Expand - Collapse

- Sec01-08-4 FAQの分類体系
  - 【2018年3月31日】
  - 概要
    - 過去の相談記録、ガイドブック、事前調査資料等に基づいて、内容を分類して汎化したQ＆Aを作成し、相談用手元資料とする【相談回答の均質化】
    - Q&A項目：分類（キーワード）、質問例、回答例（対応策、ナビゲーション先）、参考にした情報、質問者に参考になる情報の所在場所
  - FAQ分類（ガイドブック項立てに沿った分類）
    - 案件分類(SORT)
      - 01.個別サイバーセキュリティ事象の相談【Mission１】
        - 01.セキュリティ事象全般
        - 02.迷惑メール・スパムメール
        - 03.標的型攻撃による情報流出
        - 04.ビジネスメール詐欺
        - マルウェア（ウイルス）による被害
          - 051.ウイルス感染
          - 052.ランサムウェアを使った詐欺・恐喝
          - 053.アドウェアによる詐欺
        - 06.フィッシング詐欺・なりすまし
          - 061.なりすまされたECサイトの被害
          - 062.なりすましサイトの利用者の被害
          - 063.なりすまされた利用者の被害
        - 07.Web サービスからの個人情報の窃取
        - 08.集中アクセス（DoS攻撃等）によるサービス停止
        - 09.内部不正による情報漏えいと業務停止
        - 10.Web サイトの改ざん
        - 11.インターネットバンキングの不正送金
        - 12.悪意のあるスマホアプリによる攻撃
        - 13.巧妙・悪質化するワンクリック詐欺
        - 14.Web サービスへの不正ログイン
        - 15.公開された脆弱性対策情報の悪用
        - 16.ネット上の誹謗・中傷【10大脅威より】
        - 17.IoT 機器の不適切な管理【10大脅威より】
        - 18.情報モラル欠如に伴うセキュリティ問題の発生【10大脅威より】
        - 90.セキュリティ事象か不明
      - 02.全般的なサイバーセキュリティ対策の相談

Expand - Collapse

- 01.組織的対応
  - 010.全般的対策
  - 011.管理的対策
  - 012.人的対策
  - 013.技術的対策
  - 014.物理的対策
  - 015.緊急時対応
  - 018.セキュリティ人材確保
- 03.不正アクセス全般
- 04.　情報漏えい全般
- 09.参考情報

- 09.その他
  - 01.相談窓口について
  - 02.セミナー依頼
  - 03.ガイドブック等の入手、活用
  - 04.セキュリティ対象外
  - 05.電波系
  - 20.その他

- 提示する対策項目【Mission2に沿って】
  - 01.全般
  - 02.情報セキュリティ5か条+2の備え
    - 021.全般
    - 022.OS とソフトウェアのアップデート
    - 023.ウイルス対策ソフト・機器の導入
    - 024.定期的なバックアップ
    - 025.パスワードの管理
    - 026.アクセス管理
    - 027.紛失や盗難による情報漏えい対策
    - 028.持ち込み機器対策
  - 03.電子メールへの備え
    - 031.電子メールの安全利用
    - 032.標的型攻撃メールへの対応
    - 033.迷惑メール発信への対応
  - 04.今やろう！　インターネット利用への備え
    - 041.安全な Web サイト利用
    - 042.閲覧制限
    - 043.パスワード管理【追加】
  - 10.経営者が主導する対策【Mission3】

Expand - Collapse

- 20.緊急時対応手順【Mission4】
- 20.その他

- FAQ分類（「ここからセキュリティ」を参照）
  - FAQ及び各種参考情報は、「ここからセキュリティ」に準拠して分類する
    - 他機関提供情報とマージしやすくするため
  - 1.被害にあった？（侵害の予兆を含む）
    - 02.ウイルスに感染したら（ランサムウェアを含む）
    - 03.不正アクセス
    - 04.情報漏えい
    - 05.ワンクリック詐欺
    - 06.フィッシング詐欺・なりすまし
      - 061.フィッシング詐欺・なりすまし被害
      - 062.なりすまされたECサイト
    - 07.詐欺メール
      - 071.迷惑メール
      - 072.標的型攻撃メール
      - 073.ビジネスメール詐欺
    - 08.サービス妨害（DoS攻撃等）
    - 09.嫌がらせ、誹謗中傷
  - 2.事前に対策を（事象毎の予防策）
    - 01.対策の基本
      - 011.企業における対策の基本
      - 012.家庭で行う対策
      - 013.子どもを守るための対策
    - 02.ウイルス対策（ランサムウェアを含む）
    - 03.不正アクセス対策
    - 04.情報漏えい
    - 05.ワンクリック詐欺
    - 06.フィッシング詐欺・なりすまし
      - 061.フィッシング詐欺・なりすまし被害
      - 062.なりすまされたECサイト
    - 07.詐欺メール
      - 071.迷惑メール
      - 072.標的型攻撃メール
      - 073.ビジネスメール詐欺
    - 08.サービス妨害（DoS攻撃等）

Expand - Collapse

- 09.嫌がらせ、誹傷中傷
- 10.個別対策項目
  - 101.パスワード
- 20.ガイドライン等
  - 201.教育機関向け
  - 202.個人ユーザ向け
  - 203.事業者向け

3.教育・学習

- 01.一般向け
  - 011.小学生向け
  - 012.中高校生向け
  - 013.ホームユーザ向け
- 02.中小企業向け
- 03.経営者向け
- 04.システム管理者
- 05.一般社員・職員

4.セキュリティチェック

- 01.クイズ形式
- 02.安全性を診断しよう
- 03.試験・資格

5.データ＆レポート

- 01.参考になる資料、情報サイト

6.その他

- 01.相談窓口について
- 02.セミナー依頼
- 03.ガイドブック等の入手、活用
- 04.セキュリティ対象外
- 05.電波系

ケース別の事故対応の流れに沿った対応例

- 情報セキュリティ事故対応ガイドブック（情報セキュリティ大学院大学）等の対応フローとチェックシートを参考に
- 情報システムの障害（利用不能、データ喪失 等）
- 情報システムへの攻撃（ウィルス感染、不正アクセス、改ざん 等）
- 情報漏えい（可能性も含む）

- 汎化した内容をWebで公開