Barracuda
Your journey, secured.

ランサムウェア対策チェックリスト

ランサムウェア攻撃では、より高度な AI を活用した攻撃がさらに採用されるようになり、既存の防御を突破しています。このチェックリストを使用することで、組織にとって効果的な保護計画を作成できます。

1. メールの保護

ランサムウェア攻撃の大半は、管理者またはユーザの認証情報を取得するためのフィッシングメールから始まります。

1a	**フィッシング攻撃をブロック** 攻撃者はソーシャルエンジニアリング戦術を使用して、従来のメールセキュリティを回避します。AI を活用したフィッシングやアカウントの乗っ取りからの保護に加え、悪意のある活動が検出された場合のアラートを備えたメールセキュリティソリューションを使用する必要があります。	☐
1b	**ユーザ研修とトレーニング** ユーザはフィッシング攻撃に対する最後の防御線です。攻撃は時間の経過とともにより巧妙になっているため、継続的な取り組みとしてユーザへの研修とトレーニングが必要になります。	☐
1c	**是正措置の実施** メールセキュリティを回避してユーザの受信トレイに到達する電メール攻撃に対しては、迅速に対処する必要があります。事前に脅威を検出し、自動修復を実施するメールセキュリティソリューションを選択してください。	☐

2. アプリケーションの保護

攻撃者はアプリケーションをハッキングし、盗んだ認証情報を使用してデータにアクセスします。

2a	**Webアプリケーションを保護** アプリケーションには多くの場合、データアクセスに悪用される可能性がある未解決の脆弱性があります。OWASP Top 10、ゼロデイ攻撃、ブルートフォース攻撃などの Web アプリケーションの脆弱性を防御するアプリケーションセキュリティソリューションが必要です。	☐
2b	**アプリケーションへのアクセスを保護** 内部アプリケーションの場合は、許可されたユーザとデバイスのみにアクセスを許可する必要があります。ユーザに特別に許可されたアプリケーションやデータに安全にアクセスするには、ゼロトラストアクセスソリューションを選択してください。ゼロトラストにより、ユーザとデバイスの ID を継続的に検証できます。	☐
2c	**環境へのアクセスを保護** ネットワークインフラストラクチャ全体を保護することで、すべてのユーザとデバイスにセキュアな接続を提供し、どこにいても、必要なリソースにアクセスできると同時に、無許可のユーザや攻撃者を締め出すことができます。	☐

3. データのバックアップ

攻撃者はデータを暗号化し、身代金を要求します。

3a	**データのバックアップ** すべてのデータをバックアップする必要があります。オンプレミスのデータだけでなく、Microsoft 365 などのクラウド/SaaS アプリケーションのデータも必ずバックアップ保存してください。	☐
3b	**アプリケーションへのアクセスを保護** 攻撃者は、回復できないようにするためにバックアップデータをターゲットにすることがよくあります。ここでは、暗号化、アクセス制御、ネットワーク共有プロトコルの排除のどれもが重要になります。データへのアクセスは、自分にとっては簡単でも、攻撃者にとっては困難である必要があります。	☐
3c	**復旧計画の策定** 攻撃を受けている場合は、攻撃に迅速に対処し、データを回復し、身代金の支払いを回避する必要があります。技術的な対応だけでなく、ビジネス上の対応も考慮してください。問題が発生する前に、計画全体をテストしてください。フォレンジック調査は、攻撃直後に、脆弱性を見つけ出す上で役立ちます。	☐

その他の推奨事項

- **パッチ適用** – ソフトウェアにパッチが適用され、最新であることを確認してください。攻撃者は最初に既知の脆弱性を探します。そのため、攻撃者が簡単に探し出せないようにする必要があります。
- **多要素認証** – 少なくとも、すべてのアプリケーションとリソースに対してスマートフォンアプリまたはテキストベースの第 2 要素認証の義務付けを検討してください。これは、ブルートフォース攻撃によるログインの試みを防御するのに役に立ちます。

ランサムウェア対策の計画を立てましょう
https://www.barracuda.co.jp/products/ransomware/

お問い合わせ: japansales_team@barracuda.com

Barracuda
Your journey, secured.