国内EDR実態調査結果について

EDRの導入を成功させるために考えるべきポイント

タニウム合同会社

マーケティング本部長 (北アジア担当) 齊藤 純哉

市場調査の概要について

- 当社では、ITR社の第三者調査として、国内大企業のIT管理者および担当者を対象にEDR (Endpoint Detection and Response)に関する実態調査を行い、644件の有効回答を入手しました
  - 当該資料引用箇所については出典を明記しております

- アンケート回答者は従業員数1,000名以上の企業並びに公共団体となります

- 本日のセッションでは、 国内におけるEDR導入の現状や課題についてご説明させていただきます

- 加えて、EDR導入を成功裏に進めるために企業・公共団体がとるべき方向性について解説させていただきます

はじめに

タニウムの会社概要

サイバーセキュリティ領域における#1* ユニコーン企業

	Tanium Inc.	タニウム合同会社(日本)
設立	2007年(2012年まで5年間の製品開発期間)	2014年
代表	Orion Hindawi (Co-founder & CEO)	古市 力(代表執行役社長)
従業員数	約2,000名	約100名
本社	ワシントン州 カークランド	東京、大阪、名古屋
パートナー	➢ テクノロジー & サービスパートナー accenture Chronicle DXC.technology paloalto NETWORKS pwc salesforce servicenow splunk> verizon	➢ 国内主要販売パートナー CTC FUJITSU LAC macnica networks NEC net one NTT Communications NTT DATA NTT DATA INTELLILINK Corporation SB C&S TechMatrix 株式会社 日立システムズ ほか
主な実績	米国：金融機関トップ12行が採用 米国：リテール企業トップ7社が採用 米国：米国防省傘下の大半が採用 フォーチュン100の企業の50%が採用	みずほフィナンシャルグループ様、資生堂様、全日本空輸様、 NTTデータ様、NTT西日本様、ヤンマー様、福井県庁様、 各重要インフラ事業者様 他 *法人格略
ベンチャーキャピタル	ANDREESSEN HOROWITZ TPG GROWTH citi VENTURES GEODESIC CAPITAL salesforce ventures	

* CBINSIGHTS – The Complete List of Unicorn Companies (2021, 05)

激しさを増すサイバー攻撃

世界規模で官民を問わずサイバーセキュリティの強化が叫ばれている

Administration

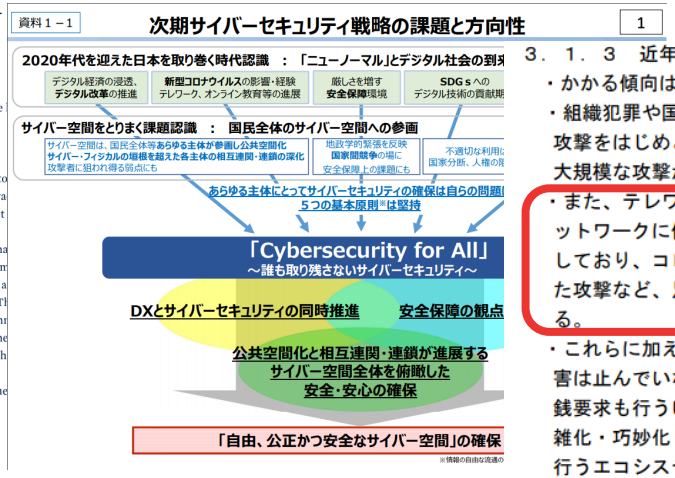
BRIEFING ROOM

Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the
the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly
sophisticated malicious cyber campaigns that threaten the public secto
private sector, and ultimately the American people's security and priva
Federal Government must improve its efforts to identify, deter, protect
against, detect, and respond to these actions and actors. The Federal
Government must also carefully examine what occurred during any ma
cyber incident and apply lessons learned. But cybersecurity requires m
than government action. Protecting our Nation from malicious cyber a
requires the Federal Government to partner with the private sector. Th
private sector must adapt to the continuously changing threat environ
ensure its products are built and operate securely, and partner with the
Federal Government to foster a more secure cyberspace. In the end, th
we place in our digital infrastructure should be proportional to how
trustworthy and transparent that infrastructure is, and to the consequ
we will incur if that trust is misplaced.



３．１．３　近年のサイバー空間における脅威の動向

・かかる傾向は、近年のサイバー空間における脅威の動向をみても明らか。

・組織犯罪や国家の関与が疑われる攻撃が多く発生しており、海外では選挙に対する攻撃をはじめとする民主プロセスへの干渉や、サプライチェーンの弱点を悪用した大規模な攻撃が猛威を奮っている。

・また、テレワーク等の普及に伴い個々の端末経由又はVPN機器の脆弱性を悪用しネットワークに侵入されるケースや、クラウドサービスが標的とされるケースが増加しており、コロナ禍に乗じたサイバー攻撃やグローバル化に伴う海外拠点を経由した攻撃など、足元の環境変化をタイムリーに捉えたサイバー攻撃も現にみられている。

・これらに加えて、ばらまき型攻撃が2020年に入り急増するなど、標的型攻撃の被害は止んでいないほか、データ復元に加え窃取したデータを公開しない見返りの金銭要求も行ういわゆる「二重の脅迫」を行うランサムウェアなど、従来の脅威が複雑化・巧妙化している。背景として、マルウェアの提供や身代金の回収を組織的に行うエコシステムが成立し、悪意のある者が高度な技術を持たなくても簡単に攻撃を行える状況が指摘されている。

・こうしたサイバー攻撃により、生産活動の一時停止、サービス障害、金銭被害、個人情報窃取、機密情報窃取など経済社会活動に大きな影響が生じている。

高まる端末（エンドポイント）管理の重要性

エンドポイントセキュリティ＝EDR?

- EDRとは、Endpoint (Threat) Detection and Responseの略語。2013年にGartner社のAnton Chuvakin氏が提唱したコンセプト
- エンドポイント(端末)における不審な挙動（および痕跡）を検出、調査ならびに対応を行うツールへの呼称。この領域に特化した新興ベンダが誕生する一方、大手企業もこの分野へ順次進出
- 旧来からあるEPP(Endpoint Protection Platform)・アンチウィルスソフトがマルウェアへの感染予防目的であるのに対し、EDRはマルウェア感染後の被害最小化を目的とする
- ゼロトラストを実装する中でもエンドポイントは注目領域
- 海外だけではなく国内でも注目度は向上傾向 (図1)

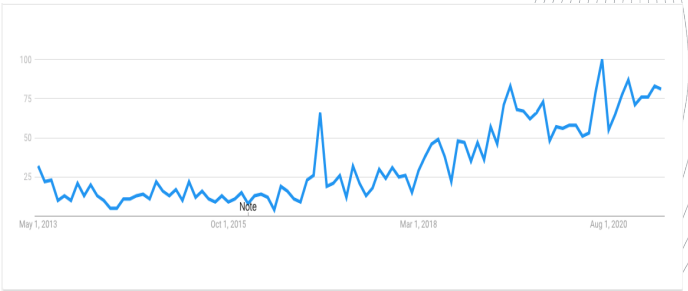
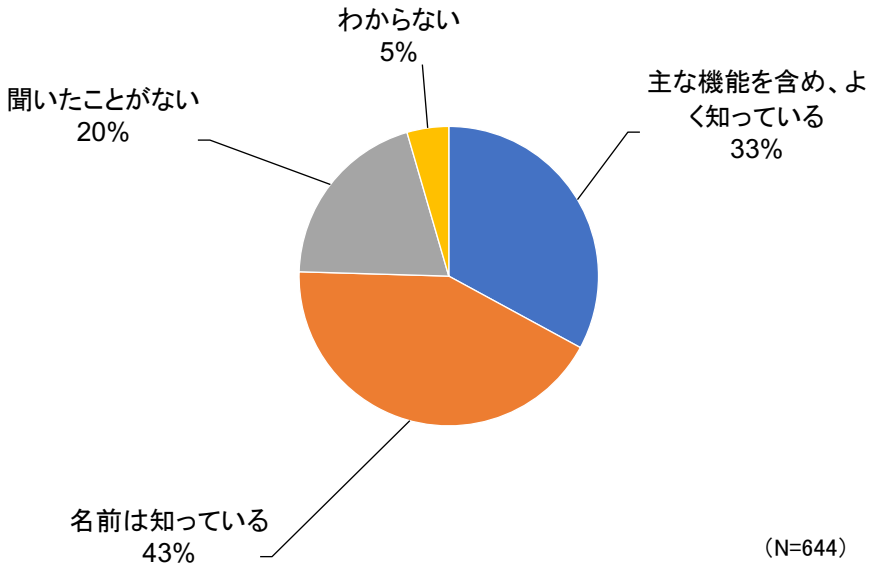


図1. “EDR”のGoogle Trendでの国内における動向 (2013.4-2021.4)

調査結果サマリ

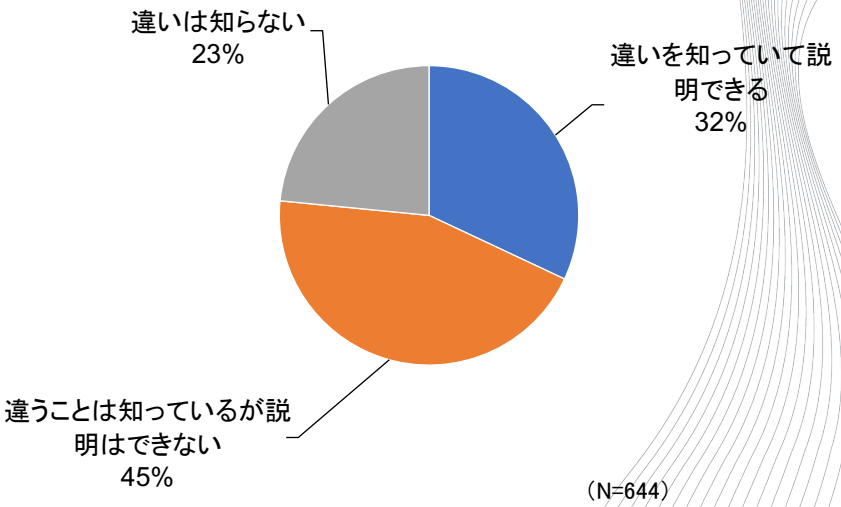
EDRの認知度は高まっているが、実態理解は低い

EDRの認知度*1



（N=644）

EDRとアンチウィルスの違い*2



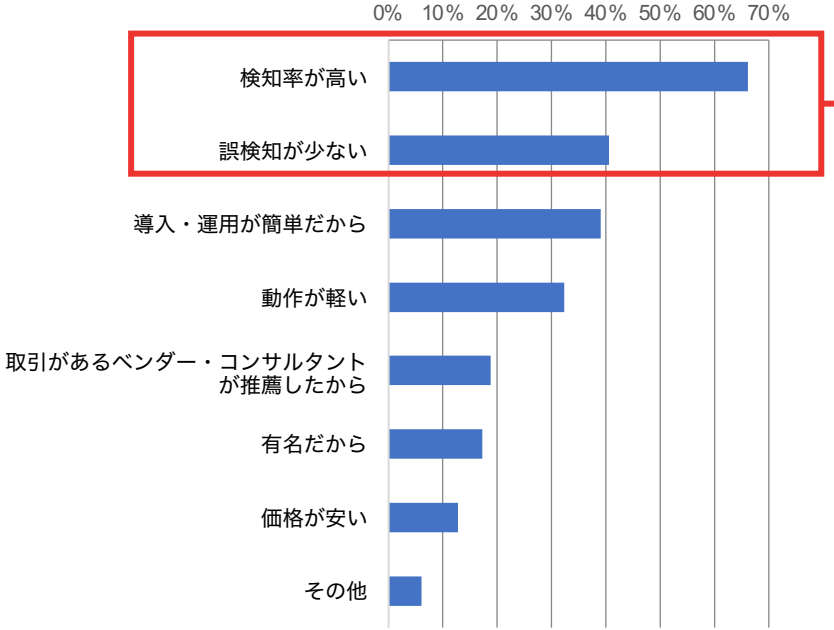
（N=644）

※1※2. 出典：ITR「国内EDR実態調査」（2021年2月調査）

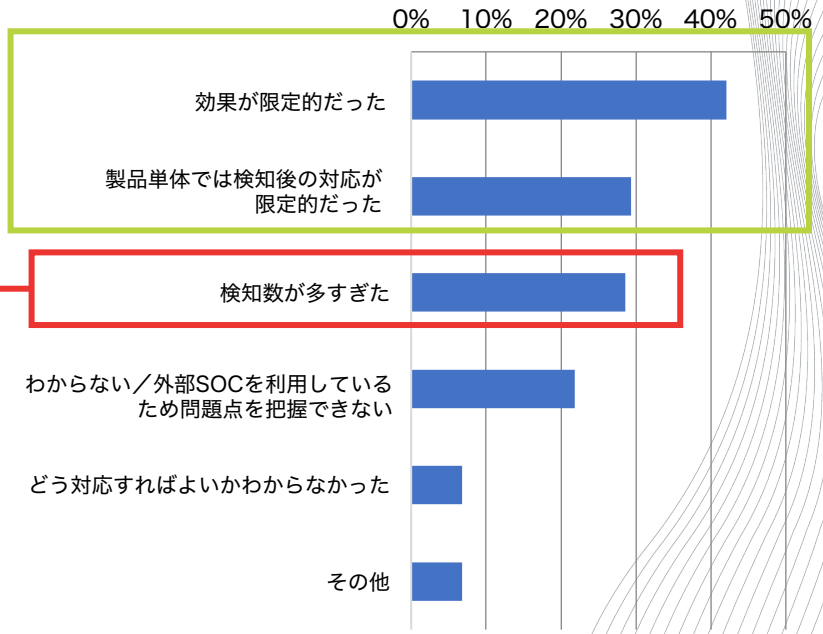
EDRへの期待と導入実態

検知能力の高さは必ずしも有用性につながらない

EDRを選定した理由*3



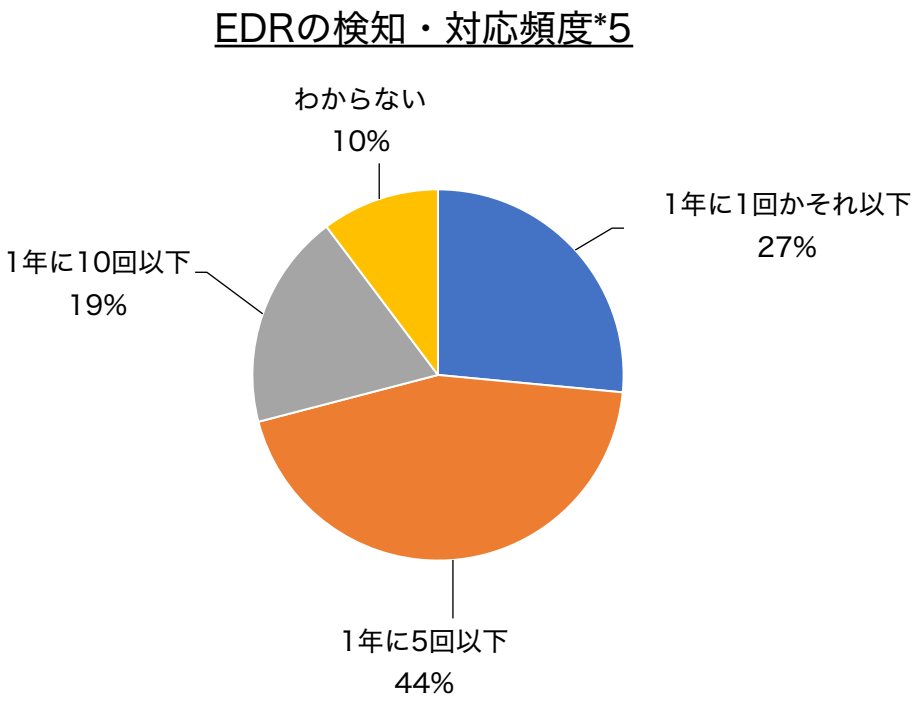
EDR導入で困ったこと*4



※3※4. 出典：ITR「国内EDR実態調査」（2021年2月調査）

EDRの利用頻度

1年に5回以下しか使われないという実態

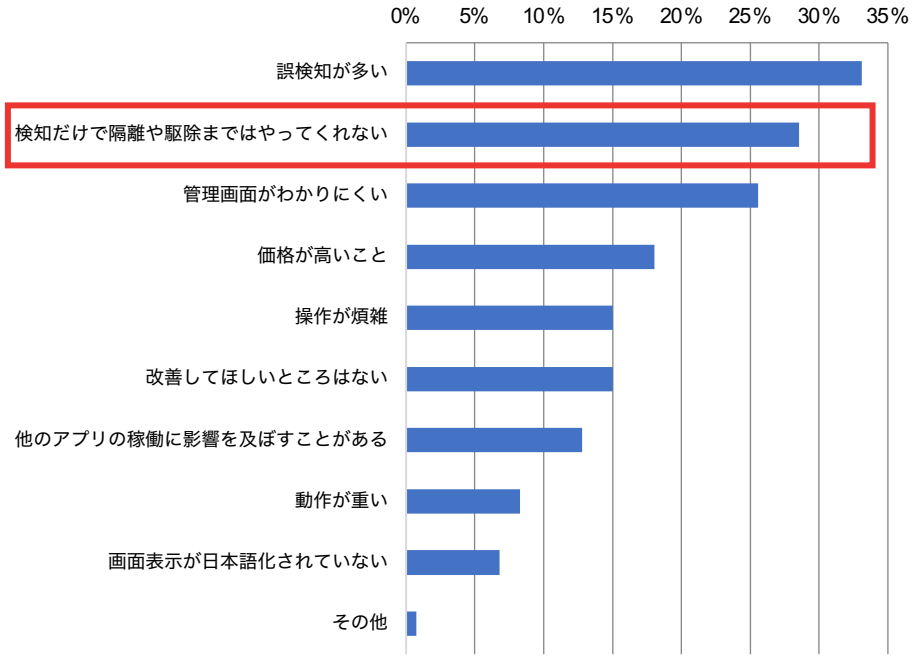


※5. 出典：ITR「国内EDR実態調査」（2021年2月調査）

- 前頁のアンケート結果にある通り、EDRを導入すると検知量そのものは総じて膨大になる
- これは脅威を見逃してしまう「フォールスネガティブ（検知漏れ）」と脅威ではない現象までも脅威として検知してしまう「フォールスポジティブ（誤検知）」のバランスと取るために、誤検知が増えてしまうという特性による
- 無数に上がる誤検知を適切に捌いた上で、実際に対応が必要となる事象は企業規模を問わず年間で**5**件以下と非常に少ない

EDRツールへの改善要望

導入済EDRの改善してほしいところ*6



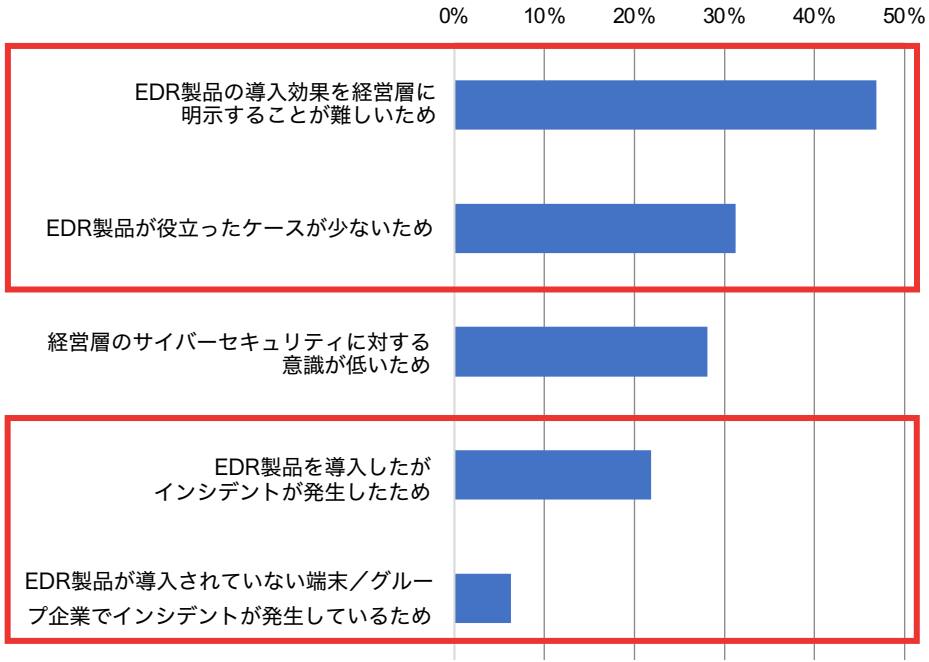
※6. 出典：ITR「国内EDR実態調査」（2021年2月調査）

- 誤検知の多さはツールの特性上、どうしてもついてまわる課題
- 注目すべきはユーザの約3割が「検知だけで隔離や駆除まではやってくれない」ことに不満をもっていること
- **EDRツールベンダの多くは検知(Endpoint Detection)精度を上げることを優先するが、対応(Response)まで必ずしも網羅出来ているわけではない**
- 特に、大規模環境で一斉隔離するといったオペレーションを実装できるツールは必ずしも多くない

EDRの導入効果を経営層に納得させることは難しい

年に数回の検知のために多額の投資を行うことが適切か

経営層の評価が低い理由*7



※7. 出典：ITR「国内EDR実態調査」（2021年2月調査）

- EDR導入後、経営層から芳しい評価を得られていない企業群への質問から、「EDR導入効果の明示化」への課題ならびに、「役立ったケースが少ない」という声が多数を占めることが確認された
- EDR導入後もインシデントが発生している割合が20%を超える
- EDR導入が、経営者観点で評価が低い背景には3点の課題が存在すると想像される
  1. 活用が年に数回にとどまること
  2. 検知のみの対応となっていること
  3. 導入後もインシデントが発生すること

タニウムからの提言

EDRツール導入前に検討すべきポイント

先行して導入したユーザの動向から意識すべき３つのポイント

1. EDRは一連のセキュリティオペレーションプロセスの一部に過ぎず、検知・対応以外のプロセスの底上げをまず図ること

2. ＜見えないものは守れない＞
監視カメラ（EDR）を設置する前に間取図の入手が必要

3. ツール導入効果がわかるような明確なKPIを事前に設定し、そのKPIの達成度を定期的に測ってレポートすること

EDRは万能ツールではない

NISTのサイバーセキュリティフレームワーク全体を踏まえた底上げが必要

1. EDRは一連のセキュリティオペレーションプロセスの一部に過ぎず、検知・対応以外のプロセスの底上げをまず図ること
2. EDRツールは検知を行う監視カメラ
監視カメラを適切に設置するためには建物の設計図が必要
3. ツール導入効果がわかるような明確なKPIを事前に設定し、
そのKPIの達成度を定期的に測ってレポートすること

特定 → 防御 → 検知 → 対応 → 復旧

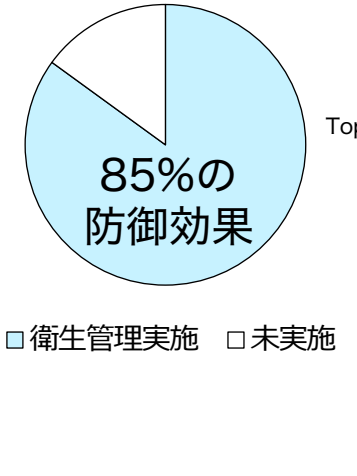
EDRが得意な領域 = 有事の対策

平時の対策 = サイバー衛生管理

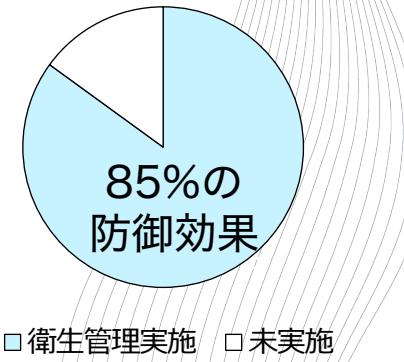
サイバー衛生管理(ハイジーン)は、「絶対的な防御は無い」前提に立ち、組織が「最初に最低限実施しなければならない施策」であり、最大限のコスト効果も証明済み

定量的な効果

カナダ サイバーインシデントレスポンスチーム(CCIRC)
Top 4 Strategies to Mitigate Targeted Cyber Intrusions



米国国土安全保障省(CISA)
Top 30 Targeted High Risk Vulnerabilities



1 EDRは一連のセキュリティオペレーションプロセスの一部に過ぎず、検知・対応以外のプロセスの底上げをまず図ること

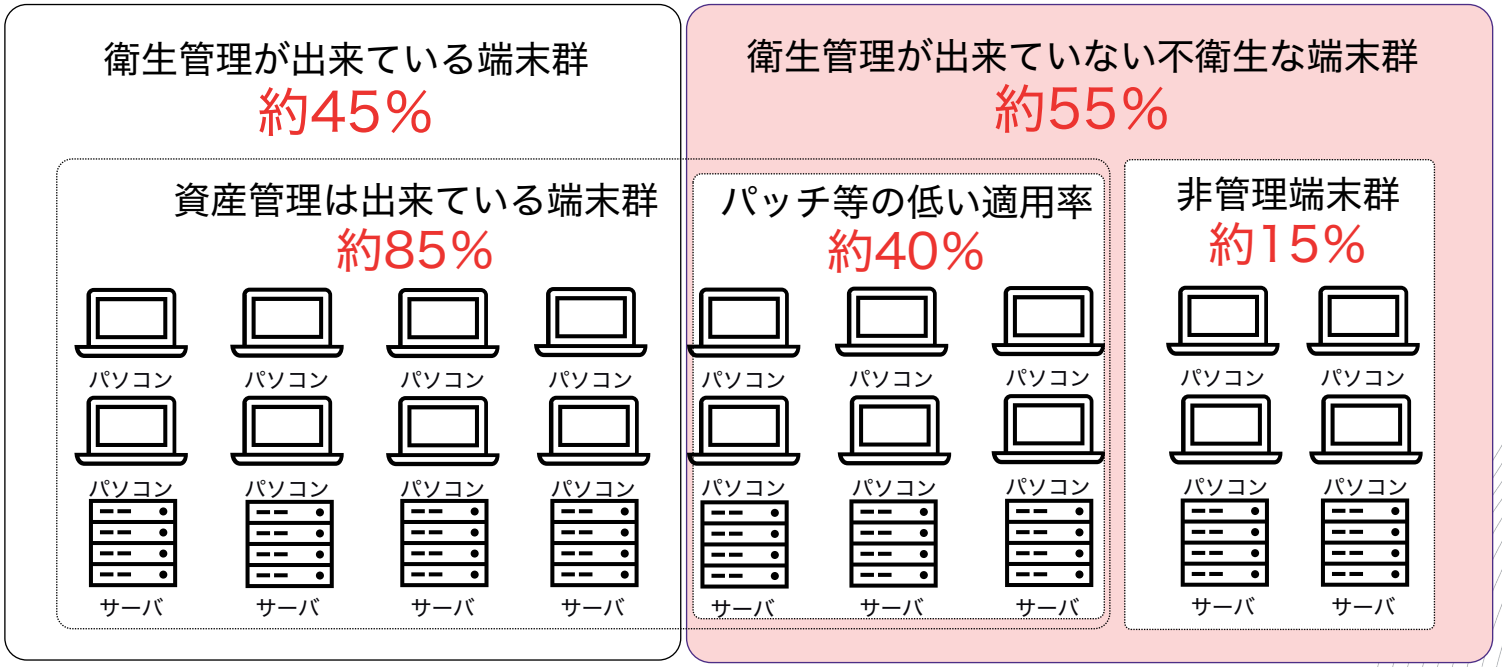
2 ＜見えないものは守れない＞
監視カメラ（EDR）を設置する前に間取図の入手が必要

3 ツール導入効果がわかるような明確なKPIを事前に設定し、そのKPIの達成度を定期的に測ってレポートすること

見えないものは守れない

自社の端末を100%見える化出来ている企業はほとんどないという事実

脆弱性の温床となる不衛生な端末が半数以上の実態*



*タニウム 日本国内での独自調査 (2021)

適切なKPIの設定と継続的評価

事後対策のみでは投資対効果を適切に計測することは難しい

1. EDRは一連のセキュリティオペレーションプロセスの一部に過ぎず、検知・対応以外のプロセスの底上げをまず図ること
2. ＜見えないものは守れない＞ 監視カメラ（EDR）を設置する前に間取図の入手が必要
3. ツール導入効果がわかるような明確なKPIを事前に設定し、そのKPIの達成度を定期的に測ってレポートすること

カテゴリ		KPI①（網羅性）	実績①（前回）	KPI②（時間軸）	実績②（前回）	相対的リスク度	トレンド
IT資産把握率	ハードウェア資産	95%以上	90%（85%）	5分	5分（5分）	中リスク	下降傾向
	ソフトウェア資産	95%以上	92%（90%）	5分	5分（5分）		
	モバイル資産	95%以上	75%（62%）	5分	5分（5分）		
主要ツール稼働率	資産管理 / 脆弱性管理	100%	99%（100%）	5分	5分（5分）	低リスク	変化なし
	EPP / EDR	100%	95%（92%）	5分	5分（5分）		
パッチ適用率	Windows OS	100%	100%（95%）	50時間	80時間（94時間）	中リスク	下降傾向
	主要アプリケーション	100%	98%（95%）	24時間	24時間（36時間）		
ポリシー違反	不正ソフトウェア利用	0件	3件（0件）	5分	5分（5分）	高リスク	上昇傾向
	USB不正利用	0件	1件（3件）	5分	5分（5分）		

リスク対応

- IT資産把握率は順次で増加しているが、拠点Bにおける把握率が悪いので対策を見直す。
- 主要ツールの稼働率は順次増加している。
- パッチ適用率は極めて良好な状態であり、次月も維持する。
- ポリシー違反は複数観測され、社員に対するポリシーの周知徹底を実施する。

世界で最も強いサイバー国家とは？

サイバーパワー世界ランキング

ハーバードケネディスクールのNational Cyber Power Index 2020レポートより

我々がベストプラクティスして
ベンチマークとすべき国家とは？

ベンチマーク(国)が実行する戦略や
フレームワーク、ガイドラインとは？

有事の対策から手を付けることが
本当に近道なのか？

引用：https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf

TANIUM

米国軍が推進する平時の対策の要諦

- 米国サイバー軍の発表(ポイントの要約)
  - ① 自組織のネットワークで起きている事の**「可視化」**の強化
  - ② オンプレミス環境から**「ゼロトラスト環境」**の全面拡大
  - ③ フィジカル領域だけでなくサイバー領域における**「説明責任」**の強化

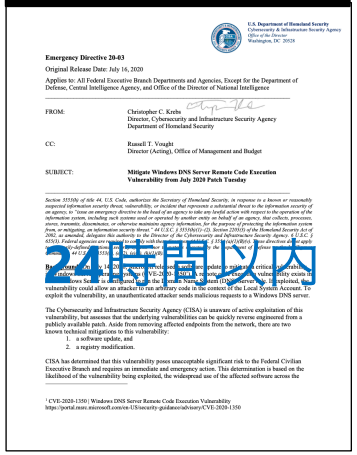
平時：プロアクティブ防御	有事：リアクティブ防御
定常的なサイバー衛生管理の リアルタイム且つ網羅的な実施	リスク最小化から汚染/破壊された環境の 復旧を目的としたサイバー・レジリエンスの実施

※：引用 :https://www.cybercom.mil/

(事例) 米国土安全保障省(DHS) からの連続要請

「平時」における安全宣言の要求 – 2020年の発令を振り返る

8月:脆弱性情報



U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Office of the Director
Washington, DC 20528

Emergency Directive 20-03

Original Release Date: July 16, 2020

Applies to: All Federal Executive Branch Departments and Agencies, Except for the Department of Defense, Central Intelligence Agency, and Office of the Director of National Intelligence

FROM: Christopher C. Krebs
Director, Cybersecurity and Infrastructure Security Agency
Department of Homeland Security

CC: Russell T. Vought
Director (Acting), Office of Management and Budget

SUBJECT: **Mitigate Windows DNS Server Remote Code Execution Vulnerability from July 2020 Patch Tuesday**

Section 3553(h) of title 44, U.S. Code, authorizes the Secretary of Homeland Security, in response to a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to the information security of an agency, to "issue an emergency directive to the head of an agency to take any lawful action with respect to the operation of the information system, including such systems used or operated by another entity on behalf of an agency, that collects, processes, stores, transmits, disseminates, or otherwise maintains agency information, for the purpose of protecting the information system from, or mitigating, an information security threat." Pursuant to 44 U.S.C. § 3553(b)(2), the Secretary delegates this authority to the Director of the Cybersecurity and Infrastructure Security Agency. 6 U.S.C. § 652(c)(5). Federal agencies are required to comply with these directives under 44 U.S.C. § 3554(a)(1)(B)(v). These directives do not apply to statutorily defined "national security systems" nor to systems operated by the Department of Defense or the Intelligence Community. 44 U.S.C. § 3553(d)-(e).

Background

On August 11, 2020, Microsoft released a software update to mitigate a critical vulnerability in Windows Server operating systems (CVE-2020-1350[1]). The vulnerability is in Microsoft Windows Domain Name System (DNS) software when it fails to properly handle requests. An unauthenticated attacker could exploit this vulnerability could allow an attacker to run arbitrary code in the context of the Local System Account. To exploit the vulnerability, an unauthenticated attacker sends malicious requests to a Windows DNS server.

The Cybersecurity and Infrastructure Security Agency (CISA) is unaware of active exploitation of this vulnerability, but assesses that the underlying vulnerabilities can be quickly reverse engineered from a publicly available patch. Aside from removing affected endpoints from the network, there are two known technical mitigations to this vulnerability:

1. a software update, and
2. a registry modification.

CISA has determined that this vulnerability poses unacceptable significant risk to the Federal Civilian Executive Branch and requires an immediate and emergency action. This determination is based on the likelihood of the vulnerability being exploited, the widespread use of the affected software across the

[1] CVE-2020-1350 | Windows DNS Server Remote Code Execution Vulnerability
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1350

24時間以内

CVE-2020-1350
CVSSスコア10：緊急

9月:脆弱性情報

U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Office of the Director
Washington, DC 20528

Emergency Directive 20-04

Original Release Date: September 18, 2020

Applies to: All Federal Executive Branch Departments and Agencies, Except for the Department of Defense, Central Intelligence Agency, and Office of the Director of National Intelligence

FROM: Christopher C. Krebs
Director, Cybersecurity and Infrastructure Security Agency
Department of Homeland Security

CC: Russell T. Vought
Director, Office of Management and Budget

SUBJECT: **Mitigate Netlogon Elevation of Privilege Vulnerability from August 2020 Patch Tuesday**

Section 3553(h) of title 44, U.S. Code, authorizes the Secretary of Homeland Security, in response to a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to the information security of an agency, to "issue an emergency directive to the head of an agency to take any lawful action with respect to the operation of the information system, including such systems used or operated by another entity on behalf of an agency, that collects, processes, stores, transmits, disseminates, or otherwise maintains agency information, for the purpose of protecting the information system from, or mitigating, an information security threat." Pursuant to 44 U.S.C. § 3553(b)(2), the Secretary delegates this authority to the Director of the Cybersecurity and Infrastructure Security Agency. 6 U.S.C. § 652(c)(5). Federal agencies are required to comply with these directives under 44 U.S.C. § 3554(a)(1)(B)(v). These directives do not apply to statutorily defined "national security systems" nor to systems operated by the Department of Defense or the Intelligence Community. 44 U.S.C. § 3553(d)-(e).

Background

On August 11, 2020, Microsoft released a software update to mitigate a critical vulnerability in Windows Server operating systems (CVE-2020-1472[1]). The vulnerability in Microsoft Windows Netlogon Remote Protocol (MS-NRPC), a core authentication component of Active Directory, could allow an unauthenticated attacker with network access to a domain controller to completely compromise all Active Directory identity services.

Applying the update released on August 11 to domain controllers is currently the only mitigation to this vulnerability (aside from removing affected domain controllers from the network).

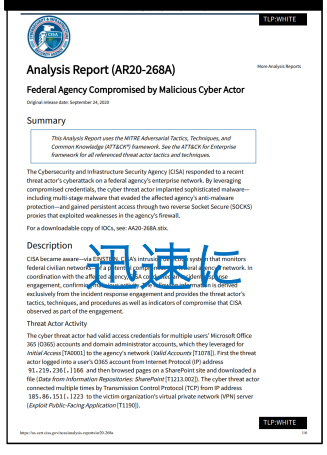
CISA has determined that this vulnerability poses an unacceptable risk to the Federal Civilian Executive Branch and requires an immediate and emergency action. This determination is based on the following:

[1] CVE-2020-1472 | Netlogon Elevation of Privilege Vulnerability
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472

76時間以内

CVE-2020-1472
CVSSスコア10：緊急

9月:CI



TLP:WHITE

Analysis Report (AR20-268A)

More Analysis Reports

Federal Agency Compromised by Malicious Cyber Actor

Original release date: September 24, 2020

Summary

This Analysis Report uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework. See the ATT&CK for Enterprise framework for all referenced threat actor tactics and techniques.

The Cybersecurity and Infrastructure Security Agency (CISA) responded to a recent threat actor's cyberattack on a federal agency's enterprise network. By leveraging compromised credentials, the cyber threat actor implanted sophisticated malware—including multi-stage malware that evaded the affected agency's anti-malware protection—and gained persistent access through two reverse Socket Secure (SOCKS) proxies that exploited weaknesses in the agency's firewall.

For a downloadable copy of IOCs, see: AA20-268A.stix.

Description

CISA became aware—via [illegible], CISA's intrusion detection system that monitors federal civilian networks—of potential [illegible] federal agency network. In coordination with the affected agency, CISA conducted [illegible] response engagement, confirmed [illegible] and collected [illegible] information is derived exclusively from the incident response engagement and provides the threat actor's tactics, techniques, and procedures as well as indicators of compromise that CISA observed as part of the engagement.

Threat Actor Activity

The cyber threat actor had valid access credentials for multiple users' Microsoft Office 365 (O365) accounts and domain administrator accounts, which they leveraged for *Initial Access* [TA0001] to the agency's network (*Valid Accounts* [T1078]). First the threat actor logged into a user's O365 account from Internet Protocol (IP) address 91.219.236.[.]166 and then browsed pages on a SharePoint site and downloaded a file (*Data from Information Repositories: SharePoint* [T1213.002]). The cyber threat actor connected multiple times by Transmission Control Protocol (TCP) from IP address 185.86.151.[.]223 to the victim organization's virtual private network (VPN) server (*Exploit Public-Facing Application* [T1190]).

TLP:WHITE

https://us-cert.cisa.gov/ncas/analysis-reports/ar20-268a

1/6

迅速に

?

CVE-2018-8453等
CVSSスコア10：緊急

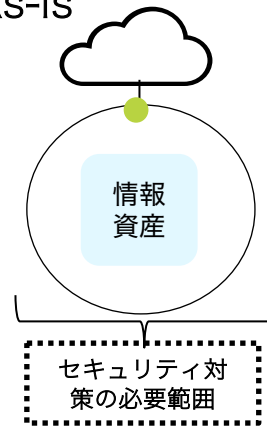
当該情報の全数端末 & 全数拠点の存在可否と対処完了の要求
増加する「平時」における安全宣言、説明責任の対応

まとめ：ゼロトラスト時代に必要となるエンドポイント管理

リモートワークが進む今日こそ、有事の対策(EDR)の前に平時の対策を強化するべき

いつの時代も「守るべき情報資産」にアクセスするのは常に「エンドポイント」である

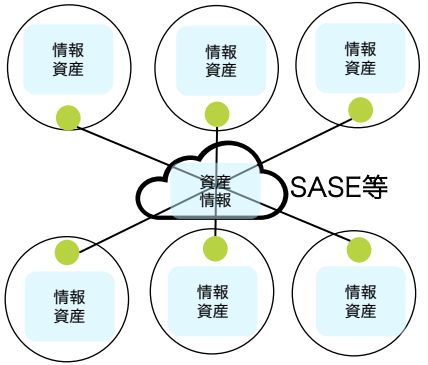
- As-Is



- 主な環境の変化
  - 「マルチ・デバイス」化
  - 「マルチ・アクセス」化
  - ⇒ 境界型セキュリティの限界
- リスク要因の変化
  - 情報資産やIT資産の点在化
  - 把握し切れない膨大な脆弱性の点在化

対策範囲の急拡大

- To-Be



ゼロトラスト共存環境

To-Beで求められるエンドポイントの要件

① ゼロトラスト環境＝「信頼出来ない環境」であり、いかにして「信頼出来る」環境を構築し、管理が出来るか？
② 信頼出来る環境とは、「全デバイスの可視化と制御」を「リアルタイム且つ網羅的」に実現出来る環境
③ NIST SP800-207では②の「サイバー衛生管理」なくして「ZTA*は実現しない」と明記

*ZTA: Zero Trust Architecture

見えないものは守れない

EDRの導入の前にサイバー衛生管理の徹底を！