最近のサイバー攻撃とインシデント対応のポイント

JPCERTコーディネーションセンター
インシデントレスポンスグループ 椎木孝斉

アジェンダ

- はじめに
  - JPCERT/CCの紹介
- 2020年度サイバー攻撃動向
  - 標的型攻撃
  - SSL VPN製品の脆弱性を悪用した攻撃
  - 新たなランサムウェア
  - Emotet
- まとめ
- 今後へ向けて

アジェンダ

- はじめに
  - JPCERT/CCの紹介
- 2020年度サイバー攻撃動向
  - 標的型攻撃
  - SSL VPN製品の脆弱性を悪用した攻撃
  - 新たなランサムウェア
  - Emotet
- まとめ
- 今後へ向けて

JPCERT/CCとは

■ 一般社団法人JPCERTコーディネーションセンター

Japan Computer Emergency Response Team / Coordination Center

- コンピューターセキュリティインシデントへの対応、国内外にセンサーをおいたインターネット定点観測、ソフトウェアや情報システム・制御システム機器等の脆弱性への対応など**国内の「セキュリティ向上を推進する活動」**を実施
- **サービス対象: 国内のインターネット利用者やセキュリティ管理担当者、ソフトウェア製品開発者等（主に、情報セキュリティ担当者）**
- インシデント対応をはじめとする、国際連携が必要なオペレーションや情報連携に関する、**日本の窓口となる「CSIRT」**

  ※各国に同様の窓口となるCSIRTが存在する
  (例、米国のCISA(US-CERT)、CERT/CC、中国のCNCERT/CC、 韓国のKrCERT/CC)

■ 経済産業省からの委託事業として

サイバー攻撃等国際連携対応調整事業を実施

JPCERT/CCの活動

インシデント予防 → インシデントの予測と捕捉 → 発生したインシデントへの対応

脆弱性情報ハンドリング

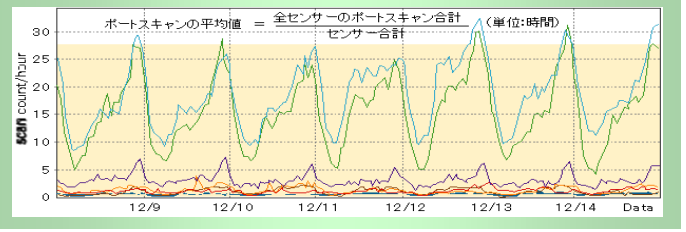
- 未公開の脆弱性関連情報を製品開発者へ提供し、対応依頼
- 関係機関と連携し、国際的に情報公開日を調整
- セキュアなコーディング手法の普及
- 制御システムに関する脆弱性関連情報の適切な流通

JVN Japan Vulnerability Notes

情報収集・分析・発信

定点観測（TSUBAME）

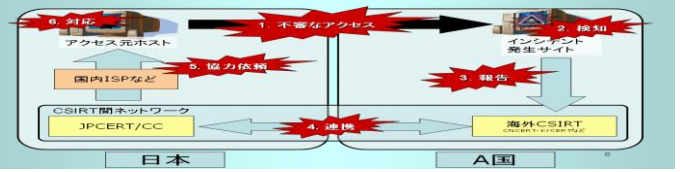
- ネットワークトラフィック情報の収集分析
- セキュリティ上の脅威情報の収集、分析、必要とする組織への提供



インシデントハンドリング

（インシデント対応調整支援）

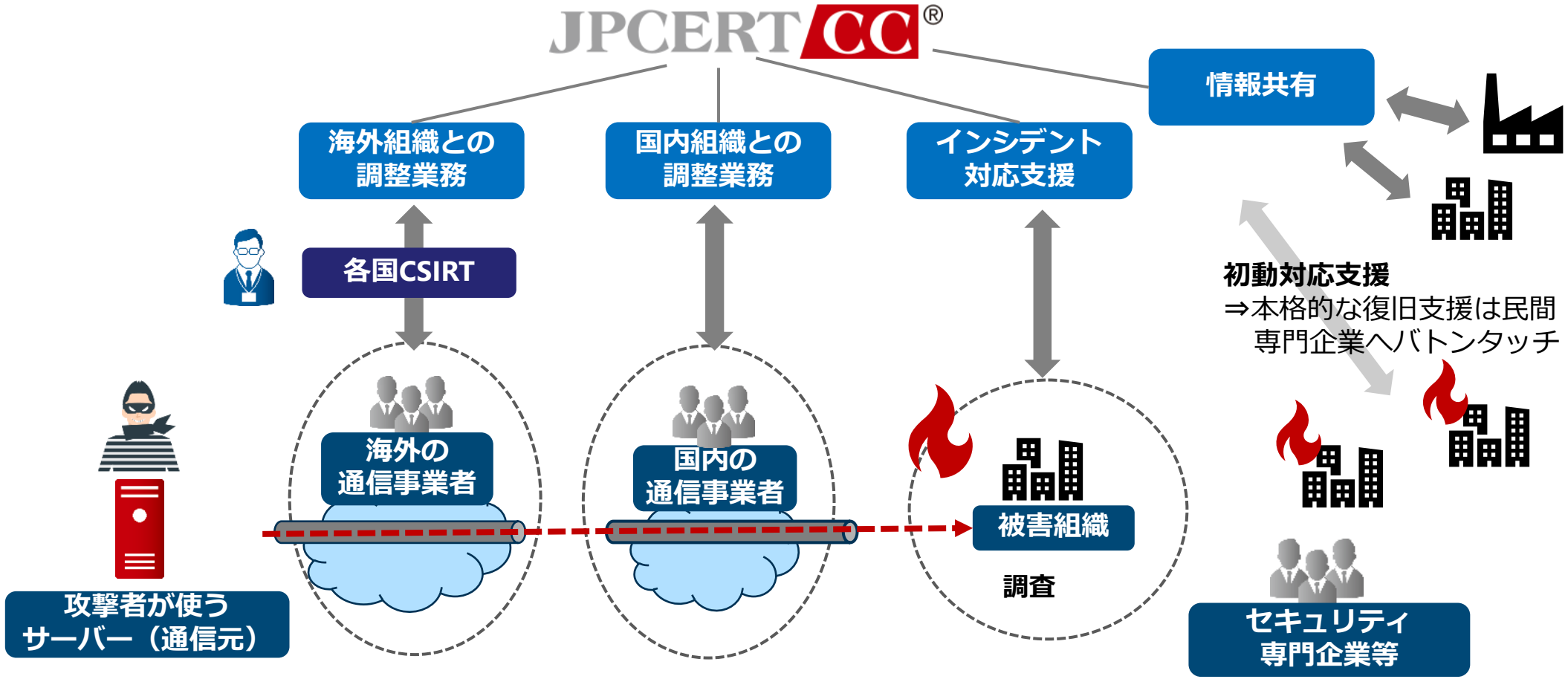
- マルウェアの接続先等の攻撃関連サイト等の閉鎖等による被害最小化
- 攻撃手法の分析支援による被害可能性の確認、拡散抑止
- 再発防止に向けた関係各関の情報交換及び情報共有



早期警戒情報	重要インフラ、重要情報インフラ事業者等の特定組織向け情報発信
脆弱性情報ハンドリング	ソフトウェア製品等の脆弱性情報に関わる開発者等との調整・公表
CSIRT構築支援	海外のNational-CSIRTや企業内のセキュリティ対応組織の構築・運用支援
アーティファクト分析	マルウェア（不正プログラム）等の攻撃手法の分析、解析
制御システムセキュリティ	制御システムに関するインシデントハンドリング/情報収集,分析発信
国内外関係者との連携	日本シーサート協議会、フィッシング対策協議会の事務局運営等
国際連携	各種業務を円滑に行うための海外関係機関との連携

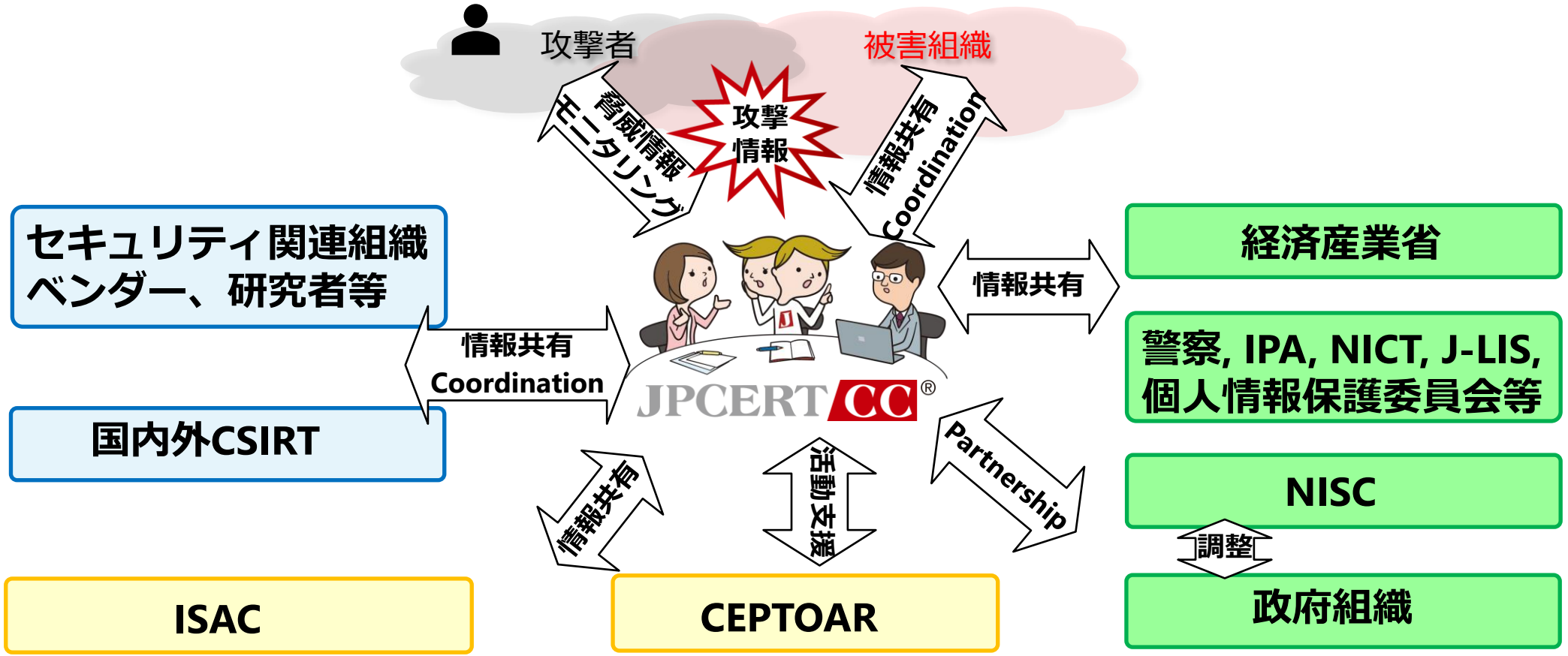
サイバー攻撃の停止に向けた国内・海外組織との調整

- 攻撃の停止に向けて国内外の複数組織間の情報共有・調整業務を実施
- 国内複数組織への広範囲な攻撃について情報を収集し、各方面へ共有



コーディネーションセンターとしての役割

さまざまなパートナーとの調整



インシデントに関する調整 (coordination) 機関として、問題解決に向けて、必要な人に必要な情報を届ける業務を行っています

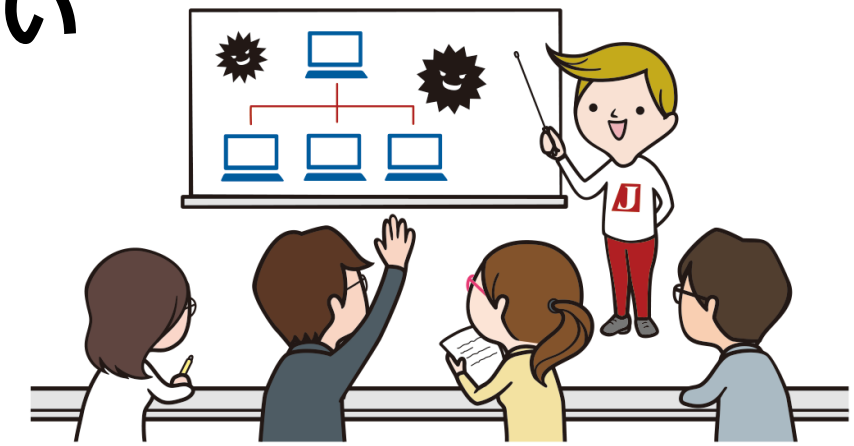
JPCERT/CCの活用

■コーディネーションセンターの役割と活用

- インシデントレスポンス
- 脆弱性・脅威情報に関する情報流通
  - 脆弱性情報　【JVN】
  - 脅威情報、注意喚起、早期警戒情報他
- アーティファクト分析【検体解析など】
- 国内外 のCSIRT連携促進、コミュニティー推進

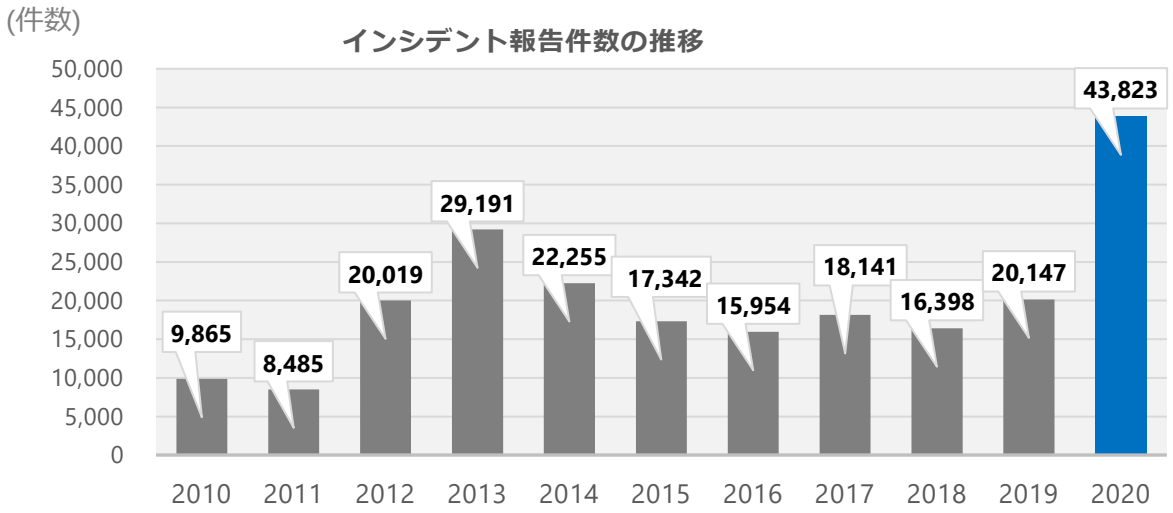
■例えば、こんなときにお役立てください

- インシデントが発生し、初動対応での技術的な支援や情報が必要となるケース
- 日々の対策を進める上で、脆弱性や脅威に関する情報が必要となるケース
- その他、お気軽にご相談ください

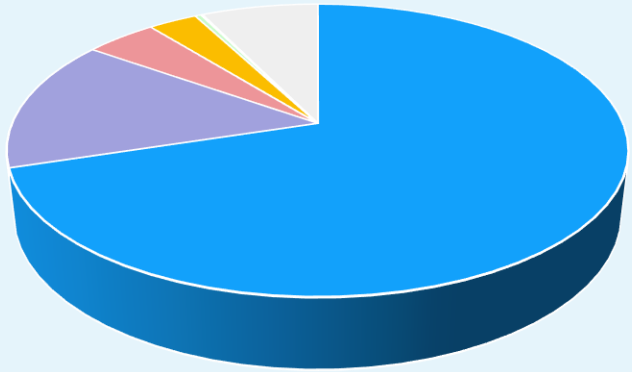


インシデント対応状況（2020年1月～2020年12月）

- JPCERT/CCへの報告
  - 全報告件数: **43,823**件
  - 全インシデント件数: **28,447**件
- JPCERT/CCからの連絡
  - 全調整件数: **17,335**件



インシデント件数のカテゴリ別割合



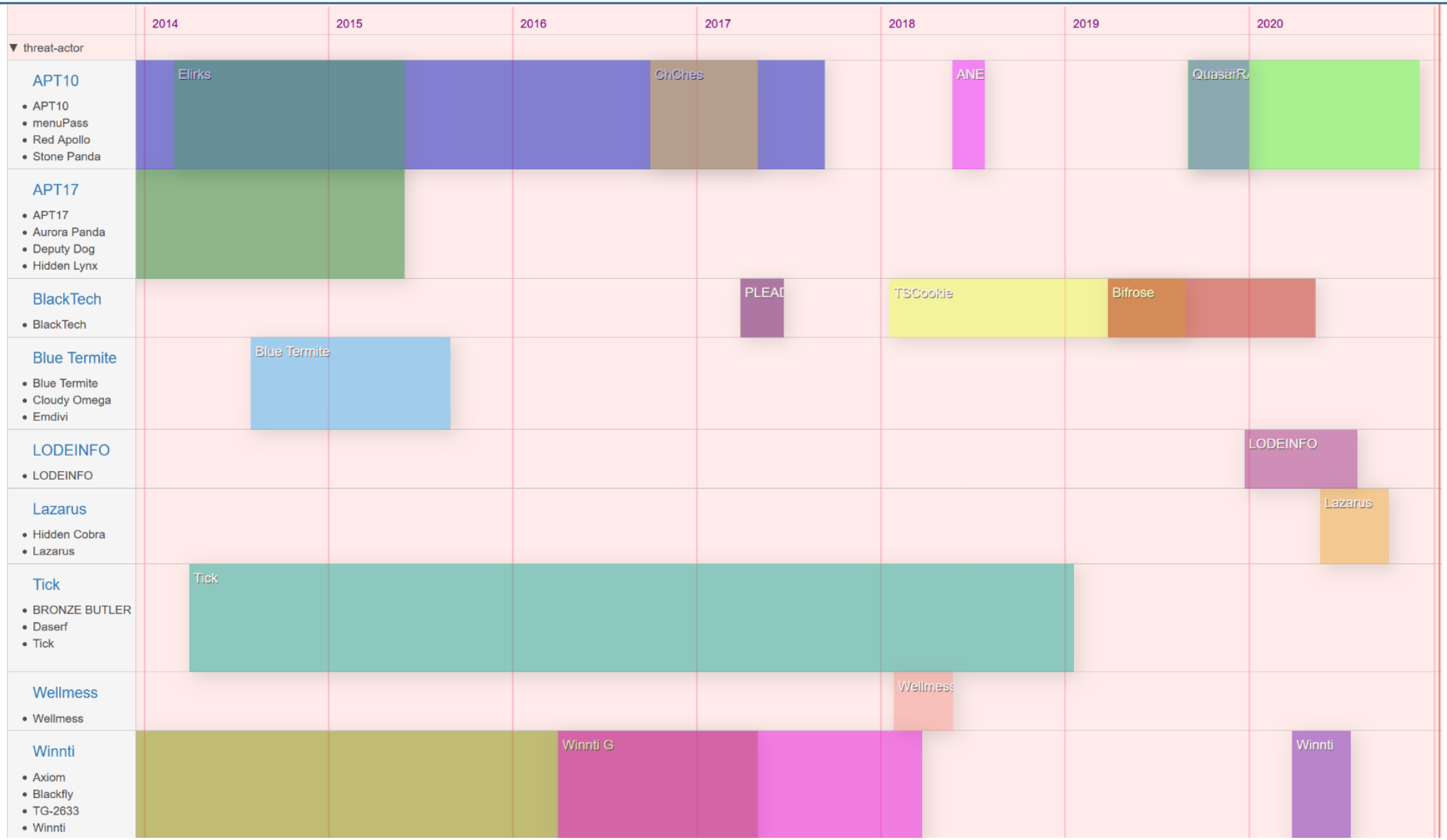
カテゴリ	割合
フィッシングサイト	70.17%
スキャン	14.63%
Webサイト改ざん	4.43%
マルウェアサイト	3.04%
DoS / DDoS	0.37%
標的型攻撃	0.04%
その他	7.32%

出典 : JPCERT/CC インシデント報告対応四半期レポート
https://www.jpcert.or.jp/ir/report.html

アジェンダ

- はじめに
  - JPCERT/CCの紹介
- 2020年度サイバー攻撃動向
  - 標的型攻撃
  - SSL VPN製品の脆弱性を悪用した攻撃
  - 新たなランサムウェア
  - Emotet
- まとめ
- 今後へ向けて

JPCERT/CCで確認した標的型攻撃活動



最近の標的型攻撃の特徴

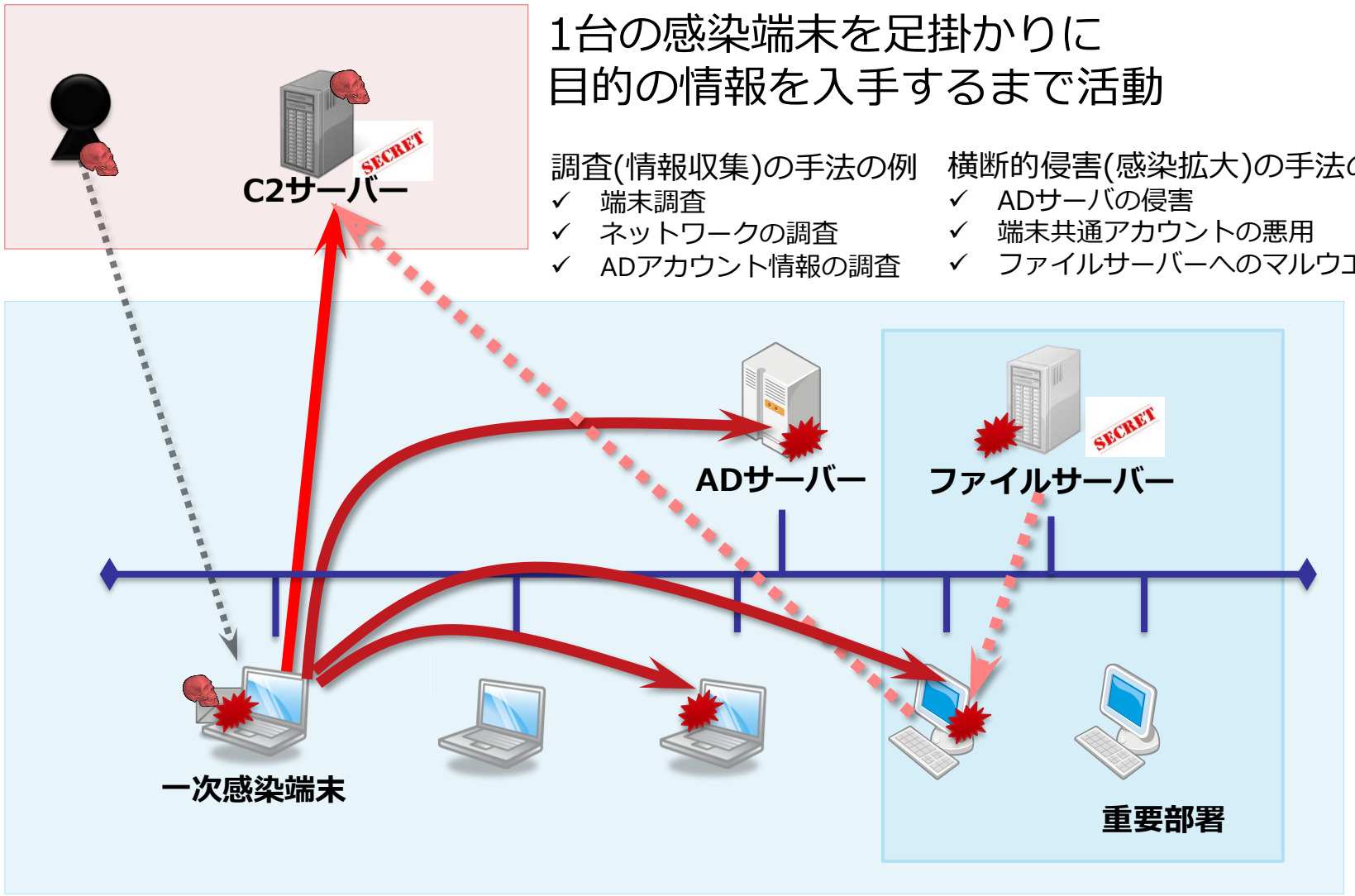
クラウドサービスの悪用

- 攻撃の入り口として (SNSサービス)
- 攻撃インフラとして
  (Microsoft Azure, Google Cloud など)
- 攻撃ターゲットとして (Office365など)
- 多段攻撃の要素として (Pastebinなど)

マルウェアの複雑化・巧妙化

- ファイルレス
- モジュール化
- 多段構成
- 難読化や耐解析機能
- サーバーターゲット
  (ELF版としての拡張)
- 汎用ツールとの組み合わせ
  (オープンソース、正規ツール、OSコマンド)

被害組織で起こっていること



1台の感染端末を足掛かりに
目的の情報を入手するまで活動

調査(情報収集)の手法の例
- ✓ 端末調査
- ✓ ネットワークの調査
- ✓ ADアカウント情報の調査

横断的侵害(感染拡大)の手法の例
- ✓ ADサーバの侵害
- ✓ 端末共通アカウントの悪用
- ✓ ファイルサーバーへのマルウエア設置

初期感染活動
↓
調査
(情報収集)
↓
横断的侵害
(感染拡大)
↓
情報窃取
(攻撃目標)
↓
潜伏
(痕跡の削除)

マルウェアの特徴(LODEINFO)

頻繁なバージョンアップと機能追加

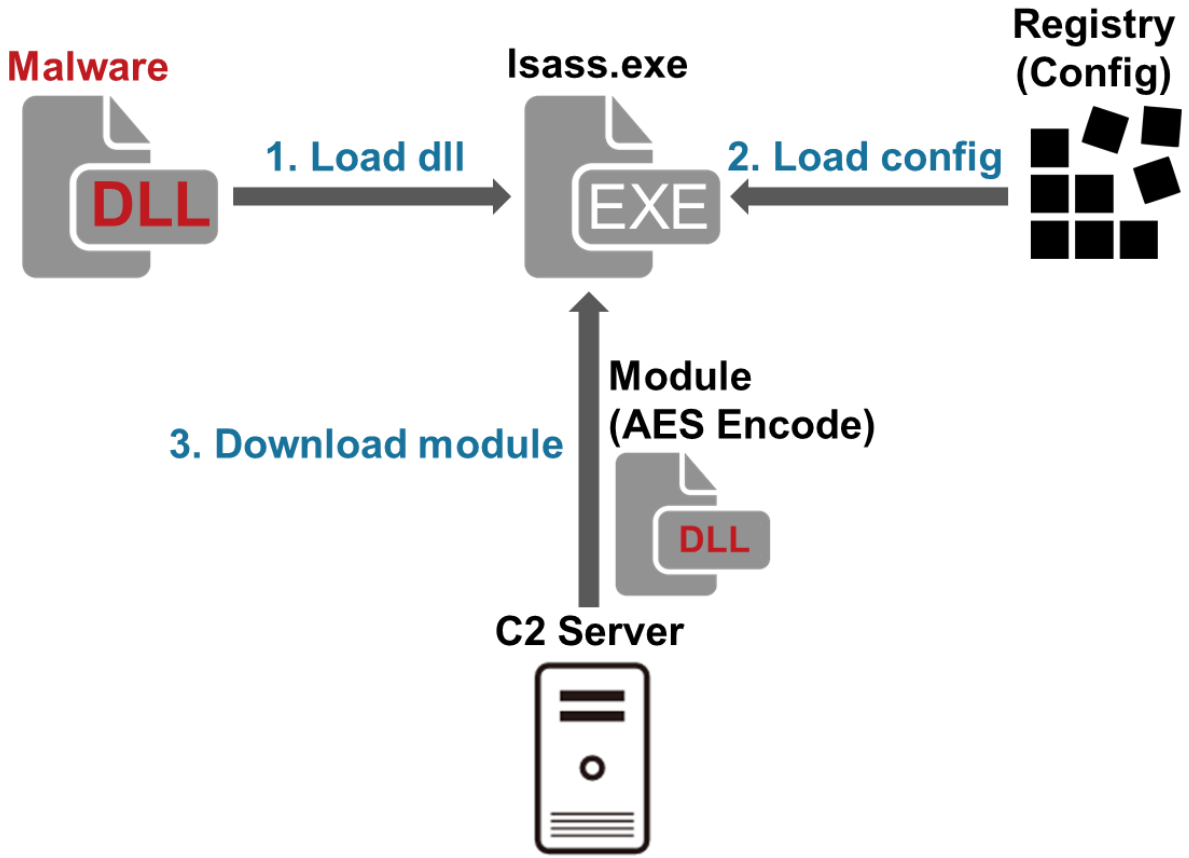
( ): コマンドのみの追加(機能は未実装)

v0.1.2	v0.2.7	v0.3.2	v0.3.4	v0.3.5	v0.3.6	v0.3.8	v0.4.6	v0.4.7	v0.4.8
•cd •ls •send •recv •cat •memory •kill •ver •command	•cd •ls •send •recv •cat •memory •kill •ver •command	•cd •ls •send •recv •cat •memory •kill •ver •command •print	•cd •ls •send •recv •cat •memory •kill •ver •command •print	•cd •ls •send •recv •cat •memory •kill •ver •command •print •rm •(ransom) •(keylog)	•cd •ls •send •recv •cat •memory •kill •ver •command •print •rm •(ransom) •(keylog)	•cd •ls •send •recv •cat •memory •kill •ver •command •print •rm •ransom •(keylog)	•cd •ls •send •recv •cat •memory •kill •ver •command •print •rm •ransom •keylog •mv •cp •mkdir •ps •pkill	•cd •ls •send •recv •cat •memory •kill •ver •command •print •rm •ransom •keylog •mv •cp •mkdir •ps •pkill	•cd •ls •send •recv •cat •memory •kill •ver •command •print •rm •ransom •keylog •mv •cp •mkdir •ps •pkill

2019/12 → 2021/02

マルウェアの特徴(Lazarus)

- モジュール化、設定情報の分離など検知・分析を難しくする工夫



- HTTPS通信やマルウェア独自のデータ暗号化を使用し、調査・分析を難しくする工夫

```
POST /[Path] HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Accept: */*
Cookie: token=[ランダムな値(4桁)][認証キー(4桁)][通信回数]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Content-Length: [Size]
Host:[Server]

[param]=[Base64 data]
```

標的型攻撃への対応のポイント

- 様々な検知トリガーの活用
  - ― 内部・外部
- 一般的なインシデントとは異なる対応（知見）が必要との認識
- 侵害は長期に渡っている可能性
  - ― 長期のログ保存、分析が重要
- 局所的、場当たり的な対応ではなく包括的、全体的な対応を
- 攻撃は繰り返し行われることの認識

高度サイバー攻撃 (標的型攻撃) に関する連絡

最終更新: 2018-08-31

目次

- はじめに
- 検知・分析
- 高度サイバー攻撃のインシデント対応について
- 参考情報
- JPCERT/CCからのお願い

はじめに

JPCERT/CCや外部組織などから高度サイバー攻撃 (Advanced Persistent Threat (APT) 、標的型攻撃とも呼ばれます) に関連する連絡を受けた場合の対応を説明します。

高度サイバー攻撃の場合、攻撃者が組織内部への侵入に成功すると組織の重要な情報が長期間窃取され続けたり、他組織への攻撃の踏み台として環境が使用される場合があるため、早急な対応が必要です。もしも高度サイバー攻撃に関する連絡を受けた場合は、これらの対応を参考に調査を進められることを推奨します。(こちらでは NIST SP800-61 のインシデント対応プロセスの「検知・分析」のフェーズを中心に紹介します)

なお、高度サイバー攻撃の全容を把握するには「準備」のフェーズが重要です。詳細については「JPCERT/CC 高度サイバー攻撃 (APT) への備えと対応ガイド」の第2章を参照してください。

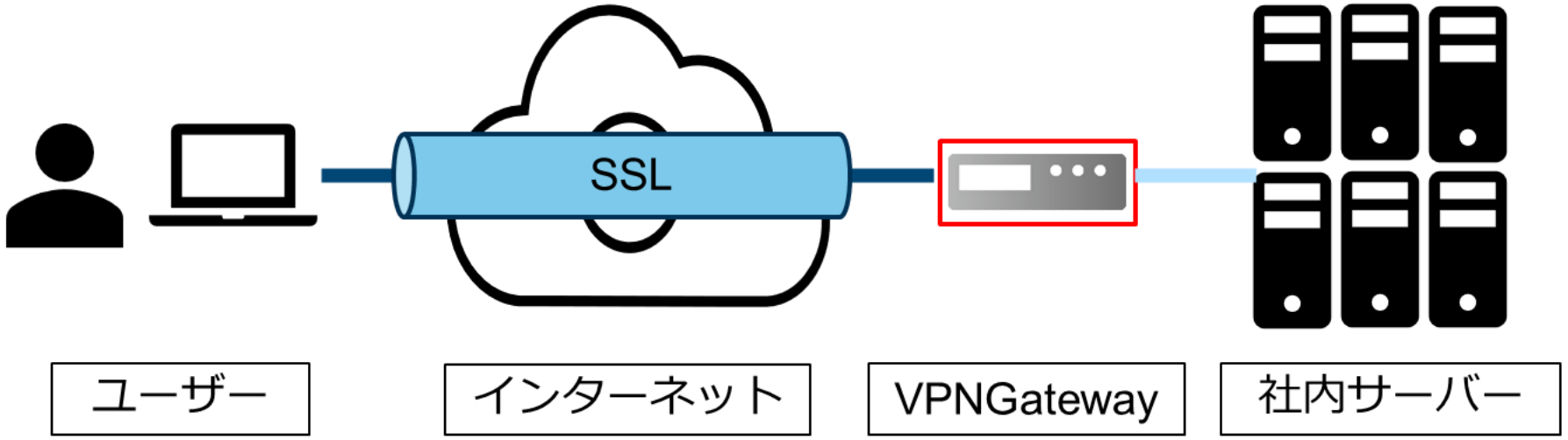
出典：JPCERT/CC 高度サイバー攻撃 (標的型攻撃) に関する連絡
https://www.jpcert.or.jp/incidentcall/

アジェンダ

- はじめに
  - JPCERT/CCの紹介
- 2020年度サイバー攻撃動向
  - 標的型攻撃
  - SSL VPN製品の脆弱性を悪用した攻撃
  - 新たなランサムウェア
  - Emotet
- まとめ
- 今後へ向けて

SSL VPN製品の脆弱性

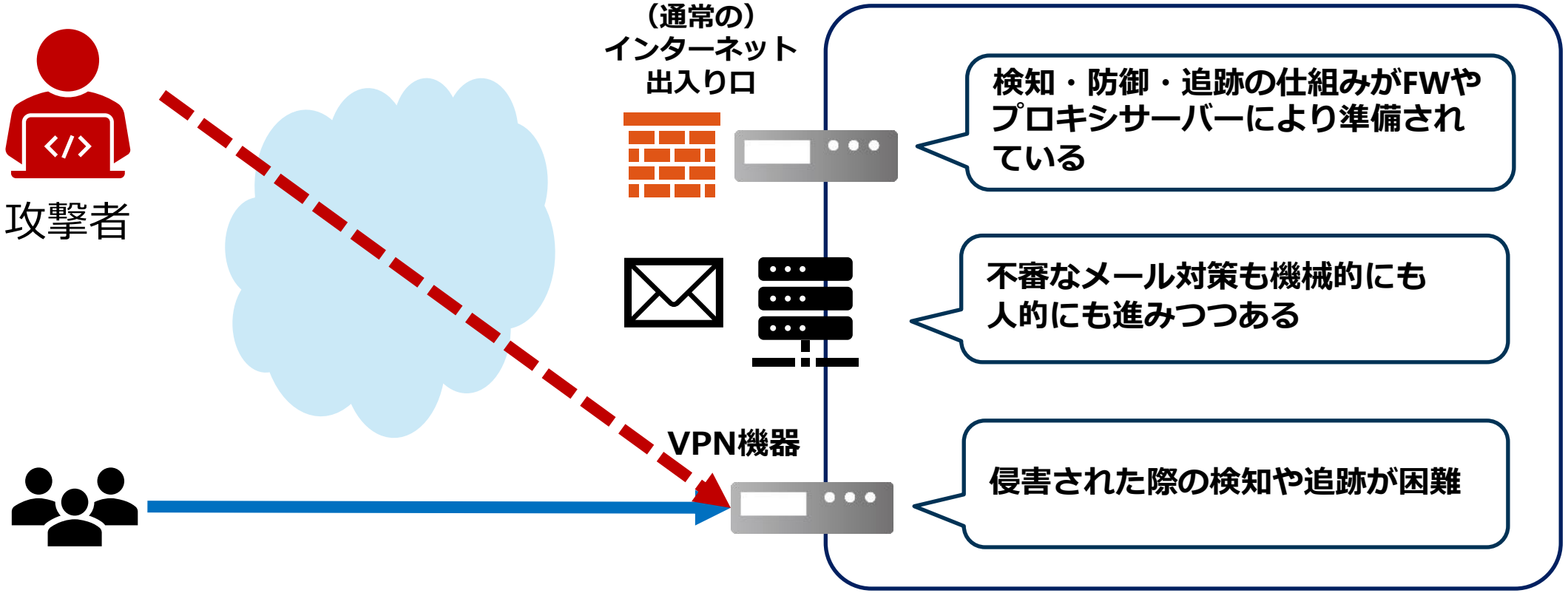
- SSL VPNとは、遠隔地間で仮想的なプライベートネットワークを構築する際に用いられる技術



SSL VPNを実現するために、インターネットから企業ネットワークへの入り口に設置される複数のSSL VPN製品に脆弱性が報告された

なぜ攻撃者はSSL VPN製品を狙うのか

- 日頃から（国内外から）多数のアクセスがされる機器であるため、IPアドレス／地域での除外などがされていない
- 他の“出入り口”に比べて対策が薄く、検知・防御だけでなく、取得・記録されるログの少なさから侵害を追跡する手段も弱い



2020年度の主なSSL VPN製品の脆弱性

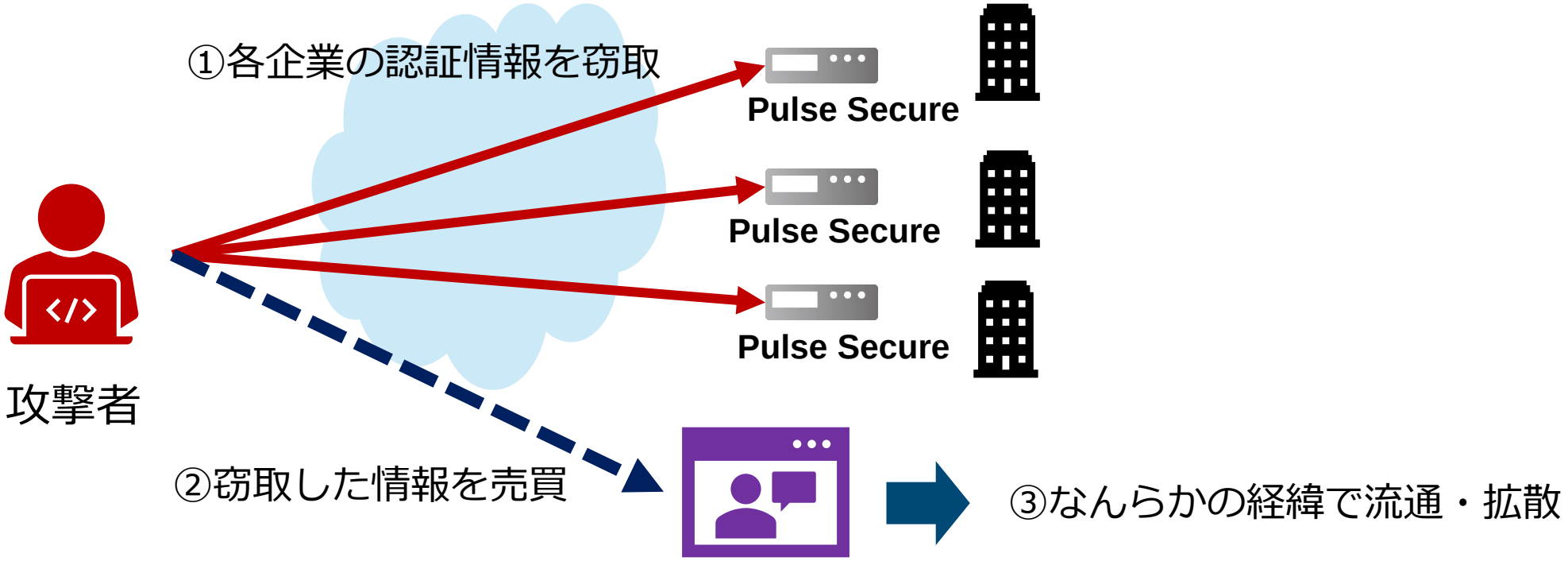
- Pulse Connect Secureの脆弱性
- 複数のCitrix製品の脆弱性
- 複数のBIG-IP製品の脆弱性
- Palo Alto Networks製品の脆弱性
- SAP NetWeaver Application Server Javaの脆弱性
- Fortinet製品（FortiOS）の脆弱性

2020年度の主なSSL VPN製品の脆弱性

- Pulse Connect Secureの脆弱性
- 複数のCitrix製品の脆弱性
- 複数のBIG-IP製品の脆弱性
- Palo Alto Networks製品の脆弱性
- SAP NetWeaver Application Server Javaの脆弱性
- Fortinet製品（FortiOS）の脆弱性

Pulse Connect Secureの脆弱性

- 2019年4月に公開された、SSL VPN製品であるPulse Secure製品の脆弱性（CVE-2019-11510他）
- 2020年8月に、過去に窃取したと思われる**認証情報が公開される**



Pulse Connect Secureの脆弱性（時系列）

2019年4/24
修正バージョン
公開

8/4 脆弱性の詳細などについて公開
8/21 攻撃コード／ツールが公開
⇒スキャン観測

2019年9月
JPCERT/CC注意喚起
残数1,511件　個別通知

2020年3/24
残数298件

2020年6月
攻撃試行の可能性

2020年8月
リスト流出

未対応

パッチ未対応の場合

・複数のタイミングで侵害されていた可能性、2020年6月の攻撃で認証情報が窃取されていた可能性ともにあり

未対応

修正済み

2020年6月頃～8月に修正対応していた場合

・修正対応実施前に攻撃試行され、認証情報が窃取されていた場合、当該認証情報で侵害される可能性あり

未対応

修正済み

注意喚起後に修正対応したが、認証情報を変更していなかった場合

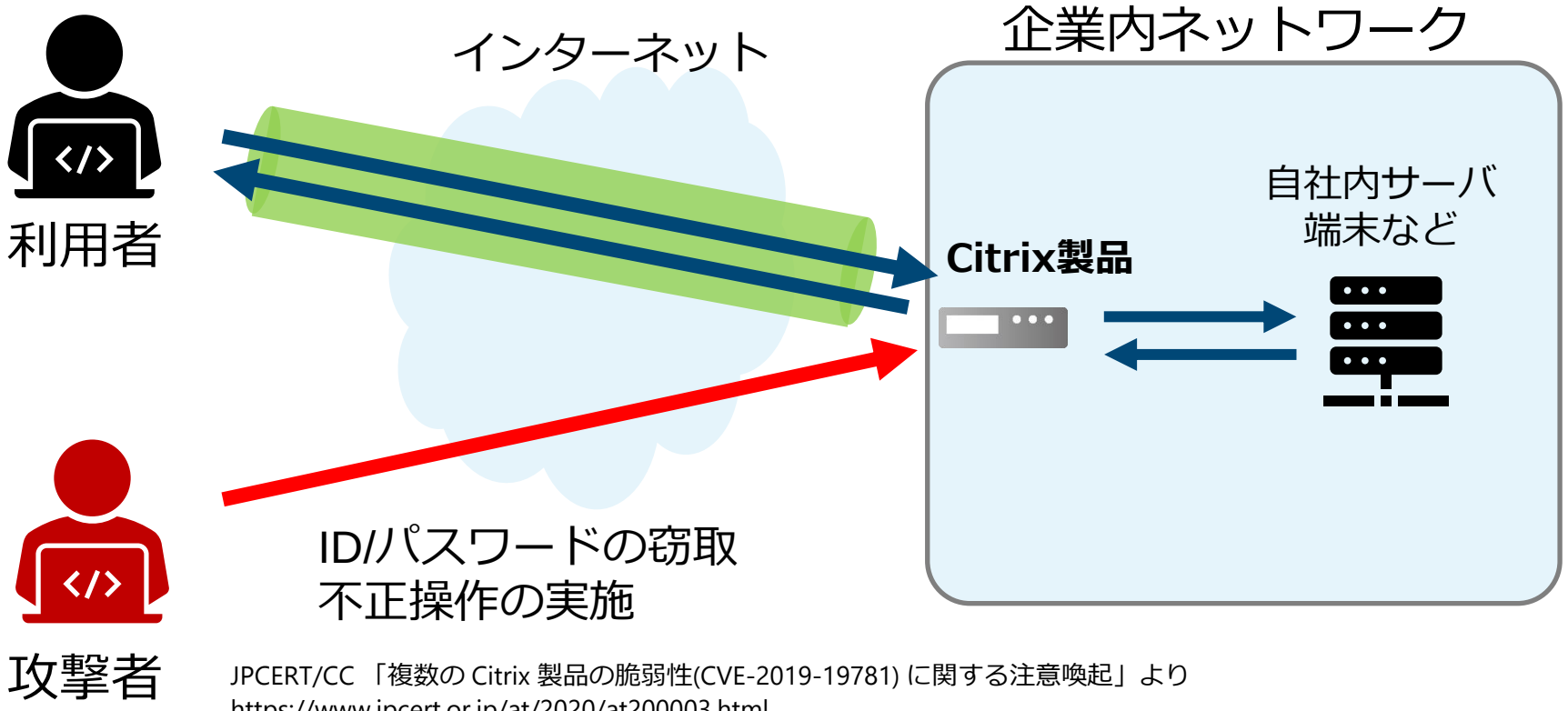
・修正対応実施前に攻撃試行され、認証情報が窃取されていた場合、当該認証情報で侵害される可能性あり

2020年度の主なSSL VPN製品の脆弱性

- Pulse Connect Secureの脆弱性
- 複数のCitrix製品の脆弱性
- 複数のBIG-IP製品の脆弱性
- Palo Alto Networks製品の脆弱性
- SAP NetWeaver Application Server Javaの脆弱性
- Fortinet製品（FortiOS）の脆弱性

複数のCitrix製品の脆弱性

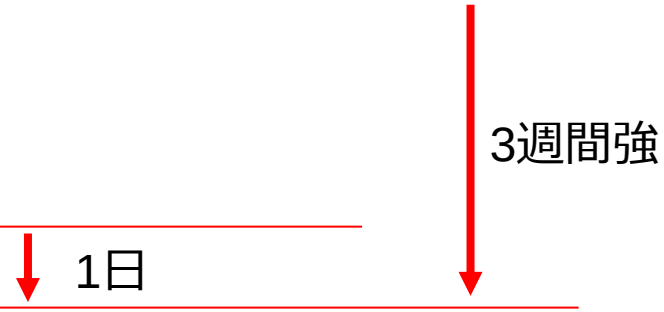
- 企業ネットワークとのセキュアな接続などに使われるCitrix社製品を容易に侵害可能な脆弱性（CVE-2019-19781）
  - 脆弱性情報は2019年12月17日に公開



JPCERT/CC 「複数の Citrix 製品の脆弱性(CVE-2019-19781) に関する注意喚起」より
https://www.jpcert.or.jp/at/2020/at200003.html

複数のCitrix製品の脆弱性（時系列）

- 2019
  - 12/17　**Citrix社から脆弱性情報（軽減策を含む）を公開**
- 2020
  - 01/10　複数組織がスキャン活動を観測
  - 01/11　**実証コードを確認**
  - 01/12　**複数組織が攻撃の試行を観測**
    ＜　JPCERT/CCから国内向けに個別連絡を開始　＞
  - 01/17　JPCERT/CCから注意喚起を発行
  - 01/19～ Citrix社がパッチを提供



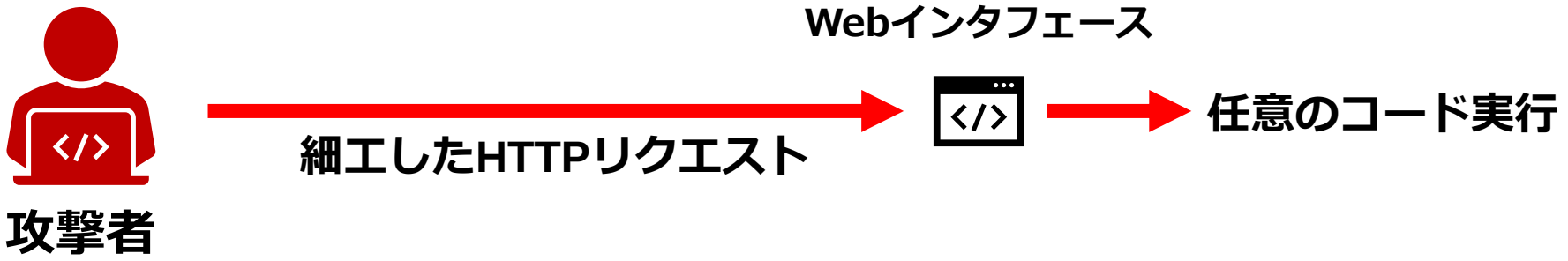
  - 07/01　**セキュリティベンダーがバックドアが残存しているホストに関する情報を公開**
  - 07/08～ 外部情報を元にJPCERT/CCから国内向けに個別連絡を開始

2020年度の主なSSL VPN製品の脆弱性

- Pulse Connect Secureの脆弱性
- 複数のCitrix製品の脆弱性
- 複数のBIG-IP製品の脆弱性
- Palo Alto Networks製品の脆弱性
- SAP NetWeaver Application Server Javaの脆弱性
- Fortinet製品（FortiOS）の脆弱性

複数のBIG-IP製品の脆弱性

- 2020年7月1日にF5 Networks社がBIG-IPの脆弱性（CVE-2020-5902）に関するアドバイザリを公開
- 遠隔の第三者が、BIG-IP製品のWebインタフェースに、細工したHTTPリクエストを送信することで任意のコードを実行することが可能



複数のBIG-IP製品の脆弱性（時系列）

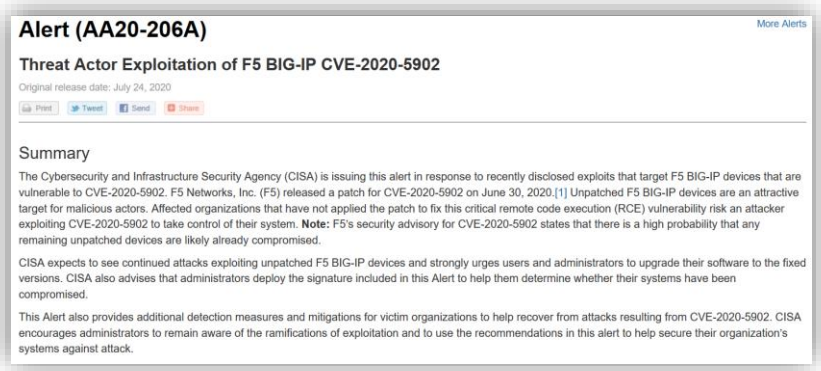
- 2020
  - 07/01 **F5 Networks社が脆弱性情報を公開**
  - 07/05 **実証コード（PoC）が公開**
  - 07/06 **複数組織が脆弱性の探索、悪用の試行を観測**

1日

5日

JPCERT/CCから注意喚起を発行（日/英）
国内対象組織に個別通知を開始

  - 07/24 CISAから注意喚起
（Alert（AA20-206A））



Alert (AA20-206A)

More Alerts

Threat Actor Exploitation of F5 BIG-IP CVE-2020-5902

Original release date: July 24, 2020

Print Tweet Send Share

Summary

The Cybersecurity and Infrastructure Security Agency (CISA) is issuing this alert in response to recently disclosed exploits that target F5 BIG-IP devices that are vulnerable to CVE-2020-5902. F5 Networks, Inc. (F5) released a patch for CVE-2020-5902 on June 30, 2020.[1] Unpatched F5 BIG-IP devices are an attractive target for malicious actors. Affected organizations that have not applied the patch to fix this critical remote code execution (RCE) vulnerability risk an attacker exploiting CVE-2020-5902 to take control of their system. **Note:** F5's security advisory for CVE-2020-5902 states that there is a high probability that any remaining unpatched devices are likely already compromised.

CISA expects to see continued attacks exploiting unpatched F5 BIG-IP devices and strongly urges users and administrators to upgrade their software to the fixed versions. CISA also advises that administrators deploy the signature included in this Alert to help them determine whether their systems have been compromised.

This Alert also provides additional detection measures and mitigations for victim organizations to help recover from attacks resulting from CVE-2020-5902. CISA encourages administrators to remain aware of the ramifications of exploitation and to use the recommendations in this alert to help secure their organization's systems against attack.

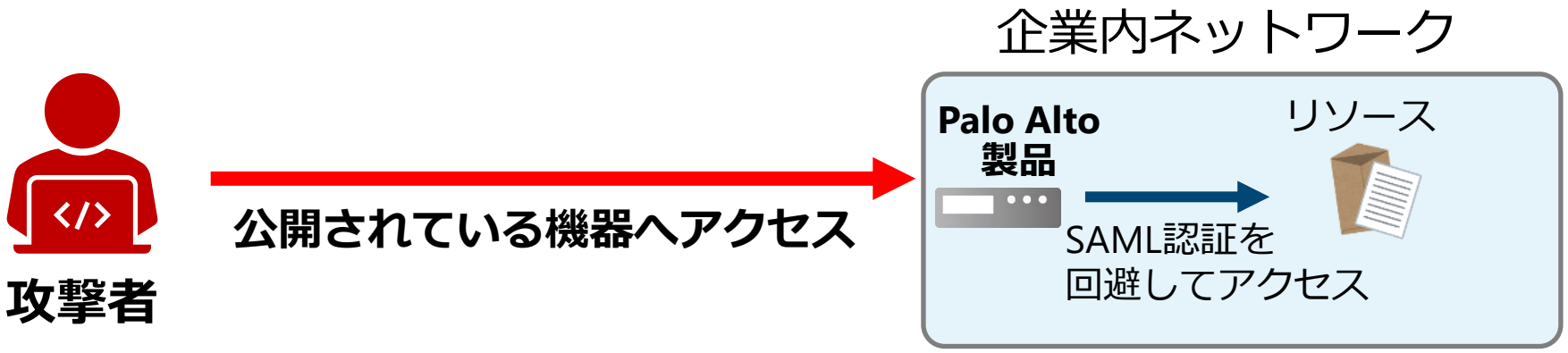
出典：Threat Actor Exploitation of F5 BIG-IP CVE-2020-5902
https://us-cert.cisa.gov/ncas/alerts/aa20-206a

2020年度の主なSSL VPN製品の脆弱性

- Pulse Connect Secureの脆弱性
- 複数のCitrix製品の脆弱性
- 複数のBIG-IP製品の脆弱性
- Palo Alto Networks製品の脆弱性
- SAP NetWeaver Application Server Javaの脆弱性
- Fortinet製品（FortiOS）の脆弱性

Palo Alto Networks製品の脆弱性

- 2020年6月29日にPalo Alto Networks社がPAN-OSの脆弱性（CVE-2020-2021）に関するアドバイザリを公開
- 遠隔の第三者によってSAML認証で保護されたリソースにアクセスされる可能性
- 本脆弱性の影響を受ける可能性がある機器が、**インターネット経由で接続可能な状態で公開**されていることを確認
  - JPCERT/CCから対象企業に個別通知を実施

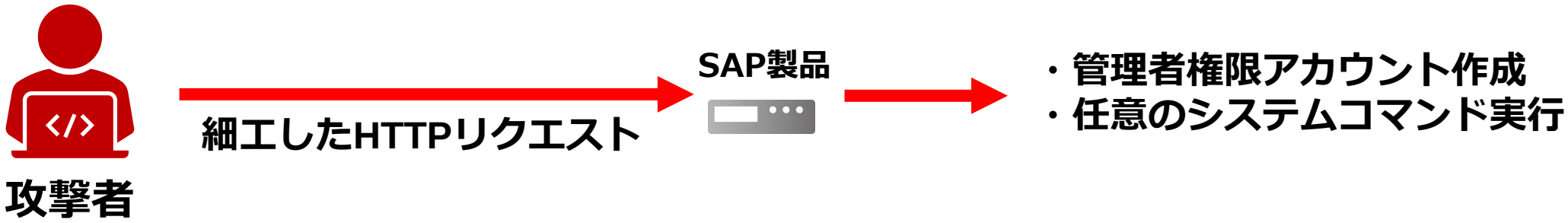


2020年度の主なSSL VPN製品の脆弱性

- Pulse Connect Secureの脆弱性
- 複数のCitrix製品の脆弱性
- 複数のBIG-IP製品の脆弱性
- Palo Alto Networks製品の脆弱性
- SAP NetWeaver Application Server Javaの脆弱性
- Fortinet製品（FortiOS）の脆弱性

SAP NetWeaver Application Server Java の脆弱性

- 2020年7月13日にSAPがSAP NetWeaver Application Server Java の脆弱性（CVE-2020-6287）に関する情報を公開
- 遠隔の第三者にSAPシステムを制御される可能性
- 本脆弱性の影響を受ける可能性がある機器が、**インターネット経由で接続可能な状態で公開**されていることを確認
  - JPCERT/CCから対象企業に個別通知を実施



2020年度の主なSSL VPN製品の脆弱性

- Pulse Connect Secureの脆弱性
- 複数のCitrix製品の脆弱性
- 複数のBIG-IP製品の脆弱性
- Palo Alto Networks製品の脆弱性
- SAP NetWeaver Application Server Javaの脆弱性
- Fortinet製品（FortiOS）の脆弱性

Fortinet製品（FortiOS）の脆弱性（時系列）

- 2019
  - 05/24 **Fortinet社が脆弱性情報を公開**
  - 09/02 **脆弱性の実証コード（PoC）を確認**
    JPCERT/CCから注意喚起を発行
    （Palo Alto Networks、Pulse Secureの脆弱性情報とまとめて公開）
- 2020
  - 11/19 **対象機器リストと認証情報の漏えい確認**
  - 11/27 JPCERT/CCからCyberNewsFlashで注意を呼びかけ
    個別組織へ通知開始

SSL VPN製品の脆弱性 – まとめ

- 脆弱性への対応が遅れれば、攻撃を受けるリスクは増大する
- 脆弱性情報が公開されてから、攻撃試行までの期間は短い
  - 脆弱性公表後、1週間以内に実証コードの公開や、悪用が始まるケースも多い
- パッチを適用していても、侵害済みの場合は不十分
  - バックドアが残存
  - 認証情報がすでに窃取されている
  - ベンダー情報等を参考に、侵害が発生しているかの確認が必要
- フォーラムなどで侵害された情報が公開されるケースも多数

アジェンダ

- はじめに
  - JPCERT/CCの紹介
- 2020年度サイバー攻撃動向
  - 標的型攻撃
  - SSL VPN製品の脆弱性を悪用した攻撃
  - 新たなランサムウェア
  - Emotet
- まとめ
- 今後へ向けて

新たなランサムウェア（1/4）

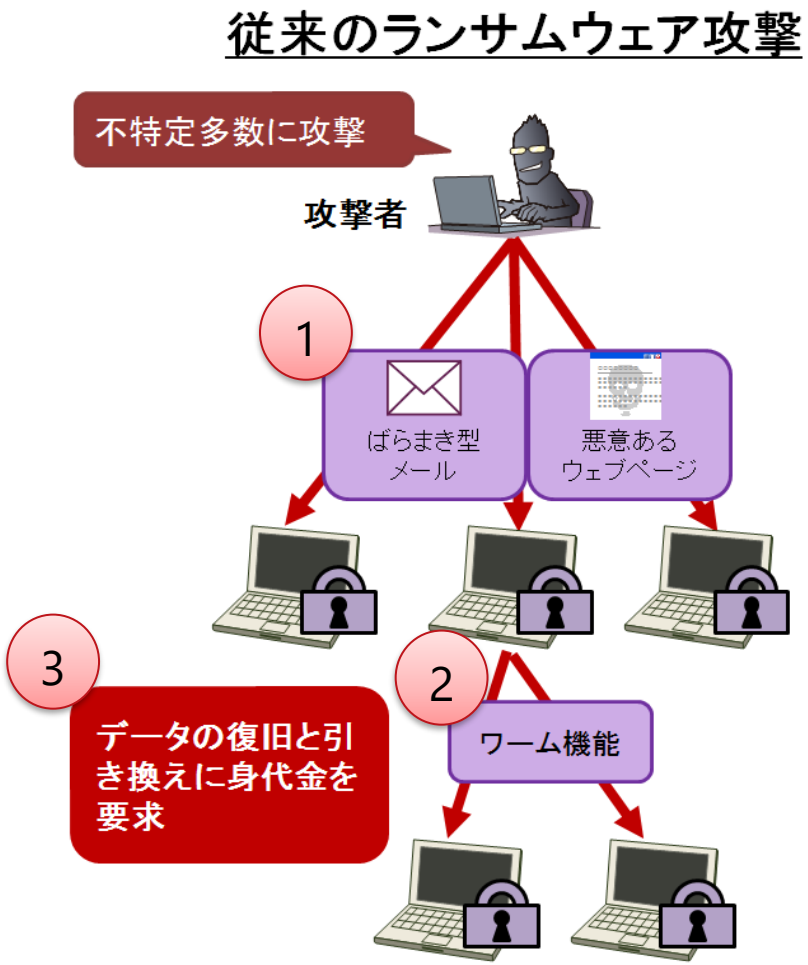
- ランサムウェアとは
  - パソコンや共有フォルダのファイルを、暗号化して使用不可にする、または画面ロック等により操作不可とするウイルスの総称
  - 復旧と引き換えに、身代金を支払うように促すメッセージを表示

出典：【注意喚起】事業継続を脅かす新たなランサムウェア攻撃について
https://www.ipa.go.jp/security/announce/2020-ransom.html

新たなランサムウェア（2/4）

- 従来のランサムウェア
  - ① 不特定多数へ広く攻撃を実施
  - ② 脆弱性を悪用した組織内端末への横展開
  - ③ 感染後、支払いに応じる被害組織から身代金を得る

  という戦略が主



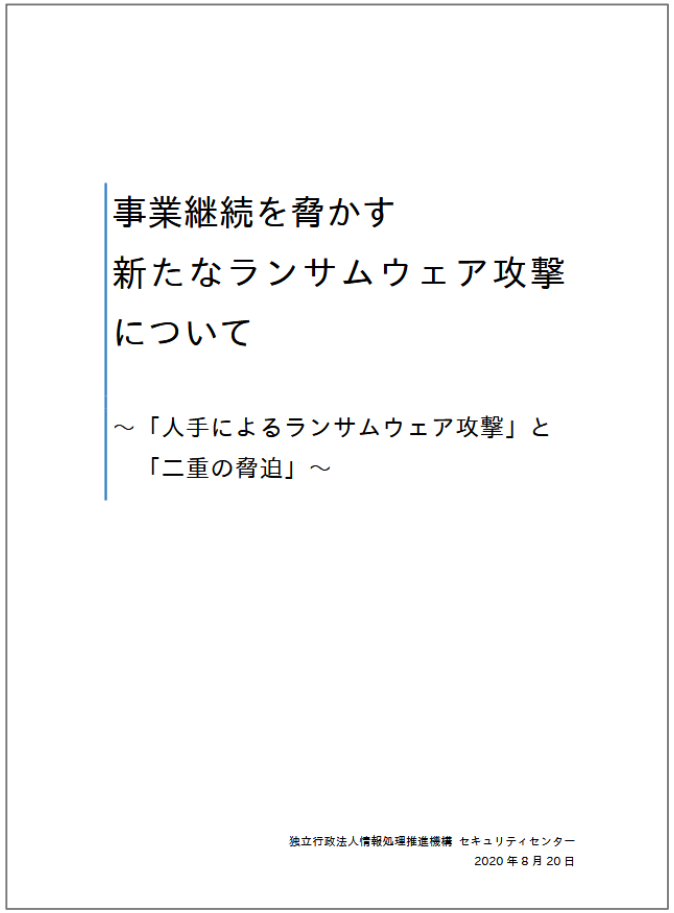
出典： IPA（独立行政法人情報処理推進機構）
【注意喚起】事業継続を脅かす新たなランサムウェア攻撃について
https://www.ipa.go.jp/security/announce/2020-ransom.html

新たなランサムウェア（3/4）

- 新たなランサムウェア
  - 人手によるランサムウェア攻撃(標的型)
  - 二重の脅迫(暴露型)

⬇

被害組織が事業継続のために金銭を支払わざるを得ない状況を作り上げ、より確実に、かつ高額な身代金を得ようという狙い


事業継続を脅かす
新たなランサムウェア攻撃
について

～「人手によるランサムウェア攻撃」と
「二重の脅迫」～

独立行政法人情報処理推進機構 セキュリティセンター
2020 年 8 月 20 日

出典：IPA（独立行政法人情報処理推進機構）
【注意喚起】事業継続を脅かす新たなランサムウェア攻撃について
https://www.ipa.go.jp/security/announce/2020-ransom.html

新たなランサムウェア（4/4）

- 人手によるランサムウェア攻撃（2018年頃～）
  - 標的型攻撃と同様に、さまざまな攻撃手法を駆使して、企業・組織のネットワークへ侵入
    - 端末やサーバーをランサムウェアに感染させる
    - 管理サーバーを乗っ取って、企業・組織内の端末やサーバーを一斉にランサムウェアに感染させる
  - データやシステムの復旧を阻害するため、バックアップなども同時に狙われることがある
- 二重の脅迫（2019年末頃～）
  - 以下2つの脅迫を行う
    1. 暗号化したデータを復旧するための身代金要求
    2. 要求に応じない場合には、暗号化以前に窃取したデータを公開するなどの脅迫
  - 2020年7月以降、国内企業を標的としたリークサイト上の書き込みも増加

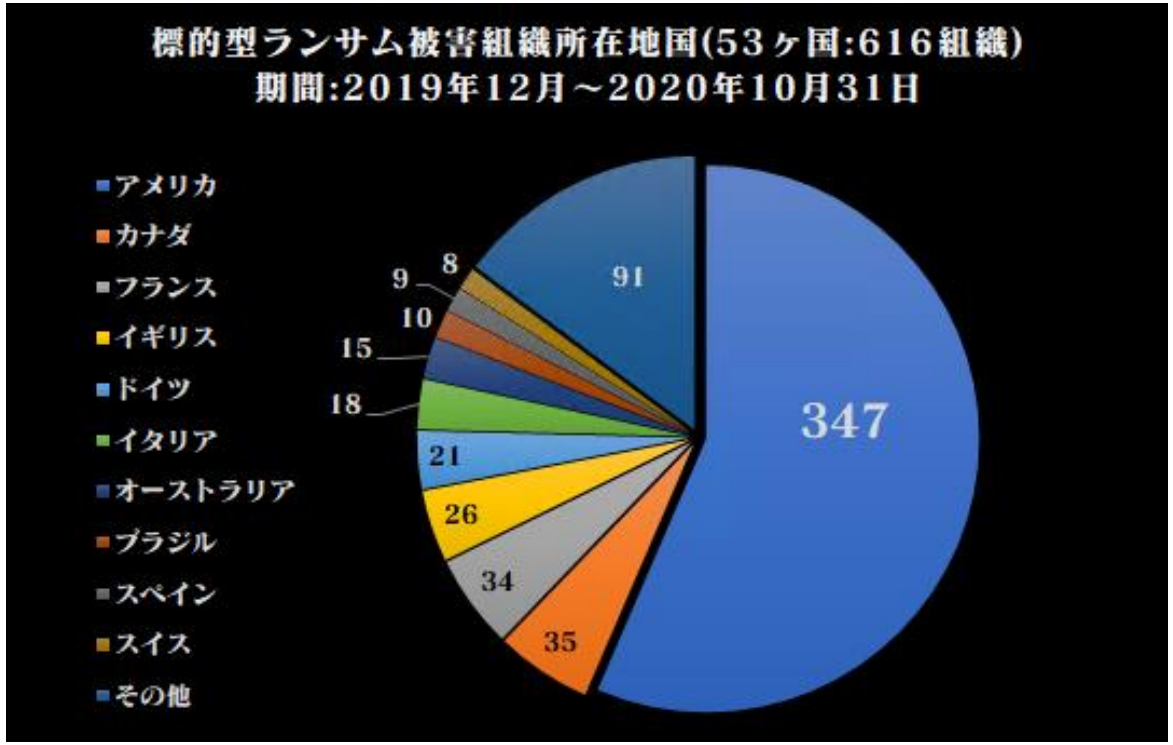
新たなランサムウェアの被害状況

国内外の被害状況

- 直近1年間で約600組織以上が被害に
- 日本企業および海外関連企業の20社以上が被害に

被害規模の大きさ

- 数億円単位の身代金要求
- 数万台単位の感染被害



出典：標的型ランサム観察記 2020年10月31日まで版
https://csirt.ninja/?p=1575

脅迫に対する金銭支払いの考え方

- 新たなランサムウェアなど脅迫をともなうサイバー攻撃では、次の理由により、基本的に金銭は支払うべきではない
  - 金銭を支払うことで復旧できる保障はない
  - 各組織が払い続ける限り、犯罪行為が止まらない
  - 犯罪組織の利益供与として罰せられる可能性（法的な確認が必要）
  - （株式会社の場合）高額支払い時の株主からの追及

新たなランサムウェアへの対策(1)

- **被害を防ぐ対策の基本的な考え方**
  - **攻撃対象領域の最小化**
    - 外部へ公開するシステム、プロトコルやサービスを最低限にする
    - システムの侵害の可能性を考慮し、接続可能な範囲を限定する
  - **アクセス制御と認証**
    - 組織内外、拠点間を接続するシステムで適切なアクセス制御や認証を設定する
    - アクセスや認証ログの監視の実装
  - **脆弱性対策**
    - OSおよび利用ソフトウェア、ネットワーク機器のファームウェア等を最新の状態に保つ
  - **内部対策**
    - 統合ログ管理、内部ネットワーク監視、エンドポイント監視の利用検討
    - 重要データやシステムのセグメント化、ネットワーク分離

新たなランサムウェアへの対策(2)

- **被害に備えた準備**
  - **データやシステムのバックアップ**
    - 重要なファイルの定期的なバックアップ
    - 装置や媒体はバックアップ時にのみ接続
    - システムの再構築も想定、バックアップの妥当性やリストア手順も確認
  - **事業継続計画（BCP）や対応方針の整理**
    - 被害によっては事業継続に大きな影響が及ぶケースも
    - 事業継続計画（BCP）や対応方針を整理し、有事に備える

新たなランサムウェアへの対応

対応のポイント

— 迅速かつ正確な初期対応

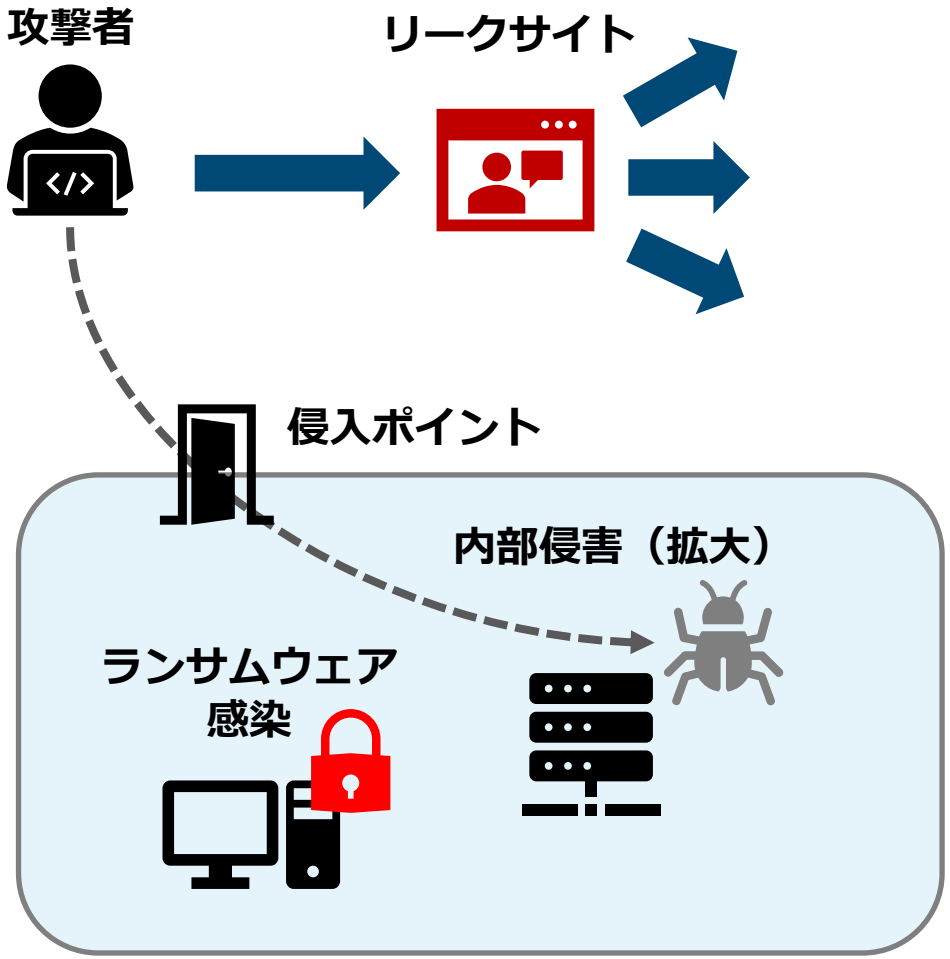
- 検知認知後は、被害拡大を防ぐため迅速な封じ込め対応が必要
- 遮断や停止が必要な場合の対応責任者、決定者の整理

— 適切な情報統制や広報対応

- リークサイト等を通じて情報拡散、問い合わせや取材殺到の恐れ
- 情報発信窓口の一本化、速やかな対外広報対応、情報管理の徹底

— 確実な封じ込めや根絶対応

- ランサムウェア以外のマルウェアやRATが残留している可能性
- 考え得る侵入経路には全て対策計画実施



アジェンダ

- はじめに
  - JPCERT/CCの紹介
- 2020年度サイバー攻撃動向
  - 標的型攻撃
  - SSL VPN製品の脆弱性を悪用した攻撃
  - 新たなランサムウェア
  - Emotet
- まとめ
- 今後へ向けて

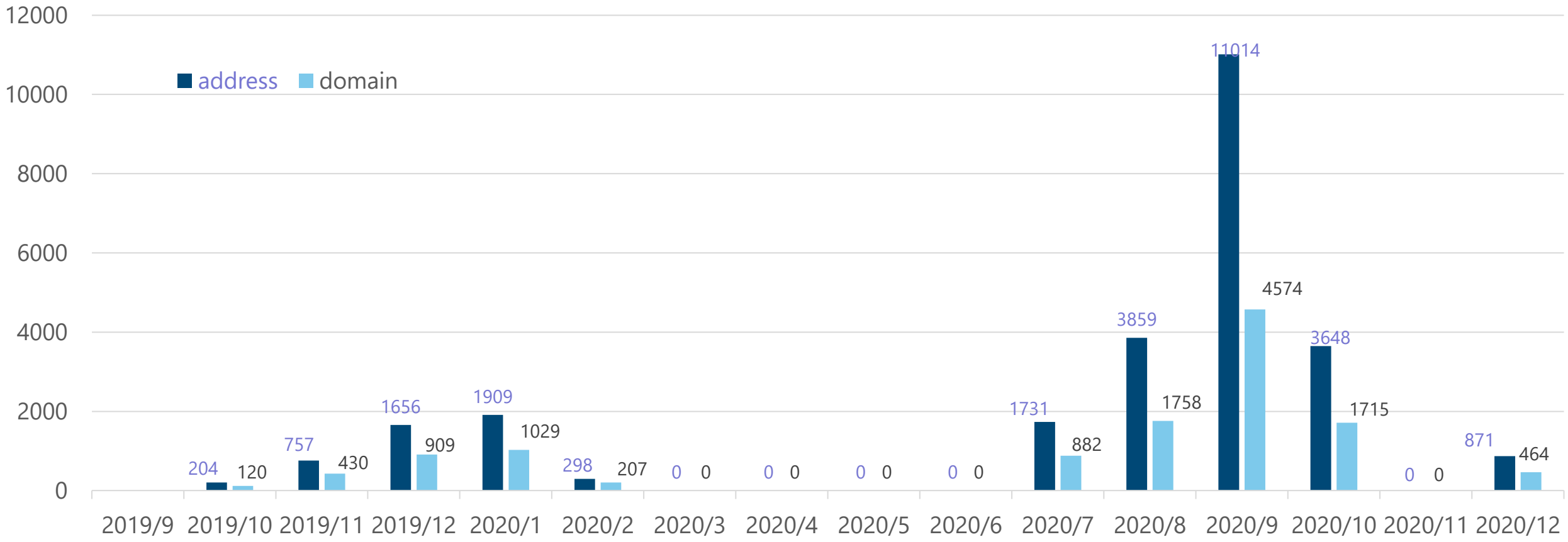
Emotetとは

- Emotetとは
  - バンキングトロジャン※の一種として2014年に確認された
  - モジュール化などを通じ、マルウェアの感染・拡散を行う機能を備えるなど年々進化を続けている

※オンラインバンキングのアカウントID、パスワード、暗証番号などを狙うマルウェア

- 主な機能
  - メール関連情報の窃取
  - 組織内の横展開
  - 感染を広げるメールの送信
  - 他のマルウェアへの感染（Trickbot, Zloaderなど）

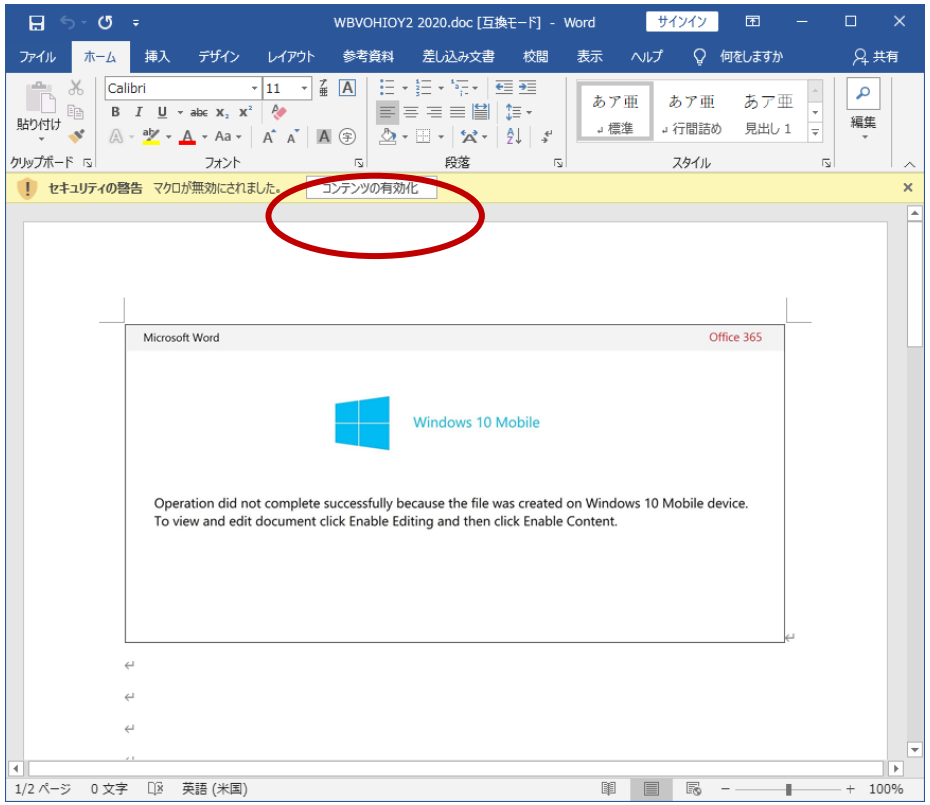
国内の感染アドレス数推移



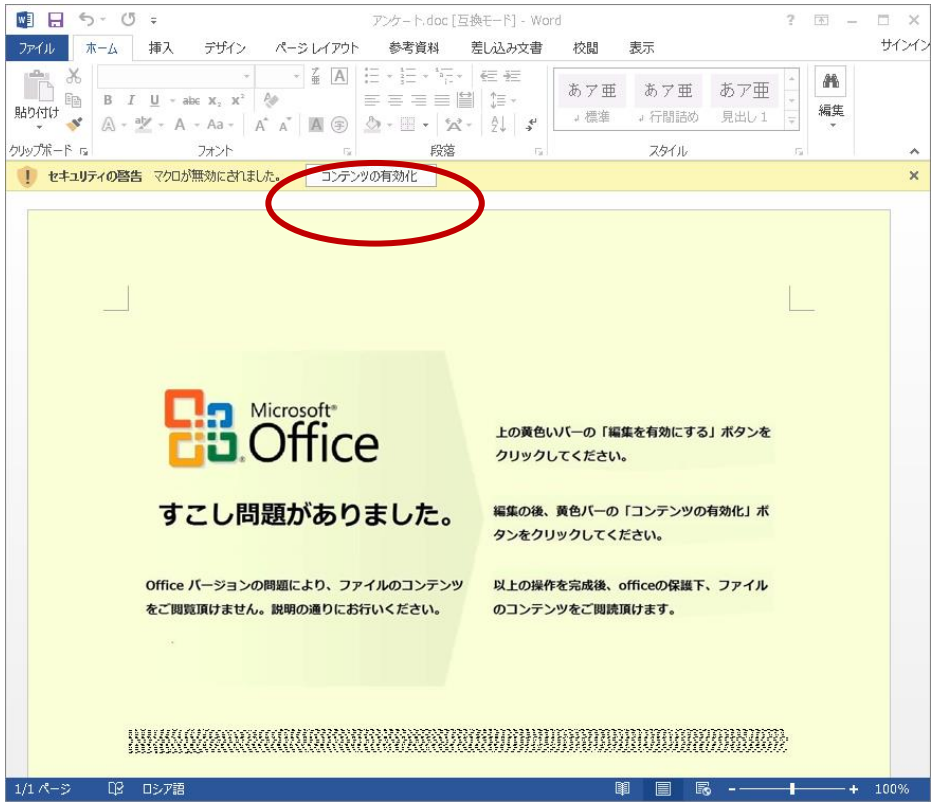
Emotetのメール送信に使われるメールアドレスのうち.jpのアドレス数推移

Emotetの感染拡大の流れ（1/3）

- 感染拡大の流れ(1)
  - ユーザーが、Emotetに感染させるメールに添付されたWord形式ファイルなどを開き「コンテンツの有効化」をする



出典：JPCERT/CC Eyes「マルウエアEmotetへの対応FAQ」
https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html



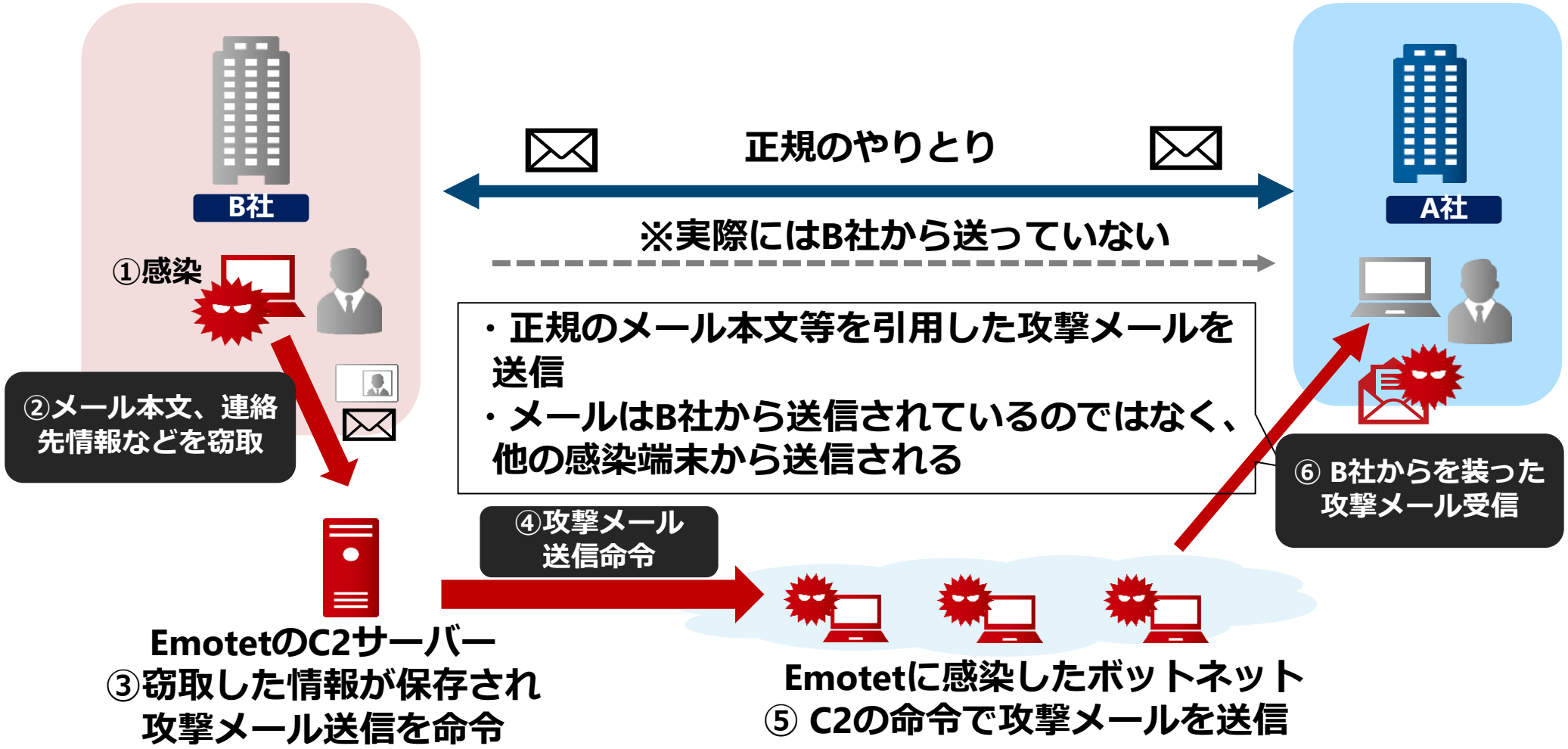
出典：JPCERT/CC Eyes「マルウエアEmotetへの対応FAQ」
https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html

Emotetの感染拡大の流れ（2/3）

- 感染拡大の流れ(2)
  - 感染した端末から情報が窃取される
  - 組織内で感染が拡大する
  - パスワードなどの認証情報が窃取される
  - 他のマルウェアがダウンロードされる可能性がある
- 感染拡大の流れ(3)
  - 窃取した情報を元に、取引先などにEmotetに感染させるメールが送信される

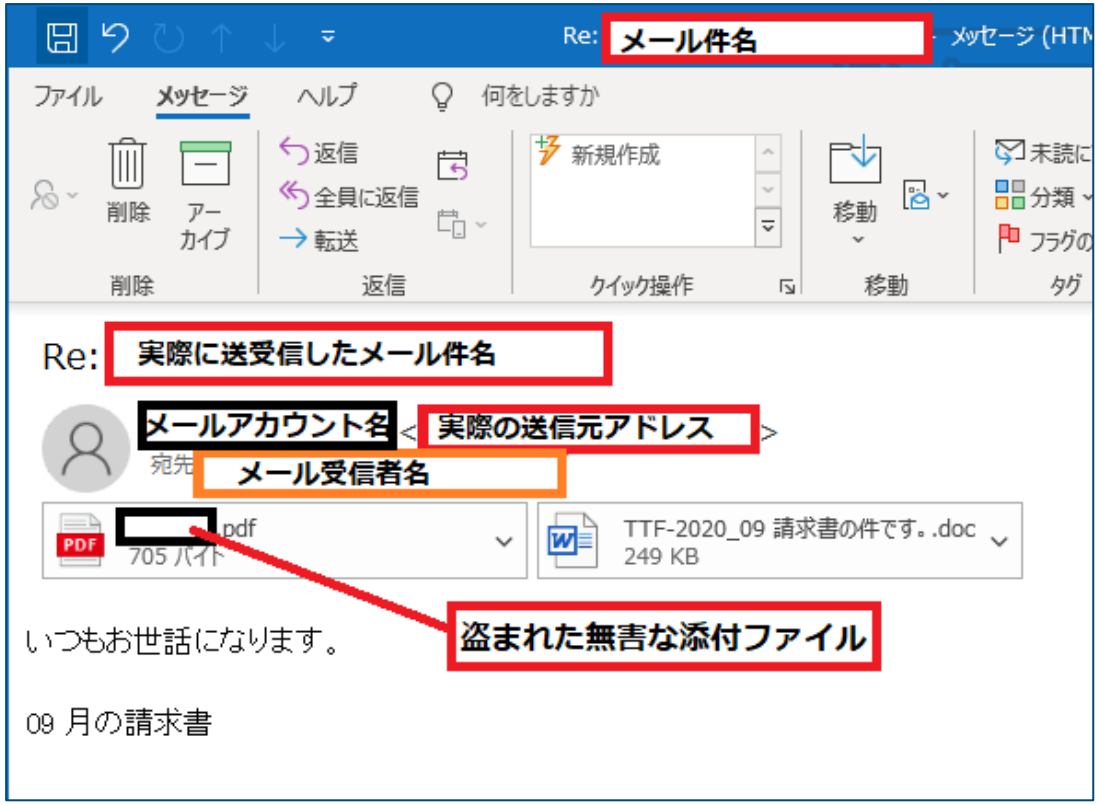
Emotetの感染拡大の流れ（3/3）

Emotetによる感染拡大のイメージ



Emotet : 2020年7月以降の特徴（1/2）

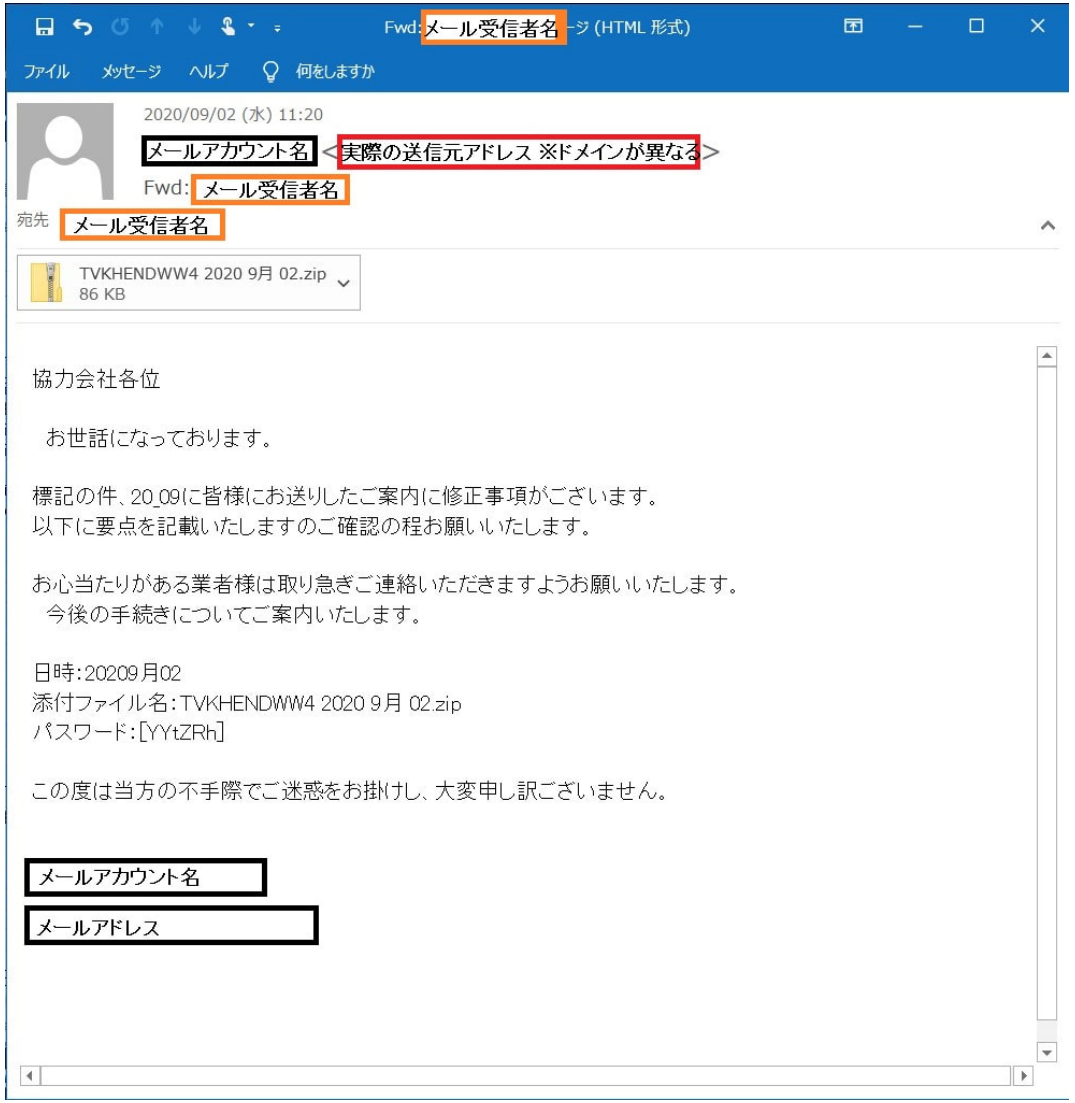
- 感染時に窃取される情報サイズが増加し、添付ファイルも窃取されるようになった
- Emotetに感染させるWord形式ファイルに加え、窃取されたファイル（無害なファイル）も添付したメールが送信される



出典：JPCERT/CC Eyes「マルウエアEmotetへの対応FAQ」
https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html

Emotet : 2020年7月以降の特徴（2/2）

- Emotetに感染させるWord形式ファイルをパスワード付きzipファイルで送付し、本文に記載されたパスワードで開封させる
- これまでメール配信経路のセキュリティ製品による検知や検疫で防いでいた組織にも届く可能性がある



出典：JPCERT/CC Eyes「マルウエアEmotetへの対応FAQ」
https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html

Emotetへの対応(1/2)

- 感染防止に向けて
  - Wordマクロの自動実行の無効化
  - メールの監査ログの有効化
  - 組織内への注意喚起
- 感染時には
  - 感染端末の隔離や証拠保全
  - 感染端末が利用していたメールアカウントや
    Webブラウザに保存されていた認証情報などのパスワード変更
  - 感染端末が接続していた組織内ネットワーク内の全端末の調査
  - 他のマルウェア（2次感染マルウェア）への感染有無の確認
    例）Emotet⇒Trickbot, Qakbot, Zloader, IcedID

➢ 詳細はJPCERT/CC Eyes「マルウェアEmotetへの対応FAQ」
（次スライドで紹介） をご確認ください

Emotetへの対応(2/2) – JPCERT/CCから

情報発信

佐條 研(Ken Sajo) 2019/12/02

マルウエアEmotetへの対応FAQ

メール

最終更新日:2021.1.27

2019年10月以降、日本国内にてEmotetの感染事例が急増しています。JPCERT/CCでは、次の通り注意喚起を発行しています。

JPCERT/CC: マルウエア Emotet の感染に関する注意喚起
https://www.jpcert.or.jp/at/2019/at190044.html
JPCERT/CC: CyberNewsFlash マルウエア Emotet の感染活動について
https://www.jpcert.or.jp/newsflash/2019112701.html
JPCERT/CC: CyberNewsFlash 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
JPCERT/CC: CyberNewsFlash マルウェア Emotet の感染拡大および新たな攻撃手法について
https://www.jpcert.or.jp/newsflash/2020090401.html

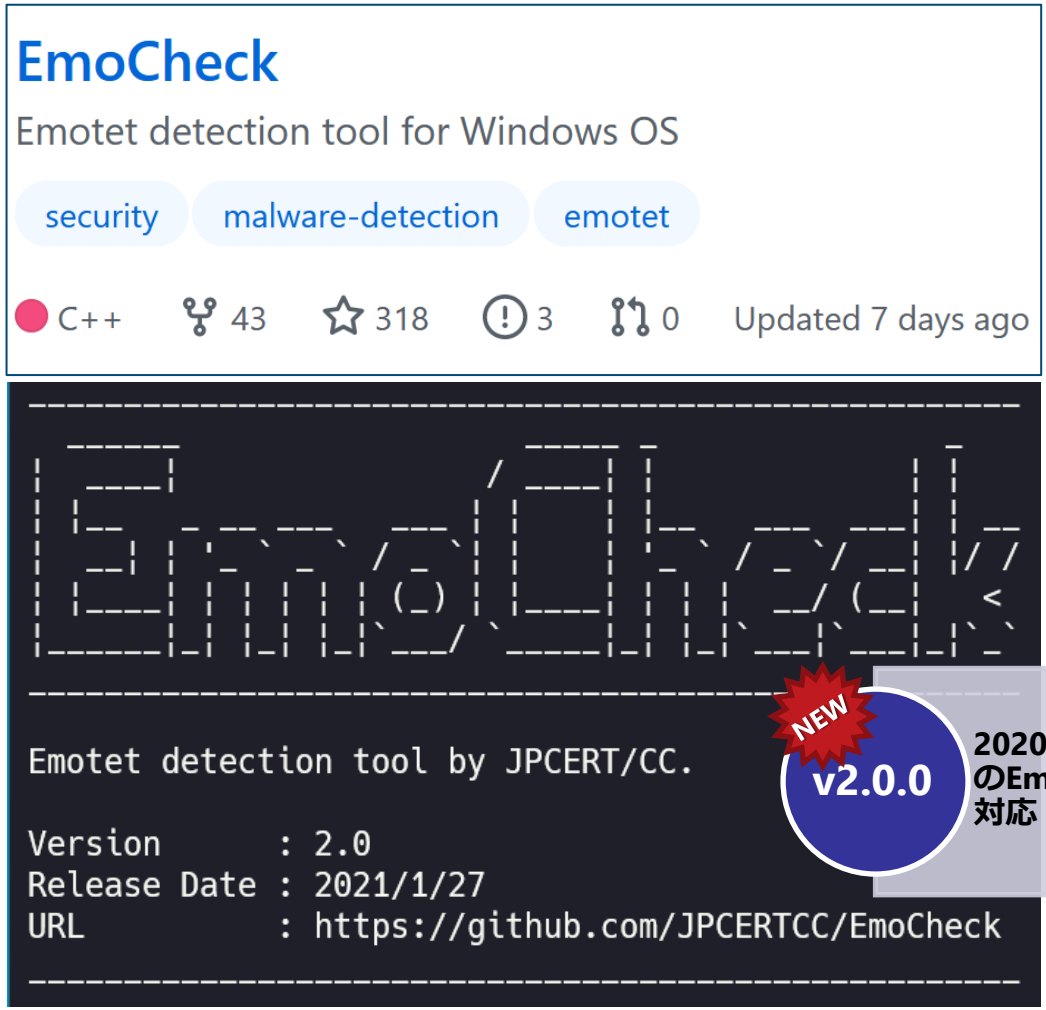
本ブログでは、2019年12月時点のEmotetに感染した疑いがある場合の確認方法や、感染が確認された場合の対処方法など、Emotetに関するFAQを掲載しています。なお、ここに記載されている調査方法がわからない場合は、専門のセキュリティベンダへの相談を検討してください。

参考： JNSAサイバーインシデント緊急対応企業一覧
https://www.jnsa.org/emergency_response/

目次
1. 外部からなりすましメールが届いたという報告があった場合どうすればよいですか?
2. Emotet の感染有無を確認するためにはどうすればよいですか?
3. EmotetはWindows OS以外に感染しますか?
4. Emotet の感染を確認した場合どのように対処すればよいですか?
5. Emotetに窃取されたメールの送信を止めるにはどうすればよいですか?
6. Emotetに感染するとどのような被害が起こりますか?
7. Emotetに感染しないためにはどのような対策が必要ですか?
（参考）メールに添付されるWordファイルを開いた場合の表示例

出典：JPCERT/CC Eyes「マルウエアEmotetへの対応FAQ」
https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html

ツール提供



EmoCheck

Emotet detection tool for Windows OS

security malware-detection emotet

C++ 43 318 3 0 Updated 7 days ago

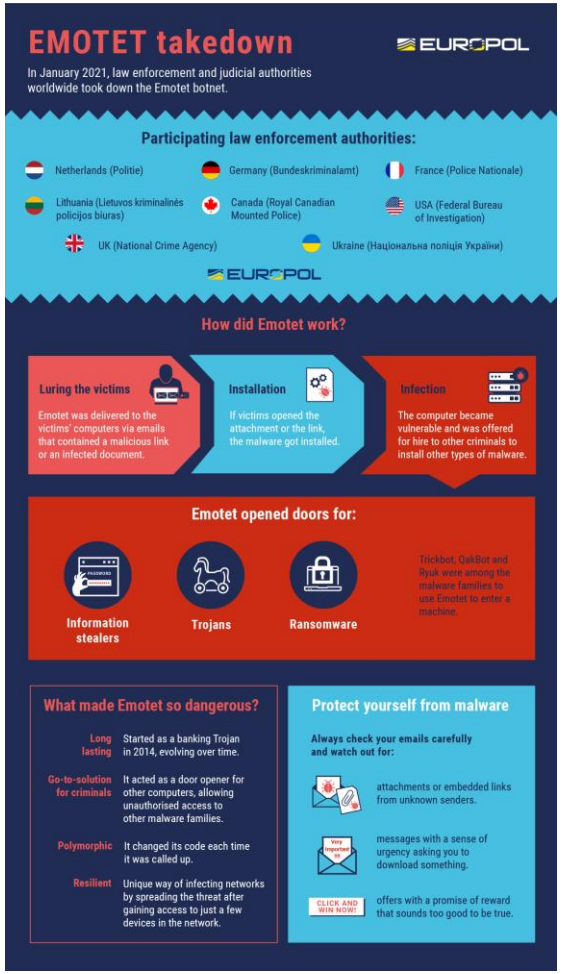
```
Emotet detection tool by JPCERT/CC.

Version      : 2.0
Release Date : 2021/1/27
URL          : https://github.com/JPCERTCC/EmoCheck
```

NEW v2.0.0

2020/12～のEmotetに対応

出典：GitHub – JPCERTCC/EmoCheck
https://github.com/JPCERTCC/EmoCheck

Emotetのテイクダウン

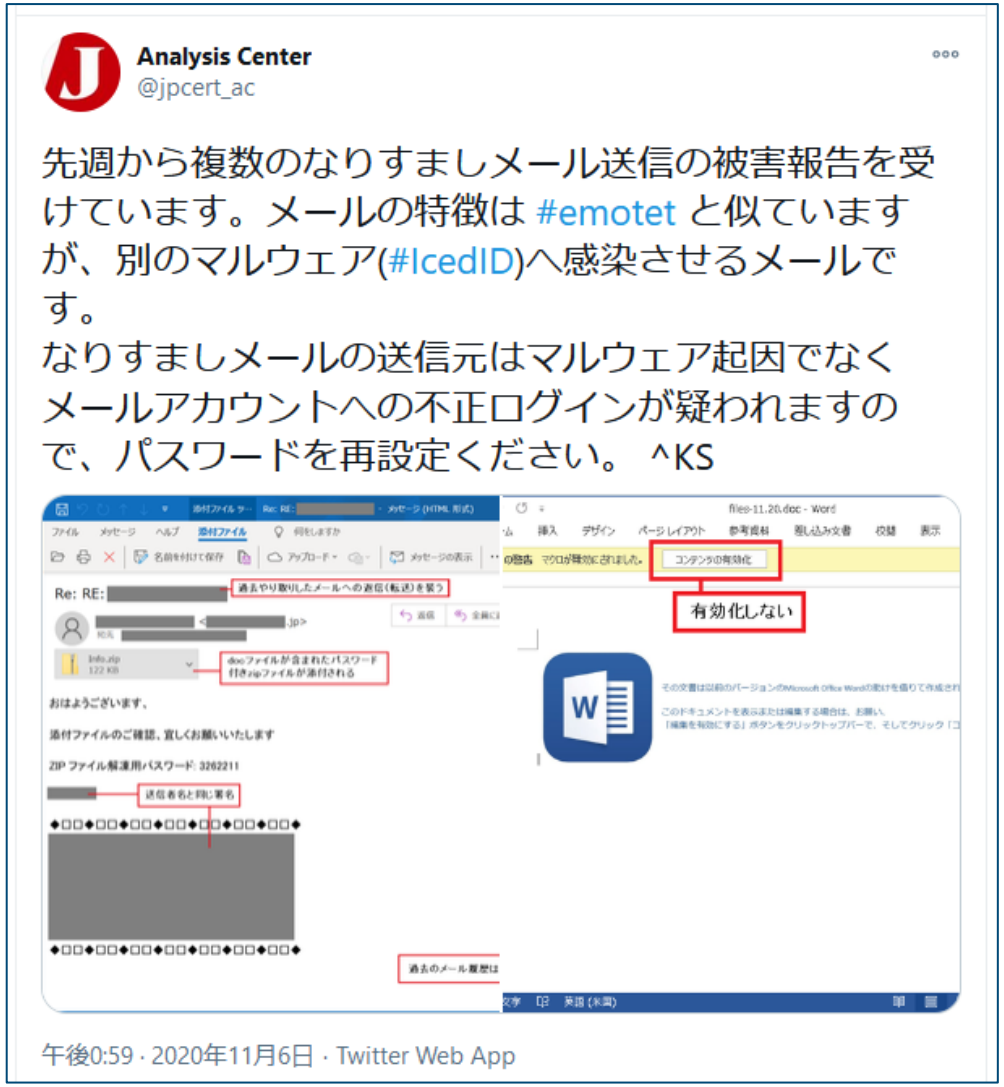


- 2021年1月27日、Europol と Eurojustが共同でEmotetのテイクダウンに関するリリースを発表
  - 8ヶ国の協調オペレーション
    - オランダ、ドイツ、フランス、リトアニア、カナダ、アメリカ、イギリス、ウクライナ
  - Emotetのインフラを法執行機関が制御
    - Emotet感染端末からの通信は法執行機関の管理するサーバーへリダイレクト
    - 感染端末のEmotetを法執行機関が用意した無害化されたファイルに置き換え
    - オランダ国家警察は侵害されたE-mailアドレス確認用のサイトを用意
      - https://www.politie.nl/emocheck
- JPCERT/CCからも関連する活動として国内の感染者への通知活動を開始

出典 : Europol : World's most dangerous malware EMOTET disrupted through global action
https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

Emotetと類似したマルウェア「IcedID」

- Emotetの活動停止期間中、 Emotetと似た特徴を持つ **IcedID** というマルウェアの被害報告あり
- マルウェア（挙動）は異なるが、受信者として注意すべき点は共通している
- Emotetと勘違いし対処を誤るケースが散見される



出典：JPCERT/CC Analysis CenterのTwitter
https://twitter.com/jpcert_ac/status/1324561915738091522

アジェンダ

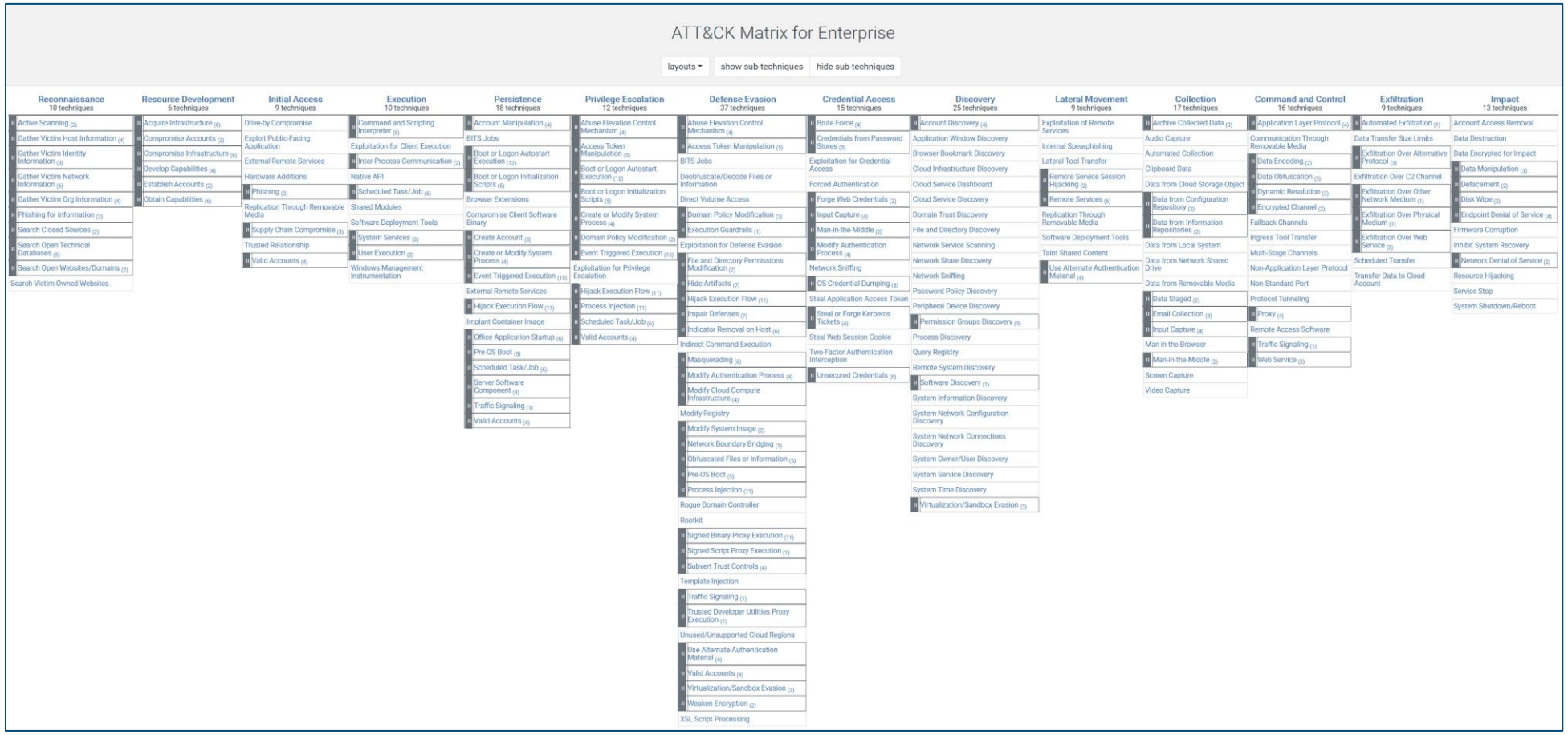
- はじめに
  - JPCERT/CCの紹介
- 2020年度サイバー攻撃動向
  - SSL VPN製品の脆弱性を悪用した攻撃
  - 標的型ランサムウェア
  - DDoS脅迫
  - Emotetの活動再開
- まとめ
- 今後へ向けて

まとめ

- サイバー攻撃は多種多様で、**どの組織も攻撃対象**になりうる
- 標的型攻撃はますます高度化し、**組織の情報は継続的に狙われ**続けている
- リモートワークでも利用される **SSL VPN製品の脆弱性**を悪用した攻撃が増加
- 新たなランサムウェアなど**脅迫をともなうサイバー攻撃**が増加（基本的に金銭は支払うべきではない）
- Emotetの経験を踏まえ、引き続き組織のコミュニケーションインフラである**メール経由の攻撃**には注視
- **脅威動向の技術的理解**は、組織としての対応を決定していく上でも重要なポイント

(参考) MITRE ATT&CK

- 攻撃者の攻撃手法を体系化したナレッジベース
- 攻撃手法を理解、整理する際の共通言語になりつつある



【出典】MITRE : ATT&CK
https://attack.mitre.org

アジェンダ

- はじめに
  - JPCERT/CCの紹介
- 2020年度サイバー攻撃動向
  - SSL VPN製品の脆弱性を悪用した攻撃
  - 標的型ランサムウェア
  - DDoS脅迫
  - Emotet
- まとめ
- 今後へ向けて

インシデントの発見

	自組織で発見		外部組織からの連絡
全体	47%	:	53%
APAC	27%	:	73%

【出典】FireEye M-Trends 2020

- インシデントは自組織で発見するものだけではないことを理解し、必要な体制構築を

協調的なインシデント対応

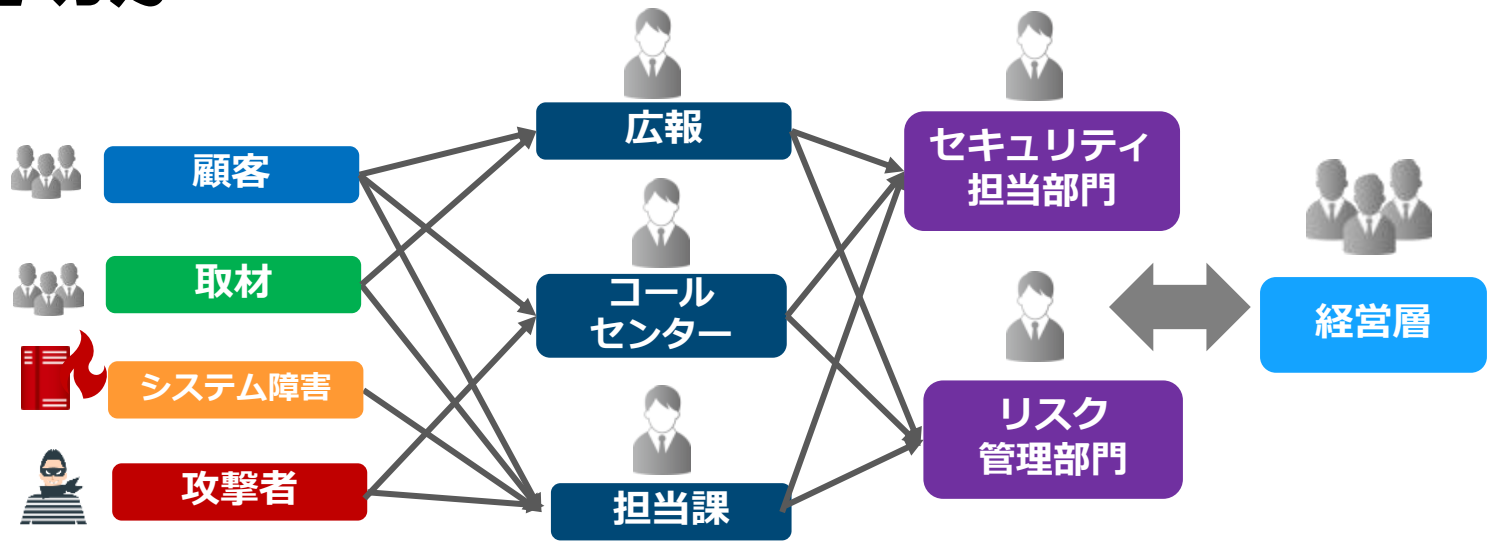
働き方の変化に伴う体制の変化

リモートワーク下のセキュリティ運用は適切か

- VPN装置や端末の適切な脆弱性管理および迅速なパッチ適用
- 未承認のリモート接続ツールの利用禁止ルールの徹底
- 外部利用端末の管理、セキュリティ運用ルールの規定と徹底

有事の対応体制は適切か

- 顧客や取材などの広報対応は
- 社内の情報共有や意思決定は
- 運用保守ベンダーの体制、作業速度は



お問い合わせ、インシデント対応のご依頼は

JPCERTコーディネーションセンター

—Email: pr@jpcert.or.jp

—Web: https://www.jpcert.or.jp/

インシデント報告

—Email: info@jpcert.or.jp

—Web: https://www.jpcert.or.jp/form/

制御システムインシデントの報告

—Email: icsr-ir@jpcert.or.jp

—Web: https://www.jpcert.or.jp/ics/ics-form.html

脆弱性に関するお問い合わせ

—Email: vultures@jpcert.or.jp

—Web: https://jvn.jp/

Thank you!