

# テレワークを狙うサイバー攻撃の 現状と対策のポイント

**Presented by**  
**Cyber Security Laboratory,**  
**Canon IT Solutions, Inc.**

# 自己紹介



## □ 保有資格

CISSP

情報処理安全確保支援士 ほか



第009576号



Certified Information  
Systems Security Professional

## 西浦 真一

### セキュリティエバンジェリスト

キヤノンITソリューションズ株式会社  
サイバーセキュリティラボ

- 2006年、セキュリティ業界へ
- ネットワークを中心とした  
セキュリティリスクへの対策の提案や  
海外セキュリティ製品のローカライズ
- セミナー等でセキュリティに関する情報を発信

## □ 社外活動

JNSA (NPO 日本ネットワークセキュリティ協会)

- セキュリティ理解度チェックWG リーダー
- インシデント被害調査WG サブリーダー

# キヤノンITソリューションズ サイバーセキュリティラボ



研究



解析



発信

サイバーセキュリティ情報局

Search

## # 本日はお話しすること

1. 2021年上半期の  
サイバーセキュリティ脅威動向
2. 対策のポイント

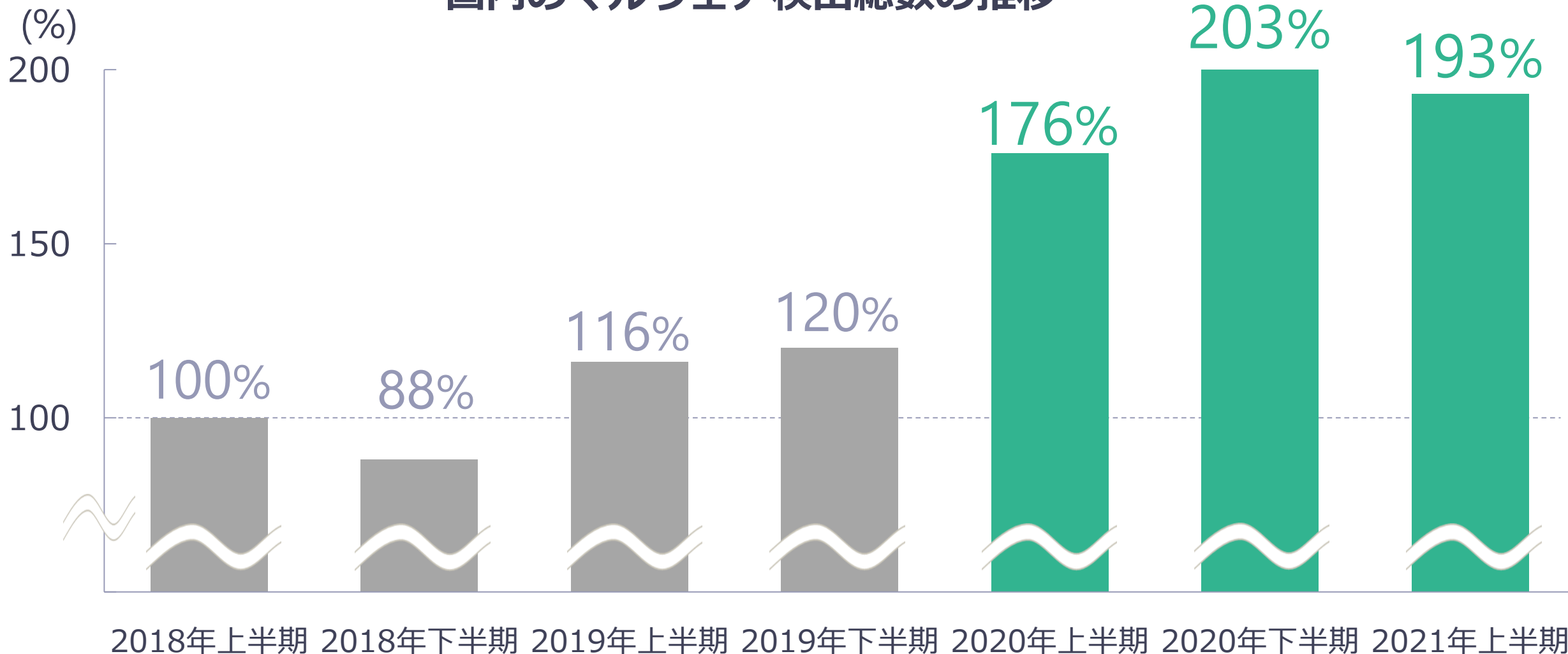
## # 本日はお話しすること

1. 2021年上半期の  
サイバーセキュリティ脅威動向
2. 対策のポイント



# Malware

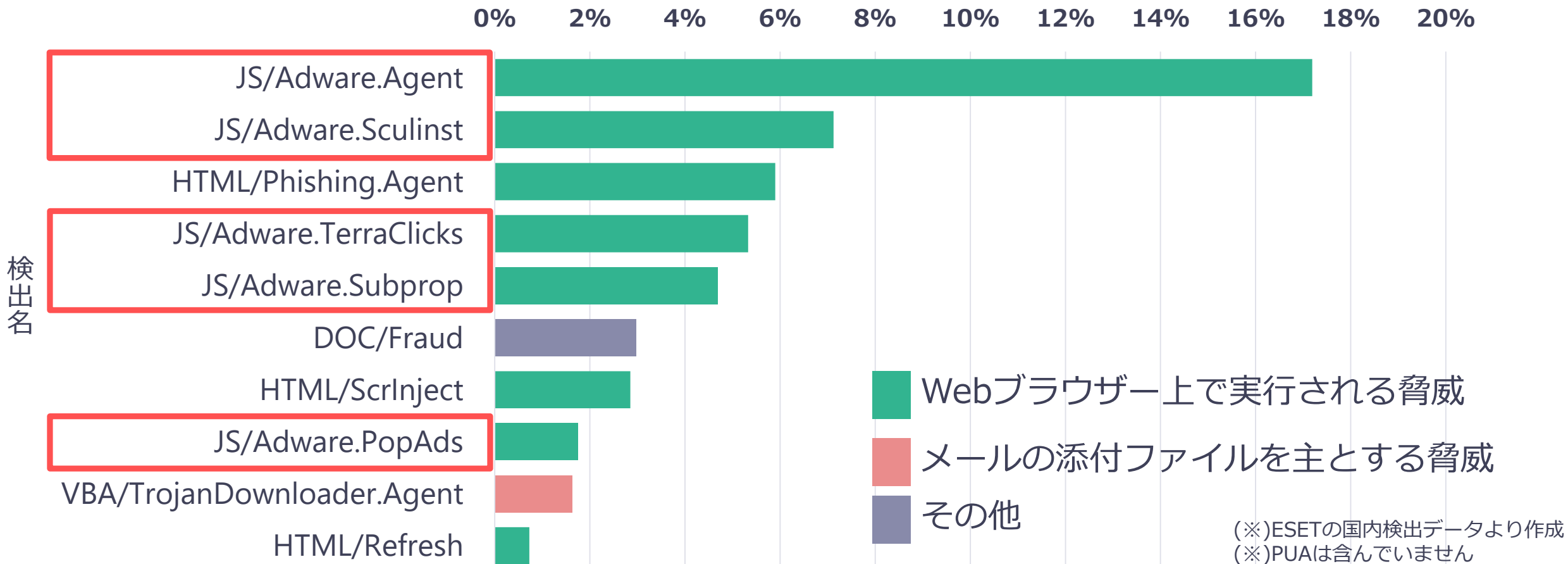
## 国内のマルウェア検出総数の推移



(※)ESETの国内検出データより作成

# 国内で検出されたマルウェアの内訳（2021年上半期）

## 検出数の上位10種



✓ 2020年に引き続き、検出の大多数をWebブラウザ上で実行される脅威が占める

✓ 電子メールの添付ファイルによる脅威も引き続き検出

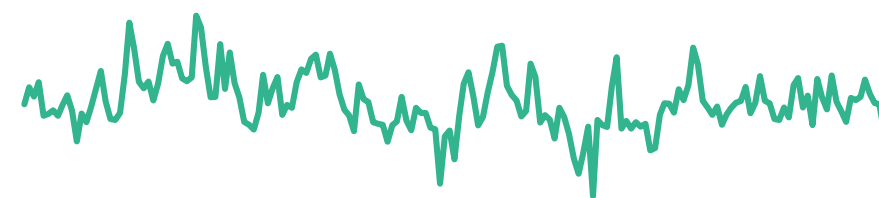
# Webブラウザ上で実行される脅威が増加



## アドウェア

Webブラウザ上などで実行され、  
不正な広告を表示するマルウェアの一種  
国内マルウェア検出数上位にも複数ある  
**JS/Adware** だけで、2021年上半期に  
日本で検出されたマルウェアの**47.9%**を占める

JS/Adware.Agentの国内検出数推移（2021年上半期）



1月1日 2月 3月 4月 5月 6月 6月30日

(※)ESETの国内検出データより作成

アドウェアの中には不正な広告を表示させるだけでなく、  
Webブラウザのアクセス履歴を外部へ送信するものもあるので注意が必要

**Webサイトアクセス時に不用意に許可やインストールを行わないことが重要**

# テレワークを狙う サイバー攻撃



# テレワーク等のニューノーマルな働き方を狙った攻撃

## IPA 情報セキュリティ10大脅威（組織）にもランクアップ

| 順位  |                          | 昨年<br>順位 |
|-----|--------------------------|----------|
| 1位  | ランサムウェアによる被害             | 5位       |
| 2位  | 標的型攻撃による機密情報の窃取          | 1位       |
| 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!     |
| 4位  | サプライチェーンの弱点を悪用した攻撃       | 4位       |
| 5位  | ビジネスメール詐欺による金銭被害         | 3位       |
| 6位  | 内部不正による情報漏えい             | 2位       |
| 7位  | 予期せぬIT基盤の障害に伴う業務停止       | 6位       |
| 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      |
| 9位  | 不注意による情報漏えい等の被害          | 7位       |
| 10位 | 脆弱性対策情報の公開に伴う悪用増加        | 14位      |

### 一部抜粋

2020年は新型コロナウイルス感染症（COVID-19）の世界的な蔓延に伴い、政府機関から感染症対策の一環として日本の組織に対してニューノーマルな働き方の一つであるテレワークが推奨された。組織のテレワークへの移行に伴いウェブ会議サービスやVPN等の本格的な活用が始まった中、**それらを狙った攻撃**が行われている。

# テレワーク等のニューノーマルな働き方を狙った攻撃

IPA 情報セキュリティ10大脅威（組織）にもランクアップ

順位

1位

2位

3位

4位

5位

6位

7位

8位

9位

10位



テレワーク環境に  
潜むリスク

順位

1位

2位

3位

4位

5位

6位

7位

8位

9位

10位



テレワーク環境を  
狙う攻撃

働き方

# テレワーク等のニューノーマルな働き方を狙った攻撃

IPA 情報セキュリティ10大脅威（組織）にもランクアップ

順位

1位

2位

3位

4位

5位

6位

7位

8位

9位

10位



テレワーク環境に  
潜むリスク

年  
順位

位

位

ew!

位

位

位

位

6位

位

4位



テレワーク環境を  
狙う攻撃

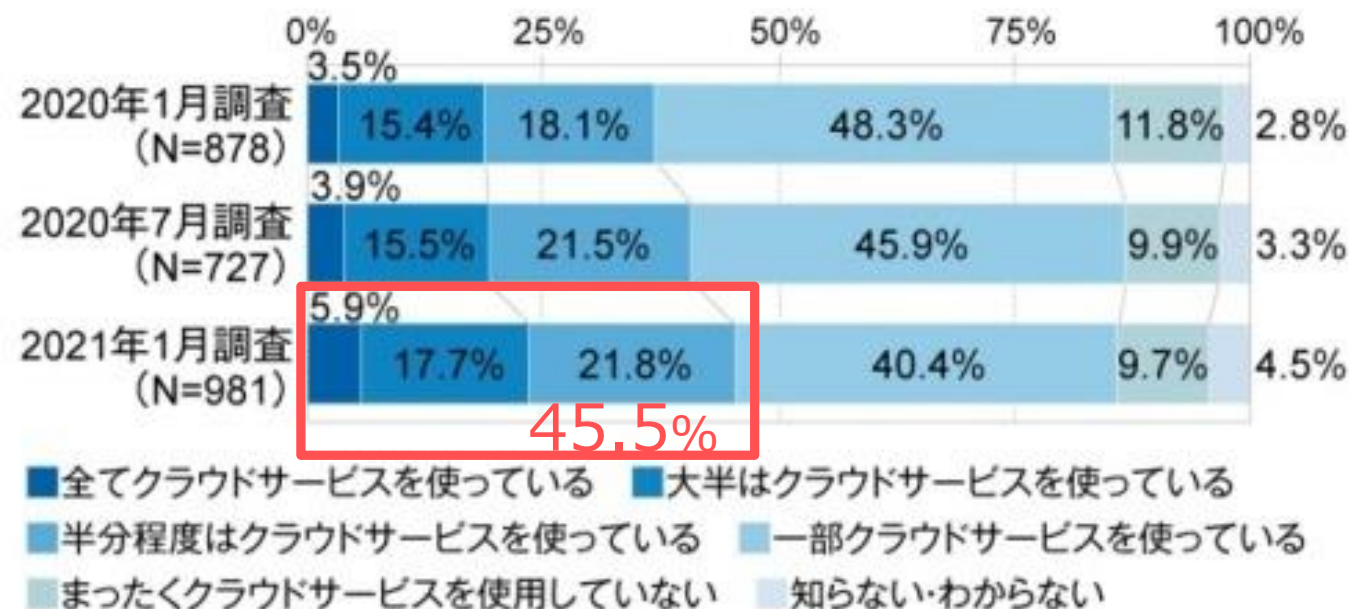
働き方

# コロナ禍におけるICT環境の変化

## クラウドサービスの利用範囲が拡大

コロナ禍によるテレワーク勤務の進展とともに、  
システムの約半分超をクラウド化した企業は1年前の37.0%から**45.5%**に上昇

### 都内企業のテレワーク実施率（東京都調べ） クラウドサービスの利用状況の推移



出典：JIPDEC（一般社団法人 日本情報経済社会推進協会）／ITR「IT-Report2021 Spring」  
<https://www.jipdec.or.jp/topics/news/20210318.html>

# クラウドサービスからの情報漏えい

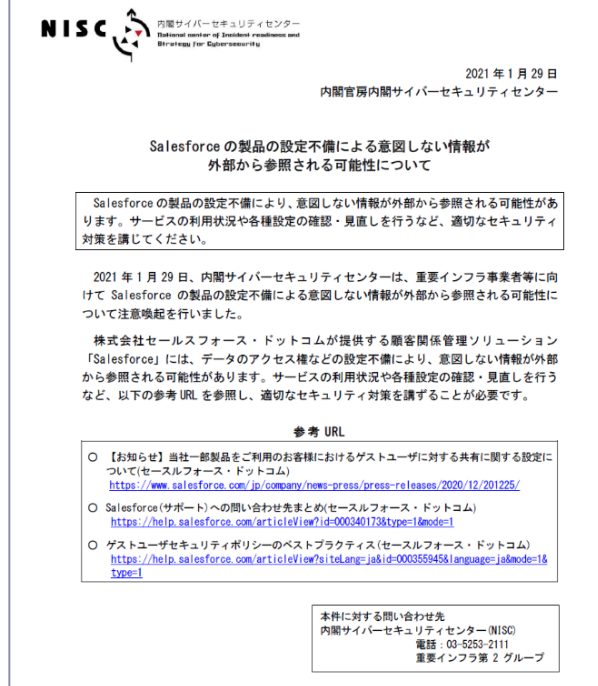
## Mis-Configuration

クラウドサービスの設定ミスによる情報漏えいが増加  
相次ぐ情報漏えいに、1月にはNISCからも注意喚起  
直近でも設定ミスによる意図しない情報露出を多く確認

クラウドサービスを利用する際は、**公開範囲などの設定**  
にご注意ください

クラウドサービスの設定ミスによる情報漏えい例（国内：2021年4月以降）

|                            |                                       |
|----------------------------|---------------------------------------|
| 地方自治体の<br>ワクチン接種予約サイト      | 接種予定者の個人情報（氏名）が操作を誤って公開               |
| オンラインセミナーサービス              | 設定ミスにより、アンケート回答者21名の情報が公開             |
| 婚活アプリ運営会社                  | システム設定の不備でお問い合わせフォームに投稿した記載内容を意図せず露出  |
| 地方放送局                      | アクセス負荷分散サービスの設定ミスにより視聴者応募データを誤表示      |
| 医療従事者等向け<br>「ワクチン接種予約システム」 | システムの設定ミスにより、接種予約者の個人情報が公開            |
| ソフトウェア開発会社など複数社            | 採用に関するサービスサイトの設定ミスにより、採用面接対象者の個人情報が公開 |

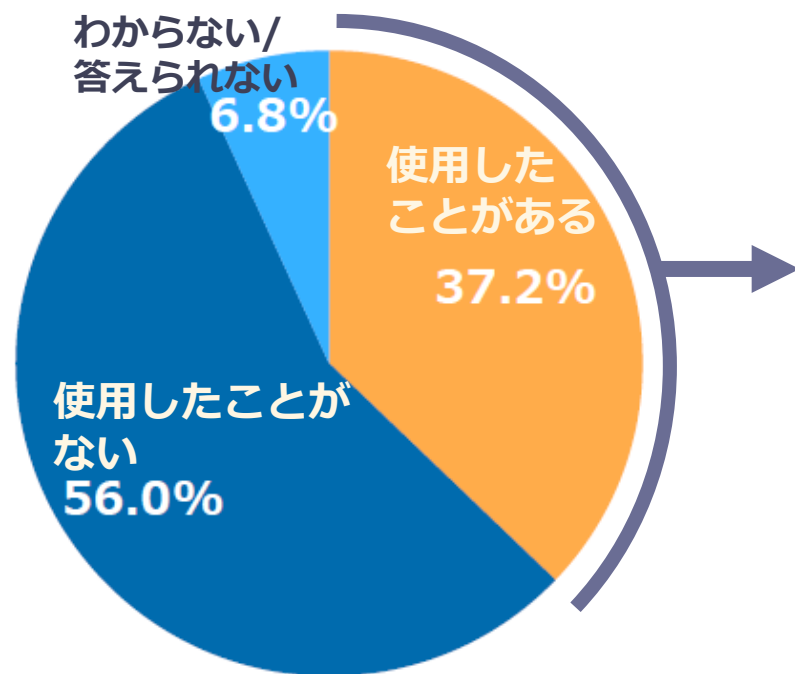


# 個人端末の業務利用

## 4割近くが「個人所有の端末」を業務で利用

テレワーク実施のため、個人所有端末の業務利用が増加

### 過去1年間に個人端末を業務に使用した人の割合と個人端末の使用頻度



| 頻度           | 回答割合  |
|--------------|-------|
| 週に3回以上       | 32.7% |
| 週に1～2回程度     | 26.5% |
| 月に1～3回程度     | 18.8% |
| 3か月に1～2回程度   | 7.6%  |
| 6か月に1回程度     | 3.6%  |
| 1年間に1回程度     | 2.7%  |
| 分からない/答えられない | 8.1%  |

59.2%

企業が管理できない個人所有端末は必要な対策ができず、  
マルウェア感染等による情報セキュリティリスクが高いと考えられる

# 管理が徹底できない個人所有端末のリスク例

12台に1台のPCがOSのサポート切れ

2020年1月14日にWindows 7、10月13日にOffice2010のサポートが終了

日本国内におけるWindows 7のシェアは8.13%

サポート終了後も多くのWindows 7 PCが稼働中

投影のみ

# サポート終了後のOSを使用するリスク

## 半年で158件の脆弱性

2019年1～6月の間に登録された脆弱性の内、  
Windows 7に関連する脆弱性は158件。

うち、**87件**が深刻度が高いCVSS7.0以上の脆弱性

危険度が高い脆弱性が発見されても、

サポート期限終了後は、原則として

セキュリティ更新プログラムが提供されないため、

**結果として、脆弱性を悪用した攻撃による**

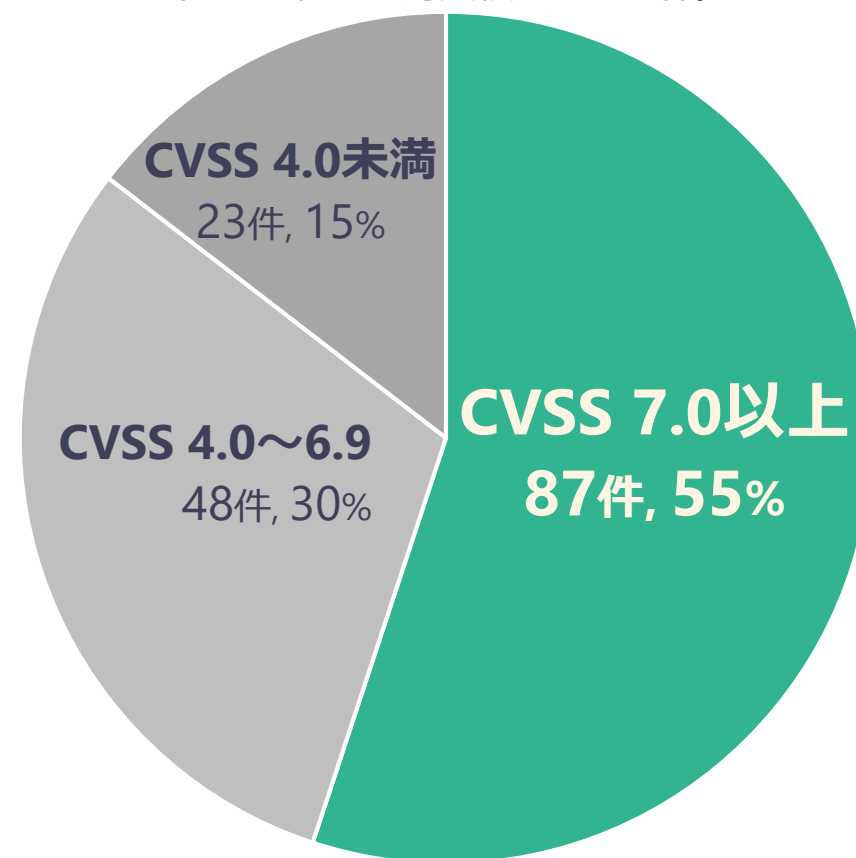
**情報漏えいや意図しないサービス停止などの被害が**

**生じる可能性が高くなる**

使用しているPCのOSやアプリケーションが

**サポート期限を迎えている場合は速やかにアップグレードを検討**

Windows7の脆弱性内訳  
(2019年1～6月実績：全158件)



# テレワーク等のニューノーマルな働き方を狙った攻撃

IPA 情報セキュリティ10大脅威（組織）にもランクアップ

順位

1位

2位

3位

4位

5位

6位

7位

8位

9位

10位



テレワーク環境に  
潜むリスク

順位

1位

2位

3位

4位

5位

6位

7位

8位

9位

10位



テレワーク環境を  
狙う攻撃

働き方

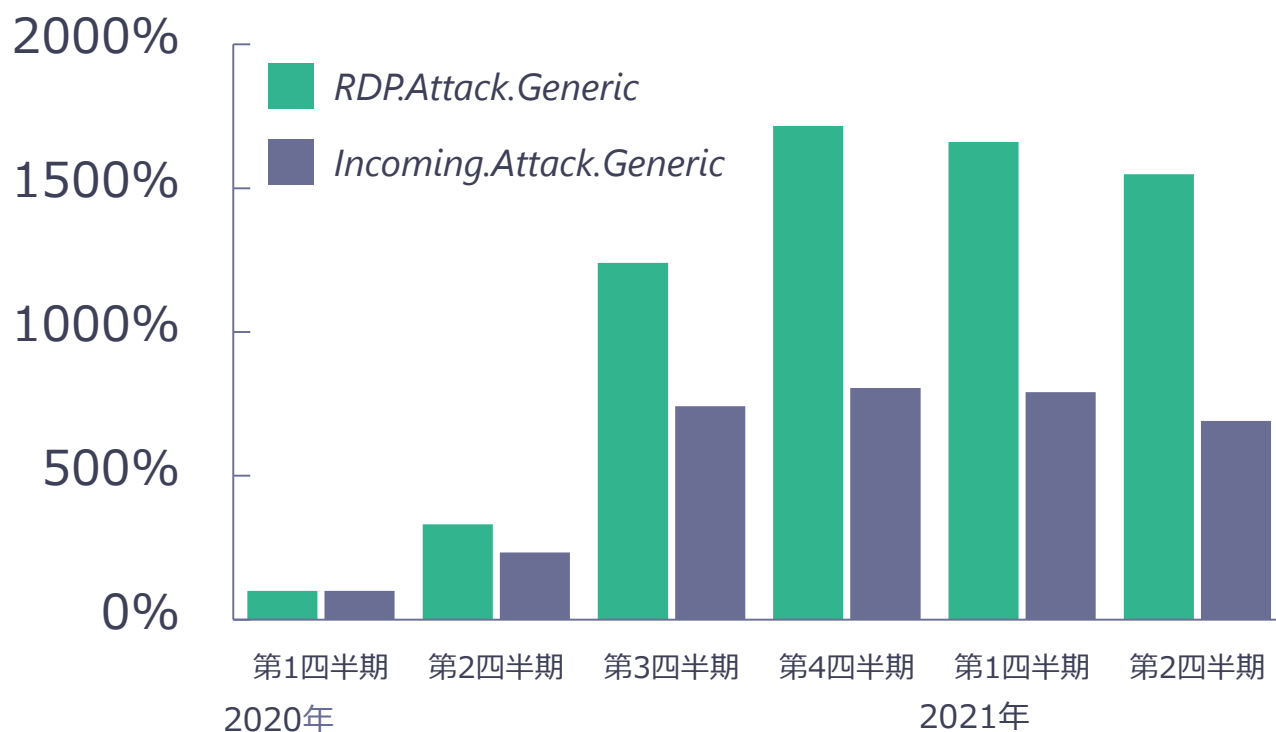
# テレワークで使用するサービスを狙う攻撃例

## RDPを使用した攻撃の増加

RDPをインターネット上に公開している機器が世界的に増加(※)

(※)参考 : Shodan | Trends in Internet Exposure <https://blog.shodan.io/trends-in-internet-exposure/>

**BlueKeep(CVE-2019-0708), DejaBlue (CVE-2019-1181/1182)**など、  
RDPの深刻な脆弱性のパッチが未適用の機器も確認されており注意が必要



ランサムウェアの感染経路や  
窃取された認証情報がダークウェブ上で  
売買されるなど、

**様々な被害につながる可能性**

使用する場合は、VPNとの併用や、  
接続にあたり十分な認証を行うなど

**セキュリティ対策と組み合わせて使用**

(※)ESETの国内検出データより作成

# VPN機器の脆弱性を悪用する攻撃例

## 脆弱性を悪用するためのコードの公開も確認

脆弱性対策が不十分なまま利用を続けてしまうと、攻撃者に脆弱性を悪用され、認証情報や組織の機密情報が外部に流出する等の被害に遭うおそれ

### **Pulse Secure製VPN機器の脆弱性**

|         |                                |
|---------|--------------------------------|
| 2019年4月 | 脆弱性情報公開                        |
| 2019年8月 | 脆弱性の悪用を狙ったとみられるスキャンを確認         |
| 2019年9月 | 脆弱性を悪用したとみられる攻撃を確認             |
| 2020年8月 | <b>国内外900社（国内は38社）の認証情報が公開</b> |

### **Fortinet製FortiOSのSSL VPN機能の脆弱性**

|          |                                                                |
|----------|----------------------------------------------------------------|
| 2019年5月  | 脆弱性情報公開                                                        |
| 2019年8月頃 | 脆弱性の詳細情報公開、悪用やスキャン開始                                           |
| 2020年11月 | <b>脆弱性の影響を受ける約5万台の機器情報が公開<br/>（IPアドレス、ユーザーアカウント名、平文パスワード等）</b> |

セキュリティパッチが  
公開されている場合は  
速やかに適用をご検討ください

攻撃が確認されている期間に  
古いファームウェアのまま  
使用されていた方は  
侵害有無の確認、  
認証情報の変更を推奨します

参考：JPCERT/CC |

Fortinet 社製 FortiOS の SSL VPN 機能の脆弱性 (CVE-2018-13379) の影響を受けるホストに関する情報の公開について

<https://www.jpcert.or.jp/newsflash/2020112701.html>

複数の SSL VPN 製品の脆弱性に関する注意喚起 <https://www.jpcert.or.jp/at/2019/at190033.html>

参考：経済産業省 | 最近のサイバー攻撃の状況を踏まえた経営者への注意喚起

<https://www.meti.go.jp/press/2020/12/20201218008/20201218008-1.pdf>

# 漏えいした認証情報

## ランサムウェアの初期感染経路

Palo alto Networks UNIT42の調査では、  
2020年にランサムウェアが導入されたケースの**50%**でRDPが初期の攻撃経路

参考 : Palo Alt Networks | 2020 Unit 42 Incident Response and Data Breach Report  
<https://www.paloaltonetworks.com/resources/research/2020-unit42-incident-response-and-data-breach-report>

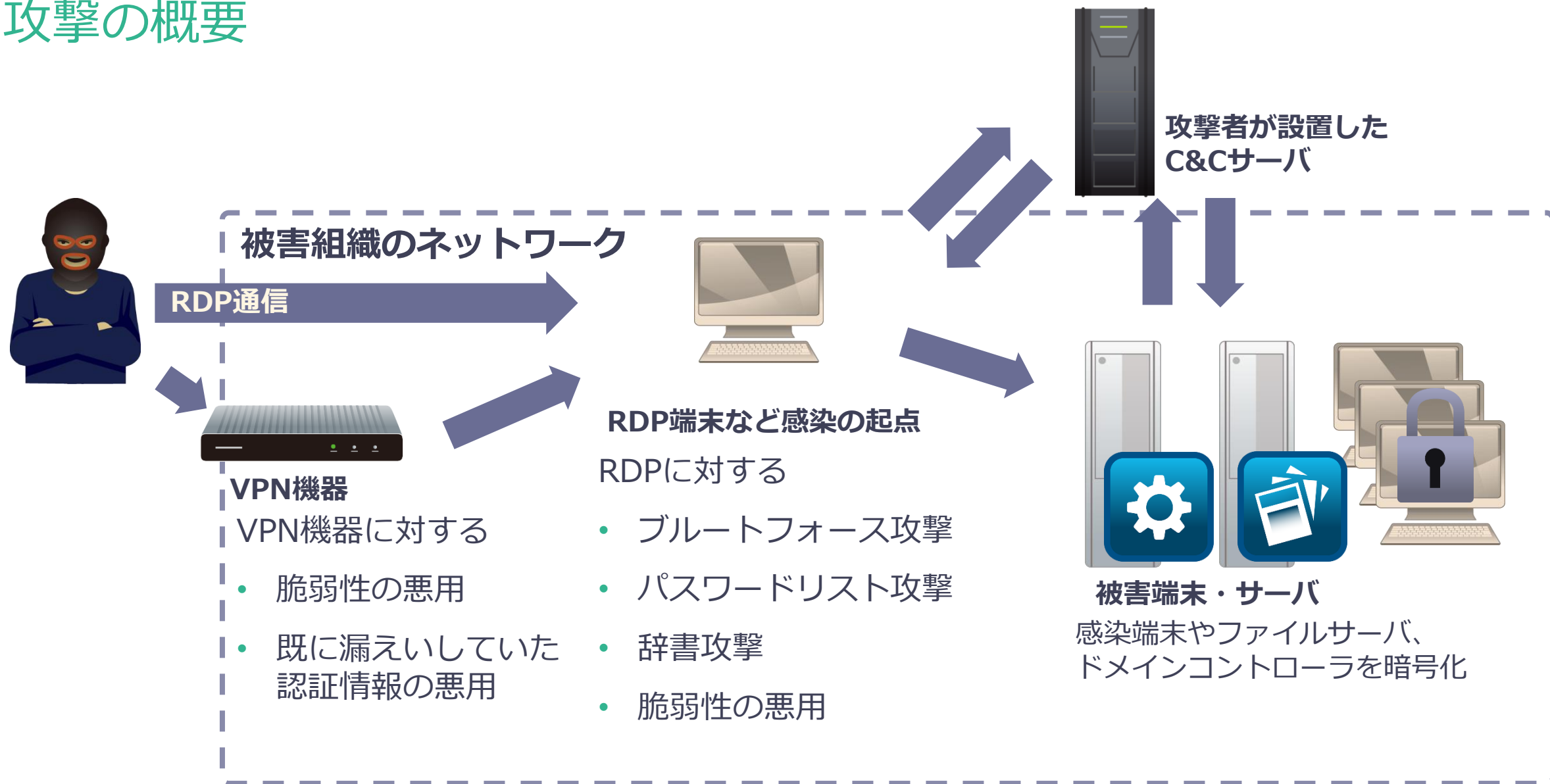
ダークウェブ上で取引されている  
RDP,VPN機器の認証情報のほか、  
**情報提供可能な内通者を募集**する  
攻撃者グループの存在も確認

投影のみ

ランサムウェア攻撃者グループによる、  
RDPやVPN機器の認証情報を提供する内通者募集告知  
暗号化されたPCに壁紙として表示される

# RDP、VPN機器を侵入経路にしたランサムウェア攻撃例

## 攻撃の概要



# 凶悪化するランサムウェア

## 四重の脅迫

ランサムウェアによる暗号化だけではなく、様々な脅迫（攻撃）手法を**併用**

### 四重の脅迫（2021~）

DarkSide

顧客や  
取引先に  
嫌がらせ

### 三重の脅迫（2020~）

Avaddon

DDoS

### 二重の脅迫（2019~）

Maze, Revil

機密情報の暴露

暗号化

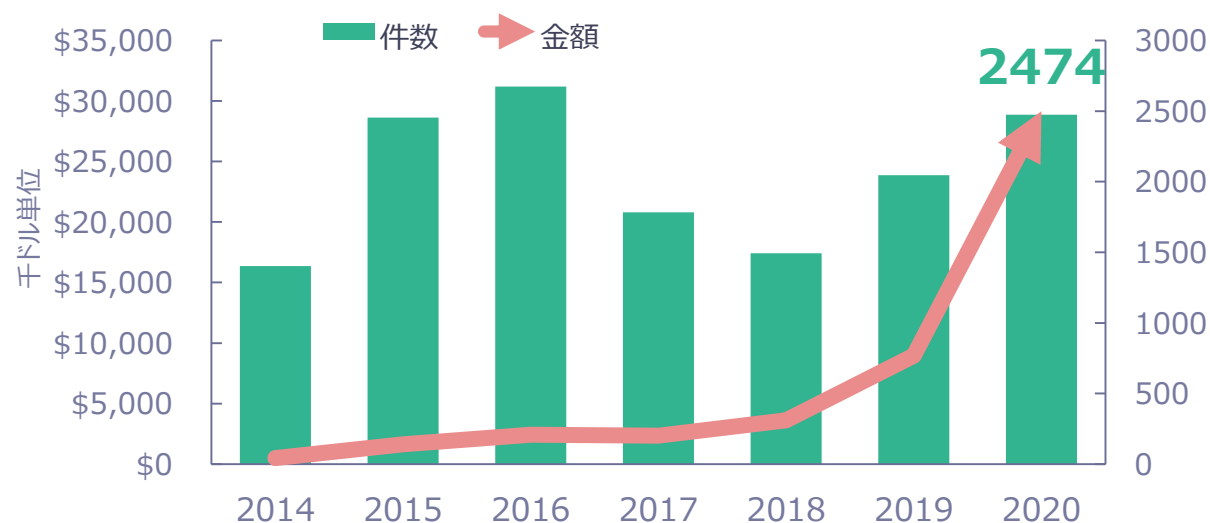
# 凶悪化するランサムウェア

## 被害金額の増加

四重の脅迫など、ランサムウェア攻撃者の攻撃手法の凶悪化とともに  
ランサムウェア被害の発生件数と被害金額が増加

2021年1Qの身代金平均額は**\$220,298（約2,400万円）**（Coveware社）

### ランサムウェア被害発生件数と被害金額（米国）



### ランサムウェアによって支払われた身代金

投影のみ

参考：Internet Crime Complaint Center (IC3) のデータをもとに作成

<https://www.ic3.gov/>

出典：Coveware

<https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound> Cyber Security Laboratory © Canon IT Solutions Inc.

# インシデント被害発生時の損害額

## インシデント損害額調査レポート

インシデント発生時に必要となる各種対応、  
その対応によって生じるコスト（損害額・損失額）  
を取りまとめ



# モデルケース：軽微なマルウェア感染

従業員がメールに添付されていたファイルを開いたところ、マルウェアに感染

- 至急、出入りのITベンダー経由で、インシデントレスポンス事業者に対応を依頼  
感染内容、被害範囲等の調査を実施
- 調査の結果、メールを介して感染が拡大するマルウェアであり、従業員端末3台とサーバー1台の感染が判明
- 個人情報の漏えいのおそれなど、顧客影響等はないことが確認

**損害額：600万円**

## 内訳

- 事故原因・被害範囲調査  
500万円
  - 端末3台、サーバー1台の調査
- 再発防止策：100万
  - メールフィルタリングサービスの導入

**ランサムウェアに感染した場合、事故原因・被害範囲調査がより困難となり復旧費用も必要となるため、より大きな損失額となることが想定される**

## # 本日は話すこと

1. 2021年上半期の  
サイバーセキュリティ脅威動向
2. 対策のポイント

# 対策のポイント



## 脆弱性への対応

- セキュリティパッチの適用
- 脆弱性診断の活用



## 製品の適切な利用

- 適切な設定で使用する
- 最新の状態を保つ
- 複数の層で守る



## 被害を受けた場合を 想定した対策

- 情報資産の適切な管理
- ログモニタリング
- インシデント発生時の対応を明確化



## 情報収集と セキュリティ教育

- 脅威情報の収集
- 脅威を知ってもらう
- ガイドラインの参照・適応

# Web会議サービスに関するガイドライン

## Web会議サービスを使用する際のセキュリティ上の注意事項

### Web 会議サービスを使用する際のセキュリティ上の注意事項

2020 年 7 月 14 日  
独立行政法人情報処理推進機構  
セキュリティセンター

#### 1. はじめに

新型コロナウイルス感染症の影響により在宅勤務が広く行われ、Web 会議サービスの利用が急速に拡大しています。Web 会議サービスの活用は大変有益である一方、盗聴、情報漏えい、サイバー攻撃等のセキュリティリスクに十分注意する必要があります。

本資料では、Web 会議の主催者が、Web 会議サービスを使用する際に注意すべきセキュリティ上のポイントを紹介いたします。

(注) 本資料における「Web 会議サービス」は、音声、映像、資料、チャット等をリアルタイムに交換可能なクラウドサービスとします(オンプレミスは除きます)。代表的な Web 会議サービスに関しては(※1)を参照下さい。

#### 2. 対象とする読者

法人組織の Web 会議主催者、および、情報システム管理部門

#### 3. Web 会議サービス選定時に考慮すべきポイント

Web 会議サービスを選定する際にセキュリティ上考慮すべきポイントを以下に示します。これらは、セキュリティリスクを極力軽減し、Web 会議サービスを安全に使用するために考慮すべき項目です。なお、米国家安全保障局 (NSA: National Security Agency)、CISA (Cybersecurity and Infrastructure Security Agency) が公表している政府職員向けの Web 会議サービス使用時の注意事項<sup>(※2、※3)</sup>を参考にしています。

##### 3. 1 会議データの所在

- Web 会議サービスは、音声、映像、共有資料、チャット、録画・録音データ等、多種のデータを扱います。これらのデータがどこに格納されるかは、情報漏えいリスクに大きく影響します。主催者は使用する Web 会議サービスがクラウドサービス、オンプレミスのいずれかを、まず確認することが必要です。
- クラウドサービスの場合、負分散のため海外のデータセンターが利用されることがあります(図1参照)。データセンターが置かれた国によっては、政府が法に基づきデータを強制収容するリスクがあります。どの国のデータセンターを使用するかは通常契約で決められますが、無料サービスでは契約プロセスを通さないため、本件は特に注意が必要です。
- クラウド上に録画・録音データを保存する場合には、復元不可能な形で完全削除ができるか(セキュアデリート機能の有無)の確認も重要です。

Web会議サービスを選定する際に考慮すべきポイントや、安全に開催するためのポイントを紹介

## Web 会議サービス選定時に考慮すべきポイント

- 会議データの所在
- 暗号化
- 会議参加者の確認・認証方式
- プライバシーポリシー
- 脆弱性と企業姿勢

# テレワークのセキュリティに関するガイドラインやチェックリスト

## テレワークセキュリティガイドライン

### 中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）



#### テレワークセキュリティガイドライン

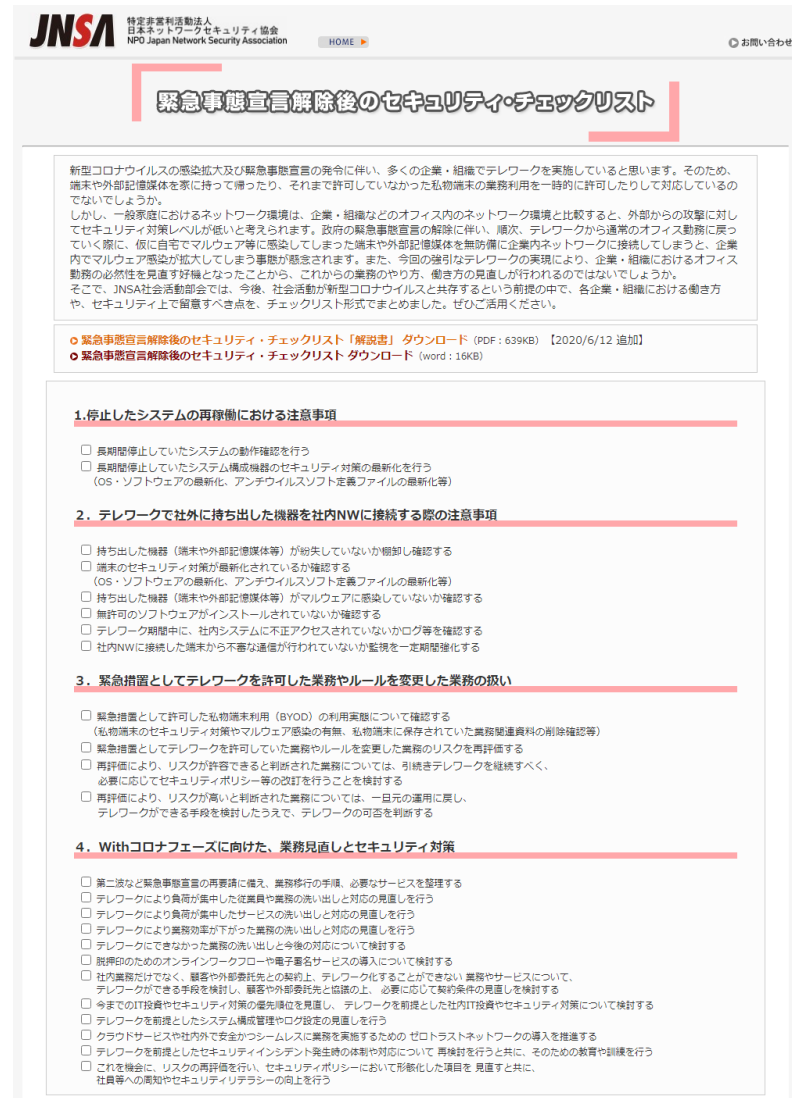
テレワークを実施する際のセキュリティ上の不安を払拭し、安心してテレワークを導入・活用するための指針として、**テレワークの導入に当たってのセキュリティ対策についての考え方や対策例を示したガイドライン**

#### 中小企業等担当者向けテレワークセキュリティの手引き

セキュリティの専任担当がない中小企業等におけるシステム管理担当者を対象とした、**テレワークを実施する際に最低限のセキュリティを確実に確保するための手引き（チェックリスト）**

# テレワークのセキュリティに関するガイドラインやチェックリスト

## 緊急事態宣言解除後のセキュリティ・チェックリスト（ JNSA ）



テレワークなどで、  
一般家庭のネットワーク環境など  
オフィス内のネットワークと比べ、  
セキュリティ強度の低い環境で使  
用した端末等を、  
再びオフィスで使用する際の注  
意点・懸念点などを  
チェックリスト化

# サイバーセキュリティ情報局のご紹介

キヤノンマーケティングジャパンと  
ESETが提供する最新のセキュリティ情報

最新のセキュリティ動向やキーワード解説のほか  
サイバーセキュリティラボがまとめた  
日本におけるマルウェア動向を  
詳細なレポートにて提供

情報収集にご活用ください

サイバーセキュリティ情報局

Search

