

ChromeOS でランサムウェアからビジネスを保護

世界的にリモートやハイブリッド型の働き方への移行が進む中、ランサムウェア関連の犯罪も急増しています。ランサムウェアは、データを暗号化してユーザーが利用できないようにするもので、さまざまな業界の組織にとって高コストの脅威となっています。



2020年に発生したランサムウェア攻撃は **150%** 増¹



ランサムウェア攻撃の平均コストは **700,000** 米ドル以上²



全世界でのランサムウェア攻撃のコストは **2021** 年に **200** 億米ドルを超えると予測³

ChromeOS は、デフォルトでランサムウェアから守られるクラウドファーストのプラットフォームです。実際に、ビジネス、教育機関、ユーザーの **ChromeOS** デバイスに対するランサムウェア攻撃はこれまで報告されていません。

ChromeOS に組み込まれた予防的なセキュリティ機能によりランサムウェアを撃退

クラウドに自動バックアップされ復元可能なデータとファイル: クラウドファーストのプラットフォームである ChromeOS では、デバイスに保存されるデータの量が大幅に抑えられるので、ランサムウェア攻撃の被害を受けにくくなっています。ユーザーデータはすべてクラウドにバックアップされます。ランサムウェアが ChromeOS のセキュリティ対策をすり抜けた場合でも、ユーザーデータとファイルはすばやく簡単に復元できます。

実行ファイルをブロック: ランサムウェアの温床となりやすい実行ファイルは ChromeOS では実行できません。ChromeOS では、Google Play ストアで選定された、マルウェアスキャン済みのアプリだけが実行されます。

読み取りのみの OS: アプリや拡張機能によって OS が変更されないよう、システムファイルは個別のパーティションに保存されるため、ランサムウェアがアクセスすることはできません。

Google セーフブラウジング: Google セーフブラウジングでは、ユーザーが危険なサイトにアクセスしたり、危険なファイルをダウンロードしたりする前に警告し、リスクを未然に防ぎます。

自動更新: ChromeOS はバックグラウンドで定期的に自動更新され、脅威から常に守られます。

確認付きブート: 攻撃を受けた場合でも、確認付きブートにより OS の改ざんの有無をチェックし、改ざんが見つかった場合は OS を以前のバージョンに戻します。

ご不明な点は、TD SYNnex 相談窓口までご相談ください。

jp_chrome@tdsynnex.com