arcserve

ランサムウェア対策リスト		
重要度	対策	
	利用者(ユーザー)が行う対策	
高	電子メールの送信元に注意する	感染経路への対策
高	Webサイトのアクセスに注意する	感染経路への対策
中	外出時、公共機関のWi-Fiサービスは PCおよびモバイルから利用しない	感染経路への対策
高	OSやアプリケーションを最新の状態に保つ	端末レベルでの対策
高	マルウェア対策(アンチウィルス)ソフトウェアを最新の状態に保つ	端末レベルでの対策
中	PCにフリーアプリケーションを勝手にインストールしない	端末レベルでの対策
中	非公式なアプリストアからアプリをインストールしない	端末レベルでの対策
中	外付けディスク利用時はアンチウィルスソフトでチェックし接続	端末レベルでの対策
	管理者が行う対策	
高	重要なデジタルデータの特定を行う	セキュリティ体制
高	セキュリティインシデント発生時の体制を整える	セキュリティ体制
高	セキュリティ対策製品を連携し、攻撃の早期段階で防御する	セキュリティ監視
高	ネットワーク セキュリティを強化する	ネットワーク対策
高	クラウドセキュリティ対策を検討する	ネットワーク対策
高	管理者権限で、リモート接続するPCを外部利用しない	エンドポイント対策
高	エンドポイント保護対策製品を導入する	エンドポイント対策
高	OSやアプリケーション等を最新の状態に保つ	パッチ管理
高	不要なアプリケーション利用を管理する	エンドポイント対策
高	ランサムウェア対策に限らず、ITセキュリティに関する社内教育や啓発を定期的に行う	社内教育
高	ランサムウェア攻撃を想定した対応訓練を行う	社内教育
中	外部サービスを検討する	外部サービス等
	バックアップで備える対策	
高	複数世代のバックアップを保持する	バックアップ
高	バックアップ環境の保全	バックアップ
高	オフラインで保管する	バックアップ
中	バックアップ3-2-1ルールの３は、本番データ＋２つコピーを持つ	バックアップ
中	バックアップ3-2-1ルールの２は、2種類のメディアにバックアップデータを保管する	バックアップ
中	バックアップ3-2-1ルールの１は、別の災害対策サイトへバックアップデータを保管	バックアップ
中	バックアップ3-2-1ルールに＋１として「不変ストレージ」を利用する	バックアップ
中	健全なデータ時点の調査ができる	バックアップ
高	健全な状態へシステム全体の復旧ができる	バックアップ
高	復旧手順書を準備する	バックアップ

※ 重要度は、ご利用の環境や業務内容に応じてIT重要度は異なります。
どこを守るべきかご検討の上、「重要度」を最終決定してください。

2021年11月