

スポットライト： 日本

セキュリティの新局面を乗り切る：
アジア太平洋地域サイバーセキュリティ対策準備
状況調査



複雑で進化す るセキュリティ 脅威



30%

がデータ侵害を経験しており、
そのうち

79%

が過去12か月間に
頻度が増加したと
回答



サイバーセキュリ ティは引き続き 最優先事項

79%

の回答者が

10%

10%以上のIT予算を
サイバーセキュリティ
に費やしていると報告



主な攻撃ベクトル：

59%

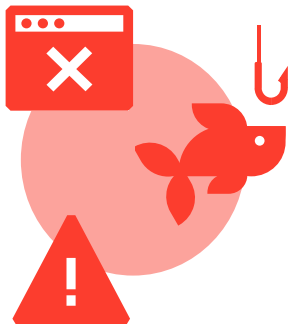
Web攻撃

43%

フィッシング攻撃

43%

マルウェア



サイバーセキュリティの最優先事項：

36%

サイバー攻撃に対
する防御

32%

顧客との通信内容
とデータの保護

28%

組織のネットワーク
とデータの保護



サイバーセキュリティアーキテクチャの重要課題：

限られた予算でのレガシーハードウェアの代替

39%

攻撃対象領域の可視性の欠如

30%

実用的データによる自社環境の可視化

28%

WAFとWANのセキュリティポリシーの一貫性欠如

28%

AIによって変化したサイバーセキュリティ情勢

90%

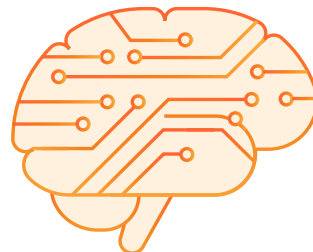
の人がAIによる侵害
の高度化と深刻化を
懸念している

58%

の人がAIを活用す
ることで脅威アク
ターの先手を打つ
ことができると考
えている

73%

の人が、自社はAI
によるデータ侵害
をある程度防ぐ準
備ができていると
考えている



ランサムウェアは明白で切迫した危険

58% 

パッチ未適用の脆弱性を悪用する攻撃が最も一般的な侵入手段と回答

31% 

過去24か月間に身代金を支払ったことがあると回答

38% 

身代金を支払うことになった最大の理由はシステム復旧を求める顧客からの圧力と回答

データ侵害の被害が増大



51%

過去12か月間のデータ侵害による損失合計は100万米ドル超と回答

ゼロトラストは重要事項として定着



42%

の組織が現在ゼロトラストソリューションに投資している

41%

の組織が今後12か月間にゼロトラストへの投資をする予定である

規制コンプライアンスの維持にメリット有



42%

42%の組織が

5%

以上のIT予算を規制/コンプライアンス要件への対応に費やしていると回答

最も広く導入されているゼロトラストソリューション：

72%

データ暗号化

71%

多要素認証

71%

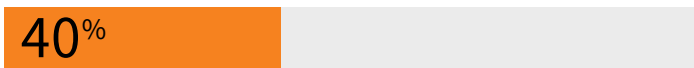
ゼロトラストネットワークアクセス (ZTNA)

コンプライアンスへの投資の主な効果：

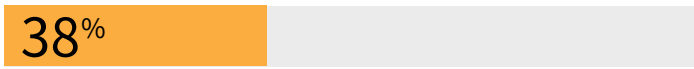
プライバシー/セキュリティの向上



テクノロジーとデータの完全性の向上



評判とブランドの向上



調査方法：上記は、14市場、主要業界、従業員250~2,500名以上の規模の組織でサイバーセキュリティを担当するリーダー3,844名を対象として2024年6月に実施されたダブルブラインド方式調査の結果に基づいています。

レポート全文はこちら：

