2022年サイバー脅威防御レポート

エグゼクティブサマリー

プラチナスポンサー

imperva

CyberEdge Groupの第9回年次サイバー脅威防御レポートでは、ITセキュリティの専門家がサイバー脅威をどのように捉えてその防御を計画しているのかについて、洞察力のある視点を示しています。2021年11月に実施された、1,200人のITセキュリティ意思決定者および実務経験者を対象とした調査に基づき、本レポートでは、ITセキュリティチームが自分たちの認識、優先順位、セキュリティ態勢が同業他社と比較してどの程度のレベルにあるのかをより良く理解するために利用できる数多くの洞察を提供しています。

調査対象

- 1,200名のITセキュリティの意思決定者と実務経験者からの回答
- 全員が従業員数500名超の企業に所属
- 北米、欧州、アジア太平洋、中東、中南米、アフリカにわたる17か国が対象
- 19の業界が対象

「5つの利点が回答者の30%以上から挙げられているということは、アプリケーションとデータセキュリティのための統合プラットフォームは、サイバーセキュリティにおいて統合と単一ベンダーによる調達が意味を持つ分野の一つであることを示しています」

– 2022年CDR

注目すべき調査結果

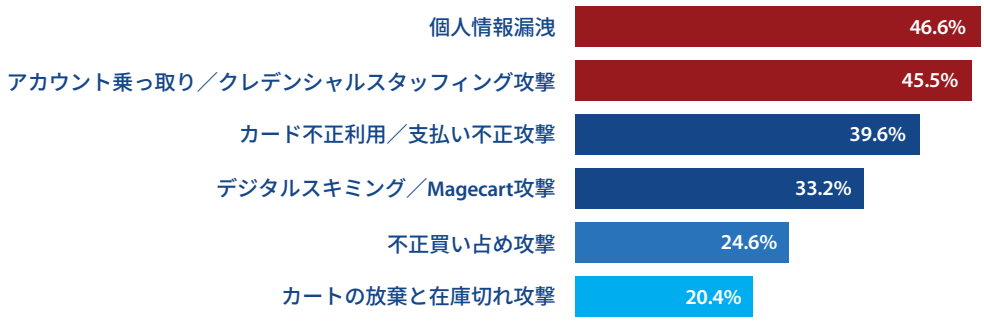
- **ATO攻撃に関する懸念が高まっています。**アカウント乗っ取り（ATO）やクレデンシャルスタッフィング攻撃に関する懸念の水準がこの1年で急上昇しました。調査で追跡しているすべての脅威の中で、マルウェアに続く2位になっています。
- **その他のウェブ攻撃も顕著です。**調査回答者は個人情報漏洩、カード不正利用／支払い不正攻撃、Magecartなどのデジタルスキミング攻撃を挙げました。
- **API保護とWAFが頼みの綱です。**60%以上の企業がAPI保護とWebアプリケーションファイアウォール（WAF）技術をインストールしています。
- **アプリケーションセキュリティとデータセキュリティ技術を統合することで効果が発揮されます。**クラウドセキュリティ体制の改善、インシデント調査の向上、顧客サポート体験の拡充などのメリットを得ることができます。

セキュリティの専門家が危惧する攻撃

ITセキュリティの専門家が最も心配しているネットワークベースの攻撃には、ATOとクレデンシャルスタッフィング攻撃（1〜5段階評価で3.97）、サービス妨害攻撃（3.85）、SQLインジェクションやXSS攻撃といったWebアプリケーション攻撃（3.83）がありました。

Webアプリケーションとモバイルアプリケーションについて最も懸念している攻撃を3つ挙げてもらったところ、回答者の46.6%が個人情報漏洩、45.5%がATOとクレデンシャルスタッフィング攻撃、39.6%がカード不正利用と支払い不正攻撃、33.2%がデジタルスキミングとMagecart攻撃を挙げました。

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



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ための必須技術と新しい技術

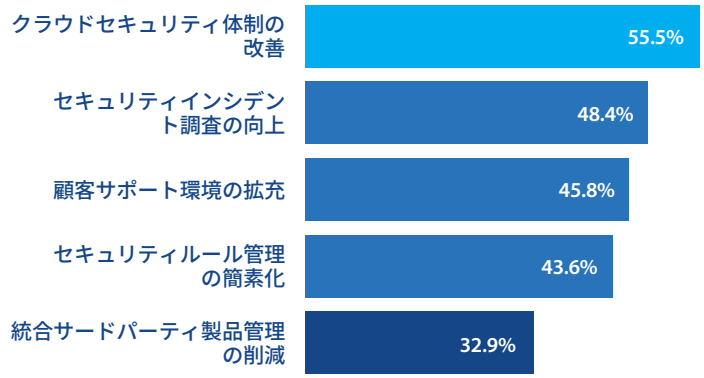
調査対象となった10企業のうちすくなくとも6企業ではAPI保護製品、Webアプリケーションファイアウォール（WAF）、データベースファイアウォールといったものが導入されており、アプリケーションセキュリティとデータセキュリティのための必須技術と考えられていることが伺えます。最も人気の高かった新しい技術（2022年に最も導入が検討されている技術）にはボット管理、高度セキュリティアナリティクス、データベースアクティビティ監視（DAM）が含まれていました。

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

関連技術の調達に関して、セキュリティの専門家は複数のベンダーから調達するか、単一ベンダーの統合ソリューションにするかという選択肢にしばしば直面します。後者を選ぶと、複数の製品を統合するコストや、互換性のない管理・報告ツールを使い複数ベンダーと作業するわずらわしさが減ります。

ところで、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防御を統合することで、具体的にどのようなメリットがあるのでしょうか？調査回答者の半数以上（55.5%）が組織のクラウドセキュリティ体制の改善を挙げました。ほぼ同数の回答者（48.4%）がセキュリティインシデント調査の向上を挙げました。その他の大まかなメリットには、顧客サポートの向上（45.8%）、セキュリティルール管理の簡素化（43.6%）、統合したサードパーティ製品管理の削減（32.9%）が含まれていました。

アプリケーションセキュリティとデータセキュリティ防御を統合して得られるメリット



導入済みおよび導入予定のアプリケーションとデータのセキュリティ技術

	導入済み	導入予定	予定なし
APIゲートウェイ／保護	64.1%	28.6%	7.3%
Webアプリケーションファイアウォール（WAF）	61.1%	29.9%	9.0%
データベースファイアウォール	59.5%	30.5%	10.0%
アプリケーションコンテナセキュリティツール／プラットフォーム	54.3%	36.5%	9.2%
クラウドアクセスセキュリティブローカー（CASB）	53.3%	33.2%	13.5%
データベースアクティビティ監視（DAM）	53.1%	35.9%	11.0%
アプリケーションデリバリコントローラー（ADC）	52.2%	33.6%	14.2%
ランタイムアプリケーション自己防衛（RASP）	50.4%	35.1%	14.5%
ファイル整合性監視／アクティビティ監視（FIM／FAM）	50.2%	37.8%	12.0%
高度セキュリティアナリティクス（機械学習やAIによるものなど）	50.2%	39.7%	10.1%
静的／動的／対話型アプリケーションセキュリティテスト（SAST／DAST／IAST）	48.0%	38.2%	13.8%
ボット管理	42.6%	39.8%	17.6%

無料レポート

http://www.imperva.com/ja/cdr2022から2022年サイバー脅威防御レポートの全文をダウンロードできます

Impervaについて

Impervaは、データとそこに至るすべてのパスの保護をミッションに掲げるサイバーセキュリティのリーダーです。デジタルトランスフォーメーションのあらゆる段階を通じて、世界6,000以上の顧客のデータをサイバー攻撃から保護しています。当社の製品はグローバルな脅威インテリジェンスコミュニティであるImperva Research Labからの情報をもとにしており、ここから最新のセキュリティとコンプライアンスに関する専門知識をソリューションに提供しています。

CYBEREDGE GROUP

CyberEdge Groupについて

CyberEdge Groupは、情報セキュリティベンダーとサービスプロバイダーのニーズに応える、受賞歴を持つリサーチ、マーケティング、および出版の企業です。当社の熟練したコンサルタントは、収益増加、競合他社に打ち勝ち、および販売サイクルの短期化を実現する上で欠かせない優位性を、お客様にお届けします。詳しくは、当社のWebサイトwww.cyber-edge.comをご覧ください。