JPCERT CC®

組織内 CSIRT 構築の参考資料
インシデント対応マニュアルの作成について

一般社団法人
JPCERT コーディネーションセンター

このドキュメントについて

- このドキュメントは、「インシデント対応マニュアル」を作成するためのノウハウや、以下の考察すべきポイントを提供することにより、マニュアル作成の支援を目的としたものである
  - インシデント対応マニュアルに含めるべき事項
  - さまざまなインシデント対応から得られたノウハウ（すべき事項等）を示すことにより、マニュアルに含めるべき事項
  - 一般的なインシデント対応のプロセスを示すことにより、現在の不文律なインシデント対応フローの文書化及び最善策の見える化

アジェンダ

- インシデント対応する人及び部署の明確化
- インシデント発生前の準備
- インシデント対応フロー
  1. インシデントの発見及び報告
  2. インシデントに対する初動対応
  3. インシデントに関する告知
  4. インシデントの抑制措置と復旧
  5. インシデントの事後対応
- インシデントの対応事例
  1. 「ノート PC による情報漏洩」
  2. 「Phishing サイトによる顧客情報の窃盗行為」
  3. 「顧客の ID の不正利用」

インシデントに対応する人及び組織の明確化

- 発生するインシデントのすべてを完全に予想することは不可能
- これまで経験したことがないインシデントに対して、対応すべき担当者や責任者が不明確となり、対応に不備が出ることがある

- マニュアルには以下の記述が必要
  - 組織にとっての「インシデント」を定義する
  - 「想定外のインシデント」に対して責任を持つ部署／担当者を明確に定義する
  - 組織内で発生したインシデント対応について、全体の統括を行う部署またはチーム等を明確に定義する

インシデント発生前の準備

- インシデント対応に必要な連絡先の確保
  - これまでに経験したインシデント、あるいはこれから発生が予想されるインシデントの対応に必要な連絡先をリスト化する
  - 連絡先との連絡手段の疎通確認を実施する
  - 各連絡先と連絡先リストについての共通認識を持つ
- 各種規則の把握と整合性の確認
  - 親組織の規則（上位規則）にインシデント対応に関する記述がある可能性があるため、関連する可能性のある規則を確認する
  - 上記を含め、インデント対応の活動に関係する規則等の相関関係を明確にしておく
- インシデント対応に有効なツールの利用
  - 組織内の情報共有のためのインフラやツールが、インシデント発生時に有効に機能するかどうか検討する
  - 有用なツール等がなければ、インシデント対応に活用できる別の手段を確保しておく
  - 可能であれば、事前に訓練や演習等を実施しておく

インシデントの対応フロー
1. インシデントの発見及び報告

- インシデントの発見者が迅速に報告する
  - 報告しやすい環境であることが必須
  - インシデントの報告窓口が設けられており、それが周知されていることが必要
- インシデントの報告を受けた者が、どのような判断で対応をするのか、あるいはより上位に報告するのか、の判断基準を明確にしておく
  - 最低限以下の判断が必要
    - 対応すべきインシデントとして認められるかどうか
    - 対応の優先度はどの程度か
    - 誰がインシデント対応を担当するのか
- すべてのインシデントの取り扱いに関する記録をとる
  - 責任の明確化のため
  - 事後の分析のため

2. インシデントに対する初動対応

- 発生したインシデントに関して、どこまで情報を共有するのかを判断する
  - 外部のセキュリティサービス会社等を利用するのか
  - 同様なインシデントの発生が予想される場合、どの範囲まで、インシデント発生に関する告知をすべきか
- これまでに経験しているインシデントなのか、経験したことのないインシデントなのかを判断する
  - これまでに経験したインシデントであれば、過去の対応ノウハウを積極的に活用する
    - そのためには記録の所在を明確にしておく必要がある
  - 経験したことのないインシデントであれば、以下のリソースを活用することを検討する
    - 過去のインシデント対応経験者
    - 他組織における同様なインシデント対応に関する情報
    - 発生したインシデントに直接関係する資産の所有者

インシデントの対応フロー
3. インシデントに関する告知

- 外部組織等に対して、インシデント発生の事実と対応状況に関する報告をする必要があるかどうかを判断する
  - 社会通念上必要性があるため
  - 公的な規則で定められているため
  - ビジネス的なインパクトを軽減させるため
- 誰に、またはどの範囲に告知をすべきかを判断する
  - 社会全体に対してか？
  - 所掌官庁等の外部組織に対してか？
  - 顧客に対してのみか？
- 告知する手段の妥当性を検討する。
  - 自社 Web サイトのみか？
  - 新聞等のメディアを利用するのか？
  - 記者会見か？
  - そのほかか？

インシデントの対応フロー
4. インシデントの抑制措置と復旧

- 発生したインシデントの被害を抑制するための検討項目
  - 抑制措置の手段
  - 抑制措置によるビジネスへの影響
  - 抑制措置の実施期間
  - 最終的な意思決定者
  - 業務時間外における意思決定と実施方法

- 復旧に関する検討項目
  - 事業継続計画（BCP）との関係
  - データ等の資産の一部損失とのトレードオフ
  - 最終的な意思決定

インシデントの対応フロー
5. インシデントの事後対応

- インシデント復旧後のモニタリングを実施する
  - 一部のウィルスやワーム等については、再発する可能性があるため、必要に応じてモニタリングを行う
  - 表面的にはインシデントが解決したように見えても、本質的には問題が解決していない場合がある
- 同様なインシデントの再発防止策を検討する
  - インシデント情報を告知することにより、同様なインシデントの発生を抑制することができる
  - ウィルスやワームには、同じ感染手法を用いた亜種などが発生する
- 他に影響がないかどうかを評価する
  - インシデントを発生させ、他の資産をねらう攻撃手法が存在する
  - 影響が表面化しにくい攻撃手法が存在しているため
- 従業員やスタッフ等への教育を実施する
  - 情報セキュリティに関する教育による、再発防止

インシデントの対応例１
「ノート PC 紛失による情報漏洩」

1. インシデントの発見及び報告
   - 以下の規則が整備され、社員に周知徹底している。
     - ノートPC 紛失時は、紛失判明後１０分以内に上司に報告しなければならない
     - 報告された上司は、１時間以内に情報セキュリティに関する問題を扱う部署に報告しなければならない
2. インシデントに対する初動対応
   - 報告を受けた上司は、紛失者による捜索の支援のために他の従業員を割り当て、期間を指定し、捜索継続を指示した
   - 紛失者は、１時間以内に顛末書を作成し、文書にて上司に報告した
   - 上司は、顛末書に基づき、紛失したノートPC 内の情報資産の重要度を評価し、２時間以内に情報セキュリティに関する問題を扱う部署に報告した
3. インシデントに関する告知
   - 情報セキュリティに関する問題を扱う部署は、CIO 及び広報部門と協議し、社外に告知するかどうかを 6時間以内に決断した
   - 必要に応じて、社外の関係者に対してインシデント発生の告知をおこなった
4. インシデントの抑制措置と復旧
   - 紛失したノートPC の発見の努力を継続し、関係者への謝罪を速やかに実施した
   - 紛失したノートPC が発見され、速やかに関係者へ連絡した
5. インシデントの事後対応
   - 紛失の原因を追究し、紛失してしまう業務環境の精査を実施した
   - 紛失してしまう業務環境の改善を実施した

インシデントの対応例２
「フィッシング サイトによる顧客情報の窃盗行為」

1. インシデントの発見及び報告
   - 組織内 CSIRT が発見者からの報告窓口となっていたため外部から報告があった
   - 日ごろから外部に対して、組織におけるインシデント連絡窓口の連絡先情報を提供していた
2. インシデント報告受領後の初動対応
   - JPCERT/CCや警察機関等へインシデントの報告を行う社内ガイドラインに基づき報告及び対応依頼を実施した
3. インシデントに関する告知
   - フィッシングサイトのサイト閲覧者（顧客等）に対する影響度及び組織のビジネスに対する影響度を評価し、関係各所にフィッシングサイトの存在に関する告知を実施した
4. インシデントの抑制措置と復旧
   - 外部協力組織(JPCERT/CC や警察機関等)との連携を継続した
5. インシデントの事後対応
   - 自サイトの顧客向けシステムにおける認証プロセスの見直しをおこなった

インシデントの対応例３
「顧客 ID の不正利用」

1. インシデントの発見及び報告
   - 顧客IDの不正利用に関する情報提供は、お客様相談窓口や広報部門、総務部門を通じて組織内 CSIRT に共有される仕組みが整っていたため、それぞれから異なった形で報告があった
   - 組織内 CSIRT にて、報告されたインシデント情報を分析し、システムに記録された情報と合わせることでID の不正利用迅速に発見できた。
2. インシデントに対する初動対応
   - 顧客に対する連絡と、被害の度合いに関する情報の収集のために、関係部署に対する告知を行なった
   - 不正 ID 利用者の特定のための情報収集を行なった
3. インシデントに関する告知
   - 今後、同様なインシデントの発生が予想される場合は、本インシデントの事実をすべての顧客に対して告知する、ということを決定した
   - 今回については、本インシデントの対応が完了してから告知をする、という判断をした。
4. インシデントの抑制措置と復旧
   - 当該顧客の ID の一時停止を実施後、顧客の了承を得て、当該顧客の ID を変更した
5. インシデントの事後対応
   - 不正 ID が取得できない環境や仕組みを見直した
   - 不正 ID 取得者に対する損害請求や刑事告訴等を検討した

インシデントの対応例４
「標的型攻撃／高度サイバー攻撃(APT)による侵入」

1. インシデントの発見及び報告
   - 自社に関連する情報流出や不審な通信についての報告を、信頼できる外部組織から受けた
   - 報告された情報から、重大なインシデントに発展する可能性の有無を判断し、組織内の関係部門による対策本部を設置した
2. インシデントに対する初動対応
   - 報告されたインシデント情報を分析し、システムに記録されたログ等の情報と照合し、攻撃の痕跡や不審な通信の有無を確認した
   - 確認された侵害の状況により、通信の遮断や、感染端末の隔離など、必要な措置を講じた
   - マルウェア検体の分析、感染システムのフォレンジックなどを、外部組織と協力して実施した
3. インシデントに関する告知
   - 流出データの関係者や関係組織（顧客、監督官庁など）への報告を実施した
   - 警察への被害届の提出を検討した
4. インシデントの抑制措置と復旧
   - 社内ネットワークに潜伏する感染端末の活動を検知するため、社外への通信の監視を継続した
   - 感染システムやそれを含むネットワークについて、ビジネス上の影響度等から対応の優先順位を判断し、隔離・分析・復旧、その他の必要な措置を実施した
5. インシデントの事後対応
   - ネットワーク内の横断的侵害を検知／防止するための方策を検討、実施した
   - 従業員に対し、侵入に用いられる攻撃手法と対策についての情報共有と注意喚起をおこなった