サイバー攻撃 2022

- 昨今のサイバー攻撃動向とその対応 -

JPCERTコーディネーションセンター
早期警戒グループ 三浦 拓也

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・制御システム機器など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
- 1995年から活動を実施。現在は経済産業省や内閣官房からの委託予算で活動
- 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のセキュリティに関わる担当者
- 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CSIRTが存在する（米国のCISA（US-CERT）、CERT/CC、中国のCNCERT/CC、韓国のKrCERT/CC等）

- 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
- サイバーセキュリティ基本法上の「サイバーセキュリティに関する事象が発生した場合における国内外の関係者との連絡調整を行う関係機関」
- サイバーセキュリティ協議会（2019年発足）の事務局をNISCとともに実施（事案対応の相談や情報共有活用の運用面を担当）

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

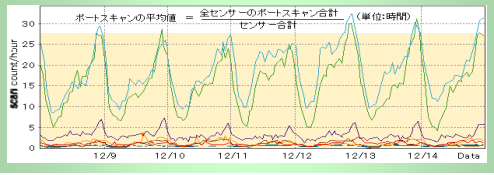
- 未公開の脆弱性関連情報を製品開発者へ提供し、対応依頼
- 関係機関と連携し、国際的に情報公開日を調整
- セキュアなコーディング手法の普及
- 制御システムに関する脆弱性関連情報の適切な流通

JVN Japan Vulnerability Notes

情報収集・分析・発信

定点観測（TSUBAME）

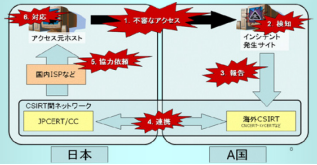
- ネットワークトラフィック情報の収集分析
- セキュリティ上の脅威情報の収集、分析、必要とする組織への提供



インシデントハンドリング

（インシデント対応調整支援）

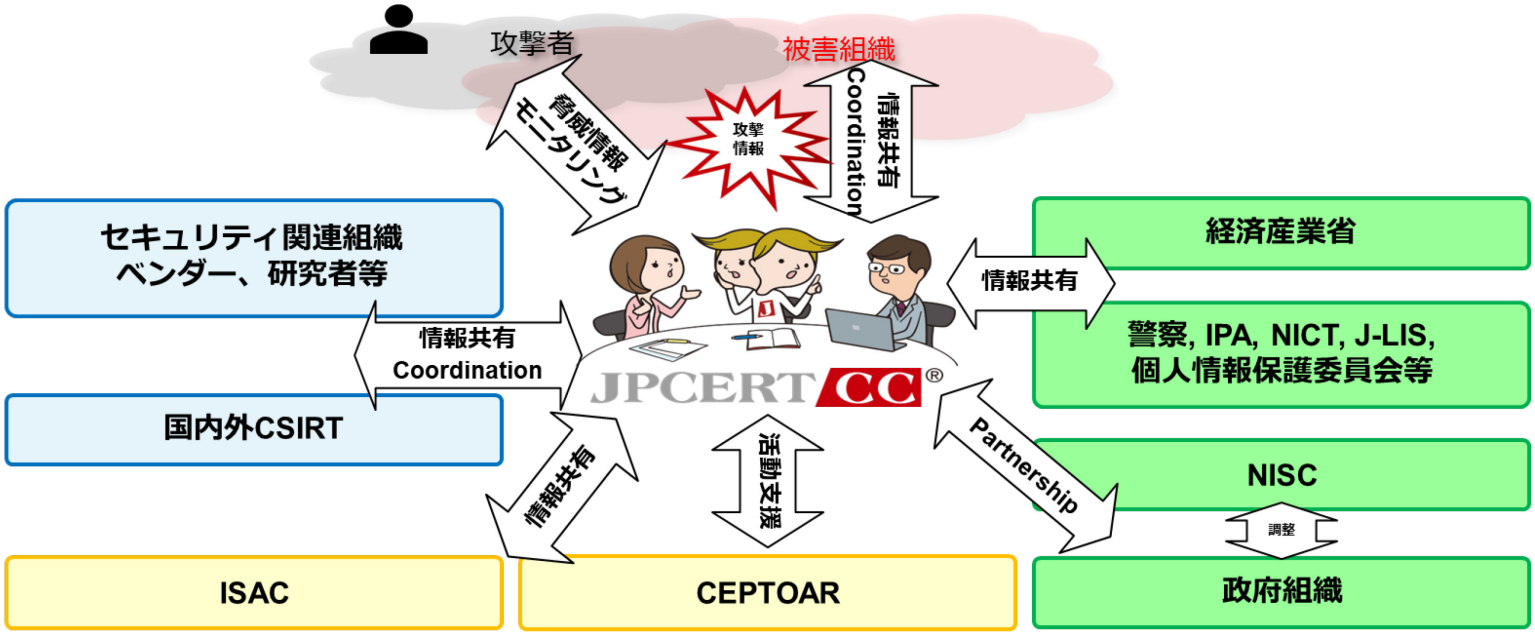
- マルウェアの接続先等の攻撃関連サイト等の閉鎖等による被害最小化
- 攻撃手法の分析支援による被害可能性の確認、拡散抑止
- 再発防止に向けた関係機関との情報交換および情報共有



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

コーディネーションセンターとしての役割

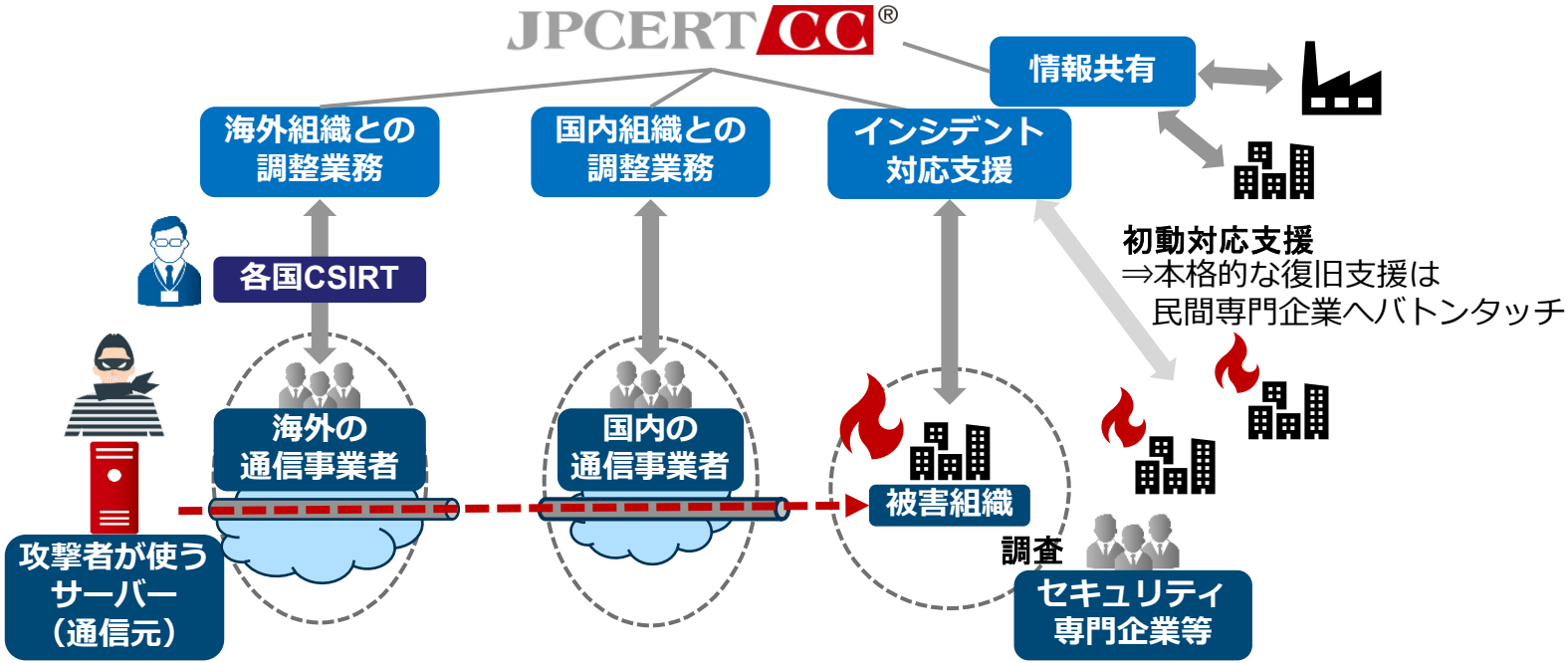
さまざまなパートナーとの調整



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

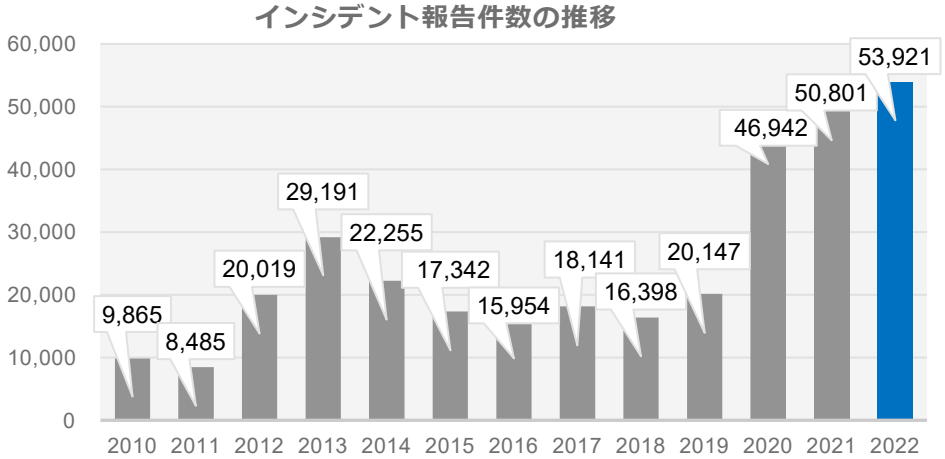
サイバー攻撃の停止に向けた国内・海外組織との調整

- 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

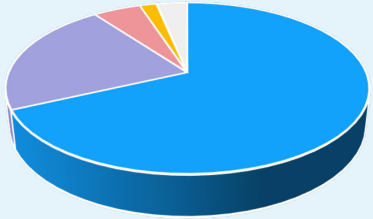


インシデント対応状況（2022年4月～2023年3月）

- JPCERT/CCへの報告
  - 全報告件数　53,921件
  - 全インシデント件数　40,263件
- JPCERT/CCからの連絡
  - 全調整件数　23,419件



インシデント件数のカテゴリー別割合



カテゴリー	割合
フィッシングサイト	68.12%
スキャン	21.75%
Webサイト改ざん	5.07%
マルウェアサイト	1.77%
DoS / DDoS	0.07%
標的型攻撃	0.02%
その他	3.20%

「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

JPCERT/CCが2022年に発信した脆弱性・脅威情報について

JPCERT/CCが公開する脆弱性・脅威情報

■ **注意喚起**（https://www.jpcert.or.jp/at/2022.html）

- 国内組織において影響が多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

47件（2022年度/更新含む）/ 2021年度 71件

■ CyberNewsFlash（https://www.jpcert.or.jp/newsflash/）

- 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

39件（2022年度/更新含む）/ 2021年度 50件

■ JVN（https://jvn.jp/）

- 「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

アラート発信の判断基準

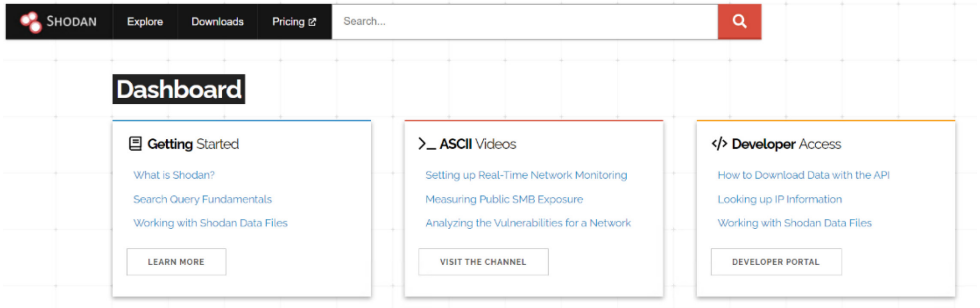
■ 次の観点でアラート発信を検討

- 脆弱性自体の脅威度
  - ➢ どういう脆弱性なのか（どういった被害が想定されるか）
    - 任意のコード実行/権限昇格/DoSなど
  - ➢ 攻撃の実現性
    - リモートから攻撃できるか/PoCが公開されているか

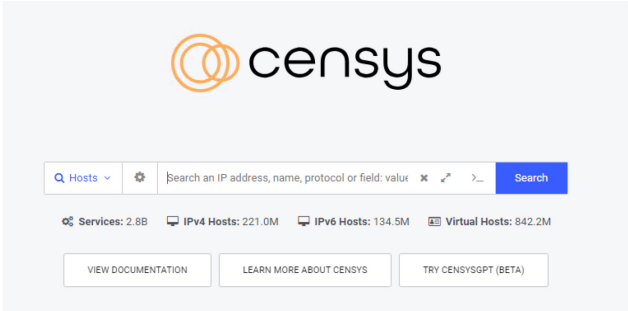
- 実際の脆弱性の悪用状況/可能性
  - ➢ 実際に攻撃活動が確認されているか
    - JPCERT/CCへの報告、センサーの検知状況
    - コミュニティー/調整ベンダーとの共有
  - ➢ 対象製品の国内利用状況/稼働状況
    - インターネット上のサービス（Shodan/Censys）の確認
    - ベンダーへの確認

（参考）Shodan、Censysとは

- Webサーバーやlot機器など、インターネットに接続している機器を無料で調査できるサービス
- サービスが収集しているバナー情報から製品名やバージョン等がわかるため脆弱性を受ける製品の数の推測が可能



出典：Shodan
https://www.shodan.io/

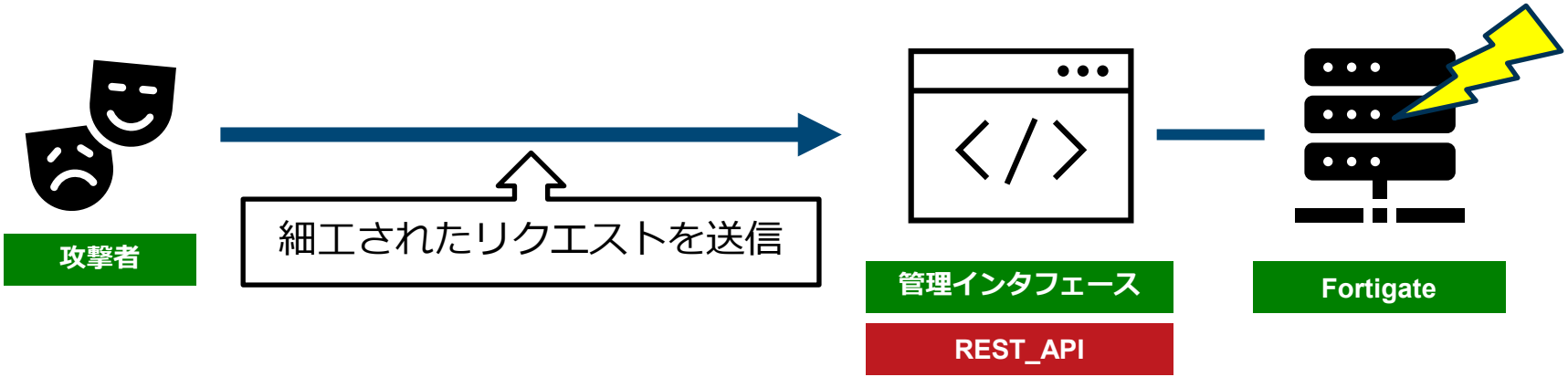


出典：Censys
https://search.censys.io/

Fortinet製FortiOS、FortiProxyおよびFortiSwitchManagerの認証バイパスの脆弱性（CVE-2022-40684）に関する注意喚起

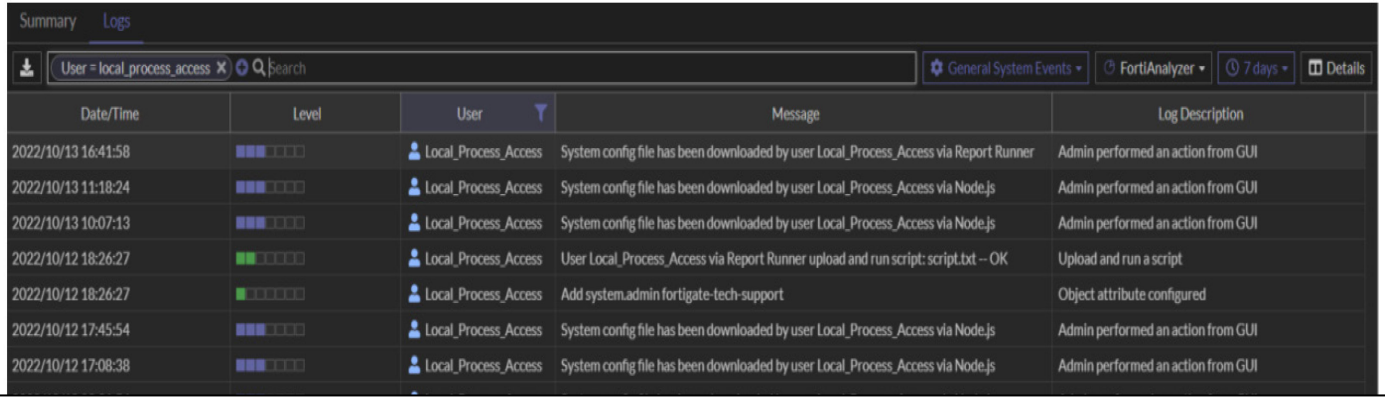
- 2022年10月10日、Fortinetが
  FortiOS、FortiProxy、FortiSwitchManager における認証バイパスの脆弱性（CVE-2022-40684）を公開

- 認証されていない遠隔の第三者が、同製品の管理インタフェースに細工したHTTPあるいはHTTPSリクエストを送信することで、結果として任意の操作を行う可能性がある



Fortinet製FortiOS、FortiProxyおよびFortiSwitchManagerの認証バイパスの脆弱性（CVE-2022-40684）に関する注意喚起

- 2022年10月14日、Fortinetが本脆弱性の悪用を報告
- また、PoCやその解説が別の組織から公開される



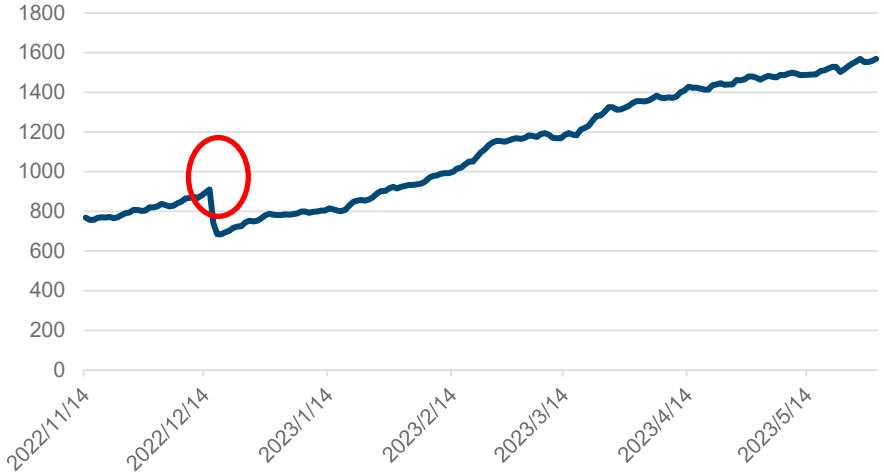
Fortinet のハニーポットで確認した当該脆弱性を狙った攻撃活動のログ

出典：Fortinet「CVE-2022-40684 に関するアップデート」
https://www.fortinet.com/jp/blog/psirt-blogs/update-regarding-cve-2022-40684

- JPCERT/CCでも本脆弱性に対するスキャンと思われる通信を確認

国内のFortiOSの管理インタフェースの露出件数

- スキャンサービスの1つのCensysのデータを活用し、FortiOSの管理インタフェースが確認できるホストを算出
  - レスポンス値からFortiOS 7系と推測するホスト件数
  - あくまで推測＋スキャンの頻度・精度に左右されるため、実態とは差分がある

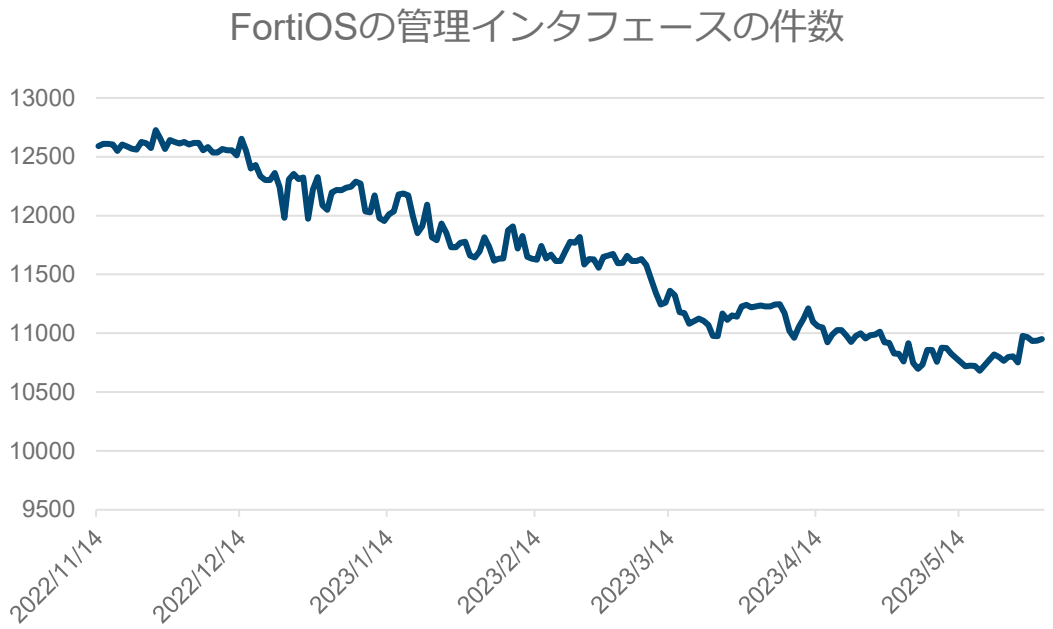


7系の管理インタフェースが露出されているホストは増加傾向
- 7系へのバージョンアップが進んでいるためと推測
- 6系を含めたFortiOSの管理インタフェースは、若干ではあるが減少傾向にある

左の図の赤枠は、後述の脆弱性の公表に伴い、若干ながら減少がみられた

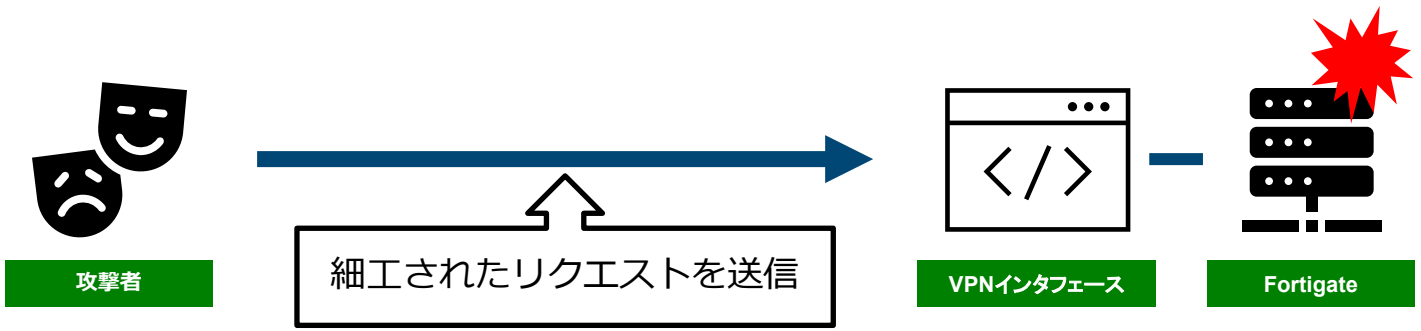
（参考）FortiOSの管理インタフェースの露出件数

- FortiOS6系を含めたFortiOSの管理インタフェースの件数



FortiOSのヒープベースのバッファーオーバーフローの脆弱性（CVE-2022-42475）に関する注意喚起

- 2022年12月12日、FortinetからFortiOS、FortiProxyのSSL-VPNにおけるヒープベースのバッファーオーバーフローの脆弱性（CVE-2022-42475）のアドバイザリ情報を公開
- SSL-VPNのWEB画面に対して、細工したリクエストを送信することで、任意のコードやコマンドを実行する可能性がある



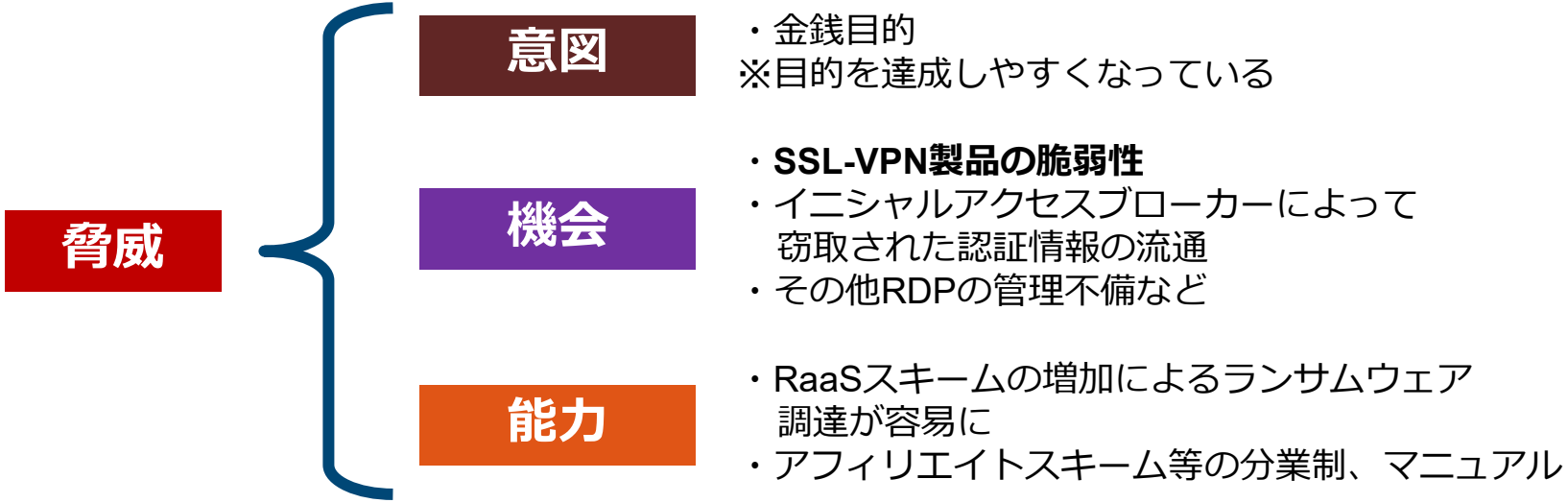
FortiOSのヒープベースのバッファーオーバーフローの脆弱性（CVE-2022-42475）に関する注意喚起

- Fortinetは本脆弱性の悪用を確認しており、アドバイザリ情報やブログにIoC情報を記載
  - Fortinetは悪用の複雑さから、高度な脅威アクターで政府または政府関連の組織を狙った可能性が高いと分析

- 対策および推奨対処
  - 修正された最新のバージョンへのアップデート
    （現在の最新版は、Fortinetが提供するアドバイザリ情報を参照）
  - 機器のログに脆弱性の悪用を示すログが記録されていないか
  - 機器に不審なファイルが設置されていないか
  - 機器から不審な通信先への通信が発生していないか

侵入型ランサムウェア

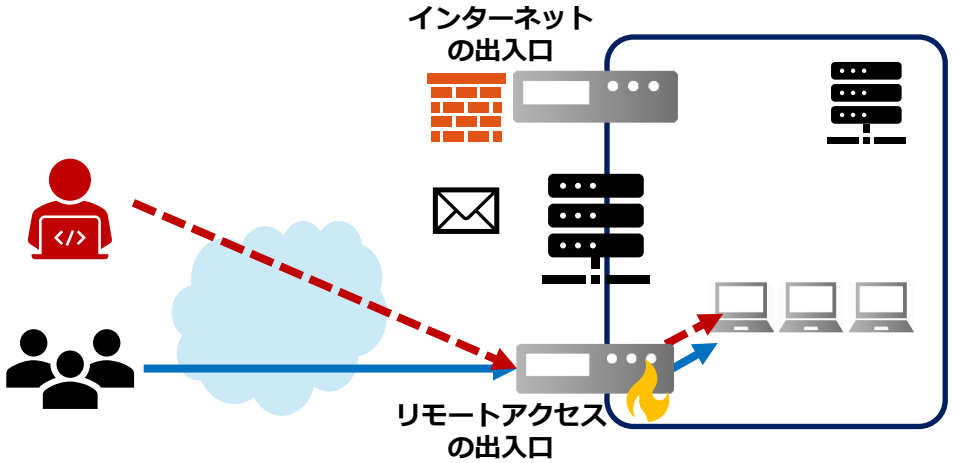
- 2022年度から引き続き、侵入型ランサムウェアによる国内組織への被害が確認されている
- さまざまな犯罪者が、侵入型ランサムウェア攻撃の市場に参入しやすい要因として、ハードルが下がっていることがあげられる



侵入経路として狙われるVPN機器

VPN機器やRDPが狙われる背景

- Webサーバーやネットワーク機器などに比べて、社内管理が弱い
- 不正アクセスに気付けるような各種ログが取得しづらい
- リモートワークの増加により、VPN機器の停止タイミングの確保が難しくなっている（＝停止による影響の増加）



侵入経路として狙われるVPN機器

■ 2022年度以降公開された情報の中でも、VPN機器への侵害が多数報告

業種	時期	報告内容（要約）
建築	2022年4月	SSL-VPNの脆弱性をついたランサムウェア「CryptXXX」による攻撃であったことが判明した
製造	2022年7月	VPN 機器の脆弱性を悪用し、窃取した認証情報を使用して侵入
製造	2022年7月	**過去にVPN機器の脆弱性により流出したと考えられる当社社員の認証情報**を利用し、7月1日～8日未明にかけて、特定の第三者が断続的に当社の社内ネットワークへアクセスした履歴が確認された
物流	2022年7月	VPN機器の脆弱性を悪用し、ネットワーク内部に侵入
行政	2022年7月	攻撃者はSSL-VPN装置の管理者アカウントの**ID／パスワード**を使用し、校務ネットワークに侵入したのち、各種サーバーにランサムウェア攻撃を実行した
情報通信	2022年9月	一部のVPN装置にて、ファームウェアを最新の状態に更新されていなかった脆弱性を悪用
製造	2022年9月	アップデート前**パスワード情報が漏えい**していたため、当時から存在していたアカウントについて、変更していなかったパスワードが不正アクセスに悪用された
食品	2022年9月	導入していたSSL-VPN機器に存在していた脆弱性を悪用され、当社VPNに不正にログインされたと判断されるとの報告を受けた

対策

- VPN機器等のアップデートを実施する
  - FortiOSに限らず、影響度の高い脆弱性が修正されているバージョンを使用する
  - EoLのバージョンを使用している場合は、EoLの情報を確認の上、EoLのないバージョンにアップデートする
- 使用していない（もしくは必要のない）管理画面を外部に公開しない
  - 必要であれば、送信元IPアドレスを制限するなどの対策を推奨
- ユーザー認証時に、多要素認証（MFA）を有効化する

（参考）侵入型ランサムウェア攻撃を受けたら読むFAQ

- 侵入型ランサムウェア攻撃について、「被害を受けたら」「被害への対応」「関連情報」に分けてインシデント対応を進める上での参考情報をFAQ形式でまとめている

[図1：侵入型ランサムウェア攻撃の特徴のイメージ]

出典： JPCERTコーディネーションセンター（JPCERT/CC）
「侵入型ランサムウェア攻撃を受けたら読むFAQ」
https://www.jpcert.or.jp/magazine/security/ransom-faq.html

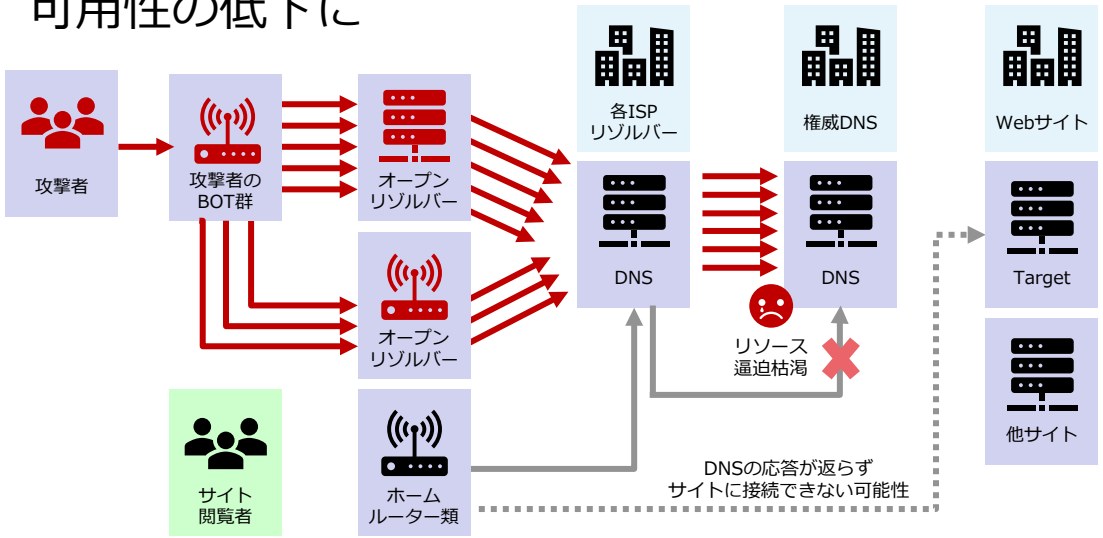
ランダムサブドメイン攻撃（DNS水責め攻撃）

概要

- 2023年3月中旬ごろからランダムサブドメイン攻撃が増加しており、国内でも影響を受けたとみられる事案を確認
- 新たな脅威ではないが、国内事例や対策のポイントについて紹介する

ランダムサブドメイン攻撃とは

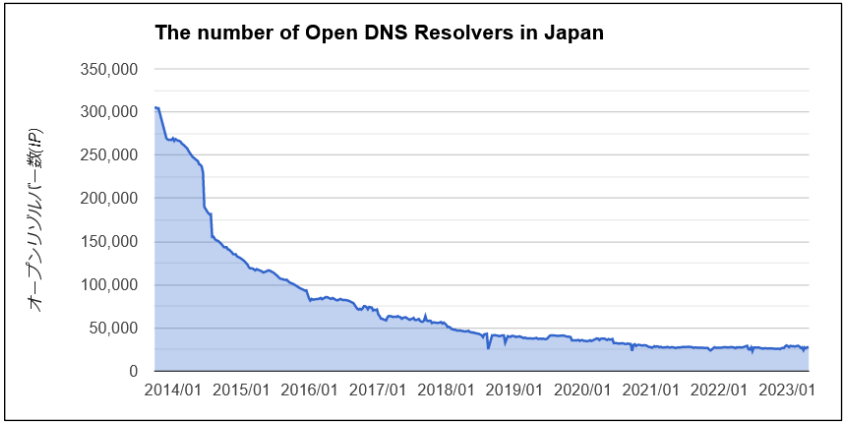
- DNSサーバーに対するDDoS攻撃手法の1つ
- 特定のドメイン名にランダムなサブドメインを付与し、
  オープンリゾルバーなどに名前解決を要求するリクエストを送信
  - 攻撃対象の権威DNSサーバーに名前解決のリクエストが集中し、
    可用性の低下に



（参考）オープンリゾルバーの国内外の状況

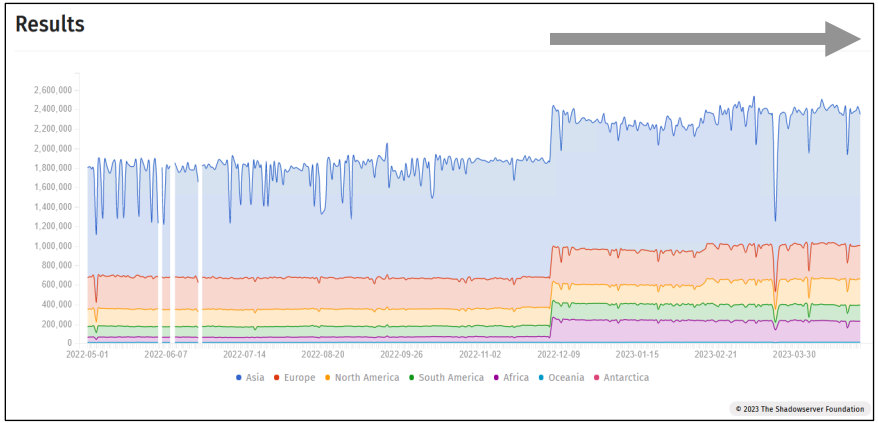
- 日本のオープンリゾルバーの数は、2023年5月時点で約3万件
  - 2013年の約30万件から約1割ほどに減少
- 2023年時点で、世界には約240万件残存していると見受けられる

国内件数（過去10年）



出典：JPCERTコーディネーションセンター（JPCERT/CC）
オープンリゾルバー確認サイト
https://www.v3.openresolver.jp/

世界的件数（過去1年）



出典：The Shadowserver Foundation「SHADOWSERVER」
https://dashboard.shadowserver.org/statistics/combined/time-series/?date_range=365&source=scan&source=scan6&tag=dns&style=stacked

直近の国内事例

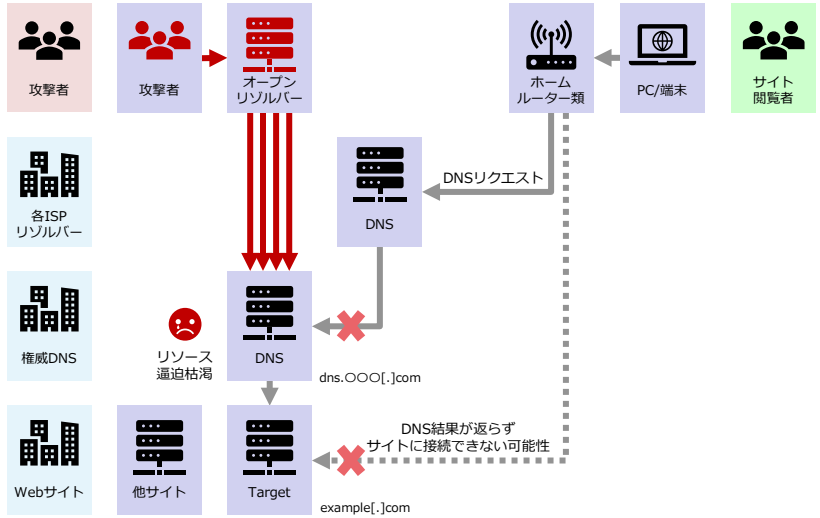
- 2023年3月中旬以降、複数の自治体などで攻撃を受け、影響が出ていた可能性がある事案
  - 主な影響は、Webサイトの閲覧不可
  - 影響時間は、1時間で収まるケースから数時間かかるケースまでさまざま

攻撃被疑日時	攻撃期間	対象組織	サイト接続観測	報告/プレス
2023/04/21 22:00 - 28:00	約 6 時間	JRおでかけネット	断続的に接続不可	つぶやき程度
2023/04/27 06:40 - 07:40	約 1 時間	JPCERT/CC	なし	なし
2023/04/28 15:30 - 21:30	約 6 時間	鹿児島県	断続的に接続不可	報道有
2023/04/29 05:00 - 12:00	約 7 時間	富山県	断続的に接続不可	なし
2023/04/29 20:45 - 21:45	約 1 時間	京都府	断続的に接続不可	なし
2023/04/30 03:10 – 14:00	約 11 時間	沖縄県	断続的に接続不可	なし
2023/04/30 03:10 - 06:45	約 3.5 時間	大阪府	断続的に接続不可	なし
2023/05/01 14:30 - 22:15	約 8 時間	ナビタイム	断続的に接続不可	関連プレス有

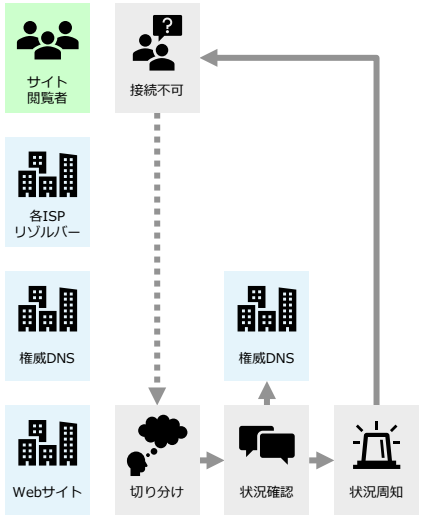
ランダムサブドメイン攻撃に対しての事前準備

- ランダムサブドメイン攻撃かどうか事象を特定する
- サーバ側では対策は不可であるため、周知方法、構成を事前に検討

攻撃イメージ図



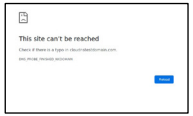
対処のポイント



事象の特徴

（1）名前解決エラーでの接続不可
（2）IPアドレスを指定すると接続可
（3）同じ権威DNSを使うサイトでも影響

例: エラー画面例



例: hostsファイルでIP指定時

周知ポイント

Webサービスでは
Webサイトに接続できない状況を想定し
別の手段での周知方法も検討する

マルウェアのEmotetについて

Emotetの国内活動

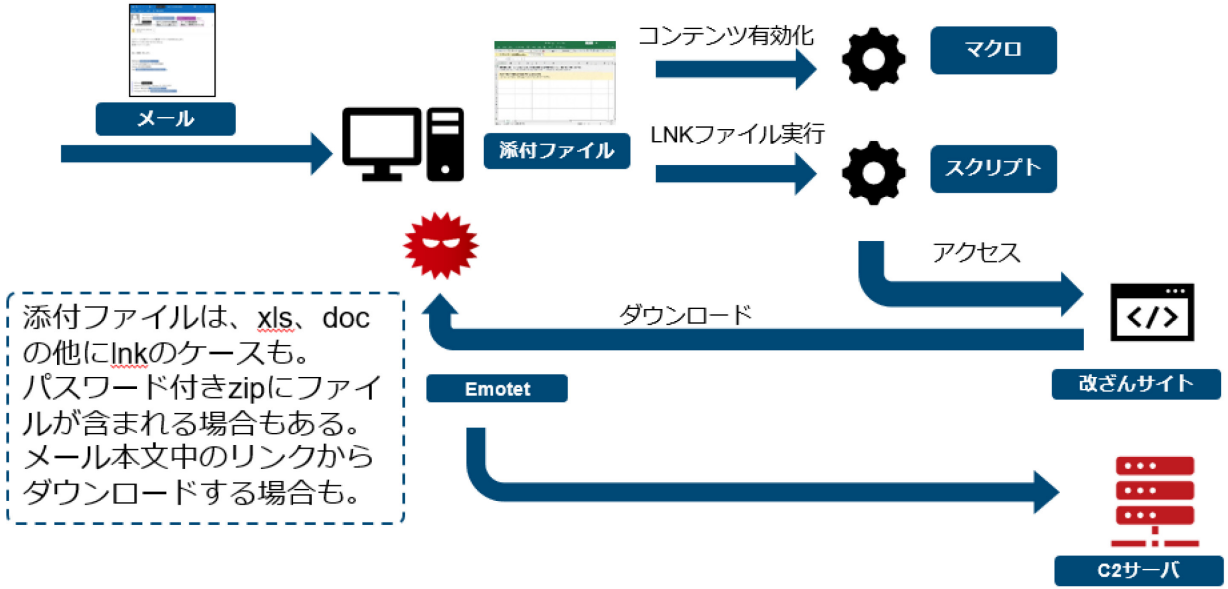
Emotetの活動

- バンキングトロジャンの一種として2014年に確認
- モジュール化など、マルウェアの感染・拡散を行う機能などを追加

時期	活動
2019年11月	国内における感染拡大および被害が増加、JPCERT/CCが注意喚起
2020年2月	活動停止
2020年7月	感染を目的としたメールの配信活動が再開
2020年9月	パスワード付きzipファイルが添付されたメールが確認される
2020年10月	活動停止
2020年12月	感染を目的としたメールの配信活動の再開（挙動の変化あり）
2021年1月	EUROPOL（欧州刑事警察機構）によるテイクダウンのプレスリリース
2021年11月	感染を目的としたメールの配信活動の再開（2022年7月活動停止）
2022年11月	**感染を目的としたメールの配信活動の再開**

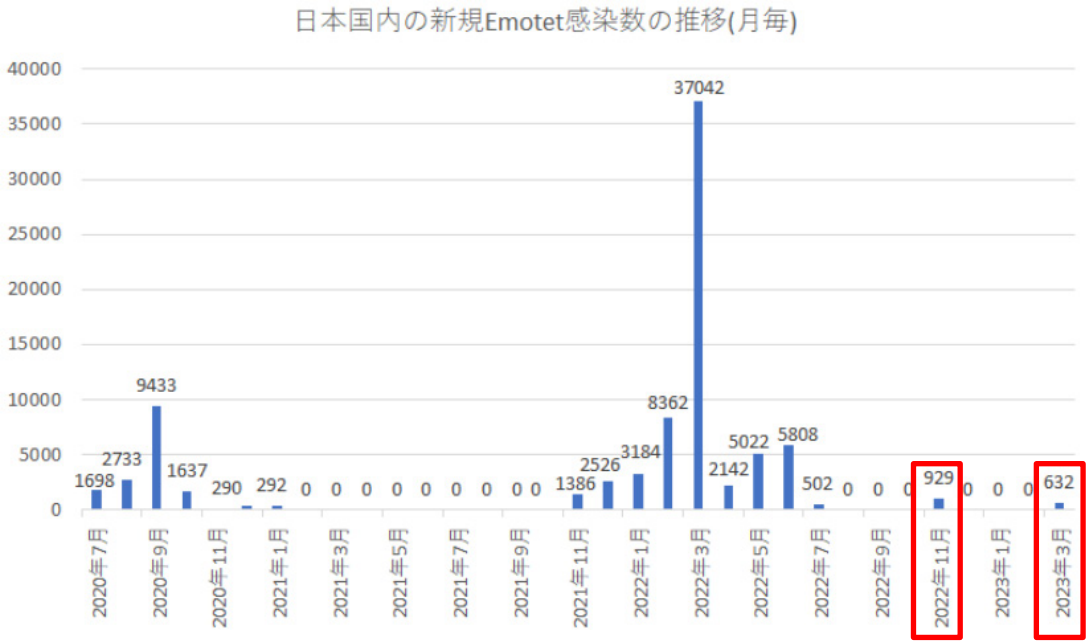
Emotetの活動

- Emotet（感染の方法）
  - ユーザーがメールに添付されたExcel形式ファイルなどを開き「コンテンツの有効化」⇒ Emotetに感染させる



Emotetの活動再開

- 2023年3月7日より、メール配布を確認
- 以前より感染数は減ったものの定期的に復活（3月以降は観測無し）

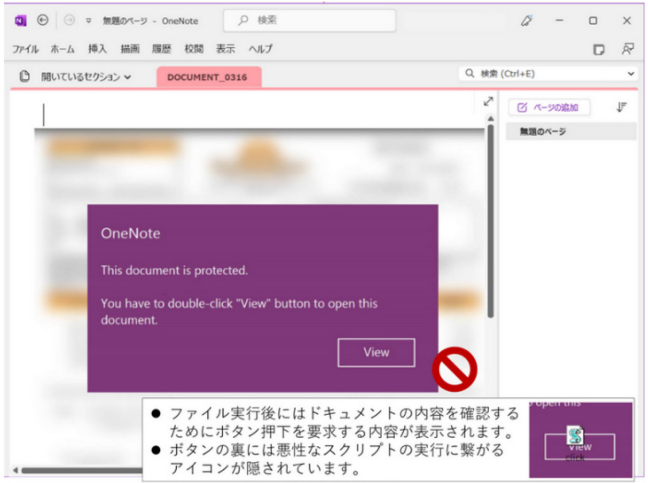


出典：JPCERTコーディネーションセンター（JPCERT/CC）
マルウェアEmotetの感染再拡大に関する注意喚起
https://www.jpcert.or.jp/at/2022/at220006.html

Emotet感染の対策

- 不審なメールの添付ファイルを開かないことが前提

1. 信頼できるものと判断できない場合は送信元へ確認する
2. エクセルやワード以外のオフィス製品も見られるが
   スクリプトを実行しないことは変わらず

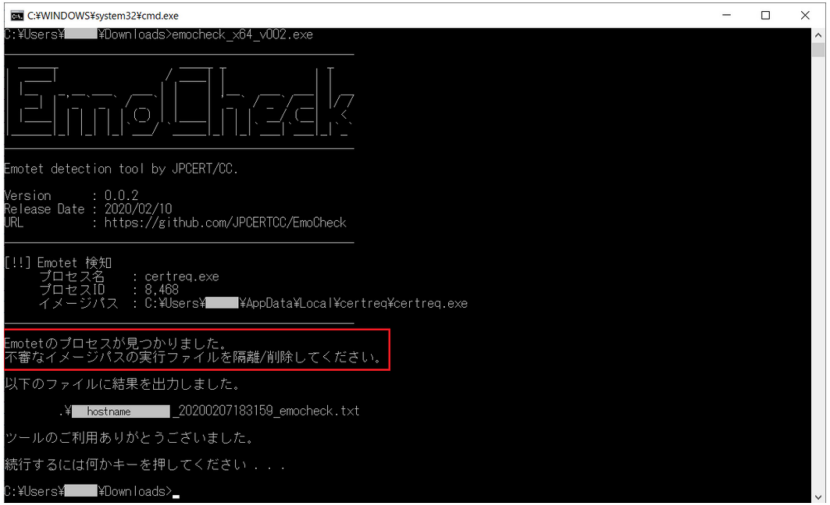


EmoCheck

- Emotetに感染しているか、確認を行うツール。
  感染が疑われる（主に通常その端末を使用しているユーザー）でログインし、ツールを実行。

- 最新のEmotetに対応できるように適宜アップデートを行っている。
  （現在の最新verはv2.4.0）

- 2022年11月以降のEmotetでも検知することを確認している



出典：JPCERTコーディネーションセンター（JPCERT/CC）
EmoCheck
https://github.com/JPCERTCC/EmoCheck

マルウエアEmotetへの対応FAQ

- 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

出典：JPCERTコーディネーションセンター（JPCERT/CC）
JPCERT/CC Eyes「マルウエアEmotetへの対応FAQ」
https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html

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
- https://www.jpcert.or.jp/reference.html

インシデント報告

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

脆弱性に関するお問い合わせ

- Email：vultures@jpcert.or.jp
- https://jvn.jp/

ご清聴ありがとうございました

Thank you!