



ランサムウェアに有効な対策を知っていますか？

ランサムウェア被害の共通点 弱いところが攻撃される！

脆弱なネットワーク



- ・接続元IPアドレス制限なし
- ・脆弱性情報の未取得と放置

総当たり攻撃
辞書攻撃

弱いパスワード



- ・推測可能なパスワードの使用
- ・初期設定パスワードのまま運用

管理者権限の付与



- ・アプリケーションの動作を優先
- ・一般ユーザへの管理者権限の付与（権限分離）

管理者パスワードが共通



- ・管理者アカウント・パスワードを使い回し
- ・機器ごとに異なるパスワードを設定していない

ウイルス対策ソフト 改ざん防止未設定



- ・ウイルス対策ソフトが更新されていない
- ・管理者権限によるウイルス対策ソフトの停止
- ・EDR、ログ監視がなく、侵入に気づけない

この2つの対策で効果大！ パスワード突破を防ぐ！



パスフレーズの採用

- ・「英数字+記号」だけの短いパスワードより、長いフレーズが強力
- ・例)
 - ・NG: P@ssw0rd (8桁)
 - ・OK: KonnichihaNagasaki2025! (23桁)
(こんにちはながさき)

解読には膨大な時間を要する

アカウントロックアウト

- ・一定回数のパスワードを間違えるとアカウントを一時停止
- ・不正アクセスの「ブルートフォース（総当たり）攻撃」を防ぐ

・Group Policy で設定

- ・[コンピュータの構成]>[Windows設定]>[セキュリティ設定]>[アカウントポリシー]>[アカウント ロックアウト ポリシー]
 - ・アカウントロックアウトのしきい値 : 10回ログオン失敗
 - ・ロックアウトカウンターのリセット : 10分後
 - ・ロックアウトの期間 : 10分
 - ・管理者のアカウントロックアウトを許可する : 有効

ランサムウェアは、侵入を防ぐこと・侵入後の拡大を防ぐことが重要！

もしも、被害に遭ってしまったら警察に通報・相談を！

最寄りの警察署又はサイバー犯罪相談窓口



<https://www.npa.go.jp/bureau/cyber/soudan.html>

