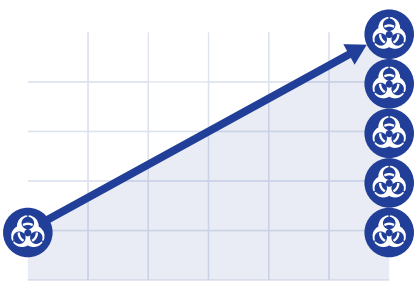
ランサムウェア対策の秘密

ランサムウェアによる企業における被害額が2020年には
200億ドルに上ると予想されている今、新しいアプローチを採用して
ランサムウェアの侵入を阻止する必要があります。

過去6か月の間に SSL経由で送り込まれた ランサムウェアの 増加率[1]は

5倍



すべてのSSLトラフィックに隠された脅威を復号化、検知、防止

サイバー犯罪者は、SSL暗号化に隠れることで、
従来型のセキュリティコントロールを
回避するようになっています。

プロキシアーキテクチャの相違点

すべてのSSLトラフィックに隠れる脅威を
クラウドのスケーラビリティと大容量の
コンピューティング能力で復号化し、検知します。

[1] Zscaler ThreatLabZ

未知の攻撃を隔離しマルウェア感染をブロック

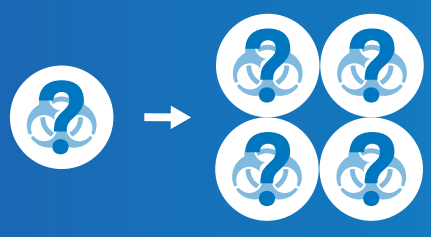
攻撃者は、標的ごとに固有のペイロードを
作成することで、シグネチャベースの防御を回避します。

プロキシアーキテクチャの相違点

従来型のファイアウォールベースのパススルー
アプローチとは異なり、AIを活用した隔離によって、
不審なコンテンツの分析を可能にすることで、
ゼロデイ攻撃を防止します。

2020年における 過去発見されたことのない ランサムウェア亜種の 増加率[2]は

4倍



[2] Zscaler ThreatLabZ

38% のリモートトラフィックが増加[3]

すべてのユーザ、すべての場所に一貫性ある同一のセキュリティ

ランサムウェアは場所に基づいて
識別できるものではありません。
全社的に一貫性あるセキュリティが必要です。

プロキシアーキテクチャの相違点

自宅、本社、外出先のどこで働くユーザにも、
優れたセキュリティが常に提供されるようにする
必要があります。

[3] Statista

攻撃対象領域を瞬時に縮小

サイバー攻撃を攻撃させるには
従来型の平坦なネットワークを
水平移動する必要があります。

プロキシアーキテクチャの相違点

ゼロトラストを種発点とすることで
水平移動を完全に防止します。アプリが攻撃者に
公開されることはありません。
ネットワーク全体ではなく
必要なリソースへのダイレクトアクセスが
認証されたユーザに許可されます。

60% の企業におけるVPNが2023年までにZTNA（ゼロトラストネットワークアクセス）に移行する[4]と予測

[4] Gartner Market Guide for Zero Trust Network Access

ランサムウェアに感染する前に被害を食い止めるには

ゼットスケーラーのゼロトラストエクスチェンジ™を導入することで
全く新しいアプローチのランサムウェア対策を取ることができます。

ウェブサイトで詳細を確認する

ゼットスケーラー株式会社
東京都千代田区大手町1-9-2
大手町フィナンシャルシティ
グランキューブ3階
www.zscaler.jp