Sec01-08-4 FAQの分類体系

1. 【2018年3月31日】
2. 概要
   1. 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】
   2. 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
3. FAQ分類（ガイドブック項立てに沿った分類）
   1. 案件分類(SORT)
      1. 01.個別サイバーセキュリティ事象の相談【Mission１】
         1. 01.セキュリティ事象全般
         2. 02.迷惑メール・スパムメール
         3. 03.標的型攻撃による情報流出
         4. 04.ビジネスメール詐欺
         5. マルウェア（ウイルス）による被害
            1. 051.ウイルス感染
            2. 052.ランサムウェアを使った詐欺・恐喝
            3. 053.アドウェアによる詐欺
         6. 06.フィッシング詐欺・なりすまし
            1. 061.なりすまされたECサイトの被害
            2. 062.なりすましサイトの利用者の被害
            3. 063.なりすまされた利用者の被害
         7. 07.Web サービスからの個人情報の窃取
         8. 08.集中アクセス（DoS攻撃等）によるサービス停止
         9. 09.内部不正による情報漏えいと業務停止
         10. 10.Web サイトの改ざん
         11. 11.インターネットバンキングの不正送金
         12. 12.悪意のあるスマホアプリによる攻撃
         13. 13.巧妙・悪質化するワンクリック詐欺
         14. 14.Web サービスへの不正ログイン
         15. 15.公開された脆弱性対策情報の悪用
         16. 16.ネット上の誹謗・中傷【10大脅威より】
         17. 17.IoT 機器の不適切な管理【10大脅威より】
         18. 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】
         19. 90.セキュリティ事象か不明
      2. 02.全般的なサイバーセキュリティ対策の相談
         1. 01.組織的対応
            1. 010.全般的対策
            2. 011.管理的対策
            3. 012.人的対策
            4. 013.技術的対策
            5. 014.物理的対策
            6. 015.緊急時対応
            7. 018.セキュリティ人材確保
         2. 03.不正アクセス全般
         3. 04．情報漏えい全般
         4. 09.参考情報
      3. 09.その他
         1. 01.相談窓口について
         2. 02.セミナー依頼
         3. 03.ガイドブック等の入手、 活用
         4. 04.セキュリティ対象外
         5. 05.電波系
         6. 20.その他
   2. 提示する対策項目【Mission2に沿って】
      1. 01.全般
      2. 02.情報セキュリティ5か条+2の備え
         1. 021.全般
         2. 022.OS とソフトウェアのアップデート
         3. 023.ウイルス対策ソフト・機器の導入
         4. 024.定期的なバックアップ
         5. 025.パスワードの管理
         6. 026.アクセス管理
         7. 027.紛失や盗難による情報漏えい対策
         8. 028.持ち込み機器対策
      3. 03.電子メールへの備え
         1. 031.電子メールの安全利用
         2. 032.標的型攻撃メールへの対応
         3. 033.迷惑メール発信への対応
      4. 04.今やろう！　インターネット利用への備え
         1. 041.安全な Web サイト利用
         2. 042.閲覧制限
         3. 043.パスワード管理【追加】
      5. 10.経営者が主導する対策【Mission3】
      6. 20.緊急時対応手順【Mission4】
      7. 20.その他
4. FAQ分類（「ここからセキュリティ」を参照）

ドキュメントを参照: [company.html](https://www.ipa.go.jp/security/kokokara/study/company.html)

* 1. 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
     1. 他機関提供情報とマージしやすくするため
  2. 1.被害にあった？（侵害の予兆を含む）
     1. 02.ウイルスに感染したら（ランサムウェアを含む）
     2. 03.不正アクセス
     3. 04.情報漏えい
     4. 05.ワンクリック詐欺
     5. 06.フィッシング詐欺・なりすまし
        1. 061.フィッシング詐欺・なりすまし被害
        2. 062.なりすまされたECサイト
     6. 07.詐欺メール
        1. 071.迷惑メール
        2. 072.標的型攻撃メール
        3. 073.ビジネスメール詐欺
     7. 08.サービス妨害（DoS攻撃等）
     8. 09.嫌がらせ、 誹謗中傷
  3. 2.事前に対策を（事象毎の予防策）
     1. 01.対策の基本
        1. 011.企業における対策の基本
        2. 012.家庭で行う対策
        3. 013.子どもを守るための対策
     2. 02.ウイルス対策（ランサムウェアを含む）
     3. 03.不正アクセス対策
     4. 04.情報漏えい
     5. 05.ワンクリック詐欺
     6. 06.フィッシング詐欺・なりすまし
        1. 061.フィッシング詐欺・なりすまし被害
        2. 062.なりすまされたECサイト
     7. 07.詐欺メール
        1. 071.迷惑メール
        2. 072.標的型攻撃メール
        3. 073.ビジネスメール詐欺
     8. 08.サービス妨害（DoS攻撃等）
     9. 09.嫌がらせ、 誹謗中傷
     10. 10.個別対策項目
         1. 101.パスワード
     11. 20.ガイドライン等
         1. 201.教育機関向け
         2. 202.個人ユーザ向け
         3. 203.事業者向け
  4. 3.教育・学習
     1. 01.一般向け
        1. 011.小学生向け
        2. 012.中高校生向け
        3. 013.ホームユーザ向け
     2. 02.中小企業向け
     3. 03.経営者向け
     4. 04.システム管理者
     5. 05.一般社員・職員
  5. 4.セキュリティチェック
     1. 01.クイズ形式
     2. 02.安全性を診断しよう
     3. 03.試験・資格
  6. 5.データ＆レポート
     1. 01.参考になる資料、 情報サイト
  7. 6.その他
     1. 01.相談窓口について
     2. 02.セミナー依頼
     3. 03.ガイドブック等の入手、 活用
     4. 04.セキュリティ対象外
     5. 05.電波系

1. ケース別の事故対応の流れに沿った対応例
   1. 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

ドキュメントを参照: [sub07.html](http://lab.iisec.ac.jp/~hiromatsu_lab/sub07.html)

* 1. 情報システムの障害（利用不能、 データ喪失 等）
  2. 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）
  3. 情報漏えい（可能性も含む）

1. 汎化した内容をWebで公開