

ランサムウェア・情報漏えい 会社存続の危機に！

社員数が少なくても、決して安全ではありません！

高額な復旧費用・業務停止・顧客情報の流出。
さらに、他社への攻撃の「踏み台」にされる危険も。

1 ランサムウェア被害がもたらす深刻な影響



多額の復旧費用

システムの復旧、データ調査、セキュリティ強化、外部専門家への依頼など、**数百万円から数千万円以上**の費用がかかるケースもあります。



業務の長期停止

受発注・請求・顧客対応などの業務が停止し、復旧までに**数週間から数か月**かかる場合もあります。

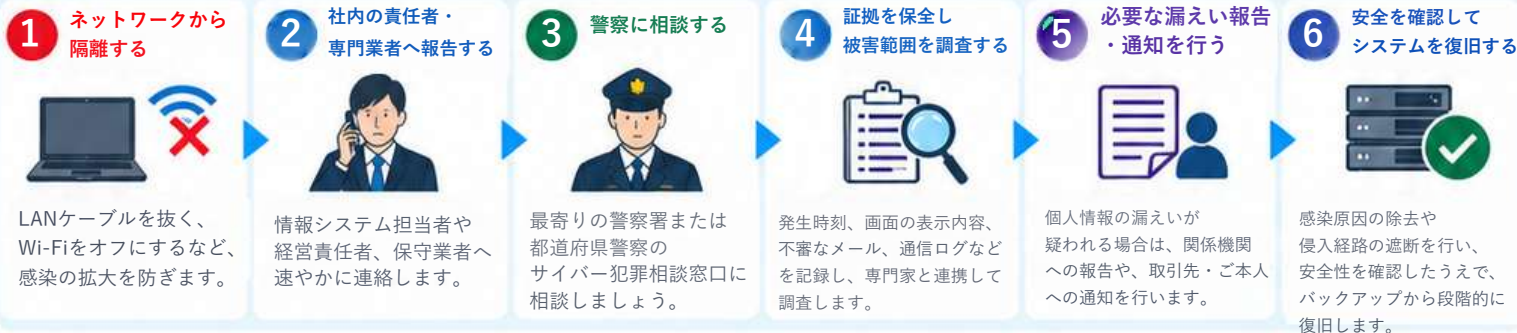


会社存続の危機

売上の減少、取引先からの信用失墜、損害賠償などが重なり、最悪の場合、事業継続が困難になる可能性もあります。

2 もし感染してしまったら？ 取るべき対応手順

被害を最小限に抑えるため、以下の手順で対応しましょう。
※状況に応じて並行して対応する場合もあります。



3 では、どう守る？ 多層防御が重要です

ランサムウェアは、一つの対策だけでは完全に防ぐことはできません。
複数のセキュリティ対策を組み合わせ、侵入・拡大・データ消失に備えましょう。



UTM (ネットワークの入口を守る)

不正な通信や危険なWebサイトへのアクセスを検知・制御し、サイバー攻撃のリスクを低減します。



端末保護・EDR (パソコンを守る)

ウイルスの侵入を防ぎ、不審な挙動を検知して被害の拡大を抑えます。



出口対策・監視 (不正通信・情報流出に備える)

不審な外部通信を検知・制御し、情報の流出や攻撃の「踏み台」化を防ぐ対策。



バックアップ (万が一の復旧に備える)

重要なデータを安全な場所に保管し、定期的に復元テストを行うことで、迅速な復旧を可能にします。



多要素認証・従業員教育 (人的リスクを減らす)

不正ログインを防ぐ多要素認証の導入や、不審なメールへの対処など従業員のセキュリティ意識向上を支援します。

4 こんな状態になっていませんか？

一つでも当てはまる場合は、今すぐセキュリティ対策の見直しをおすすめします。

- ✓ UTMを導入したが、検知ログの確認をしていない
- ✓ パソコンのウイルス対策ソフトだけで安心している
- ✓ バックアップが正常に復元できるか確認していない

- ✓ 退職者のアカウントや古い機器が放置されている
- ✓ 不審なメールへの対応方法が社内でも統一されていない
- ✓ ウイルス感染時の相談先や対応手順が決まっていない



セキュリティ対策は「導入して終わり」ではありません。
定期的な見直しと、継続的な運用が重要です。

専門家による無料相談受付中！

セキュリティ対策の見直しは フォーバルアスカへ

お客様のIT環境や業務内容に合わせて、最適なセキュリティ対策をご提案します。
まずはお気軽にご相談ください。



お問い合わせフォーム