中小企業・小規模事業者の皆様へ

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

情報漏えい？ ウイルス感染？ システム停止？
どうしたらいいの！？

セキュリティインシデント対応の必要性

セキュリティインシデントとは、セキュリティの事故・出来事のことです。単に「インシデント」とも呼ばれます。例えば、情報の漏えいや改ざん、破壊・消失、情報システムの機能停止またはこれらにつながる可能性のある事象等がインシデントに該当します。
インシデント対応は、これらの被害を想定し、あらかじめ準備することで被害や影響範囲を最小限に抑えます。また、自社だけではなく、顧客、取引先、株主、従業員等の関係者へ被害が拡大しないようにします。

インシデント発生時の想定被害

直接的な被害として、攻撃者による不正送金や金銭要求、対応人件費、原因調査や復旧のための外部委託費、復旧までの代替品費、取引先・顧客等への謝罪対応費、法的対応のための弁護士費用等の金銭的被害があります。
間接的な被害として、関係者への被害波及、会社の信用低下、事業停止による機会損失等があります。

インシデント対応の目的

インシデント発生による被害とその影響範囲を最小限に抑え、迅速に復旧し、再発を防止することで、企業の事業継続を確保することです。

インシデント対応時に整理しておくべき事項

インシデントの分類	情報漏えい、ウィルス感染、システム停止など
事業者	事業者の名称 ※自社の受託案件に関連したインシデントの場合は委託元含む関係事業者の名称
責任者・担当者	本件に関する責任者および担当者の所属、氏名
発覚日時	インシデントを認知した日時
発生日時	調査で判明したインシデントの発生日時
発生事象	表面化している事柄、被害、影響など
対応経過	発生から現時点までの時系列での経過
想定される原因	現時点で想定される直接的な原因
被害を受けたシステムの状況	被害を受けたシステムの概要・詳細
システム構成・運用状況	システムの物理的所在地やOS、アプリケーションとバージョン構成 ※可能であれば簡単な構成図等も併記 システムの運用状況やセキュリティツール・サービスの利用状況等

インシデント対応の基本ステップ

ステップ1 検知・初動対応

検知と連絡受付

・インシデントが疑われる兆候や実際の発生を発見した場合は、情報セキュリティ責任者に報告します。

・外部から通報を受け付けた場合は、通報者の連絡先等を控えます。

対応体制の立ち上げ

・情報セキュリティ責任者は、対応すべきインシデントであると判断したら、速やかに経営者に報告します。

・経営者は、インシデントが事業や顧客に与える影響を踏まえ、速やかにインシデント対応のための体制を立ち上げ、あらかじめ策定している対応方針に従い、責任者と担当者を定めて、役割分担を明確にします。

初動対応

・初動対応として、対象となる情報が外部からアクセスできる状態にある場合や、被害が広がる可能性がある場合は、ネットワークの遮断、情報や対象機器の隔離、システムやサービスの停止を行います。ただし、対象機器の電源を切る等、不用意な操作でシステム上に残された記録を消さないようにします。

ステップ2 報告・公表

第一報

・すべての関係者への通知が困難な場合や、インシデントの影響が広く一般に及ぶ場合は、状況をウェブサイトやメディアを通じて公表します。公表によって被害の拡大を招かないよう、時期、内容、対象などを考慮します。

・顧客や消費者に関係する場合は受付専用の問い合わせ窓口を開設し、被害が発生・拡大した場合にはその動向を速やかに把握し対応します。

第二報以降・最終報

・被害者や、影響を及ぼした取引先や顧客に対して、インシデントの対応状況や再発防止策等に関して報告します。また、被害者に対する損害の補償等を、必要に応じて行います。

・個人情報漏えいの場合は個人情報保護委員会、業法等で求められる場合は所管の省庁等、犯罪性がある場合は警察、ウイルス感染や不正アクセスの場合はIPAへ届け出ます。

ステップ3 復旧・再発防止

調査・対応

・適切な対応判断を行うために、5W1H（いつ、どこで、誰が、何を、なぜ、どうしたのか）の観点で、状況を調査し情報を整理します（P2「インシデント対応時に整理しておくべき事項」を参照）。

・対応方針を基に、原因を調査し、修正プログラムの適用、設定変更、機器の入替、データの復元等、必要な修復を行います。

・自社で対応が難しい場合は、IT製品のメーカー、保守ベンダー等の外部専門組織や公的機関の相談窓口等に支援、助言を依頼します（P7「インシデント発生時の相談窓口・報告先」を参照）。

・対応中は、状況や事業への影響等について経営者に適時報告します。

証拠保全

・訴訟対応等を見越して事実関係を裏付ける情報や証拠を保全し、必要に応じてフォレンジック調査（パソコンのハードディスク、メモリ内データ、サーバーやネットワーク機器のログ等の調査）を行います。

復旧

・正しく修復できたことが確認できたら、停止したシステムやサービスを復旧します。

・復旧後は、経営者に対応結果を報告します。

再発防止策

・インシデントを再発させないために根本原因を分析し、新たな技術的対策の導入、ルールの策定、教育の徹底、体制整備、運用の改善等、抜本的な再発防止策を検討し、実施します。

ウイルス感染・ランサムウェア感染の場合

ウイルス感染やランサムウェア感染の場合は、まず感染したパソコンやサーバーの利用を停止し、ネットワークから切り離すことが重要です。特にランサムウェア対応においては、日頃から適切な方法でデータのバックアップを行っておくことが被害を最小限に抑えるポイントになります。

検知・初動対応

ウイルス感染

検知と連絡受付

・パソコンの動作異常やウイルス対策ソフトの警告が表示された場合、ウイルス感染の可能性があるので、情報セキュリティ責任者に報告します。
・内部から外部への不正な通信、外部からの意図しない通信や一時的な大量の通信、ウイルスに関係する特定サイトへのアクセスなどは、ウイルス感染を疑います。
・ウイルスが添付されたメール等を受け取った外部から通知を受けて発覚することもあります。

初動対応

・感染したパソコンやサーバーの利用を停止し、ネットワークから切り離します。

ランサムウェア感染

検知と連絡受付

・パソコンの画面等に、身代金を要求するようなメッセージが表示された場合、ランサムウェア※1感染の可能性があるので、情報セキュリティ責任者に報告します。

初動対応

・感染したパソコンやサーバーの利用を停止し、ネットワークから切り離します。

報告・公表

第二報以降・最終報

・影響を及ぼした取引先や顧客に対して、インシデントに関して報告します。
・ウイルス感染による影響によって、業法等で報告が求められる場合は所管の省庁へ報告します。
・ウイルス感染やランサムウェア感染の場合は、IPAの届出窓口へ届け出ます。

復旧・再発防止

ウイルス感染

調査・対応

・他のパソコンやサーバーがウイルスに感染していないか、ウイルス対策ソフトの定義ファイルを最新にしてからチェックします。
・ウイルス対策ソフトに従ってウイルスを駆除します。
・ウイルス駆除ができない場合、OSのクリーンインストール※2を実施し、全てのプログラムを入れ直します。

復旧

・ウイルスの駆除が確認できたら、対象のパソコンやサーバーをネットワークに接続し、復旧します。

ランサムウェア感染

調査・対応

・No More Ransom※3等から復号化ツールを入手し、復旧を試みます、ただし、全てのランサムウェアに対応しているわけではありません。
・データ等のバックアップを行っている場合は、復元（リストア）します。ただし、バックアップ装置・媒体をパソコンに常時接続している場合、バックアップファイルも暗号化されている場合もあります。

＜参考＞適切なバックアップ方法

▶バックアップに使用する装置・媒体は複数用意し、バックアップ時のみパソコンと接続する、またはバックアップしたファイルのうち1つはオフサイトに保存する。

▶バックアップしたファイルは、定期的に復元（リストア）できるか確認する。

・復号化ツールでも復旧しない場合、バックアップが復元（リストア）できない場合は、感染した機器やデータの復旧を断念し、再構築します。

復旧

・データの復元（リストア）が正しいことを確認できたら、システムを復旧します。

※1 ランサムウエア
感染したパソコン等に保存されているファイルに暗号化等の制限をかけ使用不可にし、その制限の解除と引き換えに金銭を要求する不正プログラムの総称です。標的型サイバー攻撃の一環としての「人手によるランサムウェア攻撃」や、情報を窃取しそれを公開すると脅迫する「二重の脅迫」も報告されています。

※2 クリーンインストール
すでにインストールされているOSを削除した上で、新しくOSを再インストールする方法です。記憶領域にあるデータは全て消去されるので、データはバックアップから復元する必要があります。

※3 No More Ransom（ノーモアランサム）
ランサムウェアの被害者が、犯罪者に不当な支払いをすることなく、暗号化されたデータを取り戻すための支援を目的とした国際的なプロジェクトです。

情報漏えいの場合

情報漏えいには、ネットワークへの「不正アクセス」、従業員による「内部犯行」、「電子メールの誤送信やWebでの誤公開」、「紛失・置忘れ」等によるものがあります。特に「不正アクセス」による情報漏えいは、データの大量流出につながるおそれがあることから、インターネットに接続しているサーバへの対策が必要です。また、不正アクセス、内部犯行は犯罪性があるため、警察への届け出も必要になります。

検知・初動対応

検知と連絡受付

・不正アクセスの多くは企業がインターネットに接続しているサーバに対して行われ、ログの確認やセキュリティ機器のアラート（警報）によって、発見されます。

・内部犯行の場合、不正に待ちだされた名簿等が第三者に売られてたことが発覚したり、顧客から自分の情報が不正に利用されているとの問合せを受けたりすることで発覚します。

・メール誤送信やWebでの誤公開の場合、ミスをした本人またはそれを発見した第三者からの指摘により発見されます。

初動対応

・情報漏えいの全般的な対応として、漏えいした情報の種類や件数、暗号化やアクセス制限等のセキュリティ対策状況を確認します。

・不正アクセスにより、個人情報や機密情報が漏えいする危険が確認された場合は、直ちにネットワークから切り離してサービスを停止する等の処置を講じます。また、クレジットカードやアカウント情報が漏えいした場合は、カード会社への連絡やアカウント停止などの対応を行います。

・内部犯行の場合、社内システムへのアクセス制限や使用パソコン等の確保（証跡保存）を行います。メール誤送信で送信先が明らかな場合は、受信先に対して、受信した情報の削除を依頼します。
Webでの誤公開の場合は、直ちに当該情報を削除するか、アクセス制限を行い外部から参照できないようにします。

報告・公表

第二報以降・最終報

・アカウント情報等、漏えいした情報が悪用されるおそれがある場合は、被害にあった個人や取引先に対して、同じアカウント情報を使用しているサービスの登録情報の変更を促すなど、二次被害防止のための注意喚起を行います。

・個人情報漏えいの場合は個人情報保護委員会へ報告します。

・情報漏えいの原因が、不正アクセスや内部犯行等、犯罪性がある場合は警察へ届け出ます。

・情報漏えいの原因がウイルス感染や不正アクセスの場合は、IPAの届出窓口に届け出ます。

復旧・再発防止

調査・対応

・漏えいした情報の範囲、原因、被害の状況等について調査します。

- ✓不正アクセスの場合、機器に残された記録から、どのように侵入が行われたのか、どのような情報にアクセスした形跡があるかなどについて調査します。
- ✓内部犯行の場合、企業内に残された記録から漏えいした情報をなるべく正確に把握します。また、不正に持ち出された機器や媒体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。
- ✓Web等での誤公開の場合は、どういった範囲で何人が参照したかアクセスログを使って調査します。

・予想される二次被害を確認します。

復旧

・不正アクセスの場合、侵入されたサーバ等の内容を証拠保全のため保存し、再発防止策を講じた上で、サービスを復旧します。アカウント情報等が漏えいした場合には、アカウントの再発行やパスワードの変更等を行います。

再発防止策

・不正アクセスの原因により、サーバやWebアプリケーションの脆弱性への対処、Webサーバやセキュリティ対策機器等の設定の見直し、アカウント情報やアクセス権限の見直しを行います。

・内部犯行の場合は、認証やアクセス制御、ログの取得等社内の情報管理体制を強化します。

・メール誤送信やWebでの誤公開の場合は、人的な作業ミス防止のため、作業手順にチェックの仕組みを追加します。

システム停止の場合

システム停止の原因は、サイバー攻撃などのセキュリティの問題も含め、ソフトウェアのバグ・不具合、機器の故障など様々な原因が想定され、異常の発見時には原因がわからないことがあります。原因がわからない場合は、セキュリティの問題の可能性も含めて対応を行う必要があります。また、システムの停止は事業や企業経営に重大な影響を与える場合があるので、経営者は事業継続計画（BCP）※4 を策定し、これに備える必要があります。

検知・初動対応

検知と連絡受付

・システムに動作不良、障害、停止またはその兆候があれば、システム管理者または情報セキュリティ責任者に連絡します。

初動対応

・可能な限り、システムの停止や異常が事業や業務に影響しないよう、システムの稼働継続を試みます。サーバの異常の場合に、冗長化されていればサーバの切り替えを行います。

・ただし、情報漏えいが疑われる、Webサイトの安全性が確認できない等、被害が広がる可能性がある場合は、システムの停止を行います。

報告・公表

第二報以降・最終報

・取引先への影響がある場合や、取引先との取り決めがある場合には、取引先に報告します。

・システムの異常や停止が事業に影響し、業法等で報告が求められる場合は所管の省庁に報告します。

・システムの異常や停止原因がウイルス感染や不正アクセスによる場合は、IPAへ届出窓口に届け出ます。

復旧・再発防止

調査・対応

・原因の調査を行い、サイバー攻撃などのセキュリティによるものか、それ以外の原因かを判断します。

・システム異常・停止中に、サービスや業務の代替策がある場合は提供します。

・セキュリティによる原因の場合は、「基本ステップ」に準じて、対応を行います。

再発防止

・必要に応じて、事業継続計画（BCP）やIT-BCPについても見直します。

※4 事業継続計画（BCP）
自然災害やテロなどの状況において、事業の損害を最小化するとともに、主となる事業の継続や早期復旧のための方法を定めた計画。また、システムの事業継続計画のことを「IT-BCP」と呼びます。平時からシステムが事業に与える影響を踏まえシステムの重要度を評価し、システムの稼働継続や復旧に関する計画を定めておくことが有効です。

インシデント発生時の相談窓口・報告先

インシデントが発生した場合は、迅速に対応を進めるために公的機関の相談窓口や外部専門組織の活用も検討しましょう。また、ウイルスや不正アクセスの被害、個人情報等の漏えいは、関係機関への届け出が必要になります。

情報セキュリティに関する技術的な相談

独立行政法人情報処理推進機構（IPA）
情報セキュリティ安心相談窓口

一般的な情報セキュリティ（主にウイルスや不正アクセス）に関する技術的な相談に対してアドバイスを提供する窓口です。電話、メール等で相談を受け付けています。

Tel：03-5978-7509（受付時間10:00～12:00、13:30～17:00 土日祝日・年末年始は除く）
Mail：anshin@ipa.go.jp
URL：https://www.ipa.go.jp/security/anshin/about.html

サイバー犯罪に関する相談

都道府県警察本部のサイバー犯罪相談窓口

サイバー犯罪に係る情報提供や、犯罪被害、セキュリティ対策の相談を受付けています。詳細は、各都道府県警察本部のWebサイトでご確認ください。

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

インシデント対応の相談

一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）
インシデント対応依頼

国内における被害低減を目的として、広く一般からインシデントに関する対応依頼をWebフォームやメールで受け付けています。対応できる依頼や受け付けている相談はWebサイトでご確認ください。

URL：https://www.jpcert.or.jp/form/

特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）
サイバーインシデント緊急対応企業一覧

緊急で被害調査や被害切り分け、復旧などの対応（有償）を請け負ってくれる、JNSA所属企業を取りまとめています。詳細は、各企業へ直接お問い合わせください。

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

ウイルス・不正アクセスに関する届出

独立行政法人情報処理推進機構（IPA）
情報セキュリティ安心相談窓口

経済産業省の告示に基づき、IPAでは国内のコンピュータウイルスの感染被害やコンピュータ不正アクセス被害の届出を受け付けています。Webサイトで届出様式を入手してメールで報告してください。

URL：https://www.ipa.go.jp/security/todokede/crack-virus/about.html

個人情報・特定個人情報（マイナンバー）漏えいの報告

個人情報保護委員会

個人情報や特定個人情報の漏えい等についてWebフォームで報告を受け付けています。

個人情報の漏えい等
URL：https://www.ppc.go.jp/personalinfo/legal/leakAction/

特定個人情報の漏えい等
URL：https://www.ppc.go.jp/legal/rouei/

インシデント対応に役立つ情報

サイバーセキュリティ経営ガイドライン
付録C インシデント発生時に組織内で整理しておくべき事項（経済産業省）
インシデント発生時、原因調査等を行う際に組織内で整理しておくべき事項として、基本項目、情報漏えいに係る項目、ウイルス感染に係る項目、不正アクセスに係る項目、（D）DoSに係る項目、の5つの表を提供しています。
https://www.meti.go.jp/policy/netsecurity/mng_guide.html

サイバー攻撃被害に係る情報の共有・公表ガイダンス（サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会）
サイバー攻撃を受けた被害組織がサイバーセキュリティ関係組織とサイバー攻撃被害に係る情報を共有する際の実務上の参考となるガイダンスです。
https://www.nisc.go.jp/council/cs/kyogikai/guidancekentoukai.html

インシデントハンドリングマニュアル（JPCERT/CC）
インシデント発生時から解決までの一連の処理について、代表的なインシデント種別を例にあげ、対応の考え方と手順の概要を簡潔に説明した資料です。
https://www.jpcert.or.jp/csirt_material/operation_phase.html

ランサムウェア対策特設ページ（IPA）
ランサムウェア対策に必要となる情報を集約し、ランサムウェアの感染防止や被害低減のために役立つ情報をタイムリーに公開しています。
https://www.ipa.go.jp/security/anshin/ransom_tokusetsu.html

No More Ransom
ランサムウェアの被害低減を目指す国際的なプロジェクトです。ランサムウェアの危険性と対策に関する情報を公開し、無料復号ツールをはじめとしたランサムウェアの被害者に有用なリソースの提供を目的として活動しています。
https://www.nomoreransom.org/ja/index.html

対策規程を作成し、本格的に取り組もう！

情報セキュリティに関する社内規則を文書化する「情報セキュリティ関連規程」のサンプルです。
対応すべきリスクと対策を検討し、自社のリスクに応じた規程を定めるときの参考としてください。
作成後は運用し、点検や改善に努めて、取り組みを継続しましょう！


中小企業の情報セキュリティ対策ガイドライン 付録5
情報セキュリティ関連規程（サンプル）
目 次

情報セキュリティ関連規程（サンプル）
https://www.ipa.go.jp/security/keihatsu/sme/guideline/

手遅れになるまえに、手を打つ。

中小企業に対するサイバー攻撃への対処に不可欠なワンパッケージのサービスを要件としてまとめ、これを満たすことが所定の審査機関により確認された民間サービスを、IPAが登録・公表する制度です。
「見守り」「駆付け」「保険」など中小企業のセキュリティ対策に不可欠なサービスをワンパッケージで安価に提供。サイバーセキュリティお助け隊サービスの活用をご検討ください！

サイバーセキュリティ お助け隊

サイバーセキュリティお助け隊サービス制度
https://www.ipa.go.jp/security/otasuketai-pr/

IPA 独立行政法人情報処理推進機構
セキュリティセンター

〒113-6591 東京都文京区本駒込二丁目28番8号
文京グリーンコートセンターオフィス
TEL 03-5978-7508 FAX 03-5978-7546
E-mail isec-pr-nw@ipa.go.jp URL https://www.ipa.go.jp/security/

2023.4.26 Version 1.0