PSC 30th
POWER STAFF COMMUNICATIONS

セキュリティインシデント

初動対応チェックシート

「おかしい」と思ったら、まずこの1枚。
何かをする前に、まず専門家へ相談を。

インシデントに気づいてから専門家の調査が始まるまでの間に、被害を広げず証拠を守るための初動対応をまとめています。
対象：情報システムご担当者・現場の管理者・対応責任者　／　保管場所：情シスの机上・サーバ室など、すぐ手に取れる場所に

インシデント
緊急連絡窓口
24時間対応

0120-89-3189

判断に迷ったら、何かを実行する前にお電話ください。「やらない」「触らない」が正解であることが少なくありません。

最初に守っていただきたい 3つの原則

この3点を守っていただければ、調査の成否を左右する証拠の大半は残ります。

原則 1
電源を切らない 再起動・ログオフしない

メモリ上にしかない証拠（実行中のプロセス、外部との通信、攻撃ツール、暗号化の鍵）は電源を切った瞬間に失われます

お願い：画面はそのまま。ノートPCは電源アダプタに接続。スリープ・自動ロックは構いません。

例外：ランサムウェア感染の場合は、直ちにシャットダウン

原則 2
ネットワークから 切り離す

LANケーブルを抜く／Wi-Fiを無効化／スイッチのポート閉塞／EDRの隔離機能、のいずれかで。仮想マシン・クラウドは停止せずネットワーク隔離。

お願い：切り離した端末名・日時・方法・実施者を記録。

原則 3
すべてを 記録する

「いつ・誰が・何に気づき・何をしたか」を時刻付きで。画面の脅迫文やエラーは、被害端末ではなくスマートフォンで撮影。

お願い：「良かれと思って行った対応」も必ず記録。事態の発生後に施した対応が把握できていない場合、調査でその痕跡を攻撃者の行動と区別できず、時間と費用が大きく増えます。

このリーフレットの使い方

P2 最初の1時間の流れ
P3 やってはいけない10項目
P4 封じ込め判断／ランサムウェア
P5 証拠の保全（ログ最優先）
P6 準備チェック／連絡と報告
P1 緊急連絡先・3つの原則

©1996 PSC Inc.

v1.0　2026年10月23日発行　株式会社ピーエスシー　アイズオンフォレンジックチーム

直ちに行っていただくこと

最初の1時間の流れ

3原則を守ったうえで、この順で。**②以降は同時並行で構いません。**

インシデントに気づいた
アラート／外部からの通報／脅迫文の表示／ファイルが開けない　など

まず 3原則　① 電源を切らない　② ネットワークから切り離す　③ すべて記録する

迷ったら何もせず電話。**ランサムウェアの場合は例外 → 直ちにシャットダウン**

1 対応責任者と連絡窓口（PoC）を決める

各1名＋代理1名。調査会社・警察など社外とのやり取りは窓口に一本化。
窓口は社内の報告も一本化して受け、記録係を兼ねる（または記録担当を置く）。

2 被害端末・サーバを隔離し、現状を保存する

ネットワークから切り離す（電源は切らない）。仮想マシンはメモリ込みスナップショット、
クラウドは隔離用セキュリティグループ＋ディスクスナップショット。画面を写真に撮る。
「操作禁止」を表示し、部屋を施錠して誰も触れない状態にする。

3 影響範囲を一次把握する（正確でなくてよい）

何が起きているか／どの端末・システムにいつから／侵入経路の心当たり／業務への影響／
個人情報・機密情報を持つシステムが含まれるか。「分かること」と「分からないこと」を分けて記録。

被害はまだ拡大中？
複数拠点への拡大・外部への大量通信
・隔離だけでは止まらない

YES →

4 境界遮断を検討
外向き通信の制限
VPNの一時停止
業務停止を伴うため
責任者が判断し記録

NO ↓

5 社内の関係者へ「帯域外」で連絡する

経営層（状況・業務影響・封じ込め判断）／法務（報告義務と期限）／広報（一次回答の準備）／
情シス（ログ保全・遮断）／業務部門（業務継続）。電話や個人携帯で、知る範囲は必要最小限に。

6 専門家へ相談する（PSC インシデント緊急連絡窓口：0120-89-3189）

相談の際は次の5点を伝えると話が早く進みます（分かる範囲で構いません）：

- □ 被害は今も拡大中か
- □ 影響を受けた端末・サーバの数と種類（Windows端末・AD・仮想基盤・クラウド など）
- □ すでに実施した対応（隔離・遮断・スキャン・再起動など）　□ 個人情報の可能性・脅迫文の有無
- □ 現地の住所・入館手続き・リモート接続の可否

調査開始までの間に：証拠の保全・情報統制・準備チェック

ログは自動で上書きされます。最も失われやすい証拠です。保持期間の延長を最優先に。

©1996 PSC Inc.

調査が始まるまでに行わないでいただきたいこと

やってはいけない 10のこと

被害を広げるか、調査に必要な証拠を失わせます。**すでに実施済みの場合、日時と内容を記録し、専門家に伝えてください。**

1 被害端末・サーバの電源断、再起動、シャットダウン

メモリ上の証拠（プロセス・通信・鍵・攻撃ツール）が消えます。起動・終了時に痕跡を消すマルウェアもあります。

※例外：ランサムウェア感染の場合は直ちにシャットダウン。

2 ウイルス対策のフルスキャン・駆除、クリーンアップ／レジストリ修復ツールの実行

検体やファイルのタイムスタンプが変わり、「いつ・どこから・どう侵入したか」を追えなくなります。

3 不審なファイル・メール・脅迫文（ランサムノート）の削除

攻撃グループや手口を特定する材料を失います。写真を撮り、ファイルそのものも残してください。

4 OSの再インストール、端末の初期化、バックアップからの復元

侵入経路が分からないまま復旧すると再侵入されます。ディスク上の証拠も上書きされます。

5 被害端末での通常業務、Web閲覧、ファイルの開閉・移動・コピー

証拠が上書きされるほか、感染が広がるおそれがあります。被害端末は「見るだけ・触らない」。

6 相談なしの一斉パスワードリセット、AD・認証基盤の再構築、攻撃者IP・ドメインの一斉ブロック

攻撃者に気づかれ、証拠隠滅や破壊行動（データ消去・ランサムウェア起動）を誘発します。**明らかに悪用中のアカウントの無効化は例外**（内容と時刻を記録）。

7 ログの削除、ログ保持設定の放置、機器の交換・撤去

ログは自動で上書きされます。調査に必要なログが失われます。リース返却・廃棄も保留。

8 攻撃者への連絡、身代金の支払い・交渉

経営層・法務・警察と協議のうえで判断すべき事項です。単独で行わないでください。連絡があっても返答せず内容を保存。

9 侵害された可能性のあるメール・チャット・グループウェアでのインシデント連絡

攻撃者に対応状況を読まれます。電話や個人の携帯電話、別テナントのツールなど帯域外の手段で。

10 SNSや社外への未確認情報の発信、社内への広範な周知

誤情報が信用低下や法的問題につながります。知る範囲は必要最小限にし、共有先を記録。

「良かれと思って行った対応」も必ず記録してください。事態の発生後に施した対応が把握できていない場合、調査でその痕跡を攻撃者の行動と区別できず、時間と費用が大きく増えます。

©1996 PSC Inc.

封じ込めの範囲と業務継続

調査開始までの「やる／待つ」判断表

封じ込めは必要ですが、やりすぎると業務が止まり、攻撃者に気づかれることもあります。

凡例： 実施する　条件付き／相談のうえ　調査開始まで待つ　行わない

対応	調査開始までの推奨	注意点
被害端末・サーバのネットワーク隔離	実施する	電源は切らない（ランサムウェアの場合は例外→下記）。隔離した端末名・時刻・方法を記録。
明らかに悪用されているアカウントの無効化	実施してよい	対象・時刻を記録。パスワード変更より「無効化」を優先し、ログイン中のセッションも取り消す。
インターネット境界での遮断 （外向き通信の制限、VPN停止）	拡大中・持ち出しの疑いがあれば実施	業務停止を伴う。「拡大を止める」と「業務を続ける」のどちらを優先するか、責任者（必要なら経営層）が判断し記録。
攻撃者のIPアドレス・ドメインの遮断	専門家と相談	通信先の記録を先に保全。攻撃者は別経路に切り替えることがある。
一斉パスワードリセット、AD・認証基盤の再構築	調査開始まで待つ	侵入範囲が分からない段階で行うと攻撃者に気づかれ、証拠隠滅を招く。
バックアップからの復元、端末の再構築	行わない	侵入経路と安全性の確認が先。バックアップ自体を保全対象として扱う。
ウイルス対策ソフトによる駆除	行わない	検知情報（検知日時・パス・検体名）は管理コンソールから記録・エクスポート。

ランサムウェアの場合に追加でお願いすること

原則1の例外：ランサムウェア感染の端末は、直ちにシャットダウン（電源断）

ランサムウェアでは、メモリ上の証拠を残すことよりも**暗号化と被害の拡大を止めること**を優先します。感染した端末は、暗号化が進行中か終わっているかに関わらず電源を切り、可能なら同時にLANケーブルも抜いてください。実施した端末名・時刻を記録してください。

1. **脅迫文は削除せず、写真とファイルの両方を保存**
   攻撃グループの特定に必要です。
2. **暗号化されたファイルの拡張子と、暗号化ファイルを保全**
   元ファイルが分かるものがあれば併せて
3. **復号ツールの試用・「復元」の試行・バックアップからの復元はしない**
   侵入経路の特定と安全性の確認が終わるまで。
4. **攻撃者からの連絡・リークサイト掲載は、内容を保存して返答しない**
5. **身代金の支払いは経営層・法務・警察と協議のうえで**支払っても復号・非公開の保証はなく、制裁対象への送金に該当するリスクも。
6. **バックアップを直ちにオフライン化し、暗号化・削除されていないか確認**
   ランサムウェアはバックアップを狙います。

©1996 PSC Inc.

証拠の保全

ログは待ってくれない — 保全の優先順

ログは自動的に上書き（ローテーション）されます。**調査が始まるまでの間に最も失われやすい証拠です。**

STEP 1 最優先
保持期間を延長する
自動削除・ローテーションを止めるか保持期間を延ばす。ディスク容量不足で新しいログが止まらないよう注意。

STEP 2
エクスポートして別媒体へ
被害端末とは別の場所（外付けディスク・別サーバ・クラウドストレージ）に保存。日時・対象・保存先を記録。

STEP 3
時刻同期を確認する
各機器がNTPで同期されているか確認し、ずれがあればその量を記録。複数機器のログ突き合わせに必要。

ログの種類	具体例	保全のポイント
ネットワーク境界	ファイアウォール、VPN装置、プロキシ、DNS、無線LANコントローラ	**装置内ログは短期間で消えます→最優先でエクスポート。**
認証基盤	AD（ドメインコントローラのセキュリティイベントログ）、Entra ID／Google Workspaceのサインインログ、RADIUS	ログオン成功・失敗、アカウント作成・権限変更。**ドメインコントローラは全台。**
サーバ・端末	Windowsイベントログ、Linuxのauth・syslog、Webサーバのアクセスログ、DBの監査ログ	被害端末は操作せず隔離のまま保全。**SIEM等に転送済みのログを優先。**
セキュリティ製品	EDR、ウイルス対策、IDS/IPS、WAF、メールゲートウェイ、SIEM	管理コンソールの検知履歴・隔離履歴。調査時に閲覧できるアカウントをご用意ください。
クラウド・SaaS	Microsoft 365 統合監査ログ、Entra ID監査ログ、Google Workspace監査ログ、AWS CloudTrail、Azureアクティビティログ	保持期間が短い設定になっていないか確認。**メールボックスの転送設定・受信トレイルールは変更前に記録。**
物理・入退室	入退室記録、監視カメラ	内部不正や物理侵入が疑われる場合。上書きされる前に保存。

端末・サーバ・媒体

・電源を入れたまま隔離し、**「操作禁止」表示＋施錠**

・VMはメモリ込みスナップショット。クラウドはディスクスナップショット＋削除・スケールイン保護

・USBメモリ・外付けディスクは**抜かずにそのまま。**抜いてあれば他の端末に繋がず袋に保管

・リース返却・廃棄・機器交換は保留

メール・ファイル・脅迫文

・不審メールは本文転送ではなく**.eml／.msg のファイルで保存**（ヘッダが必要）

・同じメールを受信した人・添付を開いた人・リンクを踏んだ人をリスト化

・脅迫文は削除せず、写真＋ファイル本体を保存

・不審ファイルは被害端末から持ち出さない。やむを得ない場合はパスワード付き圧縮、他端末で開かない

バックアップ

・直近のバックアップを**上書きされない状態に**（オフライン化・書き込み禁止）。ランサムウェアはバックアップを狙う

・暗号化・削除されていないか、最終取得日時とあわせて確認・記録

・**復元は侵入経路と安全性を確認するまで行わない**

保全記録：保全した機器・媒体・ログ・写真は「何を・いつ・誰が・どこに保管したか」を記録し、施錠できる場所へ。持ち出し・受け渡しのたびに台帳に記録。警察相談や法的手続きで証拠として扱う際に必要です。**作業は必ず2名以上で行い、互いに立ち会って確認してください。**1人だけの作業は、後で証拠としての信頼性を問われる原因になります。

©1996 PSC Inc.

調査開始までに準備いただきたい情報と環境

準備チェックリスト

揃っているほど、封じ込めから復旧までが短くなります。**揃わないものは「未」のままで構いません。**

- ☐ **体制** 責任者・窓口・法務・広報・情シスの氏名と携帯番号、対応メンバー一覧
- ☐ **ネットワーク** 構成図（接続点・拠点間・DMZ・VPN・クラウド）、IPアドレス割り当て一覧
- ☐ **資産** サーバ・端末一覧（ホスト名・IP・OS・役割・場所・管理者）、仮想基盤・クラウド構成
- ☐ **認証・権限** AD／Entra ID等の構成、管理者・特権アカウント一覧、BitLocker回復キー
- ☐ **セキュリティ製品** 導入製品一覧（FW・EDR・AV・プロキシ・メール・SIEM）と管理コンソールの閲覧用アカウント
- ☐ **インシデント情報** 時系列の対応記録、被害端末一覧（隔離状況付き）、実施済み対応、検知のきっかけの原本
- ☐ **証拠** 不審メール・ファイル・脅迫文の保存場所、写真、保全記録
- ☐ **ログ** ログの所在一覧（機器名・保存場所・保持期間）、エクスポート済みログの保管場所
- ☐ **バックアップ** 最終取得日時、保管場所、健全性（暗号化・削除の有無）
- ☐ **保有情報** 影響システムが持つ個人情報・機密情報の種類と概算件数
- ☐ **作業環境** 作業スペース（机・電源・有線LAN）、入館手続き、サーバ室入室手配、リモート接続手段
- ☐ **データの受け渡し** ディスクイメージ等の大容量データを保存する媒体、または受け渡し方法の合意
- ☐ **契約・外部委託** 調査委託契約・NDAの担当者、外部委託先（保守ベンダー・MSP・クラウド事業者）の連絡先とインシデント時の協力条項（SLA）

連絡と情報統制

帯域外で連絡 メール・チャット・グループウェアが侵害されている可能性がある間は、電話・個人携帯・別テナントのツールで。社外との連絡も窓口の携帯電話が基本。

知る範囲を最小に 攻撃手法・被害範囲・対応状況を知る人を必要最小限にし、共有先を記録。

対外説明は断定しない 広報・法務と「一次回答文」を準備。原因・漏えいの有無・件数など未確定のことは断定しない。取引先・利用者への通知は内容・時期を法務・専門家と相談。

法令・契約上の報告（要否と期限を法務と確認し、調査担当にも共有）

個人情報保護委員会	報告対象の漏えい等は、速報は発覚後速やかに（概ね3～5日）、確報は30日以内（不正目的は60日以内）。本人通知も必要
監督官庁・業界団体	業法・業界ガイドラインの報告（金融、医療、重要インフラなど）
取引先	契約上の通知義務（委託契約、NDA、サービス契約のSLA）
警察	都道府県警察のサイバー犯罪相談窓口。被害届には保全した証拠が役立つ
JPCERT/CC・IPA	報告・相談。同種の攻撃情報の入手にも役立つ
保険会社	サイバー保険加入時は、事故連絡の期限と指定業者の有無を確認

専門家による調査の一般的な流れ（ご参考）

1 状況共有	2 証拠取得	3 封じ込め見直し	4 調査・報告	5 復旧・再発防止
対応記録と準備情報をもとに被害範囲・実施済み対応・優先事項を確認	メモリ・ディスクのイメージ取得、ログ収集。この段階で電源を落とすことがあります	判明した侵入経路・侵害範囲に基づき、遮断・無効化・リセットの範囲と順序を決定	侵入経路・影響範囲・持ち出しの有無を調査し、法令報告・対外説明に必要な事実を整理	安全性を確認したうえで復旧手順を決め、再発防止策を提示

※本リーフレットは一般的な初動対応の指針です。実際の対応は、被害の状況に応じて専門家にご相談ください。

©1996 PSC Inc.