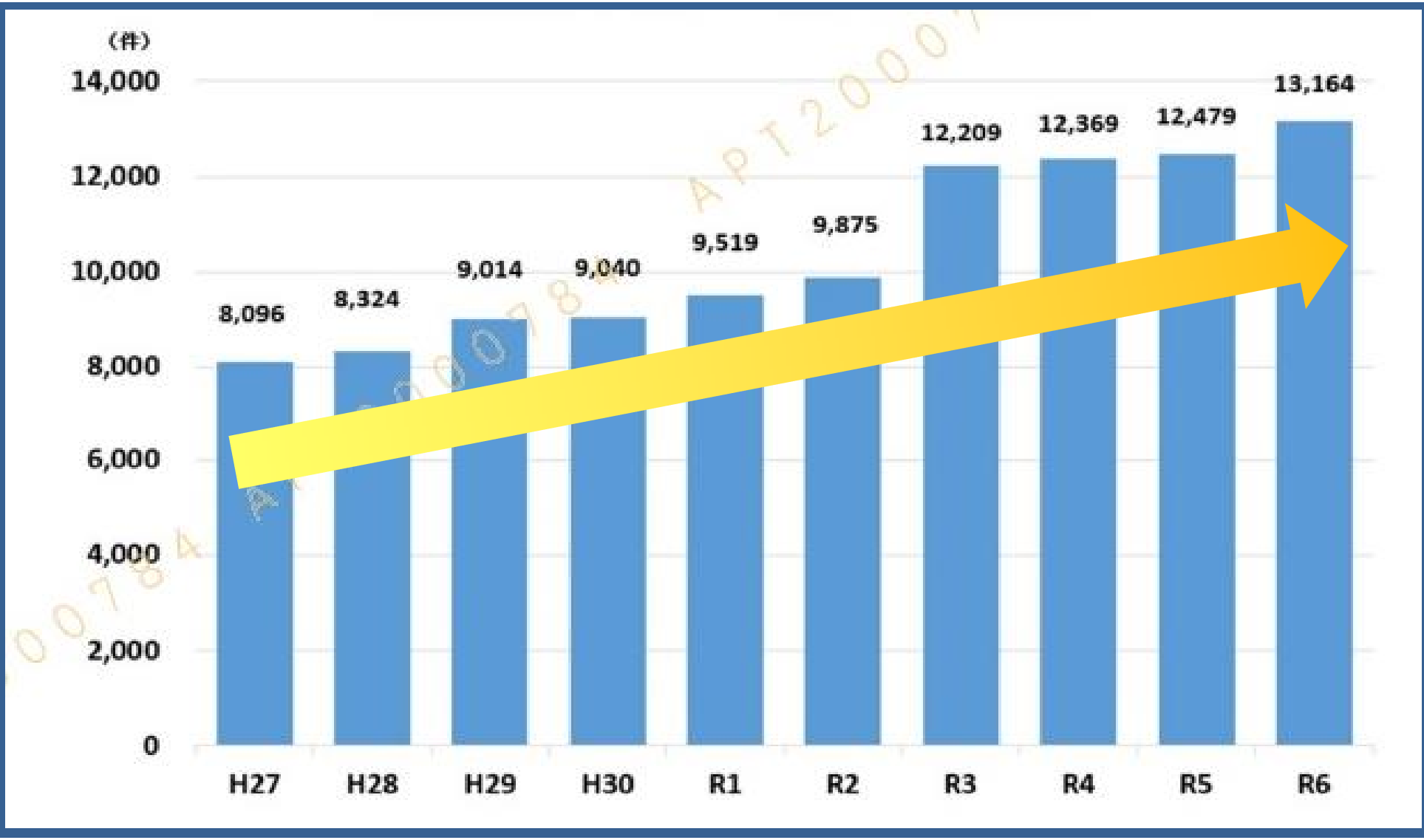
サイバー犯罪とは？

○　不正アクセス、コンピュータウイルスを使った犯罪
○　犯罪の実行にインターネット通信が不可欠な犯罪

例）・　アカウントの乗っ取り
　　⇒不正アクセス
・　パソコンにウイルスを送信し、感染させる
　　⇒ウイルス罪（不正指令電磁的記録に関する罪）
・　ＳＮＳ上で、儲け話でお金をだまし取る
　　⇒詐欺

1　サイバー犯罪の現状

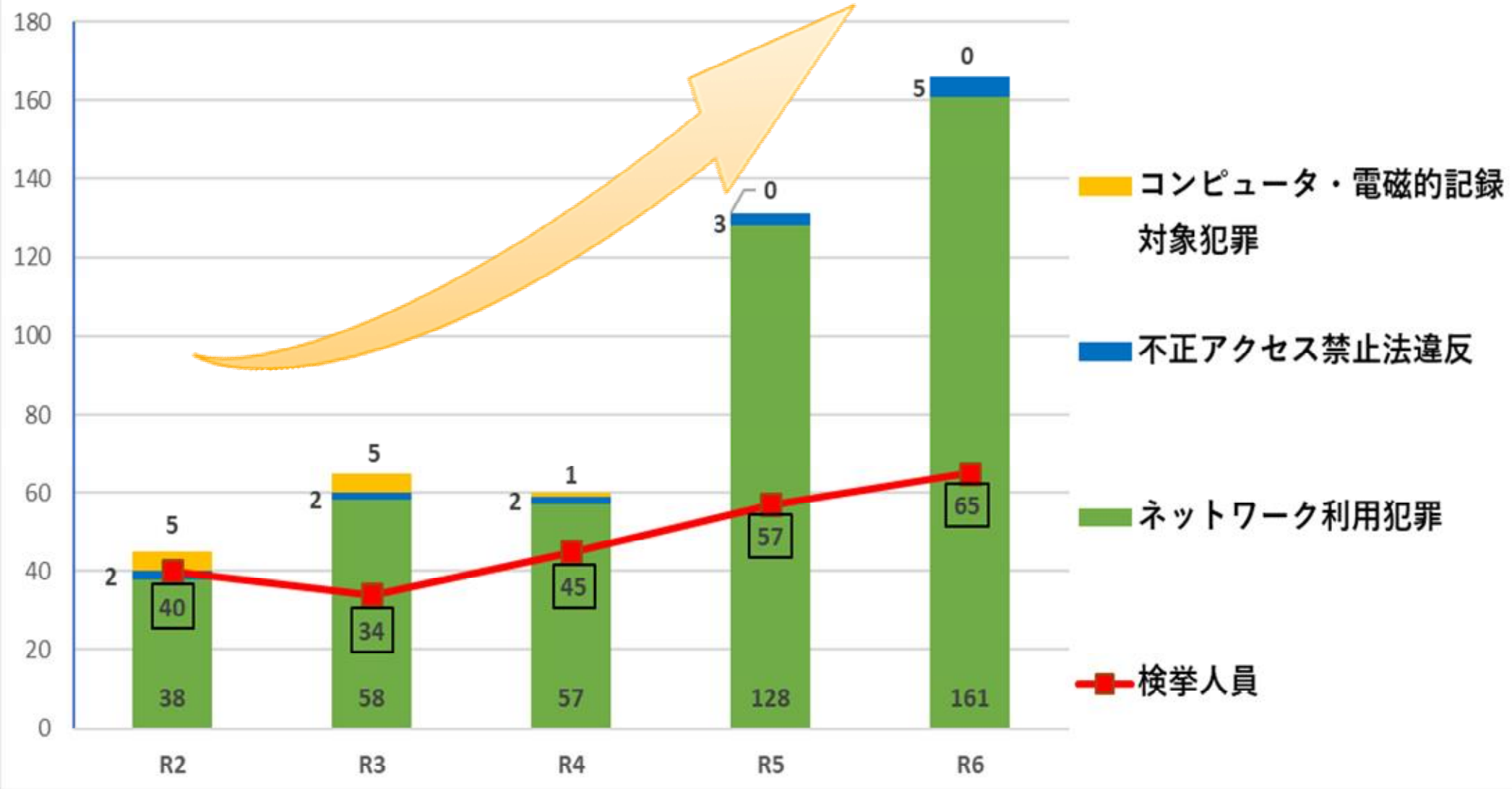
全国のサイバー犯罪検挙状況



※　（出典）警察庁「令和７年上半期における サイバー空間をめぐる脅威の情勢等について 」

1　サイバー犯罪の現状

秋田県内のサイバー犯罪検挙状況は？



1　サイバー犯罪の現状

2　事例から考える最新の手口

3　セキュリティ対策

ケース1

○　令和7年3月、東北地方の企業に対し、**地方銀行を名乗る者から電話**

○　電話で「インターネットバンキングの**ログインIDを更新**する必要がある」と説明され、企業担当者は指示に従い、インターネット上のサイトにアクセス

○　サイトで**インターネットバンキングのID、パスワード、ワンタイムパスワードを入力**した結果、企業の法人口座から預金を不正送金された

ボイスフィッシングの手口による不正送金事犯

ケース1

フィッシングとは…

実在する会社を装って、

ID、パスワード、

クレジットカード番号、

口座の暗証番号といった個人情報

を騙し取ろうとする手口

ケース1

様

[redacted]ダイレクトをご利用いただき、誠にありがとうございます。

口座の資金安全を確保するために[redacted]銀行の口座が一時利用停止されました。

ご利用環境が本人の確認してから、下記のURL を再開手続きの設定してください。

続けるにはこちらをクリック

※普段と異なる環境からのアクセスと判定された場合など、ご本人からのアクセスであることを確認するために本メールをお送りしています。

インターネットバンキングヘルプデスク
0120-[redacted]（フリーダイヤル）
050-[redacted]（通話料有料）

※21：00～9：00の時間帯はご照会のみ承ります。
お手続等は改めてお時間を頂戴する場合がありますのでご了承ください。

※[redacted]ダイレクトのセキュリティ対策について
https://direct.bk[redacted]html

※本メールの送信アドレスは送信専用となっております。
返信メールでのお問い合わせは承りかねますので、あらかじめご了承願います。

株式会社[redacted]銀行

ケース1

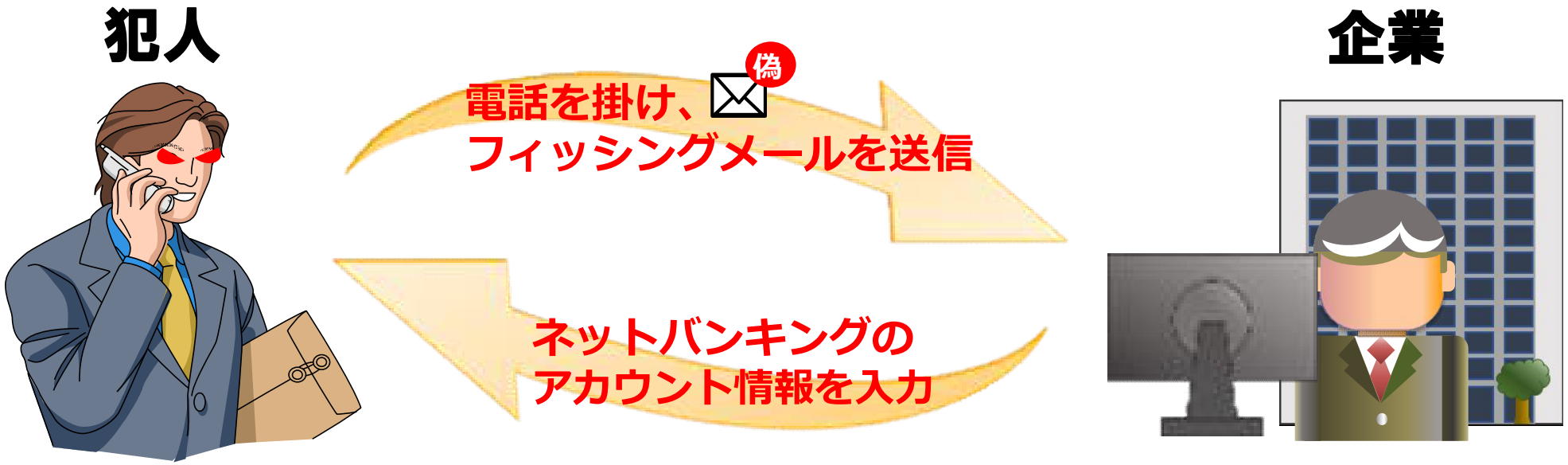

[redacted]銀行
ヘルプ
[redacted]を名乗る偽メール・偽SMSにご注意ください！（4月5日更新）パソコンのウイルス感染を装ったポップアップにご注意ください！（4月6日更新）
くわしくはこちら
店番
半角数字3桁
口座番号
半角数字7桁
または
ご契約番号
半角数字
ログインパスワード
半角英数字・記号 4～16桁
ログイン

ケース1

① 犯人が銀行職員等を騙り、企業へ電話を掛ける（自動音声の場合もある）

② 企業のメールアドレスを聞き出してフィッシングメールを送信

③ フィッシングサイトに誘導し、ネットバンキングのアカウント情報を入力させて、情報を盗み取る



ケース1

ボイスフィッシングによる法人口座の不正送金被害件数・被害額

※　（出典）警察庁「令和７年上半期における サイバー空間をめぐる脅威の情勢等について 」

ケース1

被害に遭わないために

○　見覚えのない電話番号、非通知、国際電話（＋から始まる電話番号）は信用しない

○　銀行等の代表電話番号に電話して事実確認

○　社内で情報共有

少しでも不安があれば、警察に相談を！

ケース2

クリックすることで、ウイルス感染の可能性

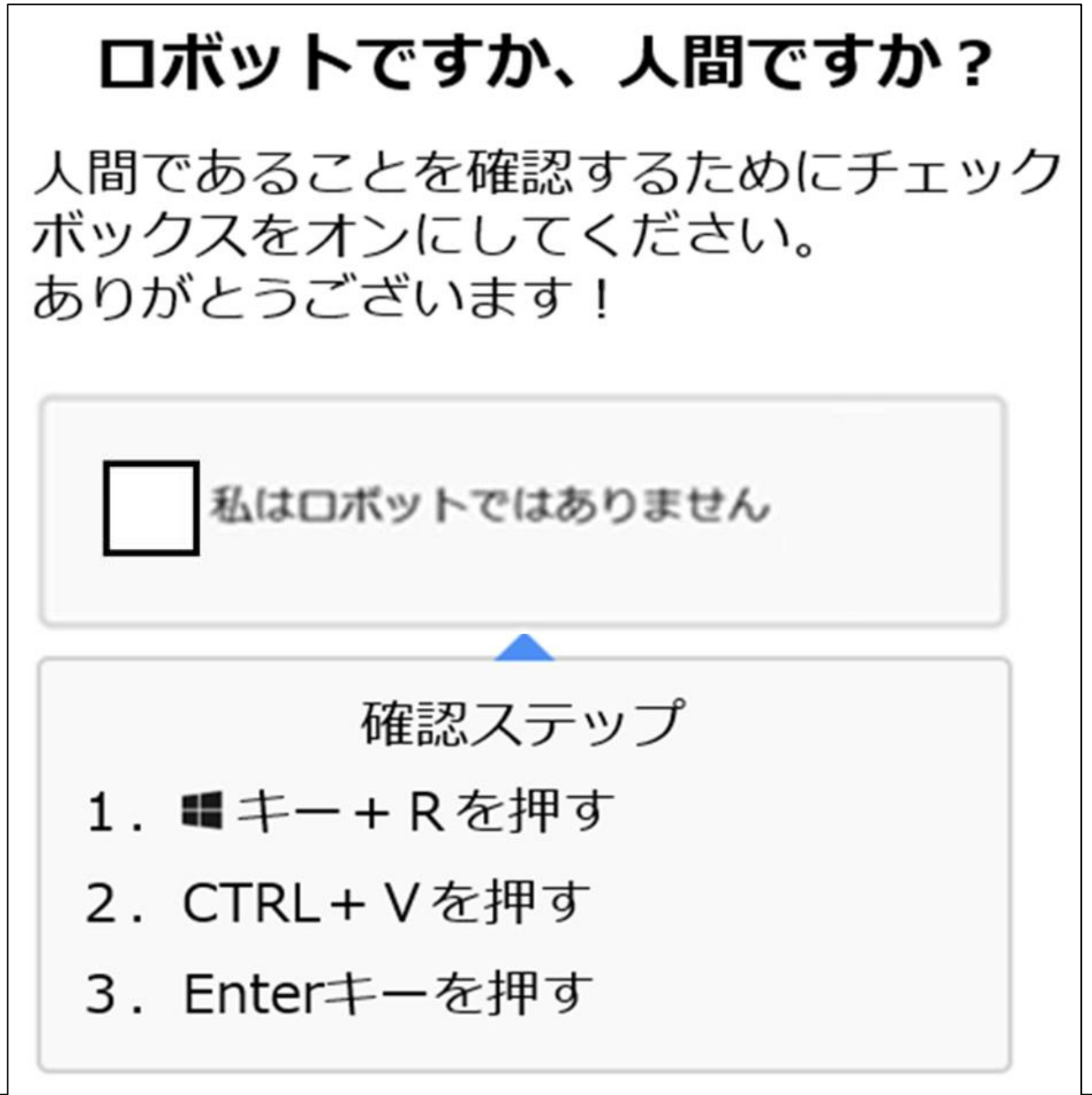
クリックフィックス（Click Fix）攻撃

ケース2

クリックフィックス（Click Fix）攻撃

パソコンの利用者等を誘導し、**利用者自身に不正コマンドを実行させる**サイバー攻撃

ケース2


ロボットですか、人間ですか？
人間であることを確認するためにチェックボックスをオンにしてください。
ありがとうございます！
私はロボットではありません
確認ステップ
1．⊞キー＋Rを押す
2．CTRL＋Vを押す
3．Enterキーを押す

ケース2

①クリックにより不正コマンドをコピー

ロボットですか、人間ですか？

人間であることを確認するためにチェックボックスをオンにしてください。
ありがとうございます！

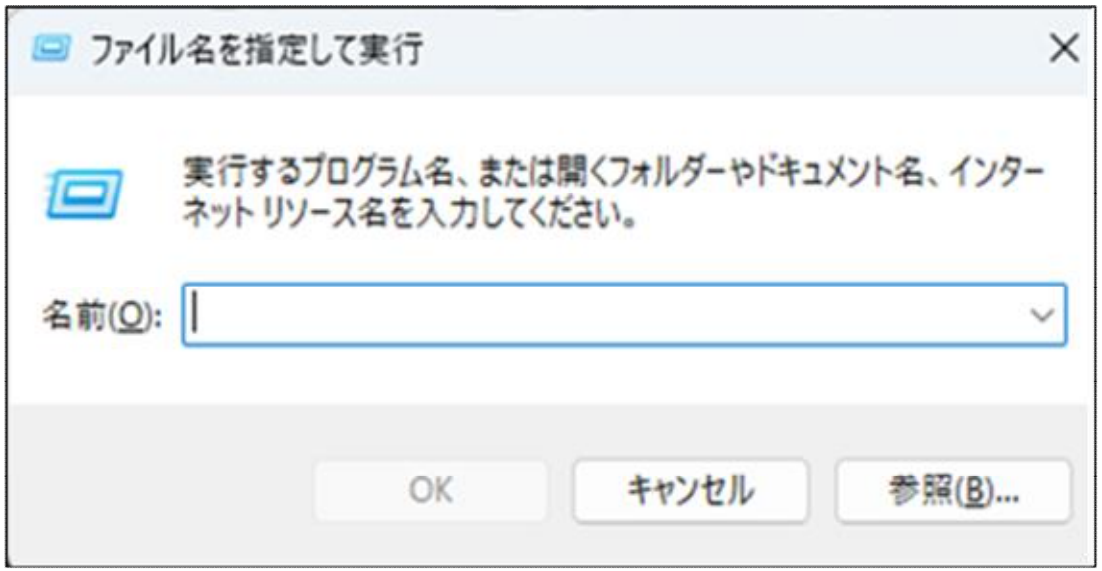
私はロボットではありません

確認ステップ

1．⊞キー＋Rを押す
2．CTRL＋Vを押す
3．Enterキーを押す

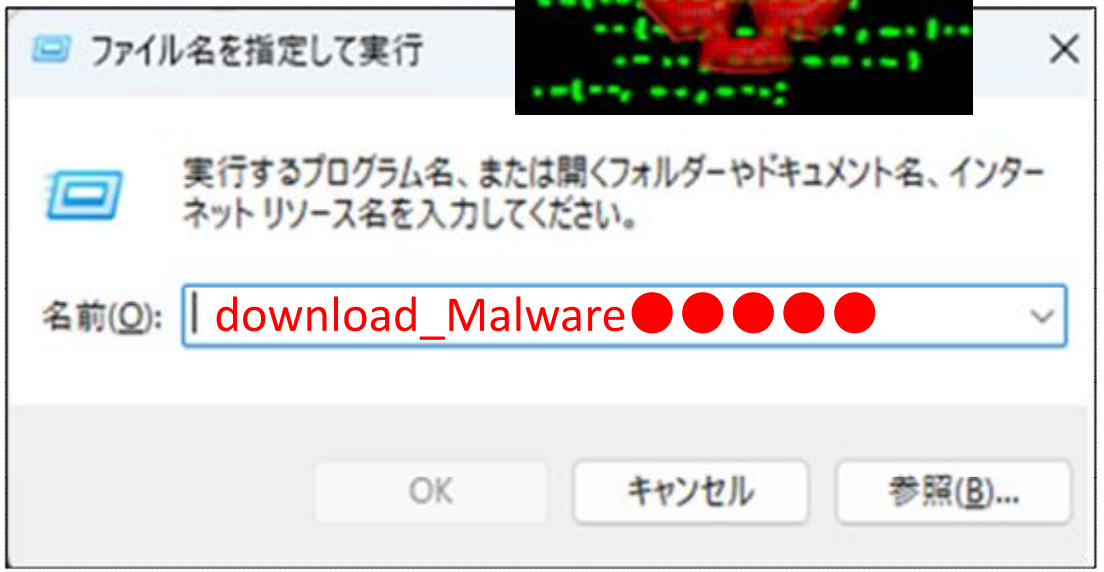
ケース2

② ⊞ ＋ R 「ファイル名を指定して実行」



ケース2

③ Ctrl ＋ V 不正コマンドの「貼り付け」



ケース2

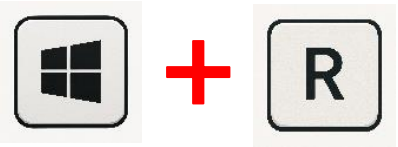
④ Enter 不正コマンドを「実行」

⇒パソコンがウイルス感染

ケース2

被害に遭わないために

○　メールのリンク、サイトの広告などを**安易にクリックしない**

○　認証画面で不審な操作を指示されたら、安易に実行しない（**特に**  **に注意！**）

○　ＯＳ、ウイルス対策ソフトを常に**最新の状態に更新**

○　社内パソコンのプログラムの**実行監視、利用制限**

ケース3

○　令和7年2月、保険大手企業がサイバー攻撃を受け、データサーバの一部のファイルが暗号化され、約510万件を超える個人情報が漏えいしたおそれがあることを発表

○　令和7年4月、国際総合物流企業がランサムウェアによるサイバー攻撃を受け、業務システムに障害が発生したと発表

○　令和7年9月には大手飲料メーカー、10月にはオフィス用品通販大手企業が相次いで被害

ランサムウェア・ノーウェアランサム

ランサムウェアとは…

金銭を脅し取ることを目的とした不正プログラム

感染すると…

- ○　パソコン内のファイルが暗号化されてファイルを開けなくなる
- ○　暗号化の解除と引換えに、高額な「身代金」を要求される
- ○　近年では、パソコン内の機密データを窃取し、公開を防ぐため更に身代金を要求する「二重脅迫」が主流

ケース3

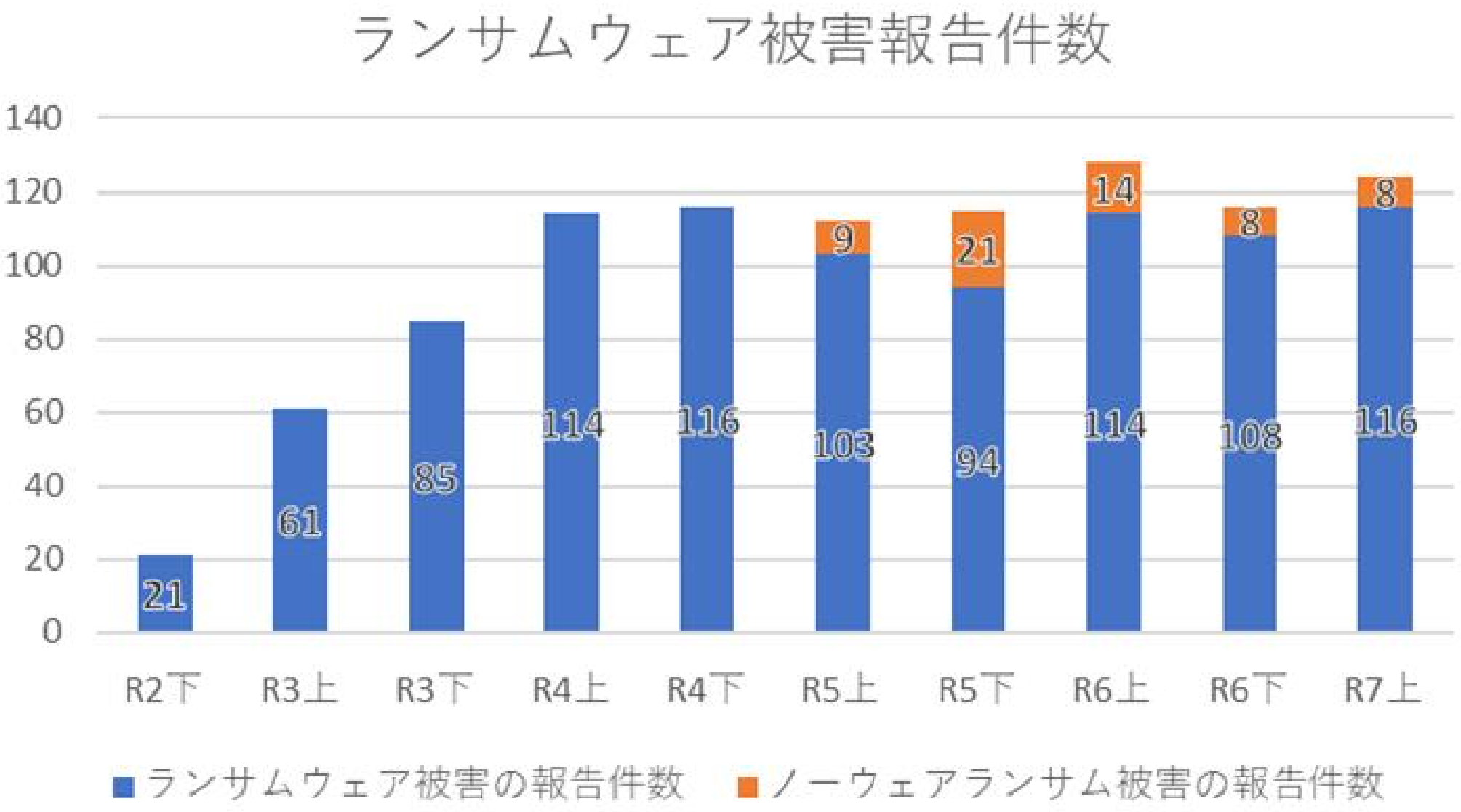
ノーウェアランサムとは…

機密情報を盗み取り、機密情報の公開を脅迫材料として金銭を要求するサイバー攻撃

ランサムウェアとの違い

- ○　データの暗号化を行わず、機密情報を盗み取り金銭を脅し取る攻撃
- ○　暗号化プロセスが不要なため迅速に攻撃可能
- ○　データを暗号化しないために検知が遅れ、短時間で大量の機密情報を窃取される可能性

ケース3

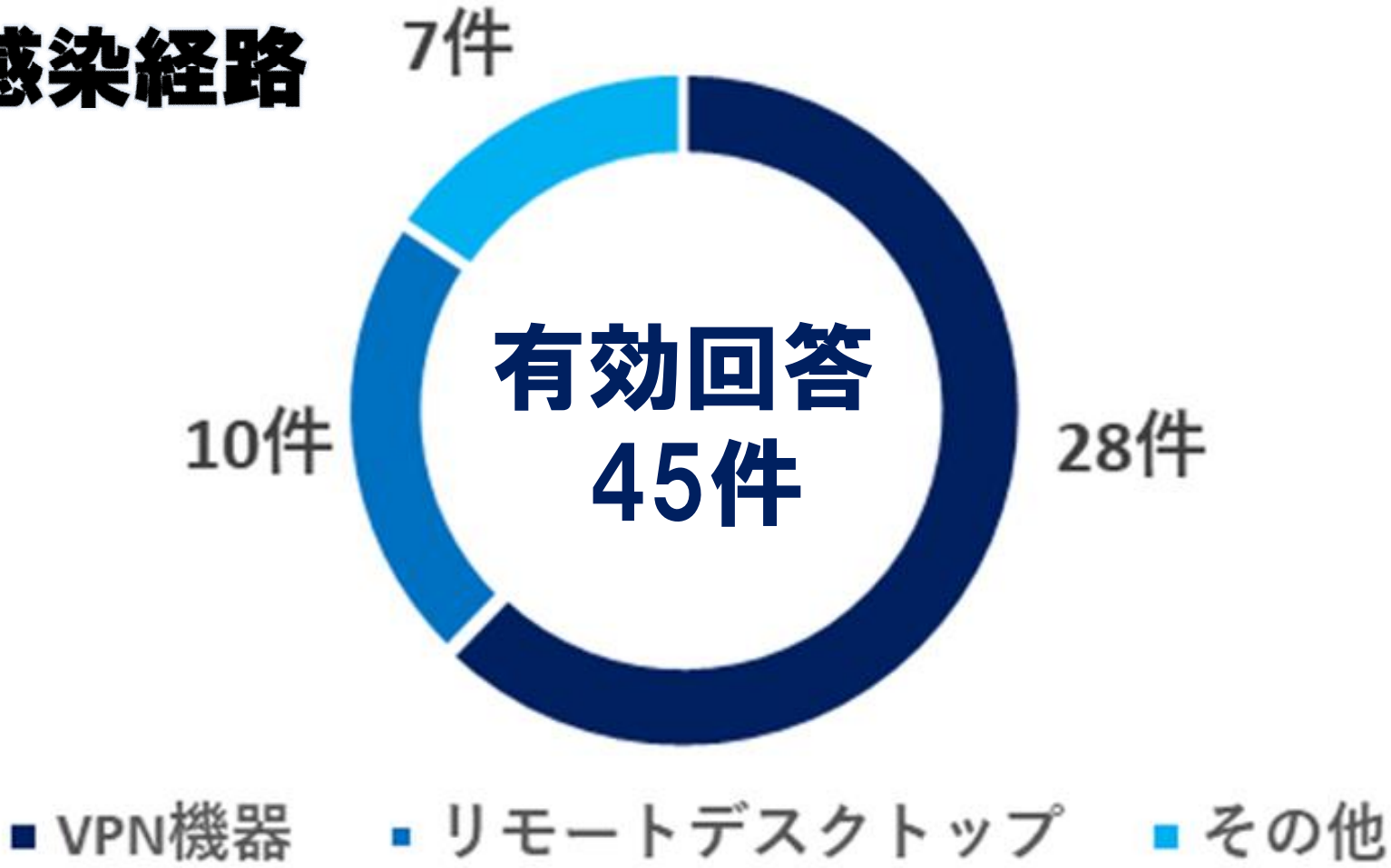


※　（出典）警察庁「令和７年上半期における サイバー空間をめぐる脅威の情勢等について 」

ケース3

ランサムウェア被害にあった企業・団体等へのアンケート調査

主な感染経路



※　（出典）警察庁「令和７年上半期における サイバー空間をめぐる脅威の情勢等について 」

ケース3

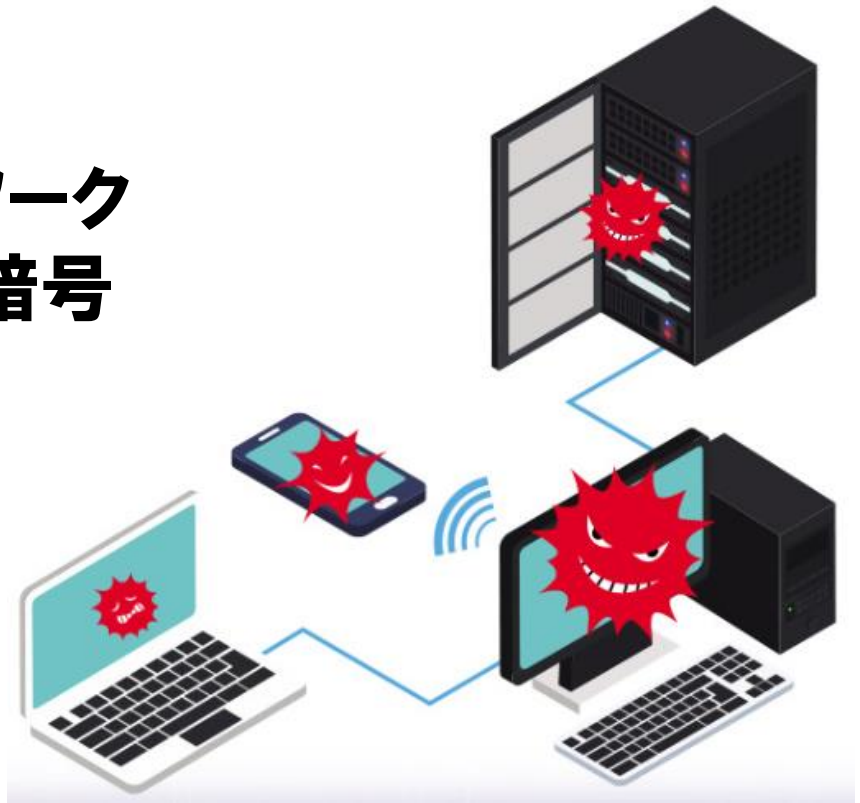
ランサムウェアの感染経路は、
ＶＰＮ機器
リモートデスクトップ用機器
からの侵入が全体の８割を占める

感染の原因は…
○安易なID・パスワード設定
（初期設定のままにしている等）
○アカウントが適切に管理されず、
不必要なアカウントを放置

ケース3

ランサムウェアに感染してしまうと、感染した端末だけではなく、その端末に接続しているハードディスクやUSBメモリー等に保存しているファイルも暗号化されてしまいます。

　また、社内LANなどのネットワーク上で共有しているファイル等も暗号化されるおそれがあります。



ケース3

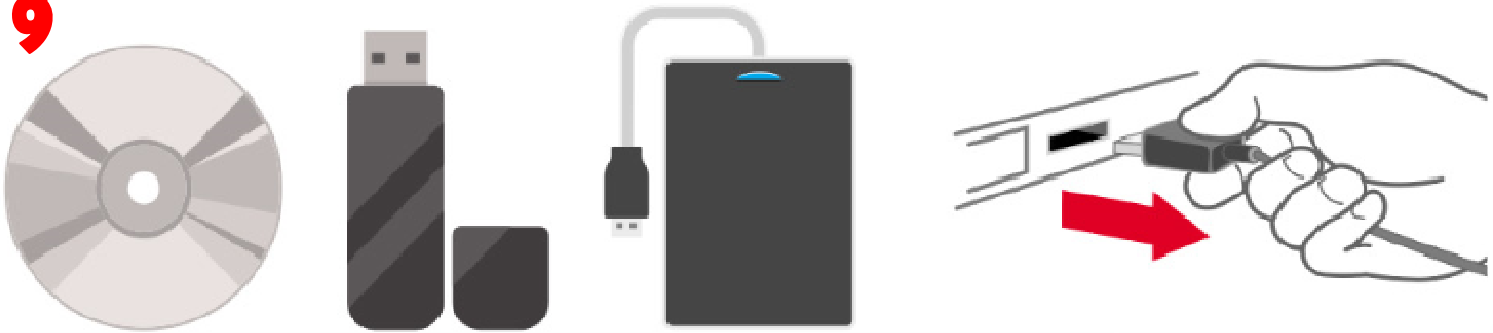
被害に遭わないために

○　不審なメールは**開かない**

○　セキュリティ対策ソフトを導入

○　ＯＳや各種ソフトウェア、セキュリティ対策ソフトを**アップデート**

○　バックアップを取った媒体は**ネットワークから切り離す**



1　サイバー犯罪の現状

2　事例から考える最新の手口

3　セキュリティ対策

秋田県警による広報啓発活動

○　サイバーセキュリティ講話、各種イベントにおける広報啓発活動

○　SNS等を活用した情報発信

○　秋田県サイバー防犯連絡協議会、秋田県サイバーテロ対策協議会による広報啓発

組織で対応してもらいたいこと

- 組織全体の**セキュリティ意識の醸成**
- 使用機器は**最新のバージョンにアップデート**
- ログの保存や定期的な確認などサイバー攻撃を**検出するための仕組み**の導入
- バックアップを取り、バックアップは**ネットワークから切り離す**
- 事案発生時の**警察への通報**

各職員ができること

- **不審なメールやウェブサイトは開かない。**
- **パスワードは適切に設定・管理する。**
- **安易にソフトウェアをインストールしない。**
  有益なフリーソフトと偽って、不正なプログラムやマルウェアをダウンロードさせる手口もある。
- サイバーセキュリティに関する**リテラシーを高める。**

ご清聴ありがとうございました

CyberSecurity for All

＃誰も取り残さないサイバーセキュリティ