サイバーセキュリティ最新攻撃動向と対策

- リモートワークで変わること、変わらないこと -

2021年 2月 25日 サイバーセキュリティセミナー2021 in 仙台

株式会社インターネットイニシアティブ　根岸 征史

自己紹介

根岸 征史 (@MasafumiNegishi)

IIJ グループの CSIRT 所属 (IIJ-SECT, 2001年結成)
https://sect.iij.ad.jp/

SANS JAPAN 公式インストラクター	(2007年〜)
OWASP Japan アドバイザリーボード	(2012年〜)
WASForum Hardening Project 実行委員	(2012年〜)
CODE BLUE レビューボード	(2015年〜)
NICT サイバーセキュリティ研究室 協力研究員	(2019年〜)
ポッドキャスト「セキュリティのアレ」	(2017年〜)

1. コロナ禍における脅威・環境の変化
2. リモートワークによる影響
3. 最近の脅威事例
4. 脆弱性への対応指針

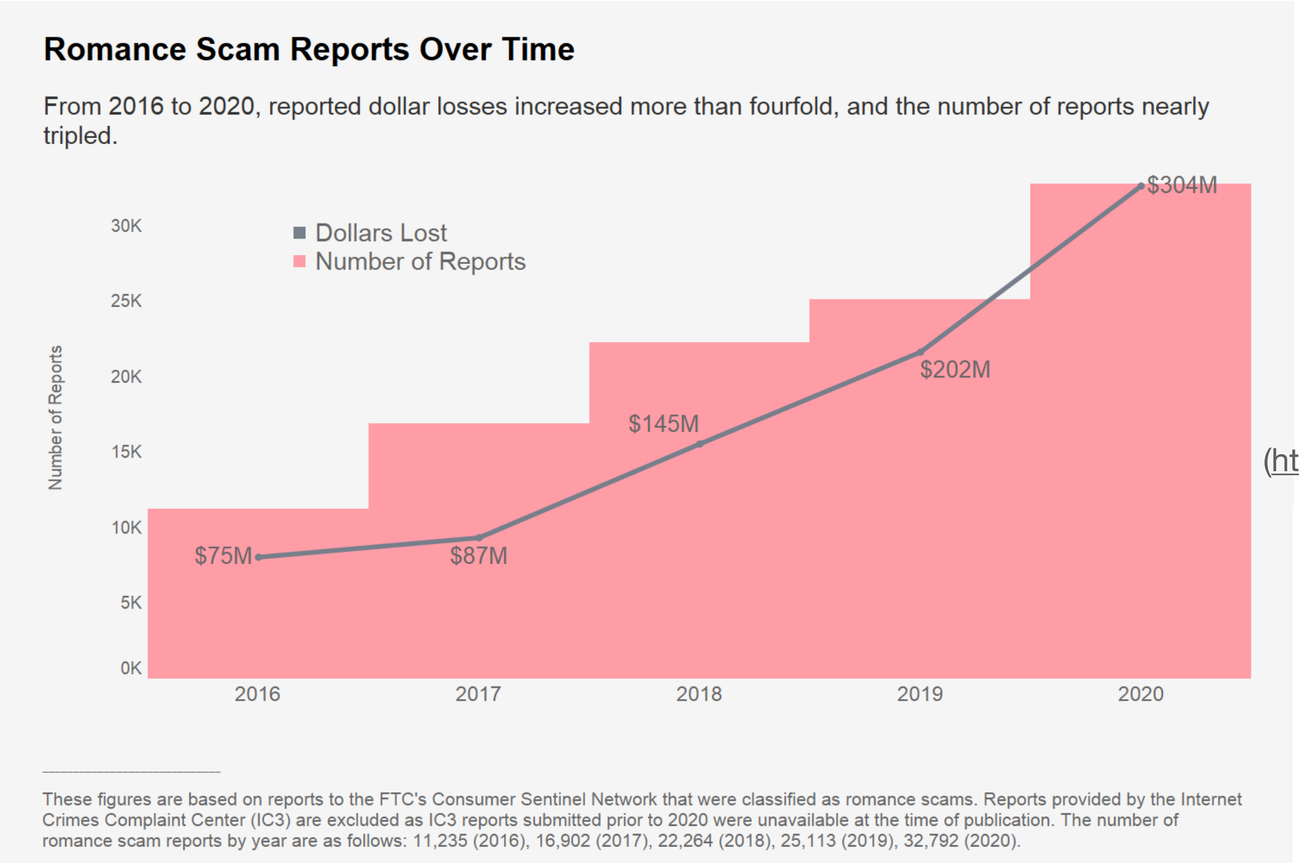
コロナ禍における脅威・環境の変化

脅威の変化

- リアル空間に起こるさまざまな制約・変化はサイバー空間にどのように影響するか
- IT 環境の変化に依存する部分も大きい
- RDP や VPN 機器の脆弱性は以前から狙われていたが、リモートワーク増加で、より攻撃者に注目される
- COVID-19 関連のフィッシング、ロマンス詐欺などが増加
- 攻撃と防御は鏡、相手のことをよく知ることが勝つために必要

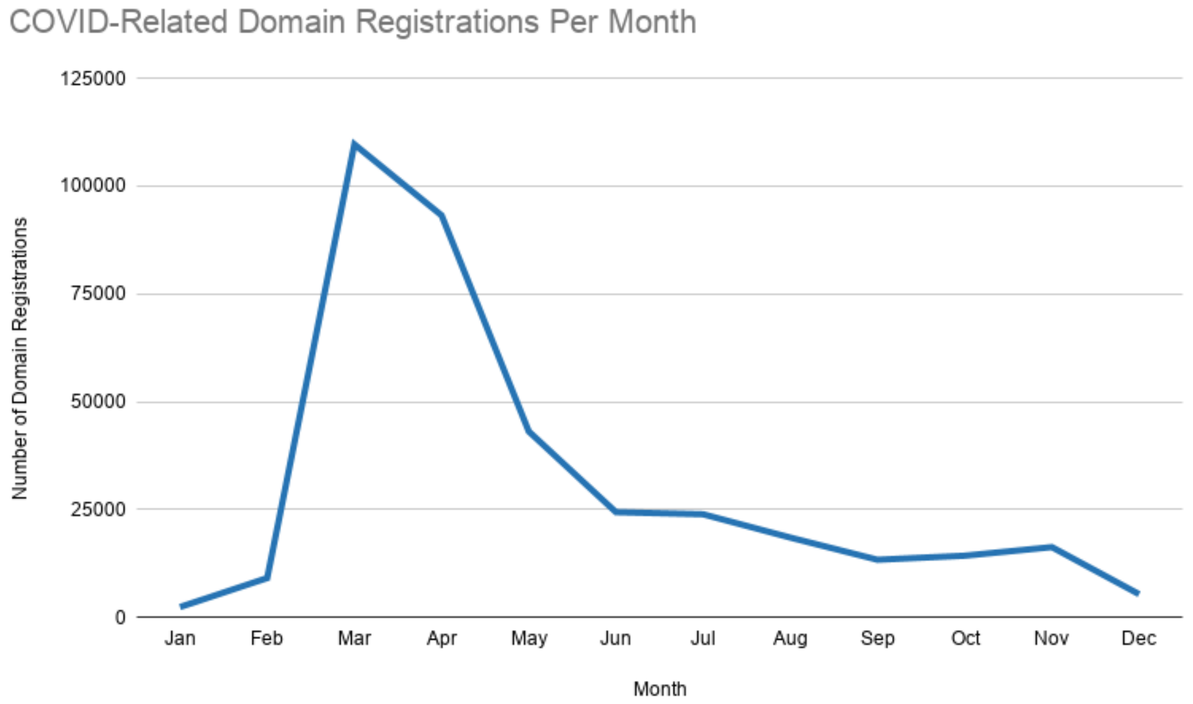
ロマンス詐欺の被害報告

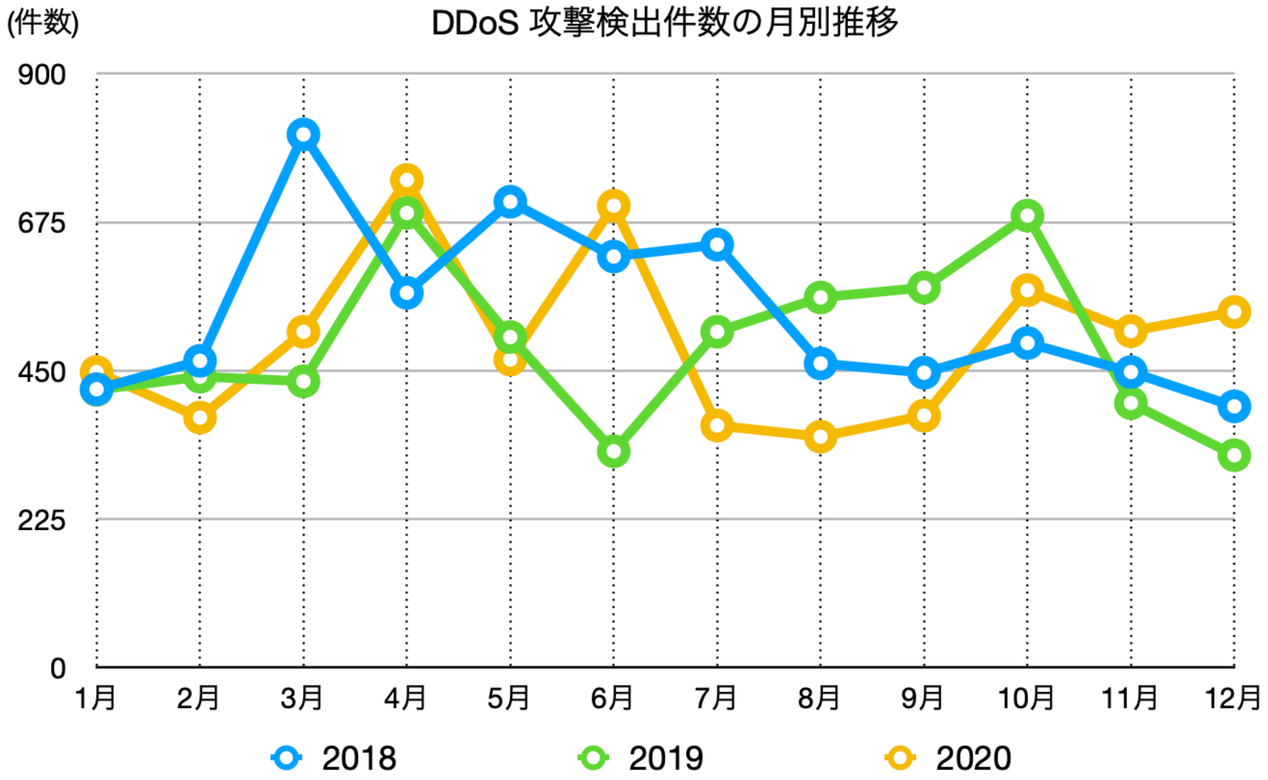
(https://www.ftc.gov/news-events/blogs/data-spotlight/2021/02/romance-scams-take-record-dollars-2020)

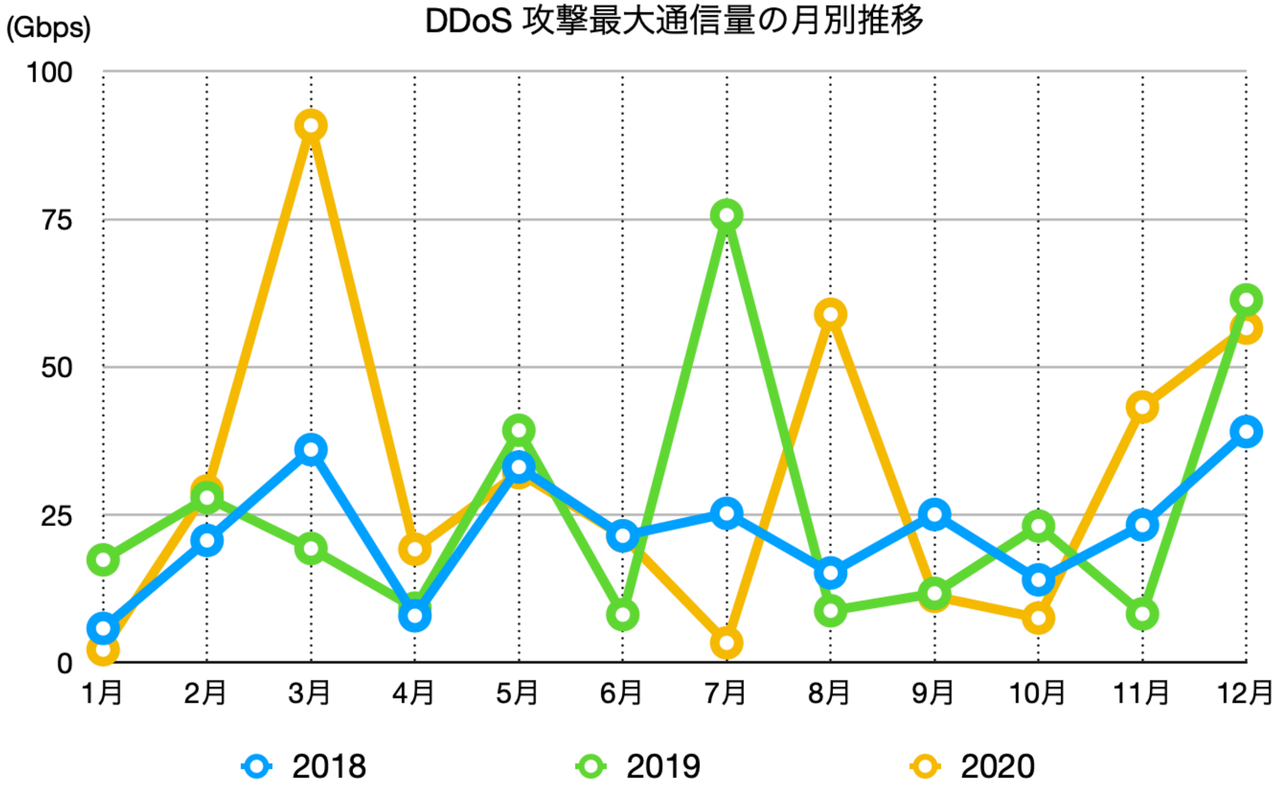


COVID-19 に関連したドメインの登録状況

(https://www.recordedfuture.com/opportunism-behind-cyberattacks-during-pandemic/)





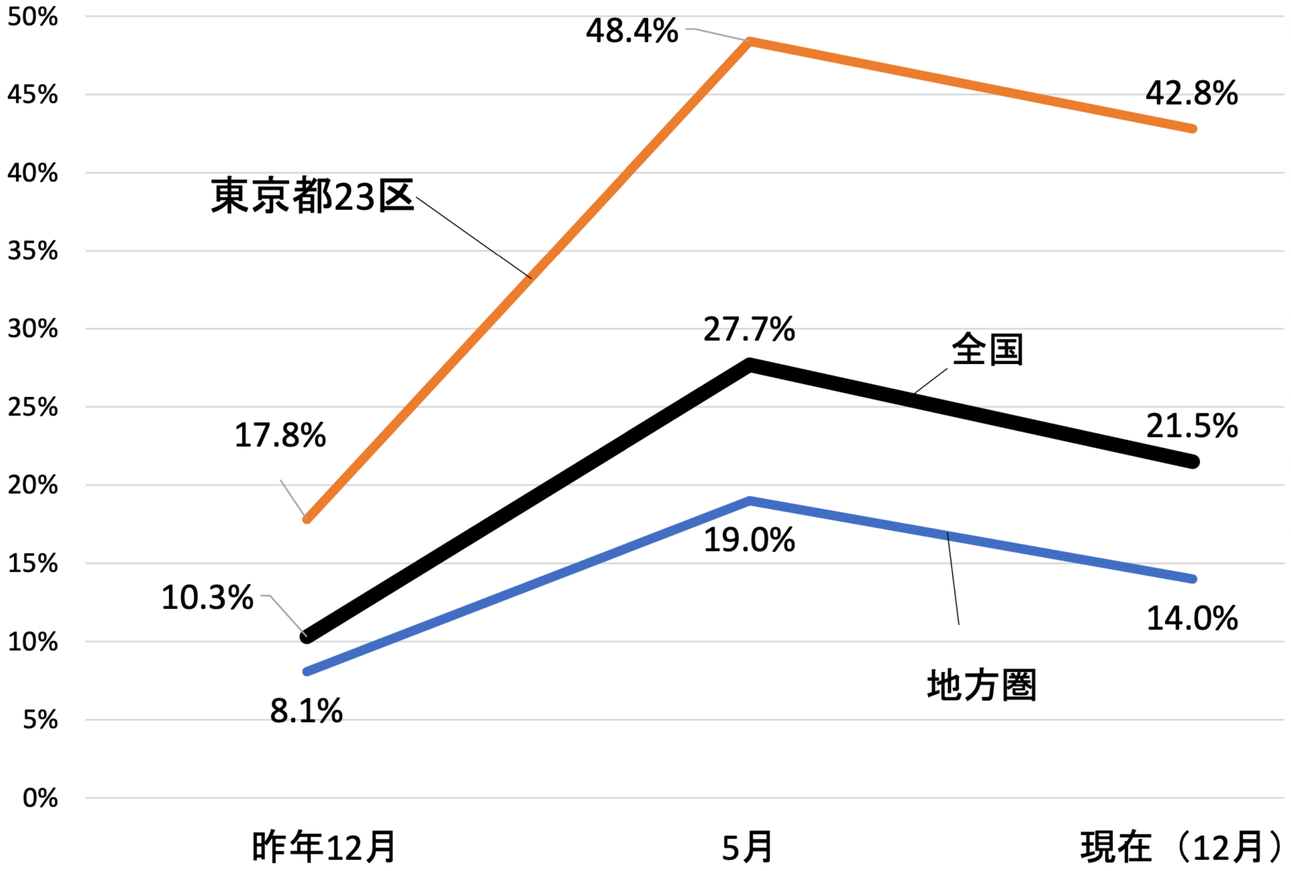


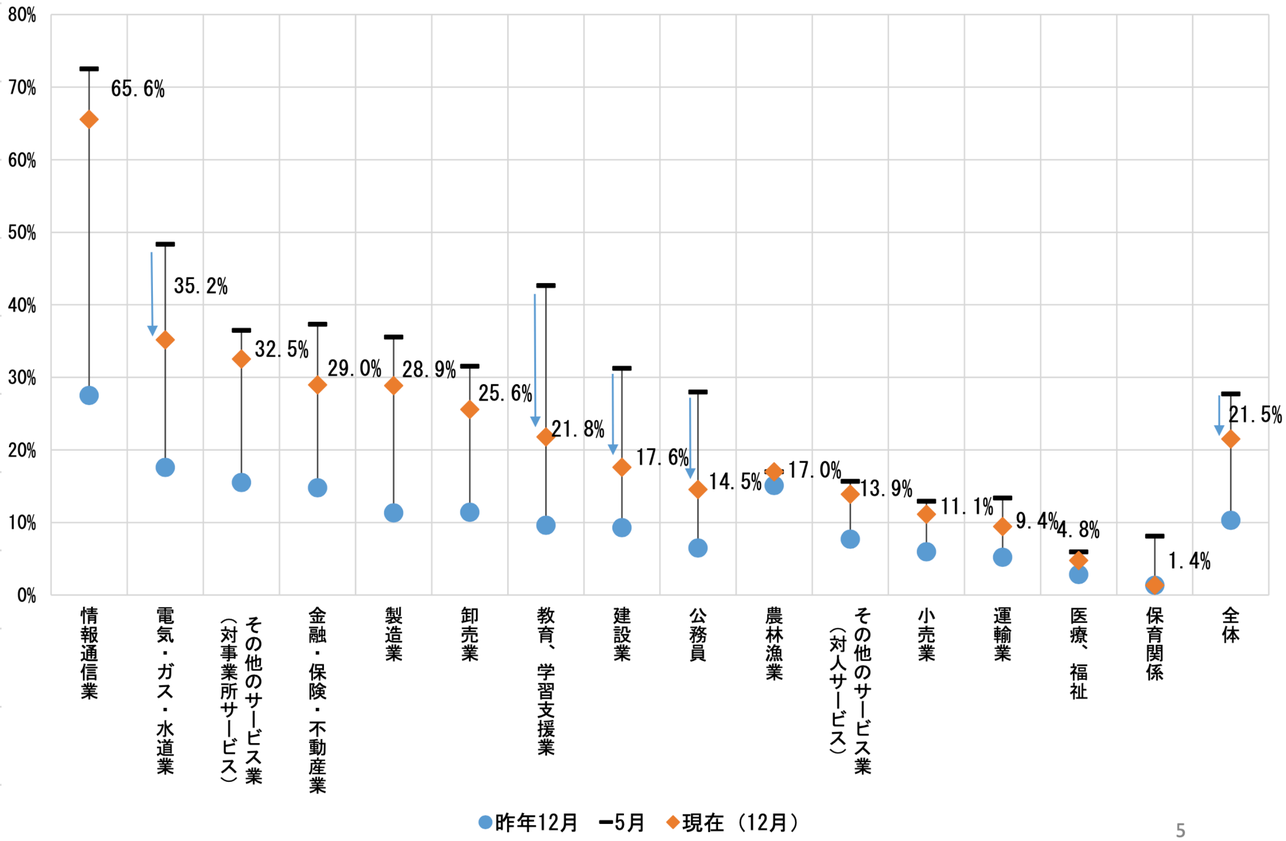
wizSafe Security Signal (https://wizsafe.iij.ad.jp/)


ノーガード
境界防御
縦深防御
Defense in Depth
侵入前提
Threat Hunting
ゼロトラスト
防止
検知
対応

リモートワークによる影響

リモートワーク実施状況

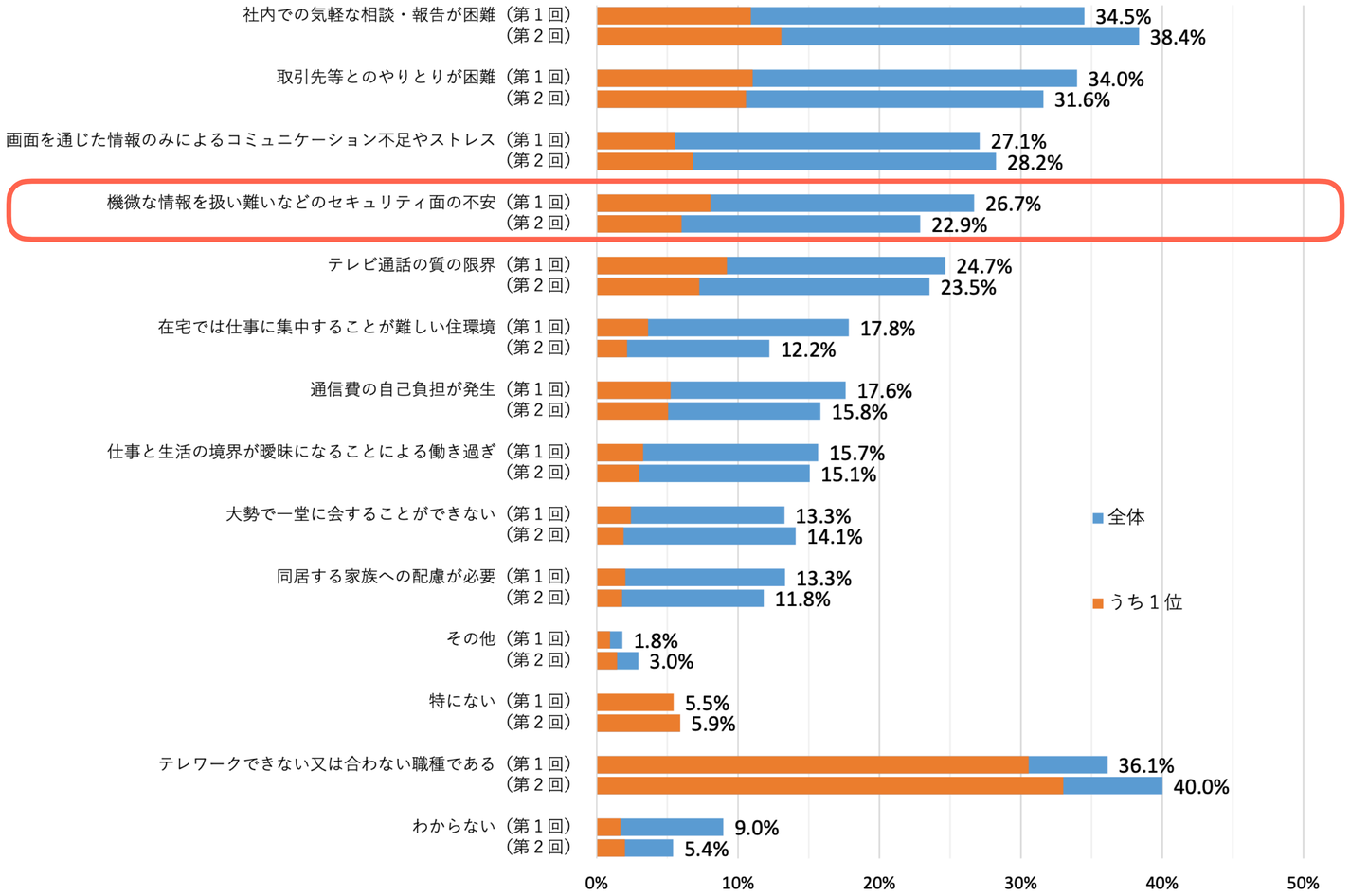




第2回 新型コロナウイルス感染症の影響下における生活意識・行動の変化に関する調査 (https://www5.cao.go.jp/keizai2/keizai-syakai/future2/20210119/agenda.html)

リモートワークの課題

1．【働き方】テレワークのデメリット（不便な点）（テレワーク経験者）



→ コミュニケーション

→ セキュリティ

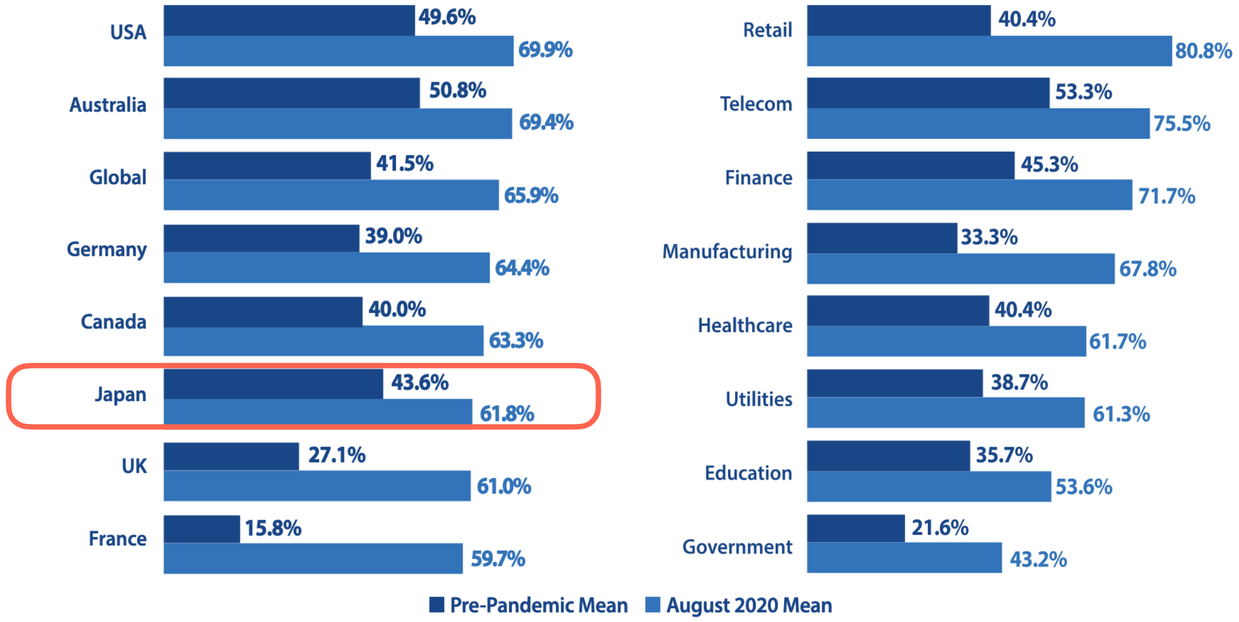
→ インフラ、環境

第2回 新型コロナウイルス感染症の影響下における生活意識・行動の変化に関する調査 (https://www5.cao.go.jp/keizai2/keizai-syakai/future2/20210119/agenda.html)

リモートワークの課題

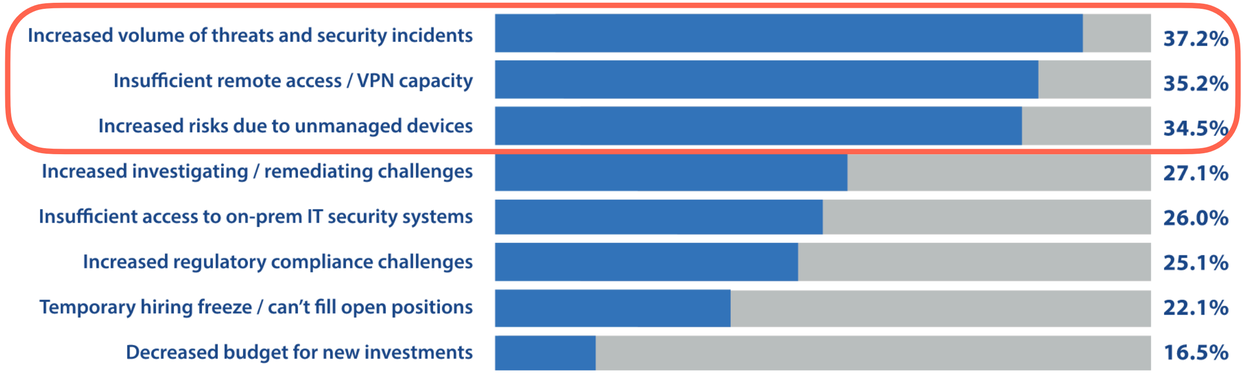
Increased BYOD Policy Adoptions

Does your organization have a BYOD (bring your own device) policy that permits employees to use personally owned devices to access company applications and data?



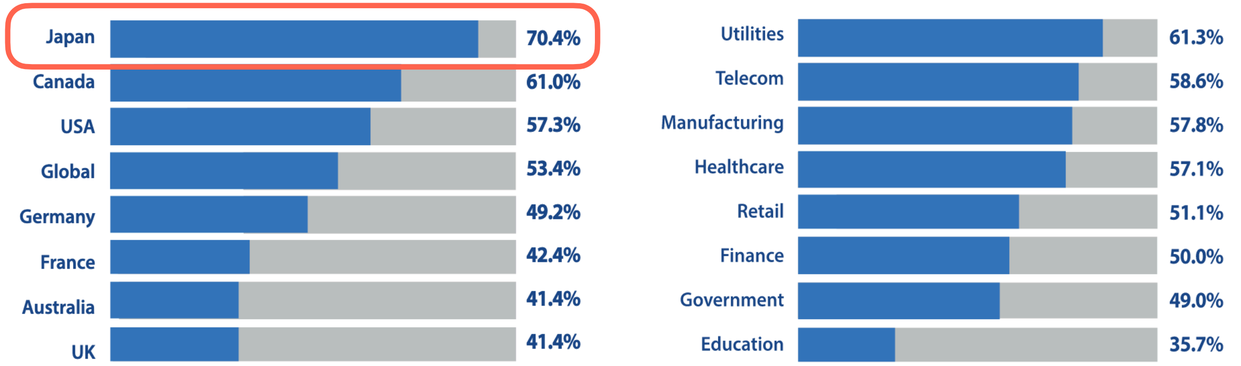
Operational Challenges

What have been the biggest challenges for your organization's IT security team during the COVID-19 pandemic? Select all that apply.



IT Security Personnel Shortage

Was your organization previously experiencing a shortage of skilled IT security personnel before the COVID-19 pandemic began?



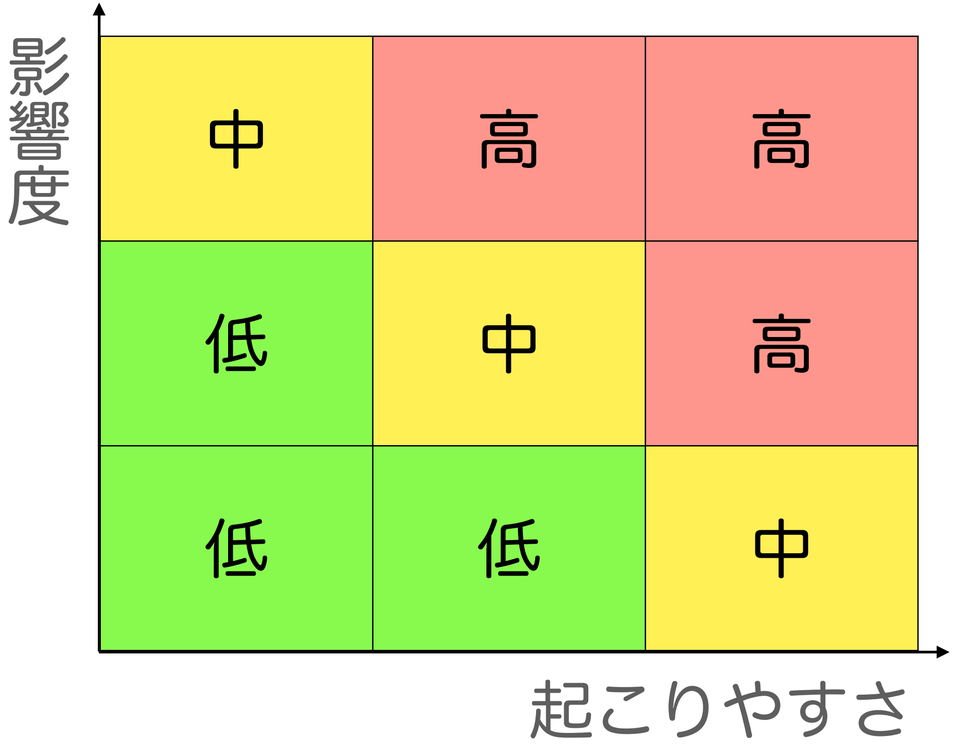
THE IMPACT OF COVID -19 ONENTERPRISE IT SECURITY TEAMS
(https://www.isc2.org/-/media/ISC2/Research/2020/COVID-19-Impact-Report/CyberEdge-COVID-19-Impact-Report.ashx)

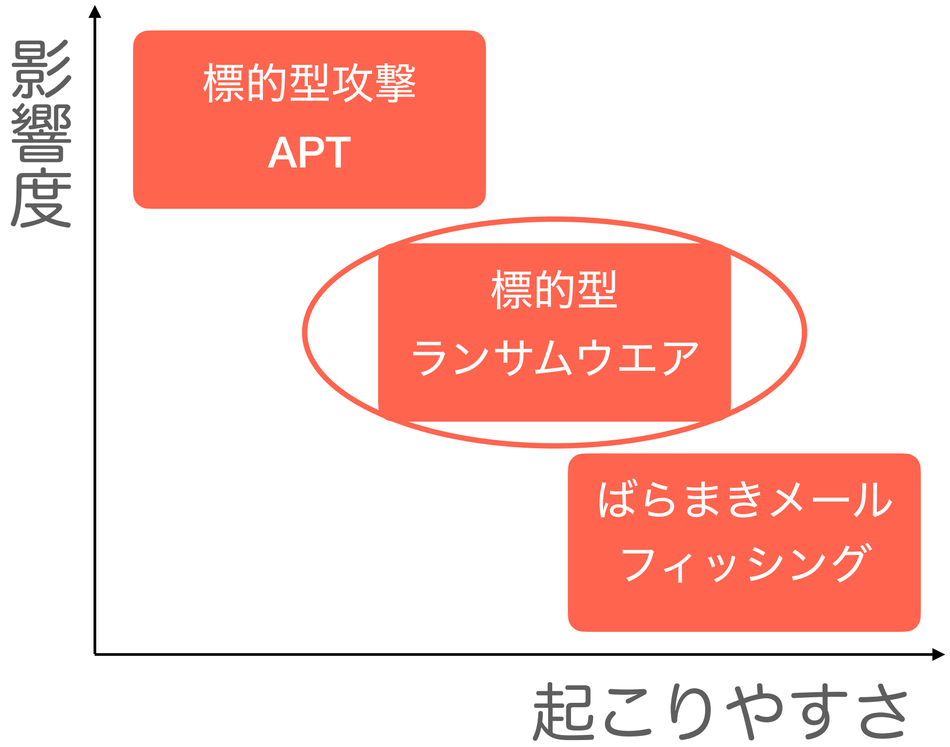
リモートワークの課題

- BYOD、VPN への対応
- インシデント発生時の初動対応
- セキュリティ人材不足の影響
- クラウドサービスのセキュリティ
- エンドポイントセキュリティ

最近の脅威事例

リスク分類


影響度
中
高
高
低
中
高
低
低
中
起こりやすさ


影響度
標的型攻撃
APT
標的型
ランサムウエア
ばらまきメール
フィッシング
起こりやすさ

標的型 + ランサムウェア + 情報流出

- 初期侵入経路はメール、RDP、VPN 機器が多い
- 侵入から感染に至る攻撃手法は標的型攻撃に近い
- 組織内で人手による横展開の活動を行い、多数の機器を一斉に感染させる
- ファイルの復号鍵の見返りとして金銭を要求する
- 感染前に組織内の情報を窃取し、身代金を支払わない場合に情報を流出させると2重に脅迫する

(参考) 【注意喚起】事業継続を脅かす新たなランサムウェア攻撃について：IPA 独立行政法人 情報処理推進機構 (https://www.ipa.go.jp/security/announce/2020-ransom.html)

“Opportunistic” Ransomware		“Targeted” Ransomware
不特定多数の個人	攻撃対象	特定企業、業種の組織
スパムメール ドライブバイダウンロード	初期感染	スピアフィッシングメール RDP や VPN からの侵入
なし (あるいは自動)	感染拡大	手動による横展開 (潜伏調査期間あり)
低額 (端末単位)	身代金	高額 (組織単位、交渉の余地あり)
Locky, Cerber など	例	Ryuk, Maze など

リモートワークに関連した攻撃事例

- M社事例 (2020年)
  4月に在宅勤務中の従業員の社有 PC が SNS 経由でマルウェアに感染し、5月の出社時に社内ネットワーク経由で感染が拡大した

- H社事例 (2020年)
  4月後半の在宅勤務(テレワーク)による VPN 機器の負荷増大への対応のため、旧 VPN 装置を急遽再稼動させたが、脆弱性に未対応だったため、外部から不正アクセスされた

脆弱性への対応指針

脆弱性のライフサイクルと攻撃活動

- 2019年の CVE 1.8万件以上のうち、実際に攻撃が観測された脆弱性は 473件 (大半の組織に影響を及ぼすものはさらに少ない)
- パッチ公開前に 1/3 の脆弱性は攻撃コードが公開ずみ
- パッチ公開から 2日以内に 5%、1ヶ月以内に 45% の脆弱性で攻撃が観測される
- 攻撃コード公開前から攻撃が観測される脆弱性は 30%、公開後 1ヶ月以内に 56% の脆弱性で攻撃が観測される

Prioritization to Prediction Volume 6
https://www.kennasecurity.com/resources/prioritization-to-prediction-reports/

2020年に悪用された脆弱性

Alert (AA20-133A) Top 10 Routinely Exploited Vulnerabilities

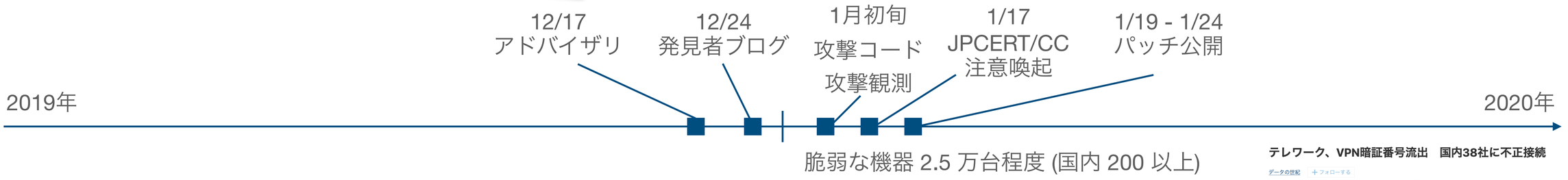
Vulnerabilities Exploited in 2020

In addition to the top 10 vulnerabilities from 2016 to 2019 listed above, the U.S. Government has reported that the following vulnerabilities are being routinely exploited by sophisticated foreign cyber actors in 2020:

- Malicious cyber actors are increasingly targeting unpatched Virtual Private Network vulnerabilities.
  - An arbitrary code execution vulnerability in Citrix VPN appliances, known as CVE-2019-19781, has been detected in exploits in the wild.
  - An arbitrary file reading vulnerability in Pulse Secure VPN servers, known as CVE-2019-11510, continues to be an attractive target for malicious actors.
- March 2020 brought an abrupt shift to work-from-home that necessitated, for many organizations, rapid deployment of cloud collaboration services, such as Microsoft Office 365 (O365). Malicious cyber actors are targeting organizations whose hasty deployment of Microsoft O365 may have led to oversights in security configurations and vulnerable to attack.
- Cybersecurity weaknesses—such as poor employee education on social engineering attacks and a lack of system recovery and contingency plans—have continued to make organizations susceptible to ransomware attacks in 2020.

https://us-cert.cisa.gov/ncas/alerts/aa20-133a

Citrix ADC (CVE-2019-19781)



脆弱な機器 2.5 万台程度 (国内 200 以上)

テレワーク、VPN暗証番号流出　国内38社に不正接続

データの世紀　＋フォローする

2020年8月24日 20:00 (2020年8月25日 5:33更新) [有料会員限定]

保存

日立化成や住友林業など国内の38社が不正アクセスを受け、テレワークに欠かせない社外接続の暗証番号が流出した恐れがあることが分かった。第三者が機密情報を抜き取ったり、ウイルスをばらまいたりする2次被害が予想される。事態を重く見た内閣サイバーセキュリティセンター（NISC）も調査に乗り出しており、企業は対策が急務となっている。

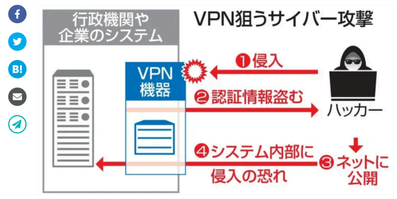
Pulse Connect Secure (CVE-2019-11510)

脆弱な機器 1.5 万台程度 (国内 1,500 以上)

600超の組織にサイバー攻撃

テレワーク機器の欠陥悪用

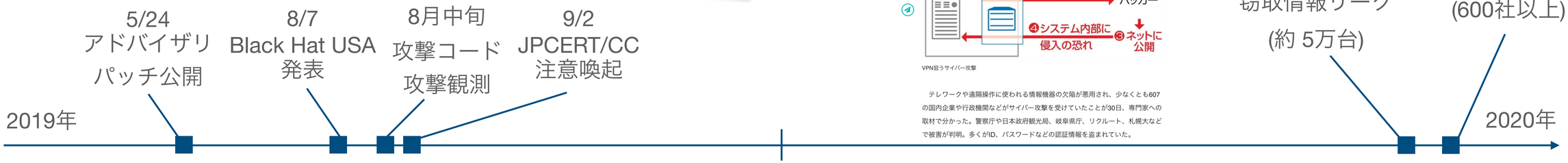
2020/12/1 06:00 (JST)　12/1 06:17 (JST) updated　©一般社団法人共同通信社



VPN狙うサイバー攻撃

テレワークや遠隔操作に使われる情報機器の欠陥が悪用され、少なくとも607の国内企業や行政機関などがサイバー攻撃を受けていたことが30日、専門家への取材で分かった。警察庁や日本政府観光局、岐阜県庁、リクルート、札幌大などで被害が判明。多くがID、パスワードなどの認証情報を盗まれていた。

Fortigate SSL-VPN (CVE-2018-13379)



脆弱性管理

- 実際に自組織に影響を及ぼす脆弱性の状況を迅速に把握し、対応の優先度を判断できているか？
- 適切な脆弱性管理を行うためには、ベースラインとなる資産管理、構成管理、変更管理、アカウント管理、などが必要となる
- 外部サービスにおけるパスワード漏洩を前提としたアカウントの保護、多要素認証の適用

まとめ

- 脅威、IT 環境の変化への対応 → 敵を知り、己を知る
- リモートワークにおける様々な課題
  → BYOD、VPN、クラウド、エンドポイント
- 標的型ランサムウェアへの対応 → 初期侵入経路
- 脆弱性への対応 → 適切な優先順位付け