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

本資料について

- 本資料は、組織内CSIRTが使用する「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、マニュアル作成を支援すること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
  - 一般的なインシデント対応プロセスの例を示し、現在の不文律なインシデント対応フローの文書化および最善策の見える化

目次

- インシデント対応を行う人や部署の明確化
- 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および報告
  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 による情報漏えい」
  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」

インシデント対応を行う人や部署の明確化

- 過去に組織内が経験したインシデントを出発点にして「組織にとってのインシデント」を定義する。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

インシデント対応への備え

- 連絡先リストの整備
  - 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
  - それらの連絡先との間で、連絡手段の疎通確認を実施する
  - 作成した連絡先リストについて、それに記載される連絡先との間で共通認識を持つ
- 各種規則の把握と整合性の確認
  - 組織の規程や規則を確認し、インシデント対応に関連する可能性のある記述を特定する
  - 上記を含む、インデント対応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
  - それらのインフラやツールが使用できなくなる事態に備え、インシデント対応に活用できる代替手段を確保しておく
  - 事前に訓練や演習を実施し、代替手段を含むインフラやツールの活用について習熟しておく

1. インシデントの発見および報告

- インシデントの発見者からの報告を受け取る
  - 報告しやすい環境であることが求められる
  - インシデントの報告窓口が開かれており、適切に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の行動基準を明確にしておく
  - どのような対応をするのか、あるいはより上位に報告するのか、
  - 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
- インシデントの取り扱いに関するすべての記録を残す
  - 責任の明確化のため
  - 事後の分析のため
  - 法的対応を行う可能性に備えるため

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の支援を導入する際に、どこまで情報を開示するか
  - 同様のインシデントの発生や被害拡大が予想されるとき、組織内への告知の中でどこまでの情報を開示するか
- 過去の経験を活用できるかどうかを判断する
  - 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活用できる
    - そのためには対応の記録が適切に残され、活用できる状態でなければならない
  - 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の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情報資産の所有者

3. インシデントに関する告知

- 組織外に対して、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、適切に報告することが求められる
  - 法規制や業界規制によって、すみやかな報告を要請される場合がある
  - 適切に報告することでビジネスへの影響を緩和する
- 誰に告知をすべきかを判断する
  - 社会全体に対する告知
  - 所掌官庁等に対する報告
  - 顧客への告知、など
- 告知する手段を検討する
  - 顧客へのレター
  - 一般に閲覧可能なWeb サイト上での告知
  - メディアへのリリース
  - 記者会見、など

4. インシデントの抑制措置と復旧

- インシデントの被害を抑制するための検討
  - 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
  - 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
  - 最終的な意思決定者

5. インシデントの事後対応

- 復旧後の監視を継続する
  - 潜伏していたマルウェア等の活動再開や、再感染が起きる可能性があるため、監視を強化し、継続する
  - 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
- 再発防止策を検討する
  - インシデント発生の根本原因に応じた対策を導入する
    - 検知や防御のためのセキュリティ管理策の導入
    - ユーザーのシステム利用ポリシー、ネットワーク利用ポリシーの変更など
  - インシデント対応の結果から、検知や防御に利用できる情報を抽出し、それらを共有することにより、同様のインシデントの発生を抑制することができる
- 他の情報資産への影響がないかどうかを評価する
  - 被害が表面化していない可能性
  - 発生したインシデントが、他の資産に対する攻撃から目を逸らすためのものである可能性
- 得られた教訓を従業員やスタッフ等への教育に反映する
  - 脅威とリスクに関する知識の更新と、理解の促進によって防御力の底上げを図る

インシデントの対応例１
「ノート PC 紛失による情報漏えい」

1. インシデントの発見および報告
   - 以下の規則が整備され、社員に周知徹底されている
     - ノートPC 紛失時は、紛失に気付いてから１０分以内に上司に報告しなければならない
     - 報告を受けた上司は、１時間以内にCSIRT（または機器の紛失を扱う部署）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、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CSIRTに報告した
3. インシデントに関する告知
   - CSIRTは組織内の情報セキュリティ委員会へ報告し、委員会での検討により社外に告知するかどうかについて6時間以内に決定された
   - 関係する社外のステークホルダーに対してインシデント発生の報告を行った
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、紛失に繋がる業務手順や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取」

1. インシデントの発見および報告
   - CSIRTは外部の発見者から自組織のフィッシングサイトに関する報告を受けた
   - CSIRTは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情報を公表し周知するための活動を行っていた

2. インシデント報告受領後の初動対応
   - CSIRTは対応手順に基づき、JPCERT/CCや警察機関等へインシデントの報告および対応依頼を行った

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）に対する影響および組織のビジネスに対する影響を評価し、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行った

インシデントの対応事例３
「顧客 ID の不正利用」

1. インシデントの発見および報告
   - 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 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
   - CSIRTは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照合して ID の不正利用を迅速に発見した
2. インシデントに対する初動対応
   - 不正利用された顧客に対する連絡と、被害内容の情報を集めるため、関係部署に連絡し協力を要請した
   - 不正 ID 利用者の特定のための情報収集を行った
3. インシデントに関する告知
   - 今後同様のインシデントの発生時には、インシデントに関する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
   - 今回のインシデントについては、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
   - 不正利用された顧客の ID を一時停止し、顧客の了承を得て 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実装した
   - 不正 ID 取得者に対する損害賠償請求や刑事告訴等を検討した

インシデントの対応事例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および報告
   - CSIRTは、信頼できる外部組織から、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受けた
   - 報告された情報を評価し、重大なインシデントに発展する可能性があると判断し、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行った