

クラウドブラウザアイソレーションによる 攻撃対象領域の最小化

サイバー攻撃のリスクが最も高いのは？



エグゼクティブ



財務チーム



機密データやIPに
アクセスするユーザ



未知の高リスクの
Web コンテンツに
アクセスするユーザ

ガートナーによる報告



公共のインターネット
経由で実行される
外部の攻撃の割合



ブラウザ経由で
エンドユーザを標的に
する攻撃の割合

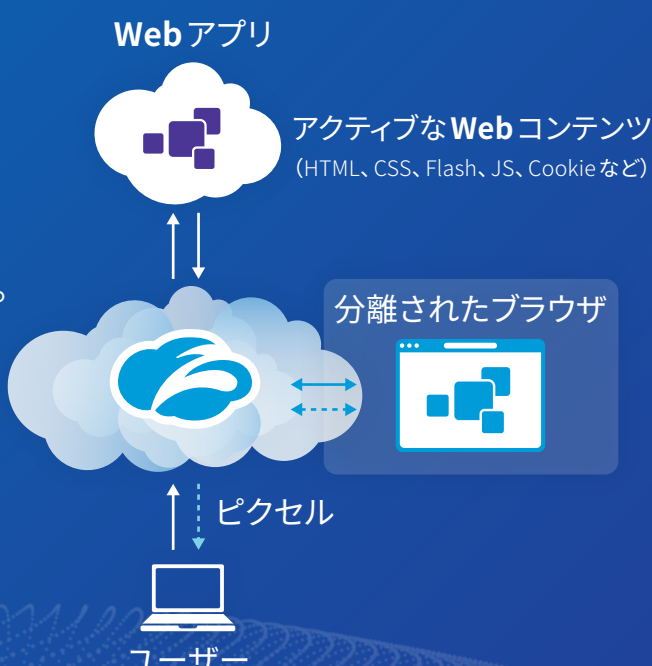
ブラウザは攻撃が送り込まれる
最大の侵入口になっている

出典: PricewaterhouseCoopers, "Time to Isolate Your Services From the Internet Castpoll", ガートナー, 2016年9月

ゼットスケラーの クラウドブラウザアイソレーションでリスクを軽減

ゼットスケラーのクラウドブラウザ
アイソレーションでブラウザを分離し、
Web ページのコンテンツを
アクティブにさせずに、ピクセルの
情報として表示させることが可能です。

ユーザは、自身のデバイスや
会社のデータをリスクにさらす
ことなく、これらのページを
確認することができます。



ゼットスケラーの クラウドブラウザアイソレーション

1 未知の高リスクのWeb コンテンツに対する 安全なアクセスを提供

新規登録ドメインや未分類のコンテンツに対する
安全なアクセスが必要不可欠

2 IPやデータの内部関係者による盗難の防止

ファイルのダウンロードやビジネスアプリからの
コピー & ペーストをポリシーに基づき
禁止することが可能

3 価値の標的の保護

エグゼクティブや機密情報を処理するユーザは
最もリスクが高いため要注意

4 ブラウザサンドボックス処理の実行

Web ページやスクリプトに埋め込まれた
ゼロデイ脅威への対策は高優先事項

ゼットスケラーの
クラウドブラウザアイソレーションについて
詳細を希望される方は、WEBサイトをご覧ください

[Webで詳細を見る](#)