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

2024年7月

独立行政法人情報処理推進機構(IPA)
セキュリティセンター

IPA Better Life with IT

中小企業のためのセキュリティインシデント対応手引き

- インシデント発生時の対応について、「**検知・初動対応**」「**報告・公表**」「**復旧・再発防止**」の３つの段階に分けて検討事項を説明
- インシデント対応時に整理しておくべき事項や相談窓口・報告先などを紹介

ステップ１
検知・初動対応
- 検知と連絡受付
- 対応体制の構築
- 初動対応

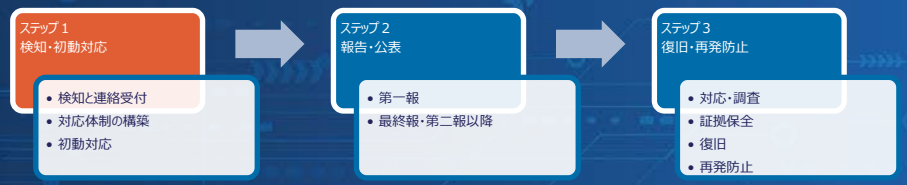
ステップ２
報告・公表
- 第一報
- 最終報・第二報以降

ステップ３
復旧・再発防止
- 対応・調査
- 証拠保全
- 復旧
- 再発防止

セキュリティインシデント対応の必要性・目的

- 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。
- インシデント発生による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は、インシデント発生によるこれら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。

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。

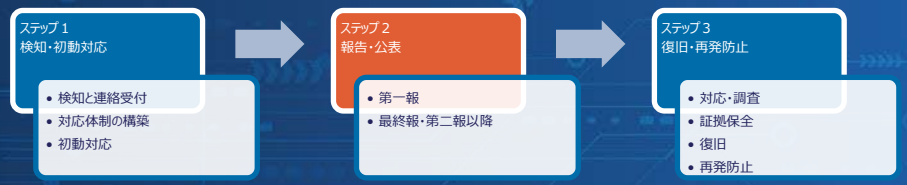
● 対応体制の構築

- 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

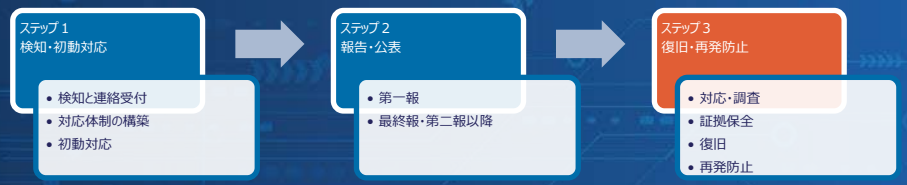
- 初動対応として、対象となる情報が外部からアクセスできる状態にある場合や、被害が広がる可能性がある場合は、ネットワークの遮断、情報や対象機器の隔離、システムやサービスの停止を行います。ただし、対象機器の電源を切る等、不用意な操作でシステム上に残された記録を消さないようにします。

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



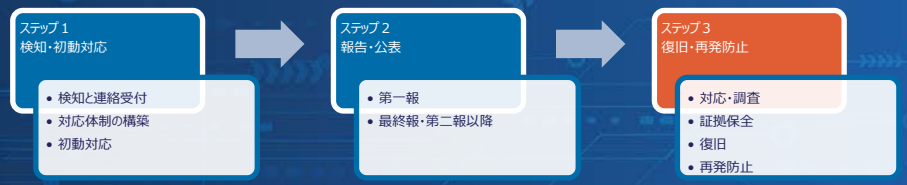
● 調査・対応

- 適切な対応判断を行うために、5W1H（いつ、どこで、誰が、誰を、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。
- 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、助言を求めます。
- 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。

ステップ３ 復旧・再発防止



- **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**
  - 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。

事象ごとの対応のポイント

- **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。

- **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」、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、不正アクセスや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。

- **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、不具合・ソフトウェアのバグ、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）を策定し、これに備える必要があります。

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
担当者・責任者	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

※サイバーセキュリティ経営ガイドライン 付録C「ンシデント発生時に組織内で整理しておくべき事項」も参考になります
https://www.meti.go.jp/policy/netsecurity/mng_guide.html

インシデント発生時の相談窓口

- **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)
  03-5978-7509（受付時間10:00～12:00、13:30～17:00）
  https://www.ipa.go.jp/security/anshin/index.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
  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
  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
  https://www.jnsa.org/emergency_response/

インシデント発生時の報告先

- **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)

  コンピュータウイルス届出窓口、コンピュータ不正アクセス届出窓口

  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

  個人情報の漏えい等

  https://www.ppc.go.jp/personalinfo/legal/leakAction/

  特定個人情報の漏えい等

  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/measures/ransom_tokusetsu.html

【参考】中小企業の情報セキュリティ対策ガイドライン

- 中小企業の経営者や実務担当者が、情報セキュリティ対策の必要性を理解し、情報を安全に管理するための具体的な手順等を示したガイドライン
- 本編2部と付録より構成
  - 経営者が認識すべき「3原則」、経営者がやらなければならない「重要7項目の取組」を記載（第1部）
  - 情報セキュリティ対策の具体的な進め方を分かりやすく説明（第２部）
  - すぐに使える「情報セキュリティ基本方針」や「情報セキュリティ関連規程」等のひな形を付録

【参考】情報セキュリティ関連規程（サンプル）

- 中小企業の情報セキュリティ対策ガイドラインでは、付録５「情報セキュリティ関連規程（サンプル）」にて情報セキュリティに関する事故対応や事業継続管理などのサンプル規程を提供

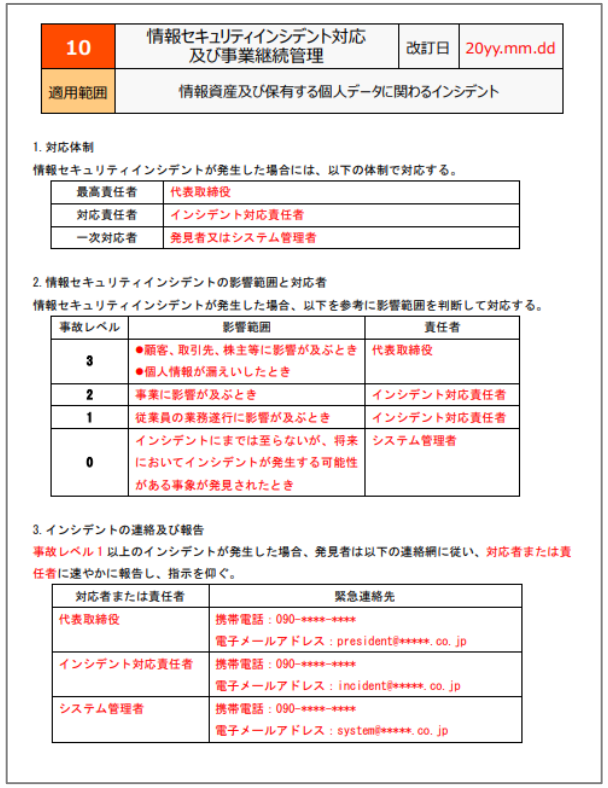
中小企業の情報セキュリティ対策ガイドライン 付録5

情報セキュリティ関連規程（サンプル）

中小企業向けの情報セキュリティ関連規程のサンプルです。必要な対策を選択し、編集することで自社の情報セキュリティ関連規程を作成することができます。
※赤字箇所は、自社の事情に応じた内容（役職名、担当者名など）に書き換えてください。
※青字箇所は、自社の事情に応じた文言を選択してください。
※黄色蛍光箇所は、中小企業の情報セキュリティ対策ガイドライン第 3 版からの変更箇所を表しております。

目 次

(Ver.2.1)



10	情報セキュリティインシデント対応及び事業継続管理	改訂日	20yy.mm.dd
適用範囲	情報資産及び保有する個人データに関わるインシデント		

1. 対応体制

情報セキュリティインシデントが発生した場合には、以下の体制で対応する。

最高責任者	代表取締役
対応責任者	インシデント対応責任者
一次対応者	発見者又はシステム管理者

2. 情報セキュリティインシデントの影響範囲と対応者

情報セキュリティインシデントが発生した場合、以下を参考に影響範囲を判断して対応する。

事故レベル	影響範囲	責任者
3	●顧客、取引先、株主等に影響が及ぶとき ●個人情報が漏えいしたとき	代表取締役
2	事業に影響が及ぶとき	インシデント対応責任者
1	従業員の業務遂行に影響が及ぶとき	インシデント対応責任者
0	インシデントにまでは至らないが、将来においてインシデントが発生する可能性がある事象が発見されたとき	システム管理者

3. インシデントの連絡及び報告

事故レベル１以上のインシデントが発生した場合、発見者は以下の連絡網に従い、対応者または責任者に速やかに報告し、指示を仰ぐ。

対応者または責任者	緊急連絡先
代表取締役	携帯電話：090-****-**** 電子メールアドレス：president@*****.co.jp
インシデント対応責任者	携帯電話：090-****-**** 電子メールアドレス：incident@*****.co.jp
システム管理者	携帯電話：090-****-**** 電子メールアドレス：system@*****.co.jp


IPA