

社内でセキュリティ事故が起きたら

ランサムウェア、不審メール、アカウントの乗っ取り、誤送信、紛失。どれも最初の1時間の動き方で、被害の大きさが変わります。見つけた人と担当者がやることを、順番どおりにまとめました。

担当者のあなたにとって

事故のときに困ること	このガイドがあると
社員から「何かおかしい」と言われても、何を指示すればいいかわからない	見つけた人向けの5つの動きを、そのまま伝えられます。机に貼るカードも付いています
上司に何をどう報告すればいいか迷う	第一報の型があります。分かっていることだけを書けば足ります
事故の種類ごとの対応を調べる時間がない	ランサムウェア・不審メール・乗っ取り・誤送信・紛失・Webサイトの6種類で、まずやることを1表にしています
国への報告の期限を知らずに過ぎてしまう	個人情報保護委員会のガイドラインどおりの期限を載せています
「なぜ準備していなかったのか」と言われる	経産省SCS★3の「インシデント対応手順」に沿った手順書として、平时に社内へ出しておけます

事故対応の5段階

経産省のSCS評価制度★3では、事故対応の手順に次の5つを含めるよう求めています(要求事項6-1-1)。このガイドが扱うのは①と②です。

① 発見・報告

見つけた人が、
すぐ担当者へ

② 初動

被害を広げない。
記録を残す

③ 調査・対応

原因と影響範囲を
調べる

④ 復旧

業務を元に戻す

⑤ 最終報告

経緯と再発防止を
まとめる

① 見つけた人がやること（全社員）

1. つながりを切る: LANケーブルを抜く、Wi-Fiをオフにする。電源は切らない、再起動しない
2. 触らない: ファイルやメールを消さない。自分で直そうとしない
3. メモを取る: 気づいた時刻、画面に出ている内容(スマホで撮影でよい)、直前にしたこと
4. すぐ連絡する: 担当者へ電話で。メールやチャットが使えないこともあります
5. 待つ: 担当者の指示があるまで、そのままにしておく

電源を切る・再起動すると、原因を調べる手がかりが消えることがあります。警察も「感染端末の電源オフ、再起動は厳禁」「感染端末をネットワークから隔離」と案内しています(長野県警察 サイバーセキュリティ通信、2025年3月)。

② 担当者の最初の1時間

1. 記録を始める: 連絡を受けた時刻・相手・内容をそのまま書く。国への報告期限はここから数えます
2. 責任者に第一報: 下の「第一報の型」で、分かっていることだけを伝える

- 3. 被害を広げない:端末の切り離し、乗っ取られた疑いのあるアカウントの停止・パスワード変更、外部への共有の停止
- 4. 範囲の当たりを付ける:何台か、どのアカウントか、どの情報が入っていたか
- 5. 証拠を残す:画面の写真、不審メールの原本、ログ。消さずにそのまま
- 6. 外への連絡を判断する:個人情報保護委員会・警察・取引先・保険会社に連絡が必要かを、責任者と決める
- 7. 次の報告時刻を決める:社内に「次は何時に何を報告するか」を伝える

個人情報保護委員会のガイドラインも、漏えい等が分かったときに講ずべき措置として、責任者への報告と被害拡大の防止、事実関係の調査と原因の究明、影響範囲の特定、再発防止策、報告と本人への通知を挙げています(通則編3-5-2)。

種類別：まずやること

起きたこと	まずやること	やってはいけないこと
ランサムウェア (ファイルが開けない、脅迫文が出た)	端末をネットワークから切り離す。同じネットワークの他の端末とバックアップの状態を確認する	電源を切る、再起動する。身代金の支払いを現場で決める
不審メールの添付・リンクを開いた	端末をネットワークから切り離す。入力したIDやパスワードがあれば、別の端末から変更する	メールを削除する(原本が手がかりになる)
アカウントの乗っ取り	パスワードを変更し、多要素認証を設定する。ログイン履歴と、転送設定などが勝手に変わっていないかを確認する	同じパスワードを使い回している他のサービスを放置する
メールの誤送信	送信先に削除をお願いする。送った情報の中身と件数を確認する	なかったことにする(個人データなら報告が必要な場合がある)
PC・スマホの紛失	遠隔でロック・消去する。その端末で使っていたアカウントのパスワードを変更する。警察に遺失届を出す	見つかるまで報告を待つ
Webサイトの改ざん・不正アクセス	サイトを一時的に閉じるか、制作会社・サーバー会社に連絡する。管理画面のパスワードを変更する	痕跡を消して元に戻すだけで終える

第一報の型（責任者へ）

件名：【第一報】セキュリティ事故の可能性（【月日 時刻】発見）

■何が起きたか

【部署・氏名】から【月日 時刻】に連絡あり。【例：PCに脅迫文が表示された】。

■今の状態

- ・影響を受けた端末・アカウント：【例：PC 1台、メールアカウント 1つ】
- ・入っていた情報：【例：顧客名簿 約〇件／不明】
- ・とった対応：【例：ネットワークから切り離し済み、電源は入れたまま】

■これからやること

- ・影響範囲の確認。次の報告は【月日 時刻】

■判断をお願いしたいこと

- ・外部（個人情報保護委員会・警察・取引先）への連絡の要否

【氏名】

国への報告が必要なとき

個人データについて次のどれかに当たる場合は、個人情報保護委員会への報告と本人への通知が必要です。期限は、社内のいずれかの部署が知った時点から数えます。

No	報告が必要な事態
1	要配慮個人情報が含まれる個人データの漏えい等（おそれを含む）
2	不正に使われると財産的被害が出るおそれがある個人データの漏えい等
3	不正の目的で行われたおそれがある漏えい等（不正アクセス・ランサムウェアなど）
4	本人の数が1,000人を超える漏えい等

0日目

社内の誰かが知った時点

概ね3～5日以内

速報（分かっている範囲で）

速やかに

本人への通知（状況に応じて）

30日以内

確報（不正の目的のおそれがある場合は60日以内）

平時にやっておくこと

準備	これで変わること	SCS
事故の連絡網を作る（不在時の代わりの人まで）	夜間・休日でも止まらない	★3 6-1-1
この手順と報告様式を社内に配り、年1回見直す	見つけた人が迷わない	★3 6-1-1

入社時と年1回、事故時の対応を研修する(記録を残す)	報告が早くなる	★3 4-2-2
バックアップを取り、戻せるか試しておく	ランサムウェアでも業務を戻せる	★3 4-3-4 ★3 7-1-1
机に「初動カード」を貼っておく	最初の5分を間違えない	★3 6-1-1

相談先

相談先	こんなとき
警察(都道府県警察のサイバー犯罪相談窓口)	ランサムウェア・不正アクセスなど、犯罪の可能性があるとき
個人情報保護委員会(漏えい等報告フォーム)	上の4つの事態に当たるとき
IPA 情報セキュリティ安心相談窓口	技術的な対処を相談したいとき
JPCERT/CC(インシデント報告)	不正アクセスなどの技術的な調整が必要なとき
Moshiru(moshiru.com/ info@moshiru.com)	何から手を付けるか一緒に整理したいとき。社内報告・取引先への説明・報告書の文面づくりを、打合せなし・テキストで支援します。初動の相談は無料です

このガイドについて

- ・経済産業省「SCS評価制度」★3 要求事項6-1-1(インシデント対応手順)、個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン(通則編)」3-5(2026年6月一部改正)に沿って作成しています。法的な判断が必要なときは、弁護士や個人情報保護委員会に確認してください
- ・改正個人情報保護法(令和8年法律第56号)の規則が決まったら、報告の扱いを見直します
- ・出典:IPA SCS評価制度 要求事項・評価基準(2026年3月27日版)
<https://www.ipa.go.jp/security/scs/rcu1hd0000007a2i-att/20260327001-c.xlsx> / 個人情報保護委員会
 通則編ガイドライン https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/ / 長野県警察
 サイバーセキュリティ通信(2025年3月27日)
<https://www.pref.nagano.lg.jp/police/anshin/cyber/documents/r7cyberdayori4.pdf>
- ・作成:Moshiru(岡崎悠太)。無料で使えます。社内で自由に改変・配布して構いません