



# 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

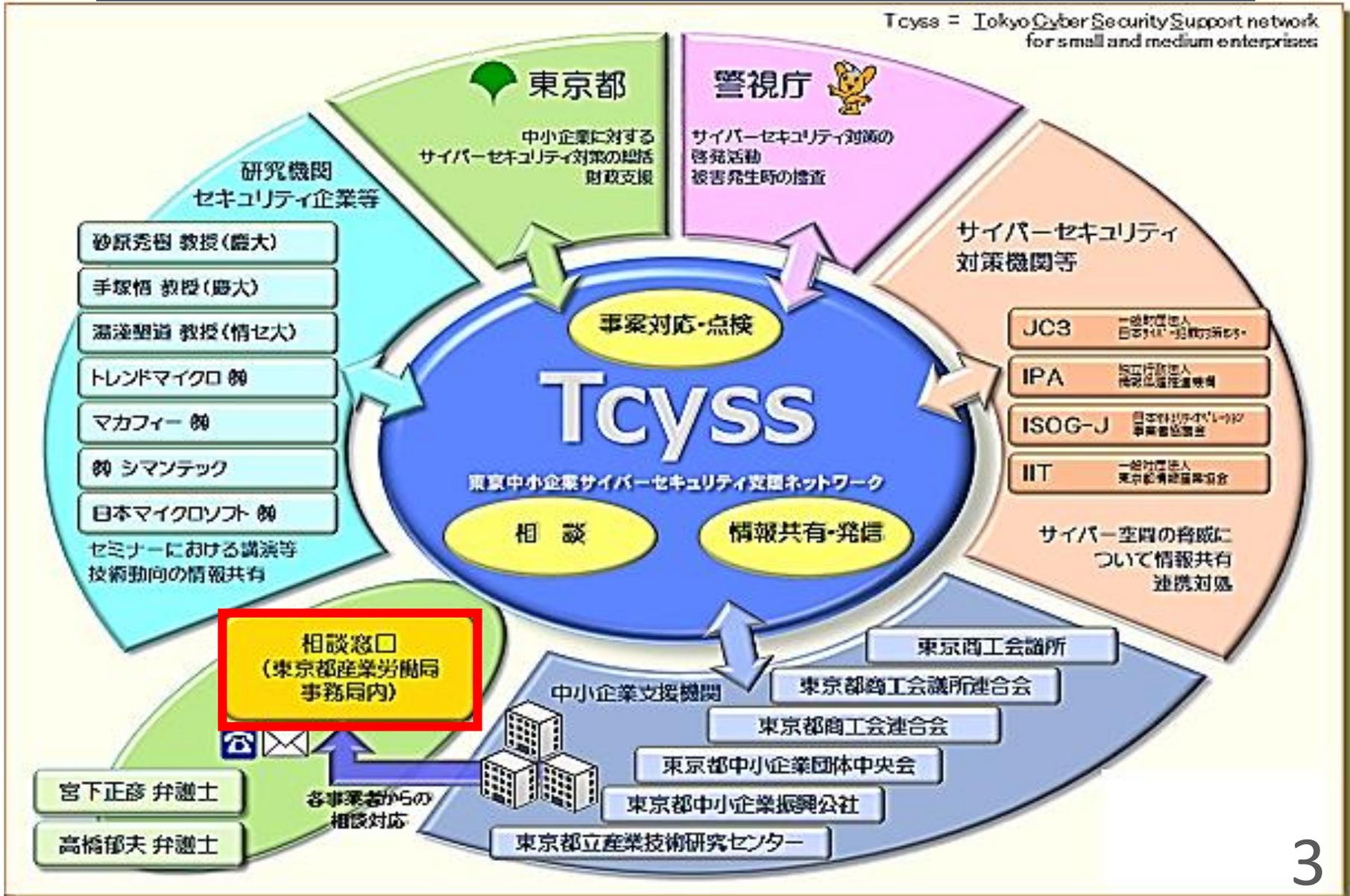
# T c y s s

(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～

Tcyss = Tokyo Cyber Security Support network for small and medium enterprises



# 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)



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



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。**

## 中小企業 サイバーセキュリティ 相談窓口

ポリシーの策定 ウイルス感染 情報流出 セミナーの依頼

東京都では、都内の中小企業者等を対象とした、サイバーセキュリティに関する**無料相談窓口**を開設しています。  
相談窓口では、情報セキュリティ対策の強化や情報流出事案、セキュリティポリシーの策定等に関する相談をお受けしています。  
相談内容により、警視庁、中小企業支援機関、サイバーセキュリティ対策機関等と連携して対応しますので、お気軽にご相談ください。

**まずは相談!!** 電話・窓口受付時間 9:00～12:00  
都庁開庁日 13:00～17:00

窓口でのご相談 ▶ 東京都産業労働局商工部 相談窓口  
(東京都新宿区西新宿2-8-1 都庁第一本庁舎20階北側)

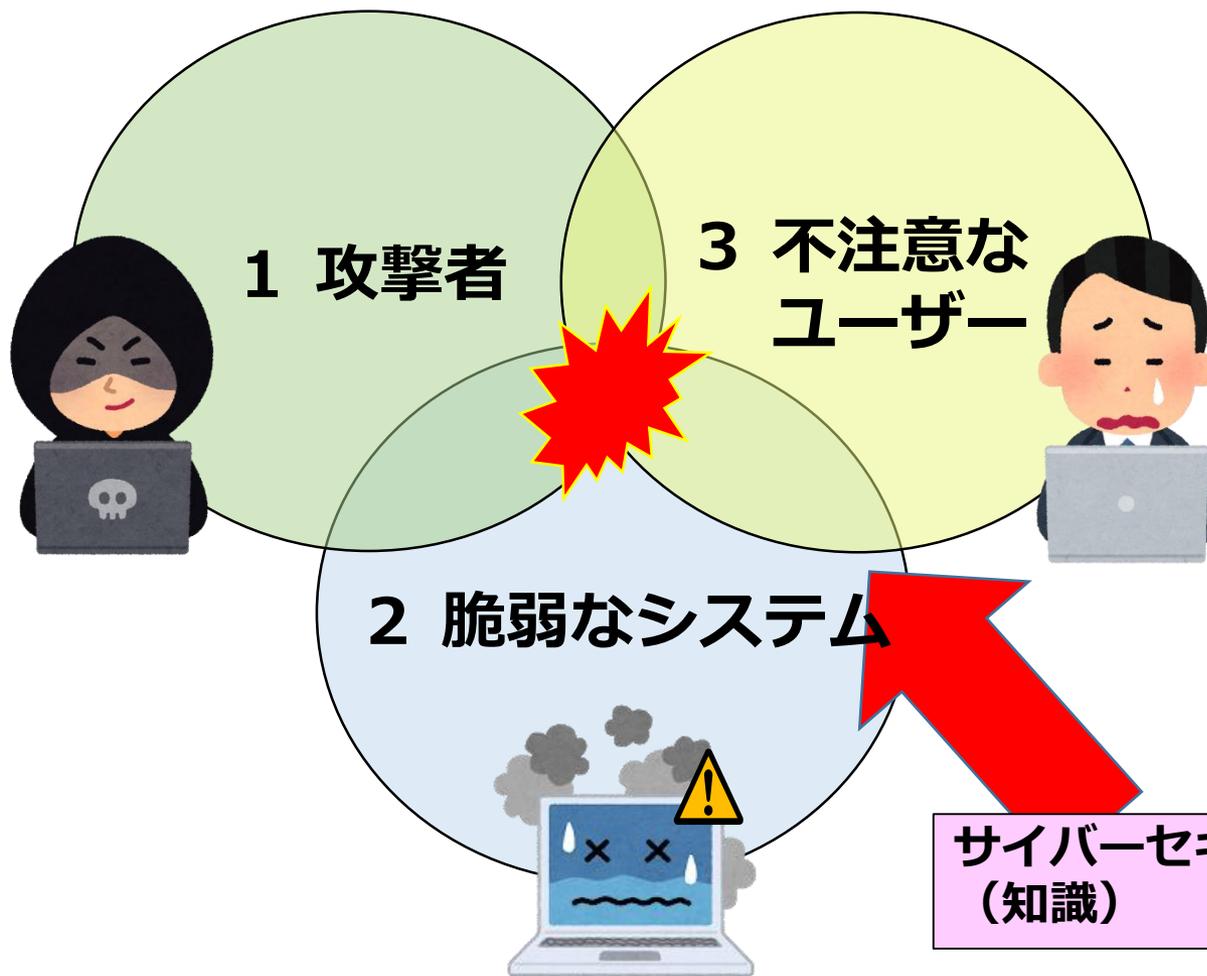
電話・Webサイト専用フォームでのご相談 ▶

**☎ 03-5320-4773**

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

東京都産業労働局

# 被害に遭う3つの要因



# — 本日のお話（目次） —

## 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	ランサムウェアによる被害	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

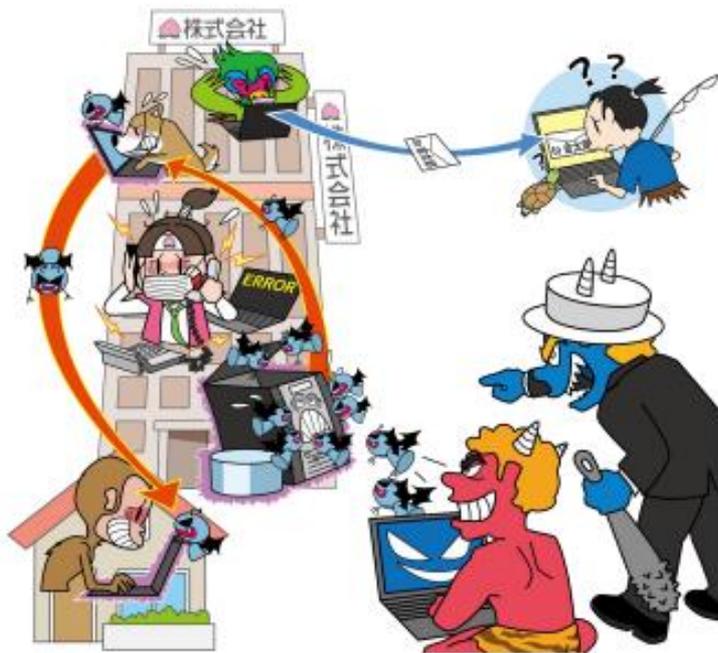
# 情報セキュリティ10大脅威 2021

毎年公表されています。

情報セキュリティ

## 10大脅威 2021

～よもや自組織が被害に！呼吸を合わせて全力防御！～



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

2021年2月

### 目次

はじめに	4
情報セキュリティ10大脅威 2021	5
1. 情報セキュリティ10大脅威（個人）	11
1位 スマホ決済の不正利用	12
2位 フィッシングによる個人情報等の詐取	14
3位 ネット上の誹謗・中傷・デマ	16
4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	18
5位 クレジットカード情報の不正利用	20
6位 インターネットバンキングの不正利用	22
7位 インターネット上のサービスからの個人情報の窃取	24
8位 偽警告によるインターネット詐欺	26
9位 不正アプリによるスマートフォン利用者への被害	28
10位 インターネット上のサービスへの不正ログイン	30
コラム：2020年も引き続き猛威を振るったEmotet、今後は・・・	32
2. 情報セキュリティ10大脅威（組織）	35
1位 ランサムウェアによる被害	36
2位 標的型攻撃による機密情報の窃取	38
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	40
4位 サプライチェーンの弱点を悪用した攻撃	42
5位 ビジネスメール詐欺による金銭被害	44
6位 内部不正による情報漏えい	46
7位 予期せぬIT基盤の障害に伴う業務停止	48
8位 インターネット上のサービスへの不正ログイン	50
9位 不注意による情報漏えい等の被害	52
10位 脆弱性対策情報の公開に伴う悪用増加	54

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。

# センサー検知アクセス件数の推移（年別）

件/1日

ポートスキャン（検索行為）とは  
リモートデスクトップサービス等で通信の  
やり取りをする出入口の不備（脆弱部）を  
探す行為

約13.2秒に1回

約4分38秒に1回

2013年9月8日 東京オリンピック開催地決定

316.3 件

252.9 件

269.7 件

310.1 件

491.6 件

729.3 件

1,692.0 件

1,893.0 件

2,752.8 件

4,192.0 件

6,506.4 件

2010年

2011年

2012年

2013年

2014年

2015年

2016年

2017年

2018年

2019年

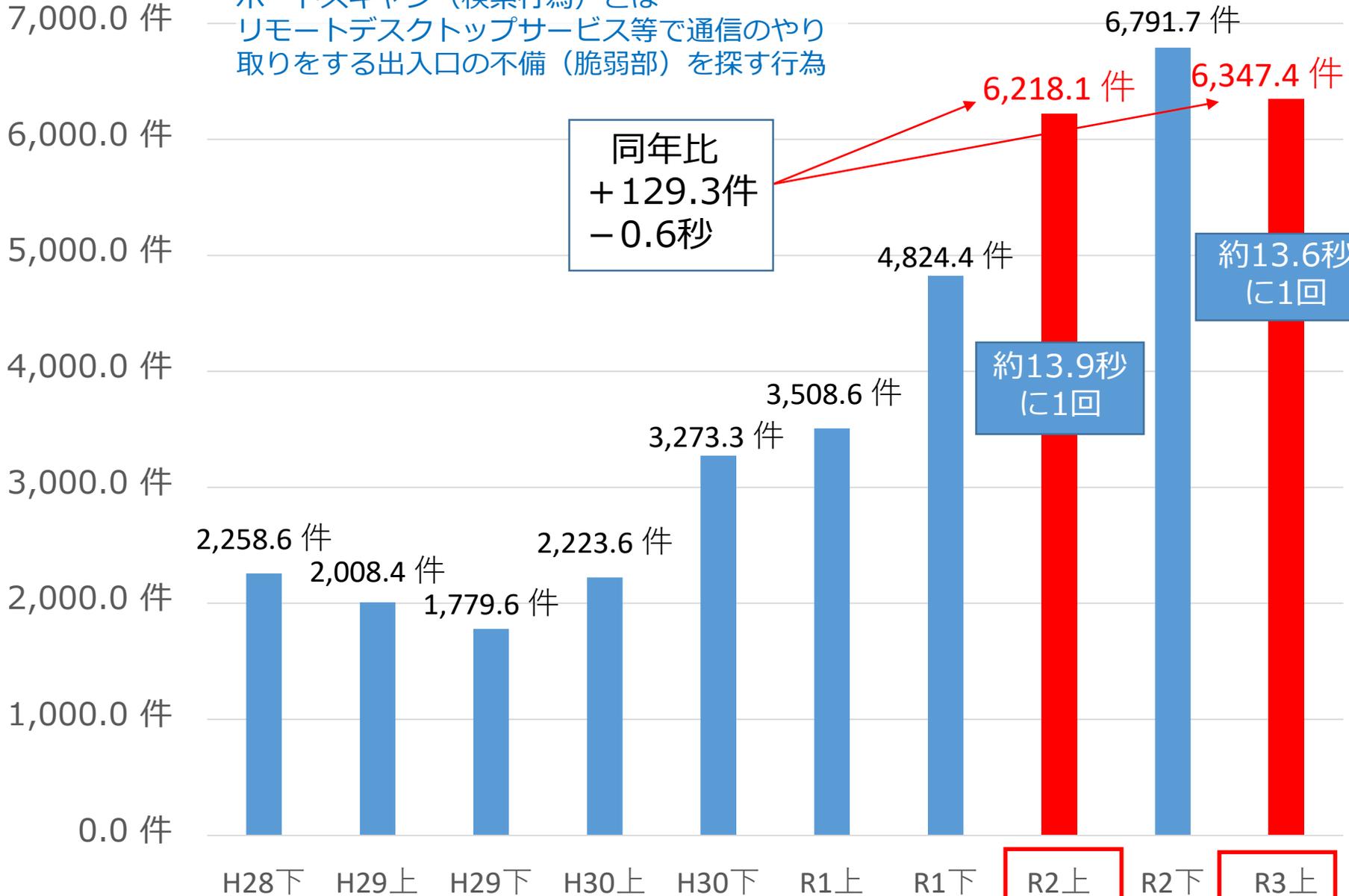
2020年

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

(件/日・IPアドレス)

ポートスキャン（検索行為）とは  
リモートデスクトップサービス等で通信のやり取りをする出入口の不備（脆弱部）を探す行為



同年比  
+129.3件  
-0.6秒

6,218.1 件  
6,347.4 件

約13.9秒  
に1回

約13.6秒  
に1回

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」

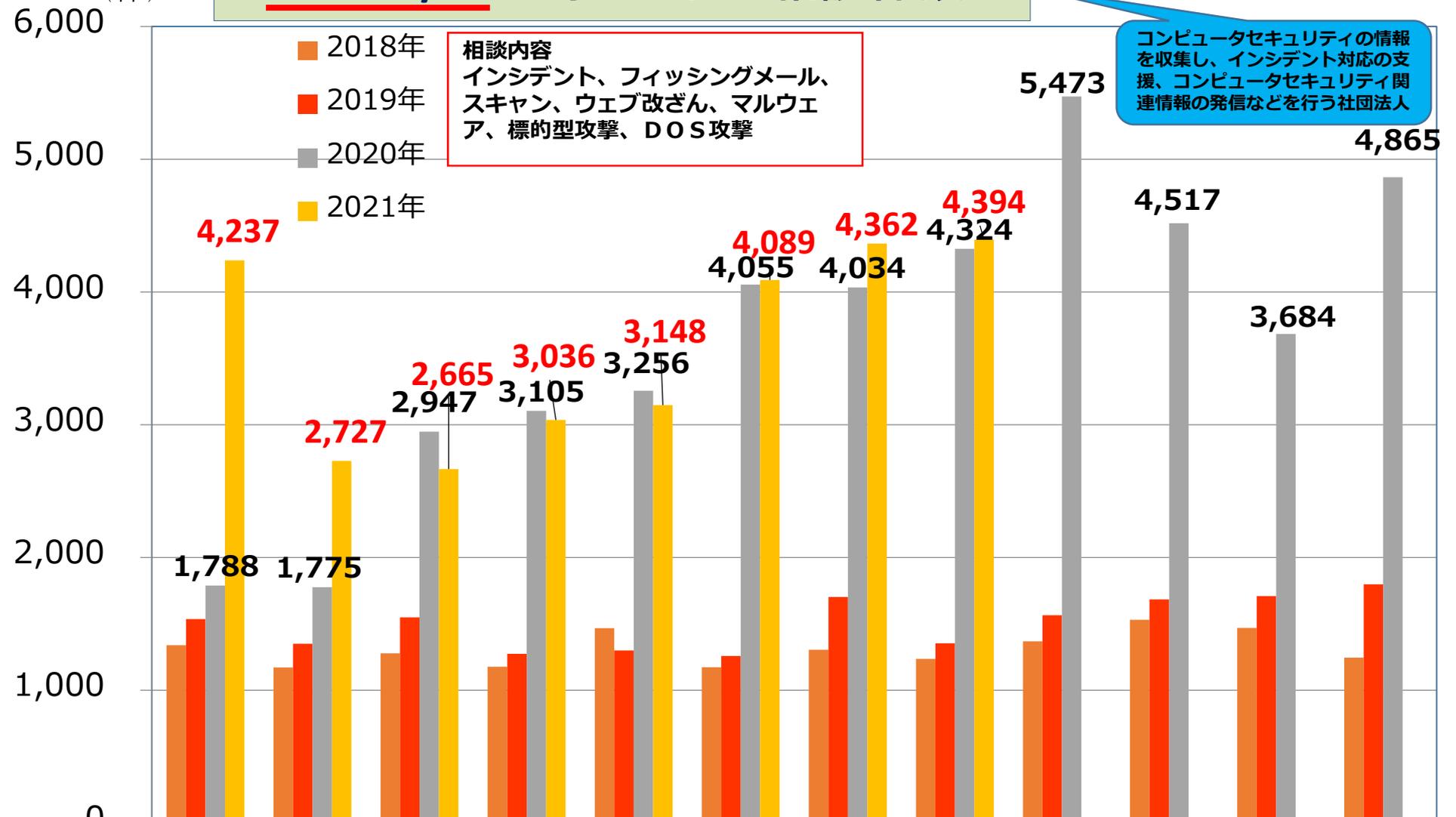
# JPCERT/CCに寄せられた相談件数

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」

(件)

相談内容  
インシデント、フィッシングメール、  
スキャン、ウェブ改ざん、マルウェア、  
標的型攻撃、DOS攻撃

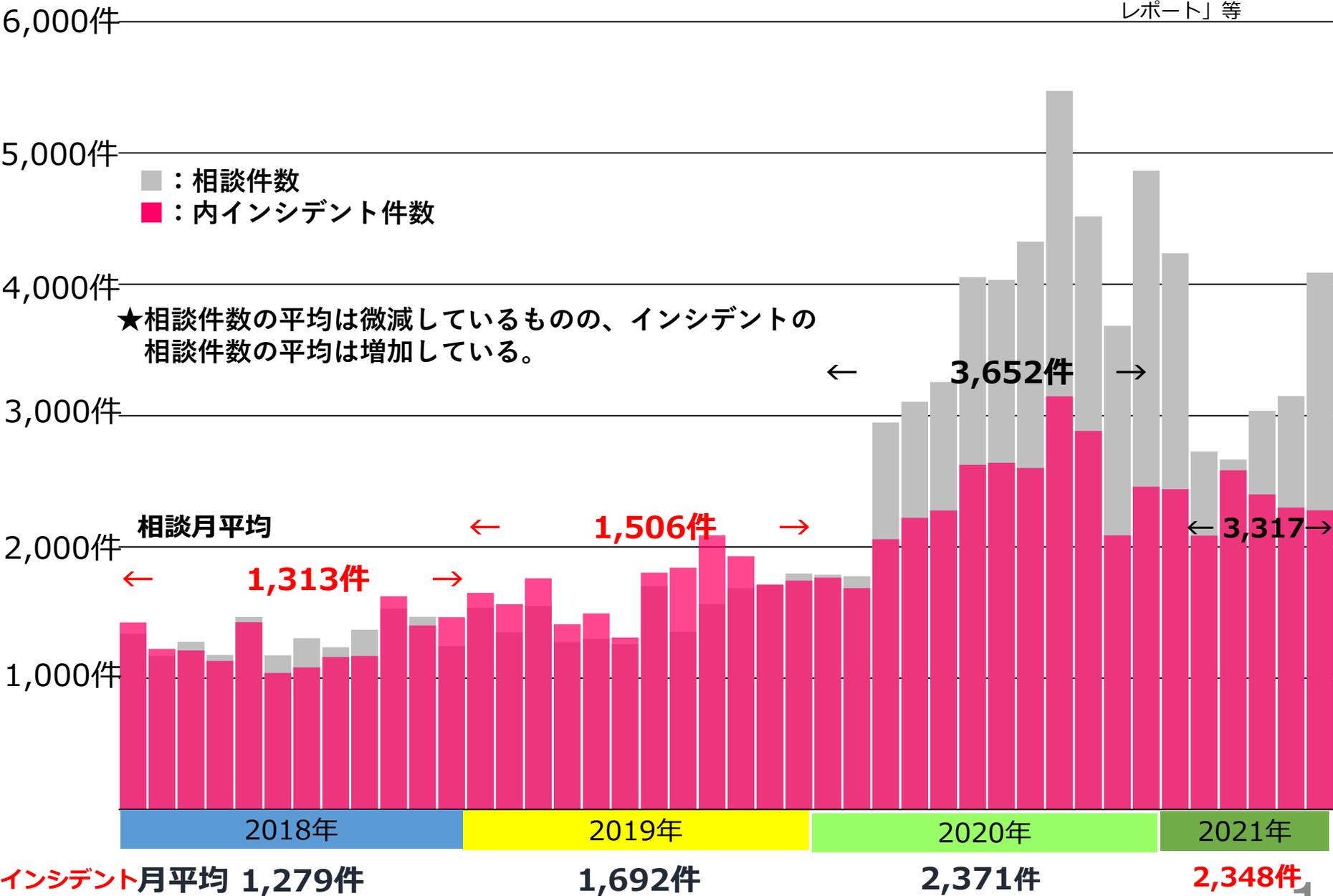
コンピュータセキュリティの情報を収集し、インシデント対応の支援、コンピュータセキュリティ関連情報の発信などを行う社団法人



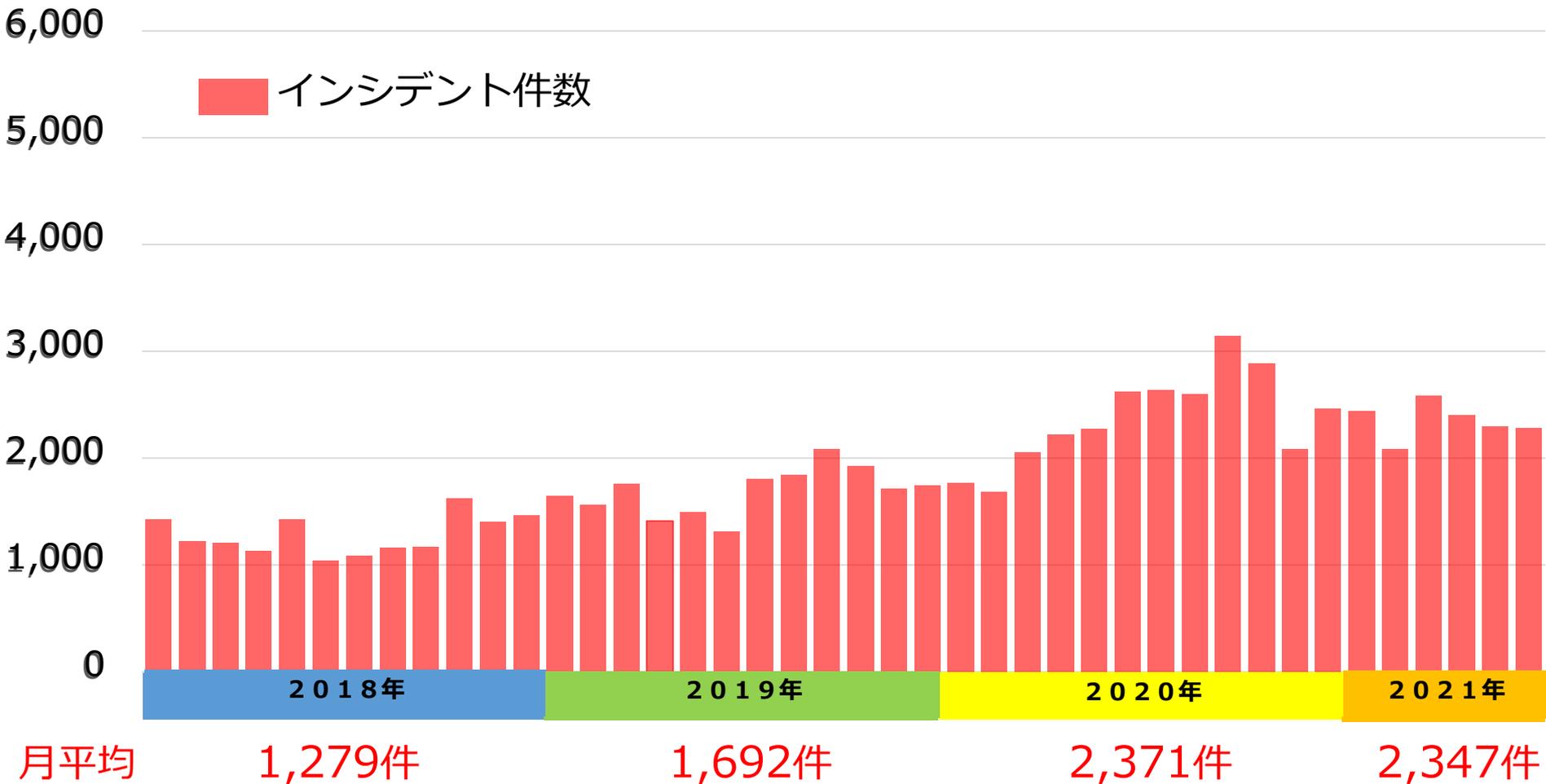
	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月
2018年	1,339	1,170	1,277	1,177	1,466	1,172	1,305	1,235	1,368	1,530	1,468	1,244
2019年	1,536	1,349	1,548	1,274	1,299	1,257	1,701	1,353	1,564	1,648	1,708	1,797
2020年	1,788	1,755	2,947	3,105	3,256	4,055	4,034	4,324	5,473	4,517	3,684	4,865
2021年	4,237	2,727	2,665	3,036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

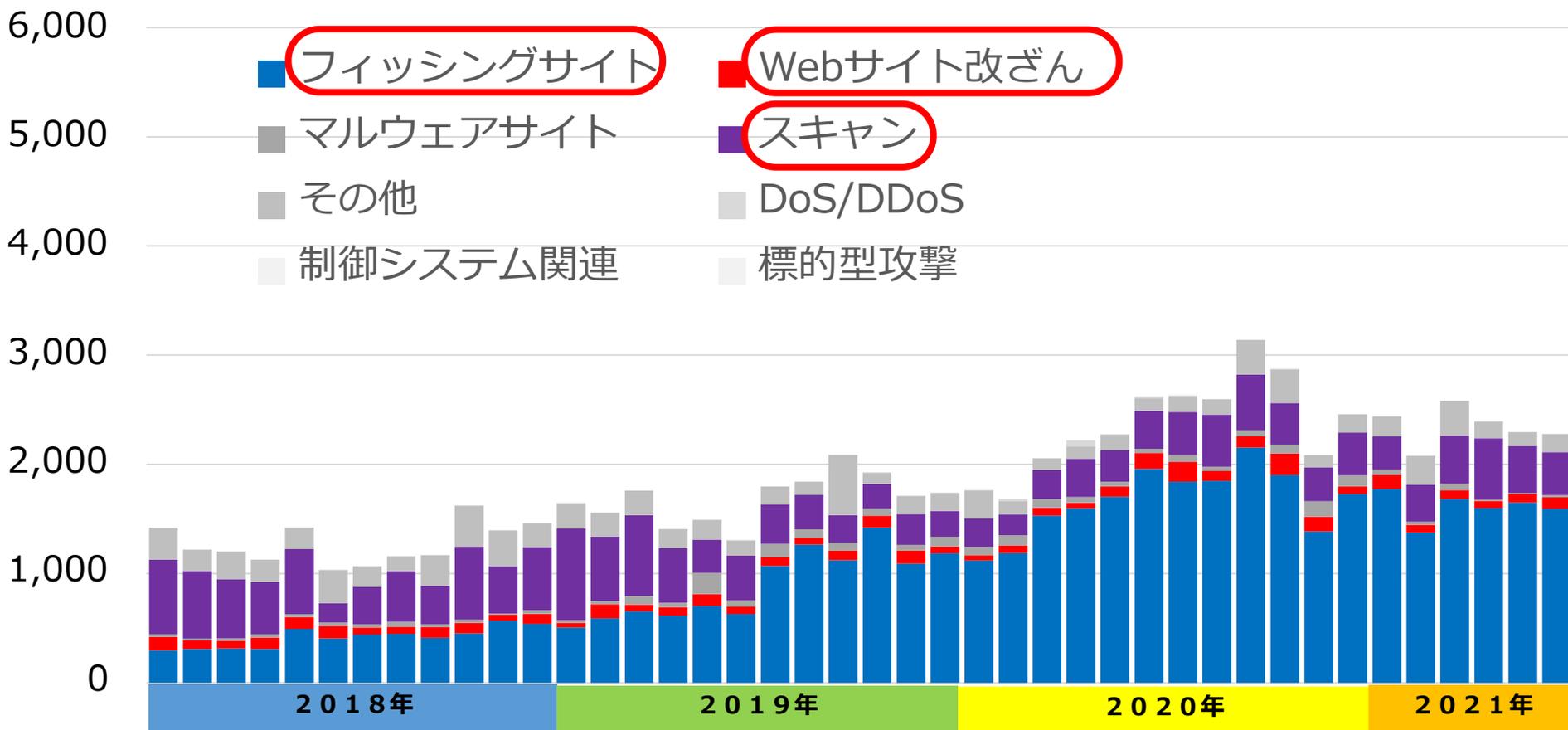


# 相談件数とインシデント件数との比較



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

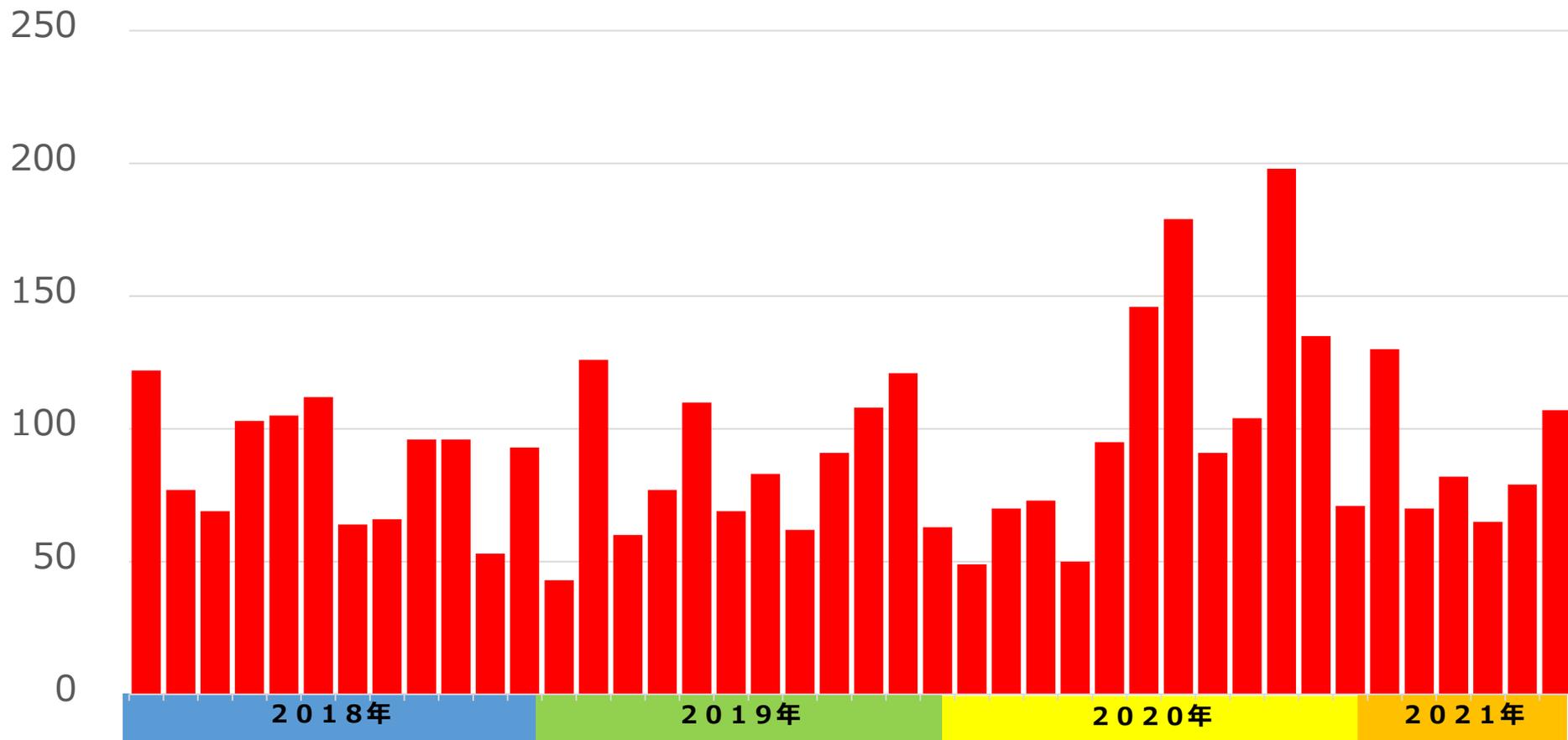
# 相談件数とインシデント件数との比較



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

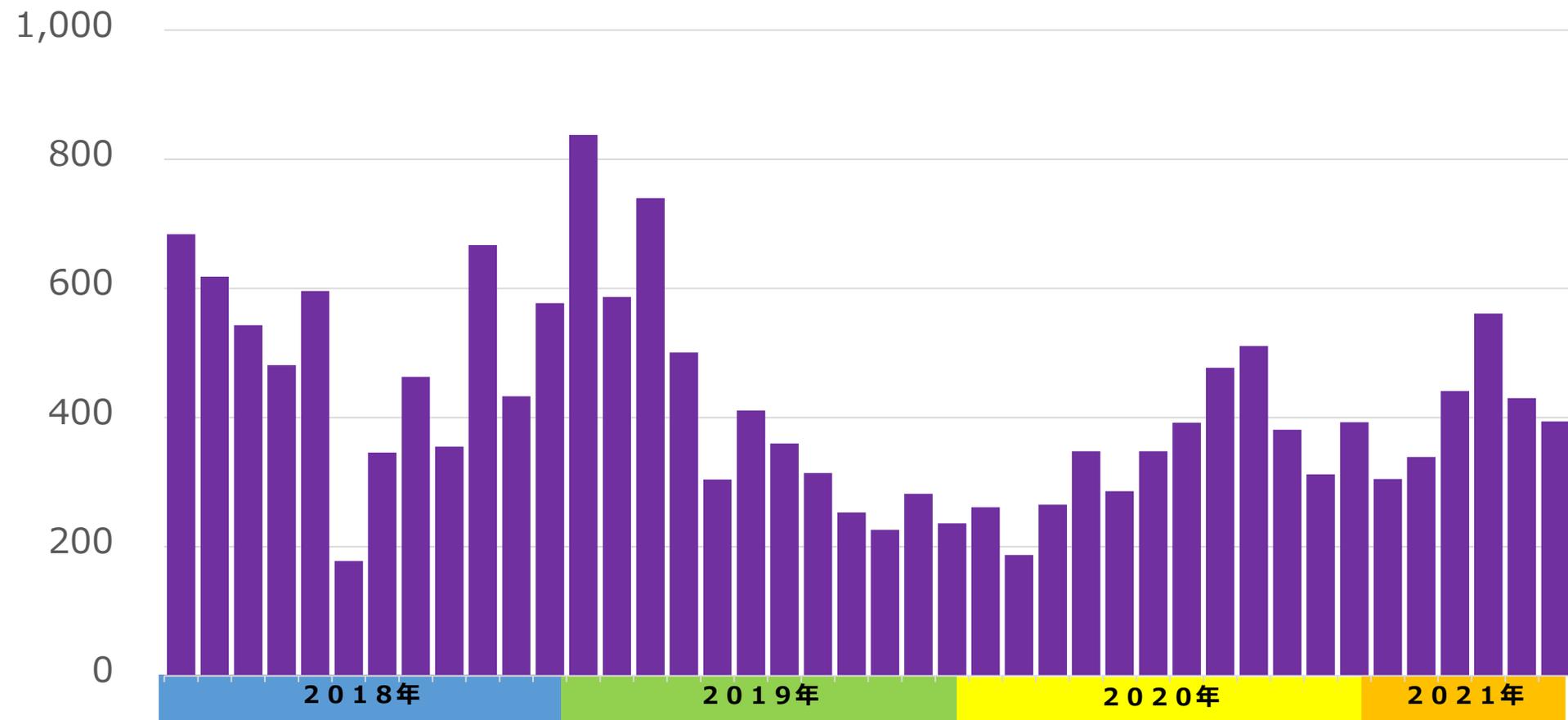
## Webサイト改ざん



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

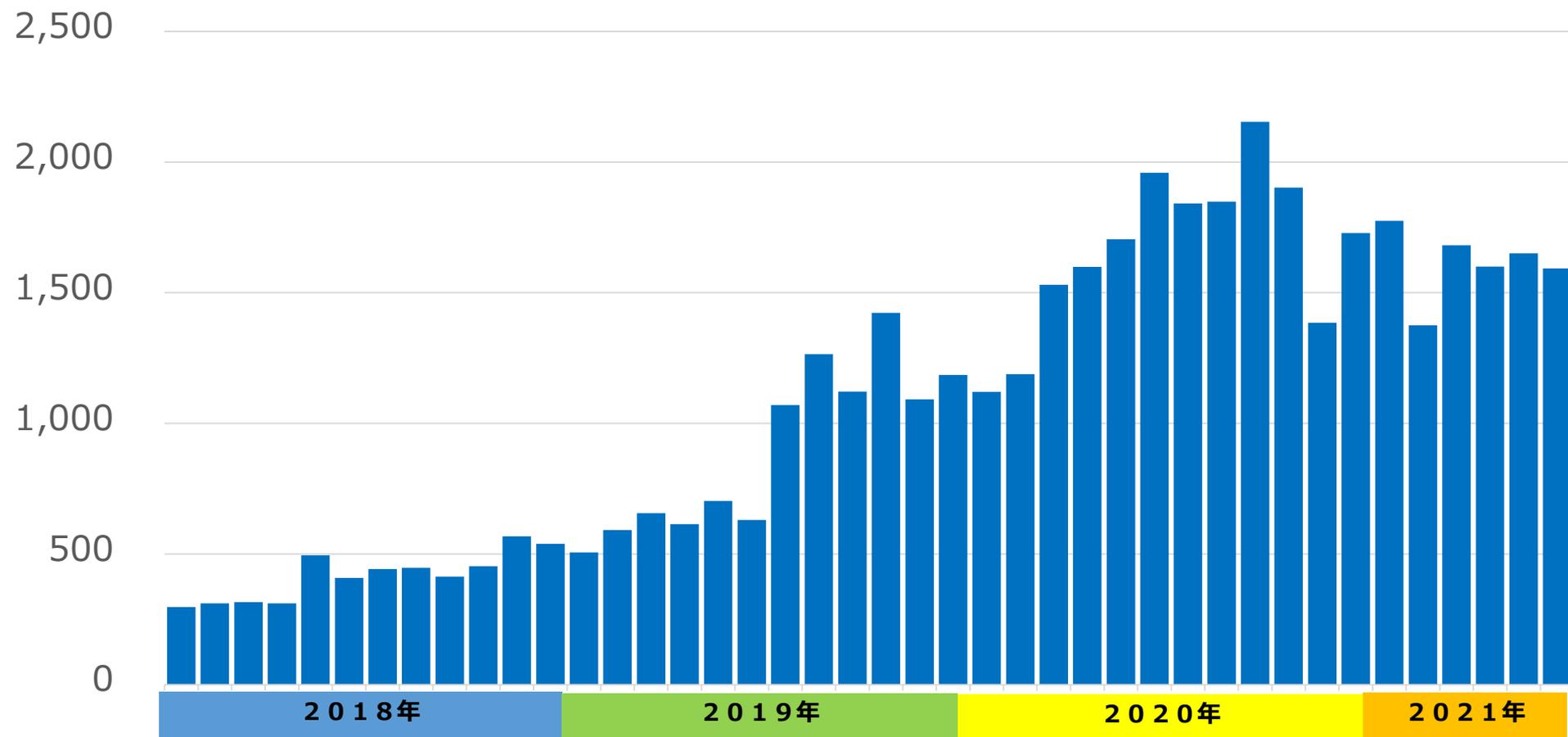
## スキャン



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

## フィッシングサイト



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1：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。

# 偽装されたWebページにご注意を

<東京オリンピック開会式開始時間> \*(東京2020オリンピック ...  
東京オリンピックテレビ放送▼(NHK東京オリンピック開会式テレビ放送ビデオ視聴インターネット無料ネットライブ配信)▶[#東京オリンピック開会式 ...  
10時間前・アップロード元: DW News

www. .... s.com ▶ video-Tok-v-Oly-jp-nhktv4

<東京 オリンピック テレビ 放送> \*TVOテレビ大阪|番組表送 ...  
東京オリンピックテレビ放送▼(NHK東京オリンピック開会式テレビ放送ビデオ視聴インターネット無料ネットライブ配信)▶[#東京オリンピック開会式 ...  
10時間前・アップロード元: Show TV

www. .... ars.com ▶ video-Tok-v-Oly-jp-nhktv1

\*テレビ-東京! \*東京オリンピック開会式放送 {「東京2020 ...  
東京オリンピックテレビ放送▼(NHK東京オリンピック開会式テレビ放送ビデオ視聴インターネット無料ネットライブ配信)▶[#東京オリンピック開会式 ...  
10時間前・アップロード元: Jantatv News

www. .... rs.com ▶ video-Tok-v-Oly-jp-nhktv2

<東京 オリンピック 放送 予定> \*BSテレ東(公式)! \*東京 ...  
東京オリンピックテレビ放送▼(NHK東京オリンピック開会式テレビ放送ビデオ視聴インターネット無料ネットライブ配信)▶[#東京オリンピック開会式 ...  
10時間前・アップロード元: V6 News Telugu

www. .... s.com ▶ video-Tok-v-Oly-jp-nhktv3

NHK<東京 オリンピック 開会式 テレビ> \*RKB毎日放送 ...  
東京オリンピックテレビ放送▼(NHK東京オリンピック開会式テレビ放送ビデオ視聴インターネット無料ネットライブ配信)▶[#東京オリンピック開会式 ...  
10時間前・アップロード元: KRT TV Canlı Yayın

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。

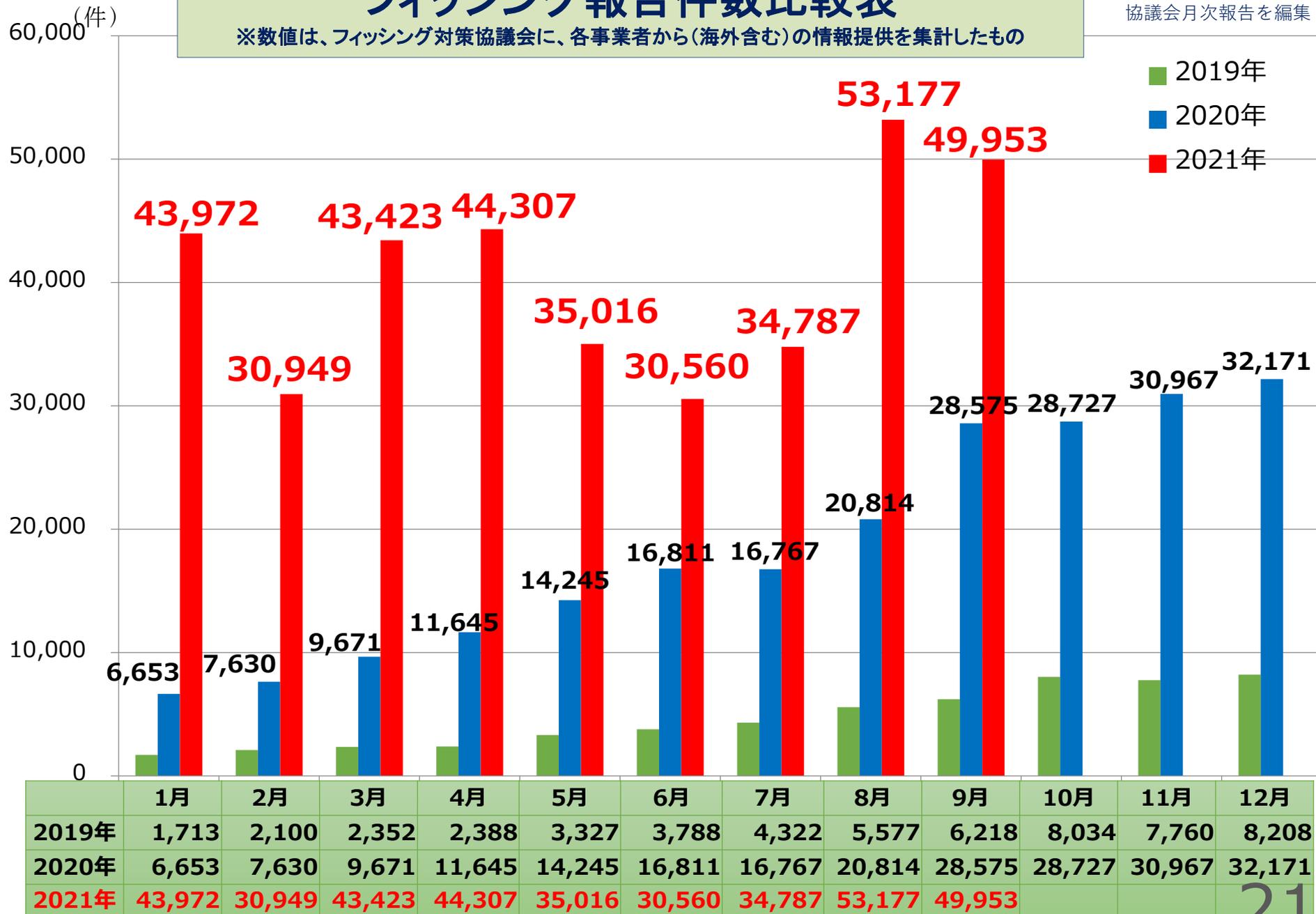
- 会社のWebが不正アクセスにされていないか確認する。
  - ・ 検索エンジンを利用し、自分のWebサイトにアクセスして「コンピューターに重大な損害を与えるおそれがある」と注意文等が表示するか確認する。(OS、ウイルス対策ソフトを最新の状態にして)
  - ・ 全部のページのソースを見て、挿入した覚えのないスクリプトの有無を確認する。
  - ・ 不審なアクセスの有無をアクセスログにて確認する。
- ソフトのシステムを必ずアップデートし最新にする。
- セキュリティソフト(ファイヤウォール等)導入する。
- セッションIDとパスワードの管理を徹底する。
- Webサーバーのファイルへのアク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

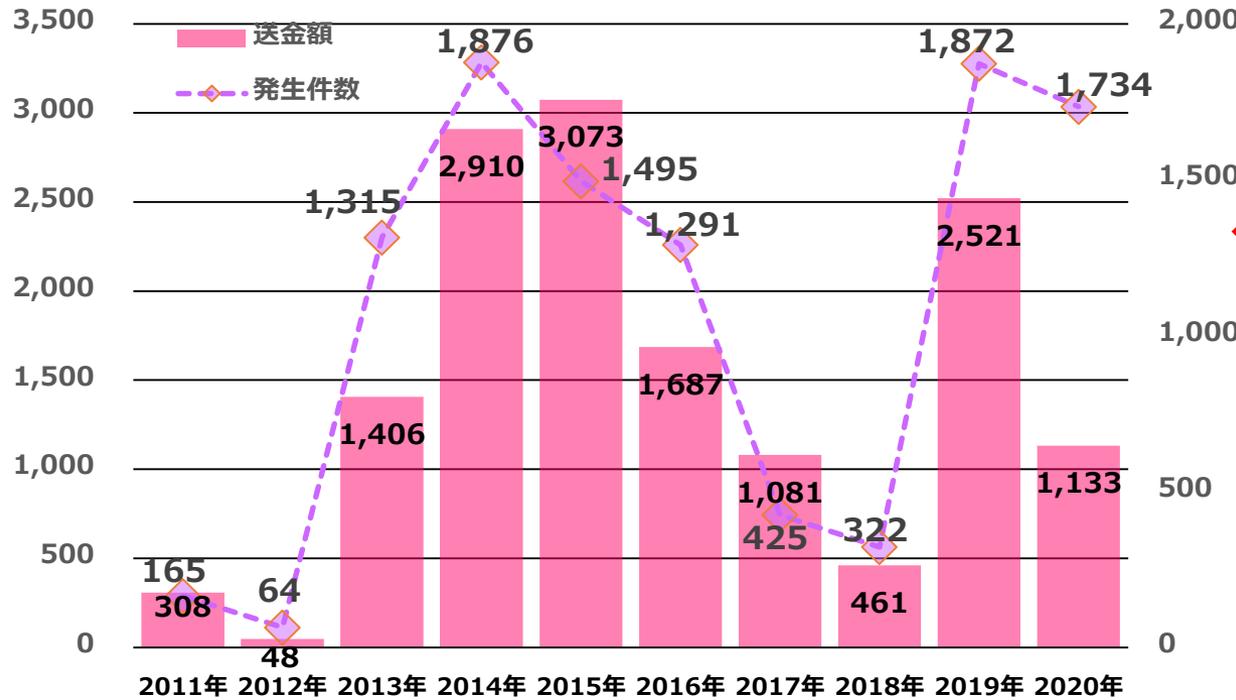
引用元：フィッシング対策協議会月次報告を編集



# 日本国内におけるネットバンキング被害件数の推移

百万円

件



前年比 (2021年、2020年)

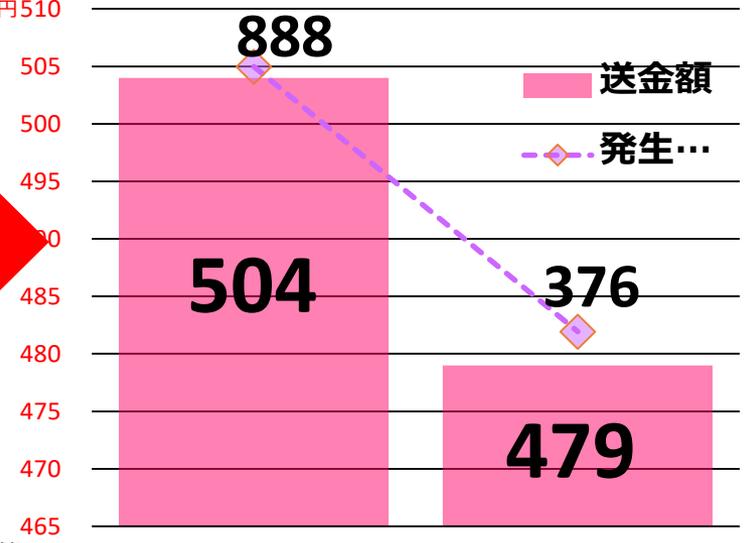
- 被害金額  
- 13億8,800万円
- 被害件数  
- 138件

百万円510

1,000 件

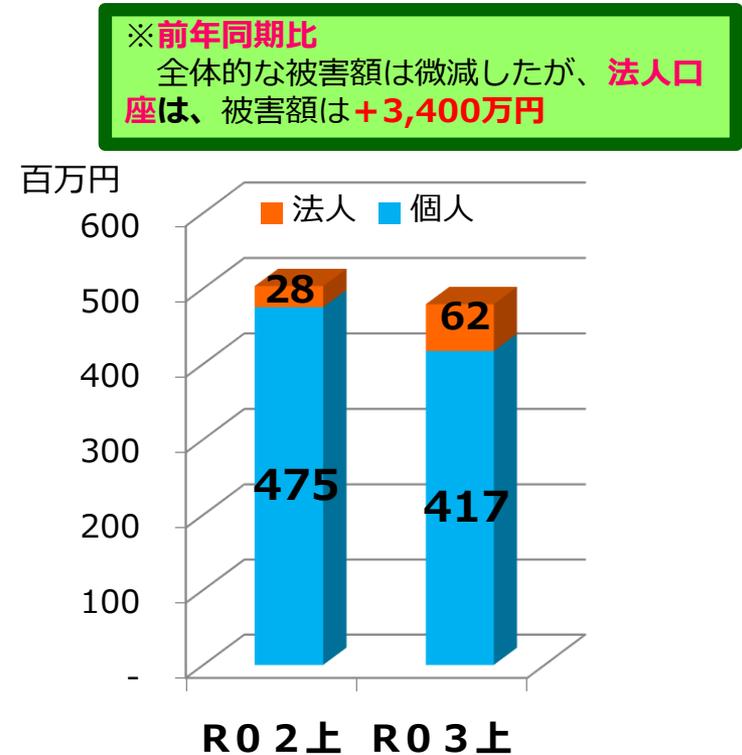
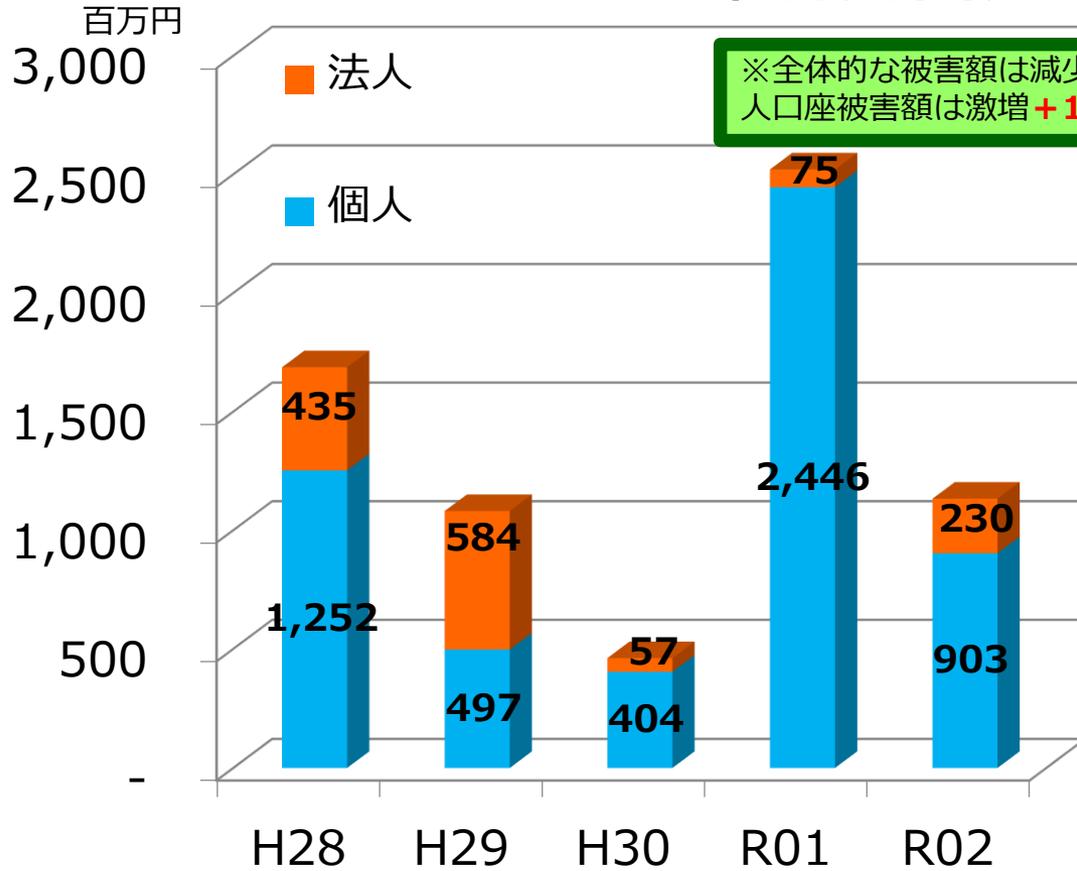
前年同期比

- 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



## 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。

# 攻撃者

## ※ C 2サーバ

Web  
サーバ

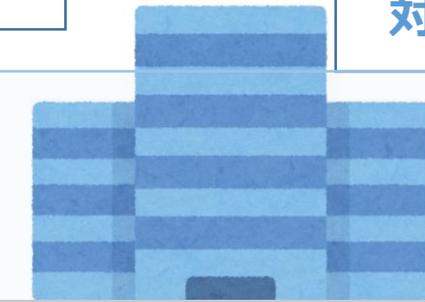


# 取引先 (拠点)



インターネット

# 対象企業



認証サーバ



発注管理サーバ



業務端末 A



業務端末 B



FW/VPN機器

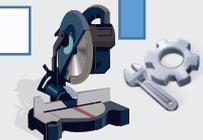


制御端末 (HMI等)



生産管理サーバ

製造装置



## ※ C 2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。

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)

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

サプライチェーンが狙われた

対象企業

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

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

⑤添付ファイル  
クリック

FW/VPN機器

制御端末 (HMI 等)

生産管理サーバー

製造装置

※GootKit Torojan

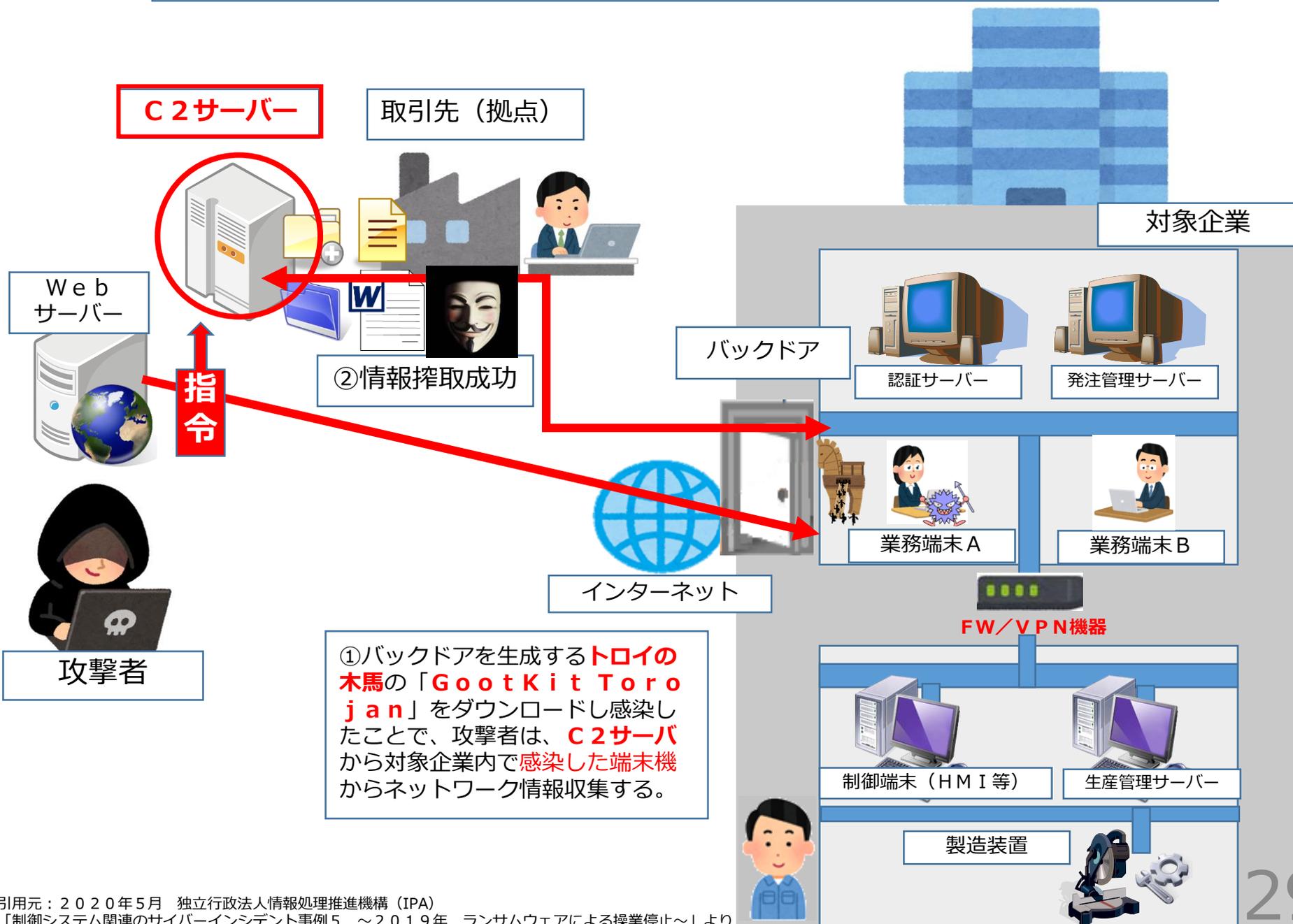
トロイの木馬で、ファイルのダウンロード機能やパスワードの機密情報を収集するアップロードする機能等を持つもの。

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

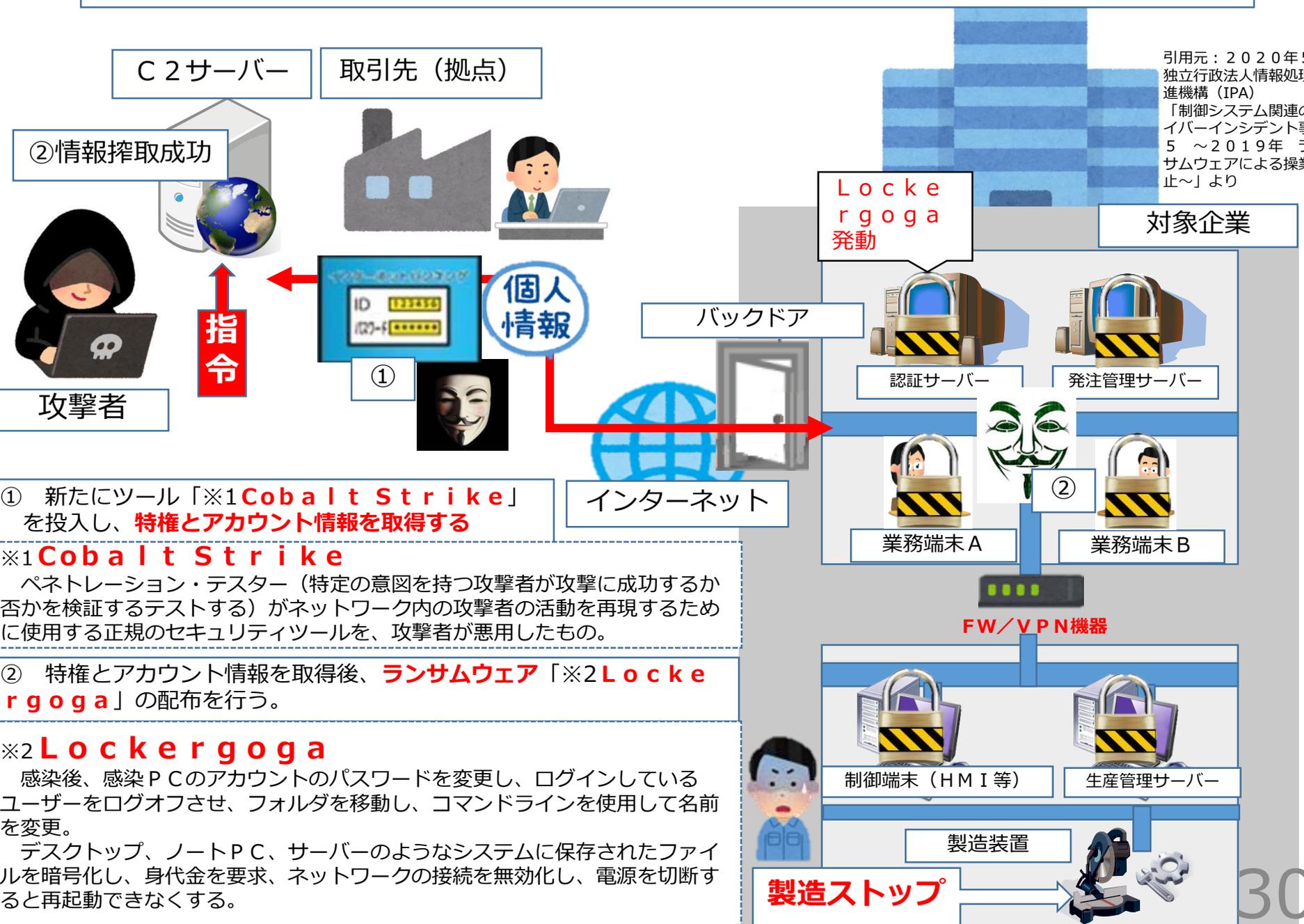
利用者が入る正規の入口とは別に、ID・パスワードがなくてもログインできる「勝手口」のようなもの

# 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)



# 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「※1Cobalt 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どう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**「※2Lockergoga」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。

**製造ストップ**

## 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ですが、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。

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～



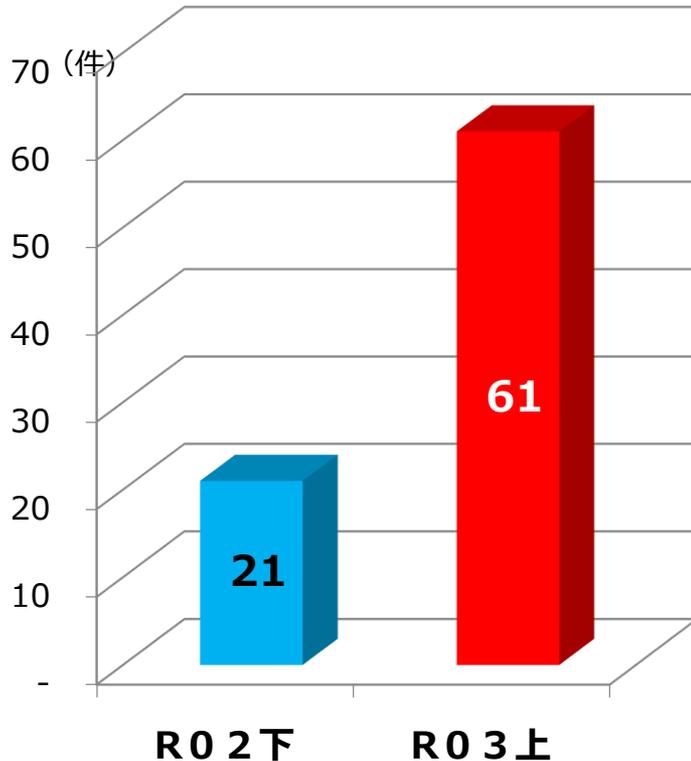
2020年3月

**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

# 国内のランサムウェアの情勢

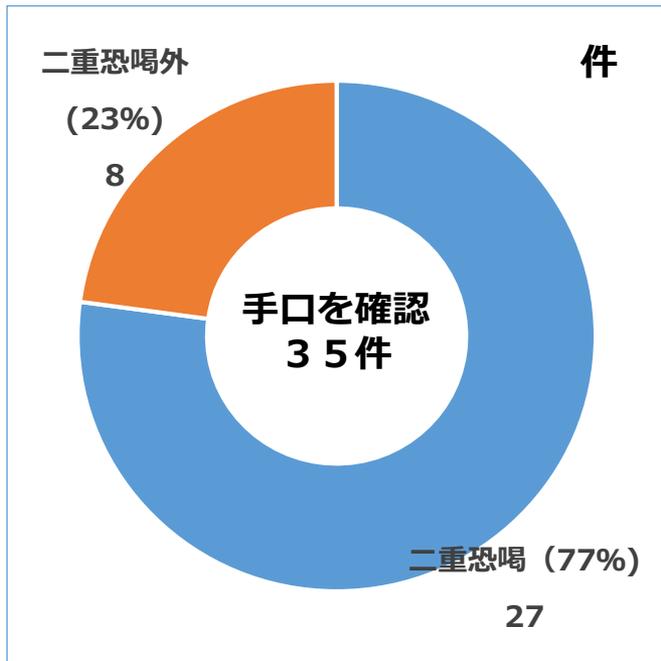
【企業・団体等におけるランサムウェア被害の報告件数の数位】



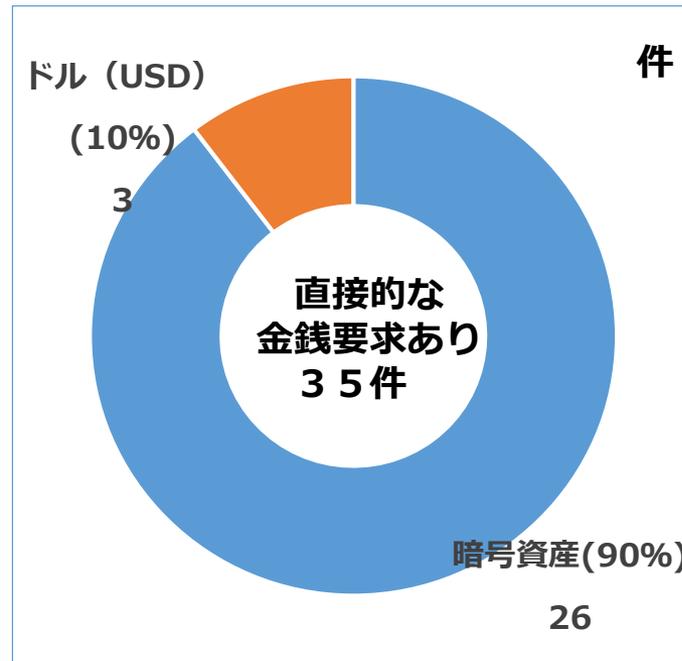
○ 従来のランサムウェアは、不特定多数の利用者狙って電子メールを送信するといった手口が一般的であったが、**現在では、VPN機器からの侵入等、特定の個人や企業・団体等を標的とした手口に変化**しており、企業のネットワーク等のインフラを狙うようになっている。

○ 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。

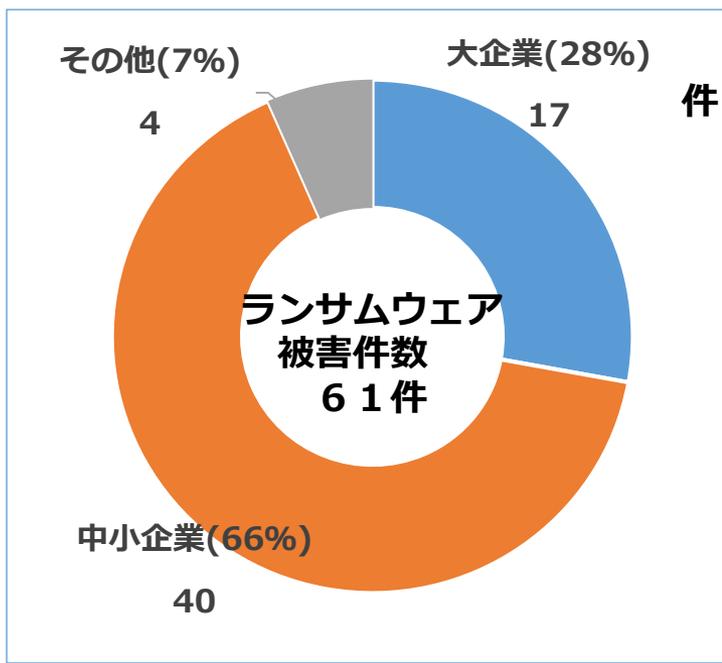
【ランサムウェア被害の手口別報告件数】



【要求された金銭支払い方法別報告件数】

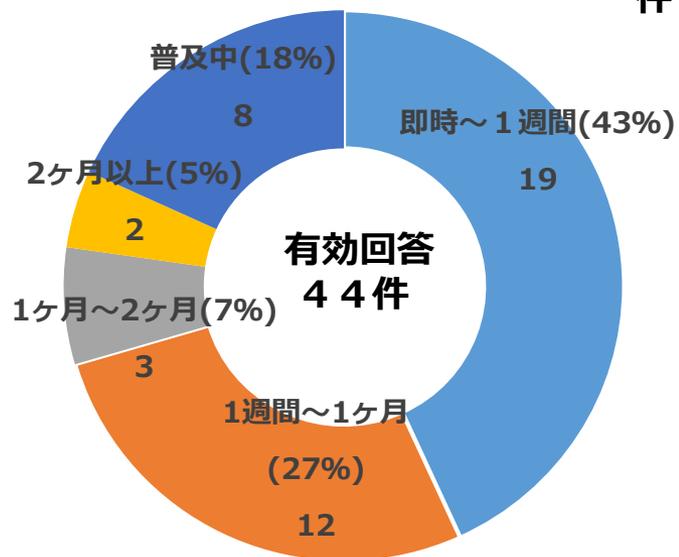


【ランサムウェア被害の被害企業・団体等の規模別報告件数】



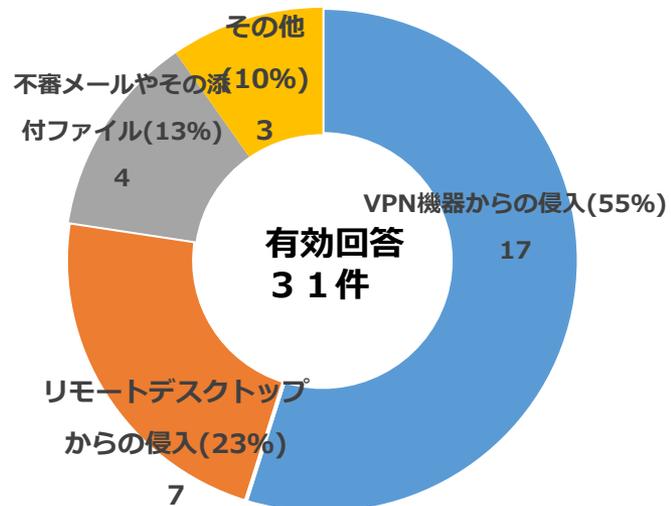
【復旧を要した期間】

件



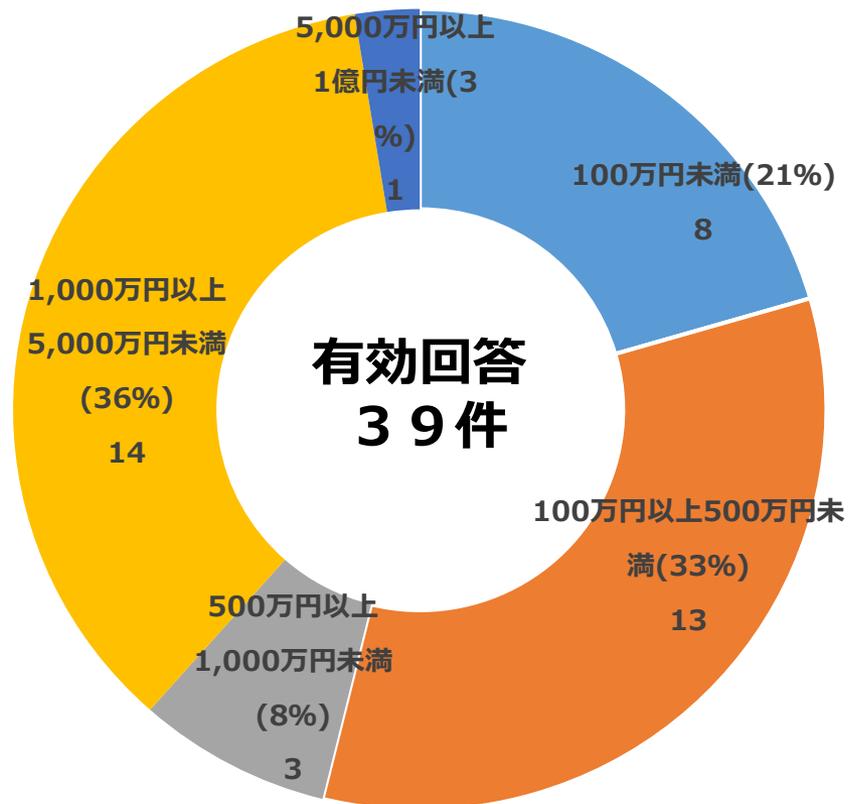
【感染経路】

件

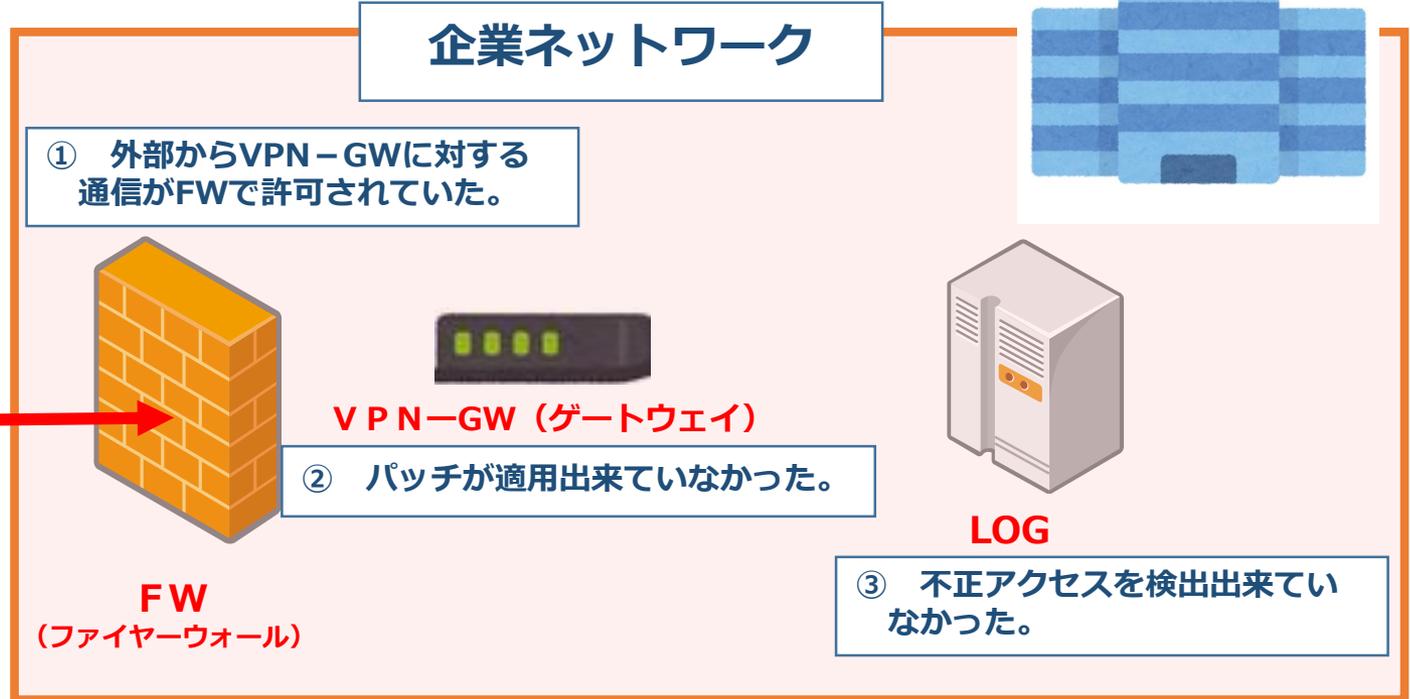


【調査・復旧費用の総額】

件



# VPN脆弱性攻撃とは



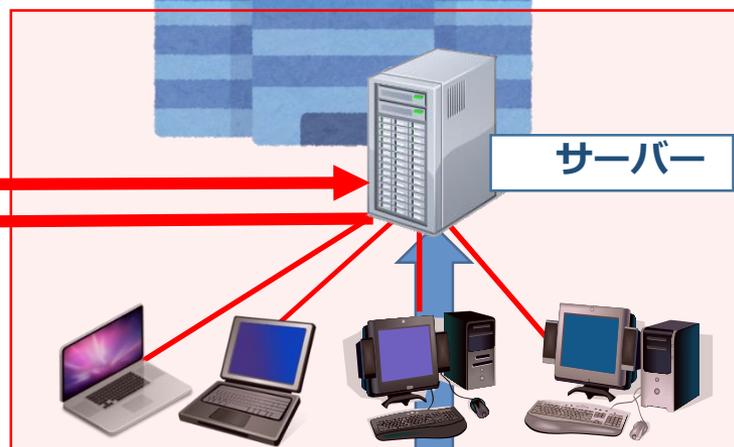
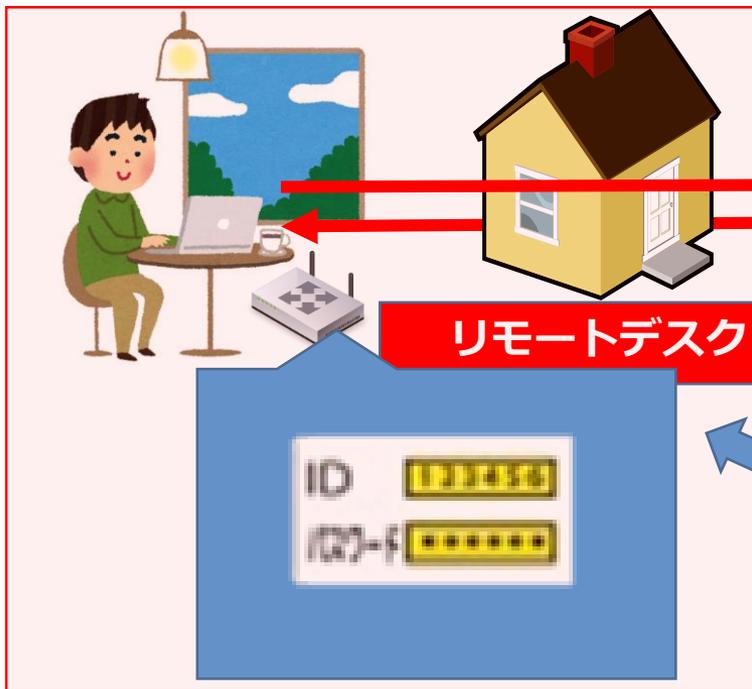
## 対策方法

- 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

企業

## テレワーク



① 既に感染している端末機を監視、盗聴したり、端末内の重要情報を窃取することで、ID・パスワードを入手し、遠隔操作を駆使してログインする。

② アクセス制限しておらず、ログイン画面が公開されている状態であると、パスワード総当たり攻撃（ブルートフォースアタック）をされログインされる。



## 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ェア。

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** (ネットウォーカー) (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に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。

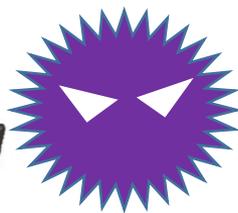
米国ペンシルベニア州デラウェア群に50万ドル支払わせた件があり、更に2021年2月、欧州の研究機関がハッキングを受けた旨の発表をしている。

# 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**を騙し取るもの。

早く電話をして来い、イヒヒ



# 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。

ウイルス除去  
マルウェア サポート

### 問題:



お使いのコンピュータが遅く、応答しない、表示エラーとなっている、またはその他の問題が発生し始めています。これらの問題は、多くの場合、ウイルス、マルウェア、またはシステムの不適切な保守によって引き起こされます。

### 症状:



マルウェアやウイルスは、プログラムのロックアップやクラッシュ、必要なソフトウェアや応答、およびPCのパフォーマンスを引き起こす可能性があります。

### ソリューション:



お使いのPCがマルウェアやその他の問題も疑念に基づいて感染している可能性があるため、それを強くお勧めします。

今すぐお電話 03-4-1111

Matt Felton - マイクロソフト ソフトウェア エキスパート



サポートチャット



Matt マットは今オフラインです。電話にてお問い合わせください。03-4199-5656

### Windowsセキュリティの重要な警告

Windowsセキュリティ&アンチウイルスサービスでエラーが発生しました。

フリーダイヤル

お使いのシステムのオンライン診断結果

Windowsは、お使いのシステム上で可能な主要なレジストリの障害を検出した可能性があります。

詳細については、フリーダイヤル: (03)-[redacted]で、カスタマーサポートにお問い合わせください。

(03)-[redacted] Windowsサポートにお問い合わせください。

個人情報露出発生リスクの可能性

クレジットカード情報や銀行情報。

電子メールのパスワード、その他のアカウントのパスワード

個人Facebook、Skype、AIM、ICQおよびその他のチャットログ  
プライベート/家族の写真やその他の機密ファイル

ウェブカメラ、VPN、ウイルス、スプーサーによってリモートでアクセス

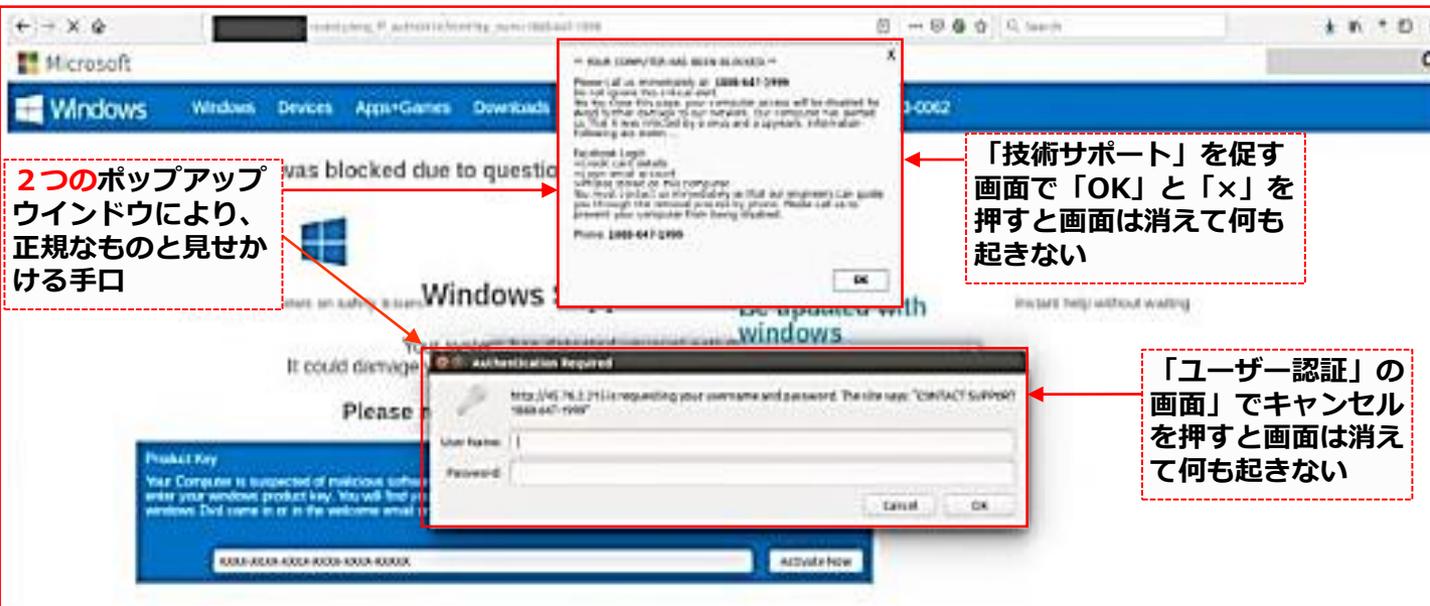
すぐに問題を修正し、データの損失を防ぐためにフリーダイヤル:

(03)-[redacted] Windowsサポートにお問い合わせください。

# サポート詐欺

## 正規ツール「iframe」悪用

典型的なMicrosoftの技術サポート窓口のWeb画面が表示され、「ユーザー認証」、「技術サポート」は消せたとしてもこのWebページに戻ってしまう



### 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、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

# 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>

サポートを装った詐欺にご注意ください | 日本マイクロソフト

Microsoft

## サポートを装った詐欺にご注意ください

セキュリティレスポンス チーム  
マイクロソフト株式会社

0:03 / 3:15

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

サポートを装った詐欺にご注意ください | 日本マイクロソフト

## マイクロソフトを装った警告表示の例

この表示はマイクロソフトから配信したものではありません。  
※こちらはあくまで一例です。類似した内容や別の電話番号が表示される場合があります。

### 手口

1:16 / 3:15

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

サポートを装った詐欺にご注意ください | 日本マイクロソフト

## マイクロソフトのサポートを装う詐欺にご注意ください

エラー画面や警告に電話番号はありません

ギフトカードやビットコインでのサポート料金の請求はありません

マイクロソフトから一方的なサポートの連絡はありません

公式サイトを確認を <https://support.microsoft.com>

### 注意喚起

2:15 / 3:15

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

サポートを装った詐欺にご注意ください | 日本マイクロソフト

## サポート詐欺の画面が表示されたら

- 画面に表示された警告をクリックしない
- 指定された番号に電話しない
- チャットやメールに返答しない

### 対処方法

2:32 / 3:15

サポートを装った詐欺にご注意ください | 日本マイクロソフト

### 画面を操作することができない場合

1. キーボードの[Ctrl] [Alt] [Del] の 3 つのキーを同時に押す
2. [タスクマネージャー] をクリックする
3. ブラウザーアプリを選択し「タスクの終了」をクリックする

**対処方法**



YouTube 3:01 / 3:15

サポートを装った詐欺にご注意ください | 日本マイクロソフト

### サポート詐欺から身を守る方法

マイクロソフト 公式 サポートサイト  
<https://support.microsoft.com>

サポート詐欺から PC を保護する  
<https://aka.ms/SupportScam>

**ご案内**



YouTube 3:07 / 3:15

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。

# 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

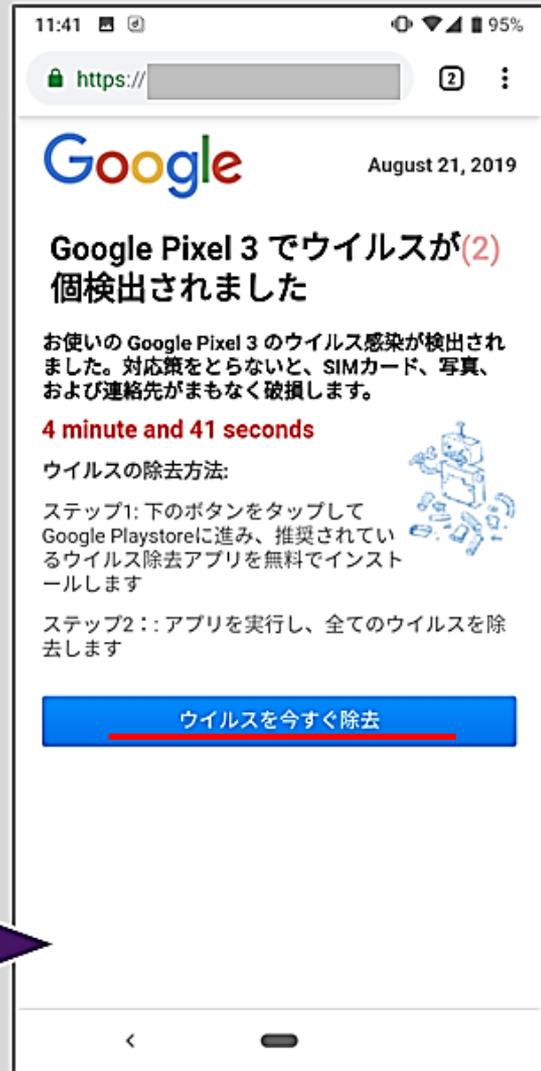
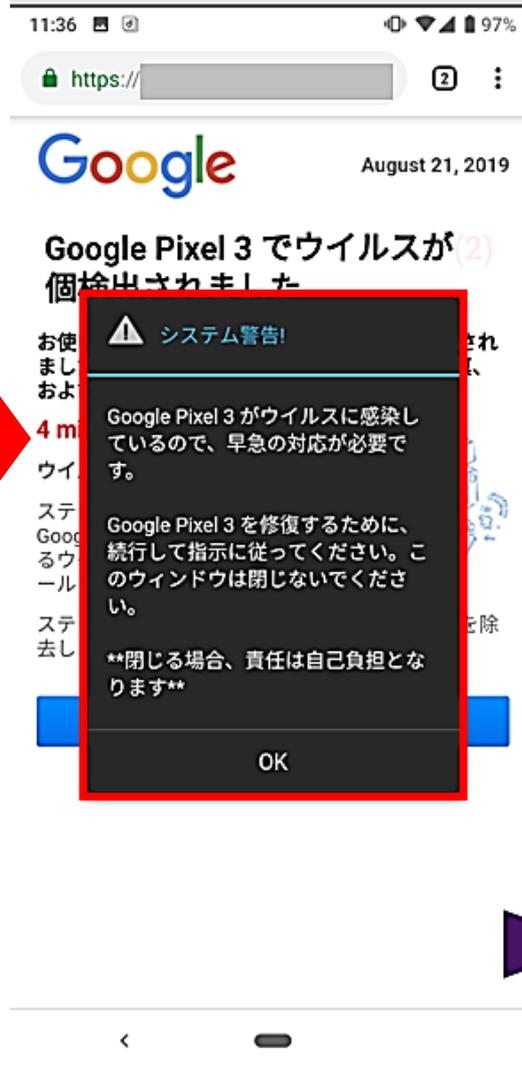
アプリに誘導する目的は不明ですが、「利用者にアプリをインストールさせることによる報酬」を得ようとするアプリウエア（成果報酬広告）と見られている、なお、セキュリティ警告の出元（広告主）と誘導されるアプリの開発元との関係は不明



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（**C t r l + A l t + D e l**）」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、ソフトウェ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相談窓口にて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

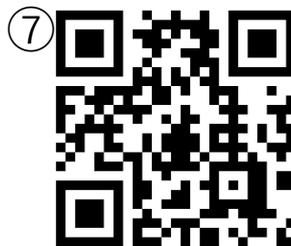
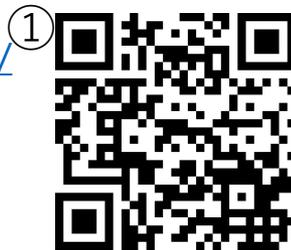
サイバー犯罪事件の捜査

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 内閣サイバーセキュリティセンター（NISC）
- ⑥ フィッシング対策協議会
- ⑦ JPCERTコーディネーションセンター（JPCERT/CC）
- ⑧ is702
- ⑨ マルウェアレポート

- ① @police <http://www.npa.go.jp/cyberpolice/>
- ② 警視庁Twitter  
[https://twitter.com/MPD\\_cybersec](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 内閣サイバーセキュリティセンター (NISC)  
<http://www.nisc.go.jp>
- ⑥ フィッシング対策協議会  
<https://www.antiphishing.jp/>
- ⑦ JPCERT/CC  
<https://www.jpcert.or.jp/>
- ⑧ is702  
<https://www.is702.jp/>
- ⑨ マルウェアレポート  
[https://eset-info.canon-its.jp/malware\\_info/malware\\_topics/](https://eset-info.canon-its.jp/malware_info/malware_topics/)



# CS対策本部リーフレット

**ランサムウェアに (身代金ウイルス) 要注意!**

街とともに。人とともに。  
FOR MORE COMMUNICATION  
警視庁

**ストップ!! それ、信用できません!**

サポートに連絡しない!

URLをクリックしない!

URL付きのSMSを受信したとき

警告画面が表示されたとき

パスワードの変更を!

ネット家電の設定が買ったままのとき

えっ! (#D) 個人情報流出の危機!! セキュリティ対策を!!

**ちょっと待って! その操作、大丈夫!?**

個人情報流出

ウイルス感染

ユーザーID:\*\*\*\*  
パスワード:\*\*\*\*

乗っ取り

クレジットカード

**スマートフォンのセキュリティ対策を!**

- アプリのインストールは慎重に!
- システムやアプリは最新バージョンに!
- ウイルス対策ソフトを導入!

情報セキュリティ広場 検索

# 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



サイバーセキュリティが  
あなたを救う

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

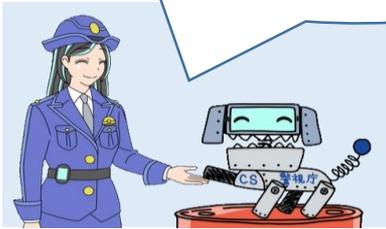
◆ 「You Tube」警視庁公式チャンネルにも公開しています

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

中小企業向け ver

## 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

正義感が強くちょっぴりドジな「サイバー官」と、サイバー犯罪を嗅ぎ分けるブルドック型AIロボットの「サイバーAI犬」がサイバー犯罪に遭わないためのポイントを教えてくれる短編アニメです。

各テーマ 30秒、15秒

### ① 標的型攻撃編

ウイルスが含まれている添付ファイルを開かせる標的型攻撃。騙されないためのポイントをお伝えします。

アクセスはこちらから

### ② サプライチェーン攻撃編

サプライチェーンの弱点について紹介しながら、取引先のセキュリティ対策の重要性についてお伝えします。

アクセスはこちらから

### ③ テレワークのセキュリティ基本編

テレワーク開始時そのパソコンをいきなり使うのは危険かもしれません。テレワーク前に行うべき最低限のセキュリティ対策をお伝えします。

アクセスはこちらから

### ④ なりすましによる振り込め詐欺編

相手の顔が見えないメールによる振り込め詐欺。その手口と対策をお伝えします。

アクセスはこちらから

### ⑤ なりすましウイルス付きメール編

メールで広がる史上最悪のウイルス。感染すると気付かないうちに周りにも被害が及ぶ可能性あり！注意すべきポイントをお伝えします。

アクセスはこちらから

### ⑥ ランサムウェア編

感染後PCをロック、ファイルを暗号化し、元に戻すこと引き換えに身代金を要求してくるウイルス。日頃から取るべき対策をお伝えします。

アクセスはこちらから

お！メールだ。至急確認？分らないけどどろあえず見てみるか。

**STOP!!**

この添付ファイル、本当に大丈夫？

都内中小企業者向け  
Tcyss無料相談窓口  
サービス  
**03-5320-4773**  
受付時間 9:00~12:00  
(都庁階層白) 13:00~17:00

🐾 動画視聴はこちらから 🐾 個人向け ver も公開中 🐾

**YouTube**  
警視庁公式チャンネル

警視庁サイバーセキュリティ  
対策本部公式ツイッター

# テレワークに関する広報資料

## ちょっと待って! そのテレワーク、 セキュリティは大丈夫?

テレワーク=時間や場所の有効活用。でも、サイバー空間には悪意ある犯罪者がたくさん。  
テレワーク環境=コンピュータやインターネットのセキュリティ対策をしていますか?

**たとえば...**

**Webサイトやアプリケーション**  
を介してコンピュータウイルスに感染し、  
情報を盗まれることがあります。

— 利用するコンピュータのOSやウイルス対策ソフトは常に最新の状態に更新し、必ず利用前及び定期的にウイルススキャンを実施しましょう。

**カフェ等のWi-Fiスポットは**  
セキュリティが十分でないものもあり、  
通信内容を傍受されるおそれがあります。

— 不特定多数が接続できるWi-Fiスポット(=公衆無線LAN)は、通信が暗号化されていないものやパスワードが公開されているものなど、そのセキュリティレベルはさまざま。  
利用時はファイル共有機能をオフにし、通信経路を暗号化(VPN)するとき以外は、たとえ無料でもセキュリティ対策のやりとりに留意しましょう。

**自宅のWi-Fiルータの管理用IDとパスワード。**  
初期設定のままだとコンピュータ内に  
侵入されるおそれがあります。

— そもそも変更した覚えがない...そんな方はルータの管理画面で確認。  
「admin」や「password」等のありがちな初期設定になっていたら危険です。  
他人に推測されにくいものに今すぐ変更しましょう。

**その他にも...**

- 各種パスワードは使い回しを避け、一定以上の長さで他人に推測されにくいものにする。
- 公共の場では覗き見や盗聴のリスクを考え、長時間離席しない、密着の席に座るなどの配慮をする。
- テレワークについての相談を事前に確認しておき、不安なことがあればすぐに対応する。 etc...

**万全のセキュリティ対策で情報や資産を守り、  
安全にテレワークを活用しましょう。**

© 総務省サイバーセキュリティ対策本部

## ちょっと待って!! そのPC、社内に戻して大丈夫!?

世界とつながるサイバー空間。  
そこには皆さんの大切なデータや資産を狙った  
悪意ある犯罪者もたくさんいます。

知らないうちにウイルス感染したPCを、  
社内システムに繋いでしまったら大変なことに!

テレワーク後のPC、USBメモリ等の記録媒体は  
社内に戻す前に、  
セキュリティソフトのウイルススキャンで  
まず**安全確認を!**



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

→音声読み上げ・文字拡大 →Multilingual →携帯サイト →警察署一覧 →サイトマップ 検索

**警視庁** 安全な暮らし 交通安全 相談・お悩み 手続き 事件・事故 警視庁について

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！

## テレワーク勤務のサイバーセキュリティ対策！

更新日：2020年4月16日

### テレワークで勤務をされる方へ

テレワークでの勤務は、オフィスのサイバーセキュリティの環境とは異なり、勤務先のシステム等へ外部からアクセスしますので、マルウェア（ウイルス）への感染リスクが高まります。テレワークで使用するパソコン等（タブレット、スマートフォン）は、勤務先が導入したテレワーク専用のものであればサイバーセキュリティ対策が考慮されている場合がほとんどです。しかしながら、急速、テレワークをすることになり、普段勤務先で使用しているパソコンや自宅のパソコンを使用する場合は、サイバーセキュリティ対策が十分とは言えませんので、特に注意する必要があります。



**注目情報**

- テレワーク勤務のサイバーセキュリティ対策！
- [ようこそ情報セキュリティ広場へ](#)
- [ランサムウェアに要注意！](#)
- [東京中小企業サイバーセキュリティ支援ネットワーク\(Tcyss\)](#)

<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

情報セキュリティ広場(警視庁HP) @MPD\_cybersec




Tcyss相談窓口




警視庁公式チャンネル YouTube(H P 経由)

## サイバー保険取り扱い事業者

MS&AD

あいおいニッセイ同和損保

あいおいニッセイ同和損害保険株式会社

Allianz

アリアantz火災海上保険株式会社

AIG AIG損保

A I G 損害保険株式会社

HDI

H D I G l o b a l 保険会社

共栄火災

共栄火災海上保険株式会社

SOMPO 損保ジャパン

損害保険ジャパン日本興亜株式会社

大同火災

大同火災海上保険株式会社

CHUBB

C h u b b 損害保険株式会社

東京海上日動

東京海上日動火災保険株式会社

MS&AD 三井住友海上

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 SONPO  
The General Insurance Association of Japan

外国損害保険協会

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



サイバー保険特設サイト

