
accenture
State of Cybersecurity Resilience 2025: Japan
サイバーセキュリティ・レジリエンスの現状 2025（日本）
AI時代の脅威を乗り切るためのサイバーセキュリティ

なぜ今、セキュリティ強化に取組むべきか？

サイバー脅威は、企業が防御策を導入するよりも速く進化しています。

AIにより、攻撃者はかつてないスピードと規模で、レガシーシステムを突破し、セキュリティチームを凌駕しています。従来の防御策ではもはや不十分です。

日本における調査結果

24%

AIが自社のセキュリティ能力を上回っていることを認識しているテクノロジーリーダーの割合

92%

の企業は、AIで拡大するサイバー脅威に対抗できる成熟度を備えていない

82%

の組織は、重要なビジネスモデル、データパイプライン、クラウド・インフラストラクチャを保護する基礎的なデータおよびAIセキュリティ対策がなされていない

出典: サイバーセキュリティレジリエンスレポート 2025
日本: n=166

AIの導入スピードに対するセキュリティの対応状況

日本における調査結果

わずか42%*

AI開発とセキュリティ投資のバランスを取っている組織の割合

わずか25%

ビジネス変革の取組みにセキュリティを組み込んでいる組織の割合

出典: サイバーセキュリティレジリエンスレポート2025; *WEFグローバルセキュリティアウトルック2025（グローバル数値）
日本: n=166

サイバー脅威の状況は、テクノロジーだけでなく、地政学的な要素によっても状況が変化します。

高まる世界の緊張、変化する貿易力学や規制が、サイバーリスクを増大させています。

セキュリティ体制成熟度

日本の現状

求められるセキュリティとのギャップが拡大しており、組織は防御を強化する必要に迫られています。

しかし、組織は壁に直面しています。

日本における調査結果

84%

の組織が、変革目標と合致するサイバーリスクストラテジーの策定、運用に苦慮しています

78%

の組織が、サイバーフィジカルシステム（CPS）：Cyber-Physical System）を効果的に保護できていません

92%

の組織が、変革中にデジタルコア全体を保護する「ゼロトラスト」原則の適用に課題を感じています

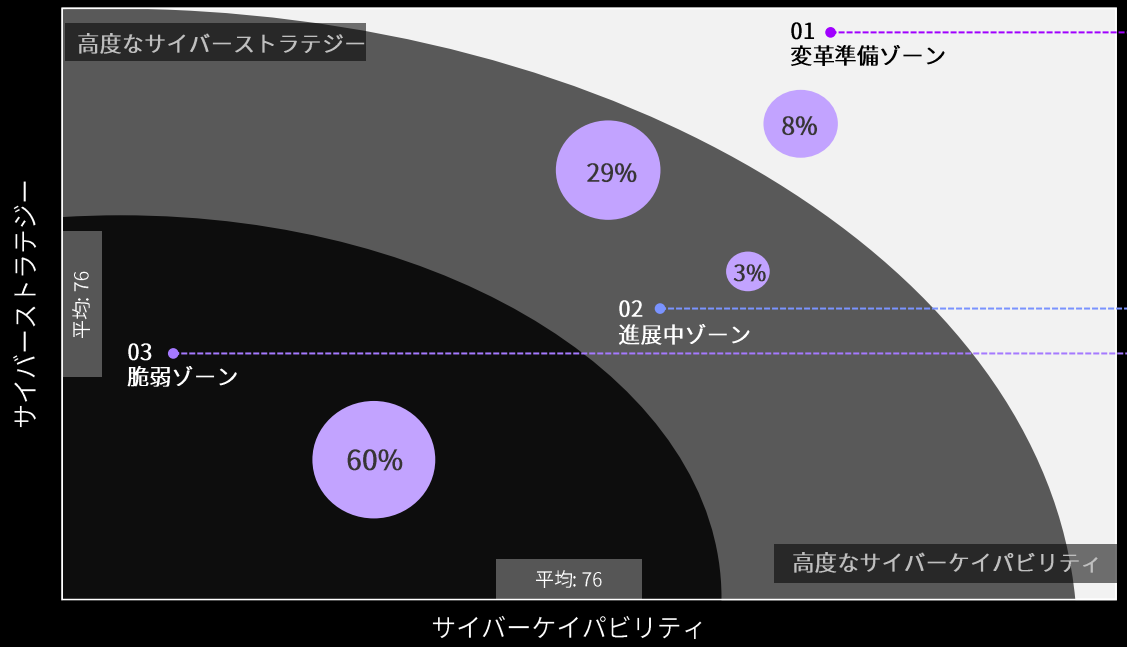
97%

の組織が、防御のストレステスト、新たな脅威の理解、迅速なサイバー攻撃への対応といったレジリエンスの確立に苦戦しています

出典: サイバーセキュリティレジリエンスレポート 2025
日本: n=166

セキュリティ体制成熟度

セキュリティの整備状況をさらに理解するために、「セキュリティ体制成熟度」として３つのカテゴリに分類、定義します。



日本: n=166

カテゴリの分類

01 | 変革準備完了ゾーン

このゾーンの組織は、サイバーセキュリティにおいて主導的な立場にあり、サイバープロテクション、レジリエンス、サイバーフィジカルセキュリティを有しています。同時に、変革を推進し、顧客の信頼を構築するためのリスク戦略を設計し、運用しています。この**適応力と回復力のあるセキュリティ体制は、新たな脅威に対抗するために継続的に進化しています。**

02 | 進展中ゾーン

このゾーンの組織は、**サイバーセキュリティにおいて強みを見せるものの、戦略的な方向性の策定、あるいはセキュリティ防御の実装のいずれかに課題を抱えています。**技術的な防御、すなわちサイバープロテクション、レジリエンス、サイバーフィジカルセキュリティにおいては強みを持つものの、戦略的ビジョンの欠如により、部分的かつ事後対応的なアプローチを取っている組織もあります。また、明確なサイバーセキュリティストラテジーを持つものの、実行力に限りがあり、ビジョンを成果に結びつけられていない組織もあります。サイバープロテクションとストラテジー、いずれかでは優れていても、リスク戦略を効果的に設計し運用するための包括的な能力が不足しています。

03 | 脆弱ゾーン

最も脆弱なカテゴリーです。このカテゴリーの組織は**一貫したサイバーストラテジーと必要なサイバーケイパビリティ共に不足しており、**重大なセキュリティリスクにさらされています。サイバープロテクション、レジリエンス、サイバーフィジカルセキュリティいずれにおいても不十分であり、変革の推進、顧客の信頼を築くためのリスク戦略を設計し、運用する能力が欠如しています。

「変革準備完了ゾーン」の優位性

調査によると、「変革準備完了ゾーン」にある企業は、大きな優位性を示しています。

「脆弱ゾーン」にある企業との比較

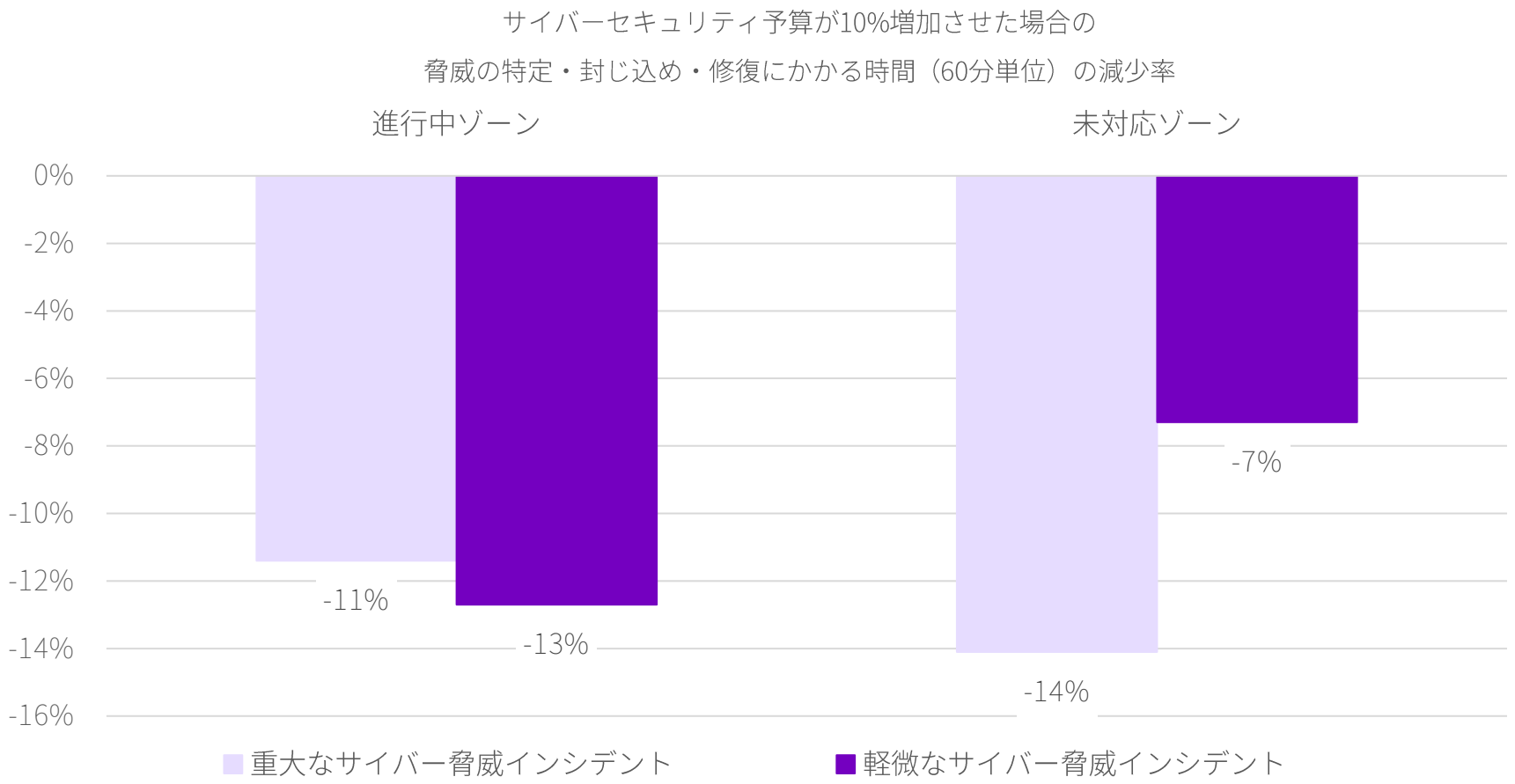
セキュリティ視点の効果

- AIを活用したサイバー攻撃など
  高度な攻撃を受ける可能性が69%低い
- 攻撃を阻止する成功率が1.5倍高い

セキュリティ以外の効果

- 顧客の信頼が1.6倍向上
- セキュリティ対策の改善により、
  技術的負債削減の規模が1.5倍に拡大

「脆弱ゾーン」の企業は、セキュリティ体制強化へ投資を増やすことで、大小の幅広い脅威に対してレジリエンスを強化できます。



重大なサイバー脅威インシデントの特定、封じ込め、修復にかかる時間の短縮において、サイバーセキュリティ予算を増やすことで大幅な改善が期待されるのは、「**未対応ゾーン**」の企業です。予算が10%増加するごとに、対処に要する時間が約28時間短縮されると見込まれています。

一方、軽微な影響のインシデントの場合、サイバーセキュリティ予算の増加で、改善が最も期待されるのは「進行中ゾーン」の企業です。

出典: サイバーセキュリティレジリエンスレポート2025

変革の一歩を踏み出しましょう

企業は、AIへの投資を確保し、AIを最大限活用するために4つの重要なアクションを取る必要があります。

01

目的に即したセキュリティガバナンスフレームワークと運用モデルの構築・導入する

02

企画段階から生成AI対応のセキュアなものとして、デジタルコアを設計する

03

強固な基盤とプロアクティブな脅威管理により、回復力のあるAIシステムを維持する

04

生成AIでサイバーセキュリティを再構築する：自動化、リスクの早期検知、防御の強化

出典: サイバーセキュリティレジリエンスレポート 2025

AIトランスフォーメーションへのセキュリティ導入による成長・信頼構築・レジリエンス維持の実現

「変革準備完了ゾーン」は既に実現可能ですが、一方で、さらなる実践が必要です。

セキュアなガバナンスフレームワークの採用、レジリエントなAIシステムの構築、生成AIの活用、そしてAI開発のあらゆるプロセスにセキュリティを組み込むことで、企業はセキュリティギャップを埋めることができます。

その結果、サイバー脅威が加速する時代を自信を持って乗り切ることができます。

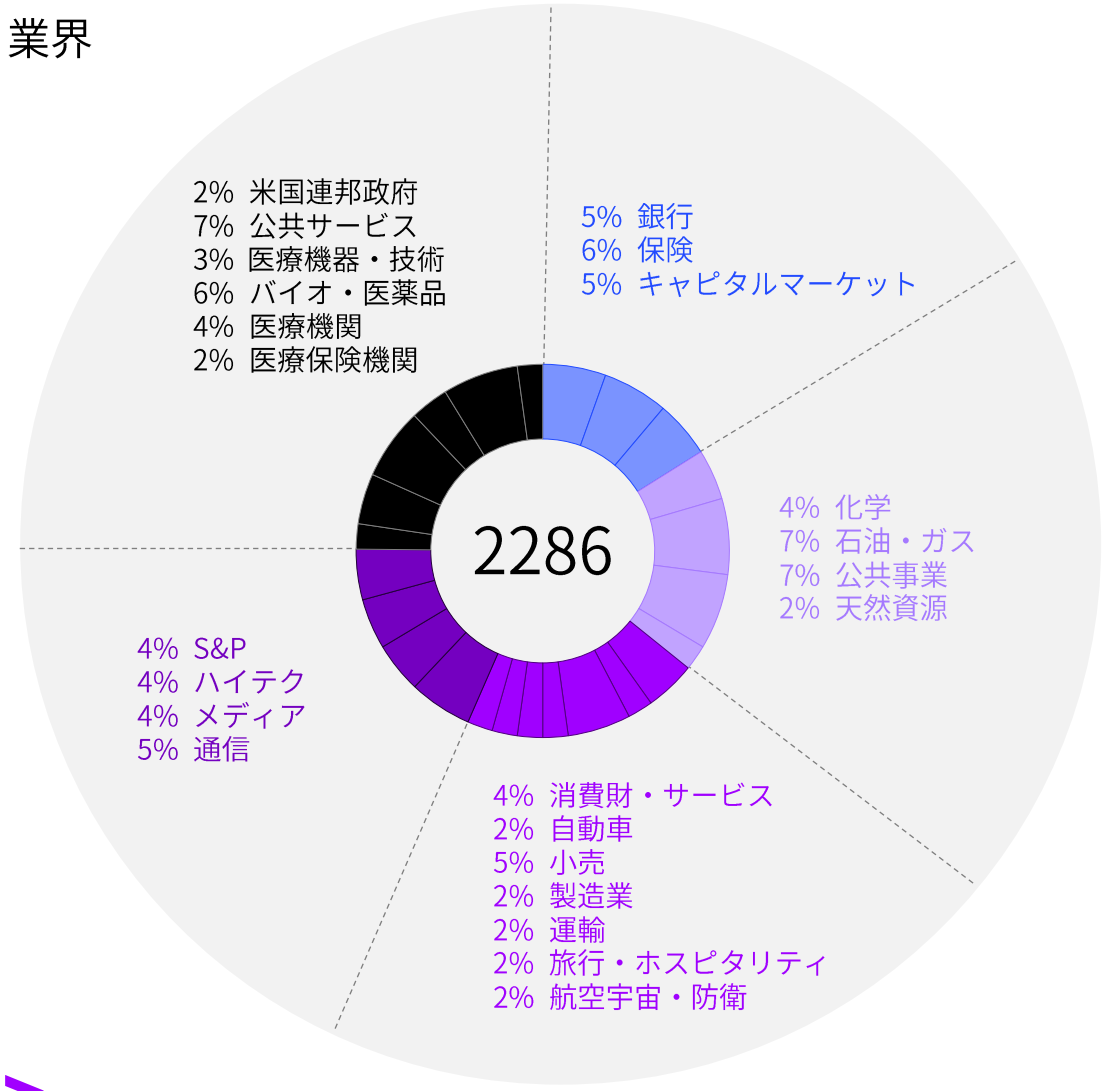
進むべき道は明確です—

セキュリティは単なる保護手段ではありません。
イノベーション、信頼そして長期的な成功を戦略的に実現する要素です。

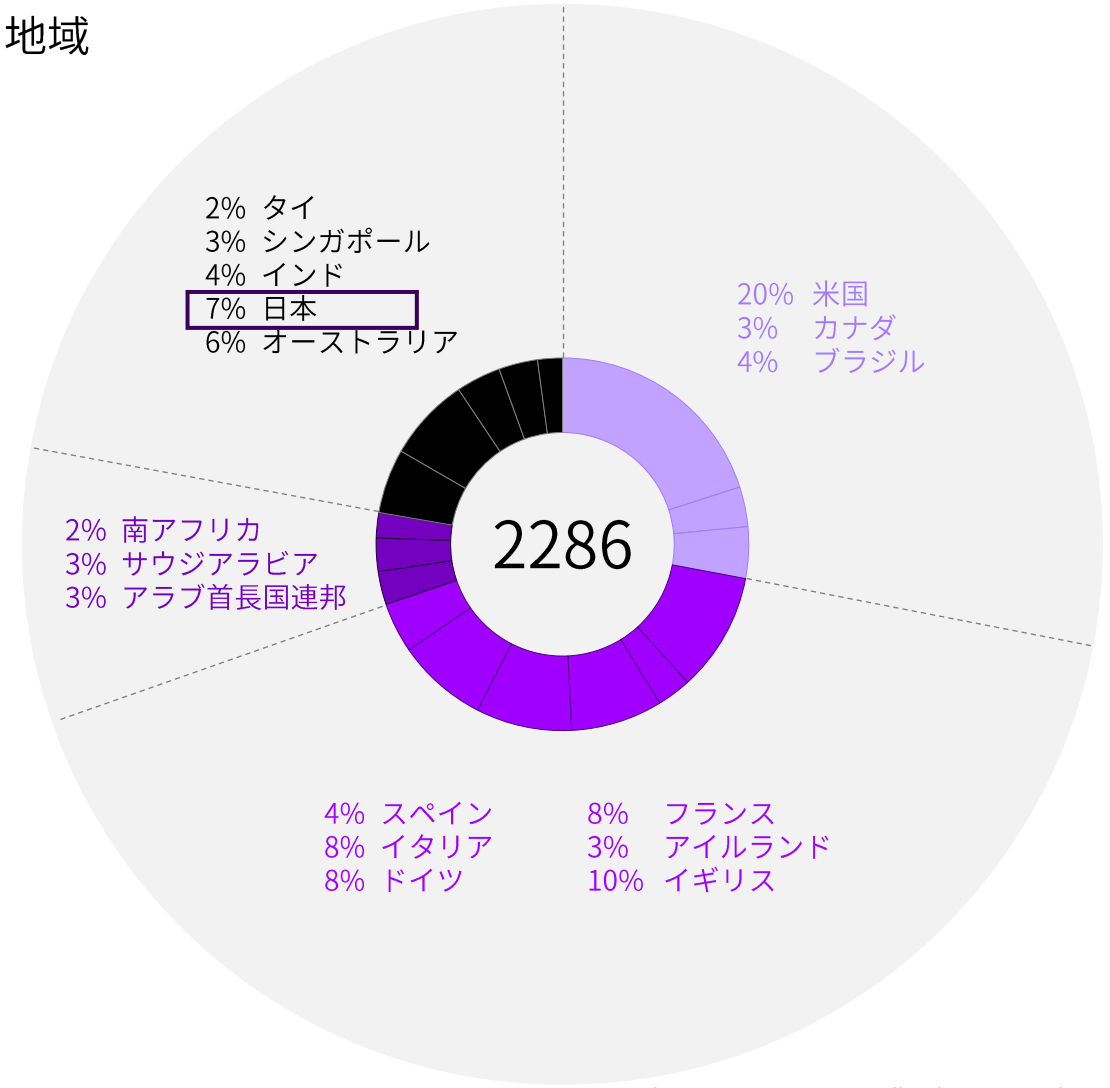
調査について

領域別統計

業界



地域



セキュリティ体制成熟度：アプローチと手法

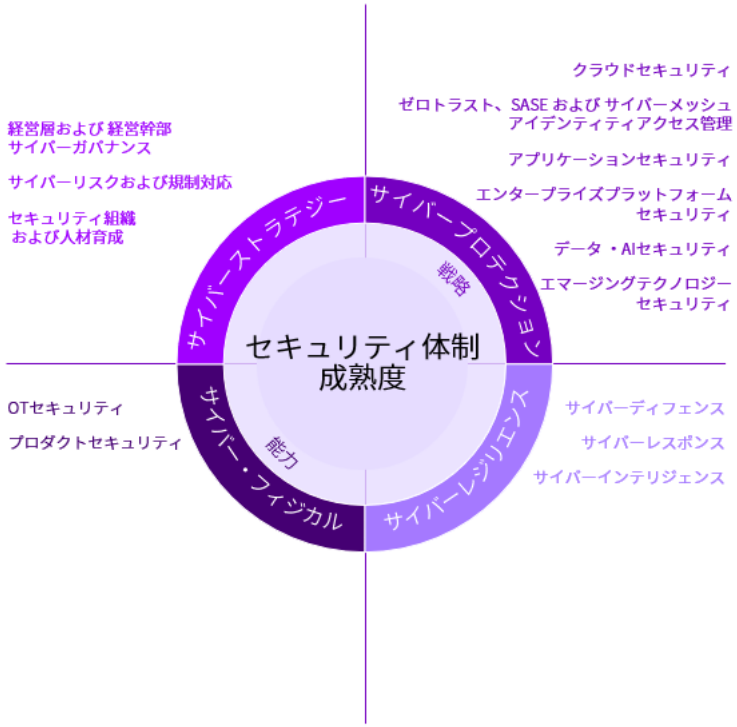
アプローチ：

1. 戦略

- サイバーストラテジー：
  変革を保護・加速し、顧客の信頼を築くためのサイバーリスクストラテジーの設計と運用

2. 能力

- サイバープロテクション：
  ゼロトラスト原則を適用したデジタルコア全体を保護することで、変革中のビジネスの保護を実現
- サイバーレジリエンス：
  防御のストレステスト、新たな脅威の理解、攻撃への迅速な準備と対応
- サイバーフィジカルセキュリティ：
  産業用制御システムとコネクテッド製品のライフサイクルの一貫した保護、それによる運用上の信頼性と完全性の保護



手法：

発見：ベストプラクティスの開発
- AIを活用した実証文献のレビュー
- 社内外専門家へのインタビュー
- ハイパフォーマンス組織との自社の協業経験の活用

デザイン：
- 企業のセキュリティ成熟度を測定、ベンチマーク、評価するため「**セキュリティ体制成熟度フレームワーク**」を設計
- サイバー戦略、サイバープロテクション、レジリエンス、サイバーフィジカルセキュリティの４つの領域で94の実践項目を設定

詳述：
- サイバーセキュリティ成熟度の２つの側面から2,286社の企業を分析し、採点方法に基づいて各企業を「変革準備完了ゾーン」、「進展中ゾーン」、「脆弱ゾーン」の３つの領域に分類

検証：
- 複数の計量経済モデルを開発し、**セキュリティおよび顧客信頼度などのセキュリティ以外のパフォーマンス指標**を各ゾーンに当てはめる
- その結果、「変革準備完了ゾーン」の項目を実践する組織は、セキュリティおよびセキュリティ以外のどの指標においても優れているという**正の相関性**が示された

Thank you