



**TeamViewer**  
Remote Management



# 5つの身近な IT リスクと 回避方法

# 目次

# はじめに



## IT 部門がリスクに気づけないのはなぜですか？

リスクを警告するツールを持っていないからかもしれません。



IT リーダーや管理サービスプロバイダ (MSP) は、IT インフラにいつでもさまざまな問題が起こりうることを知っています。一般的にリスクは小さなものから始まります。しかし、すぐに対応をしないと、やがてビジネスに深刻な影響を及ぼすほど大きくなります。

そうならないために必要なのがリモート監視と管理 (RMM) 用のソリューションです。今日の RMM ソリューションは、リスクを識別し、通知して、早期に警告を出し、その対処を行うためのツールを提供し、IT 部門にリスクを回避する機会を与えます。

この eBook では、5つの身近な IT リスクを検証し、RMM ソリューションが問題をどのように未然に防ぐのかを説明します。



ネットワークと  
リモートデバイスの  
問題



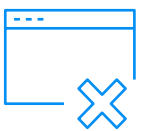
サイバー攻撃



データの喪失



不十分な監視



体験の悪い  
Web サイト



# リスク1: ネットワークと リモートデバイスの問題



私たちのネットワークは優れています。何か問題が起きますか？

問題が起きてからでは遅いのです。



ネットワークやリモートデバイスにはさまざまな問題が発生します。

- プリンタの故障
- バッテリー残量の低下
- 古いマルウェア対策ソフト

些細なものから重大な問題までさまざまです。

- スイッチとルーターのポートステータスが予期せずに変化する
- 高い CPU 使用率
- ディスク領域の不足

些細なものから重大な問題まで、いずれを回避する場合でも重要なことは早期の発見です。

- 古い OS
- メモリの異常な動作
- ファイアウォールの無効化
- オフライン状態

そのためには、ネットワークとリモートデバイスを監視して、早期に兆候を発見します。

- 過度な回数の失敗ログイン施行
- オンラインでもデータを提供しない状態のサーバー

このようなリスクを回避するために、IT にはネットワークとデバイスが正常に動作していることを確認するための完全な可視性が必要です。潜在的な問題をリアルタイムで検出するための自動アラートにより、IT 担当者は問題が起きてからではなく、プロアクティブに素早く対処を行い、IT インフラをスムーズに稼働させることが可能になります。

# リスク2: サイバー攻撃



ファイルが暗号化されたという通知を受け取りました。何が起きているのでしょうか？

状況によりませんが、ランサムウェアに対して、大金を支払いますか？



サイバー犯罪者にとって、脆弱性のあるエンドポイントは攻撃を仕掛けるための格好の標的です。今日、それらの攻撃は一般的なコンピュータウイルスよりも、さらに高度化しています。

なぜ、エンドポイントは格好の標的となってしまうのでしょうか？それは、コンピュータやモバイルデバイスといったエンドポイントは、サーバーのように保護されていないからです。さらに、グローバルなパンデミックによって自宅で仕事をする人が増えたことで、以前にも増してエンドポイントが狙われやすくなりました。

フィッシング詐欺、ランサムウェア、ゼロデイ攻撃は、最も一般的で、かつ最も被害額の大きなエンドポイント攻撃です。



**フィッシング詐欺**は、Eメールを開かせるためにソーシャルエンジニアリングを使用してユーザーを信用させます。本文に記載されたリンクをクリックすると悪意のあるサイトが開き、マルウェアをエンドポイントへダウンロードします。



**ランサムウェア**はユーザーのデータを暗号化して次のように身代金を要求します。「支払いに応じれば、データの暗号化を解除するが、応じない場合は暗号化を解除したデータをネットに公開する。」



**ゼロデイ攻撃**は、ランダムに配布されたマルウェアが自分が侵入できる脆弱性を見つけたときに発動します。潜伏期間は数か月から数年におよび、一度脆弱性に侵入すると攻撃を開始します。

RMM プラットフォームでは、1 つのダッシュボードから、3 通りの方法でエンドポイントを保護します。

- **マルウェア対策** ソフトはサイバー攻撃を防ぎ、修復を行います。
- **パッチ管理** ツールはサイバー攻撃を招くソフトウェアの脆弱性にパッチを適用します。
- **エンドポイントバックアッププロテクション** は、データを確実にクラウドへバックアップして、サイバー攻撃が成功してしまっても、復元できるようにします。

## リスク3: データの喪失



私のノート PC はどこ？  
ほんの数分前にここに置いたんだけど。

盗難を含め、さまざまな理由でデータを失う可能性があります。



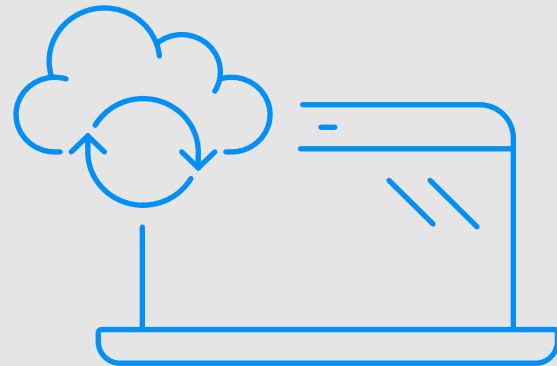
多くの会社では、マルウェア対策ソフトだけで十分だと考えて、エンドポイントのバックアップを行っていません。また、データの喪失リスクには次のようなものがあることを理解していません。

- 毎日のように、自宅、オフィス、カフェからコンピュータが盗み出されています。
- 従業員がうっかりハードディスクからファイルを削除することがあります。
- 電力サージによってマザーボードが焼けてしまうことがあります。
- 洪水、火事などの自然災害が起こると、オフィスのコンピュータが損傷または破壊されます。

従業員にバックアップ作業をさせている会社もあります。トレーニングされていない従業員が日常的にバックアップを行うことのリスクもありますが、外付けドライブに行われているはずのバックアップについて、IT 部門はどの程度の可視性を持っているのでしょうか。

答えは、ゼロです。

IT 部門にバックアップの可視性がなければ、エンドポイント デバイスの復元が必要になったときにバックアップの存在を確認することができません。



### エンドポイントのバックアップによるデータ喪失リスクの防止

定期的にクラウドへエンドポイントをバックアップすることの利点は次のとおりです。

- 自然災害、アクシデントによる削除、盗難、どのような理由でエンドポイントのデータを喪失しても、データを復元できます。
- ハッカーにデータを暗号化されても身代金の支払いを避けられます。

## リスク4: 不十分な監視



今週、新しい Windows アップデートは、  
いくつありましたか？



IT 部門はどのようにすべてのエンドポイントが正しく動作していることを確認できるでしょうか？ また、いくつかのエンドポイントが会社のネットワークに接続しているか、いつでも確認できるでしょうか？ すべてのエンドポイントの可視性を完全に確保できなければ、監視は不十分となり、エンドポイントはリスクにさらされることになります。

監視が不十分であれば、サイバー攻撃への脆弱性を持つデバイスにパッチが適用されません。OS とサードパーティのソフトウェアはアップデートされません。リスクはそのエンドポイントだけでなく、**ネットワーク全体**に波及します。

RMM プラットフォームはネットワークのすべてのエンドポイントを監視できるアセット管理ソフトを提供し、次のようなことを行えます。

- ✓ ネットワークを自発的に監査して、禁止されたソフトウェアや潜在的に有害なソフトウェアを見つけます。
- ✓ エンドユーザーの入力に頼ることなく、デバイスの重要な情報を収集します。
- ✓ バックアップ、ソフトウェアアップデート、パッチの状況を確認します。
- ✓ 重要なタスクの試行と失敗を追跡します。
- ✓ 未承認のデバイスを特定します。

アセットマネジメントは次のようなネットワークデバイスの情報をリアルタイムで提供します。

- デバイスタイプ / 名前
- OS
- ドメイン
- グローバルとプライベート IP アドレス
- CPU
- メモリ
- マザーボード
- グラフィックカード
- ディスクドライブ





# リスク 5 : 体験の悪い Web サイト



多くの訪問者がいるのに、ビジネスに結びつきません。

把握していない技術的な問題が顧客を遠ざけているのかもしれない。



Web サイトがうまく機能することで、スムーズな体験をもたらすことができます。それは、訪問者があなたの会社とビジネスをしたいと思うかどうか決める、重要な要素です。多くの会社では次のような問題で Web サイトの体験が悪くなり、売上げが犠牲になることに気づいていません。



### 地域的な障害

Web サイトが正常に稼働している地域もあれば、ダウンしている地域があるかもしれません。どの地域においても、ダウンしていればビジネスチャンスは失われます。



### ページ読み込みが遅い

Web サイトのページが 3 秒以内に読み込まれなければ、多くの人は離脱してしまいます。Google によると、e コマースのサイトにおいて許容できるページ読み込み時間は 2 秒までです。



### 機能の貧弱さ

Web サイトは訪問者に登録、ログイン、購入、買い物カゴへの商品の追加、チェックアウトなどを行わせます。これらのトランザクションのいずれかに問題が発生すれば、Web サイトの見込み客や顧客を失うことになります。

適切な Web サイト監視ソリューションでは次のことを行えます。

- ✓ 世界中で Web サイトのパフォーマンスを監視します。
- ✓ 読み込みの遅いページを確認します。
- ✓ いずれかの地域でサイトがダウンするとアラートを受け取ります。
- ✓ トランザクション機能を最適化します。

これらにより、IT 部門と Web サイトの開発者は問題が大きくなる前に素早く対処できます。

# 重要ポイント

RMM ソリューションによる集中管理で、問題を未然に防ぐとことができます。コストのかかる IT リスクを避け、すべてのエンドポイントデバイスの安全な稼働を保ち、Web サイトの機能のピークパフォーマンスを確保します。



IT 部門はビジネスに悪い影響をもたらす、身近なリスクを避けるツールを手に入れることができます。



ネットワークとデバイスを監視して、ダウンタイムを最小化し、従業員の生産性を保ちます。



高度なマルウェア保護によってサイバー攻撃を未然に防ぎます。



定期的なクラウドバックアップによっていつでもエンドポイントデータを復元できます。



ネットワーク内のすべてのデバイスを完全に可視化して、適切な管理と保守を行います。



技術的な問題で Web サイトの訪問者に悪い体験を提供しないように監視します。

# まとめ

これら 5 つの身近なリスクは、適切な技術があれば容易に避けることができます。IT 部門と MSP は 健全で安全な組織の IT インフラについて、リアクティブな姿勢からプロアクティブな姿勢に変化することができます。方法は？ TeamViewer リモートマネジメントのような集中管理型の RMM ツールを使用します。ビジネスにダメージを与える前に潜在的な問題を見つけ、対応することが可能になります。

さらに、TeamViewer リモートマネジメントはカスタマイズ可能でエンドポイントベースなので、最小限の構成から開始して、必要に応じてツールを選択し、ビジネスの成長に合わせてスケールアップすることができます。

TeamViewer リモートマネジメントを試してみませんか？

無料体験版をリクエスト



**TeamViewer**  
Remote Management

## お問い合わせ

詳しくは、**03 4563 9650** まで  
または、<https://www.teamviewer.com/ja/customer-support/>へアクセス

TeamViewerジャパン株式会社  
東京都千代田区丸の内1-5-1  
新丸の内ビルディング EGG JAPAN 10F

## TeamViewer について

世界的なテクノロジー企業として、TeamViewer はあらゆるプラットフォームのあらゆるデバイスに、どこからでもアクセス、制御、管理、監視、サポートできる安全なリモート接続プラットフォームを提供しています。60 万以上のお客様にご利用いただいている TeamViewer は、個人用途・非商用目的であれば無料で使用でき、25 億台以上のデバイスにインストールされています。TeamViewerは、リモート接続、拡張現実、IoT、デジタル・カスタマー・エンゲージメントの分野で継続的に革新を続けています。あらゆる業界の企業がシームレスな接続を通じてビジネスクリティカルなプロセスをデジタルに変革できるようにしています。2005 年に設立され、ドイツのゲッピンゲンに本社を置く TeamViewer は、全世界で約 1,400 名の従業員を擁する株式公開企業です。TeamViewer AG (TMV) はフランクフルト証券取引所に上場している、MDAX の構成銘柄です。

**快適な接続をお楽しみください**



[www.teamviewer.com](https://www.teamviewer.com)