






# コロナ禍のセキュリティ侵害状況 新たなIT環境構築と法整備

花村 実  
CISSP, CCSP, MBA, CFE (公認不正検査士)  
Chief Security Advisor, Microsoft Corporation

## 目次

-  はじめに
-  第 1 章: サイバー犯罪の状況
-  第 2 章: 国家レベルの脅威
-  第 3 章: セキュリティとリモート ワーカー
-  第 4 章: すぐ実践できる研究成果

# Cybercrime is borderless

The Internet grants anonymity

Cybercrime disregards geopolitical borders

Crimes span multiple enforcement jurisdictions

Need for cross-agency collaboration

“ セキュリティは最優先事項です。  
お客様を守るために業界横断で  
取り組むことをお約束します。

”

SATYA NADELLA

Chief Executive Officer, Microsoft Corporation



# Tech intensity

セキュリティ  
コンプライアンス

$$\begin{matrix} \text{デジタル} \\ \text{テクノロジー活用} \end{matrix} \times \begin{matrix} \text{デジタル} \\ \text{テクノロジー} \\ \text{人材/スキル} \end{matrix} \overset{\text{Trust}}{\wedge} = \text{Tech intensity}$$

デジタルトランス  
フォーメーション  
遂行能力

## 政策渉外・法務本部 (CELA)



**Diverse**

1500+ FTEs

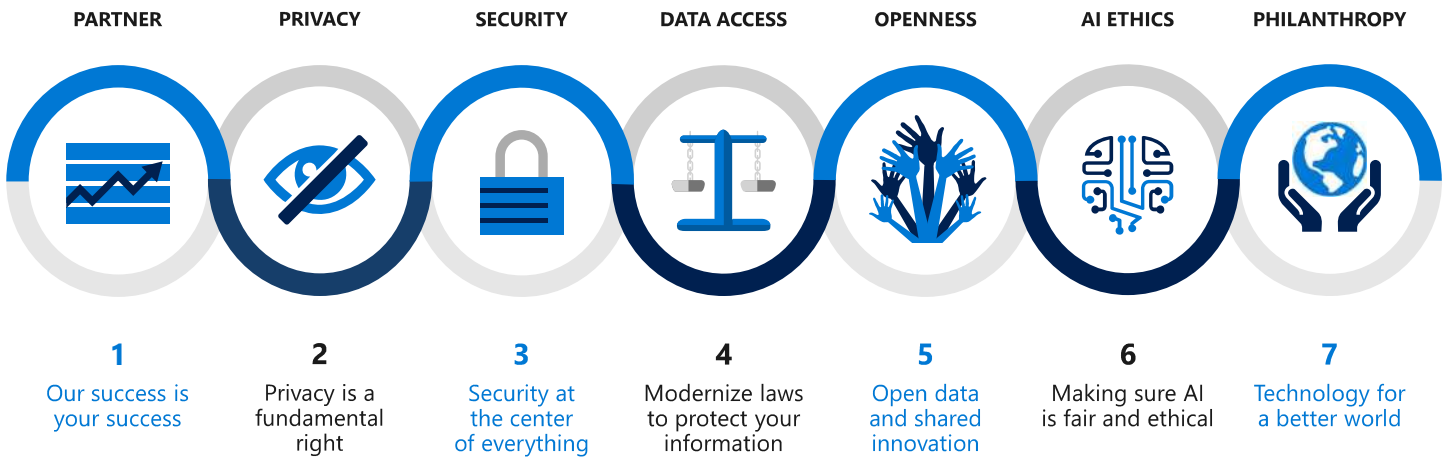
**Global**

100+ cities and  
50+ countries

**Innovative**

Early adopters  
of new technology

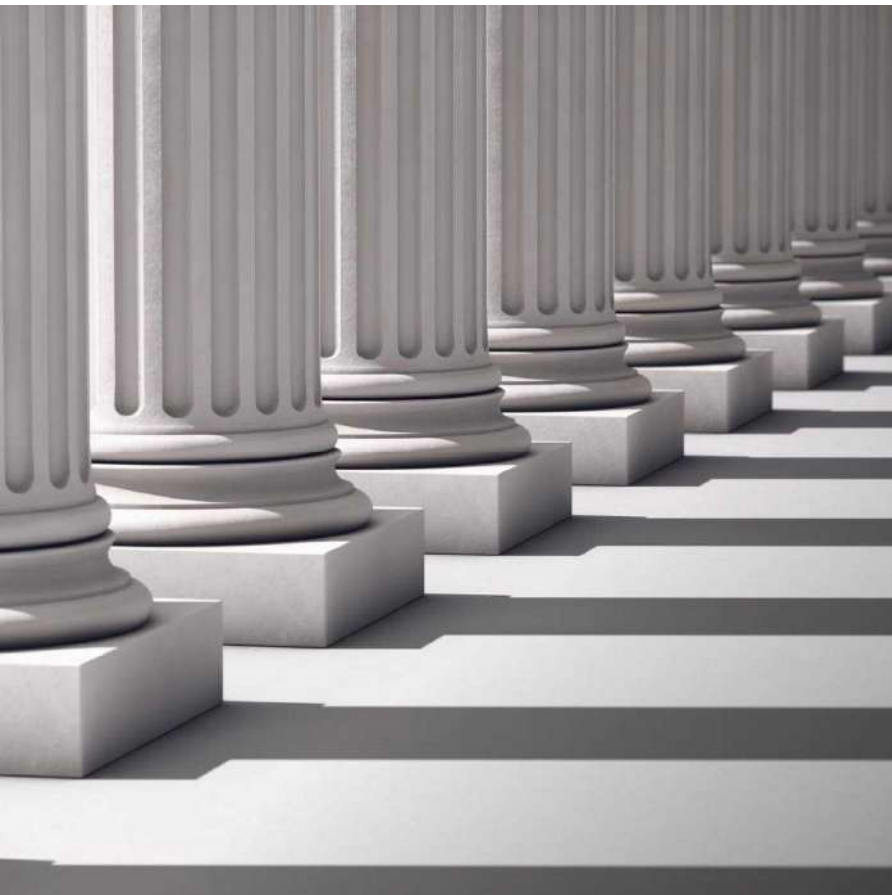
# 7 Microsoft priorities for customer success



## We are leading the global fight against cybercriminals

The Microsoft digital crimes unit is a team of legal and security experts specialized in taking down botnets and fighting nation-state hackers





**We cooperate with law enforcement, but we also stand up to governments when they overreach**

We have stringent requirements for providing governments with information

We believe that customers should control their data

We make contractual commitments on these points

We have a broad commitment to transparency

## Our principles for ethical AI



Fairness



Reliability and safety



Privacy and security



Inclusiveness



Transparency



Accountability



## We're investing to bring the benefits of technology to all

Green data centers that protect the environment

Rural broadband with TV whitespace

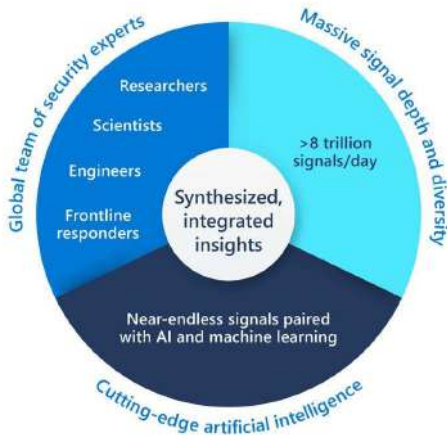
AI for Good

Reskilling and education



# レポートの構成

マイクロソフトのエキスパート、技術者、防御担当者からの情報を統合



マイクロソフトの 2020 年の重点分野

- 1 サイバー犯罪の状況
- 2 国家レベルの脅威
- 3 セキュリティとリモートワーカー
- 4 すぐ実践できる研究成果

## 協カチーム

サイバー防御運用センター

カスタマー セキュリティおよびトラスト

検出対応チーム

デジタル セキュリティとリスク エンジニアリング

デジタル セキュリティ ユニット

GitHub セキュリティ ラボ

IoT セキュリティ研究チーム

Microsoft Defender チーム

Microsoft Digital Crimes Unit

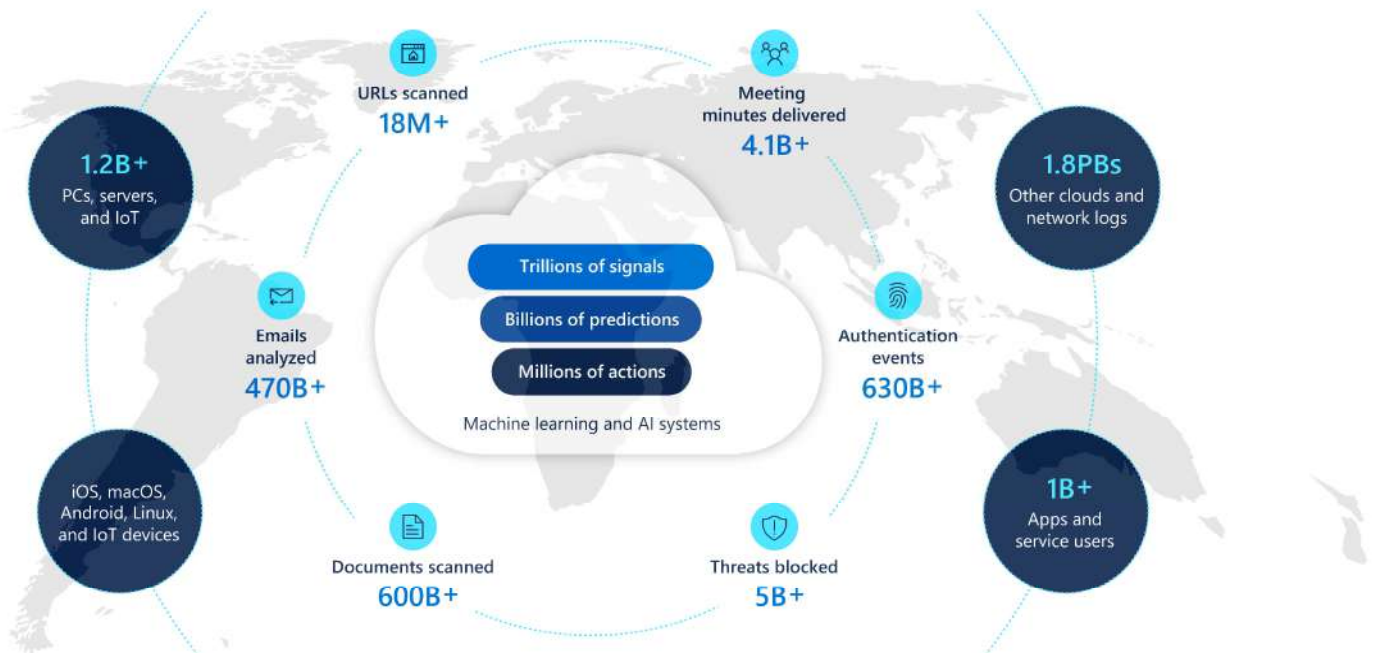
マイクロソフト セキュリティ レスポンス センター

マイクロソフト脅威インテリジェンス センター



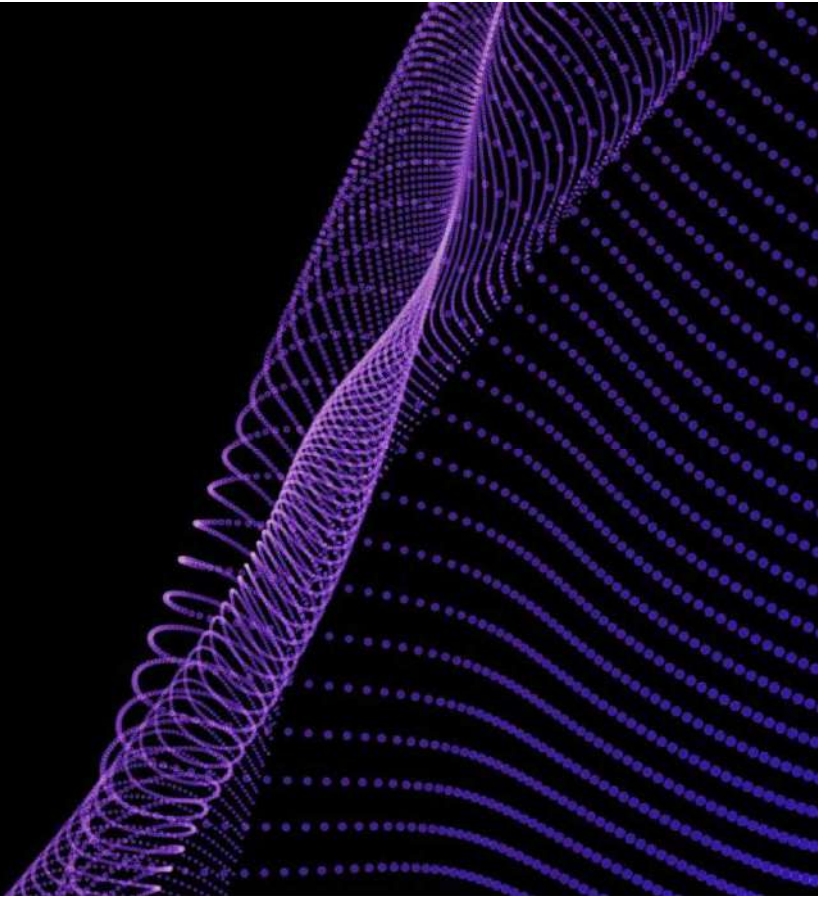
# 数兆にのぼる兆候から得た独自の洞察

マイクロソフトのセキュリティオペレーションから得られる 1 か月あたりのシグナル



# 1

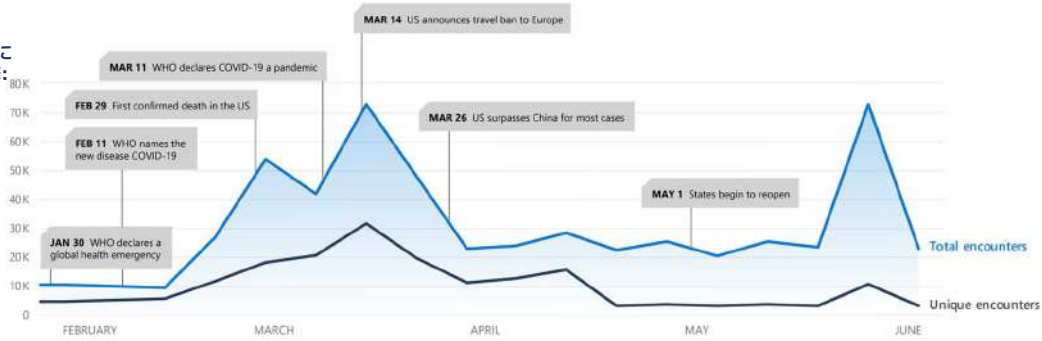
## サイバー犯罪の状況



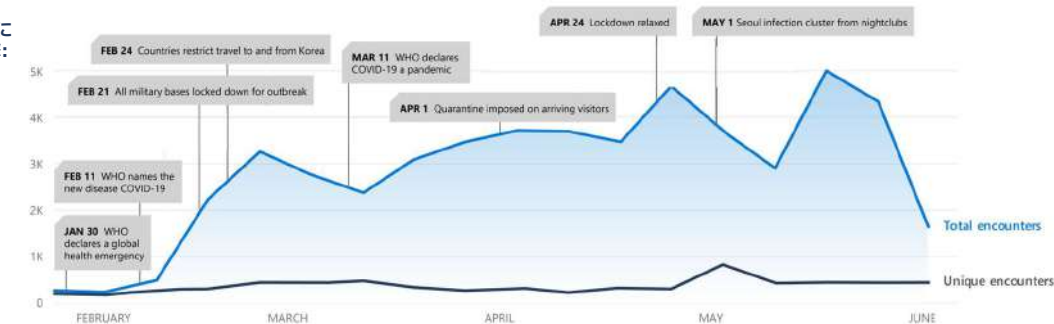
## サイバー犯罪が日々の話題に

はニュースの見出し数とマルウェア検出件数との相関関係

COVID-19 に関連する攻撃: 米国



COVID-19 に関連する攻撃: 韓国






# フィッシングとビジネス メール詐欺

昨年の  
検出件数:

6T   
Messages  
scanned

~13B   
Malicious emails  
blocked

~1.6B   
URL-based email  
phishing threats  
blocked

~1.7-2B   
URL payloads being created  
each month, orchestrated  
through thousands of  
phishing campaigns

マイクロソフトが認識している主な 3 種類のフィッシング:

クレデンシャルフィッシング

ビジネス メール詐欺

両方の組み合わせ

なりすましに使われた  
上位 5 ブランド:

マイクロソフト  
UPS  
Amazon  
Apple  
Zoom

フィッシング攻撃活動ターゲットとなった上位 10 業界:

会計とコンサルティング 医療  
卸売業 化学  
IT サービス ハイテクとエレクトロニクス  
不動産 司法サービス  
教育 アウトソーシング サービス

数年前まで、サイバー犯罪者は最大の ROI を得るためにマルウェア攻撃に注力していました。

最近では、ユーザークレデンシャルの収集を目的とするフィッシング攻撃に焦点が移っています。

## 資格情報フィッシング

例

1 →

Set up criminal  
Infrastructure



Set up fake domains  
or compromise  
legitimate ones



Gather information on  
potential victims

2 →

Send malicious  
messages



3 →

Entice victim  
to click



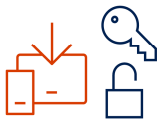
Click sends victim  
to fake domain  
(spoofed site)

4 →

Victim's  
credentials  
are stolen



Victim inserts  
credentials into a  
fake web form



Or, malware is  
downloaded to  
victim's device to  
gather credentials

5

Victim's data is  
sent to "drop  
account"



Cybercriminals use  
victim's credentials on  
other legitimate sites



Or, use them to gain  
access to corporate  
networks and data



# ビジネス メール詐欺 (BEC)

例



1 →

Cybercriminal poses as CEO using any of a variety of methods (such as spoofing, impersonation, or credential theft)

2 →

Cybercriminal gains access to mail account and may monitor the CEO's mail to gain additional information, to increase the sophistication of the attack and the likelihood of success



Monitors mail for information on:

- Relationships
- Common phrases
- Calendar, business activities, travel
- Wire transfers



Sets mailbox forwarding rules using keywords, keeping certain email traffic hidden from the CEO

- Sample keywords: "invoice," "accounts receivable," "funds," "overdue," "payroll," "IBAN"
- Mails with keywords are forwarded to a collection email account controlled and monitored by the cybercriminal

3 →

Cybercriminal masquerades as CEO



Cybercriminal sends email that is crafted to appear as though it's coming from a trusted or important position at work, such as the victim's manager, CEO, CFO, vendor/business partner, or someone the person would take notice of.

4

Victim wires business payment to fraudulent bank account



Victim (e.g. Accounts Receivable clerk) wires payment to a fraudulent bank account, as directed by the cybercriminal masquerading as the CEO, CFO, or business partner.

## ランサムウェア

影響の大きい人手による脅威

### マイクロソフトが認識している状況:

#### マイクロソフトインシデント対応チーム (DART)

- ランサムウェアの対応がインシデントレスポンスの主要な要因 (2019年10月 - 2020年7月)。

#### マイクロソフト脅威防御インテリジェンス

- サイバー犯罪者は、インターネットの隅々まで大規模に探索して脆弱なエントリポイントを見つけ、攻撃に最も有利なタイミングでアクセスを作動させます。

いくつかの事例では、サイバー犯罪者が最初の侵入からランサムウェア攻撃完了までに要した時間は45分未満。

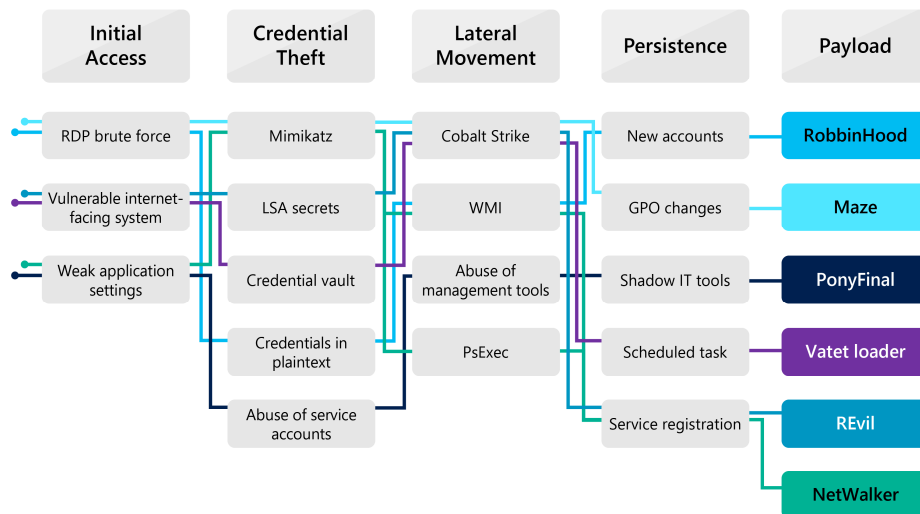


# ランサムウェア: 影響の大きい人手による脅威

マイクロソフトのインシデント対応の実施理由として最も一般的 (2019 年 10 月 - 2020 年 7 月)



マイクロソフト脅威防御  
インテリジェンスが  
2020 年初めに確認した、  
ランサムウェアによる  
攻撃パターンの詳細



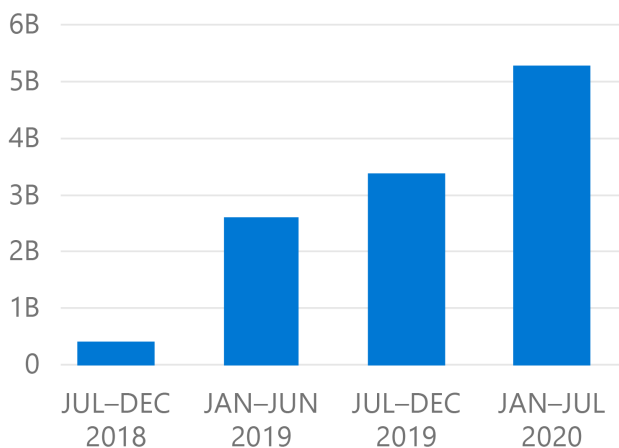
サイバー犯罪者が最初の侵入から 45 分未満でネットワーク全体にランサムウェア攻撃を実行した事例もいくつかあります。

## IoT セキュリティに関する洞察

IoT への脅威は絶え間なく拡大し、進化している



ハニーポットへの合計攻撃件数



2020 年前半のハニーポット データは、合計攻撃件数が 2019 年後半と比較して約 35% 増加していることを示しています。

脆弱性管理が、IoT 資産の保護において重要な役割を果たします。

# CyberX リスク レポート

1,800 か所の産業用制御システム ネットワークからのデータ



71%

定期的にパッチを適用せずに Windows の旧バージョンを使用している現場

64%

侵害を容易にする非暗号化パスワードを使用している現場

66%

自動的に最新のアンチウイルス定義に更新していない現場

54%

攻撃者が検出されずに足掛かりにすることができる、リモートアクセス可能なデバイスがある

27%

インターネットに直接接続している ICS デバイス



CyberX: マイクロソフトが最近買収した企業

## 第 1 章: サイバー犯罪の状況

多様な攻撃者と絶え間なく進化する戦術に対する防御の複雑さ



### この章の内容:

#### サイバー犯罪者は機会に乗じる

- サイバー犯罪はビジネス
- 日々の話題に追隨して進化: COVID-19
- 電子メール フィッシングが引き続き主要な攻撃ベクトル
- フィッシングとビジネス メール詐欺の手法が急速に進化
- 人手によるランサムウェア

#### 重点項目: サプライ チェーンのセキュリティ

- 検出対応チーム (DART) がサプライ チェーン攻撃の増加を確認
- オープン ソース ソフトウェア: GitHub
- ハニーポットから得られる IoT セキュリティに関する洞察
- CyberX のグローバル IoT リスク レポートと推奨事項
- サプライ チェーン リスク管理に関する規制の進展

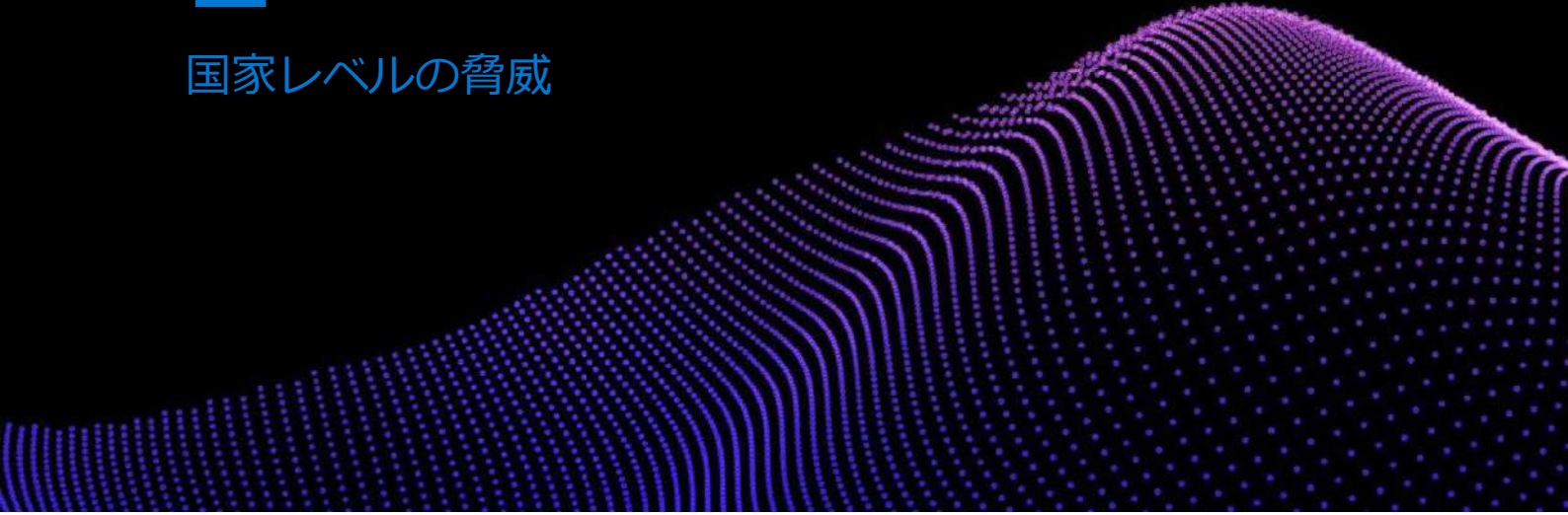
#### セキュリティにおける機械学習 (ML)

- ML システムへの攻撃に対する業界の準備
- ML モデル ポイズニング
- ML の民主化

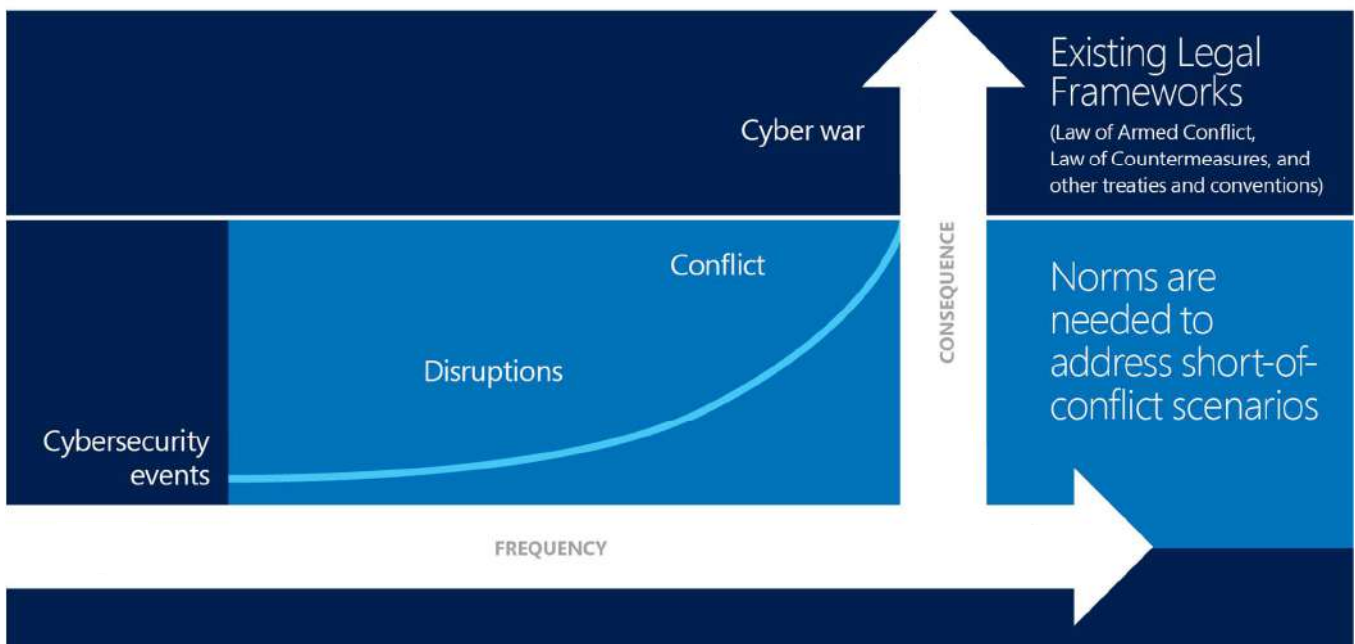


# 2

## 国家レベルの脅威



### Risk to civilians from cyber-conflict needs a response



# A Digital Geneva Convention...

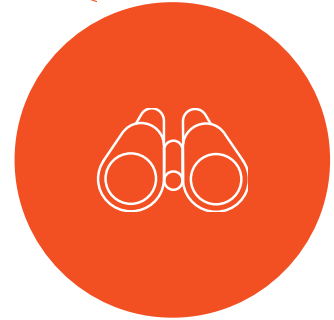
## TO PROTECT PEOPLE ONLINE IN TIMES OF PEACE



**BINDING  
GOVERNMENT  
AGREEMENTS**



**TECH SECTOR  
ACCORDS**

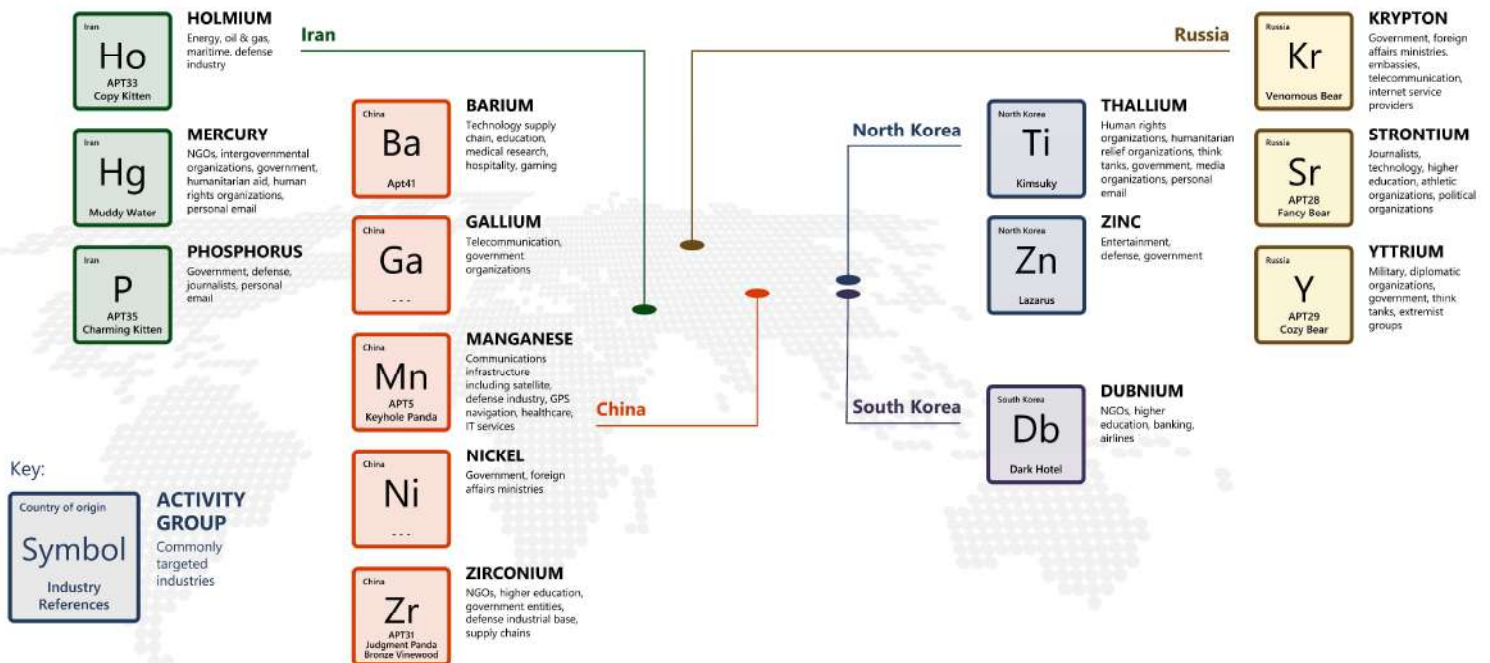


**ATTRIBUTION  
ORGANIZATION**

## REDUCING CONFLICT, NOT CONTROLLING CONTENT

# 国家スポンサーによる攻撃の例

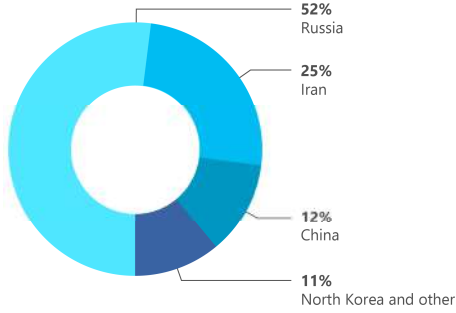
## Sample of nation state actors and their activities



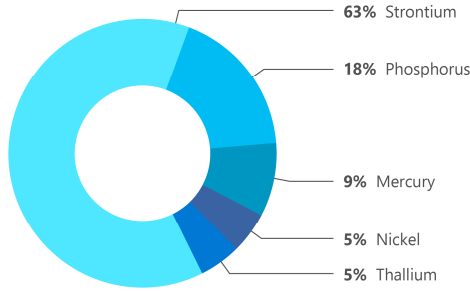
# 国家レベルの脅威 (2019年7月 - 2020年6月)



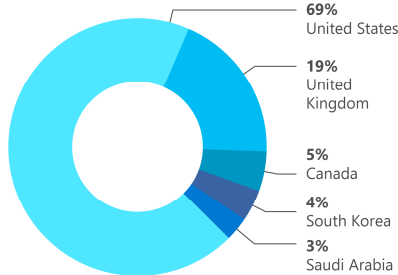
NSN\* 対象の  
アクティビティ発信国



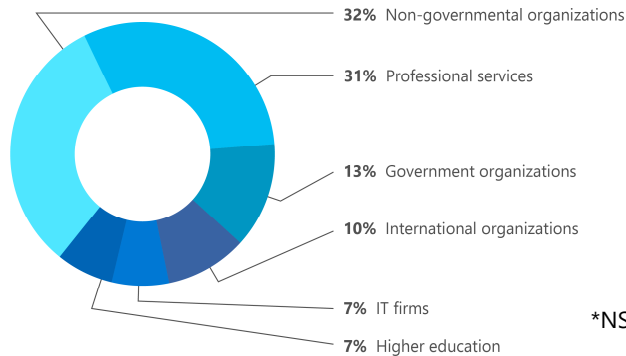
マイクロソフトの顧客をターゲットとしていることが検出された  
上位5つの国家レベル アクティビティグループ



ターゲットになった  
上位5地域



ターゲットになった  
上位6業種 (NSNの送信件数順)



国家レベルの脅威に関する通知の90%以上が、重要インフラストラクチャ部門以外に送信されました。

\*NSN (Nation State Notification)

## 国家レベルの脅威

理解をより深める

### 一般的な攻撃目的

- スパイ活動
- 混乱や破壊

### 一般的な攻撃手法

- 偵察
- マルウェア
- クレデンシャルの収集
- 仮想プライベート ネットワーク (VPN) の悪用

### 偵察

PHOSPHORUS によって利用された類似の名前形式の例


J.Smith@contoso.com  
John.smith@contoso.com  
John.m.smith@contoso.com  
JohnSmith@contoso.com  
johnsmith@contoso.com

### クレデンシャルの収集

THALLIUM は、ターゲット組織の名前と似ている偽のドメインの購入と利用に多大なリソースを費やしています。




# Ransomware Activity



**JOINT  
CYBERSECURITY  
ADVISORY**

**Ransomware Activity Targeting the  
Healthcare and Public Health Sector**

AA20-3024  
October 28, 2020



Microsoft  
**THREAT INTELLIGENCE**

NOTE: The data in this document is provided to you subject to the following conditions: Your organization may use the data solely for informational, remediation, and defensive purposes. The data may be inaccurate and/or may refer to legitimate but compromised properties. THIS DOCUMENT IS PROVIDED "AS-IS" AND FOR INFORMATIONAL PURPOSES ONLY. MICROSOFT DISCLAIMS ALL EXPRESS, IMPLIED, OR STATUTORY WARRANTIES. THIS INCLUDES THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT.

**MSTI Activity Alert – Human-Operated Ransomware Threat to Healthcare**

NOTE: Microsoft notifies any customers that are targeted or compromised by the activity described in this report. This update is for advisory purposes only.

Trickbot was first spotted in 2016 as a banking trojan and designed to steal credentials from online banks and financial services. Over the years, Trickbot's operators were able to build a sophisticated attack infrastructure which evolved into a modular payload available for malware-as-a-service. Microsoft tracks a cluster of threat actor activity related to the Trickbot ecosystem that has been responsible for a significant amount of human-operated campaigns including attacks that steal credentials, exfiltrate data, and deploy additional payloads, most notably Cobalt Strike beacon and Ryuk<sup>2</sup> ransomware, in target networks.

In recent attacks involving Trickbot, the time from initial compromise to enterprise-wide ransomware deployment has dropped significantly and is often 24-48 hours or less in some cases. These threat actors have used the malware families publicly referred to as "Bazalloader/NEGTA" to initially compromise victims.

This summary is part of a deeper analysis of Trickbot, published in the following recent blog posting:  
<https://www.microsoft.com/security/blog/2020/10/12/trickbot-debated/>

Microsoft also recently took action against this activity and published the following blog posting:  
<http://blogs.microsoft.com/on-the-issues/2020/10/12/trickbot-ransomware-cyberthreat-cs-reflectors/>

Microsoft is distributing this Activity Alert to customers within the healthcare industries to share important information toward assisting in the identification or defense of customer assets.

**Activity description**

Microsoft is aware of Trickbot infrastructure actively targeting customers in the healthcare sector. Trickbot commonly targets customers with sophisticated malware and human-operated ransomware attacks.

- The actors gain initial access through Trickbot or Bazalloader/NEGTA.
- The actors will then move to human-operated phases involving credential theft and lateral movement.
- Finally the actors will use stolen domain admin or other privileged credentials to deploy a ransomware payload through PiSec or Group Policy.

It is critical that customers implement protections using the IDCs accompanying this document and hardening guidance as quickly as possible to minimize potential impact to their business operations.

# Detection And Response Team (DART)

## Our Mission

To respond to security incidents and help our customers become cyber-resilient

**Microsoft Security Solutions Area**

Incident Response	Office 365 Incident Response
<b>IR</b>	<b>O365IR</b>
<b>REACTIVE</b>	<b>REACTIVE</b>
Cybersecurity Operations Service	Security and Crisis Response Exercise
<b>COS</b>	<b>SCRE</b>
<b>PROACTIVE</b>	<b>PROACTIVE</b>



# DCU

## マイクロソフトの取り組み

テクノロジー

最先端の技術



Microsoft  
Security

オペレーション

お客様のための  
セキュリティ・  
オペレーション



法的措置、  
政策提言と連携

世界が複雑さを増す中、21世紀  
に求められる政策と連携



# Microsoft Cybercrime Center

## Digital Crimes Unit

サイバー犯罪との戦いを主導

サイバー犯罪者に対するグローバルな**法的執行**を通じて、  
人、組織、マイクロソフトのクラウドを保護

調査、フォレンジクス、分析

機械学習、AI、データの可視化

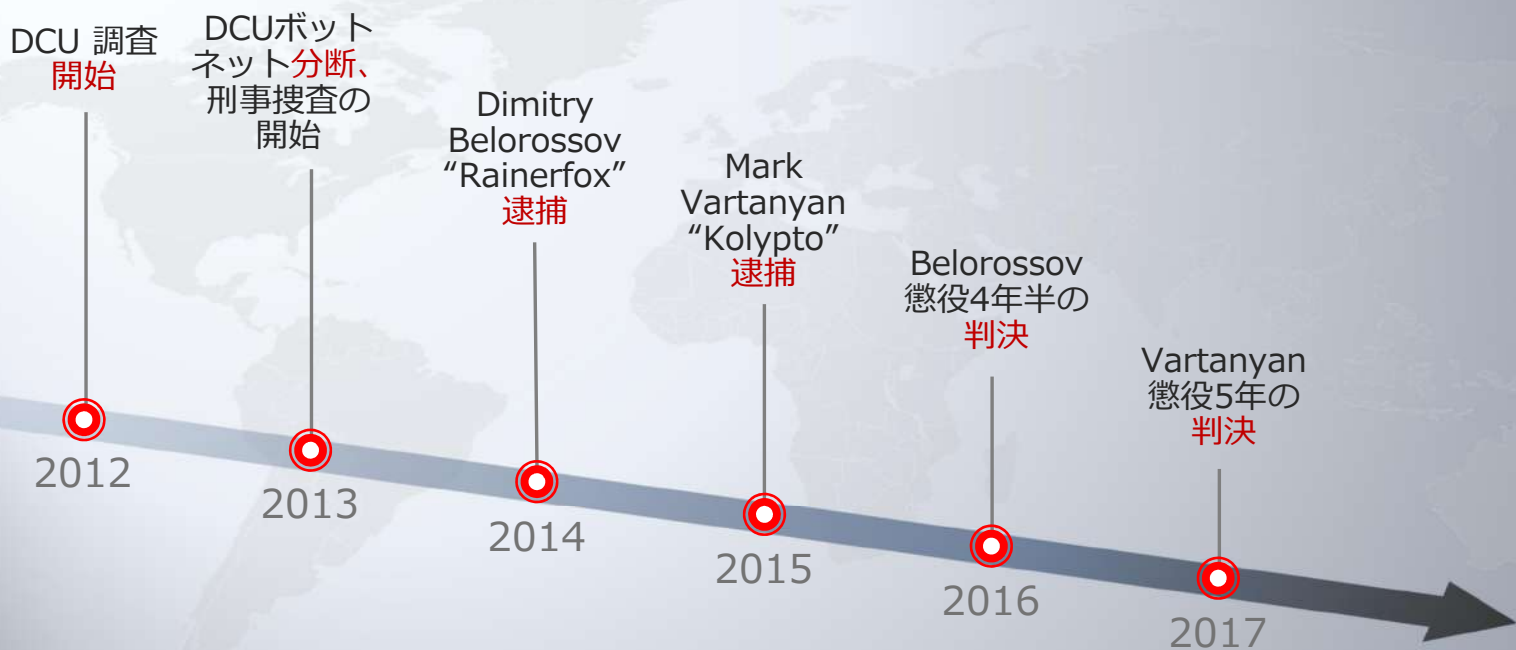
官民のパートナーシップ

創意ある法的戦略



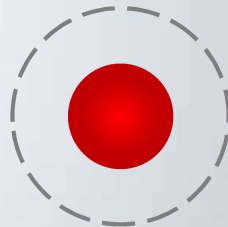


## Citadel の例



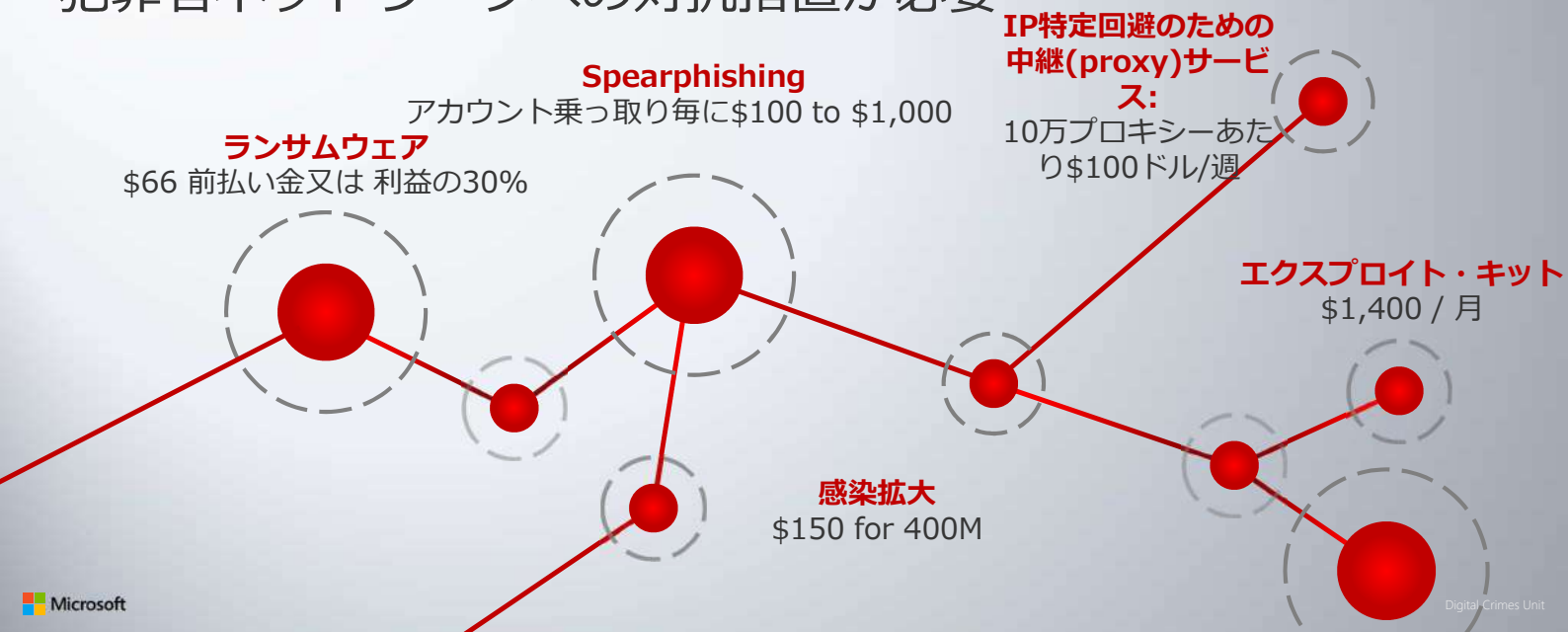
# 攻撃者の生態系の拡大

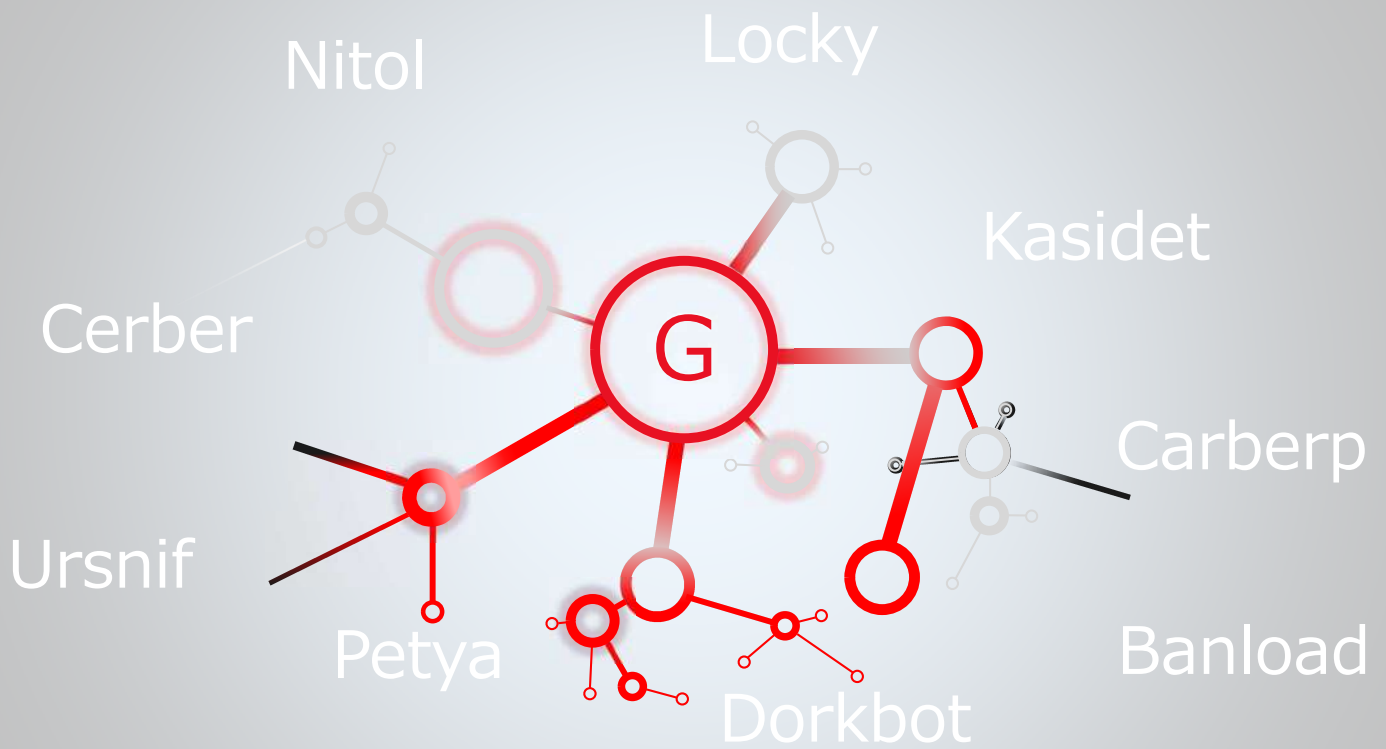
個のサイバー犯罪者ではなく、  
犯罪者ネットワークへの対抗措置が必要



# 攻撃者の生態系の拡大

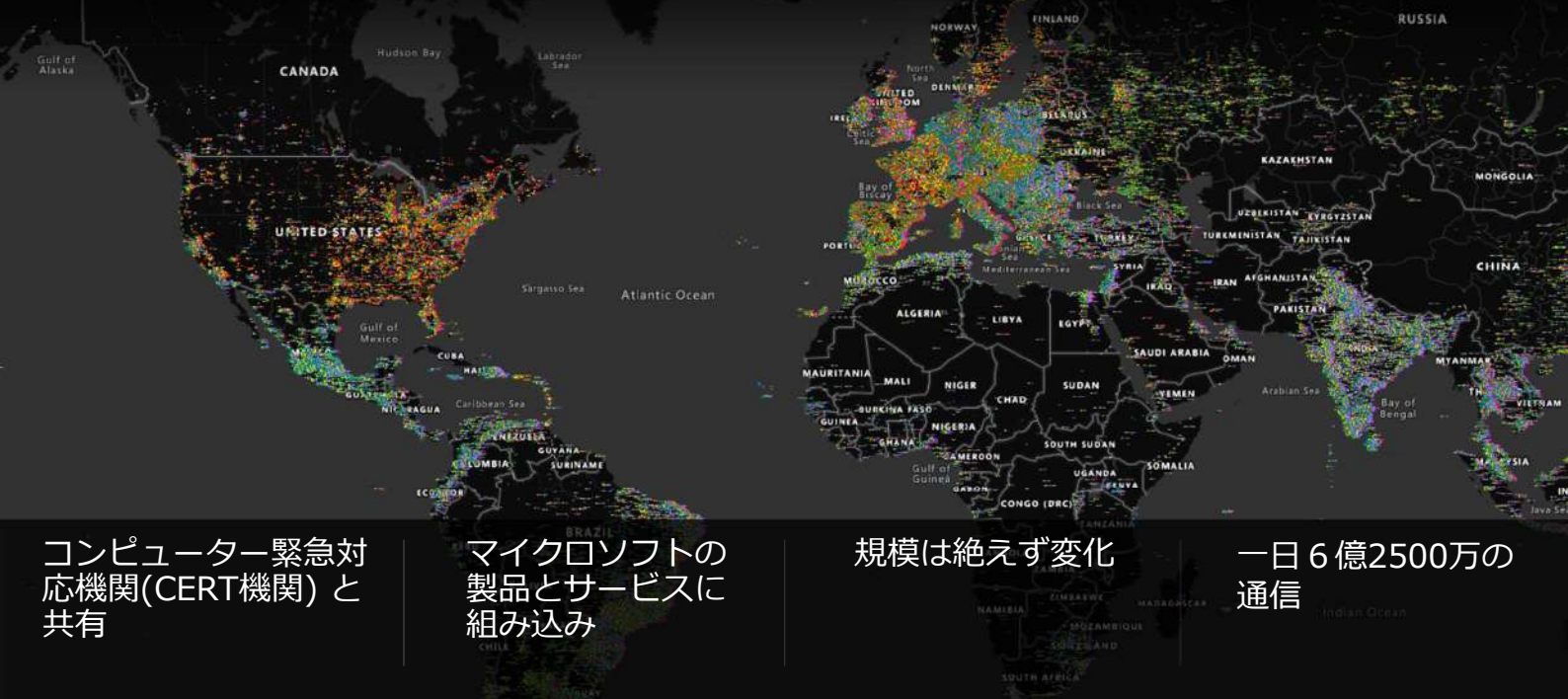
個のサイバー犯罪者ではなく、  
犯罪者ネットワークへの対抗措置が必要





## Cyber Threat Intelligence Program (CTIP: サイバー脅威対策プログラム)

マルウェア・テイクダウンから得られた、行動につながるインテリジェンス



コンピューター緊急対応機関(CERT機関)と共有

マイクロソフトの製品とサービスに組み込み

規模は絶えず変化

一日6億2500万の通信

# Trickbot とは?

- 元々は金融機関のサイトを狙い、認証情報を盗むように設計されていた
- Malware-as-a-serviceとして発展したことで多様なサイバー犯罪の基盤となる。例：認証情報の窃取、データ抜き取り

ランサムウェア攻撃

RYUK CRYPTO-RANSOMWARE

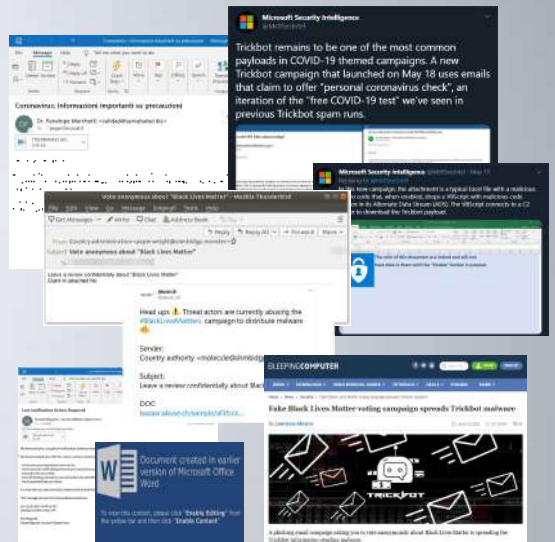
被害コンピュータ

Trickbot payload

感染したルーターなどのIoT機器

Trickbot Tier 1 犯罪インフラ

ホスティング事業者がサービス提供しているネットワーク (IPアドレス)



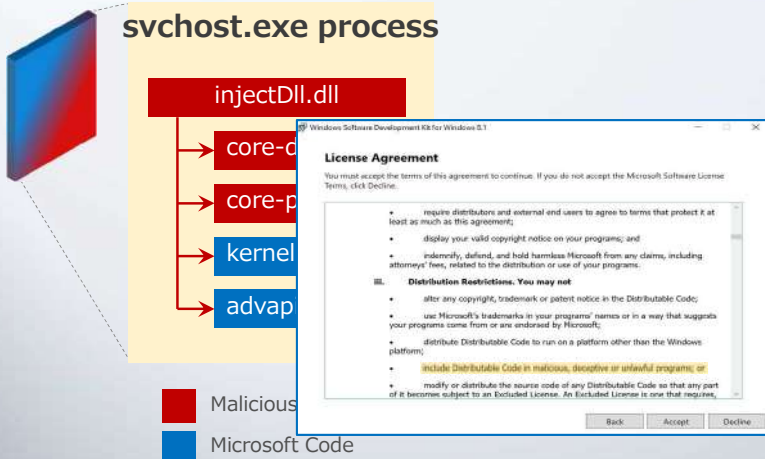
- 既に乗っ取られたことのあるemailを使いまわしたり、時のトピック（コロナやBLM）、または金銭的なおびき寄せを使って、ユーザーが悪意ある添付ファイルを開いたり、悪意あるファイルをホストしているウェブサイトにアクセスしてしまうように巧みに誘導

## Trickbot: テイクダウンを可能としたテクノロジーと法的戦略、そしてパートナーシップ

### 新規な法的手段の遂行

- マイクロソフトのソフトウェアコードの不正使用である、という著作権法上の主張
- その他商標法など、既存の法律をも分析し、使える法的手段を戦略的にとる
- 世界各国の法律についても検討

### 世界のパートナー様との連携



# 第 2 章: 国家レベルの脅威

国家レベルの攻撃を監視、分析、阻止する中でマイクロソフトが認識している状況



## この章の内容:

### 国家レベルの脅威の追跡

- 国家レベルの脅威に関する通知

### 国家レベルのアクティビティへの対抗

- 国家レベルのアクティビティグループに関する概要説明
- マイクロソフトのアプローチ: テクノロジーの活用、悪意のある攻撃に対するアクションの実施、法的措置の活用、公的な議論や政策への情報提供

### 一般的なターゲットと一般的な攻撃手法 包括的な防御が必要 動機

- 重要インフラストラクチャ
- 頻繁にターゲットにされる部門
- 大規模なイベントや、選挙活動のような攻撃機会がターゲット
- 一般的な攻撃目的
- 偵察
- 資格情報の収集
- マルウェア
- VPN の悪用
- 徹底的な防御戦略

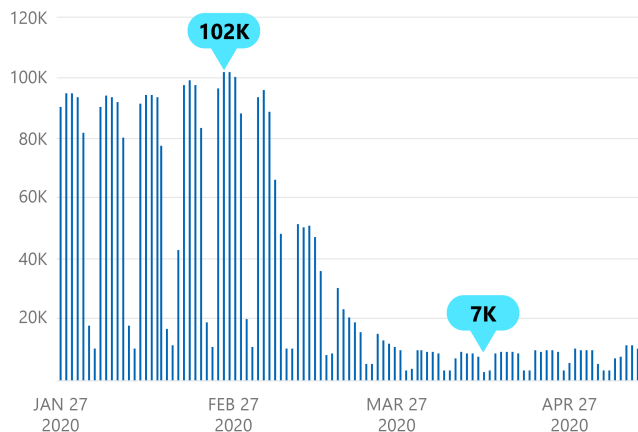


# 3

## セキュリティとリモートワーカー



# リモート ワーカーのためのインフラストラクチャ 企業セキュリティ境界の概念が劇的に変化



インフラストラクチャの多くは、元々はオフィス内での作業用に設計されていたため、リモートワーカー向けの移行の緊急性と規模に対応する準備ができていませんでした。

ビルに入館するためのマイクロソフト社員バッジのスキャン回数が、移行の緊急性と規模を示しています。

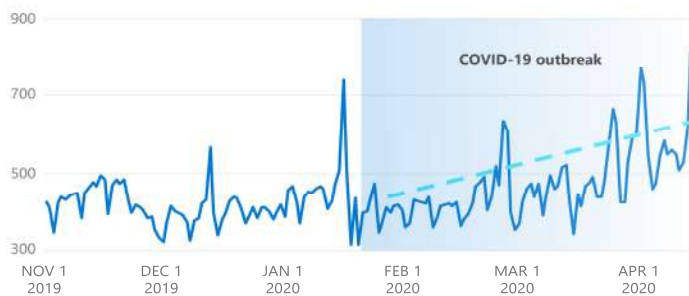


## インフラストラクチャのセキュリティ: ゼロトラスト戦略

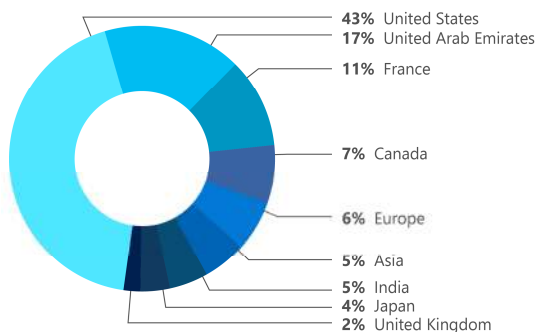
- 信頼できないネットワークから実行されたものとして、すべてのアクセス試行を扱う
- 不明なデバイスや管理されていないデバイスを排除する - ネットワークアーキテクチャではなく IDaaS を利用する

# インフラストラクチャへの攻撃: DDoS マイクロソフトの脅威研究者が認識している状況

COVID-19  
感染拡大中の  
DDoS 攻撃  
件数



攻撃対象地域の分布  
(2020年1月 - 6月)



マイクロソフトが3月中に対処した DDoS 攻撃の1日あたりのユニーク数は600 - 1,000件で、COVID-19発生前のレベルと比べて約50%増加しました。





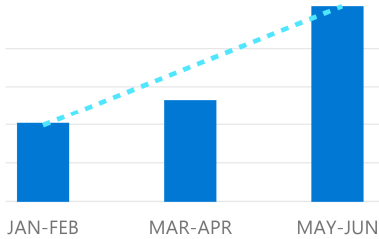
# ID とアクセスの管理



## ID ベースの攻撃

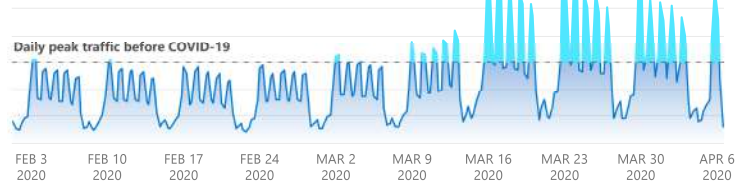
Azure AD アカウントに対するパスワードブルート フォース攻撃の試行数

Azure Active Directory では 2020 年前半、企業アカウントに対してブルート フォース手法を使用する ID ベースの攻撃件数が増加しました。



このような攻撃を防御するには強力な認証方法が重要である

多要素認証 (MFA) における毎週の有効化リクエストの件数 (2020 年 2 月 3 日 - 4 月 6 日)



COVID-19 の発生後、在宅勤務方針が定められたことに伴い、MFA 有効化リクエストの件数が約 2 倍に増加。

## 企業の回復力: 新しい現実

パンデミックを生き抜くために学んだ教訓と実施された戦略

- ✓ オンサイトの境界を越えて企業のセキュリティ境界を拡張
- ✓ 回復力の優先
- ✓ 社員の対応力 (Work-Life **Balance Integration**)

COVID-19 への対応策を既存の運用手順を見直すだけでなく、教訓を基にした**新しい前提条件 (ベースライン)** から記述



# 第3章: セキュリティとリモートワーカー

移行の緊急性と規模によって生じる課題



## この章の内容:

### リモートワーカーのための インフラストラクチャ

- ゼロトラストセキュリティモデル
- 仮想プライベートネットワーク (VPN) アーキテクチャ
- 企業リソースへのアクセス制御
- デバイスとパッチの管理
- インフラストラクチャへの攻撃: DDoS

### データの機密性、 コンプライアンス、保護

- 情報に対する権利の管理

### 人員

- ID とアクセスの管理
- ID ベースの攻撃
- 内部関係者の脅威

### 企業の回復力: 新しい現実

- パンデミックを生き抜くために学んだ教訓と実施された戦略



S

# 4

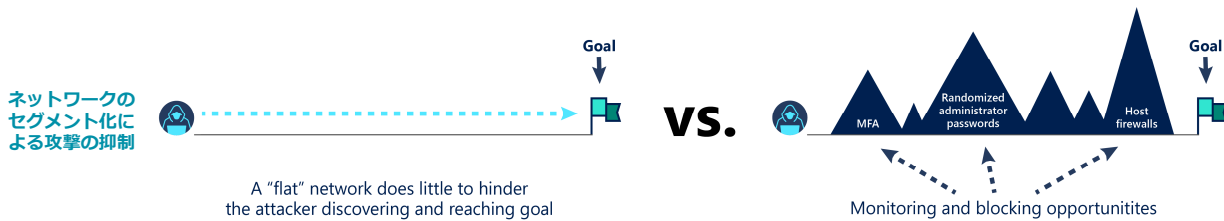
すぐ実践できる研究成果

# すぐ実践できる研究成果: 今日からできること

レポートで要約されている 20 項目の「トップ 5」



- 1 多要素認証 (MFA) の採用
- 2 電子メールの「ハイジーン (衛生)」の適切な実施
- 3 アプリとシステムへのパッチ適用
- 4 最低限の特権によるアクセスの制限
- 5 ネットワークのセグメント化による攻撃の抑制



## セキュリティにおける機械学習

機械学習への攻撃がソフトウェア業界でますます現実化



### Attacks on machine learning systems

**Poisoning attack** Attacker contaminates the training phase of ML systems to get intended result

**Model stealing** Attacker is able to recover the model by constructing careful queries

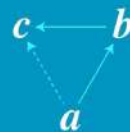
**Model inversion** Attacker recovers the secret features used in the model through careful queries

モデルポイズニングは、ビジネス意思決定者向けの機械学習に対する最大の脅威として認知されています。



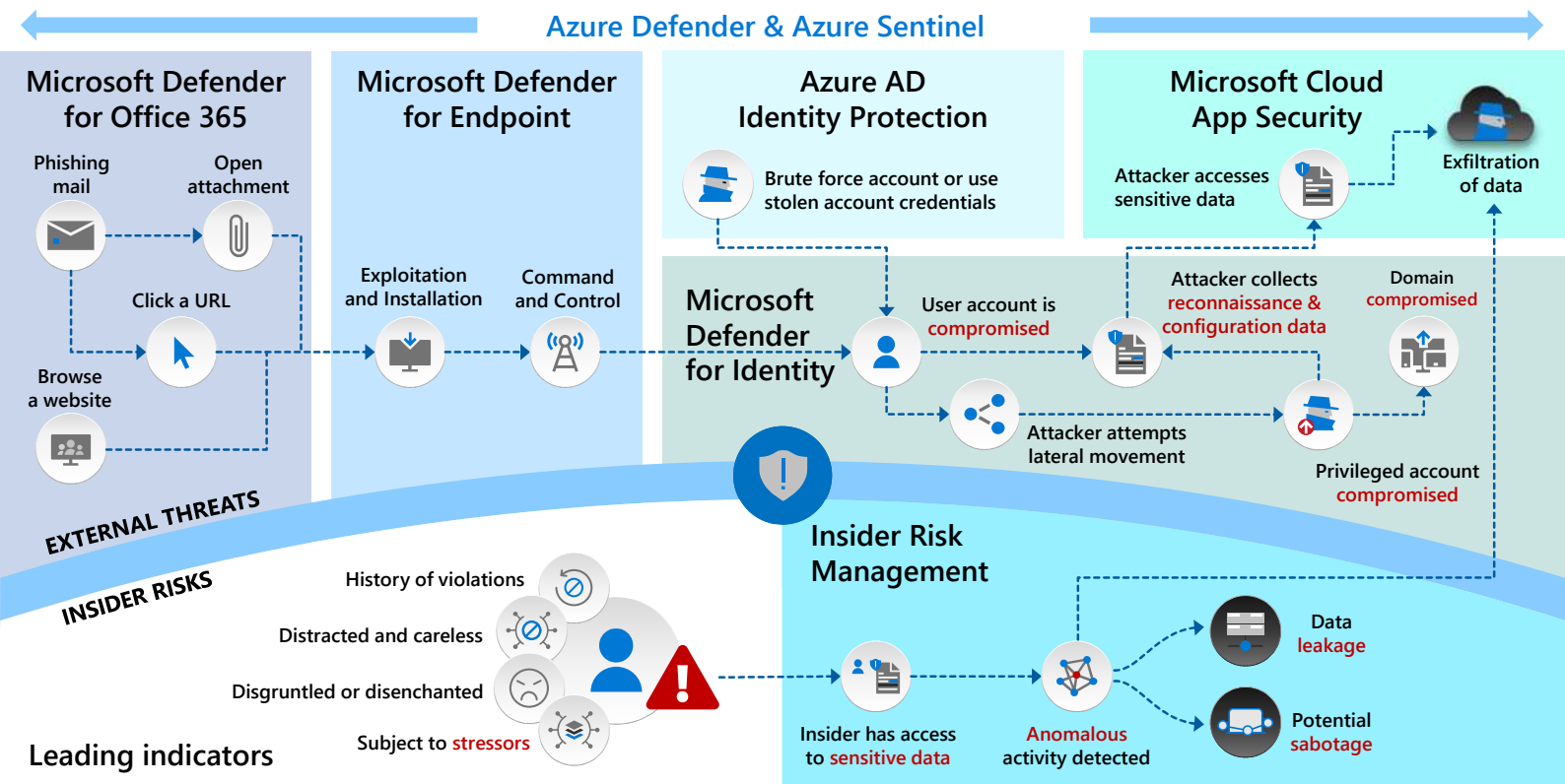
### BLAST RADIUS:

The full privileges of an entity in your cloud include hidden/transitive privileges.



The full impact if an entity in your cloud is compromised.

# Internal and external protection across the threat kill chain



## Q&A

詳細なレポートとその他の情報については、SharePoint サイトを参照：  
<https://aka.ms/DigitalDefenseReport>