2021 年 6 月 22 日
タレス DIS CPL ジャパン株式会社

ご参考資料

2021 年タレス・グローバル・データ脅威レポート
日本に関する主要な調査結果

2021 年タレス・グローバル・データ脅威レポートは、オーストラリア、ブラジル、フランス、ドイツ、香港、インド、日本、メキシコ、オランダ、ニュージーランド、シンガポール、韓国、スウェーデン、アラブ首長国連邦、英国、米国の主要業界に従事する、IT とデータ・セキュリティに責任や影響力を持つ経営幹部 2,600 人以上を対象に実施されました。なお、日本の回答者は 201 人です。本資料では、日本において、マルチクラウド環境でのデータ利用が進んでいる実態やクラウド上のデータ管理の現状、また今後のセキュリティ対策の方向性について紹介します。

■マルチクラウド利用の浸透とリスクの露呈

- 日本の組織の 6 割以上（63%）が、自社のデータの 40%以上が外部のクラウド環境に保管されていると回答しています。
- 日本の組織の 20%は現在、50 個を超える SaaS（Software as a Service）アプリを使用していると回答しています。
- 日本の組織の 43%が 2 つの PaaS（Platform as a Services）プロバイダーを使用していると回答しています。
- クラウドに保管されているデータのうち、40%超が機密データにあたると回答した日本の組織の割合は 54%でした。にもかかわらず、78%と約 8 割の日本の組織が、クラウドに保存してある機密データの半分も暗号化していないことがわかりました。
- 自社のデータがどこに保存されているのか完全に把握していると回答した日本の割合は、26%にとどまっています。
- 日本の組織の 30%が、過去 1 年間において、クラウドに保存されているデータおよびアプリケーションに関わる侵害を受けた、または、監査に通らなかったと回答しています。

■コロナ禍の影響と最近の脅威動向

- 日本の組織の 50%が、自社のセキュリティ・インフラ環境は Covid-19 がもたらすリスクに対応できる態勢にないと回答しています。かなりの準備態勢が整っていると考えている日本の組織は、16%にとどまっています。
- 日本の組織の 82%が、リモートで働く従業員のセキュリティ・リスクを懸念していると回答しています。
- 日本の組織の 39%が過去 12 か月に侵害を経験したと回答しています。
- 日本の組織の 38%が過去 12 か月にサイバー攻撃の数、重篤度、範囲が増加したという認識を持っています。
- 増加がみられる攻撃について、日本の回答者は、マルウェア（51%）、ランサムウェア（45%）、フィッシング（45%）を上位 3 つに挙げています。

2021 年 6 月 22 日
タレス DIS CPL ジャパン株式会社

■セキュリティ投資のトレンド

- 日本の組織の 42%が公式にゼロトラスト戦略を持っていると回答しました。**この数字は全世界の平均（30%）よりも 10 ポイント以上高い結果となっています。**
- 日本の組織の 77%が、クラウドセキュリティ戦略を形成するために、ゼロトラストセキュリティの概念を採用していると回答しています。
- パンデミック中に投資した先進的技術として日本の回答者に多く挙げられていたのは、1 位ゼロトラスト・ネットワーク・アクセス（ZTNA）／ソフトウェア定義ペリメーター（SDP）（43%）、2 位クラウドベースアクセス管理（41%）、3 位条件つきアクセス（36%）でした。
- サイバー攻撃から機密データを守るうえで最も効果的なテクノロジーとして日本の回答者に多く挙げられていたのは、1 位暗号化（43%）、2 位ネットワークセキュリティ（41%）、3 位データ検出と分類（37%）でした。

調査について

本調査は 2021 年 1 月から 2 月に実施されました。調査対象組織は幅広い業界にわたり、医療、金融サービス、小売、テクノロジー、政府機関に重点が置かれています。職位は、CEO、CFO、最高データ責任者、CISO、最高データサイエンティスト、最高リスク責任者の C レベル幹部から、SVP や VP、IT アドミニストレーター、セキュリティアナリスト、セキュリティエンジニア、システムアドミニストレーターにわたっています。回答者の組織規模は幅広く、多くの組織の従業員数は 500 人から 1 万人です。