Expand - Collapse

- Sec01-07 情報セキュリティ対策ガイド（初心者向け抜粋版）
  - 【2017年8月1日】
  - 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】
    - OS やソフトウェアは常に最新の状態にしておこう
    - パスワードは貴重品のように管理しよう
    - ログインID・パスワード絶対教えない用心深さ
    - 身に覚えのない添付ファイルは開かない
    - ウイルス対策ソフトを導入しよう
    - ネットショッピングでは信頼できるお店を選ぼう
    - 大切な情報は失う前に複製しよう
    - 外出先では紛失・盗難に注意しよう
    - 困ったときはひとりで悩まず まず相談
  - 情報セキュリティ5か条（全2ページ、721KB）【IPA】pdf
    - こんな情報があるはず！
      - 従業員のマイナンバー、住所、給与明細
      - お客様や取引先の連絡先一覧
      - 取引先ごとの仕切り額や取引実績
      - 新製品の設計図などの開発情報
      - 組織の経理情報
      - 取引先から取扱注意と言われた情報
    - 漏れたら大変！こんなダメージが！
      - 被害者への損害賠償などの支払い
      - 取引停止、顧客の他社への流出
      - ネットの遮断などによる生産効率のダウン
      - 従業員の士気低下
    - まずは始めてみよう
      - ①OSやソフトウェアは常に最新の状態に使用！
        - OSやソフトウェアのセキュリティ上の問題点を放置していると、それを悪用したウイルスに感染してしまう危険性があります。お使いのOSやソフトウェアに修正プログラムを適用する、もしくは最新版を利用しましょう。
      - ②ウイルス対策ソフトを導入しよう！
        - ID・パスワードを盗んだり、遠隔操作を行ったり、ファイルを勝手に暗号化するウイルスが増えています。ウイルス対策ソフトを導入し、ウイルス定義ファイル(パターンファイル)は常に最新の状態になるようにしましょう。
      - ③パスワードを強化しよう！

Expand - Collapse

- パスワードが推測や解析されたり、ウェブサービスから窃取
  - ドが流用されることで、不正にログインされる被害が増えています。パスワードは「長く」「複雑に」「使い回さない」ようにして強化しましょう。

- ④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。

- ⑤脅威や攻撃の手口を知ろう！
  - 取引先や関係者と偽ってウイルス付のメールを送ってきたり、正規のウェブサイトに似せた偽サイトを立ち上げてID・パスワードを盗もうとする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。

- ネットワークビギナーのための情報セキュリティハンドブック（小冊子）【2016年02月02日NISC】⇒【2016年12月02日NISC】

  - 目次
    - 人物紹介
    - おうちのCSIRTになってね
    - Black Hat the Cracker

  - プロローグ サイバー攻撃ってなに？誰がやっているの？どんなことが起こるの？～サイバー攻撃のイメージ

    - S1. サイバー攻撃のイメージ
      - S1. サイバー攻撃って誰がやっているの？どうするの？
      - コラム：攻撃者とハッカーとクラッカー

      - コラム：攻撃者が使う武器「マルウェア」
        - どんな種類があるの？
        - どんな機能を持つの？
        - どんなものが感染したり、感染させたり、悪さするようになるのか

      - S2. サイバー攻撃の例
        - 偽サイトでのフィッシング詐欺や重要情報の不正送信
        - ランサムウェアで身代金要求
        - ボットネットに組み込まれる

      - S3. サイバー関連の犯罪やトラブル
        - なりすましや略取・誘拐（連れ去り）
        - セクスティング
        - ネットいじめ

      - S4. 人の心の隙を突く「ソーシャルエンジニアリング」攻撃
        - 「ソーシャルエンジニアリング」は現実でもネットでも心の隙を突いてだます

Expand - Collapse

- 第1章 基本のセキュリティ～ステップバイステップでセキュリテ
  - S1. 4つのポイントでセキュリティを守る
    - P1. システムを最新に保つ。セキュリティソフトを入れて防ぐ
      - 様々な段階でセキュリティを守る
    - P2. 複雑なパスワードと多要素認証で侵入されにくくする
    - P3. 攻撃されにくくするには侵入に手間（コスト）がかかるようにする
      - 守りを何重にもして侵入されにくくする
    - P4. 心の隙を作らないようにする（対ソーシャルエンジニアリング）
  - S2. 環境を最新に保つ、セキュリティソフトを導入する
    - P1. セキュリティソフトを導入して守りを固めよう
      - 単純なウイルス検知ソフト
      - 進化したセキュリティソフト（ふるまい検知、ヒューリスティック分析）
      - 手配書が間に合わないゼロディ攻撃も
    - P2. パソコン本体とセキュリティの状態を最新に保とう
      - 本体もOSもセキュリティソフトも重要ソフトもアップデート
    - P3. スマートフォンやネットワーク機器も最新に保とう
      - アプリやセキュリティソフトの更新は基本的に自動にし、まめにチェック
      - ネットにつながる家電もファームウェア更新、設定ページのID・パスワードは変更しておくこと
    - P4. ソフトやアプリは信頼できる場ところ所から。権限にも気をつける
      - 不審な場所からアプリをインストールしない。権限に気をつける
    - コラム：必要ならばスマホにはセキュリティパックを検討しよう
      - 必要性を感じるなら、スマホにはセキュリティパック導入を検討しよう
      - スマホの改造をしてはいけません
      - スマート家電の中にはパソコンやスマホがある？
    - コラム：パソコンやスマホを最新の状態に保っても防げない攻撃がある。それがゼロディ攻撃！
      - ゼロディ攻撃とは？ 対処の例
      - ゼロディ攻撃に対抗するには？
  - S3. 複雑なパスワードと多要素認証で侵入されにくくする
    - P1. パスワードの安全性を高める
      - パスワードは少なくとも英大文字小文字＋数字＋記号で10桁
    - P2. パスワードの使い回しをしない
      - 同じパスワードを使い回さない。似たパスワード、法則性のあるパスワードは×

Expand - Collapse

- P3. パスワードを適切に保管する
  - パスワードを使用する場所に置かない。パソコンの中も×
  - パスワードはノートに書いて保管するか、パスワード管理アプリで守る
  - ブラウザの自動入力にパスワードを覚えさせない
- P4. 秘密の質問にはまじめに答えない。多要素や生体認証を使う
  - 秘密の質問にはまじめに答えない。答えは使い回さない
  - 多要素認証やログイン通知でセキュリティを向上
- コラム：パスワードはどうやって漏れるの？どう使われるの？
  - 様々なID・パスワードの抜き取り方法
  - 盗んだID・パスワードを使い様々なサービスを乗っ取れるか試す

- S4. 攻撃されにくくするには、手間（コスト）がかかるようにする
  - 攻撃されにくくするには手間がかかるようにする
  - 金銭目的ではない攻撃にも備えよう
  - 攻撃者に操られて内側から鍵を開けてしまわないように心がまえを持とう
- S5. 心の隙を作らないようにする（対ソーシャルエンジニアリング）
  - 古典的なソーシャルエンジニアリング
  - デジタル世代のソーシャルエンジニアリング
  - 標的型メールの例
  - フィッシングメールの例
  - 悪意はないが拡散してしまう例
  - コラム：軍事スパイ、産業スパイに狙われてしまったら
    - 職業スパイにはコストによる防御が効かない
    - スパイ活動の今昔
  - コラム：映画「ザ・ハッカー」にみるソーシャルエンジニアリング
  - コラム：スパムメールとその由来

- 第2章セキュリティを理解して、ネットを安全に使う
  - S1. パスワードを守る、 パスワードで守る
    - P1. パスワードってなに？
    - P2. 3種類の「パスワード」を理解する
      - 1を「PINコード」
      - 2を「ログインパスワード」
      - 3を「暗号キー」
    - P3. 「PI Nコード」と「ログインパスワード」に求められる複雑さの違い
    - P4. 「暗号キー」に求められる複雑さ
    - P5. どちらの「パスワード」か、わかりにくい例
      - トピック：パスワードを破る手段は色々

Expand - Collapse

- ブルートフォース攻撃（総当たり攻撃）
- リスト型攻撃（アカウントリスト/パスワードリスト攻撃）
- 辞書攻撃（ディクショナリアタック）

- P6. 総当たり攻撃以外のパスワードを破る攻撃や生体認証を使った防御
  - トピック：多要素認証の構成要素は？
    - ①知っているもの
    - ②持っているもの
    - ③本人自身に関するもの
  - トピック：指紋認証が破られることも…
- P7. パスワードの定期変更は必要なし。流出時は速やかに変更する
- P8. パスワード流出時の便乗攻撃に注意
- P9. 厳重なパスワードの保管
  - トピック：ブラウザにはパスワード保存しない
  - トピック：パスワード管理方法の例
  - トピック：パスワード管理方法のメリットデメリット
- P10. パスワード情報をクラウドで利用する善し悪し
- P11. ノートやスマホを失くした場合のリカバリ考察
- P12. 次善の策のソーシャルログイン。二段階認証などで防御
- P13. ソーシャルログインで連携される情報に注意
  - トピック：ソーシャルログインに使えるアカウント
    - 二段階認証
    - ログイン通知
  - トピック：ソーシャルログインとサービス・アプリ連携の違い
    - ソーシャルログイン
    - アプリ・サービス連携
  - トピック：アプリなどの連携は定期的に棚卸ししよう
- P14. ソーシャルログインとは性格が違うサービス連携
- コラム：暗号化の超簡単説明
  - トピック：暗号化ってなに？
    - 平文での通信は読めてしまう
    - 暗号化の魔法は内容を読めなくする
    - 暗号化したものを送れば攻撃者が読めない
    - 事前に決めておいた方法（暗号化方法）と呪文（「暗号キー」）で暗号文を復元（復号）する
  - トピック：暗号が破られる場合
    - 暗号化方法の種類はいろいろ

Expand - Collapse

- 暗号破られ①　呪文がバレている！
- 暗号破られ②　方法が古くて解読可能！
- 暗号破られ③　呪文が簡単すぎて解読される

⊟ S2. 通信を守る、無線LANを安全に利用する

⊟ P1. それぞれの状況に合わせた暗号化の必要性

⊟ トピック：それぞれの状況に合わせた暗号化

- 通信の暗号化
- ファイルの暗号化

⊟ P2. 無線LAN通信(Wi-Fi)の構成要素

- トピック：暗号を使う無線LANの構成要素
- トピック：公衆無線LANが安全とは限らない
- トピック：「暗号キー」共有は接続しちゃダメ

- P3. 暗号化なしや、方式が安全ではないものは危険
- P4. 暗号化方式が安全でも「暗号キー」が漏れれば危険
- P5. 家庭内での安全な無線LANの設定（暗号化方式

⊟ P6. 家庭内での安全な無線LANの設定（その他

⊟ トピック：家庭でのWi-Fiの利用

- ①出荷時の管理者パスワード、「暗号キー」の変更
- ②「暗号キー」は家族のヒミツ
- ③ルータと機器の安全な運用

- P7. 公衆無線LAN の安全な利用
- P8. 個別の「暗号キー」を用いる方式の無線LAN

⊟ P9. 公衆無線LAN に関して新規に購入したスマホなどで行うこと

⊟ トピック：公衆無線LAN通信の表示の意味

- ①スマホやパソコンの画面から見た無線LAN暗号化
- ②詳細な区分けから見た無線LAN暗号化

- トピック：新しいスマホを購入したら…

- P10. 公衆無線LAN が安全ではない場合の利用方法
- P11. 自前の暗号化による盗聴対策

⊟ P12. まとめて暗号化するVPN、現状は過信できないが今後に期待

⊟ トピック：様々な場所から安全なアクセスを可能にするVPN新しいスマホを購入したら…

- ①詳細なVPNのイメージ
- ②簡単なVPNのイメージ

⊟ S3. ウェブを安全に利用する、暗号化で守る

Expand - Collapse

- P1. 無線LAN の暗号化とVPNの守備範囲
  - トピック：それぞれの暗号化の守備範囲
    - ①無線LANの暗号化
    - ②VPNによる暗号化
    - ③ウェブ、メールの暗号化
    - ④VPN＋ウェブメールの暗号化
- P2. 全ての通信と、その一部であるウェブの通信
- P3. httpsで始まる暗号化通信にはどんなものがあるか
- P4. より厳格な審査の「EVSSL証明書
- P5. 「EV-SSL証明書」を持つサイトを見分ける方法
- P6. 有効期限が切れた証明書は拒否する
- P7. 他にも証明書に関する警告が出るサイトは接続しない
- P8. ウェブサービスのログインは二段階認証などを使う
  - トピック：httpsの暗号化通信で情報を守る
    - 個人情報の入力は基本的には……
  - トピック：攻撃者が不正に取得した証明書に注意
  - トピック：証明書の内容をチェックする
- P9. 二段階認証を破る「中間者攻撃」
  - トピック：間に入ってなりすます中間者攻撃の例
    - ①中間者攻撃で二段階認証が破られる例
    - ②中間者攻撃で二段階認証が破られにくい例
  - トピック：ウェブを使ったサイバー攻撃の例
    - ①メール等による感染
    - ②水飲み場攻撃による感染
- P10. ウェブを使ったサイバー攻撃に対応する

S4. メールを安全に利用する、暗号化で守る

- P1. メールにおける暗号化
- P2. スパムメールの嵐と、メールの暗号化
- P3. 受信側も暗号化で保護
- P4. メールにおける暗号化の守備範囲
  - トピック：メールの送受信は暗号化されているか
    - メールソフトやアプリが暗号化（SSL）利用になっているか？
  - トピック：しかしSSLの通信は自分のサーバまで
  - トピック：暗号化している同じサービスを利用する
- P5. 暗号化から見たウェブメールの利用と、同一サービス内の暗号化
- P6. 怪しいメールとはなにか. . .

Expand - Collapse

- P7. マルウェア入りの添付ファイルに気をつける
  - トピック：ウェブメールの送受信は暗号化されているか
  - トピック：怪しいメールとはなにか
    - ①仕事のメールを装う
    - ② 銀行、カード会社、ECサイト、プロバイダ関係を装うメール
  - トピック：本当の仕事仲間のメールでも攻撃は来る
- P8. メールアドレスのウェブサービスなどからの流出
- P9. 流出・スパム対策としての、変更可能メールアドレスの利用
- P10. 通信の安全と永続性を考えたSNSやメールの利用
  - トピック：マルウェア入りファイルの偽装
  - トピック：メールアドレスを変えてスパムメールから逃げる

- S5. データファイルを守る、暗号化で守る
  - トピック：データの暗号化は保険
  - トピック：データを持ち運ぶときは必ず暗号化メディアを使う
  - トピック：「暗号キー」が1個の方式（共通鍵暗号方式）
  - トピック：「暗号キー」が2個の方式（公開鍵暗号方式）
  - コラム：クラウドサービスからのデータ流出。原因は？

- 第3 章 スマホ・パソコンのより進んだ使い方やトラブルの対処の仕方
  - 1. スマホのセキュリティ設定.. .
    - 1 スマホにはロックをかけよう。席において離れたり、人に貸したりするのは×
    - 2 情報漏れを防ぐ①
    - 3 情報漏れを防ぐ②
    - 4 スムーズな機種変更と、予期せぬデータ流出の防ぎ方
    - 5 防水機能を過信してデータを失わないように
    - コラム：GPS、位置情報、ジオタグの管理
  - 2. パソコンのセキュリティ設定..
    - 1 パソコンを買ったら初期設定などを確実に
    - 2 暗号化機能等でセキュリティレベルを高める
    - 3 マルウェア感染に備え、バックアップ体制を整える
    - 4 売却や廃棄するときはデータを消去する
    - 5 盗難や紛失のとき、スマホとパソコン、どっちが安全？
    - コラム：ダブルラインでトラブルに備える
  - 3. 屋外・海外でのネットワーク利用..
    - 1 一見なにもないように見えて、危険がいっぱい
    - 2 インターネットカフェの利用
  - 4. それでも攻撃を受けてしまったときの対処..

Expand - Collapse

- 1 兆候に気をつけて被害が出たら対処
- コラム：究極の防御手段「ネットにつながない」エアギャップ
  - 有線でも無線でも、つながっていないパソコンにはマルウェアは感染しない
  - しかし、USBメモリを介して感染することも
  - ネットに接続していなくても、少量のデータであれば盗める
  - オンラインで銀行口座が狙われるなら
  - インターネットバンキングを止めるという手も
- コラム：無料ということの意味は何か
  - 試食サービスのコストの例
  - 無料ウェブサービスの例
  - 無料の公衆無線LANサービスの例

第4章 被害に遭わないために、知らない間に加害者にならないために

1. 攻撃者に乗っ取られるとこんなことが起こる

- 1 被害に遭わない、そして加害者にならないために
- 2 盗まれた情報は犯罪に使われる
- 3 乗っ取られた機器はサイバー攻撃に使われる
- 4 IoTも乗っ取られる。知らずにマルウェアの拡散も…

2. サイバー関連でやってはいけないこと

- 1 アニメ・マンガ・音楽の違法なシェア。パクリなどの著作権侵害
- 2 ゲームの不正行為。恋人や家族でもプライバシーは守る
- 3 クラッキングはクールじゃない！
- コラム：モラルを逸脱すると炎上を生む
  - モラルを逸脱することが炎上を生む
  - 自作自演やアオリ行為、嘘の書き込み

第5 章 自分を守る、家族を守る、災害に備える

1. SNSやネットとのつきあい方、守り方

- 1 SNSやネットの楽しみと気をつけること
- 2 SNSやネットの怖さ、こんなことが実際に起こっている
  - 略取
  - ストーカー
  - 犯罪勧誘
  - ネットいじめ
  - リベンジポルノ・デジタルタトゥー
- 3 SNSやネットとのつきあい方の基本
  - 個人情報は基本的に公開しない
  - 会ったことがない人とむやみに友だちにならない
  - 現実世界で会おうとする人を警戒する。出会い系に近づかない

Expand - Collapse

- 個人が特定される情報はSNSなどに投稿しない
- 4 存在するデータは流出することがある。流出したら消すことは難しい
- コラム：SNSや学校裏サイトを使ったいじめに備える（いじめ経験者からのアドバイス）
- コラム：デマに踊らされない！　ソースを探せ！　確かめよう！

2. デジタルテクノロジーで家族を守る.. .

- 1 子ども達を守る
- 2 お年寄りを守る

3. 大災害やテロに備える..

- 1 まずは自分の身の安全を確保する
- 2 電池をもたす、情報収集をする
- 3 ラジオ、ワンセグを使った情報収集
- 4 徒歩帰宅。海外での災害やテロに備えて
- コラム：屋外でのゲームを安全に楽しむ
- 5 ネットを使わない移動トレーニング（現代オリエンテーリング）
- コラム：デジタル遺産相続

エピローグ 来たるべき新世界

- 1 ネットの「今」と、どう守っていくか
- 2 デジタルネイティブと未来
- 3 バーチャル空間を超えて世界へ
- 4 おわりに

- 用語集.

情報セキュリティ関連サイト一覧

- 情報セキュリティ関連のサイト
- 海外旅行関連のサイト
- 災害時関連のサイト
- 災害時関連のサイト
- いじめ対策関連
- Twitterアカウント
- アプリ（Android、iOS）
- その他

- 索引..

マンガで学ぶサイバーセキュリティ【NISC】【初心者向け】

スマートフォンのセキュリティ

注意点

- 最近ではパソコンだけでなく、スマートフォンでも悪意のあるウイルスが横行している

- ウイルス感染は「無料のアプリ」からが多い
- OSやアプリのバージョンが古いままだと、ウイルス感染の危険性あり

対策

- スマートフォンへのウイルス対策ソフトの導入を検討しよう
- アプリの詳細、提供企業やレビューを確認し、信頼できるサイトからアプリをダウンロードしよう
- OSやアプリは常に最新のバージョンにアップデートしよう

豆知識

- 最近ではマンガのような、画面をロックしてお金を要求するウイルス（ランサムウェアと呼ぶ）が流行している
- スマートフォンだけでなく、PCも被害が出ているので注意しよう
- 迷惑メールの添付ファイルを実行すると、ウイルスに感染してしまうこともあるため、注意しよう

無線LANのセキュリティ

注意点誰でも接続できる無線LANのアクセスポイントの中には、悪意をもって設置されているものがある

- 悪意をもって設置されたアクセスポイントに接続すると、通信内容を見られてしまうことがある
- インターネット接続業者が提供している公衆無線LANでも、通信が暗号化などで保護されていないものがあり、通信内容が傍受されるおそれがある

対策

- 不審な公衆Wi-Fiには接続しない
- 公衆Wi-Fiに接続する場合は、出来るだけ暗号化された、信頼できるWi-Fiを利用しよう

豆知識

- ファイル共有機能をONにして公衆Wi-Fiに接続すると、同じWi-Fiにつないでいる人からデータが見られてしまう
- 公衆Wi-Fiを使う場合は、設定に注意しよう
- 自宅のWi-Fiにはきちんとパスワードをかけ、知らない人が接続できないようにしよう

インターネット上の詐欺

注意点

- インターネット上には、ネットショッピングやインターネットバンキング等を利用する上で、お金に関する詐欺が存在する
- ユーザを巧妙な偽サイト（フィッシングサイト）に誘導して騙す手法も増加している
- 安易にjメールを信用してUrlや添付ファイルを開くと、偽物のサイトに飛んでしまったり、ウイルスに感染してしまうことがある

Expand - Collapse

- 対策
  - ウェブサイトのURLやメール所送付先が正規のものか、注意深く確認しよう
  - 言語がカタコトだったり。連絡先が書いていないなど、疑わしいサイトは利用しない
- 豆知識
  - フィッシングサイトでは銀行のウェブサイトを模倣して、インターネットバンキングのIDやパスワードを盗むものも多く存在するため、注意しよう。

- SNSの利用上の注意
  - 注意点
    - SNSでは、悪意のあるユーザが、女性などの画像を使用してなりすまし、接触を図ってくることがある
    - 悪意のあるユーザは「直接会おう」などと接近してくることもあり、犯罪に巻き込まれることもある
  - 対策
    - 見知らぬユーザとは、コンタクトをとらない
    - 「会おう」などと誘われても絶対に会わない
  - 豆知識
    - 見知らぬ人が接触してくるのは、悪事を目的としていることが多い
    - 見知らぬ人が写真や住所、電話番号など、個人情報を要求してくることもあるが、決して応じないこと
    - 知り合いに成りすまして接近してくることも有るので、知っている人だからと言って油断しない

- 基礎知識｜国民のための情報セキュリティサイト【総務省】
  - インターネットを使ったサービス｜基礎知識｜国民のための情報セキュリティサイト【総務省】
    - インターネットって何？
    - インターネットの仕組み
    - ホームページの仕組み
    - 電子メールの仕組み
    - ブログの仕組み
    - 電子掲示板の仕組み
    - SNS（ソーシャルネットワーキングサービス）の仕組み
    - チャットの仕組み
    - メーリングリストの仕組み
    - ショッピングサイトの仕組み
    - ネットオークションの仕組み
    - インターネットバンキングの仕組み
    - クラウドサービスとは？

Expand - Collapse

- スマートフォンとは？
- 無線LANの仕組み

- どんな危険があるの？｜基礎知識｜国民のための情報セキュリティサイト【総務省】
  - ウイルスとは？
  - ウイルスの感染経路と主な活動
    - ウイルスの感染経路
    - ウイルスの主な活動
  - 不正アクセスとは？
    - ホームページやファイルの改ざん
    - 他のシステムへの攻撃の踏み台に
  - 詐欺等の犯罪
  - 事故・障害
  - 脆弱性（ぜいじゃくせい）とは？
  - 情報発信に関するトラブル
- インターネットの安全な歩き方｜基礎知識｜国民のための情報セキュリティサイト【総務省】
  - IDとパスワード
    - 認証の仕組みと必要性
    - 設定と管理のあり方
  - ウイルスに感染しないために
  - 不正アクセスに遭わないために
  - 詐欺や犯罪に巻き込まれないために
  - 事故・障害への備え
  - 情報発信の心得
- 情報セキュリティ関連の技術｜基礎知識｜国民のための情報セキュリティサイト【総務省】
  - ファイアウォールの仕組み
  - 暗号化の仕組み
  - SSLの仕組み
  - ファイル共有ソフトとは？
- 情報セキュリティ関連の法律・ガイドライン｜基礎知識｜国民のための情報セキュリティサイト
  - 法律違反の事例
  - 刑法
  - サイバーセキュリティ基本法
  - 著作権法

Expand - Collapse

- 電気通信事業法
- 電子署名及び認証業務に関する法律
- 電子署名に係る地方公共団体の認証業務に関する法律
- 電波法
- 特定電子メールの送信の適正化等に関する法律
- 不正アクセス行為の禁止等に関する法律
- 有線電気通信法

一般利用者の対策｜国民のための情報セキュリティサイト【総務省】

基本的な対策

- ソフトウェアを最新に保とう

ウイルス対策をしよう

- ウイルス対策ソフト
- 記憶媒体からのウイルス感染

- ホームページ閲覧の危険性
- パスワードの設定と管理
- フィッシング詐欺に注意
- ワンクリック詐欺に注意
- 無線LANの安全な利用
- 機器の廃棄
- 個人に関する情報の取扱い
- プライバシー情報の取扱い
- サポート期間が終了するソフトウェアに注意
- サーバ証明書の切り替えによる影響について

インターネット上のサービス利用時の脅威と対策

【インターネット】

- ホームページ閲覧における注意点
- ネットオークションにおける危険性
- ショッピングサイトの利用
- インターネットバンキングの注意点
- SNS利用上の注意点
- クラウドサービス利用上の注意点
- 動画配信サイトなどの注意点
- オンラインゲームの注意点

【電子メール】

- ウイルス添付メールなどへの対応
- 迷惑メールへの対応
- チェーンメールの問題点
- メールの誤送信

Expand - Collapse

- 【情報機器】
  - 家族共用パソコンの注意点
  - 携帯電話・スマートフォン・タブレット端末の注意点
  - ゲーム機の注意点
  - インターネット対応機器（家電、記憶媒体等）の注意点
- 【その他】
  - ファイル共有ソフトの利用とその危険性

情報発信の際の注意

- 著作権侵害に注意
- 個人情報の公開の危険性
- ネットを使ったいやがらせや迷惑行為
- 発信内容は慎重に

事故・被害の事例

- 事例1：資料請求の情報が漏洩した
- 事例2：私の名前で誰かがメールを
- 事例3：ホームページを見ただけで・・・
- 事例4：猛威！デマウイルス
- 事例5：メールが他人に読まれている？
- 事例6：ネットストーカーに注意
- 事例7：ウイルス対策はしていたはずなのに・・・
- 事例8：送った覚えがないのに・・・
- 事例9：オークションの商品が届かない
- 事例10：メールの儲け話に注意
- 事例11：中古パソコンによるデータの漏洩
- 事例12：クレジットカード番号が盗まれた
- 事例13：ファイル共有ソフトが原因で・・・
- 事例14：ワンクリック詐欺に注意
- 事例15：自分の名前で勝手に書き込みが・・・
- 事例16：インターネットバンキングで情報が盗まれた
- 事例17：有名サイトからダウンロードしたはずなのに・・・
- 事例18：ブロードバンドルータから認証情報が盗まれた・・・