Sec01-02-53\_各種ガイドブックの内容要約\_一般ユーザ向け【零細企業を含む】【SK3】

ドキュメントを参照: [Sec01-02-50\_サイバーセキュリティ関連\_各種ガイドブックの内容要約.mmap](file:///D:\Cloud_Storage\OneDrive%20-%20ＮＰO知的資源イニシアティブ（ＩＲＩ）\git_repository_Duo\Sharing_Knowledge3\MindManager3\Sec01-02-50_サイバーセキュリティ関連_各種ガイドブックの内容要約.mmap)

1. 一般ユーザ向け【零細企業を含む】
2. 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】

ドキュメントを参照: [leaflet\_20150201.pdf](http://www.nisc.go.jp/security-site/files/leaflet_20150201.pdf)

* 1. OS やソフトウェアは常に最新の状態にしておこう
     1. 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。
  2. パスワードは貴重品のように管理しよう
     1. 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。
  3. ログインID・パスワード絶対教えない用心深さ
     1. 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。
  4. 身に覚えのない添付ファイルは開かない
     1. 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。
  5. ウイルス対策ソフトを導入しよう
     1. 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）
  6. ネットショッピングでは信頼できるお店を選ぼう
     1. 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。
  7. 大切な情報は失う前に複製しよう
     1. 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。
  8. 外出先では紛失・盗難に注意しよう
     1. 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て持ち歩きましょう。
  9. 困ったときはひとりで悩まず まず相談
     1. 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。

1. ネットの危険からお子様を守るために、 保護者ができる3つのポイント 【2017年4月6日政府広報】

ドキュメントを参照: [3.html](http://www.gov-online.go.jp/useful/article/201303/3.html)

* 1. 1.自分の携帯電話やスマートフォンを持つ子供が増えている

ドキュメントを参照: [3.html](http://www.gov-online.go.jp/useful/article/201303/3.html#section2)

* 1. 2.子供たちのインターネット利用に潜む危険

ドキュメントを参照: [3.html](http://www.gov-online.go.jp/useful/article/201303/3.html#section2)

* 1. 3.保護者ができる3つのポイント

ドキュメントを参照: [3.html](http://www.gov-online.go.jp/useful/article/201303/3.html#section3)

* 1. ポイント1　被害者にも加害者にもしないために、 適切なインターネットの利用を促しましょう

ドキュメントを参照: [3.html](http://www.gov-online.go.jp/useful/article/201303/3.html#point1)

* 1. ポイント2　家庭のルールをお子様と一緒に作り、 成長と共に少しずつ改定していきましょう

ドキュメントを参照: [3.html](http://www.gov-online.go.jp/useful/article/201303/3.html#point2)

* 1. ポイント3　不適切な情報や危険な出会い等を防ぐために、 フィルタリングを賢く利用しましょう

ドキュメントを参照: [3.html](http://www.gov-online.go.jp/useful/article/201303/3.html#point3)

* 1. 子供の携帯電話利用に関するトラブルの例

ドキュメントを参照: [3.html](http://www.gov-online.go.jp/useful/article/201303/3.html#column1)

* + 1. 総務省「インターネットトラブル事例集」

ドキュメントを参照: [jireishu.html](http://www.soumu.go.jp/main_sosiki/joho_tsusin/kyouiku_joho-ka/jireishu.html)

* 1. 関連リンク
     1. 内閣府「青少年有害環境対策（青少年のインターネット利用環境整備を含む）」

ドキュメントを参照: [index.html](http://www8.cao.go.jp/youth/youth-harm/index.html)

* + 1. 総務省「インターネットトラブル事例集」

ドキュメントを参照: [jireishu.html](http://www.soumu.go.jp/main_sosiki/joho_tsusin/kyouiku_joho-ka/jireishu.html)

* + 1. 総務省「国民のための情報セキュリティサイト」

ドキュメントを参照: [index.htm](http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/index.htm)

* + 1. 法務省「インターネットを悪用した人権侵害をなくしましょう」

ドキュメントを参照: [jinken88.html](http://www.moj.go.jp/JINKEN/jinken88.html)

1.  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Ver.2.11（小冊子） 【2017年02月08日NISC】

ドキュメントを参照: [index.html](https://www.nisc.go.jp/security-site/handbook/index.html)

* 1. 電子書籍【無料】【2017年７月13日】
     1. ibooksStore、 Kindle ストア、 ebookjapan、 BOOKFAN、 コミックシーモア、 d ブック、 ひかりTV ブック、 music.jp 、 DMM.com 、 Kinoppy 、 Yahoo! ブックストア、 GooglePlay ブックス、 GALAPAGOS STORE、 セブンネットショッピング、 honto、 漫画全巻ドットコム、 Dijital ehon、 ニコニコ静画、 cdjapan eBooks 、 Neowing eBooks 、 フジテレビオンデマンド、 BOOKWALKER、 BookLive!、 ブックパス、 ReaderStore、 BookPlace、 楽天Kobo
     2. https://www.amazon.co.jp/

ドキュメントを参照: [www.amazon.co.jp](https://www.amazon.co.jp/)

* 1. PDF版【2017年02月08日】
     1. 全体版（68.8MB）

ドキュメントを参照: [handbook-all.pdf](https://www.nisc.go.jp/security-site/files/handbook-all.pdf)

* + 1. 部分版（各章別）
    2. プロローグ　サイバー攻撃ってなに？（7.5MB）

ドキュメントを参照: [handbook-prologue.pdf](https://www.nisc.go.jp/security-site/files/handbook-prologue.pdf)

* + 1. 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ィを固めよう～（19.5MB）

ドキュメントを参照: [handbook-01.pdf](https://www.nisc.go.jp/security-site/files/handbook-01.pdf)

* + 1. 第2章　セキュリティを理解して、 ネットを安全に使う（7.0MB）

ドキュメントを参照: [handbook-02.pdf](https://www.nisc.go.jp/security-site/files/handbook-02.pdf)

* + 1. 第3章　スマホ・パソコンのより進んだ使い方やトラブル対処の仕方（13.0MB）

ドキュメントを参照: [handbook-03.pdf](https://www.nisc.go.jp/security-site/files/handbook-03.pdf)

* + 1. 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（6.3MB）

ドキュメントを参照: [handbook-04.pdf](https://www.nisc.go.jp/security-site/files/handbook-04.pdf)

* + 1. 第5章　自分を守る、 家族を守る、 災害に備える（12.8MB）

ドキュメントを参照: [handbook-05.pdf](https://www.nisc.go.jp/security-site/files/handbook-05.pdf)

* + 1. エピローグ　来たるべき新世界（4.6MB）

ドキュメントを参照: [handbook-epilogue.pdf](https://www.nisc.go.jp/security-site/files/handbook-epilogue.pdf)

* + 1. 用語集・情報セキュリティ関連サイト一覧・索引（2.1MB）

ドキュメントを参照: [handbook-glassary.pdf](https://www.nisc.go.jp/security-site/files/handbook-glassary.pdf)

* 1. 目次
     1. 人物紹介
     2. おうちのCSIRTになってね
     3. Black Hat the Cracker
  2. 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
     1. S1. サイバー攻撃のイメージ
        1. S1. サイバー攻撃って誰がやっているの？どうするの？
        2. コラム：攻撃者とハッカーとクラッカー
        3. コラム：攻撃者が使う武器「マルウェア」
           1. どんな種類があるの？
           2. どんな機能を持つの？
           3. 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
        4. S2. サイバー攻撃の例
           1. 偽サイトでのフィッシング詐欺や重要情報の不正送信
           2. ランサムウェアで身代金要求
           3. ボットネットに組み込まれる
        5. S3. サイバー関連の犯罪やトラブル
           1. なりすましや略取・誘拐（連れ去り）
           2. セクスティング
           3. ネットいじめ
        6. S4. 人の心の隙を突く「ソーシャルエンジニアリング」攻撃
           1. 「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
  3. 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ィを固めよう！
     1. S1. 4つのポイントでセキュリティを守る
        1. 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
           1. 様々な段階でセキュリティを守る
        2. 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
        3. 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
           1. 守りを何重にもして侵入されにくくする
        4. 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）
     2. S2. 環境を最新に保つ、 セキュリティソフトを導入する
        1. P1. セキュリティソフトを導入して守りを固めよう
           1. 単純なウイルス検知ソフト
           2. 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）
           3. 手配書が間に合わないゼロディ攻撃も
        2. P2. パソコン本体とセキュリティの状態を最新に保とう
           1. 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
        3. P3. スマートフォンやネットワーク機器も最新に保とう
           1. 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
           2. 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
        4. 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
           1. 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
        5. 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
           1. 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
           2. スマホの改造をしてはいけません
           3. スマート家電の中にはパソコンやスマホがある？
        6. 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！
           1. ゼロディ攻撃とは？ 対処の例
           2. ゼロディ攻撃に対抗するには？
     3. 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
        1. P1. パスワードの安全性を高める
           1. 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
        2. P2. パスワードの使い回しをしない
           1. 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ｘ
        3. P3. パスワードを適切に保管する
           1. パスワードを使用する場所に置かない。 パソコンの中もｘ
           2. 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
           3. ブラウザの自動入力にパスワードを覚えさせない
        4. 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
           1. 秘密の質問にはまじめに答えない。 答えは使い回さない
           2. 多要素認証やログイン通知でセキュリティを向上
        5. 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？
           1. 様々なID・パスワードの抜き取り方法
           2. 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
     4. 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
        1. 攻撃されにくくするには手間がかかるようにする
        2. 金銭目的ではない攻撃にも備えよう
        3. 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
     5. 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）
        1. 古典的なソーシャルエンジニアリング
        2. デジタル世代のソーシャルエンジニアリング
        3. 標的型メールの例
        4. フィッシングメールの例
        5. 悪意はないが拡散してしまう例
        6. コラム：軍事スパイ、 産業スパイに狙われてしまったら
           1. 職業スパイにはコストによる防御が効かない
           2. スパイ活動の今昔
        7. 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
        8. コラム：スパムメールとその由来
  4. 第2章セキュリティを理解して、 ネットを安全に使う
     1. S1. パスワードを守る、 パスワードで守る
        1. P1. パスワードってなに？
        2. P2. 3種類の「パスワード」を理解する
           1. 1を「PINコード」
           2. 2を「ログインパスワード」
           3. 3を「暗号キー」
        3. 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
        4. P4. 「暗号キー」に求められる複雑さ
        5. P5. どちらの「パスワード」か、 わかりにくい例
           1. トピック：パスワードを破る手段は色々

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）

* + - 1. 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
         1. 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

* + - * 1. トピック：指紋認証が破られることも
      1. 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
      2. P8. パスワード流出時の便乗攻撃に注意
      3. P9. 厳重なパスワードの保管
         1. トピック：ブラウザにはパスワード保存しない
         2. トピック：パスワード管理方法の例
         3. トピック：パスワード管理方法のメリットデメリット
      4. P10. パスワード情報をクラウドで利用する善し悪し
      5. P11. ノートやスマホを失くした場合のリカバリ考察
      6. 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
      7. P13. ソーシャルログインで連携される情報に注意
         1. 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

* + - * 1. 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

* + - * 1. トピック：アプリなどの連携は定期的に棚卸ししよう
      1. P14. ソーシャルログインとは性格が違うサービス連携
      2. コラム：暗号化の超簡単説明
         1. 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

* + - * 1. 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

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

* + 1. S2. 通信を守る、 無線LANを安全に利用する
       1. P1. それぞれの状況に合わせた暗号化の必要性
          1. 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

* + - 1. P2. 無線LAN通信(Wi-Fi)の構成要素
         1. トピック：暗号を使う無線LANの構成要素
         2. トピック：公衆無線LANが安全とは限らない
         3. トピック：「暗号キー」共有は接続しちゃダメ
      2. P3. 暗号化なしや、 方式が安全ではないものは危険
      3. P4. 暗号化方式が安全でも「暗号キー」が漏れれば危険
      4. P5. 家庭内での安全な無線LANの設定（暗号化方式
      5. P6. 家庭内での安全な無線LANの設定（その他
         1. 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

* + - 1. P7. 公衆無線LAN の安全な利用
      2. P8. 個別の「暗号キー」を用いる方式の無線LAN
      3. 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
         1. 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

* + - * 1. トピック：新しいスマホを購入したら
      1. P10. 公衆無線LAN が安全ではない場合の利用方法
      2. P11. 自前の暗号化による盗聴対策
      3. 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
         1. 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

* + 1. S3. ウェブを安全に利用する、 暗号化で守る
       1. P1. 無線LAN の暗号化とVPNの守備範囲
          1. 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

* + - 1. P2. 全ての通信と、 その一部であるウェブの通信
      2. P3. httpsで始まる暗号化通信にはどんなものがあるか
      3. P4. より厳格な審査の「EVSSL証明書
      4. P5. 「EV-SSL証明書」を持つサイトを見分ける方法
      5. P6. 有効期限が切れた証明書は拒否する
      6. 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
      7. P8. ウェブサービスのログインは二段階認証などを使う
         1. 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

* + - * 1. トピック：攻撃者が不正に取得した証明書に注意
        2. トピック：証明書の内容をチェックする
      1. P9. 二段階認証を破る「中間者攻撃」
         1. 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

* + - * 1. 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

* + - 1. P10. ウェブを使ったサイバー攻撃に対応する
    1. S4. メールを安全に利用する、 暗号化で守る
       1. P1. メールにおける暗号化
       2. P2. スパムメールの嵐と、 メールの暗号化
       3. P3. 受信側も暗号化で保護
       4. P4. メールにおける暗号化の守備範囲
          1. 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？

* + - * 1. トピック：しかしSSLの通信は自分のサーバまで
        2. トピック：暗号化している同じサービスを利用する
      1. 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
      2. P6. 怪しいメールとはなにか.. .
      3. P7. マルウェア入りの添付ファイルに気をつける
         1. トピック：ウェブメールの送受信は暗号化されているか
         2. 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

* + - * 1. トピック：本当の仕事仲間のメールでも攻撃は来る
      1. P8. メールアドレスのウェブサービスなどからの流出
      2. 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
      3. P10. 通信の安全と永続性を考えたSNSやメールの利用
         1. トピック：マルウェア入りファイルの偽装
         2. 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
    1. S5. データファイルを守る、 暗号化で守る
       1. トピック：データの暗号化は保険
       2. 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
       3. トピック：「暗号キー」が1個の方式（共通鍵暗号方式）
       4. トピック：「暗号キー」が2個の方式（公開鍵暗号方式）
       5. コラム：クラウドサービスからのデータ流出。 原因は？
  1. 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. 1. スマホのセキュリティ設定.. .
        1. 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ｘ
        2. 2 情報漏れを防ぐ①
        3. 3 情報漏れを防ぐ②
        4. 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. 5 防水機能を過信してデータを失わないように
        6. コラム：GPS、 位置情報、 ジオタグの管理
     2. 2. パソコンのセキュリティ設定..
        1. 1 パソコンを買ったら初期設定などを確実に
        2. 2 暗号化機能等でセキュリティレベルを高める
        3. 3 マルウェア感染に備え、 バックアップ体制を整える
        4. 4 売却や廃棄するときはデータを消去する
        5. 5 盗難や紛失のとき、 スマホとパソコン、 どっちが安全？
        6. コラム：ダブルラインでトラブルに備える
     3. 3. 屋外・海外でのネットワーク利用..
        1. 1 一見なにもないように見えて、 危険がいっぱい
        2. 2 インターネットカフェの利用
     4. 4. それでも攻撃を受けてしまったときの対処..
        1. 1 兆候に気をつけて被害が出たら対処
        2. 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
           1. 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
           2. しかし、 USBメモリを介して感染することも
           3. 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
           4. オンラインで銀行口座が狙われるなら
           5. インターネットバンキングを止めるという手も
        3. コラム：無料ということの意味は何か
           1. 試食サービスのコストの例
           2. 無料ウェブサービスの例
           3. 無料の公衆無線LANサービスの例
  2. 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. 1. 攻撃者に乗っ取られるとこんなことが起こる
        1. 1 被害に遭わない、 そして加害者にならないために
        2. 2 盗まれた情報は犯罪に使われる
        3. 3 乗っ取られた機器はサイバー攻撃に使われる
        4. 4 IoTも乗っ取られる。 知らずにマルウェアの拡散も
     2. 2. サイバー関連でやってはいけないこと
        1. 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. 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. 3 クラッキングはクールじゃない！
        4. コラム：モラルを逸脱すると炎上を生む
           1. モラルを逸脱することが炎上を生む
           2. 自作自演やアオリ行為、 嘘の書き込み
  3. 第5 章 自分を守る、 家族を守る、 災害に備える
     1. 1. SNSやネットとのつきあい方、 守り方
        1. 1 SNSやネットの楽しみと気をつけること
        2. 2 SNSやネットの怖さ、 こんなことが実際に起こっている
           1. 略取
           2. ストーカー
           3. 犯罪勧誘
           4. ネットいじめ
           5. リベンジポルノ・デジタルタトゥー
        3. 3 SNSやネットとのつきあい方の基本
           1. 個人情報は基本的に公開しない
           2. 会ったことがない人とむやみに友だちにならない
           3. 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
           4. 個人が特定される情報はSNSなどに投稿しない
        4. 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
        5. 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）
        6. コラム：デマに踊らされない！　ソースを探せ！　確かめよう！
     2. 2. デジタルテクノロジーで家族を守る.. .
        1. 1 子ども達を守る
        2. 2 お年寄りを守る
     3. 3. 大災害やテロに備える..
        1. 1 まずは自分の身の安全を確保する
        2. 2 電池をもたす、 情報収集をする
        3. 3 ラジオ、 ワンセグを使った情報収集
        4. 4 徒歩帰宅。 海外での災害やテロに備えて
        5. コラム：屋外でのゲームを安全に楽しむ
        6. 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）
        7. コラム：デジタル遺産相続
  4. エピローグ 来たるべき新世界
     1. 1 ネットの「今」と、 どう守っていくか
     2. 2 デジタルネイティブと未来
     3. 3 バーチャル空間を超えて世界へ
     4. 4 おわりに
  5. 用語集.
  6. 情報セキュリティ関連サイト一覧
     1. 情報セキュリティ関連のサイト
     2. 海外旅行関連のサイト
     3. 災害時関連のサイト
     4. 災害時関連のサイト
     5. いじめ対策関連
     6. Twitterアカウント
     7. アプリ（Android、 iOS）
     8. その他
  7. 索引..

1. マンガで学ぶサイバーセキュリティ【NISC】【初心者向け】

ドキュメントを参照: [CSmanga\_JPN.pdf](http://www.nisc.go.jp/security-site/files/CSmanga_JPN.pdf)

* 1. スマートフォンのセキュリティ
     1. 注意点
        1. 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
        2. ウイルス感染は「無料のアプリ」からが多い
        3. 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
     2. 対策
        1. 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
        2. 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
        3. 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
     3. 豆知識
        1. 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
        2. 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
        3. 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
  2. 無線LANのセキュリティ
     1. 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
        1. 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
        2. 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
     2. 対策
        1. 不審な公衆Wi-Fiには接続しない
        2. 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
     3. 豆知識
        1. 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
        2. 公衆Wi-Fiを使う場合は、 設定に注意しよう
        3. 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
  3. インターネット上の詐欺
     1. 注意点
        1. 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
        2. 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
        3. 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
     2. 対策
        1. 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
        2. 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
     3. 豆知識
        1. 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。
  4. SNSの利用上の注意
     1. 注意点
        1. 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
        2. 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
     2. 対策
        1. 見知らぬユーザとは、 コンタクトをとらない
        2. 「会おう」などと誘われても絶対に会わない
     3. 豆知識
        1. 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
        2. 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
        3. 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

1. IPA 対策のしおり【IPA】

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

* 1. IPA対策のしおりシリーズ
     1. ウイルス対策のしおり（第10版）PDF（815KB）

ドキュメントを参照: [01\_virus.pdf](https://www.ipa.go.jp/security/antivirus/documents/01_virus.pdf)

* + 1. スパイウェア対策のしおり（第10版）PDF（822KB）

ドキュメントを参照: [02\_spyware.pdf](https://www.ipa.go.jp/security/antivirus/documents/02_spyware.pdf)

* + 1. ボット対策のしおり（第10版）PDF（1.0MB）

ドキュメントを参照: [03\_bot.pdf](https://www.ipa.go.jp/security/antivirus/documents/03_bot.pdf)

* + 1. 不正アクセス対策のしおり（第6版）PDF（779KB）

ドキュメントを参照: [04\_fusei.pdf](https://www.ipa.go.jp/security/antivirus/documents/04_fusei.pdf)

* + 1. 情報漏えい対策のしおり（第7版）PDF（795KB）

ドキュメントを参照: [05\_roei.pdf](https://www.ipa.go.jp/security/antivirus/documents/05_roei.pdf)

* + 1. インターネット利用時の危険対策のしおり（第4版）

ドキュメントを参照: [06\_kiken.pdf](https://www.ipa.go.jp/security/antivirus/documents/06_kiken.pdf)

* + 1. 電子メール利用時の危険対策のしおり（第4版）PDF（1.1MB）

ドキュメントを参照: [07\_mail.pdf](https://www.ipa.go.jp/security/antivirus/documents/07_mail.pdf)

* + 1. スマートフォンのセキュリティ<危険回避>対策のしおり

ドキュメントを参照: [08\_smartphone.pdf](https://www.ipa.go.jp/security/antivirus/documents/08_smartphone.pdf)

* + 1. 初めての情報セキュリティ対策のしおり（第1版）

ドキュメントを参照: [09\_hazimete.pdf](https://www.ipa.go.jp/security/antivirus/documents/09_hazimete.pdf)

* + - 1. スライド版PDF（2.4MB）

ドキュメントを参照: [09\_hazimete\_slide.pdf](https://www.ipa.go.jp/security/antivirus/documents/09_hazimete_slide.pdf)

* + 1. 標的型攻撃メール<危険回避>対策のしおり（第1版）PDF

ドキュメントを参照: [10\_apt.pdf](https://www.ipa.go.jp/security/antivirus/documents/10_apt.pdf)

* + 1. 無線LAN<危険回避>対策のしおり（第1版）

ドキュメントを参照: [11\_wireless\_lan.pdf](https://www.ipa.go.jp/security/antivirus/documents/11_wireless_lan.pdf)

* + 1. 暗号化による<情報漏えい>対策のしおり（第1版）

ドキュメントを参照: [12\_crypt.pdf](https://www.ipa.go.jp/security/antivirus/documents/12_crypt.pdf)

* 1. IPAセキュリティマネジメントのしおりシリーズ
     1. 企業（組織）における最低限の情報セキュリティ対策のしおり+1PDF

ドキュメントを参照: [01\_guidebook.pdf](https://www.ipa.go.jp/security/keihatsu/shiori/management/01_guidebook.pdf)

* + 1. 「新5分でできる情報セキュリティ自社診断シート」

ドキュメントを参照: [5minutes.html](https://www.ipa.go.jp/security/keihatsu/sme/guideline/5minutes.html)

* + 1. 中小企業における組織的な情報セキュリティ対策ガイドライン チェック項目

ドキュメントを参照: [02\_checklist.pdf](https://www.ipa.go.jp/security/keihatsu/shiori/management/02_checklist.pdf)

* + 1. 中小企業における組織的な情報セキュリティ対策ガイドライン事例集

ドキュメントを参照: [03\_casestudy.pdf](https://www.ipa.go.jp/security/keihatsu/shiori/management/03_casestudy.pdf)

* + 1. 情報セキュリティ対策ベンチマーク（企業・組織のためのセキュリティ対策自己診断ツール Ver.4.x）

ドキュメントを参照: [04\_benchmark.pdf](https://www.ipa.go.jp/security/keihatsu/shiori/management/04_benchmark.pdf)

* 1. 姉妹冊子
     1. クラウドサービス安全利用のすすめPDF（2.5MB）

ドキュメントを参照: [cloud\_tebiki\_handbook\_V1.pdf](https://www.ipa.go.jp/security/cloud/cloud_tebiki_handbook_V1.pdf)

* + 1. 情報漏えい発生時の対応ポイント集PDF （0.8MB）

ドキュメントを参照: [rouei\_taiou.pdf](https://www.ipa.go.jp/security/awareness/johorouei/rouei_taiou.pdf)

1. 「やられたかな？その前に」【2015年10月14日 ISOG-J】

ドキュメントを参照: [Yararetakana-Guide-20151014.pdf](http://isog-j.org/output/2015/Yararetakana-Guide-20151014.pdf)

* 1. 概要
     1. 従業員数や端末数
        1. どの程度の台数が存在し、 調査が必要か概要を確認する。
     2. 問 1～5
        1. 相談の経緯について
           1. 現在の被害の有無や外部からの指摘といった状況についてのヒヤリングとなる。
           2. 相談の際に被害はまだないのだが不安がある場合は不安な箇所がどこかといったところからのヒヤリングとなる。
     3. 問 6～10
        1. 症状の詳細について
           1. 主にシステム管理を行っている方への質問となる。
           2. 既に何か症状がある場合、 どのような症状があるかの確認となる。
           3. わからない場合は「□わからない」を選択頂きたい。
           4. 症状はシステム利用者に聞くことや、 主観での回答でも良い。 調査を開始する際に、 ネットワーク、 サーバ、 パソコンや端末、 ログや心当たりをヒヤリングしておくことで、 どこから着手するかの手がかりとなる。
     4. 問 11～14
        1. 現在の管理状況について
           1. 主にシステム管理を行っている方への質問となる。
           2. 調査に必要な現状把握の設問である。 ネットワークやシステムに関連した社内文書の有無や、 調査の対象となるログについて確認する。
           3. 調査の中心がログの分析となる場合、 社内のどこに何があるかがはっきりしていると、 分析の手がかりとなる。
           4. 分析作業のために、 ログの保管場所や保存期間を把握する必要がある。
           5. IT 関連をいつもお願いしている事業者や関連業者があれば記載をお願いしたい。
           6. 普段からのどの程度のセキュリティの対策を行っているかなどの把握が調査の手助けとなる。
     5. 問 15～19
        1. 社内の組織体制について
           1. 主に事案や事件の対応者や責任者の方向けの質問となる。
           2. 明確に組織が存在しない場合は、 システム管理者の方の回答でも良い。
           3. 今後の相談や調査、 社内の対応に向けての確認となる。
           4. 調査や分析では、 お客様の協力が必要不可欠である。
           5. 業者との窓口という意味だけではなく、 調査や分析に当たって、 社内の手続きを含めてどういった手順で進めることができるかを事前に把握する。
     6. 問 20～22
        1. IPA 10 大脅威 2017の基本対策
           1. 主に事案や事件の対応者や責任者の方向けの質問となる。
           2. 明確に組織が存在しない場合は、 システム管理者の方の回答でも良い。
           3. セキュリティの基本対策がどの程度実施されているか確認する。
           4. 対策の内容によって調査や分析の手助けになる部分があるかの確認となる。
           5. 各項目の詳細な内容については「10 大脅威 2017」を確認されたい。
  2. 問診票

ドキュメントを参照: [Yararetakana-Guide-CheckList-20151014.docx](http://isog-j.org/output/2015/Yararetakana-Guide-CheckList-20151014.docx)

* + 1. 問合せ者
       1. 会社名：
       2. 従業員数（　　　　　　）人、 　端末数（　　　　　）台、 　拠点数（　　　　　）箇所
    2. 相談のきっかけや経緯について伺います。
       1. 問1：外部から通報や連絡がありましたか？
          1. 例：情報が漏えいしている、 改ざんされている、 パソコンがおかしくなった、 など
          2. □はい　（連絡元と、 連絡の内容：　　　　　　　　　　　　　　　　）　□いいえ
       2. 問2：過去にサイバー攻撃と思われる被害を受けたことはありますか？
          1. □はい　（被害の状況：　　　　　　　　　　　　　　　　　　　　　）　□いいえ
       3. 問3：相談しようとするまでに、 何か対処はしましたか？
          1. □はい　（時系列でお答えください：　　　　　　　　　　　　　　　）　□いいえ
       4. 問4：現在どのような不安がありますか？（複数回答可）
          1. □公開しているサーバへの攻撃がある　□パソコンがウイルスに感染している
          2. □内部から情報が漏えいしている　□その他（　　　　　　　　　　）
       5. 問5：相談のきっかけや経緯についてできるだけ具体的にお書きください
    3. 主にシステム管理者の方に、 現在の症状についてより詳細に伺います
       1. 問6：ネットワークが繋がりにくい・使えない
          1. □はい　 ・いつごろからですか？　（　　　　　　　　　　　　　　　　　　　） ・頻度はどの程度ですか？（1回だけ・数回・決まった時間・決まった曜日） ・どのような時に症状を感じますか？　（　　　　　　　　　　　　　）
          2. □いいえ　□わからない
       2. 問7：サーバの反応が悪い・反応がなくなる
          1. □はい　 ・いつごろからですか？　（　　　　　　　　　　　　　　　　　　　） ・頻度はどの程度ですか？（1回だけ・数回・決まった時間・決まった曜日） ・どのようなサーバですか？　（　　　　　　　　　　　　　　　　　）
          2. □いいえ　□わからない
       3. 問8：PC・携帯端末の反応が悪い・動かなくなる
          1. □はい　 ・いつごろからですか？　（　　　　　　　　　　　　　　　　　　） ・頻度はどの程度ですか？（1回だけ・数回・決まった時間・決まった曜日） ・どのような端末ですか？　（　　　　　　　　　　　　　　　　　） ・何台で起こっていますか？　（　　　　　　　　　　　　　　　　）
          2. □いいえ　□わからない
       4. 問9：不正な通信、 アクセスの形跡がある・気になるログがある
          1. □はい　　 ・いつごろからですか？　（　　　　　　　　　　　　　　　　　　） ・どのような内容、 不審点がありますか？　（　　　　　　　　　　）
          2. □いいえ　□わからない
       5. 問10：症状が始まった頃に、 下記のような出来事がありましたか？
          1. □はい　　 ・システム変更を行った / 新しいソフトを導入した ・怪しいサイトやメールにアクセスした ・情報記録媒体を紛失した ・その他不安なこと（　　　　　　　　　　　　　　　　　　　　　）
          2. □いいえ　□わからない
    4. 主にシステム管理を行っている方に、 管理状況について伺います
       1. 問11：情報機器や情報資産、 ネットワークの構成について把握されていますか？
          1. □はい　□いいえ　□わからない
       2. 問12：ネットワークやシステムのログを取得していますか？
          1. □はい　□いいえ　□わからない
       3. （問12が「はい」の方にお聞きします） 問13：ログの保存期間は決めていますか？
          1. □はい　（期間：　　　　　　　　　　　　　　）　□いいえ　□わからない
       4. 問14：普段から付き合いのあるセキュリティ事業者やITサービス事業者はいますか？
          1. □はい　（会社名：　　　　　）※複数社あれば複数社お答え下さい
          2. □いいえ　□わからない
    5. 主に事案や事件の対応者や責任者の方に、 社内の組織体制についてお聞きします
       1. 問15：事案や事件の窓口担当者は決めていますか？
          1. □はい　□いいえ
       2. 問16：相談について事案や事件対応責任者の了解を得ていますか？
          1. □はい　□いいえ
       3. 問17：事案や事件の上位職への相談や報告をする順序は決まっていますか？
          1. □はい　□いいえ　□わからない
       4. 問18：既にどこかへ報告しましたか？
          1. □はい（責任者、 経営陣、 関係者（監督官庁、 取引先、 顧客））　□いいえ
       5. 問19：社内での調査や対処をする権限を持つ責任者や担当者がいますか？
          1. □はい　□いいえ　□わからない
    6. 主に事案や事件の対応者や責任者の方に、 IPA 「10大脅威 2017」で示された「セキュリティ対策の基本」をどの程度実施しているかの確認です。
       1. 問20：「対策の前に」はどの程度実施していますか？（複数回答可）
          1. □守りたい情報資産の把握
          2. （情報資産とその場所： 　　　　　　　　　　　　　　　　　　　　　　　　　）
          3. □自発的なセキュリティ対策への取り組み
          4. □計画を策定し、 必要な予算の確保
       2. 問21： 現在行っているセキュリティ対策はどのようなものですか？（複数回答可）
          1. □利用しているソフトウェアを更新・最新のものに（OSやアプリケーションなど）
          2. □セキュリティソフト（ウイルス対策ソフトなど）の導入
          3. □パスワードの適切な管理と認証の強化（多要素認証など）
          4. □ソフトウェアや機器の設定を見直す（サーバ・ネットワーク設定の管理）
          5. □ソフトウェアや機器の脆弱性や犯罪への対策などの情報収集
       3. 問22：その他に実施している対策はありますか？（複数回答可）
          1. □文書による実施すべき対策の明文化　　□システムによる制限や強制
          2. □バックアップやシステムの冗長化　　□検査や監査
          3. □認証の取得（プライバシーマークやISO/IEC27001 など）
          4. □その他（　　　　　　　　　　　　　　　　　　　　　　　　　　　　　）

1. 2017年度版「撃退！迷惑メール」迷惑メール対策BOOK【迷惑メール相談センター】

ドキュメントを参照: [gmeiwaku\_book.pdf](https://www.dekyo.or.jp/soudan/data/info/gmeiwaku_book.pdf)

* 1. ☆1　こんなメールに気をつけよう
     1. 1.メールde詐欺
     2. 2.架空請求メール
     3. 3.銀行を装ったメール
     4. 4.芸能人を装ったメール
     5. 5.不正アプリをインストールさせようとするメール
     6. 6.懸賞金当選メール
     7. 7.宅配便の不在通知を装ったメール
     8. 8.ウイルスメール
     9. 9.チェーンメール
  2. ☆2　迷惑メールをブロックしよう
     1. 1.どうやって設定するの？
     2. 2.スマートフォンのおすすめ設定
     3. 3.ケータイのおすすめ設定
     4. 4.パソコンで設定する時は？
  3. ☆3　迷惑メールを予防しよう
     1. 1.迷惑メールの受信にはきっかけがあります
     2. 2.アドレスを使い分けよう
     3. 3.覚えておきたい迷惑メールへの対処法
  4. ☆4　スマートフォンのセキュリティ
     1. 1.スマートフォンに必須！セキュリティ対策
     2. 2.狙われるスマートフォンの個人情報
     3. 3.不正アプリインストールや個人情報流出を防ぐ
  5. ☆5　子どものスマートフォン利用案内
     1. 1.子どもの安全なスマートフォン利用のために
     2. 2.スマートフォンを持たせる前にまず確認してください
     3. 3.家庭でスマホ利用のルールを作る
     4. 4.フィルタリングを設定する
     5. 5.有害サイトから守る
     6. 6.有害アプリから守る
     7. 7.こんな時どうする？保護者のお悩みにお答えします
  6. ☆6　迷惑メールでお困りの方へ
     1. 1.迷惑メールは法律違反
     2. 2.情報提供のお願い
     3. 3.トラブル別相談窓口
     4. 4.用語解説
     5. 5.迷惑メール相談センターのご案内
  7. ☆7　おまけ
     1. 1.ぼくたち、 サギかもファミリーです
     2. 2.ヒヤリ・ハット体験SONGができました