

# 公開情報により攻撃動向の予測を行う 新たな試みと調査手法の共有

2023/1/25  
株式会社マクニカ  
瀬治山 豊

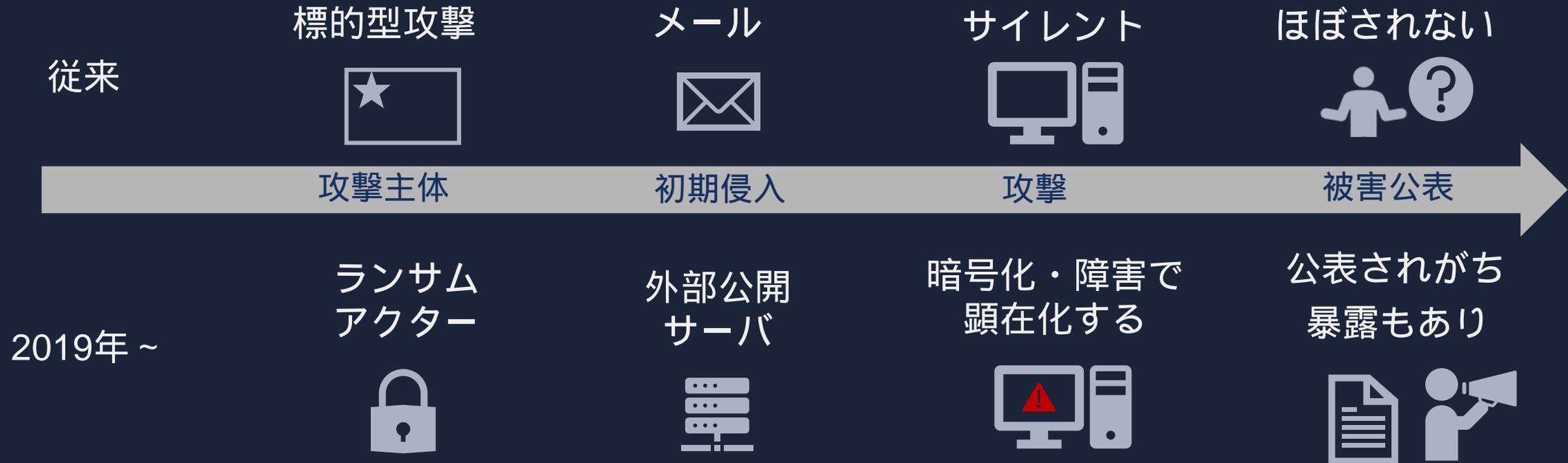
# 自己紹介

## 瀬治山 豊 Yutaka Sejiyama

- ✓ セキュリティ脅威動向の情報収集と発信
  - ・脆弱性関連の脅威動向リサーチ
  - ・Twitter @nekono\_naha
  - ・ばらまきメール回収の会
  - ・(ISC)2 Japan Chapter Annual Conference 2022
- ✓ マクニカグループ グローバルCSIRT担当者
  - ・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



# この数年の大きな潮流の変化



様々な面でインシデント情報が表に出る傾向になっている。  
公開情報の活用により攻撃の傾向や戦術変化が捉えられる可能性がある？

# 本セッションのアジェンダ

- ✓ 第1部 昨今のインシデント発生傾向分析
  - ・ランサムギャングによるリーク情報
  - ・日系企業の被害プレスリリース
  - ・セキュリティ機関/ベンダの公開レポート
- ✓ 第2部 外部公開アセットの管理状況の変化
  - ・RDPの公開状況
  - ・サポート切れOSの利用
  - ・脆弱性対処スピードの変化（2020年と2022年の比較）
  - ・日系企業の対策状況
- ✓ 第3部 攻撃者の戦術変化を捉える試み
  - ・過去調査事例（Pandora、AvosLocker、Deadbolt）
  - ・デバイス検索エンジンでの調査方法の共有

# 本セッションのアジェンダ

## ✓ 第1部 昨今のインシデント発生傾向分析

- ・ランサムギャングによるリーク情報
- ・日系企業の被害プレスリリース
- ・セキュリティ機関/ベンダの公開レポート

## ✓ 第2部 外部公開アセットの管理状況の変化

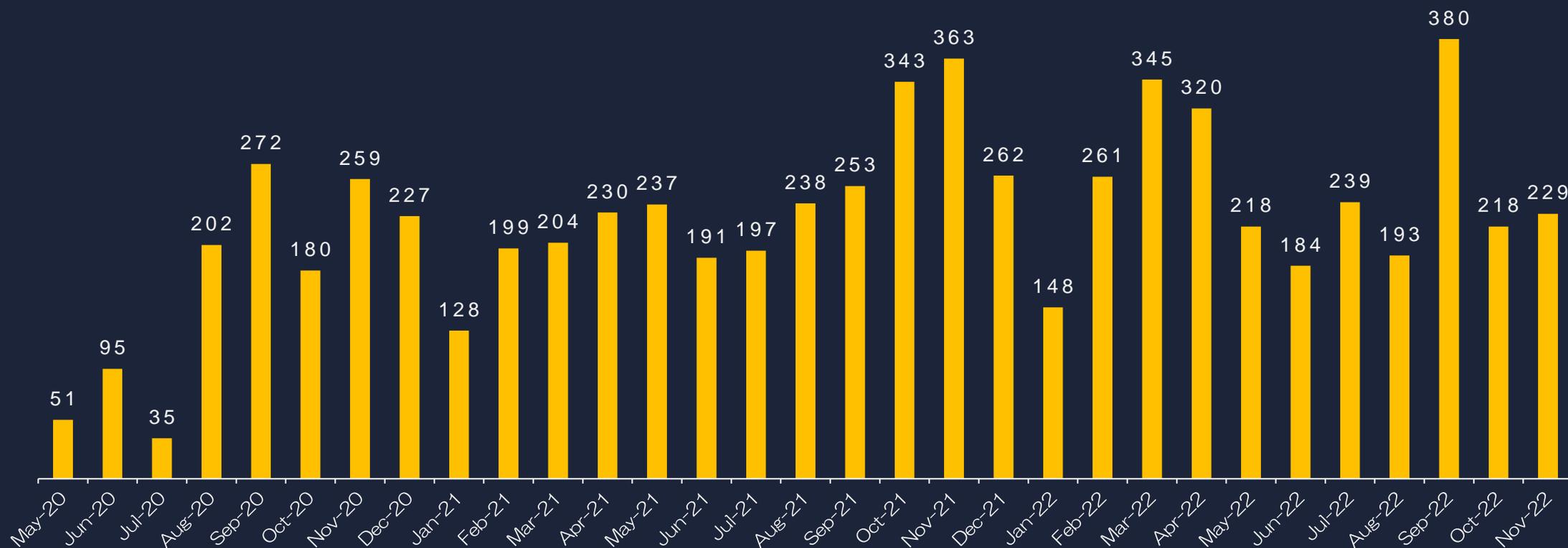
- ・RDPの公開状況
- ・サポート切れOSの利用
- ・脆弱性対処スピードの変化（2020年と2022年の比較）
- ・日系企業の対策状況

## ✓ 第3部 攻撃者の戦術変化を捉える試み

- ・過去調査事例（Pandora、AvosLocker、Deadbolt）
- ・デバイス検索エンジンでの調査方法の共有

# ランサムアクターによるグローバルでのリーク件数

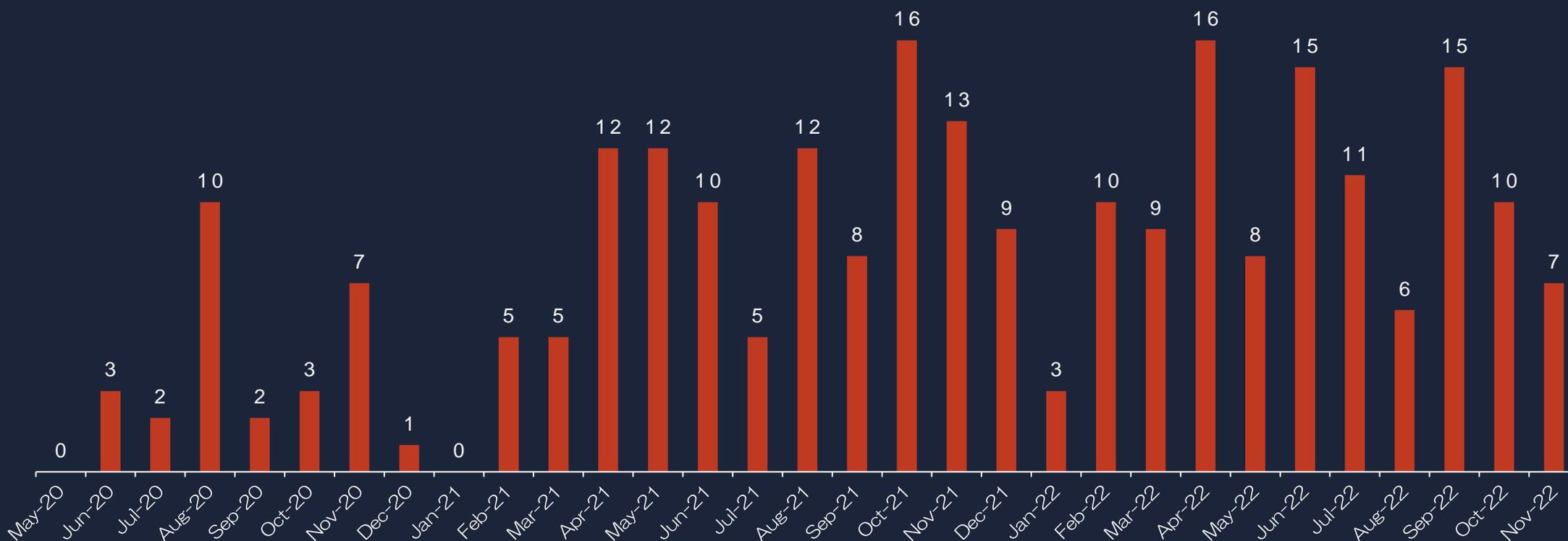
- ✓ 個別の企業や業種をターゲットにした標的型ランサム、データ暗号化と情報漏えいによる二重の脅迫を行う暴露型ランサムの被害が世界的に増加
- ✓ 2022年11月末時点で**約6932件**が暴露型ランサムの被害（リークサイトに掲載）にあっている  
インテリジェンスベンダDarkTracer (<https://darktracer.com/>)のデータを元に集計
- ✓ リークされていないランサムウェアの被害数も含めると被害企業は上記の数倍以上～にのぼる可能性がある



# 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**245件のセキュリティインシデント**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
- ・ 主にランサム系攻撃と極一部はAPTと思われる企業NW侵入型インシデントを集計  
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～2022年11月の31ヶ月間の集計
- ・ プレスリリースはGoogleアラート、ニュース、リサーチ情報 (@piyokango、@autumn\_good\_35) を活用し収集



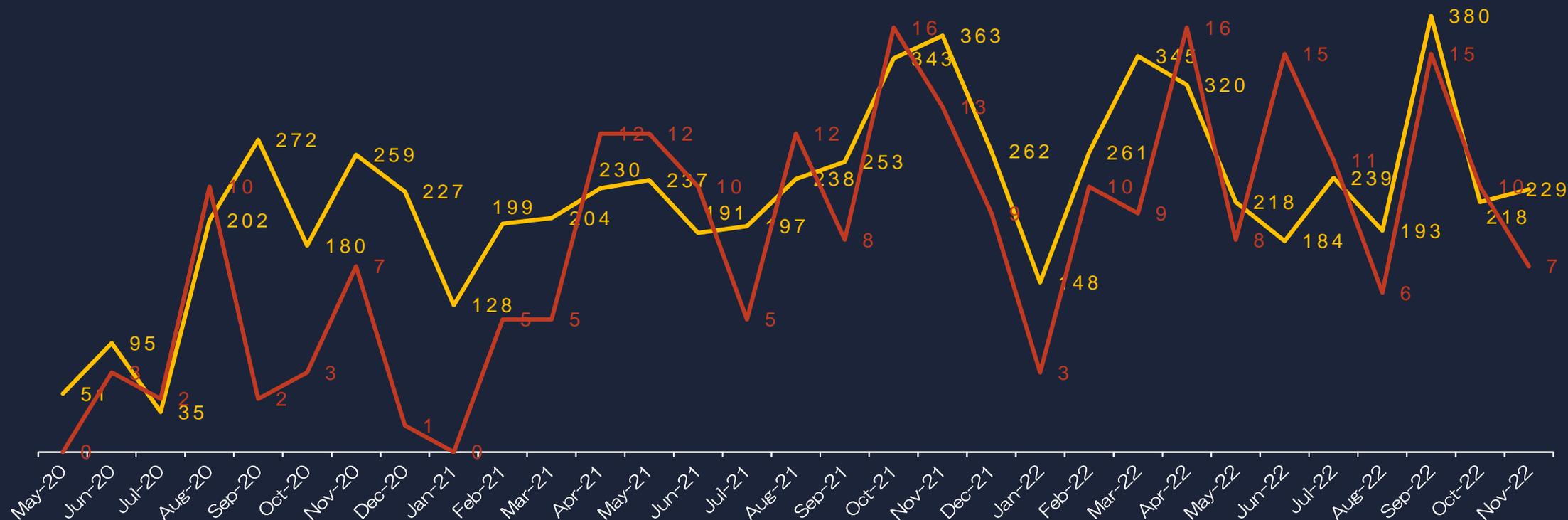
# インシデント発生傾向の比較

- 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

— グローバルでのリーク件数

— 日系企業のインシデント件数

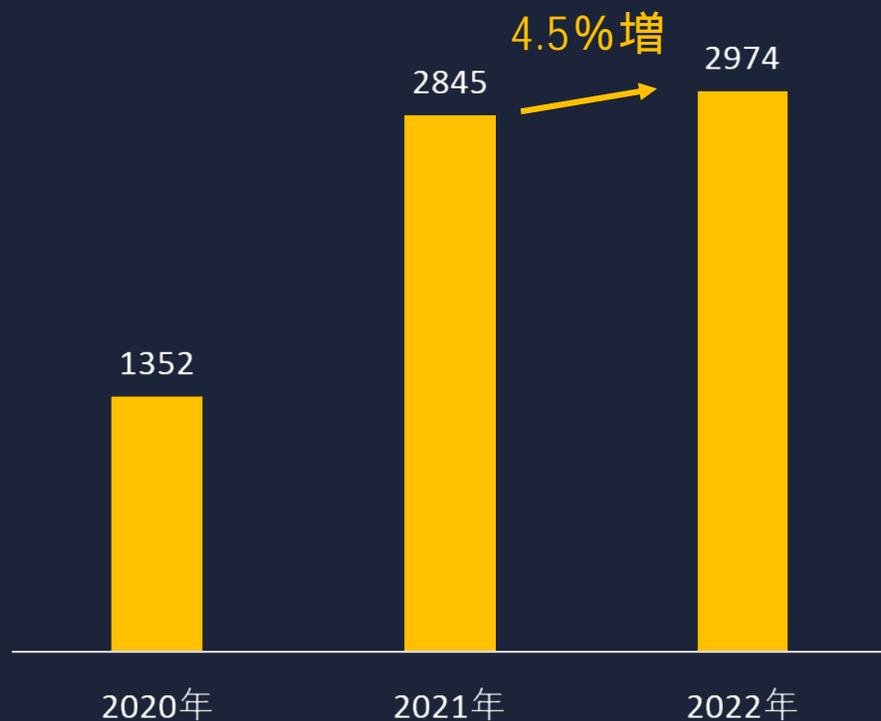


# インシデント発生傾向分析 このスライドのみ2022年12月の件数を含みます

- 2022年はグローバル、日本国内ともに被害件数が微増
- 日本はグローバルでの被害件数の伸びよりやや高い

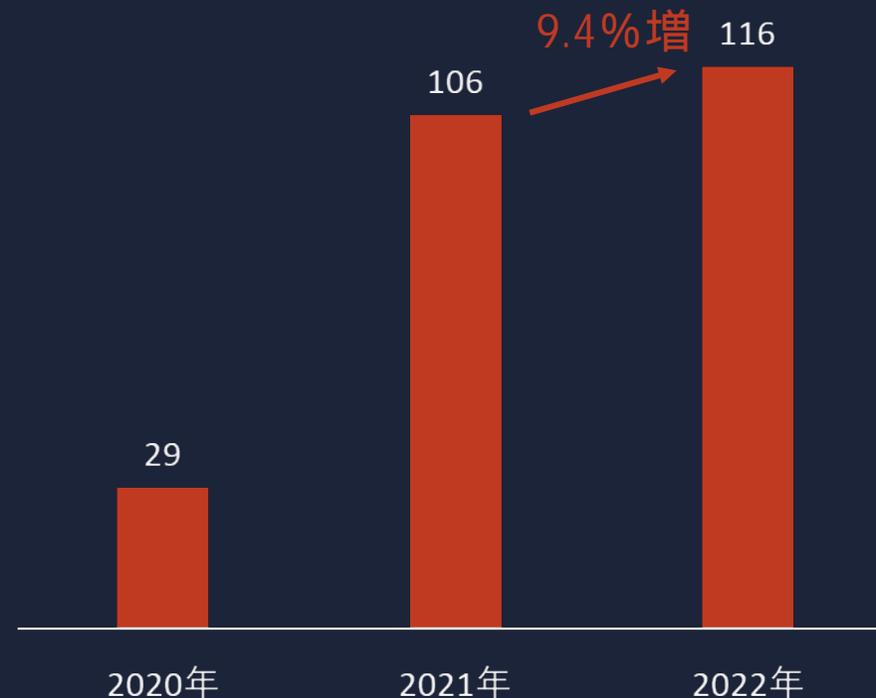
## ✓ グローバルでの件数（年毎）

2020年1月～2022年12月までの件数



## ✓ 日系組織での件数（年毎）

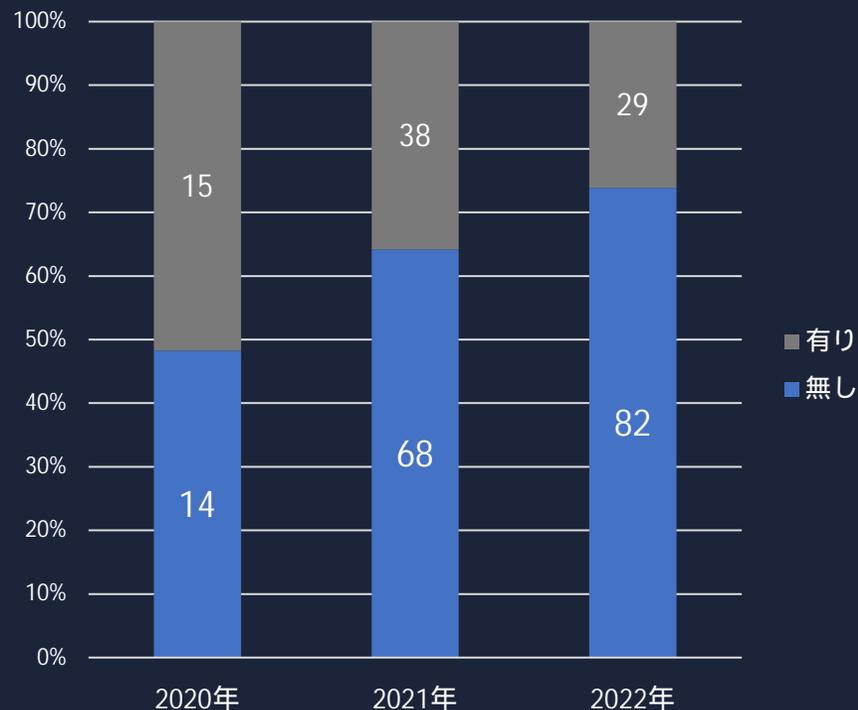
2022年は2023年1月3日までの判明分のため  
更に数件増加する可能性が高い



# 日系組織のインシデント発生傾向

- 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り、企業からの公表が増加
- 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も影響か

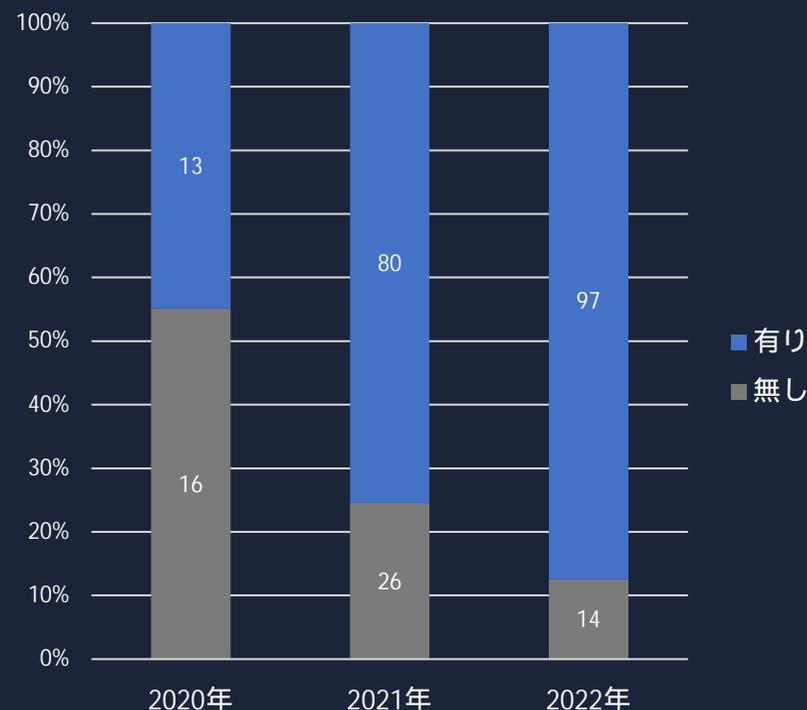
## ✓ 攻撃者による日系組織のリーク件数



約1/4しかリークされない 4倍すれば世界の被害総数？

\*2022年の被害総数2,275 × 4 = 9,100

## ✓ 日系組織のプレスリリースでの公表件数



約1/4しか公表しない\* 4倍すれば日本の被害総数？

\*ExtraHop 2022 CYBER CONFIDENCE INDEX:

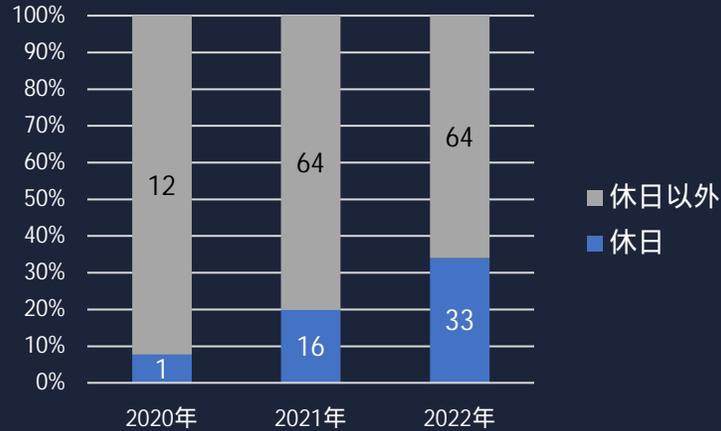
ASIA PACIFIC <https://assets.extrahop.com/pdfs/industry-reports/cyber-confidence-index-apac.pdf>

# 日系組織のプレスリリース分析

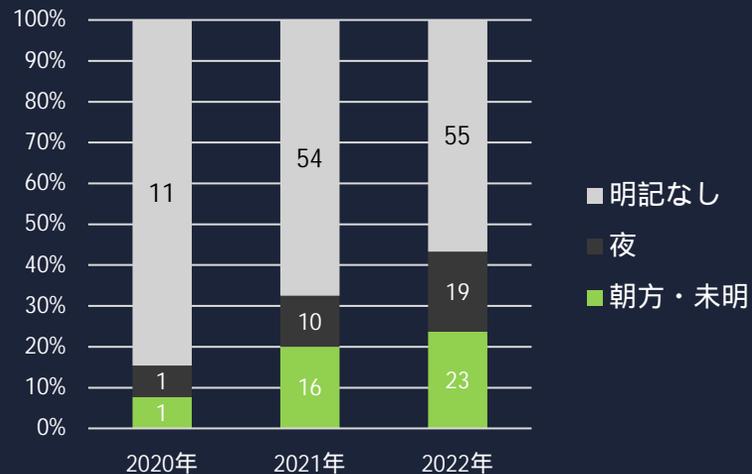
2020年4月～2022年11月公表のランサム系プレスリリース190件の分析

- 休日や祝日、夜間や早朝等の人が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

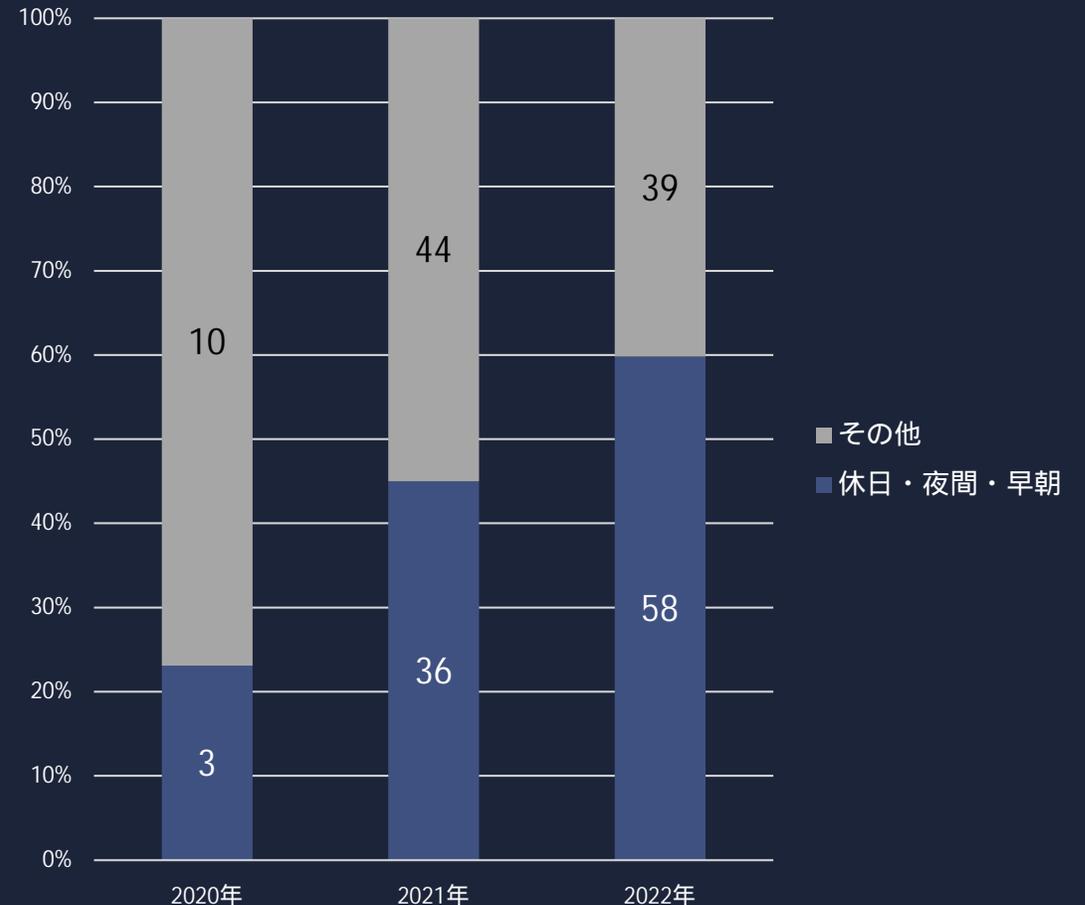
## ✓ 攻撃発生日



## ✓ 攻撃時間



## ✓ 夜間・早朝・休日等の攻撃

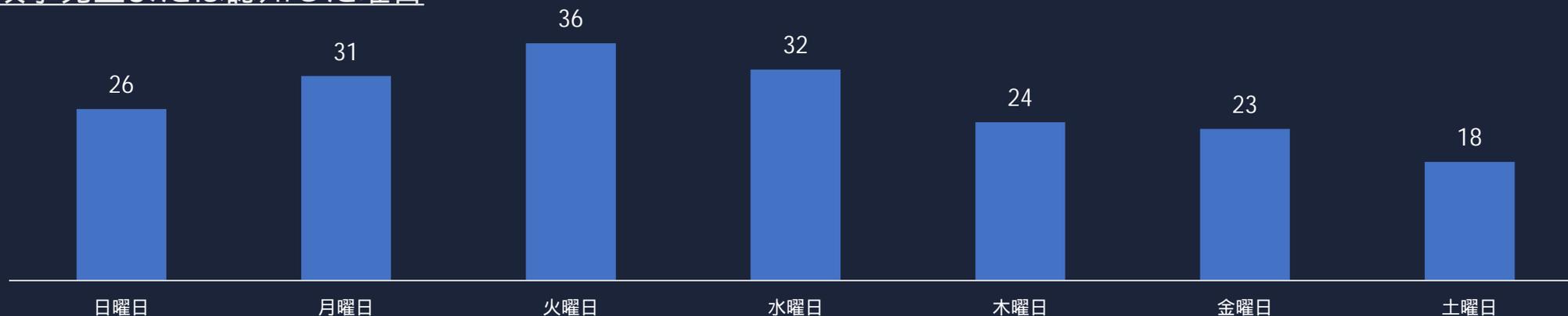


# 日系組織のプレスリリース分析

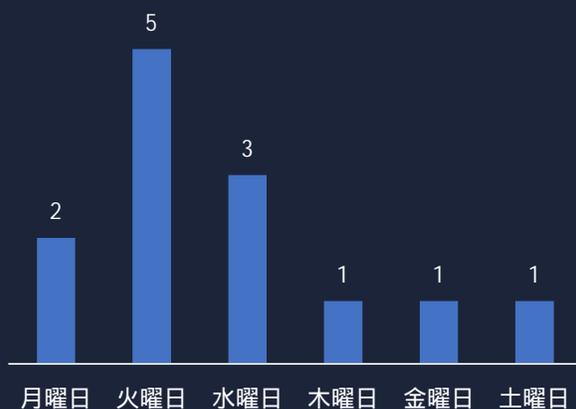
2020年4月～2022年11月公表のランサム系プレスリリース190件の分析

- 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
- 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

## ✓ 攻撃発生または認知した曜日



## ✓ 2020年



## ✓ 2021年



## ✓ 2022年

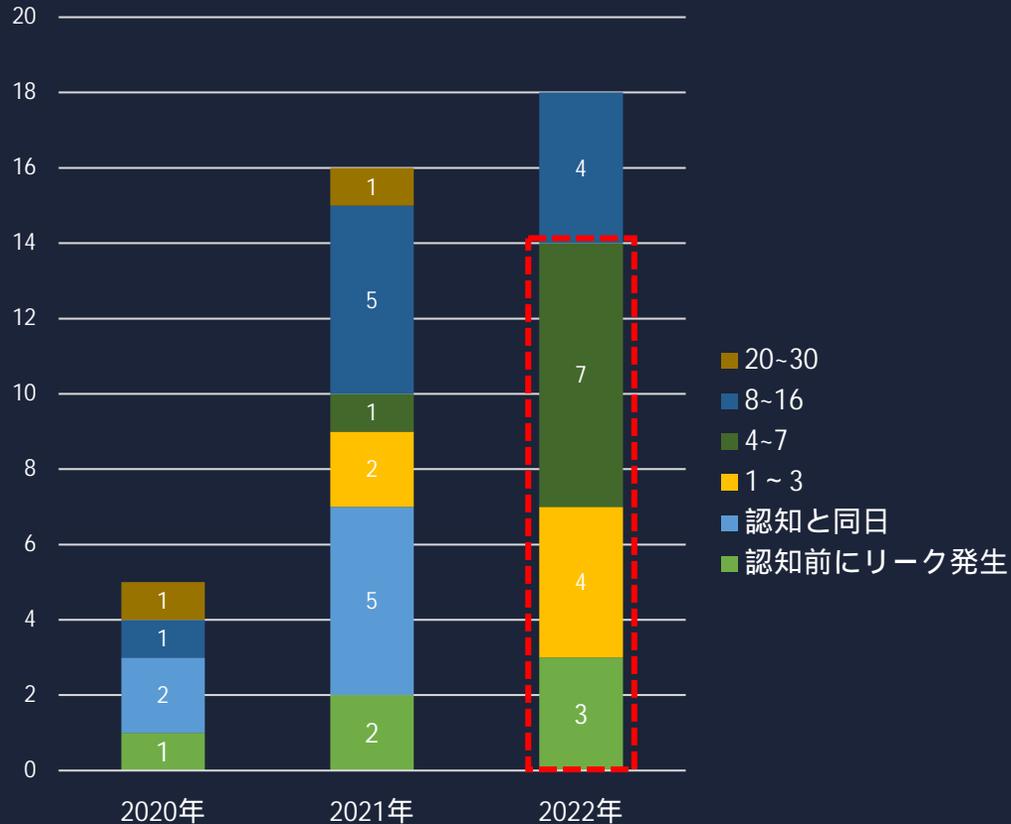


# 日系組織のプレスリリース分析

2020年4月～2022年11月公表のランサム系プレスリリース190件の分析

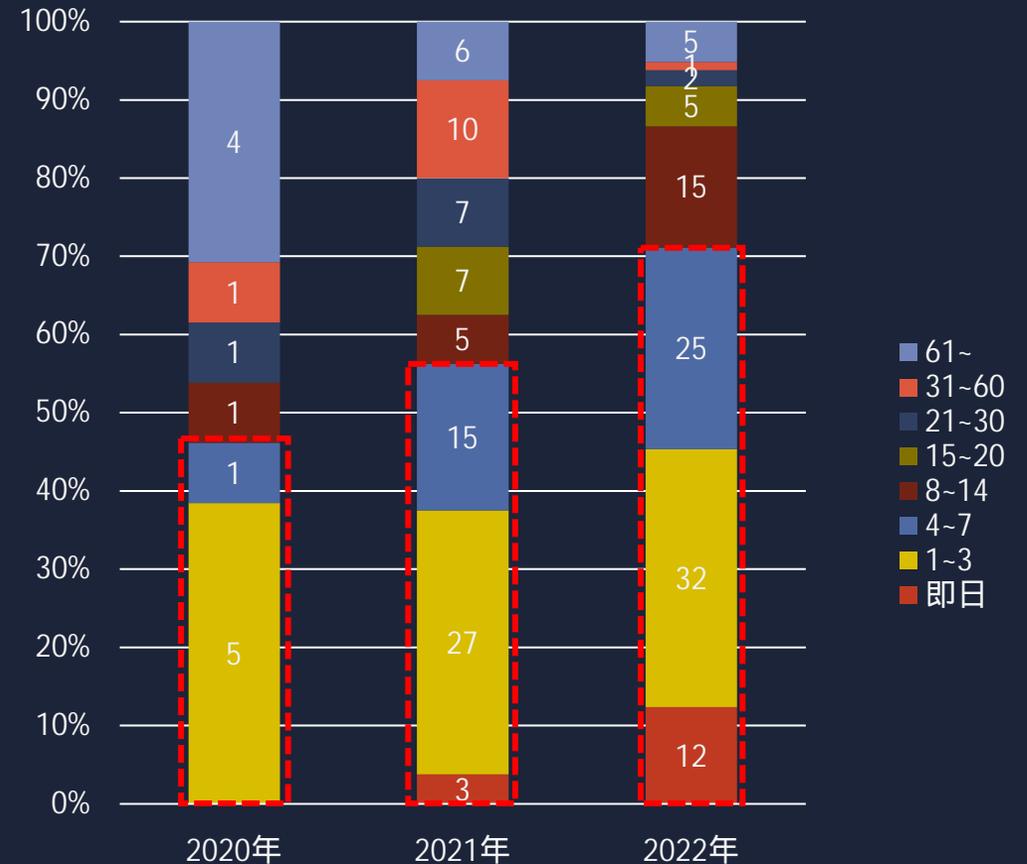
## ✓ 攻撃認知からリーク発生までの日数

リークされプレス公開もある39件を対象に集計



- 2022年は1週間以内にリーク（赤枠）されるケースが多い

## ✓ 攻撃認知からプレス公開までの日数

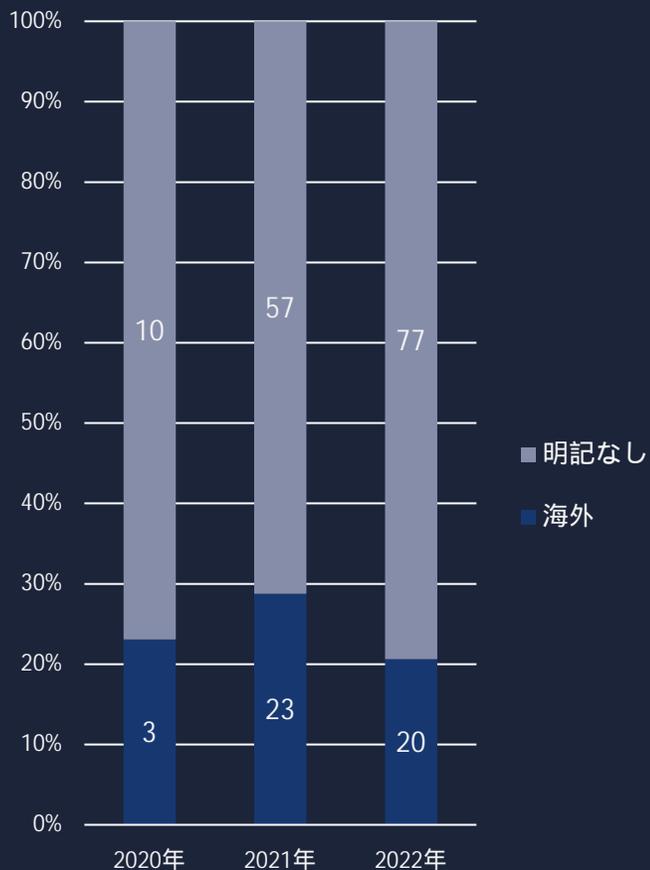


- 攻撃認知からプレスまでの間隔も短くなっている
- 2022年は7割が1週間以内（赤枠）に公表
- インシデント公表の心理的障壁低下や業務影響周知のためか

# 日系企業のプレスリリース内容分析

- 以前は約30%が海外被害だったが2022年は海外拠点の被害が明記される割合が20%まで低下している
- 攻撃者側の戦術の変化により標的が大企業中心から小規模組織へ移り変わり始めていることも一因か

## ✓ 被害拠点の明記



## ✓ 被害が発生した拠点の分布

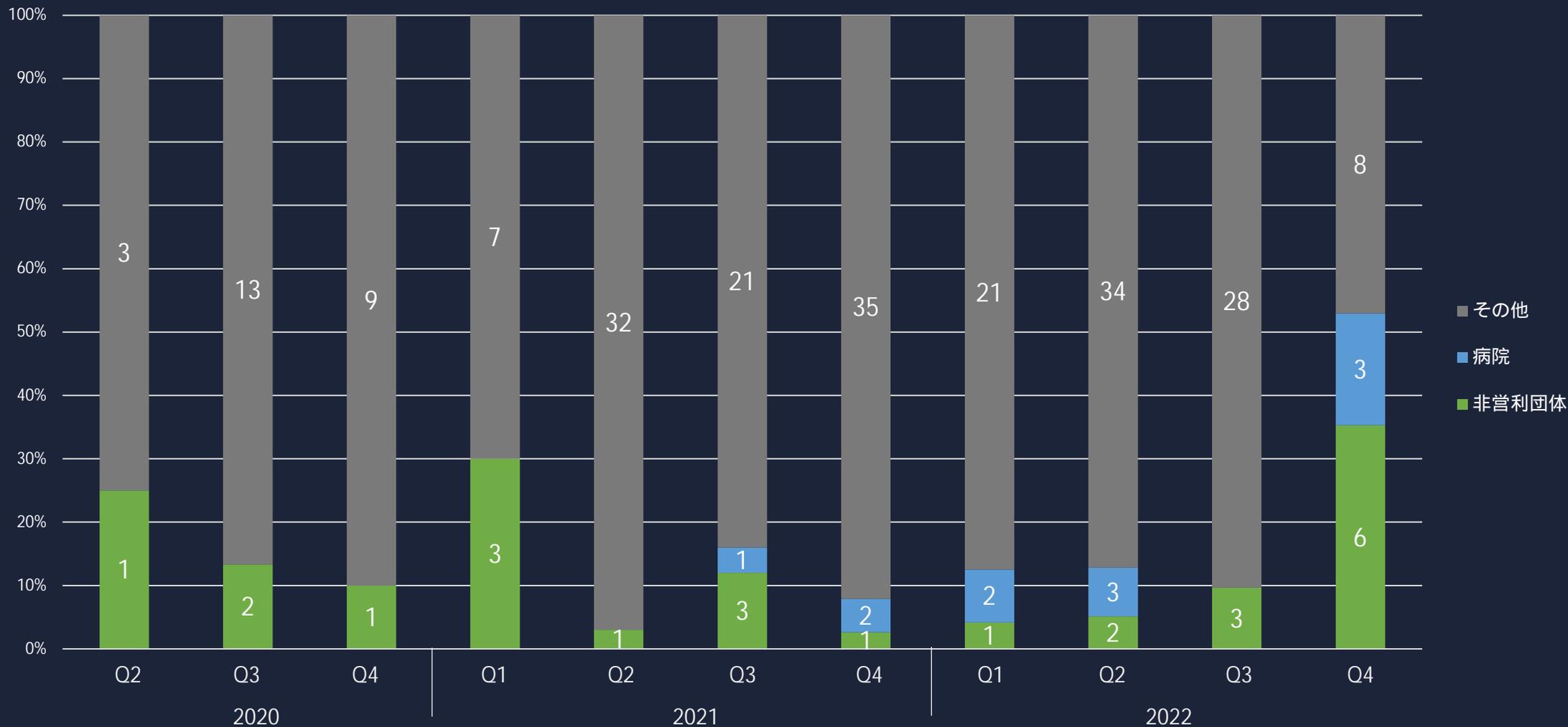
( ) 内はプレスは無いがリークによって判明した件数



# 日系企業のインシデント発生傾向

2020年4月～2022年11月に確認できるランサム系プレスリリース及びリーク情報245件の分析

- 以前2022年Q4は病院や非営利団体（組合、機構、協会、学校）の被害が多く発生している。
- 大規模組織の狙い撃ちではなく小規模組織狙い、または、流れ弾による被害の可能性もある。



# 外部公開アセット経由で発生するインシデントの割合

- 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）は少ない

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	
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%	<a href="https://www.secureworks.com/resources/p-state-of-the-threat-2022">https://www.secureworks.com/resources/p-state-of-the-threat-2022</a>
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%	<a href="https://www.trendmicro.com/ja_jp/research/22/j/fortinet.html">https://www.trendmicro.com/ja_jp/research/22/j/fortinet.html</a>
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%）	<a href="https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_kami_cyber_jousei.pdf">https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_kami_cyber_jousei.pdf</a>
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%+	<a href="https://www.coveware.com/blog/2022/7/27/fewer-ransomware-victims-pay-as-medium-ransom-falls-in-q2-2022">https://www.coveware.com/blog/2022/7/27/fewer-ransomware-victims-pay-as-medium-ransom-falls-in-q2-2022</a>
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%、その他 3%	<a href="https://unit42.paloaltonetworks.jp/incident-response-report/">https://unit42.paloaltonetworks.jp/incident-response-report/</a>
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%	<a href="https://news.sophos.com/en-us/2022/06/07/active-adversary-playbook-2022/">https://news.sophos.com/en-us/2022/06/07/active-adversary-playbook-2022/</a>
Arctic Wolf	2022年6月	Q1 2022 Incident Response Insights from Tetra Defense	82%	External Vulnerabilities 57% RDP 25%	—	<a href="https://arcticwolf.com/resources/blog/q1-2022-incident-response-insights-from-tetra-defense">https://arcticwolf.com/resources/blog/q1-2022-incident-response-insights-from-tetra-defense</a>
Group-IB	2022年5月	Ransomware Uncovered 2021/2022	68%	External remote services 47% Exploit public-facing application 21%	Phishing 26%、Other 6%	<a href="https://www.group-ib.com/media-center/press-releases/ransomware-2022/">https://www.group-ib.com/media-center/press-releases/ransomware-2022/</a>
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%）	<a href="https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf">https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf</a>
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%	<a href="https://www.ibm.com/reports/threat-intelligence/">https://www.ibm.com/reports/threat-intelligence/</a>
Kaspersky	2021年9月	Incident response analyst report	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%	<a href="https://media.kaspersky.com/jp/pdf/pr/Kaspersky_IRAnalystReport2020-PR-1056.pdf">https://media.kaspersky.com/jp/pdf/pr/Kaspersky_IRAnalystReport2020-PR-1056.pdf</a>
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%	<a href="https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound">https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound</a>

# 脆弱性悪用傾向に関する警告レポートの集計

- ここ数年の脆弱性悪用傾向に関するレポート25本を集計し製品毎の登場回数を調査  
NW製品やアンチウイルスでの脆弱性を突く通信の検知件数に関するレポートは除外しインシデント中での悪用情報のみを収集

No	発行期間	レポート名	発行時期	URL
1	CISA	CISA Alets	2022-2022	<a href="https://www.cisa.gov/uscert/ncas/alerts">https://www.cisa.gov/uscert/ncas/alerts</a>
2	Fortinet	Zerobot – New Go-Based Botnet Campaign Targets Multiple Vulnerabilities	Dec-22	<a href="https://www.fortinet.com/blog/threat-research/zerobot-new-go-based-botnet-campaign-targets-multiple-vulnerabilities">https://www.fortinet.com/blog/threat-research/zerobot-new-go-based-botnet-campaign-targets-multiple-vulnerabilities</a>
3	CISA	Iranian Government-Sponsored APT Actors Compromise Federal Network, Deploy Crypto Miner, Credential Harvester	Nov-22	<a href="https://www.cisa.gov/uscert/ncas/alerts/aa22-320a">https://www.cisa.gov/uscert/ncas/alerts/aa22-320a</a>
4	CISA	StopRansomware: Hive	Nov-22	<a href="https://www.cisa.gov/uscert/ncas/alerts/aa22-321a">https://www.cisa.gov/uscert/ncas/alerts/aa22-321a</a>
5	CISA	Top CVEs Actively Exploited By People’s Republic of China State-Sponsored Cyber Actors	Oct-22	<a href="https://www.cisa.gov/uscert/ncas/alerts/aa22-279a">https://www.cisa.gov/uscert/ncas/alerts/aa22-279a</a>
6	Arctic Wolf	Root Point Product of Compromise	Sep-22	<a href="https://arcticwolf.com/resources/blog/incident-response-insights-from-arctic-wolf-labs-1h-2022/">https://arcticwolf.com/resources/blog/incident-response-insights-from-arctic-wolf-labs-1h-2022/</a>
7	CISA	Iranian Islamic Revolutionary Guard Corps-Affiliated Cyber Actors Exploiting Vulnerabilities for Data Extortion and Disk Encryption for Ransom Operations	Sep-22	<a href="https://www.cisa.gov/uscert/ncas/alerts/aa22-257a">https://www.cisa.gov/uscert/ncas/alerts/aa22-257a</a>
8	Palo Alto	Unit 42	Jul-22	<a href="https://unit42.paloaltonetworks.jp/incident-response-report/">https://unit42.paloaltonetworks.jp/incident-response-report/</a>
9	Group IB	Ransomware Uncovered2021/2022	Jun-22	<a href="https://www.group-ib.com/resources/threat-research/ransomware-2022.html">https://www.group-ib.com/resources/threat-research/ransomware-2022.html</a>
10	CISA	People’s Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices	Jun-22	<a href="https://www.cisa.gov/uscert/ncas/alerts/aa22-158a">https://www.cisa.gov/uscert/ncas/alerts/aa22-158a</a>
11	IBM	X-Force Research Update: Top 10 Cybersecurity Vulnerabilities of 2021	May-22	<a href="https://securityintelligence.com/posts/x-force-top-10-cybersecurity-vulnerabilities-2021/">https://securityintelligence.com/posts/x-force-top-10-cybersecurity-vulnerabilities-2021/</a>
12	CISA	2021 Top Routinely Exploited Vulnerabilities	Apr-22	<a href="https://www.cisa.gov/uscert/ncas/alerts/aa22-117a">https://www.cisa.gov/uscert/ncas/alerts/aa22-117a</a>
13	Tenable	Behind the Scenes: How We Picked 2021’s Top Vulnerabilities – and What We Left Out	Mar-22	<a href="https://www.tenable.com/blog/behind-the-scenes-how-we-picked-2021s-top-vulnerabilities-and-what-we-left-out">https://www.tenable.com/blog/behind-the-scenes-how-we-picked-2021s-top-vulnerabilities-and-what-we-left-out</a>
14	ANSSI	Panorama de la menace informatique 2021	Mar-22	<a href="https://www.cert.ssi.gouv.fr/uploads/20220309_NP_WHITE_ANSSI_pano-rama-menace-ANSSI.pdf">https://www.cert.ssi.gouv.fr/uploads/20220309_NP_WHITE_ANSSI_pano-rama-menace-ANSSI.pdf</a>
15	CISA	Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure	Jan-22	<a href="https://www.cisa.gov/uscert/ncas/alerts/aa22-011a">https://www.cisa.gov/uscert/ncas/alerts/aa22-011a</a>
16	Recorded Future	2021 Vulnerability Landscape	Jan-22	<a href="https://go.recordedfuture.com/hubfs/reports/cta-2022-0210.pdf">https://go.recordedfuture.com/hubfs/reports/cta-2022-0210.pdf</a>
17	CISA	Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities	Nov-21	<a href="https://www.cisa.gov/uscert/ncas/alerts/aa21-321a">https://www.cisa.gov/uscert/ncas/alerts/aa21-321a</a>
18	Twitter	Top Critical Vulnerabilities Used by Ransomware Groups	Sep-21	<a href="https://twitter.com/uuallan/status/1438899102448820224">https://twitter.com/uuallan/status/1438899102448820224</a>
19	CISA	Top Routinely Exploited Vulnerabilities	Jul-21	<a href="https://www.cisa.gov/uscert/ncas/alerts/aa21-209a">https://www.cisa.gov/uscert/ncas/alerts/aa21-209a</a>
20	NISC	ランサムウェアによるサイバー攻撃に関する注意喚起について	Apr-21	<a href="https://www.nisc.go.jp/pdf/policy/infra/ransomware20210430.pdf">https://www.nisc.go.jp/pdf/policy/infra/ransomware20210430.pdf</a>
21	Tenable	IN THE 2020 THREAT LANDSCAPE RETROSPECTIVE (TLR), YOU WILL READ ABOUT:	Jan-21	<a href="https://www.tenable.com/cyber-exposure/2020-threat-landscape-retrospective">https://www.tenable.com/cyber-exposure/2020-threat-landscape-retrospective</a>
22	CISA	Russian State-Sponsored Advanced Persistent Threat Actor Compromises U.S. Government Targets	Oct-20	<a href="https://www.cisa.gov/uscert/ncas/alerts/aa20-296a">https://www.cisa.gov/uscert/ncas/alerts/aa20-296a</a>
23	CISA	APT Actors Chaining Vulnerabilities Against SLTT, Critical Infrastructure, and Elections Organizations	Oct-20	<a href="https://www.cisa.gov/uscert/ncas/alerts/aa20-283a">https://www.cisa.gov/uscert/ncas/alerts/aa20-283a</a>
24	CISA	Potential for China Cyber Response to Heightened U.S.–China Tensions	Oct-20	<a href="https://www.cisa.gov/uscert/ncas/alerts/aa20-275a">https://www.cisa.gov/uscert/ncas/alerts/aa20-275a</a>
25	CISA	Chinese Ministry of State Security-Affiliated Cyber Threat Actor Activity	Sep-20	<a href="https://www.cisa.gov/uscert/ncas/alerts/aa20-258a">https://www.cisa.gov/uscert/ncas/alerts/aa20-258a</a>



# 脆弱性悪用傾向に関する警告レポートの集計

- ここ数年の脆弱性悪用傾向に関するレポート25本を集計し製品毎の登場回数（黄色字）を調査  
NW製品やアンチウイルスでの脆弱性を突く通信の検知件数に関するレポートは除外しインシデント中での悪用情報のみを収集

Product	回数	レポート番号																								
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Atlassian Confluence Server and Data Center	5					CVE-2022-26134, CVE-2021-26084				CVE-2021-26084			CVE-2021-26084						CVE-2021-26084							CVE-2019-3396
Cisco	5					CVE-2021-1497						CVE-2018-0171, CVE-2019-1652, CVE-2019-15271		CVE-2018-0171			CVE-2019-1653								CVE-2019-1652, CVE-2019-1653, CVE-2020-3118	
MobileIron	4													CVE-2020-15505						CVE 2020-15505					CVE-2020-15505	CVE-2020-15505
QNAP QTS and QuTS hero	4											CVE-2019-7192, CVE-2019-7193, CVE-2019-7194, CVE-2019-7195		CVE-2020-2509					CVE-2020-36198, CVE-2021-28799				CVE-2021-28799, CVE-2020-36195, CVE-2020-2509			
Exim	3																CVE-2019-10149							CVE-2019-10149	CVE-2018-6789	
D-Link	3		CVE-2020-25506									CVE-2019-16920													CVE-2019-16920	
Atlassian Crowd and Crowd Data Center	2																			CVE-2019-11580					CVE-2019-11580	
DrayTek	2											CVE-2020-8515													CVE-2020-8515	
GitLab CE/EE	2					CVE-2021-22205														CVE-2021-22205						
Kaseya VSA	2									CVE-2021-30116										CVE-2021-30116, CVE-2021-30119, CVE-2021-30120						



# 本セッションのアジェンダ

## ✓ 第1部 昨今のインシデント発生傾向分析

- ・ランサムギャングによるリーク情報
- ・日系企業の被害プレスリリース
- ・セキュリティ機関/ベンダの公開レポート

## ✓ 第2部 外部公開アセットの管理状況の変化

- ・RDPの公開状況
- ・サポート切れOSの利用
- ・脆弱性対処スピードの変化（2020年と2022年の比較）
- ・日系企業の対策状況

## ✓ 第3部 攻撃者の戦術変化を捉える試み

- ・過去調査事例（Pandora、AvosLocker、Deadbolt）
- ・デバイス検索エンジンでの調査方法の共有

# RDP 3389/TCPに関する調査



✓ Shodanを用いて外部にRDP ( 3389/TCP ) を公開するサーバやPCの台数を調査

- グローバルでは430万件、国内では約12万台が公開されている。
- 日本国内ではコロナ禍前後で大きく増加傾向だったが2021年3月の143,671件をピークに減少傾向である、
- 個人利用PCも多いが明確に企業利用のPCも少なくとも500社以上分が確認できる。

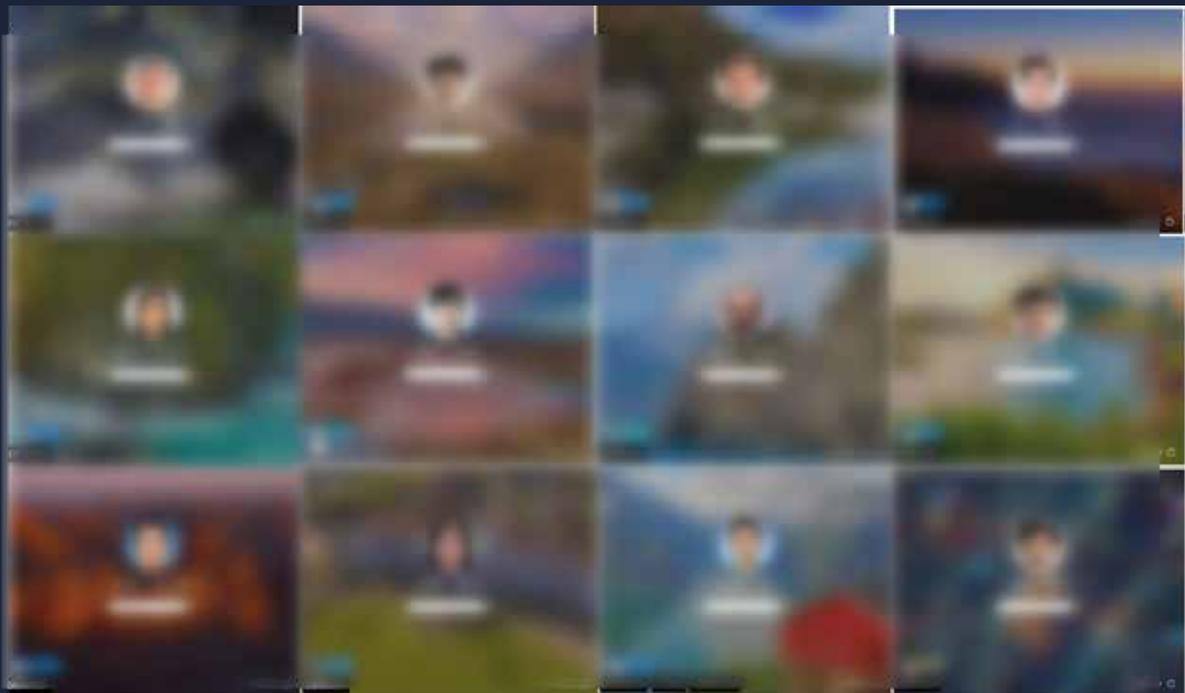
✓ 3389/TCPの公開台数が多い国 TOP30

Country	Nov-2019	May-2020	Nov-2020	May-2021	Nov-2021	May-2022	Nov-2022	増減
— Global	5,548,173	5,246,373	4,574,509	5,326,991	4,872,514	4,629,133	4,329,536	-22%
1 United States	2,465,109	1,775,745	1,512,654	1,675,269	1,641,343	1,398,938	1,281,178	-48%
2 China	1,252,901	1,485,333	1,137,537	1,412,295	1,274,560	1,216,480	1,234,529	-1%
3 Germany	157,910	195,439	190,848	224,883	213,436	219,561	204,047	29%
4 <b>Japan</b>	<b>95,499</b>	<b>106,456</b>	<b>109,979</b>	<b>128,105</b>	<b>127,740</b>	<b>122,696</b>	<b>120,375</b>	<b>26%</b>
5 Netherlands	108,227	123,904	117,754	150,779	135,745	126,445	112,322	4%
6 UK	97,892	110,345	128,085	135,266	118,249	123,375	105,318	8%
7 Hong Kong	64,445	83,439	81,176	140,919	122,775	121,117	95,544	48%
8 Singapore	63,051	71,371	81,654	87,687	109,980	117,955	92,763	47%
9 Russia	99,283	108,936	107,153	125,012	112,107	103,944	90,156	-9%
10 Korea	87,110	98,430	89,274	104,676	91,285	103,532	85,012	-2%
11 France	95,681	106,573	108,828	146,557	82,744	89,499	82,128	-14%
12 India	49,107	54,196	56,413	69,310	72,923	79,263	81,815	67%
13 Brazil	104,606	112,926	87,252	90,793	73,802	72,023	67,068	-36%
14 Canada	68,073	69,149	65,763	88,981	73,978	72,836	60,859	-11%
15 Turkey	30,524	32,263	31,373	36,956	33,772	37,466	40,698	33%
16 Australia	43,427	46,921	51,000	51,995	45,711	65,386	39,161	-10%
17 Viet Nam	28,953	37,532	40,616	40,645	33,046	37,219	36,841	27%
18 Ireland	40,246	45,590	41,571	40,719	39,349	36,558	34,615	-14%
19 Israel	6,593	7,679	12,518	14,220	13,437	5,888	32,191	388%
20 Italy	38,898	41,578	36,864	40,957	31,942	32,524	29,236	-25%
21 Taiwan	46,139	45,088	40,318	40,986	31,095	32,476	29,230	-37%
22 Mexico	34,758	36,284	31,550	35,846	28,361	28,606	25,544	-27%
23 Spain	37,627	38,960	35,146	35,042	27,731	28,133	24,951	-34%
24 Thailand	21,275	25,777	21,326	24,589	21,950	22,896	21,978	3%
25 South Africa	30,225	24,397	19,389	21,142	17,313	17,751	17,178	-43%
26 Finland	6,934	9,007	10,533	16,307	15,287	16,730	16,758	142%
27 Poland	19,691	18,470	22,515	23,356	17,513	18,511	16,648	-15%
28 Indonesia	10,851	12,377	11,823	14,502	16,861	13,963	15,647	44%
29 Sweden	15,115	14,339	14,255	15,210	13,813	17,553	14,646	-3%
30 Czechia	19,281	18,646	16,928	16,949	14,633	13,963	13,587	-30%

# RDP 3389/TCPに関する調査

- ・NW情報などからテレワーク利用のSIM付PCと思われるものも3000台以上が確認可能

## ✓ 某A社のテレワークPC



## ✓ 某B社のテレワークPC

The screenshot displays a network analysis tool interface with the following data:

- TOTAL RESULTS:** 1,143
- TOP CITIES:**

Tokyo	268
Yokohama	225
Osaka	89
Fukuoka	75
Kawasaki	14
More...	
- TOP ORGANIZATIONS:**

Internet	1,119
Internet (Mobile)	21
Internet (Mobile)	3
- TOP OPERATING SYSTEMS:**

Windows (Build 10.0.19041)	812
Windows (Build 10.0.17763)	264
Windows (Build 10.0.14393)	58
Windows (Build 6.3.9600)	2

Additional details shown include:

- SSL Certificate:** Issued By: self-signed, Issued To: self-signed, Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2.
- Device Info:** Windows 10/Windows Server (version 20H1), Build: 10.0.19041.

# サポート切れWindows OSに関する調査

- ✓ Shodanを用いて外部公開サーバーのバナー中のIISバージョンからWindows Versionを推測しサポート切れ台数を調査
  - グローバルでは132万台が公開され、日本国内では約1万4千台（世界15位の台数）が確認できる
  - 2019年11月と2022年11月の台数を比較するとアジア圏は軒並み減少率が良くない

## IIS6.0

Windows 2003 Server /2015年7月EOL

```
HTTP/1.1 404 Not Found
Date: Thu, 22 Dec 2022 11:05:23 GMT
Server: Microsoft-IIS/6.0
X-UA-Compatible: IE=emulateIE7
X-Powered-By: ASP.NET
Content-Length: 2320
```

## IIS7.0

Windows Server 2008/2020年1月EOL

```
HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Wed, 03 Jun 2009 19:16:59 GMT
Accept-Ranges: bytes
ETag: "85ea41de7fe4c91:0"
Server: Microsoft-IIS/7.0
X-Powered-By: ASP.NET
```

## IIS7.5

Windows Server 2008 R2/2020年1月EOL

```
HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Mon, 27 Jul 2020 10:46:27 GMT
Accept-Ranges: bytes
ETag: "b7ab512e354c51:0"
Server: Microsoft-IIS/7.5
```

## ✓ 台数が多い国 TOP30

	Country	Nov-2019	Nov-2020	Nov-2021	Nov-2022
-	Global	5,500,255	2,945,700	1,824,451	1,323,633
1	China	774,106	641,059	595,457	493,195
2	United States	2,532,017	1,179,770	464,793	267,506
3	Hong Kong	439,127	253,189	184,906	155,440
4	Korea	54,005	43,262	40,050	31,894
5	Germany	108,929	67,073	41,567	28,097
6	United Kingdom	96,194	57,877	35,205	24,441
7	Brazil	39,669	28,709	26,012	16,954
8	Taiwan	34,680	27,580	21,784	16,457
9	Russian Federation	42,891	25,668	22,133	16,390
10	Italy	36,255	35,095	23,007	16,177
11	Canada	54,564	36,209	24,249	15,776
12	Australia	54,620	35,652	20,983	15,047
13	India	52,305	23,670	21,235	14,841
14	Malaysia	17,225	15,359	19,530	14,662
<b>15</b>	<b>Japan</b>	<b>32,103</b>	<b>30,691</b>	<b>30,880</b>	<b>13,932</b>
16	France	38,415	31,900	18,905	12,923
17	Argentina	16,165	15,008	13,578	11,121
18	Singapore	19,026	24,818	7,480	9,079
19	Netherlands	43,270	27,106	12,646	9,042
20	Spain	22,457	15,991	12,153	8,987
21	Mexico	19,867	14,399	11,100	8,449
22	South Africa	628,316	82,357	7,945	8,187
23	Turkey	23,963	21,369	12,560	7,974
24	Thailand	13,758	9,801	9,602	7,962
25	Indonesia	11,815	5,810	5,333	5,592
26	Iran	20,750	10,840	10,839	5,482
27	Viet Nam	10,617	8,815	6,918	5,004
28	Ireland	13,862	9,514	7,459	4,828
29	Sweden	14,402	9,737	6,833	4,088
30	Czechia	11,354	7,582	5,750	3,913

## ✓ 減少率が悪い順

	Country	増減率
1	Malaysia	-15%
2	Argentina	-31%
3	China	-36%
4	Korea	-41%
5	Thailand	-42%
6	Singapore	-52%
7	Taiwan	-53%
8	Indonesia	-53%
9	Viet Nam	-53%
10	Italy	-55%
<b>11</b>	<b>Japan</b>	<b>-57%</b>
12	Brazil	-57%
13	Mexico	-57%
14	Spain	-60%
15	Russian Federation	-62%
16	Hong Kong	-65%
17	Ireland	-65%
18	Czechia	-66%
19	France	-66%
20	Turkey	-67%
21	Canada	-71%
22	Sweden	-72%
23	India	-72%
24	Australia	-72%
25	Iran	-74%
26	Germany	-74%
27	United Kingdom	-75%
-	Global	-76%
28	Netherlands	-79%
29	United States	-89%
30	South Africa	-99%

# サポート切れCentOSに関する調査

- ✓ Shodanを用いて外部公開サーバーのバナー中のApacheバージョンからCentOS Versionを推測しサポート切れ台数を調査
  - グローバルでは約38万台が公開され、日本国内では約7万台超（世界2位の台数）が確認できる
  - CentOS5系は国内で約2万台弱があり世界で最も多い

## Apache/2.2.3 (CentOS) CentOS 5/2017年EOL

```
HTTP/1.1 200 OK
Date: Thu, 22 Dec 2022 23:53:01 GMT
Server: Apache/2.2.3 (CentOS)
X-Powered-By: PHP/5.4.31
Content-Language: sl
Content-Length: 1401
Connection: close
Content-Type: text/html; charset=UTF-8
```

## Apache/2.2.15 (CentOS) CentOS 6/2020年EOL

```
HTTP/1.1 403 Forbidden
Date: Thu, 22 Dec 2022 23:25:04 GMT
Server: Apache/2.2.15 (CentOS)
Accept-Ranges: bytes
Content-Length: 4861
Connection: close
Content-Type: text/html; charset=UTF-8
```

## ✓ 台数が多い国 TOP30

	Country	Nov-2019	Nov-2020	Nov-2021	Nov-2022
-	Global	1,138,405	993,855	570,403	378,597
1	United States	361,371	273,302	151,814	96,675
2	Japan	132,819	113,143	94,122	71,338
3	Russian Federation	54,011	61,206	26,318	17,264
4	France	38,811	34,308	21,912	16,778
5	China	54,530	40,911	24,467	14,973
6	Korea, Republic of	20,895	21,251	16,349	14,082
7	Italy	18,685	21,392	14,894	11,248
8	Canada	48,816	27,309	16,311	10,679
9	Germany	40,460	36,758	22,471	9,994
10	United Kingdom	39,284	33,149	15,410	9,734
11	Taiwan	11,618	12,811	9,205	7,704
12	Ukraine	20,407	21,921	19,063	7,671
13	Brazil	17,541	15,268	9,751	6,707
14	Netherlands	26,970	23,528	10,267	6,097
15	India	30,809	28,609	14,021	5,164
16	Hong Kong	11,904	11,212	6,575	4,728
17	Thailand	7,102	6,090	5,235	4,157
18	Singapore	14,146	17,709	5,272	4,123
19	Spain	9,470	7,683	4,721	3,419
20	Malaysia	4,788	4,388	3,312	3,344
21	Indonesia	8,239	6,020	3,925	3,112
22	Mexico	5,262	2,968	2,491	3,101
23	Czechia	7,227	5,979	3,607	2,897
24	Romania	10,125	7,356	4,539	2,571
25	Argentina	4,105	2,891	2,551	2,355
26	Australia	8,972	6,414	3,665	2,276
27	Turkey	14,703	22,119	3,222	2,221
28	Poland	7,148	6,069	4,990	1,967
29	Bulgaria	6,248	3,449	3,524	1,839
30	Viet Nam	5,466	5,599	2,214	1,656

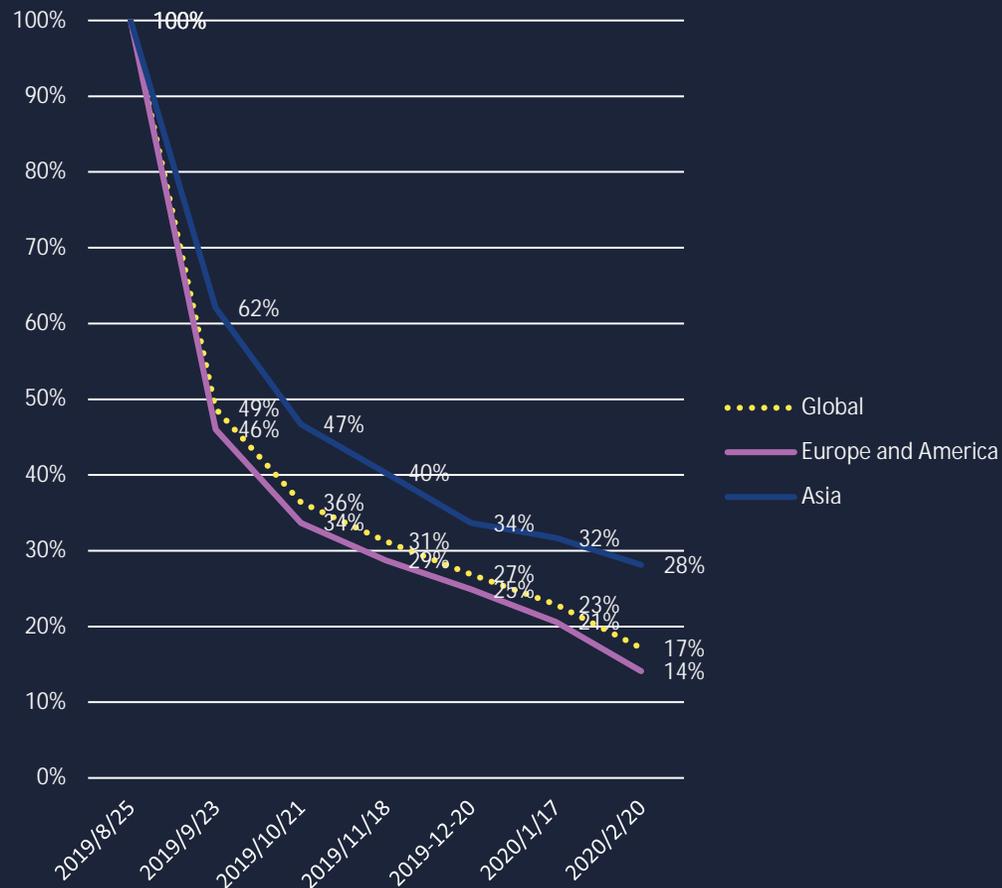
## ✓ 減少率が悪い順

	Country	増減率
1	Malaysia	-30%
2	Korea	-33%
3	Taiwan	-34%
4	Italy	-40%
5	Mexico	-41%
6	Thailand	-41%
7	Argentina	-43%
8	Japan	-46%
9	France	-57%
10	Czechia	-60%
11	Hong Kong	-60%
12	Brazil	-62%
13	Indonesia	-62%
14	Ukraine	-62%
15	Spain	-64%
16	Global	-67%
17	Russian Federation	-68%
18	Viet Nam	-70%
19	Bulgaria	-71%
20	Singapore	-71%
21	Poland	-72%
22	China	-73%
23	United States	-73%
24	Romania	-75%
25	Australia	-75%
26	United Kingdom	-75%
27	Germany	-75%
-	Netherlands	-77%
28	Canada	-78%
29	India	-83%
30	Turkey	-85%

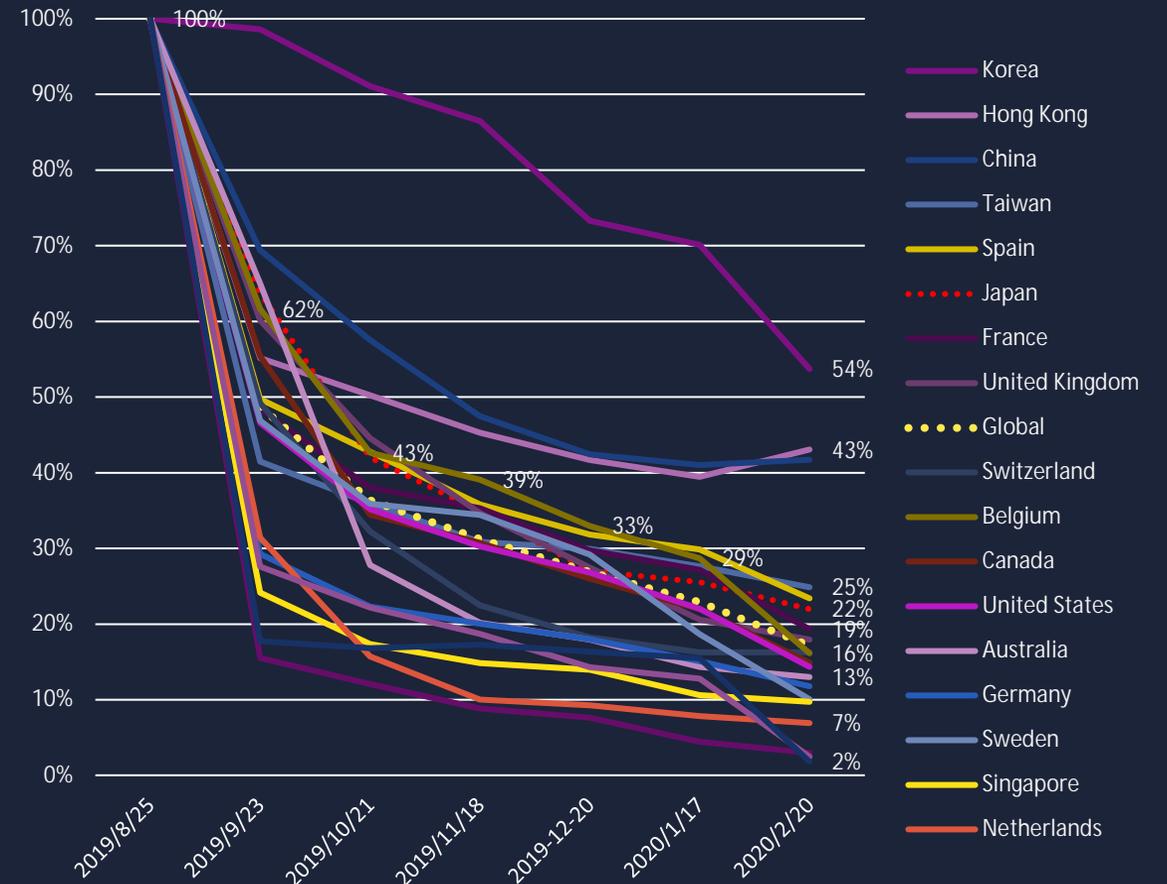
# Pulse Secure/CVE-2019-11510の脆弱性の国別対策傾向

- 2019年4月にパッチが公開、同年8月のBlackHat等でのDEVCORE Orange氏による発表を受け攻撃が増加
- Bad Packets社 (@bad\_packets) 公開のスキャンデータをもとに地域・国別の対策スピードを集計
- 欧米の国は対処が早くアジア圏は遅い。日本はグローバル平均よりやや遅いペースで対処が進んでいることがわかる。

✓ 脆弱サーバの割合推移（地域別）



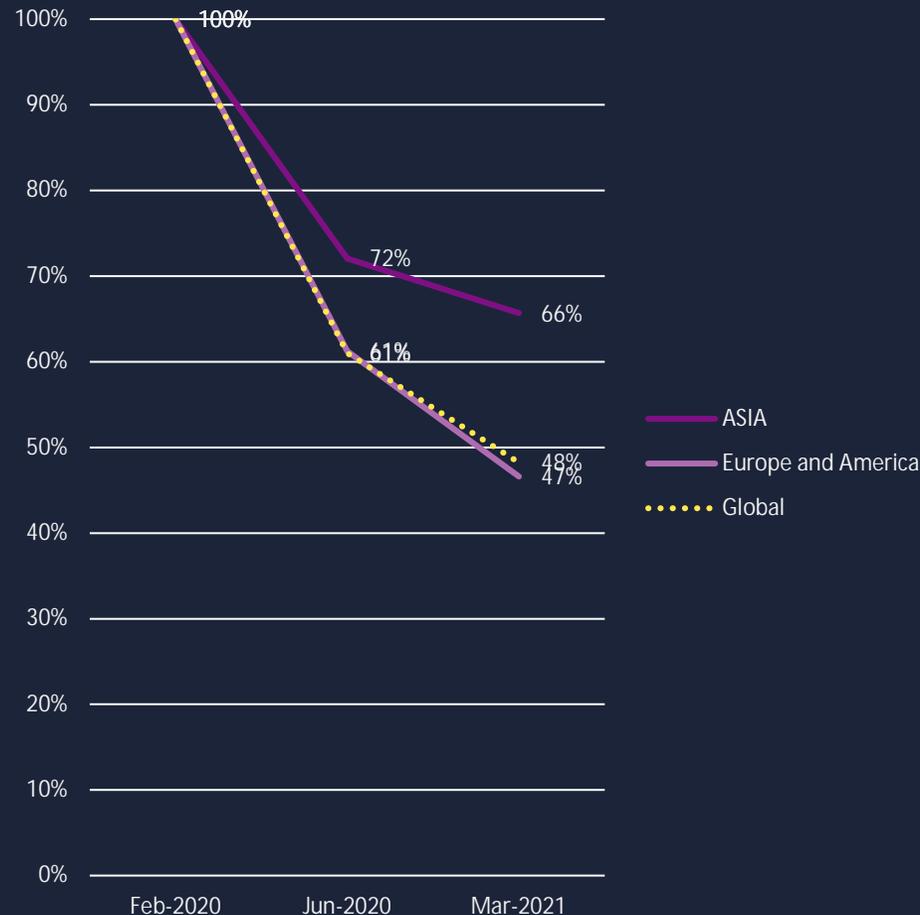
✓ 脆弱サーバの割合推移（国別）



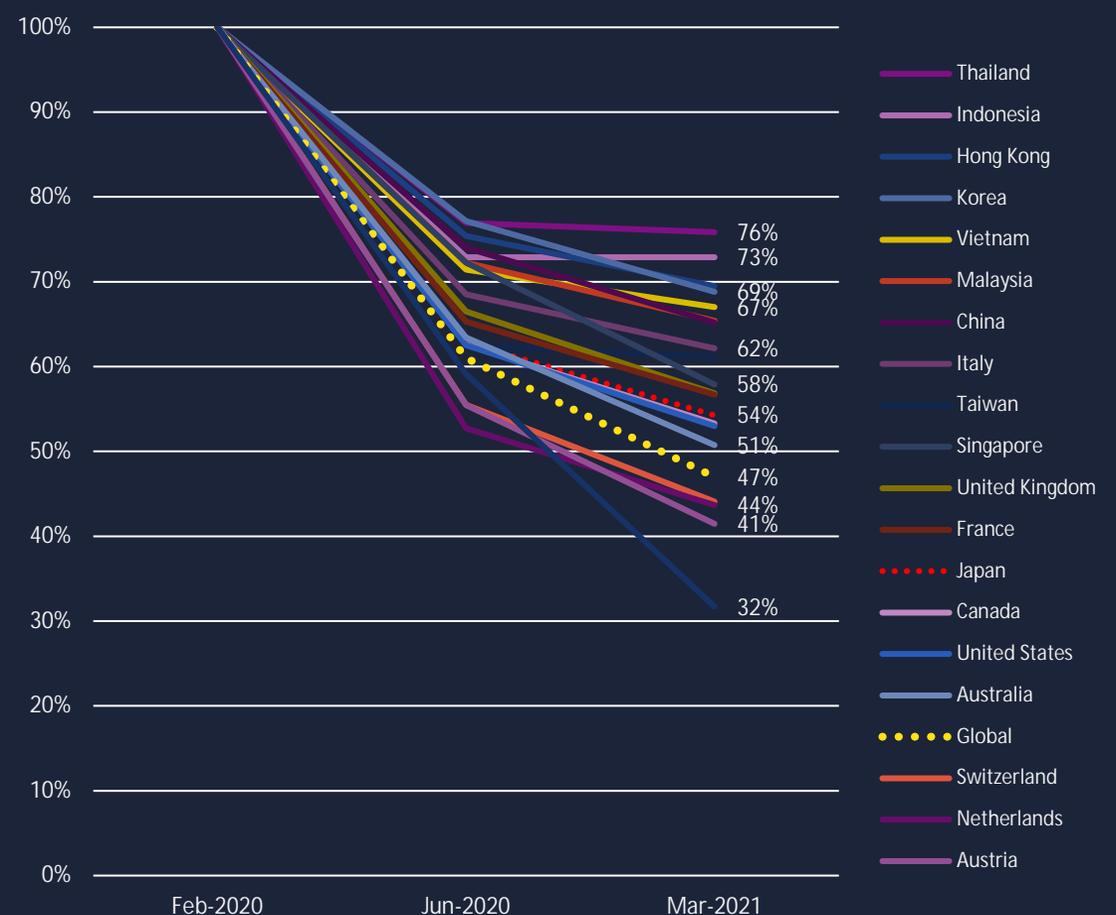
# Exchange Server/CVE-2020-0688の脆弱性の国別対策傾向

- 2020年2月25日にパッチが公開、同年3月頃から攻撃活動が活発に観測されはじめる
- 欧米圏は半年で39%、1年で52%のサーバが対処されたが、アジア圏は半年で28%、1年で34%だった

✓脆弱サーバの割合推移（地域別）



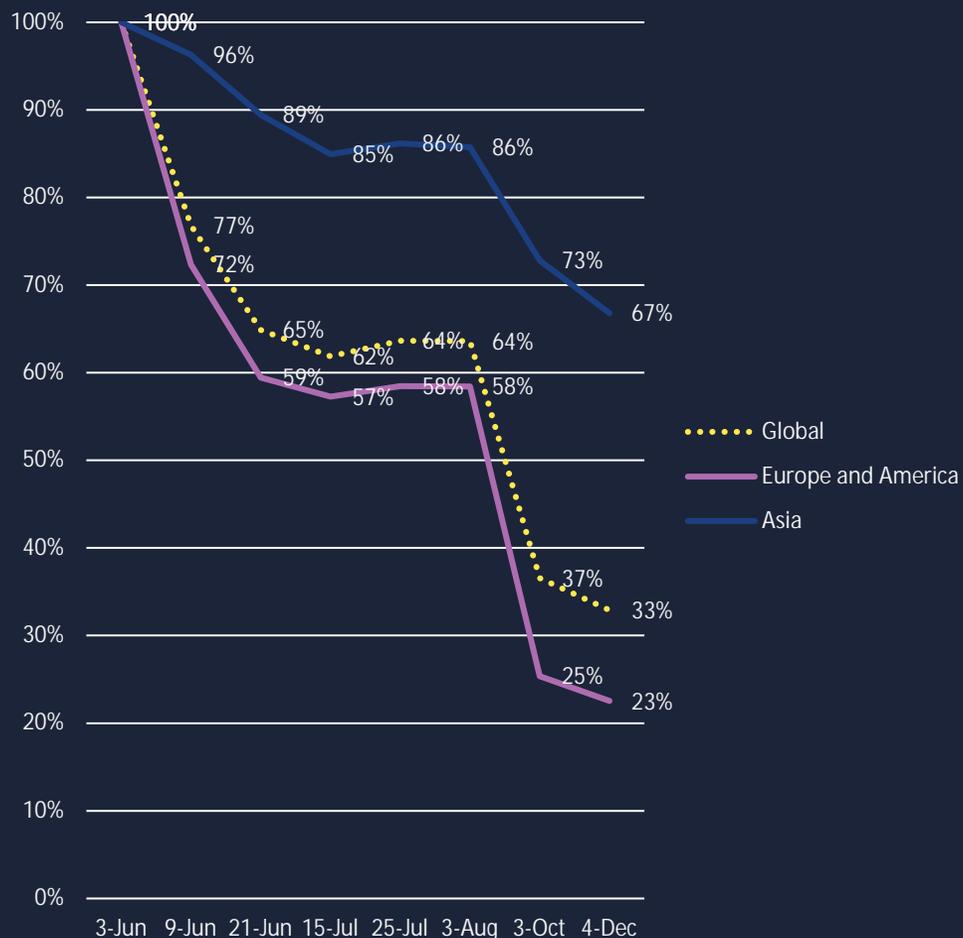
✓脆弱サーバの割合推移（国別）



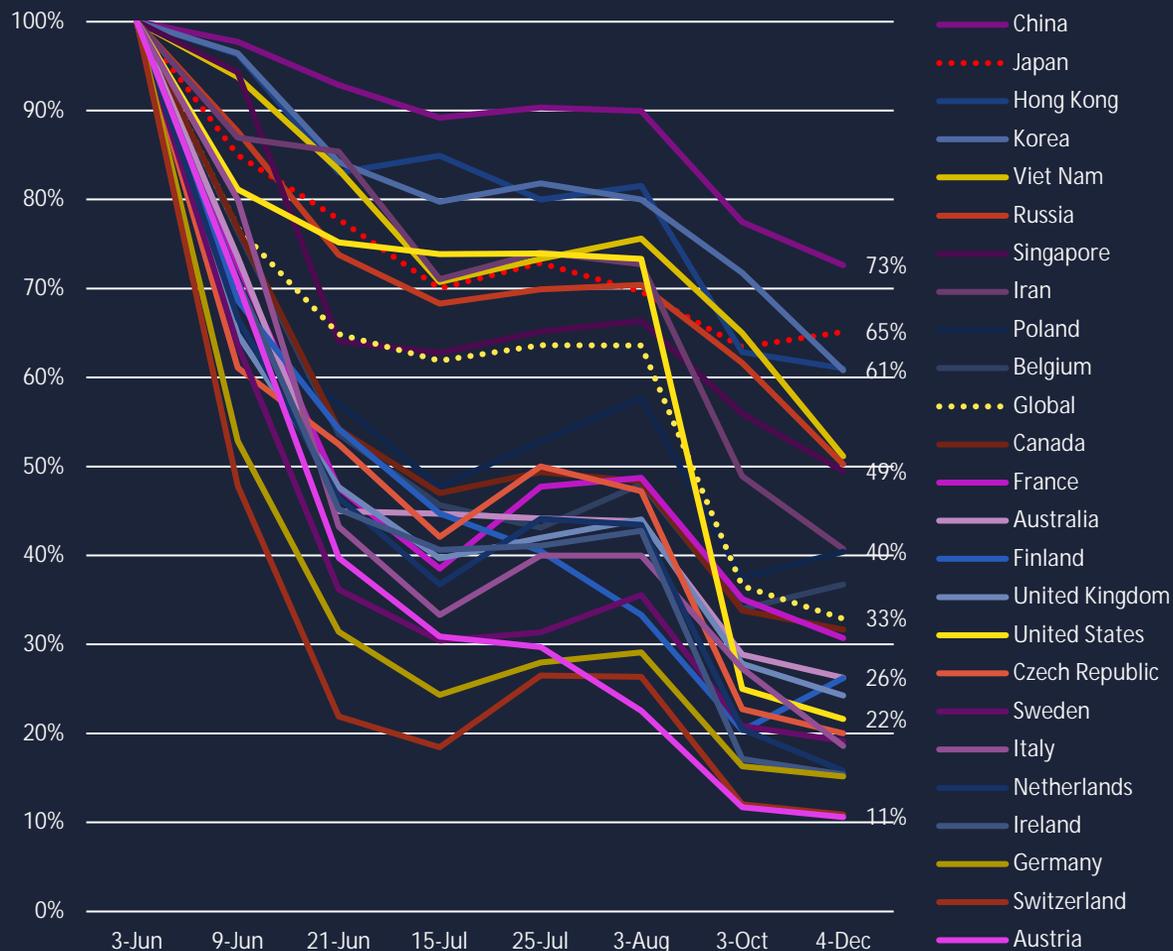
# Atlassian Confluence/CVE-2022-26134の脆弱性の国別対策傾向

- 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

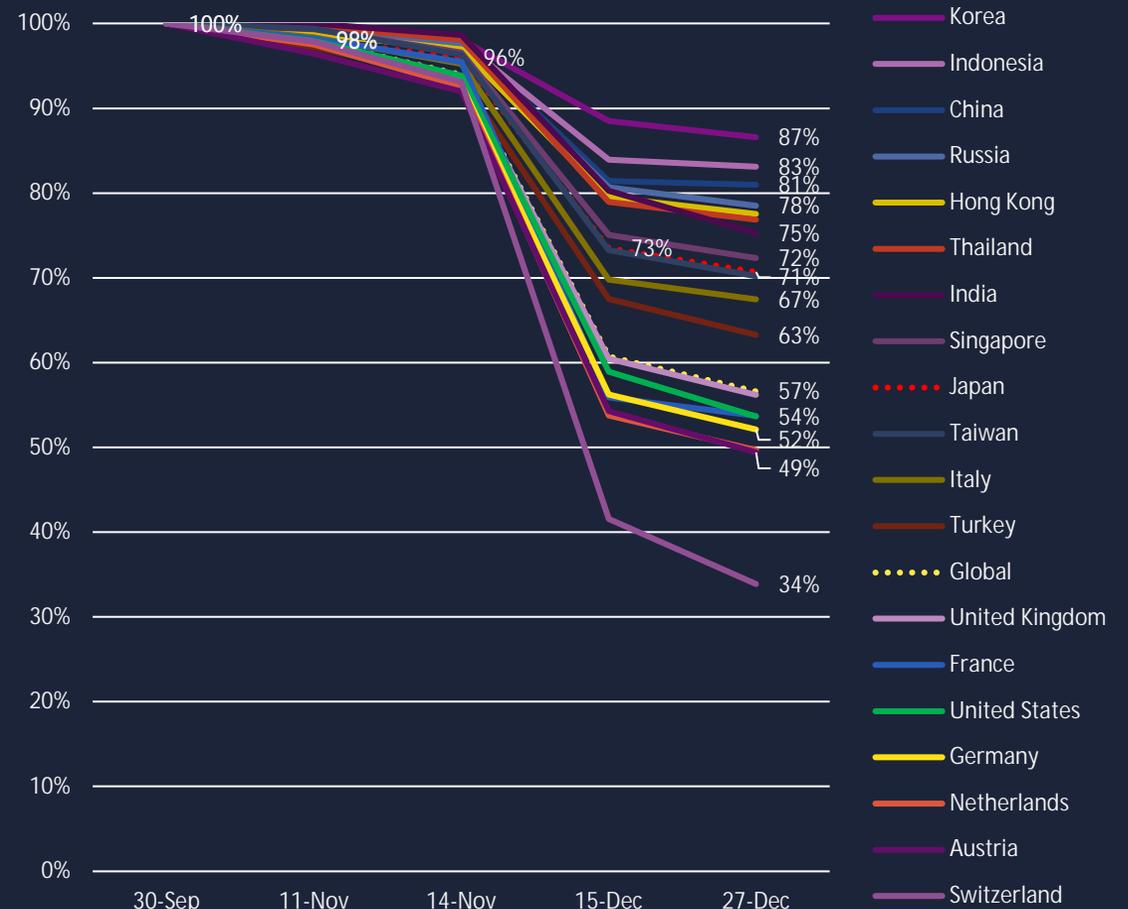
# Exchange Server/ProxyNotShellの脆弱性の国別対策傾向

- 2022年9月にゼロデイとして報告されパッチ公開は2022年11月9日（CVE-2022-41040、CVE-2022-41082）
- Exchange Serverの狭い範囲の一部バージョンが影響を受けるため、該当バージョンを利用する台数と脆弱性修正バージョンを利用するサーバ台数のみをカウントし脆弱サーバの割合を調査

✓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

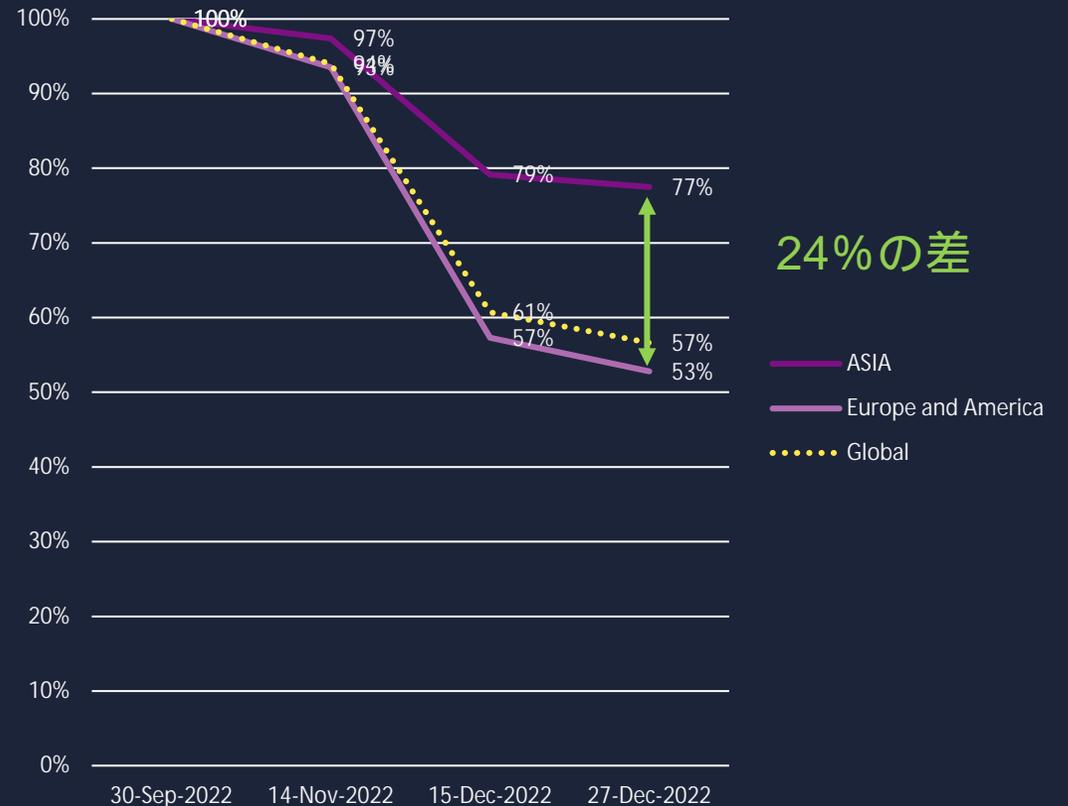
# 2020 vs 2022 Exchange Serverの脆弱性対処

- 2020年2月修正のCVE-2020-0688と2022年11月修正のProxyNotShellを同じ国を対象に対処速度を比較
- 欧米では2020年時には約1年を要した脆弱性対処率 約50%の進捗を2022年には約1ヶ月で達成  
ProxyNotShellが比較的新しいバージョンに影響する脆弱性だったことが関連している可能性はあり(パッチ適用の意識の高い層が多い)
- 約2年が経過しアジア圏と欧米圏の対処スピードの差が開いている状況

✓ CVE-2020-0688に脆弱な割合推移 (地域別)



✓ ProxyNotShellに脆弱な割合推移 (地域別)



# 2020 vs 2022 Exchange Serverの脆弱性対処

- 2020年2月修正のCVE-2020-0688と2022年11月修正のProxyNotShellを同じ国を対象に比較
- 対処速度（赤枠）の順位はほとんど入れ替わりがない

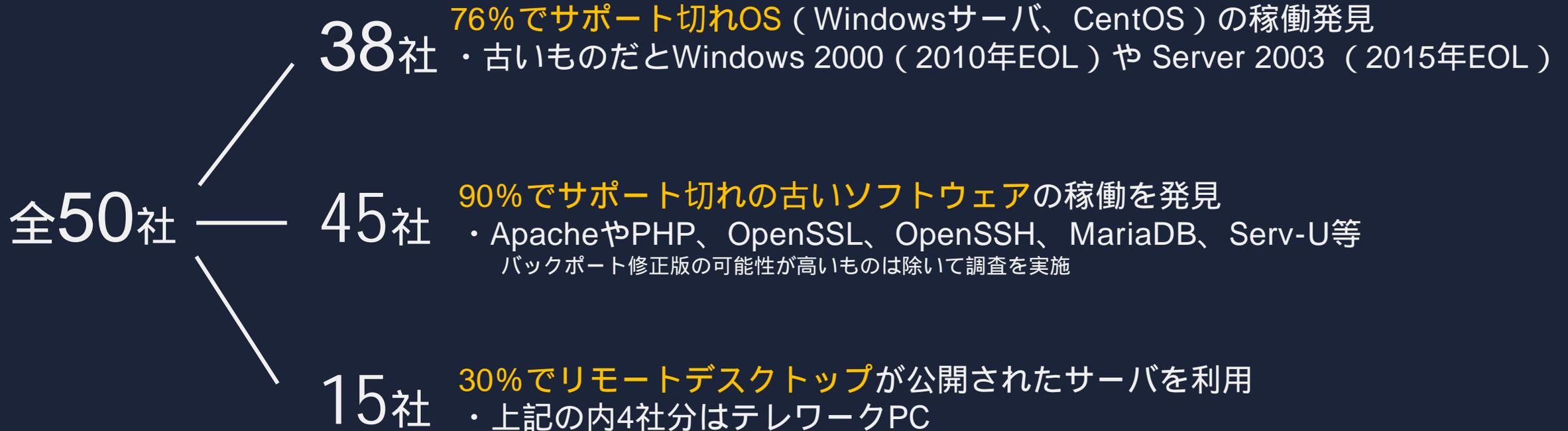
国	地域	CVE-2020-0688 約1年後脆弱サーバ割合	ProxyNotShell 約1.5ヶ月後の脆弱サーバ割合	差分	CVE-2020-0666の約1年後の進捗 悪い国順位	ProxyNotShellの約1.5ヶ月後の進捗 悪い国順位
Korea	ASIA	69%	87%	18%	4	1
Indonesia		73%	83%	10%	2	2
China		65%	81%	16%	7	3
Vietnam		67%	78%	11%	5	4
Malaysia		65%	78%	12%	6	5
Hong Kong		69%	78%	8%	3	6
Thailand		76%	77%	1%	1	7
Singapore		58%	72%	14%	10	8
Japan		54%	71%	16%	13	9
Taiwan		61%	70%	9%	9	10
Italy	Europe and America	62%	67%	5%	8	11
Canada		53%	56%	3%	14	12
United Kingdom		57%	56%	-1%	11	13
Australia		51%	55%	4%	16	14
France		57%	54%	-3%	12	15
United States		53%	54%	1%	15	16
Germany		32%	52%	20%	20	17
Netherlands		44%	50%	6%	18	18
Austria		41%	49%	8%	19	19
Switzerland		44%	34%	-10%	17	20

# 参考：脆弱性対処スピードの調査について

- 調査手法(Shodan CLI利用時)
  1. 脆弱性の影響を受けるサーバを特定するための検索クエリを検討する  
Shodan `http.title:outlook`
  2. 検索クエリでデバイス検索エンジンのDBからデータを取得する  
`shodan download --limit -1 filename http.title:outlook`
  3. 2を1ヶ月毎等定期的に実施する（データ容量が数GB以上になるため注意）
  4. 取得したデータの中から必要なデータ項目をパースする（パース項目は脆弱性毎に都度検討する）  
`shodan parse --fields ip_str,port,location.country_code,data sourcefilename > targetfilename`
  5. 抽出したデータを整形し比較可能なデータにする
- 脆弱性対処スピードの調査は実施できる条件が整うことが極めて少ないため機会を逃さないことが重要
  1. 外部公開されることが多いサーバの脆弱性であること。当然、内部サーバはOSINTで観測できないため。
  2. 外部からスキャンをせずともHTML等でバージョン情報や脆弱性有無が把握できること。法的にスキャンできない為。
  3. Shodan等のデバイス検索エンジンが保持するデータの中にバージョン情報が格納されていること。  
例えばSonicWallはVPNログイン画面のソースにバージョン情報が表示されるがShodanやCensysは保持しない
  4. PoCや攻撃が観測されパッチ適用の必要性が広く/強くアナウンスされること（必須条件ではない）。
  5. 公開サーバ総数が多くも無く少なくもないこと。台数が少ないと傾向が読み取れず多すぎるとデータが処理できない。

# 日本企業の状況について

- ✓ 2022年1月に旧東証一部上場企業から抽出した特定企業50社の本社・海外拠点・グループの外部公開サーバの管理状況を調査  
脆弱性スキャンやサーバへのアクセスは実施せずShodanの情報をもとに調査
- ✓ 本社企業が問題を有するケースが約4割、海外や子会社まで含めると**9割の企業**で問題点が見つかった。
- ✓ この調査以外にも100社以上の調査実績として一切問題点が見つからない企業はほぼ存在しない。



# 本セッションのアジェンダ

## ✓ 第1部 昨今のインシデント発生傾向分析

- ・ランサムギャングによるリーク情報
- ・日系企業の被害プレスリリース
- ・セキュリティ機関/ベンダの公開レポート

## ✓ 第2部 外部公開アセットの管理状況の変化

- ・RDPの公開状況
- ・サポート切れOSの利用
- ・脆弱性対処スピードの変化（2020年と2022年の比較）
- ・日系企業の対策状況

## ✓ 第3部 攻撃者の戦術変化を捉える試み

- ・過去調査事例（Pandora、AvosLocker、Deadbolt）
- ・デバイス検索エンジンでの調査方法の共有

# 再掲 この数年の大きな潮流の変化



暴露された企業・組織の外部公開サーバを継続的に調査することで  
侵入経路になっているサーバの傾向がみえてくるのでは？

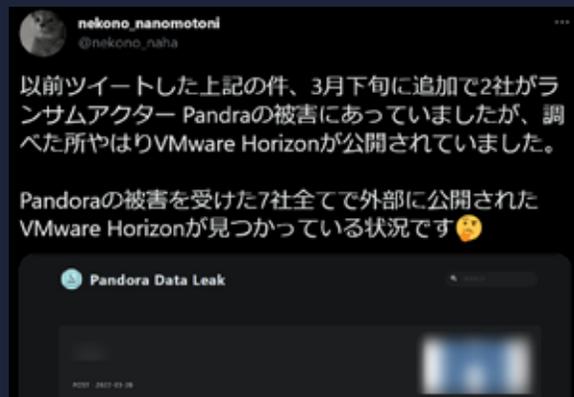
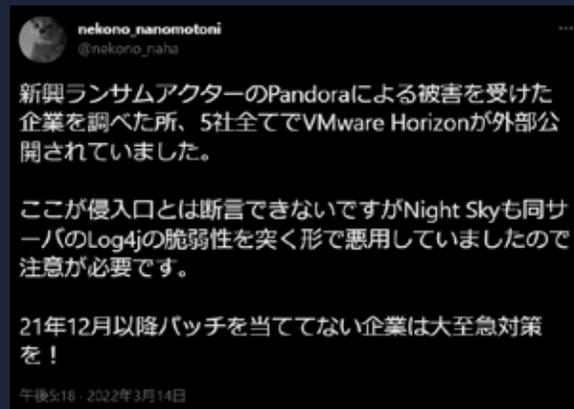
# 例1 ランサムアクター Pandoraの例

- 22年3月に活動を開始しすぐに終了した（リブランド）ランサムアクターで日本企業も3社ほど標的になっている
- 被害企業は共通してVMware Horizonを公開していたことから侵入口になっていた可能性を推測
- 2022年6月にTrend Micro社からもPandora事案とVMware Horizon(Log4j)の関連が言及される  
Log4Shell Vulnerability in VMware Leads to Data Exfiltration and Ransomware  
[https://www.trendmicro.com/en\\_us/research/22/g/log4shell-vulnerability-in-vmware-leads-to-data-exfiltration-and-ransomware.html](https://www.trendmicro.com/en_us/research/22/g/log4shell-vulnerability-in-vmware-leads-to-data-exfiltration-and-ransomware.html)

## ✓被害企業一覧

被害企業	掲載日	国	被疑箇所
H社	22/3/30	日本	VMware Horizonあり
U社	22/3/30	米国	VMware Horizonあり
O社	22/3/13	米国	VMware Horizonあり
R社	22/3/13	米国	VMware Horizonあり
D社	22/3/13	日本	VMware Horizonあり
G社	22/3/5	日本	VMware Horizonあり
J社	22/3/5	米国	VMware Horizonあり

## ✓注意喚起ツイート

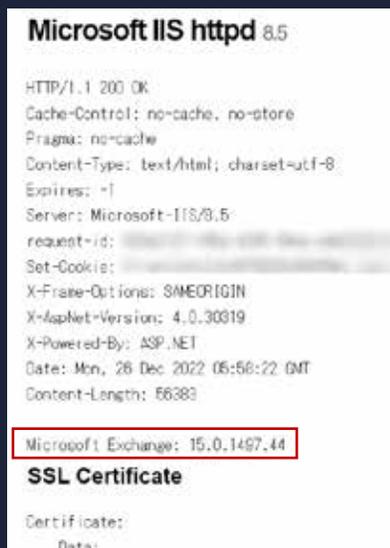
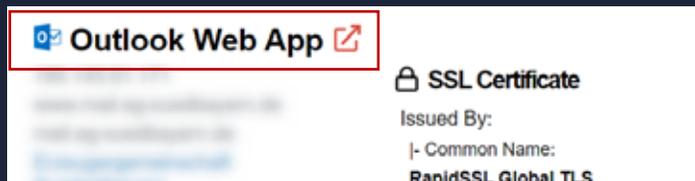


## ✓VMwareHorizonのLog4jに関する注意喚起

時期	報告者	国
22/1/5	英国 NHS/CC-4002	未知の脅威グループ
22/1/10	マイクロソフト	ランサムアクター-DEV-0401 ( NightSky )
22/3/14	nekono_nanomotoni	ランサムアクター-Pandora
22/3/29	SOPHOS	マイニングボット
22/6/23	米国 CISA/AA22-174A	APT含む複数の脅威アクター
22/8/16	トレンドマイクロ	ランサムアクター-Pandoraを含む複数事例
22/8/25	マイクロソフト	イラン系/MERCURY
22/9/7	BlackBerry	ランサムアクター/MONTI
22/9/8	Cisco Thalos	Lazarus/APT38
22/9/14	米国 CISA/AA22-257A	イラン系APT/IRGC

# 例2 ランサムアクター AvosLockerの例

- 2021年6月頃から活動を開始したRaaSモデルを採用するランサムウェア
- 2022年6月の被害企業は共通してExchange Serverを公開し、約2週間後の調査時点でいずれの企業も最新版かProxyShellに該当するバージョンだったことから、同サーバが侵入口になっていた可能性を推測
- 2022年3月にFBIがAvosLocker の複数の被害がProxy Shell起因で発生しているとの勧告を発出していた  
Indicators of Compromise Associated with AvosLocker Ransomware  
<https://www.ic3.gov/Media/News/2022/220318.pdf>

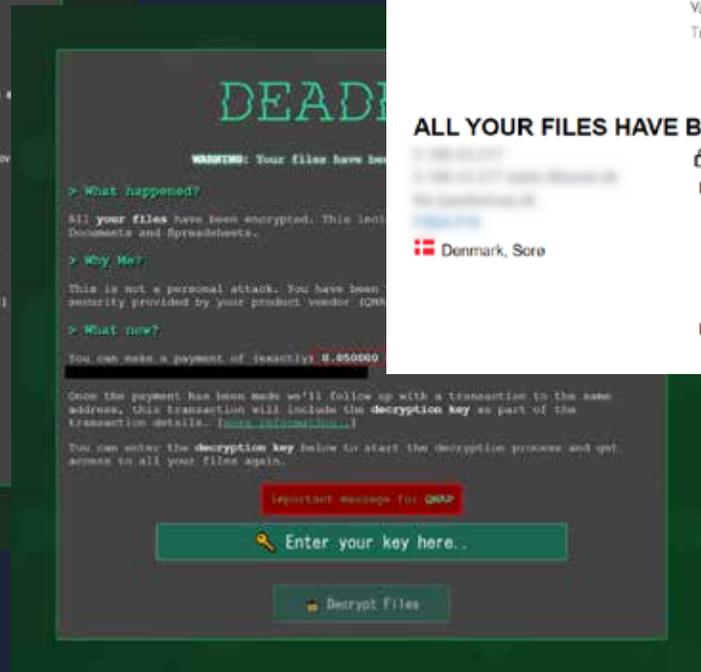
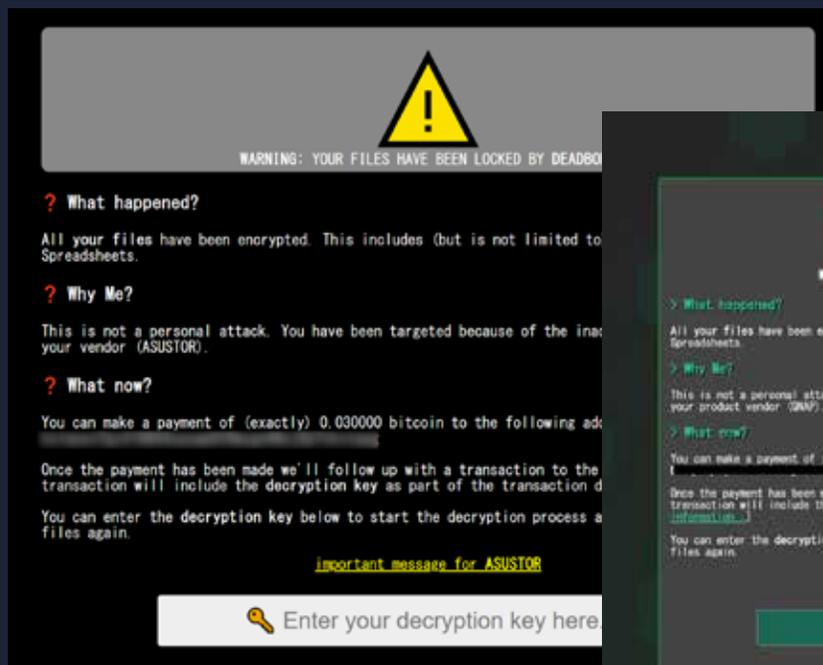


リークサイト掲載日	被害企業名	Exchange 有無	Exchange Version *22年6月下旬時点
2022/6/17	C****	あり	アクセス不可
2022/6/17	B*****	あり	最新版
2022/6/8	L*****	あり	ProxyShellに該当
2022/6/7	Y*****	あり	最新版
2022/6/7	C*****	あり	最新版
2022/6/7	C*****	あり	ProxyShellに該当
2022/6/3	T*****	あり	最新版
2022/6/3	C*****	あり	ProxyShellに該当
2022/6/3	P*****	未発見	—
2022/6/3	B*****	未発見	—
2022/6/3	C*****	未発見	—
2022/4/6	K*****	未発見	—
2022/4/6	M*****	未発見	—
2022/4/6	A*****	未発見	—

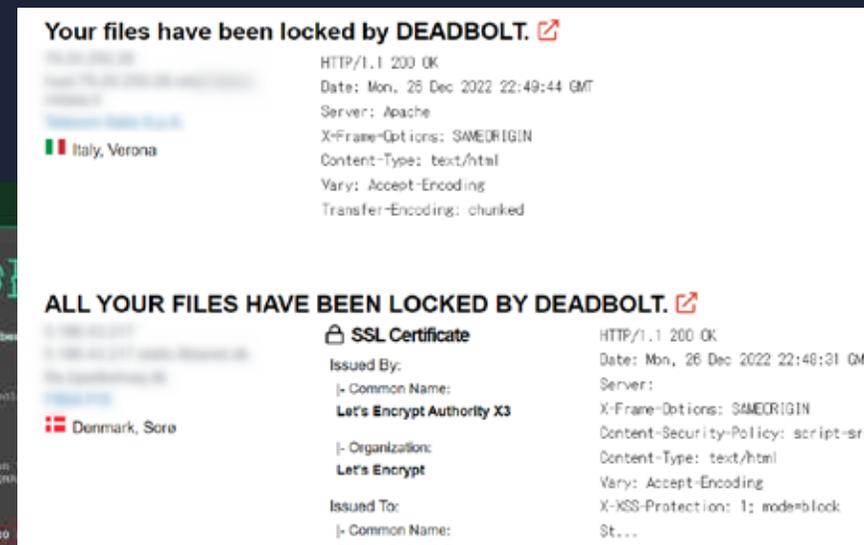
# 例3 DeadBoltランサムウェアの例

- 2022年1月頃からQNAP社及びASUSTOR社製のNASを標的にした活動を行っているランサムウェア
- 2022年中に1月、5月、6月、8月頃と複数回のキャンペーン展開し国内外で多くの被害が出た
- ログイン画面に脅迫文が表示されるため被害を受けたNASの台数やバージョン情報を直接的に補足可能

## ✓被害を受けたNASに表示されるランサムノート



## ✓被害を受けたNASのShodanでの捕捉



# 例3 DeadBoltランサムウェアの例

- 各キャンペーンにおいて被害台数がQNAP NASの総数（32.7万台）と大きく乖離しており特定バージョンやモデルを標的にしている可能性を推測
- 調査を実施したところ第1次～3次までは特定バージョン/モデルが標的になっていたためQNAP社へ通知し国内外での注意喚起に活用

## ✓ キャンペーンごとの被害件数

月	被害件数	備考
1月	1,889	第1次攻撃キャンペーン
2月	3,566	
3月	3,678	
4月	2,300	
5月	3,696	第2次攻撃キャンペーン
6月	6,494	第3次攻撃キャンペーン
7月	1,5017	第4次攻撃キャンペーン

## ✓ 暗号化前後のサーバレスポンス

```

QNAP TS-253Be 4.3.5

HTTP/1.1 200 OK
Date: Thu, 16 Jun 2022 00:57:15 GMT
Server: http server 1.0
X-Frame-Options: SAMEORIGIN
Content-type: text/html; charset=UTF-8
Last-modified: Tue, 13 Nov 2018 22:38:01 GMT
Accept-Ranges: bytes
Content-length: 500
Vary: Accept-Encoding

QNAP TS-253Be:
  Hostname: IZUMI48911
  Model:
    Model Name: TS-253B
    Display Model Name: TS-253Be
    Platform: TS-NAD300
    Platform Era: X86_APOLLOLAKE
  Firmware:
    Version: 4.3.5
    Number: 0790
    Build: 20181114
  Apps:
    Filestation:
      Version: 5.1.0
      Build: 20181114
    Photostation:
      Version: 5.7.5
      Build: 20181030
      Checksum: 997a9c3
  
```

```

Apache httpd

HTTP/1.1 200 OK
Date: Mon, 20 Jun 2022 10:38:28 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
Content-Type: text/html
Vary: Accept-Encoding
Transfer-Encoding: chunked

SSL Certificate

Certificate
  Data:
    Version: 3 (0x2)
    Serial Number:
      fe:8a:58:07:58:05:47:26
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=TW, ST=Taipei, L=Taipei, O=QNAP Systems, Inc.
    Validity
      Not Before: Mar 11 10:45:27 2016 GMT
      Not After: Mar 9 10:45:27 2026 GMT
    Subject: C=TW, ST=Taipei, L=Taipei, O=QNAP Systems, Inc.
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (2048 bit)
      Modulus:
  
```

## ✓ QNAP社からの注意喚起



### Summary

QNAP recently detected a new DeadBolt ransomware campaign. According to victim reports so far, the campaign appears to target QNAP NAS devices running outdated versions of QTS 4.2.x, 4.3.x and 4.4.x, and outdated applications.

QTS 4.5.x, and 5.0.x, and QuTS hero h4.5.x and h5.x, with updated applications, are not affected.

<https://www.qnap.com/en-me/security-news/2022/take-immediate-actions-to-secure-qnap-nas-and-update-qts-to-the-latest-available-version>  
<https://www.qnap.com/ja-jp/security-advisory/QSA-22-19>

# 調査方法の共有

リーク情報  
チェック



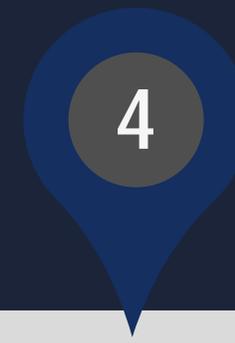
被害企業サーバ  
OSINT



初期侵入被疑箇所  
共通項の抽出



サーバ停止やバージョン  
アップ等の状態監視



**注** 今回は無償または最小工数で効率よく調査可能な手法を紹介する点に主眼をおいています。  
高額な有償ツールやインテリジェンスを活用したOSINT手法は今回は時間と実践可能性を考慮し説明対象外とします。

**注** 製品特定の方法についても様々な観点や手法があるため代表的なポイントのみを記載しています。記載されている手法であれば100%網羅的にサーバが捕捉できるわけではありません。また検索対象ではない製品が交じる場合もあります。予めご了承ください。

# リーク情報のチェック



- 攻撃者のリークサイトを監視しておき被害企業を把握する  
独力での追跡はそれだけで多大な工数を要するためDarkTracerの無償アカウント利用も推奨  
<https://xoxo.darktracer.com/>
- リーク情報から被害企業のドメイン情報を収集する

*Claimed* Victim	Ransomware Gang	Detection Date (UTC+0)	Ransomware URL	Victim Site	Victim Country	Industrial Sector
...	Royal	2022-12-21 15:52:33	Not supported to FREE version	...	USA	Security And Commodity Brokers, Dealers, Exchanges, And Services
...	Hive	2022-12-21 12:58:40	Not supported to FREE version	...	USA	Textile Mill Products
...	Royal	2022-12-20 19:48:25	Not supported to FREE version	...	USA	Eating And Drinking Places

被害企業名  
ランサムギャング名  
掲載日  
被害企業URL/ドメイン  
国  
業種

特定の国の被害の検索

*Claimed* Victim	Ransomware Gang	Detection Date (UTC+0)	Ransomware URL	Victim Site	Victim Country	Industrial Sector
...	LockBit	2022-12-12 08:43:29	Not supported to FREE version	...	Japan	Machinery, Computer Equipment
...	BlackCat (ALPHV)	2022-12-05 21:53:15	Not supported to FREE version	...	Japan	Miscellaneous Manufacturing Industries
...	LockBit	2022-11-22 06:03:03	Not supported to FREE version	...	Japan	Miscellaneous Manufacturing Industries

特定のランサムウェアギャングによる被害の検索

*Claimed* Victim	Ransomware Gang	Detection Date (UTC+0)	Ransomware URL	Victim Site	Victim Country	Industrial Sector
...	BlackCat (ALPHV)	2022-12-13 13:30:00	Not supported to FREE version	...	USA	Construction
...	BlackCat (ALPHV)	2022-12-13 13:30:00	Not supported to FREE version	...	Switzerland	Electronic, Electrical Equipment, Components
...	BlackCat (ALPHV)	2022-12-10 11:09:09	Not supported to FREE version	...	USA	Health Services
...	BlackCat (ALPHV)	2022-12-10 01:29:10	Not supported to FREE version	...	USA	Aerospace
...	BlackCat (ALPHV)	2022-12-08 17:16:20	Not supported to FREE version	...	USA	Educational Services

# 被害企業サーバの特定について



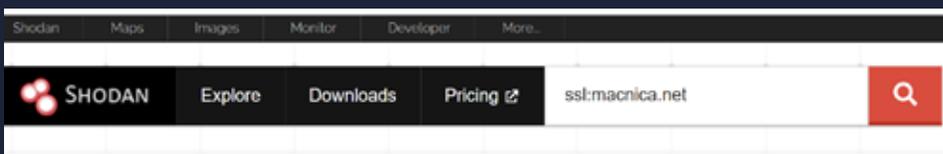
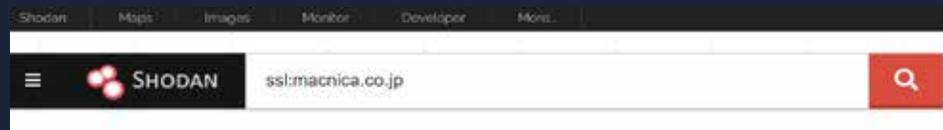
- 収集したドメイン情報をもとにデバイス検索サービス（Shodan,Censys,ZoomEye等）でSSL検索
- 被害組織が所有するドメイン情報が設定されているサーバ 当該組織が管理/所有するサーバが効率よく把握できる

- 以下URLにアクセスし、STEP1で洗い出したドメインで以下のように検索

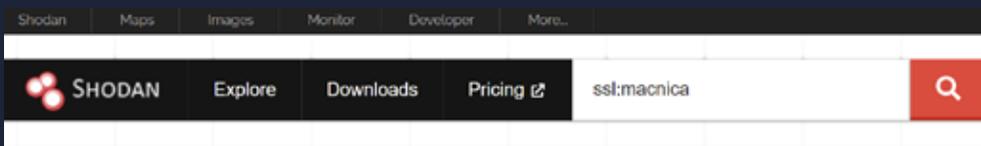
<https://www.shodan.io/dashboard>

ssl:被害組織のドメイン 例：ssl:macnica.co.jp

- この検索により、SSL証明書に当該ドメインを持つサーバが一気に検索可能



- 企業名が珍しい、ユニークな場合はドメインのトップレベルやセカンドレベルを省略すると一気に検索を行うと効率が良い



ZoomEyeの場合



Censysの場合



対象箇所に応じて以下のパターンでも検索する必要がある

services.tls.certificates.leaf\_data.subject\_dn="\*targetname\*"

services.tls.certificates.leaf\_data.issuer\_dn="\*targetname\*"

services.tls.certificates.leaf\_data.issuer.common\_name="\*targetname\*"

services.tls.certificates.leaf\_data.issuer.organization="\*targetname\*"

services.tls.certificates.leaf\_data.subject.common\_name="\*targetname\*"

services.tls.certificates.leaf\_data.subject.organization="\*targetname\*"

# 被害企業サーバの特定について



- 前ページのSSL検索の結果から当該企業が所有するIPアドレスレンジを割り出して検索（Shodanのみ）

- 以下URLへアクセスする

<https://www.shodan.io/search/facet>

- 前ページで検索したドメインを左側に入力し、右側はリストから“org”をセットした状態で検索する

ssl:macnica.co.jp org

- 検索対象のSSL証明書を持つサーバが、どの企業が所有するIPアドレスセグメントで何台稼働しているか確認できる

- 調査対象企業名が出てきたらその名称をコピーしメモ等で控える



Amazon Technologies Inc.	3
AIOO ROW GmbH	2
ARTERIA Networks Corp.	2
Amazon.com, Inc.	2

MACNICA DHW LTDA	7
MACNICA CYTECH PTE LTD	4
Macnica GmbH	4
MACNICA, Inc.	3
reassign to Macnica Thailand Co.,Ltd.	3
Macrica, Inc.	2
MACNICA	1

- Shodanの通常の検索ページへアクセスする

<https://www.shodan.io/>

- STEP3-1で洗い出したorganization名を使い以下のように検索する  
org:"organization名"

org:"Macnica GmbH"

org:"MACNICA DHW LTDA"

- この検索により、検索した組織名がWhoisに登録されているIPアドレスレンジで稼働するサーバを洗い出すことが可能
- 組織名がユニークな場合は社名だけで検索すると一気に洗い出すことができる場合がある（例：org:macnica）
- MACNICA, Inc.のように組織名に,(カンマ)が含まれる場合はカンマより右側を削除して検索する必要がある  
例：org:"MACNICA, Inc." → org:"MACNICA"

ZoomEyeではorg:macniacのような検索も可能だが  
Shodanとは異なりZoomEye側で検索対象組織と関連があると判断されたサーバも含まれてしまう（Whois検索ではない）

CensysではWhois上の組織名補足が弱いのと

autonomous\_system.name=でワイルドカード検索が使えないため使いづらい

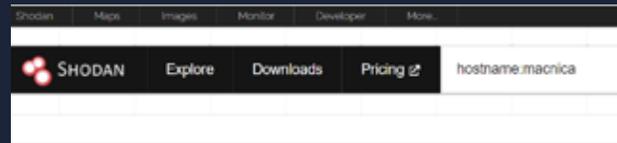
# 被害企業サーバの特定について



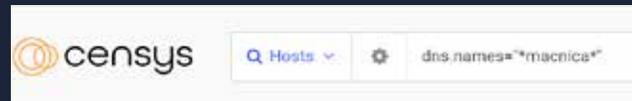
- 前述の手法で被疑サーバが出てこない場合は？

## 1. Hostname検索

hostname:targetname



dns.names="\*targetname\*"



hostname:targetname



## 2. 調査対象ドメインの膨らまし

Viewdns.info

<https://viewdns.info/reversewhois/>



検索対象ドメインとWhois情報上で関連性があるドメインを自動で列挙してくれる（稀にノイズあり）

Registrant Name or Email Address:

Reverse Whois results for macnica.com  
\*\*\*\*\*

There are 7 domains that matched this search query.  
These are listed below:

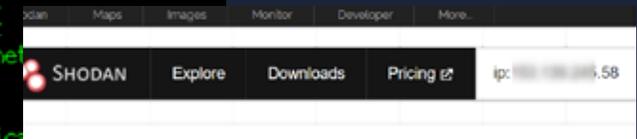
Domain Name	Creation Date	Registrar
b3smart.com	2005-12-03	PAIR NETWORKS INC./D/B/A PAIRNIC
macnica-apps.com	2016-05-18	LAUNCHPAD.COM, INC.
macnica.com.tw		
macnica.com	1996-05-21	PAIR NETWORKS INC./D/B/A PAIRNIC
macnica.org	2014-10-22	IAPI GMBH
macnicatech.com	2012-07-18	LAUNCHPAD.COM, INC.
myb3smart.com	2006-04-14	PAIR NETWORKS INC./D/B/A PAIRNIC

## 3. サブドメイン列挙→IPアドレス列挙→IP検索

OWASP Amass

<https://github.com/OWASP/Amass>

```
$ amass enum -active -d macnica.net
macpws.tech.macnica.net
macpws2.tech.macnica.net
nav01.macnica.net
vlab2.macnica.net
ib.tech.macnica.net
vlab.macnica.net
so.macnica.net
macnica-eye.macnica.net
arimac.macnica.net
saml-test.tech.macnica.net
ca-test.tech.macnica.net
mlip.macnica.net
mac-box-ds-demo.tech.macnica.net
macnica-eye-dev.macnica.net
blog.macnica.net
www1.macnica.net
oss.macnica.net
www.macnica.net
search.macnica.net
ftp2.macnica.net
lala.tech.macnica.net
nsl.tech.macnica.net
inc.macnica.net
mac-eye.macnica.net
search2.macnica.net
autodiscover.macnica.net
files.macnica.net
makomanager.macnica.net
makomanager-stg.macnica.net
em.macnica.net
```

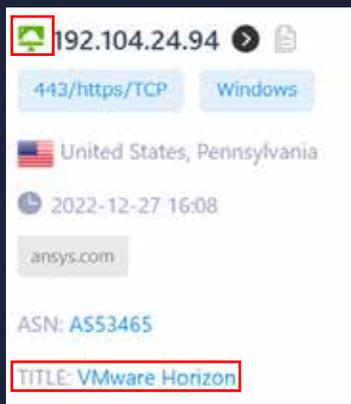
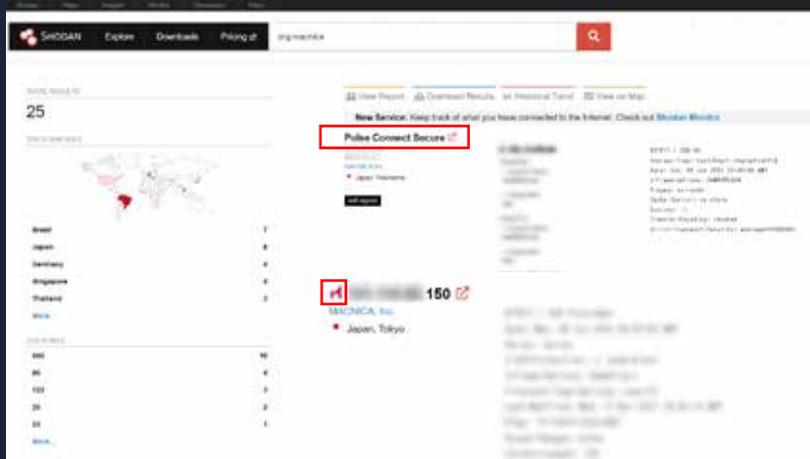


# 検索結果の確認時の着目ポイント



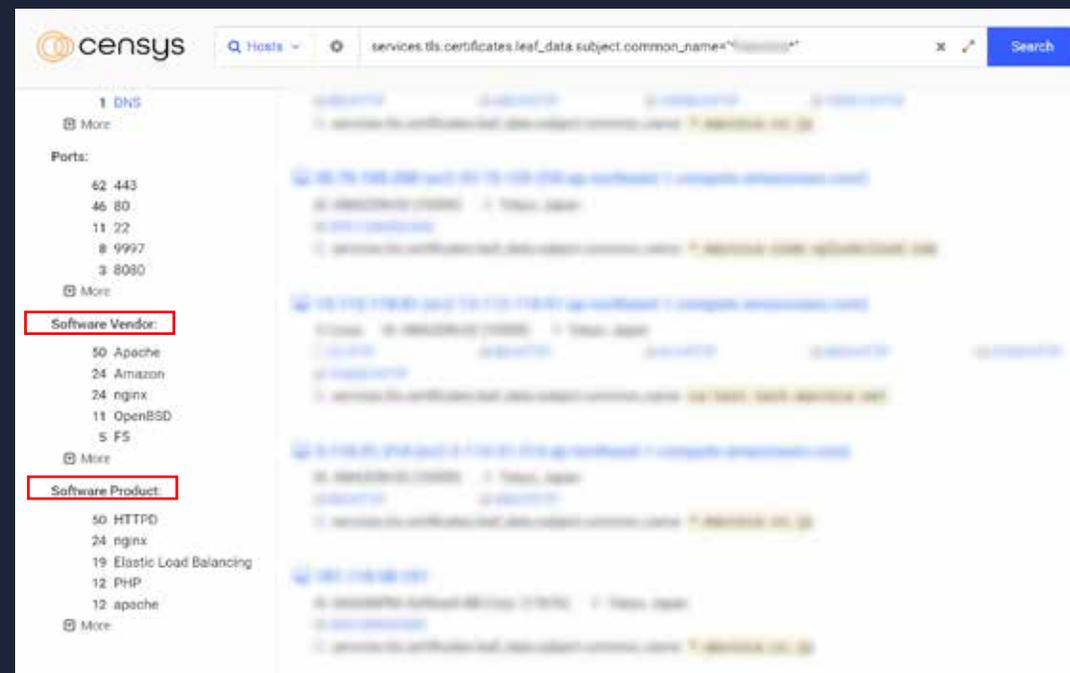
## ✓ Shodanと ZoomEyeの場合

製品特定はHTTPタイトルとファビコンから  
目視で行う



## ✓ Censysの場合

検索結果のSoftware VendorとSoftware Productに注目  
特定に対応していない一部製品はタイトルに注目



# まとめ デバイス検索エンジン毎の長所短所



・デバイス検索エンジンの特性に応じて検索や結果の確認を行っていく

## ✓ Shodanと ZoomEyeの場合

SSL/TLS証明書の中の文字列を一気に検索することができるので被害企業サーバの抽出が楽

ssl:targetname

IPアドレスのWhois内の組織名をターゲットにした検索が行える

org:targetname

検索エンジン側での製品特定力が弱いため、検索結果中のHTTPタイトルとファビコン、サーババナーを記憶し参照していくことが必要。

User Portal 217.145.100.200 TMT GmbH & Co. KG Germany, Bayreuth

HTTP/1.1 200 OK  
Date: Sun, 01 Jan 2023 05:27:52 GMT  
Server: xxxx  
X-Frame-Options: SAMEORIGIN  
Strict-Transport-Security: max-age=31536000  
X-Content-Type-Options: nosniff  
Referrer-Policy: strict-origin-when-cross-origin  
Content-Security-Policy: default-src https: data: ws:

## ✓ Censysの場合

SSL/TLS証明書の中の文字列を一気に検索することができず証明書のIssuerやSubject毎に検索を行う必要がある

```
services.tls.certificates.leaf_data.subject_dn="*targetname*"
services.tls.certificates.leaf_data.issuer_dn="*targetname*"
services.tls.certificates.leaf_data.issuer.common_name="*targetname*"
services.tls.certificates.leaf_data.issuer.organization="*targetname*"
services.tls.certificates.leaf_data.subject.common_name="*targetname*"
services.tls.certificates.leaf_data.subject.organization="*targetname*"
```

IPアドレスのWhois内の組織名をターゲットにした検索が行えない。  
Whois内の組織名の補足も弱そうなため

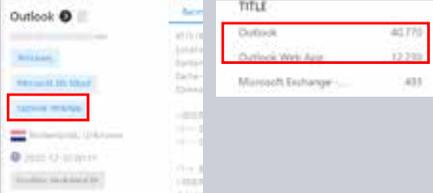
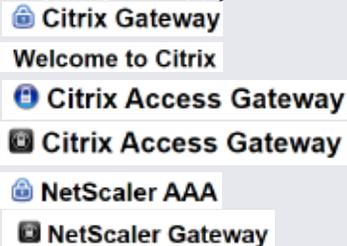
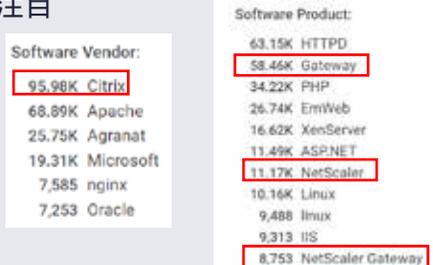
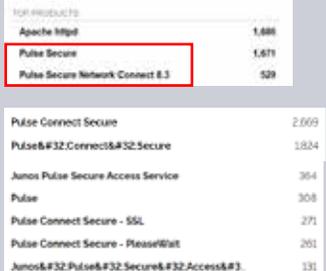
Censys側である程度自動的に製品の識別を実施してくれるため侵入被疑箇所の抽出が楽に行える。一部特定に対応していないものもあるが、それがタイトルやファビコンハッシュから特定を行う。

Software Vendor:

584.91K Agranat  
444.34K Sophos

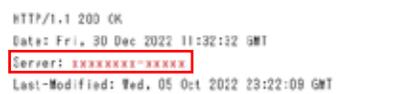
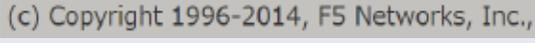
# 製品特定の方法



製品	Shodan	ZoomEye	Censys	備考
Exchange Server	<p>以下HTTPタイトルとファビコンから特定</p> 	<p>以下クエリでソフトウェア特定が可能だが捕捉力が弱いためShodanと同様にTITLEからの特定を推奨 +app:"Outlook WebApp"</p> 	<p>ソフトウェア特定が可能 ただし2010系は特定不可のためタイトルから判断する必要がある</p> 	<p>組織のドメインが証明書に紐づいている事が多く特定可能性が高い。 Shodanでは詳細バージョンが記録されているためパッチレベルや脆弱性有無が判断できる（CensysやZoomEyeでは一部情報が欠落している）。</p> 
Citrix	<p>以下HTTPタイトルとファビコンから特定（種類が多いため一部のみ記載。CitrixやNetscalerという文字に注目）</p> 	<p>ソフトウェア特定可能 +app:"citrix"</p>  <p>またShodanと同様にHTTPタイトルから特定</p>	<p>ベンダやソフトウェア特定が可能。 ベンダー欄では"Citrix"に、ソフトウェア欄ではNetscalerやGatewayに注目</p> 	<p>組織のドメインが証明書に紐づいている事が多く特定可能性が高い。</p> <p>HTMLの内容から詳細バージョンや脆弱性有無が可能との情報もあり。</p> <p><a href="https://blog.fox-it.com/2022/12/28/cve-2022-27510-cve-2022-27518-measuring-citrix-adc-gateway-version-adoption-on-the-internet/">https://blog.fox-it.com/2022/12/28/cve-2022-27510-cve-2022-27518-measuring-citrix-adc-gateway-version-adoption-on-the-internet/</a></p>
Pulse Secure	<p>product:"Pulse Secure"で製品特定可能。 HTTPタイトルからも特定可能</p> 	<p>ソフトウェア特定が可能。 +app:"PulseSecure Pulse Connect Secure"</p>  <p>またShodanと同様にHTTPタイトルから特定</p> <p>TITLE: Pulse Connect Secure</p>	<p>ソフトウェア特定可能だが精度が低いためShodanと同様にHTTPタイトルから特定を推奨</p> <p>HTML Title Pulse Connect Secure</p> 	<p>組織のドメインが証明書に紐づいている事が多く特定可能性が高い。</p> <p>HTTPレスポンスからバージョン特定が可能（Shodanでは正規化されバージョンが表示される）。</p>  <p><a href="https://gist.githubusercontent.com/lz-censys/856ab8f2b68c2504d036ce34fdf3965d/raw/92f84c7e4753ed4de43bcfa9112d100501dbdbdc/pulse_vuln_matrix.csv">https://gist.githubusercontent.com/lz-censys/856ab8f2b68c2504d036ce34fdf3965d/raw/92f84c7e4753ed4de43bcfa9112d100501dbdbdc/pulse_vuln_matrix.csv</a></p>

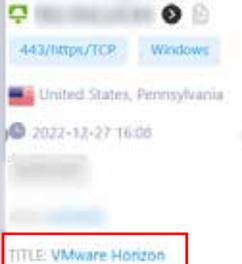
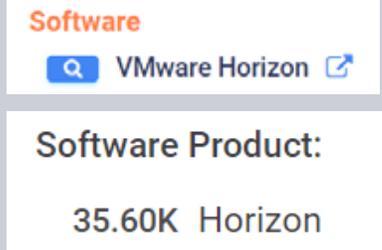
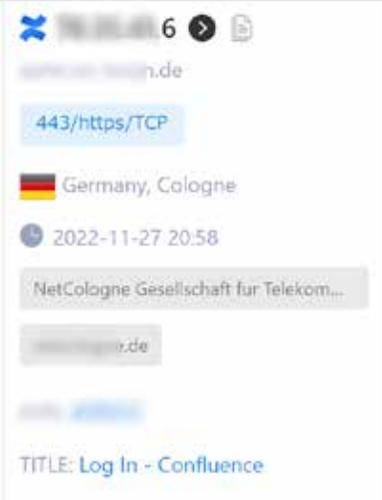
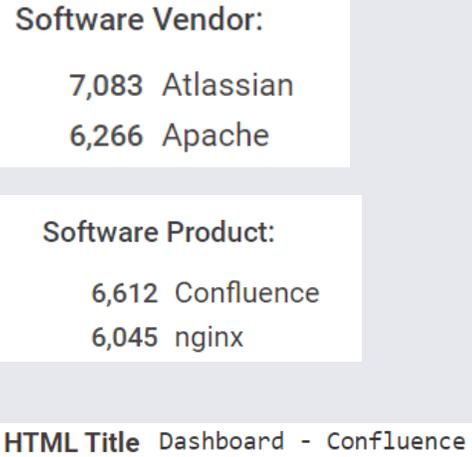
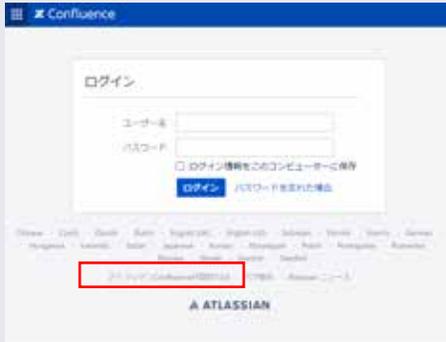
# 製品特定の方法



製品	Shodan	ZoomEye	Censys	備考
Fortinet	<p>ファビコン（6系以下のユーザ向け、管理者向け画面共通で表示） 7系のファビコンはShodanは捕捉できず検索結果に表示されない</p>  <p>6系のユーザ、管理者向けログイン画面と7系のユーザ向け画面に特徴的なレスポンスから判断</p>  <p>証明書中のFortiGate/Fortinetから判断</p> 	<p>ソフトウェア特定が可能 +app:"FortiGate" +app:"Fortinet"</p>  <p>Shodanと同様にファビコンハッシュがタイトルでも特定可能だが捕捉されているケースは多くないためタイトルでの判断が良い。</p> 	<p>ベンダやソフトウェア特定が可能（6系以下も7系も特定が可能）</p> 	<p>製品が発行する証明書が設定されておりSSL検索で組織が特定できないことが多いためIPアドレスの組織名を参照する必要がある。</p>  <p>右記ユーザ向けログイン画面ハッシュ http.html_hash:-1454941180</p> <p>ユーザ及び管理者向けログイン画面ではファビコンデザインよりメジャーバージョンを特定可能。左が6系、右が7系</p>  <p>管理者向けログイン画面ハッシュ（6系以下のみ） http.html_hash:-1968569468 管理者向けログイン画面ハッシュ（7系以下のみ） http.headers_hash:-841816352</p> <p>管理画面は色や形状からおおよそのバージョンが特定可能。左から5系、6系、7系（色がパステル調）</p>  <p>6系以上の画面の色はカスタマイズ可能なため他の色もあり</p>
F5 BIG-IP	<p>HTTPタイトルとファビコンから特定</p> 	<p>Shodanと同様のファビコンやタイトルに注目</p>  <p>+app:"F5 BIG-IP load balancer"で製品特定は可能だが同器機のログイン画面がでてくるわけではない</p>	<p>ベンダやソフトウェア特定が可能だが製品のログイン画面が出てくるわけではない</p>  <p>以下クエリでログイン画面を特定</p> 	<p>製品が発行する証明書が設定されておりSSL検索で組織が特定できないことが多いためIPアドレスの組織名を参照する必要がある。</p> <p>ログイン画面のフッターの表記から大まかなバージョンを推測できる可能性がある。</p>  <p>(c) Copyright 1996-2022, F5, Inc.</p>  <p>(c) Copyright 1996-2014, F5 Networks, Inc.,</p>

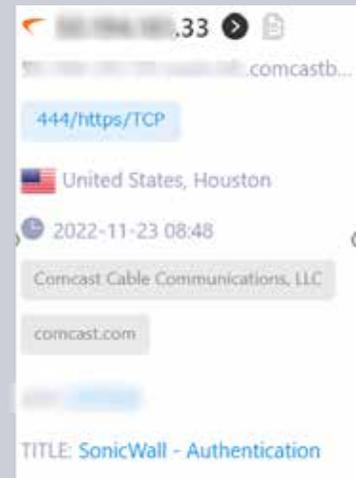
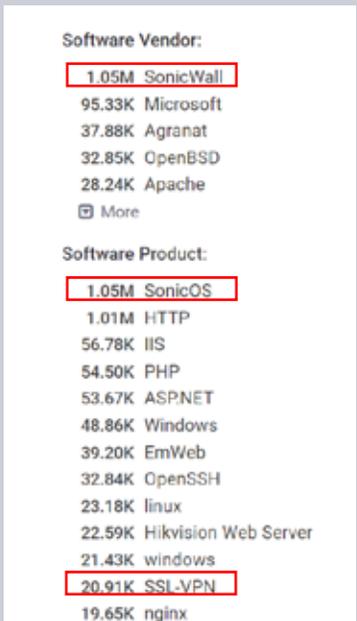
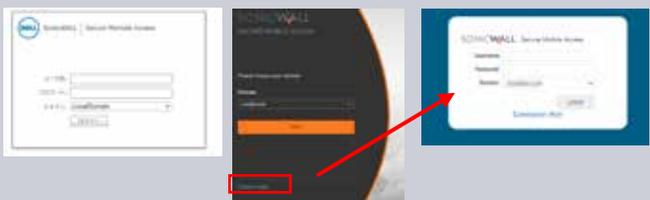
# 製品特定の方法



製品	Shodan	ZoomEye	Censys	備考
VMware Horizon	<p>HTTPタイトルとファビコンから特定</p> 	<p>+app:“VMware Horizon”で製品特定可能。HTTPタイトルとファビコンからも特定可能。</p> 	<p>ベンダやソフトウェア特定が可能</p> 	<p>組織のドメインが証明書に紐づいている事が多く特定可能性が高い。</p> <p>同製品に内在するLog4jの脆弱性が悪用されることが多いが外部からOSINTでのバージョン特定や脆弱性判断は不可</p>
Atlassian Confluence	<p>HTTP.COMPONENT:Confluenceで特定が可能（赤枠のマークに注目）</p>  <p>HTTPタイトルやファビコンでも特定が可能だがタイトルやファビコンがカスタマイズされていることが多い点は注意</p> 	<p>+app:“Atlassian Confluence” でソフトウェア特定が可能。HTTPタイトルとファビコンからも特定可能。</p> 	<p>ベンダやソフトウェア特定が可能</p> 	<p>証明書中に企業名が記載されていることが多く組織の特定可能性が高い。</p> <p>ログイン画面のフッターにバージョンが表示されているため脆弱性判断が可能</p>  <p>アトラシアンConfluenceが提供7.0.4</p>

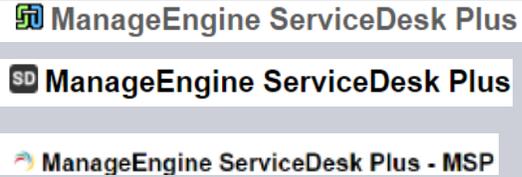
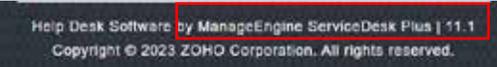
# 製品特定の方法



製品	Shodan	ZoomEye	Censys	備考
<p>SonicWall</p>	<p>product:“SonicWALL“で特定が可能。</p> <p>検索結果上はHTTPタイトルやファビコンから特定が可能</p>  <p>UTM/FWのNsaシリーズは検索結果のサーバレスポンスの以下箇所にメジャーバージョンの表記がある</p> <pre>HTTP/1.0 200 OK Server: SonicWALL Expires: -1 Cache-Control: no-cache Content-type: text/html; charset=UTF-8; X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block X-Frame-Options: SAMEORIGIN Content-Security-Policy: default-src 'self' 'unsafe-  SonicOS Version: 7.1.4 Serial Number: 2026000930</pre> <p>SSL VPNのSMAシリーズは以下レスポンスがある</p> <pre>HTTP/1.1 200 OK Date: Mon, 02 Jan 2023 03:23:54 GMT Server: SonicWALL SSL-VPN Web Server</pre>	<p>+app:“SonicWALL“ で特定が可能</p> 	<p>ベンダやソフトウェア特定が可能</p>  <p>SSL-VPNはVPNのSMAシリーズを特定</p>	<p>製品が発行する証明書が設定されておりSSL検索で組織が特定できないことが多いためIPアドレスの組織名を参照する必要がある。</p> <p>SecureMobileAccess及びSecure Remote Accessシリーズの以下デザインのログイン画面のHTMLソースを参照すると詳細バージョンが確認でき脆弱性が特定できる</p> <p>SMAでもContemporary Mode（左から2番目）では表示されないためClassicMode（一番右）に切り替える必要がある</p> <p>似たデザインのNetwork Security ApplianceおよびそのSSLVPNログイン画面では特定不可</p>  <pre>&lt;link type="text/css" href="/swl_styles/10.2.1.6-37sl.css" rel="stylesheet"&gt; &lt;link href="/swl_login/10.2.1.6-37sl.css" type="text/css" rel="stylesheet"&gt; &lt;link href="/swl_header/10.2.1.6-37sl.css" type="text/css" rel="stylesheet"&gt; &lt;link href="/swl_content/overrides/10.2.1.6-37sl.css" type="text/css" rel="sty</pre> <p>Network Security Applianceと記載されているUTM/FWのNsaシリーズはログイン画面のデザインからメジャーバージョンの特定が可能で左から5系、6系、7系（5系と6系はロゴがDELLのものもある）。ただし詳細バージョンは特定不可</p> 

# 製品特定の方法



製品	Shodan	ZoomEye	Censys	備考
Zoho ManageEngine ServiceDesk Plus	<p>HTTPタイトルとファビコンから特定</p> 	<p>製品特定不可のためHTMLタイトルから判断する（ファビコンも収集されていない）</p> 	<p>製品特定不可のためHTMLタイトルから判断する</p> 	<p>HTTPSが設定されていれば証明書中に企業名が記載されていることが多く組織の特定可能性が高い。</p> <p>ログインページのフッターにバージョン情報が表記されているためおおよそのバージョン把握は可能</p> 
Zoho ManageEngine Desktop Central	<p>HTTPタイトルとファビコンから特定</p> 	<p>製品特定不可のためHTMLタイトルから判断する（ファビコンも収集されていない）</p> 	<p>製品特定不可のためHTMLタイトルから判断するしかないが、1件しかヒットせず、同製品のタイトルはCensysで捕捉できていない可能性がある。</p>	<p>HTTPSが設定されていれば証明書中に企業名が記載されている場合があり、組織の特定できる可能性がある。</p> <p>ログイン画面にバージョン情報は表示されていないがSecurityパッチ適用の通知が表示されるためこのことからバージョン情報が特定できる可能性がある。</p> 

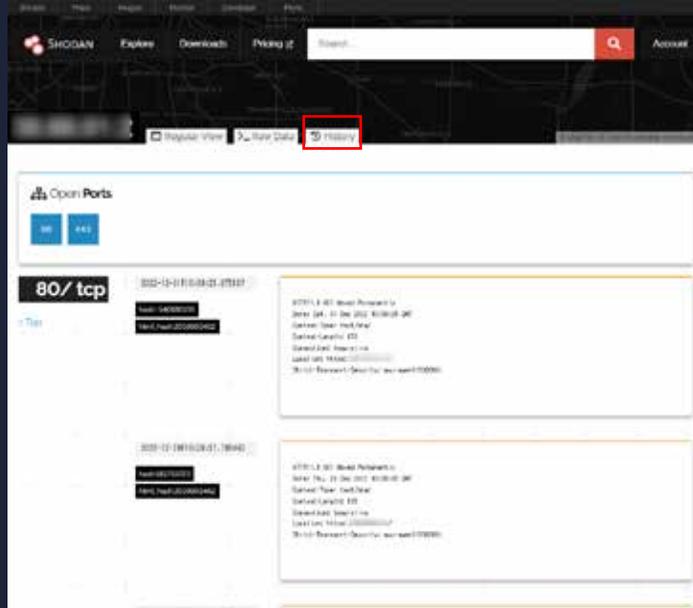
# バージョンアップやサーバ停止の確認



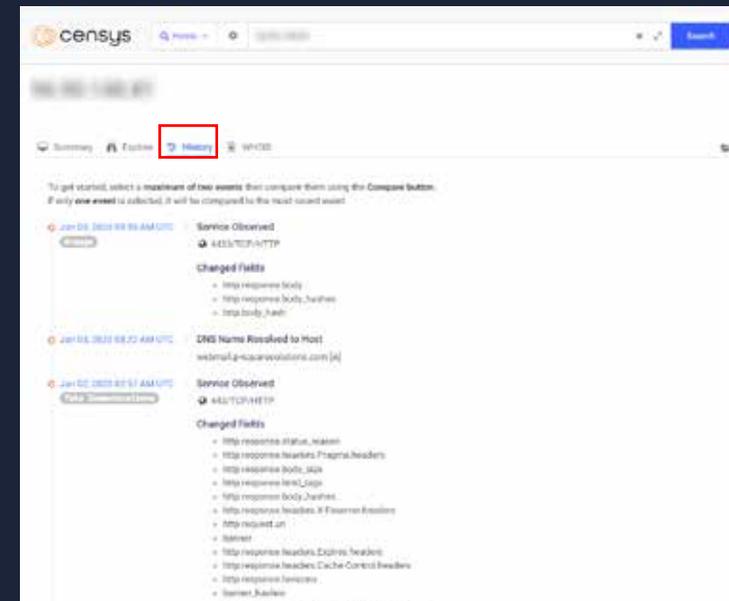
- 侵入被疑サーバの状態を継続確認する事で侵入経路の推測にも有用な材料となる
  - サーバレスポンスからバージョンアップ（パッチ適用）の推測
  - Webアクセスを行い疎通の確認。アクセス不可 撤去の可能性

- デバイス検索エンジンでも過去の結果が参照できる機能が提供されているため適宜活用する

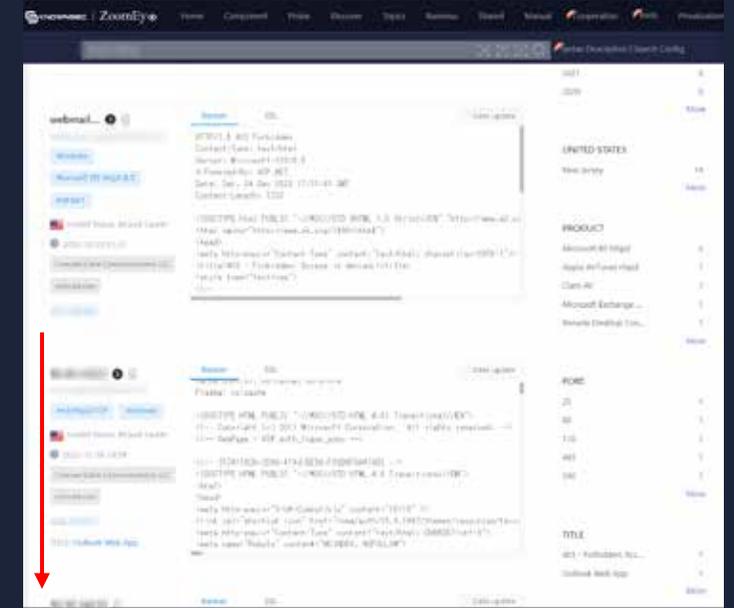
Shodan:Historyタブ参照



Censys:Historyタブ参照



ZoomEye:検索結果スクロールで過去分表示



# 最後に

攻撃者が狙う外部公開サーバの特定と防御は今後数年でも重要な施策になると考えます。

特に日本含むアジア圏では対処スピードも速くないため何らかの対策強化が必要です。  
本日までご参加・ご視聴いただいている皆様と一緒に現状をより良い方向へ動かすことができれば幸いです。

第3部の調査手法については追加検証が必要であるため是非実践いただき、  
なにかあれば右記アカウントまでご連絡いただけますと嬉しいです。

