GMO CYBER SECURITY IERAE

Mac vs Windows
攻撃と防御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）

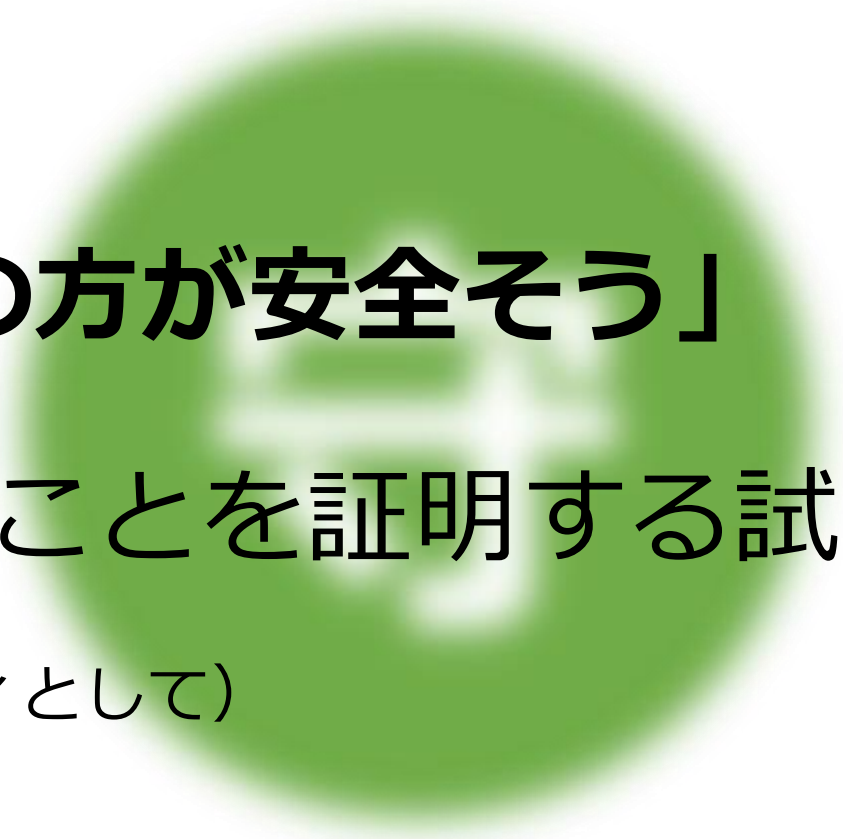
- **GMOサイバーセキュリティ byイエラエ株式会社**
  - **サイバーセキュリティ事業本部　執行役員　副本部長**
  - **ディフェンシブセキュリティ部　部長**
- 日本セキュリティオペレーション事業者協議会（ISOG-J）
  - 副代表
  - セキュリティオペレーション認知向上・普及啓発WG（WG4）リーダー
- 日本SOCアナリスト情報共有会（SOCYETI）
  - 主宰
- X.1060 および JT-X1060
  - メインエディター
- IPA専門委員
- CISSP

Macのセキュリティを2つの観点で

GMO CYBER SECURITY IERAE

Macのセキュリティを2つの観点で

GMO CYBER SECURITY IERAE



「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

GMO CYBER SECURITY IERAE

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

GMO CYBER SECURITY IERAE

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）

GMO CYBER SECURITY IERAE

❶ 攻撃手法の多さ → 攻撃値

×

❷ 攻撃発生状況 → 攻撃倍率

×

❸ 保護対象数 → 被弾率

×

❹ 守備状況 → ダメージ低減率

=

被ダメージ

被ダメージが少ない方が勝ち

❶ 攻撃手法の多さ＝MITRE ATT&CK®

https://attack.mitre.org/

米国MITRE社がとりまとめてる、
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。

❶ 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

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

❶ 攻撃値＝MITRE ATT&CK®

GMO CYBER SECURITY IERAE

	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

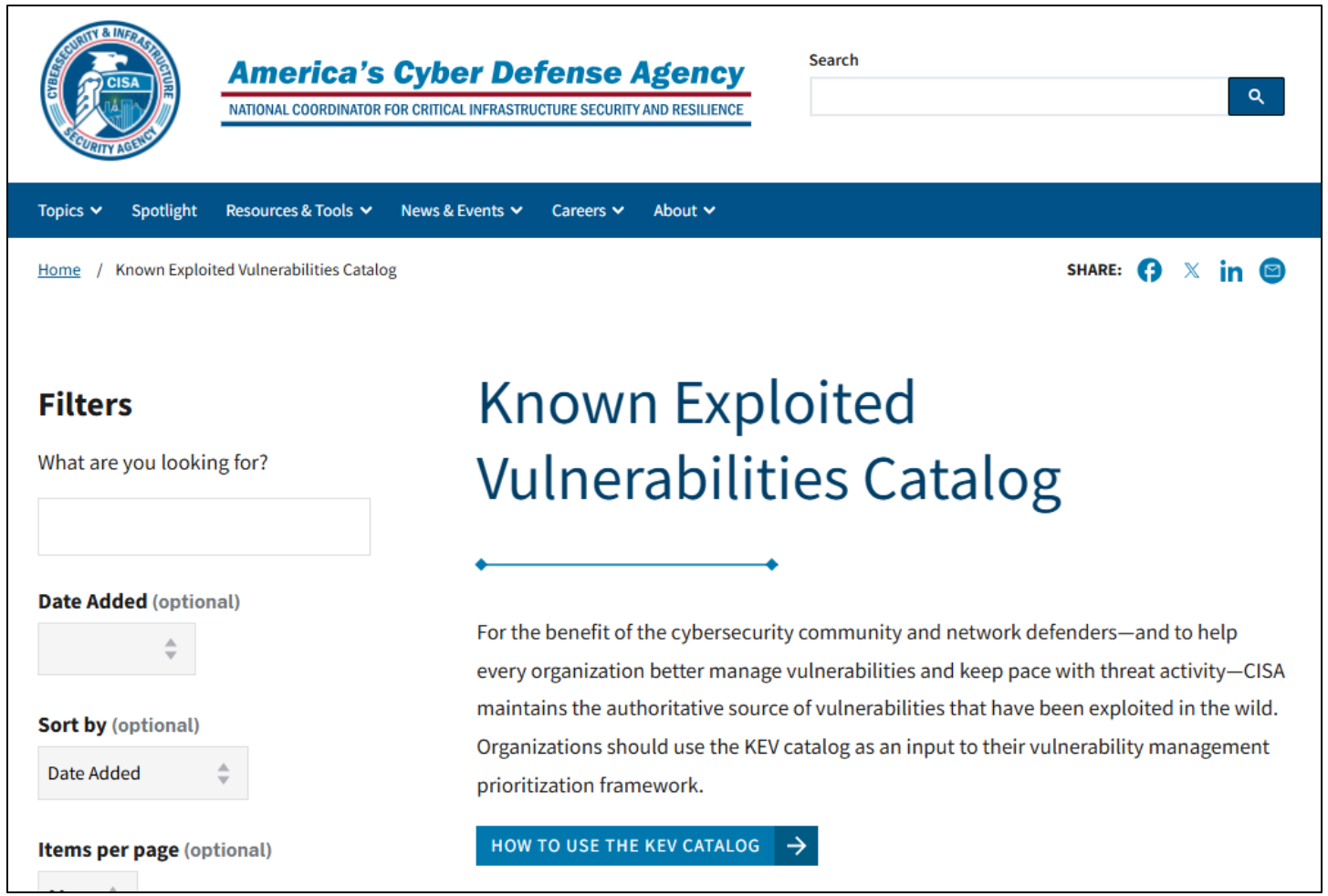
176

ダメージ計算

GMO CYBER SECURITY IERAE

❶ 攻撃値		❷ 攻撃倍率		❸ 被弾率		❹ ダメ低減		被ダメ
MITRE ATT&CK								
202	×		×		×		=	202
176	×		×		×		=	176

❷ 攻撃倍率＝CISA KEV



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

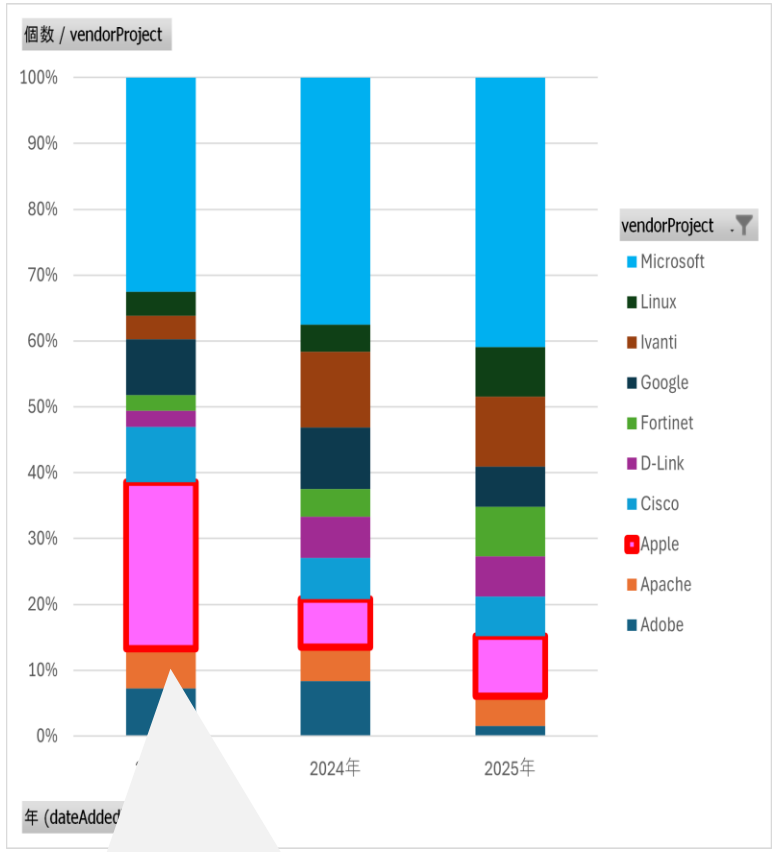
米国サイバーセキュリティ・インフラセキュリティ庁（CISA）によってまとめられた、実際に悪用が確認された脆弱性のカタログ。

❷ 攻撃倍率＝CISA KEV

GMO CYBER SECURITY IERAE

CISA KEVにおけるOS別割合

Known Exploited Vulnerabilities Catalog – OS Top10



モバイル狙いが多かった（Webkitの脆弱性含む）

2025年の割合：

41%

9%

ダメージ計算

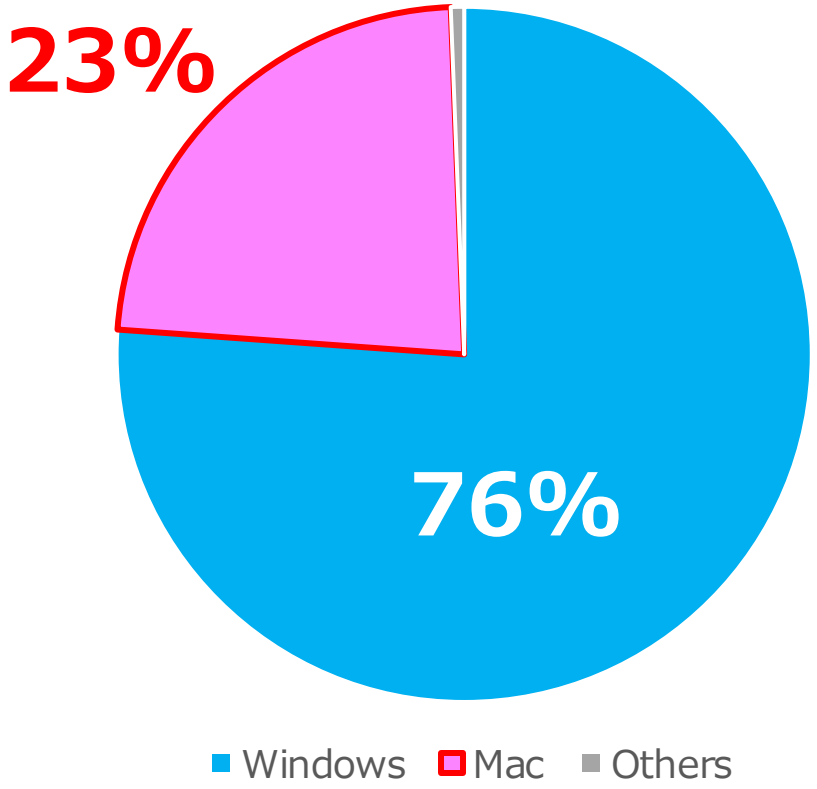
GMO CYBER SECURITY IERAE

❶ 攻撃値		❷ 攻撃倍率		❸ 被弾率		❹ ダメ低減		被ダメ
MITRE ATT&CK		CISA KEV						
202	×	+41%	×		×		=	285
176	×	+9%	×		×		=	192

❸ 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



76%

23%

ダメージ計算

GMO CYBER SECURITY IERAE

❶ 攻撃値		❷ 攻撃倍率		❸ 被弾率		❹ ダメ低減		被ダメ
MITRE ATT&CK		CISA KEV		OS別端末割合				
202	×	+41%	×	76%	×		=	?
176	×	+9%	×	23%	×		=	?

❹ ダメージ低減＝バージョンアップ率

GMO CYBER SECURITY IERAE

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%
				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%

◆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%）**

❹ ダメージ低減＝バージョンアップ率

GMO CYBER SECURITY IERAE

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%
				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%

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

GMO CYBER SECURITY IERAE

❶ 攻撃値		❷ 攻撃倍率		❸ 被弾率		❹ ダメ低減		被ダメ
MITRE ATT&CK		CISA KEV		OS別端末割合		VerUP割合		
202	×	+41%	×	76%	×	-70% (30%)	=	?
176	×	+9%	×	23%	×	-35% (65%)	=	?

ダメージ計算

GMO CYBER SECURITY IERAE

❶ 攻撃値		❷ 攻撃倍率		❸ 被弾率		❹ ダメ低減		被ダメ
MITRE ATT&CK		CISA KEV		OS別端末割合		VerUP割合		
202	×	+41%	×	76%	×	-70% (30%)	=	65
176	×	+9%	×	23%	×	-35% (65%)	=	29

結論

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

GMO CYBER SECURITY IERAE

❶ 攻撃値		❷ 攻撃倍率		❸ 被弾率		❹ ダメ低減		被ダメ
MITRE ATT&CK		CISA KEV		OS別端末割合		VerUP割合		
202	×	285 (+41%)	×	216 (76%)	×	-70% (30%)	=	65
176	×	192 (+9%)	×	44 (23%)	×	-35% (65%)	=	29

振り返り①

GMO CYBER SECURITY IERAE

❶ 攻撃値		❷ 攻撃倍率		❸ 被弾率		❹ ダメ低減		被ダメ
MITRE ATT&CK		CISA KEV		OS別端末割合		VerUP割合		
202	×	285 (+41%)	×	216 (69%)	×	-70% (30%)	=	65
176	×	192 (+9%)	×	44 (23%)	×	-35% (65%)	=	29

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

GMO CYBER SECURITY IERAE

① 攻撃値		② 攻撃倍率		③ 被弾率		④ ダメ低減		被ダメ
MITRE ATT&CK		CISA KEV		OS別端末割合		VerUP割合		
202	×	285 (+41%)	×	216 (76%)	×	70% (30%)	=	65
176	×	192 (+9%)	×	44 (23%)	×	35% (65%)	=	29

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りない

振り返り③

GMO CYBER SECURITY IERAE

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
202	×	285 (+41%)	×	216 (76%)	×	-70% (30%)	=	65
176	×	192 (+9%)	×	44 (23%)	×	-35% (65%)	=	29

台数の割合によっては

リスクは逆転しうる

振り返り④

GMO CYBER SECURITY IERAE

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
202	×	285 (+41%)	×	216 (76%)	×	-70% (30%)	=	65
176	×	192 (+9%)	×	44 (23%)	×	-35% (65%)	=	29

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

❹ ダメージ低減＝バージョンアップ率

GMO CYBER SECURITY IERAE

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%
				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%

◆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%）**

❹ ダメージ低減＝バージョンアップ率

GMO CYBER SECURITY IERAE

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%

Catalin					
Versio					
19H20					
	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%

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%）**

❹ ダメージ低減＝バージョンアップ率

GMO CYBER SECURITY IERAE

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%

Catalin						
Versio						
19H20						
	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%

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%）**

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 CYBER SECURITY IERAE

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イエラエの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

国内No.1 ※1 ホワイトハッカー在籍数150名以上

国内No.1 ※2 国内最大級のセキュリティコンテスト

2年連続 世界No.1 ※3 世界最高峰のセキュリティコンテスト

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

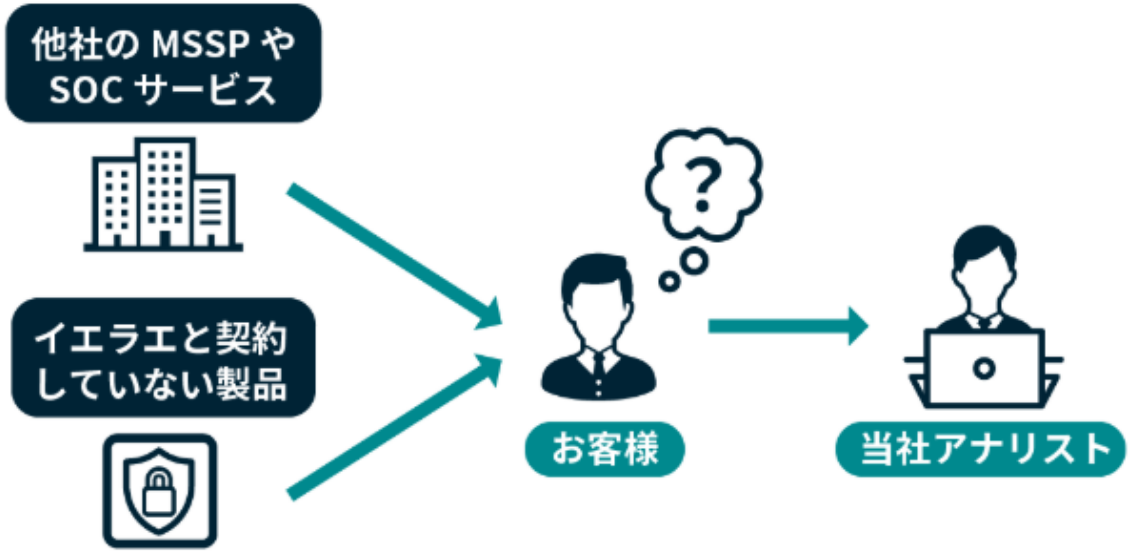
対応製品

aws　CLOUDFLARE

なんでもログ相談窓口

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行います。



ご清聴ありがとうございました