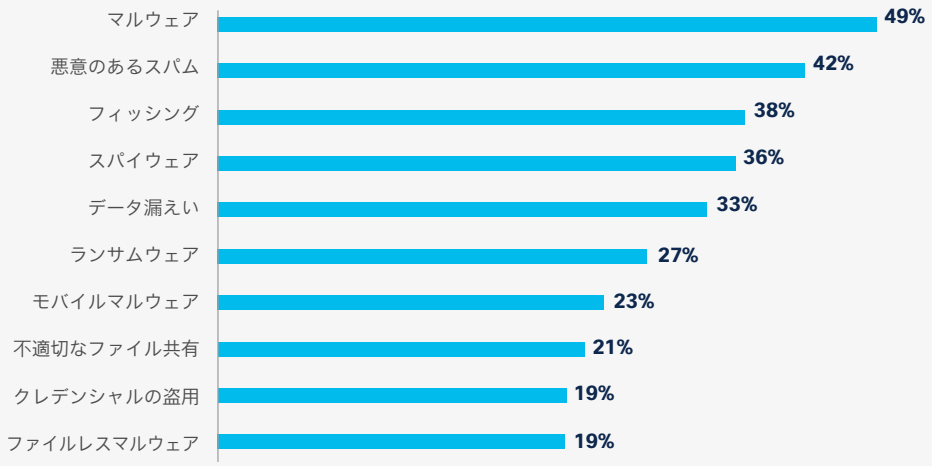
デバイス、接続、ネットワーク、データの保護

サイバーセキュリティは、ビジネスや個人のオンライン活動のためにインターネットを使用するすべての人にとって最優先事項です。デジタル資産の保護には、拡大し続けるデジタル環境も含まれます。2018 年に 184 億台であった全世界のネットワーク接続されたデバイスは、2023 年までに 293 億台に達すると予測されています（出典：Cisco Annual Internet Report, 2018–2023）。これらの接続の約半分が、幅広い Internet of Things（IoT）アプリケーションをサポートするようになります（2018 年の 61 億から 2023 年までに 147 億に増加）。従業員のデバイス、IoT 接続、インフラストラクチャ、専有データを保護するには、実用的な分析情報と拡張性の高いソリューションが必要です。また、不正なイベントが発生した際に、侵害をすばやく特定して修復するための適切なパートナーも必要になります。

過去 1 年間に遭遇したセキュリティインシデントおよび攻撃の種類

シスコの 2019 年度最高情報セキュリティ責任者ベンチマーク調査によると、セキュリティ問題の上位 3 件のうち 2 件は電子メールのセキュリティに関するものでした。Microsoft Office 365 への移行に向けて保護に投資している場合や、Domain-based Message Authentication、Reporting and Conformance（DMARC）を使用してビジネス電子メール詐欺（BEC）からの保護を図っている場合でも、電子 メールが依然として一番の脅威媒体であることに変わりありません。上位 10 件の攻撃のうち 2 件が内部関係者による脅威の問題（ファイル共有とログイン情報の盗用）であるという事実から、外部と同じように内部で起こっていることにも注意を払わなければならないことがわかります。システムを破って侵入するのではなく、ログインして内部に入ってくる攻撃者もいるのです。

企業のセキュリティに関する主な問題



出典：未知の脅威に先手を打つ：CISO ベンチマーク調査、シスコ、2019 年 3 月。
[回答者の割合、N = 2,909]

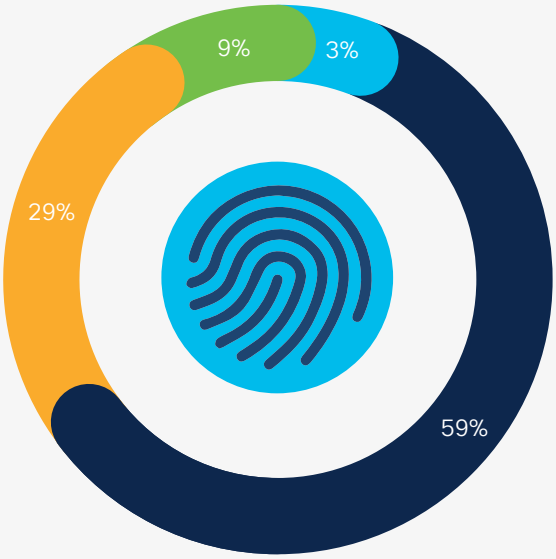
推奨されるアクション

今日のセキュリティ問題から、より優れた多要素認証（MFA）の必要性が明らかになりました。セキュリティポリシーは、データ保護と使いやすさの最適なバランスを実現する必要があります。効果的なサイバーセキュリティ アプローチは、適切なユーザにアクセスを与えつつも、権限を持つユーザのエクスペリエンスを損なわないようにする必要があります。

現在の一般データ保護規則（GDPR）への準拠

シスコの 2019 年度データ プライバシー ベンチマーク調査によると、世界の企業の 59% が現在の GDPR の要件のすべてまたは大部分に対応していると回答しました。また 1 年以内に対応する予定と回答した割合も 29% に達しましたが、9% は対応に 1 年以上を要すると回答しています。GDPR は、EU に拠点を置く企業、または EU に拠点を置く個人に関して収集された個人データの処理に適用されますが、シスコのグローバル調査で自らの組織には GDPR が適用されないと述べた割合はわずか 3% でした。

GDPR コンプライアンス



- 現時点で GDPR の要件の大部分、またはすべてに対応している
- まだ GDPR の要件の大部分、またはすべてに対応しておらず、対応するまでに 1 年以上かかる予定
- まだ GDPR の要件の大部分、またはすべてに対応していないが、1 年以内に対応する予定
- 該当なし：GDPR は適用されない

出典：データプライバシーへの投資価値を最大化する、シスコ、2019 年 1 月。
[回答者の割合：N = 3,206]

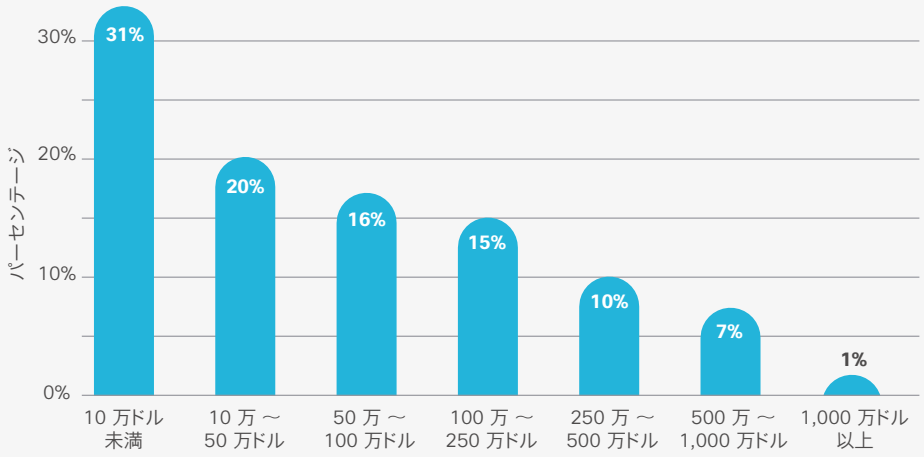
推奨されるアクション

GDPR に対応する上での主な課題としては、データセキュリティ、従業員のトレーニング、拡大する規制への対応が挙げられました。データプライバシーは多くの組織で経営に関わる問題となり、顧客はベンダーやパートナーとビジネスを始める前に、プライバシーに関する懸念に対して適切に対応できるかどうかを確認しています。

過去 1 年間に組織が受けたセキュリティ侵害中の財務的損失の最高額

財務的損失、ブランドの評価の低下や崩壊、株主の信頼への影響、貴重なデータの損失、法規制およびコンプライアンス違反の罰金など、侵害が招きうる結果は誰もが認識しています。明らかに、印象や情緒的な問題にシフトしています。オペレーションの継続はもちろん重要ですが、カスタマーエクスペリエンスとブランド評価もまた、サイバーセキュリティ問題に付随する重大な懸念事項です。

重大なセキュリティ侵害による財務上の影響



出典 : 未知の脅威に先手を打つ : CISO ベンチマーク調査、シスコ、2019 年 3 月。
[回答者の割合 : N = 2,386]

推奨されるアクション

組織内のすべての従業員、特にセキュリティに関わる従業員は、インシデント対応に精通している必要があります。残念ながら、シスコの調査回答者のうち、セキュリティ侵害を受けた後にやることを把握していると回答したのはわずか 75% でした。トレーニングが不可欠であることを、あらゆる組織のサイバーセキュリティ計画においてさらに強調する必要があります。

シスコは、サイバーセキュリティ戦略と戦術計画の構築と強化を支援します。

より詳細な情報は、Cisco Annual Internet Report にてご覧いただけます。

- シスコ サイバーセキュリティ レポート シリーズを読む。
- シスコの包括的なセキュリティ ソリューションについて読む。