異変に気づいたら、まず連絡

対象：一般の業務PC・メール・クラウド・Webサイト。自社の緊急手順に沿って使用。

不正アクセス・情報漏えいが疑われたら

第一報は「いつ・何に・何が・何をしたか」

発見時刻／対象／見つけた異変／実施済み操作を伝えます。
不明点は「未確認」と記載。全項目が埋まる前に連絡できます。

対応責任者・確認済みの連絡先：

不在時の代行者・確認済みの連絡先：

連絡と認められた緊急措置を進め、次を並行して行います

拡大防止	通信・接続・公開範囲を制限
記録保全	ログ・画面・操作と取得条件を保存
報告判断	認知日時・該当性・担当・期限を確認

対応の6ステップ

1 第一報 → 2 役割決定 → 3 拡大防止 → 4 記録保全
→ 5 外部相談・報告 → 6 継続対応への引き継ぎ
番号は説明の順番です。前の記入完了を待たずに並行して対応します。

一般PCは利用を止め、社内手順に沿って通信を隔離。電源断・再起動は、被害と記録保全への影響を管理者が判断します。医療・制御設備等は専用の緊急手順へ。ログ削除や、原因未確認のままの再開を独断で進めないでください。

役割と緊急連絡先

平時に記入し、PCや社内メールが使えなくても参照できる場所へ保管します。

会社・部署／更新日／更新者：

対応責任者：判断できる範囲／連絡先

代行者：引き継ぐ条件／連絡先

操作担当：管理できる対象／代行先

記録・連絡担当：記録の保存先／連絡先

経営・個人情報管理・法務：担当／相談先

保守会社・技術支援先：サービス／窓口／時間外窓口

委託元・取引先・保険等：連絡条件／窓口

契約識別情報・緊急手順・記録票の保管場所：

パスワードや秘密鍵は記載せず、権限を限定した保管先を参照します。

警察・JPCERT/CC・行政の公式窓口：12ページの出典リンクから確認。
事故時は送信だけで終えず、受領・受付番号・次の回答時刻を記録します。

社内第一報の記入票

不明点は未確認と記入。行政の公式報告様式の代わりには使いません。

件名：【至急・状況確認依頼】対象／確認した異変

発見日時・タイムゾーン／発見者・折り返し先

対象の端末・アカウント・サービス・URL

確認した事実

根拠となる画面・通知・ログの保管先

実施済みの操作・実施者・時刻

現在の業務影響

まだ分からないこと／依頼したい対応

受領した責任者・受領時刻／次の状況確認時刻

架空の記入例

17時10分（日本時間）、顧客管理画面にログインとデータ出力の記録を確認。操作した人物、出力対象、外部流出は未確認。画面を保存し、設定変更はしていません。管理者による確認をお願いします。

保守会社への保全・対応依頼票

責任者が依頼範囲と費用条件を確認。記録の完成を待って拡大防止を遅らせません。

宛先・サービス・契約識別情報

確認した事象・発見日時・タイムゾーン

現在の制限・停止状況／業務への影響

保全を依頼する対象・期間（開始〜終了、タイムゾーン）

取得できるログ種別・期間・取得条件・保存先／未取得範囲

不正なアクセスを制限する方法・影響／現状変更前の保全方針

当社の判断担当・安全な折り返し先／不明な範囲

送信・受領時刻／受付番号／次の回答時刻・担当

依頼文の冒頭例：上記の事象を確認しました。関連ログの保全、不正なアクセスの制限方法、現状変更・復旧前の保全方針について、対応可否をご連絡ください。

対応経過・証跡の台帳

発生時刻と取得・操作時刻を分け、タイムゾーンを記入。続きはこのページを複製。

対応経過：何が起き、誰が何をしたか

時刻・時差 発生／実施	事象・操作 実施者	結果・不明点	証跡番号 次の担当

証跡：取得条件と原記録の所在

番号・取得者 取得日時	取得元・対象期間 取得条件	原記録の保管先 共有用コピー	未取得・欠落

原記録は閲覧者を限定して保存。共有用コピーで必要な情報だけを渡し、共有先・日時も記録します。保存期間切れや未記録の範囲は、被害がないことの根拠にしません。

社外報告・本人通知の判断票

民間企業の個人データ漏えい等を想定。該当性は公式資料と個別の事実を照合します。

報告対象の4類型：漏えい等のおそれも含む

①要配慮個人情報を含む ②財産的被害のおそれ
③不正目的の行為によるおそれ ④本人の数が1,000人を超える
漏えいだけでなく、滅失・毀損とそのおそれも確認。人数と件数、暗号化等の条件を区別します。

対象データ／人数・件数／該当類型・判断根拠・不明点：

報告対象事態を知った日時・タイムゾーン／部署／判断者：

報告・通知	時期	期限・担当・提出状況
速報	知った後、速やかに。概ね3〜5日以内は目安。	
確報	知った日から30日以内。不正目的の行為による類型は60日以内。	
本人通知	報告対象事態について、状況に応じて速やかに。	

認知の基準は、法人のいずれかの部署が当該事態を知った時点。確報は認知日を1日目とする扱い等を確認。本人通知と一般公表は別に判断します。

委託先の報告義務の免除は、報告義務を負う委託元へ、把握済みの法定事項を速やかに通知した場合。通知内容と受領を記録し、委託元の報告に協力します。業法・契約の条件も確認。出典：12ページ S03〜05。

社外連絡台帳：続きは余白または別紙へ

相手・目的 必要性と根拠	内容・担当 承認者	期限・実施時刻 受付・次の対応

初動確認チェックリスト 01〜08

完了＝判断・操作と根拠を確認。不明点は別途記録。完了数は安全度や終結の判定ではありません。

状態は該当する欄にチェック。根拠欄に証跡番号・不明点・対象外の理由を記入。

01 発見日時と対象を記録した

残す根拠：日時・タイムゾーン、端末名・アカウント・URL等

☐ 完了 ☐ 対応中 ☐ 未着手 ☐ 対象外 担当 期限

根拠・不明点等

02 確認済みの事実と不明点を分けた

残す根拠：通知・画面・ログの内容と、未確認事項の一覧

☐ 完了 ☐ 対応中 ☐ 未着手 ☐ 対象外 担当 期限

根拠・不明点等

03 責任者または代行者へ第一報を伝えた

残す根拠：宛先、連絡方法、受領時刻

☐ 完了 ☐ 対応中 ☐ 未着手 ☐ 対象外 担当 期限

根拠・不明点等

04 侵害が疑われる経路以外で連絡できる

残す根拠：確認済みの電話番号等と連絡先

☐ 完了 ☐ 対応中 ☐ 未着手 ☐ 対象外 担当 期限

根拠・不明点等

05 対応責任者と代行者を決めた

残す根拠：氏名、判断できる範囲、連絡先

☐ 完了 ☐ 対応中 ☐ 未着手 ☐ 対象外 担当 期限

根拠・不明点等

06 操作担当と記録・連絡担当を決めた

残す根拠：担当者名と役割

☐ 完了 ☐ 対応中 ☐ 未着手 ☐ 対象外 担当 期限

根拠・不明点等

07 いま被害が広がる経路を確認した

残す根拠：通信、サインイン、公開範囲等の確認結果・不明点

☐ 完了 ☐ 対応中 ☐ 未着手 ☐ 対象外 担当 期限

根拠・不明点等

08 対象の隔離・制限を実施または判断した

残す根拠：操作内容と結果、未実施なら理由・代替策・次の担当

☐ 完了 ☐ 対応中 ☐ 未着手 ☐ 対象外 担当 期限

根拠・不明点等

初動確認チェックリスト 09〜16

完了＝判断・操作と根拠を確認。不明点は別途記録。完了数は安全度や終結の判定ではありません。

状態は該当する欄にチェック。根拠欄に証跡番号・不明点・対象外の理由を記入。

09 アカウントの残るアクセス経路を確認した

残す根拠：セッション、認証方法、APIキー、転送、連携アプリ等の確認結果

☐ 完了 ☐ 対応中 ☐ 未着手 ☐ 対象外 担当 期限

根拠・不明点等

10 関係するほかの対象を確認した

残す根拠：他端末・管理者・サービス・共通DB権限等への影響と調査範囲

☐ 完了 ☐ 対応中 ☐ 未着手 ☐ 対象外 担当 期限

根拠・不明点等

11 電源断・再起動・削除等の操作を管理した

残す根拠：操作の有無、判断者、時刻、保全への影響

☐ 完了 ☐ 対応中 ☐ 未着手 ☐ 対象外 担当 期限

根拠・不明点等

12 原記録の保管先と閲覧権限を決めた

残す根拠：保管先、責任者、アクセス範囲

☐ 完了 ☐ 対応中 ☐ 未着手 ☐ 対象外 担当 期限

根拠・不明点等

13 必要なログと保存期限を確認した

残す根拠：ログ種別、取得期間、保全依頼先、未取得範囲

☐ 完了 ☐ 対応中 ☐ 未着手 ☐ 対象外 担当 期限

根拠・不明点等

14 事象と対応を時系列に記録した

残す根拠：時刻、実施者、操作・連絡、結果、証跡参照

☐ 完了 ☐ 対応中 ☐ 未着手 ☐ 対象外 担当 期限

根拠・不明点等

15 対象データと影響人数の確認を始めた

残す根拠：情報の種類、件数・人数の区別、確認方法と不明点

☐ 完了 ☐ 対応中 ☐ 未着手 ☐ 対象外 担当 期限

根拠・不明点等

16 外部支援先へ依頼し受領を確認した

残す根拠：依頼内容、受付番号、応答、次の連絡予定。不要なら判断理由

☐ 完了 ☐ 対応中 ☐ 未着手 ☐ 対象外 担当 期限

根拠・不明点等

初動確認チェックリスト 17〜24

完了＝判断・操作と根拠を確認。不明点は別途記録。完了数は安全度や終結の判定ではありません。

状態は該当する欄にチェック。根拠欄に証跡番号・不明点・対象外の理由を記入。

17 犯罪が疑われる場合の警察相談を判断した

残す根拠：相談先、相談内容・時刻、または判断理由

☐ 完了 ☐ 対応中 ☐ 未着手 ☐ 対象外 担当 期限

根拠・不明点等

18 漏えい等の報告対象と期限を確認した

残す根拠：4類型の検討、認知日時、判断者、報告先と期限

☐ 完了 ☐ 対応中 ☐ 未着手 ☐ 対象外 担当 期限

根拠・不明点等

19 本人通知と公表をそれぞれ判断した

残す根拠：対象、必要性、内容、時期、窓口、承認者

☐ 完了 ☐ 対応中 ☐ 未着手 ☐ 対象外 担当 期限

根拠・不明点等

20 委託元・取引先等への連絡条件を確認した

残す根拠：契約・業法・保険等の条件、担当、期限

☐ 完了 ☐ 対応中 ☐ 未着手 ☐ 対象外 担当 期限

根拠・不明点等

21 停止範囲と業務の継続方法を決めた

残す根拠：停止対象、影響業務、認められた代替手段、顧客案内

☐ 完了 ☐ 対応中 ☐ 未着手 ☐ 対象外 担当 期限

根拠・不明点等

22 再開の判断者と確認条件を決めた

残す根拠：入口修正・残存経路・保全・業務動作・監視・再停止条件

☐ 完了 ☐ 対応中 ☐ 未着手 ☐ 対象外 担当 期限

根拠・不明点等

23 未完了項目に担当者と期限を付けた

残す根拠：作業内容、実名の担当、期限、必要な回答

☐ 完了 ☐ 対応中 ☐ 未着手 ☐ 対象外 担当 期限

根拠・不明点等

24 次の担当者への引き継ぎを確認した

残す根拠：引き継ぎ票、受領者・時刻、次の状況確認時刻

☐ 完了 ☐ 対応中 ☐ 未着手 ☐ 対象外 担当 期限

根拠・不明点等

継続対応への引き継ぎ票

次の担当者が、確認済みの事実と未完了の作業を区別して続きを始めるための記録。

事案の名称・管理番号／引き継ぎ日時・時差

前任者・後任者／安全な連絡方法

確認済みの事実と根拠（証跡番号・保管先）

不明点と次に必要な確認

隔離・停止・制限中の対象／継続できる業務・代替手段

実施済み操作と結果／記録の保管先

外部連絡・法定報告・本人通知・公表の状況と期限

再開の判断者・確認条件／再停止する条件（詳細は11ページ）

受領確認（氏名・時刻）／次の状況確認時刻・連絡方法

再開条件と未完了作業

技術担当の確認結果を受け、責任者が再開を判断。残る影響と判断理由も記録します。

再開前の確認	確認結果・根拠／未完了の影響
入口修正・不正ファイル等の残存確認	
必要な記録の保全	
復元元の妥当性・対象時点	
鍵・セッション・関連サービスの確認	
認証情報更新後の業務・連携の完了	
再開後の監視・担当・再停止条件	

再開する範囲／判断者／日時／判断理由：

未完了の作業：誰が、いつまでに確認するか

未完了の作業・不明点	担当者	期限／必要な回答

次の状況確認時刻・参加者／追加の連絡が必要になる条件：

出典・版と、平時の準備

資料名から一次資料を開きます。2026年10月21日版。確認日は資料ごとに記載。

S01 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	10/16確認
S02 JPCERT/CC インシデントハンドリングマニュアル	10/16確認
S03 個人情報保護委員会 通則編（3-5 漏えい等への対応）	10/21再確認
S04 個人情報保護委員会 漏えい等の対応とお役立ち資料	10/16確認
S05 個人情報保護委員会 漏えい等報告・本人への通知の義務化	10/21再確認
S06 Microsoft 365 侵害されたメールアカウントへの対応	10/21再確認
S07 Microsoft Entra ID 緊急時のユーザーアクセス取り消し	10/21再確認
S08 JPCERT/CC 高度サイバー攻撃への対処におけるログの活用	10/16確認
S09 警察庁 サイバー事案に関する相談窓口	10/21再確認
S10 JPCERT/CC インシデント相談・情報提供	10/21再確認
S11 サイバー攻撃被害に係る情報の共有・公表ガイダンス	10/16確認
S12 NIST SP 800-61 Rev. 3（2025年最終版）	10/16確認
S13 IPA 経営者向けインシデント対応机上演習	10/16確認
S14 アルカディア 不正アクセスの経過と当社の対処について（10月19日）	10/20確認

6ステップ・24項目・記入票は、資料を踏まえてレイズが編集した実務用の整理です。社内第一報・判断票は行政の公式様式ではありません。法令・窓口・製品の操作条件は利用時に公式情報を確認してください。

自社の版・見直し日／記入・管理責任者／社内保管場所：

連絡先を埋め、操作権限を確認し、架空の事案で記入して手順を直します。

公開Web設定も、無料で点検できます

初動と調査を進めた後の改善に。公開Web情報を対象とする検査で、端末感染や情報漏えいの有無を判定するものではありません。事故対応中は管理者と実施時期・範囲を確認してください。

自社サイトの無料AIセキュリティ検査 →