国内事例から考える、ネットワーク層で守るランサムウェア対策のベストプラクティス

Netskope Japan株式会社
エバンジェリスト　大元 隆志

netskope

自己紹介

【セキュリティに関する社会貢献】

■セキュリティニュース解説

ヤフーニュース公式
コメンテータとして
国内外のセキュリティ
トピックに関する
記事寄稿、解説を担当

■学生向けセキュリティ教育

人と社会を支える力
国士舘大学
Kokushikan

国士舘大学にて
セキュリティに関する
非常勤講師を担当

■企業向けセキュリティ研修講座監修

最高評価

IPA SECURITY ACTION
に対応した従業員用
セキュリティ講座監修

［アニメで学ぶ］情報セキュリティ」

■Netskope Japanにおける職務内容

Netskope Japan エバンジェリスト兼
パートナ担当 SE。

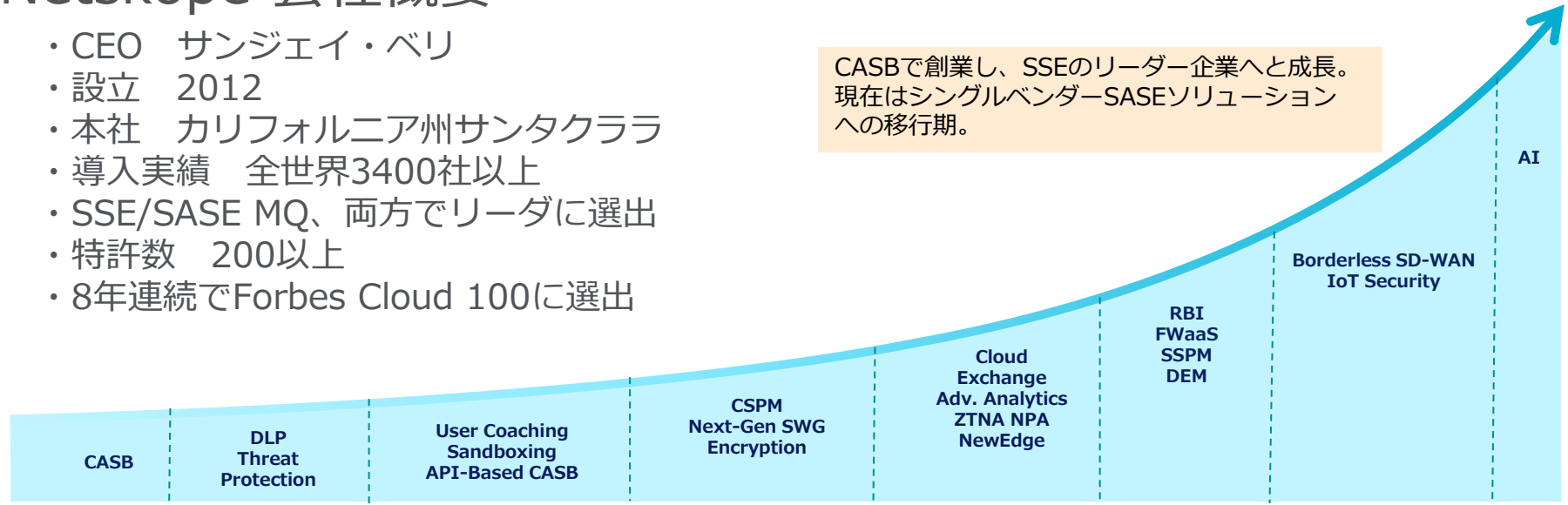
Netskope パートナー企業様の提案活動の支援。
- 共同セミナー開催、社内向け勉強会開催
- お客様提案支援
- Netskope 技術者育成
- その他、クラウドセキュリティに関する全般的な相談についてお気軽にお声がけください。

・所有資格:CISM、CISA、CDPSE、AWS SA Pro、CCSK、個人情報保護監査人、シニアモバイルシステムコンサルタント。

Netskope 会社概要

- CEO　サンジェイ・ベリ
- 設立　2012
- 本社　カリフォルニア州サンタクララ
- 導入実績　全世界3400社以上
- SSE/SASE MQ、両方でリーダに選出
- 特許数　200以上
- 8年連続でForbes Cloud 100に選出

CASBで創業し、SSEのリーダー企業へと成長。
現在はシングルベンダーSASEソリューション
への移行期。



各業界を代表する企業がNetskopeを導入

金融	医療	通信 キャリア	小売	製造業
トップ 4のうち2	トップ 7のうち5	トップ 3のうち2	トップ 5のうち2	トップ 9のうち4

決算に影響を与えたランサムウェア国内事例

2024年、決算に影響を与えたランサムウェア国内事例

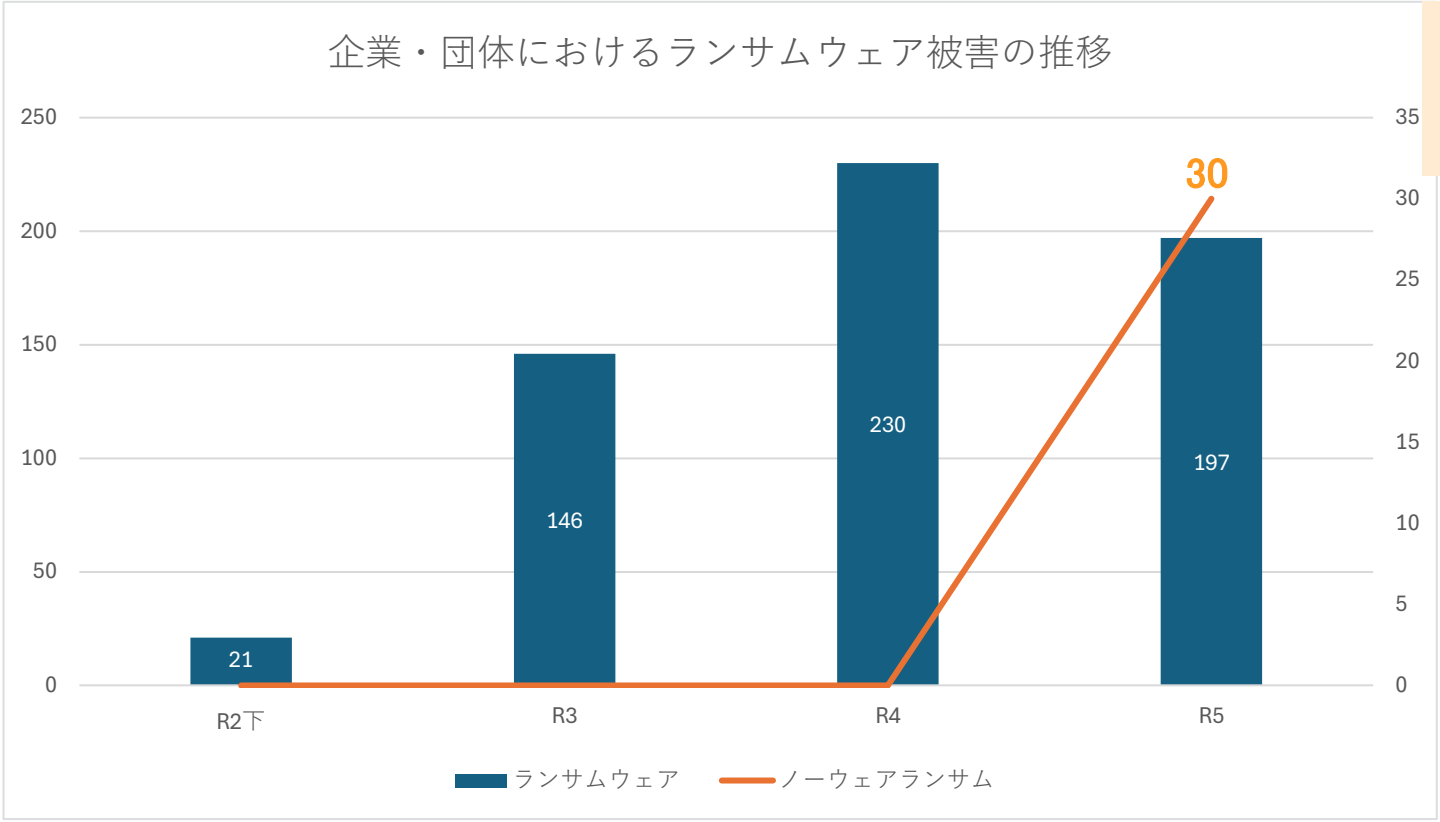
2024年1月1日から8月31日までに開示された決算報告書を対象としてGoogle検索にて調査。
日本国内の事例でも、ランサムウェアの被害は企業経営に多大なインパクトを与える状況に。

・**特別損失**(主にシステム復旧、セキュリティ強化に伴う費用)
情報・通信業:システム障害対応費用として**19億8千7百万円**
情報・通信業:システム障害対応費等で2億7千6百万円
製造業:情報セキュリティ対策費として6千2百万円

・**機会損失**(主に営業活動による販売機会の逸失)
流通業:販売機会逸失などによる利益影響、**約29億円**
製造業:営業活動、売上受注に対する影響が発生。逸失売上、年間売上に対して1%程度

・**決算発表の延期**
流通業:2月15日に被害発生。4月9日に予定していた決算発表を延期。
製造業:1月16日に被害発生。2月13日に概ね復旧、金融商品取引法第24条の４の７第１項に定める法定提出期限である2024年３月18 日までの提出に間に合わないと判断。

急増するノーウェアランサム



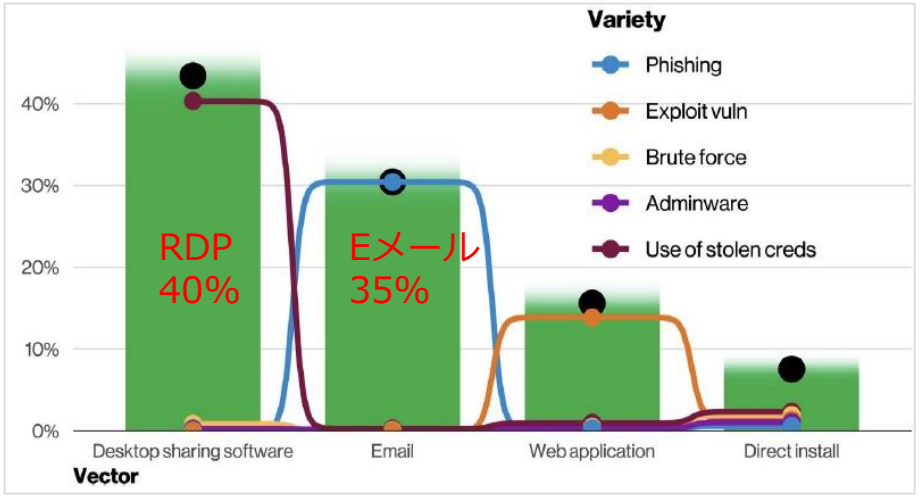
ノーウェアランサム
データを暗号化せず
(ランサムウェアを使わない)
データを盗難し恐喝する攻撃

図:警察庁「令和5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」を基にNetskope Japan作成

ランサムウェア侵入傾向

ランサムウェアの侵入経路は世界と日本で若干異なりますが、狙われるのは外部との境界点。
かつ、**管理者が把握出来ていない「IT資産や脆弱性が放置された機器」**であることが多い。

グローバルでの侵入傾向



出典:Verizon DBIR 2022

日本での侵入傾向

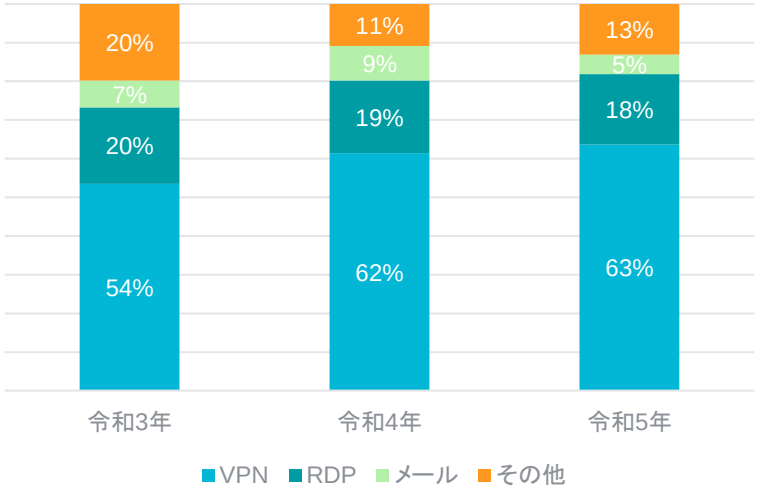


図:警察庁「サイバー空間をめぐる脅威の情勢」を基にNetskope Japan作成

日本ではVPNからの侵入が圧倒的

CISA、FBI、VPNからSASE/SSEへの移行を推奨

America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Search

Topics | Spotlight | Resources & Tools | News & Events | Careers | About

Home / Resources & Tools / Resources

Modern Approaches to Network Access Security

Publish Date: June 18, 2024

RELATED TOPICS: SECURING NETWORKS, CYBERSECURITY BEST PRACTICES, ORGANIZATIONS AND CYBER SAFETY

CISA, in collaboration with the following organizations, co-authored this joint guidance:

- Federal Bureau of Investigation (FBI)
- New Zealand's Government Communications Security Bureau (GCSB);
- New Zealand's Computer Emergency Response Team (CERT-NZ); and
- The Canadian Centre for Cyber Security (CCCS).

The guidance urges business owners of all sizes to move toward more robust security solutions—such as Zero Trust, Secure Service Edge (SSE), and Secure Access Service Edge (SASE)—that provide greater visibility of network activity. Additionally, this guidance helps organizations to better understand the vulnerabilities, threats, and practices associated with traditional remote access and VPN deployment, as well as the inherent business risk posed to an organization's network by remote access misconfiguration.

米国CISAが、以下組織と共同でレガシーVPNからSASE/SSEへの移行を推奨するガイダンスを発表。

連邦捜査局（FBI）
ニュージーランド政府通信保安局（GCSB）
ニュージーランドのコンピュータ緊急対応チーム（CERT-NZ）
カナダサイバーセキュリティセンター（CCCS）

これまではレガシーVPN経由での不正アクセス等が発生しても、あくまで企業側は被害者でした。

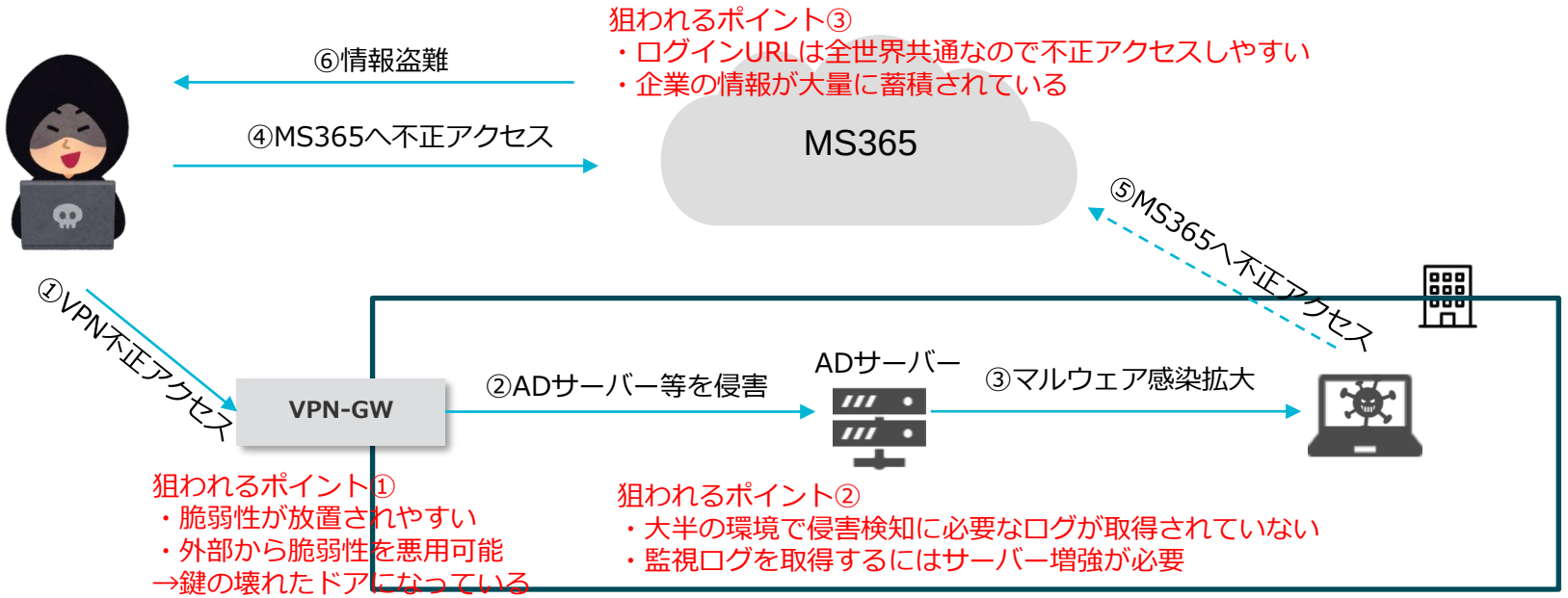
しかし、このようなガイダンスが発表されたことで、今後はランサムウェアや不正アクセス被害を受けた際に、レガシーVPNが原因となった場合には、「脆弱な部分を放置していた」となり、CISO等の説明責任が問われる可能性が御座います。

出典:https://www.cisa.gov/resources-tools/resources/modern-approaches-network-access-security

ケース1:
VPNからの侵入

国内事例1

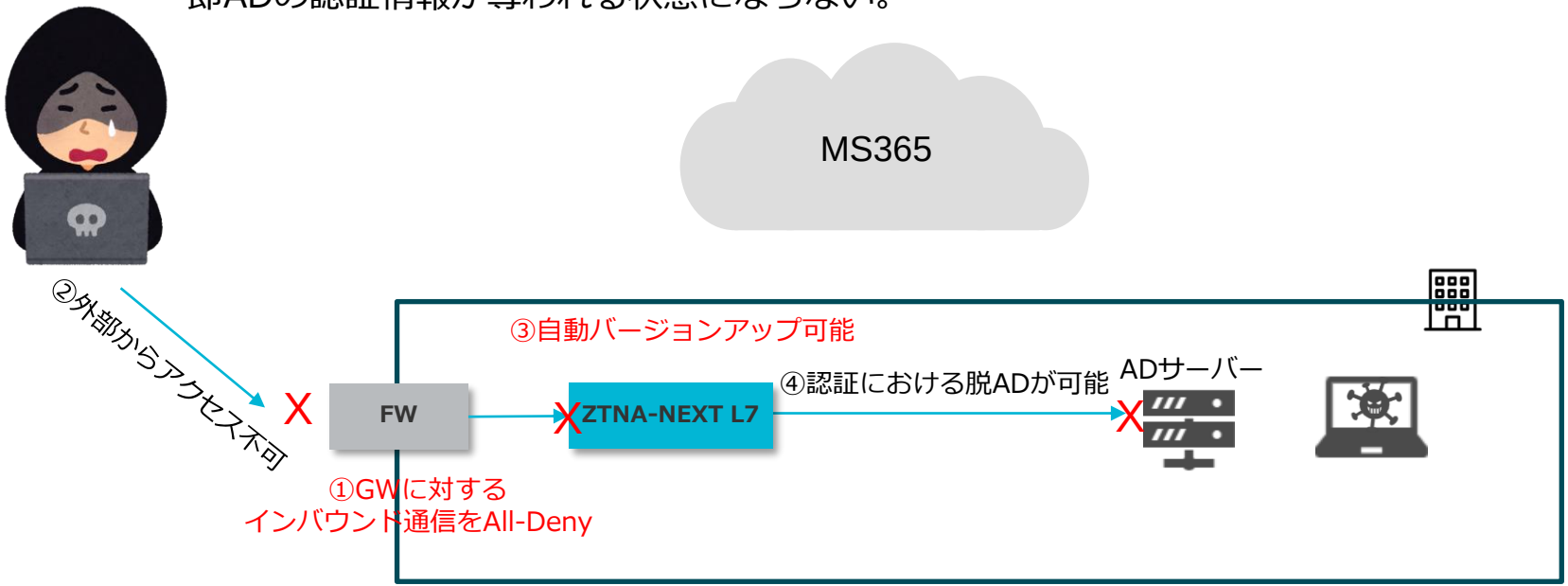
A社公表の侵害範囲
①第三者がVPN装置の脆弱性を起点にA社の一部のサーバ及び端末に侵入。
②侵入したサーバからさらに侵害を広げ、アカウント情報等を窃取。
③窃取したアカウント情報等を用いて、MS365に対して正規ユーザを装った不正アクセスを実施。



もし、Netskopeがあったなら

①VPN
不正アクセス

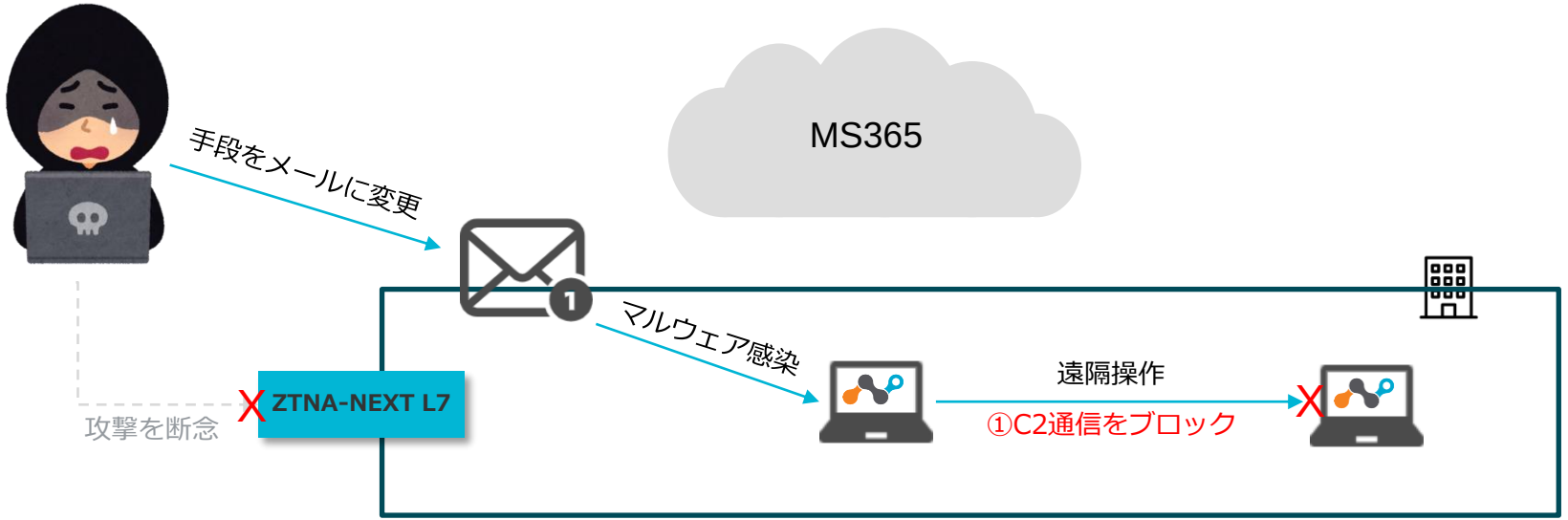
①Netskope ZTNA NEXT L7ならGWに対するインバウンド通信をAll-Deny可能
②従って、外部からの偵察活動不可、外部からアクセス不可
③仮に脆弱性が発見されても、自動バージョンアップ可能(脆弱性が放置されない)
④万が一、GWが侵害されてもADに依存しない認証形式が可能。
　即ADの認証情報が奪われる状態にならない。



もし、Netskopeがあったなら

③マルウェア
感染拡大

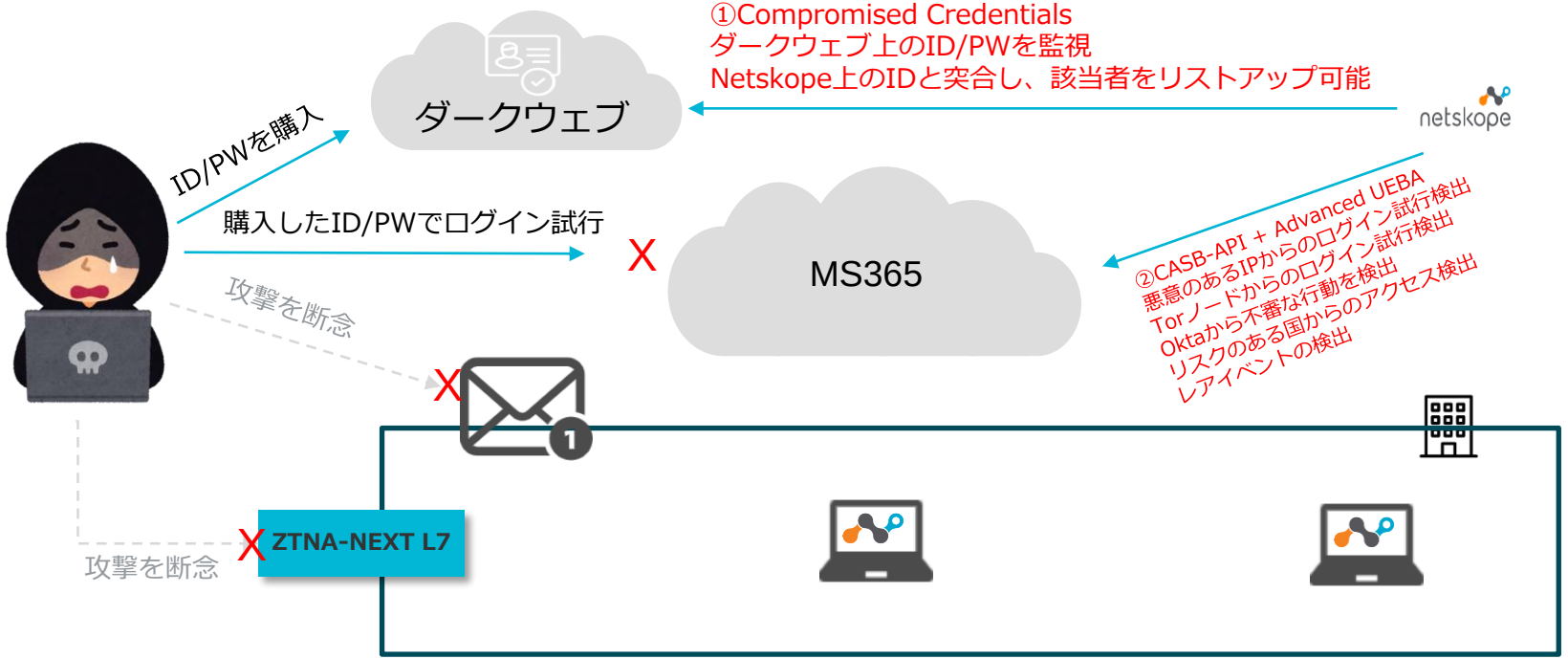
①万が一、社内に侵入された場合には、遠隔操作に用いられるC2通信をブロック可能です。
※EDR/EPP等を併用し、多層防御推奨



もし、Netskopeがあったなら

④MS365への
不正アクセス

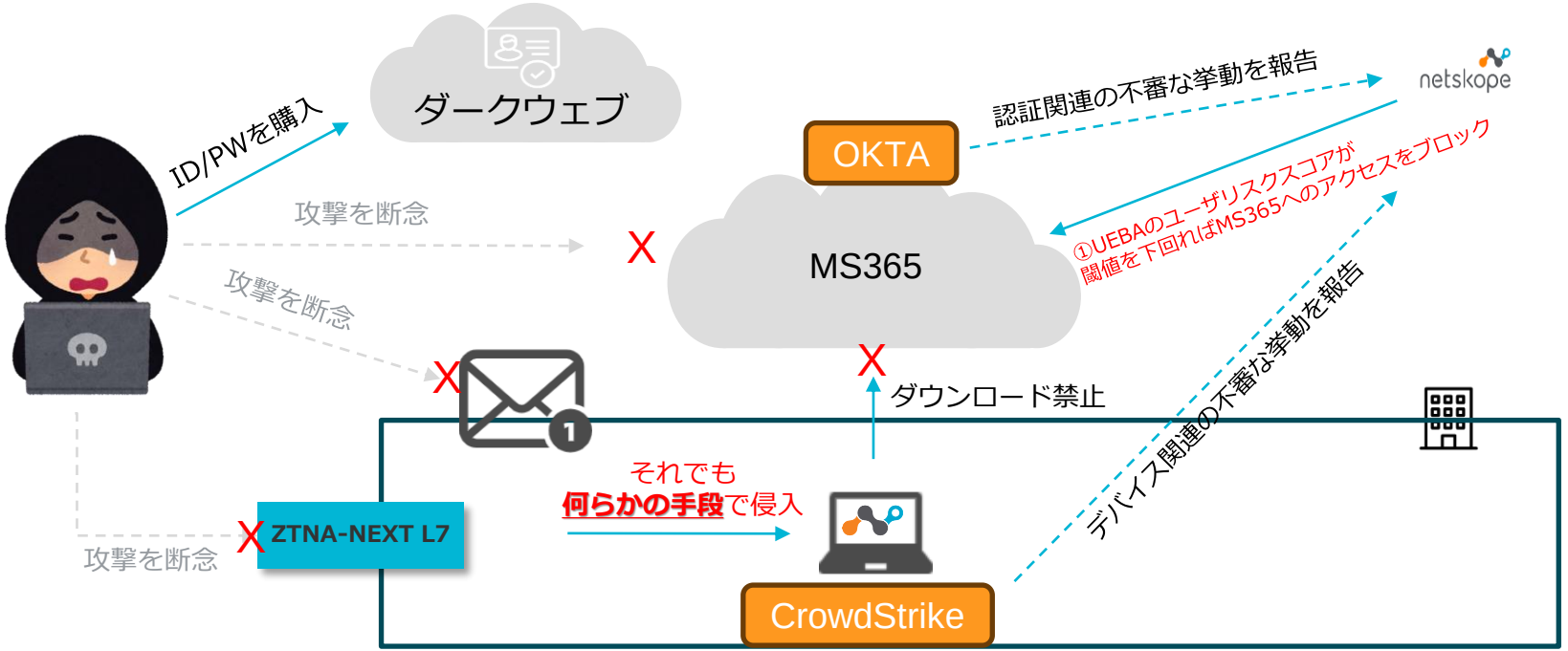
①ダークウェブ上に流出したIDを検出可能です。
②CASB-APIとUEBAから不審なアクセスを早期検出可能です。
※OKTA等との多要素認証併用を推奨



もし、Netskopeがあったなら

⑤MS365への
不正アクセス

①何らかの手段で多層防御をすり抜けられた場合であっても
UEBAによるスコアリングにより、スコア値が一定値を下回ればMS365への
アクセスを禁止することが可能。



「侵入される前提」ではなく「侵入されにくい」対策へ

「**何らかの手段**」**での侵入を想定した場合、対策コストは無尽蔵になります**。入口対策を最優先とし、「侵入されにくい」状態を維持することが、まずは現在のランサムウェア対策における最優先事項と捉えることを推奨します。

ウィルス、マルウェアが主流の時代

業務停止等の被害に発展することが少なく「**何らかの手段**」を想定し、**侵入される前提**での防御が主流でした。

・主な被害
情報盗難、Bot化

・有効な対策手段
感染防止　：　アンチマルウェア
異常検知等：　EDR

侵入される前提の防御でOKだった

ランサムウェアが主流の時代

ランサムウェアの場合は身代金を支払わせることが目的であるため
システム停止等も仕掛けられるため「事前対策」がより重要となります。

・主な被害
情報盗難、**恐喝、システム破壊**

・有効な対策手段
入り口対策　：　外部との接点のセキュリティ強化
感染防止　：　アンチマルウェア
復旧対策　：　オフラインバックアップ対策
暴露対策　：　データ保護
異常検知等：　EDR

“侵入されにくい”状態の維持が大切

Netskopeによるランサムウェアに「侵入されにくい」対策例

低コストで仕掛けられる80%の攻撃を軽減

攻撃対象領域の最小化

攻撃手口
・外部からスキャン可能なRDP
・外部から偵察可能な脆弱性を含むVPN

Netskopeによる対策
・野良IaaS利用者の可視化
・ZTNAによるゲートウェイの隠蔽

初期侵害の防止

攻撃手口
・フィッシングメール
・ダークウェブ等から入手したID/PW

Netskopeによる対策
・AI/MLによるフィッシングサイト検出
・RBIによる危険なサイトでの行動制限
・ダークウェブ上に流出したID/PW情報の検出

ラテラルムーブメントの防止

攻撃手口
・遠隔操作を実行し、感染拡大を試みる

Netskopeによる対策
・C&C通信のブロック
・UEBA/IPSで不審な挙動をブロック

EDR/EPPによるデバイス保護

データ流出の防止

攻撃手口
・シャドーITへの情報流出

Netskopeによる対策
・シャドーITの利用状況可視化
・新規登録ドメイン等へのアクセスブロック

データ盗難の防止

攻撃手口
・認可クラウドからの情報取得

Netskopeによる対策
・DLPによる機密情報保護

多層防御で防ぐ

ケース2:
SNSでの拡散

国内事例2

報道内容から推測
ダークウェブに情報が公開され、その後SNS等で公開されたデータが拡散された。

ダークウェブ上のデータが
SNSで拡散されるという異常事態

ダークウェブに情報公開

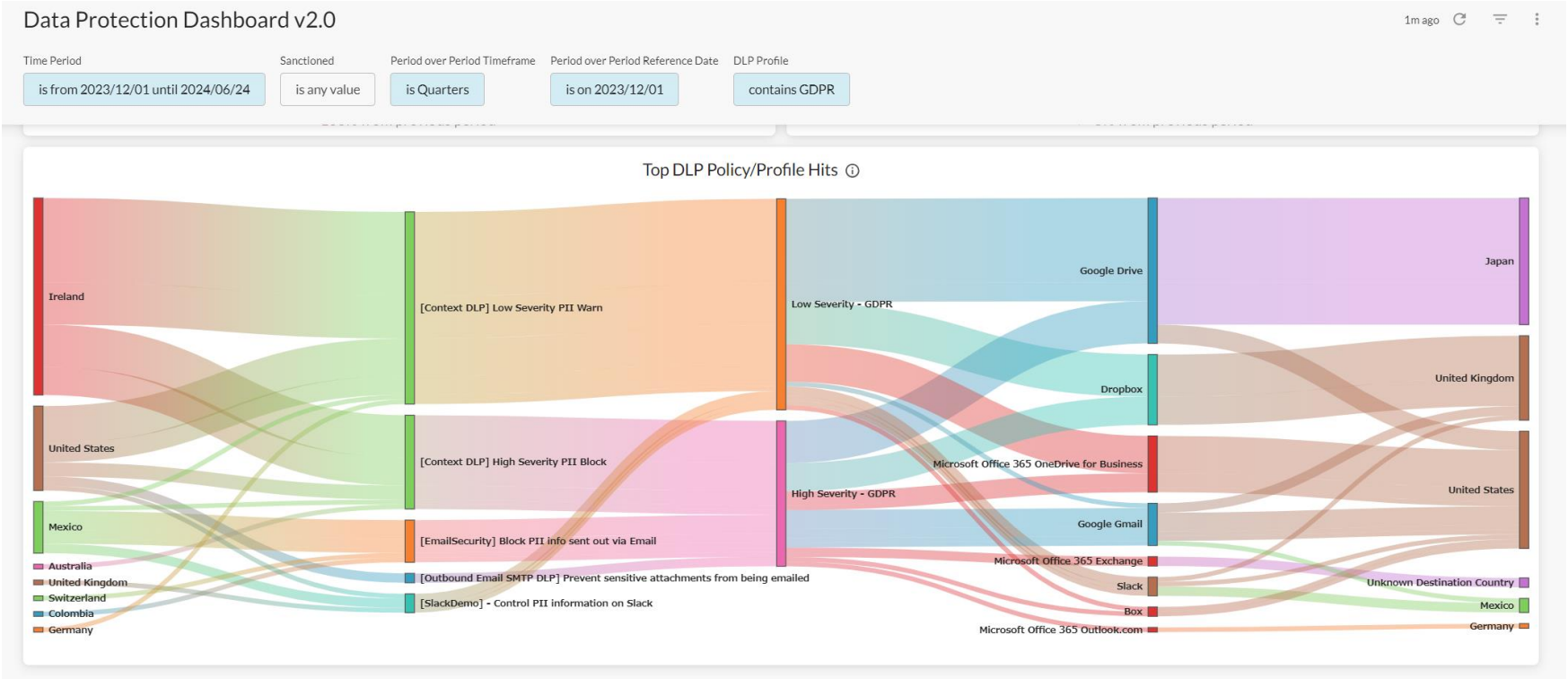
ダークウェブ

ダークウェブに
アクセス

■認識しておくべき社会環境の変化
・世の中の興味を集めることで、マネタイズ出来るようになった社会環境の変化
・プライバシーに関する情報は注目を集めやすい

もし、Netskopeがあったなら

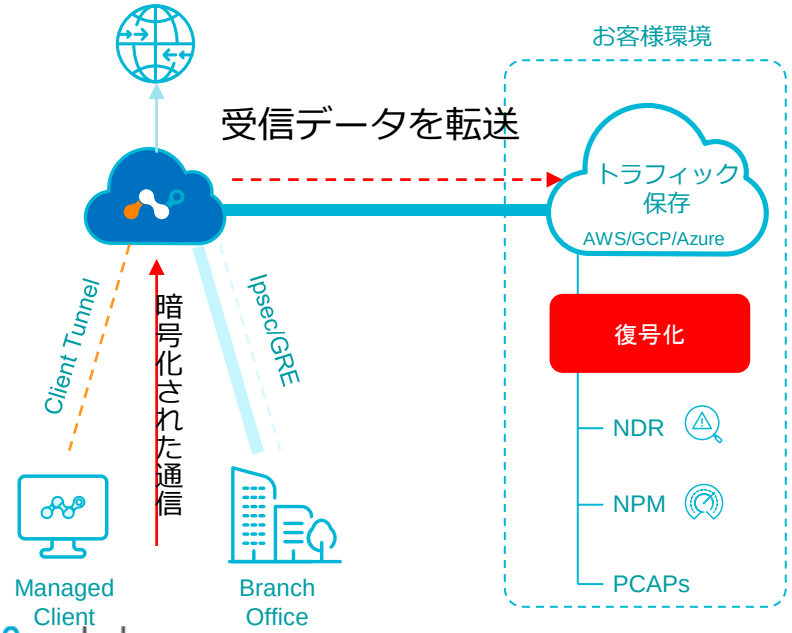
社内に存在する個人情報等がどこに保存され、どこに共有されていたか、普段から把握しておくことが可能です。「**想定外の場所に個人情報があった**」という状態を回避出来た可能性があります。



新機能の紹介

ネットワーク保護を近代化する、新機能のご紹介

Cloud Tap	C2 Beacon Detect (RoadMap)
TAPのCloud版。Netskopeで受信した トラフィックをNDR/NPM等で分析可能に。	Advanced UEBAの高度なMLを用いて動的に C2ビーコンを検出。



従来の主な方法:
- URLフィルタリングを用いて既知のC2インフラストラクチャへのアクセスをブロック
- IPSを用いてブロック

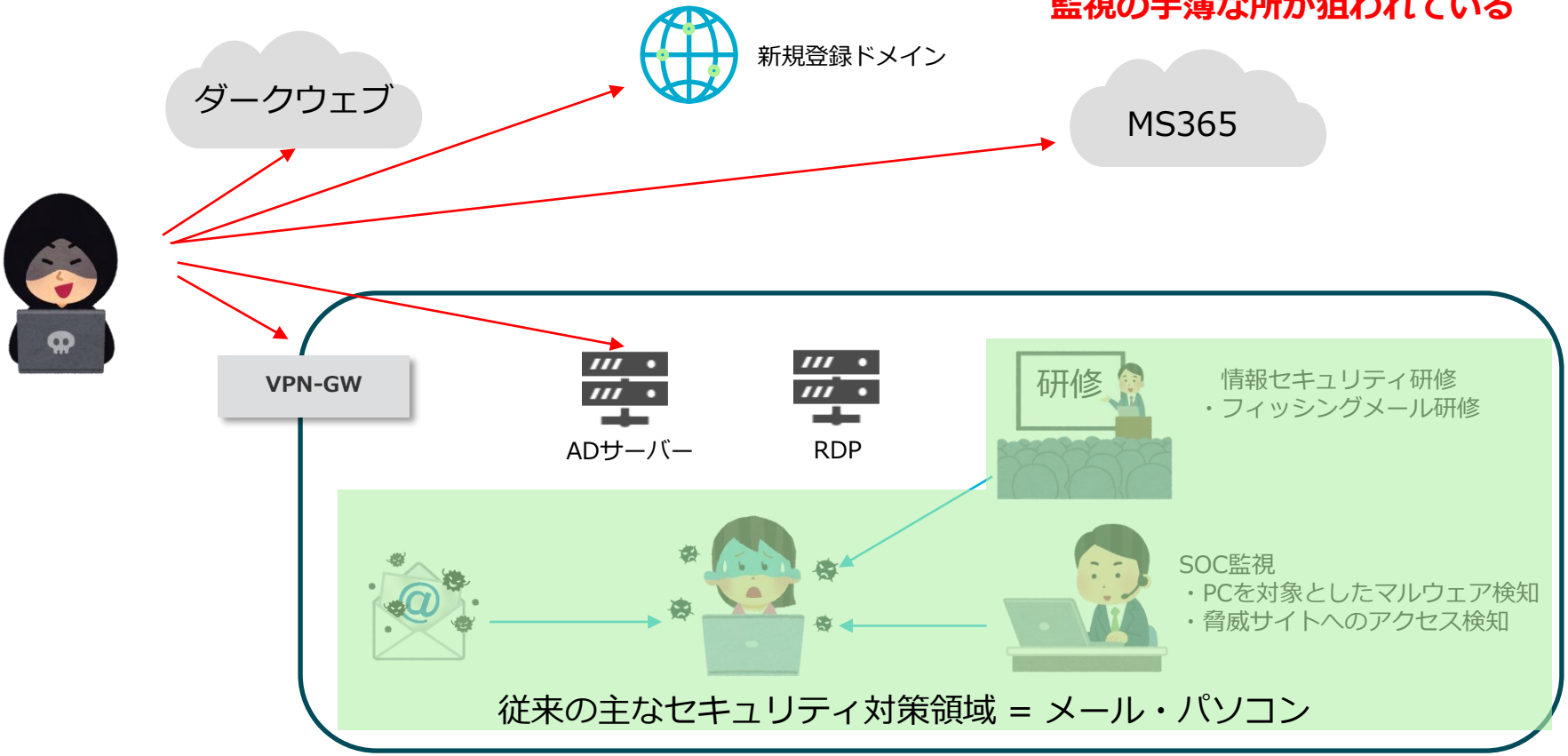
＋

・C2 Beacon Detect:
- Advanced UEBAを用いてこれまで検出が難しいとされていた、CobaltStrike等を悪用して生成されるC2 Beaconを検出可能に。

Summary

攻撃対象の変化を理解する重要性

監視の手薄な所が狙われている



NetskopeとEDR/EPPによる多層防御の有効性

- 日本からのインターネットアクセスの94%はHTTPSで暗号化されている
- メジャーなクラウドサービスがマルウェアの配信経路として悪用されている
- ProxyによるURLフィルタリングでは、Google.com等をブロックするしか出来ず、大半の脅威は検査されることなく、スルーされる。

- ノーウェアランサム攻撃対策に有効
- MS365やGoogle等のHTTPSトラフィックも復号化して、トラフィックをスキャン
- EPP/EDRが停止していても、ネットワーク層で脅威を検出、ブロック
- ファイルレス攻撃やフィッシングサイトに対する脅威保護
- ファイルが端末に到達する前に、悪意のあるファイルを保護し、SOCの負荷を軽減

- セキュリティツールの最優先で導入が検討される
- 定番ツールのため攻撃ツールは、EPP/EDRプロセスを検出し、停止しようとする
- ファイルレス攻撃やフィッシングにはあまり重点が置かれていない

Better Together