# 2020

# SONICWALL
# サイバー脅威レポート

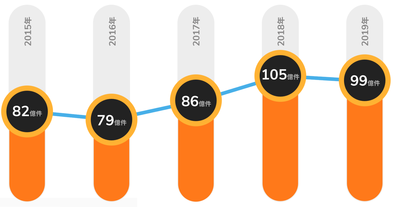
デジタルの世界では境界は無限です。かつては限られており防御可能なスペースであったものが、今、デバイス、アプリ、アプライアンス、サーバー、ネットワーク、クラウド、ユーザーの広域にわたるフットプリントから成る無限の領域となっています。

**サイバー犯罪者の考え方をより良く理解し、次に行われることに十分備えるために、SonicWallだけが提供可能な脅威インテリジェンスをご確認ください。**

## マルウェアは低減したが、標的化と回避が増加

## 99億件

マルウェア攻撃は2019年にSonicWallにより記録されたもので*、2018年の記録的な105.2億件から6%減少しています。




## ランサムウェアが新しい標的を発見

## 1億8,790万件

所有している機密データや資金（またはその両方）を奪い、その引き換えに金銭を支払う可能性がある被害者を巧みに狙うランサムウェアが利用されています。

2019年には、1億8,790万件のランサムウェア攻撃の多くが州政府や地方自治体、および教育システムに対して行われています。

## クリプトジャックの崩壊

ビットコインの価格や補完的な暗号通貨は、Coinhiveベースのクリプトジャック・マルウェアと正当なCoinhiveマイニング・サービスの間にどうしようもない状況を生み出しました。

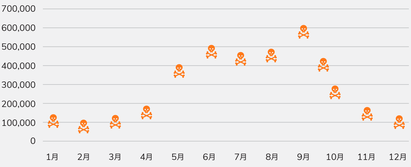
## 78%↓

Coinhiveの終了後、2019の後半に、クリプトジャックの件数は78%減少しました。

## 第3四半期、ファイルレスマルウェアがピークに

ファイルレスマルウェアはメモリベースのアーティファクトとしてのみ存在し、コンピュータのハードドライブにアクティビティを書き込まないため、既存のコンピュータのフォレンジック分析がうまく働きません。その件数は第3四半期にピークを迎え、SonicWallは2019年9月だけで57万以上の攻撃を記録しました。

**2019年のファイルレスマルウェアの件数**




## 暗号化された脅威が衰えることなく継続的に増加

巧妙なサイバー犯罪者は、従来のセキュリティ制御による検査から攻撃を隠すために、TLS/SSL暗号化の使用を続けています。2019年、SonicWall Capture Labsの脅威研究者は、TLS/SSLトラフィック経由で送信されるマルウェアの前年比27.3%増を記録しました。

## 27%↑

2019年にTLS/SSLトラフィック経由で送信されるマルウェアは27%増加。

## IOT攻撃の件数が増加

2019年、SonicWallは、IoTマルウェアの5%の増加と総攻撃数が3,430万件に達したことを発見しました。

しかし、おびただしい数のIoTデバイスが新たに毎日接続されていることから、IoTマルウェア攻撃の増加を見込むだけにとどまらず、それに対する計画が必要とされます。

## 3,430↑
## 万件

## 次なる攻撃に備えて

完全版**2020年SonicWallサイバー脅威レポート**のダウンロードには、SonicWall.com/ThreatReportをご覧ください。サイバー犯罪者の考え方をより良く理解し、次に行われることに十分備えるために不可欠な脅威インテリジェンスを取得することができます。

**レポートの全文を見る**


SONICWALL®

SonicWall.com

* ベストプラクティスとして、SonicWallではデータ収集、分析、およびレポート作成の手法を定期的に最適化しています。これにはデータクレンジングの調整、データソースの変更、および脅威フィードの統合が含まれます。以前のレポートで発表された数値は、様々な期間、地域または業界にわたって調整されている場合があります。

本書に含まれる資料および情報（文章、図表、写真、アートワーク、アイコン、画像、ロゴ、ダウンロード、データおよび編集物を含むがこれらに限定されない）はSonicWallまたは著作者に帰属し、適用法令（アメリカ合衆国および各国の著作権法と規制を含むがこれらに限定されない）によって保護されています。