情報漏洩対応チェックリスト

メール誤送信・web誤公開の場合

誤送信・誤公開とは？

（例1）： 電子メールの宛先を間違えて送信する
（例2）： Webの設定ミスによる、非公開情報の公開

真っ先にすべき対応は？

→メール宛先ミスの場合は、送付先へ削除依頼
→web上で誤公開の場合は、すみやかに情報の削除

＜発覚＞

☐ **発覚した経緯は、次のうちどれですか？**

・本人の自己申告
・ミスを発見した第3者からの連絡
→ 連絡先を控える

＜初動と1次対応＞

☐ **誤送信・誤公開したのは自社の情報だけですか、他社の情報も含まれますか？**

※ 業務委託先の情報なら、他社の情報になります
→ 他社の情報が含まれる場合は、情報の所有者に連絡します

☐ **誤送信・誤公開された情報は、どのような内容ですか？**

☐ 個人情報が含まれますか？

・個人情報とは、取引先・社員など個人に関する情報です
→ 個人情報の漏えいは、個人情報保護法に準拠した対応が必要です
☐ 個人情報は何件程度の数（情報量）ですか？（基準：1000人を超えるか）
☐ 個人情報は要配慮個人情報が含まれていますか？（人種、病歴など）
☐ 個人情報は財産的被害が生じる恐れがありますか？（カード情報など）
☐ 個人情報は不正目的をもって行われた漏洩でしたか？
※ 上記に該当する場合、個人情報保護委員会への報告義務が発生します
速報として、概ね3～5日以内に報告が必要となります

☐ クレジットカードなどの金融情報が含まれますか？

→ 含まれる場合は、カード会社など金融機関に連絡します

☐ 公共性の高い情報が含まれますか？

・公共性の高い情報とは発電所、通信設備のように社会インフラに影響する情報です
→ 特別法などの規制がある場合、法令に則った対応になります

☐ 取引先の情報が含まれますか？

→ 取引先に連絡し、先方の意向に沿った対応をします

☐ 機密情報が含まれますか？

・機密情報とは図面データなど、外部に出せない情報です

→ 機密性の重要度に応じて、経営判断をします

☐ 誤送信・誤公開された、情報のタイプは？

☐ メールには添付ファイルがありましたか？

☐ 関連リンクがありましたか？

☐ Webにはダウンロードできるファイルがありましたか？

☐ 誤送信・誤公開された情報は、何らかの形で保護されていましたか？

・パスワードで保護されていた

・暗号化されていた

・何ら保護はなく、平文の状態だった

☐ 誤送信・誤公開に気づいたのは、何月何日何時ですか？

☐ なぜ、誤送信・誤公開が起きてしまったのですか？

・単純な操作ミス、確認不足など

・システムの不具合

・運用ルールの違反（公開・送信時のダブルチェックなど規定作業の未実施など）

<1次対応のまとめ>

→ 誤公開（自社サイト）の場合、すぐに情報を削除するか、アクセスを制限します

→ 誤公開（他社サイト）の場合、すぐに情報の削除を依頼します

→ メール誤送信の場合、受信者にお詫びし、メールの削除を依頼します

<検討と公表>

→ 予想される2次被害を確します

→ 事態の重要度を判断します

→ 個人情報が含まれる場合には、本人への通知とお詫びをします

→ クレジットカード情報など、金融情報が含まれる場合は、カード停止を促すよう対応します

→ 漏洩規模や社会的影響など必要に応じて、監督官庁（例：クレジットカード情報など、金融情報が含まれる場合は金融庁）および 個人情報保護委員会 に届け出ます

→ 社会的な影響が大きいと判断した場合は、Webなどを通じて公表します

<復旧>

→ システムの不具合が原因の場合、プログラムを修正し、システムを復旧させます

→ Webページの設定を確認し、正しく表示されていることを確認します

→ 検索サイトに残ったキャッシュを削除します

＜再発防止＞

→ 違反や管理ミスがあった場合は、適切な処分を行います

→ 情報管理の作業手順やチェックの仕組みを見直します

紛失・盗難の場合

紛失・盗難とは？

（例1）： PCの入った鞄を電車に置き忘れる

（例2）： ポケットにいれたUSBメモリがないことに気づく

真っ先にすべき対応は？

→対象物（PC、スマホ等）のアカウント停止、ログインパスワードの変更

＜発覚＞

☐ **発覚した経緯は、次のうちどれですか？**

・紛失者の自己申告

→紛失した場所の管理者（鉄道会社の窓口、店舗の担当者など）へ連絡

・警察からの連絡

→警察の連絡先を書き留める

・取得者からの連絡

→取得者の連絡先を書き留める

＜初動と1次対応＞

☐ **失ったのは、自社の情報だけですか、他社の情報も含まれますか？**

※ 業務委託先の情報なら、他社の情報になります

→ 他社の情報が含まれる場合は、情報の所有者に連絡します

☐ **紛失・盗難にあった対象物（PC、スマホ、USBメモリなど）は、なにですか？**

☐ 対象物には、シリアルナンバーなど、識別できる記号がありましたか？

☐ 対象物のメーカー名、モデル名、色、サイズなど、特徴を詳しく教えてください

→対象物（PC、スマホ等）のアカウント停止、ログインパスワードの変更

☐ **失った情報は、どのような内容ですか？**

☐ 個人情報が含まれますか？

・個人情報とは、取引先・社員など個人に関する情報です

→個人情報の漏えいは、個人情報保護法に準拠した対応が必要です

☐ 個人情報は何件程度の数（情報量）ですか？（基準：1000人を超えるか）

□ 個人情報は要配慮個人情報が含まれていますか？（人種、病歴など）
□ 個人情報は財産的被害が生じる恐れがありますか？（カード情報など）
□ 個人情報は不正目的をもって行われた漏洩でしたか？
※ 上記に該当する場合、個人情報保護委員会への報告義務が発生します。
速報として、概ね3～5日以内に報告が必要となります。

□ クレジットカードなどの金融情報が含まれますか？
→ 含まれる場合は、カード会社など金融機関に連絡します

□ 公共性の高い情報が含まれますか？
・公共性の高い情報とは発電所、通信設備のように社会インフラに影響する情報です
→特別法などの規制がある場合、法令に則った対応になります

□ 取引先の情報が含まれますか？
→取引先に連絡し、先方の意向に沿った対応をします

□ 機密情報が含まれますか？
・機密情報とは図面データ等、外部に出せない情報です
→機密性の重要度に応じて、経営判断をします

□ 失った情報は、パスワードなどで保護されていましたか？
・パスワードで保護されていた
・暗号化されていた
・何ら保護はなく、平文の状態だった

□ 紛失・盗難にあった対象物は、鞄や入れ物に入っていましたか？
□ 鞄や入れ物の特徴（色、形、素材など）を詳しく教えてください

□ 紛失・盗難に気づいたのは、何月何日何時ですか？

□ 失った場所は、どこですか？
→鉄道、店舗に連絡します

□ なぜ、紛失・盗難にあってしまったのですか？
（例：眠ってしまった、トイレで席を外したなど、その時の状況を詳しく）

<1次対応のまとめ>
→対象物（PC、スマホ等）のアカウント停止、ログインパスワードの変更
→他社の情報が含まれる場合は、情報の所有者に連絡します
→鉄道、店舗に連絡します
→警察に届け出ます
→紛失盗難にあった機器が、オークションや中古市場に出回っていないか確認します

＜検討と公表＞

→ 予想される2次被害を確します
→ 事態の重要度を判断します
→ 個人情報が含まれる場合には、本人への通知とお詫びをします
→ クレジットカード情報など、金融情報が含まれる場合は、カード停止を促すよう対応します
→ 漏洩規模や社会的影響など必要に応じて、監督官庁(例:クレジットカード情報など、
金融情報が含まれる場合は金融庁) および 個人情報保護委員会 に届け出ます
→ 社会的な影響が大きいと判断した場合は、Webなどを通じて公表します

＜再発防止＞

→自社の情報管理ポリシーに則り、再発防止策を講じ、周知徹底します

外部攻撃の場合

外部攻撃の場合とは？

(例1)： ウィルス等の不正プログラムに感染し、情報が漏洩した場合
(例2)： システムの脆弱性等から外部者の不正アクセスを許し、情報が漏えいした場合

真っ先にすべき対応は？

→ **不正アクセスがあった機器・サイトの停止、ないしは隔離(他のネットワークから切断)**

＜発覚＞

☐ **発覚した経緯は、次のうちどれですか？**

・風評を含む外部からの指摘
→ 指摘してくれた方の連絡先を書き留める
・ウィルス対策ソフト、ネットワーク監視サービスなどからの連絡
・ランサムウェアによる身代金要求があった

＜初動と1次対応＞

☐ **失ったのは、自社の情報だけですか、他社の情報も含まれますか？**

※ 業務委託先の情報なら、他社の情報になります
→ 他社の情報が含まれる場合は、情報の所有者に連絡します。

☐ **外部攻撃を受けた機器は、なにですか？**

→ 対象物(PC、スマホなど)のアカウント停止、ログインパスワードの変更
→ 対象物(PC、スマホなど)のネットワークからの切り離し

☐ **外部攻撃を受けた範囲は、どこまでですか？(ネットワークのすべてなのか、一部なのか？)**

→ 攻撃を受けたネットワークのサービス停止、外部からの隔離

□ 漏洩した情報は、どのような内容ですか？

□ 個人情報が含まれますか？

・個人情報とは、取引先・社員など個人に関する情報です

→ 個人情報の漏えいは、個人情報保護法に準拠した対応が必要です

□ 個人情報は何件程度の数（情報量）ですか？（基準：1000人を超えるか）

□ 個人情報は要配慮個人情報が含まれていますか？（人種、病歴など）

□ 個人情報は財産的被害が生じる恐れがありますか？（カード情報など）

□ 個人情報は不正目的をもって行われた漏洩でしたか？

※ 上記に該当する場合、個人情報保護委員会への報告義務が発生します。
速報として、概ね3～5日以内に報告が必要となります。

□ クレジットカードなどの金融情報が含まれますか？

→ 含まれる場合はカード会社など、金融機関に連絡します

□ 公共性の高い情報が含まれますか？

・公共性の高い情報とは発電所、通信設備のように社会インフラに影響する情報です

→ 特別法などの規制がある場合、法令に則った対応になります

□ 取引先の情報が含まれますか？

→ 取引先に連絡し、先方の意向に沿った対応をします

□ 機密情報が含まれますか？

・機密情報とは図面データなど、外部に出せない情報です

→ 機密性の重要度に応じて、経営判断をします

□ 漏洩した情報は、パスワードなどで保護されていましたか？

・パスワードで保護されていた

・暗号化されていた

・何ら保護はなく、平文の状態だった

□ 外部攻撃に気づいたのは、何月何日何時ですか？

＜調査・検討＞

→ 漏洩情報の内容から事態の深刻度を判断します

→ 必要に応じて専門業者に調査を依頼します

・JPCERT　※主に不正アクセス、マルウェア感染、DoS/DDoS攻撃などに対応
https://www.jpcert.or.jp/

・JNSA：サイバーインシデント緊急対応企業一覧
https://www.jnsa.org/emergency_response/

→ 必要に応じて警察（警察庁サイバー警察局）に相談します

・警視庁：サイバー警察局　相談窓口
https://www.npa.go.jp/bureau/cyber/soudan.html

→ サーバーなどに残された情報はバックアップをとり、証拠を保全します

→ 実態が解明されるまでは、システムの再稼働は控えます

→ バックアップに不正プログラムがないことを確認し、
再発防止措置を取った後、システムを復旧します

＜公表＞

→ 他社の情報が含まれる場合は、情報の所有者に連絡します

→ 個人情報が含まれる場合には、本人への通知とお詫びをします

→ クレジットカード情報など、金融情報が含まれる場合は、カード停止を促すよう対応します

→ 漏洩規模や社会的影響など必要に応じて、監督官庁（例：クレジットカード情報など、
金融情報が含まれる場合は金融庁）および 個人情報保護委員会 に届け出ます

→ 社会的な影響が大きいと判断した場合は、Webなどを通じて公表します

＜再発防止＞

→ 自社の情報管理ポリシーに則り、再発防止策を講じ、周知徹底します

・システムの脆弱性修正、パッチ適用など

・ウィルス対策ソフトの導入、変更、最新化の徹底など

・フィッシングサイト、標的型メールに対応した定期的な教育など

→ 必要に応じて、情報漏洩の被害にあった方へ補償をします

内部犯行の場合

内部犯行とは？

・内部の人間が不正に情報を持出し、外部の業者等に販売・譲渡するケースです

真っ先にすべき対応は？

→ 対象サイト（ファイルサーバーなど）の停止、アクセス制限

→ 内部犯行者が使用した機器の確保（証拠の保全）

＜発覚＞

□ 発覚した経緯は、次のうちどれですか？

・顧客からの連絡（架空請求を受けた、個人情報が不正に利用されているなど）

→ 連絡先を控える

・マスコミからの連絡

→ 連絡先を控える

・情報が漏洩しているとの風評が広まった

・名簿を買い取るよう、脅迫を受けた

＜初動と1次対応＞

□ 内部犯行の当事者が、まだ社内にいる可能性がありますか？

・まだ社内にいる可能性あり（特定できない場合は、いることを想定する）

→ 証拠隠滅されないよう注意する

・社内にいる可能性はない

→ 以下のプロセスへ

□ 持ち出された情報は、自社の情報だけですか、他社の情報も含まれますか？

※ 業務委託先の情報なら、他社の情報になります

→ 他社の情報が含まれる場合は、情報の所有者に連絡します

□ 漏洩した情報の保管場所は、どこですか？

→ 対象サイト（ファイルサーバーなど）

該当サイト（サーバー）の停止、アクセス制限

→ 執務室、倉庫、書類保管場所（※物理的な書類など）

立ち入り制限もしくは残りの書類を施錠できる場所に退避

□ なにを（PC、USBメモリ、紙など）を、持ち出されましたか？

□ 持ち出された情報は、どのような内容ですか？

□ 個人情報が含まれますか？

・個人情報とは、取引先・社員など個人に関する情報です

→ 個人情報の漏えいは、個人情報保護法に準拠した対応が必要です

□ 個人情報は何件程度の数（情報量）ですか？（基準：1000人を超えるか）

□ 個人情報は要配慮個人情報が含まれていますか？（人種、病歴など）

□ 個人情報は財産的被害が生じる恐れがありますか？（カード情報など）

□ 個人情報は不正目的をもって行われた漏洩でしたか？

※ 上記に該当する場合、個人情報保護委員会への報告義務が発生します。

速報として、概ね3～5日以内に報告が必要となります。

□ クレジットカードなどの金融情報が含まれますか？

→ 含まれる場合は、カード会社など金融機関に連絡します

□ 公共性の高い情報が含まれますか？

・公共性の高い情報とは、発電所、通信設備のように社会インフラに影響する情報です

→ 特別法などの規制がある場合、法令に則った対応になります

□ 取引先の情報が含まれますか？

→ 取引先に連絡し、先方の意向に沿った対応をします

□ 機密情報が含まれますか？

・機密情報とは、図面データなど外部に出せない情報です

→ 機密性の重要度に応じて、経営判断をします

□ 持ち出された情報は、保管時に何らかの形で保護（対策）されていましたか？

・パスワードで保護されていた

・暗号化されていた

・何ら保護はなく、平文の状態だった

・施錠できる適切な場所で保管されていた

・だれでも閲覧できる場所に置かれていた

□ 内部犯行に気づいたのは、何月何日何時ですか？

＜調査・検討＞

→ 漏洩情報の内容から事態の深刻度を判断します

→ 必要に応じて専門業者に調査を依頼します

・JPA：情報セキュリティに関する技術的なご相談

https://www.jpcert.or.jp/

・JNSA ：サイバーインシデント緊急対応企業一覧

https://www.jnsa.org/emergency_response/

→ 必要に応じて警察（警察庁サイバー警察局、不正アクセス対策）に相談します

・警視庁 ：サイバー警察局 不正アクセス対策

https://www.npa.go.jp/bureau/cyber/countermeasures/unauthorized-access.html

→ サーバーなどに残された情報はバックアップをとり、証拠を保全します

→ 実態が解明されるまでは、システムの再稼働は控えます

→ バックアップに不正プログラムがないことを確認し、
再発防止措置を取った後、システムを復旧します
また、脆弱性等の解消（改修、パッチ適用）を行います

＜公表＞

→ 他社の情報が含まれる場合は、情報の所有者に連絡します

→ 個人情報が含まれる場合には、本人への通知とお詫びをします

→ クレジットカード情報など、金融情報が含まれる場合は、カード停止を促すよう対応します

→ 漏洩規模や社会的影響など必要に応じて、監督官庁（例：クレジットカード情報など、
金融情報が含まれる場合は金融庁） および 個人情報保護委員会 に届け出ます

→ 社会的な影響が大きいと判断した場合は、Webなどを通じて公表します

<再発防止>

→ 自社の情報管理ポリシーに則り、再発防止策を講じ、周知徹底します

・情報へのアクセス件の見直し

・システムの脆弱性が原因の場合は、改修やパッチ適用

・重要情報を扱う業務での相互牽制できる体制の構築

・外部記憶装置（外付けHDD、USBメモリ）を制限するツールの導入

・クラウドストレージへのアクセスを制限する

・書類等の保管ルール（施錠できる場所への保管、鍵の管理など）

→ 必要に応じて、情報漏洩の被害にあった方へ補償をします

※本チェックシートは情報漏洩被害の対応すべてを担保するものではありません。

本シートをご参考に、お客様のご状況に合わせて加工のうえご利用ください。　2024年2月

情報漏洩対応チェックリスト

メール誤送信・web誤公開の場合

誤送信・誤公開とは？

（例1）： 電子メールの宛先を間違えて送信する
（例2）： Webの設定ミスによる、非公開情報の公開

真っ先にすべき対応は？

→メール宛先ミスの場合は、送付先へ削除依頼
→web上で誤公開の場合は、すみやかに情報の削除

＜発覚＞

☐ **発覚した経緯は、次のうちどれですか？**

・本人の自己申告
・ミスを発見した第3者からの連絡
→ 連絡先を控える

＜初動と1次対応＞

☐ **誤送信・誤公開したのは自社の情報だけですか、他社の情報も含まれますか？**

※ 業務委託先の情報なら、他社の情報になります
→ 他社の情報が含まれる場合は、情報の所有者に連絡します

☐ **誤送信・誤公開された情報は、どのような内容ですか？**

☐ 個人情報が含まれますか？

・個人情報とは、取引先・社員など個人に関する情報です
→ 個人情報の漏えいは、個人情報保護法に準拠した対応が必要です
☐ 個人情報は何件程度の数（情報量）ですか？（基準：1000人を超えるか）
☐ 個人情報は要配慮個人情報が含まれていますか？（人種、病歴など）
☐ 個人情報は財産的被害が生じる恐れがありますか？（カード情報など）
☐ 個人情報は不正目的をもって行われた漏洩でしたか？
※ 上記に該当する場合、個人情報保護委員会への報告義務が発生します
速報として、概ね3～5日以内に報告が必要となります

☐ クレジットカードなどの金融情報が含まれますか？

→ 含まれる場合は、カード会社など金融機関に連絡します

☐ 公共性の高い情報が含まれますか？

・公共性の高い情報とは発電所、通信設備のように社会インフラに影響する情報です
→ 特別法などの規制がある場合、法令に則った対応になります

☐ 取引先の情報が含まれますか？

→ 取引先に連絡し、先方の意向に沿った対応をします

□ 機密情報が含まれますか？

・機密情報とは図面データなど、外部に出せない情報です

→ 機密性の重要度に応じて、経営判断をします

□ 誤送信・誤公開された、情報のタイプは？

□ メールには添付ファイルがありましたか？

□ 関連リンクがありましたか？

□ Webにはダウンロードできるファイルがありましたか？

□ 誤送信・誤公開された情報は、何らかの形で保護されていましたか？

・パスワードで保護されていた

・暗号化されていた

・何ら保護はなく、平文の状態だった

□ 誤送信・誤公開に気づいたのは、何月何日何時ですか？

□ なぜ、誤送信・誤公開が起きてしまったのですか？

・単純な操作ミス、確認不足など

・システムの不具合

・運用ルールの違反（公開・送信時のダブルチェックなど規定作業の未実施など）

<1次対応のまとめ>

→ 誤公開（自社サイト）の場合、すぐに情報を削除するか、アクセスを制限します

→ 誤公開（他社サイト）の場合、すぐに情報の削除を依頼します

→ メール誤送信の場合、受信者にお詫びし、メールの削除を依頼します

<検討と公表>

→ 予想される2次被害を確します

→ 事態の重要度を判断します

→ 個人情報が含まれる場合には、本人への通知とお詫びをします

→ クレジットカード情報など、金融情報が含まれる場合は、カード停止を促すよう対応します

→ 漏洩規模や社会的影響など必要に応じて、監督官庁（例：クレジットカード情報など、金融情報が含まれる場合は金融庁） および 個人情報保護委員会 に届け出ます

→ 社会的な影響が大きいと判断した場合は、Webなどを通じて公表します

<復旧>

→ システムの不具合が原因の場合、プログラムを修正し、システムを復旧させます

→ Webページの設定を確認し、正しく表示されていることを確認します

→ 検索サイトに残ったキャッシュを削除します

<再発防止>

→ 違反や管理ミスがあった場合は、適切な処分を行います

→ 情報管理の作業手順やチェックの仕組みを見直します

※本チェックシートは情報漏洩被害の対応すべてを担保するものではありません。

本シートをご参考に、お客様のご状況に合わせて加工のうえご利用ください。 2024年2月

情報漏洩対応チェックリスト

紛失・盗難の場合

紛失・盗難とは？

（例1）： PCの入った鞄を電車に置き忘れる
（例2）： ポケットにいれたUSBメモリがないことに気づく

真っ先にすべき対応は？

→対象物（PC、スマホ等）のアカウント停止、ログインパスワードの変更

＜発覚＞

☐ **発覚した経緯は、次のうちどれですか？**

・紛失者の自己申告
→紛失した場所の管理者（鉄道会社の窓口、店舗の担当者など）へ連絡
・警察からの連絡
→警察の連絡先を書き留める
・取得者からの連絡
→取得者の連絡先を書き留める

＜初動と1次対応＞

☐ **失ったのは、自社の情報だけですか、他社の情報も含まれますか？**

※ 業務委託先の情報なら、他社の情報になります
→ 他社の情報が含まれる場合は、情報の所有者に連絡します

☐ **紛失・盗難にあった対象物（PC、スマホ、USBメモリなど）は、なにですか？**

☐ 対象物には、シリアルナンバーなど、識別できる記号がありましたか？
☐ 対象物のメーカー名、モデル名、色、サイズなど、特徴を詳しく教えてください
→対象物（PC、スマホ等）のアカウント停止、ログインパスワードの変更

☐ **失った情報は、どのような内容ですか？**

☐ 個人情報が含まれますか？
・個人情報とは、取引先・社員など個人に関する情報です
→個人情報の漏えいは、個人情報保護法に準拠した対応が必要です
☐ 個人情報は何件程度の数（情報量）ですか？（基準：1000人を超えるか）
☐ 個人情報は要配慮個人情報が含まれていますか？（人種、病歴など）
☐ 個人情報は財産的被害が生じる恐れがありますか？（カード情報など）
☐ 個人情報は不正目的をもって行われた漏洩でしたか？
※ 上記に該当する場合、個人情報保護委員会への報告義務が発生します。
速報として、概ね3～5日以内に報告が必要となります。

□ クレジットカードなどの金融情報が含まれますか？

→ 含まれる場合は、カード会社など金融機関に連絡します

□ 公共性の高い情報が含まれますか？

・公共性の高い情報とは発電所、通信設備のように社会インフラに影響する情報です

→特別法などの規制がある場合、法令に則った対応になります

□ 取引先の情報が含まれますか？

→取引先に連絡し、先方の意向に沿った対応をします

□ 機密情報が含まれますか？

・機密情報とは図面データ等、外部に出せない情報です

→機密性の重要度に応じて、経営判断をします

□ 失った情報は、パスワードなどで保護されていましたか？

・パスワードで保護されていた

・暗号化されていた

・何ら保護はなく、平文の状態だった

□ 紛失・盗難にあった対象物は、鞄や入れ物に入っていましたか？

□ 鞄や入れ物の特徴（色、形、素材など）を詳しく教えてください

□ 紛失・盗難に気づいたのは、何月何日何時ですか？

□ 失った場所は、どこですか？

→鉄道、店舗に連絡します

□ なぜ、紛失・盗難にあってしまったのですか？

（例：眠ってしまった、トイレで席を外したなど、その時の状況を詳しく）

<1次対応のまとめ>

→対象物（PC、スマホ等）のアカウント停止、ログインパスワードの変更

→他社の情報が含まれる場合は、情報の所有者に連絡します

→鉄道、店舗に連絡します

→警察に届け出ます

→紛失盗難にあった機器が、オークションや中古市場に出回っていないか確認します

<検討と公表>

→ 予想される2次被害を確します

→ 事態の重要度を判断します

→ 個人情報が含まれる場合には、本人への通知とお詫びをします

→ クレジットカード情報など、金融情報が含まれる場合は、カード停止を促すよう対応します

→ 漏洩規模や社会的影響など必要に応じて、監督官庁(例:クレジットカード情報など、
金融情報が含まれる場合は金融庁) および 個人情報保護委員会 に届け出ます

→ 社会的な影響が大きいと判断した場合は、Webなどを通じて公表します

<再発防止>

→自社の情報管理ポリシーに則り、再発防止策を講じ、周知徹底します

※本チェックシートは情報漏洩被害の対応すべてを担保するものではありません。
本シートをご参考に、お客様のご状況に合わせて加工のうえご利用ください。 2024年2月

情報漏洩対応チェックリスト

外部攻撃の場合

外部攻撃の場合とは？

（例1）：ウィルス等の不正プログラムに感染し、情報が漏洩した場合
（例2）：システムの脆弱性等から外部者の不正アクセスを許し、情報が漏えいした場合

真っ先にすべき対応は？

→ **不正アクセスがあった機器・サイトの停止、ないしは隔離（他のネットワークから切断）**

＜発覚＞

☐ **発覚した経緯は、次のうちどれですか？**

・風評を含む外部からの指摘
　→ 指摘してくれた方の連絡先を書き留める
・ウィルス対策ソフト、ネットワーク監視サービスなどからの連絡
・ランサムウェアによる身代金要求があった

＜初動と1次対応＞

☐ **失ったのは、自社の情報だけですか、他社の情報も含まれますか？**

※ 業務委託先の情報なら、他社の情報になります
→ 他社の情報が含まれる場合は、情報の所有者に連絡します。

☐ **外部攻撃を受けた機器は、なにですか？**

→ 対象物（PC、スマホなど）のアカウント停止、ログインパスワードの変更
→ 対象物（PC、スマホなど）のネットワークからの切り離し

☐ **外部攻撃を受けた範囲は、どこまでですか？（ネットワークのすべてなのか、一部なのか？）**

→ 攻撃を受けたネットワークのサービス停止、外部からの隔離

☐ **漏洩した情報は、どのような内容ですか？**

☐ 個人情報が含まれますか？

・個人情報とは、取引先・社員など個人に関する情報です
→ 個人情報の漏えいは、個人情報保護法に準拠した対応が必要です
☐ 個人情報は何件程度の数（情報量）ですか？（基準：1000人を超えるか）
☐ 個人情報は要配慮個人情報が含まれていますか？（人種、病歴など）
☐ 個人情報は財産的被害が生じる恐れがありますか？（カード情報など）
☐ 個人情報は不正目的をもって行われた漏洩でしたか？
※　上記に該当する場合、個人情報保護委員会への報告義務が発生します。

速報として、概ね3～5日以内に報告が必要となります。

□ クレジットカードなどの金融情報が含まれますか？

→ 含まれる場合はカード会社など、金融機関に連絡します

□ 公共性の高い情報が含まれますか？

・公共性の高い情報とは発電所、通信設備のように社会インフラに影響する情報です

→ 特別法などの規制がある場合、法令に則った対応になります

□ 取引先の情報が含まれますか？

→ 取引先に連絡し、先方の意向に沿った対応をします

□ 機密情報が含まれますか？

・機密情報とは図面データなど、外部に出せない情報です

→ 機密性の重要度に応じて、経営判断をします

□ 漏洩した情報は、パスワードなどで保護されていましたか？

・パスワードで保護されていた

・暗号化されていた

・何ら保護はなく、平文の状態だった

□ 外部攻撃に気づいたのは、何月何日何時ですか？

＜調査・検討＞

→ 漏洩情報の内容から事態の深刻度を判断します

→ 必要に応じて専門業者に調査を依頼します

・JPCERT　※主に不正アクセス、マルウェア感染、DoS/DDoS攻撃などに対応

https://www.jpcert.or.jp/

・JNSA：サイバーインシデント緊急対応企業一覧

https://www.jnsa.org/emergency_response/

→ 必要に応じて警察（警察庁サイバー警察局）に相談します

・警視庁：サイバー警察局　相談窓口

https://www.npa.go.jp/bureau/cyber/soudan.html

→ サーバーなどに残された情報はバックアップをとり、証拠を保全します

→ 実態が解明されるまでは、システムの再稼働は控えます

→ バックアップに不正プログラムがないことを確認し、
再発防止措置を取った後、システムを復旧します

＜公表＞

→ 他社の情報が含まれる場合は、情報の所有者に連絡します

→ 個人情報が含まれる場合には、本人への通知とお詫びをします

→ クレジットカード情報など、金融情報が含まれる場合は、カード停止を促すよう対応します

→ 漏洩規模や社会的影響など必要に応じて、監督官庁(例:クレジットカード情報など、
金融情報が含まれる場合は金融庁) および 個人情報保護委員会 に届け出ます

→ 社会的な影響が大きいと判断した場合は、Webなどを通じて公表します

<再発防止>

→ 自社の情報管理ポリシーに則り、再発防止策を講じ、周知徹底します

・システムの脆弱性修正、パッチ適用など

・ウィルス対策ソフトの導入、変更、最新化の徹底など

・フィッシングサイト、標的型メールに対応した定期的な教育など

→ 必要に応じて、情報漏洩の被害にあった方へ補償をします

※本チェックシートは情報漏洩被害の対応すべてを担保するものではありません。
本シートをご参考に、お客様のご状況に合わせて加工のうえご利用ください。 2024年2月

情報漏洩対応チェックリスト

内部犯行の場合

内部犯行とは？

・内部の人間が不正に情報を持出し、外部の業者等に販売・譲渡するケースです

真っ先にすべき対応は？

→ **対象サイト（ファイルサーバーなど）の停止、アクセス制限**

→ **内部犯行者が使用した機器の確保（証拠の保全）**

＜発覚＞

☐ **発覚した経緯は、次のうちどれですか？**

・顧客からの連絡（架空請求を受けた、個人情報が不正に利用されているなど）

→ 連絡先を控える

・マスコミからの連絡

→ 連絡先を控える

・情報が漏洩しているとの風評が広まった

・名簿を買い取るよう、脅迫を受けた

＜初動と1次対応＞

☐ **内部犯行の当事者が、まだ社内にいる可能性がありますか？**

・まだ社内にいる可能性あり（特定できない場合は、いることを想定する）

→ 証拠隠滅されないよう注意する

・社内にいる可能性はない

→ 以下のプロセスへ

☐ **持ち出された情報は、自社の情報だけですか、他社の情報も含まれますか？**

※ 業務委託先の情報なら、他社の情報になります

→ 他社の情報が含まれる場合は、情報の所有者に連絡します

☐ **漏洩した情報の保管場所は、どこですか？**

→ 対象サイト（ファイルサーバーなど）

該当サイト（サーバー）の停止、アクセス制限

→ 執務室、倉庫、書類保管場所（※物理的な書類など）

立ち入り制限もしくは残りの書類を施錠できる場所に退避

☐ **なにを（PC、USBメモリ、紙など）を、持ち出されましたか？**

☐ **持ち出された情報は、どのような内容ですか？**

☐ 個人情報が含まれますか？

・個人情報とは、取引先・社員など個人に関する情報です

→ 個人情報の漏えいは、個人情報保護法に準拠した対応が必要です

☐ 個人情報は何件程度の数（情報量）ですか？（基準：1000人を超えるか）

☐ 個人情報は要配慮個人情報が含まれていますか？（人種、病歴など）

☐ 個人情報は財産的被害が生じる恐れがありますか？（カード情報など）

☐ 個人情報は不正目的をもって行われた漏洩でしたか？

※ 上記に該当する場合、個人情報保護委員会への報告義務が発生します。
速報として、概ね3～5日以内に報告が必要となります。

☐ クレジットカードなどの金融情報が含まれますか？

→ 含まれる場合は、カード会社など金融機関に連絡します

☐ 公共性の高い情報が含まれますか？

・公共性の高い情報とは、発電所、通信設備のように社会インフラに影響する情報です

→ 特別法などの規制がある場合、法令に則った対応になります

☐ 取引先の情報が含まれますか？

→ 取引先に連絡し、先方の意向に沿った対応をします

☐ 機密情報が含まれますか？

・機密情報とは、図面データなど外部に出せない情報です

→ 機密性の重要度に応じて、経営判断をします

☐ **持ち出された情報は、保管時に何らかの形で保護（対策）されていましたか？**

・パスワードで保護されていた

・暗号化されていた

・何ら保護はなく、平文の状態だった

・施錠できる適切な場所で保管されていた

・だれでも閲覧できる場所に置かれていた

☐ **内部犯行に気づいたのは、何月何日何時ですか？**

＜調査・検討＞

→ 漏洩情報の内容から事態の深刻度を判断します

→ 必要に応じて専門業者に調査を依頼します

・JPA：情報セキュリティに関する技術的なご相談
https://www.jpcert.or.jp/

・JNSA ：サイバーインシデント緊急対応企業一覧
https://www.jnsa.org/emergency_response/

→ 必要に応じて警察（警察庁サイバー警察局、不正アクセス対策）に相談します

・警視庁　：サイバー警察局　不正アクセス対策
https://www.npa.go.jp/bureau/cyber/countermeasures/unauthorized-access.html

→ サーバーなどに残された情報はバックアップをとり、証拠を保全します

→ 実態が解明されるまでは、システムの再稼働は控えます

→ バックアップに不正プログラムがないことを確認し、
再発防止措置を取った後、システムを復旧します
また、脆弱性等の解消（改修、パッチ適用）を行います

＜公表＞

→ 他社の情報が含まれる場合は、情報の所有者に連絡します

→ 個人情報が含まれる場合には、本人への通知とお詫びをします

→ クレジットカード情報など、金融情報が含まれる場合は、カード停止を促すよう対応します

→ 漏洩規模や社会的影響など必要に応じて、監督官庁（例：クレジットカード情報など、
金融情報が含まれる場合は金融庁）および 個人情報保護委員会 に届け出ます

→ 社会的な影響が大きいと判断した場合は、Webなどを通じて公表します

＜再発防止＞

→ 自社の情報管理ポリシーに則り、再発防止策を講じ、周知徹底します
・情報へのアクセス件の見直し
・システムの脆弱性が原因の場合は、改修やパッチ適用
・重要情報を扱う業務での相互牽制できる体制の構築
・外部記憶装置（外付けHDD、USBメモリ）を制限するツールの導入
・クラウドストレージへのアクセスを制限する
・書類等の保管ルール（施錠できる場所への保管、鍵の管理など）

→ 必要に応じて、情報漏洩の被害にあった方へ補償をします

※本チェックシートは情報漏洩被害の対応すべてを担保するものではありません。
本シートをご参考に、お客様のご状況に合わせて加工のうえご利用ください。　2024年2月