

サイバー攻撃の国際動向と対応

Microsoft Digital Defense Report

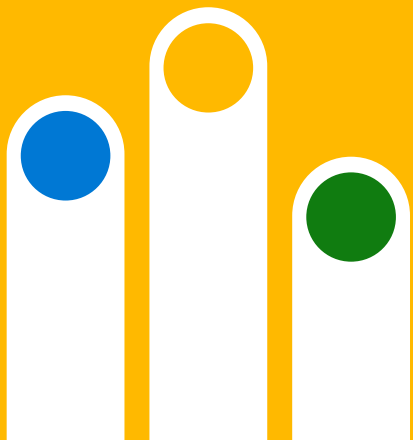
日本マイクロソフト株式会社
セキュリティ & コンプライアンス統括本部
本部長
高田 祐二

セキュリティは今までに
ないほど重要なもの
になっています

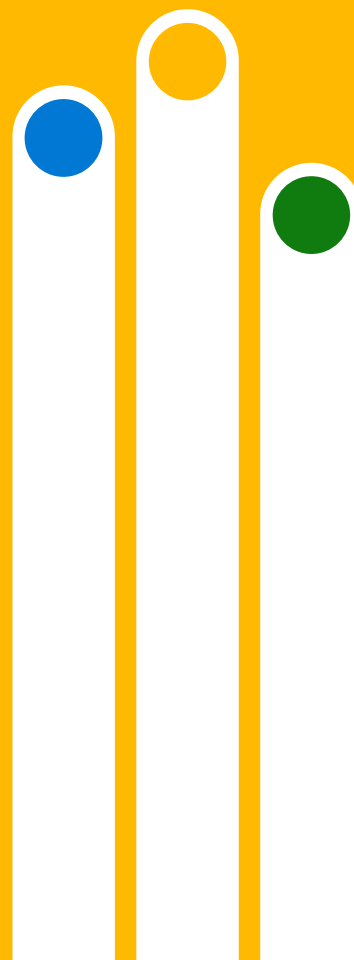
サイバー攻撃はこれまで以上に
頻繁かつ洗練されたものになっています

マルチクラウドIT環境への
サイバーセキュリティの対応を迫られています

増加し複雑化する法規制環境



驚異的な速度で
攻撃が進んでいます



1,287件

1秒間に発生している
パスワード攻撃数
毎年120%増加し続けている

1時間 12分

フィッシングメールの被害に
遭った場合に攻撃者が個人
情報に到達するための平均
時間

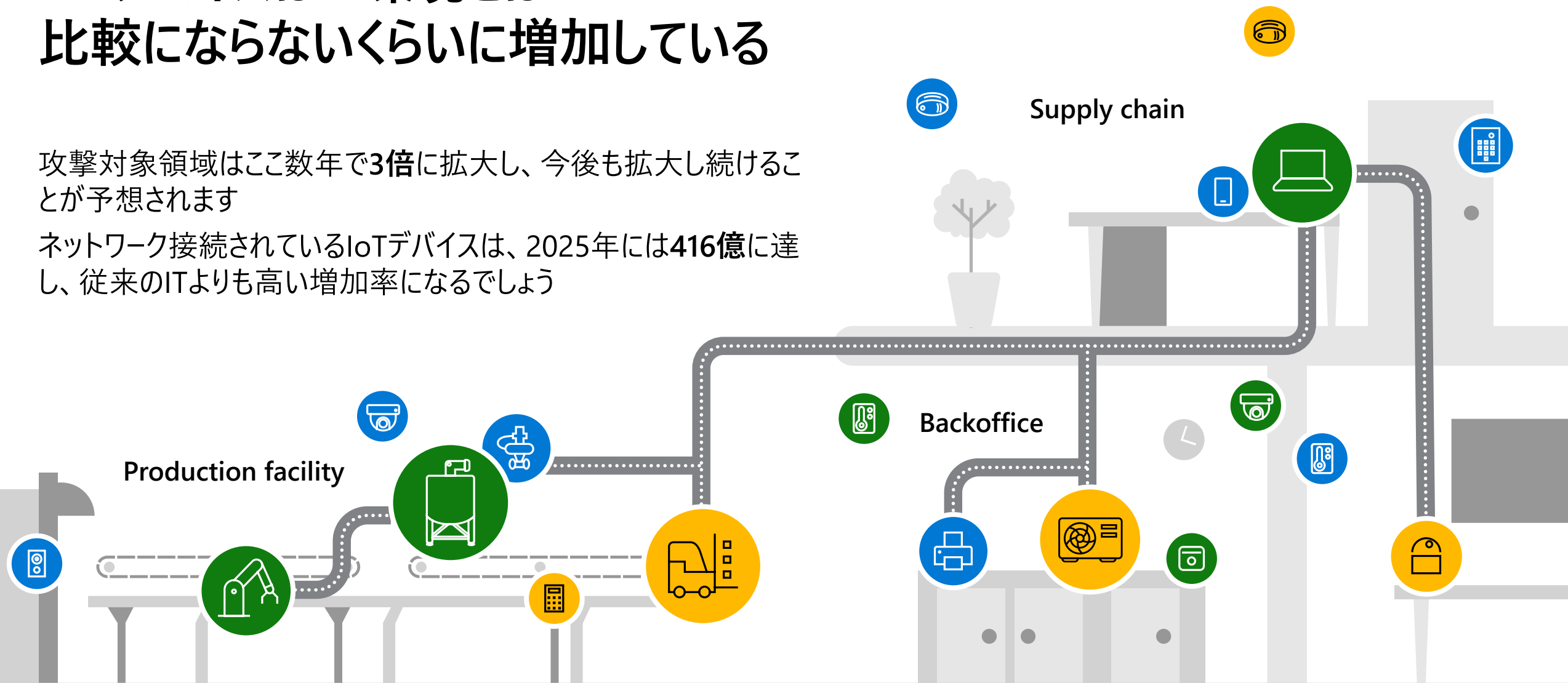
1時間 42分

デバイスが侵害されてから、
攻撃者が社内ネットワークで
ラテラルムーブメントを始める
までの平均時間

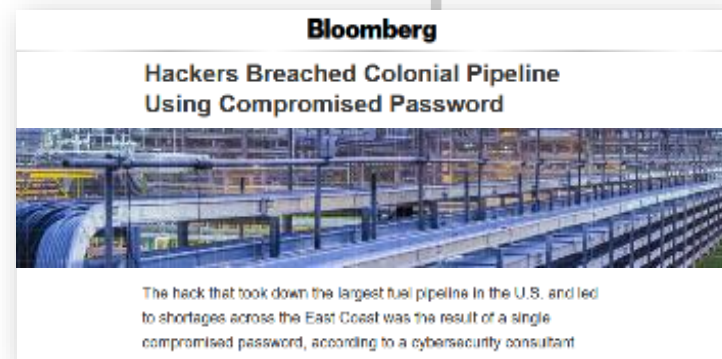
IoTデバイスはIT環境とは 比較にならないくらいに増加している

攻撃対象領域はここ数年で**3倍**に拡大し、今後も拡大し続けることが予想されます

ネットワーク接続されているIoTデバイスは、2025年には**416億**に達し、従来のITよりも高い増加率になるでしょう



重要インフラがサイバー戦争の主戦場となる



IoTとOT の複雑さが セキュリティをより難しいものとしている

脆弱性が蔓延し、
さらに増加し続け
ている

75%

産業用制御用システム
の75%に深刻度の高い
未パッチの脆弱性が存
在する。

+78%

産業用制御用システム
における深刻度の高い
脆弱性の露出が増加

攻撃ツールの入手
により、だれでも簡
単に機器を悪用で
きる

72%

産業用制御システム専
用エリアの72%にオン
ラインから簡単にアク
セス可能





Microsoft Digital Defense Report 2022

Illuminating the threat landscape
and empowering a digital defense.

01 Microsoft Digital Defense Report 2022

Contents

The data, insights, and events in this report are from July 2021 through June 2022 (Microsoft fiscal year 2022), unless otherwise noted.

For the best experience viewing and navigating this report, we recommend using Adobe Reader, available as a free download from the Adobe website.

Report
Introduction

The State of
Cybercrime

Nation State
Threats

Devices and
Infrastructure

Cyber Influence
Operations

Cyber
Resilience

Contributing
Teams

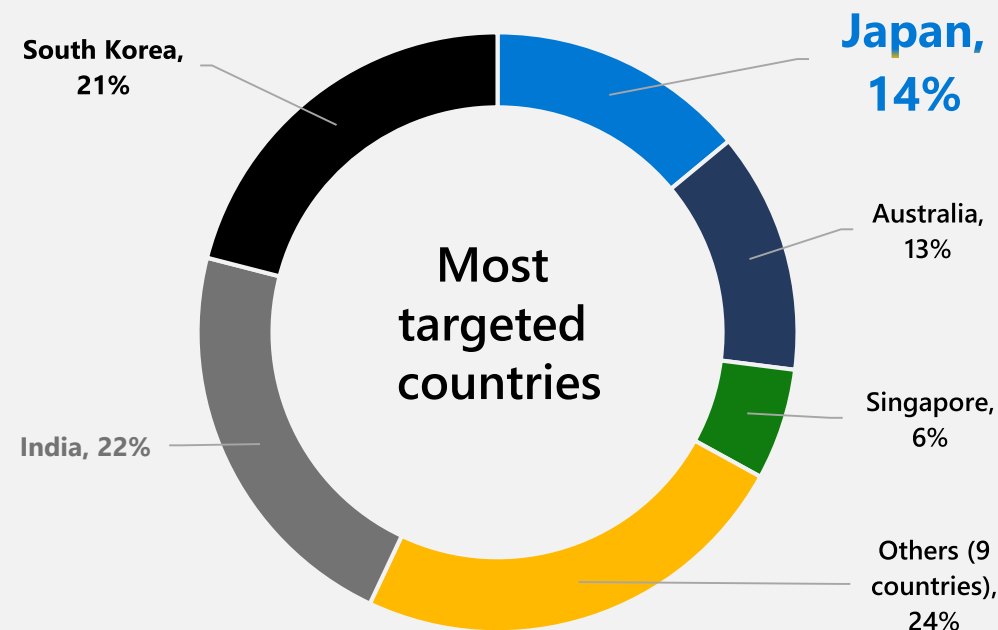


Report Introduction	02	Iran growing increasingly aggressive following power transition	46	Cyber Resilience	86
The State of Cybercrime	06	North Korean cyber capabilities employed to achieve regime's three main goals	49	An overview of Cyber Resilience	87
An overview of The State of Cybercrime	07	Cyber mercenaries threaten the stability of cyberspace	52	Introduction	88
Introduction	08	Operationalizing cybersecurity norms for peace and security in cyberspace	53	Cyber resiliency: A crucial foundation of a connected society	89
Ransomware and extortion: A nation-level threat	09	Devices and Infrastructure	56	The importance of modernizing systems and architecture	90
Ransomware insights from front-line responders	14	An overview of Devices and Infrastructure	57	Basic security posture is a determining factor in advanced solution effectiveness	92
Cybercrime as a service	18	Introduction	58	Maintaining identity health is fundamental to organizational well-being	93
The evolving phishing threat landscape	21	Governments acting to improve critical infrastructure security and resilience	59	Operating system default security settings	96
A timeline of botnet disruption from Microsoft's early days of collaboration	25	IoT and OT exposed: Trends and attacks	62	Software supply chain centrality	97
Cybercriminal abuse of infrastructure	26	Supply chain and firmware hacking	65	Building resilience to emerging DDoS, web application, and network attacks	98
Is hacktivism here to stay?	28	Spotlight on firmware vulnerabilities	66	Developing a balanced approach to data security and cyber resiliency	101
Nation State Threats	30	Reconnaissance-based OT attacks	68	Resilience to cyber influence operations: The human dimension	102
An overview of Nation State Threats	31	Cyber Influence Operations	71	Fortifying the human factor with skilling	103
Introduction	32	An overview of Cyber Influence Operations	72	Insights from our ransomware elimination program	104
Background on nation state data	33	Introduction	73	Act now on quantum security implications	105
Sample of nation state actors and their activities	34	Trends in cyber influence operations	74	Integrating business, security, and IT for greater resilience	106
The evolving threat landscape	35	Influence operations during the COVID-19 pandemic and Russia's invasion of Ukraine	76	The cyber resilience bell curve	108
The IT supply chain as a gateway to the digital ecosystem	37	Tracking the Russian Propaganda Index	78		
Rapid vulnerability exploitation	39	Synthetic media	80		
Russian state actors' wartime cyber tactics threaten Ukraine and beyond	41	A holistic approach to protect against cyber influence operations	83		
China expanding global targeting for competitive advantage	44			Contributing Teams	110

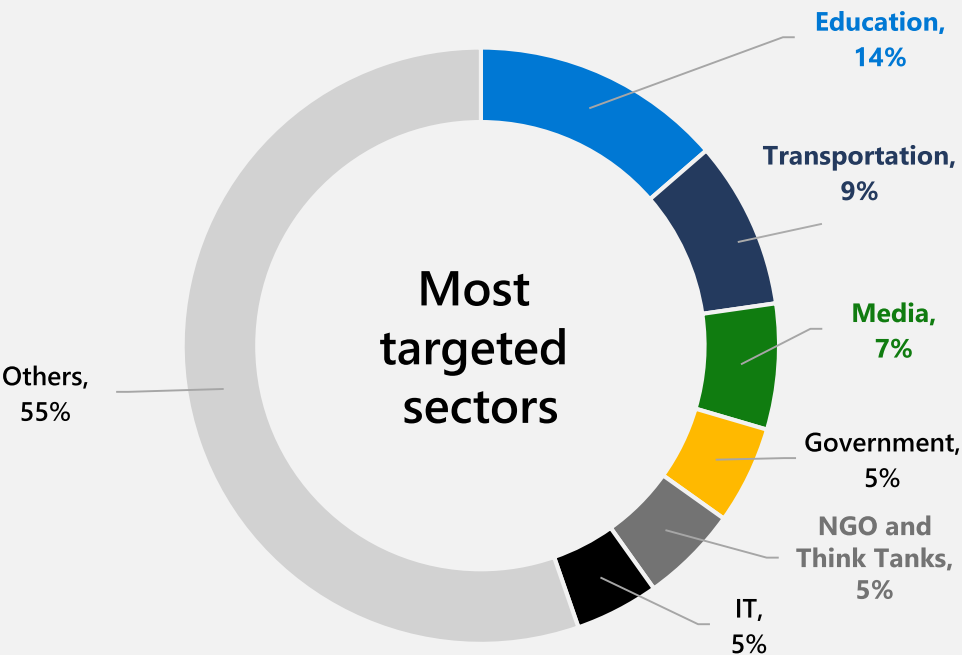
攻撃者の現状 - APAC

July 2022 – January 2023

インドは主にイラン脅威勢力の標的となった。韓国と日本は北朝鮮の主な敵国であり、北朝鮮の攻撃者の主要な標的となっています。



北朝鮮の脅威者は、シンクタンク、メディア、学術機関など、さまざまな分野に関心を持っていた。イランの攻撃者は、交通機関を積極的にターゲットにしていた。



Numbers in charts and graphs are taken from Microsoft's Nation State Notification process

98%

基本的なサイバーハイジーンで
98%の攻撃から保護できます



多要素認証の適用



ゼロトラストの適用



モダンなエンドポイント保護



最新環境の維持



データ単位での保護

自動バックアップとクリーンアップ – OneDrive



脅威インテリジェンスを活用した動的モニタリングと選択式のオンデマンド対応

全ての人がサイバーセキュリティの役割を果たさなくてはならない

マイクロソフトは、すべての人がサイバー・スマートになれるよう支援し、次世代の人材を育成することを約束します。



サイバーセキュリティ・アウェアネス

Microsoft Security



『サイバースマートになろう』キットを入手する

最新のサイバーセキュリティのインサイトとベストプラクティスを組織の共有しましょう。『サイバースマートになろう』キットをダウンロードして、組織の教育に役立ててください。

『サイバースマートになろう』キットには、お客様や関係者の習得を支援するためのインフォグラフィック、ビデオ、メールが含まれています。

- ID、デバイス、データを保護します。
- フィッシングやその他の詐欺から身を守ります。
- パスワードを効果的に管理します。
- ソフトウェアを最新の状態に保ちます。

キットをダウンロード

必要事項をご入力ください

名 *

姓 *

ビジネス用メールアドレス *

会社名 *

所属部署 *

職種 *

関心のあるセキュリティ領域 *

勤務地の電話番号 *

国コード *



教育・スキリング イニシアチブ

- » 技術教育・学習支援（TEALS）・DigiGirlz
- » ラストワンマイルの奨学金プログラム
- » NGOと連携したメンターシップとスキリングプログラム

セキュリティリーダーとしてのマイクロソフト

目標を達成

\$200億 年間の
セキュリティ収益

導入組織数

86万 120か国での
導入組織数

分析能力

65兆 毎日の
シグナル数

研究開発

\$200億 5年間の
研究開発費

攻撃の追跡

250以上 国家アクターなどの
攻撃者の延べ数

攻撃防御

70億 2022年の
攻撃防御数

Thank you

