サイバー攻撃２０２１+

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
脅威アナリスト
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
  （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

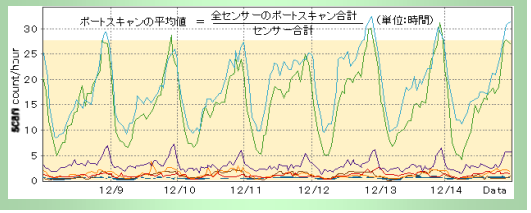
- 未公開の脆弱性関連情報を製品開発者へ提供し、対応依頼
- 関係機関と連携し、国際的に情報公開日を調整
- セキュアなコーディング手法の普及
- 制御システムに関する脆弱性関連情報の適切な流通

JVN Japan Vulnerability Notes

情報収集・分析・発信

定点観測（TSUBAME）

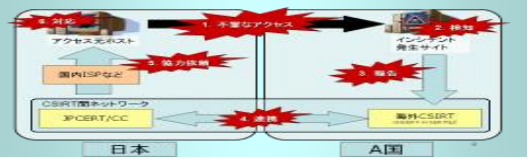
- ネットワークトラフィック情報の収集分析
- セキュリティ上の脅威情報の収集、分析、必要とする組織への提供



インシデントハンドリング

（インシデント対応調整支援）

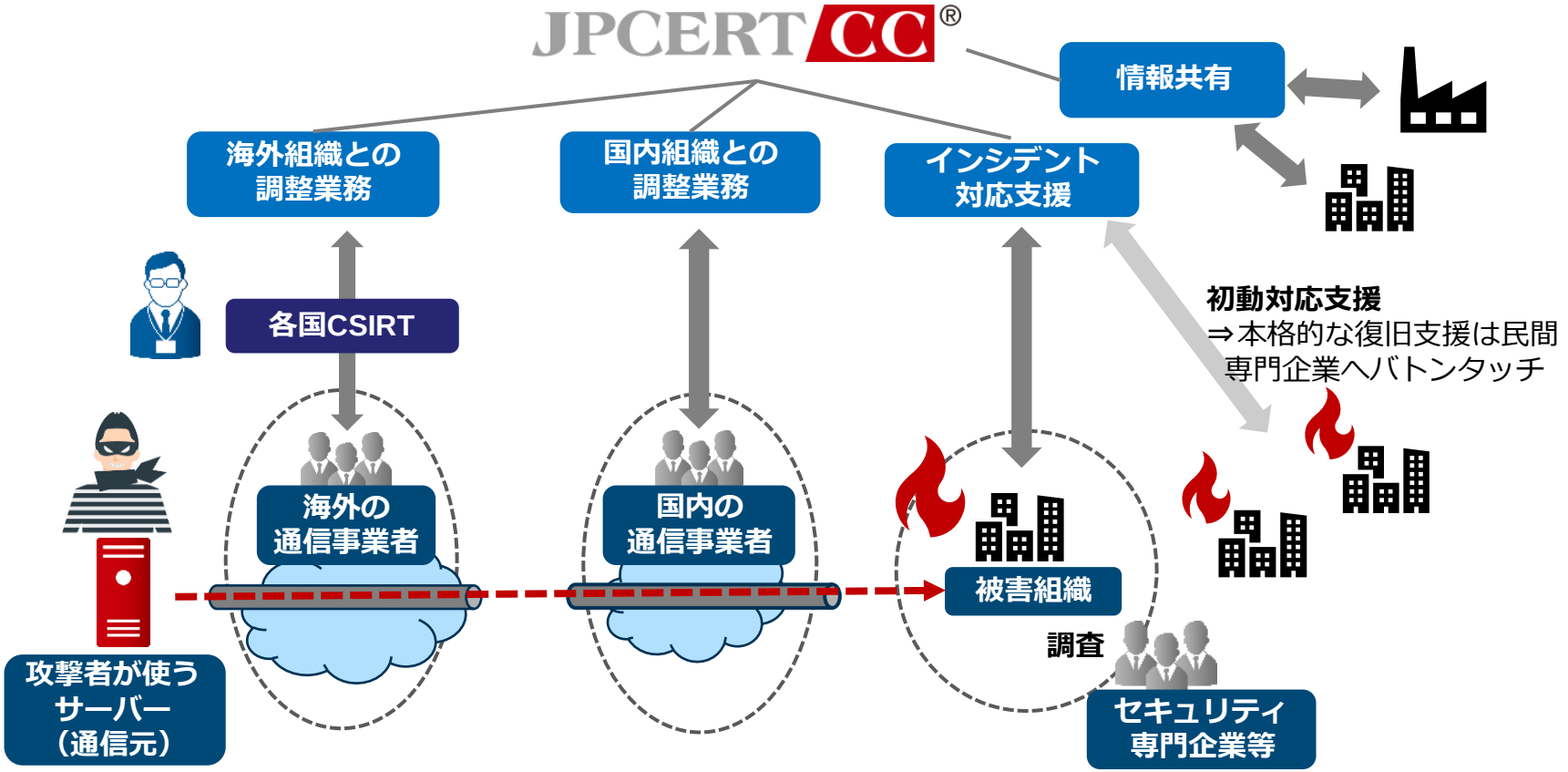
- マルウェアの接続先等の攻撃関連サイト等の閉鎖等による被害最小化
- 攻撃手法の分析支援による被害可能性の確認、拡散抑止
- 再発防止に向けた関係各関の情報共有



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

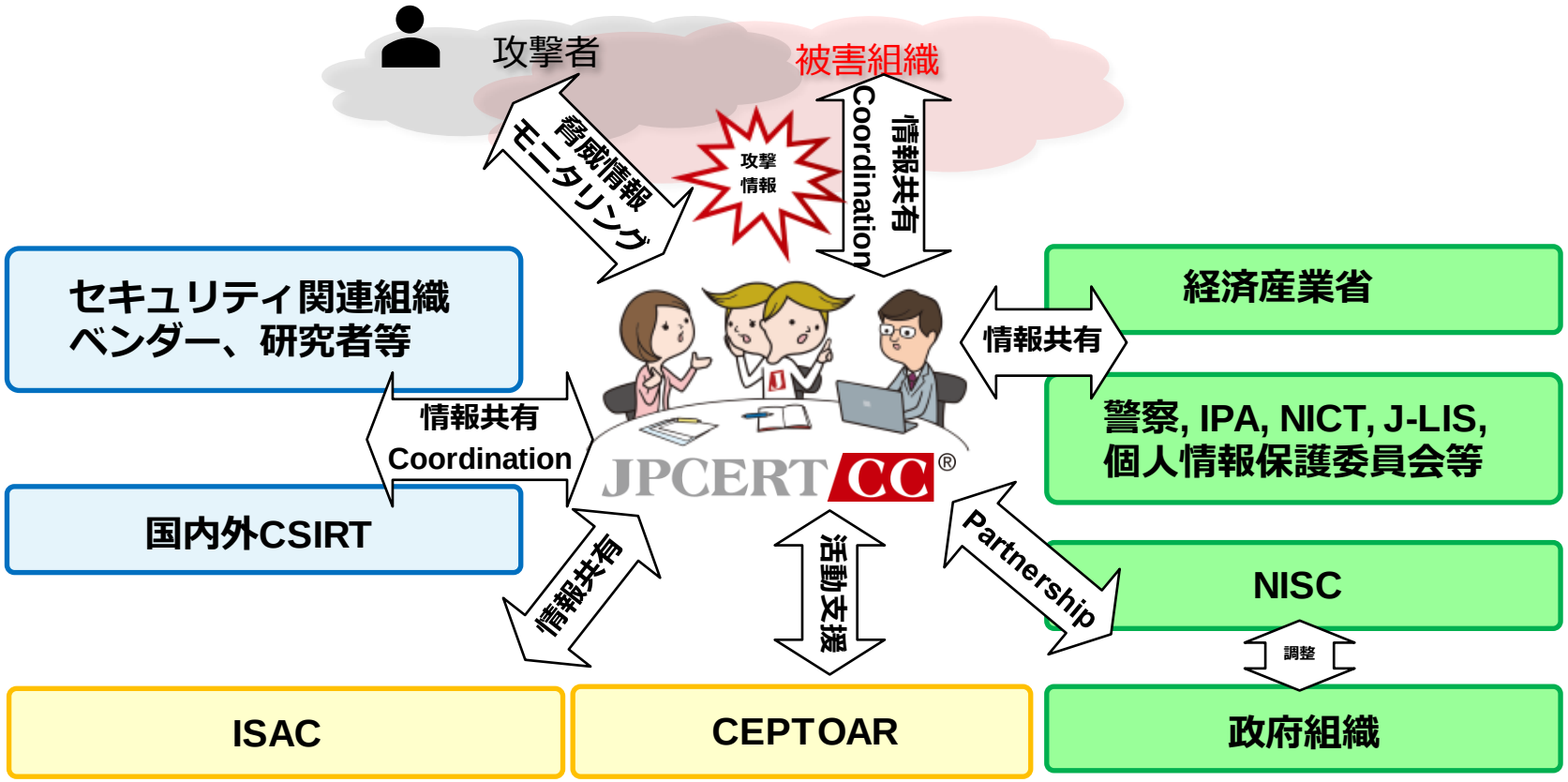
サイバー攻撃の停止に向けた国内・海外組織との調整

- 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

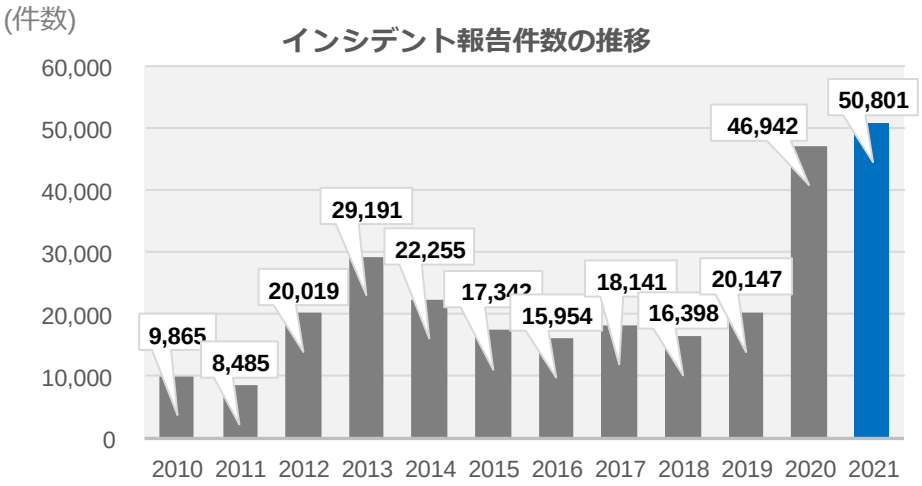
さまざまなパートナーとの調整



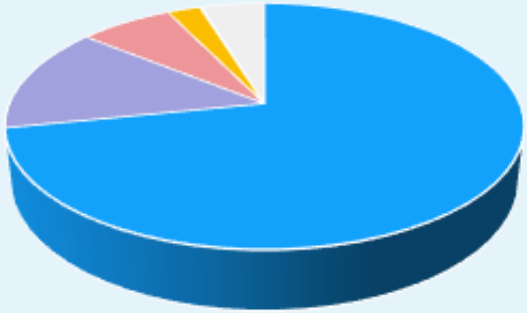
インシデントに関する調整（coordination）機関として、問題解決に向けて、必要な人に必要な情報を届ける業務を行っています

インシデント対応状況（2021年4月～2022年3月）

- JPCERT/CCへの報告
  - 全報告件数
    50,801件
  - 全インシデント件数
    34,938件
- JPCERT/CCからの連絡
  - 全調整件数
    20,571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	71.83%
スキャン	13.91%
Webサイト改ざん	6.98%
マルウエアサイト	2.44%
DoS / DDoS	0.11%
標的型攻撃	0.03%
その他	4.69%

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
2021年度に発信した
脆弱性・脅威情報について

JPCERT/CCが発信する脆弱性・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　74件（更新含む）

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　60件（更新含む）

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

Microsoft Exchange Serverの複数の脆弱性に関する注意喚起(CVE-2021-26855等)

- Microsoft Exchange Serverに存在する脆弱性が4つ公開された。脆弱性が悪用された場合、遠隔の第三者がSYSTEM権限で任意のコードを実行するなどの可能性がある。
  - 2021/3/2 マイクロソフトから情報公開、注意喚起を発行
  - 対策は公開されたセキュリティ更新プログラムの実施
- 本脆弱性の悪用も確認されており、アップデートに加えて、脆弱性を悪用する攻撃の被害有無の調査を推奨するとともに、侵入の痕跡有無を調査するPowerShellスクリプトなどをGithubで公開している

マイクロソフト株式会社
Exchange Server の脆弱性の緩和策
https://msrc-blog.microsoft.com/2021/03/07/20210306_exchangeoob_mitigations/

他にも今年はMicrosoft MSHTMLの脆弱性(CVE-2021-40444)など定例外で公開された

Movable TypeのXMLRPC APIにおける脆弱性（CVE-2021-20837）に関する注意喚起

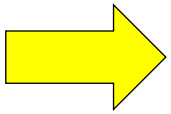
- Movable TypeのXMLRPC APIに存在するOSコマンドインジェクションの脆弱性
  - 10/20 ベンダーより情報公開、同日にJVN/注意喚起発行（https://www.sixapart.jp/movabletype/news/2021/10/20-1100.html）
  - Movable Type 4.0以降のすべてのバージョンが本脆弱性の影響を受ける（サポート終了をしたバージョンを含む）

- Movable TypeのXMLRPC APIに細工したメッセージをPOSTメソッドで送信することで、任意のOSコマンドが実行可能となる
  - 対策済みバージョンへのアップデート
  - XMLRPC APIへのアクセス制限等の対処が必要
    - 「/mt-xmlrpc.cgi」への外部アクセスがないかの確認

2021年11月以降に公表された影響の大きい脆弱性

Apache Log4jの任意のコード実行の脆弱性（CVE-2021-44228等）

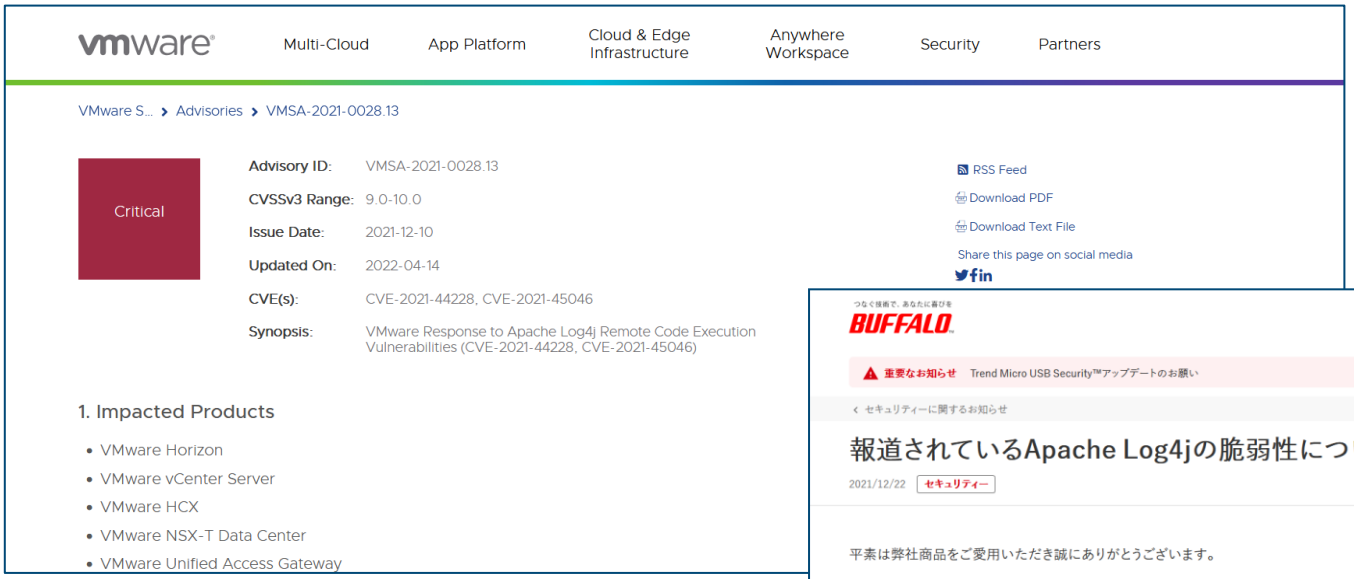
- 2021年12月10日、Javaベースの**オープンソースのロギングライブラリ**のApache Log4jに関して複数の脆弱性が報告された。
- 「Log4Shell」とも呼ばれる
- Apache Log4jのJNDI Lookup機能を悪用するもの。遠隔の第三者が細工した文字列を送信し、**Log4jがログとして記録すること**で、Log4jはLookupにより指定された通信先もしくは内部パスからjava classファイルを読み込み実行し、結果として任意のコードが実行される可能性がある。



Log4jの利用方法によっては、チャットに特定の書き込みをするだけで、任意のコード実行が実行可能に！

本脆弱性の影響範囲

- オープンソースのロギングライブラリであり、Javaのログ出力に関してはデファクトスタンダードとして利用するソフト/製品/サービスが多く存在している。



出典：VMware,Inc.
Advisories VMSA-2021-0028.13
https://www.vmware.com/security/advisories/VMSA-2021-0028.html

出典：株式会社バッファロー（BUFFALO INC.）
報道されているApache Log4jの脆弱性について
https://www.buffalo.jp/news/detail/20211222-01.html

関連する脆弱性

- 12月10日に**CVE-2021-44228**が公開されてから、修正不備等の理由で関連する脆弱性が複数公表された

CVE-2021-45046
- 2.15.0での修正不十分による、特定条件下で任意のコード実行が可能な脆弱性
- 公開当初はサービス運用妨害の脆弱性と報告されたが、のちにリモートからの任意のコード実行が可能と修正された

CVE-2021-45105
- 自己参照による制御不能な再帰から保護されていないことに起因し、Log4jの特定の設定のみ影響を受けるサービス運用妨害攻撃の脆弱性

CVE-2021-44832
- Apache Log4jのJava Naming and Directory Interface（JNDI）機能で特定のデータソースを使用する場合に起因するリモートからの任意のコード実行の脆弱性

⇒ 脆弱性の対応にあわせて一か月の間に複数回のアップデートが公開された

【参考情報】脆弱性公開のタイムライン

日付	CVE-2021-44228	CVE-2021-45046	CVE-2021-45105	CVE-2021-44832
2021/11/25	脆弱性の報告			
2021/12/10	修正バージョン 2.15.0の公開			
2021/12/11	悪用の確認			
2021/12/15		修正バージョン 2.16.0（Java 8以降のユーザー向け）及び 2.12.2（Java 7のユーザー向け）の公開		
2021/12/18		CVSS評価値の更新		
2021/12/19			修正バージョン 2.17.0（Java 8以降のユーザー向け）の公開	
2021/12/22	2.12.3（Java 7のユーザー向け）及び修正バージョン 2.3.1（Java 6のユーザー向け）を公開	2.12.3（Java 7のユーザー向け）及び修正バージョン 2.3.1（Java 6のユーザー向け）を公開	2.12.3（Java 7のユーザー向け）及び修正バージョン 2.3.1（Java 6のユーザー向け）を公開	
2021/12/28				2.17.1（Java 8以降のユーザー向け）、2.12.4（Java 7のユーザー向け）及び2.3.2（Java 6のユーザー向け）を公開

悪用事例

- 複数のランサムウェア攻撃の侵入の際にLo4Shellを利用
  - 「NightSky」と呼ばれるランサムウェア
    - MS社によると中華アクター「DEV-401」によるもの
    - VMwareHorizon に存在するLog4Shellを利用し、侵入
  - 「Conti」と呼ばれるランサムウェア
    - vCenterServerに対しての本脆弱性を悪用
    - PoC公開の3日後には、興味を示していたとの話も
- 「log4Shell」の脆弱性を狙う数十万回もの攻撃試行を検出したとのベンダの報告もされている
  - 攻撃試行の大半は米国を標的としており、次いで英国、オランダ、チェコとなっており、およそ180の国と地域が攻撃を受けていることが確認した

アラート発信の判断基準

- 次のような観点でアラート発信を検討
  - 脆弱性としての観点
    - どういう脆弱性なのか（どういう被害が想定されるか）
      - コード実行なのか/権限昇格なのか/DoSに繋がるものなのか …
    - 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 …
  - 脅威としての観点
    - 実際に攻撃活動が確認されているか
      - JPCERT/CCへの報告やセンサーの検知状況
      - コミュニティー/調整ベンダとの共有
      - 国内/海外のリサーチャーの反応…
    - 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 等）の確認
      - 取り扱いベンダー等へのコンタクト
      - JPCERT/CCの発信情報を見てもらえるか

JPCERT/CCから発信される情報について

- 日々、収集する情報の中で影響が大きいと判断するものを注意喚起/CyberNewsFlashとして出している
- 中には攻撃活動/国内被害を確認している事象もありますので、是非一度確認を！

- 対策としてはパッチ（対策バージョン）の適用が多い
  - 注意喚起起因だけでなく、自組織で利用している製品の管理状況、**更新情報の取り方**の整備を行い、気付けるように
    - log4jのようにパッとはわからないことも、、
  - そもそも、利用製品が必要なく外にさらされていないかなど、**設定が意図したものになっている**かなどの管理も重要

ランサムウェア攻撃による国内組織の被害

ランサムウェアとは

- 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、または画面ロックなど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： 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

「個人」向け脅威	順位	「組織」向け脅威
スマホ決済の不正利用	1	ランサムウェアによる被害
フィッシングによる個人情報等の詐取	2	標的型攻撃による機密情報の窃取
ネット上の誹謗・中傷・デマ	3	テレワーク等のニューノーマルな働き方を狙った攻撃
メールや SMS 等を使った脅迫・詐欺の手口による金銭要求	4	サプライチェーンの弱点を悪用した攻撃
クレジットカード情報の不正利用	5	ビジネスメール詐欺による金銭被害
インターネットバンキングの不正利用	6	内部不正による情報漏えい
インターネット上のサービスからの個人情報の窃取	7	予期せぬ IT 基盤の障害に伴う業務停止
偽警告によるインターネット詐欺	8	インターネット上のサービスへの不正ログイン
不正アプリによるスマートフォン利用者への被害	9	不注意による情報漏えい等の被害
インターネット上のサービスへの不正ログイン	10	脆弱性対策情報の公開に伴う悪用増加

出典：IPA（独立行政法人情報処理推進機構）「情報セキュリティ10大脅威 2021」
https://www.ipa.go.jp/security/vuln/10threats2021.html

ランサムウェア／脅迫攻撃の種類

(参考) 類型別比較

最近の傾向

最近対応件数が少ない ⟵ ⟶ 最近対応件数が多い

攻撃類型	メール経由	DB侵害/手動操作	ボット経由侵害	RDP経由侵害		SSL-VPN経由侵害	
				非暴露	暴露型	非暴露	暴露型
攻撃例	Locky 2016年 GandCrab 2018年	DB削除攻撃 2020年 AWS S3攻撃 2021年	Ryuk 2019年頃 （Trickbot経由）	Phobos 2020年	Maze 2020年	Cring 2021年	Lockbit2. 0 2021年
侵入後活動	感染端末データ暗号化 SMB拡散機能で横展開	情報窃取、サーバ操作 データ削除および脅迫	感染端末ボット化 感染拡大機能の横展開 人手の侵害拡大 感染端末データ暗号化	人手の 侵害拡大 感染端末 暗号化	Cobalt Strike/RAT実行 人手の侵害拡大 情報窃取と暴露脅迫 感染端末データ暗号化		
被害規模	限定的 感染端末 ファイルサーバー	限定的 インターネットから 直接接続可能な 侵入対象サーバー	中規模 マルウェア感染ボット 横展開後の感染ボット 人手による横展開	中規模 接続先 システム 横展開	中／大規模 ADサーバー侵害後は 組織内で広く被害に		
国内被害 JPCERT/CCへの 相談状況	大きな被害にならず 相談件数は少ない	以前から被害報告は あるものの少ない 2021年前半で複数相談有	疑義のある事案あるも 具体的に確認できず	日本企業海外法人の 被害で疑義ある事案有 原因特定に至らず		複数の被害事例で確認 疑義のある事案確認	

国内組織の被害事例

※ 復旧期間は、業務復旧の公表タイミングを参考にしています。

	A社 建設業	B社 食料品業	C社 情報・通信業	D社 倉庫・運輸関連業
類型	暴露型	非暴露型	暴露型	暴露型
影響対象	業務システム メールサーバーなど	財務会計システムなど	国内外社内システムなど	国外業務システムなど
影響内容	サーバー利用不可など	基幹ITアプリ利用不可など	サーバー利用不可 個人情報流出の可能性など	サーバー利用不可 情報窃取および暴露など
侵入原因	メール経由の マルウェア感染	原因不明	SSL-VPN製品の 脆弱性悪用	原因不明
復旧手段	クリーンインストール バックアップから復旧	仮サーバー設置導入	システム再構築	システム再構築
復旧期間	約2か月	約2か月以上	約1-3か月	約2か月以内

事案A

2020年9月発生、サーバ70台のうち95%が暗号化
23日発生、基幹システム復旧は30日、ファイル
サーバー復旧は翌4日（復旧までに約10日以上）

事案B

2020年11月発生、2021年4月最終報
最大約39万人分の個人情報漏洩の可能性
11.5億円の身代金要求 日本米国で被害

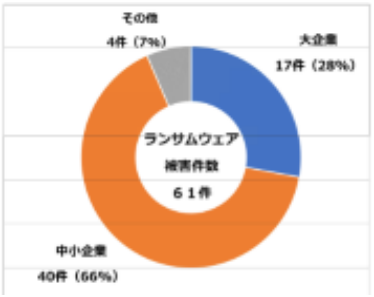
※ 公表されているプレスリリースから

今年のランサムウェア攻撃の相談件数

警察庁へのランサムウェア被害の相談報告

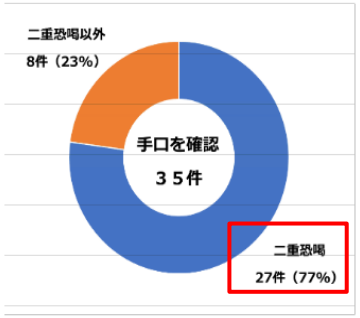
令和2年下半期
21件

令和3年上半期
61件

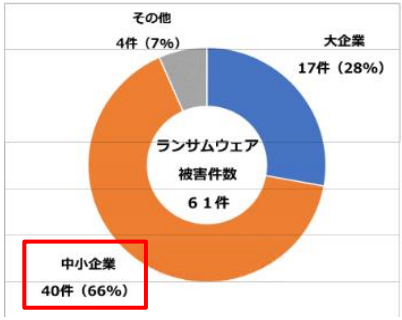


警察庁 - 令和３年上半期におけるサイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_kami_cyber_jousei.pdf

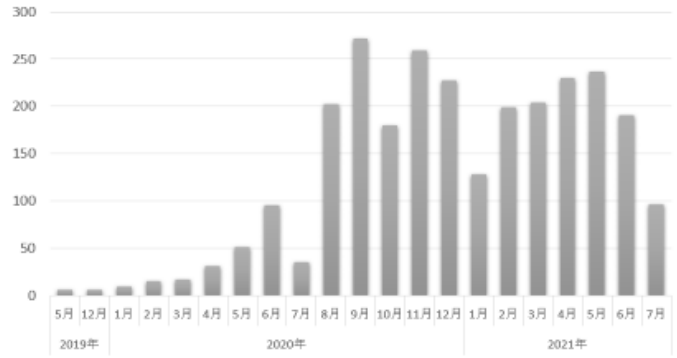
約半数が二重脅迫型
27件



中小企業での被害
40件



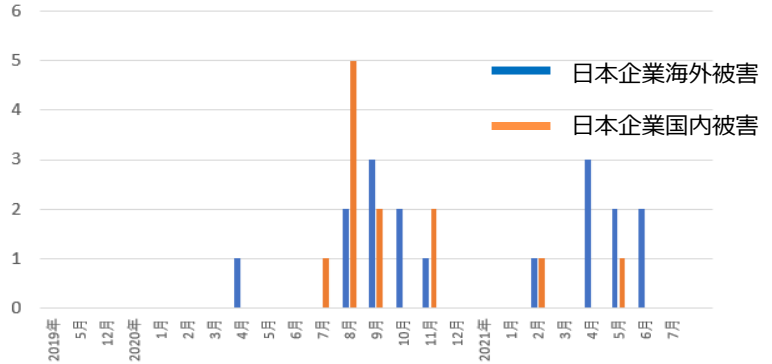
二重脅迫のリークサイトの投稿件数



2020年6-12月
1175件

2021年1-6月
1189件

内、日本組織に関係する投稿件数



2020年6-12月
18件

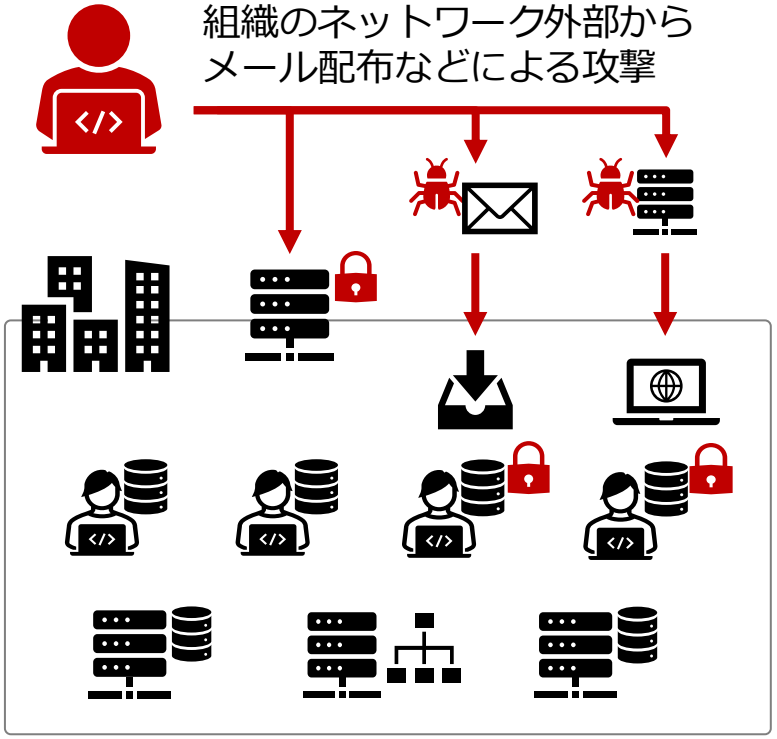
2021年1-6月
12件

DarkTracer@darktracer_int 公開データより作成（https://twitter.com/darktracer_int）

ランサムウェア攻撃の変化

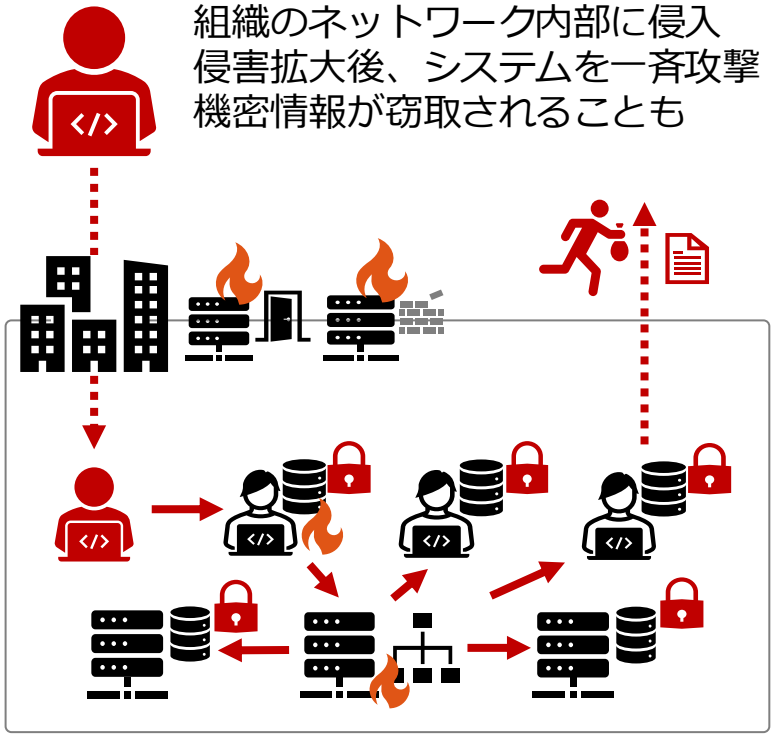
これまでのランサムウェア攻撃

組織のネットワーク外部から
メール配布などによる攻撃



最近みられるランサムウェア攻撃

組織のネットワーク内部に侵入
侵害拡大後、システムを一斉攻撃
機密情報が窃取されることも



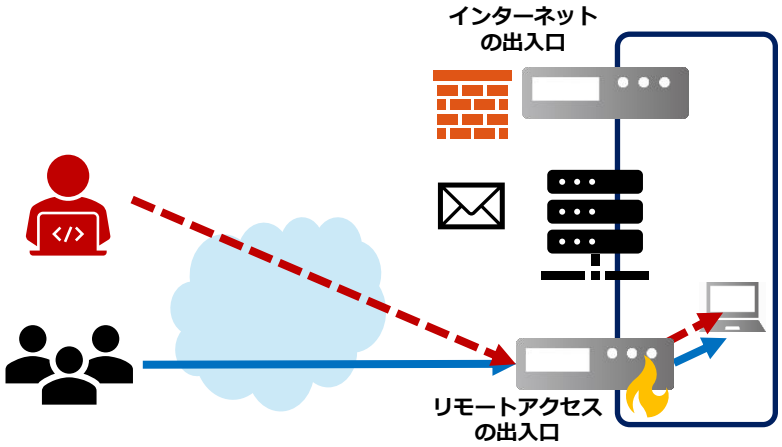
標的型攻撃に似た手法

JPCERT/CCでは、
新入型ランサムウェア攻撃と呼んでいる

リモートアクセス対策について

SSL-VPNやRDPの見直しを

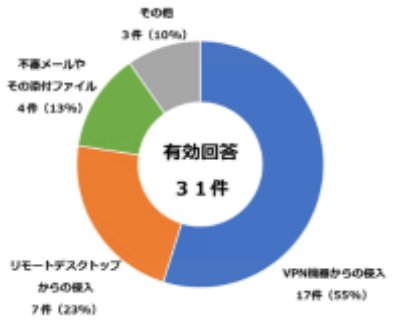
- コロナ禍でリモートアクセス増
- MFA未実装、アクセス制限不十分
  脆弱性未対応の出入口は、
  攻撃者にも魅力的な侵入経路



警察庁レポート

55% VPN機器からの侵入

23% RDPからの侵入



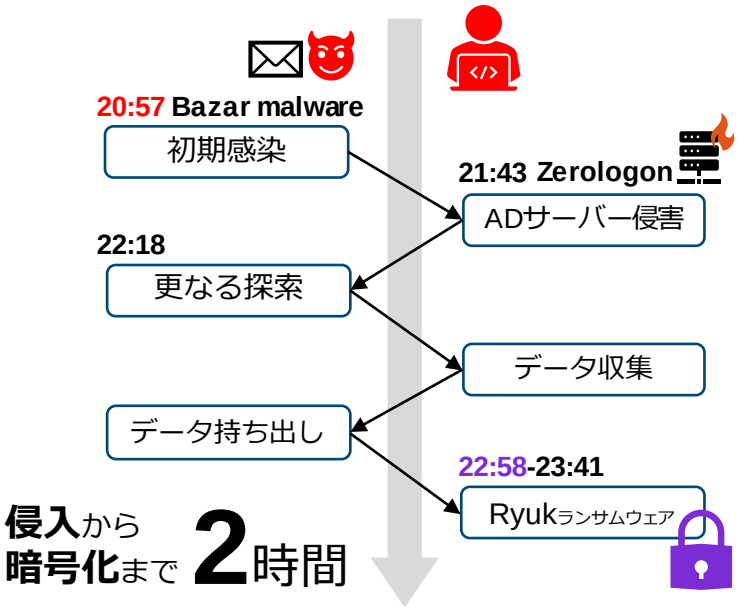
対策

- リモートアクセス出入口の点検
- 深刻な脆弱性への迅速な対応
- 対策以外にも必要な対応を徹底

警察庁 - 令和３年上半期におけるサイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_kami_cyber_jousei.pdf

脆弱性およびEoL対策について

■内部でも深刻な脆弱性には確実に対応を



The DFIR Report - Ryuk Speed Run, 2 Hours to Ransom
https://thedfirreport.com/2020/11/05/ryuk-speed-run-2-hours-to-ransom/

手法

- 脆弱性を悪用しADサーバーの管理者アカウントを容易に掌握
- 情報窃取や暗号化まで迅速に達成

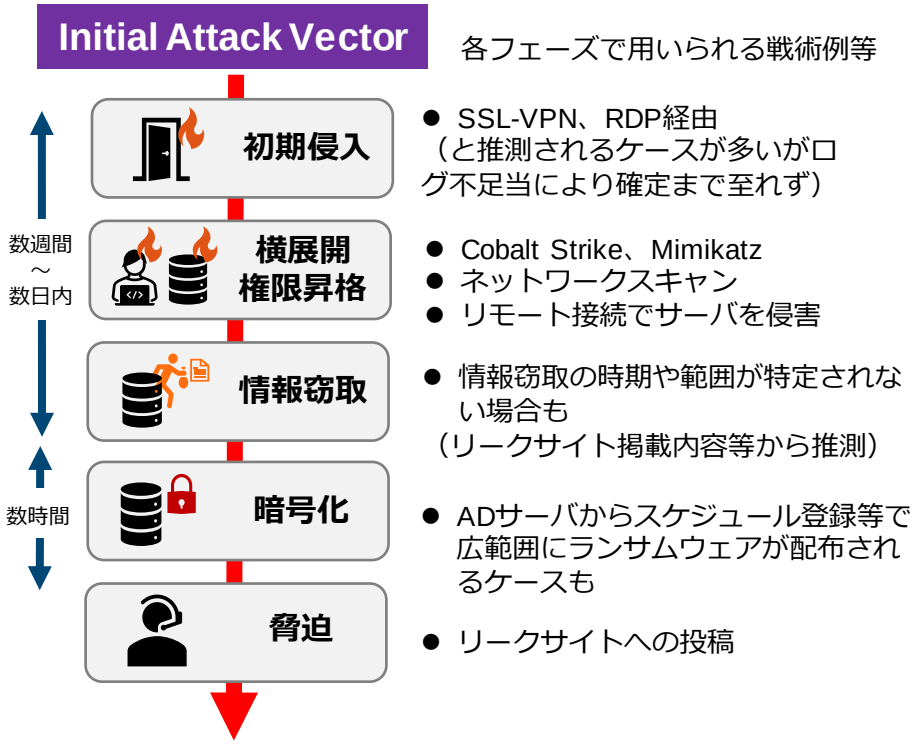
対策

- 内部ネットワークのシステムでも深刻な脆弱性には確実に対応
- サポート終了の製品への対応

JPCERT/CC 対応事案の特徴

事案の特徴

- ランサムウェアの暗号化被害後の相談リークサイト暴露投稿後の相談が大半
- ある程度の調査が終わってから、原因が特定できない等の相談が来るケースも
- 日本企業の海外子会社／拠点が被害を受けるケースが大半
- 原因特定に至れないケースが大半
  2021年においては、2020/11に発覚した脆弱なFortiGateリストに該当している被害組織が多い
- ADサーバはじめ、サーバを中心に数十台規模で暗号化されるケースも
- 調査・復旧に1か月以上かかるものが大半
- 初動対応段階でランサムウェア特定を誤るなどして、用いられた侵入方法を推測できず、原因特定に至れていないケースが散見される



侵入型ランサムウェア攻撃を受けたら読むFAQ

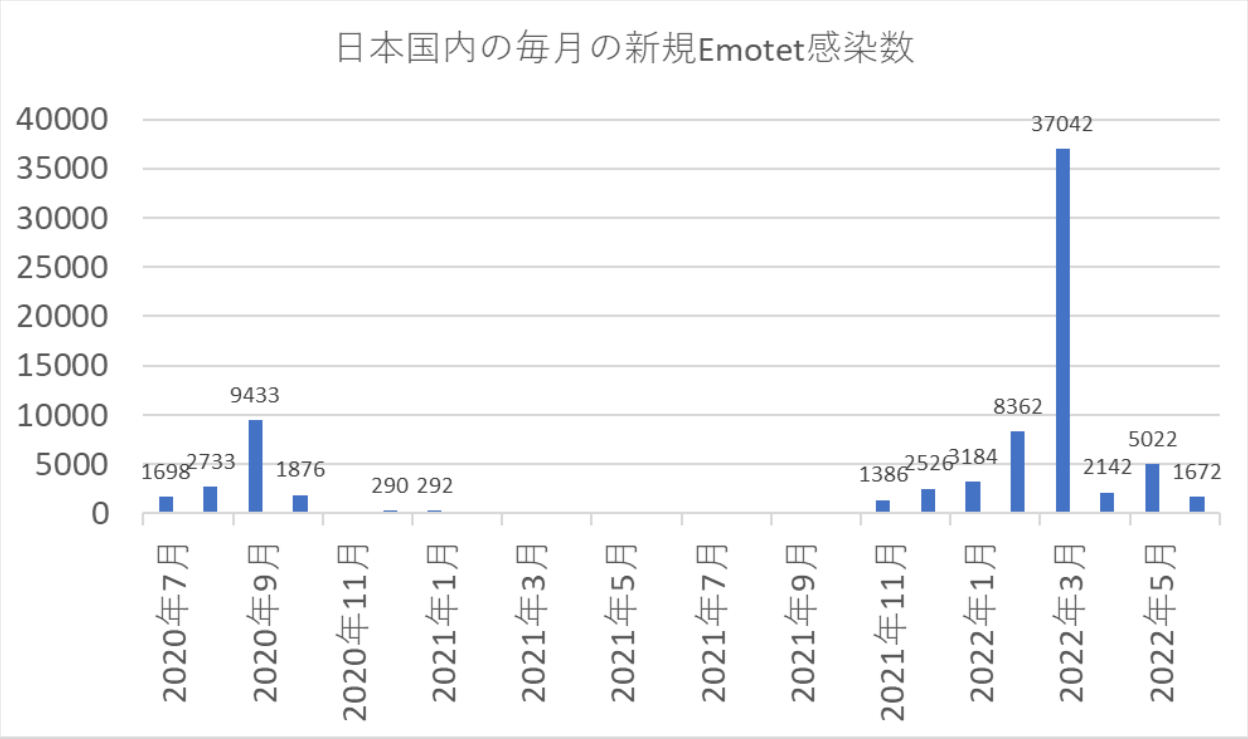
- 侵入型ランサムウェア攻撃について、「被害を受けたら」「被害への対応」「関連情報」に分けてインシデント対応を進める上での参考情報をFAQ形式でまとめている。

https://www.jpcert.or.jp/magazine/security/ransom-faq.html

マルウェアEmotetの感染再拡大

マルウェアEmotetの感染再拡大

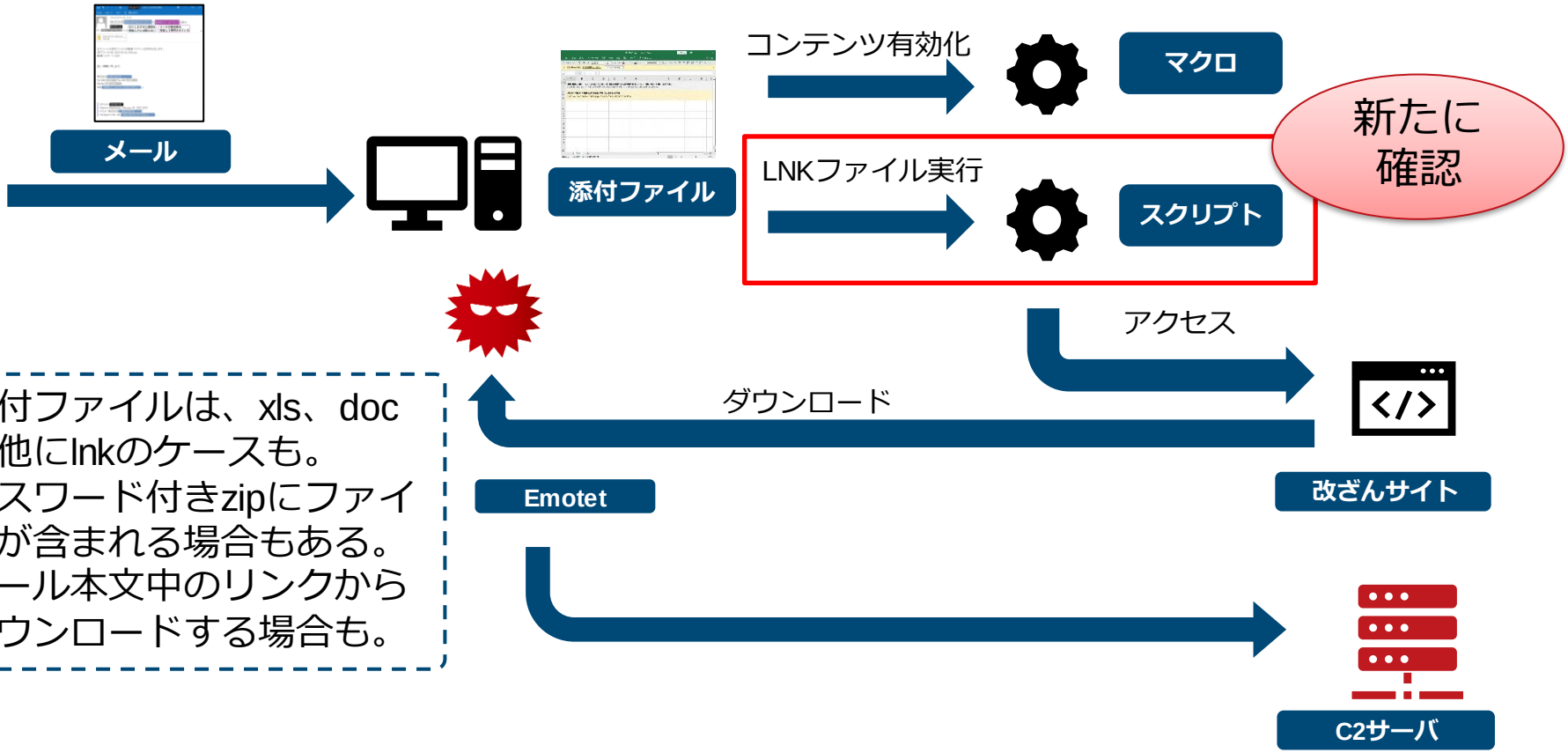
- 2021年1月のテイクダウン作戦以降落ち着いていた、Emotetの感染活動について、2021年11月頃よりEmotetの感染が急速に拡大していることを確認
- 2022年6月に入っても感染を確認している



JPCERT/CCから見る脅威動向

マルウェアEmotetの感染に至るメール配布

— 手法を変えてばらまき活動を継続



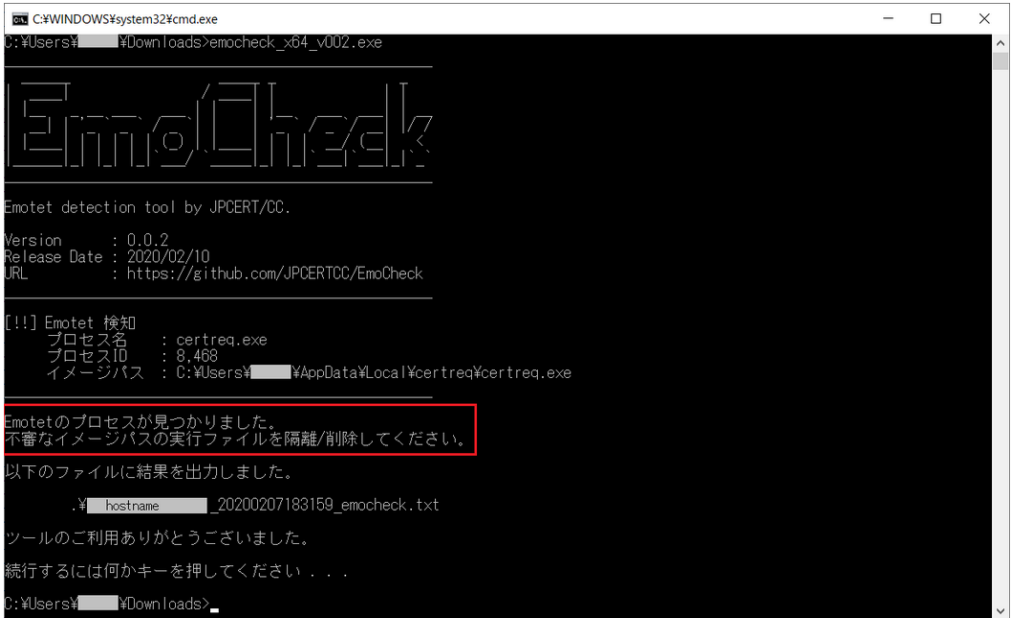
添付ファイルは、xls、docの他にlnkのケースも。
パスワード付きzipにファイルが含まれる場合もある。
メール本文中のリンクからダウンロードする場合も。

クレジットカード情報の窃取

- Webブラウザ「Google Chrome」に保存されたクレジットカード番号や名義人氏名、カード有効期限を盗み、外部に送信する機能が追加された
- Google Chromeでは個人情報を暗号化して安全に保存しているが、Emotetの新機能は暗号データを元に戻すための鍵も同時に盗み出すため、Emotetに感染すると、使用しているクレジットカード情報が第三者に知られるおそれがある

Emocheck

- 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）でログインし、ツールをダブルクリックし実行、Emotetに感染しているか、確認を行うツール
- 検知できない検体が確認されるたびアップデートを行っている。（現在の最新verはv2.3.2）



https://github.com/JPCERTCC/EmoCheck

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：ew-info@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