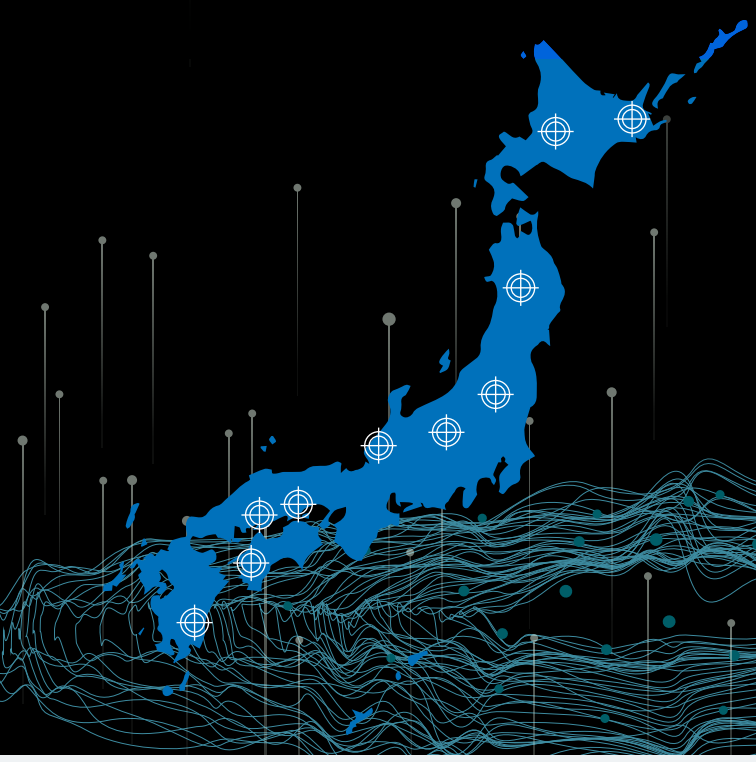
Microsoft

マイクロソフト セキュリティ インテリジェンス レポート:

日本のサイバー攻撃の現状



サイバー攻撃の数が増え、巧妙さが増す中、日本でもインターネットを利用する個人や組織は、発生数の多いサイバー攻撃への理解を深め、その影響を最小限に抑えるための対策を取ることが急務となっています。

こうした進化を続けるサイバー攻撃の現状を、個人や企業の皆様にとって理解しやすくするために、マイクロソフトは**セキュリティ インテリジェンス レポート (SIR)** 第 24 版を作成しました。SIR は Microsoft クラウドを経由する 1 日 6.5 兆件の脅威シグナルの分析結果と世界中のセキュリティ研究者やレスポンダーから得た研究成果と実例を基にしています (集計期間: 2018 年 1 月～ 12 月)。

日本におけるサイバー攻撃トップ 4

マルウェア

マルウェアには個人や企業にとって、ユーザビリティの低下、データ損失、知的財産の盗難、金銭的損失、精神的苦痛といったさまざまな悪影響を与えるリスクがあります。

▼**70%** **世界**の平均値との比較

▼**78%** **アジア太平洋地域**の平均値との比較

仮想通貨のマイニング

不正な利益を得ることを目的に、攻撃者がマルウェアを利用して被害者のコンピューター経由で仮想通貨のマイニングを行うケースが増えています。

▼**83%** **世界**の平均値との比較

▼**86%** **アジア太平洋地域**の平均値との比較

ランサムウェア

日本では個人や組織によるランサムウェアへの対応は合理化されつつありますが、依然として大きな脅威であることに変わりはありません。

▼**80%** **世界**の平均値との比較

▼**86%** **アジア太平洋地域**の平均値との比較

ドライブ バイ ダウンロード

攻撃者が Web ページの脆弱性を悪用して不正なサイトにユーザーを誘導し、ウイルスに感染させようとします。何もダウンロードしていなくても、気づかないうちに感染している可能性もあります。

▼**89%** **世界**の平均値との比較

▼**91%** **アジア太平洋地域**の平均値との比較

サイバー セキュリティのベスト プラクティス

組織向け

1. **予防:** 予防策を講じることで、サイバー犯罪者が負担する攻撃コストが増えるため、低コストで効果的なタイプのサイバー攻撃を阻止できます。

   - **クラウド バックアップ:** クラウド ストレージ サービスを導入し、重要なデータが自動でバックアップされるようにする
   - **アクセス制御:** ネットワークをセグメント化する。アプリへのアクセス許可時に警告を表示する
   - **サイバーセキュリティ研修:** 従業員にサイバー攻撃に関する研修を行い、堅牢な IT ポリシーを維持する

2. **検出と対応:** クラウド テクノロジを活用して攻撃者によるデータ アクセスを制限しセキュリティ運用部門が攻撃により的確に対応できるようにします。

個人向け

1. **サイバー衛生:** ウイルス対策ソリューションを使用して、ソフトウェアやオペレーティングシステムが常に最新の状態に維持されるようにします。

2. **正規ソフトウェア:** 海賊版ソフトウェアの使用を避け、信頼できる発行元のソフトウェアのみを使用するようにします。
3. **パスワード管理:** アカウントごとに個別の強力なパスワードを使用し定期的に変更するようにします。

4. **個人ファイルのバックアップ:** 写真などの重要な個人データは、信頼できるクラウド ストレージ プラットフォームにバックアップするようにします。
5. **常に警戒:** 個人情報を扱うやり取りには、ユーザー本人のデバイスを使用し、信頼できるネットワーク上でのみ行うようにします。

マイクロソフト セキュリティ インテリジェンス レポート第 24 版の全文は **https://www.microsoft.com/sir** (英語) で入手できます。