

自分でできるランサムウェア対策

書き込み式チェックリスト / 復元テスト記録 / 改善依頼票

50

項目

設定を確かめ、根拠を残し、
次に動く担当者を決める。

会社・部署：

対象範囲：

記入者： 確認日：

最初に見る10項目

01 重要データの場所

06 OSの更新結果

08 サポート期限

09 端末の保護状態

14 多要素認証

26 VPN機器の更新

32 バックアップ対象

34 保存先の保護

38 架空ファイルの復元

46 事故時の連絡先

状態は4種類で記入します

済＝根拠を確認した 未対応＝作業が残っている

不明＝確認先や回答待ち 該当なし＝理由を記録する

本人が確認できる範囲から進め、機器・通信・権限の変更は管理者と実施します。一部の端末だけを確認した場合は、その対象を残してください。チェックの合計は安全度の点数ではありません。

既に感染や暗号化が疑われる場合は、責任者へ連絡し、社内手順に沿って隔離と記録を進めます。感染が疑われる機器へバックアップ媒体を接続しないでください。

A 守るデータと担当を決める

対象の業務・保存先・担当を対応付けます。

01 止まると困る業務のデータと保管場所を列挙した

優先

受注・請求等の業務名、ファイルやシステム、保存場所が一覧にある。Web・メール・クラウド・端末を含めて業務担当と照合

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

02 端末・サーバー・NAS・VPN・主要ソフトの台帳がある

所有者、製品名、バージョン、利用者を記録し、実物や管理画面と対応する

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

03 システムごとの管理者と代行者を決めた

01・02の各対象について、設定を変更できる担当と、不在時の依頼先が分かる

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

04 復旧する順番と目標を業務ごとに決めた

「何時間止まると困るか」「何時間分の更新を失えるか」を業務担当が決め、順序を記録。数値は会社ごとに設定

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

05 外部委託先と自社の担当範囲を確認した

更新、バックアップ、復旧、事故連絡の担当が契約・回答で分かる。外部から接続する経路も確認

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

確認した根拠・対象範囲・該当なしの理由

B 更新と端末の保護

操作した記憶ではなく、現在の状態と結果を確かめます。

06 OSのセキュリティ更新が適用されている

優先

更新画面で失敗・保留・再起動待ちを確認。管理対象端末は管理者の配信結果と照合

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

07 ブラウザ・Office・PDF閲覧等のアプリを更新した

各アプリの版と更新結果を確認。OS更新だけでアプリも完了としない

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

08 サポート切れの製品を放置していない

優先

メーカーの期限と台帳を照合。期限切れは置換または専門担当が代替対策を実施。交換予定だけなら未対応

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

09 承認されたマルウェア対策が稼働している

優先

正規の管理画面で保護状態、更新日時、未処理の警告を見る。インストール済みだけで確認済みにしない

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

10 端末のファイアウォールが適切に有効

利用中のネットワークで有効か確認。業務の都合で全体を無効化したままにせず、例外は管理者が確認

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

11 対応端末の重要フォルダに追加の保護を適用した

WindowsのCFA等は条件・業務影響を確認して段階導入。監査だけなら防止機能は未対応。非対応OSは理由と代替策を記録

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

12 業務で使えるソフトの範囲を管理している

承認ソフトの一覧と実際の導入状況を照合し、不要・未承認の実行を抑える運用や設定がある

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

C 認証と権限

誰が入れるか、何をできるかを確認します。秘密値は書かないでください。

13 重要サービスでパスワードを使い回していない

承認済みの管理手段でサービス別に管理する。初期値・他サービスとの共用を解消。表に秘密値は書かない

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

14 メール・VPN・管理者アカウントで多要素認証を使う

優先

対象一覧と登録・適用状況を照合し、正規画面からログイン確認。使えないサービスは管理者が代替策を判断

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

15 日常作業と管理者作業のアカウントを分けた

普段のメール・Web閲覧は必要最小限の権限。管理権限が必要な作業だけ切り替える運用を確認

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

16 退職者・未使用アカウントを停止した

在籍者・利用者とアカウント一覧を照合。外部委託先の終了アカウントも確認

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

17 共有フォルダの書込・管理権限を絞った

利用目的と権限表を照合し、全員が全フォルダを書き換えられる状態等を見直す

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

18 認証機器を失った際の回復手段を確保した

承認された予備の認証方法や管理者の回復手順がある。回復情報は安全に保管し、記事・記入済みPDFへ載せない

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

19 管理操作をした人が記録から分かる

原則として個人別の管理アカウントを使い、共用が必要なら利用者を追える仕組みと記録を設ける

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

D メールとWeb閲覧

不審な指示を受けたときの確認先と、保護設定を確かめます。

20 不審な依頼を別の経路で確認する手順がある

添付やログイン要求を受けたら、既知の連絡先や正規の管理画面で確認する。送信者名だけを根拠にしない

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

21 文書の指示でマクロや保護解除を許可しない

社内ルールとOfficeの制御を確認。正当な業務マクロの例外は管理者が発行元と必要性を確認

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

22 不審メールを報告する方法を全員が知っている

連絡先と操作を周知し、安全な模擬例で説明できるか確認。不審添付を全社転送しない

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

23 メールの不審添付・迷惑メール対策を確認した

契約サービスのフィルタ設定、対象ファイル、隔離時の確認担当が分かる

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

24 不要な拡張機能や外部アプリの連携を整理した

ブラウザ・業務クラウドの一覧と権限を見て、不要なものは影響を確認して解除

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

25 アプリ取得先とWeb警告への対応を決めた

正式な配布元・承認ストアを使用。広告等の偽更新や保護機能の解除要求を受けたら管理者へ確認

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

確認した根拠・対象範囲・該当なしの理由

E VPNと社内ネットワーク

機器・通信の設定は管理者や保守会社へ確認します。

26 VPN等の外部接続機器を更新した

優先

型番・現在版をメーカーの修正情報と照合。適用結果と、暫定対策が必要な場合の処置を残す

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

27 リモートデスクトップを不用意に公開していない

外部接続の構成と許可対象を確認。不要な接続は停止し、必要な場合は管理者が認証・接続制限を設定

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

28 ルーター・NAS等の管理画面の公開範囲を絞った

管理用画面へ誰がどこから接続できるか確認。初期設定のまま外部へ公開しない

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

29 遠隔操作・保守ツールの利用を把握している

正規の保守ツール、接続者、権限、利用記録を照合し、不要なものは担当と停止する

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

30 来客用・私物端末等と重要システムの通信を分けた

ネットワーク構成とアクセス制御を確認。Wi-Fiの名前が別というだけで分離済みとしない

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

31 不要な共有・サービス・古い通信方式を止めた

利用実態と依存関係を調べ、不要なものを管理者が停止。業務上必要なものと、変更後の動作確認を記録

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

確認した根拠・対象範囲・該当なしの理由

F バックアップを取る・守る

対象、成功日時、接続状態、権限、保持期間を確認します。

32 重要データがバックアップ対象に入っている

優先

01の保存元と対象設定・除外設定を照合。クラウド上だけにあるデータの扱いも確認

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

33 必要な頻度でバックアップが成功している

04の許容範囲に合う取得間隔を決め、最新の成功日時・対象を確認。設定ONだけで終えない

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

34 攻撃された端末からバックアップを壊しにくい

優先

物理的な切り離し、または改変・削除を制限する保存方式を確認。通常フォルダの別コピーだけなら未対応

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

35 バックアップ管理の認証・権限を分けている

日常業務や通常の管理アカウントの侵害が、バックアップの破壊につながらない構成を確認。対応時はMFAも使用

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

36 戻せる時点と保持期間が業務に合っている

世代数だけでなく期間・完全削除の条件を確認。同期サービスは契約と復元仕様を照合

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

確認した根拠・対象範囲・該当なしの理由

F バックアップから戻す

本番と分けた正常な検証環境で、復元と内容の確認を行います。

37 一つの場所の障害で全コピーを失わない

主データとバックアップの装置・設置場所・障害範囲を確認。別フォルダや同一装置の別領域だけで済ませない

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

38 検証用ファイルをバックアップから復元できた

優先

正常な検証環境で架空ファイルを復元し、使用した世代・場所・手順を記録。本番データを上書きしない

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

39 復元したデータが業務で使えることを確かめた

件数・内容・文字化け・関連ファイル等を確認し、必要なアプリで読み込みや集計を試す

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

40 復元にかかった時間を目標と比べた

探索、認証、復元、内容確認を分けて測定。ファイル一つの時間を全社の復旧時間とみなさない

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

41 元の端末が使えなくても復旧に必要な情報を取り出せる

手順書、暗号鍵等の所在、認証の回復先を正常な環境から確認。秘密値をチェック表へ記載しない

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

確認した根拠・対象範囲・該当なしの理由

G 異常を見つける仕組み

何が記録され、誰に通知され、誰が対応するかを確かめます。

42 ログイン・VPN・管理操作等の記録を保存している

保存対象、期間、時刻、取得担当を確認。対象機器が使えない場合の保全方法も決める

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 期限

43 不審なログインや権限変更の通知先が決まっている

対応するサービスの通知・検知設定を確認し、受信者と確認手順を記録。通知だけで対応完了としない

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 期限

44 バックアップ失敗・削除・容量不足を見逃さない

製品の通知設定と通知履歴を確認し、失敗時に代行者も動ける。安全なテスト通知があれば到達を確認

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 期限

45 大量変更や不審な操作を検知した際の対応が決まっている

端末保護・NAS・監視サービス等の対応範囲と警告の扱いを確認。必要な監視がない場合は不足として予算・委託を検討

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 期限

通知先・代行者・確認する記録の保管先

H 事故時と継続運用の備え

PCや会社のメールが使えない場合も想定します。

46 事故時の連絡先をPCなしで確認できる

優先

社内責任者、保守会社、警察・相談窓口を紙や別の安全な手段で確認できる。夜間・不在時も決める

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

47 発見時の連絡・隔離・記録の手順を共有した

社内手順に沿ってネットワークから隔離し、画面や時刻を記録する流れを確認。無断の初期化やバックアップ接続を避ける

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

48 復旧後に再接続する条件と承認者を決めた

原因への対処、対象範囲の調査、正常性確認を担当と整理。データが開けただけで元のネットワークへ戻さない

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

49 システム停止中の最低限の業務手順がある

受注・連絡等の代替手段、データの保管方法、再入力時の照合を決め、架空例で確認

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

50 再確認日と訓練の担当を決めた

未対応の項目に担当・期限を付け、変更後や定期の確認予定を記録。安全な机上訓練・復元試験で見直す

☐ 済 ☐ 未対応 ☐ 不明 ☐ 該当なし 担当 _____ 期限 _____

連絡先・代行者・次回確認日（紙でも確認できるように記入）

復元テスト記録

架空のデータと正常な検証環境を使います。本番を上書きしないでください。

実施日時・実施者	実施日、作業者、内容を確認する業務担当
対象と環境	架空データ、OS・アプリ、バックアップ製品・プラン
戻したい状態	対象ファイル、戻したい日時・世代
保存元と復元先	検証用の保存元、復元する領域、元の場所へ戻す場合の条件
取得の状態	最終成功日時、対象・除外設定で確認したこと
保存先の保護	切り離し・削除保護・管理権限で確認したこと
内容の照合	ファイル数、行数、値、使用するアプリでの確認
結果と残った課題	成功・一部未達・失敗・未確認とその理由

工程ごとの時間を記録する

探索	認証	復元処理	内容確認
開始：	開始：	開始：	開始：
終了：	終了：	終了：	終了：

次の改善：項目番号 担当 期限 再試験日

測定した範囲だけを記録します。一つのファイルの復元成功や所要時間は、全社の復旧能力や情報窃取の有無を示すものではありません。

改善計画と管理者への依頼票

未対応・不明の項目を転記し、確認できた根拠をもって完了にします。

1 項目番号： 担当： 期限：

現状・依頼：

完了の根拠：

2 項目番号： 担当： 期限：

現状・依頼：

完了の根拠：

3 項目番号： 担当： 期限：

現状・依頼：

完了の根拠：

4 項目番号： 担当： 期限：

現状・依頼：

完了の根拠：

5 項目番号： 担当： 期限：

現状・依頼：

完了の根拠：

6 項目番号： 担当： 期限：

現状・依頼：

完了の根拠：

依頼例：「VPNの型番・現在の版・メーカーの修正情報との照合結果を確認してください」。顧客情報やパスワード等の秘密値を記入せず、必要な記録の保管先を示してください。

出典と用語

一次資料を参考に株式会社レイズが編集。確認日：2026年10月16日。

- S01 警察庁 ランサムウェア被害防止対策
- S02 IPA 中小企業向け対策ガイドライン 第4.0版
- S03 NCSC Mitigating malware and ransomware attacks
- S04 NCSC オンプレミスバックアップの原則
- S05 NCSC クラウドバックアップの原則
- S06 Microsoft Windowsセキュリティのウイルスと脅威の防止
- S07 Microsoft Controlled folder access overview
- S08 Microsoft インターネットからのマクロのブロック
- S09 Google Workspace 2段階認証プロセスを導入する
- S10 Microsoft Windowsの更新プログラムのインストール
- S11 Apple Time MachineでMacをバックアップする
- S12 Apple Time Machineでバックアップした項目を復元する
- S13 Microsoft OneDriveを復元する
- S14 IPA クラウドサービス安全利用の手引き 説明資料
- S15 警視庁 ランサムウェアの脅威と対策 対策編
- S16 IPA 中小企業のためのセキュリティインシデント対応の手引き
- S17 JPCERT/CC 侵入型ランサムウェア攻撃を受けたら読むFAQ
- S18 個人情報保護委員会 漏えい等の対応

VPN：社外等から社内へ接続する仕組み。

NAS：ネットワーク上でファイルを共有する保存装置。

多要素認証：パスワード等に、別の要素による本人確認を加えること。

公開Web設定の点検も無料で

Web AI Securityは、自社サイトの公開情報を確認します。社内端末・VPN内部・バックアップの状態や、感染の有無を判定する検査ではありません。

[自社サイトを無料でチェックする →](#)