リモートワークでリスク増大！
企業の情報資産の守り方

18th March 2022

Yoshitaka Nishikawa

IIJ Europe

自己紹介

IIJ Europe

西川 善高（にしかわ よしたか）

大学専攻：インフォメーション・サイエンスおよび確率理論

2000年3月に大学卒業後、
　某商社金融部門や宇宙開発関連企業を経て、
　ベンチャービジネス(スタートアップ)に挑戦。

2007年より、　東南アジア　～　2020年12月まで(新規事業開発など)
2021年4月より、　ロンドン駐在 (UKおよびEUでの新規事業開発など)

　欧州への赴任は初めてで、日々驚かされる毎日です。そもそもはエンジニアでありましたが、最近は事業開発が中心となり現場仕事が少なくなりましたが、それでもエンジニアだと思い続けています。

趣味：ゴルフ、お酒（ビール・ワイン）、Gym(過去?)
言語：日本語・英語・インドネシア語・マレー語

英国における、在宅勤務制度の恒久化

2020年3月

COVID-19の感染拡大と政府によるロックダウンにより多くの企業・従業員は強制的な自宅勤務を開始する。

2021年1-4月頃

複数の企業より自宅勤務とオフィス勤務を合わせたHybrid workingを恒久的な制度として導入が始まる。

英国商工会議所によると英国の66％以上の企業が何らかの自宅勤務を従業員にオファー

2022年現在

イングランド政府は１月１９日以降は、在宅勤務勧告を撤廃したが、
Work from homeは求人サイトの主要な検索条件となっており、就業条件の一つとして一般化しつつある。

英国内のオフィスで、恒久的Hybrid workingを導入済みの主な企業
NatWest, Lloyds, HSBC, PricewaterhouseCoopers, Unilever

英国において、定常的に自宅勤務を行っている割合は37％*となり、パンデミック以前の18%から倍増している。
*CIPD 参照
https://www.cipd.co.uk/about/media/press/home-working-increases

情報セキュリティ 事案 トレンド

JPCERTのインシデント報告対応レポート(*1)による、
2021年前半期の報告内訳

エンドユーザが所持するデバイスが影響を受ける攻撃
フィッシングサイト、Webサイト改ざん、マルウェアサイト

全体の７４％

インシデント報告件数
2018-2020の3年間

15,000 件→30,000 件

インシデント	2021年1-6月合計
フィッシングサイト	9,672
Webサイト改ざん	533
マルウェアサイト	176
スキャン	2,470
DoS/DDoS	10
制御システム関連	0
標的型攻撃	12
その他	1,212

PCが攻撃対象となりうるケース
74%

*1 https://www.jpcert.or.jp/pr/2021/IR_Report20210715.pdf

情報セキュリティ 事案 トレンド

IIJ Europe

■「情報セキュリティ10大脅威 2021」

NEW：初めてランクインした脅威

昨年順位	個人	順位	組織	昨年順位
1位	スマホ決済の不正利用	1位	ランサムウェアによる被害	5位
2位	フィッシングによる個人情報等の詐取	2位	標的型攻撃による機密情報の窃取	1位
7位	ネット上の誹謗・中傷・デマ	3位	テレワーク等のニューノーマルな働き方を狙った攻撃	NEW
5位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	4位	サプライチェーンの弱点を悪用した攻撃	4位
3位	クレジットカード情報の不正利用	5位	ビジネスメール詐欺による金銭被害	3位
4位	インターネットバンキングの不正利用	6位	内部不正による情報漏えい	2位
10位	インターネット上のサービスからの個人情報の窃取	7位	予期せぬIT基盤の障害に伴う業務停止	6位
9位	偽警告によるインターネット詐欺	8位	インターネット上のサービスへの不正ログイン	16位
6位	不正アプリによるスマートフォン利用者への被害	9位	不注意による情報漏えい等の被害	7位
8位	インターネット上のサービスへの不正ログイン	10位	脆弱性対策情報の公開に伴う悪用増加	14位

出典：「情報セキュリティ10大脅威 2021」
独立行政法人情報処理推進機構（IPA:Information-technology Promotion Agency, Japan）

情報セキュリティ 事案による被害内容・被害額

情報セキュリティ・インシデント発生率

5,000名以上の法人組織 → **75.8%**

50名～99名の法人組織 → **40.6%**

↳ セキュリティ**対策が十分でない**

↳ インシデントの**発生に気づいていない可能性**

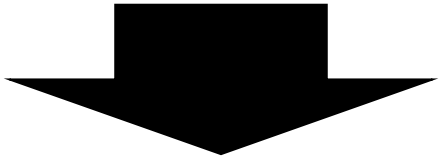
民間企業、官公庁及び自治体を対象に実施した調査において、

組織全体での年間平均被害総額は**約2.4億円となり、4年連続で2億円を超え**ている
(被害額：システム・サービスの停止/インシデント対応/原因特定の費用/改善策の導入/損害賠償…)

*令和二年版総務省情報通信白書
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r02/html/nd134120.html
*トレンドマイクロ法人組織におけるセキュリティ実態調査 2019年版
https://www.trendmicro.com/ja_jp/about/press-release/2019/pr-20191015-01.html

まとめ ＆ 対応策

- 多くのPCが**社外で使用されオンライン**となっている状態
- **PCが攻撃対象**となっている割合は70%を超え、件数増加
- インシデントが**起きたことに気が付けていない**可能性
- インシデント発生時に原因究明・改善策の作成に**多くの時間・労力を必要**



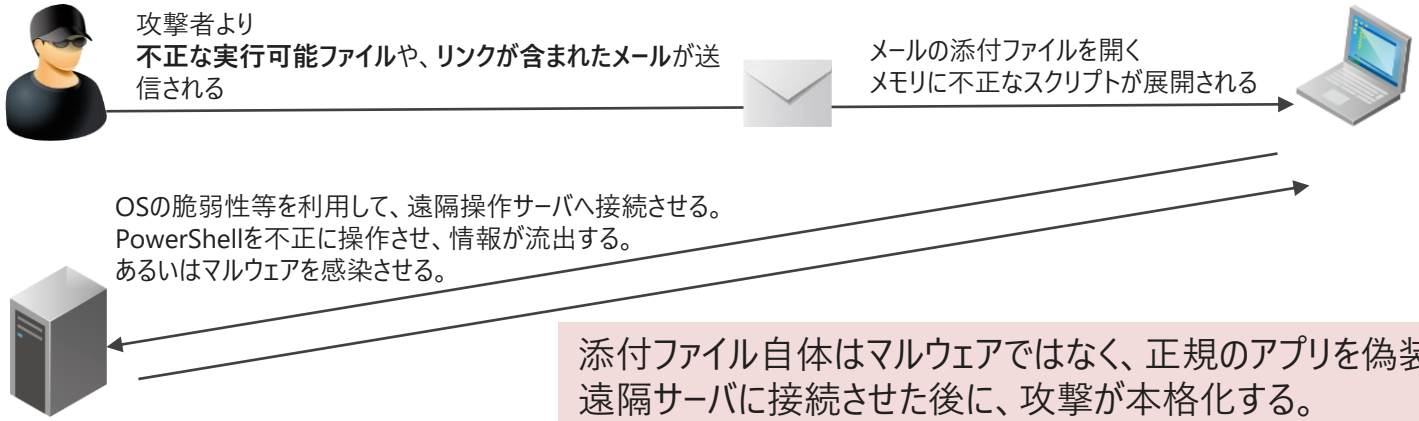
EDR (Endpoint Detection and Response)
感染や侵入を前提とし、感染後の素早い検知、感染した端末をネットワークから切り離すことで、組織内での感染拡大を遮断する新しいセキュリティ手法/サービスで近年注目が集まっている。

多くのセキュリティベンダーより提供されているが、ブランド・製品毎の個性や機能が評価されてきている。
その中で、**検知・阻止・調査・復旧の4機能が搭載されているEDRの導入が必要とされている。**

従来型アンチウイルスソフトの限界

従来型のアンチウイルスソフトでは攻撃を防ぎきることができないケースが増えてきている。

- ファイルレス攻撃 (メモリ常駐型)



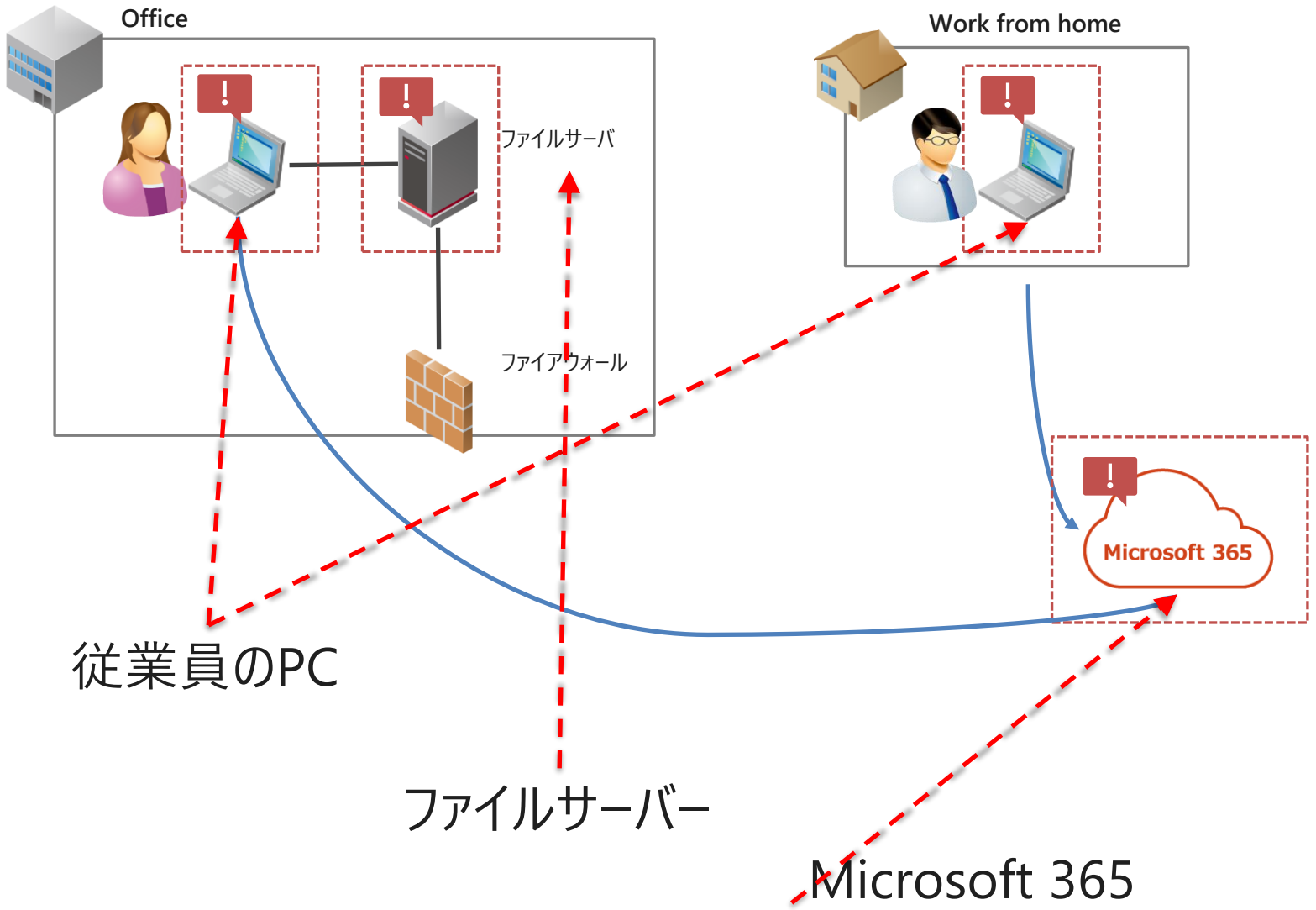
添付ファイル自体はマルウェアではなく、正規のアプリを偽装している。
遠隔サーバに接続させた後に、攻撃が本格化する。

- 標的型攻撃の増加 (不特定多数から特定の対象への攻撃)

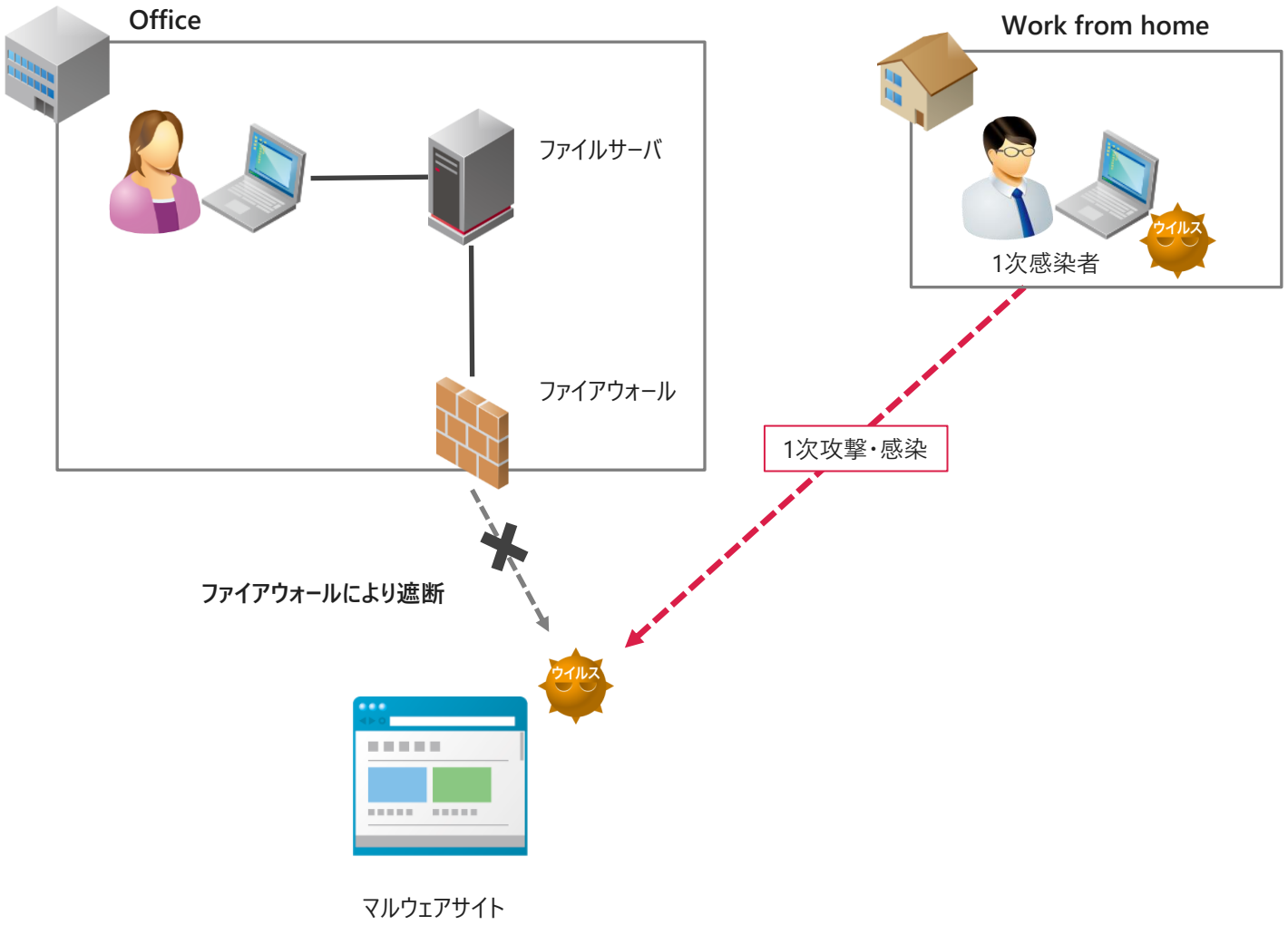
最近の攻撃手法において無差別に多くをターゲットとする場合も引き続きあるものの、
一方で未知のウイルスを用いて、特定の組織を狙い撃ちにする事象も増加している。

アンチウイルスは**シグネチャという予め登録されたデータと照合しマルウェアを検出するのが基本的**な動作であるが、標的型攻撃は未知のマルウェアを少数特定の攻撃対象へ使用されることにより、アンチウイルスベンダーがマルウェア検体の入手と**シグネチャ作成と配布が完了するまでの**タイムラグを狙った攻撃である。

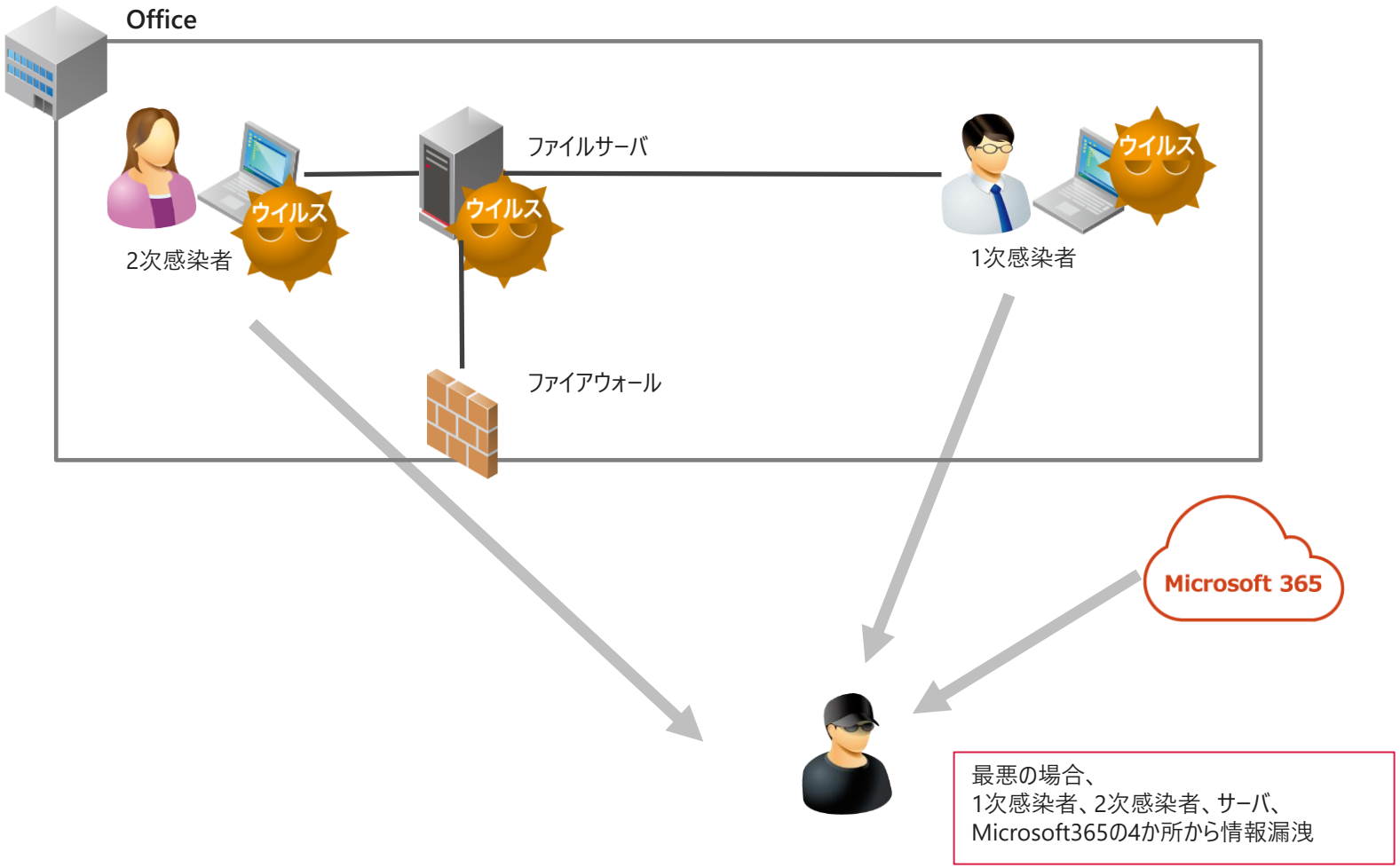
保護すべき情報資産の保管場所



ケーススタディ、マルウェアによる情報漏洩



ケーススタディ、マルウェアによる情報漏洩



あらためて、EDRの機能

検知 - マルウェアなどに感染した後の対策が行える

未知のマルウェアであっても脅威を早い段階で自動的に検知することで、素早い対策が可能。
EDR は、感染を防ぐのではなく、感染することを前提とし、仮に感染してしまった後でも、対策を行なえる点が特徴。

阻止 - ネットワークの遮断による2次被害の防止

EDR はパソコンなどにおいてサイバー攻撃を検知すると、素早くネットワークを遮断。
感染済みの端末を隔離することで、被害の拡大を防止するのはもちろん、二次被害も効果的に防ぐ。

調査 - マルウェアなどの侵入経路、被害範囲の特定

EDR はマルウェアがどのような経路を辿り侵入に至ったか、その経路と被害の範囲を特定することが可能。
侵入経路や被害の範囲を特定できるため、被害状況を可視化するのに役立つ。
今までのマルウェア感染対応のようにトレースに時間やリソースが過大に消費される事態を防ぎ、適切な対処が可能となる。

復旧 - 的確な対処が行える

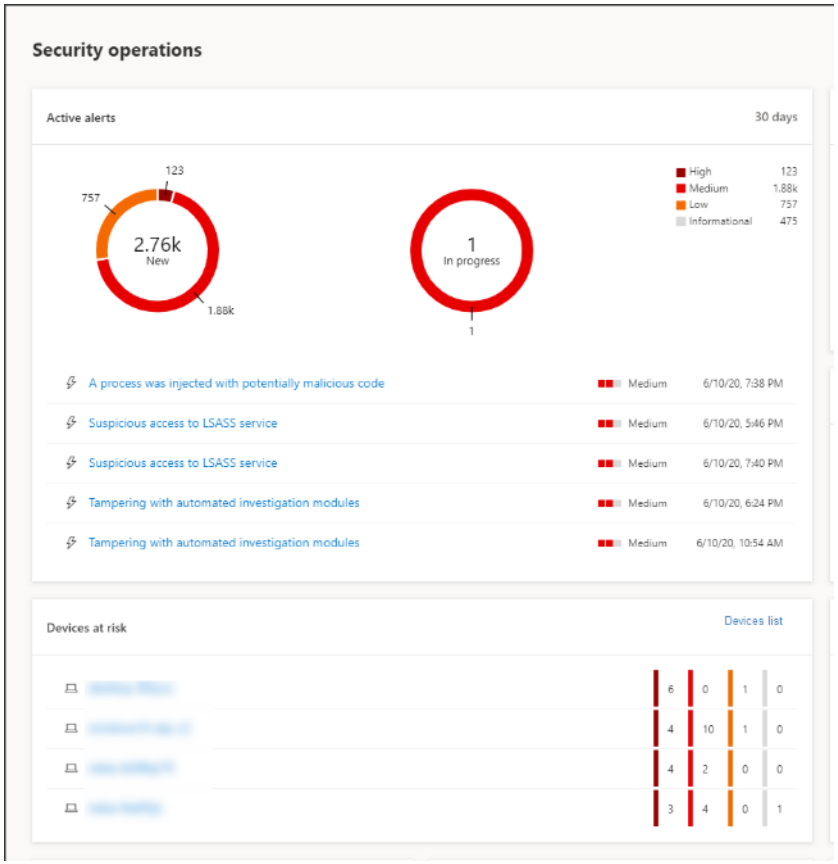
感染端末を隔離した状態で調査が行われ、その結果判明した影響範囲に対し対処を行うことが可能。
念のため、PCを全台初期化するなどの対策は不要。
比較的軽微な感染に対しては無害化処理を行い、自動復旧を行うことも可能。

Microsoft 365へのアクセス制御

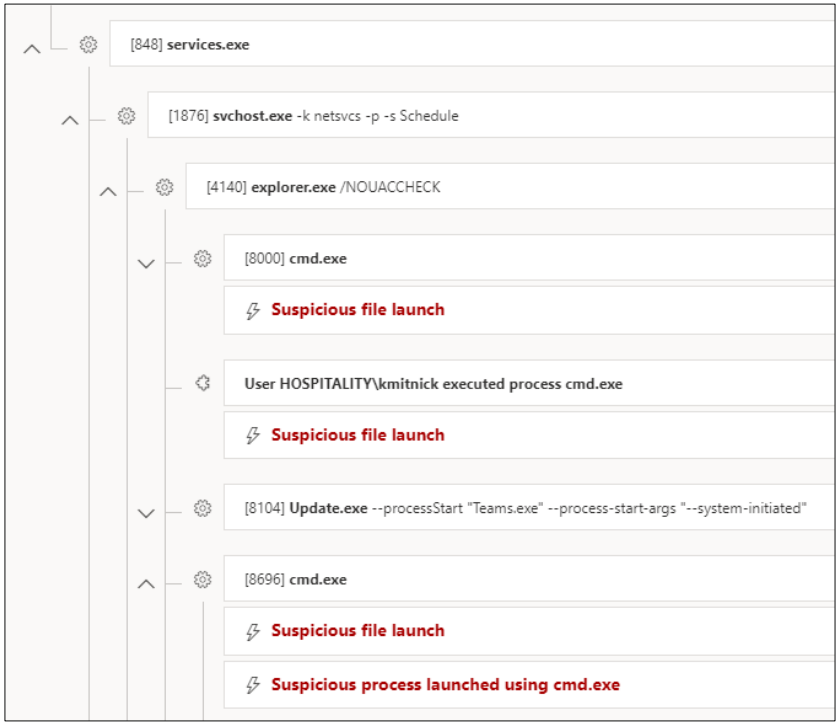
さらに感染端末からの遮断に加え、Microsoft 365のクラウド側からも端末の状況を確認し、アクセス遮断を行うことが可能な製品もあります。

管理画面サンプル

Microsoft Defender ATP



ダッシュボード画面



特定のPCのプロセス実行順序の例

代表的なEDR製品

- **Microsoft Defender ATP**
  EDR単体の製品ではなく、多くの企業が既に導入済みのMicrosoft 365の一部メニューに含まれる
  追加のエージェントソフトが不要で、Winodws10/11に搭載されているMicrosoft DefenderがEDR機能をあわせ持つ

  導入企業例

- **CrowdStrike Falcon**
  従来のアンチウイルスソフトと異なり、クラウドストライクはセキュリティのアップデートをクラウド上で行い、
  デバイスがインターネットを通じて管理基盤に接続されている間はクラウド側でデバイスのチェックを行うため、エージェントが軽量

  導入企業例

サイバー戦争

企業間の技術革新競争、国家の利権や領土問題が、サイバー戦争の原因になることが多く、主に想定される「敵」やその他の第三者が管理するサーバー及びコンピュータを目標とする。「敵」の場合には侵入、諜報、企業のイントラネットに不正アクセスして技術情報や意思決定等のデータを収集、サービスの停止、もしくは破壊が行われる。
広義には、利益誘導、世論形成、煽動を目的とするインターネットを使用したプロパガンダを含む。

例：ウクライナ・香港・ミャンマー

Q&A

IIJ Europe

ご視聴ありがとうございました。