第12回情報セキュリティマネージャー ISACAカンファレンス in Tokyo
「リスクの変化とセキュリティマネジメント」

今知っておくべきサイバーセキュリティの脅威実態 ～ランサムウェアとランサムウェア以外の話～

株式会社マクニカ
セキュリティ研究センター
センター長補佐
瀬治山 豊

Co.Tomorrowing

MACNICA

自己紹介

瀬治山 豊 Yutaka Sejiyama

✓ **セキュリティ脅威動向の情報収集と発信**
- 脆弱性、ランサム関連の脅威動向リサーチ
- X/Twitter @nekono_naha
- ばらまきメール回収の会
- (ISC)2 Japan Chapter Annual Conference 2022
- JSAC 2023 （Best Speaker賞受賞）
- JSAC 2024

✓ マクニカグループ グローバルCSIRT担当者
- 23カ国/地域、81拠点
- 国内外でのセキュリティインシデント対応
- パッチマネジメント

✓ マクニカ独自のセキュリティサービス企画・運営
- 外部公開サーバ調査 等
- SOC（セキュリティ監視代行）

セキュリティ研究センター

セキュリティ研究センター
powered by macnica

日本を狙った標的型攻撃をリサーチし得られた知見を様々な社会活動に還元（リサーチ、教育、カンファレンス）

センター長
政本 憲蔵

センター長補佐
瀬治山 豊

主幹
凌 翔太

主幹
柳下 元

主席
竹内 寛

主席
勅使河原 猛

主席
山﨑 剛弥

実績（一部）

国際カンファレンス

- Black Hat USA Arsenal 2013 – 2016、2023
- HITCON CMT 2023
- Mandiant Cyber Defense Summit 2021
- VB2020 localhost
- CONFidence 2020
- HITCON Pacific 2018
- BSides Austin 2018
- Black Hat Asia Arsenal 2017
- DEF CON 25 Demo Labs 2017

国内カンファレンス

- JSAC 2018、2021、2022、2023、2024
- BSides Tokyo 2023
- (ISC)² Japan Chapter Annual Conference 2022
- 笹川平和財団サイバーセキュリティセミナー 2019, 2021
- 情報セキュリティワークショップin越後湯沢 2021
- 白浜シンポジウム 第18回

書籍監訳

- インシデントレスポンス 第3版

その他の社会活動

- セキュリティキャンプ全国大会　講師
- 官公庁　セキュリティアドバイザー
- 日本経済団体連合会 21世紀政策研究所　研究委員
- 令和3年度多国間サイバー防護競技会
- セキュリティコミュニティ 濱せっく 運営

脅威リサーチ

- セキュリティ研究センターブログ
  https://security.macnica.co.jp/

標的型攻撃の実態と対策アプローチ　検索

日本を狙うエスピオナージ　検索

ビジネスメール詐欺の実態と対策アプローチ　検索

本日のトピック

1　日系企業のランサム被害傾向と関連情報

2　脆弱性対処のトレンド

3　要警戒 情報窃取特化型マルウェア Info Stealer

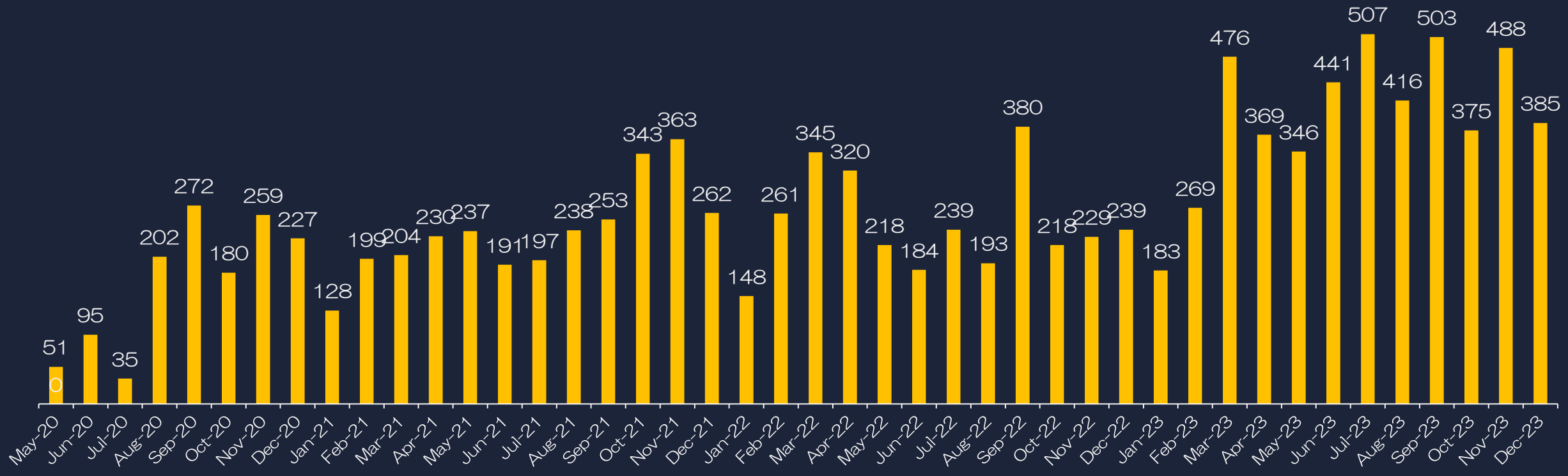
4　日本企業を狙う標的型攻撃の印象的な事件

5　（予備）多要素認証を無力化する攻撃

日系企業のランサム被害傾向と関連情報

ランサムアクターによるグローバルでのリーク件数

- ✓個別の企業や業種をターゲットにした標的型ランサム、データ暗号化と情報漏えいによる二重の脅迫を行う暴露型ランサムの被害が世界的に増加
- ✓ 2023年12月末時点で**11899件**が暴露型ランサムの被害（リークサイトに掲載）にあっている
- ✓リークされていないランサムウェアの被害数も含めると被害企業は上記の数倍以上～にのぼる可能性がある

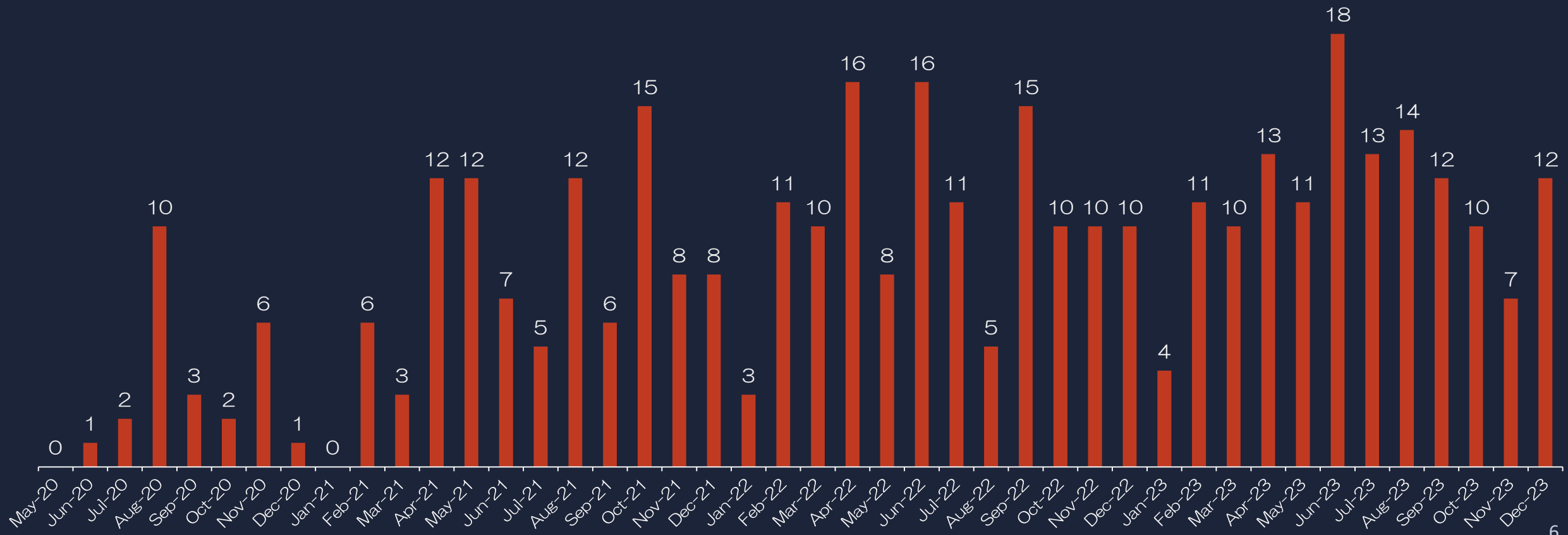


※2023年2月～12月のデータはMBSD社MBSD Cyber Intelligence Group (CIG)データを引用
https://www.mbsd.jp/research/20240118/cig-monthly/

日系企業・組織のランサム系インシデント

✓公開情報から確認できる範囲でも**380件のランサムインシデント**が発生

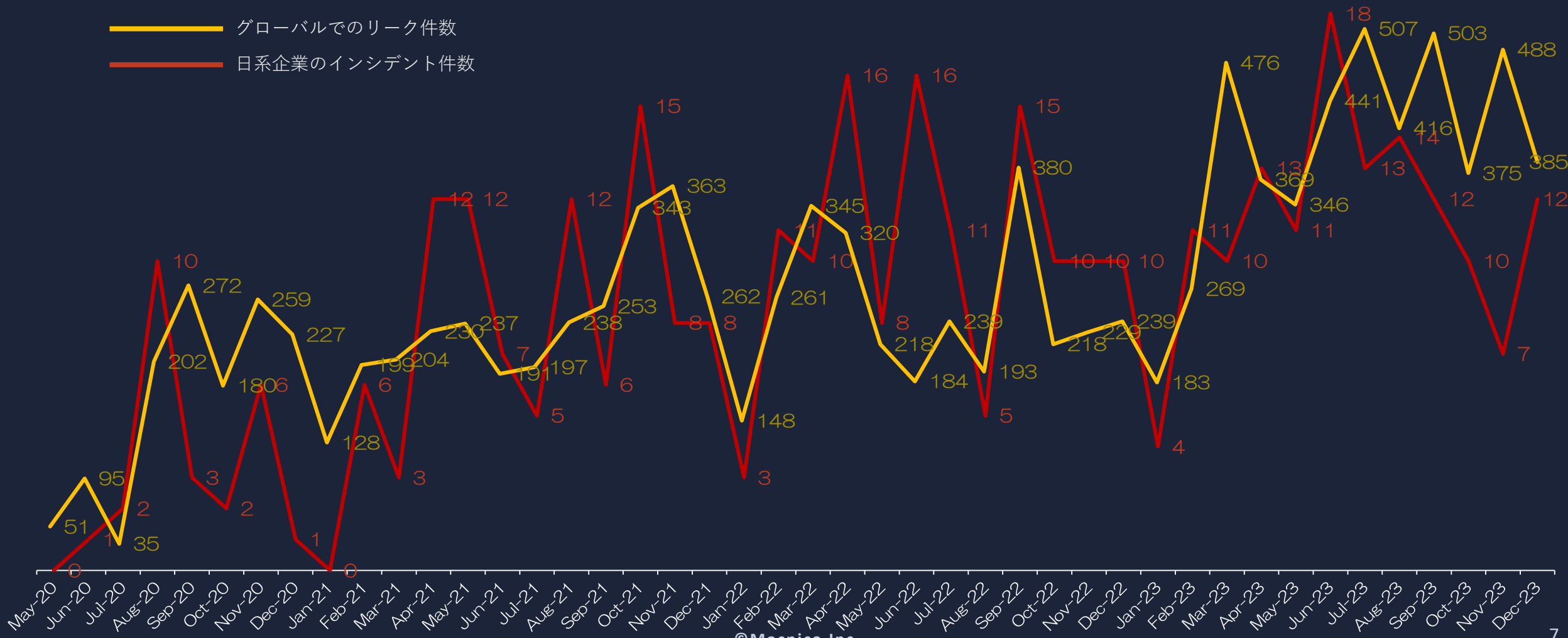
・各企業や組織のプレスリリースやランサムウェア攻撃者のダークウェブ上の犯行声明を集計
※Webサイトの改ざんやWebサイト経由での情報漏えい、Emotetの感染事案は除く
・2020年5月～2023年12月の45ヶ月間の集計
・情報公開されていないランサムウェアの被害数も含めると被害企業は上記の数倍以上～にのぼる可能性がある



インシデント発生傾向の比較

- 日本だけの被害数が増加しているわけではなく世界的なランサム系活動の増減に連動して日本”も”増減

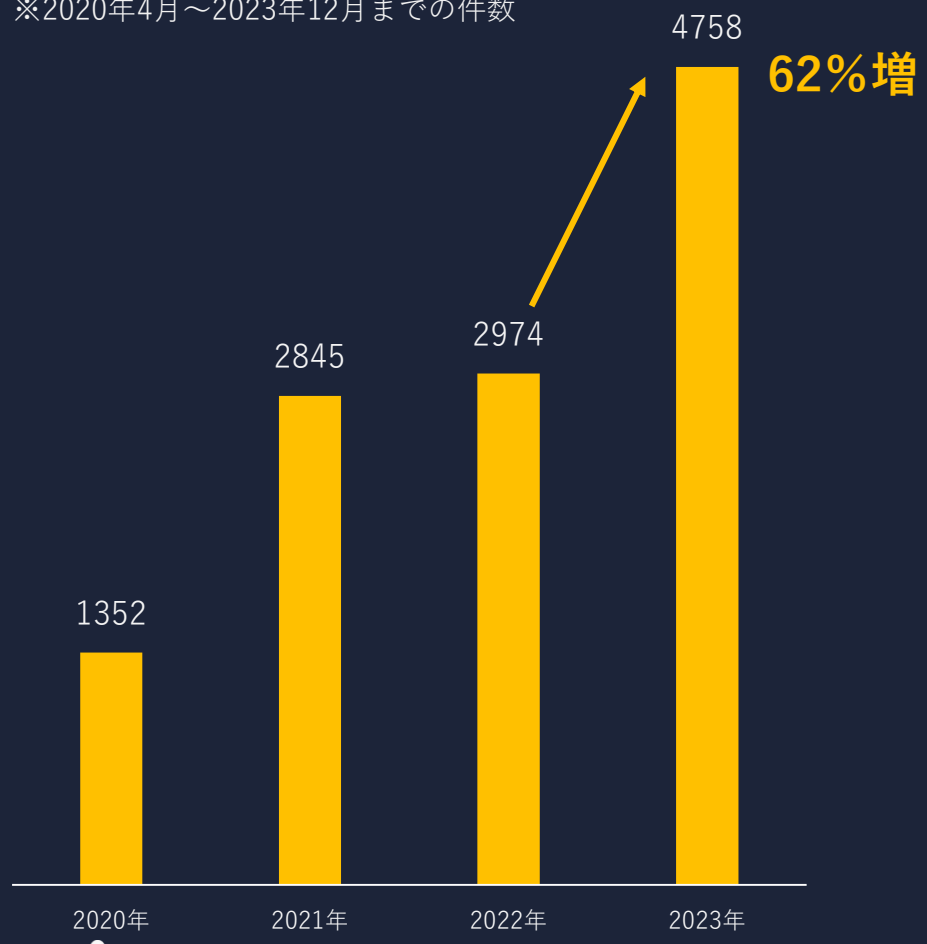
✓ グローバルと日系組織インシデントの件数比較



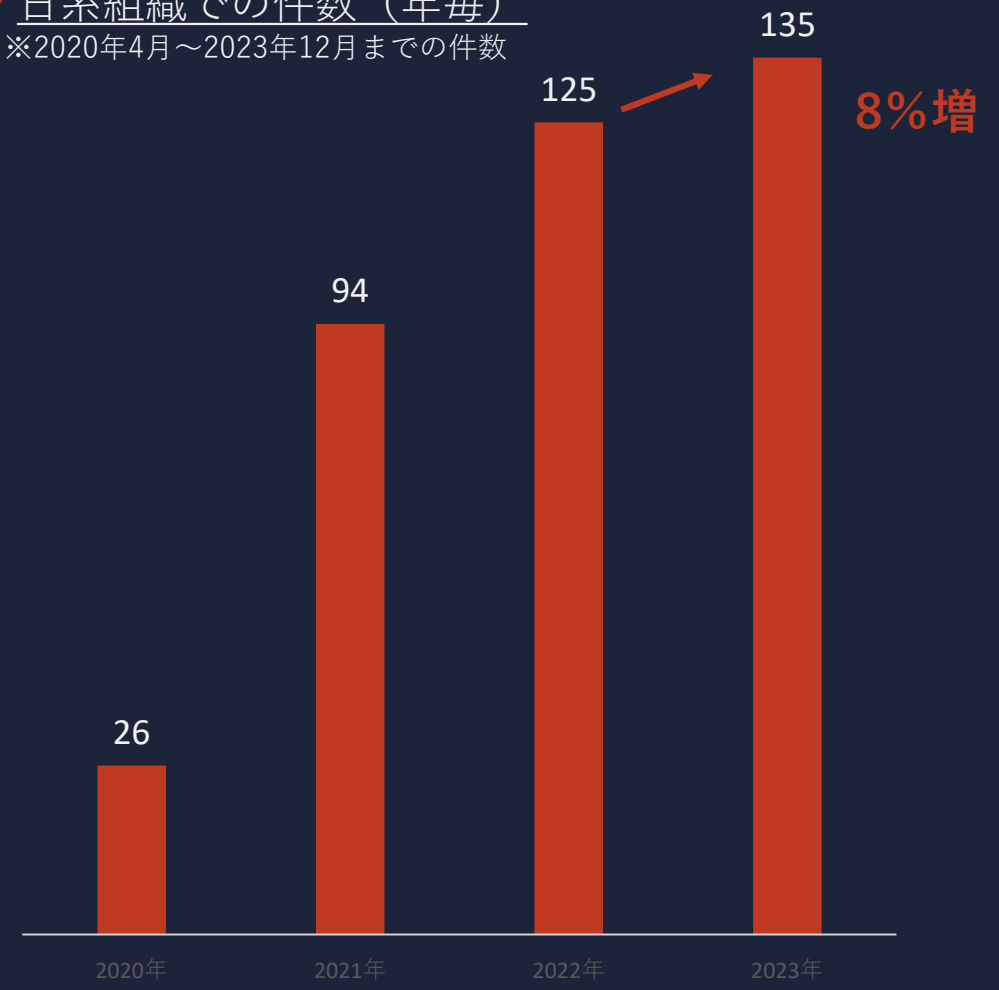
インシデント発生傾向分析

- 国内外ともに被害件数は年々増加しており歯止めが効いていない状況
- グローバルではある手法（P23参照）の影響で被害が特に増加

✓ グローバルでの件数（年毎）
※2020年4月～2023年12月までの件数



✓ 日系組織での件数（年毎）
※2020年4月～2023年12月までの件数



日系組織のプレスリリース分析

- 以降のスライドでは日系組織の被害380件の内、被害公表があった281件やリーク事案157件の情報を分析し被害傾向を確認
- ただし、企業によっては情報非公開範囲が広いケースもあるため以降の数値は下限の情報となる点に注意

情報公開日

攻撃発生日時

被害拠点

侵害原因

業務影響

2023年4月13日
株式会社　〇〇〇〇
代表取締役　〇〇〇〇

ランサムウェアによるサイバー攻撃の発生について（第2報）

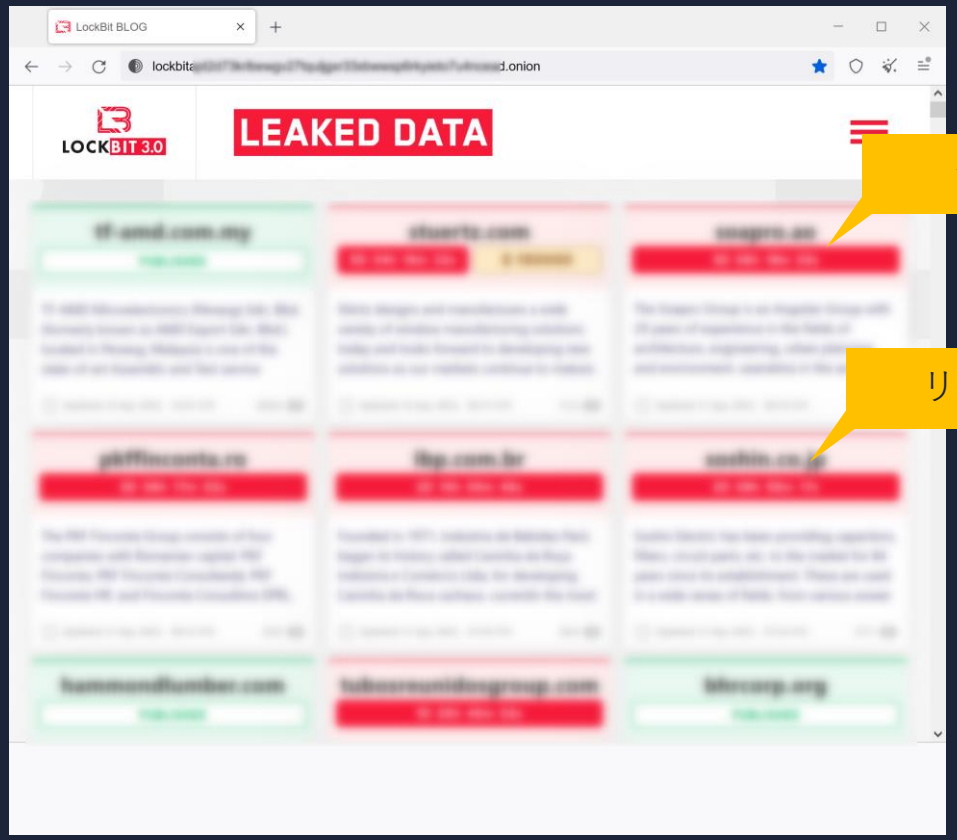
2023年4月7日付「ランサムウェアによるサイバー攻撃の発生について」にて公表した通り、当社は、2023年4月1日未明にランサムウェアによるサイバー攻撃を受けました。調査および弊社業務復旧状況についてお知らせいたします。

攻撃は、当社の海外拠点（タイ）が標的にされ、VPN機器の脆弱性をつかれたものと判明しました。その結果、基幹システムまで攻撃が及び、業務に影響が出ています。現在も復旧作業を進めておりますが、完全な復旧には至っておりません。

このような事態を招き、お客様や関係者の皆様にご迷惑をおかけし、誠に申し訳ございません。当社では、復旧作業に全力を尽くすとともに、関係機関と協力し、再発防止策を講じてまいります。

以上のとおり、当社では、事態を真摯に受け止め、誠実な対応に取り組んでまいります。今後も、お客様や関係者の皆様に信頼される企業を目指し、より一層の努力を続けてまいります。

お問い合わせ先
株式会社　〇〇〇〇
担当者　〇〇〇

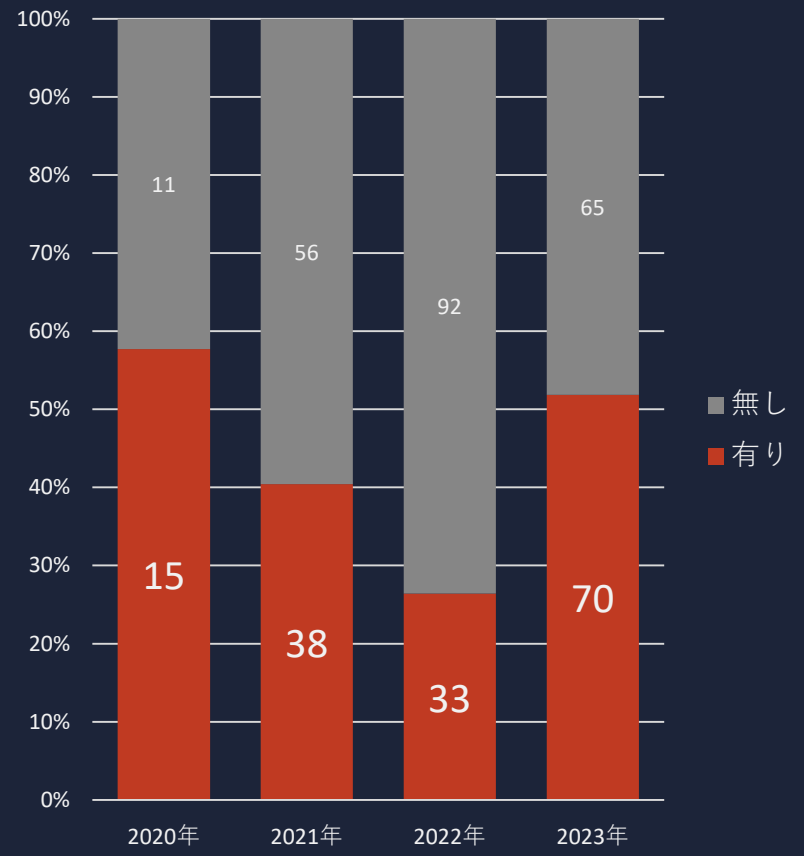


企業名

リーク日

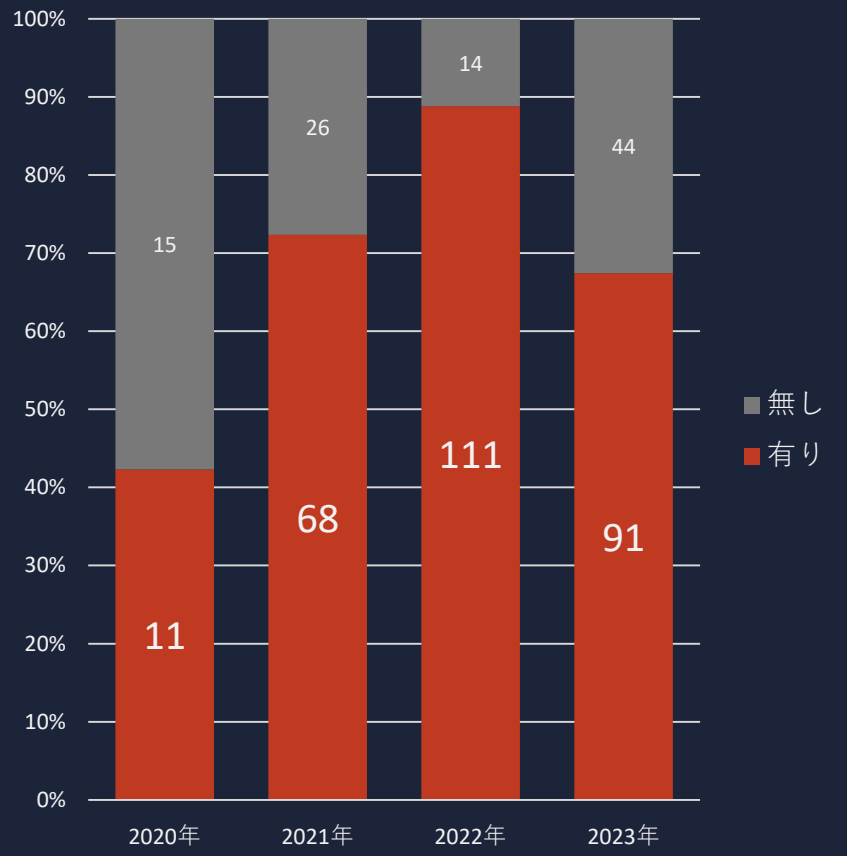
日系組織のインシデント発生傾向

✓攻撃者による日系組織のリーク件数



- ランサム系インシデントが攻撃者のリーク行為により発覚する割合は年々減っていたが2023年に再度上昇。身代金支払い圧力の強化も関係か。

✓日系組織のプレスリリースでの公表件数

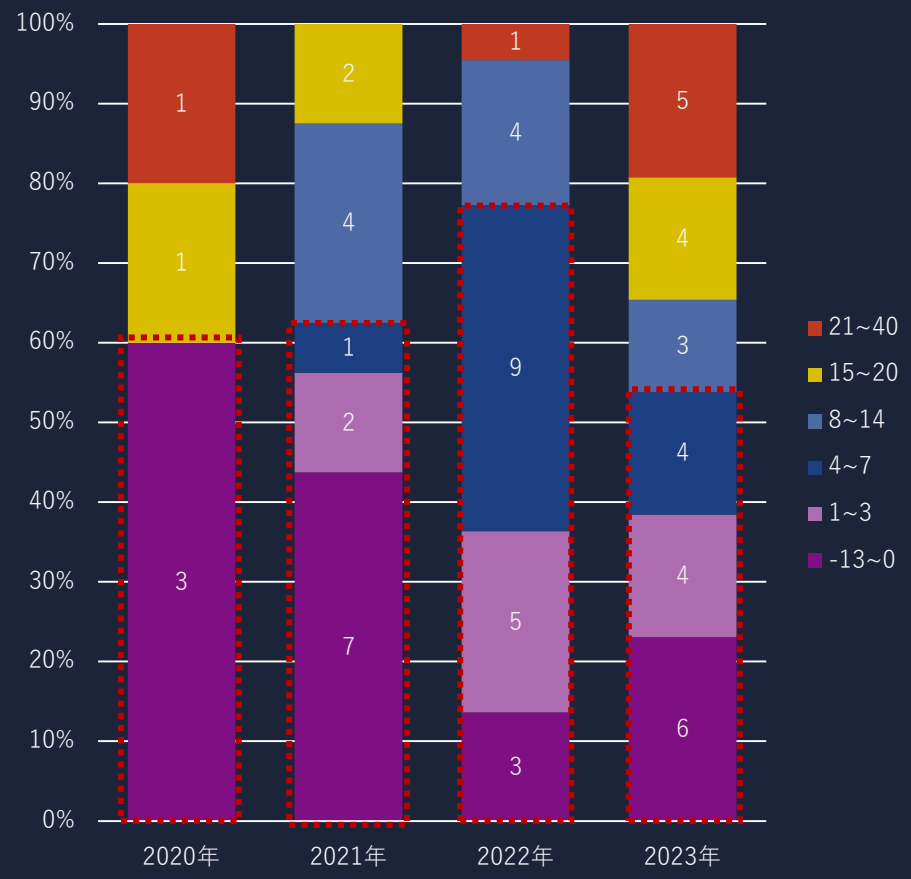


- 公表割合増加についてはランサム系インシデントの世間的な認識の変化や個人情報保護法改正も影響か
- 2023年は海外拠点被害（攻撃者からのリーク）でプレスが公表されないケースが増加

日系組織のプレスリリース分析

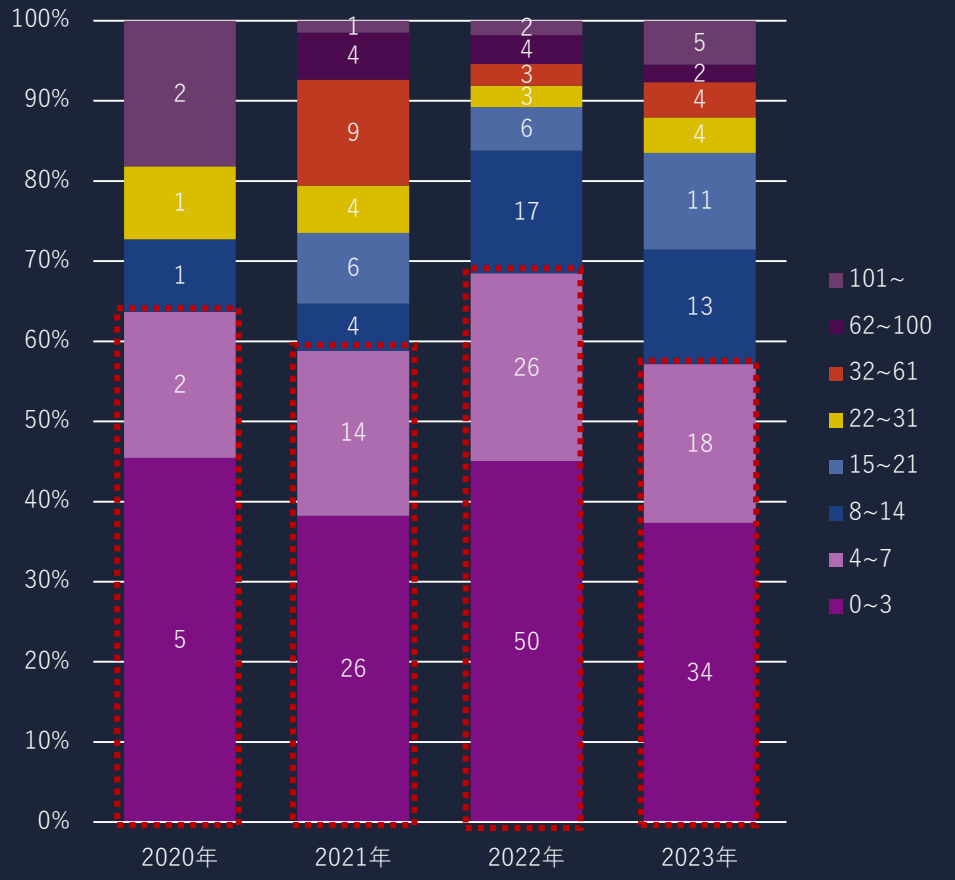
✓攻撃認知からリーク発生までの日数

※攻撃者にリークされ企業からのプレス公開（正確な攻撃発生日情報）がある69件を対象に集計



- 約6割のケースでは企業が攻撃を認知してから7日以内にリークサイトへの掲載が発生

✓攻撃認知からプレス公開までの日数

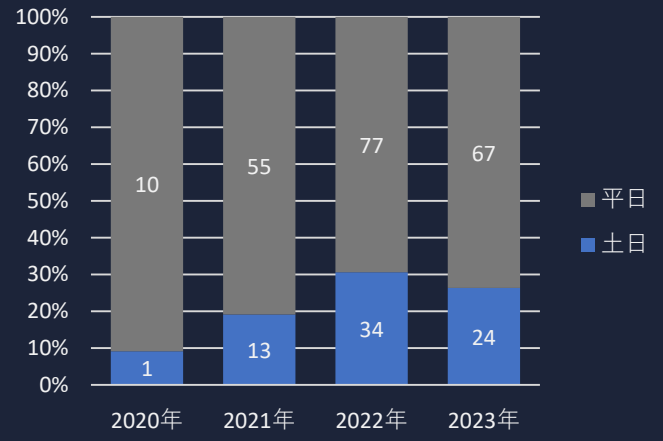


- 約6割のケースでは企業が攻撃を認知してから7日以内にプレスリリースでの情報公開が行われている

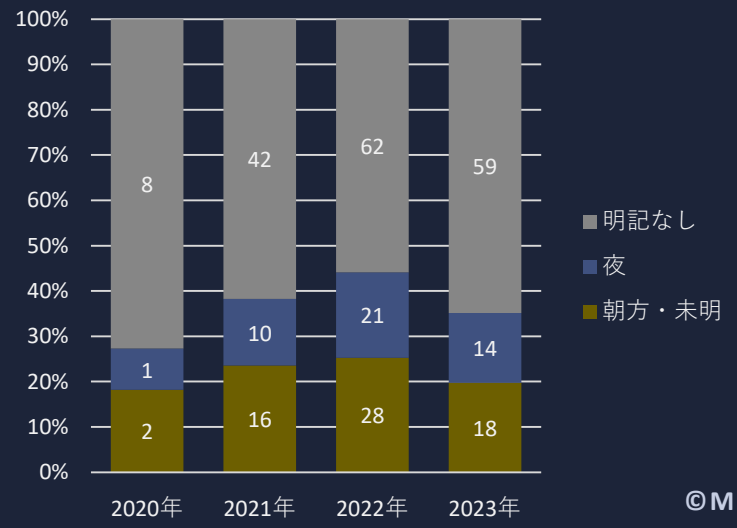
日系組織の攻撃発生タイミング分析

- 休日や祝日、夜間や早朝等の**人がいない時間帯を狙って攻撃**されるケースは年々増加傾向
- 認知や対処を遅らせ被害範囲（暗号化対象ホストやファイル数）拡大を狙った攻撃者側の戦術の変化と考えられる
- 2023年は海外拠点の被害が多く詳細が記載されないケースが増加しやや減少

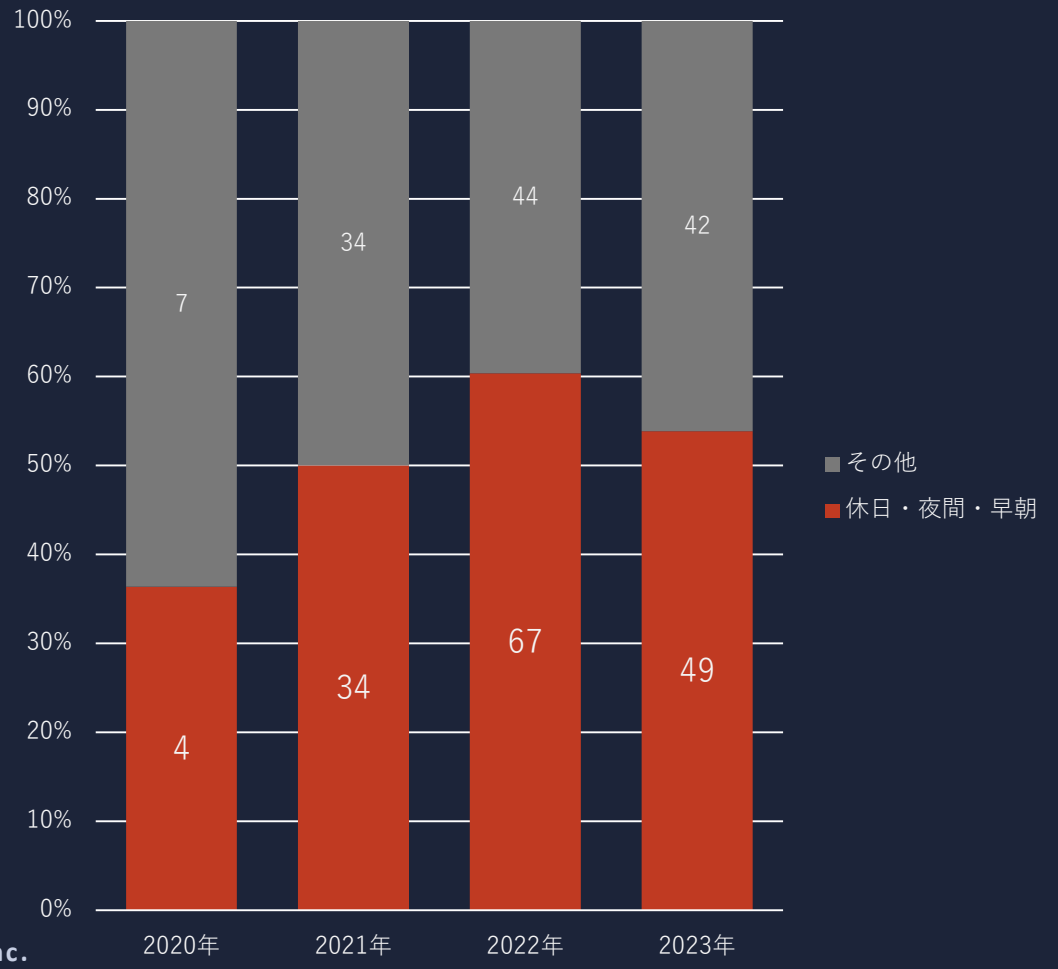
✓攻撃発生日



✓攻撃時間



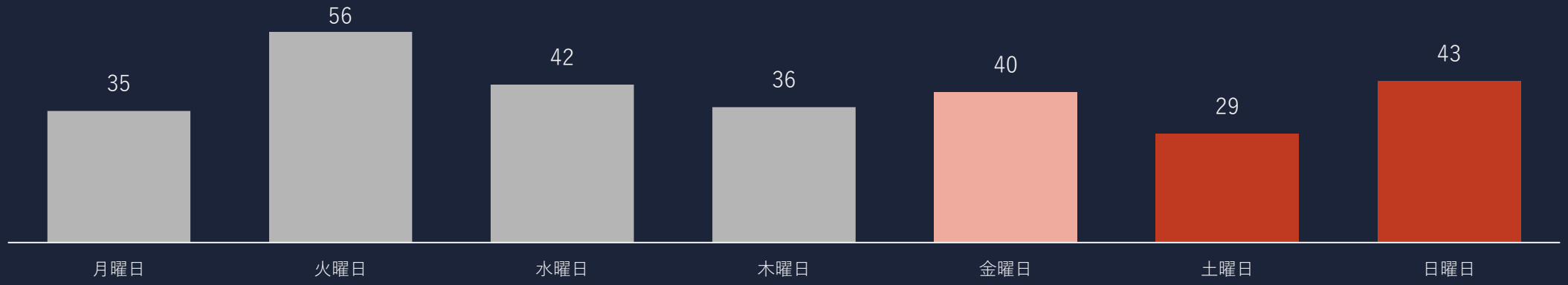
✓夜間・早朝・休日等の攻撃



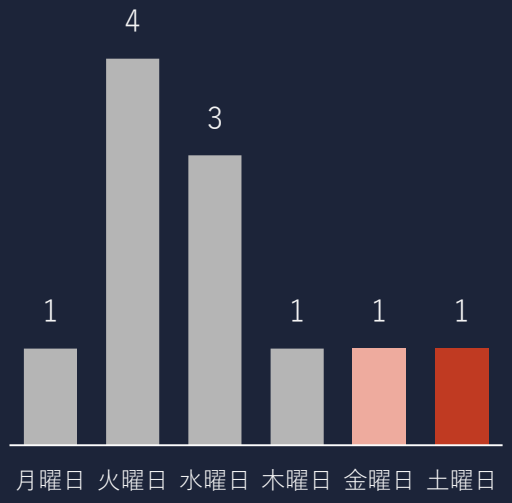
日系組織の攻撃発生タイミング分析

- 平日ではなく**土日や金曜を狙って攻撃**をしかける傾向は年々強まっている
- 暗号化対象ホストやファイル数などの**被害範囲拡大を狙った**攻撃者側の戦術の変化と考えられる

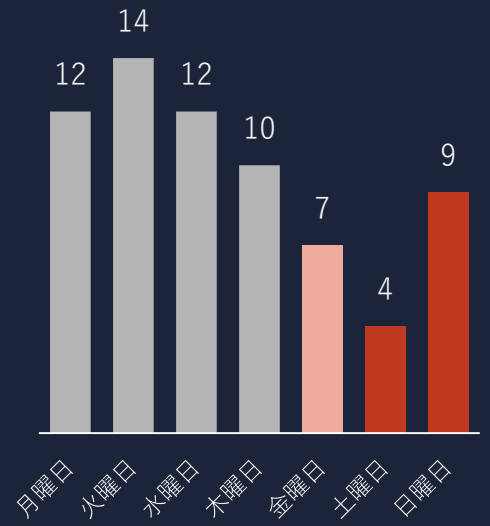
✓攻撃が発生または認知した曜日（20～23年）



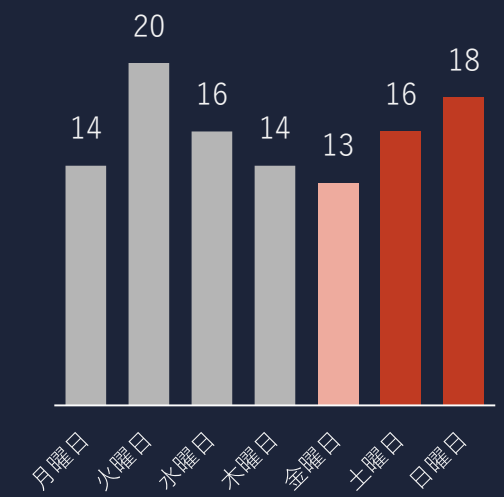
✓2020年



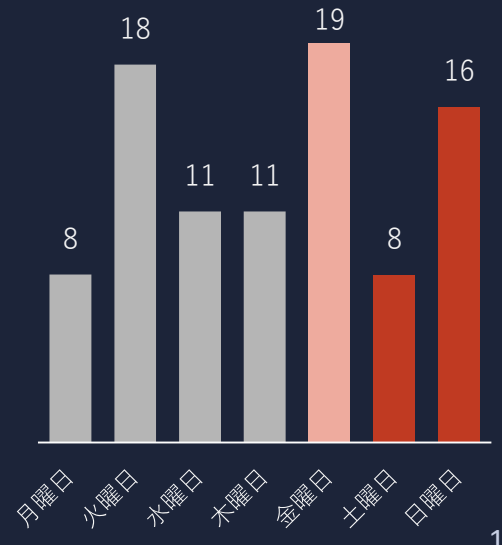
✓2021年



✓2022年



✓2023年



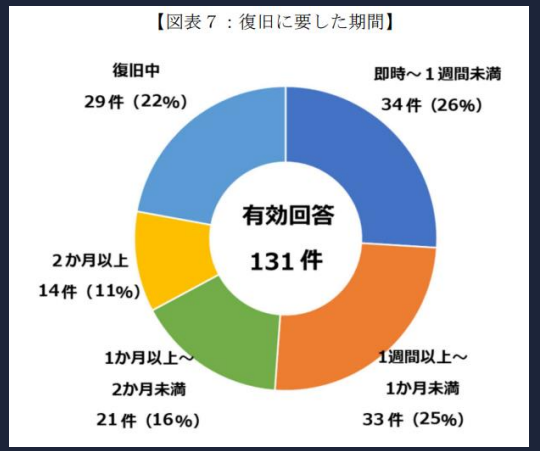
深刻化する事業継続への影響

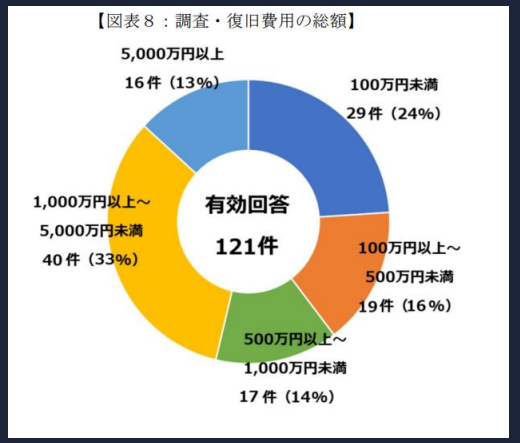
被害に関する公表事例

業種	時期	事業への影響
サービス	2023年3月	**ネットワーク広域に攻撃の被害**が及んでいることもあり、全ての特定・調査完了と日常業務への完全な復旧までにはしばらくの時間がかかる見込み
製造	2023年3月	基幹システムが使用できない状況。**紙ベースにて復旧作業**を進めているが、**すべて復旧するには1カ月から2カ月程度要する**見込み
製造	2023年2月	被害の拡大を防ぐため、速やかにサーバーの停止やネットワークの遮断などの対応を行いましたが、**基幹システムや関連システムにも被害**が及んでいる
サービス	2022年9月	**基幹システムや関連システムにも被害**が及んでおり、一部の業務に影響が出ている
サービス	2022年7月	**基幹システムや関連システムにも被害**が及んでおり、自社のオンラインサイトでの販売や取引先への配送にも影響。今回の不正アクセスは、サーバー内の情報を暗号化し、アクセスログの抹消を伴うものであったため、調査や被害状況の確認にも時間を要している
サービス	2022年7月	弊社では、不正アクセスの内容と範囲の特定を進めておりますが、システム障害の発生により、**各種業務への影響が継続**している
製造	2022年7月	**攻撃の被害が広範**に及んでいることもあり、全ての特定・調査完了と日常業務へ復旧するまでには今しばらくの時間がかかる見込み
小売	2022年7月	サイバー攻撃により**販売管理システムを含めて機能が停止**。伝票起票などが不可となり事務処理や取引が遅延
メディア	2022年6月	制作システムを含めてサーバがランサムウェアの攻撃を受ける。製作作業に影響が出たため**他社の協力を得て事業を継続**
金融	2022年6月	ランサムウェアによりシステムが暗号化され、データの読み取りができない状態。**お問い合わせへのご回答や書類の発送等に支障**
製造	2022年5月	業務復旧にしばらく時間を要する見込み。**約1ヶ月後にシステムが復旧したものの一部の業務は継続して提供が不可**
化学	2022年5月	社内システムがランサムウェアによる攻撃を受ける。翌日には生産・受注・出荷は再開できたものの**基幹システム復旧には時間を要する**見込みで関連会社2社も同様の状況
小売	2022年5月	不正アクセスによりシステム障害が発生。2日程度**キャッシュレス決済**が停止。商品の取り寄せサービスや店舗間配送にも影響が発生
小売	2022年4月	サーバが不正アクセスを受け、受注出荷システム含めて停止。**復旧目処が立たずほぼ全ての日常業務に影響**が発生し子会社も同様の状況
製造	2022年4月	ランサムウェアによる不正アクセスで約10日後にメールが復旧したものの、全社内システムは障害継続。**完全復旧には約2ヶ月**
製造	2022年4月	所有するパソコンのメールの送受信、サーバー等へのアクセスが始業より不可で**全ての復旧には数週間**程度かかる見込み

- 軽微な被害ですんだケースもあるが、多くの場合は復旧に1週間以上、深刻なケースでは数ヶ月を要したケースもある
- 期間は少なくとも代替システムの確保やサーバ入れ替え、対外対応等の様々な対応が必要となる

✓警察庁まとめによるランサムウェア被害詳細





警察庁公表「令和４年におけるサイバー空間をめぐる脅威の情勢等について」より
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf

近年のランサムウェアにより大きな事業影響が出る理由

✓数年前のランサムウェア
- ランサムウェアを実行した**PC1台が被害**にあう
  - 周辺PCが暗号化されることもあり（自動拡散）
- PCが暗号化されてもバックアップで**復旧可能**

✓最近のランサムウェア
- **攻撃者が手動操作**で組織NW内を渡り歩き奥深くに侵入される
  - AVやEDRが未導入の箇所を経由するか**無効化**される
- 二重脅迫のために暗号化前に情報を持ち出す
  - バックアップサーバも事前に攻撃し**復旧不可能**にする
- Active Directory等を経由し全PCやサーバを一気に暗号化
  - 被害拡大のため夜間、休日、早朝に攻撃
  - 侵入から最終攻撃の実行までは約1週間

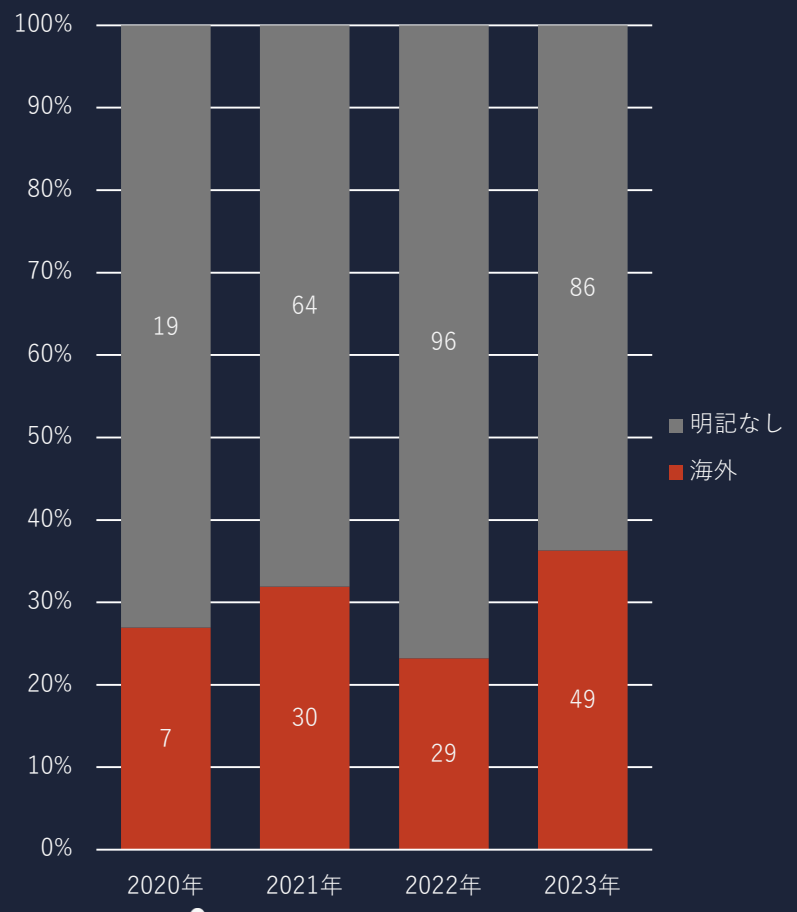
  ※ただし2023年に入り攻撃の被害レベルが2極化しつつある

  ※暗号化をせず情報だけ窃取するケースも流行

日系企業の海外拠点の被害

- 公開情報から確認できる範囲でも日本企業の被害の多くは**海外拠点で発生**している事が多い
- 被害総数**380件中 115件 (30%)**が海外拠点または海外拠点きっかけのインシデントとなっている
- 実態としてもこの**数字以上に日本企業のインシデントは海外で発生**している

✓被害拠点の明記

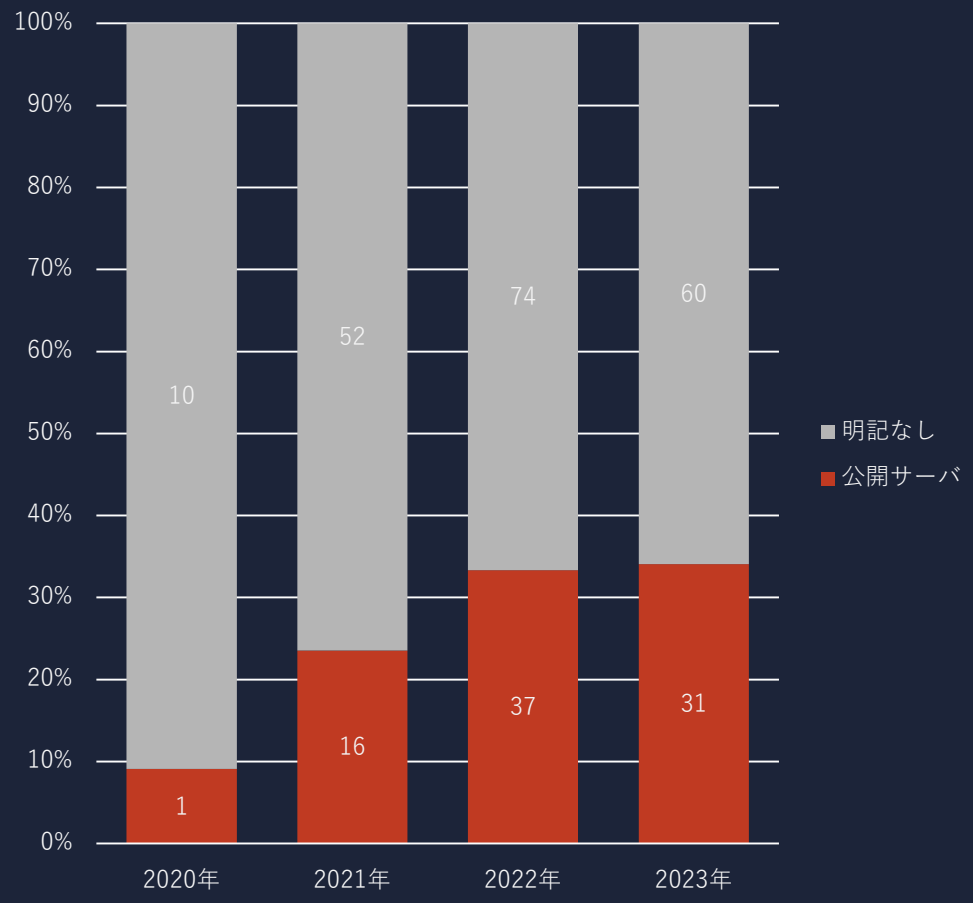


✓被害が発生した拠点の分布

日系企業のインシデント発生原因

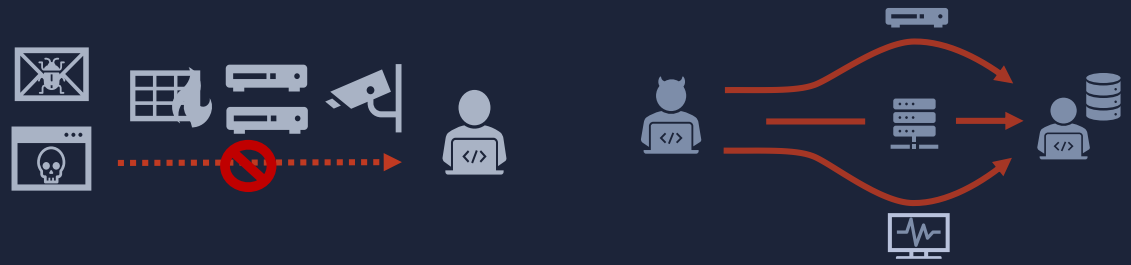
- 侵入経路として外部に**公開されたサーバの脆弱性や設定不備**が悪用されるケースが多くなっている
- 侵入経路まで明記されるケースは稀だが、それでも2022～23年は30%超の事例で公開サーバが侵入経路

✓侵入経路の記述



✓なぜ公開サーバが悪用されるのか

- 従来のWebやメール経由の侵入が困難になる一方で
  公開サーバの企業側の守りや対策が未だに薄い



- 攻撃者にとって悪用しやすいクリティカルな脆弱性が
  高頻度で発見されてしまう
  ※研究者、攻撃者がそれぞれ脆弱性を探している

外部公開サーバ経由で発生するインシデントのグローバル統計

- 様々なセキュリティ関連組織発行の公開IRレポートからその組織が対応したインシデントの発生原因のデータを抽出
- 外部サーバが起点となっているインシデントの割合（黄色字）は少なくなく**平均で63%**

発行機関	発行時期	レポート名	外部公開サーバや脆弱性が原因になった割合		その他	URL
Trend Micro	2023年12月	4年半にわたる国内組織のインシデントレスポンスから見えてきた「ランサムウェア攻撃のリアル」とは？	67%	VPN/RDP/脆弱性 ※2021年1月～2023年6月	その他 33.3%	https://www.trendmicro.com/ja_jp/jp-security/23/l/securitytrend-20231211-03.html
警察庁	2023年9月	令和５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	81%	VPN機器 35件（71%） リモートデスクトップ 5件（10%）	不審メールやその添付ファイル 2件（4%） その他 7件（14%）	https://www.npa.go.jp/publications/statistics/cybersecurity/data/R05_kami_cyber_jousei.pdf
警察庁	2023年3月	令和４年におけるサイバー空間をめぐる脅威の情勢等について	81%	VPN機器 63件（62%） リモートデスクトップ 19件（19%）	不審メールやその添付ファイル 9件（9%） その他 11件（11%）	https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf
SecureWorks	2022年12月	【年次レビュー】 2023年サイバー脅威の実態	32%	脆弱性スキャン・悪用 – 32%	・窃取した認証情報の利用 – 32% ・フィッシングメール経由で配布したマルウェアの利用 – 14%	https://www.secureworks.jp/resources/rp-state-of-the-threat-2023
SecureWorks	2022年10月	2022 State of the Threat:A Year in Review	52%	Exploitation of remote services　52%	Credentials　39%、commodity malware infection　3% Drive by download　2%、Phishing　2%、Network misconfiguration　2%	https://www.secureworks.com/resources/rp-state-of-the-threat-2022
Trend Micro	2022年10月	直接侵入に繋がるネットワーク機器の侵害： 新たな脆弱性「CVE-2022-40684」に注意	50%	ネットワーク機器経由　25% RDP経由　25%	メール経由 4%、その他 13%、不明 33%	https://www.trendmicro.com/ja_jp/research/22/j/fortinet.html
警察庁	2022年9月	令和４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	83%	VPN機器 32件（68%） リモートデスクトップ 7件（15%）	不審メールやその添付ファイル 4件（9%） その他 4件（9%）	https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_kami_cyber_jousei.pdf
COVEWARE	2022年7月	Fewer Ransomware Victims Pay, as Median Ransom Falls in Q2 2022	50%	RDP Compromise 約～30% Software Vulnerability 約20%＋	Email Phishing 約30%～ Other 約20%＋	https://www.coveware.com/blog/2022/7/27/fewer-ransomware-victims-pay-as-medium-ransom-falls-in-q2-2022
Palo Alto	2022年7月	Attackers Move Quickly to Exploit High-Profile Zero Days: Insights From the 2022 Unit 42 Incident Response Report	46%	ソフトウェアの脆弱性 31% 総当たりによるクレデンシャル攻撃　9% 以前に流出したクレデンシャル 6%	フィッシング　37%、内部脅威　5%、ソーシャルエンジニアリング　5%、信頼関係の悪用・信頼されたツールの悪用　4%、そのほか　3%	https://unit42.paloaltonetworks.jp/incident-response-report/
SOPHOS	2022年6月	The Active Adversary Playbook 2022	55%	Exploited Vulnerability 47% Compromised Credentials 5% Brute Force Attack 3%	Unknown 36%、Phishing 8%、Download 1%	https://news.sophos.com/en-us/2022/06/07/active-adversary-playbook-2022/
Arctic Wolf	2022年6月	Q1 2022 Incident Response Insights from Tetra Defense	82%	External Vulnerabilities 57% RDP 25%	–	https://arcticwolf.com/resources/blog/q1-2022-incident-response-insights-from-tetra-defense
Group-IB	2022年5月	Ransomware Uncovered 2021/2022	68%	External remote services 47% Exploit public-facing application 21%	Phishing 26%、Other 6%	https://www.group-ib.com/media-center/press-releases/ransomware-2022/
警察庁	2022年4月	令和３年におけるサイバー空間をめぐる脅威の情勢等について	74%	VPN機器 41件（54%） リモートデスクトップ 15件（20%）	不審メールやその添付ファイル 5件（4%） その他 15件（20%）	https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf
IBM	2022年1月	X-Force Threat Intelligence Index 2022	53%	Vulnerability exploitation 47% Stolen credentials 3% Brute force 3%	Phishing 40%、Removable media 7%	https://www.ibm.com/reports/threat-intelligence/
Kaspersky	2021年9月	Incident response analyst repot	63%	総当たり攻撃 31.6% 脆弱性の悪用 31.5%	悪意のあるメール　23.7%、ドライブバイダウンロード　7.89%、リムーバブルメディア 2.63%、内部関係者 2.63%	https://media.kaspersky.com/jp/pdf/pr/Kaspersky_IRAnalystReport2020-PR-1056.pdf
COVEWARE	2021年4月	Ransomware Attack Vectors Shift as New Software Vulnerability Exploits Abound	70%	RDP Compromise 約～50% Software Vulnerability 約20～%	Email Phishing 約～30% Other 約～5%	https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound

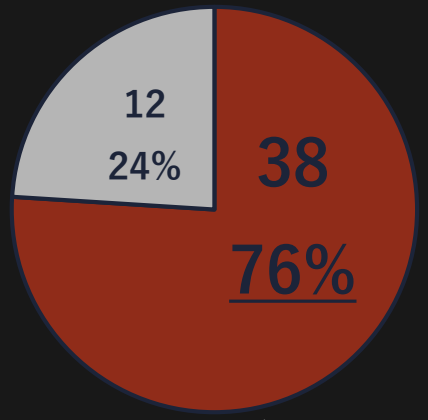
日系企業の外部公開サーバの状況

- 一般的な大企業では1グループあたり**数百～2、3千台（平均1400台）**の外部公開サーバを運用している
- その内、平均で約67%程度のサーバを本社情シスが把握できていない

旧東証一部上場企業 50社のサンプル調査

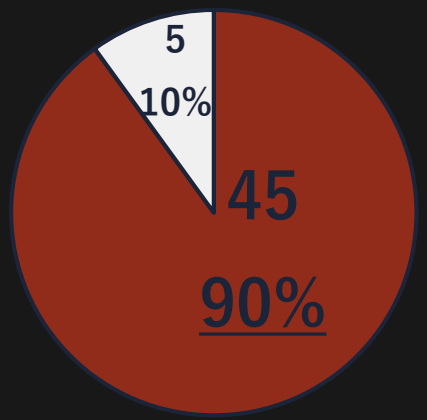
- 本社企業が問題を有するケースは約40%も、海外や子会社まで含めると**90%もの企業で問題点**を検出
- 膨大な数のサーバを常時セキュアにすることは難易度が極めて高い

サポート切れOS
（Windowsサーバ、CentOS）が稼働



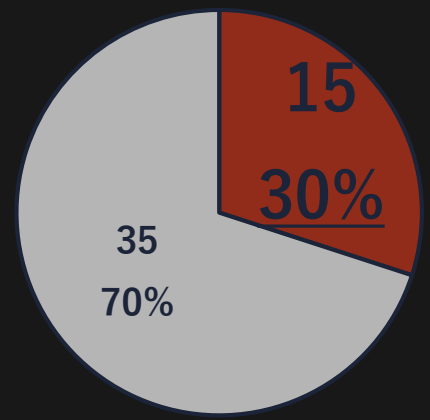
・古いものだとWindows 2000（2010年EOL）や Server 2003 （2015年EOL）

サポート切れソフトウェアが稼働



・ApacheやPHP、OpenSSL、OpenSSH、MariaDB、Serv-U等
※バックポート修正版の可能性が高いものは除いて調査を実施

リモートデスクトップが
公開されたサーバを利用

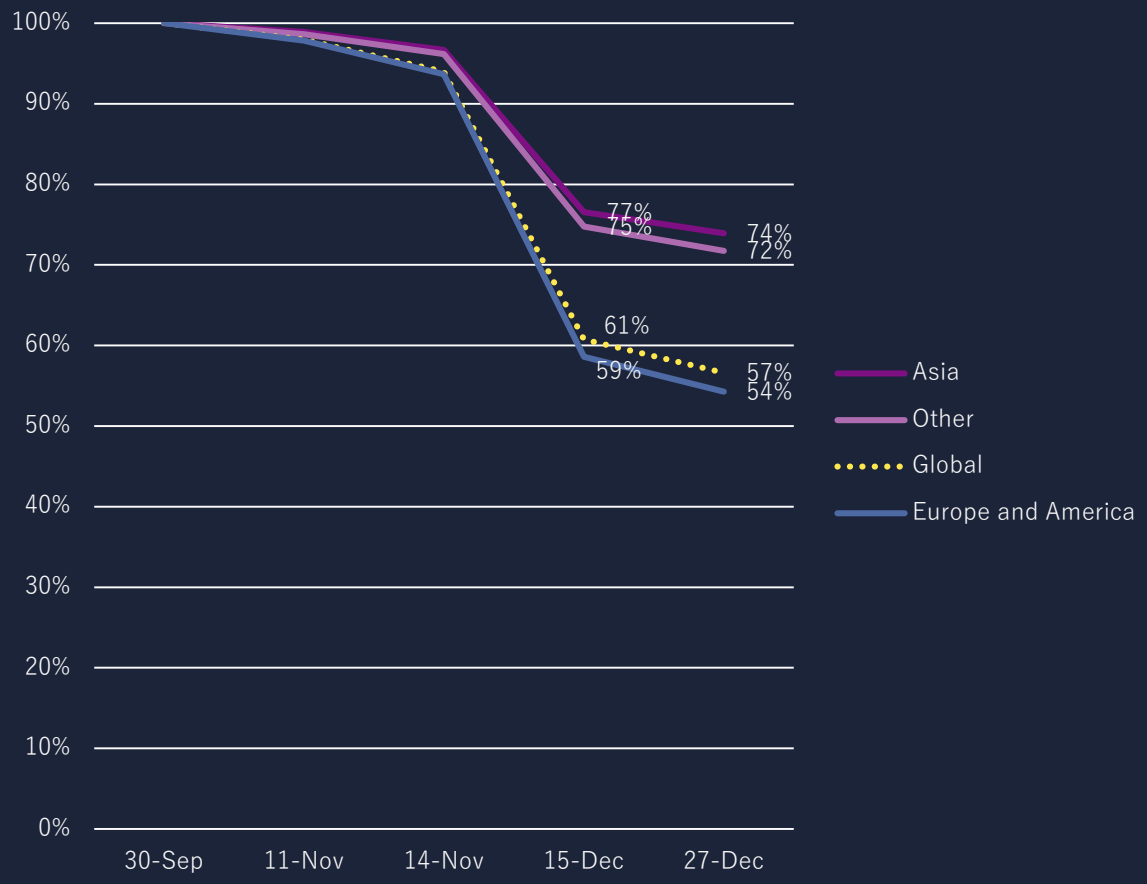


・上記の内4社分はテレワークPC

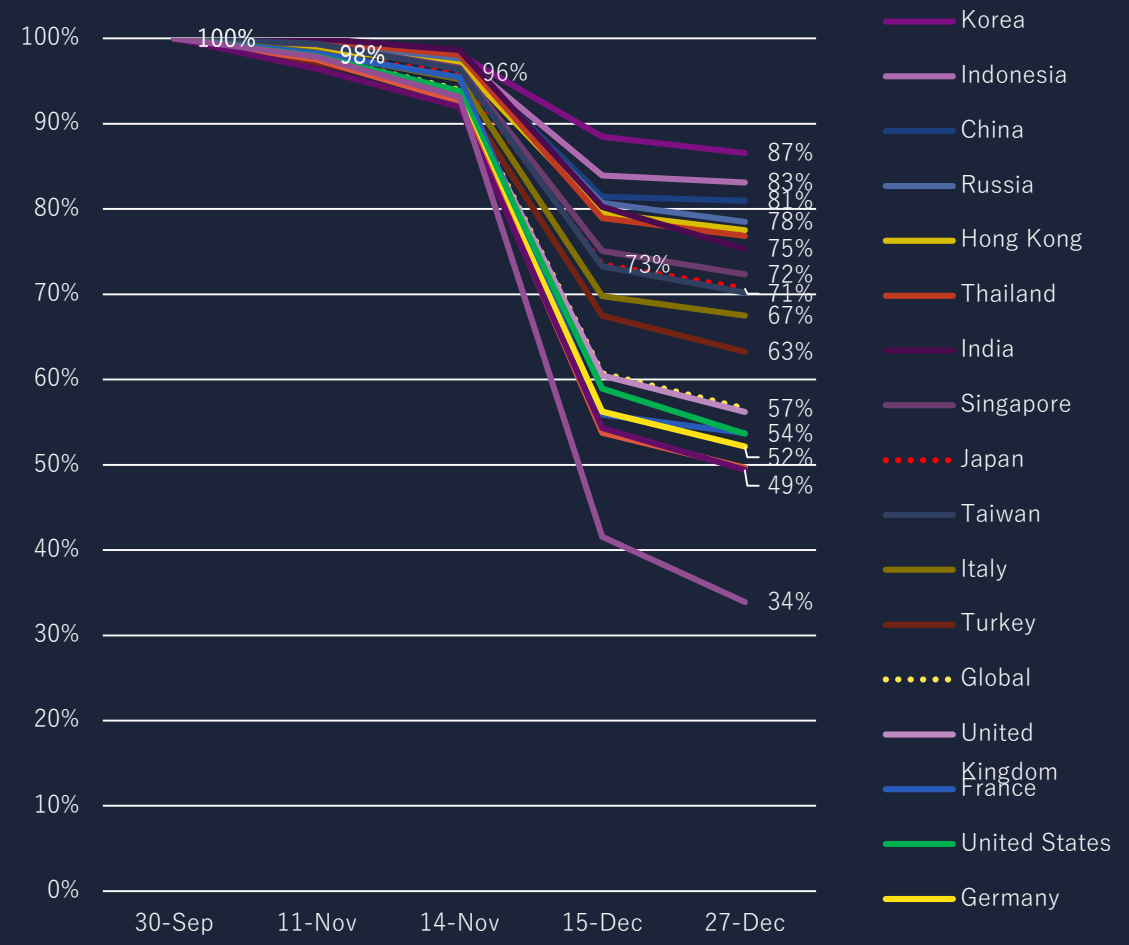
Exchange Server/ProxyNotShellの脆弱性の国別対策傾向

- 2022年9月にゼロデイ脆弱性として報告され2022年11月にパッチが公開された脆弱性 ProxyNotShellの対処スピード観測
- 欧米はパッチ公開から1ヶ月で約半数が対処されているところ、アジア圏では25％程度しか完了していない
- 対処が遅い国（右グラフ）もアジア圏ばかりが上位を占めている

✓脆弱サーバの割合推移（地域別）



✓脆弱サーバの割合推移（国別）

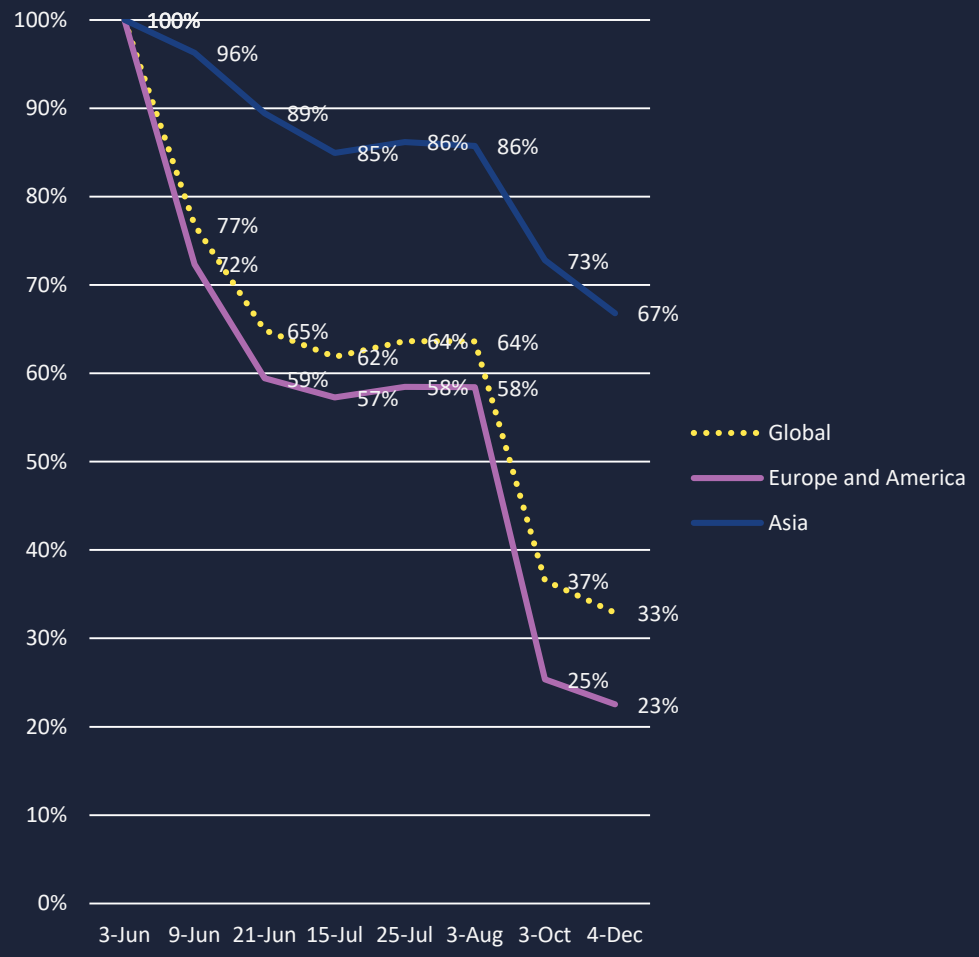


※データ取得タイミングの都合上グラフの日付が等間隔ではない点にご留意ください

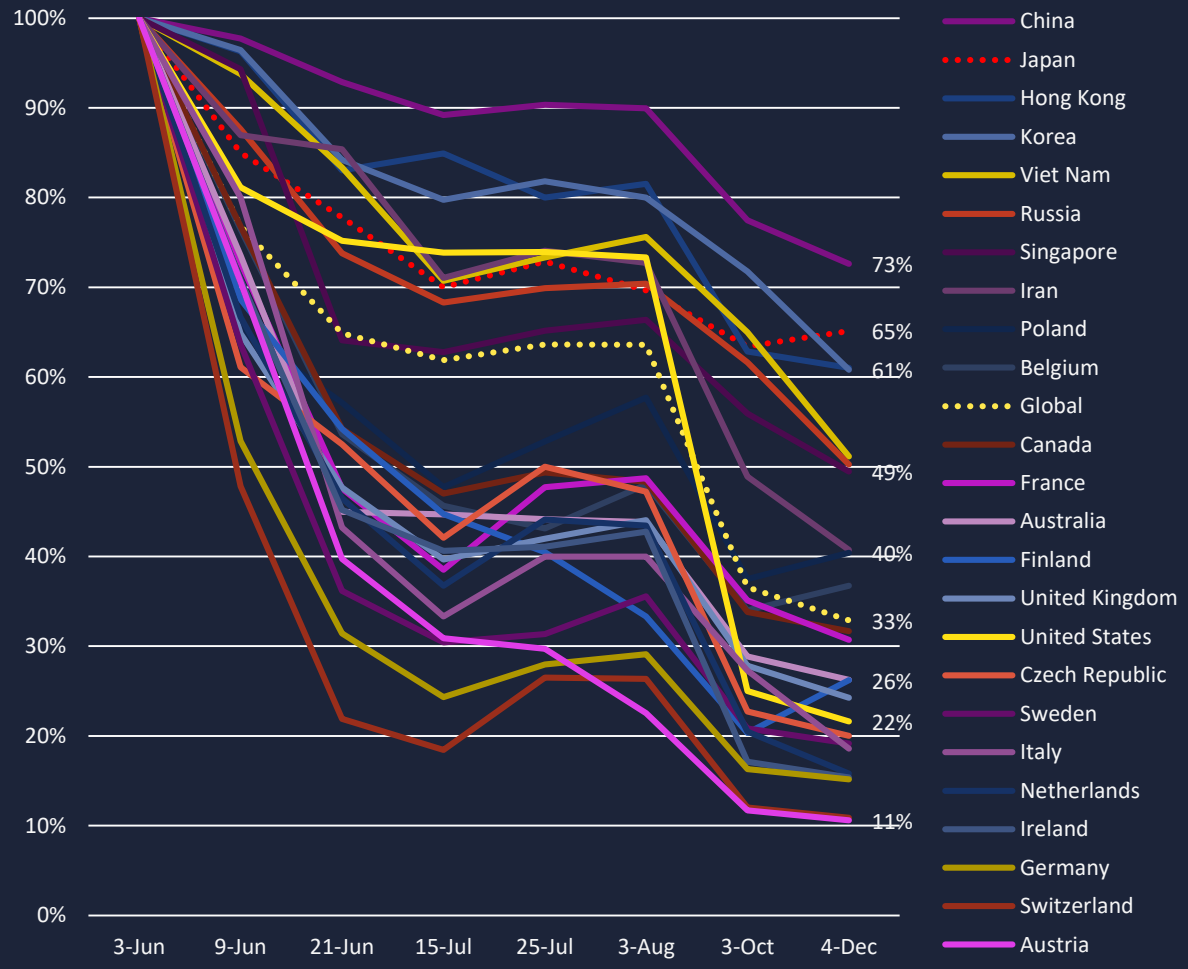
Atlassian Confluence/CVE-2022-26134の脆弱性の国別対策傾向

- ゼロデイの脆弱性で2022年6月2日にパッチが公開、その後も継続的に悪用が報道されている
- 2022/12/4時点ではグローバルで7001台中2303台、日本国内では43台中28台が脆弱なまま
- パッチ公開から約半年が経過し欧米では脆弱サーバが2割まで減少するもアジア圏では7割残る

✓脆弱サーバの割合推移（地域別）



✓脆弱サーバの割合推移（国別）



※データ取得タイミングの都合上グラフの日付が等間隔ではない点にご留意ください

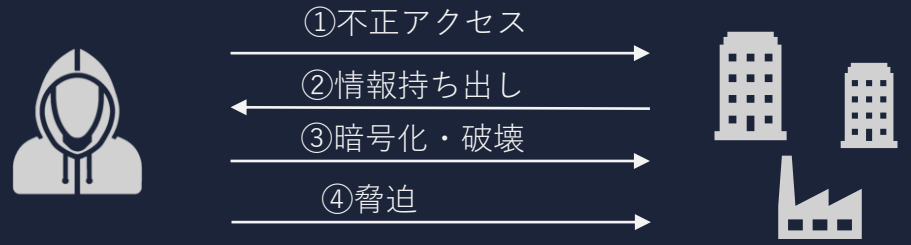
ゼロデイ脆弱性の悪用によりグローバルでの被害が急増

・ゼロデイ脆弱性＝メーカによるパッチ公開前に攻撃者がセキュリティホールを発見し攻撃に利用される脆弱性
・ゼロデイ脆弱性の悪用は年々増加しており2023年は特に被害が深刻化し**グローバルでの被害が急増した要因**となった

話題になった時期	製品	CVE	ゼロデイ	大規模被害
2023年1月	ZOHO ManageEngine	CVE-2022-47966		
	Exchange Server	CVE-2022-41040等		○
	Cacti	CVE-2022-46169		
	CentOS Web Panel	CVE-2022-44877		
	FortiGate	CVE-2022-42475	○	
2023年2月	IBM Aspera Fasted	CVE-2022-47986		
	VMware ESXi	CVE-2021-21974		○
	SugarCRM	CVE-2023-22952	○	
	Go Anywhere	CVE-2023-0669	○	○
2023年3月	FortiGate	CVE-2022-41328	○	
	Adobe ColdFusion	CVE-2023-26359等	○	
2023年4月	Papercut MF/NG	CVE-2023-27350		○
	Veeam Backup	CVE-2023-27532		
2023年5月	Barracuda ESG	CVE-2023-2868	○	○
	Rucks Wireless Admin	CVE-2023-25717		
	Zexel	CVE-2023-28771等		
2023年6月	FortiGate	CVE-2023-27997	○	
	MoveIT Transfer	CVE-2023-34362	○	○
2023年7月	Zimbara	CVE-2023-37580	○	
	ArrayAG	CVE-2023-28461		○
	Adobe ColdFusion	CVE-2023-29298等	○	
	Citrix ADC/Gateway	CVE-2023-3519	○	○
	Ivanti MDM	CVE-2023-35078等	○	
	Citrix Share File	CVE-2023-24489		
	ノースグリッド Proself	CVE-2023-39415等	○	
2023年8月	Ivanti Sentry	CVE-2023-38035	○	
	OpenFire	CVE-2023-32315		
	Apache RocketMQ	CVE-2023-33246		
	MinIO	CVE-2023-28432		
2023年9月	JetBrains TeamCity	CVE-2023-42793		
	Cisco ASA	CVE-2022-47966	○	○
2023年10月	Progress WS FTP Server	CVE-2023-40044		
	F5 BIG-IP	CVE-2023-46747等		
	Cisco IOS XE	CVE-2023-20198	○	○
	Atlassian Confluence	CVE-2023-22515	○	
	Citrix ADC/Gateway	CVE-2023-4966	○	○
	ノースグリッド Proself	CVE-2023-45727	○	
2023年11月	ownCloud	CVE-2023-49103	○	
	Atlassian Confluence	CVE-2023-22518		
	Apache ActiveMQ	CVE-2023-46604		○
	SysAid	CVE-2023-47246	○	
	Qlik Sense	CVE-2023-41265		
2023年12月	Apache Struts 2	CVE-2023-50164		
	Barracuda ESG	CVE-2023-7102		
	Apache OFBiz	CVE-2023-51467	○	

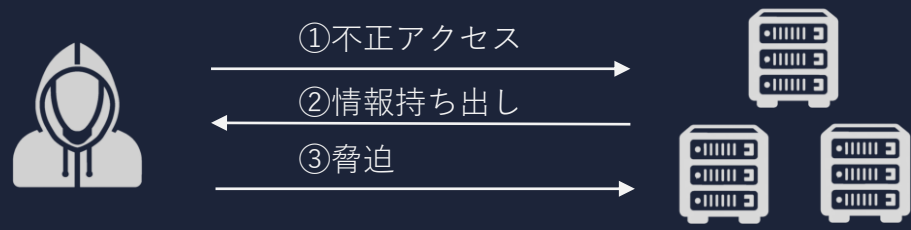
通常のランサムウェア

・標的組織を数日～数週間をかけてじっくりと攻撃するため被害組織数は限定的
・攻撃の過程で被害組織に気づかれて阻止される可能性も高い



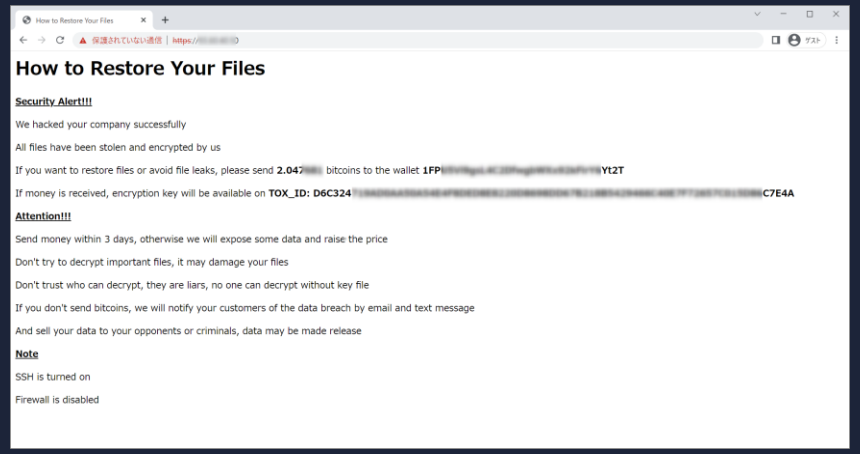
ノーウェアランサム（情報窃取型ランサム）

・ゼロデイを悪用し一気に世界中の数百～数千の公開サーバへ攻撃を行う
・情報窃取のみとなるため気づかれるリスクもなく暗号化機能の開発コストも不要

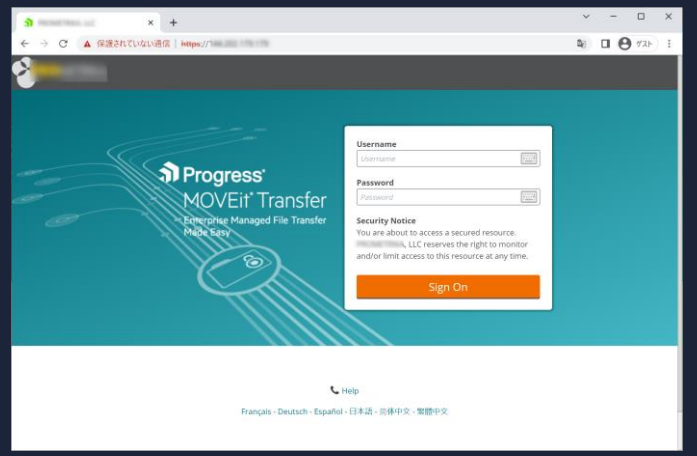


被害急増の原因となった主な事件

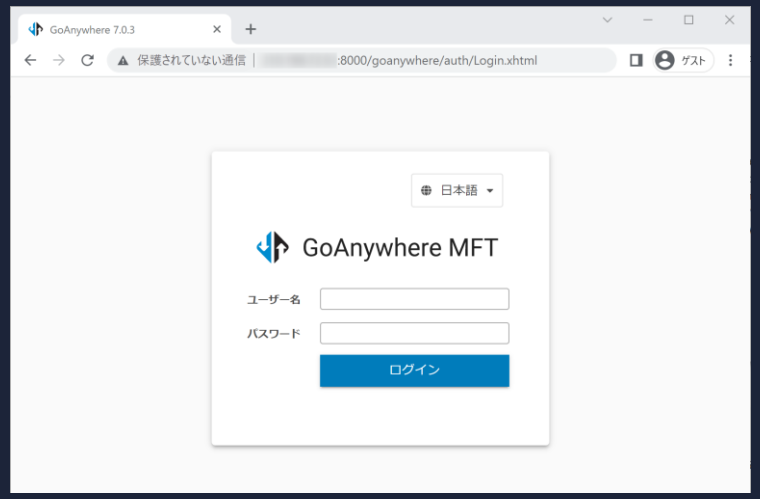
ESXi Args
・2月にVMware ESXiの既知脆弱性を悪用
・数日間で4000台超のサーバが暗号化



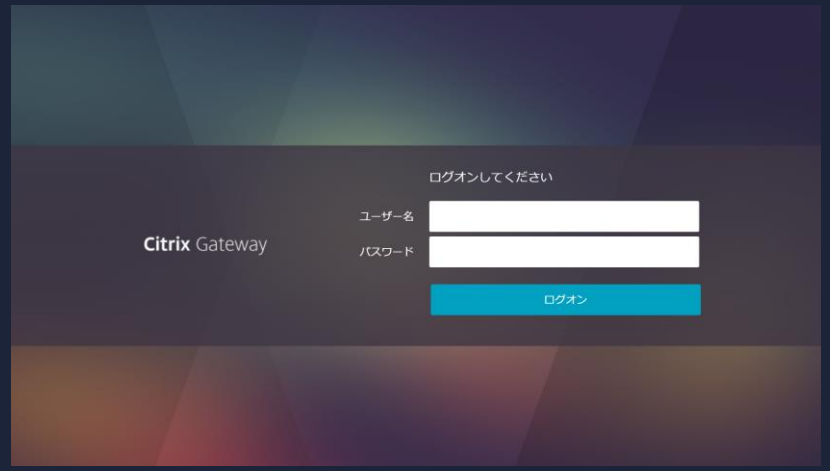
MoveIT Transfer
・6月にランサム攻撃者ClOPがゼロデイ脆弱性を悪用
・グローバル3000社弱が被害にあい7700万人分の個人情報が漏洩



GoAnyWhereMFT
・2月にランサム攻撃者ClOPがゼロデイ脆弱性を悪用
・グローバル約130社が被害にあう



Citrix
・ゼロデイ脆弱性で7月頃認証情報を窃取するWebShellが数百台に設置される事案が発生
・ゼロデイ脆弱性で11月頃にセッショントークンを窃取可能な脆弱性 Citrix Bleedが発生し被害続発

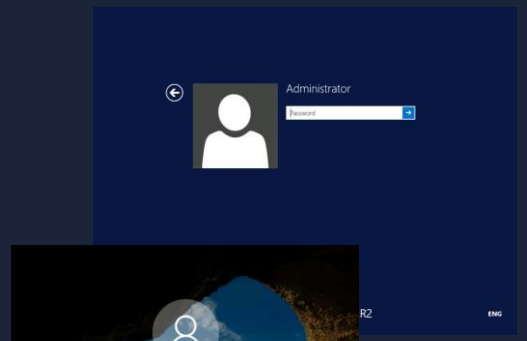


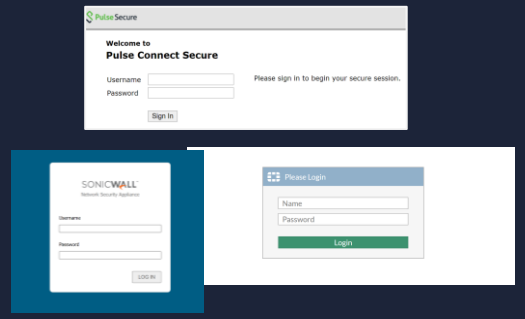
要注意ホスト、要注意プロダクト

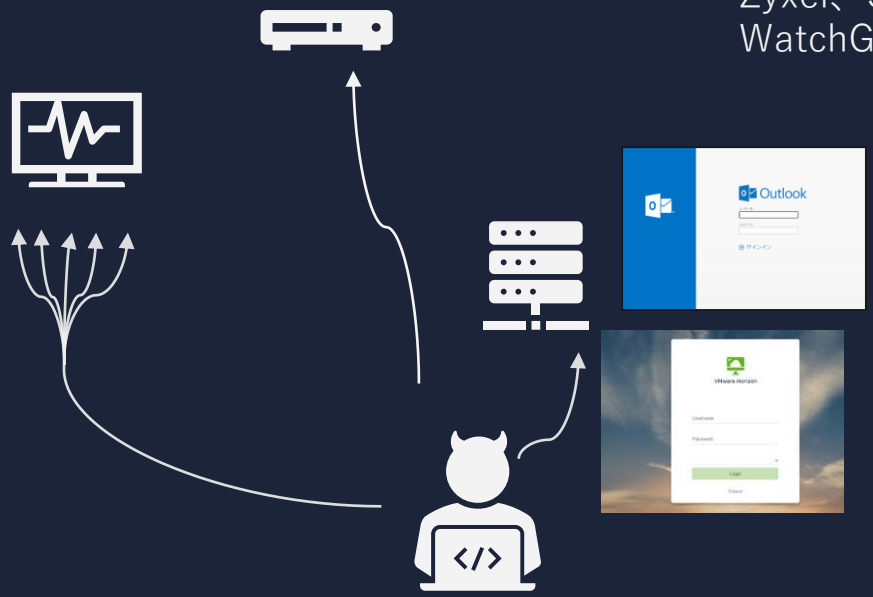
自社環境での1のようなサーバの駆逐、2・3の製品のパッチ管理が非常に重要

1 特定ポートに対する不正ログイン

RDP、WinRM、SMB







2　ネットワークアプライアンスへの攻撃（不正ログイン、脆弱性悪用）

Citrix（ADC、Gateway）、
Ivanti（EPMM、Sentry、Pulse Secure、旧 MobileIron ）
Cisco（IOS/IOSXE機器、ASA、RV、Small Buisiness等）
Fortinet（FortiOS機器）
SonicWall（SMA） F5(Big-IP)、Palo Alto（PAN-OS機器）、
Zyxel、Sophps（UTM、FireWall、 Web Appliance ）、
WatchGuard、Juniper（Junos OS機器）

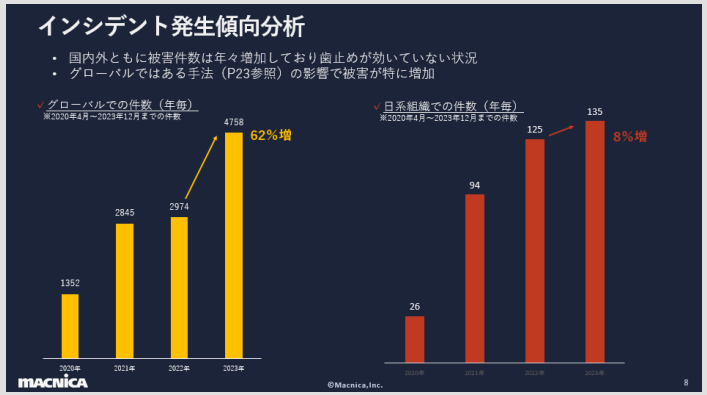
3 サーバーソフトウェアの脆弱性悪用

Microsoft Exchange Server、Zimbra、
ZOHO（ManageEngine、Service Desk、 Desktop Central ）
Atlassian（Confluence 、BitBucket、Crowd、Jira）
Vmware（ESXi、Workspace ONE、Horizon、vCenter等）
Mitel MiVoice、Microsoft Sharepoint

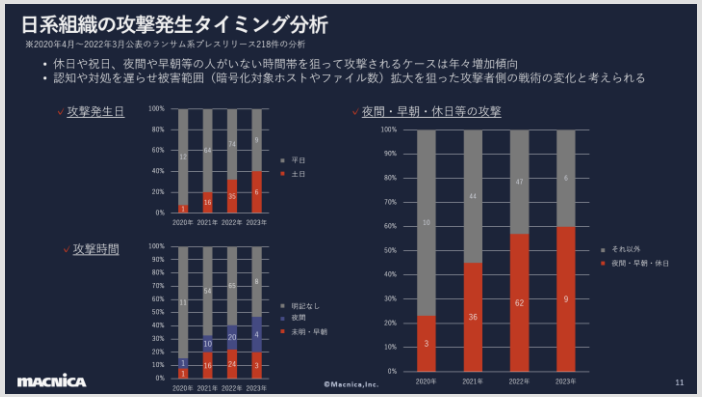
※本スライドは**上記メーカや製品に問題があることを示すものではありません**。脆弱性はいかなるソフトウェアでも発生し、上記製品は世界中で広く・多く利用されているため、特に狙われやすいという背景もあります。

ここまでのまとめ

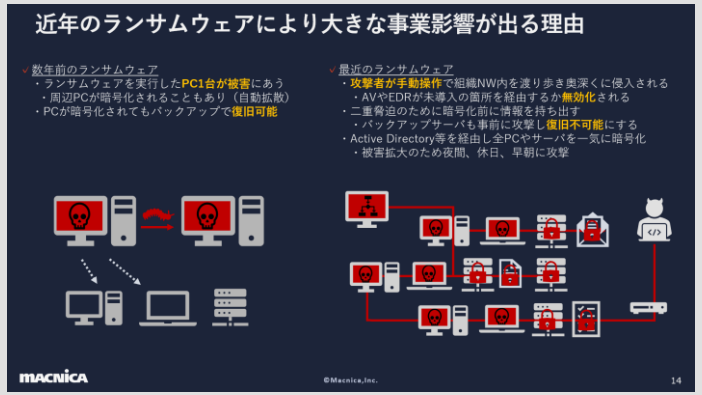
1 ランサム攻撃件数は高止まり 今後数年間は継続する



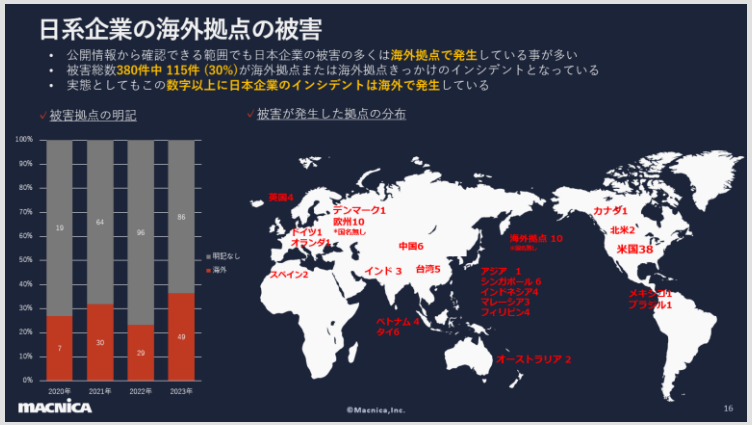
2 土日・早朝・夜間などの 人がいない時間帯の攻撃に注意



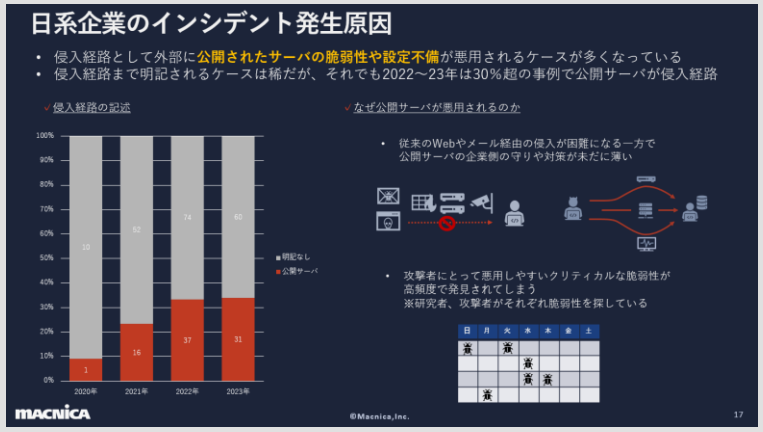
3 侵入後の横移動により 被害範囲が拡大する



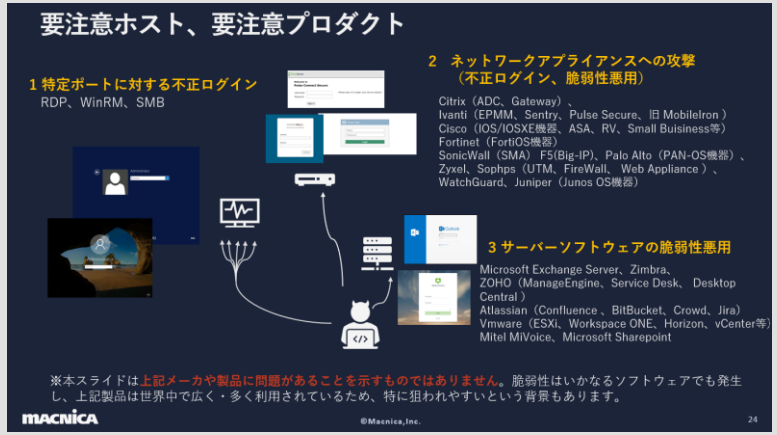
4 日本企業は海外が弱い 特にアジア圏の拠点に注意



5 公開サーバ起因の インシデントが再び増加中



6 自社グループの国内外サーバの 把握と脆弱性管理（ASM）の徹底を



脆弱性対処のトレンド

脆弱性対策のあり方・常識の変化について

これまでの脆弱性対策

- ✓ 可能な限りすべてのパッチを適用
  - ・CVSS 7.0以上の場合は優先度を上げる
- ✓ 脆弱性を抱える資産の性質は加味しない
  ※サーバやホストが侵害された場合のビジネスリスク
  ※サーバの設置セグメント　等
- ✓ Excelなどで対応状況を人手で管理
- ✓ 結果として本来対処が必要な脆弱性にも対処の手が回らずインシデントにつながっている

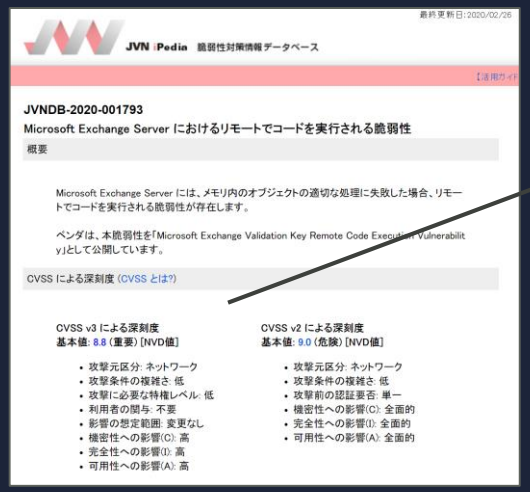
これからの脆弱性対策

- ✓ **リスクの高い脆弱性を最優先で対処**
- ✓ 攻撃を受ける可能性や保持する情報やインパクトも加味
- ✓ 専用の脆弱性管理ツールの活用
  ※新たなソリューションカテゴリの出現
  - ・Risk Based Vulnerability Management（RBVM）
  - ・Vulnerability prioritization technology（VPT）
  - ・Software Bill of Materials（SBOM）
- ✓ 限られたリソースの中でも効果的にリスクに対抗

リスクの高い脆弱性とはなにか？

脆弱性に関するよくある誤解

✓ CVSS7.0以上の脆弱性は特に危険なため優先して対処が必要である



CVSS v3 による深刻度
基本値: 8.8 (重要) [NVD値]

- 攻撃元区分: ネットワーク
- 攻撃条件の複雑さ: 低
- 攻撃に必要な特権レベル: 低
- 利用者の関与: 不要
- 影響の想定範囲: 変更なし
- 機密性への影響(C): 高
- 完全性への影響(I): 高
- 可用性への影響(A): 高

✓ 脆弱性は全てリスクがあり危険なので対処すべき

IT News

- ○○の複数の緊急の脆弱性 202X年4月
- ○○に複数の脆弱性、○百万台に影響 202X年4月
- ○○に緊急の脆弱性、至急アップデートを 202X年4月
- ○○の定例アップデートで○件の脆弱性 202X年4月

CVSS7.0以上は特に危険なため、優先して対処が必要か

✓ CVSS管理関係団体（CERT/CC）からCVSSによる優先度付は誤用である旨が指摘されている

The Common Vulnerability Scoring System (CVSS) is widely misused[1] for vulnerability prioritization and risk assessment, despite being designed to measure technical severity. Furthermore, the CVSS scoring algorithm is not justified, either formally or empirically. Misuse of CVSS as a risk score means you

CVSSは、脆弱性の技術的な深刻度を測定するように設計されているにも関わらず、
脆弱性の**優先順位付けとリスクの評価の手段として広く誤用**されています。

CVSS scores severity, not security risk

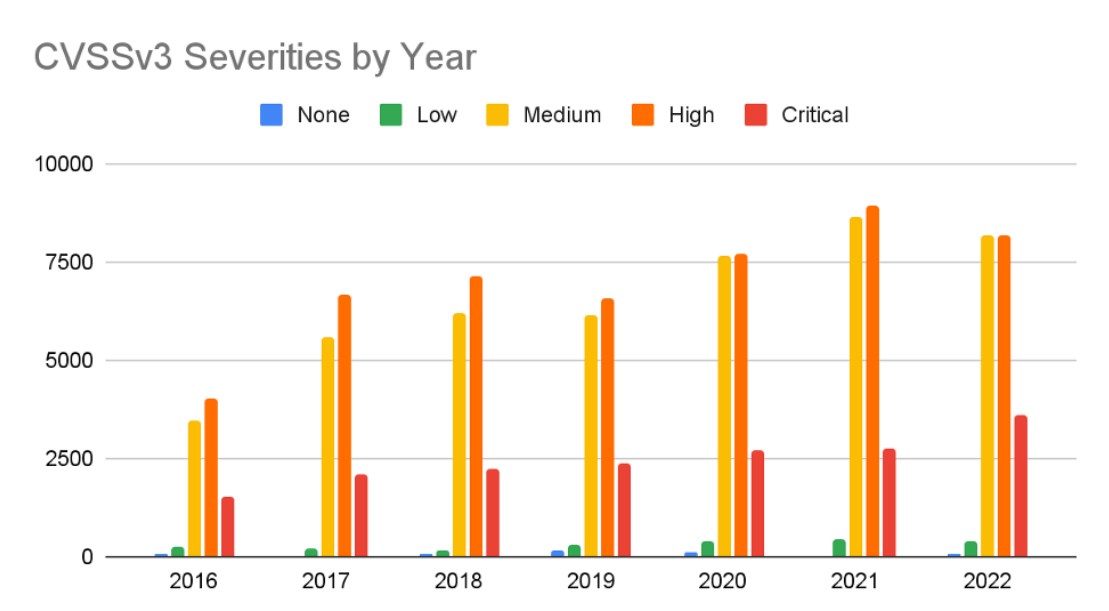
CVSS is designed to identify the technical severity of a vulnerability. What people seem to want to know, instead, is the risk a vulnerability or flaw poses to them, or how quickly they should respond to a vulnerability. If so, then either CVSS needs to change or the community needs a new system.

CVSSは脆弱性の深刻度を評価します。**セキュリティリスクではありません。**

TOWARDS IMPROVING CVSS/ December 2018
https://resources.sei.cmu.edu/asset_files/WhitePaper/2018_019_001_538372.pdf
https://insights.sei.cmu.edu/blog/towards-improving-cvss/

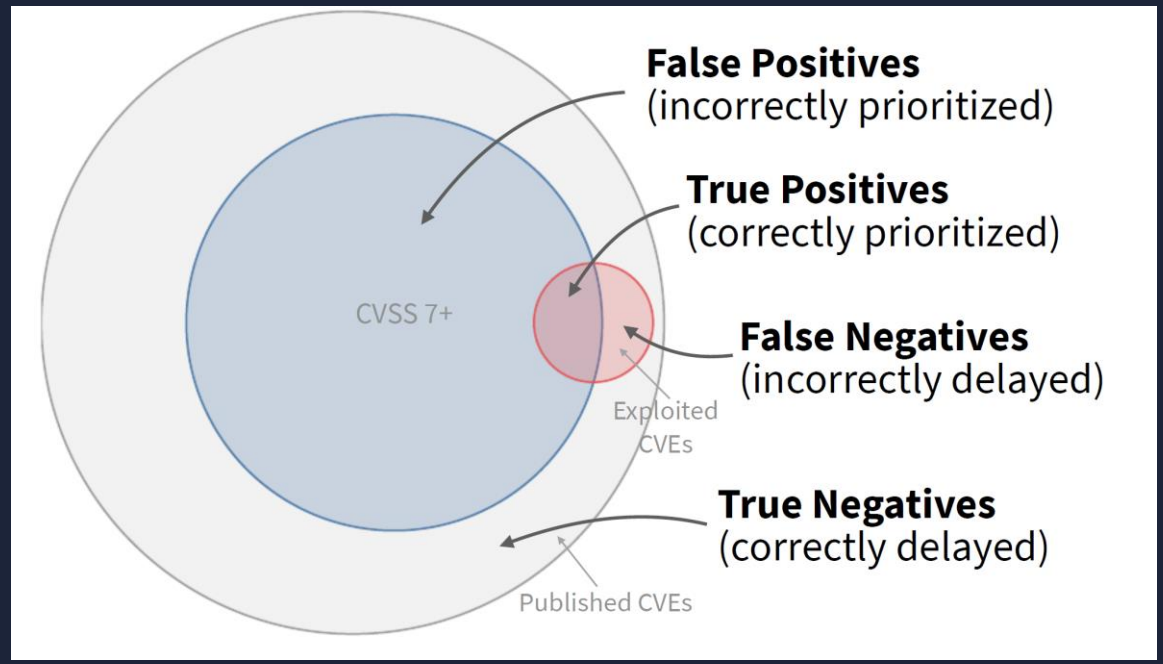
CVSSによる優先度付の限界

- ✓ 2022年に特定された約20000件の脆弱性
  - ・High/7.0-8.9　が **40%**
  - ・Critical/9.0-10.0 が **17%**
  - → CVSSベースでは半数以上が至急対処となる



https://www.tenable.com/blog/you-cant-fix-everything-how-to-take-a-risk-informed-approach-to-vulnerability-remediation

- ✓ CVSS 7.0未満でも優先して対処すべき脆弱性は存在する
  - ※主に権限昇格系の脆弱性
  - ※CVSS7.0 未満の脆弱性組み合わせでの攻撃もしばしば発生



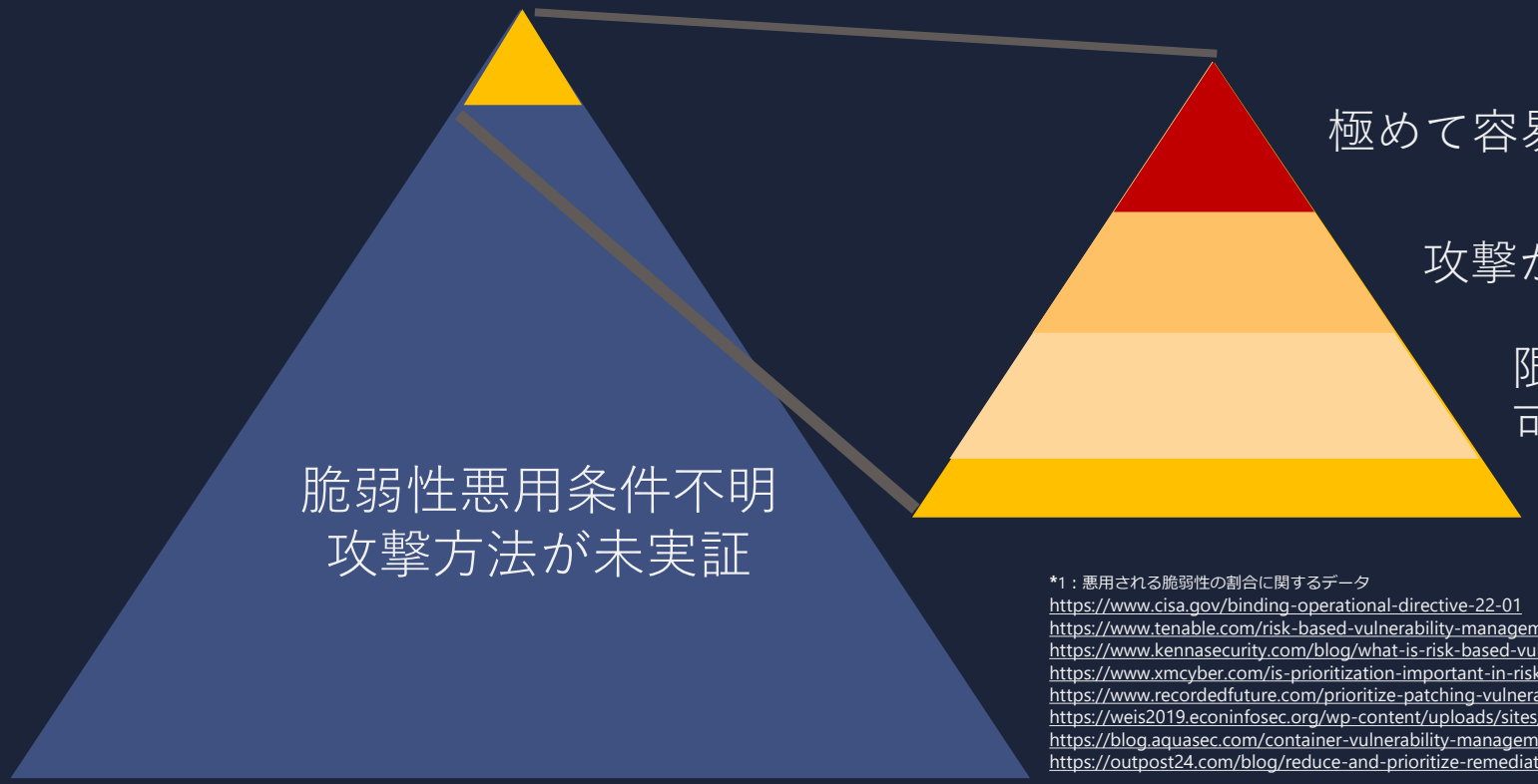
https://www.first.org/epss/model

CVSSは脆弱性を評価する重要な指標だが、対処の優先度付としてはそれのみを根拠とすべきではない

実際にリスクとなる脆弱性は全体のごく一部である

✓公表される脆弱性（CVE付）の中で攻撃が可能で実際に悪用される脆弱性は約 **約5%程度**しかない*1

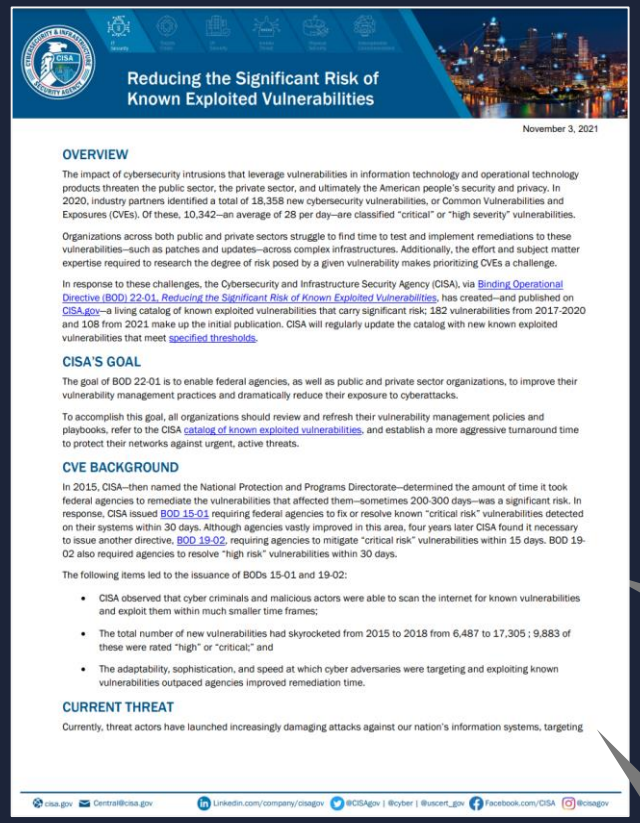
✓悪用が報告された脆弱性は自社への攻撃へ使われる可能性があるため最速での対処が必要



*1：悪用される脆弱性の割合に関するデータ
https://www.cisa.gov/binding-operational-directive-22-01
https://www.tenable.com/risk-based-vulnerability-management
https://www.kennasecurity.com/blog/what-is-risk-based-vulnerability-management/
https://www.xmcyber.com/is-prioritization-important-in-risk-based-vulnerability-management/
https://www.recordedfuture.com/prioritize-patching-vulnerability-intelligence/
https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_53.pdf
https://blog.aquasec.com/container-vulnerability-management
https://outpost24.com/blog/reduce-and-prioritize-remediation-efforts-with-likelihood-of-an-actual-attack

少し前の大きなニュース

✓ 米国連邦政府の方針変更　CISAによるKEVカタログの運用開始とリスクベースへの転換



Reducing the Significant Risk of Known Exploited Vulnerabilities

November 3, 2021

OVERVIEW

The impact of cybersecurity intrusions that leverage vulnerabilities in information technology and operational technology products threaten the public sector, the private sector, and ultimately the American people's security and privacy. In 2020, industry partners identified a total of 18,358 new cybersecurity vulnerabilities, or Common Vulnerabilities and Exposures (CVEs). Of these, 10,342—an average of 28 per day—are classified "critical" or "high severity" vulnerabilities.

Organizations across both public and private sectors struggle to find time to test and implement remediations to these vulnerabilities—such as patches and updates—across complex infrastructures. Additionally, the effort and subject matter expertise required to research the degree of risk posed by a given vulnerability makes prioritizing CVEs a challenge.

In response to these challenges, the Cybersecurity and Infrastructure Security Agency (CISA), via Binding Operational Directive (BOD) 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities*, has created—and published on CISA.gov—a living catalog of known exploited vulnerabilities that carry significant risk; 182 vulnerabilities from 2017-2020 and 108 from 2021 make up the initial publication. CISA will regularly update the catalog with new known exploited vulnerabilities that meet specified thresholds.

CISA'S GOAL

The goal of BOD 22-01 is to enable federal agencies, as well as public and private sector organizations, to improve their vulnerability management practices and dramatically reduce their exposure to cyberattacks.

To accomplish this goal, all organizations should review and refresh their vulnerability management policies and playbooks, refer to the CISA catalog of known exploited vulnerabilities, and establish a more aggressive turnaround time to protect their networks against urgent, active threats.

CVE BACKGROUND

In 2015, CISA—then named the National Protection and Programs Directorate—determined the amount of time it took federal agencies to remediate the vulnerabilities that affected them—sometimes 200-300 days—was a significant risk. In response, CISA issued BOD 15-01 requiring federal agencies to fix or resolve known "critical risk" vulnerabilities detected on their systems within 30 days. Although agencies vastly improved in this area, four years later CISA found it necessary to issue another directive, BOD 19-02, requiring agencies to mitigate "critical risk" vulnerabilities within 15 days. BOD 19-02 also required agencies to resolve "high risk" vulnerabilities within 30 days.

The following items led to the issuance of BODs 15-01 and 19-02:

- CISA observed that cyber criminals and malicious actors were able to scan the internet for known vulnerabilities and exploit them within much smaller time frames;
- The total number of new vulnerabilities had skyrocketed from 2015 to 2018 from 6,487 to 17,305 ; 9,883 of these were rated "high" or "critical;" and
- The adaptability, sophistication, and speed at which cyber adversaries were targeting and exploiting known vulnerabilities outpaced agencies improved remediation time.

CURRENT THREAT

Currently, threat actors have launched increasingly damaging attacks against our nation's information systems, targeting

cisa.gov　Central@cisa.gov　LinkedIn.com/company/cisagov　@CISAgov | @cyber | @uscert_gov　Facebook.com/CISA　@cisagov

https://cyber.dhs.gov/bod/22-01/#what-is-the-difference-between-vulnerabilities-listed-in-the-national-vulnerability-database-nvd-and-those-in-cisas-catalog-of-known-exploited-vulnerabilities-kevs

・Known Exploited Vulnerabilities Catalog
  ・米国 国土安全保障省　サイバーセキュリティ・インフラセキュリティ庁が運用
  ・実際に悪用されていることが報告された脆弱性のリスト

  ・21年11月3日に運用が開始
  ・合計1072件の脆弱性が掲載されている（2024年1月29日現在）
  ・CISAが悪用を認識し24時間以内に不定期に情報が更新される
  ・米国 連保政府機関は掲載された脆弱性は指定期日（原則2週間）までに対処必須

・以下URLより無償で誰でも参照可能
  ・WEB、JSONやCSV、メール通知で情報取得が可能
  https://www.cisa.gov/known-exploited-vulnerabilities-catalog

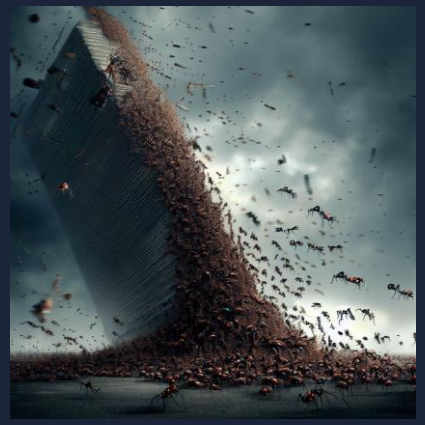
sends a clear message to all organizations across the country to focus remediation efforts on the subset of vulnerabilities that are causing harm now

全国のすべての組織に対し、**今まさに被害をもたらしている脆弱性**のサブセットに改善の努力を集中させるという明確なメッセージを発信しています。

Agencies are not required to patch all CVEs. To be effective, vulnerability management programs must take active threats into consideration.

政府機関は、**すべてのCVEにパッチを適用する必要はありません**。脆弱性管理プログラムを効果的にするには、アクティブな脅威を考慮に入れる必要があります。

限られたリソースは現実的なリスクへの対策に投入すべき



大量の蟻に壁が
かじられてビルが倒壊

隕石の直撃に備えた
シェルターハウス

高度な知能に進化した
イルカの襲来

地震対策

火災対策

不審者対策

脆弱性情報のソース

- 全パッチ適用が可能な組織はそれを継続すべきだが、それが難しい場合は特にリスクの高い脆弱性について対処する
- リスクの高い脆弱性を把握するための推奨の情報ソース

✓ Bleeping Computer
- 脆弱性に関する情報以外も配信する海外メディア
- 取り上げる事案の選定、内容の粒度や信頼性、スピードに優れる
- 脆弱性ニュース内のPoCや攻撃発生に関する記述に留意

https://www.bleepingcomputer.com/

✓ 無償の脆弱性インテルサイト

PoC code：脆弱性の利用を実証したコード

The researchers found that an attacker could exploit the vulnerability by sending a specially crafted packet to the VPN server, causing it to crash and leak memory contents. By analyzing the leaked data, an attacker could obtain the private key used for encryption and decryption, as well as user credentials and session data. To demonstrate the severity of the vulnerability, the researchers also **released a proof-of-concept (PoC) code**, which can be used to reproduce the exploit.

In the wild：脆弱性を悪用した攻撃発生を示す言葉

A critical vulnerability in SecureLink VPN has been **exploited in the wild,** according to reports by multiple security firms. The vulnerability, which was discovered last month by security researchers, allows attackers to bypass encryption and access sensitive information, including user credentials and session data. The flaw affects the latest version of SecureLink VPN on all major platforms, including Windows, macOS, iOS, and Android.

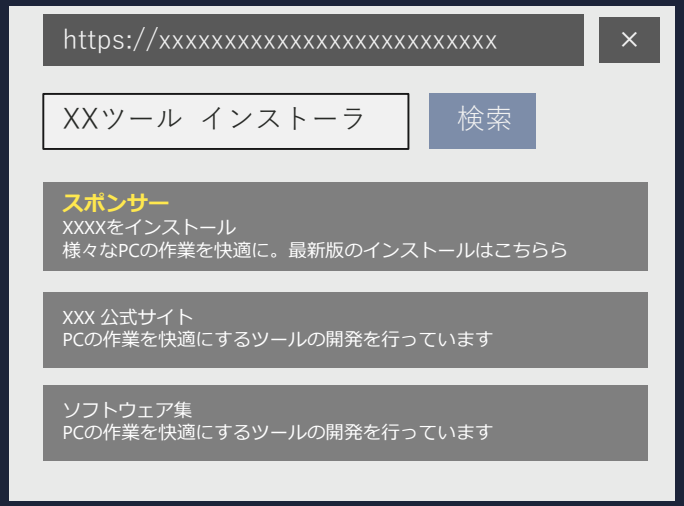
※上記は実際のBleeping Computerの記事ではなく架空のサンプル文章です
Written with ChatGPT

当日配布資料でのみ掲載

要警戒 情報窃取特化型マルウェア
InfoStealer

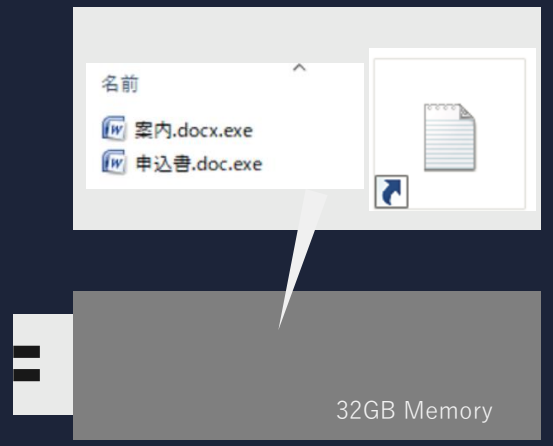
Info Stealerとは？

- 情報窃取に特化したマルウェアのこと
- Webやメール経由でPCに感染し様々な情報を攻撃者へ送信する



Webサイト（広告の悪用）
※ニセソフトやアドウェア

メール添付ファイル



USBメモリ中のファイル

認証情報の漏洩とその悪用による不正侵入に警戒

・何らかの理由でシステムログイン用のIDとパスワードが漏洩し、それを悪用され不正侵入されるケースが急増中
・2023年に国内セキュリティベンダが実施した調査でも国内500社中100社超の情報がInfo Stealer経由で漏洩していることが確認
https://image.sompo-rc.co.jp/infos/20231016_1.pdf

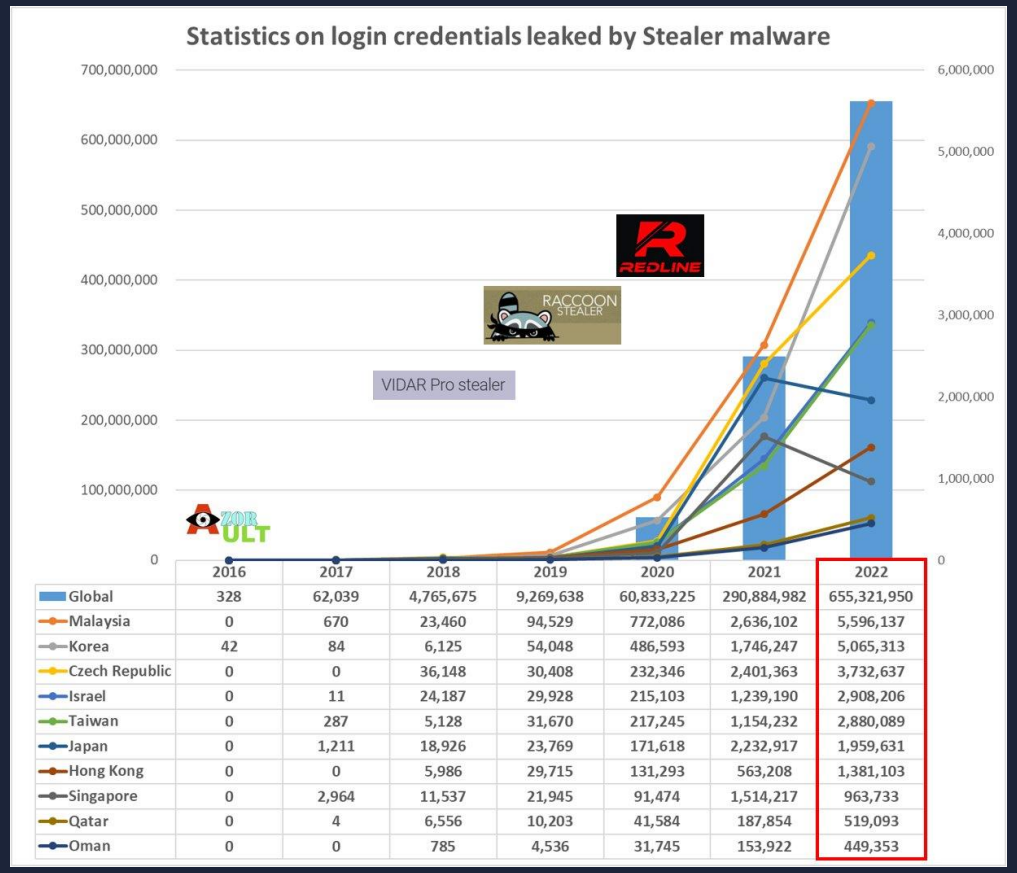
認証情報窃取により組織への侵入が発生したインシデント

・日系企業のプレスリリースの中でこのパターンが大きく増加
・昨年まではこのような記載は見られず2023年の特徴

時期	企業	コメント
2023年10月	IT	攻撃者により一部社員の**アカウント／パスワード情報が盗まれました**。これを起点に以下の攻撃を受けました。
2023年8月	製造	攻撃者は、**流出済みのVPN の認証情報**を利用し、弊社の業務用サーバ等に不正にアクセスし、ランサムウェアを実行し、データの暗号化を行ったものと考えられます。
2023年6月	製造	リモートアクセスで実際に利用する**IDやパスワードを何らかの方法で攻撃者により特定され**、内部ネットワークへ侵入されたものと見られる。特定された背景などはわかっていない。
2023年6月	IT	クラウドAZタワーの利用者に対して、**IDとパスワードをパーパスが割り当て**ている。ある事業者が使っていた正規のIDとパスワードを使用して侵入してきた。1社だけでなく、複数の企業にそれぞれ発行したIDとパスワードだった
2023年5月	IT	再発防止策として以下内容を対応しております。 ・各種アカウントの**認証情報リセット**、管理ポリシーの見直し、社内ネットワーク通信のセキュリティ強化
2023年4月	建設	当社が管理運用していたVPN機器の**管理アカウントのパスワードが推測可能なもの**であったため、当社が導入していたVPN機器を経由して当社内サーバー等への不正なアクセスに利用されていたとのことでした。
2023年3月	製造	調査の結果によれば、攻撃者は、**何らかの方法で当社の VPNに侵**入し、これを通じて当社社内サーバーに侵入して、ランサ ムウェアを実行し、ファイルの暗号化を行ったものと考えられます。
2023年1月	サービス	今回の不正アクセスは、サーバーの脆弱性を利用した攻撃であり、弊社のネットワーク設定や**パスワードの強度の問題**により発生したものと考えております。

Info Stealerの感染台数推移

・毎年、前年比で2倍以上の勢いで感染台数が増加中
・様々な種別のInfo Stealerが開発されており攻撃者側も本領域に注力中



	2016	2017	2018	2019	2020	2021	2022
Global	328	62,039	4,765,675	9,269,638	60,833,225	290,884,982	655,321,950
Malaysia	0	670	23,460	94,529	772,086	2,636,102	5,596,137
Korea	42	84	6,125	54,048	486,593	1,746,247	5,065,313
Czech Republic	0	0	36,148	30,408	232,346	2,401,363	3,732,637
Israel	0	11	24,187	29,928	215,103	1,239,190	2,908,206
Taiwan	0	287	5,128	31,670	217,245	1,154,232	2,880,089
Japan	0	1,211	18,926	23,769	171,618	2,232,917	1,959,631
Hong Kong	0	0	5,986	29,715	131,293	563,208	1,381,103
Singapore	0	2,964	11,537	21,945	91,474	1,514,217	963,733
Qatar	0	4	6,556	10,203	41,584	187,854	519,093
Oman	0	0	785	4,536	31,745	153,922	449,353

https://x.com/stealthmole_int/status/1656528528287088642?s=20

特に考慮が必要なポイント

✓ アジア、東南アジア圏

- 外部ファイルの取得/実行に抵抗が少ない
- Info Stealerの感染数が非常に多い
  - 被害の多い国を攻撃者も狙っている
- 海外拠点から未把握経路での国内侵入に注意

✓ 社員の私用PC感染

- 社内システムの認証情報が個人PC経由で漏洩
- Chromeの同期機能での認証情報流出に注意

備考：Cisco、Retool、Oktaも同期機能要因で被害発生

https://blog.talosintelligence.com/recent-cyber-attack/
https://retool.com/blog/mfa-isnt-mfa
https://www.okta.com/jp/blog/2023/11/harfiles/

Info Stealer対策

✓ **ダークウェブ調査サービス**
- 自社の情報がダークウェブに漏洩していないかを調査するサービス
- InfoStealer経由の情報漏えいも調査可能な場合が多い
- ただし、大なり小なり情報漏洩はあるため慌てない、高額なサービスを購入しないことに注意

✓ **基本的な情報セキュリティルールの徹底**
- 業務で利用する情報を私用PCに持ち出させない、保存させない
  ※P38のシナリオの対策
- 同じパスワードを使い回さない
  ※会社PCと個人PCが同期していない場合でもパスワードの使いまわしがあれば不正ログインリスクが高まる

✓ **テクノロジーでの解決**
- CASB機能でGoogleアカウントのログインを制御する
- エンタープライズブラウザでGoogleアカウントのログインを制御する
- Googleの企業向け管理機能を利用する
  https://support.google.com/a/answer/1668854?hl=ja

日本企業を狙う標的型攻撃の印象的な事件

サイバー攻撃における脅威分類例

	標的型攻撃	ランサムウェア	ばらまき型攻撃	ハクティビスト	個人
標的	特定の組織	組織	不特定多数の組織と個人	政府や特定組織	政府や特定組織
目的	設計図/政治動向などの知財 個人情報	金銭(身代金の要求)	金銭(オンラインバンキングアカウントなど)	自らが主張する政治的または社会的な理念の推進	自己顕示、個人的な動機
攻撃	検知率の低い遠隔操作マルウェ アをシステムに常駐させて、長 期に組織に潜伏して情報を窃取 する	ランサムウェアでファイルを暗号 し解除のための身代金を要求する。近年は更に暗号前にデータを窃取 して、データ開示に対する身代金 も要求するケースが増加	主に侵害されたメールアカウントからのスピアフィッシングメールに添付のファイルを実行することで、マルウェアに感染する。オンライン取引の盗聴、感染者のクレデンシャルやメールの窃取、組織内での感染拡大	大量のトラフィックを対象組織に送りサービスを不可にするDDoSや、サイトの改ざん、情報の暴露等	大量のトラフィックを対象組織に送りサービスを不可にするDDoS代行サービスの利用、サイトの改ざん、情報窃取等
例	LODEINFO Operation RestyLink A41APT攻撃キャンペーン	LockBit CL0P ALPHV (BlackCat)	Emotet RedLine Stealer QakBot	Anonymous Operation Payback	Kevin David Mitnick Adrian Lamo

タイムチャート

当日配布資料でのみ掲載

特に注意が必要な企業

当日配布資料でのみ掲載

XXXXXを使った配送

当日配布資料でのみ掲載

物理的な接近

当日配布資料でのみ掲載

進むEDR対策

当日配布資料でのみ掲載

マクニカオリジナルの標的型攻撃分析レポート

以下URLより個人情報登録不要で無償配布中
https://www.macnica.co.jp/business/security/security-reports/

標的型攻撃対策

当日配布資料でのみ掲載

本日のまとめ

1 日系企業のランサム被害傾向と関連情報

被害増加傾向は変わらず
海外、子会社含めた**公開サーバの管理**を

2 脆弱性対処のトレンド

CVSS基準の脆弱性対処ではなく
特に**リスクの高い脆弱性**を最速で対処

3 要警戒 情報窃取特化型マルウェア Info Stealer

情報漏洩被害が急増中
アジア拠点や**私用PC**からの漏洩にも注意

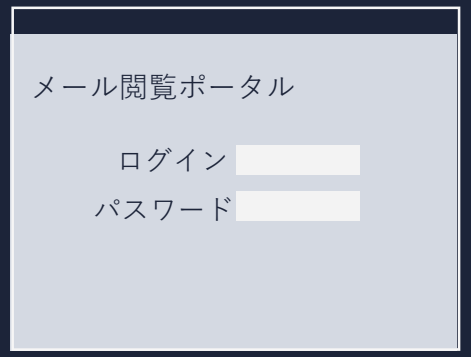
4 日本企業を狙う標的型攻撃の印象的な事件

物理的なアプローチ
EDR未導入端末の保護

（予備セッション）
多要素認証を無力化する攻撃

多要素認証/MFAとは

1：IDとパスワードを入力する

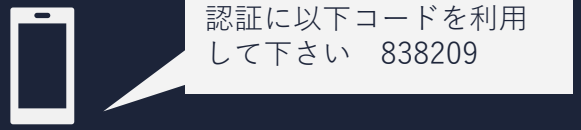


2：認証方式に応じて追加の認証操作が要求される

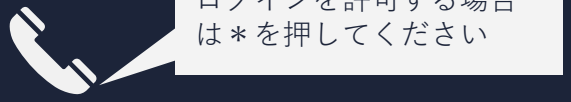
ワンタイムコード入力

モバイルアプリプッシュ通知

SMS経由ワンタイムコード



電話認証（機械音声）



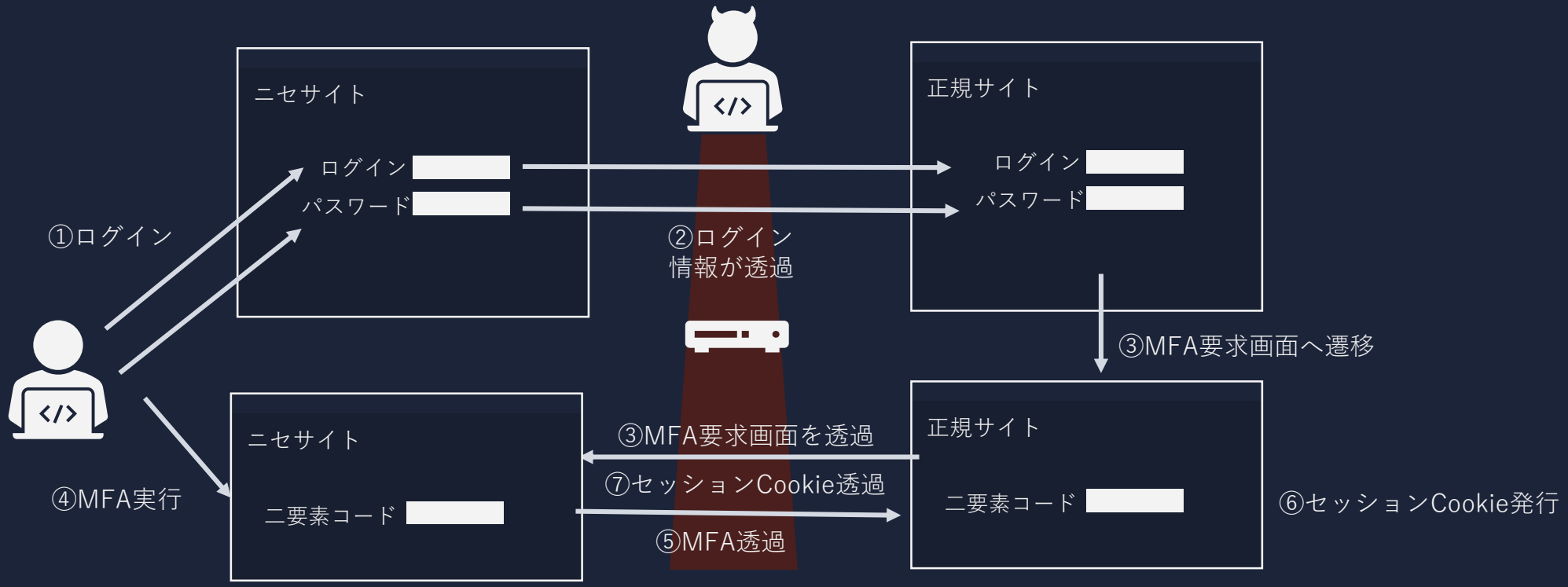
QRコード読み取り

デバイス証明書

生体認証（指紋等）

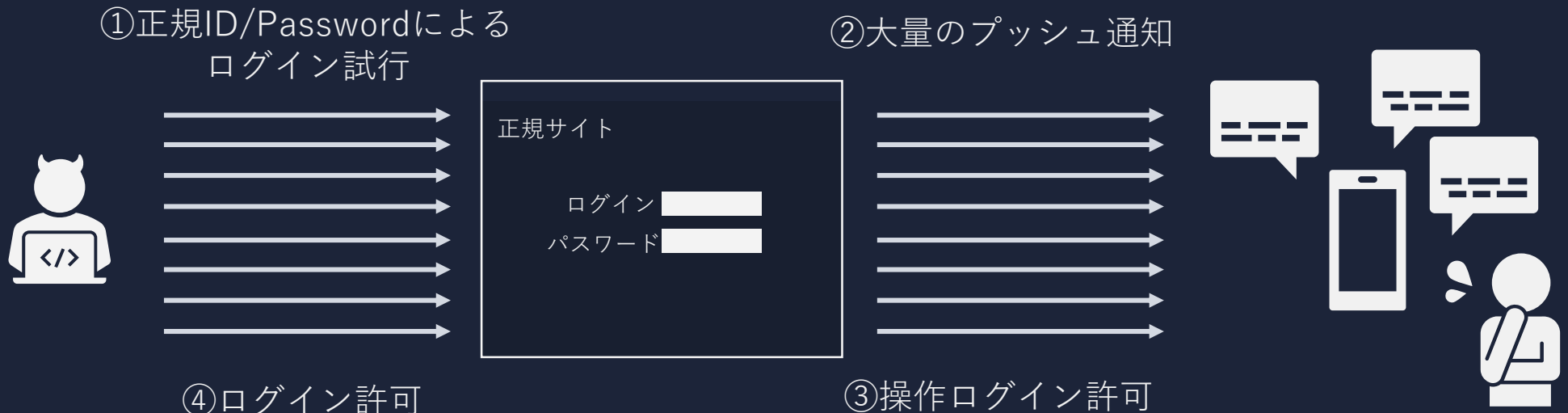
AiTM/Adversary-in-the-Middle

- 攻撃者が設置した**偽サイトがProxy的に動作**しておりユーザが入力したID/Passwordを正規サイトへ中継しつつ、MFA認証後に発行されるCookieも窃取する
- 攻撃者は窃取したCookieを利用しユーザのサービスにアクセスする手法
- 現在の**フィッシングサイトの多くはAiTMの機能を有している**ため種類によってはMFAが有効打とならずに自社のM365のテナント等への侵入が行われてしまう



MFA疲労攻撃（MFA Fatigue）/MFA爆撃（MFA bombing attacks）

- ユーザがログインを許可するまで**MFAリクエストを送り続ける**手法
- 一時期この手法が流行し被害が多発していたが現在はサービス側で対処され減少傾向
- 見覚えのないログイン承認要求は拒否するようなユーザ教育は継続して必要



※攻撃者が正規のITスタッフを装い利用者へ
連絡して認証の許可操作を迫ることもあり

2022年8月 Cisco：従業員が個人Googleアカウント侵害＋MFA疲労＋ヴィッシングで攻撃を受けるCisco社内のデータが窃取されリーク
https://blog.talosintelligence.com/2022/08/recent-cyber-attack.html
2022年9月 Uber：外部委託先のカスタマー サポート エンジニアのアカウントをMFA疲労＋ヴィッシングで侵害VPN経由で社内の様々なシステム情報が暴露される
https://www.uber.com/newsroom/security-update/

多要素認証を回避する手法まとめ

当日配布資料でのみ掲載

AiTMについての対策案

当日配布資料でのみ掲載

Co.Tomorrowing

MACNICA