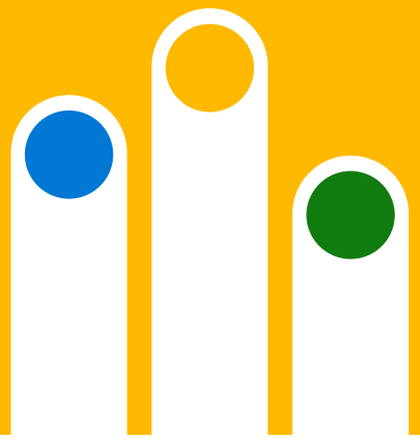
Microsoft Security

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

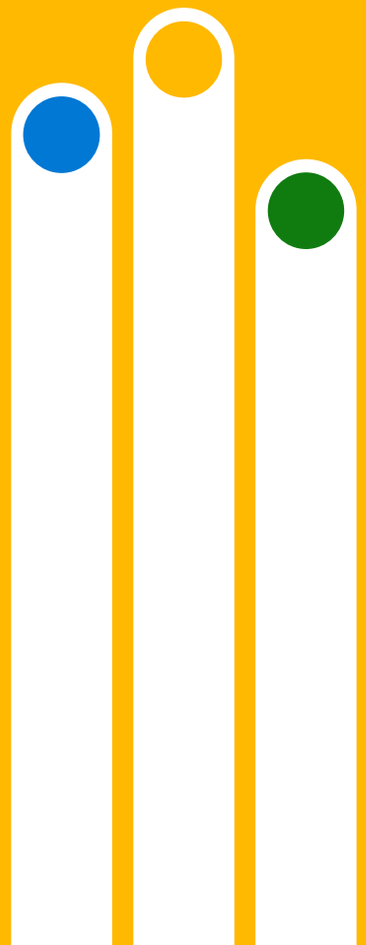


サイバー攻撃はこれまで以上に
頻繁かつ洗練されたものになっています

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

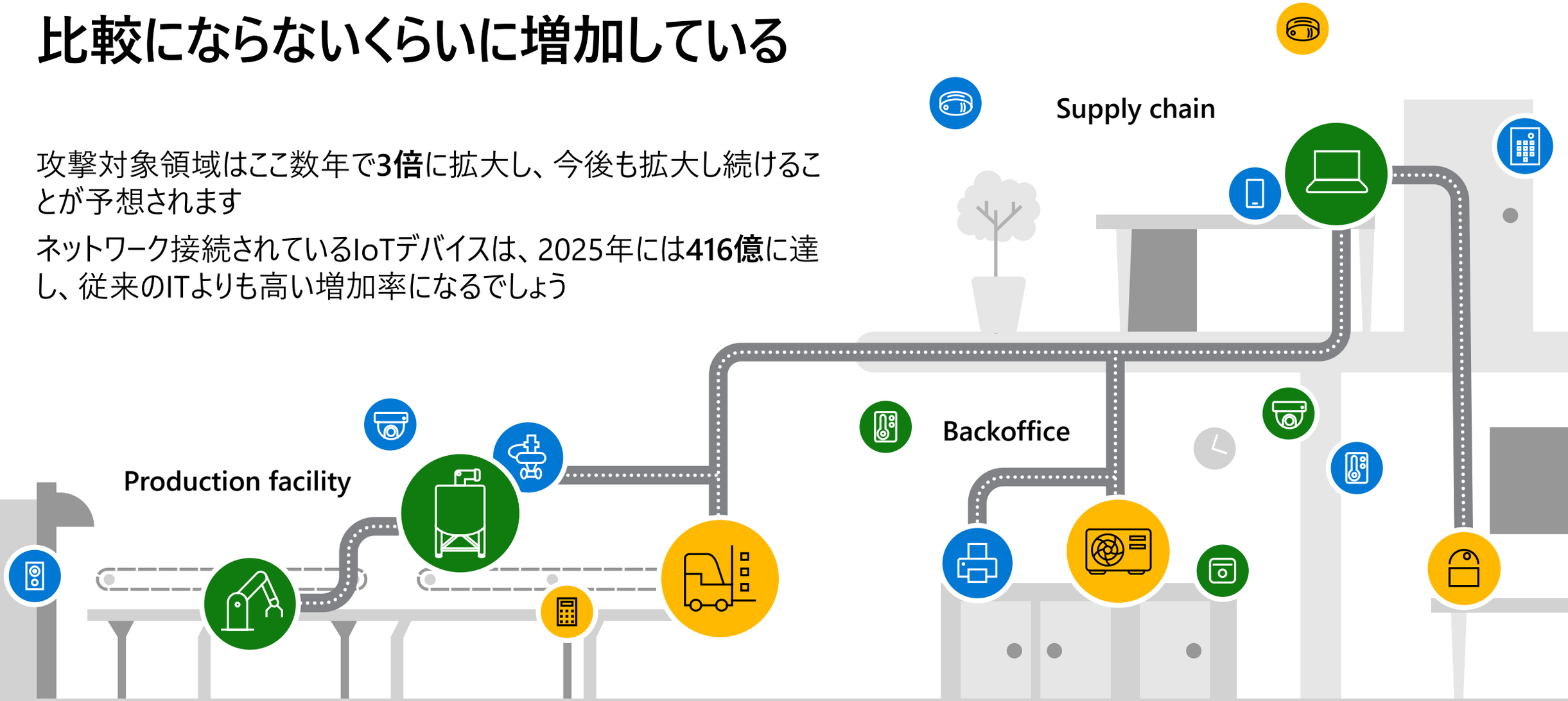
1時間12分
フィッシングメールの被害に
遭った場合に攻撃者が個人
情報に到達するための平均
時間

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
ラテラルムーブベントを始める
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



1. IDC

重要インフラがサイバー戦争の主戦場となる

ZDNet

NASA hacked because of unauthorized Raspberry Pi connected to its network

NASA described the hackers as an "advanced persistent threat," a term generally used for nation-state hack

DARKReading | SIGN UP FOR OUR NEWSLETTERS

Verkada Breach Demonstrates Danger of Overprivileged Users

In re-evaluating supply chains, companies should classify vendors with super admin privileges to devices or backdoors as a significant threat.

ZDNet

Hackers are attacking smart building access systems

More than 2,300 building access systems can be hijacked due to a severe vulnerability left without a fix.

ZDNet

Triton hackers return with new, covert industrial attack

Traces of a hacking group behind the destructive Triton malware have been found at a new infrastructure facility following an infamous attack in the Middle East.

Bloomberg

Hackers Breached Colonial Pipeline Using Compromised Password

The hack that took down the largest fuel pipeline in the U.S. and led to shortages across the East Coast was the result of a single compromised password, according to a cybersecurity consultant

The New York Times

'Dangerous Stuff': Hackers Tried to Poison Water Supply of Florida Town

For years, cybersecurity experts have warned of attacks on small municipal systems. In Oldsmar, Fla., the levels of lye were changed and could have sickened residents.

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

Microsoft Digital Defense Report 2022

Illuminating the threat landscape and empowering a digital defense.

Contents

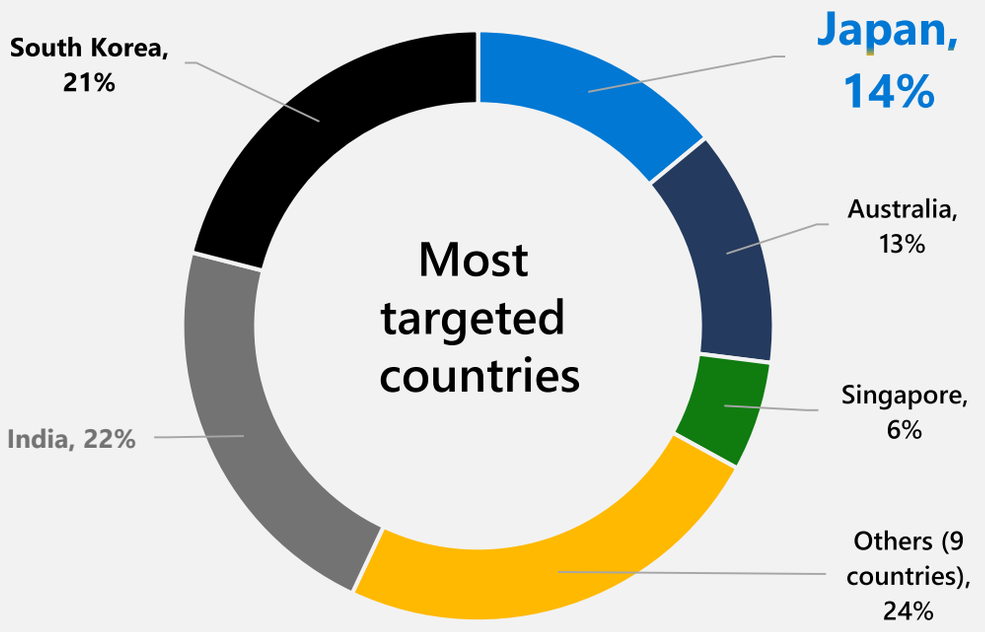
The data, insights, and events in this report are from July 2021 through June 2022 (Microsoft fiscal year 2022), unless otherwise noted.

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

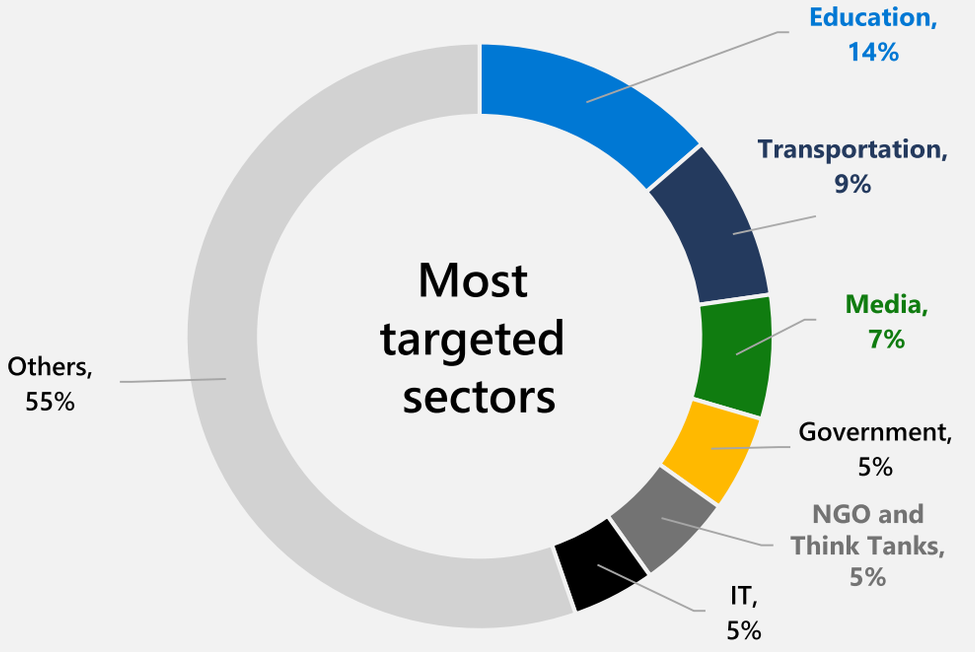
攻撃者の現状 - APAC

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。



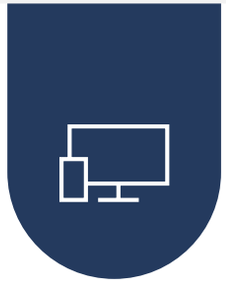
北朝鮮の脅威者は、シンクタンク、メディア、学術機関など、さまざまな分野に関心を持っていた。イランの攻撃者は、交通機関を積極的にターゲットにしていた。



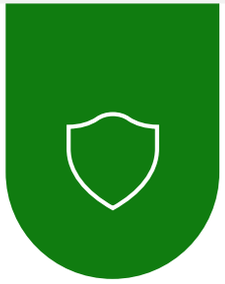
Numbers in charts and graphs are taken from Microsoft's Nation State Notification process

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

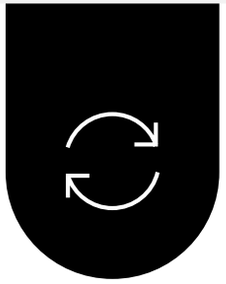


多要素認証の適用



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

OneDrive

異常をリアルタイム監視

攻撃手法などをアップデート

65兆のシグナルから得られる
脅威インテリジェンス

警告と確認

デバイスクリーンアップ

復元元の選択

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

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

Microsoft Security

Thank you