情報セキュリティインシデント発生時の対応要領（例）

私立大学情報教育協会
2019年度　大学情報セキュリティ研究講習会
セキュリティ政策・運営コース

アジェンダ

1. 情報セキュリティインシデントとは
2. 情報セキュリティインシデント対応の基本事項
3. インシデント報告基準
4. 情報セキュリティインシデント発生時の対応
5. 遵守すべき規則類

1. 情報セキュリティインシデントとは
2. 情報セキュリティインシデント対応の基本事項
3. インシデント報告基準
4. 情報セキュリティインシデント発生時の対応
5. 遵守すべき規則類

定義

情報セキュリティインシデント（以下「インシデント」という。）

望まない単独若しくは一連の情報セキュリティ事象

又は予期しない単独若しくは一連の情報セキュリティ事象

であって、事業運営を危うくする確率及び情報セキュリティを

脅かす確率が高い事象のことを言う。

具体例

個人情報、特定個人情報（個人番号を内容に含む個人情報）又は機密情報の漏えい（その可能性がある場合も含む）

- PC、USBメモリ、CD-ROM、携帯電話等の紛失／盗難
- 委託業者、関係者等によるデータの持ち出し
- メール誤送信（宛先違い、Cc、不要ファイル添付）
- システム（クラウドサービスや複合機含む）の設定の不備
- 業務外の情報持ち出し

具体例　情報システムへの攻撃

- ウイルス（マルウェア）感染
- 情報システムへのサービス妨害（DoS）攻撃
- 情報システムへの不正アクセス
- メールアカウントの乗っ取り（フィッシングメールの送信等）
- Webページ等の外部公開サイトの改ざん
- 標的型攻撃（高度サイバー攻撃）

具体例　情報システムの障害（利用不能・データ障害等）

- ネットワーク停止やシステムサービスダウン等

  ※サイバー攻撃に起因すると推測されるもの

1. 情報セキュリティインシデントとは
2. 情報セキュリティインシデント対応の基本事項
3. インシデント報告基準
4. 情報セキュリティインシデント発生時の対応
5. 遵守すべき規則類

基本的事項

「情報セキュリティインシデント発生時の確認事項リスト」に確認事項を記載する。

確認事項リストについて全ての項目を埋められなくても、判明している状況を迅速に文部科学省を含めた報告先に報告する。

1. 情報セキュリティインシデントとは
2. 情報セキュリティインシデント対応の基本事項
3. インシデント報告基準
4. 情報セキュリティインシデント発生時の対応
5. 遵守すべき規則類

【報告レベル１】他者や業務に対する影響が殆ど無いと考えられるインシデント

■ 具体例

- サービス妨害攻撃(DDoS等)を受けたがサービス提供に大きな影響が無かったと判断できる事案
- 機密度の低い情報を保存した端末や媒体の紛失、業務に影響が無い範囲でのメール誤送信

■ 報告者名（例）：当該課課長，情報センター(部長)

【報告レベル２】社会的影響が軽微と考えられるインシデント

■具体例

- Ｗｅｂページ改ざん（閲覧によるウイルス感染のおそれや悪意サイトへの誘導が無い場合）
- 第三者（他機関等）に被害を及ぼす可能性が低いと判断できる事案
- 個人情報や重要情報の漏えいの可能性が客観的事実に基づき低いと判断できる事案

■報告者名（例）：情報センターセンター長

※ 報告当初で詳細な状況等が不明な場合には、このレベルを当初レベル想定して対応を行う

【報告レベル３】情報セキュリティ運用管理上で大きな影響があると考えられるインシデント

■具体例

- 標的型攻撃、または高度サイバー攻撃と判断できる事案
- Ｗｅｂページ改ざん（閲覧によるウイルス感染のおそれや悪性サイトへの誘導が有る場合）
- 第三者（他機関等）に被害を及ぼす可能性が高いと判断できる事案
- 個人情報や重要情報の漏えいした、または、漏えいの可能性が高い事案
- 社会的な関心が強く報道機関等への対応が必要とされる事案

■報告者名（例）：ＣＩＳＯ(担当副学長)

※ 報告様式を必ず作成し、公表や報道への対応が想定される場合は、報告様式に『公表日時』、『公表内容』も記載する

【報告レベル４】一般国民、他機関へ重大な被害を拡大させていると思われるインシデント

■具体例

- 標的型攻撃、または高度サイバー攻撃と判断でき、かつ特に重大な事案
- 一般国民や他機関へ重大な被害を及ぼしたと客観的に思われる事案
- 社会的な反響が大きく、報道等で対応が大きく問われると想定される事案
- 政府機関や他機関・法人等に重大な被害を与えている（与える可能性が高い）と判断される事案
- 特定個人情報、要配慮個人情報（病歴、健康診断等の結果、心身の機能の障害、人種、信条、犯罪の経歴等）、収入、成績、機微技術等といった極めて重要な情報が漏えいしている可能性が高い事案

■ 報告者名（例）：学長，理事長

1. 情報セキュリティインシデントとは
2. 情報セキュリティインシデント対応の基本事項
3. インシデント報告基準
4. 情報セキュリティインシデント発生時の対応
5. 遵守すべき規則類

【個人情報に関連するインシデント】

■個人情報保護委員会への報告

1. 「個人データの漏えい等の事案が発生した場合等の対応について」（平成29年個人情報保護委員会告示第１号）に沿って対応する。
2. 原則として、個人情報保護委員会のwebサイト「漏えい等の対応」ページにある報告フォームから報告する。
   報告フォーム➢https://www.ppc.go.jp/legal/rouei/

※ 重大な影響が生じると判断された事案、公表事案等の急を要する報告は、事前に電話で一報する。電話番号　03-6457-9685

【特定個人情報に関連するインシデント】

■個人情報保護委員会への報告

1. 「事業者における特定個人情報の漏えい事案等が発生した場合の対応について」（平成27年特定個人情報保護委員会告示第２号）に沿って対応する。
2. 重大事態の場合は、個人情報保護委員会のwebサイト「漏えい等の対応」ページにある報告フォームから報告する。
   報告フォーム➢https://www.ppc.go.jp/legal/rouei/
3. 重大事態に該当しない場合は、郵送により報告する。

【重大事態】

① 情報提供ネットワークシステム、個人番号利用事務若しくは個人番号関係事務に使用する情報システム又は個人番号関係事務の委託を受けた者が当該事務処理に使用する情報システムにおいて、特定個人情報が漏えいし、滅失し、又は毀損した事態

② 次に掲げる特定個人情報に係る本人の数が100人を超える事態

ア 漏えいし、滅失し、又は毀損した特定個人情報

イ 番号法（※）第９条（利用範囲）に反して利用された特定個人情報

ウ 番号法（※）第19条（提供の制限）に反して提供された特定個人番号

③ 特定個人情報を電磁的方法により不特定多数の者が閲覧可能な状態となり、かつ、閲覧された事態

④ 不正な目的で特定個人情報を利用し、又は提供した者がいる事態

※ 番号法：行政手続における特定の個人を識別するための番号の利用等に関する法律