今こそ振り返る！

2020年の サイバーセキュリティ脅威動向と 対策のポイント

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

自己紹介

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

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

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

Cyber Security Lab © Canon IT Solutions Inc.

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

＃本日お話しすること

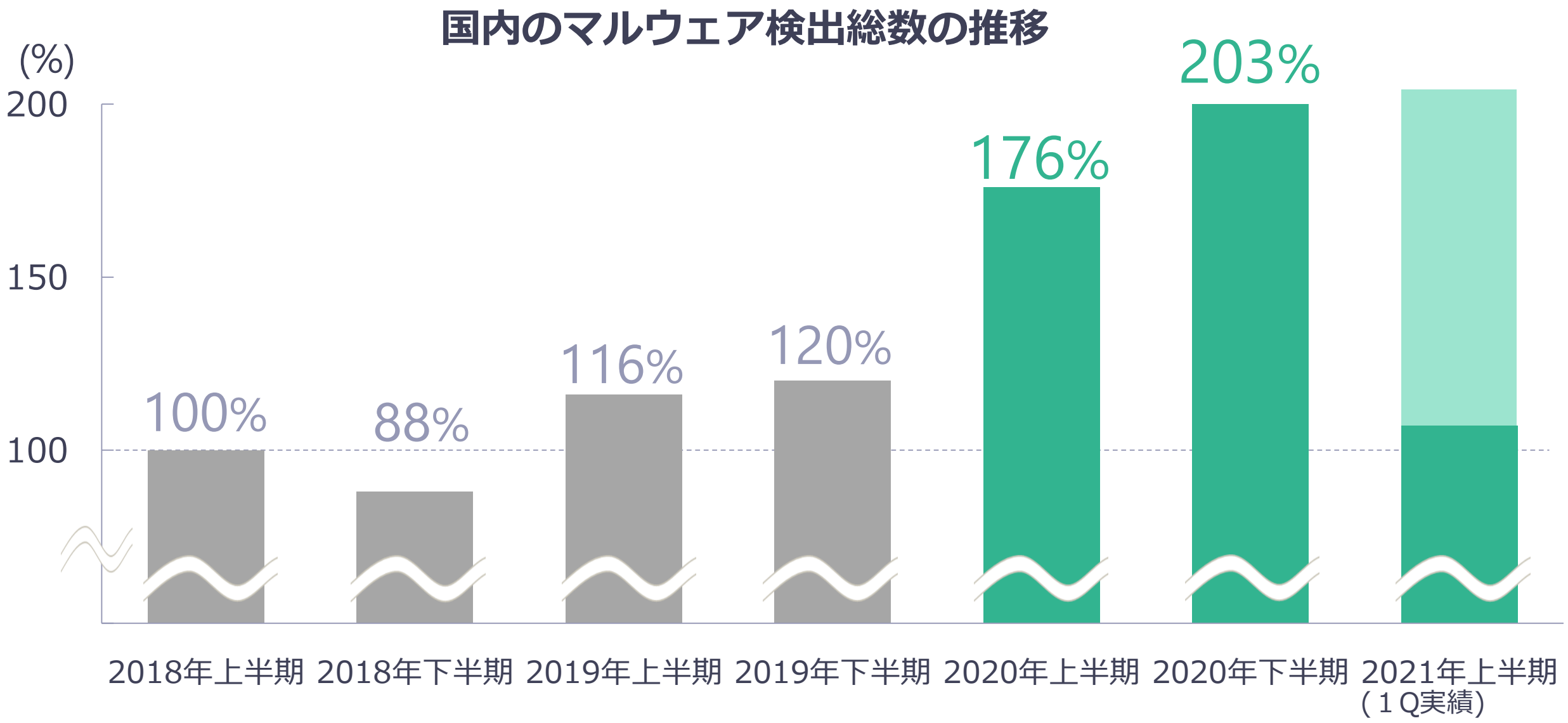
1. 2020年の
   サイバーセキュリティ脅威動向
2. 対策のポイント

＃本日お話しすること

1. 2020年の
   サイバーセキュリティ脅威動向
2. 対策のポイント

Malware

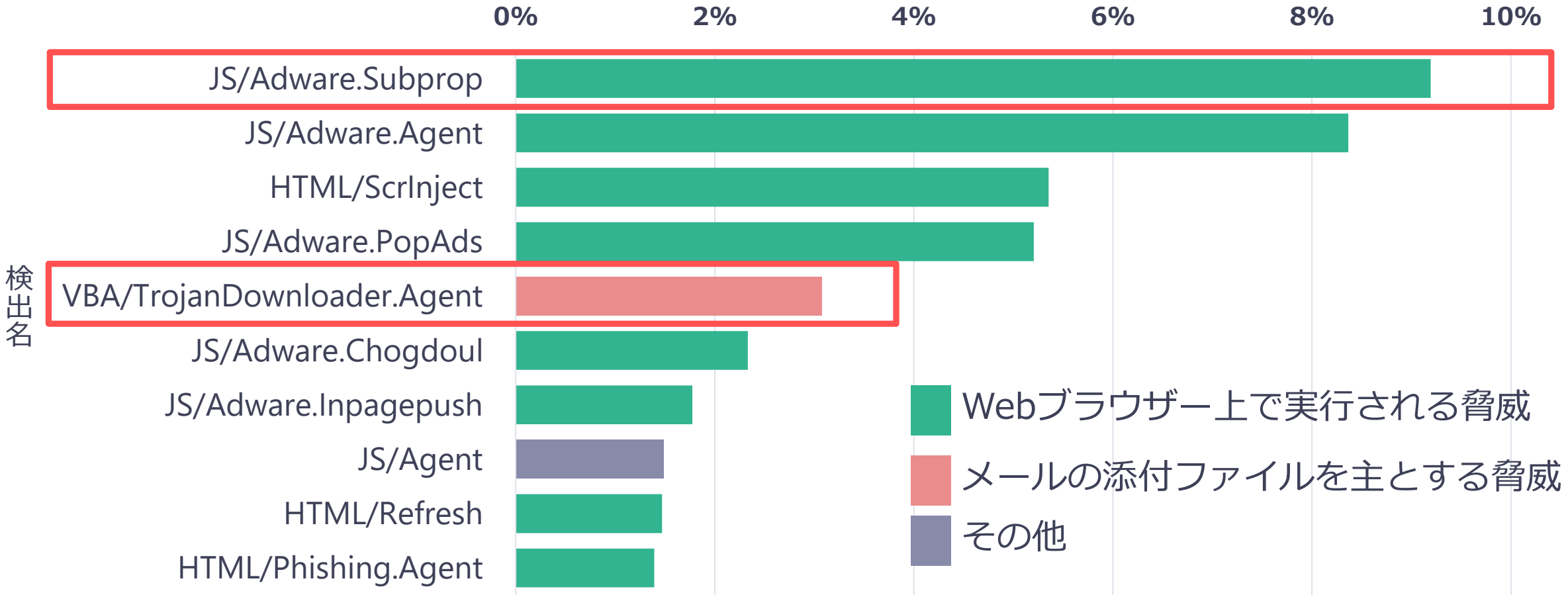
国内のマルウェア動向



Cyber Security Lab © Canon IT Solutions Inc.

国内で検出されたマルウェアの内訳（2020年）

検出数の上位10種



✓ 検出の大多数をWebサイト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

(※)PUAは含んでいません

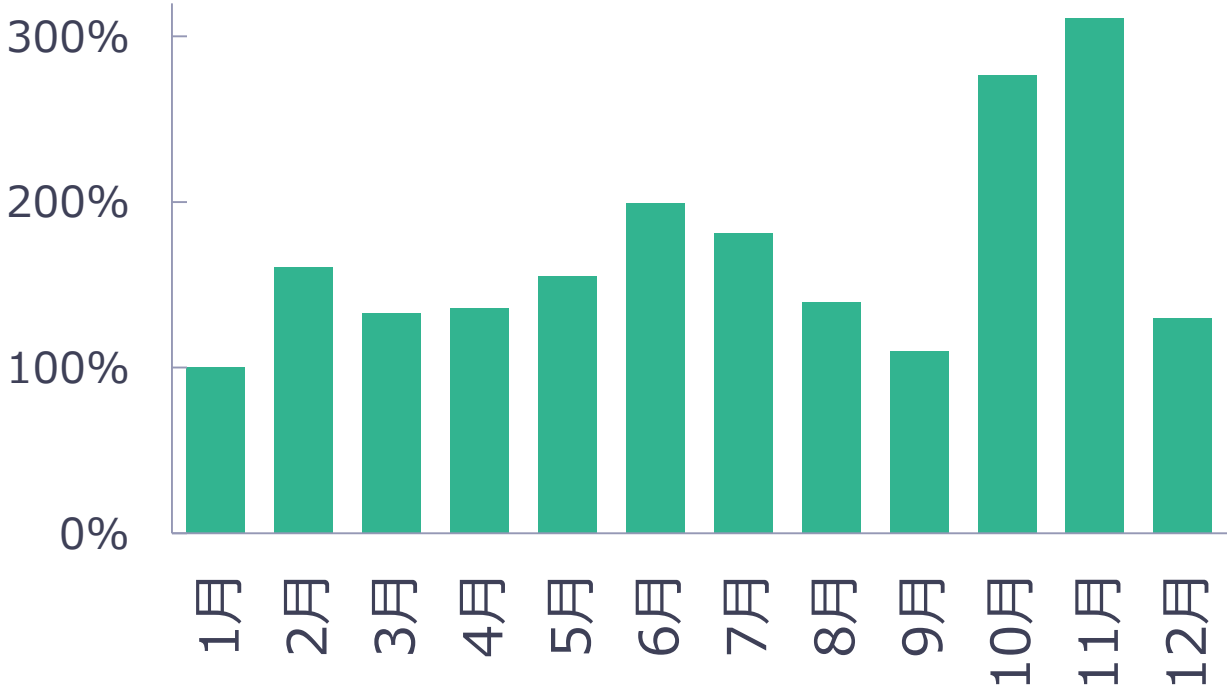
Cyber Security Lab © Canon IT Solutions Inc.

Webサイトで実行される脅威の例

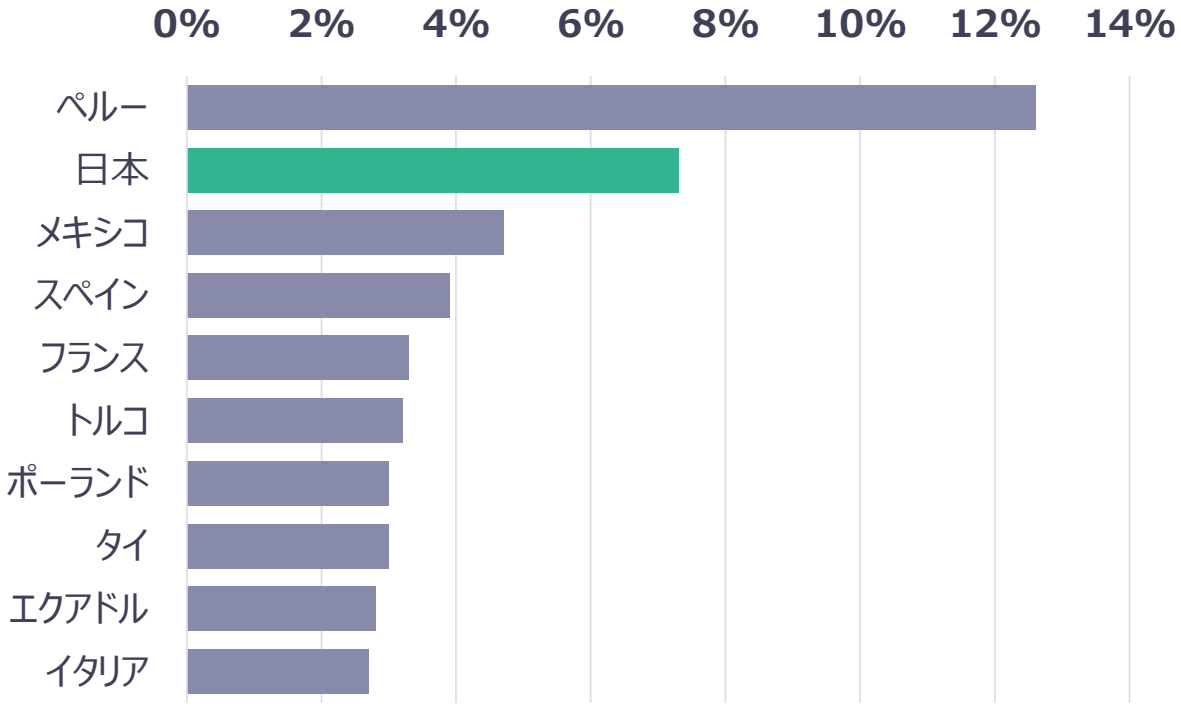
JS/Adware.Subprop

2020年、日本及び全世界で最も多く検出されたマルウェア
偽のAdobe Flash Playerのアップデートや、有名ベンダーのWebバナーを悪用し、悪意あるコンテンツや不要なソフトウェアを配布するスクリプト

国内検出数推移（2020年）



検出数 TOP10の国と地域（2020年）



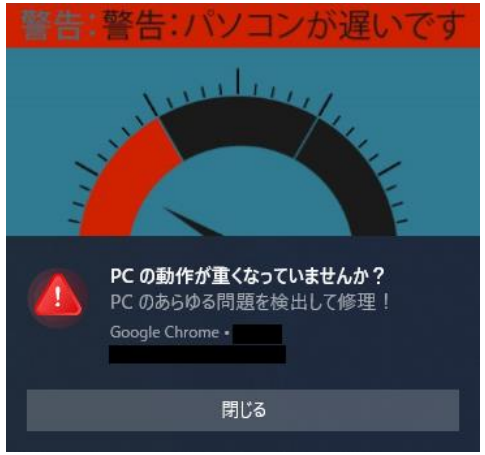
Cyber Security Lab © Canon IT Solutions Inc.

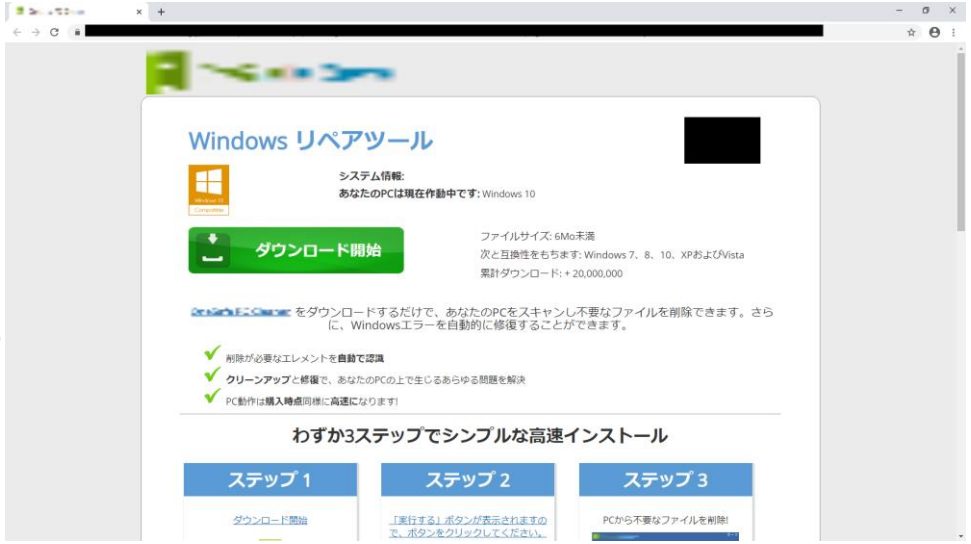
JS/Adware.Subprop: 感染例

JS/Adware.Subpropが仕込まれたサイトにアクセスし、
ポップアップ等でJavaScriptの実行を許可すると感染。
感染すると、デスクトップ画面に広告が表示。
広告をクリックすると、誘導先のWebサイトにアクセス

感染例

PCの動作が遅くなったと偽った広告が表示
クリックすると、Windowsを
リペアするためと称したツールを
インストールさせようとするサイトに誘導





アドウェアの中には、このような不正な広告を表示させるもの以外にも、
Webブラウザー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。

不用意に許可やインストールを行わないことが重要

JS/Adware.Subpropは2020年6月のマルウェアレポートで詳しく解説しています
https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware2006.html

Cyber Security Lab © Canon IT Solutions Inc.

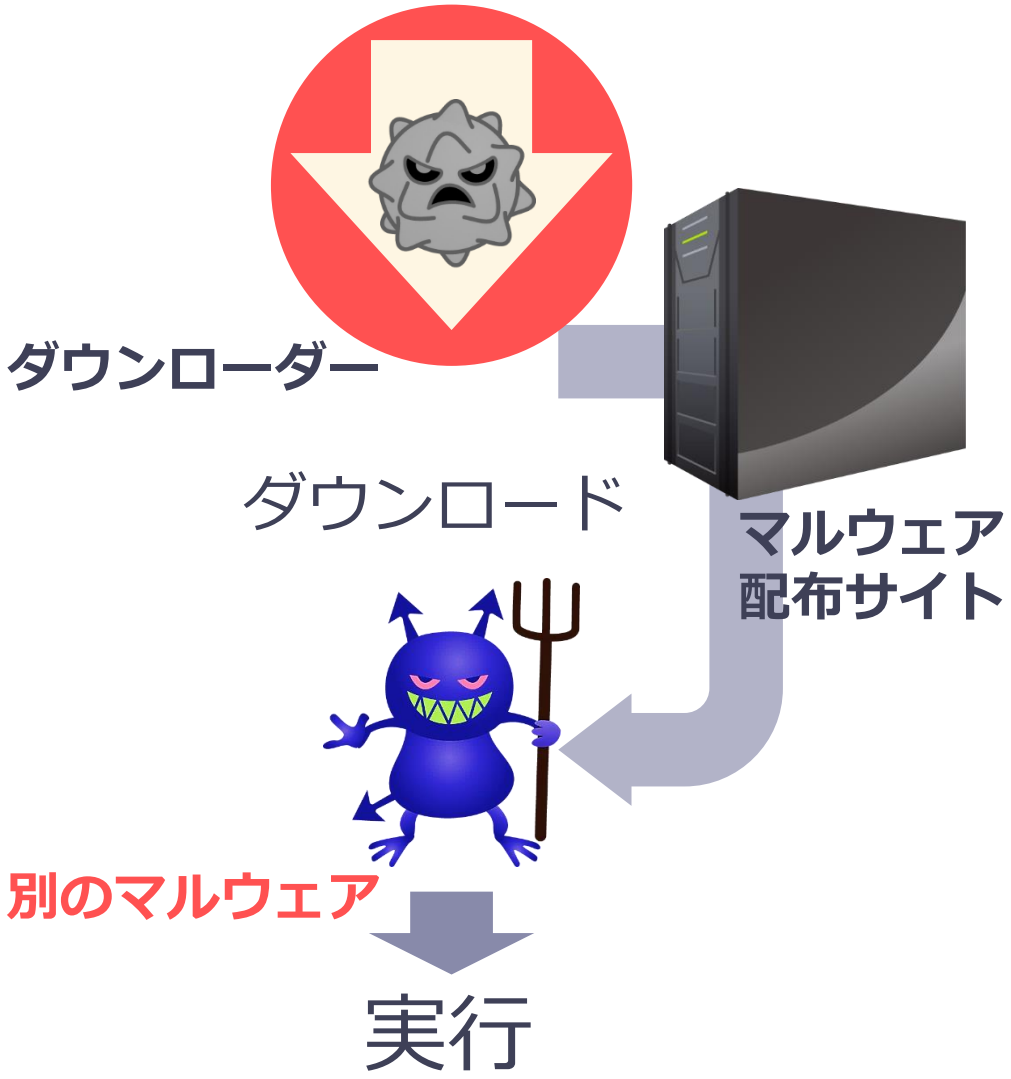
電子メールの添付ファイルを主とする脅威

VBA/TrojanDownloader.Agent

Office製品で利用されるVBA
（Visual Basic for Application）で
作成されたダウンローダー

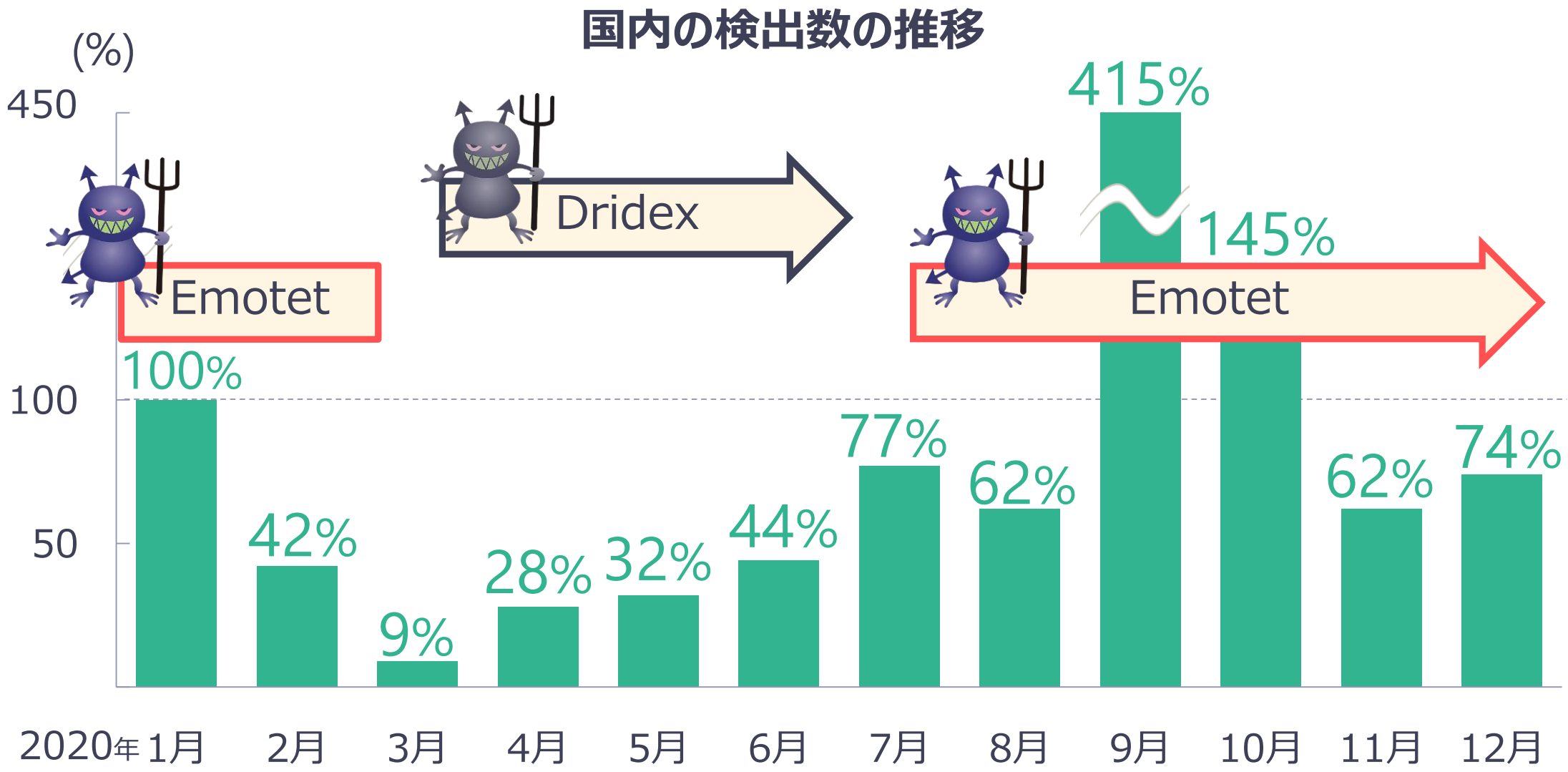
ダウンローダー

感染したシステムに悪意のあるソフトウェアを
ダウンロードし、実行することを目的とする
不正なプログラム



Cyber Security Lab © Canon IT Solutions Inc.

VBA/TrojanDownloader.Agentの検出数推移



サイバーセキュリティ情報局にて、「Dridex」について、詳細な解析レポートを公開しています
https://eset-info.canon-its.jp/malware_info/trend/detail/201120.html

Cyber Security Lab © Canon IT Solutions Inc.

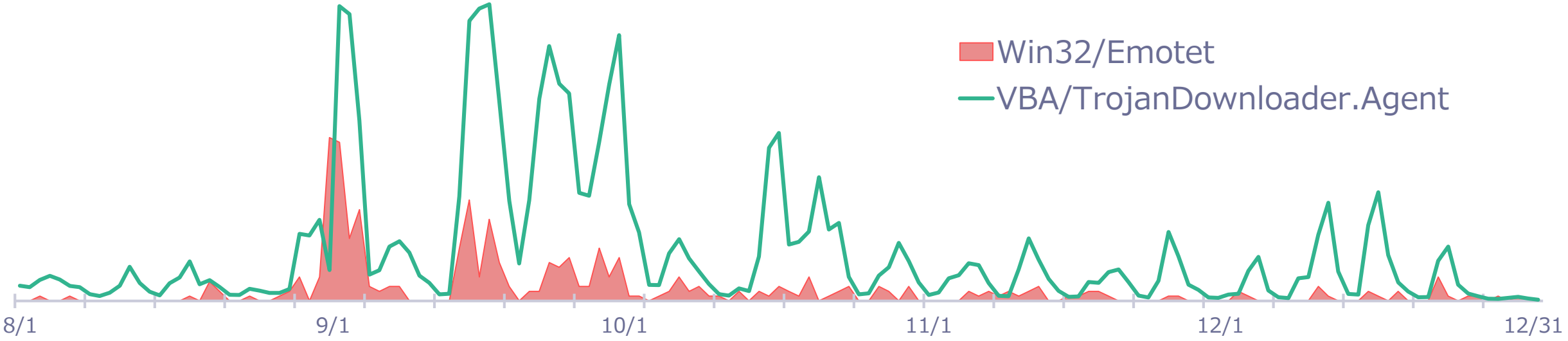
Emotet

2014年5月から全世界で確認されているマルウェア

国内では2019年10月から2020年2月にかけて少なくとも3,200の組織が感染
2月初旬以降、活動は確認されていなかったが、7月中頃から活動再開

2021年1月末にユーロポールを中心とした「Operation Ladybird」により
テイクダウンされるまで日本を含む全世界に大きな被害をもたらした

2020年8月以降のEmotetとVBA/TrojanDownloader.Agentの検出数推移（国内）



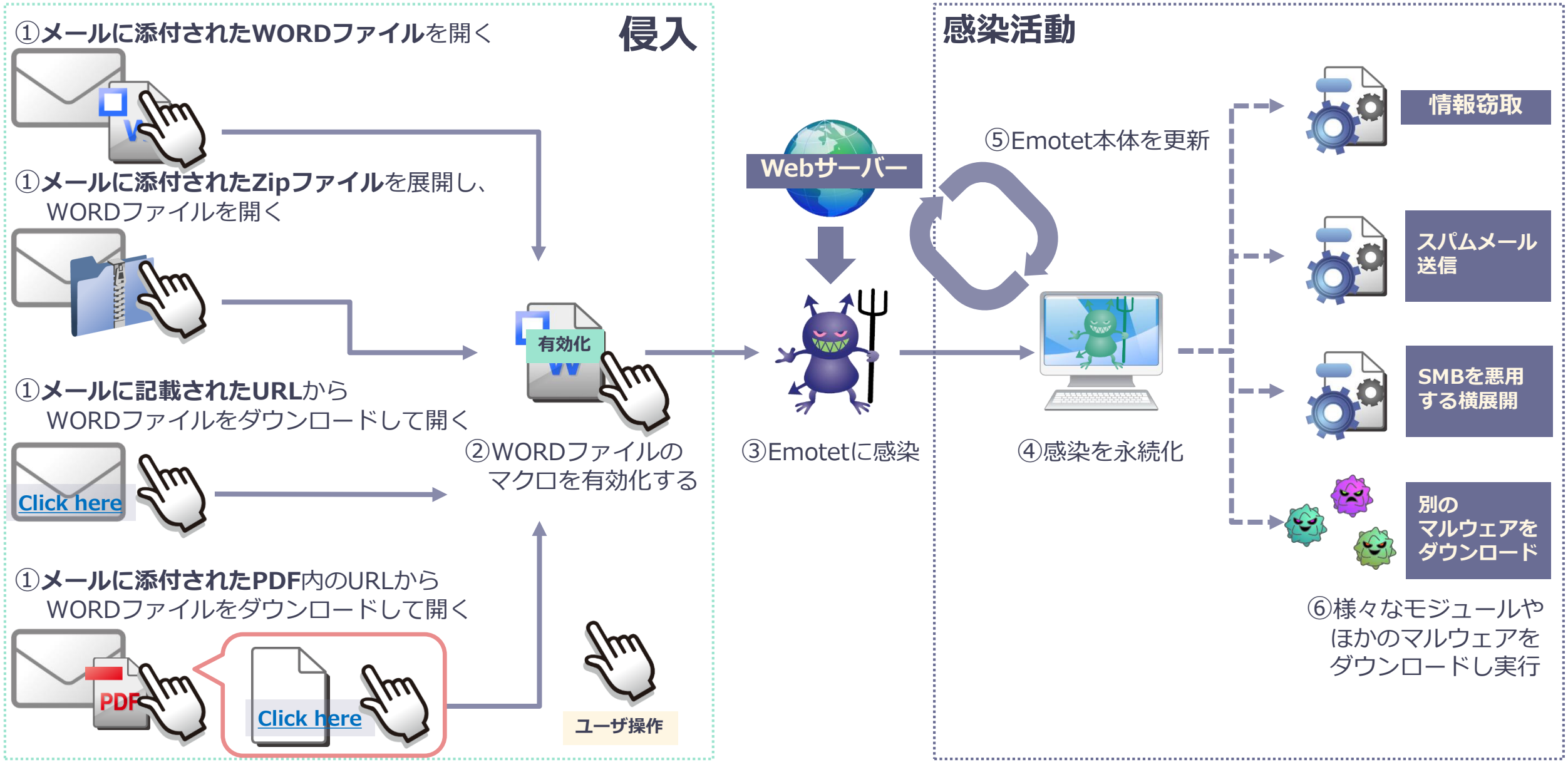
(※)日本国内でESETが検出した攻撃数をもとに作成

出典：JPCERT CC |マルウエア Emotet の感染に繋がるメールの配布活動の再開について (追加情報)
https://www.jpcert.or.jp/newsflash/2020072001.html

Cyber Security Lab © Canon IT Solutions Inc.

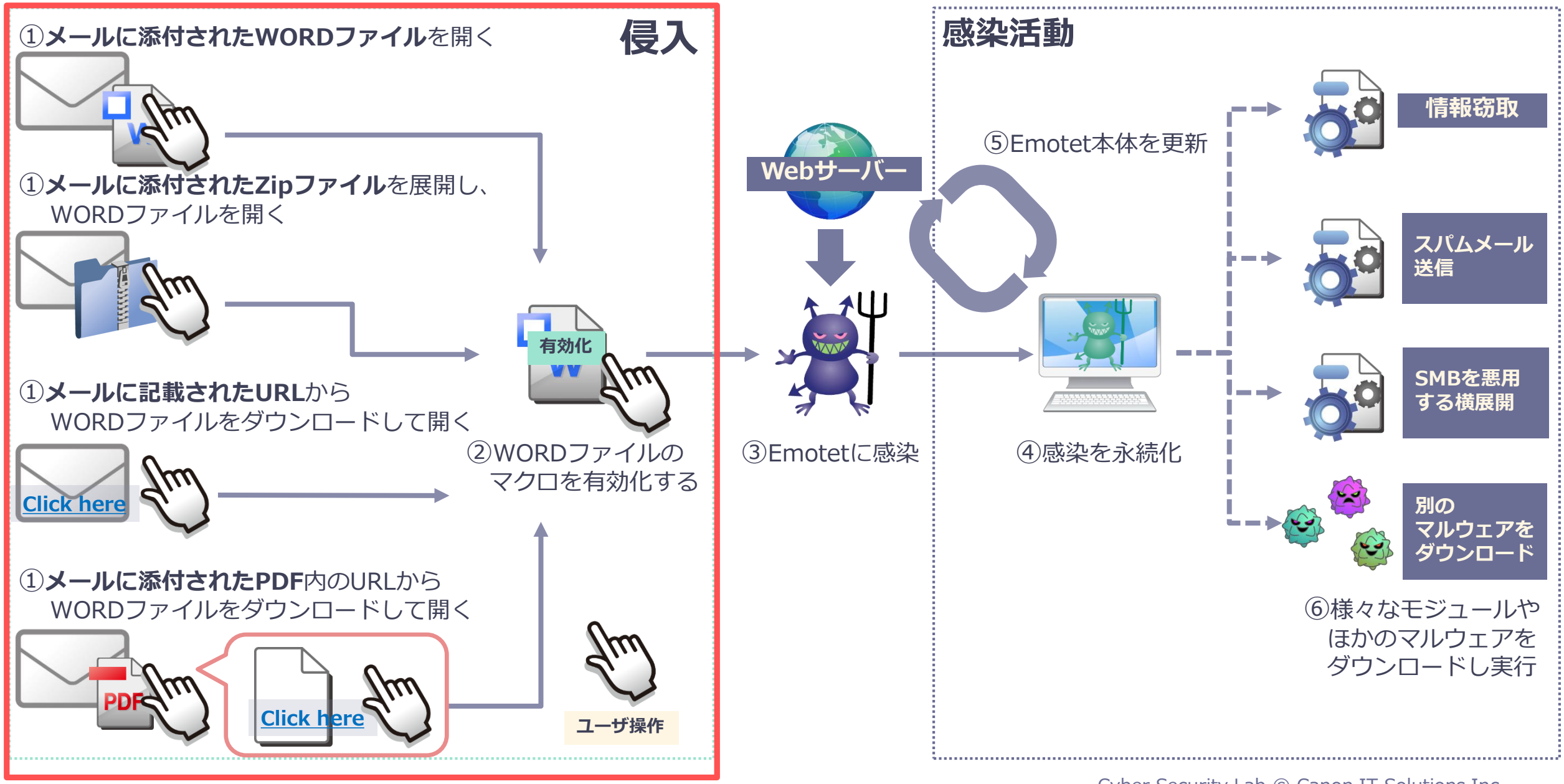
なぜ、Emotetはこれほど大きな被害につながったのか？

感染の流れ



Cyber Security Lab © Canon IT Solutions Inc.

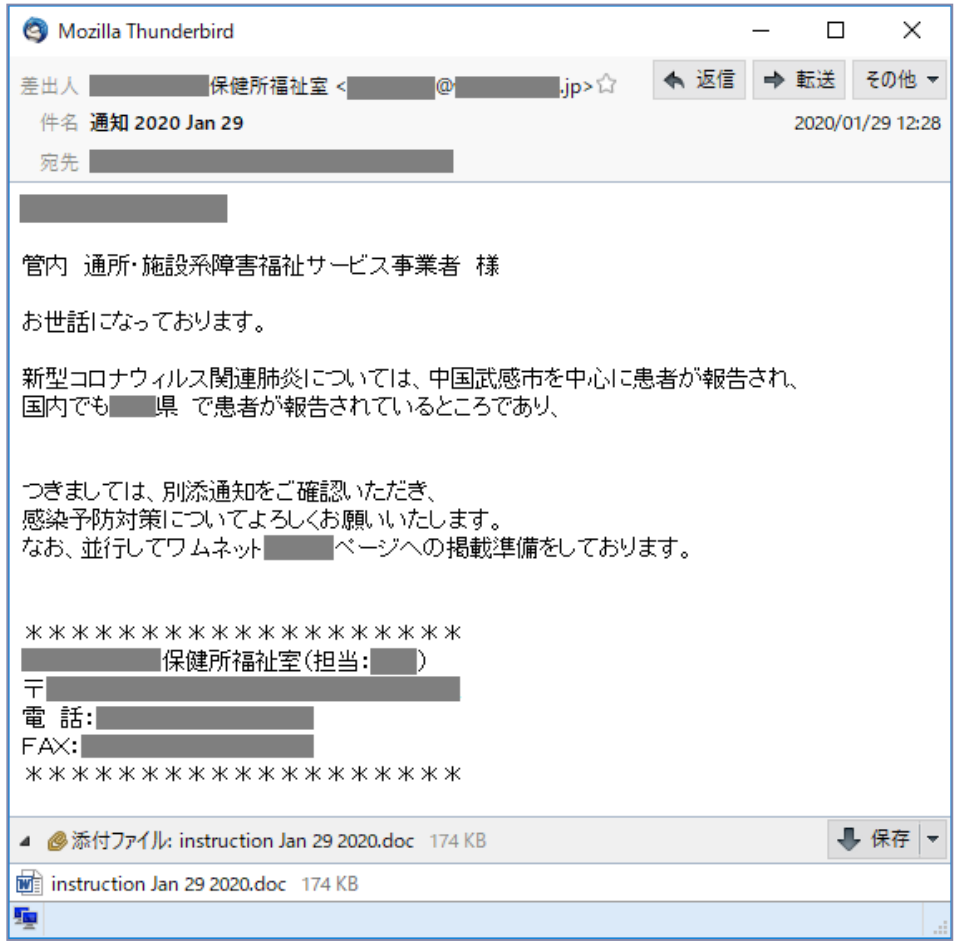
感染の流れ



Cyber Security Lab © Canon IT Solutions Inc.

Emotetの侵入手口

多く使われた手口であり、多数の感染につながった理由



Emotet感染端末から盗み出された情報を元に

心理的に添付ファイルを開きやすいメールを使用

- 送信メールに対する返信を装う返信型
- 時節、対象地域の文化に合わせた

  キーワードを盛り込む
  - “賞与”など日本文化に合わせたキーワード
  - **新型コロナウイルス感染症の流行**など

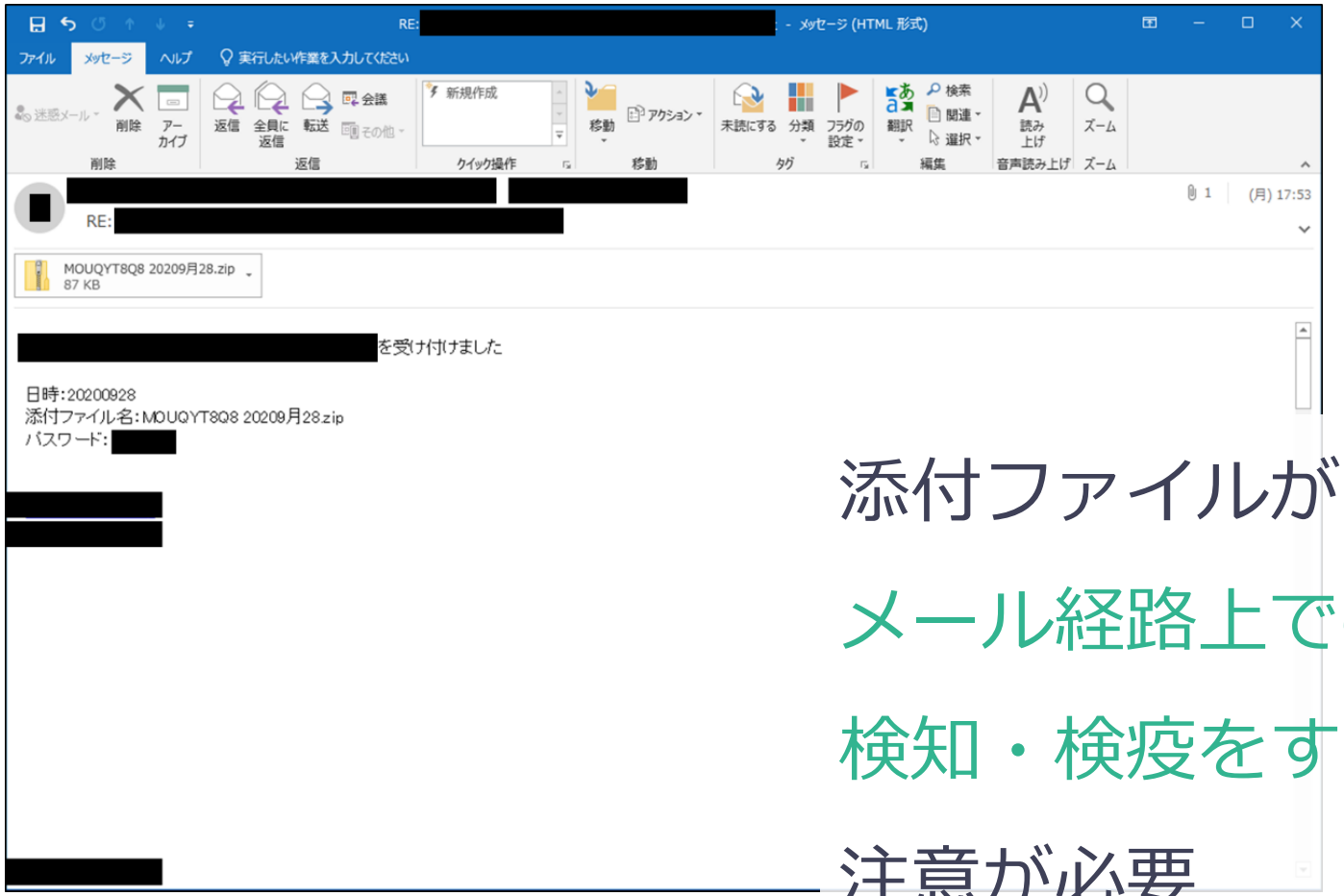
    旬のキーワード

出典： IPA |「Emotet」と呼ばれるウイルスへの感染を狙うメールについて
https://www.ipa.go.jp/security/announce/20191202.html

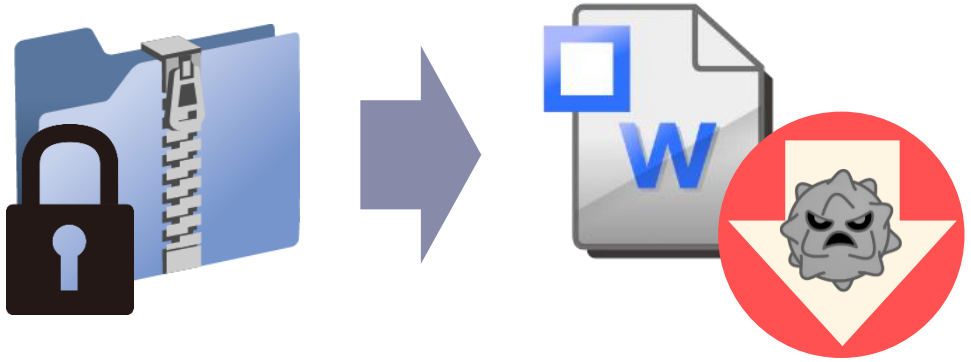
Cyber Security Lab © Canon IT Solutions Inc.

2020年9月以降に確認された手口

パスワード付きZIPファイルを使用する事例（2020年9月下旬に確認）



展開すると、
ダウンローダー付きWORDファイル



添付ファイルが暗号化されていることにより、

メール経路上でのセキュリティ製品の

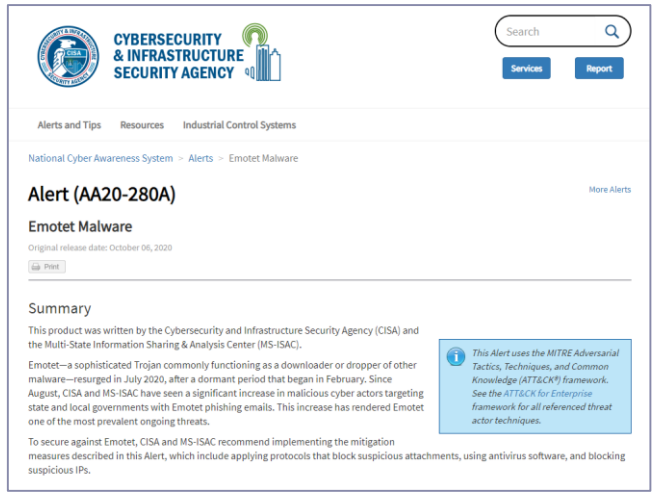
検知・検疫をすり抜ける可能性が高いため、

注意が必要

Cyber Security Lab © Canon IT Solutions Inc.

参考情報：メールでのパスワード付きZIP利用縮小の動き

投影のみ



日本

中央省庁の職員が文書などのデータを
メールで送信する際に使う
パスワード付きZIPファイルを廃止する方針

米国

CISAがEmotetの緩和策として、
パスワード付きZIPファイルのブロックを提言

Mitigations（抜粋）

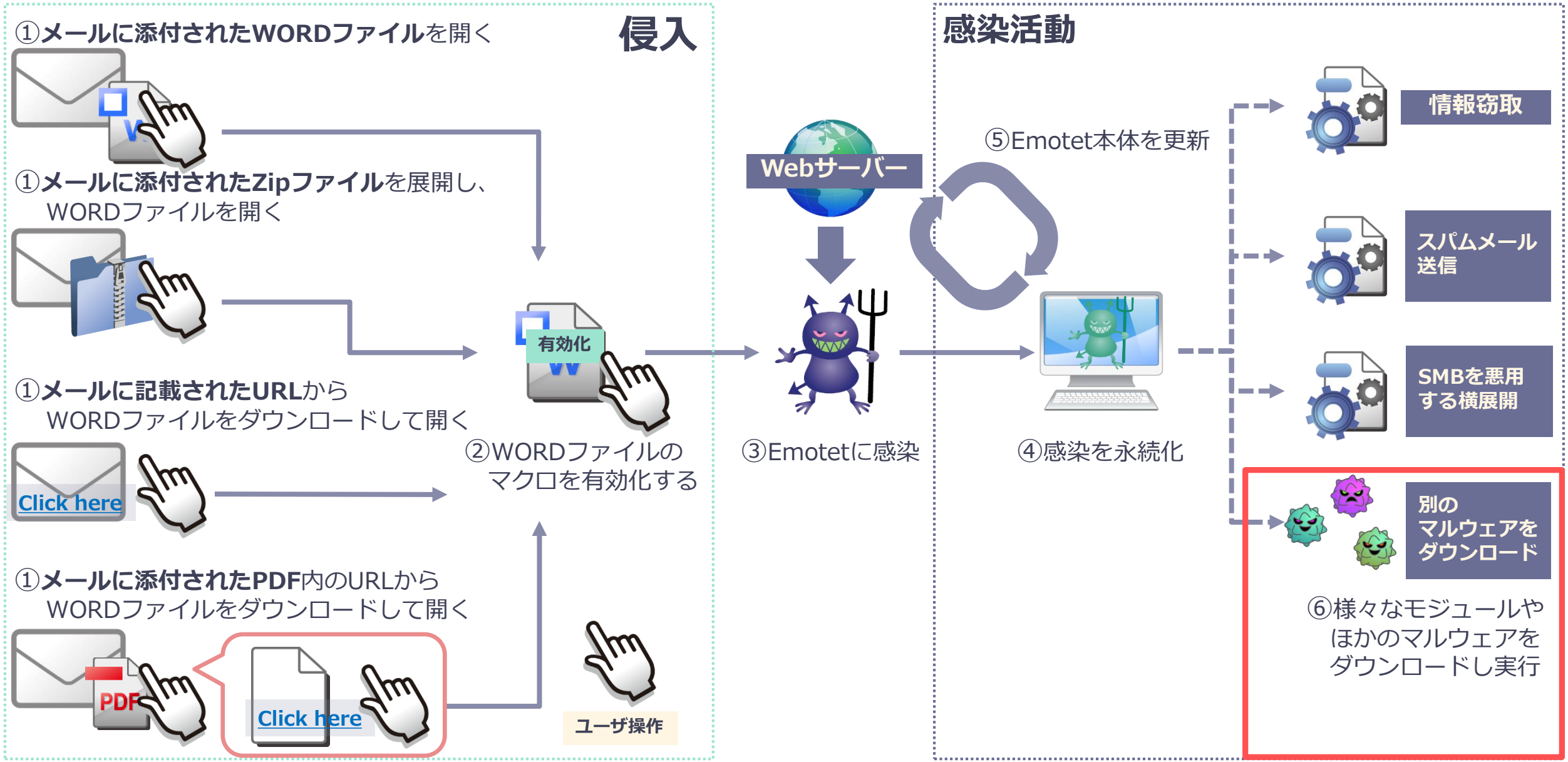
Block email attachments that cannot be scanned by antivirus software (e.g., .zip files).

※CISA:米国土安全保障省 サイバーセキュリティ・インフラセキュリティ庁

出典： CISA | Alert（Emotet Malware）https://us-cert.cisa.gov/ncas/alerts/aa20-280a

Cyber Security Lab © Canon IT Solutions Inc.

感染の流れ



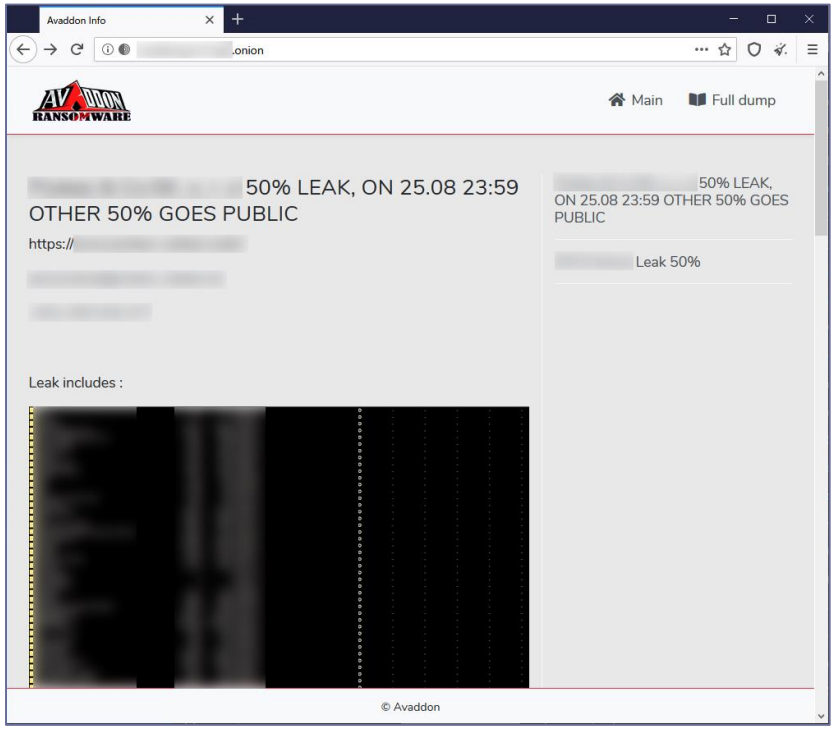
Cyber Security Lab © Canon IT Solutions Inc.

凶悪化するランサムウェア

ドキシング（晒し）による二重の恐喝

暗号化されたファイルを復号するための
身代金要求に加え、
「事前に盗み出されたデータを公開する」と脅し、
更なる身代金を要求する手口が登場

身代金の支払いを拒否したことにより、機密情報が
インターネット上に公開されてしまったケースも確認



犯罪者グループが運営するリークサイト
ドキシングが行われている

バックアップ等により、ランサムウェア被害に
備えている企業にとっても、
ランサムウェアがより大きな脅威に

サイバーセキュリティ情報局にて、「Avaddon」ランサムウェアについて、詳細な解析レポートを公開しています
https://eset-info.canon-its.jp/malware_info/trend/detail/201027.html

テレワーク環境を狙う
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。

参考：IPA｜情報セキュリティ10大脅威 2021
https://www.ipa.go.jp/security/vuln/10threats2021.html

Cyber Security Lab © Canon IT Solutions Inc.

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	**国内外900社（国内は38社）の認証情報が公開**

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	**脆弱性の影響を受ける約5万台の機器情報が公開** **（IPアドレス、ユーザーアカウント名、平文パスワード等）**

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

Cyber Security Lab © Canon IT Solutions Inc.

テレワークで使用するサービスを狙う攻撃例

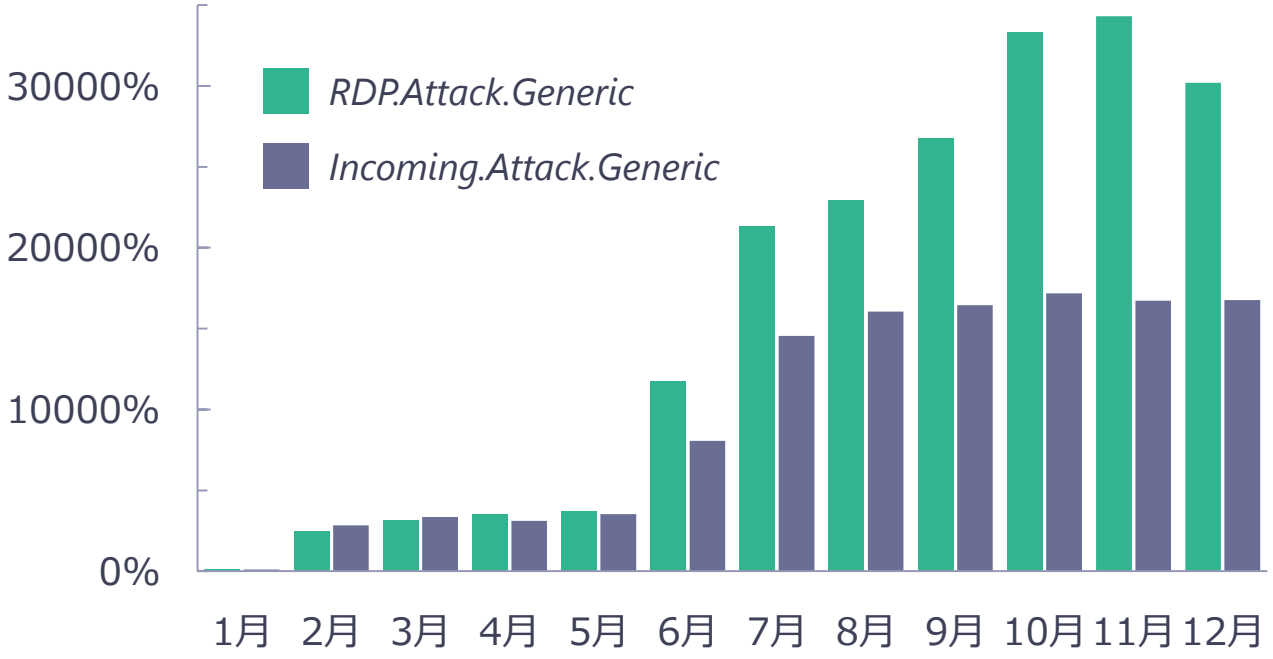
RDPを使用した攻撃の増加

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

国内のRDPを使用した攻撃検出数の推移（2020年）



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

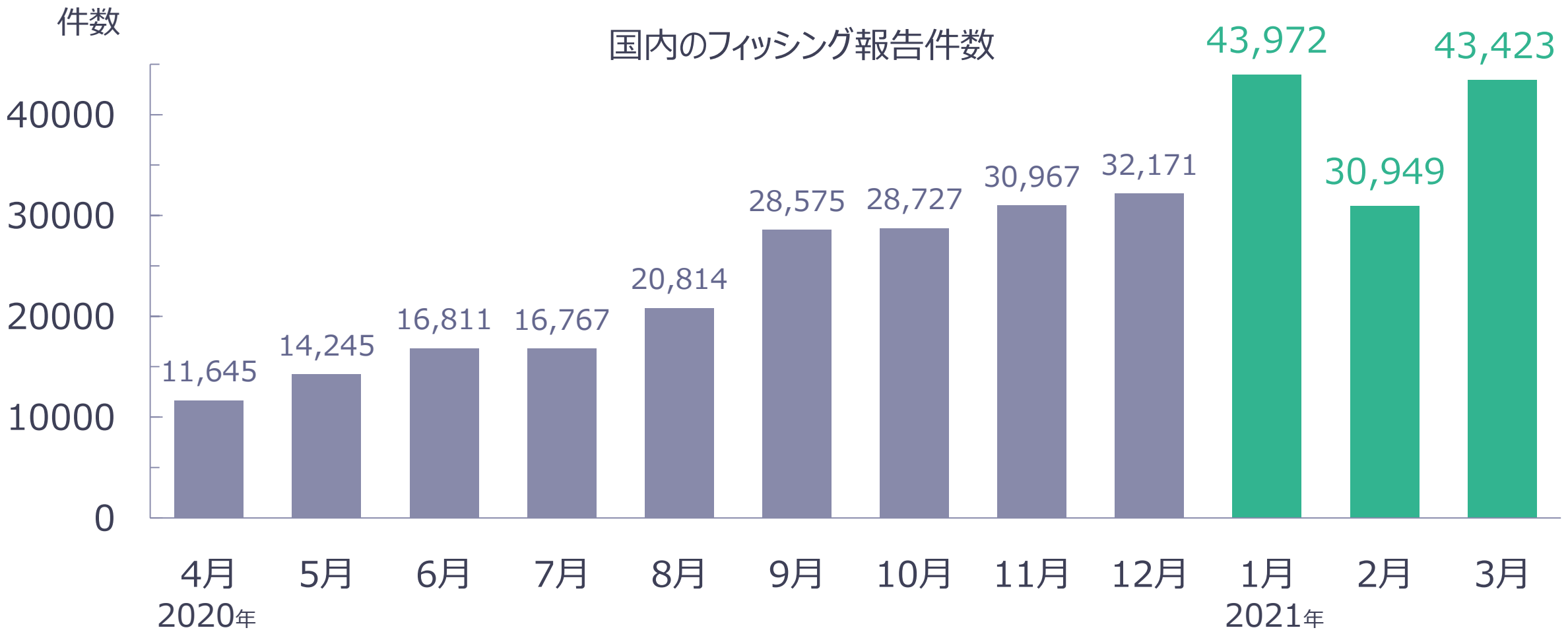
使用する場合は、VPNの利用や、
接続にあたり十分な認証を行うなど
セキュリティ対策と組み合わせて使用

Cyber Security Lab © Canon IT Solutions Inc.

Phishing

フィッシング攻撃が爆発的に増加

報告件数が1年で約4倍



(※)フィッシング対策協議会の資料をもとに作成

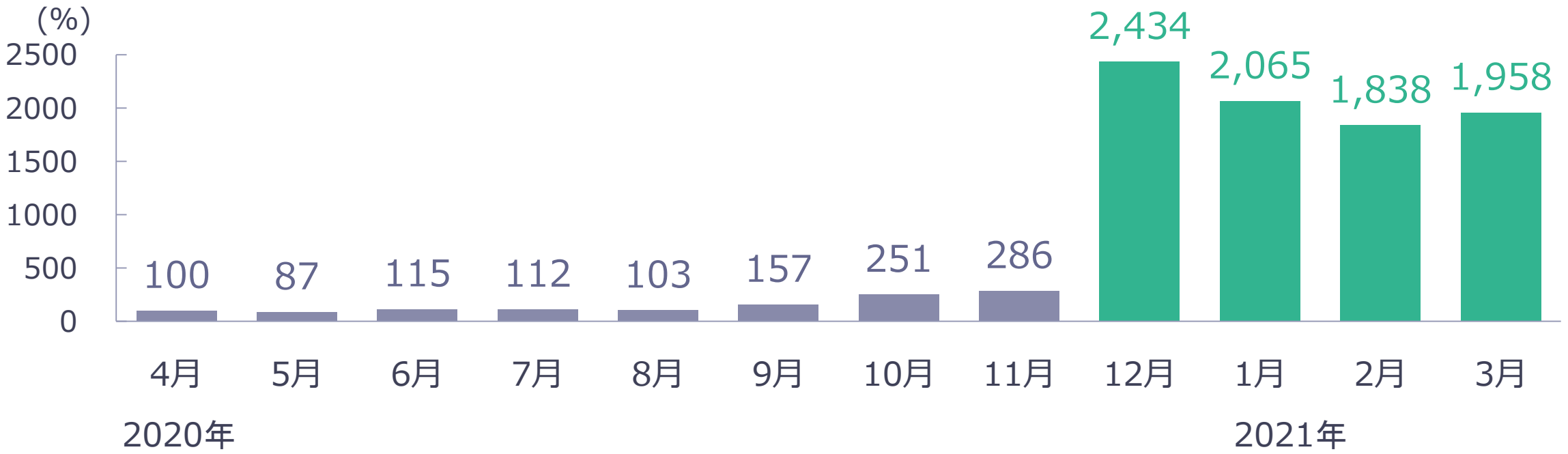
Cyber Security Lab © Canon IT Solutions Inc.

フィッシングマルウェアの増加

HTML/Phishing.Agent

メールに添付されたHTMLファイル形式のマルウェア
ファイルを開くと、ローカルでフィッシングサイトの画面が表示され
入力した情報は攻撃者が用意したURLへ送信される

国内検出数推移

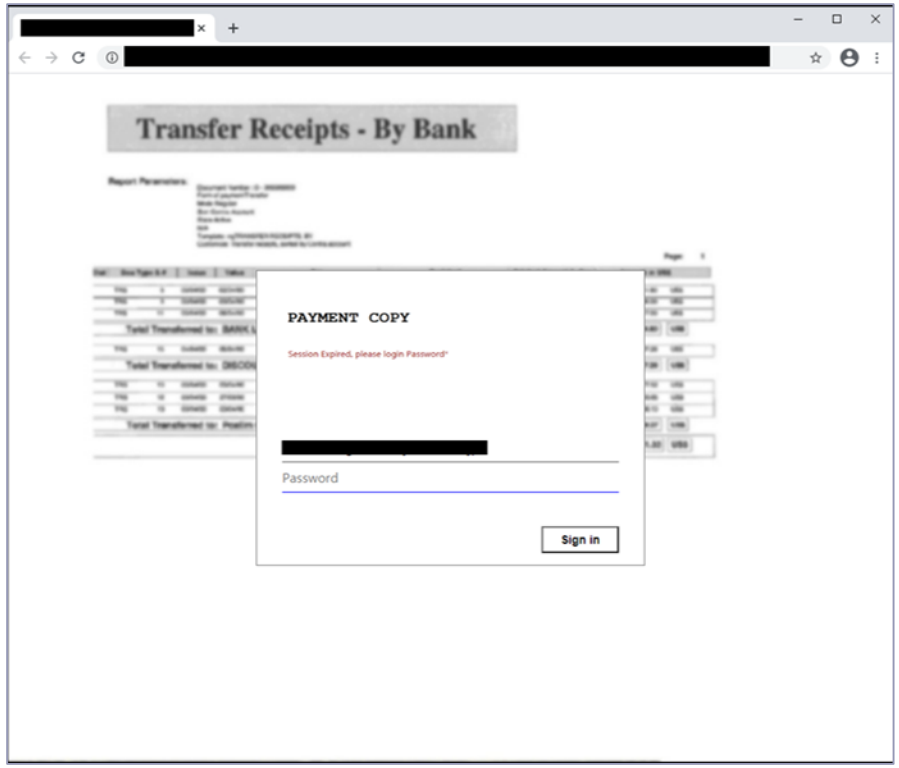


HTML/Phishing.Agentは2021年1月・2月 マルウェアレポートで詳しく解説しています
https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware2102.html

Cyber Security Lab © Canon IT Solutions Inc.

フィッシングマルウェアの増加

メールの宛先がユーザーIDとして
事前に設定されているものを確認。
普段利用しているサービスだと勘違いさせ、
パスワード入力への警戒心を解く狙いがあると
考えられる。
現在確認されているものは請求書を装ったものや
物流会社などのロゴを悪用した英語表記が主。
今後、より洗練されたものが登場する可能性があり
注意が必要




```
125  <DIV id=em><INPUT id=i0116 readOnly size=50 value=
126  required="required" placeholder="Email address, phone number or Skype"></DIV>
127  <DIV id=ep><INPUT id=i0117 size=50 type=password name=passwd required="required"
128  placeholder="Password" autofocus="autofocus"><
129  <DIV id=sign-opt class=sign-opt>
130  <DIV id=no-acc></A></DIV>
131  <DIV class=button><A href="                                    ><BUTTON id=i983893 class=newbutton
132  style="HEIGHT: 32px; WIDTH: 92px" type=submit name=submit><STRONG><FONT
133  color=#000000>Sign in</FONT></STRONG></BUTTON></A></DIV>
```

フィッシングメールの宛先となっているメールアドレスがユーザーIDとして入力されている

画面を開いたときパスワード欄の入力から始まるように設定されていることで、
IDの入力が出来ないことに気づきにくくなっている

入力したパスワードの送信先URL

HTML/Phishing.Agentは2021年1月・2月 マルウェアレポートで詳しく解説しています
https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware2102.html

Cyber Security Lab © Canon IT Solutions Inc.

スミッシング

正規の SMS と同じスレッドに偽の SMS が表示

Amazon をかたるスミッシングでは、
差出人が「Amazon」で
正規の SMS と同じスレッドに偽の SMS が
表示されるケースを確認。
本物と誤認する可能性が高いため、注意が必要

フィッシングサイトのURL例

- https://user-amazon.●●●.top/
- http://user-amazon.●●●.top/
- https://user-amazon.●●●.xyz/

SMS 文面の例

参考： フィッシング対策協議会 |2021/01 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202101.html

出典：フィッシング対策協議会 | Amazon をかたるフィッシング (2020/11/27)
https://www.antiphishing.jp/news/alert/amazon_20201127.html

Cyber Security Lab © Canon IT Solutions Inc.

＃本日お話しすること

1. 2020年の
   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

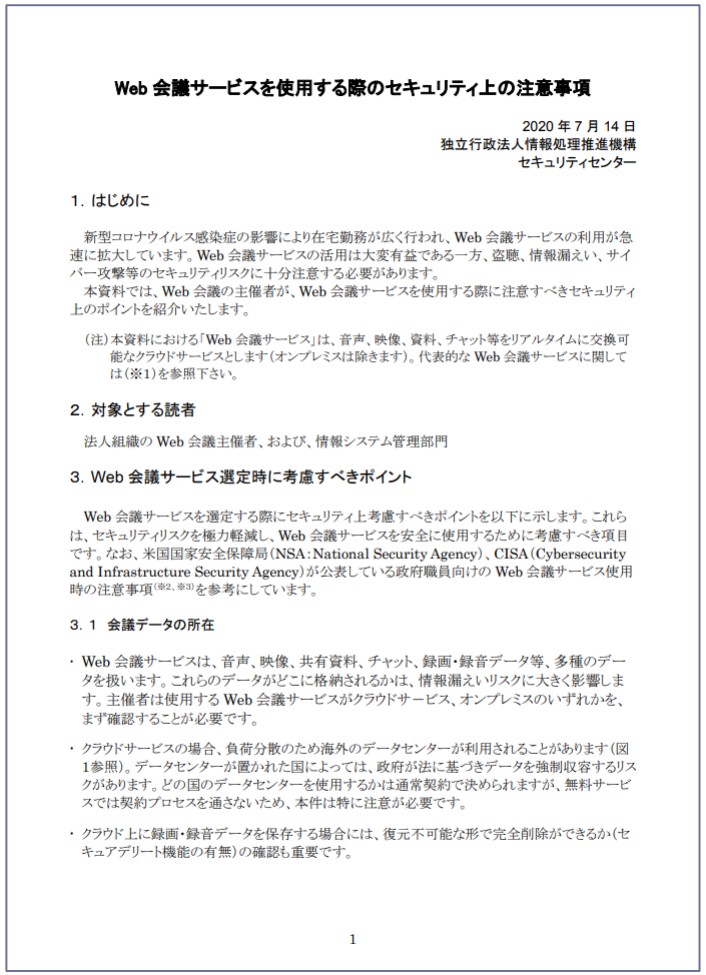
- 脅威情報の収集
- ガイドラインの参照・適応
- 脅威を知ってもらう

Cyber Security Lab © Canon IT Solutions Inc.

Web会議サービスに関するガイドライン

配布のみ

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(※2, ※3)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、負荷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。

1

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

<u>Web 会議サービス選定時に考慮すべきポイント</u>

- 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

出典： IPA - 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
https://www.ipa.go.jp/security/announce/webmeeting.html

Cyber Security Lab © Canon IT Solutions Inc.

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

配布のみ

テレワークセキュリティガイドライン（総務省）

これからテレワークを導入する企業において、
情報セキュリティ対策に関する検討の参考としてもらうことを
目的として策定。多くの企業にとって参考としやすいように、
日本企業の多くで採用されている情報セキュリティ対策の
考え方をベースとして対策を説明

緊急事態宣言解除後のセキュリティ・チェックリスト（ JNSA ）

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

出典： 総務省 –テレワークセキュリティガイドライン（第４版）
https://www.cloud-for-all.com/hubfs/resources/pdf/000545372.pdf

出典： JNSA -緊急事態宣言解除後のセキュリティ・チェックリスト
https://www.jnsa.org/telework_support/telework_security/index.html

Cyber Security Lab © Canon IT Solutions Inc.

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

Cyber Security Lab © Canon IT Solutions Inc.