imperva

2023年サイバー脅威防御レポート

ITセキュリティ専門家が現在最も懸念している サイバー脅威とは？ 2023年の最優先セキュリティ技術とは？

CyberEdge Groupは世界中のITセキュリティに関する意思決定者と実務経験者1,200名を対象に調査を実施し、直面している課題やアプリケーションとデータ保護に関するさまざまな技術の評価に関する知見をお届けしています。

重要なポイント：

Webおよびモバイル攻撃が主な懸案事項です。 このカテゴリーで上位に挙げられた3つの脅威は、個人情報漏洩、乗っ取り（ATO）、カード処理と決済の不正行為による攻撃です。

API保護が現時点における最大の問題です。 クラウドアプリケーションへの移行が進みつつある状況から、60%以上の企業がAPIゲートウェイまたはAPI保護ソリューションを導入済みです。

ボット管理に注目が集まっています。 調査の対象となったアプリケーションおよびデータセキュリティ技術の中で、導入を予定している企業が最も多いものは、ボット管理です。

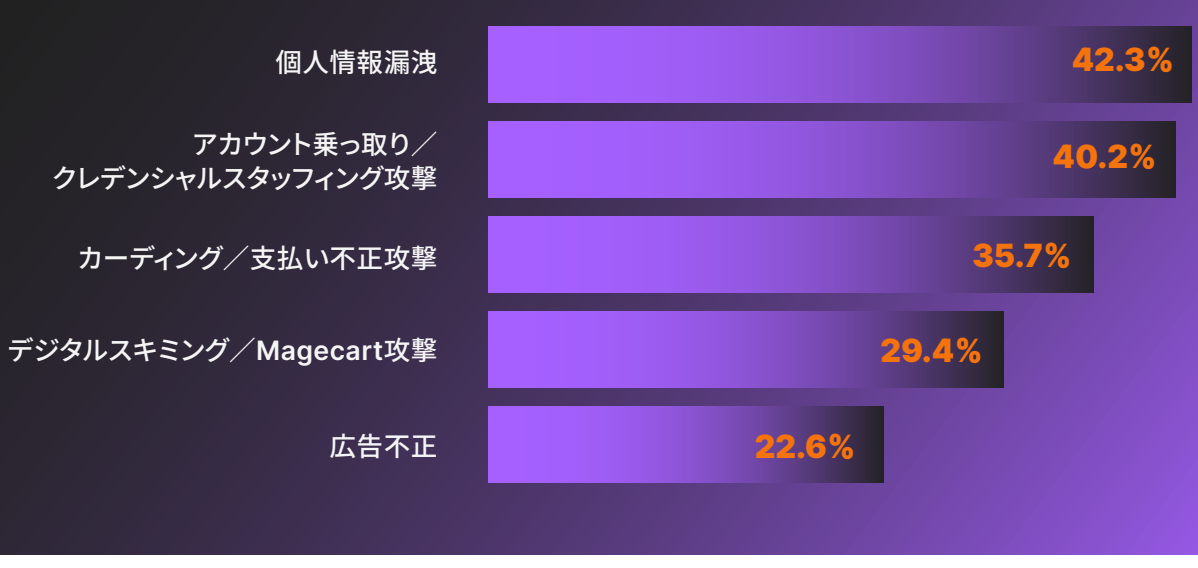
ITセキュリティ専門家は、アプリケーションとデータのセキュリティ技術を一元化するプラットフォームの利点を認めています。 クラウドセキュリティ態勢の改善、インシデント調査能力の強化、セキュリティルール管理の簡素化などの利点があります。

ネットワークベースのサイバー脅威

ITセキュリティチームは、最大の懸念事項として次のようなネットワークベースのサイバー脅威を挙げました。

- アカウント乗っ取り／クレデンシャルスタッフィング攻撃
- DoS攻撃
- Webアプリケーション攻撃
- サプライチェーンの脅威

最も懸念すべきWebアプリケーションとモバイルアプリケーションの攻撃



必要不可欠なセキュリティ技術

最も多く導入されているアプリケーションおよびデータセキュリティ技術

- APIゲートウェイ／保護
- データベースファイアウォール
- Webアプリケーションファイアウォール（WAF）

革新的なソリューション

最も多く導入が予定されているアプリケーションセキュリティとデータセキュリティの技術

- ボット管理
- 高度セキュリティアナリティクス
- データアクティビティ監視（DAM）

アプリケーションとデータのセキュリティを一元化する利点

アプリケーションとデータのセキュリティ防御（WAF、DDoS防御、APIセキュリティ、データリスク分析、データベースセキュリティなど）のために一元化されたプラットフォームを活用する最大の利点。

総合的な
デジタルセキュリティ

レポート全文はwww.imperva.com/cdr2023からダウンロードできます

ライセンス先：IMPERVA, INC.

CYBEREDGE GROUP