サイバーセキュリティセミナー

サイバー空間をめぐる脅威の情勢と今後の対策

令和３年２月２５日
宮城県警察本部
サイバー犯罪対策課

サイバー空間をめぐる脅威の情勢等について

新型コロナウイルス感染症に関連したサイバー攻撃が発生

- 国内外で医療機関や研究機関等に対する攻撃を確認

新型コロナウイルス感染症に関連したサイバー犯罪が発生

- マスク販売を装った詐欺サイトや不審メール等を確認

国内外において、政府や企業等に対するサイバー攻撃が発生

- 防衛関連企業や電気通信事業者に対する不正アクセスが発生

インターネットバンキングに係る不正送金事犯の被害が急増

- 令和2年上半期の被害が、前年同期と比べて大幅に増加

キャッシュレス決済を悪用した犯罪が発生

- ドコモ口座を悪用した事件が発生

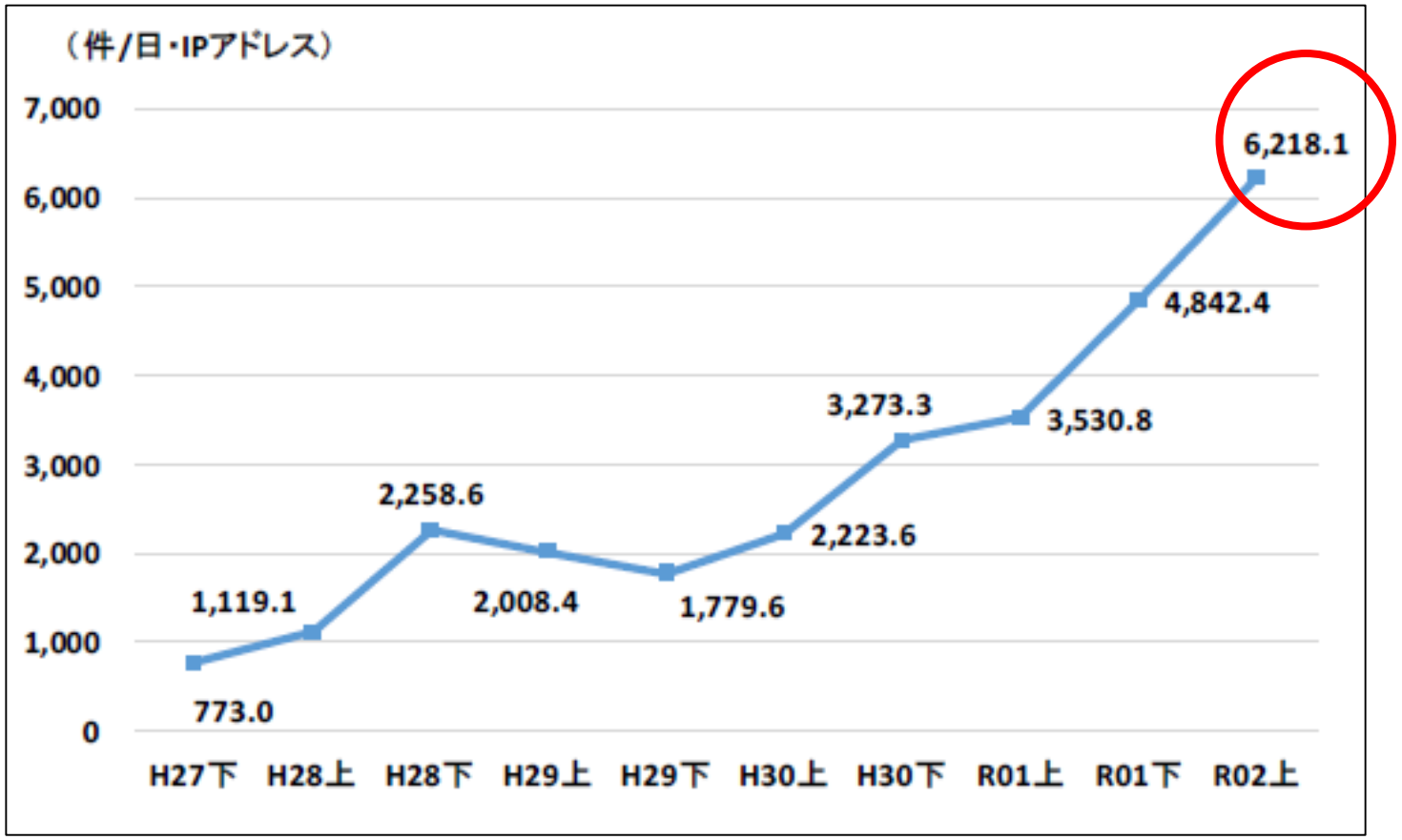
サイバー空間の現状

～令和2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～

- サイバー攻撃の情勢等
- サイバー犯罪の情勢等

新型コロナウイルス感染症絡みの
サイバー犯罪が発生

サイバー攻撃の情勢等（全国）



センサーにおいて検知したアクセス件数の推移

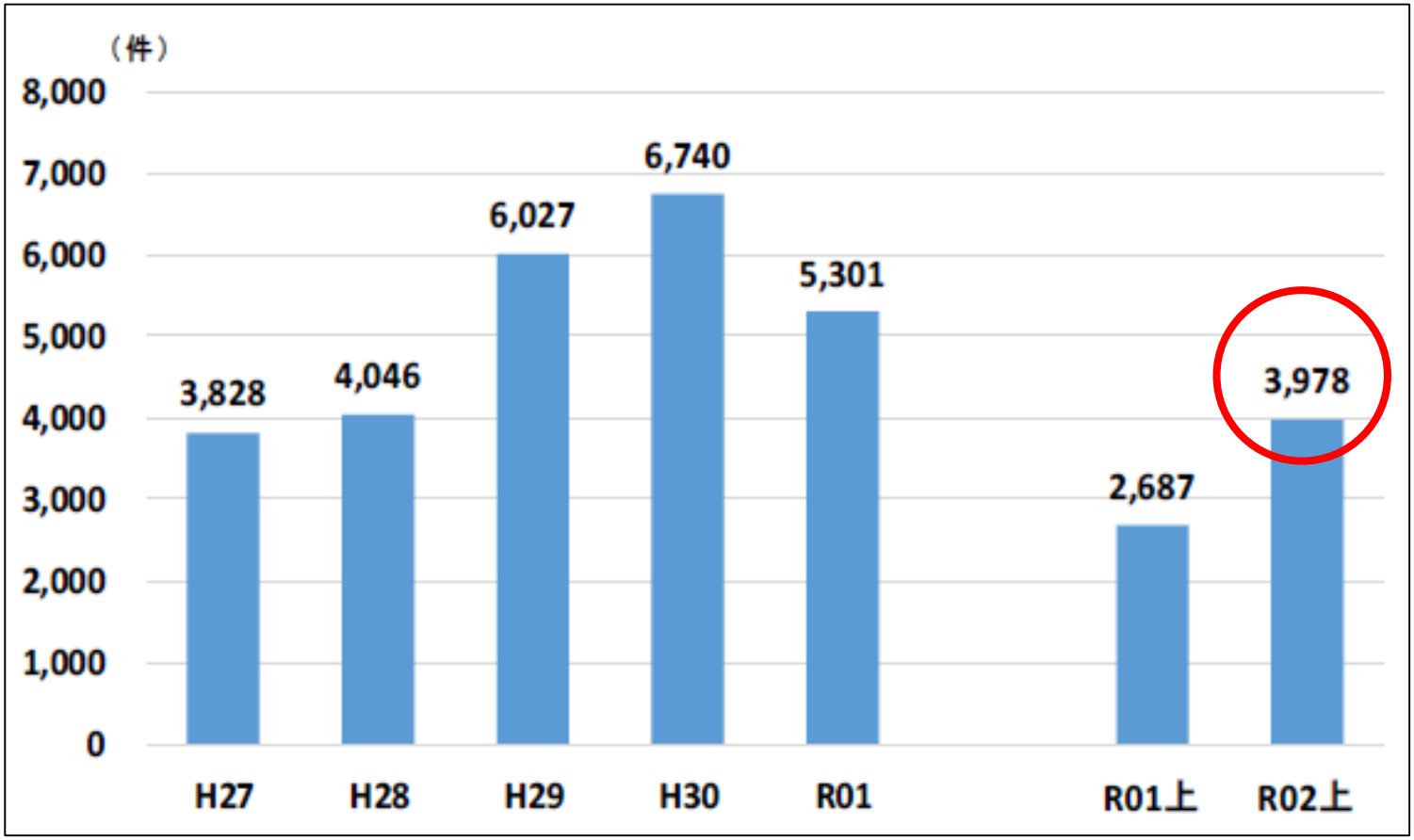
サイバー空間における探索行為等

○　センサーにおいて検知したアクセスの概況

センサーにおいて検知したアクセス件数は、１日・1IPアドレス当たり6，218．１件と増加傾向にある。

※出典元：　警察庁　“令和2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”

サイバー攻撃の情勢等（全国）



標的型メール攻撃の件数の推移

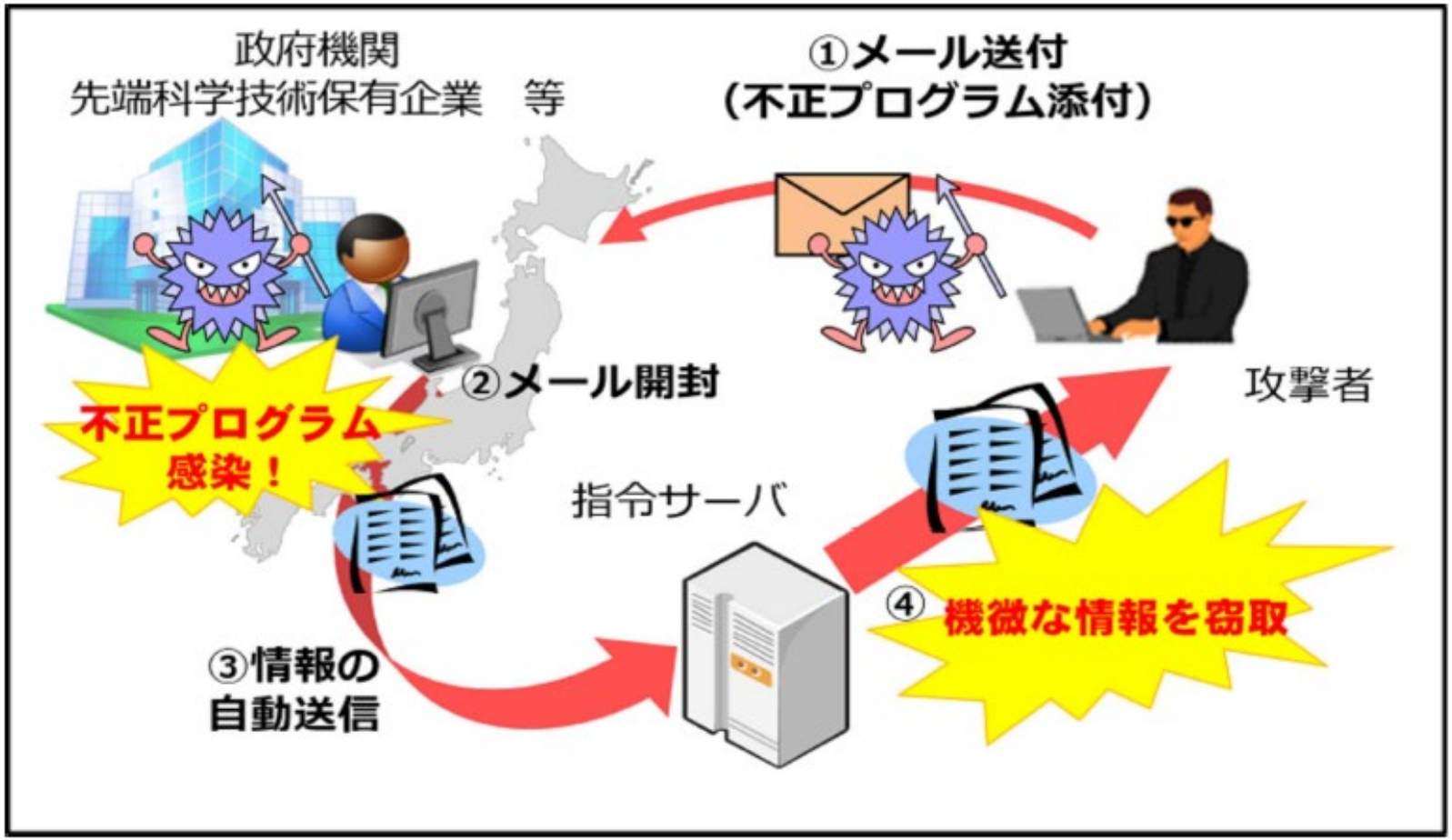
標的型メール攻撃の件数の推移

警察では、情報窃取を企図したとみられるサイバー攻撃に関する情報を、サイバーインテリジェンス情報共有ネットワークにより事業者等と共有し、集約された情報を総合的に分析し、事業者等に対し、分析結果に基づく情報提供を実施している。

本年上半期の同ネットワークを通じて把握した標的型メール攻撃の件数は、３，９７８件と前年同期と比べて増加した。

※出典元：　警察庁　“令和2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”

標的型メール攻撃の概要



標的型メール攻撃とは

　警察庁では、市販のウイルス対策ソフトでは検知できない不正プログラムを添付して、業務に関連した正当なものであるかのように装った電子メールを送信し、これを受信したコンピュータを不正プログラムに感染させるなどして、情報の窃取を図るものを「標的型メール攻撃」としている。同じ文面や不正プログラムが10か所以上に送付されていた標的型メール攻撃を「ばらまき型」と呼んでいる。

標的型メール攻撃による被害事例

2016年　JTBに対する標的型メール攻撃

大手旅行会社JTBに勤務する従業員が、取引先を偽装したメールを開封したことがきっかけで、不正プログラムに感染した事案。

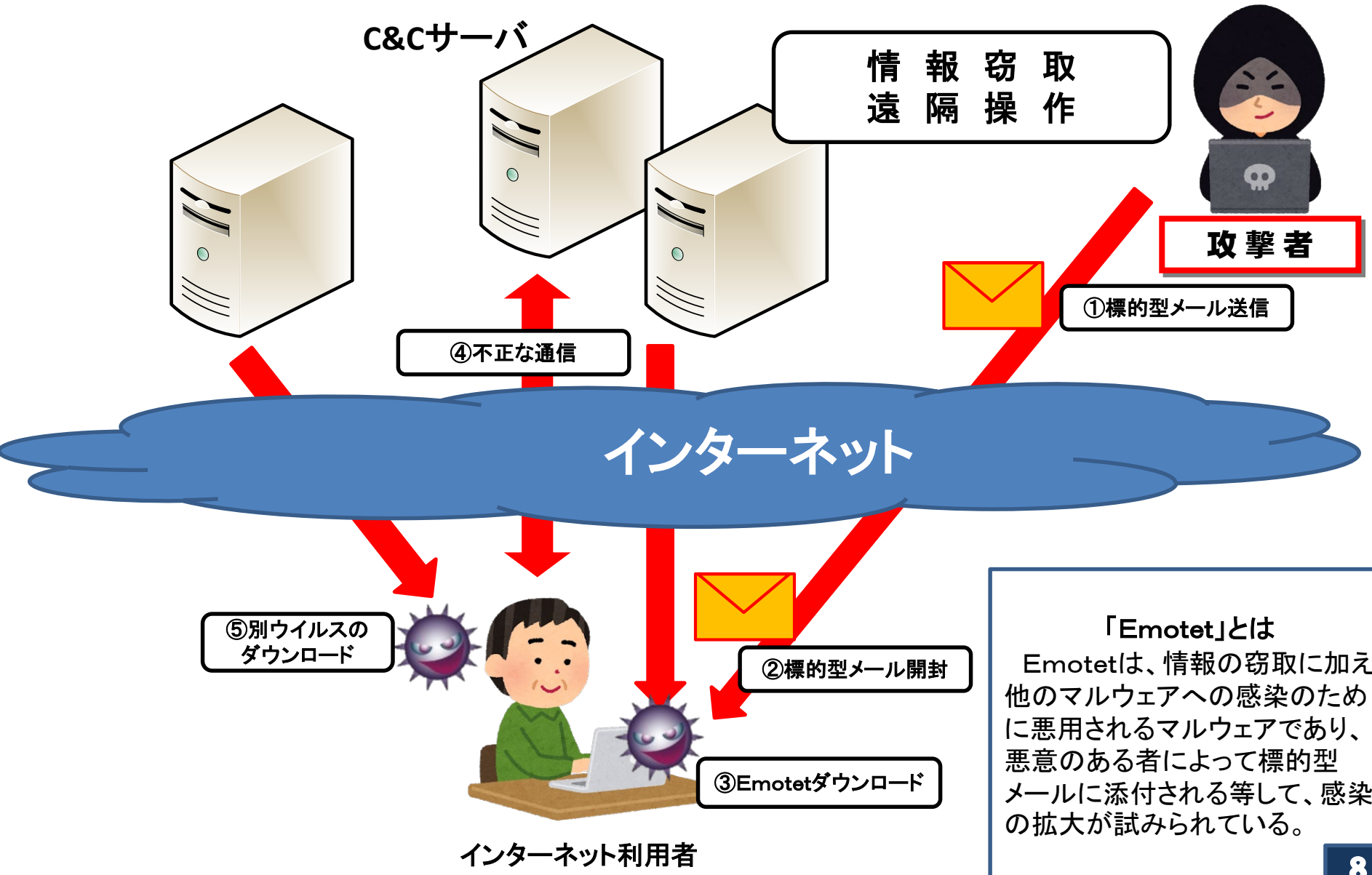
被害規模はすさまじく、同社のデータベースに登録されていた顧客情報793万人分のデータが流出。

2015年　日本年金機構に対する標的型メール攻撃

日本年金機構九州ブロックに勤務する職員が、仕事の内容を偽った標的型メールを開封し、不正プログラムに感染した事案。外部のネットに接続したPCを使って個人情報を管理していたため、年金情報が流出。

公的機関では最大規模となる、125万件の情報漏えい事件に発展。

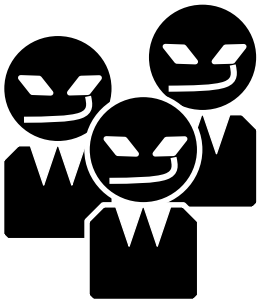
マルウェア「Emotet」が活発化



「Emotet」とは

Emotetは、情報の窃取に加え、他のマルウェアへの感染のために悪用されるマルウェアであり、悪意のある者によって標的型メールに添付される等して、感染の拡大が試みられている。

標的型メール攻撃による被害事例（令和元年11月発生）



犯人グループ

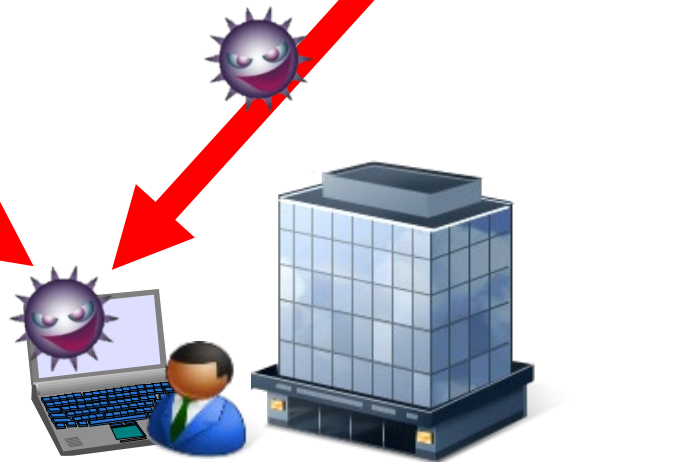
標的型メールの解析結果
取引先を偽装したメール。
発信元は、パキスタン。
Wordファイルをクリックするとマルウェア「Emotet」をダウンロードする。

標的型メール

Word
ファイル

①取引先を装った
メールを送信

外部サーバ

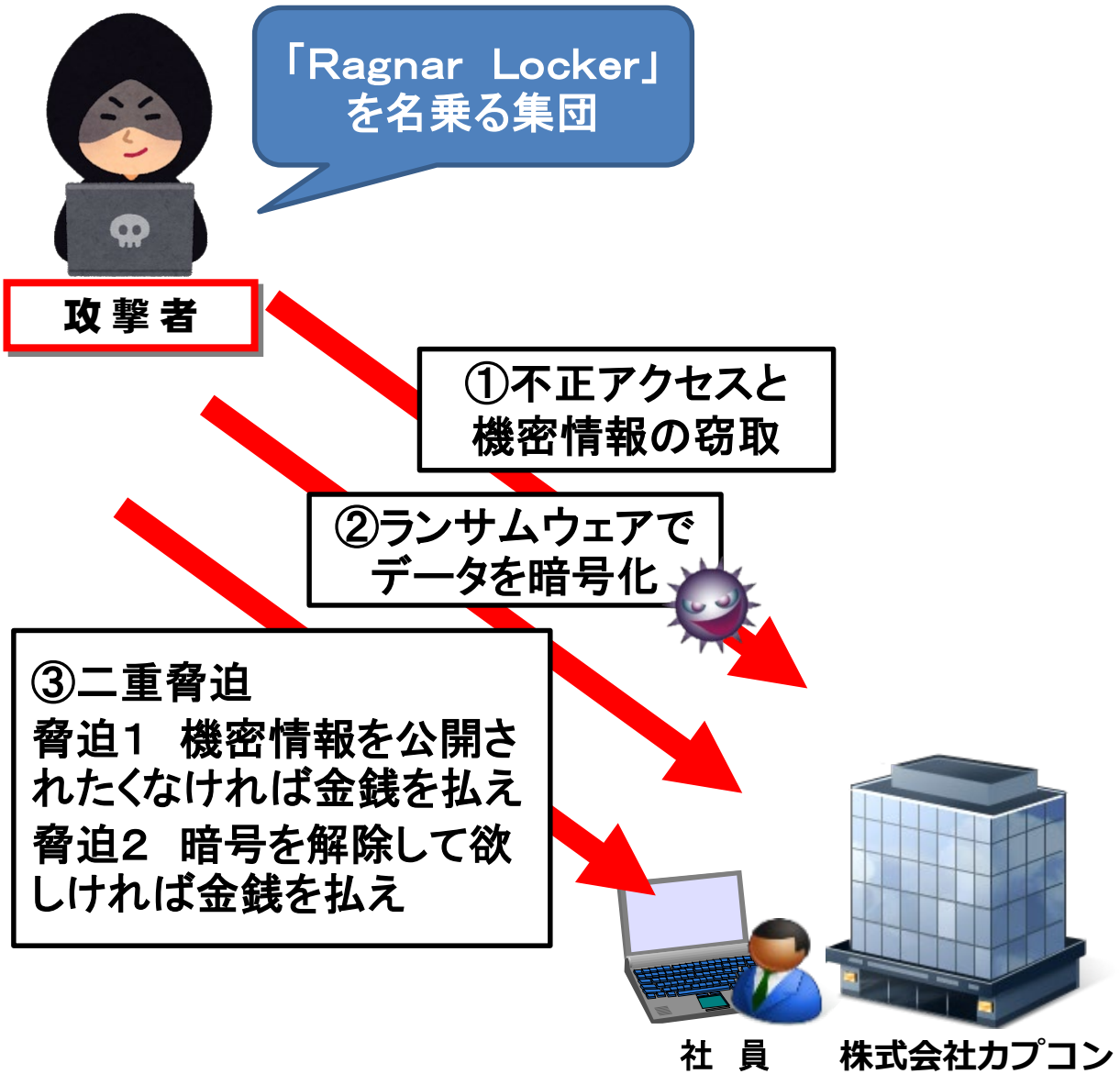


A社　社員　　A社（仙台市）

②Ｗｏｒｄファイルをクリック
③外部サーバからウイルスをダウンロード

「Emotet」の影響
○端末やブラウザに保存されたパスワード等の認証情報が窃取される。
○窃取されたパスワードを悪用されSMBによりネットワーク内に感染が広がる。
○メールアカウントとパスワードが窃取される。
○メール本文とアドレス帳の情報が窃取される。
○窃取されたメールアカウントや本文などが悪用され、Emotetの感染を広げるメールが送信される。

カプコンに対するサイバー攻撃（令和2年11月発覚）



事案の概要

株式会社カプコンは、サイバー犯罪集団によって、社内システムに不正アクセスされ、機密情報を盗み取られるとともに、機密情報を公開しないことと引換えに金銭を要求されたことを公表した。

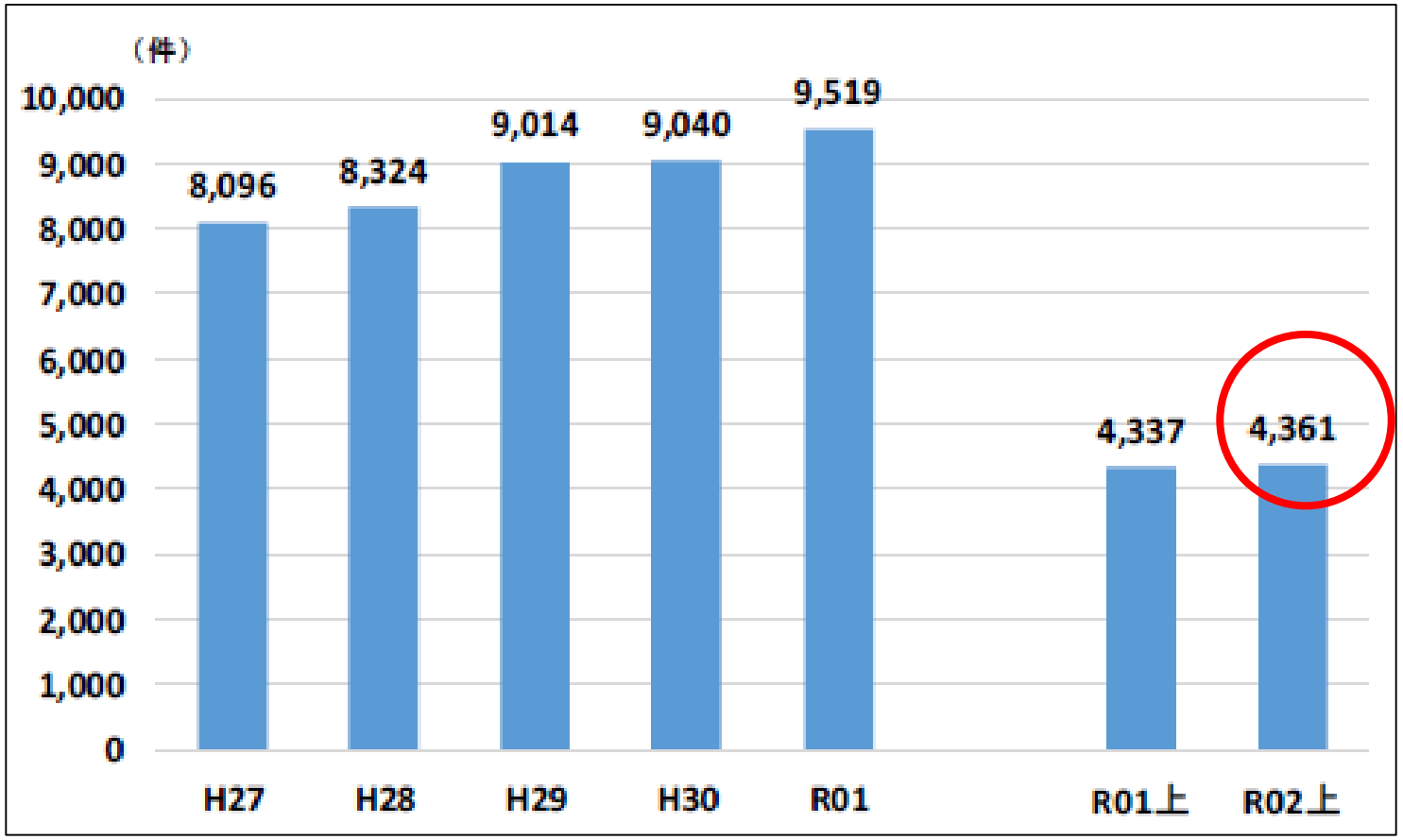
更に、同社はランサムウェアを用いたサイバー攻撃も受け、データを暗号化されるとともに、暗号化の解除と引換えに金銭を要求されたことを公表した。

最大約39万件の個人情報（顧客、取引先等）の流出の可能性があることも公表した。

発覚と対応の経緯（11/16）

〇11/2　サイバー攻撃を確認
〇11/2　大阪府警に通報
〇11/4　システム障害を公表
〇11/12　個人情報の流出を確認
〇個人情報保護委員会等に報告
〇対応窓口の開設等

サイバー犯罪の情勢等（全国）



サイバー犯罪の検挙件数の推移

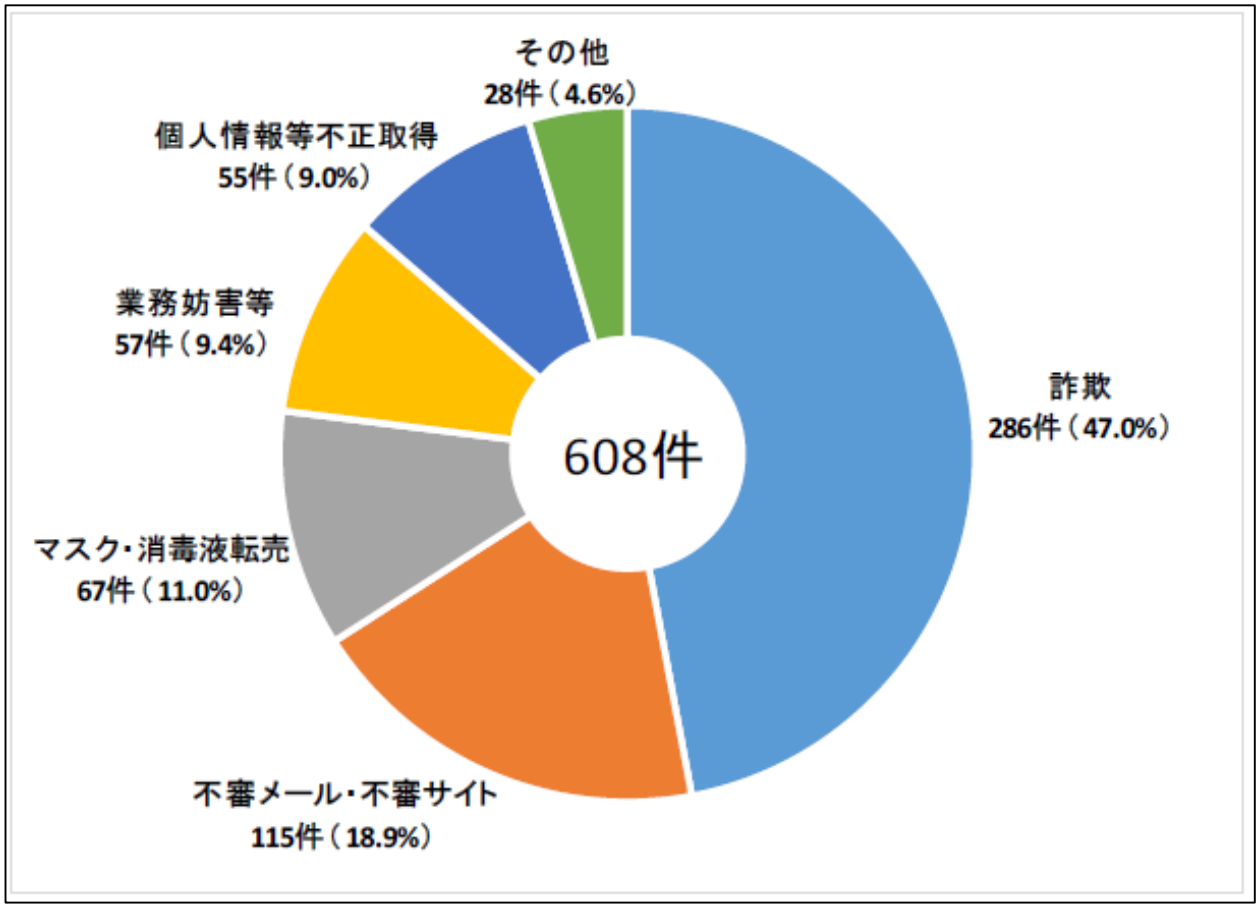
サイバー犯罪の情勢等

○　サイバー犯罪の検挙状況

　サイバー犯罪の検挙件数は増加傾向にあり、本年上半期の検挙件数は、4,361件と、前年同期と同水準となった。

※出典元：　警察庁　“令和2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”

サイバー犯罪の情勢等（全国）



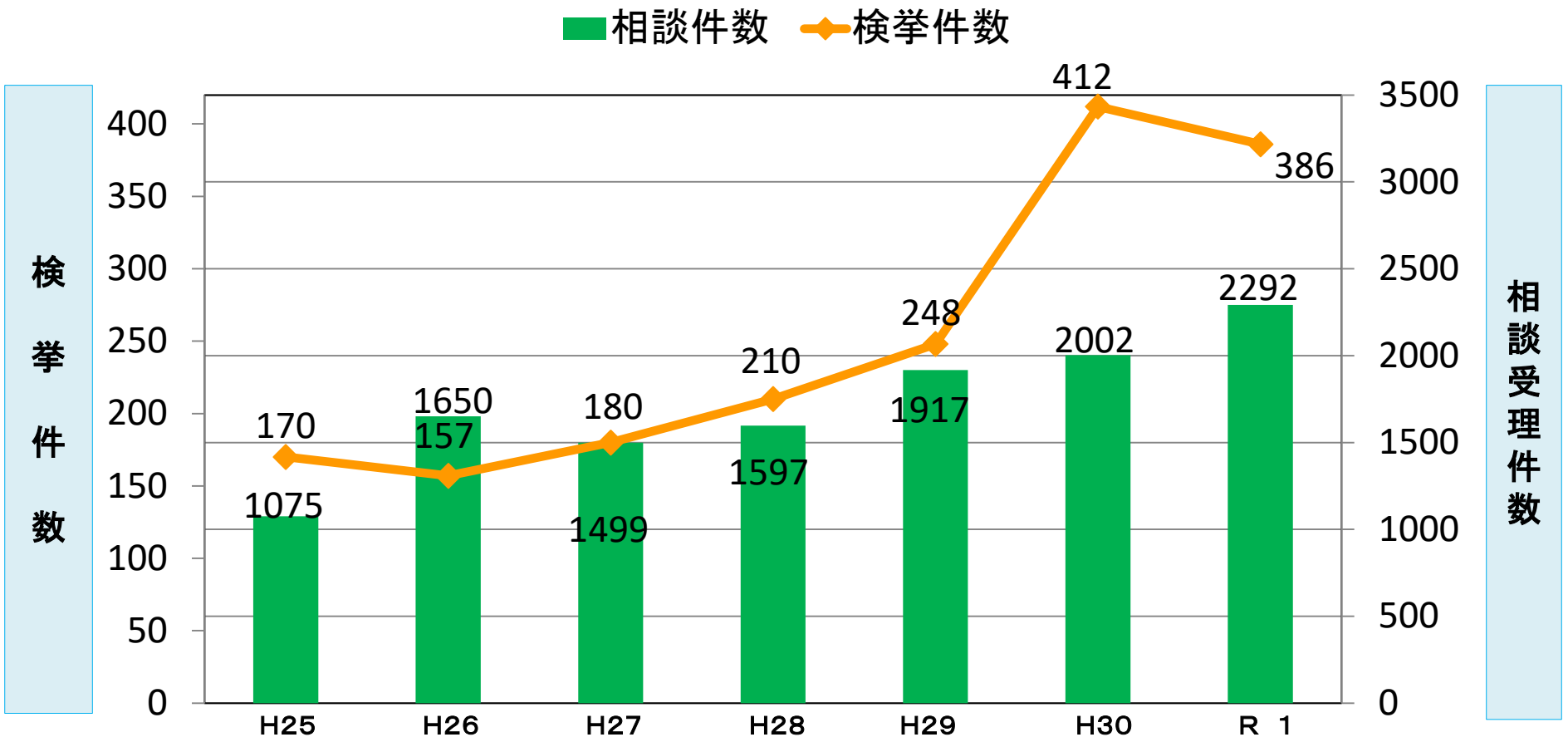
新型コロナウイルス感染症に関連するサイバー犯罪が疑われる事案の報告件数

〇サイバー犯罪が疑われる事案の発生状況

新型コロナウイルス感染症に関連するサイバー犯罪が疑われる事案として、６月末までに都道府県警察から警察庁に報告のあった件数は608件であった。その内訳としては、詐欺が286件で全体の約47.0%と最も多く、次いで不審メール・不審サイトが115件で全体の約18.9%を占めている。

※出典元：　警察庁　“令和2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”

サイバー犯罪の検挙及び相談受理状況（宮城県）



4月　サイバーセキュリティ統括官の新設
サイバー犯罪対策課の新設

検挙386件（前年比－26件）
相談2292件（前年比＋290件）

新型コロナウイルス感染症に関連するサイバー犯罪の発生
マスク販売を装った詐欺サイト被害の発生（宮城）

犯　人

①詐欺サイトの開設

犯人の手口

1　HPアドレス
　www.vobiksale.●●

2　開設場所
　アメリカ合衆国

3　運営会社
　実在する企業名を掲載

4　振込先
　ネット銀行

マスク販売を装った詐欺サイト
（令和2年3月）

②購入申込み
③代金振込

被害者

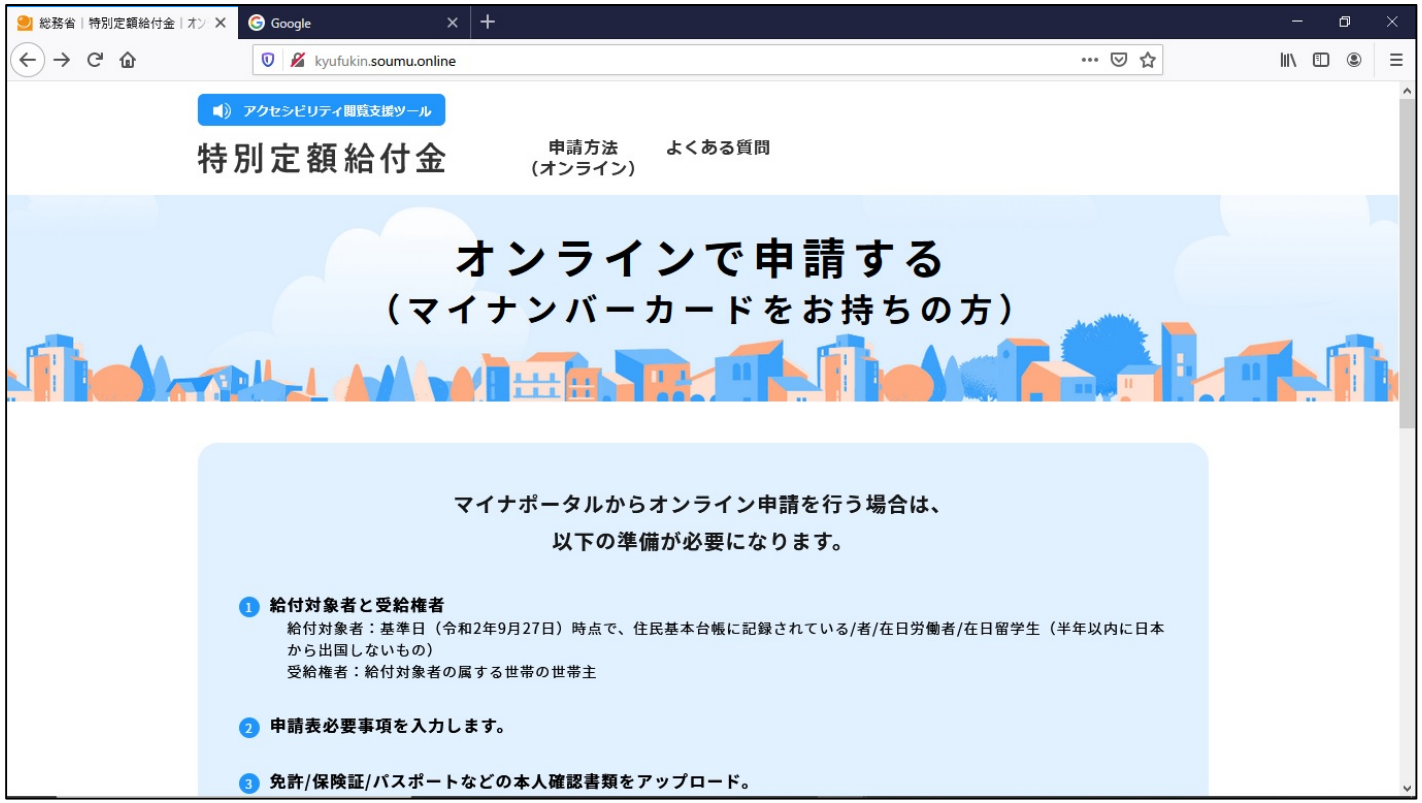
新型コロナウイルス感染症に関連するサイバー犯罪の発生
特別定額給付金の偽サイトが出現

犯　人

総務省を
騙った
誘導メール

被害者

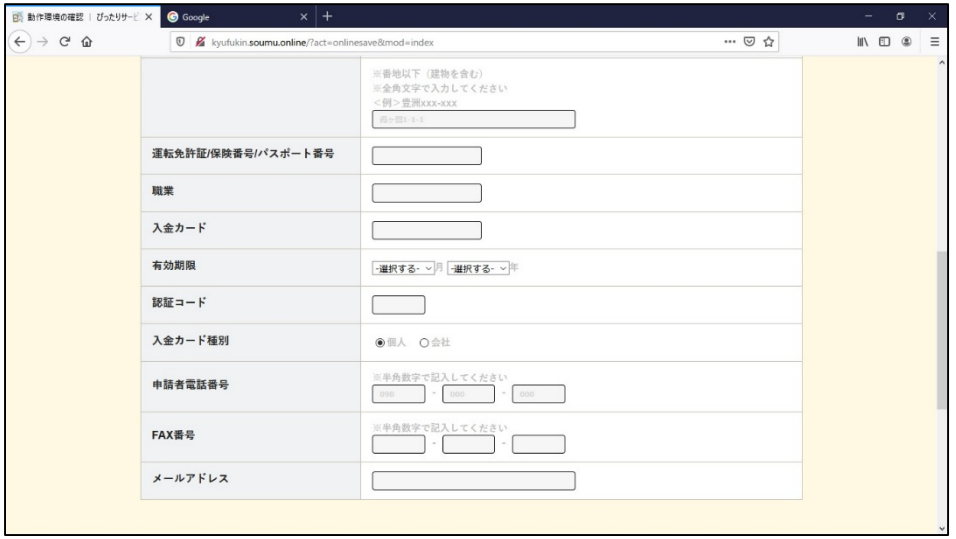
正規サイト　kyufukin.soumu.go.jp
偽サイト　　kyufukin.soumu.online



特別定額給付金の偽サイト（令和2年10月）

新型コロナウイルス感染症に関連するサイバー犯罪の発生
特別定額給付金の偽サイトが出現

① 住所、氏名等の個人情報を入力させ窃取



② 暗証番号を入力させ窃取

特別定額給付金の偽サイトの特徴

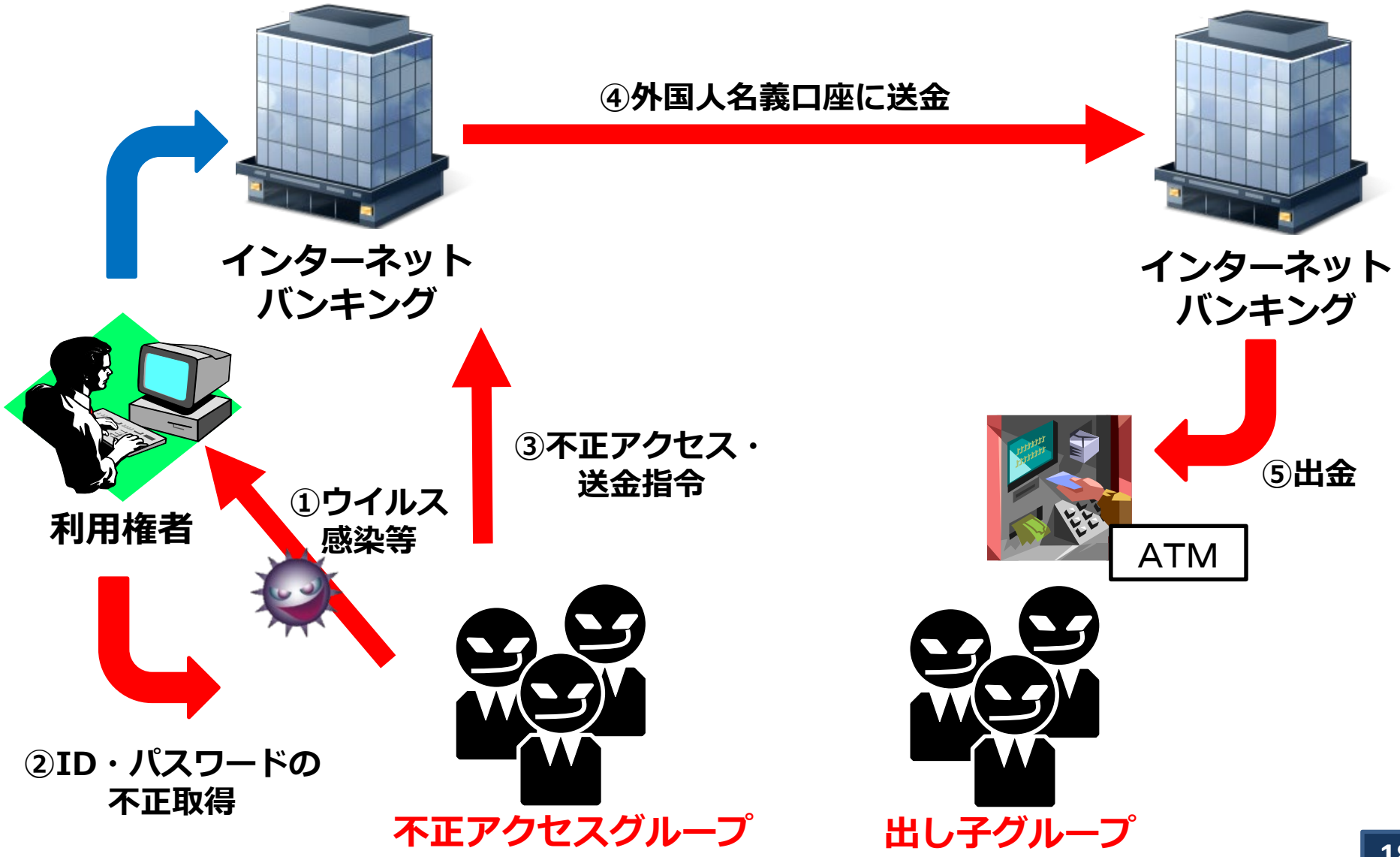
① 住所、氏名等の個人情報を入力させ窃取
② 暗証番号を入力させ窃取
③ 通帳やキャッシュカード等の口座情報を送信させ窃取

③ 通帳やキャッシュカード等の口座情報を送信させ窃取

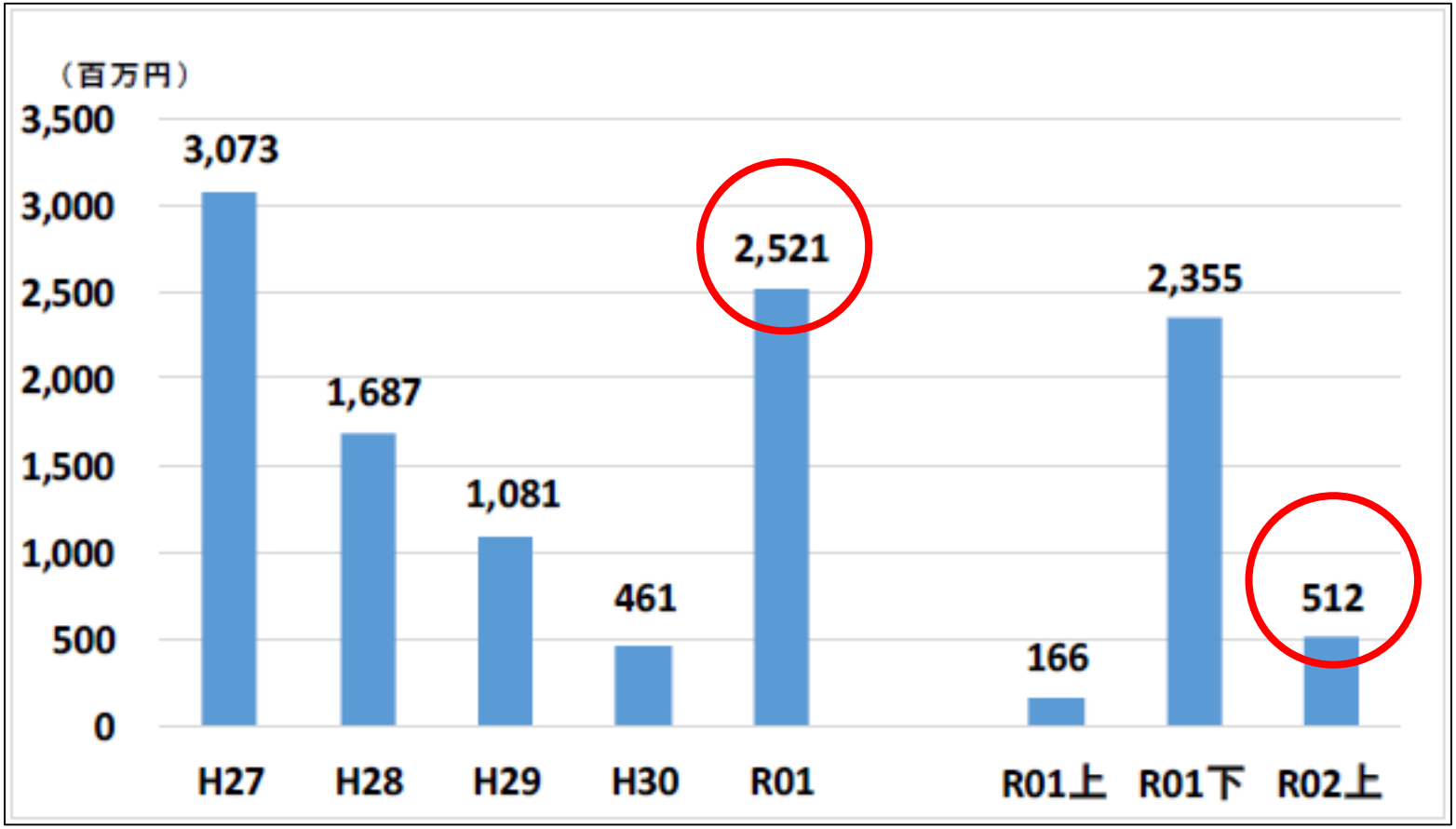
最近の懸案事案と被害防止対策

- インターネットバンキングに係る不正送金事犯
- キャッシュレス決済の不正利用
- 偽サイト・詐欺サイト

インターネットバンキングに係る不正送金事犯



～ 最 近 の 懸 案 事 案 ～



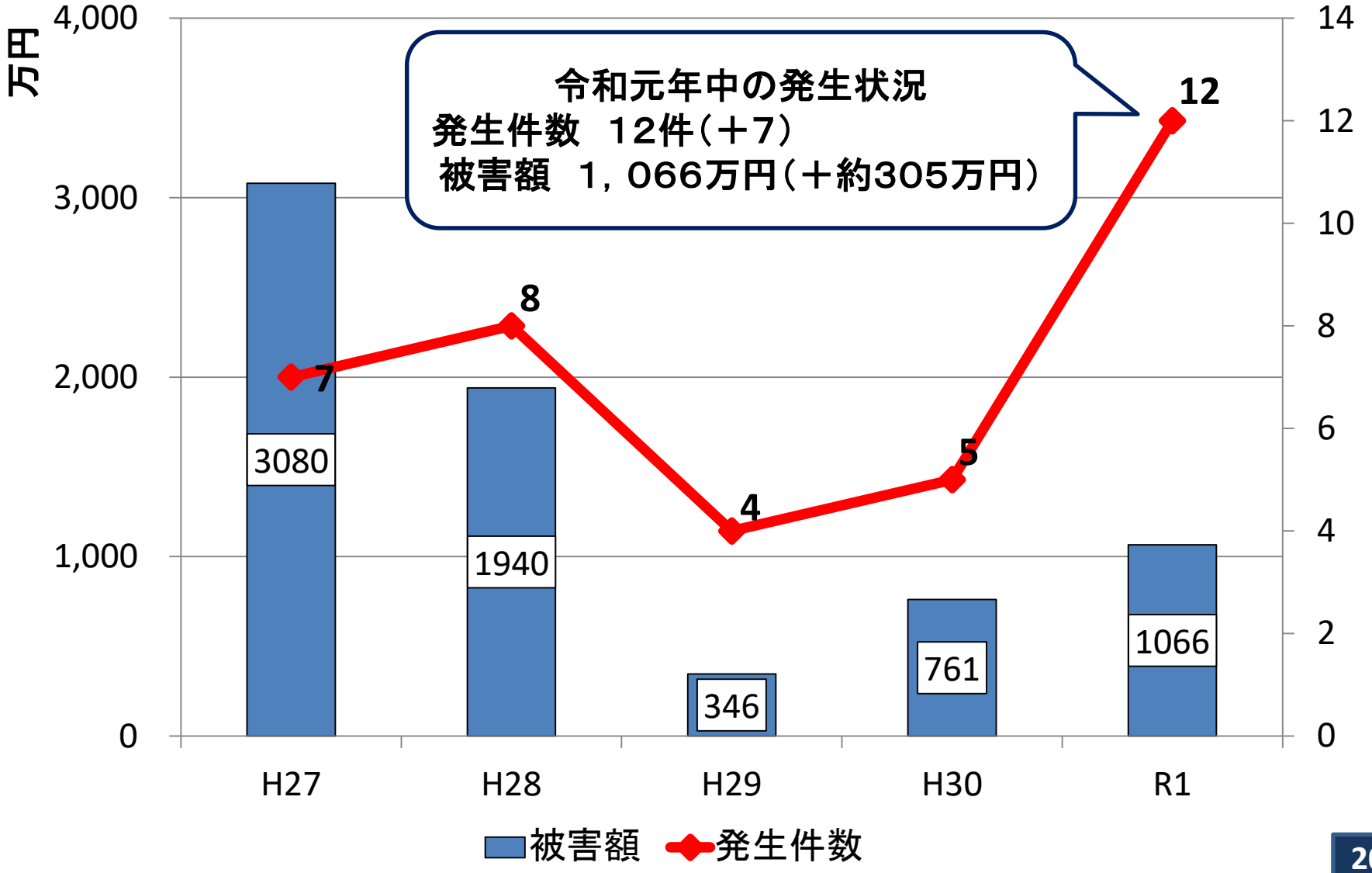
インターネットバンキングに係る不正送金事犯の被害額の推移

特徴

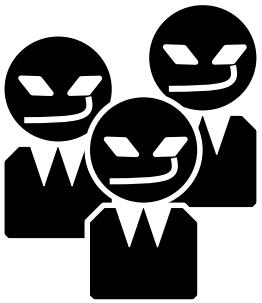
- 前年上半期は、発生件数・被害額ともに以前と比べて減少傾向にあったものの、９月から被害が急増した。
- 令和２年上半期は、被害が急増した前年下半期と比べて減少しているものの、前年同期と比べて大幅に増加しており、その被害の多くは、前年９月以降から引き続いているSMSや電子メールを用いて金融機関を装ったフィッシングサイトへ誘導する手口によるものと考えられる。

※出典元：　警察庁　“令和２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”

インターネットバンキングに係る不正送金事犯
県内の発生状況（H27～R1）



フィッシングによる不正送金の被害が急増



犯人グループ

②フィッシングメール（ＳＭＳ）を送信

メール

セキュリティ強化のため利用を一時的に停止しています。

インターネットバンキング（Ｂ銀行）

制限を解除しなくては･･･

インターネットバンキング利用者

⑥出 金

①フィッシングサイトを開設

フィッシングサイト

〇〇銀行　インターネットバンキング
ようこそ
ログインID
パスワード
ログイン

ワンタイムパスワードを入力してください
ワンタイムパスワード

③フィッシングサイトにアクセス

ATM

⑤Ａ銀行からＢ銀行に不正送金

④入力データをもとにＡ銀行からＢ銀行に対して不正送金指令

インターネットバンキング（A銀行）

ワンタイムパスワードによるセキュリティ対策を突破

インターネットバンキングに係る不正送金事犯（平成31年3月発生）
～ワンタイムパスワードを破る手口による被害が発生～

インターネット
バンキング
（A銀行）

⑤ベトナム人名義口座に送金
（口座から約５０万円送金）

インターネット
バンキング
（B銀行）

④入力された情報を元に送金指令

利 用 権 者
（仙 台）

③ＩＤ、パスワード、
ＯＴＰの入力

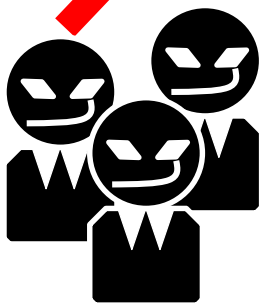
レンタルサーバ

①フィッシング
サイトの開設

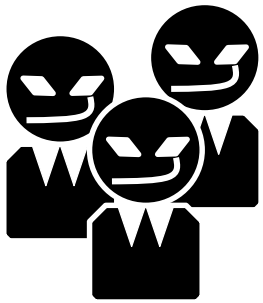
⑥出金

ATM

神奈川県内の
コンビニATM



不正アクセスグループ



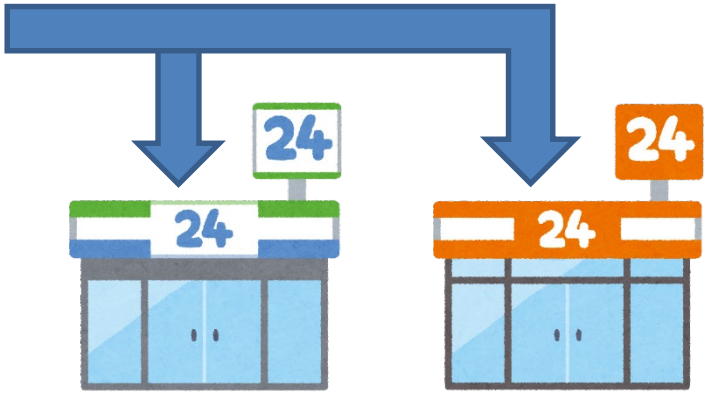
出し子グループ

②フィッシングサイトへの
誘導メールの送信

合同・共同捜査の推進
インターネットバンキングに係る不正送金等事件
（愛知、宮城、千葉、兵庫等１０県合同捜査本部）

インターネットバンキングに係る不正送金事件等の出し子グループを逮捕

インターネットバンキング



愛知県内のコンビニ

千葉県内のコンビニ

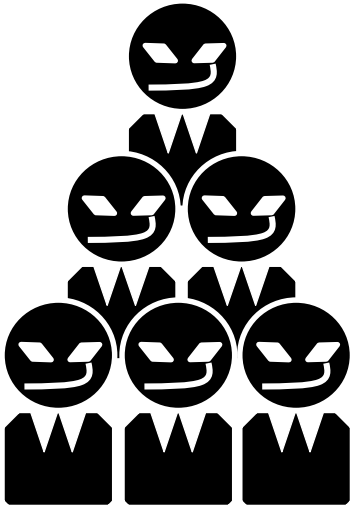
令和元年10月、
中国人1人を通常逮捕！

令和2年10月、
中国人5人を通常逮捕！

令和2年11月、
中国人5人を通常逮捕！

宮城、愛知等
１０県合同捜査本部

逮　捕



中国人出し子グループ

他人名義のキャッシュカードを使い現金自動預払機（ATM）から現金を引き出した窃盗の疑い。

被害防止対策「インターネットバンキングに係る不正送金事犯」

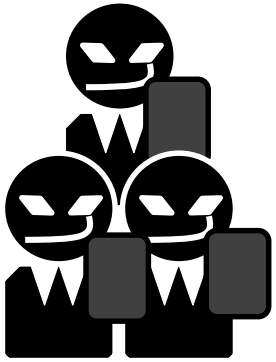
1 基 本

- **ウイルス対策ソフトの利用**
  ウイルス対策ソフトの導入と最新のパターンファイルへの更新を確実に行う。
- **OS等の更新**
  基本ソフト（OS）、ウェブブラウザ等各ソフトウェアを最新の状態に更新する。
- **メールに注意する**
  メールに記載された添付ファイルを安易に実行しない。
  また、メールに記載されたリンクに安易にアクセスしないことが重要。

2 高度なセキュリティ対策の利用

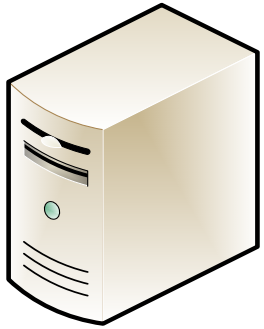
- **ワンタイムパスワードの利用**
  一定時間ごとに自動的に新しいパスワードに変更され、しかも、一度しか使うことができないパスワードであり、不正送金被害のリスクを低減させる。
- **トランザクション認証の利用**
  取引（トランザクション）の内容が、通信の途中で改ざんされていないことを確認する方法であり、不正送金被害のリスクを低減させる。

キャッシュレス決済の不正利用



犯人グループ

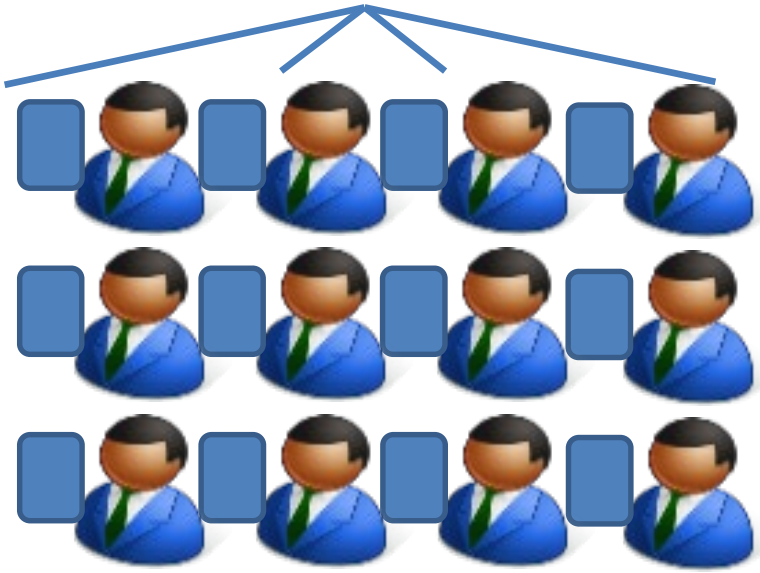
不正アクセス等により他人名義で
家電などを購入し、キャッシュレス決済



キャッシュレス決済を
管理するサーバコンピュータ

家電量販店

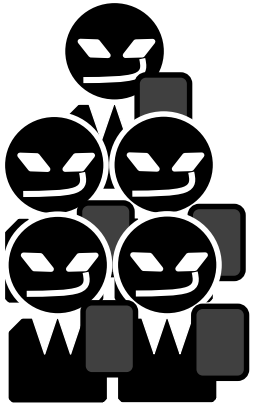
コンビニ



キャッシュレス決済利用者

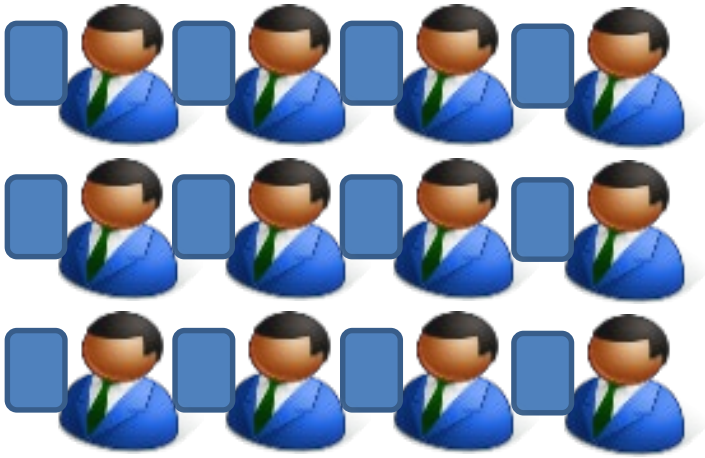
※　キャッシュレス決済とは、クレジットカードや電子マネーなどを利用して、
紙幣・硬貨といった現金を使わずに支払い・受け取りを行う決済方法のこと。

ドコモ口座を悪用した不正送金事件（令和３年１月検挙）
（宮城・埼玉等１１府県合同捜査本部、警視庁サイバー犯罪対策課）



犯人グループ

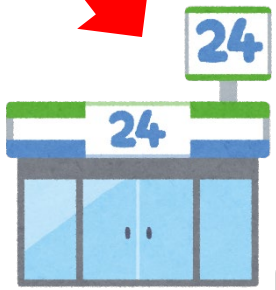
①口座情報等を不正に入手



被 害 者（宮城県ほか全国）

ドコモ口座

②「ドコモ口座」を開設
※メールアドレスだけで開設可能
③ドコモ口座と銀行口座を連携
④銀行口座からドコモ口座にチャージ



コンビニ
（埼玉県）

⑤D払いで
たばこなどを購入

逮 捕

警 察

中国人の男ら5名を
私電磁的記録不正作出・同供用と詐欺
等で通常逮捕！

被害防止対策「キャッシュレス決済の不正利用」

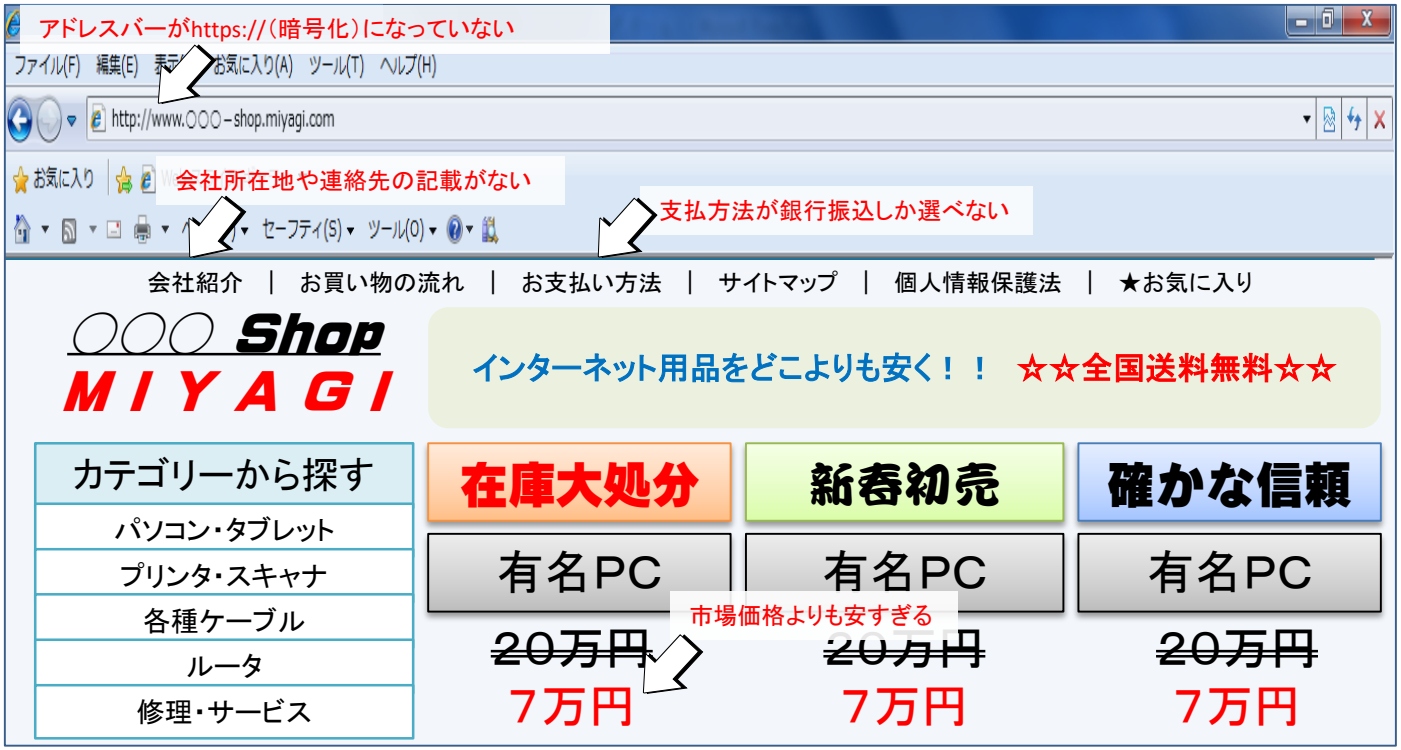
1 基 本

- **フィッシングによるアカウント情報の漏えいに注意する**
  犯人は、「キャリア決済が不正に利用された可能性がある」などと通信事業者を装うメールで偽サイトに誘導し、そこでIDとパスワードなどのアカウント情報を入力させようとすることから注意する。
- **IDとパスワードの使い回しをしない**
  犯人は、過去に漏えいしたパスワードをリスト化し、総当たりでログインを試みる傾向があるため、IDとパスワードの使い回しをしないよう注意する。
- **クレジットカード情報の漏えいに注意する**
  犯人は、何らかの方法で流出したクレジットカード情報を入手しており、その情報を悪用していることから、クレジットカード情報の漏えいに注意する。

2 高度なセキュリティ対策の利用

- **ワンタイムパスワードの利用**
  一定時間ごとに自動的に新しいパスワードに変更され、しかも、一度しか使うことができないパスワードであり、不正利用被害のリスクを低減させる。

偽サイト・詐欺サイト



実在する企業やショッピングサイトなどに似せて作られた「偽のサイト」に関する相談が多く寄せられています。

偽サイトには、代金を支払っても商品が発送されないものや、個人情報やクレジットカード情報等を盗み取るものがあります。

偽サイトの特徴　～ひとつでも該当すれば偽サイトの可能性～

1　サイト運営者・連絡先の記載がない
2　サイトの日本語が不自然である
3　個人情報や決済情報を入力する際のページのアドレスバーに「https://～(通信を暗号化する鍵マーク)」がない
4　支払い方法の説明と実際の決済画面とで、対応可能な支払い方法が異なっている
5　商品の価格が市場価格よりも安すぎる

CyberNews

令和2年12月
宮城県警察本部
サイバー犯罪対策課

ニトリネット偽サイトに注意！

本年11月下旬頃から、宮城県内でも家具通販サイト「ニトリネット」を装った偽のショッピングサイトに関する相談が急増しています。

これまでに確認されている偽のショッピングサイトのURLの一部に
「 mitori 」
などの文字列が使われていることを知っていますか!?

商品を注文する前に要チェック！ こんなショッピングサイトは危険かもしれない・・・・

- 販売している商品が極端に値引きされていないか確認する
- 開いているショッピングサイトのURLが正しいものであるかよく確認する
- サイトの連絡先に電話番号が記載されているか確認する
- サイト内の文章は、機械翻訳されている可能性が高いため、不自然な日本語が使用されていないか確認する
- スマートフォンでのサイト閲覧では、URLが表示されません！画面上のアドレスバーをタップして、表示されるURLを確認する

ショッピングサイトを利用する際は、これらのことに注意するほか、公式ホームページからサイトにアクセスするようにして下さい！

その他の特徴として、
JPドメインを使用
開設場所は米国
HTTPS通信（電子証明書取得）
などが確認されています。
偽サイトの手口が巧妙になっているので、みなさんも注意しましょう。

警察による海外の偽サイト・詐欺サイト対策

海 外 の 偽サイト・詐欺サイト

遮 断

遮 断

インターネット利用者

インターネット利用者

①偽サイト情報の収集

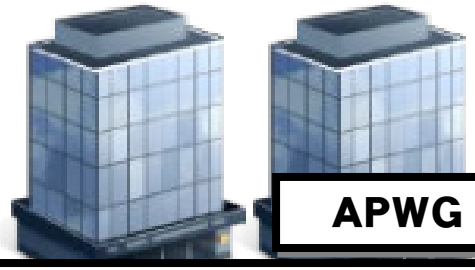
都道府県警察

②偽サイト情報の収集

警 察 庁

③ 情報提供

④対策の実施（警告画面の表示）



APWG

情報セキュリティ関連事業者

APWGとは、米国に本拠を置く世界最大のフィッシング対策の国際機関

企業におけるサイバーセキュリティ

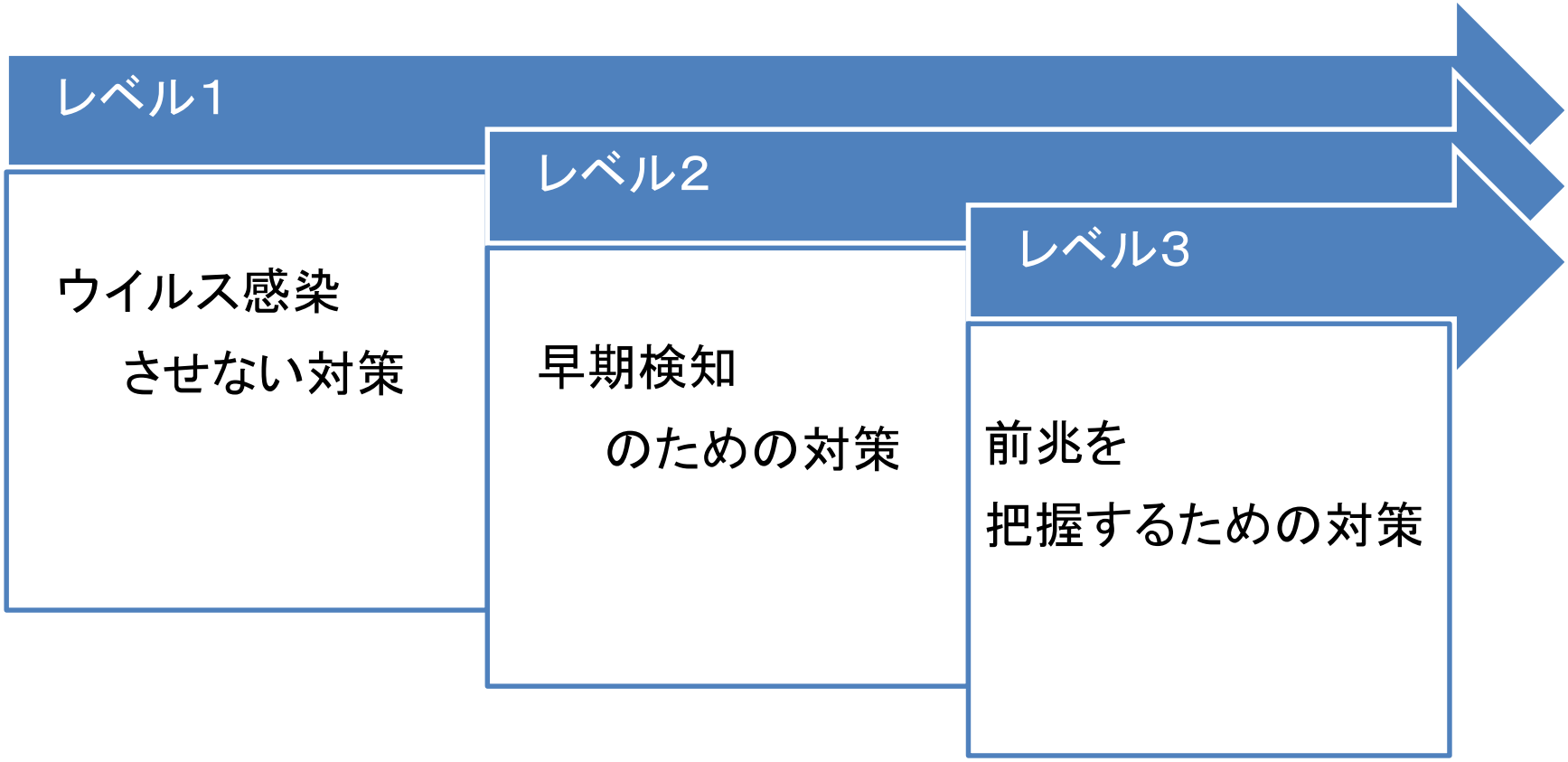
サイバーセキュリティは経営課題

- 事業継続性が危うくなる
- サイバーセキュリティを誤ると、顧客や取引先等から信用を損ねる
- 成長の鍵であるデジタルイノベーションを生かす基盤

経営者がなすべきこと

- 何を守るかを優先付けて、優先度に応じた多層防御を講じる
- １００パーセントの防御ではなく、セキュリティ上の侵害が起こることを前提に、早期検知、対応、復旧を実行できる組織力を整える
- 上記２点を経営会議で定期的にレビューする。

企業におけるサイバーセキュリティ対策



企業におけるサイバーセキュリティ対策

早期対応と被害状況の早期特定	• 体制の確立と対処訓練 • 社内ネットワークの監視 • ログの保存
適切な情報開　示	• 警察への届出 • 個人情報の漏えいがあれば、個人情報保護委員会や顧客・取引先等への通知を検討
再発防止対策の策　定	• 組織全体で対応する必要があるため、部門を超えて指揮できる責任者（CISO）が指定 • CSIRTの設置と発生時に備えた訓練

経営者は何をやらなければならないのか
～　認識すべき「３原則」　～

原則１　情報セキュリティ対策は経営者のリーダーシップで進める

原則２　委託先の情報セキュリティ対策まで考慮する

原則３　関係者とは常に情報セキュリティに関するコミュニケーションをとる

※出典元：独立行政法人情報処理推進機構 “中小企業の情報セキュリティ対策ガイドライン　第３版”

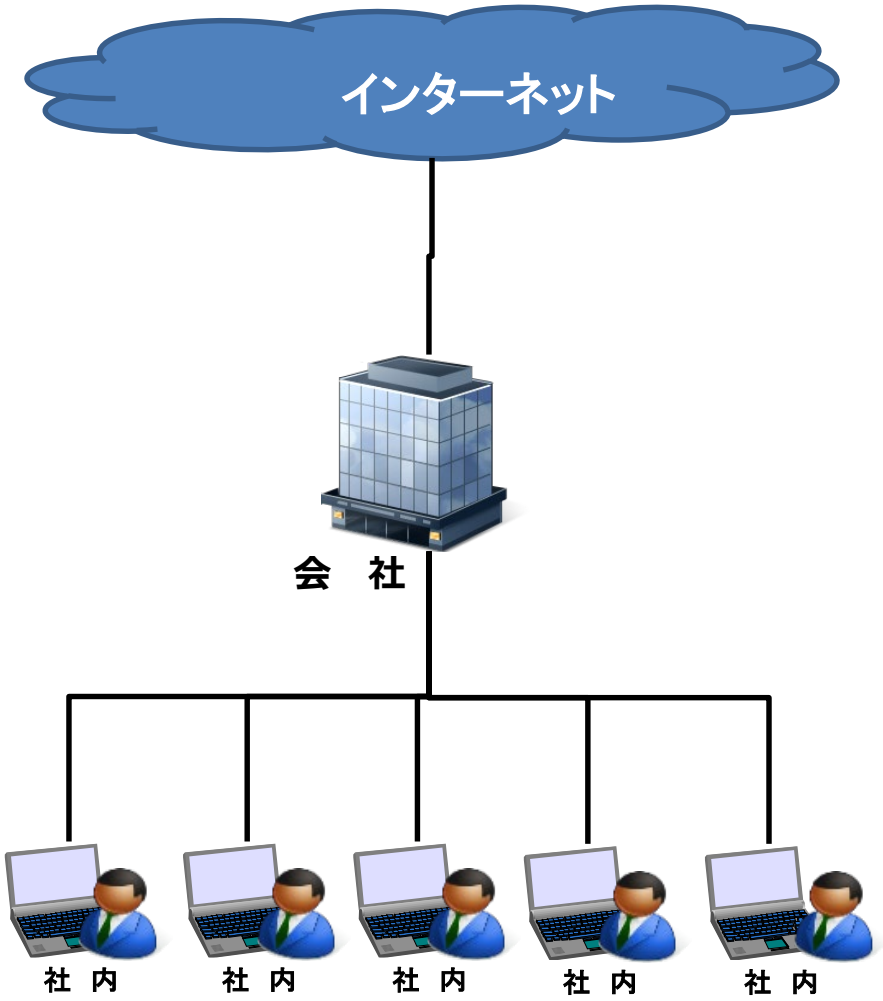
実行すべき「重要7項目の取組」

	実行すべき「重要7項目の取組」
取組1	情報セキュリティに関する組織全体の対応方針を定める
取組2	情報セキュリティ対策のための予算や人材などを確保する
取組3	必要と考えられる対策を検討させて実行を指示する
取組4	情報セキュリティ対策に関する適宜の見直しを指示する
取組5	緊急時の対応や復旧のための体制を整備する
取組6	委託や外部サービス利用の際にはセキュリティに対する責任を明確にする
取組7	情報セキュリティに関する最新動向を収集する

※出典元： 独立行政法人情報処理推進機構 “中小企業の情報セキュリティ対策ガイドライン 第3版”

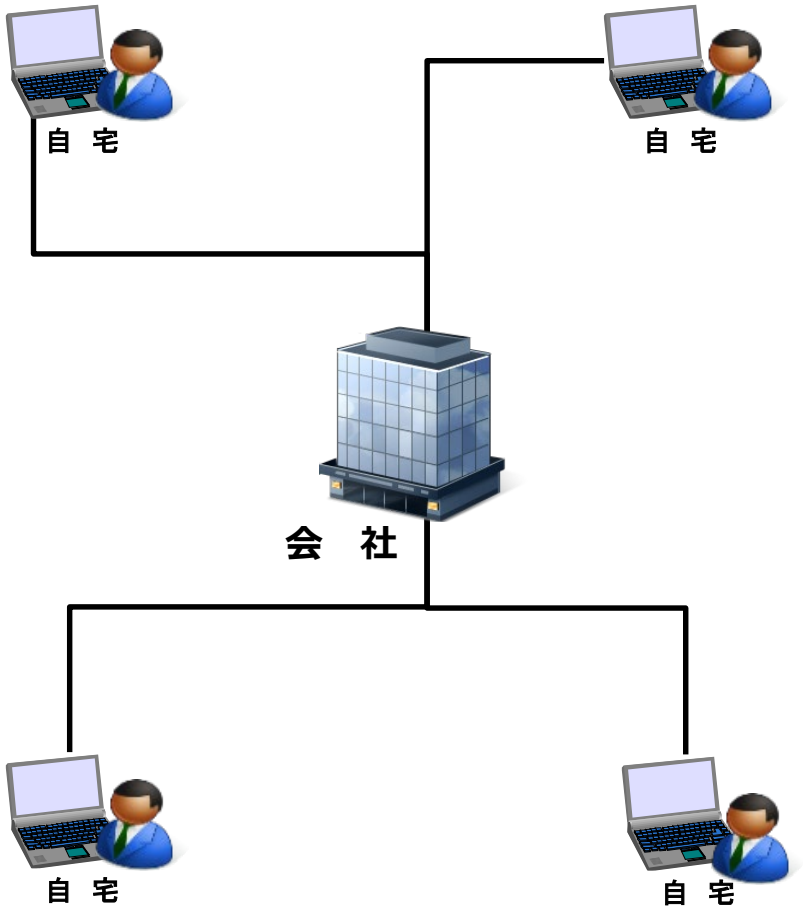
コロナ禍におけるネットワーク環境で注意すべき点

社内ネットワーク環境



社内ネットワークである程度防御できる

テレワーク環境



インターネット経由のため防御が難しい
トラブルが発生してもすぐ相談できない

テレワーク時の被害防止対策

1 基 本

・ **ウイルス付きメールに注意**
　犯人は、ウイルスが添付されたメールを送信してくることから、ウイルス添付メールを不用意に開封して感染しないよう注意する。また、添付ファイルを開封する際は、メール文をよく確認してから開封する。

・ **一人で悩まず相談する**
　テレワーク時は、一人で仕事をしているためすぐに相談できない場合が多いが、そのような場合でも不審な点については、電話等で上司、同僚に相談する。

・ **無線LANの利用に注意する**
　フリーWi-Fiを利用する際は、通信内容の傍受に注意し、通信経路が暗号化(WPA2、WPA3)されていることを確認する。

2 自宅のルータの管理を徹底する

・ **パスワードを適切に設定する**
　アクセス用及び管理用パスワードを推測が不可能なものに設定する。

・ **ファームウエアを最新の状態に更新する**
　ファームウエアの更新状況を確認し、常に最新に保つ。

サイバー捜査官募集！

募　集　内　容

1　職種・採用予定人員・職務内容
　警察官（サイバー捜査官）
　採用予定人員　3人程度

2　応募資格
　昭和59年4月2日～平成10年4月1日までに生まれた者で、次のいずれかに該当するもの。
（1）　情報処理安全確保支援士試験の合格者
（2）　応用情報技術者試験等の合格者
（3）　（1）又は（2）に掲げる者と同等の知識及び能力を有すると認められる者

3　申込受付期間
　令和元年7月26日（金）から8月23日（金）までの間

さあ、サイバー犯罪との戦いへ

警察官採用案内　https://www.police.pref.miyagi.jp/hp/keimu/police/shikenn/shikenn.html

サイバー空間情勢は依然として厳しい状況

サイバー空間の脅威
に対する対策の強化が必要

生活安全に関する不安や
悩みは警察相談専用電話
＃9110
へ御相談ください。