

# Cortex Xpanse\_Xpanse\_WP\_ASM Report-JP

2021 Cortex Xpanse 攻撃対象領域に関する脅威レポート

先進的なグローバル企業から学ぶ、攻撃対象領域管理



## 2021 Cortex Xpanse 攻撃対象領域に関する 脅威レポート

先進的なグローバル企業から学ぶ、攻撃対象領域管理

2021年5月 | この記事は約15分で読めます。

新しいセキュリティ脆弱性が表面化するたびに、サイバー空間では熾烈な競争が幕を開けます。攻撃側はインターネットをスキャンして、脆弱なシステムの特定しようとし、防御側はネットワークを保護するため、大急ぎでパッチを適用するとともに、被害の拡大を食い止めようとします。

計算資源を驚くほど安価に入手できるようになったため、にわかサイバー犯罪者でも、10ドルほどを支払うだけで、インターネット全体をおおまかにスキャンして、脆弱なシステムを発見するに足るクラウドコンピューティング能力をレンタルできます。攻撃による被害の急増から分かることは、レースに勝つのは攻撃側が多く、防御側が新しい脆弱性を修正する前に、脆弱な資産を発見できるということです。サイバー恐喝の急増を裏付ける連日の報道や、デジタルライフを脅かす攻撃を目の当たりにすることが増えており、このまま見過ごすことはできません。

Cortex Xpanse by Palo Alto Networks | 2021 Cortex Xpanse 攻撃対象領域に関する脅威レポート | ASM レポート

1

攻撃者と、平均棚卸時間 (MTTI) を競う

サイバー犯罪者はハゲタカのように、セキュリティ対策の甘い標的を常に探しています。残念ながら、攻撃側が防御の手薄な資産を発見するのは、防御側が保護の必要な資産を発見するよりはるかに高速です。サイバー攻撃とセキュリティ対策は、軍拡競争というだけでなく、どちらが先にサイバー攻撃に弱いシステムを検出できるかを競う、短距離競争の側面もあるのです。

企業の戦いを支援するため、パロアルトネットワークスの**Cortex® Xpanse™**リサーチ

チームは、国際的な大企業を対象に、公共インターネットからアクセス可能な攻撃対象領域を調査しました。調査は**2021年1月から3月**にかけて行われ、**Fortune 500**企業を含むグローバル企業**50社**に関する、**5,000**万件のIPアドレスをスキャンし、モニタリングしました。調査の目的は、攻撃対象の脆弱なシステムを、攻撃者がどれくらい早く発見できるのかを把握することです。

このレポートでは、主要な調査結果や、攻撃対象領域管理における最大の脅威に関する情報、および、確実なセキュリティ対策のための知見をご紹介します。