

フロンティア AI時代のサイバーセキュリティ戦略

染谷 征良
チーフサイバーセキュリティストラテジスト

パロアルトネットワークス株式会社

パロアルトネットワークス について

グローバル本社

- **2005 年** 設立、米国カリフォルニア州サンタクララに本社
- 世界 **150 以上の国・地域** の **90,000 超** の企業・組織へのソリューション導入実績
- Fortune100 の **97 社超**、Global2000の **77%** が採用
- 2023年5月サイバーセキュリティ企業初の **S&P500 銘柄**、2026年9月から **S&P100 銘柄** に選定
- グローバル従業員数 **21,000 人以上**

日本法人

- 日本法人 **2009 年** 設立
- 東京、大阪、名古屋に拠点
- 国内従業員数 **400 名以上**



アライ ヒロシ
代表取締役社長兼会長
パロルトネットワークス株式会社



米国本社(カリフォルニア州サンタクララ)



ニケシュ・アローラ
会長兼最高経営責任者(CEO)
Palo Alto Networks Inc.



リー・クラリッチ
最高製品・技術責任者(CPO/CTO)
Palo Alto Networks Inc.

変革を実現する次世代セキュリティプラットフォームとサービス



近年発生した日本国内における顕著なセキュリティインシデント

	製造業A社 2025年9月	物流業B社 2025年10月
事象	ランサムウェア被害でシステム障害が発生、個人情報約200万件が漏えい、工場が稼働停止し受発注・物流が約半年間停滞、決算報告も延期	ランサムウェア被害で物流・社内・問い合わせ管理各システムが侵害され、個人情報約73万件漏えい、サービス全面復旧まで約7ヶ月を要す
原因・課題	- パスワードの脆弱性が悪用 - データセンター内の複数サーバーや業務端末が暗号化被害 - 初期侵入後被害まで約10日間気付かず - バックアップから復旧可能も業務完全正常化に190日を要す	- 業務委託先管理アカウントが漏えいし悪用された可能性 - 多要素認証も未適用 - サーバーへのEDR未導入 - セキュリティ常時監視も未実施 - バックアップデータも暗号化被害 - 初期侵入後被害まで約4ヶ月間気付かず
求められる 対応・対策	- パスワード、多要素認証などのアイデンティティ管理 - ASMIによる脆弱性・設定ミスなどリスク資産の特定と対処 - EDRでの業務端末やサーバーでの振る舞い検知 - ログデータを統合したAIによる分析とリアルタイムの検知 - ネットワークのセグメンテーション - ペネトレーションテストやスレットハンティングの実施	- 権限管理、多要素認証をはじめとしたアイデンティティ管理 - ASMIによる脆弱性・設定ミスなどリスク資産の特定と対処 - EDRでの業務端末やサーバーでの振る舞い検知 - ログデータを統合したAIによる分析とリアルタイムの検知 - 情報系・工場系ネットワークの横断的なリスク管理 - ペネトレーションテストやスレットハンティングの実施

近年発生した日本国内通信事業者における顕著なセキュリティインシデント

	通信事業者 C社 2025年4月	通信事業者 D社 2026年6月	通信事業者 F社 2025年10月
事象	法人向けメールサービスの不正アクセスで、586契約法人メールアカウント31万件の認証情報、メールなどが漏えい	ISP事業者向けメールシステムに対する不正アクセスで、メールアドレスやパスワード最大約1,200万人分漏えい	派遣社員によるコールセンターシステムからの情報窃取で、約928万の個人情報が漏えい、名簿業者に流出
原因・課題	- サードパーティ製Webメールソフトのゼロデイ脆弱性が悪用 - システム上にすでに存在する既存ツール群が悪用 - 初期侵入後被害まで約8ヶ月間把握できず	- 自社システムに導入していたサードパーティ製ソフトの脆弱性が悪用 - 外部通信を制御する全サーバーでEDR未導入 - 一部ISP事業者からの報告から17日間把握できず	- アカウント管理や特権管理の未実施 - 外部記録媒体、メール、私物端末でデータが流出した可能性 - サーバーでの変更監視等の未実施 - 端末やユーザー単位での監視の未実施 - セキュリティルールが形骸化 - 不正行為を10年以上把握できず
求められる対応・対策	- 権限管理などのアイデンティティ管理 - ログデータを統合したAIによる分析とリアルタイムの検知 - Webアプリケーションへの脆弱性攻撃に対する防御 - ペネトレーションテストやスレットハンティングの実施	- 権限管理などのアイデンティティ管理 - ペネトレーションテストやスレットハンティングの実施 - EDRでの業務端末やサーバーでの振る舞い検知 - ログデータを統合したAIによる分析とリアルタイムの検知	- 特権含めたアイデンティティ管理全般 - デバイスコントロール - 経路別での情報漏洩対策 - EDRでの業務端末やサーバーでの振る舞い検知 - ログデータを統合したAIによる分析とリアルタイムの検知

近年発生した顕著な海外通信事業者におけるセキュリティインシデント

	通信事業者 F社 2025年4月	通信事業者 G社 2024年1月	通信事業者 H社 2021年8月
事象	約4年前の管理サーバー侵入が原因で、サーバー28台がマルウェア33件に感染、USIM情報2,696万件が流出	ヨーロッパ、中東、中央アジア全域のIP情報の管理アカウントが侵害され、通信の半分近くで障害が約3時間発生	社会保障番号を含む約7,600万人以上の利用者情報が流出し、ダークウェブ上で販売
原因・課題	- 管理者情報を平文保存、パスワード有効期限が未設定 - 異常発生時に一部ログしか点検せず - USIM認証鍵や通話記録なども平文保存 - 資産管理情報の記録も存在せず - 事故発生後にサーバーから証拠隠滅 - 法廷事故報告の不履行並びに遅延	- 業務端末が情報窃取型マルウェアに感染し管理アカウントが流出した可能性 - 管理アカウントでの簡易なパスワード - 管理アカウントへの多要素認証未導入 - 経路設定情報に対する不正変更 - 管理アカウント流出後、事故発生まで約4ヶ月間気づけず	- テスト用ゲートウェイがインターネット上に露出 - 総当たり攻撃によってSSH接続 - テスト環境と本番環境のセグメンテーションの欠如 - ラテラルムーブメントを含め侵害に数週間気づけず
求められる対応・対策	- 権限管理、暗号化、多要素認証をはじめとした特権アカウント管理 - ログデータを統合したAIによる分析とリアルタイムの検知 - デジタル資産の可視化と資産管理 - 原因・影響範囲特定のためのログ保全 - 事故報告体制の整備	- EDRによる端末での振る舞い検知 - DLPによる情報の外部流出の防止 - パスワード管理、多要素認証を含む特権アカウント管理 - ログデータを統合したAIによる分析とリアルタイムの検知 - 重要システムにおける変更管理	- ASMによるリスク資産の特定と対処 - パスワード管理、多要素認証を含む特権アカウント管理 - アドレス制限やアカウントロック - ログデータを統合したAIによる分析とリアルタイムの検知 - ネットワークのセグメンテーション

日本の金融保険業界のインシデント(保険会社 I社)

1. 事案発生・対応タイムライン(2026年)

- **6月10日～30日:発生・検知・緊急対応**
 - **6/10～25:** 不正アクセス複数回実施(精査で判明)
 - **6/25 06:30:** CPU高負荷検知。漏えい判明後、即座に通信遮断・システム停止
 - **6/30:** 第一報公表。金融庁より報告徴求命令を受領
- **7月10日～31日:調査・顧客対応・最終報告**
 - **7/10～30:** 該当顧客(約440万人)へお詫び状順次発送
 - **口座連携:** 二次被害防止のため関係金融機関へ口座情報提供
 - **7/31:** 金融庁へ最終報告・原因公表
・被害規模確定(顧客440万人、代理店4万店)
・役員4名の報酬自主返納決定(20～30%×1ヶ月)
- **9月～10月:段階的再開・防犯周知**
 - **9/28:** 一部除きサービス再開(初回登録改定、パスキー推奨等で強化)
 - **10/1:** 詐欺・不審連絡への注意喚起&FAQ公表

2. 被害規模の全貌

440万人 **22万人** **4万店**
対象顧客数 うち口座情報含む 対象代理店数

- **漏えい項目:** 氏名、住所、電話番号、証券番号、保障内容、口座情報等
- **安全確認済:** マイナンバー、カード情報、Pass、Mailは対象外
- **二次被害:** 現時点で不正利用・金銭被害は確認されず

3. 発生原因と「正規酷似」の背景

Q. 検知できなかった理由(正規酷似アクセス)

プログラム破壊等のバグ侵入ではなく、正規サービス機能の仕組み・リクエスト形式にそのまま沿って攻撃が行われたため、初期段階で自動遮断できなかった。

Q. 「脆弱性」の有無

プログラムのバグではなく、「**認証・認可およびアクセス制御の設計上の不備・脆弱性**」が存在。

特定された3つの主要要因:

- **認可・制御の不備:** 正規手順を装った照会に対し、適切な権限に基づくアクセスかを厳格に制御する機能が不十分。
- **大量照会の監視不足:** 短時間の大量データ照会に対する制限・ブロック機能(レートリミット等)の不足。
- **事前検証のリスク想定不足:** リリース前テストで「正規挙動に酷似させた大量照会」という手口自体を想定できていなかった。

4. 7つの対応分野と再発防止策

① アクセス制御・照会制限の厳格化

本人確認プロセスの厳格化(パスキー導入・推奨)、データ照会時のユーザー権限・妥当性チェック(認可機能)の徹底強化。

② 大量アクセス監視・自動制御(WAF等)

アプリ層とWAF等のセキュリティ機器の双方で大量照会を検知し、即座に通信制限(レートリミット等)をかける仕組みを導入。

③ 事前検証の高度化(ペネトレーションテスト)

最新手口を反映した要件定義の見直し、設計時レビュー強化、正規挙動模倣など多様な攻撃シナリオによる侵入テストの実施。

④ 管理態勢・人財の拡充(ライフサイクル全体)

高度専門人財の増強、開発～運用ライフサイクル全5領域の再整備、PDCAモニタリング体制の確立。

⑤ 顧客サポート&金融機関連携

専用コールセンターの拡充、約22万件の口座情報を金融機関へ提供し不正取引の監視強化・突合を実施。

⑥ 経営責任の明確化

会長・社長(30%×1ヶ月)、CDIO・CRO(20%×1ヶ月)の役員報酬自主返納を実施。

事例 9 APIが悪用される事例

個人情報取扱事業者が提供するスマートフォンアプリやWebサービスにおいて、API（※6）を利用していたところ、APIの設計・設定不備により、攻撃者が当該サービスにログインした後、パラメータを書き換えることで、本来であれば取得できない他のユーザー情報を取得できる状態となっており、個人データの漏えい等が発生した事案。



原因

- ✓ 管理対象から漏れているAPIが存在した。
- ✓ URLや会員ID等のパラメータを書き換えることで、他ユーザーのデータにアクセス可能な状態であった。
- ✓ レスポンスに不要な情報が含まれていたことや、会員ID等が連番となっていたことから、攻撃者によるAPIの仕様等の推測が容易であった。
- ✓ 大量アクセスを制御するためのアクセス回数制限（レートリミット）がなかった。

対策例

- ✓ 定期的にAPIの棚卸しを行う。
- ✓ 認証（本人確認）に加え、認可（そのユーザーが当該データにアクセスする権限を有するかの確認）を都度行う仕組みを実装する。
- ✓ 不要な情報をレスポンスに含めないように設計する。会員IDや管理番号にランダムな値（UUID等）を採用する。
- ✓ 短時間での大量アクセスを検知・遮断するためのアクセス回数制限（レートリミット）を実装する。

※6 Application Programming Interfaceの略称であり、異なるシステムやアプリ間をつないでデータや機能を共有する仕組み。 12

個人情報保護委員会「Warning 不正アクセスによる個人データ漏えい防止のための注意喚起」（令和6年 12月11日、令和8年10月7日改訂）
※上記事例9は令和8年改訂時に追加されたもの。

セキュリティインシデントの現実 — 被害がなくなる**3つの決定的要因**



予防可能なギャップ

90%

対策上の不備や隙が
原因で被害が発生



権限管理の弱点

89%

アイデンティティ関連の弱点が
悪用され被害に



対策の複雑性

87%

攻撃の痕跡があるにも
関わらず気づけずに被害

現在のサイバーセキュリティのアーキテクチャと体制を再評価して
インフラ全体で対策上の課題や弱点を洗い出すことが不可欠

2026年下半期にみられるセキュリティインシデントの変化



情報漏洩に被害が 急速にシフト

ランサムウェア被害が
減少する一方で
急増する情報漏洩被害



Webシステムでの 被害が急増

個人情報を保持する
Webシステムでの
被害が圧倒的多数



攻撃手法の 多様化

脆弱性から設定不備まで
一貫性が見られない
手口による攻撃

攻撃のスケールを可能にするマシンスピードで行われる AIエージェントを活用したサイバー攻撃が世界的に台頭

上場企業におけるセキュリティインシデント被害の適時開示が急増

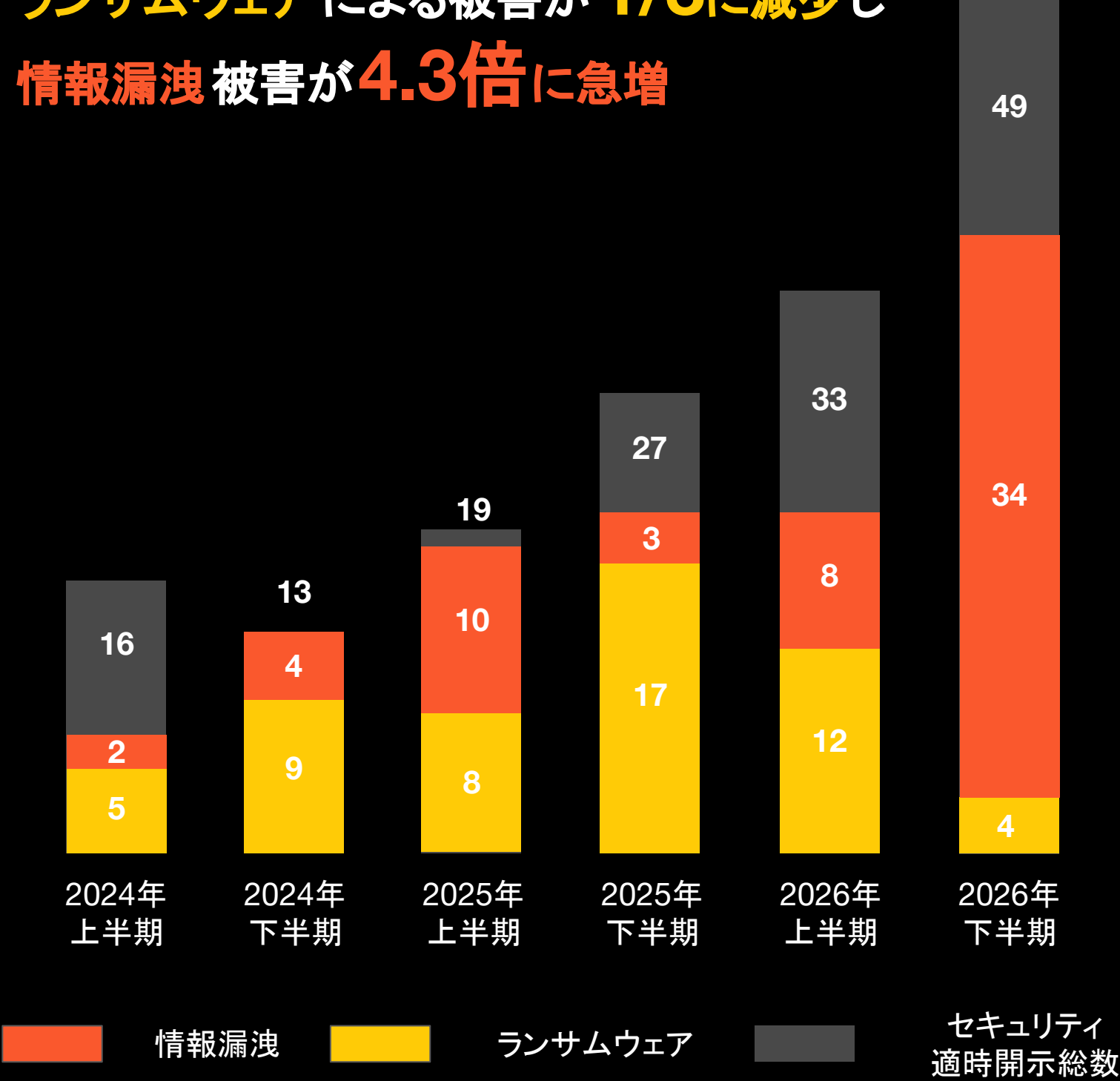


過去最多ペースの
国内上場企業による
セキュリティインシデントの
適時開示

82件 (2026年)

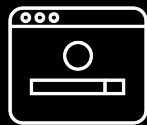
昨年1年間と比較して **78%増**
(2026年10月20日時点)

ランサムウェアによる被害が **1/3に減少**し
情報漏洩被害が **4.3倍に急増**



上場企業による適時開示をもとにパロアルトネットワークス集計2026年10月20日時点)
「情報漏洩」は公表内容での「可能性」の言及を含む、「原因」は公表内容での言及に限定

2026年下半期に入り Webシステムでの被害が急増



73%

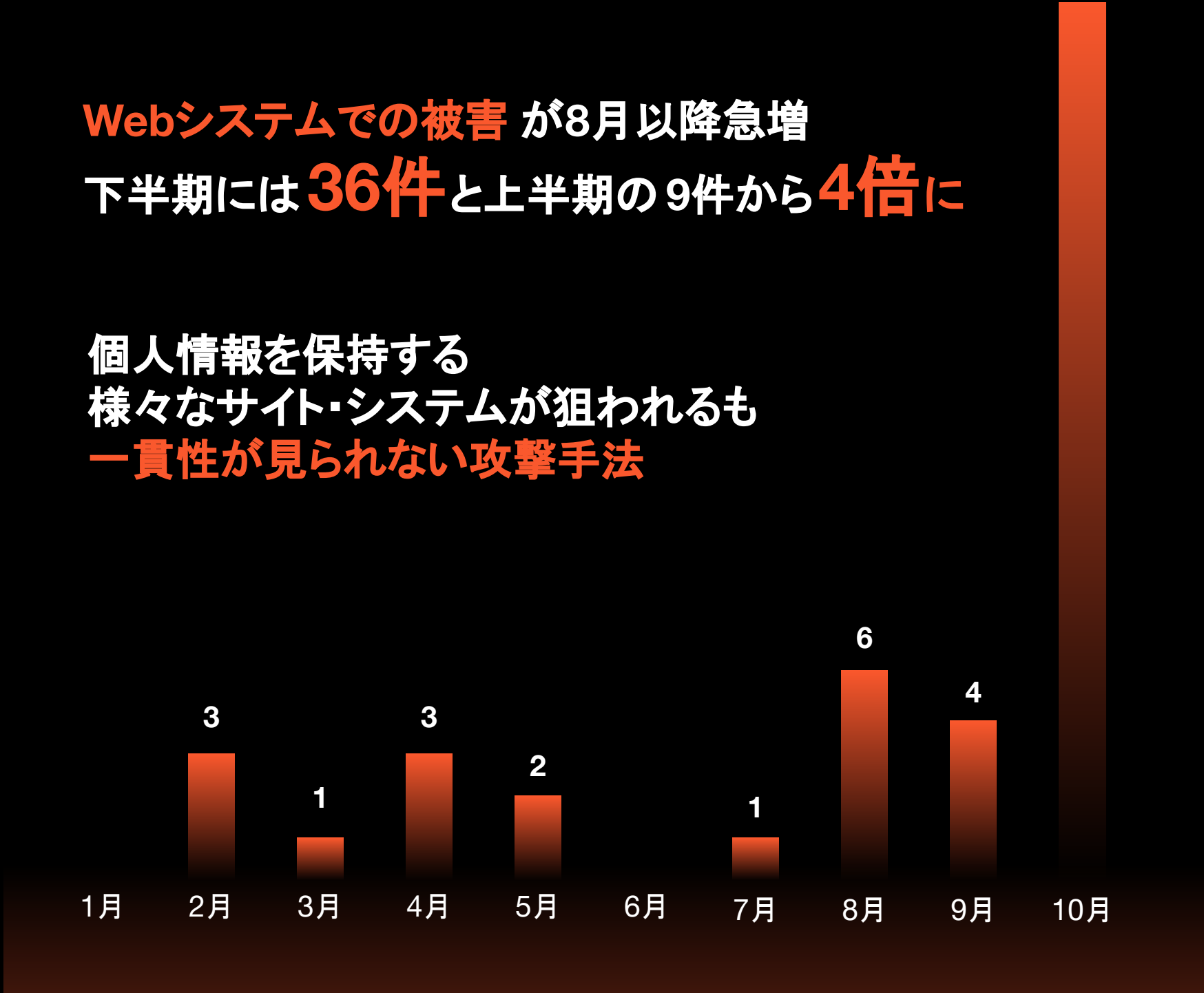
上場企業によるセキュリティインシデントに関する
2026年下半期の適時開示全体に占める Webシステムでの被害

25

時期	業種	被害	原因	対象システム
7月	情報・通信	情報漏洩	不明	コンテンツ管理システム
8月	情報・通信	情報漏洩	不明	業務管理システム
8月	建設・不動産	情報漏洩	設定不備	業務管理システム
8月	卸小売	情報漏洩	アカウント窃取	ECサイト
8月	卸小売	情報漏洩	不明	予約サイト・予約管理システム
8月	製造	情報漏洩	不明	業務管理システム
8月	情報・通信	乗っ取り	不明	製品・サービス紹介サイト
9月	卸小売	情報漏洩	BIツール脆弱性	業務管理システム
9月	卸小売	不明	アカウント窃取	コンテンツ管理システム
9月	建設・不動産	情報漏洩	不明	会員サイト・会員管理システム
9月	製造	障害	不明	製品・サービス紹介サイト
10月	卸小売	情報漏洩	不明	会員サイト・会員管理システム
10月	金融	情報漏洩	不明	問い合わせサイト
10月	卸小売	情報漏洩	設定不備	会員サイト・会員管理システム
10月	情報・通信	情報漏洩	脆弱性	会員サイト・会員管理システム
10月	卸小売	情報漏洩	脆弱性	会員サイト・会員管理システム
10月	サービス	情報漏洩	脆弱性	予約サイト・予約管理システム
10月	情報・通信	情報漏洩	不明	業務管理システム
10月	サービス	情報漏洩	脆弱性	予約サイト・予約管理システム
10月	情報・通信	情報漏洩	不明	予約サイト・予約管理システム
10月	サービス	情報漏洩	BIツール脆弱性	業務管理システム
10月	情報・通信	情報漏洩	不明	会員サイト・会員管理システム
10月	卸小売	情報漏洩	不明	ECサイト
10月	情報・通信	情報漏洩	BIツール脆弱性	業務管理システム
10月	情報・通信	情報漏洩	設定不備	ECサイト
10月	情報・通信	情報漏洩	Web制作脆弱性	コンテンツ管理システム
10月	金融	情報漏洩	設定不備	業務管理システム
10月	製造	情報漏洩	不明	ECサイト
10月	製造	情報漏洩	Web制作脆弱性	製品・サービス紹介サイト
10月	情報・通信	情報漏洩	設定不備	ECサイト
10月	情報・通信	情報漏洩	Web制作脆弱性	問い合わせサイト
10月	建設	情報漏洩	Web制作脆弱性	問い合わせサイト
10月	卸小売	情報漏洩	脆弱性	ECサイト
10月	情報・通信	情報漏洩	脆弱性	ECサイト
10月	サービス	情報漏洩	不明	ECサイト
10月	サービス	情報漏洩	Web制作脆弱性	問い合わせサイト

Webシステムでの被害 が8月以降急増
下半期には 36件 と上半期の 9件から 4倍に

個人情報を保持する
様々なサイト・システムが狙われるも
一貫性が見られない攻撃手法



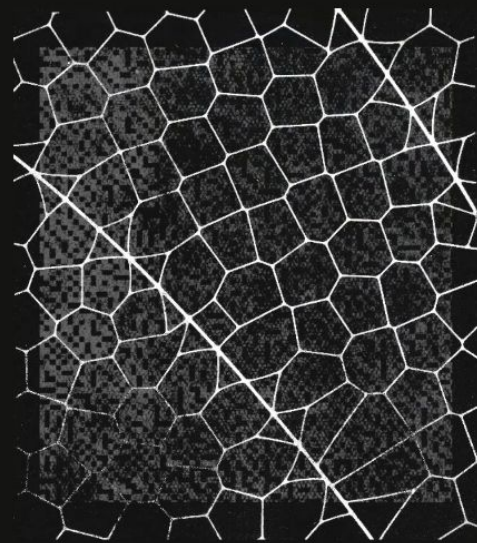
上場企業による適時開示をもとにパロアルトネットワークス集計2026年10月20日時点）
「情報漏洩」は公表内容での「可能性」の言及を含む、「原因」は公表内容での言及に限定

Project Glasswing: AI時代に向けた重要ソフトウェアのセキュリティ確保

ANTHROPIC

Project Glasswing

Securing critical software
for the AI era



12社のローンチパートナー

aws

ANTHROPIC



BROADCOM

CISCO

CROWDSTRIKE

Google

JPMorganChase

THE
LINUX
FOUNDATION

Microsoft

NVIDIA

paloalto
NETWORKS

- Mythosベースのスキャンにより
従来のペネトレーションテスト
2年以上分を3週間で達成
- 2026年5月に、新たに見つかった
脆弱性 75件を含む**CVE 26件**を発表
- 先端サイバーモデルの機能が
オープンソース化・学習され、
攻撃者の手に渡るまで**3~5ヶ月のラグ**

出典: Anthropic社 <https://www.anthropic.com/glasswing>

13

各国機関の動向にみるフロンティア AIの脅威に対して求められる具体策



経営層のリーダーシップと全社的なガバナンス

- 将来事業への必須投資として経営が直接関与
- 経営課題として予算や人材の意思決定を主導
- 取締役会での監督や組織の壁を超えた連携



基本的対策の徹底と多層防御

- 全アクセスを検証するゼロトラストの導入
- アクセス制御やログ監視の強化
- 不要な接続やリスク面の削減



脆弱性対応の高速化と技術的負債の解消

- パッチ適用プロセスの高速化・自動化
- 事業影響に応じて優先順位をつけた対応
- レガシーシステムの迅速な更新・解消



レジリエンスの強化とインシデントへの備え

- 侵入を前提とした被害最小化と迅速な復旧
- BCPや対応手順の策定と訓練の実施
- 最悪の事態を想定した運用・復旧の準備



防御におけるAI技術の積極的活用

- マシンスピードでの攻撃にはAIが不可欠
- 脆弱性の発見や異常な振る舞いの早期検知
- 対応やトリアージで解決時間の大幅短縮

フロンティア AIがもたらす脅威に対する各国機関の動向



参考：海外と日本の重要インフラ・金融のサイバーセキュリティ対策（フロンティア AI関連のみ）

- フロンティアAI関連のFive Eyes等の国際的な注意喚起においては、監視・検知を含めて防御側へのAIの活用が必須とされている。
※あくまでフロンティア AIモデル対策に特化した注意喚起であるため、EDRの実装等の具体的な対策については省略されていると考えられる。
- 基本的には、インシデント発生時に国内・グローバルな社会経済に重大な影響がある金融分野において、サイバーセキュリティ対策の具体的な実装が先行。

対策の種類	求められる対策例	海外		重要インフラ 安基・統一基準・注意喚起・経営 GL	金融 要請（2026-05-22）・金融 GL・経営 GL
		ASIC	FE		
ガバナンス・ リスク評価	年1回以上の計画・態勢レビュー	○	○	● 安基2.8②-2	● 金融GL2.1.1②④
	相互に関連する脆弱性の累積的影響の評価	●	—	— 未記載	— 未記載
	停止判断の要素（猶予・影響・代替）	○	—	● 安基6.2.4①-3	● 金融GL2.5.2.4①
	自己点検を超える独立した監査・検証	●	○	● 経営GL指示6（安基2.6①-2は○）	● 金融GL2.1.4①②・2.1.5①②
	重要サービス全体の有効性を証拠で経営に報告	●	○	● 経営GL指示6（有効性評価・経営への報告）	● 経営GL指示6（有効性評価・経営への報告）
脆弱性対応 パッチ適用と、 パッチできない 場合の個別対策	重大度別の対応期限と実績管理	○	○	● 安基3.6③-2（実績管理のみ）	● 金融GL2.2.3①③、要請別添 §2⑤
	大量・高頻度パッチの処理能力（委託先含む）	●	○	● 安基3.6③-3	● 要請別添 §2④⑤
	脆弱性対応の自動化への移行（中長期）	—	—	— 未記載	● 要請別添 §2柱書き
	パッチ困難時のリスクに応じた代替措置	—	—	● 安基3.6③-1、4.4.2②-2	● 要請別添 §2⑦、金融GL2.3.4.1③
	仮想パッチ（WAF等）・ボット対策	—	—	● 安基3.6②-2解説等（仮想パッチを例示）	● 要請別添 §2⑦（仮想パッチ等を例示）
	未適用の残存リスク評価と経営の承認	—	—	● 安基3.6③-1解説（経営層の承認を「検討」）	● 金融GL2.2.3③、要請別添 §2⑦
	更新困難なレガシーの移行計画の実行	—	○	● 安基4.4.2②-3	● 金融GL2.3.4.1③
	ネットワーク分離・不要な外部接続からの隔離	○	●	● 安基4.6.1①-4	● 金融GL2.3.4.4①
	侵害を前提にした多層防御	●	●	● 経営GL指示5（安基4.4.4①-3・①-4は○）	● 金融GL2.3①、要請別添 §2⑦
	マイクロセグメンテーション等による横展開の制限	●	○	● 安基4.6.1①-7	● 金融GL2.3.4.4 c、要請別添 §2⑦
	特権IDへの多要素認証	○	○	● 安基4.1.1①-3解説・4.1.2①-5（①-9は○）	● 金融GL2.3.1①（多要素認証を例示）
	EDR等による端末の検知・対応	—	—	● 安基4.4.4①-4（NDR等も）	● 要請別添 §2⑦
	ゼロトラストに基づく設計・運用	—	—	● 注意喚起 §2（安基は関連対策のみ）	— 関連対策あり、導入・移行の明示なし
	職員・委託先のアクセス監視（内部脅威）	●	○	● 安基5.2①-1解説（アクセス監視を例示）	● 金融GL2.4.1③④
検知・監視と 防御AI	SIEM等による相関分析（AI搭載は問わない）	—	●	● 安基5.2①-2・5.3①-2	● 金融GL2.4.1 c
	防御へのAI活用（検知・脆弱性発見等）	●	●	● 安基7①-3-1解説（中長期で推奨）・注意喚起 §2	— 未記載
演習・復旧の 実証	侵入試験（ペネトレーションテスト）	○	○	● 経営GL指示6（安基3.6②-3は○）	● 金融GL2.2.4①
	経営層が参加する演習	○	○	● 経営GL指示7（安基4.2.2①-2は○）	● 金融GL2.2.5②
	隔離バックアップからの実復元試験	○	○	● 安基4.3.3②-1・②-2	● 金融GL2.3.3⑤
	再接続前の原因除去・正常性確認	○	○	● 安基6.2.5①-4～6	● 金融GL2.5.2.6①④⑤
	業界横断・合同演習への参加	○	○	● 安基4.2.2①-3	● 金融GL2.2.5①
	隔離状態でのサービス継続・復旧（隔離運転）	○	○	△ 安基6.1①-1解説・注意喚起 §2（CISAの紹介）	— 未記載
委託先・ 供給網	共通依存先・集中リスクの評価	●	—	— 未記載	● 金融GL2.6 b・c
	委託先停止に備えた出口戦略・代替手段の試験	○	—	● 安基2.9②-1解説（代替手段の「検討」まで）	● 金融GL2.6 d
	安全な初期設定の製品を調達	—	○	● 安基2.9③-1・③-4解説（JC-STAR等）	● 金融GL2.3.4.1 a

凡例

●	必須
○	推奨
△	言及のみ
—	未記載

出典・略称

ASIC: Australian Securities & Investments Commission “[ASIC calls for urgent cyber uplift as AI accelerates cyber threats](#)” (2026年5月8日)

Five Eye: Five Eyes Cyber Security Agencies “[Five Eyes Cyber Security Agencies Statement](#)” (2026年6月22日)

注意喚起: NCO他「[AI性能の高度化を踏まえたサイバーセキュリティ対策の強化について（重要インフラ事業者等に対する注意喚起）](#)」(2026年5月18日)

統一基準: サイバーセキュリティ戦略本部「重要インフラのサイバーセキュリティ対策のための統一基準」(2026年7月31日)

安基: NCO「[重要インフラのサイバーセキュリティに係る安全基準等策定ガイドライン](#)」(2026年9月11日)

経営GL: 経済産業省・IPA「[サイバーセキュリティ経営ガイドライン Ver.3.0](#)」(2023年3月24日)

要請: 金融庁・日銀「[「フロンティア AI」による脅威変化を踏まえた金融機関等の短期的な対応](#)」に係る要請について」(2026年5月22日)

金融GL: 金融庁「[金融分野におけるサイバーセキュリティに関するガイドライン](#)」(2024年10月4日)

その他参考: NCO「[安全基準等策定ガイドライン\(案\)に関するパブリックコメントの主な結果一覧](#)」(2026年9月11日)

※その他各分野の対策については、関係省庁からの注意喚起や関係事業者間（金融ISAC、ICT ISAC等）で検討されているものの、非公開のものあるためここでは割愛。

AIによる自律的な攻撃は現実のものに



企業に対する AI支援型のサーバー攻撃 ^{*1}

2026年9月

- 攻撃者がフロンティアAIを用いてネットワーク侵入からAI基盤乗っ取りまで自律的に行っているインシデントに対応
- AIエージェントを活用してMITRE ATT&CK手法50件を駆使して10時間以内に攻撃を完遂
- 複数エージェントを並列で活用して、特権から自動実行まで永続性を確保
- 被害組織のリソースを活用して隠蔽とコスト効率化を実現
- 構造化された情報など人間とは異なる特有の痕跡を残す



韓国金融機関へのサイバー攻撃

2026年9～10月

- エージェントツールによる攻撃で、金融機関16社で情報漏洩被害が9月末以降発生^{*2}
- Unit 42 は攻撃に使われたサーバーとの通信を複数の顧客環境で9月6日に確認^{*3}
- 検索ツール、モバイルリバースエンジニアリングツール、カスタムエクスプロイトを露出したオープンディレクトリから8月29日に確認
- 複数の攻撃者の存在を示唆する同一ツールの展開をアジア太平洋地域を中心に世界45箇所でも確認^{*2}

LLMと一般的な攻撃ツールを組み合わせたエージェントックフレームワークは、大規模な形で偵察とエクスプロイト開発の敷居を下げ、エクスプロイトの作成をリアルタイムで可能に

脆弱性、設定不備、過剰な権限を発見・修正してインフラ全体でアタックサーフェスを削減し、リアルタイムで脅威の検出と対応を可能にする AIへの投資が不可欠に

^{*1}: Unit 42 'An AI-Assisted Cyber Attack: Inside a Unit 42 Investigation'

^{*2}: <https://www.fsc.go.kr/eng/pr010101/87928?srchCtgr=&curPage=&srchKey=&srchText=&srchBeginDt=&srchEndDt=>

^{*3}: Unit 42 調査

参考: アンケート結果の総括・分析(2026年7月7日及び21日)

2026年7月7日及び21日の当社イベントの際に、112社・215名の日本企業(経営層・セキュリティ責任者等)へのフロンティアAI対策の課題等のアンケート結果から、以下の実態が浮き彫りとなった。

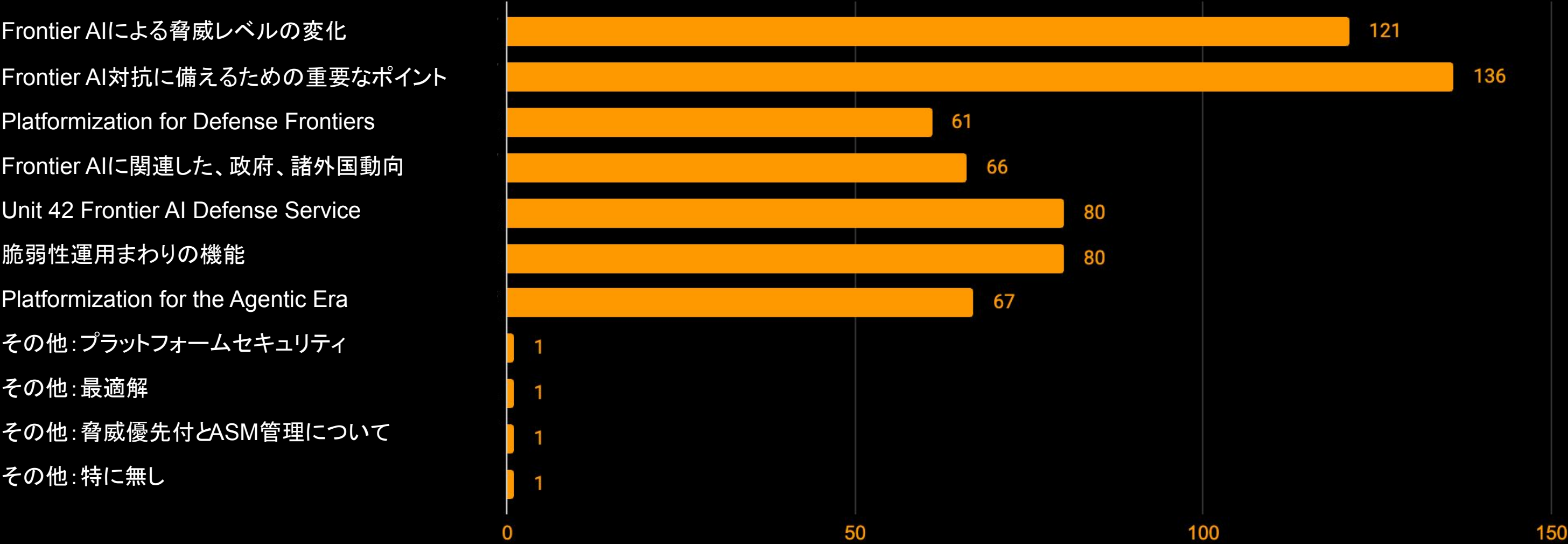
- **脅威の認識と「実行への戸惑い」のギャップ**
 - フロンティアAIモデル出現に伴う脅威の変化と対策に強い関心が示されている。
 - 一方で、政府が求めるような高度な対策(リスクベースでのパッチ適用や多層防御など)を実行する上での障壁として、レガシーシステムへの対応等の難しさに加えて、「そもそも何から手をつけたら良いか分からない」と回答した層も約2割存在し、企業単独での方針策定が行き詰まっている実態が明確になった。
- **「外部丸投げ」からの脱却と「内製化・自立」への強い意欲**
 - 政府への支援策の要望において、「補助金等の財政支援」の用途として「適切なセキュリティ製品・サービスの導入」と「内部人材の育成支援」が上位を占めた。これは、企業が単に外部ベンダーに作業を委託するための資金を求めているだけではなく、「自社に最適なツールを導入し、それを運用できる社内人材を育成(内製化)したい」という、抜本的なサイバーセキュリティ対策・対応基盤の強化を求めていることを示している。
- **「道標」としてのガイドライン・ベストプラクティスの必要性**
 - 上記のような「自立した対策」を推進するための土台として、アンケートでは財政支援以上に「ガイドライン・マニュアルの策定」が最も優先度の高い支援策として求められている。企業が製品導入や人材育成の具体的な一歩を踏み出すために、実務的かつ具体的な手順書やベストプラクティスが求められていると考えられる。

<https://www.paloaltonetworks.jp/company/press/2026/panw-announces-survey-results-on-the-current-state-of-security-measures>

参考: 問1 参加者の関心・理解

- フロンティアAIの「脅威の全体像」や「具体的対策」といった直近の実務課題への関心が中心となる一方で、Frontier AI model対策、諸外国・政府の動向やAgentic AI対策などにもまんべんなく関心が広がっていることが判明。

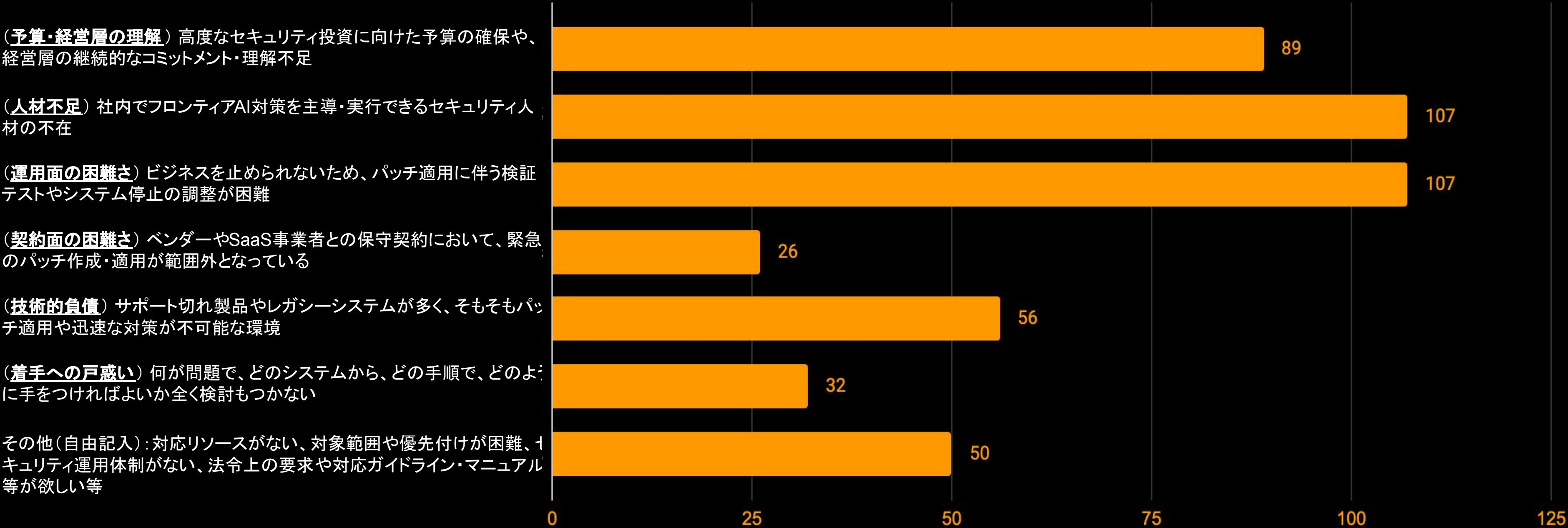
本日の内容で、気になったポイント、有益だったポイントを教えてください(215名回答、複数回答可)。



参考: 問2 フロンティア AI対策における懸念

- 予算・人材不足という慢性的課題に加え、運用面・技術的負債の対応に苦慮する実情が浮き彫りとなった。
- 更に「何から着手すべきか不明」と回答した層も約2割存在し、初期段階でのガイドラインやロードマップの欠如が課題となっている。

政府が求める対策(リスクベースでの迅速なパッチ適用や多層防御の強化など)を実行する上で、最大の障壁は何ですか？(175名回答、複数選択可)

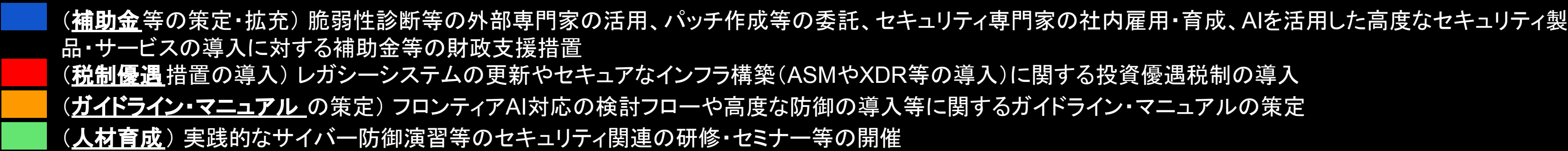


<https://www.paloaltonetworks.jp/company/press/2026/panw-announces-survey-results-on-the-current-state-of-security-measures>

参考: 問3 フロンティア AI対策に必要な支援策

- 「ガイドライン・マニュアルの策定」に対する要望が最も高く、問2で顕在化した具体的な対応策や着手への迷いを裏付ける結果となった。
- 各企業が自社単独での方針策定に限界を感じており、国や業界主導の標準的なガイドライン・ベストプラクティスが強く求められている。

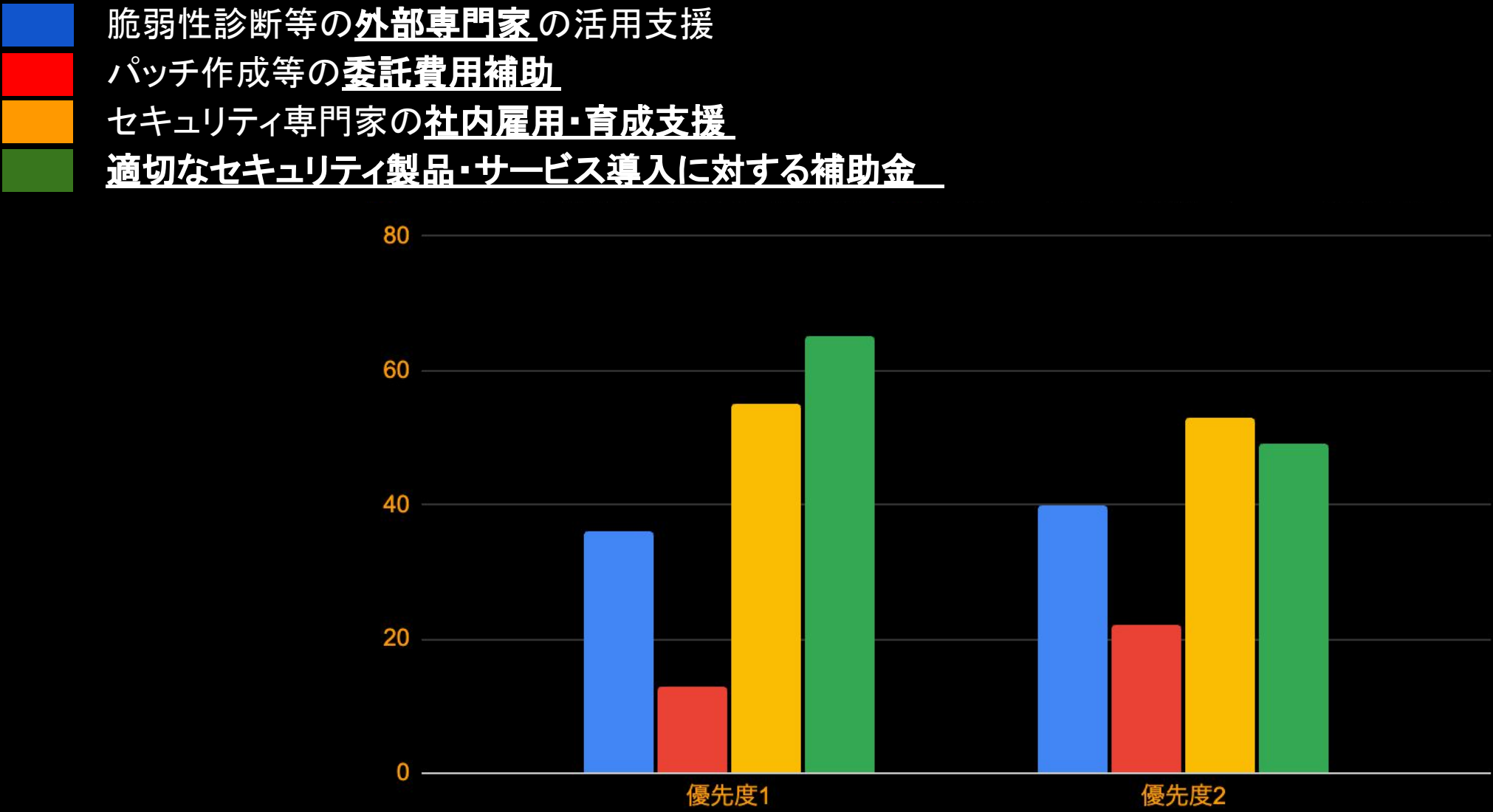
質問 Frontier AI時代における我が国のサイバー防衛力を底上げするために、日本政府に対して最も期待する支援策・施策は何ですか？
(174名回答、単一選択)



参考: 問4 財政支援の対象

- 「セキュリティ製品・サービスの導入」への補助金要望が最多となり、次いで「内部人材の育成支援」が続いた。
- 企業が対症療法的な脆弱性対応にとどまらず、ツールと人材の両面から組織のセキュリティ基盤を抜本的に強化したいという意向が伺える。

質問 補助金等の財政支援措置のうち、特に重要なものを2つお選びください
(169名回答、単一選択)



まとめ: フロントティア AIの脅威を踏まえて求められる対策

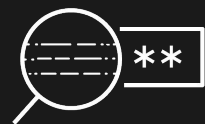


経営層のリーダーシップによる投資・リソース確保とガバナンス強化



リスクが残存する 露出資産の継続した削減

- 露出しているデジタル資産の可視化
- 優先度に応じた脆弱性への対策・緩和策
- 設定ミスや不必要な接続・機能の解消



アクセス制御と 重要リソースの保護

- サーバーへの悪意ある攻撃コードからの保護
- 重要リソースでの不審な挙動・異常監視
- 全ての通信の可視化と制御



アイデンティティ保護と 権限管理の強化

- 管理アカウントのセキュリティ強化
- リソースに対する最小権限の徹底
- ハードコードされたキーや認証情報の対処



侵入した脅威の 迅速な検出と対応

- 統合的なセキュリティ監視基盤の構築
- AIを活用した脅威検出による平均検出時間MTTRの短縮
- 自動化・プレイブックによるMTTRの短縮



レジリエンス強化と 有事への継続した備え

- BCPや対応手順の策定と訓練の実施
- 有事の際の専門家との迅速な連携
- 演習によるリスク面の洗い出しと対応

統治

特定

防御

検知

対応

復旧

マシンスピードで行われる攻撃に対して AI・自動化を最大限に活用したセキュリティの実現を

参考: フロンティア AIの脅威を踏まえてドメインごとに注力すべき施策

	短期的対策	中長期的対策	弊社 ソリューション例
アタックサーフェス	- 露出したデジタル資産の可視化 - 脆弱性や設定ミスの検出・対応	継続的なリスク資産の検出・対応 サイクルの確立	 
アプリケーション	- アタックパス分析によるリスク極小化 - Webシステム上での変更・改ざん検知 - ハードコードされているシークレットの検出・対応	- アプリケーション・APIへの脆弱性 攻撃からの防御 - 不審なコマンド実行のブロック - サプライチェーン攻撃のリスクに対応	
ネットワーク	仮想パッチによる脆弱性攻撃からの防御		
アイデンティティ	- アカウント、権限、キーや シークレットの可視化 - 不要なアカウント・権限の削除	- シークレットの一元的な管理 - Zero Standing Privilege の実装 - アイデンティティによる挙動監視・制御	
セキュリティ運用	- 端末・システム上での操作履歴・APIコールの監視 - ネットワーク内部でのログ監視	- 統合的な監視基盤の構築 - インシデント対応の自動化・自律化	 

まとめ: フロントティア AIの脅威に備え・対応するための支援・共助

1 公的支援

- サイバーセキュリティ対策の財政支援(製品・サービス導入や脅威ハンティング・ペネトレーションテスト等のサービス活用支援、レガシーシステム更改に係る投資優遇税制等、下記の共同化支援など)
- 中小企業なども含めたステップバイステップの分かりやすいAI時代の対策マニュアルや工程表・チェックリスト、ベストプラクティス集の策定
- 経営陣、一般社員、メディア、国民全体へのセキュリティに対する啓発活動
- 最新のセキュリティの動向や製品・サービスを踏まえたセキュリティ人材育成
- 中小企業・スタートアップ向けのセキュリティ相談窓口の設置・強化(よろず支援拠点、市町村窓口、国の出先機関等)
- SCS評価制度等の活用促進及び取得支援

※ただし、資格取得自体が目的ではなく、必要な対策の実装・適切な運用が確保されていることが重要であり、下請けいじめ等に繋がらないように留意する必要がある。

また、評価・認証制度の乱立も望ましくなく、海外類似制度との相互認証、制度間の審査項目の統一・流用、関連制度の一括申請・審査等の申請事業者の負担軽減も同時に行っていくべき。

2 公的支援も含めた私的共助等

- ISACに加え業界横断のベストプラクティスの共有、経営陣同士の意見交換・勉強会の実施等
- 上記マニュアル・ベストプラクティス等を踏まえた事業者別のソリューションの整理
- サイバーセキュリティ対策の共同化(企業群や業界、地域等での共同防衛体制の構築・運用によるコスト削減と対策強化の両立)

※例えば、総務省「地方公共団体におけるサイバーセキュリティに関する」援策及び実効性確保の検討に係るワーキンググループ報告書(2026年4月)には、地方版ASMの構築・実施やペネトレーションテストへの支援等が記載。

https://www.soumu.go.jp/main_content/001069311.pdf

Thank You

paloaltonetworks.jp