サイバー空間をめぐる脅威の情勢と
サイバーセキュリティ対策

令和３年１０月１５日（金）

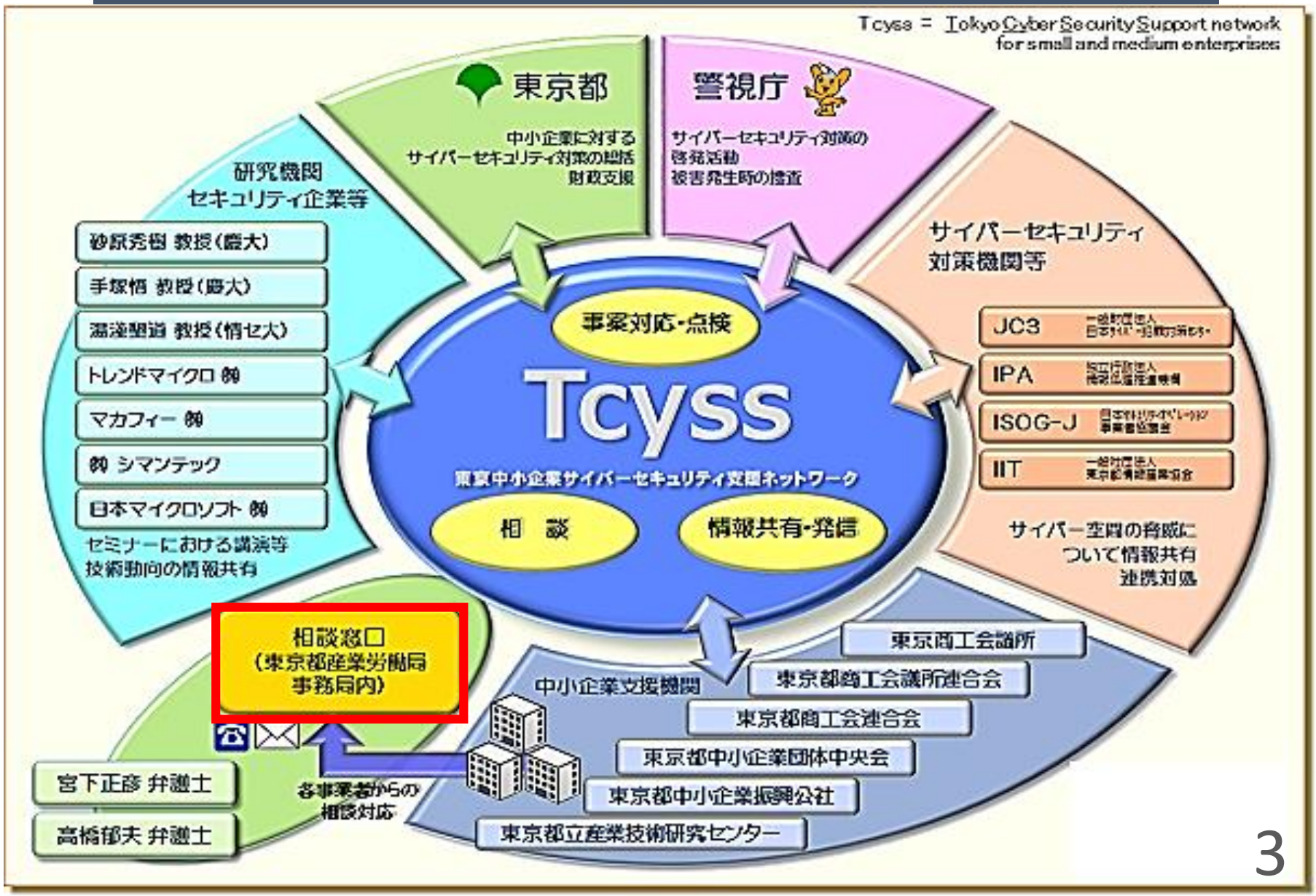
警視庁サイバーセキュリティ対策本部

Ｔｃｙｓｓ

（東京中小企業サイバーセキュリティ支援ネットワーク）
についてのご紹介

東京中小企業サイバーセキュリティ支援ネットワーク発足（平成28年４月）

～中小企業のサイバーセキュリティ強化に向けた産学官連携の枠組み～



都内の中小企業者に限られますが

中小企業サイバーセキュリティ相談窓口（無料）

対象：都内中小企業者

電話・窓口受付時間	
都庁開庁日	９：００～１２：００
	１３：００～１７：００

03-5320-4773
(Tcyss事務局直通)

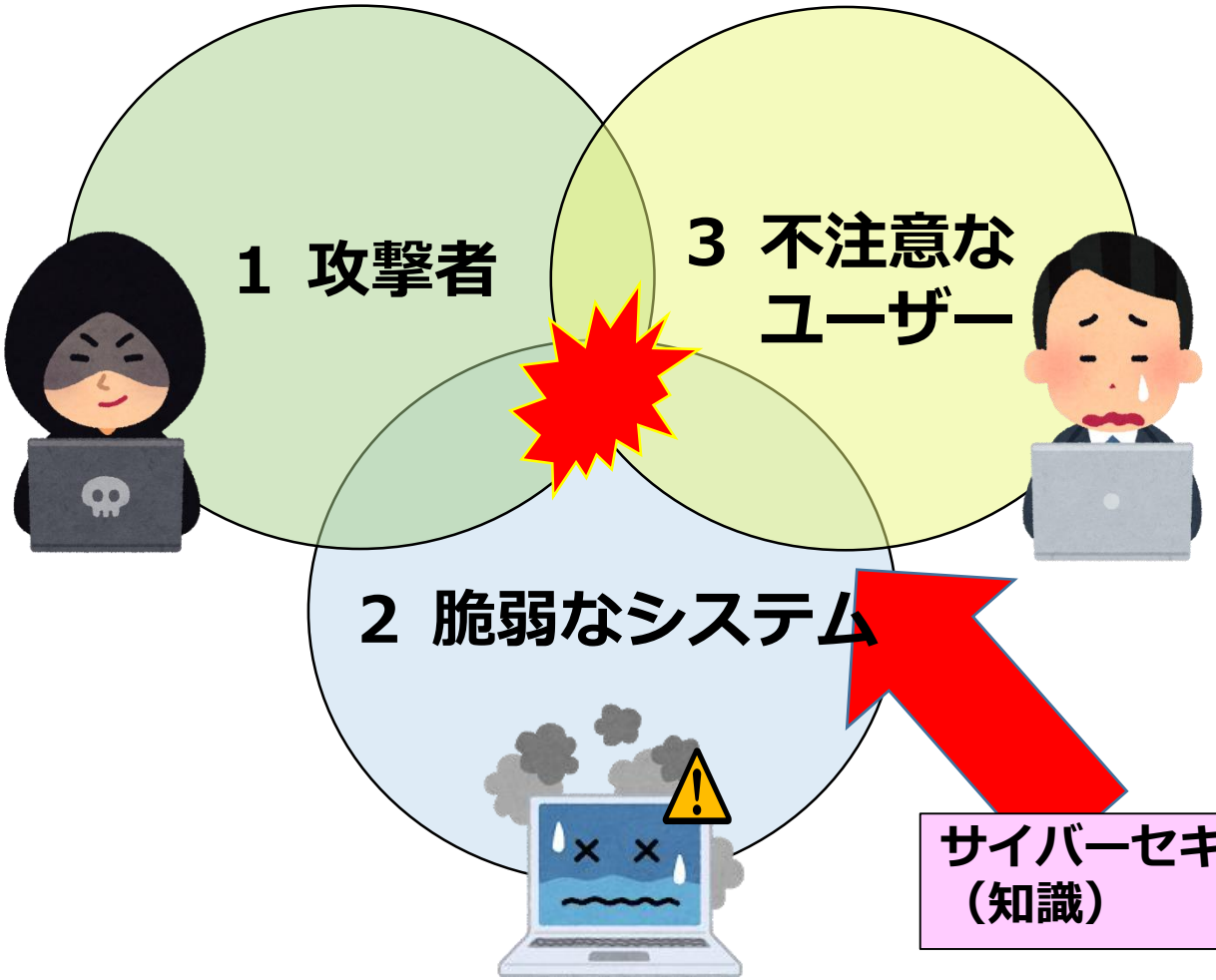
Web
http://www.sangyo-rodo.metro.tokyo.jp/chushou/shoko/cyber/

相談窓口
東京都産業労働局商工部
東京都庁第一本庁舎20階北側
（Ｔｃｙｓｓ事務局）

■社内パソコンの環境について相談したい。
■サイバーセキュリティに関する研修を実施したい。
■サイバーセキュリティ導入の具体的なやり方について。

サイバーに関して相談できる人がいないという方は、是非ご活用ください。

被害に遭う３つの要因



ー　本日のお話（目次）　ー

１．サイバー空間をめぐる脅威の情勢等について

- 情報セキュリティ１０大脅威２０２１
- センサー検知アクセス件数の推移
- JPCERT/CCに寄せられた相談件数
- 相談件数とインシデント件数との比較
- 偽装されたＷｅｂページにご注意を
- フィッシング報告件数比較表
- 日本国内におけるネットバンキング被害件数の推移
- 口座開設者別被害状況

２．製造会社が狙われたサイバー犯罪

（サプライチェーンが悪用された標的型メール攻撃からランサムウェアまで）

- 事例紹介
- 国内のランサムウェアの情勢
- VPN脆弱性攻撃とは
- リモート脆弱性攻撃とは
- 最も危険なランサムウェア　トップ５

３．サポート詐欺

４．お知らせ

１．サイバー空間をめぐる脅威の情勢等について

情報セキュリティ　１０大脅威２０２１

昨年順位	個　人	順位	組　織	昨年順位
1位	スマホ決済の不正利用	1位	ランサムウエアによる被害	5位
2位	フィッシングによる個人情報の詐取	2位	標的型攻撃による機密情報の窃取	1位
7位	ネット上の誹謗・中傷・デマ	3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	NEW
5位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	4位	サプライチェーンの弱点を悪用した攻撃	4位
3位	クレジットカード情報の不正利用	5位	ビジネスメール詐欺による金銭被害	3位
4位	インターネットバンキングの不正利用	6位	内部不正による情報漏えい	2位
10位	インターネット上のサービスからの個人情報の窃取	7位	予期せぬIT基盤の障害に伴う業務停止	6位
9位	偽警告によるインターネット詐欺	8位	インターネット上のサービスへの不正ログイン	16位
6位	不正アプリによるスマートフォン利用者への被害	9位	不注意による情報漏えい等の被害	7位
8位	インターネット上のサービスへの不正ログイン	10位	脆弱性対策情報の公開に伴う悪用増加	14位

２０２１年１月２７日付　IPA（情報処理推進機構）「情報セキュリティ１０大脅威２０２１」より

情報セキュリティ10大脅威 2021

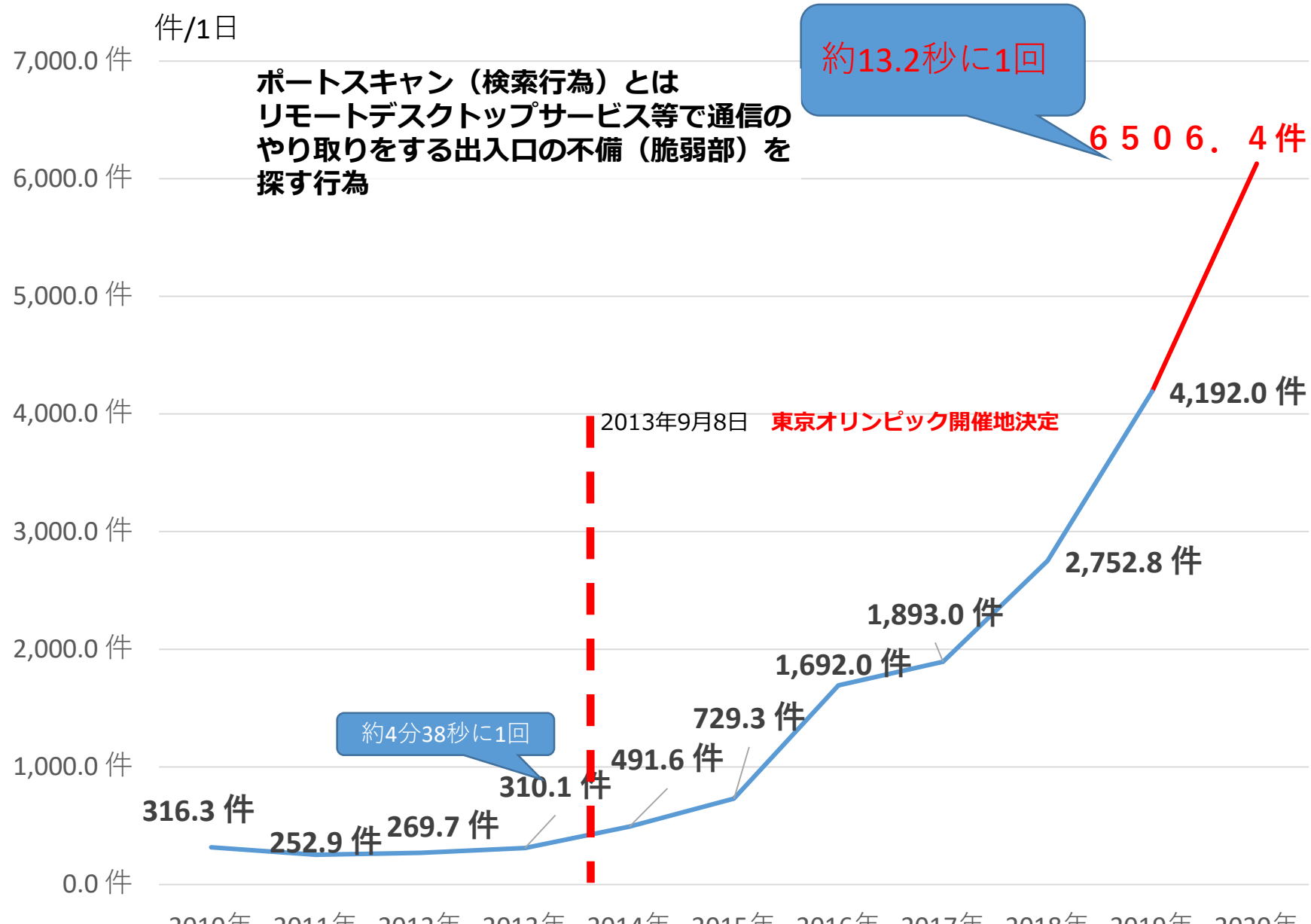
毎年公表されています。

目次

公表される前年に発生した攻撃や事故等から今年注意すべき脅威を、約１６０名の有識者選出してランク付けしたものです。

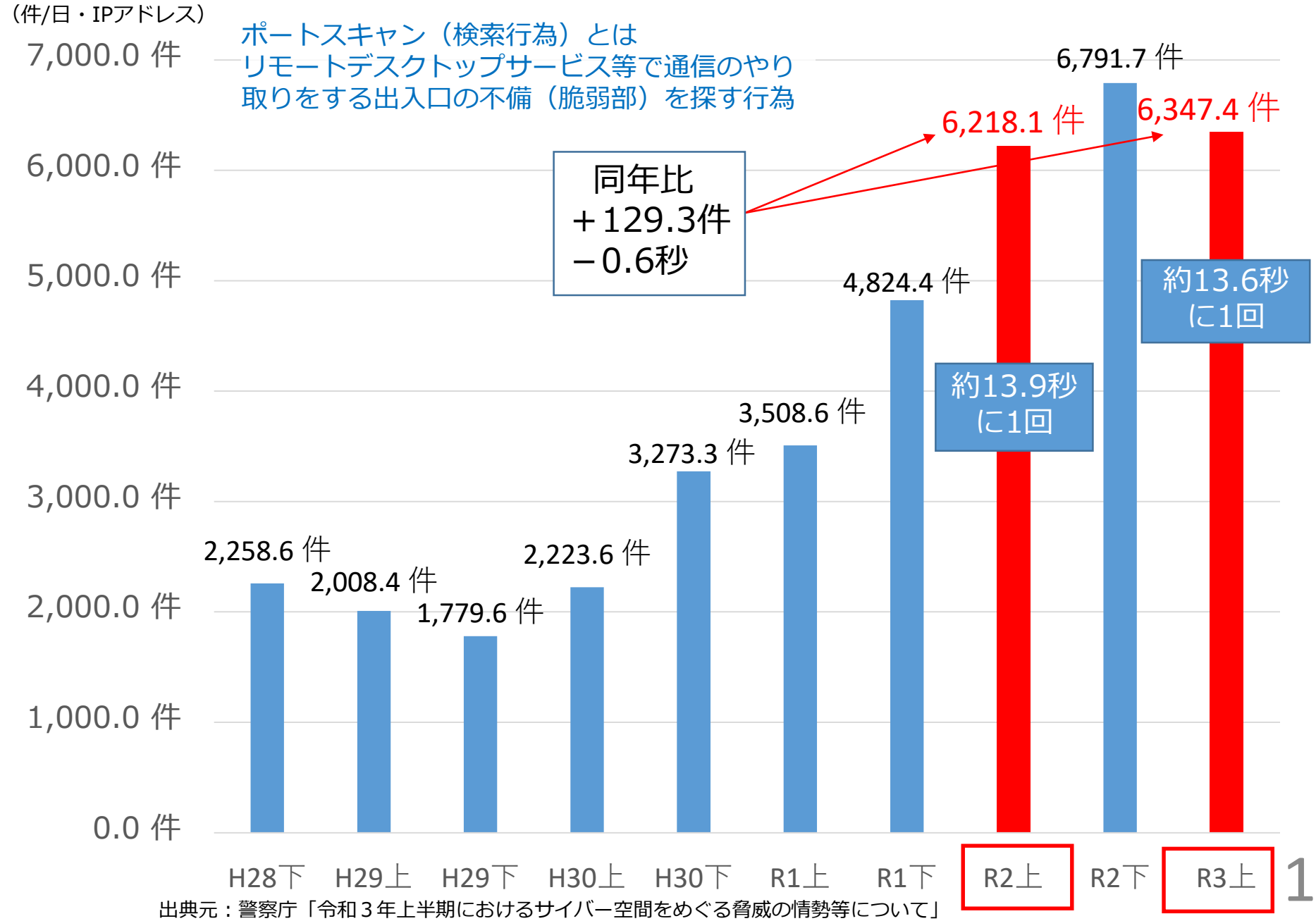
出典元：独立行政法人情報処理推進機構（IPA）https://ipa.go.jp/security/vuln/10threats2021.html

センサー検知アクセス件数の推移（年別）



出典元：警察庁「令和２年におけるサイバー空間をめぐる脅威の情勢等について」

センサー検知アクセス件数の推移

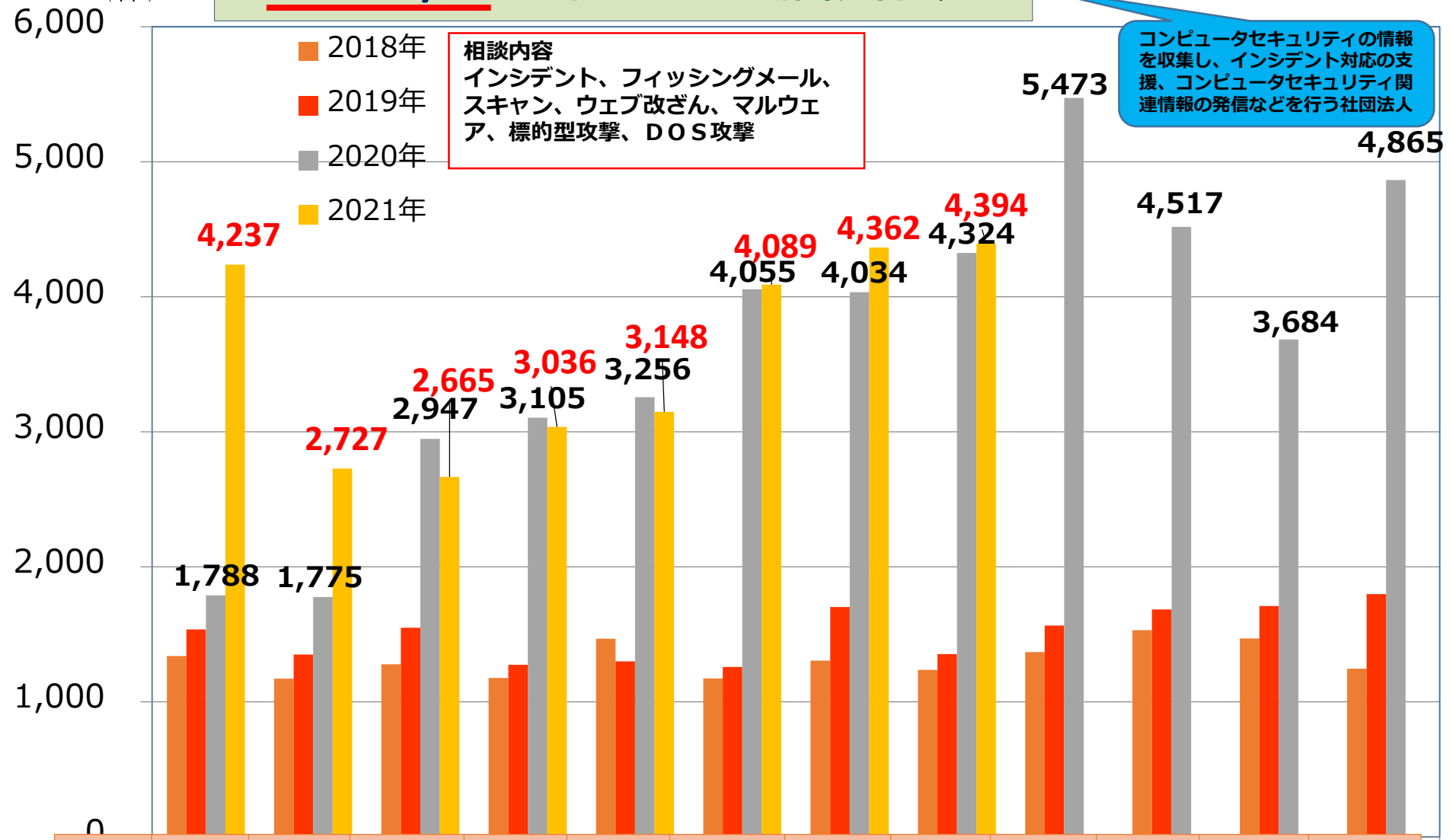


出典元：警察庁「令和３年上半期におけるサイバー空間をめぐる脅威の情勢等について」

JPCERT/CCに寄せられた相談件数

引用元：ＪＰＣＥＲＴ／Ccコーディネーションセンター「インシデント報告対応レポート」

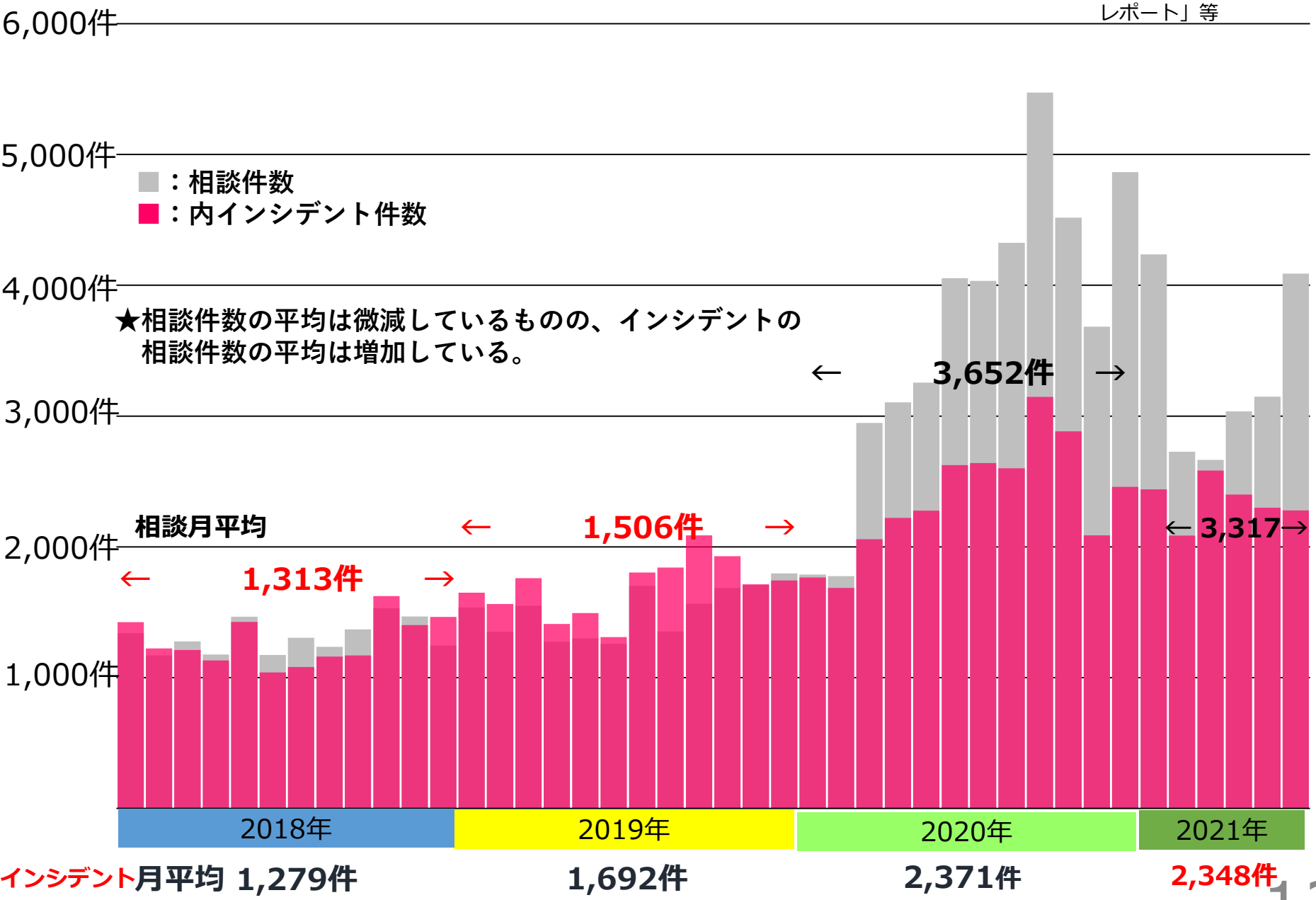
コンピュータセキュリティの情報を収集し、インシデント対応の支援、コンピュータセキュリティ関連情報の発信などを行う社団法人



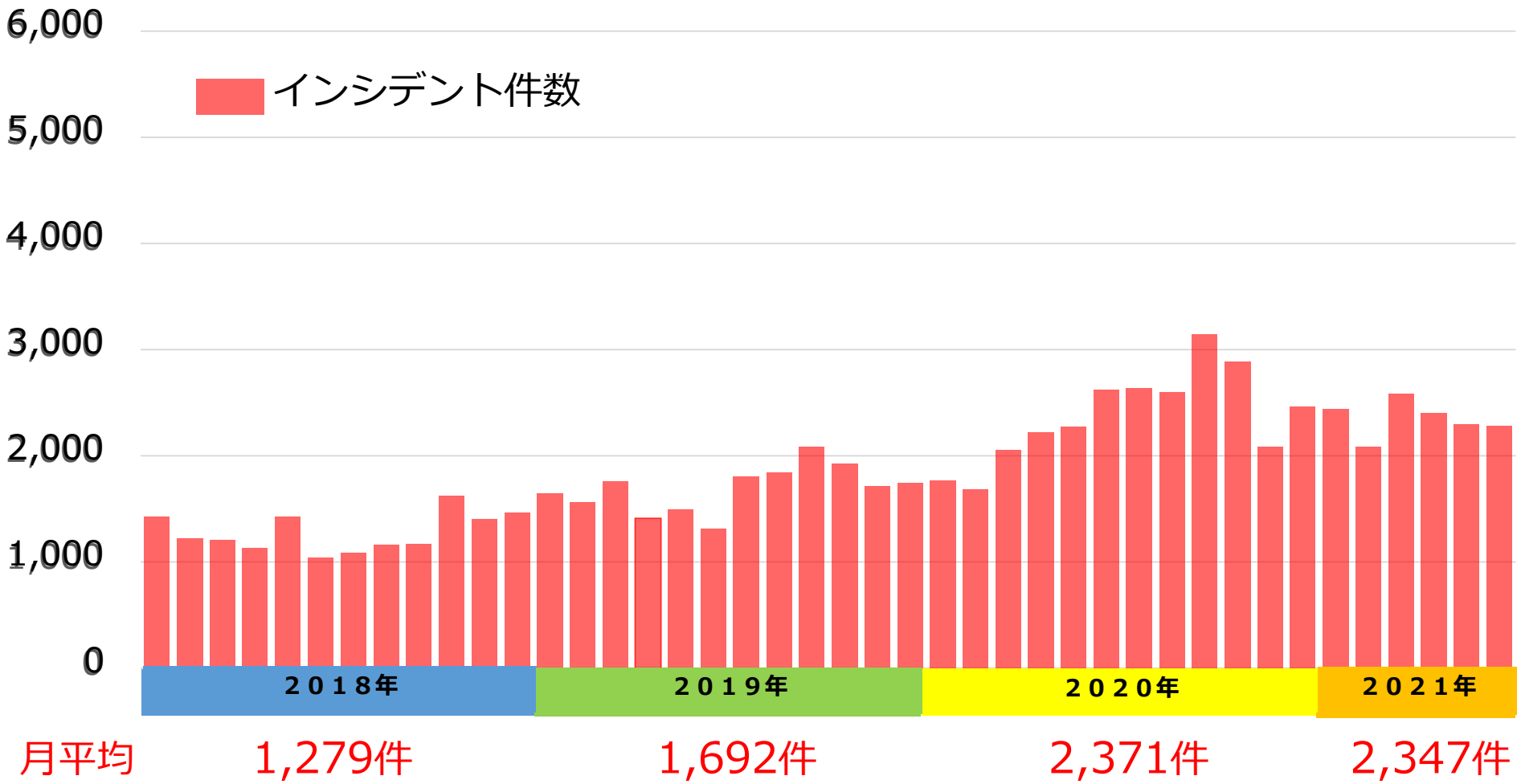
	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月
2018年	1,339	1,170	1,277	1,177	1,466	1,172	1,305	1,235	1,368	1,530	1,468	1,244
2019年	1,536	1,349	1,548	1,274	1,299	1,257	1,701	1,353	1,564	1,648	1,708	1,797
2020年	1,788	1,755	2,947	3,105	3,256	4,055	4,034	4,324	5,473	4,517	3,684	4,865
2021年	4,237	2,727	2,665	3,036	3,149	4,089	4,362	4,394				

相談件数とインシデント件数との比較

引用元：JPCERTコーディネーションセンター「2021年7月15日公開 インシデント報告対応レポート」等

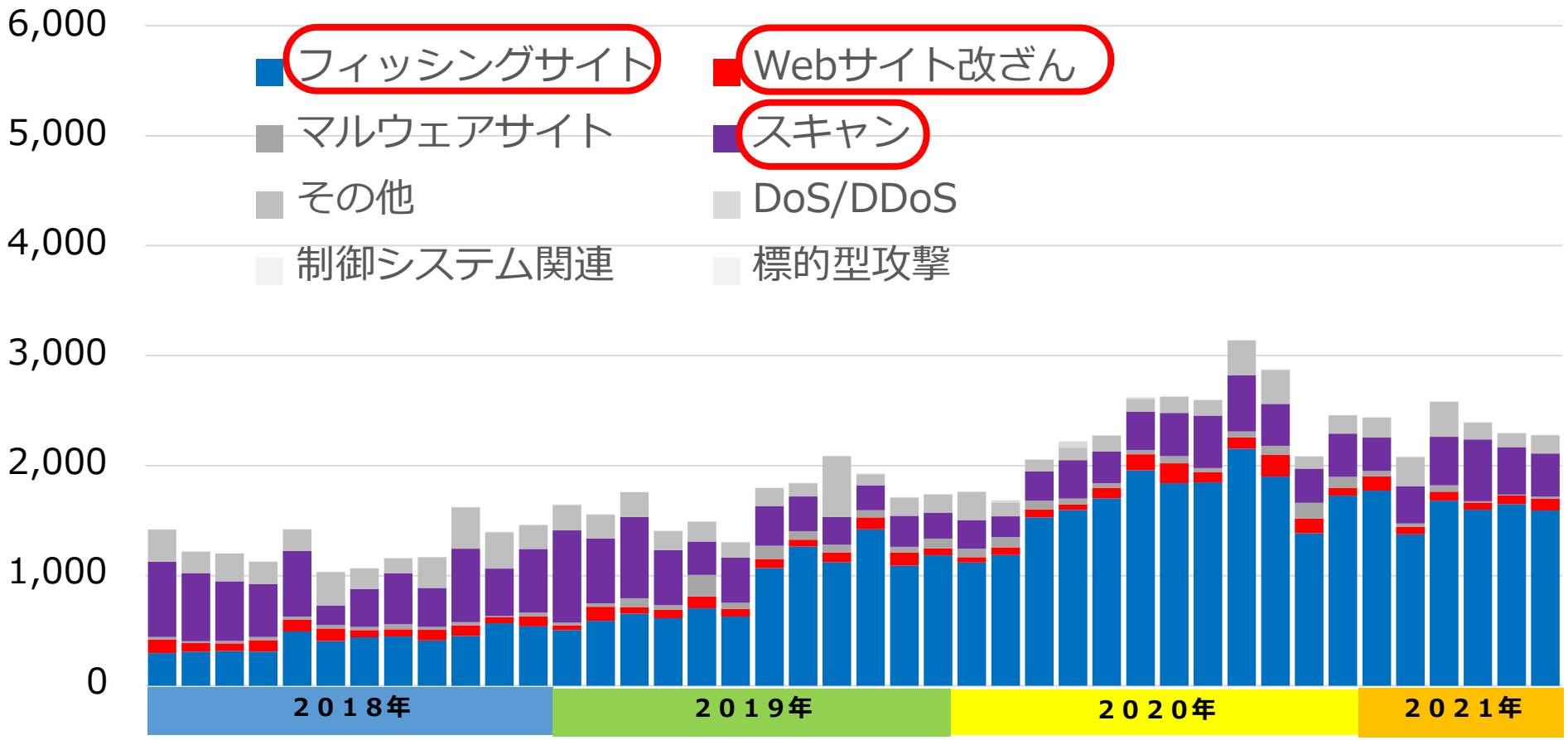


相談件数とインシデント件数との比較



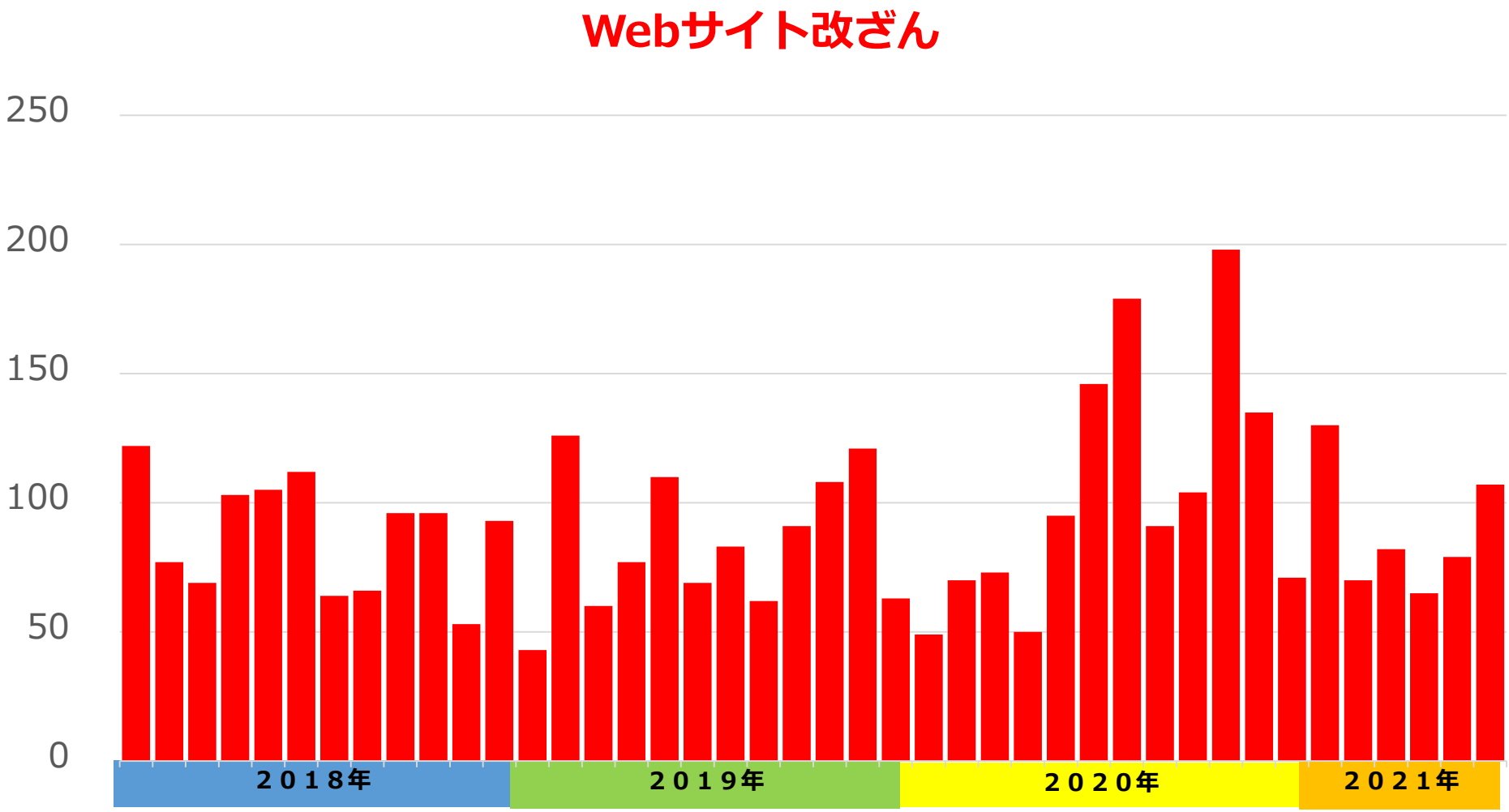
出典元：JPCERTコーディネーションセンター「２０２１年７月１５日公開　インシデント報告対応レポート」等

相談件数とインシデント件数との比較



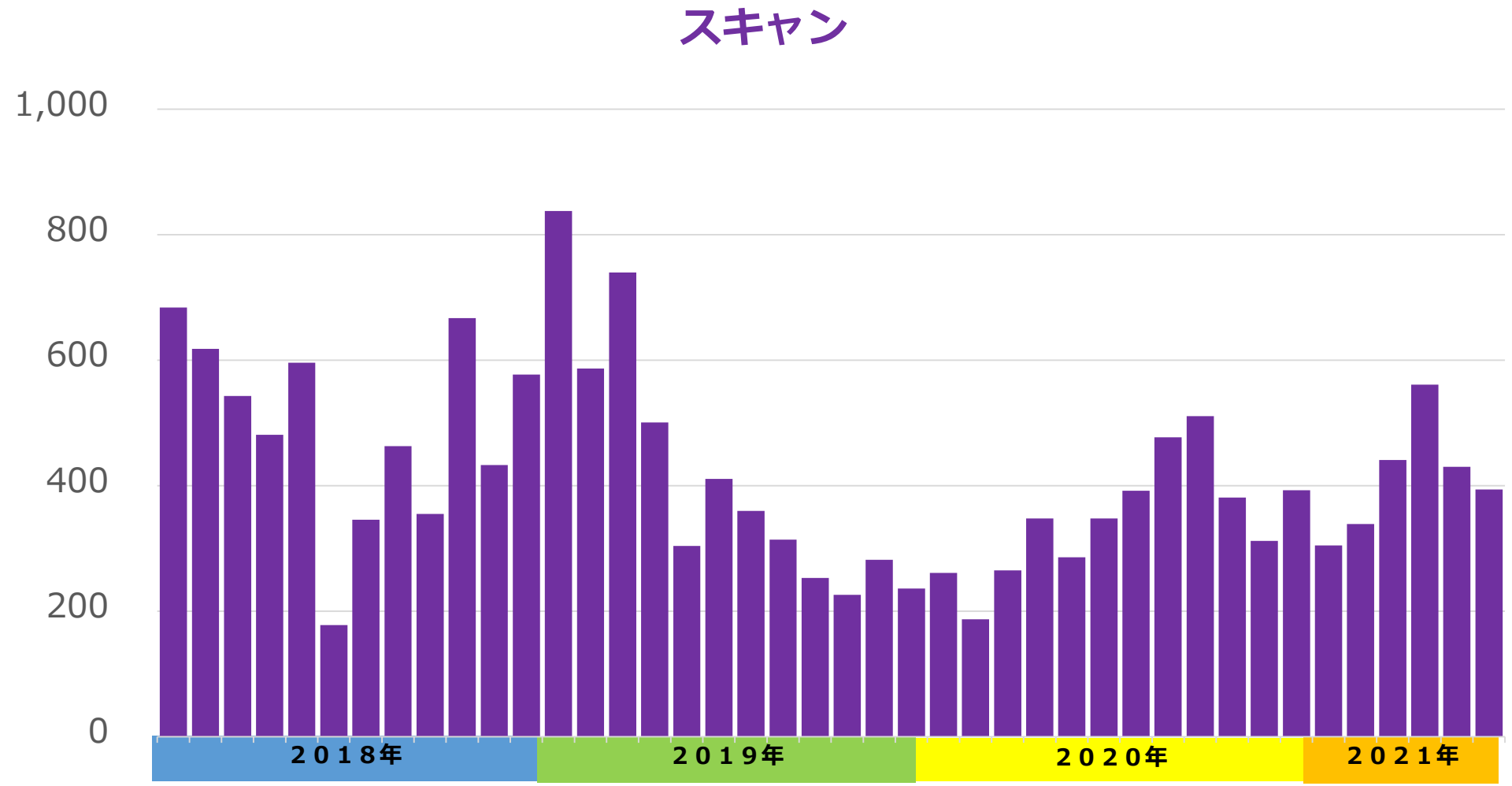
出典元：JPCERTコーディネーションセンター「２０２１年７月１５日公開　インシデント報告対応レポート」等

相談件数とインシデント件数との比較



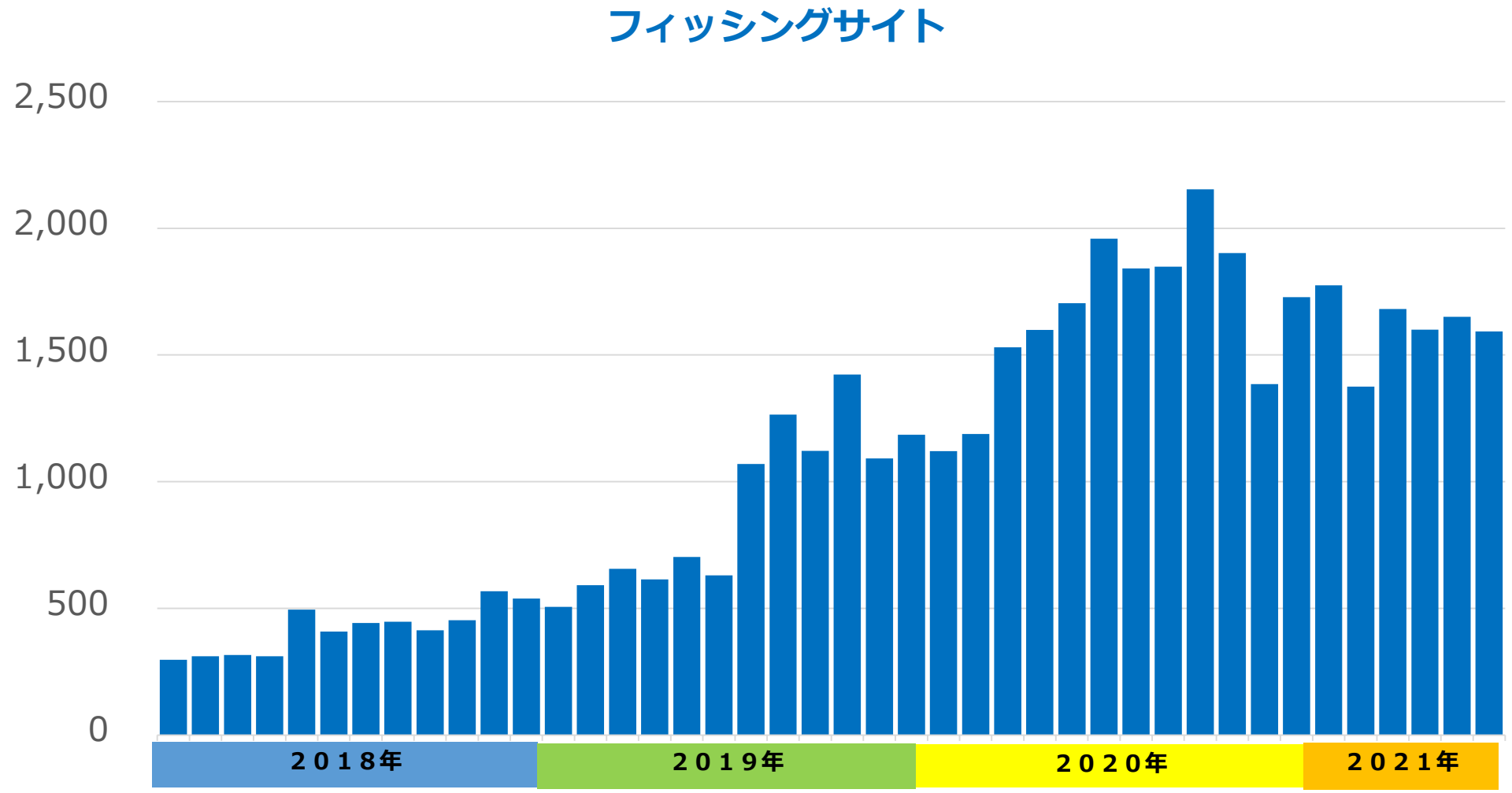
出典元：JPCERTコーディネーションセンター「２０２１年７月１５日公開　インシデント報告対応レポート」等

相談件数とインシデント件数との比較



出典元：JPCERTコーディネーションセンター「２０２１年７月１５日公開　インシデント報告対応レポート」等

相談件数とインシデント件数との比較



出典元：JPCERTコーディネーションセンター「２０２１年７月１５日公開　インシデント報告対応レポート」等

偽装されたＷｅｂページにご注意を

図：偽造Ｗｅｂサイト画面

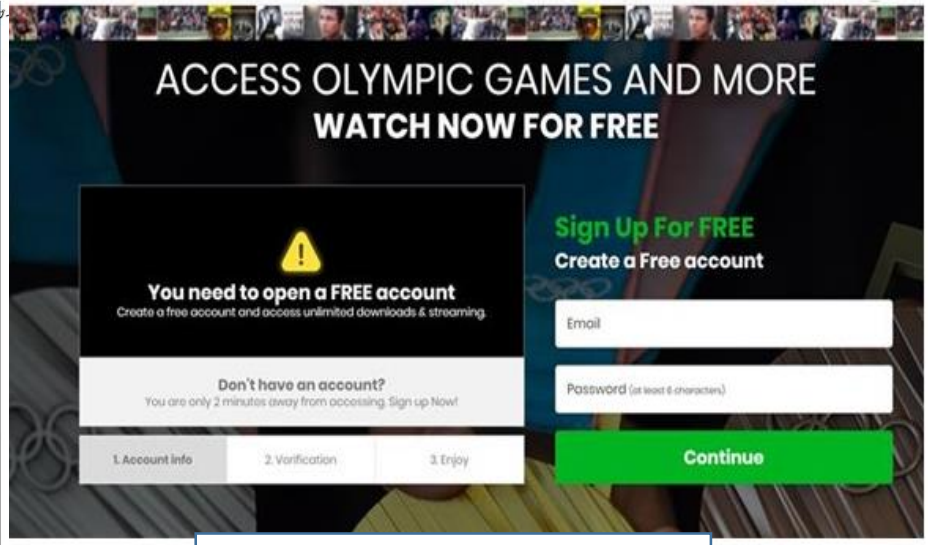


図2：別の不審スポーツ中継サイト例。
視聴のために会員登録を促す

図3：不審なスポーツ中継サイト内のリンクをクリックした際に表示される別サイトの例。キャプチャ認証と誤解させてブラウザ通知の「許可」ボタンをクリックさせる手口

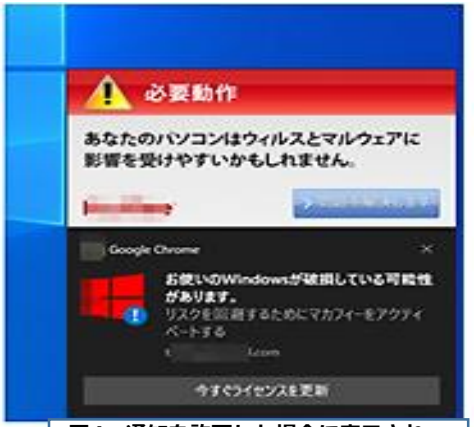


図4：通知を許可した場合に表示される「ブラウザ通知スパム」の例。セキュリティ製品の購入ページへ誘導し購入を促すアフィリエイト目的と推測される

○　２０２１年７月１９日、トレンドマイクロが、東京オリンピックＴＶ放送予定を**偽装したＷｅｂページ**から不審なスポーツ中継へ誘導されるものを発見。
○　このスポーツ中継サイトは利用者に**ブラウザ通知を許可させ悪質な広告を表示する**いわゆる「**ブラウザ通知スパム**」に誘導するものだった。
○　以降においても、同種の不審スポーツ中継サイトへ誘導する偽装ページがＷｅｂ検索で確認されている。
○　偽装ページは**正規サイトの改ざん**もしくは**乗っ取り**による**手口**は**変わっていない**。
○　誘導先は**ブラウザ通知スパム**に加え、不審サイト上で動画視聴のためと称して**メールアドレスなどの個人情報の登録させる**手口も確認されている。

引用元：２０２１年７月２６日　トレンドマイクロ セキュリティブログ「東京オリンピック開会直前、偽のＴＶ放送予定ページからブラウザ通知スパムへ誘導する攻撃を確認」より

偽装されたＷｅｂページにご注意を

トレンドマイクロが**Ｇｏｏｇｌｅ検索を行い確認**した、不正なＷｅｂページの検索**結果**画面
※７月１９日１２時時点では表示されなくなった。

○ **利用者側の注意点**

- ブックマークした公式サイトや普段利用しているニュースサイト等の直接閲覧する方法が安全。
- 検索サイトを利用する場合は、検索結果のＵＲＬを確認する。
- ネット経由でオリンピック等を観戦する場合は、公式サイトや携帯サイトのストリーミングのみで観戦する。
  ※今回のオリンピックでは、「ＮＨＫ＋」,「gorin.jp」,「TVer」 などの正規の配信サイトから観戦する。
- ストリーミングサイトで、「アクセス制限のない動画サイト」などと強調しているサイトは巧妙な仕掛けがある可能性があるのでクリックする際は十分注意する。

○ **Ｗｅｂ開設側の注意点**

Ｗｅｂ改ざんが増加しているので、自社のＷｅｂの状況について必ず確認しましょう。

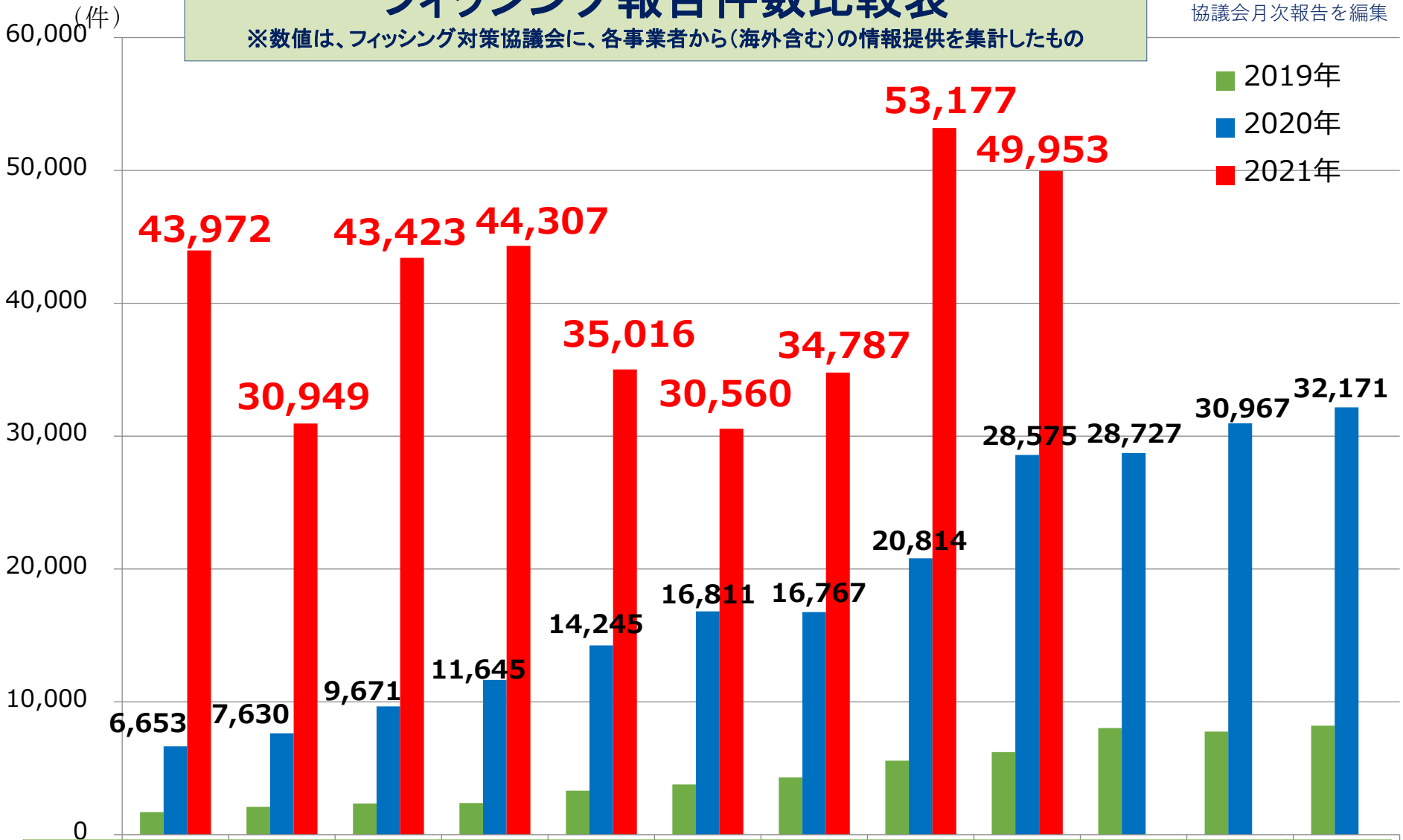
- 会社のＷｅｂが不正アクセスにされていないか確認する。
  - 検索エンジンを利用し、自分のＷｅｂサイトにアクセスして「コンピューターに重大な損害を与えるおそれがある」と注意文等が表示するか確認する。（OS、ウイルス対策ソフトを最新の状態にして）
  - 全部のページの**ソース**を見て、挿入した覚えのない**スクリプト**の有無を確認する。
  - 不審なアクセスの有無を**アクセスログ**にて確認する。
- ソフトのシステムを必ずアップデートし最新にする。
- セキュリティソフト（ファイヤをール等）導入する。
- セッションＩＤとパスワードの管理を徹底する。
- Ｗｅｂサーバーのファイルへのアクセス権限を制限する。
- 長く使っていない、更新していない場合は一度閉鎖する。

引用元：２０２１年７月２６日　トレンドマイクロ セキュリティブログ「東京オリンピック開会直前、偽のＴＶ放送予定ページからブラウザ通知スパムへ誘導する攻撃を確認」より

フィッシング報告件数比較表

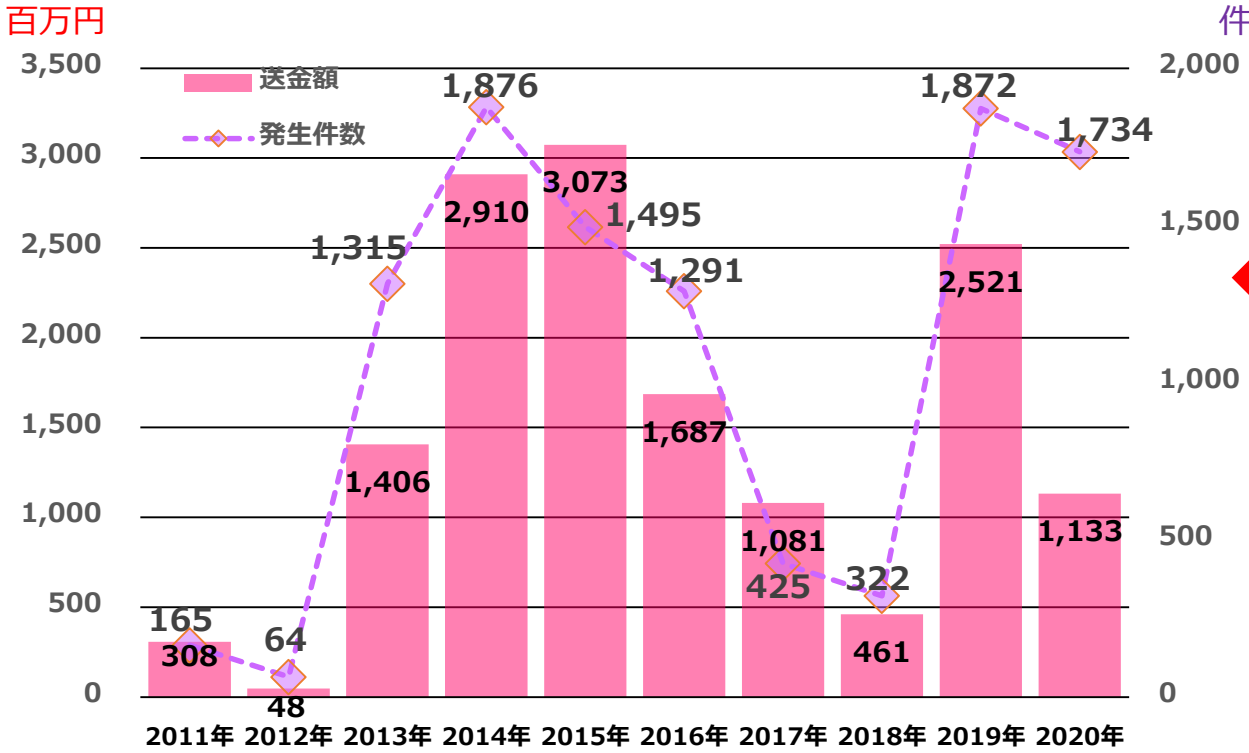
※数値は、フィッシング対策協議会に、各事業者から（海外含む）の情報提供を集計したもの

引用元：フィッシング対策協議会月次報告を編集



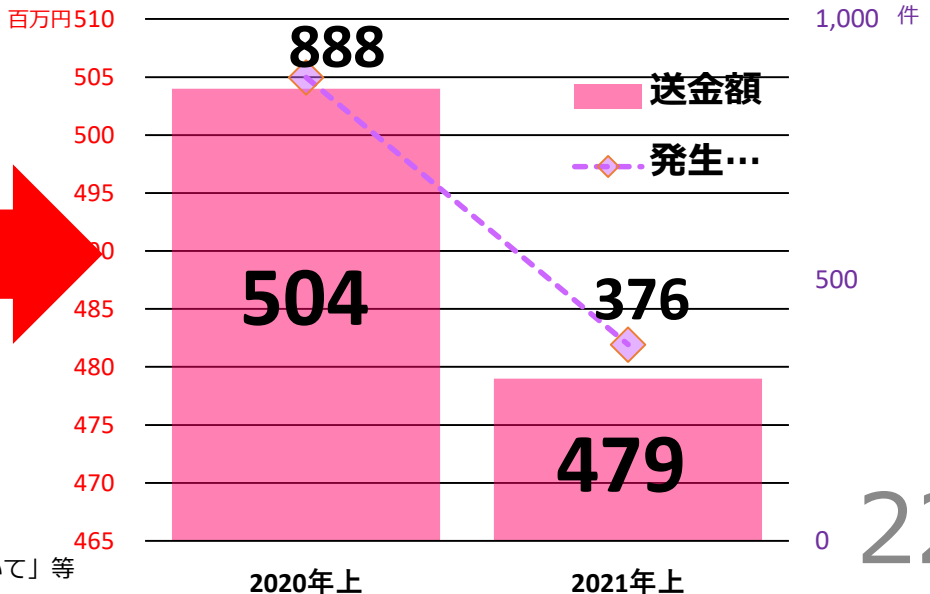
	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月
2019年	1,713	2,100	2,352	2,388	3,327	3,788	4,322	5,577	6,218	8,034	7,760	8,208
2020年	6,653	7,630	9,671	11,645	14,245	16,811	16,767	20,814	28,575	28,727	30,967	32,171
2021年	43,972	30,949	43,423	44,307	35,016	30,560	34,787	53,177	49,953			

日本国内におけるネットバンキング被害件数の推移



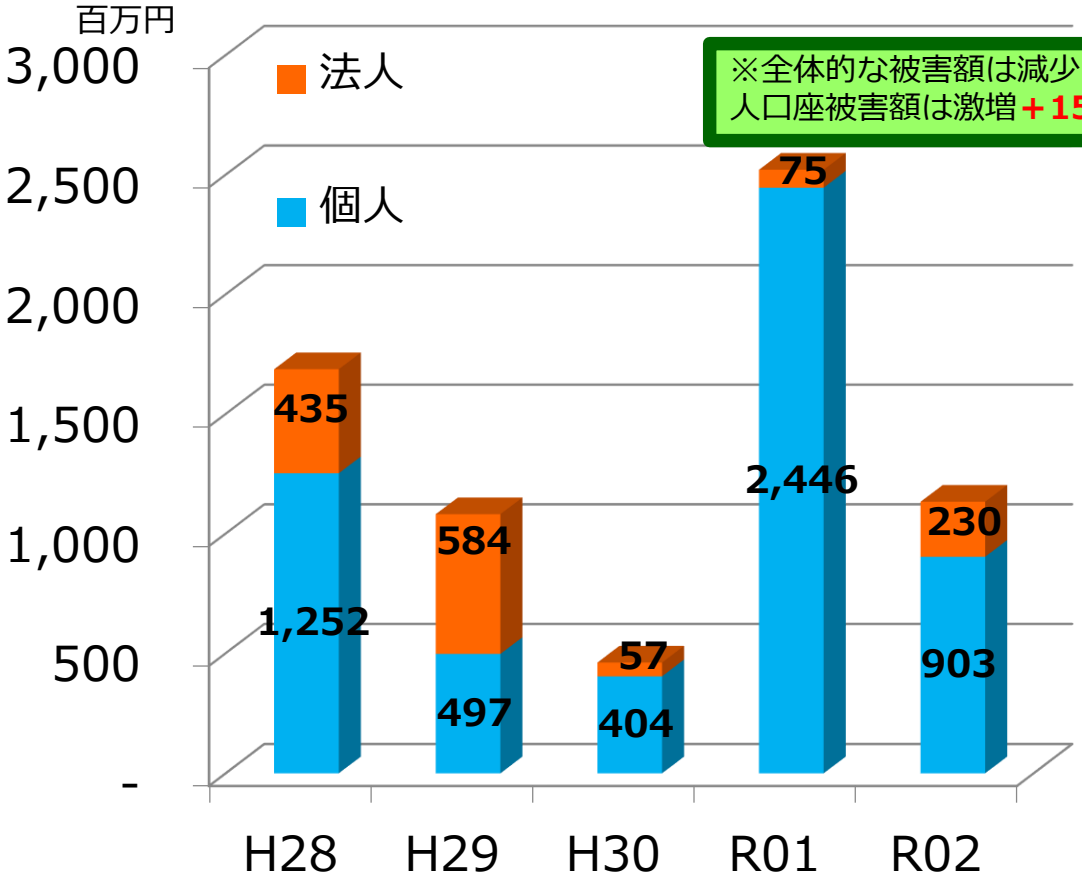
前年比（２０２１年、２０２０年）
- 被害金額
  －１３億８，８００万円
- 被害件数
  －１３８件

前年同期比
- 被害金額
  －２，５００万円
- 被害件数
  －５１２件

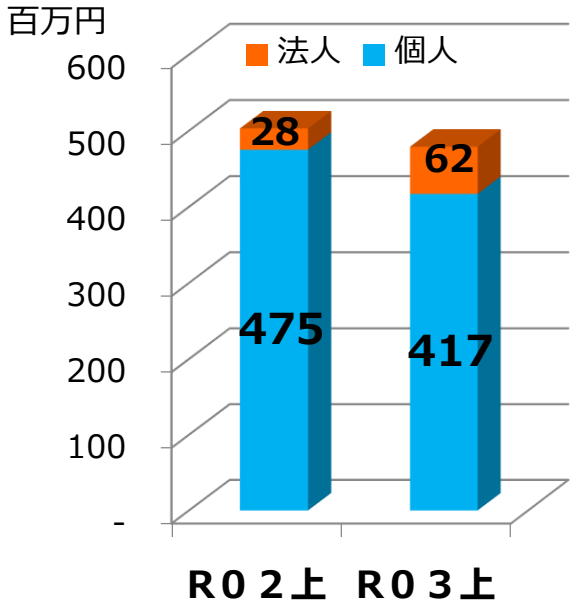


引用元：警察庁「令和３年上半期におけるサイバー空間をめぐる脅威の情勢等について」等

口座開設者別被害状況



※全体的な被害額は減少したが、法人口座被害額は激増**＋155百万円**



※**前年同期比**
全体的な被害額は微減したが、**法人口座は**、被害額は**＋3,400万円**

引用元：警察庁「令和3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」

2　製造会社が狙われたサイバー犯罪

（サプライチェーンが悪用された標的型メール攻撃からランサムウェアまで）

引用元：２０２０年５月　独立行政法人情報処理推進機構（IPA）
「制御システム関連のサイバーインシデント事例５　～２０１９年　ランサムウェアによる操業停止～」より

１，事案概要

２０１９年３月、ノルウェーに本社を置く世界有数のアルミニウム生産企業Ｎ社が、ランサムウェアの「**ＬｏｃｋｅｒＧｏｇａ**」の被害受け数か月後の長時間にわたり生産量が低下した。

引用元：２０２０年５月　独立行政法人情報処理推進機構（IPA）「制御システム関連のサイバーインシデント事例５～２０１９年　ランサムウェアによる操業停止～」より

２，被害状況

４０カ国１６０の拠点で、２３，０００台のパソコンのうち感染が１１，０００台、暗号化されたものが２，７００台。
３，０００台のサーバーのうち、１，１００台が感染、５００台が暗号化された。

被害を受けた多くはメール、発注や顧客情報管理のコンピューターなどと言われているが、製造用のコンピューターも被害を受けたと推定され、長時間に亘り手作業による製造を強いられた。
損失額は６５～７７億円と見積もられた。

しかし、このインシデントは、Ｔｒａｎｓｐａｒｅｎｃｙ（透明性）とＯｐｅｎｎｅｓｓ（率直さ）をポリシーとし、今後の参考とするため情報公開の姿勢を貫いたことが高く評価を受けた。

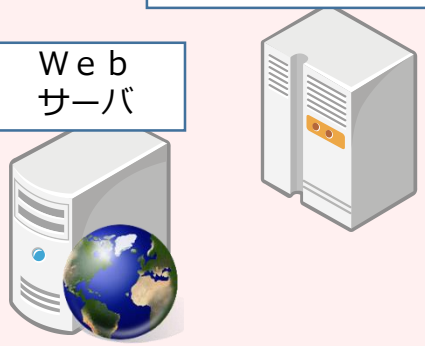
引用元：２０２０年５月　独立行政法人情報処理推進機構（IPA）　「制御システム関連のサイバーインシデント事例５　～２０１９年　ランサムウェアによる操業停止～」より

本事案の構図

攻撃者

※Ｃ２サーバ

Ｗｅｂ
サーバ

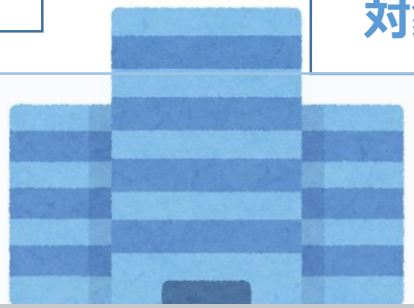


※Ｃ２サーバ（Ｃ＆Ｃサーバ）
　コントロール＆コマンドサーバの略。
　攻撃者が、不正なコマンドを遠隔にて頻繁に送信するために利用するサーバ。

取引先（拠点）

インターネット

対象企業



引用元：２０２０年５月　独立行政法人情報処理推進機構（IPA）「制御システム関連のサイバーインシデント事例５　～２０１９年　ランサムウェアによる操業停止～」より

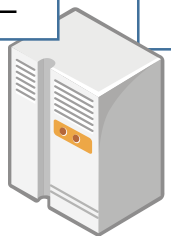
攻撃局面１：対象企業への侵入（取引先（拠点）を攻略し、対象企業への侵入成功まで）

サプライチェーンが狙われた

対象企業

引用元：２０２０年５月
独立行政法人情報処理推進機構（IPA）
「制御システム関連のサイバーインシデント事例５　～２０１９年　ランサムウェアによる操業停止～」より

C２サーバー



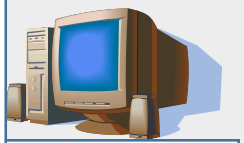
取引先（拠点）

②添付ファイルクリック

Ｗｅｂサーバー

③マルウェアが仕組まれたメールを送り感染させ、取引先（拠点）の攻略に成功

⑥添付ファイルをクリック、業務端末Ａがトロイの木馬の「※**ＧｏｏｔＫｉｔ Ｔｏｒｏｊａｎ**」が感染



発注管理サーバー

※バックドア

④対象企業の従業員とのメールのやりとりを傍受して、何らかの方法で乗っ取り（不正アクセス、遠隔操作など）、悪意あるサイトへのリンクを含むメールを送信する

インターネット

業務端末Ａ

業務端末Ｂ

攻撃者

⑤添付ファイルクリック

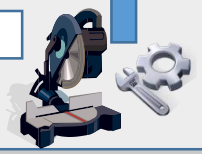
ＦＷ／ＶＰＮ機器

①ターゲットの企業の取引先（拠点）を特定し標的型メール攻撃を実施する

⑦業務端末Ａにトロイの木馬の「**ＧｏｏｔＫｉｔ Ｔｏｒｏｊａｎ**」が感染したことにより、**バックドア**を生成する

制御端末（ＨＭＩ等）

生産管理サーバー

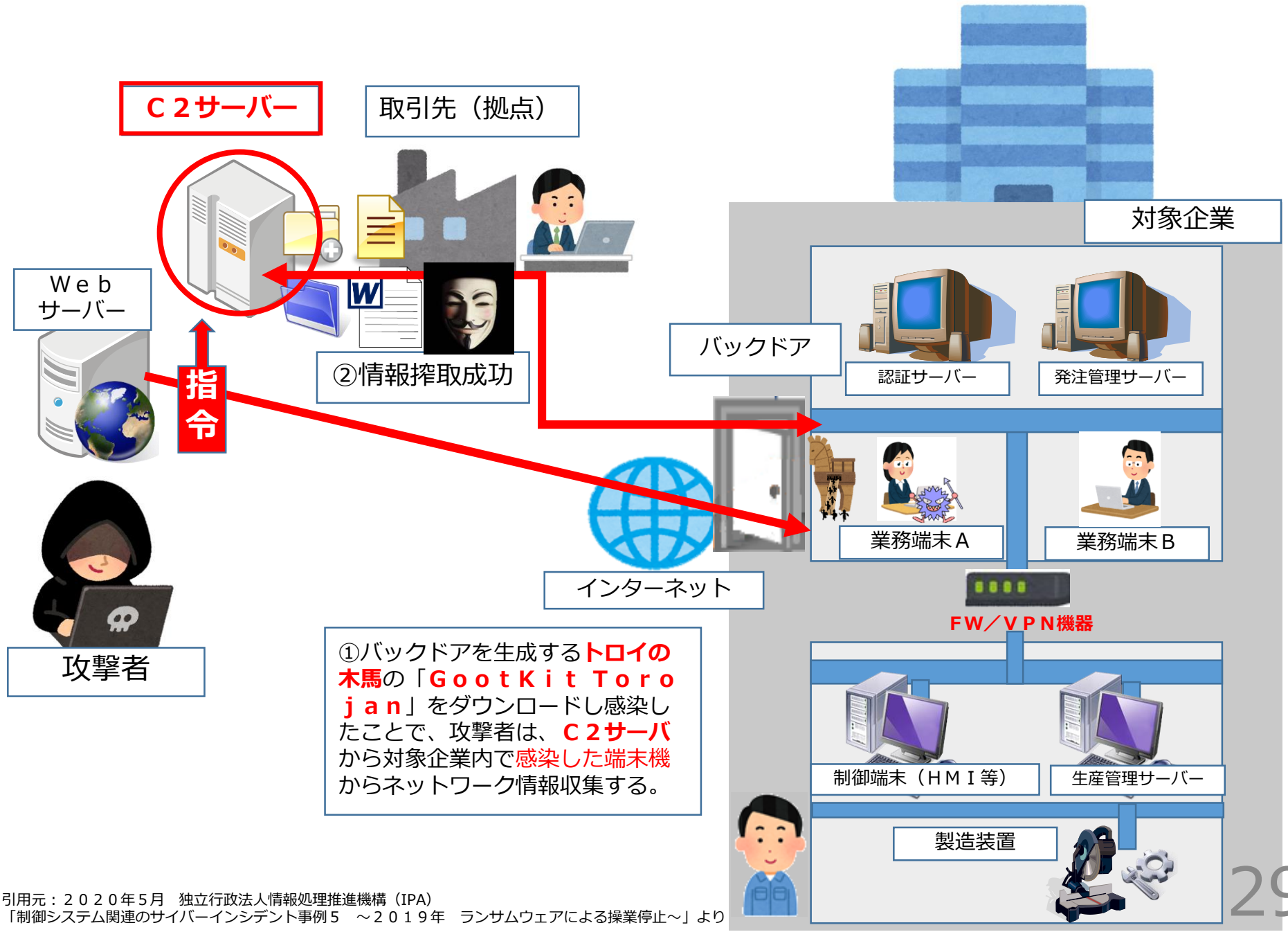


製造装置

※ＧｏｏｔＫｉｔＴｏｒｏｊａｎ
トロイの木馬で、ファイルのダウンロード機能やパスワードの機密情報を収集するアップロードする機能等を持つもの。
このトロイの木馬が生成した「※バックドア」を通じて対象企業ネットワークの情報を収集する。

※バックドア
利用者が入る正規の入口とは別に、ＩＤ・パスワードがなくてもログインできる「勝手口」のようなもの

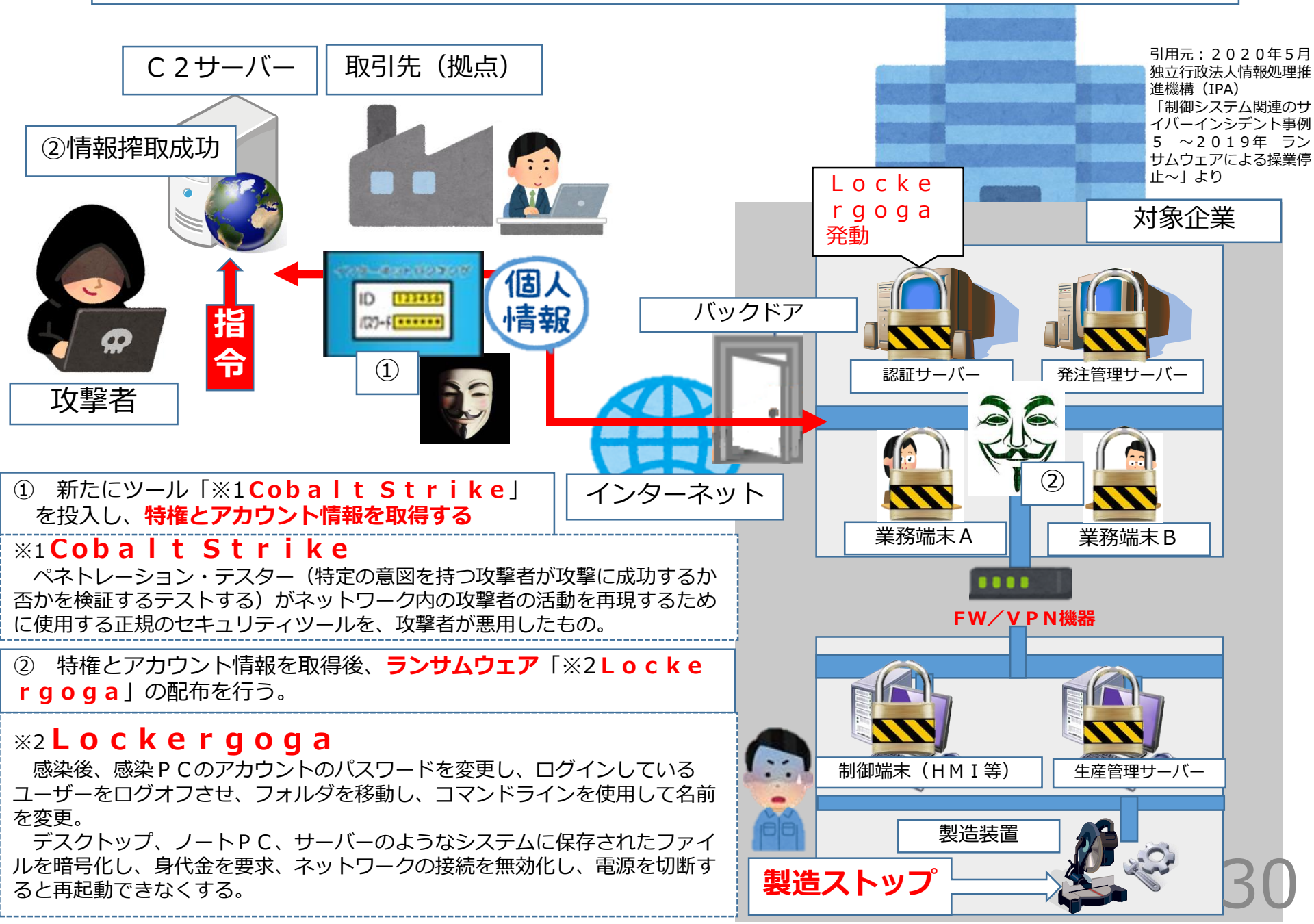
攻撃局面２：対象企業への侵入（対象企業からの情報搾取まで）



①バックドアを生成する**トロイの木馬**の「**ＧｏｏｔＫｉｔ Ｔｏｒｏｊａｎ**」をダウンロードし感染したことで、攻撃者は、**Ｃ２サーバ**から対象企業内で感染した端末機からネットワーク情報収集する。

引用元：２０２０年５月　独立行政法人情報処理推進機構（IPA）
「制御システム関連のサイバーインシデント事例５　～２０１９年　ランサムウェアによる操業停止～」より

攻撃局面３：対象企業への侵入（特権とアカウント窃取、ランサムウェアを仕掛けられるまで）



引用元：２０２０年５月
独立行政法人情報処理推進機構（IPA）
「制御システム関連のサイバーインシデント事例５　～２０１９年　ランサムウェアによる操業停止～」より

① 新たにツール「※1**Ｃｏｂａｌｔ Ｓｔｒｉｋｅ**」を投入し、**特権とアカウント情報を取得する**

※1**Ｃｏｂａｌｔ Ｓｔｒｉｋｅ**
ペネトレーション・テスター（特定の意図を持つ攻撃者が攻撃に成功するか否かを検証するテストする）がネットワーク内の攻撃者の活動を再現するために使用する正規のセキュリティツールを、攻撃者が悪用したもの。

② 特権とアカウント情報を取得後、**ランサムウェア**「※2**Ｌｏｃｋｅｒｇｏｇａ**」の配布を行う。

※2**Ｌｏｃｋｅｒｇｏｇａ**
感染後、感染ＰＣのアカウントのパスワードを変更し、ログインしているユーザーをログオフさせ、フォルダを移動し、コマンドラインを使用して名前を変更。
デスクトップ、ノートＰＣ、サーバーのようなシステムに保存されたファイルを暗号化し、身代金を要求、ネットワークの接続を無効化し、電源を切断すると再起動できなくする。

本資料による代表的な対策・緩和策の例

1．システムのバックアップを作成し、リストの確認を行う

ランサムウェアによって暗号化された場合は、あらかじめバックアップしたデータからリストアするしか確実な対応策しかない。ランサムウェアによっては、共有フォルダや接続された外部の記録媒体のバックアップやボリュームシャドウコピーを削除するものもあるため、バックアップデータをオフラインで保管する。また、定期的なバックアップが取得できているのかの確認も行う。

2．不明または未確認の送信者からの電子メールおよび添付ファイルを開くことに注意する

人的ミスによるところが大きいが、昨今の標的型メールは、ターゲットの組織の関係者を装った内容やアドレスからのものもあるため、既知の人からのメールでもマクロの展開やリンク先のアクセスには十分に注意する必要がある。また、模擬メールによるトレーニングも有効である。

3．システムが最新のパッチで更新されていることを確認する

特に脆弱性を利用したランサムウェア（例えばＷａｎｎａＣｒｙの場合）の一般的な対応策となる。

4．インシデントレスポンスを策定し、トレーニングを行う

緊急時にすぐに対応が可能となるようにすべきことをまとめ、組織の体制を構築し、日常から備えておくという意味である。

5．最小権限の原則の遵守

ユーザーが職務を遂行するための必要最小限のアクセスレベルで設定する。

引用元：２０２０年５月　独立行政法人情報処理推進機構（IPA）「制御システム関連のサイバーインシデント事例５　～２０１９年ランサムウェアによる操業停止～」より

制御システムのセキュリティリスク分析ガイド補足資料

制御システム関連のサイバーインシデント事例5

～2019 年 ランサムウェアによる操業停止～

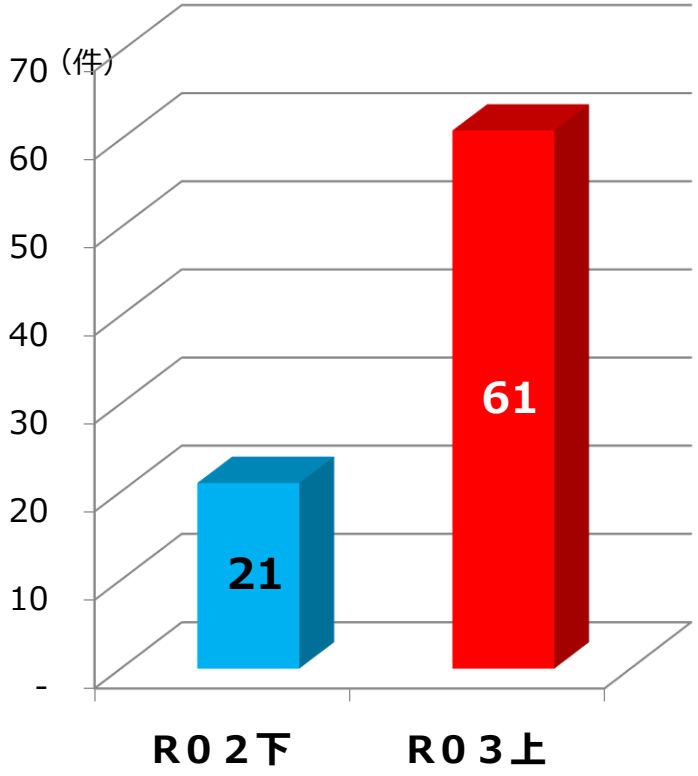
2020 年 3 月

IPA 独立行政法人情報処理推進機構
セキュリティセンター

引用元：２０２０年５月　独立行政法人情報処理推進機構（IPA）「制御システム関連のサイバーインシデント事例５　～２０１９年ランサムウェアによる操業停止～」より

国内のランサムウェアの情勢

【企業・団体等におけるランサムウェア被害の報告件数の数位】

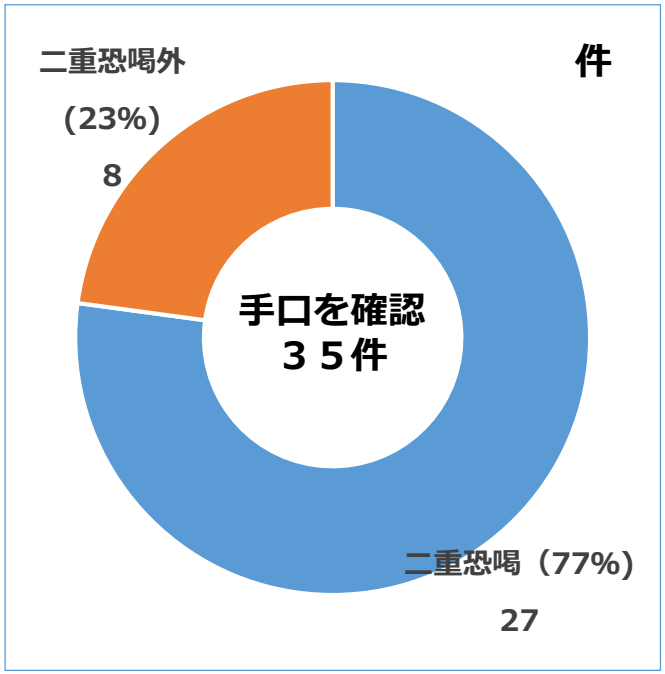


○　従来のランサムウェアは、不特定多数の利用者狙って電子メールを送信するといった手口が一般的であったが、現在では、VPN機器からの侵入等、特定の個人や企業・団体等を標的とした手口に変化しており、企業のネットワーク等のインフラを狙うようになっている。

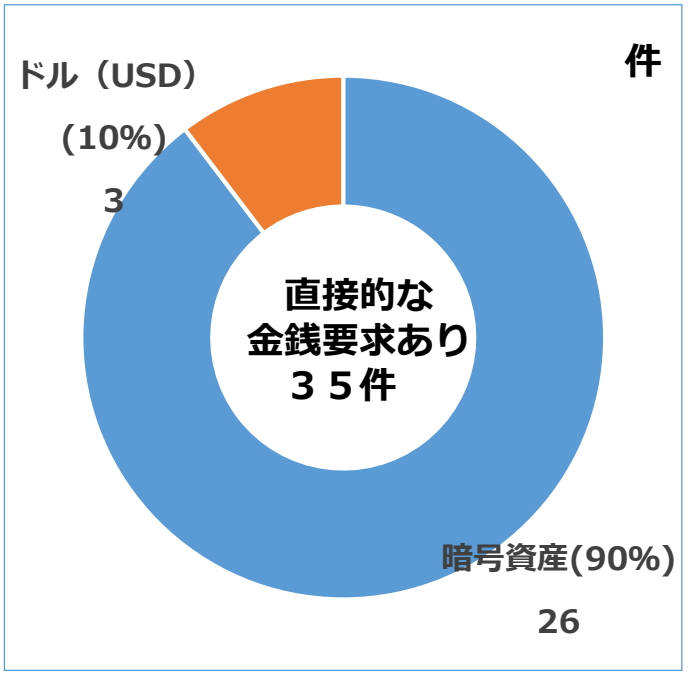
○　最近の事例では、データの暗号化のみならず、データを窃取した上、企業等に対し「対価を払わなければ該当データを公開する」などと金銭を要求する二重恐喝（ダブルエクストーション）という手口を認められるようになっている。

出典元：警察庁「令和３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」

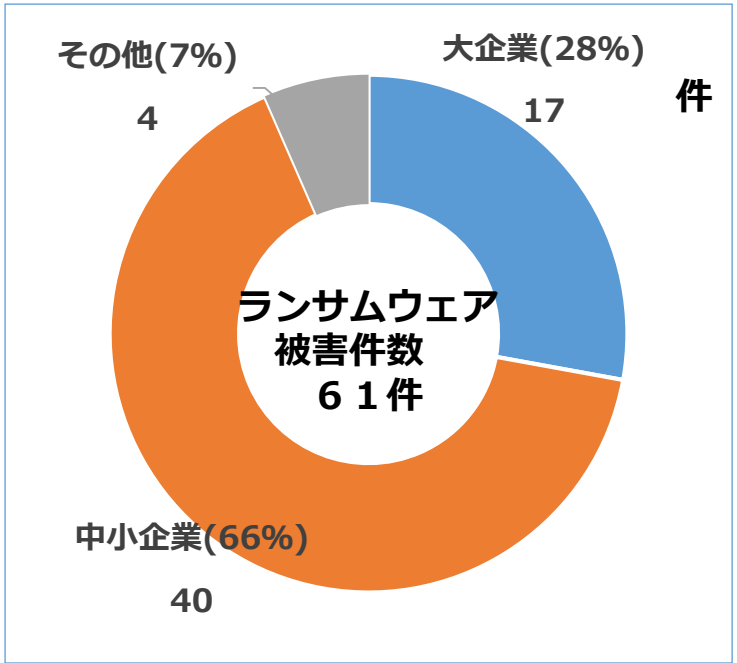
【ランサムウェア被害の手口別報告件数】



【要求された金銭支払い方法別報告件数】

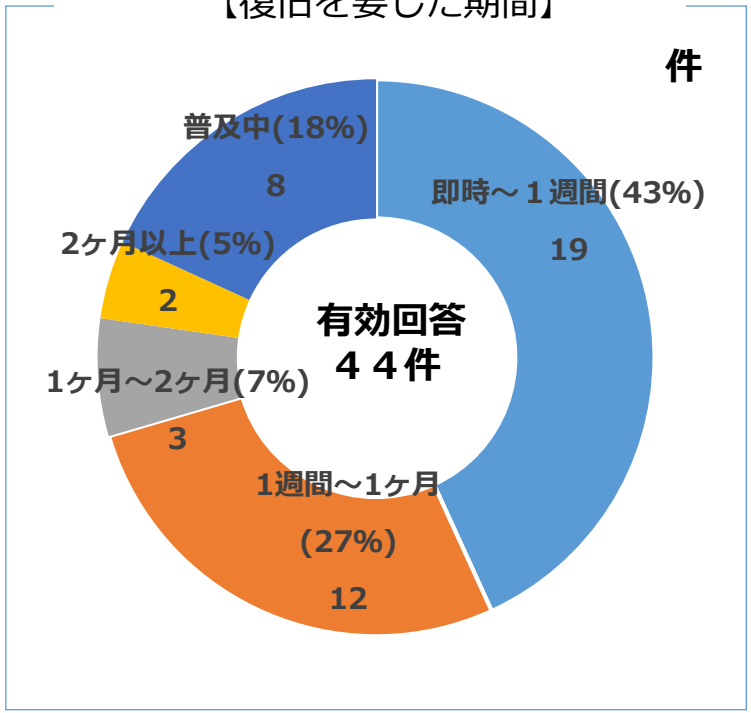


【ランサムウェア被害の被害企業・団体等の規模別報告件数】

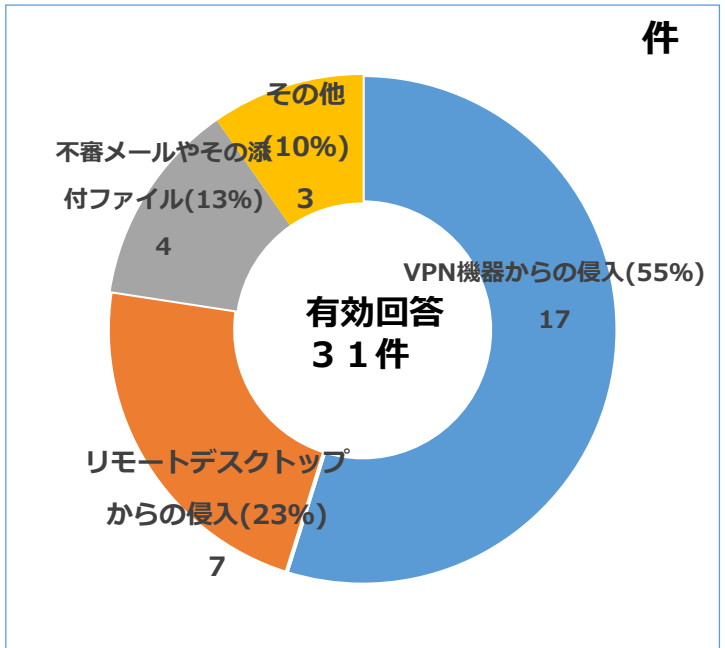


出典元：警察庁「令和３年上半期におけるサイバー空間をめぐる脅威の情勢等について」

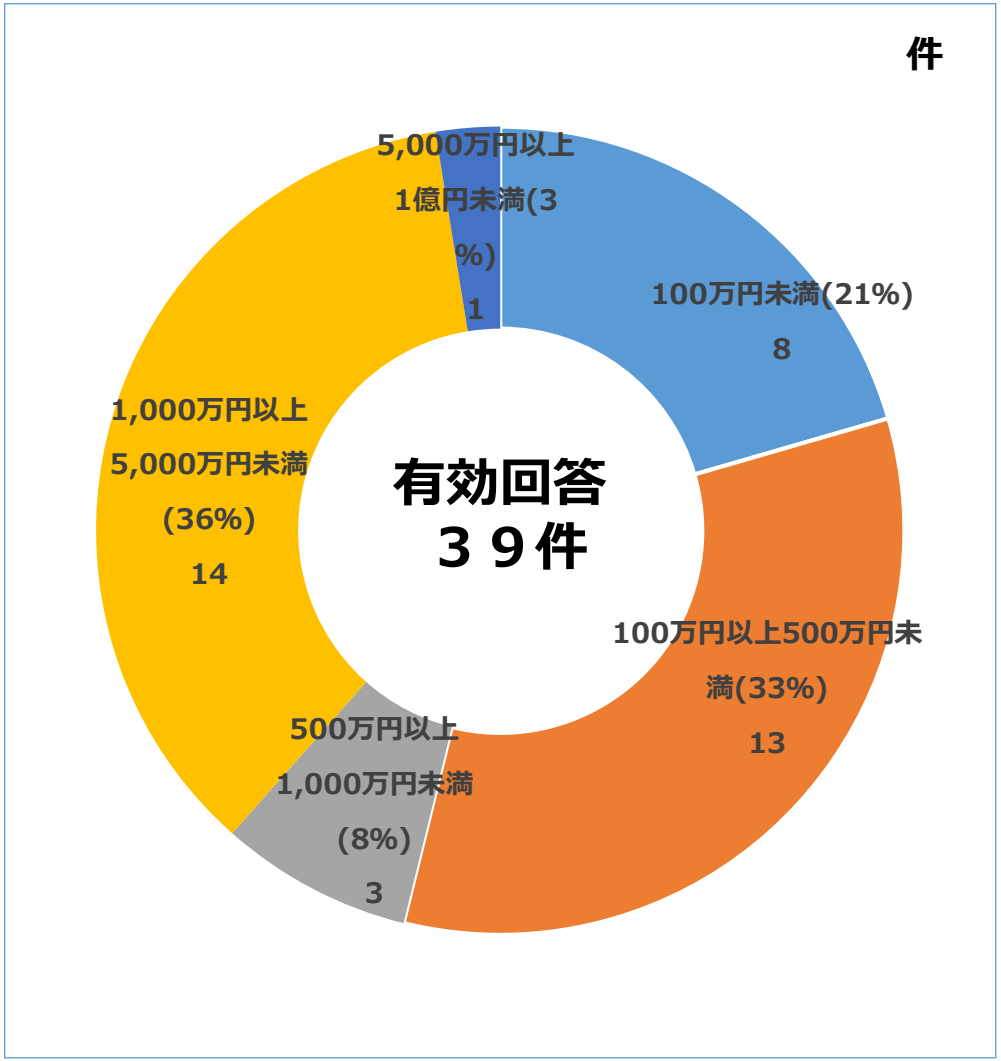
【復旧を要した期間】



【感染経路】



【調査・復旧費用の総額】



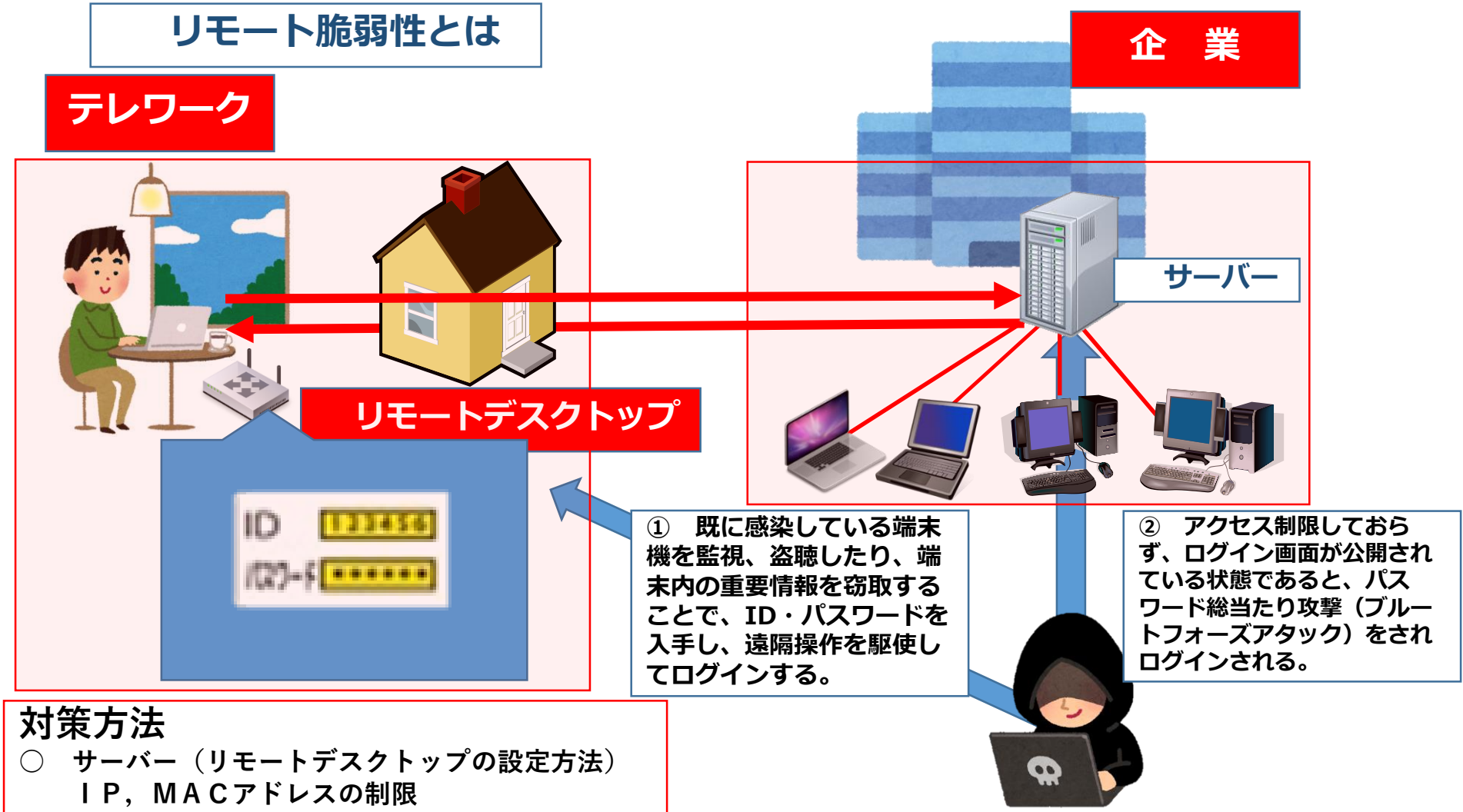
出典元：警察庁「令和３年上半期におけるサイバー空間をめぐる脅威の情勢等について」

VPN脆弱性攻撃とは

対策方法

- 使用しているＶＰＮの脆弱性報告の有無を逐一確認する。脆弱性情報があった場合は、必ず対処するだけでなく、パスワード変更等を行い徹底する。
- ＶＰＮ－ＧＷを隠蔽する（ゼロトラストセキュリティ機器を導入し、通信制限をかける）
- 不正アクセス検出を可視化する仕組みにする。（ログイン失敗履歴や海外からのログイン履歴など）

リモート脆弱性とは



対策方法

○　サーバー（リモートデスクトップの設定方法）
　　ＩＰ，ＭＡＣアドレスの制限
　　ログイン試行回数の制限
　　イベントログの常時取得
　　パスワードのきめ細かな更新
○　端末機（テレワーク）
　　ＯＳ、ウイルスソフトを最新化する
　　ＩＤ、パスワードをＰＣ内に保管しない
　　重要データは暗号化しておく
　　接続時にＳＭＳ等を利用した二要素認証

最も危険な**ランサムウェア**　ベスト**5**

1, **Ｍａｚｅ（メイズ）**（別名：ＣｈａＣｈａ）
　２０１９年に初めて存在が確認されて以降、瞬く間にトップクラスになったランサムウア。
　ランサムウェア被害総数のうち、Ｍａｚｅは1／３以上を占める。
　身代金の支払いに応じない被害者に対し、「支払わなければ、盗んだファイルを公開する」と脅す手口の二重恐喝の先駆けで、後のランサムウェアの攻撃者はこの方法を取り入れた。
　実際に脅すだけではなく、盗んだデータをとあるフォーラムで公開した。

2，**Ｃｏｎｔｉ（コンティ）**（別名：ＩＯＣＰ）
　２０１９年の終わりごろに出現、２０２０年を通じて猛威を振るった。
　標的になった企業に対し、身代金と引き換えにセキュリティ強化の支援を提案する。
　Ｍａｚｅと同様、ファイルを暗号化するだけでなく、不正侵入したシステムから、ファイルのコピーを犯罪者グループに送信、要求に応じなければこのファイルをインターネット上に公開する。

3，**Ｒｅｖｉｌ（レビル）**（別名：Ｓｏｄｉｎ又はＳｏｄｉｎｏｋｉｂｉ）
　２０１９年初めにアジアで確認され、正当なプロセッサー機能を利用してセキュリティシステムによる検知を回避するなど、このランサムウェアを巧みな技術はたちまちエキスパートたちの注意を引くこととなった。
　このマルウェアのコードには、リース用に作成されたことを示す特徴的な兆候があり、攻撃を受けた業種は約２０に及び、一番被害が多かったのは生産・製造（約３０％）だった。
　また、犯罪者グループは２０２１年３月、Acerに5,000万ドル（約５５億円）を要求し、現時点では身代金最高額となった。

4，**Ｎｅｔｗａｌｋｅｒ（ネットウォカー）**（別名：Ｍａｉｔｏ）
　標的には物流大手、企業グループ、エネルギー企業その他の大企業が連ねている。２０２０年のわずか数ヶ月の間に、このサイバー犯罪者グループは２，５００万ドル（２７億５，０００万円）を超える利益をあげた。
　この作成者たちは、単独で詐欺活動する者に対し、攻撃で得た利益の一部と引き換えにNetwalkerのリース契約を提案する。こういったビジネスモデルおいて契約の中身は身代金の７０％に達していたと言われている。
　２０２１年１月に検挙されるまで、これを操る攻撃者のグループは、意図を明確に示すため、高額送金のスクリーンショットを公開、リース手続きが円滑に進むように、盗んだデータを身代金支払い期限後に公開するWebサイトまで開設していた。

5, **Ｄｏｐｐｅｌｐａｙｍｅｒ（ドッペルペイマー）**
　この作成者達は、バイキング型トロイの木馬であるDridexやBitPaymerなど、他のマルウェアを作りだしている。
　この攻撃を受けた企業は、電子機器メーカー、自動車メーカー、中南米の大手石油会社などである。
　この他、医療、救急、教育関連その他政府機関も、世界各地でたびたび標的となっている。
　米国ペンシルベニア州デラウェア群に５０万ドル支払わせた件があり、更に２０２１年２月、欧州の研究機関がハッキングを受けた旨の発表をしている。

引用元：カスペルスキー公式ブログ「企業狙いのランサムウェア：活動の活発な５つの犯罪者グループ」より

3．サポート詐欺

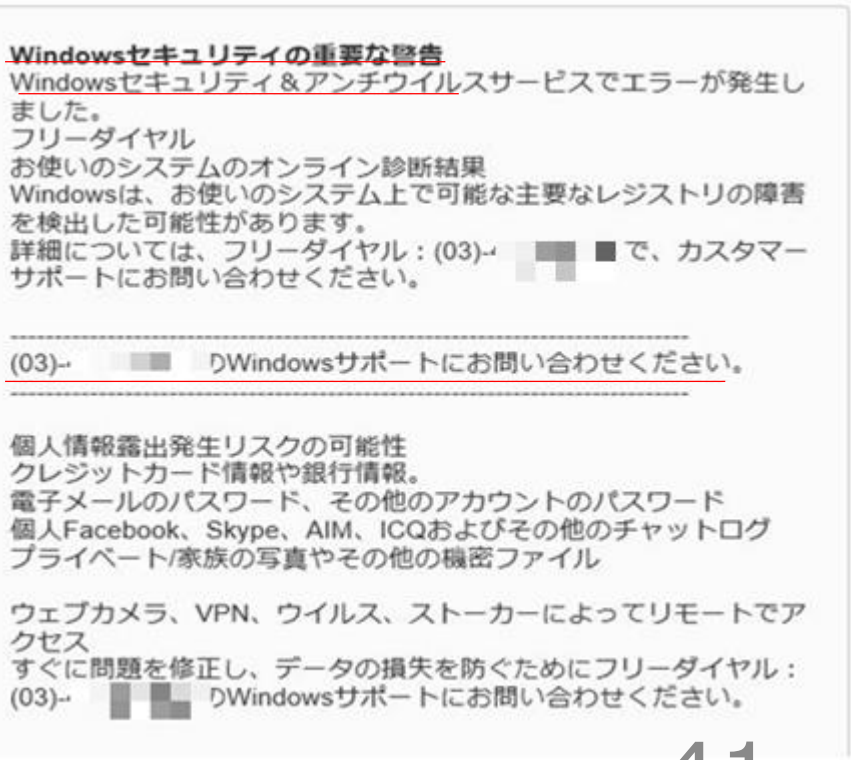
サポート詐欺

パソコンやスマートフォンの、突然警告音が鳴り、画面に「ウイルスの感染しました、削除するには０３-●●●●-●●●●に電話をしてください」「ウイルスソフトをすぐインストールしてください」等のメッセージが表示されたり、更にその内容の音声等が流れて不安を煽り、嘘の有償サポート契約やウイルスを隠したセキュリティソフトをダウンロードさせ、ウイルス感染をさせるとともに、金銭、個人情報等を騙しとるもの。

サポート詐欺

偽の警告画面が表示された

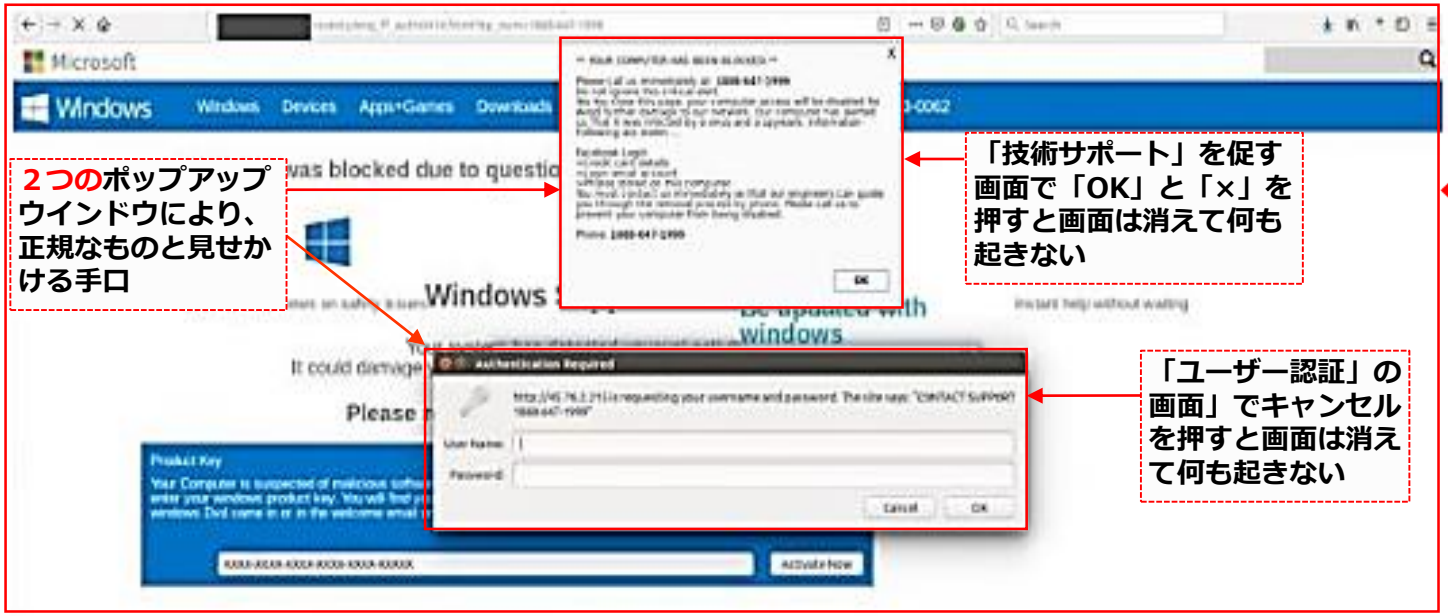
ネットをしていたら、急に警告画面が出て、警告音や日本語のメッセージが流れてきた。画面が消えないので仕方なく表示された番号に電話したら、遠隔操作用ソフトをインストールするよう言われ、お金まで請求された。



引用元：トレンドマイクロ「セキュリティブログ」より

サポート詐欺

正規ツール「iframe」悪用



サポート詐欺活動で使用されているフリーズした偽のMicrosoftサポート窓口

今までのベーシック認証のポップアップと、HTMLの「**iframe**」を使った要素を組み合わせて、ブラウザを操作不能にする攻撃です。
（トレンドマイクロ　is702「サポート詐欺新手法、正規ツール「iframe」悪用事例登場より）

「Iframe」（アイフレーム若しくはインラインフレーム）とは、Webサイトに外部のWebサイト（HP、地図、写真、動画）を埋め込み、その画面を表示させ、クリックするとそのURLにアクセスすることができるプログラム
※例　HP上にYouTube、GoogleMapを表示
枠以外のデザインを変更する「JavaScript」を使用

2019年5月29日付　トレンドマイクロ　is702「サポート詐欺で新手法、正規ツール「iframe」悪用事例登場」より

マイクロソフトを騙るサポート詐欺（２０２１年1月２９日、2月４日公表）

主な騙す言葉として、

『このＰＣへのアクセスはブロックされました』

『このウィンドウを閉じると、個人情報が危険にさらされＷｉｎｄｏｗｓ登録が停止されます』

『この重要な警告を無視しないでください』

『Ｔｒｏｊａｎスパイウェアアラート-エラーコード#0x898778』

が突然表示される。

引用元：Microsoft　「２０２１年１月２９日マイクロソフトを装った詐欺にご注意ください」より

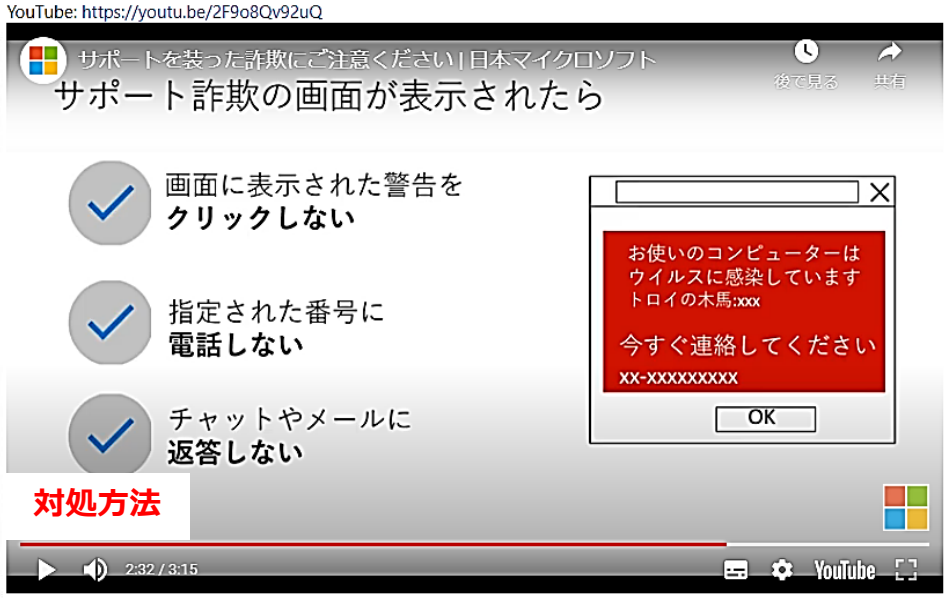
マイクロソフト社からの注意喚起と対策　※約３分間の動画

YouTube: https://youtu.be/2F9o8Qv92uQ

YouTube: https://youtu.be/2F9o8Qv92uQ

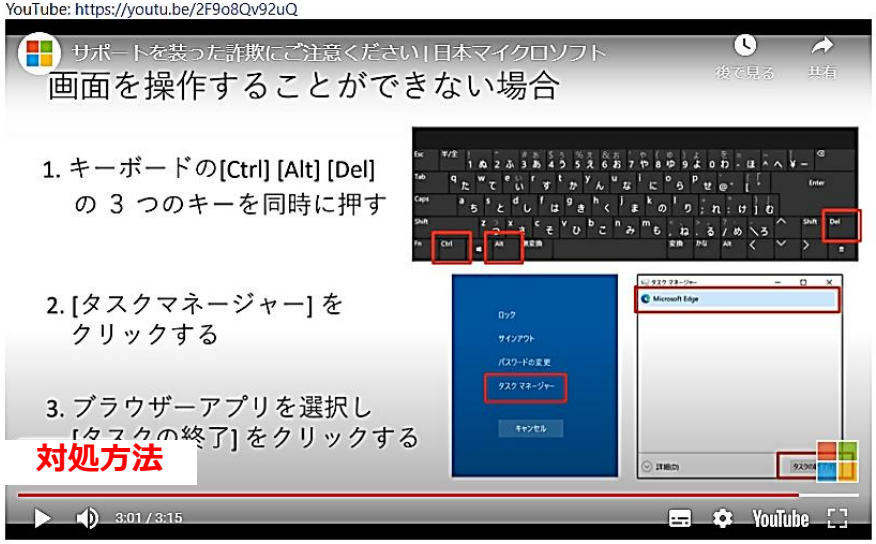
YouTube: https://youtu.be/2F9o8Qv92uQ

YouTube: https://youtu.be/2F9o8Qv92uQ



画面：ＹｏｕＴｕｂｅ　日本マイクロソフト公式チャンネル「サポートを装った詐欺にご注意ください」より

YouTube: https://youtu.be/2F9o8Qv92uQ



YouTube: https://youtu.be/2F9o8Qv92uQ

サポート詐欺は、パソコンだけとは限りません。
普段使用しているスマホでも被害が出ています。

画面：ＹｏｕＴｕｂｅ　日本マイクロソフト公式チャンネル「サポートを装った詐欺にご注意ください」より

サポート詐欺（iPhoneを狙った手口）

iPhoneで偽のセキュリティ警告からのアプリのインストールへ誘導する手口登場

アプリに誘導する目的は不明ですが、「利用者にアプリをインストールさせることによる報酬」を得ようとするアプリウエア（成果報酬広告）と見られている、なお、セキュリティ警告の出力元（広告主）と誘導されるアプリの開発元との関係は不明

拡大

アプリへ誘導

2019年5月から「iOS」をターゲットにしたサポート詐欺が急増してます
中にはアプリへ誘導だけでなく、更に自動継続課金へ誘導するものもあります

2019年9月18日　IPA「スマートフォンで、偽のセキュリティ警告からアプリインストールへ誘導する手口に注意」～意図をせずアプリの自動継続課金の契約をしていないか、確認を～より

サポート詐欺（Androidを狙った手口）

Androidで偽のセキュリティ警告からのアプリのインストールへ誘導する手口登場

「Android」を狙ったサポート詐欺は、２０１６年に増加し、２０１８年には減少しましたが、いつ流行してもおかしくはありませんので要注意です

2019年9月18日　IPA「スマートフォンで、偽のセキュリティ警告からアプリインストールへ誘導する手口に注意」～意図をせずアプリの自動継続課金の契約をしていないか、確認を～より

サポート詐欺対策

- 慌てて、表示された画面の電話番号に電話をしたり、画面の指示に従って安易にウイルスソフトと称するものをインストールしないようにしましょう（電話番号やサイト・ソフト名を検索エンジンにて確認するとサポート詐欺であることが判明する場合があります）。

- パソコン、スマートフォンの電源を切る若しくは再起動する（通常の状態に戻る可能性が高い）。
  それでも消えない場合は、システム「タスクマネージャー（Ｃｔｒｌ＋Ａｌｔ＋Ｄｅｌ）」から「ブラウザを終了」を利用して終了する。

- 誘導された画面のソフトをインストールをしてしまった場合は、「アンインストール」をして完全削除するか、ソフトウエアをインストールする前の状態（システムの復元）にする。

- 契約しているセキュリティベンダー、Tcyss相談窓口に電話相談して情報収集をする。

４．お知らせ

企業の皆様へ　サイバー犯罪の被害は警察に相談を！

サイバー犯罪の実態を明らかにし、被害を拡大させないためには、被害を潜在化させないことが重要です。

被害にあわれたら、悩まずに最寄りの警察署へ相談して下さい。

警察に寄せられたサイバー犯罪に関する情報を分析し、事件捜査を行うほか、被害企業における対策に必要な情報提供・助言、他の企業等への被害拡大を防止するための注意喚起等の被害防止するための取組を行っています。

警察では、サイバー犯罪に対する様々な対策を行っています

企業の皆様からの情報提供がサイバー空間の安全につながります

サイバー犯罪に関する情報の分析

サイバー犯罪事件の捜査

被害の拡大防止・再発防止

サイバーセキュリティに関して日ごろ見ている
サイト、下の９つのうち何個かありますか？

① @police　　② 警視庁Twitter
③ 東京都産業労働局
④ 情報処理推進機構（IPA）
⑤ 内閣ｻｲﾊﾞｰｾｷｭﾘﾃｨｾﾝﾀｰ（NISC）
⑥ ﾌｨｯｼﾝｸﾞ対策協議会
⑦ JPCERTｺｰﾃﾞｨﾈｰｼｮﾝｾﾝﾀｰ（JPCERT/CC）
⑧ is702　　⑨ ﾏﾙｳｪｱﾚﾎﾟｰﾄ

① @police http://www.npa.go.jp/cyberpolice/

② 警視庁Twitter
https://twitter.com/MPD_cybersec

③ 東京都産業労働局
http://www.sangyo-rodo.metro.tokyo.jp/chushou/shoko/cyber/

④ 情報処理推進機構（IPA）
http://www.ipa.go.jp/security/

⑤ 内閣ｻｲﾊﾞｰｾｷｭﾘﾃｨｾﾝﾀｰ（NISC）
http://www.nisc.go.jp

⑥ ﾌｨｯｼﾝｸﾞ対策協議会
https://www.antiphishing.jp/

⑦ JPCERT/CC
https://www.jpcert.or.jp/

⑧ is702
https://www.is702.jp/

⑨ ﾏﾙｳｪｱﾚﾎﾟｰﾄ
https://eset-info.canon-its.jp/malware_info/malware_topics/

CS対策本部リーフレット

サイバー犯罪防止啓発動画のご案内

◆ 企業にDVDの貸出を行っています（数に限りがあります）
◆警視庁ホームページで視聴出来ます
警視庁トップページ＞警視庁について＞情報発信＞動画ライブラリー＞サイバー
◆ 「You Tube」警視庁公式チャンネルにも公開しています
警視庁トップページ＞警視庁SNS・動画＞「You Tube」警視庁公式チャンネル

＜平成29年度＞

◆ エピソード１：経営者編 （8分39秒）
◆ エピソード２：システム管理者編 （6分53秒）
◆ エピソード３：一般社員編 （6分03秒）

＜最新版＞

◆ テーマ１：情報流出防止対策 (12分34秒)
◆ テーマ２：詐欺被害防止対策 (11分46秒)
◆ テーマ３：まさか自分が加害者に (10分06秒)

※　その他警視庁サイバー部門で
作成の動画多数あり!!

サイバー犯罪啓発短編動画

令和元年度制作（約５分）
「サイバーセキュリティがあなたを救う」
◆中小企業が狙われる理由
◆中小企業のサイバーセキュリティ対策の必要性
◆中小企業が狙われるサイバー犯罪
※セミナー公開用動画

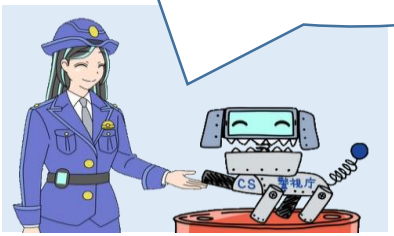
令和２年度制作（約１分４０秒）
「そのテレワーク、犯罪者が狙っている」
◆テレワークで守ってほしい大事なこと
- **OSは最新の状態に**
- **ウイルス対策ソフトの導入**
- **パスワード複雑に、使い回ししない**
- **Ｗｉ－Ｆｉルーターの管理者設定を適切に**
- **利用するサテライトオフィスのＷｉ－Ｆｉスポットは安全？**
- **ファイル共有機能はオフにする**
- **席を離れない、覗かれないようにする**

◆警視庁ホームページで視聴出来ます
警視庁トップページ＞警視庁について＞情報発信＞動画ライブラリー＞サイバー
◆「You Tube」警視庁公式チャンネルにも公開しています
警視庁トップページ＞警視庁SNS・動画＞「You Tube」警視庁公式チャンネル

サイバーセキュリティ啓発
短編アニメ動画

「短い」、「たのしい」、「わかりやすい」サイバーセキュリティ短編アニメーション映像（６話）を公開してます。

ぜひ一度ご覧ください。



①標的型攻撃

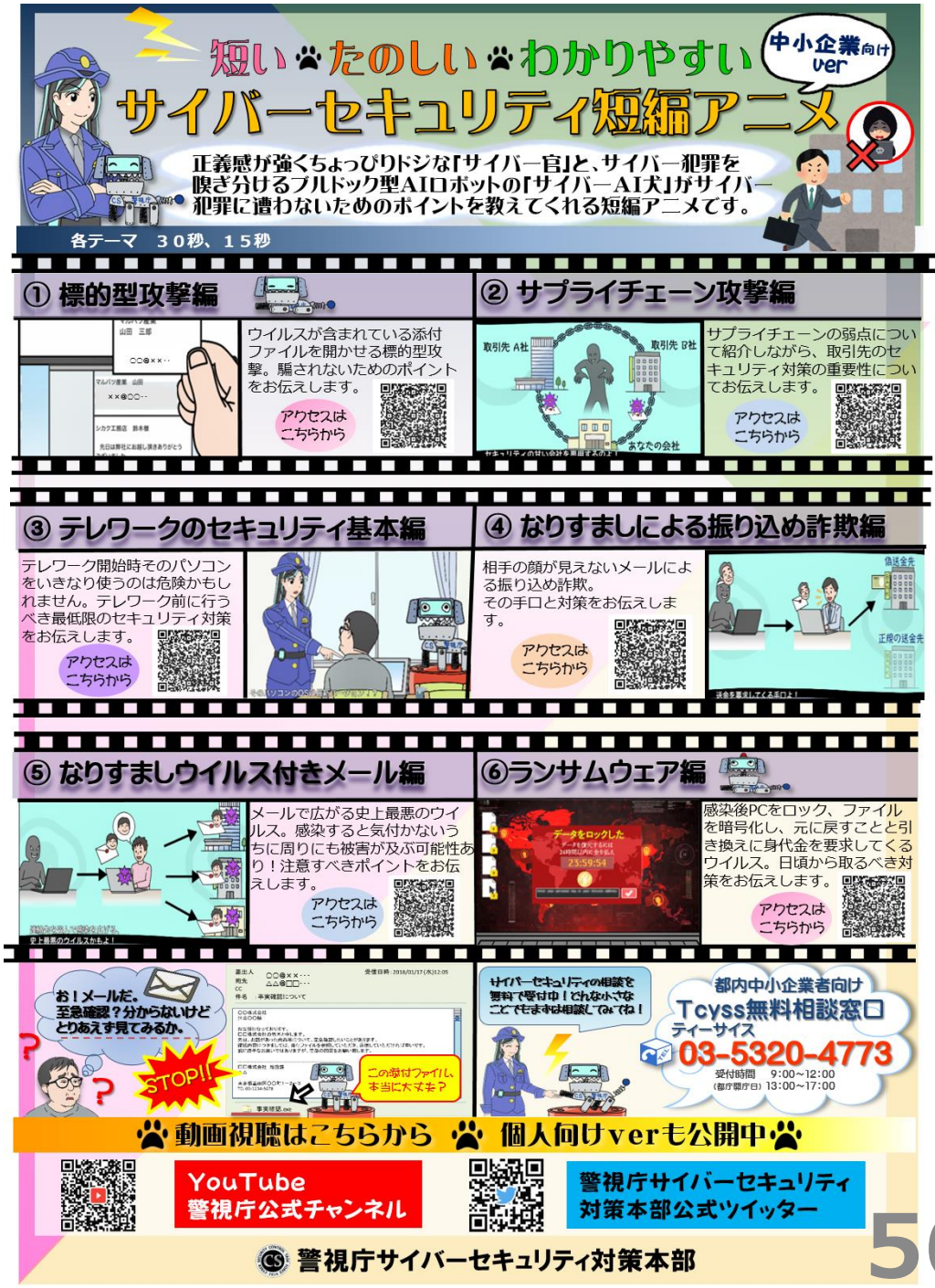
②サプライ

③テレワーク

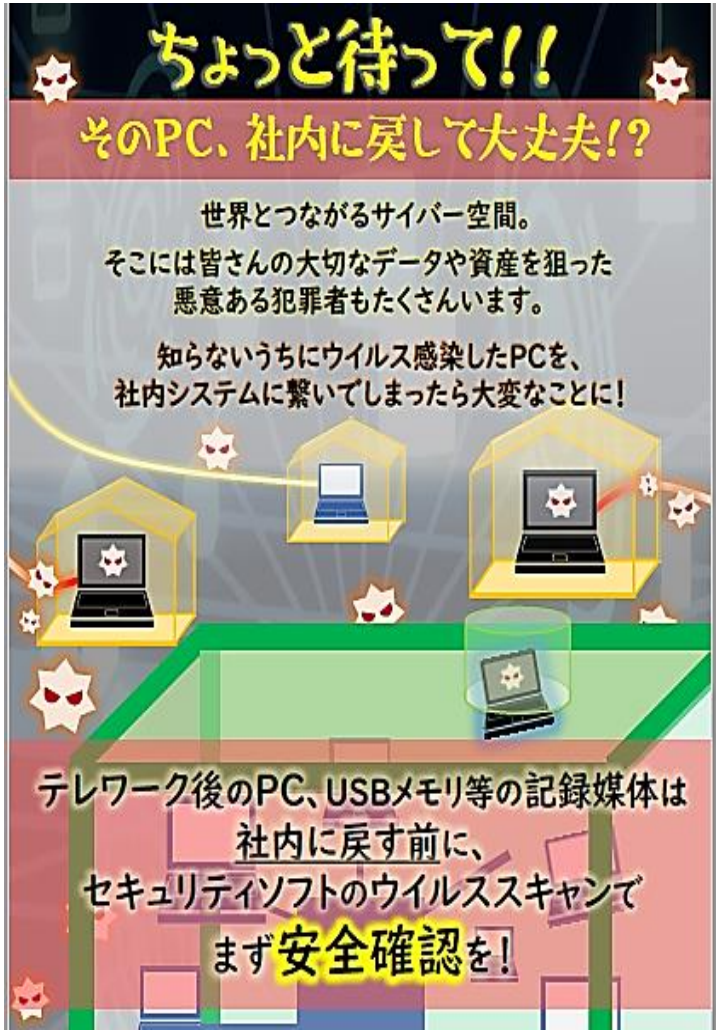
④なりすまし（振り込め）

⑤なりすまし（ウイルス）

⑥ランサム



テレワークに関する広報資料



その他の対策は、警視庁ホームページを確認
(Twitter、You Tube他)

https://www.keishicho.metro.tokyo.lg.jp/

トップページ→安全な暮らし→情報セキュリティ広場→注目情報
→テレワーク勤務のサイバーセキュリティ対策

サイバー保険取り扱い事業者

あいおいニッセイ同和損害保険株式会社

アリアンツ火災海上保険株式会社

ＡＩＧ損害保険株式会社

ＨＤＩ Ｇｌｏｂａｌ 保険会社

共栄火災海上保険株式会社

損害保険ジャパン日本興亜株式会社

大同火災海上保険株式会社

Ｃｈｕｂｂ 損害保険株式会社

東京海上日動火災保険株式会社

三井住友海上火災保険株式会社

(注)50音順で掲載

日本損害保険協会

一般社団法人 日本損害保険協会 The General Insurance Association of Japan SONPO

外国損害保険協会

一般社団法人 外国損害保険協会 FNLIA Foreign Non-Life Insurance Association of Japan

サイバー保険

サイバー保険特設サイト