DELL Technologies

サイバー セーフティーに関する チート シート

ますます仮想化が進むこの世界において、サイバー犯罪が驚異的な速度で増加しているのは驚くことではありません。実際、**2021年にサイバー犯罪の被害額は約6兆ドルにも上っており**、これは国家の経済規模に換算すると、米国と中国に次ぐ世界第3位となります*。攻撃者は日々、より巧妙かつ高度になっています。しかし、最新の脅威について認識し、保護対策を実施していれば、オンラインでの安全を簡単に確保することができます。**Dellのサイバーセキュリティ エキスパートが予防に力を入れている脅威について、そして職場や家庭のセキュリティを維持するためのヒントについてご紹介します。**

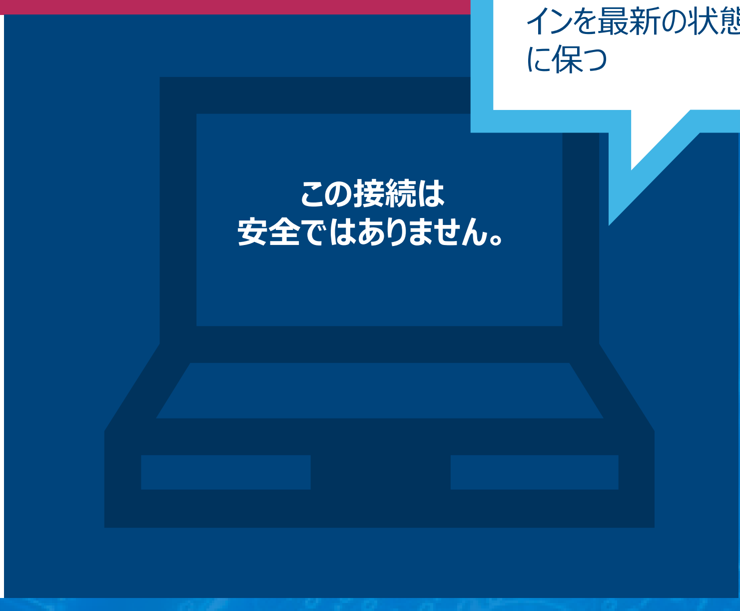
ドライブバイ攻撃

安全ではないWebサイトや改ざんされたWebサイトにお客様が遭遇した際に、悪意のある者がお客様のシステムにアクセスすることをいいます。

検出方法：

自分では追加していない新しいファイルやネットワーク接続がシステム上にある

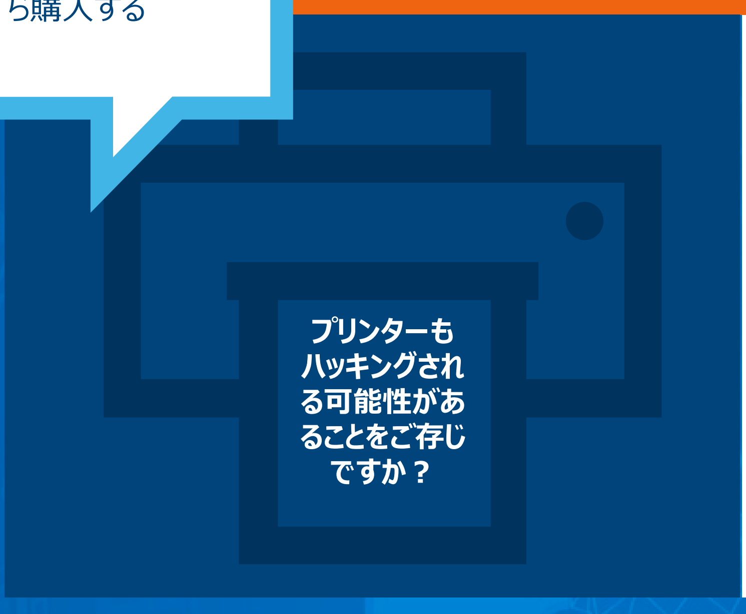
構成情報に関するリクエストが一方的に送られてくる



ヒント：
ブラウザーとプラグインを最新の状態に保つ

安全ではないハードウェア

ヒント：
正規の販売業者から購入する



攻撃者が、ハードウェアや周辺機器に直接脆弱性を埋め込むことをいいます。

検出方法：

話がうますぎるセール品

ソーシャル エンジニアリング

詐欺師が、法人やその他の権威ある団体のふりをして相手を操り、機密性の高い**個人情報や財務情報**を盗むことをいいます（「フィッシング」とも呼ばれます）。Eメール、ダイレクト メッセージ、テキスト メッセージのリンクや添付ファイルを介して、悪質なコードが送信されます。

検出方法：

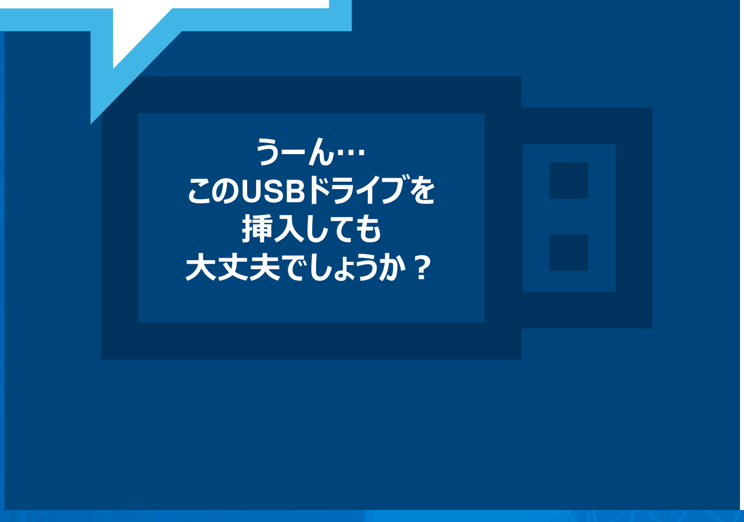
一方的に送られてきたEメールやテキスト メッセージに、リンクや添付ファイルを開くよう指示が記載されていて、個人情報を要求される

送信元Eメール アドレス、表現、綴りに疑わしい点がある

ヒント：
政府機関（国税庁など）は、まず郵便で連絡をしてくる

USBマルウェア攻撃

ヒント：
友人から共有された場合でも、未知のUSBドライブに注意する



犯罪者が、USBドライブ、ポータブルHDD、スマートフォン、音楽プレーヤー、SDカード、光学メディア（CD、DVD、Blu-ray）などのリムーバブル ストレージ デバイスを使って、コンピューターやネットワークを感染させることをいいます。

検出方法：

ファイルに対して予期しないアクセスがある、または デバイス上に新たに作成されたファイルがある

信頼関係

ハッカーが、信頼されている第三者、例えば診療所のセキュリティを侵害し、その評判を利用して患者を攻撃することをいいます。

検出方法：

異常なログイン動作

ヒント：
強力で他と重複しないパスワードを使用する

サイバー セーフティーを 維持する方法：

すべきこと

すべてのアカウントにおいて、強力で他と重複しないパスワードと多要素認証を使用しましょう。

インターネットに接続されたデバイスはすべて、攻撃を受ける可能性があります。
ソフトウェアを最新の状態に維持しましょう。

警戒し、疑い深くなりましょう。詐欺師の戦術について認識しましょう。

声を上げましょう。攻撃についてIT部門に報告し、同僚、家族、友人に知らせましょう。

すべきでないこと

手を抜かず、常にすべてのセキュリティ プロトコルに従ってください。

一方的に送られてきたEメールやダイレクト メッセージに埋め込まれているリンクをクリックしないでください。

「この接続は安全ではありません」または「この接続ではプライバシーが保護されません」などの警告がブラウザーに表示された場合、無視しないでください。

ヒント：
詳しくは、こちらをご覧ください：
Dell.com/Endpoint-Security

DELL Technologies

---

* Cybersecurity Ventures『2022 Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics』