Expand - Collapse

Sec01-09サイバーセキュリティ相談対応ハンドブック（相談者へのアドバイス）

- 【2017年11月10日】

今起きてる事象？

【緊急】サイバー犯罪行為の届出

- 警視庁所轄への相談を促す

【緊急】サイバー犯罪の可能性（情報漏えい・改ざん・サービス妨害等）

- 警視庁サイバー犯罪対策課への相談を促す

【緊急】ウイルス感染・不正アクセスに遭っているようだ

- まずは、導入しているセキュリティ対策ソフトのホットラインへの相談を促す

セキュリティ被害の届け出

- iIPAセキュリティセンタへの届出を促す

インシデント発生元等への連絡、対処、調査の実施依頼

- JPCERT/CCへの届出を促す

PCがおかしい？

セキュリティ上の問題の可能性あり

- IPAセキュリティセンターへの相談を促す

セキュリティ上の問題ではなさそう

- PCの保守業者への相談を促す

セキュリティ案件以外

- 消費者ホットラインへの相談を促す

一般論での相談

予防対策【事前対策】

インターネットを安全に利用するための情報セキュリティ対策9か条【NISC・IPA】＋情報セキュリティ5か条【IPA】

OS やソフトウェアは常に最新の状態にしておこう

- 新たにひろまるコンピュータウイルスに対抗するため製造元から無料で配布される最新の改良プログラムにアップデートしましょう。

パスワードは貴重品のように管理しよう

- パスワードは自宅の鍵と同じく大切です。パスワードは他人に知られないように、メモをするなら人目に触れない場所に保管しましょう。

ログインID・パスワード絶対教えない用心深さ

- 金融機関を名乗り、銀行口座番号や暗証番号、ログインIDやパスワード、クレジットカード情報の入力を促すような身に覚えのないメールが届いた場合、入力せず無視しましょう。

Expand - Collapse

- 身に覚えのない添付ファイルは開かない
  - 身に覚えのない電子メールにはコンピュータウイルスが潜んでいる可能性があります。添付されたファイルを開いたり、URL（リンク先）をクリックしないようにしましょう。
- ウイルス対策ソフトを導入しよう
  - ウイルスに感染しないように、コンピュータにウイルス対策ソフトを導入しましょう。（家電量販店などで購入できます）
- ネットショッピングでは信頼できるお店を選ぼう
  - 品物や映画や音楽も購入できるネットショッピング。詐欺などの被害に遭わないように信頼できるお店を選びましょう。身近な人からお勧めのお店を教わるのも安心です。
- 大切な情報は失う前に複製しよう
  - 家族や友人との思い出の写真など、大切な情報がパソコンの故障によって失われることのないよう、別のハードディスクなどに複製して保管しておきましょう。
- 外出先では紛失・盗難に注意しよう
  - 大切な情報を保存したパソコン、スマートフォンなどを自宅から持ち出すときは機器やファイルにパスワードを設定し、なくしたり盗まれないように注意して持ち歩きましょう。
- 困ったときはひとりで悩まず まず相談
  - 詐欺や架空請求の電子メールが届く、ウイルスにより開いているウェブページが閉じないなどの被害に遭遇したら、一人で悩まず各種相談窓口に相談しましょう
- 共有設定を見直そう！
  - データ保管などのクラウドサービスやネットワーク接続の複合機の設定を間違ったため無関係な人に情報を覗き見られるトラブルが増えています。クラウドサービスや機器は必要な人にのみ共有されるよう設定しましょう。
- 脅威や攻撃の手口を知ろう！
  - 巧妙な手口が増えています。脅威や攻撃の手口を知って対策をとりましょう。
  - 正規のウェブサイトを改ざん
  - ウェブサイトにアクセスするだけでマルウェア感染
  - 標的型メールでの不正サイトへの誘導
  - 不審なメールのマルウェア添付
  - テクニカルサポート詐欺

- 緊急対応【事後対策】
  - ■緊急対応（自然災害、大火災、感染症、テロ、、、）
    - 予兆検知から原状復旧まで

Expand - Collapse

- 事象の検知、報告受付(Detect)
- 事実確認、対応の判断

- 被害の局所化(拡大防止)(Triage)
  - 該当システムをネットワークから切り離し、使用を中止する。
  - 被害の範囲を確認し、使用を停止する
- 早期復旧・事業継続(Respond)
  - 分析、対処、エスカレーション、連携
- 原因調査
  - なぜ情報セキュリティ侵害が起きたか？
- 復旧
  - システム管理者に連絡してその指示に従って、適切な復旧を行う。
- 再発防止策
  - インシデントからの知見の学習
  - 恒久的対策

- 恒久的対策
  - 定期的なバックアップ
    - ランサムウェアも含めた対策
  - ルールの策定
    - 事業継続計画（BCP）の策定
    - 情報セキュリティポリシーの策定
      - 情報資産台帳の作成及びリスク分析
      - 重要度（リスク×脆弱性×（機密性＋完全性＋可用性確保の必要性））の高いものから優先的に、管理的・人的・技術的・物理的対策を実施
  - フールプルーフ対策
    - 人間が間違えても危険にならない仕組みにしておく、
  - フェールセーフ対策
    - 機械が壊れても危険にならない仕組みにしておく
  - ルールの遵守、監査

- 相談窓口業務
  - 相談者に的確な回答のために
    - FAQの作成
      - FAQは、本来過去に多い質問と回答を提示するものであるが、Qが溜まらない段階では、想定で準備する
    - 予測調査
      - 相談が来そうな内容をあらかじめ調べておくことが重要

Expand - Collapse

- レファレンス用情報の収集と、情報提供のための整理
  - 日々のサイバーセキュリティ関連情報の収集と整理
  - サイバーセキュリティ関連の情報の所在、内容の確認とインデキシング
    - 参考とする関連ガイドラインの内容構成のリストの作成及び更新
- ナレッジデータ、レファレンスデータの収集と整理
  - 相談窓口として、次にとるべきことを、的確に示唆するためには、事前に有用と思われる情報源、情報の内容を把握し、それを参考に回答するテキストデータベースを構築
  - 的確な情報へのナビゲーションのためのインデキシング
  - セキュリティ関連のナレッジデータベースの構築
    - 全文検索が可能なWebページ、電子書籍形式
- 相談されない大多数の人に一般論として対策を知ってもらうために
  - FAQの公開
  - 予測調査内容の公開
  - ガイドブックのWeb公開
  - ガイドブックの配布
  - 緊急情報の発信、情報源へのナビゲート