

Mac vs Windows

攻撃と防衛から見たセキュリティの実態

阿部 慎司

2025/8/8

自己紹介

阿部 慎司 (ABE Shinji)

- **GMOサイバーセキュリティ byイエラエ株式会社**
 - サイバーセキュリティ事業本部 執行役員 副本部長
 - ディフェンシブセキュリティ部 部長
- 日本セキュリティオペレーション事業者協議会 (ISOG-J)
 - 副代表
 - セキュリティオペレーション認知向上・普及啓発WG (WG4) リーダー
- 日本SOCアナリスト情報共有会 (SOCYETI)
 - 主宰
- X.1060 および JT-X1060
 - メインエディター
- IPA専門委員
- CISSP



Macのセキュリティを2つの観点で



「WindowsよりMacの方が安全そう」

と、なんとなく思っていることを証明する試み

(企業のセキュリティとして)

Macのセキュリティを2つの観点で

これらをなるべく定量的に可視化してみる



Macのセキュリティを2つの観点で

これらをなるべく定量的に可視化してみる

攻撃手法の多さ
&
実際の攻撃発生状況

守る対象の多さ
&
実際の守備状況

どのような指標で可視化するか？



① 攻撃手法の多さ

➔ MITRE "ATT&CK"

② 実際の攻撃発生状況

➔ CISA "KEV"



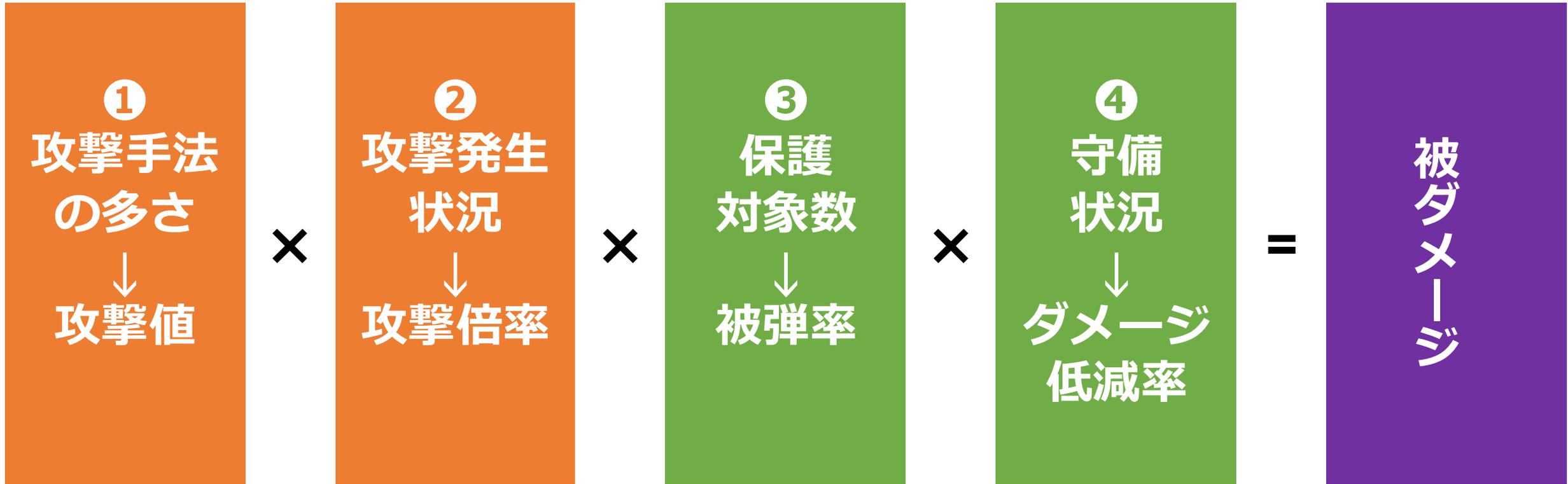
③ 守る対象の多さ

➔ 保護対象数

④ 実際の守備状況

➔ OS最新化率

今回の数値化モデル（ゲームっぽく）



 被ダメージが少ない方が勝ち 

① 攻撃手法の多さ = MITRE ATT&CK®



The screenshot shows the MITRE ATT&CK website. At the top, there is a red navigation bar with the MITRE logo and a hamburger menu icon. Below the navigation bar, a grey banner announces "ATT&CKcon 6.0 is coming October 14-15 in McLean, VA and live online. Tickets are available now!". The main content area features the "ATT&CK" logo in large red letters. To the left of the logo is a navigation menu with links for "Get Started", "Take a Tour", "Contribute", "Blog", "FAQ", and "Random Page". To the right of the logo is a text block describing the ATT&CK knowledge base as a globally-accessible resource for adversary tactics and techniques, used for developing threat models and methodologies. It also mentions that MITRE is fulfilling its mission to solve cybersecurity problems by bringing communities together.

米国MITRE社がとりまとめている、
サイバー攻撃の大枠の流れ（Tactics）や
具体的な手法（Techniques）を分類し、
手口の理解や対策の検討を推進するための
フレームワーク。

<https://attack.mitre.org/>

1 攻撃手法の多さ = MITRE ATT&CK®

Windows Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Windows platform. The techniques below are known to target hosts running Microsoft Windows operating systems. The Matrix contains information for the Windows platform.

[View on the ATT&CK® Navigator](#)

[Version Permalink](#)

layout: side ▾ show sub-techniques hide sub-techniques help

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	10 techniques	19 techniques	14 techniques	35 techniques	16 techniques	27 techniques	9 techniques	15 techniques	18 techniques	8 techniques	14 techniques
Content Injection	Command and Scripting Interpreter (7)	Account Manipulation (3)	Abuse Elevation Control Mechanism (1)	Abuse Elevation Control Mechanism (1)	Adversary-in-the-Middle (3)	Account Discovery (3)	Exploitation of Remote Services	Application Layer Control	Automated Exfiltration	Account Access Removal	
Drive-by Compromise	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Destruction	
Exploit Public-Facing Application	Inter-Process Communication (2)	Boot or Logon Autostart Execution (10)	Account Manipulation (3)	Debugger Evasion	Credentials from Password Stores (3)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Data Encrypted for Impact	
External Remote Services	Native API	Boot or Logon Autostart Execution (10)	Boot or Logon Initialization Scripts (2)	Deobfuscate/Decode Files or Information	Debugger Evasion	Device Driver Discovery	Remote Service Session Hijacking (1)	Automated Collection	Data Encoding (2)	Data Manipulation (3)	
Hardware Additions	Scheduled Task/Job (2)	Browser Extensions	Boot or Logon Initialization Scripts (2)	Direct Volume Access	Exploitation for Credential Access	Domain Trust Discovery	Remote Service Session Hijacking (1)	Browser Session Hijacking (1)	Data Encoding (2)	Defacement (2)	
Phishing (4)	Shared Modules	Compromise Host Software Binary	Boot or Logon Initialization Scripts (2)	Execution Guardrails (2)	Forceful Authentication	File and Directory Discovery	Remote Services (3)	Clipboard Data	Data Obfuscation (3)	Disk Wipe (2)	
Replication Through Removable Media	Software Deployment Tools	Create Account (2)	Create or Modify System Policy (1)	Exploitation for Defense Evasion	Forge Web Credentials (2)	Group Policy Discovery	Replication Through Removable Media	Data from Information Repositories (1)	Dynamic Resolution (3)	Endpoint Denial of Service (2)	
Supply Chain Compromise (3)	User Execution (2)	Event Triggered Execution (12)	Event Triggered Execution (12)	Hide Artifacts (11)	Input Capture (4)	Network Service Discovery	Software Deployment Tools	Data from Local System	Encrypted Channel (2)	Financial Theft	
Trusted Relationship	Windows Management Instrumentation	External Remote Services	Hijack Execution Flow (11)	Hijack Execution Flow (11)	Multi-Factor Authentication Interception	Network Sniffing	Data from Network Shared Drive	Data from Network Shared Drive	Fallback Channels	Firmware Corruption	
Valid Accounts (3)											

macOS Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® macOS platform. The techniques below are known to target hosts running macOS operating systems. The Matrix contains information for the macOS platform.

[View on the ATT&CK® Navigator](#)

[Version Permalink](#)

layout: side ▾ show sub-techniques hide sub-techniques help

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
9 techniques	9 techniques	12 techniques	11 techniques	24 techniques	15 techniques	24 techniques	7 techniques	14 techniques	18 techniques	8 techniques	14 techniques
Content Injection	Command and Scripting Interpreter (6)	Account Manipulation (2)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (2)	Account Discovery (2)	Exploitation of Remote Services	Application Layer Protocol (5)	Automated Exfiltration	Account Removal	
Drive-by Compromise	Exploitation for Client Execution	Boot or Logon Autostart Execution (2)	Debugger Evasion	Debugger Evasion	Archive Collected Data (3)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Destruction	
Exploit Public-Facing Application	Inter-Process Communication (1)	Boot or Logon Autostart Execution (2)	Deobfuscate/Decode Files or Information	Deobfuscate/Decode Files or Information	Credentials from Password Stores (4)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Data Encrypted for Impact	
External Remote Services	Native API	Boot or Logon Autostart Execution (2)	Exploitation for Credential Access	Exploitation for Defense Evasion	Debugger Evasion	Device Driver Discovery	Remote Service Session Hijacking (1)	Automated Collection	Data Encoding (2)	Data Manipulation (3)	
Hardware Additions	Scheduled Task/Job (2)	Browser Extensions	File and Directory Permissions Modification (1)	File and Directory Permissions Modification (1)	Device Driver Discovery	Domain Trust Discovery	Remote Service Session Hijacking (1)	Clipboard Data	Data Encoding (2)	Defacement (2)	
Phishing (4)	Shared Modules	Compromise Host Software Binary	Input Capture (2)	Input Capture (2)	File Enumeration	Log Enumeration	Replication Through Removable Media	Data from Information Repositories (1)	Data Obfuscation (3)	Disk Wipe (2)	
Supply Chain Compromise (3)	Software Deployment Tools	Create Account (2)	Network Service Discovery	Network Service Discovery	Log Enumeration	Network Service Discovery	Software Deployment Tools	Data from Local System	Dynamic Resolution (3)	Endpoint Denial of Service (4)	
Trusted Relationship	System Services (1)	Event Triggered Execution (3)	Network Sniffing	Network Sniffing	Multi-Factor Authentication Process (2)	Network Sniffing	Data from Network Shared Drive	Data from Local System	Encrypted Channel (2)	Financial Theft	
Valid Accounts (3)											



① 攻撃値 = MITRE ATT&CK®

	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Win	11	11	21	14	36	16	28	9	15	18	8	15
Mac	10	10	18	11	25	15	25	7	14	18	8	15

MatrixにおけるTechniqueの数 :



202



176

ダメージ計算

①

攻撃値

MITRE ATT&CK



×

②

攻撃倍率



×

③

被弾率



×

④

ダメ低減



=

被ダメ



×



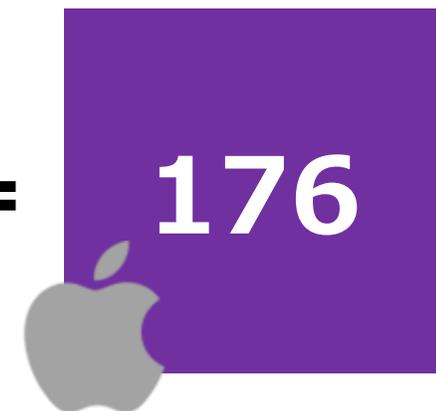
×



×



=



② 攻撃倍率 = CISA KEV

The screenshot shows the homepage of the CISA Known Exploited Vulnerabilities Catalog. The header includes the CISA logo and the text "America's Cyber Defense Agency" and "NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE". A search bar is located in the top right. The main navigation bar contains links for Topics, Spotlight, Resources & Tools, News & Events, Careers, and About. The breadcrumb trail shows "Home / Known Exploited Vulnerabilities Catalog". There are social media share buttons for Facebook, X, LinkedIn, and Email. The page title is "Known Exploited Vulnerabilities Catalog". The main content area features a heading "Known Exploited Vulnerabilities Catalog" and a sub-heading "Known Exploited Vulnerabilities Catalog". Below the heading is a paragraph: "For the benefit of the cybersecurity community and network defenders—and to help every organization better manage vulnerabilities and keep pace with threat activity—CISA maintains the authoritative source of vulnerabilities that have been exploited in the wild. Organizations should use the KEV catalog as an input to their vulnerability management prioritization framework." There is a button labeled "HOW TO USE THE KEV CATALOG" with a right arrow.

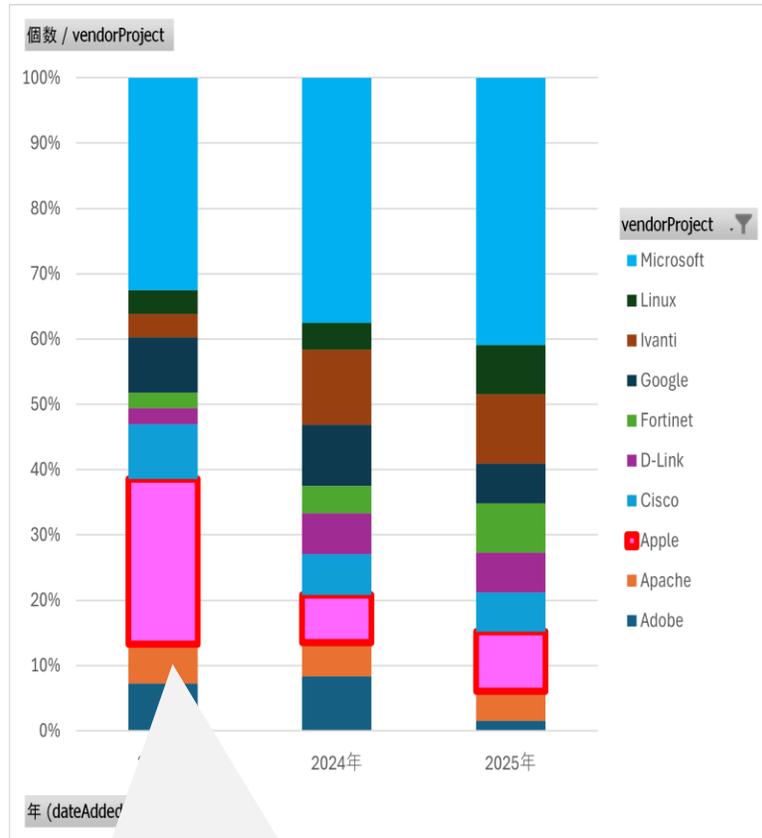
米国サイバーセキュリティ・インフラセキュリティ庁（CISA）によってまとめられた、実際に悪用が確認された脆弱性のカタログ。

<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

② 攻撃倍率 = CISA KEV

CISA KEVにおけるOS別割合 Known Exploited Vulnerabilities Catalog - OS Top10

2025年の割合：



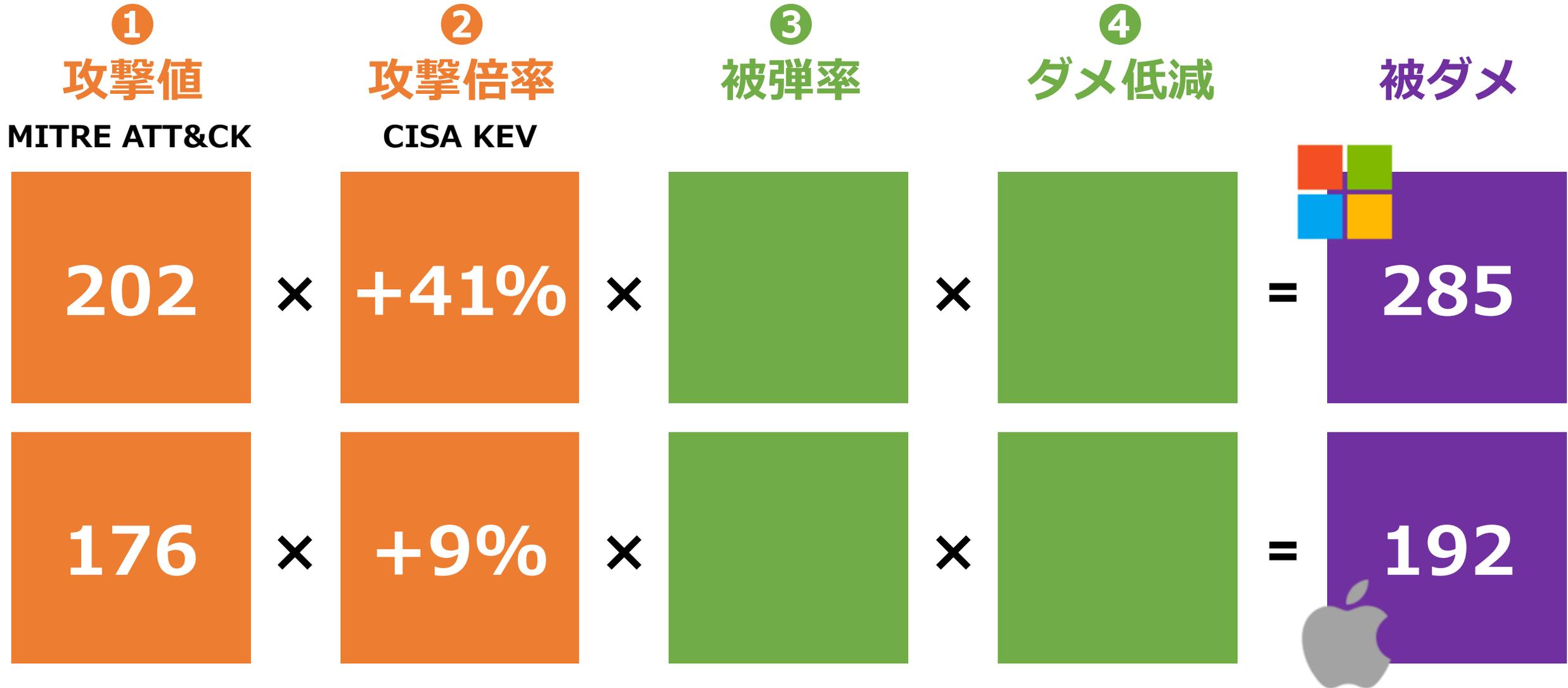
41%



9%

モバイル狙いが多かった（Webkitの脆弱性含む）

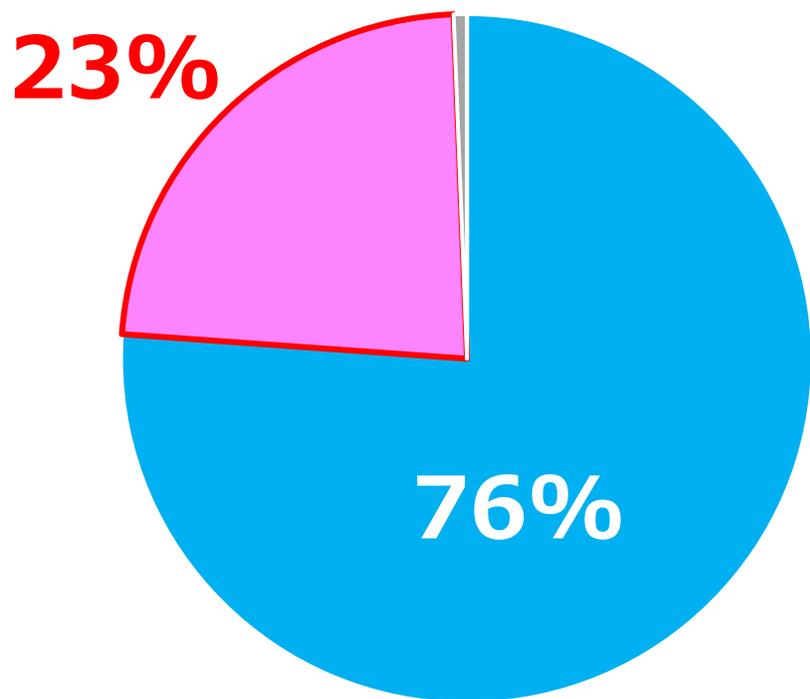
ダメージ計算



③ 被弾率 = 社内の端末割合

弊社SOCにおけるEDR監視OS別割合

弊社の顧客特性もありますので、ご参考まで



■ Windows ■ Mac ■ Others

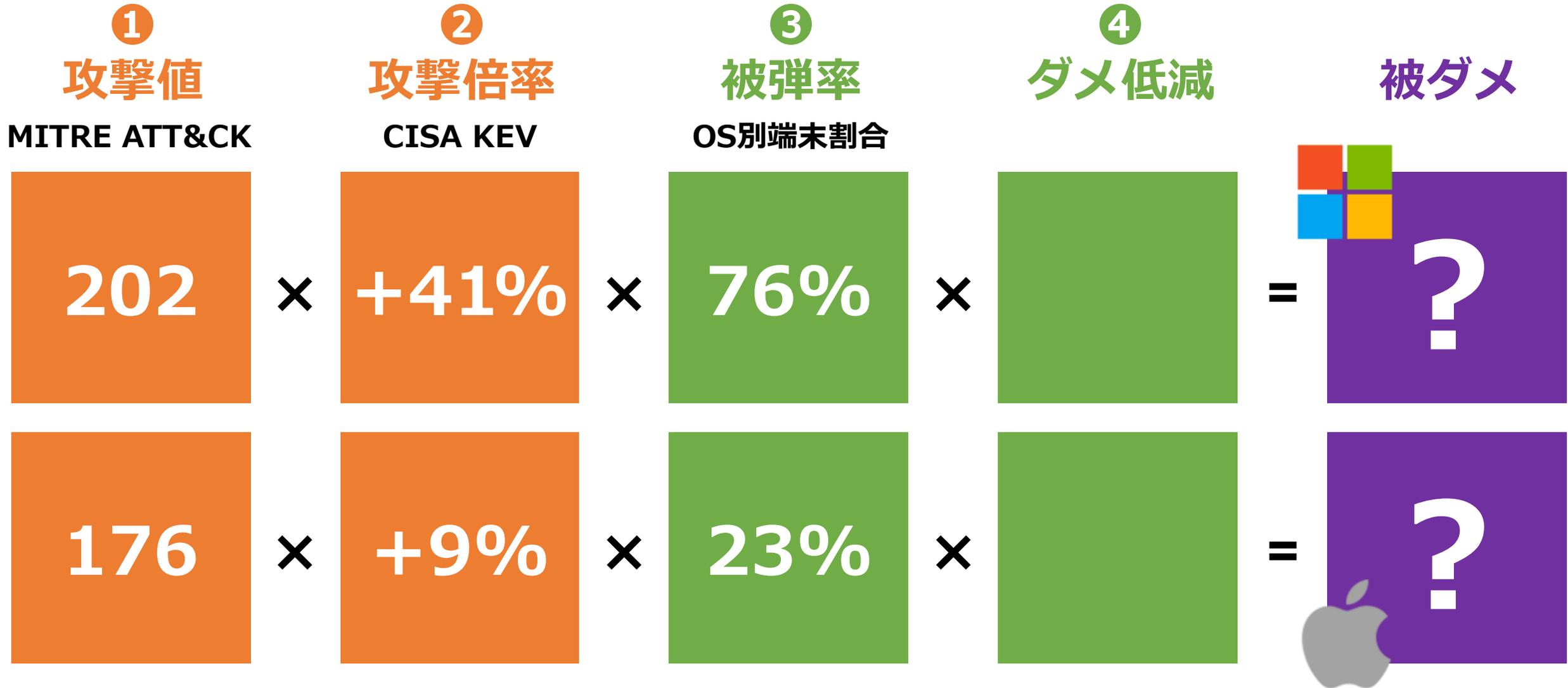


76%



23%

ダメージ計算



④ ダメージ低減 = バージョンアップ率

企業におけるOSバージョンアップ状況

Windows vs Mac

* 弊社の顧客特性もありますので、ご参考まで
 * 0%は0.5%未満の確率で存在しているというデータです
 * 赤字はサポート切れ扱い（ESU等は加味せず）

Windows			
10		11	
Version	割合	Version	割合
19045	53%	26100	32%
19044	1%	22631	11%
18362	0%	22621	1%
17134	0%	22000	0%

Mac									
Catalina (10.15)		Monterey (12)		Ventura (13)		Sonoma (14)		Sequoia (15)	
Version	割合	Version	割合	Version	割合	Version	割合	Version	割合
19H2026	0%	21H1320	1%	22H313	1%	23H527	1%	24E248	27%
		21G115	0%	22G830	1%	23H420	5%	24D81	21%
		21F79	0%	22G630	0%	23H311	1%	24D70	15%
		21D62	0%	22G513	1%	23H222	1%	24D60	1%
		21C52	0%	22G436	1%	23H124	1%	24D2082	0%
				22F77082 0d	0%	23G93	5%	24C101	4%
				22F66	0%	23F79	2%	24B91	4%
				22E77261 0a	0%	23E224	0%	24B83	1%
				22E261	0%	23E214	1%	24B2091	0%
				22D68	0%	23D56	1%	24B2083	2%
						23B81	1%	24A348	0%
								24A335	0%

◆ポイント：

- サポート切れバージョンの利用率は同等（2%）
- 最新OSの利用率はMacの方が高い（75%:45%）
- 最新OSでのVerUP率はWinの方が高い（70%:35%）

④ ダメージ低減 = バージョンアップ率

企業におけるOSバージョンアップ状況

Windows vs Mac

- * 弊社の顧客特性もありますので、ご参考まで
- * 0%は0.5%未満の確率で存在しているというデータです
- * 赤字はサポート切れ扱い（ESU等は加味せず）

Windows			
10		11	
Version	割合	Version	割合
19045	53%	26100	32%
19044	1%	22631	11%
18362	0%	22621	1%
17134	0%	22000	0%

Mac									
Catalina (10.15)		Monterey (12)		Ventura (13)		Sonoma (14)		Sequoia (15)	
Version	割合	Version	割合	Version	割合	Version	割合	Version	割合
19H2026	0%	21H1320	1%	22H313	1%	23H527	1%	24E248	27%
		21G115	0%	22G830	1%	23H420	5%	24D81	21%
		21F79	0%	22G630	0%	23H311	1%	24D70	15%
		21D62	0%	22G513	1%	23H222	1%	24D60	1%
		21C52	0%	22G436	1%	23H124	1%	24D2082	0%
				22F77082 0d	0%	23G93	5%	24C101	4%
				22F66	0%	23F79	2%	24B91	4%
				22E77261 0a	0%	23E224	0%	24B83	1%
				22E261	0%	23E214	1%	24B2091	0%
				22D68	0%	23D56	1%	24B2083	2%
						23B81	1%	24A348	0%
								24A335	0%

最新OSでのVerUP率



70%



35%

← 最新OSの中で最新Verにしている割合を計算したものなので表中の数字とはズレてます

ダメージ計算

①

攻撃値

MITRE ATT&CK

202

×

②

攻撃倍率

CISA KEV

+41%

×

③

被弾率

OS別端末割合

76%

×

④

ダメ低減

VerUP割合

-70%
(30%)

=

被ダメ

?

176

×

+9%

×

23%

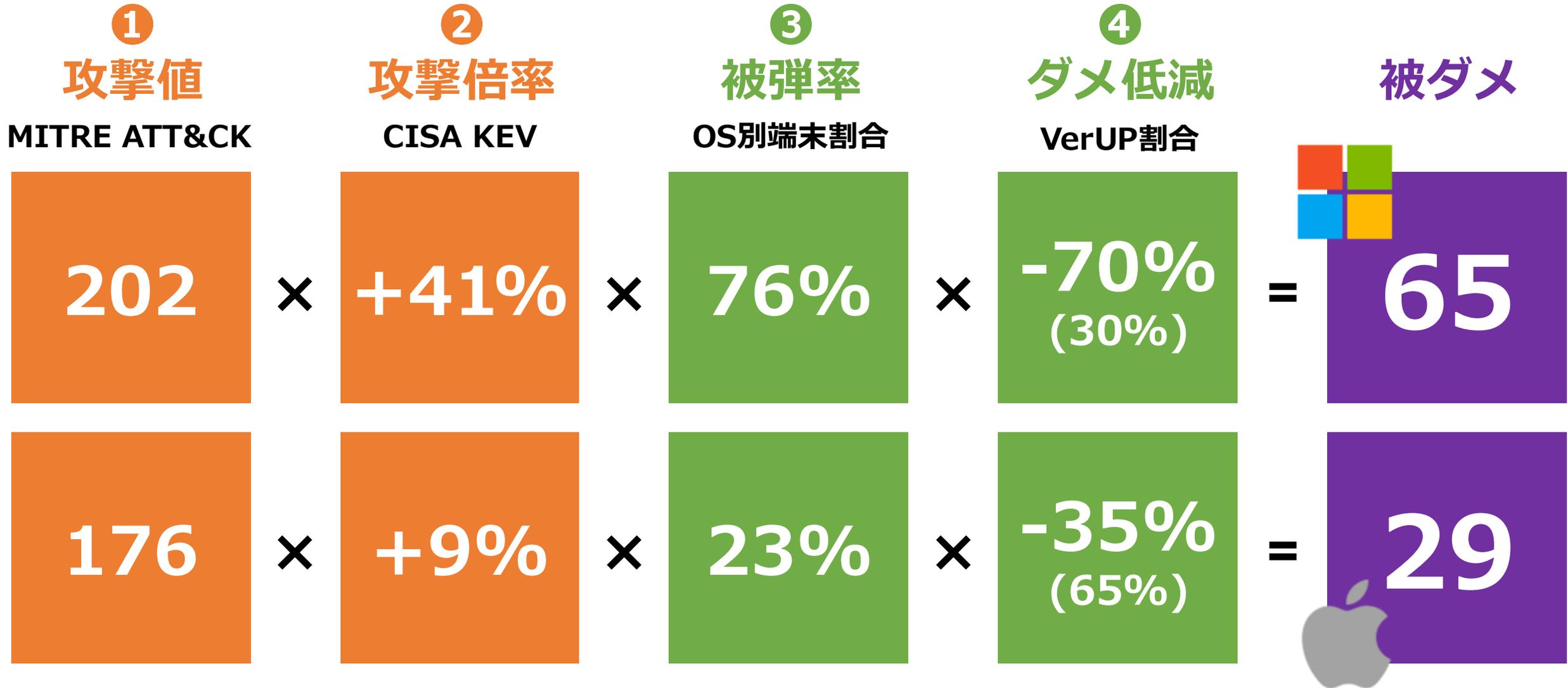
×

-35%
(65%)

=

?

ダメージ計算



なんとなくみんなが思っている

「WindowsよりMacの方が安全じゃね？」

は、一応正しかった！

振り返りをしてきましょう

①

攻撃値

MITRE ATT&CK



×

②

攻撃倍率

CISA KEV



×

③

被弾率

OS別端末割合



×

④

ダメ低減

VerUP割合



=

被ダメ



×



×



×



=



振り返り①

①

攻撃値

MITRE ATT&CK

202

176

②

攻撃倍率

CISA KEV

285
(+41%)

192
(+9%)

③

被弾率

OS別端末割合

216
(67%)

44
(23%)

④

ダメ低減

VerUP割合

-70%
(37%)

-35%
(65%)

被ダメ



攻撃者から見てMacが
著しく攻撃しにくいということはない

振り返り②

①

攻撃値

MITRE ATT&CK



×

②

攻撃倍率

CISA KEV



×

③

被弾率

OS別端末割合



×

④

ダメ低減

VerUP割合



被ダメ



比較すればMacはWinより狙われにくいとも言えなくはないが、危険な攻撃が

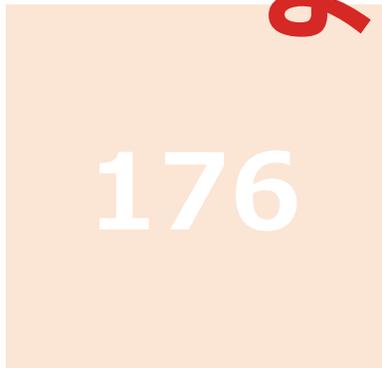
In-the-wildであることには変わらない

振り返り③

①

攻撃値

MITRE ATT&CK



②

攻撃倍率

CISA KEV



③

被弾率

OS別端末割合



④

ダメ低減

VerUP割合



被ダメ



台数の割合によつては

リスクは逆転しうる

振り返り④

①

攻撃値

MITRE ATT&CK



②

攻撃倍率

CISA KEV



③

被弾率

OS別端末割合



④

ダメ低減

VerUP割合



被ダメ



バージョンアップの有無が
戦況をひっくり返してしまう

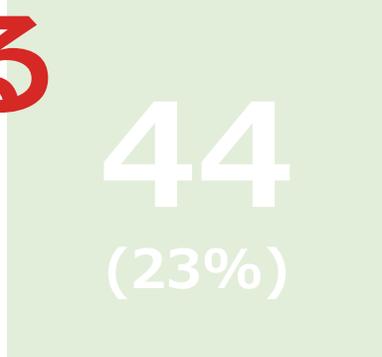
可能性がある



×



×



×



=



④ ダメージ低減 = バージョンアップ率

企業におけるOSバージョンアップ状況

Windows vs Mac

* 弊社の顧客特性もありますので、ご参考まで
 * 0%は0.5%未満の確率で存在しているというデータです
 * 赤字はサポート切れ扱い（ESU等は加味せず）

Windows			
10		11	
Version	割合	Version	割合
19045	53%	26100	32%
19044	1%	22631	11%
18362	0%	22621	1%
17134	0%	22000	0%

Mac									
Catalina (10.15)		Monterey (12)		Ventura (13)		Sonoma (14)		Sequoia (15)	
Version	割合	Version	割合	Version	割合	Version	割合	Version	割合
19H2026	0%	21H1320	1%	22H313	1%	23H527	1%	24E248	27%
		21G115	0%	22G830	1%	23H420	5%	24D81	21%
		21F79	0%	22G630	0%	23H311	1%	24D70	15%
		21D62	0%	22G513	1%	23H222	1%	24D60	1%
		21C52	0%	22G436	1%	23H124	1%	24D2082	0%
				22F77082 0d	0%	23G93	5%	24C101	4%
				22F66	0%	23F79	2%	24B91	4%
				22E77261 0a	0%	23E224	0%	24B83	1%
				22E261	0%	23E214	1%	24B2091	0%
				22D68	0%	23D56	1%	24B2083	2%
						23B81	1%	24A348	0%
								24A335	0%

◆ポイント：

- サポート切れバージョンの利用率は同等（2%）
- 最新OSの利用率はMacの方が高い（75%:45%）
- 最新OSでのVerUP率はWinの方が高い（70%:35%）

④ ダメージ低減 = バージョンアップ率

企業におけるOSバージョンアップ状況 Windows vs Mac

Windows			
10		11	
Version	割合	Version	割合
19045	53%	26100	32%
19044	1%	22631	11%
18362	0%	22621	1%
17134	0%	22000	0%

Mac	
Version	割合
Catalina	45%
Version 19H20	75%

Windowsの方がきちんとVerUP管理されている
(**Mac**は最新OSに上げた後は“油断”がある…?)

◆ポイント：

- サポート切れバージョンの利用率は同等（2%）
- 最新OSの利用率はMacの方が高い（75%:45%）
- 最新OSでのVerUP率はWinの方が高い（70%:35%）

22F770820d	0%	23G93	5%	24C101	4%
22F66	0%	23F79	2%	24B91	4%
22E772610a	0%	23E224	0%	24B83	1%
22E261	0%	23E214	1%	24B2091	0%
22D68	0%	23D56	1%	24B2083	2%
		23B81	1%	24A348	0%
				24A335	0%

④ ダメージ低減 = バージョンアップ率

企業におけるOSバージョンアップ状況 Windows vs Mac

Windows			
10		11	
Version	割合	Version	割合
19045	53%	26100	32%
19044	1%	22631	11%
18362	0%	22621	1%
17134	0%	22000	0%

Catalina	
Version	割合
19H20	45%

Windowsの方がきちんとVerUP管理されている
(**Mac**は最新OSに上げた後は"油断"がある...?)

Macのデバイス管理を徹底する必要がある

◆ポイント：

- サポート切れバージョンの利用率は同等 (2%)
- 最新OSの利用率はMacの方が高い (75%:45%)
- 最新OSでのVerUP率はWinの方が高い (70%:35%)

22F66	0%	23F79	2%	24B91	4%
22E772610a	0%	23E224	0%	24B83	1%
22E261	0%	23E214	1%	24B2091	0%
22D68	0%	23D56	1%	24B2083	2%
		23B81	1%	24A348	0%
				24A335	0%



企業におけるapple製品のデバイス管理の重要性を訴えることでJamfにゴマをする人

何か助けられることがあればぜひ

GMOサイバーセキュリティ

SOC

24時間365日監視のサイバー攻撃防御・分析サービス

GMOサイバーセキュリティ byイエアエのSOC (Security Operation Center) は、「見直す・見守る・身を守る・みんなで守る」の4つの観点で、お客様と共にセキュリティ運用上の課題解決に取り組む伴走型セキュリティ運用サービスです。

[SOC\(Security Operation Center\)とは？概要や必要性を解説](#)

SOCサービスはこんなお悩みを持つ企業におすすめです

情報システム部門・CSIRTの担当者様



ログの取得やアラートへの対応に懸念がある



高度な攻撃への対策をしたい



運用体制を整えたい
セキュリティ人材を育成したい

AWS WAF運用ならおまかせ

GMOサイバーセキュリティ

WAFエイド

世界トップレベルのホワイトハッカーの知見を活かしたツールでWAFの運用/保守を24時間365日自動で行います



資料ダウンロード

お問い合わせ

※1 当社調べ ※2 HTB Business CTF 2024:国内1位 ※3 2023年 DEF CON 31 Cloud Village CTF:世界1位、2024年 DEF CON 32 Cloud Village CTF :世界1位

▼ 特長

▼ 機能

▼ 料金

▼ よくある質問

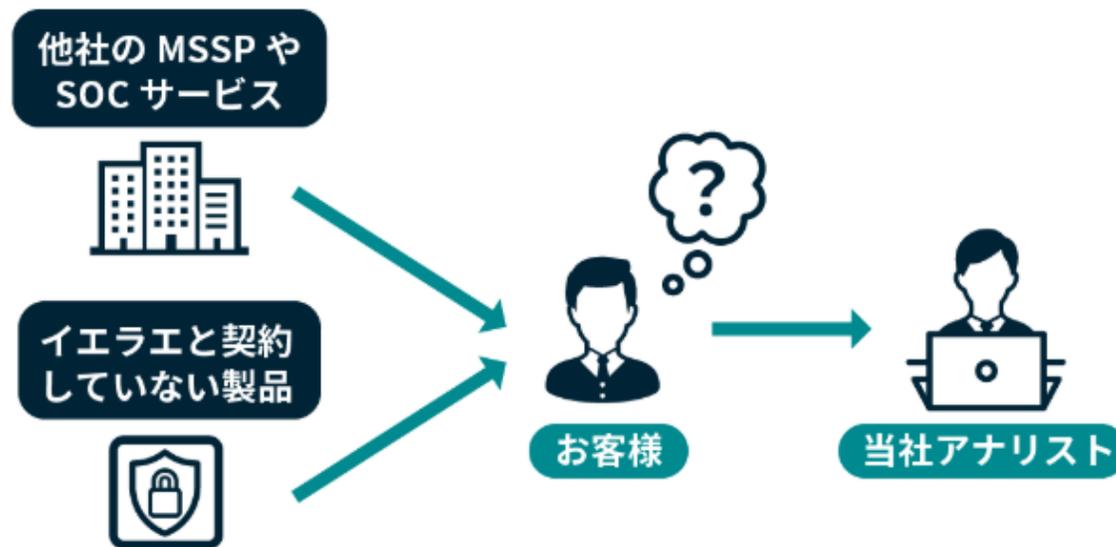
対応製品



セカンドオピニオン

弊社サービス以外にお客様が契約しているセキュリティ製品、SIEM、SOC等が発報したログやアラート、レポートなどの内容についてお問い合わせいただけます。

本メニューのみのご契約も可能で、お客様と共に他のセキュリティ製品やサービスに関するログも横断的に確認しながら専門のセキュリティアナリストがアドバイスをを行います。



ご清聴ありがとうございました