Sec01-08-3 相談対応手順書（マニュアル）

1. インデックス
   1. 【緊急】情報の漏えい・改ざんが起きているようだ
      1. Webサーバ改ざん？
      2. 情報漏えい・流出？
      3. 犯罪の可能性がある場合は
      4. 対応策の相談の場合は
      5. 実被害にあった場合は
   2. **【緊急】マルウェア（ウイルス・ランサム・アドウェア）**
      1. **Emotet等のマルウェア感染**
   3. 【緊急】なりすましECサイト被害・フィッシング詐欺
      1. 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
   4. **【緊急】メール等を使った脅迫・詐欺の手口による金銭要求**
   5. 【緊急】「ビジネスメール詐欺」により偽振込先に振り込んでしまった
      1. 04.ビジネスメール詐欺
   6. 【緊急】実在する企業名で架空請求を受けた場合
   7. 【緊急】PC、 スマホの動きがおかしくなった、 データが壊れたようだ
   8. 平時の備え
      1. 情報セキュリティ侵害に遭わないように事前に何をすればいいか
      2. これから検討の標準回答
   9. 啓発（教育・学習）
   10. 各種セキュリティ対策のサービス提供機関の紹介
   11. セキュリティ以外
   12. 資料請求
   13. 【ガイドブック】に沿った案件別FAQ
       1. 01.個別サイバーセキュリティ事象の相談【Mission１】
          * 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
          * 05.マルウェア（ウイルス）による被害
            + 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】
          * 19.犯罪のビジネス化【10大脅威より】
          * ・・・・
       2. 02.全般的なサイバーセキュリティ対策の相談
          * 01.組織的対応
            + 一般論としての緊急対応、 恒久的対策
       3. 提示する対策項目【Mission2に沿って】
   14. 

相談対応時参考資料・Webサイトへのリンク

* + 1. 警察署一覧
  1. 汎用の手順書へのリンク

1. 目的
   1. 具体的な相談対応時の回答の均質化を目指す
2. 相談受付対応手順
   1. 用件のカテゴリの確認
      1. 相談か？
      2. 資料請求か？
   2. 何の相談か？二次対応へのディスパッチ
      1. どんな事象が起きているのかの概要を確認
      2. セキュリティ被害の可能性がある 【緊急】へ
      3. セキュリティ対策に不安がある 【平時の備え、 啓発】へ
      4. セキュリティ以外の相談 【セキュリティ以外】へ
      5. 資料請求の場合
3. クイックリスト掲載案件の相談対応手順
   1. 相談のきっかけ
      1. どこでこの窓口を知ったか？
      2. 既にどこかに相談したか？
   2. 正確な状況把握のために相談者の立場を確認
      1. 相談者は経営者か？システム管理者か？一般の従業員か？
         * セキュリティ担当者、 システム管理者から状況を聞く
      2. システム管理者がいない場合は、 運用保守支援業者がいるか確認
   3. 【緊急】どんな環境で何が起きているかを確認
      1. まずは落ち着いて今起きている事象を確認しましょう
      2. セキュリティ問診票「『やられたかな？その前に』ガイド～ 『やられてる』！と思ったら ～」【ISOG-J】(pdf形式)

参照:

<http://isog-j.org/output/2015/Yararetakana-Guide-20151014.pdf>;

* 1. 緊急
     1. 【緊急】セキュリティ侵害の可能性があるが、 どこに問い合せていいかわからない?
     2. 【緊急】情報の漏えい・改ざんが起きているようだ （ウィルス感染、 不正アクセス、 改ざん、 データ喪失、 情報漏えい等）
        + どんな被害か？
        + ウイルス感染？
        + Webサーバ改ざん？
        + 情報漏えい・流出？
        + 犯罪の可能性がある場合は
        + 対応策の相談の場合は
        + 実被害にあった場合は
     3. 【緊急】なりすましECサイト被害
        + 実被害者は顧客
        + 【相談】なりすましECサイトを立ち上げられた事業者からの相談
          - なりすましECサイト対策協議会のHPを紹介

参照:

<https://www.saferinternet.or.jp/narisumashi/>;

* + - * + 顧客に対して
      * 【相談】なりすましECサイトと知らずに取引をした利用者からの相談
      * 

なりすましECサイト標準回答

* + - * + ●緊急対応
        + ●風評被害について
        + ●相談及び届出
    1. 【緊急】メール等を使った脅迫・詐欺の手口による金銭要求
    2. 【緊急】「ビジネスメール詐欺」により偽振込先に振り込んでしまった
    3. 【緊急】実在する企業名で架空請求を受けた場合
    4. 【緊急】PC、 スマホの動きがおかしくなった、 データが壊れたようだ
    5. その他
  1. 平時の備え
     1. 情報セキュリティ侵害に遭わないように事前に何をすればいいか
     2. 

これから検討の標準回答

* 1. 啓発（教育・学習）
  2. 各種セキュリティ対策のサービス提供機関の紹介
     1. IPAセキュリティプレゼンター検索
     2. 情報セキュリティサービス審査登録制度
        + サービスの種類
          - ・セキュリティ監査サービス
          - ・脆弱性診断サービス
          - ・デジタルフォレンジックサービス
          - ・セキュリティ運用・監視サービス
     3. ITコーディネータ協会　「経営とIT化相談」窓口
     4. 東京都中小企業振興公社ワンストップ総合相談
  3. セキュリティ以外
     1. 消費生活全般に関する苦情や問合せ
     2. 嫌がらせ、 ネットストーカー
     3. 振り込め詐欺・オレオレ詐欺
     4. 人権侵害
     5. 個人情報の取り扱い
  4. 資料請求

1. 【ガイドブック】に沿った案件別FAQ
   1. 作成方法
   2. 01.個別サイバーセキュリティ事象の相談【Mission１】
   3. 02.全般的なサイバーセキュリティ対策の相談
   4. 09.その他
   5. 提示する対策項目【Mission2に沿って】
2. 相談対応時参考資料・Webサイトへのリンク
3. 汎用の手順書へのリンク