2023 サイバーセキュリティ グローバル調査

新型コロナウイルス流行の影響 により 日本のITセキュリティ環境の抜本的な立て直しは今でも続いています。過去12ヵ月間の調査結果からは、日本企業が直面したサイバー攻撃の種類、対応方法、2023年の最優先事項が明らかになりました。

26%
過去1年間に少なくとも1回はデータ侵害の被害に遭った日本企業の割合

¥460 百万
侵害を受けた企業の損失額の平均

97
過去1年間にあったサイバー攻撃の1社あたりの平均回数

- **38** メール/フィッシン
- **14** ランサムウェア
- **13** ネットワーク
- **11** クラウ
- **9** アプリケーション
- **7** デバイス / エンドポイント
- **5** サードパーティ/サプライチェーン

新型コロナウイルス発生直後の日本企業の対応

- **39%** リモートワーカーをサポートするためにデジタルトランスフォーメーションを加速した
- **36%** 従業員や顧客のサポートを強化するための対策はとらなかった
- **24%** 顧客からの問い合わせページのサポートを強化した

サイバー攻撃対策でのDNSの使用

日本企業がセキュリティ戦略でDNSをどのように活用したか

- **41%** 不正な宛先へのDNSリクエストを阻止し境界防御の負担を軽減した
- **35%** 不正な宛先に接続しているデバイスにフラグを立てた
- **32%** DNSトンネリングとDGAに対する保護対策をとった

最大の課題

1. ITセキュリティスキルの不足
2. 予算不足
3. リモートワーカーのアクセスを監視

今後12ヵ月間の最も緊急性の高い脅威

- **57%** データ漏えい
- **50%** ランサムウェア
- **33%** リモートワークのネットワーク接続を悪用した攻撃

「リモートワーカーの増加により、セキュリティが低下する恐れがあります

–日系テクノロジー企業課長

> レポート全文を入手する

来年に向けて検討すべきサイバーセキュリティに関する重要な問題と優先事項は 2023年サイバーセキュリティ グローバル調査(日本)でご覧いただけます。

この調査はInfobloxが出資により、CyberRisk Allianceが実施しています。