**サイバーセキュリティ対策相談対応の手引き（メモ）**

2016年6月16日

中山正樹

目次

[**サイバーセキュリティ対策相談対応の手引き（メモ）** 1](#_Toc453840711)

[1. 問合せ事例 6](#_Toc453840712)

[1.1. 東京都中小企業サイバーセキュリティ相談Webフォーム 7](#_Toc453840713)

[1.2. セキュリティ侵害の実態 8](#_Toc453840714)

[1.3. 中小企業の現状から 8](#_Toc453840715)

[1.3.1. 情報セキュリティ対策の必要性を認識していない 8](#_Toc453840716)

[1.3.2. システムをベンダーに任せて開発もしくは導入、運用している 9](#_Toc453840717)

[1.3.3. 効果的な情報セキュリティ対策の方法がわからない 9](#_Toc453840718)

[1.4. 経済的損失⇒社会的信用の喪失、組織存立の危機 9](#_Toc453840719)

[1.4.1. ネットバンキングのセキュリティ対策 9](#_Toc453840720)

[1.5. OS コマンドインジェクション・SQLインジェクション等の防止 10](#_Toc453840721)

[1.6. インシデント発生 11](#_Toc453840722)

[1.6.1. ネットワークに繋がりにくい、サーバの反応が悪い 11](#_Toc453840723)

[1.6.2. PCの調子が悪い 11](#_Toc453840724)

[1.6.3. ウイルスに感染したみたい 11](#_Toc453840725)

[1.6.4. ランサムウェアを使った詐欺・恐喝 12](#_Toc453840726)

[1.7. システム運用管理をしている客のシステムが、ランサムウェアに感染して、ファイルが読めなくなった 13](#_Toc453840727)

[1.8. 水飲み場攻撃とは 13](#_Toc453840728)

[1.9. 標的型メール攻撃とは 13](#_Toc453840729)

[1.10. 偽サイトを開設された 14](#_Toc453840730)

[1.11. 偽サイトにアクセスしてしまった 14](#_Toc453840731)

[1.12. スマホ等のセキュリティ対策は？ 14](#_Toc453840732)

[2. 脆弱性情報の届出 16](#_Toc453840733)

[3. サイバーセキュリティとは 16](#_Toc453840734)

[4. 情報セキュリティに関する基礎知識 17](#_Toc453840735)

[4.1. 情報セキュリティ 10 大脅威（個人） 17](#_Toc453840736)

[4.1.1. 【一覧】情報セキュリティ 10 大脅威（個人） 17](#_Toc453840737)

[4.1.2. 【一覧】情報セキュリティ 10 大脅威（組織） 17](#_Toc453840738)

[4.1.3. 情報セキュリティ対策の基本 18](#_Toc453840739)

[4.1.4. 【対策】情報セキュリティ 10 大脅威（個人） 18](#_Toc453840740)

[4.1.5. 【対策】情報セキュリティ 10 大脅威（組織） 19](#_Toc453840741)

[4.1.6. 【対策】注目すべき脅威や懸念 22](#_Toc453840742)

[5. サービス提供と情報セキュリティ対策 23](#_Toc453840743)

[6. 事業継続計画（BCP）とセキュリティインシデント対応 24](#_Toc453840744)

[6.1. BCPとは 24](#_Toc453840745)

[6.2. BCPはなぜ必要か？ 24](#_Toc453840746)

[6.3. 何のためにBCPを策定するのか？ 25](#_Toc453840747)

[6.4. セキュリティインシデント対応はBCPの１つ 25](#_Toc453840748)

[7. 対策の概念 26](#_Toc453840749)

[7.1. リスクの要因 26](#_Toc453840750)

[7.2. 情報セキュリティにおけるさまざまな対策 26](#_Toc453840751)

[7.3. 情報セキュリティ対策の意義（参照：NDL） 27](#_Toc453840752)

[7.4. 情報セキュリティ対策のポイント（私見） 27](#_Toc453840753)

[8. 情報セキュリティポリシー、実施手順 29](#_Toc453840754)

[8.1. 情報セキュリティポリシーの構成 29](#_Toc453840755)

[8.2. 情報セキュリティポリシー（基本方針） 29](#_Toc453840756)

[8.3. 情報セキュリティポリシー（対策基準） 30](#_Toc453840757)

[8.4. 情報セキュリティ実施手順 30](#_Toc453840758)

[8.5. 情報セキュリティマネジメントシステム（ISMS）構築手順 31](#_Toc453840759)

[8.6. ISMSとPDCAサイクル 31](#_Toc453840760)

[8.7. 脅威・対策・脆弱性・リスクの関係 31](#_Toc453840761)

[8.8. 情報セキュリティマネジメントの規格や標準 33](#_Toc453840762)

[8.8.1. 情報セキュリティマネジメントの実践のための規範JIS Q 27002:2006 33](#_Toc453840763)

[8.8.2. 情報セキュリティマネジメントシステム - 要求事項JIS Q 27001:2006 33](#_Toc453840764)

[8.9. リスクマネジメント 34](#_Toc453840765)

[8.9.1. 情報資産の格付け 34](#_Toc453840766)

[8.9.2. ITセキュリティマネジメントのための手法（JIS TR X 0036-3:2001） 35](#_Toc453840767)

[9. 「情報セキュリティ管理基準（平成20年改正版）」 36](#_Toc453840768)

[9.1. 構成 36](#_Toc453840769)

[9.2. マネジメント基準 36](#_Toc453840770)

[9.3. 「管理策基準」 38](#_Toc453840771)

[10. 「政府機関の情報セキュリティ対策のための統一基準群（平成26年度版）」 40](#_Toc453840772)

[10.1. 41](#_Toc453840773)

[11. 人材育成 41](#_Toc453840774)

[11.1. ITパスポート試験シラバス 41](#_Toc453840775)

[11.2. まとめ）企業の情報セキュリティ対策と人材面の対策 42](#_Toc453840776)

[11.3. 情報処理技術者試験　情報セキュリティ人材育成の取り組み 43](#_Toc453840777)

[11.4. 情報セキュリティマネジメント試験　シラバス 43](#_Toc453840778)

[11.5. 情報セキュリティマネジメントタスクプロフィール 44](#_Toc453840779)

[11.6. 情報セキュリティ人材の職種 44](#_Toc453840780)

[12. 個人情報保護 45](#_Toc453840781)

[13. サイバーセキュリティ相談窓口の業務 46](#_Toc453840782)

[13.1. 中小企業に特化した情報セキュリティ対策の相談対応方針 46](#_Toc453840783)

[13.1.1. 中小企業の現状 46](#_Toc453840784)

[13.1.2. 中小企業への支援 47](#_Toc453840785)

[13.1.3. 相談対応フロー 48](#_Toc453840786)

[14. 情報セキュリティ関連法規 51](#_Toc453840787)

[14.1. サイバーセキュリティ基本法 51](#_Toc453840788)

[14.2. 不正アクセス禁止法 51](#_Toc453840789)

[14.3. 個人情報保護法 51](#_Toc453840790)

[14.4. 刑法 51](#_Toc453840791)

[14.5. その他のセキュリティ関連法規 51](#_Toc453840792)

[14.6. 知的財産権 51](#_Toc453840793)

[14.7. 労働関連・取引関連法規 51](#_Toc453840794)

[14.8. その他の法律・ガイドライン・技術者倫理 52](#_Toc453840795)

[14.9. 知的財産計画2016 52](#_Toc453840796)

[15. ここからセキュリティ！ 情報セキュリティ・ポータルサイト（IPA）【相談事例集作成候補】 53](#_Toc453840797)

[15.1. ここからセキュリティ！ 情報セキュリティ・ポータルサイト 53](#_Toc453840798)

[15.2. トップページ 53](#_Toc453840799)

[15.3. 被害にあったら 54](#_Toc453840800)

[15.3.1. ウイルス（マルウェア）に感染したら 54](#_Toc453840801)

[15.3.2. 不正アクセス（サーバーが攻撃された・ウェブページを書き換えられた） 55](#_Toc453840802)

[15.3.3. 情報漏えい（情報の紛失・流失・盗難） 56](#_Toc453840803)

[15.3.4. ワンクリック請求（料金画面が消えない・料金請求された） 56](#_Toc453840804)

[15.3.5. 迷惑メール（スパムメール） 57](#_Toc453840805)

[15.3.6. フィッシング詐欺・なりすまし（銀行やカード会社を騙るメール・送信元のアドレスを偽るメール） 57](#_Toc453840806)

[15.4. 対策する 58](#_Toc453840807)

[15.4.1. 対策の基本（まずはここから！） 58](#_Toc453840808)

[15.4.2. ウイルス対策 64](#_Toc453840809)

[15.4.3. 不正アクセス対策 65](#_Toc453840810)

[15.4.4. 情報漏えい 65](#_Toc453840811)

[15.4.5. ワンクリック請求（料金画面が消えない・料金請求された）【LEVEL1】【詳細】 67](#_Toc453840812)

[15.4.6. パスワード 67](#_Toc453840813)

[15.4.7. フィッシング詐欺・なりすまし 69](#_Toc453840814)

[15.4.8. 標的型攻撃メール 71](#_Toc453840815)

[15.4.9. 迷惑メール 73](#_Toc453840816)

[15.4.10. ガイドライン等 74](#_Toc453840817)

[15.5. 教育・学習 81](#_Toc453840818)

[15.5.1. 一般向け 81](#_Toc453840819)

[15.5.2. ホームユーザ向け 85](#_Toc453840820)

[15.5.3. 中小企業向け・より大きな企業・組織向け 91](#_Toc453840821)

[15.5.4. OSのアップデート（サポート終了関連情報を含む） 101](#_Toc453840822)

[15.6. セキュリティチェック 102](#_Toc453840823)

[15.6.1. クイズに挑戦 102](#_Toc453840824)

[15.6.2. 安全性を診断しよう 103](#_Toc453840825)

[15.6.3. 試験・資格 104](#_Toc453840826)

[15.7. データ＆レポート 104](#_Toc453840827)

[15.8. （情報セキュリティ　FAQ） 106](#_Toc453840828)

[16. 参考サイト 107](#_Toc453840829)

[16.1. 中小企業経営者向け 107](#_Toc453840830)

[16.2. IoT開発におけるセキュリティ設計の手引き 107](#_Toc453840831)

[16.3. 内閣サイバーセキュリティセンター（NISC） 108](#_Toc453840832)

[16.3.1. 高度情報通信ネットワーク社会推進戦略本部（IT総合戦略本部） 109](#_Toc453840833)

[16.3.2. 国家安全保障会議 109](#_Toc453840834)

[16.3.3. 警察庁 109](#_Toc453840835)

[16.3.4. 総務省 109](#_Toc453840836)

[16.3.5. 外務省 109](#_Toc453840837)

[16.3.6. 経済産業省 109](#_Toc453840838)

[16.3.7. JPCERTコーディネーションセンター 110](#_Toc453840839)

[16.3.8. 防衛省 111](#_Toc453840840)

[16.4. 東京都 111](#_Toc453840841)

[16.5. 警視庁 111](#_Toc453840842)

[16.6. 中小企業庁 111](#_Toc453840843)

[16.7. IPA 112](#_Toc453840844)

[16.7.1. 全体 112](#_Toc453840845)

[16.7.2. 基本情報 112](#_Toc453840846)

[16.7.3. 情報セキュリティ啓発（IPA） 112](#_Toc453840847)

[16.7.4. セキュリティ設定共通化手順SCAP概説（IPA） 113](#_Toc453840848)

[16.7.5. サイバー情報共有イニシアティブ（J-CSIP（ジェイシップ））（IPA） 114](#_Toc453840849)

[16.7.6. 情報セキュリティスキル強化についての取り組み（IPA） 114](#_Toc453840850)

[16.8. サイバーレスキュー隊J-CRAT（ジェイ・クラート）：IPA 114](#_Toc453840851)

[17. セキュリティ関連機関 115](#_Toc453840852)

[17.1. 日本セキュリティオペレーション事業者協議会（ISOG-J） 115](#_Toc453840853)

[17.2. ノートン 115](#_Toc453840854)

[17.3. トレンドマイクロ 115](#_Toc453840855)

[17.4. ＠IT 115](#_Toc453840856)

[17.5. 一般社団法人 電気通信事業者協会（TCA） 116](#_Toc453840857)

[18. 消費者庁 116](#_Toc453840858)

[19. 東京商工会議所 117](#_Toc453840859)

[20. Tcyss会議 117](#_Toc453840860)

[20.1. 第1回会議より（4月25日） 117](#_Toc453840861)

[21. 文献 118](#_Toc453840862)

[21.1. NDLアーカイブ 118](#_Toc453840863)

[22. 情報セキュリティ関連文書 119](#_Toc453840864)

[22.1. NISCサイバーセキュリティ戦略本部 119](#_Toc453840865)

[23. 情報システムの整備と運用管理を調達する際の情報セキュリティ対策として考慮すべき要件 119](#_Toc453840866)

[23.1. 「政府情報システムの整備及び管理に関する標準ガイドライン実務手引書」より 119](#_Toc453840867)

[24. 東京都の取り組み【公開情報】 119](#_Toc453840868)

[24.1. 東京都の行政改革 - 総務局行政改革推進部のホームページ - | ＩＴ・業務改革 119](#_Toc453840869)

[24.2. 高度情報化推進の取り組み 119](#_Toc453840870)

[25. 情報セキュリティマネジメント試験（シラバス） 119](#_Toc453840871)

[25.1. 119](#_Toc453840872)

[26. 情報処理技術者試験（シラバス） 119](#_Toc453840873)

[26.1. 基礎 119](#_Toc453840874)

[26.2. 応用 119](#_Toc453840875)

[27. 情報セキュリティ想定事例集 120](#_Toc453840876)

[27.1. 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（IPA） 120](#_Toc453840877)

# 体系的で特に有用な情報提供元【抽出中】

## ポータルサイト

### ホット情報

* 情報セキュリティ関連機関twitter
  + https://twitter.com/BlueMoon55/lists/security

### 全般

* 情報セキュリティって何をするの？「ここからセキュリティ！」:情報セキュリティ・ポータルサイト（事象・対象別）【IPA】
  + <http://www.ipa.go.jp/security/kokokara/>
* [みんなでしっかりサイバーセキュリティ]【NISC】
  + <http://www.nisc.go.jp/security-site/index.html>
* 国民のための情報セキュリティサイト【総務省】
  + <http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/index.html>
* 情報セキュリティ広場【警視庁】
  + <http://www.keishicho.metro.tokyo.jp/kurashi/cyber/index.html>
* IS702【トレンドマイクロ】
  + <http://www.is702.jp/>
* Security & Trust : 企業ネットワークセキュリティのためのノウハウ＆情報フォーラム - ＠IT
  + <http://www.atmarkit.co.jp/ait/subtop/security/>

### 中小企業向け

* 中小企業の情報セキュリティ対策ガイドライン（全8ページ、80KB）【IPA】
  + <http://www.ipa.go.jp/files/000014017.pdf>
  + 別冊1：委託関係における情報セキュリティ対策ガイドライン（全10ページ、333KB）
    - <http://www.ipa.go.jp/files/000014018.pdf>
  + 別冊2：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（全49ページ、803KB）
    - <http://www.ipa.go.jp/files/000014023.pdf>
  + 別冊3-1：5分でできる自社診断シート（全2ページ、156KB）
    - <http://www.ipa.go.jp/files/000014022.pdf>
  + 別冊3-2：5分でできる！自社診断パンフレット（全8ページ、2.67MB）
    - <http://www.ipa.go.jp/files/000014021.pdf>
* 中小企業における組織的な情報セキュリティガイドライン(IPA) 【IPA】
  + <http://www.ipa.go.jp/security/manager/know/sme-guide/sme-security_guidline.html>
  + 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[1,090KB]
    - <http://www.ipa.go.jp/files/000014950.pdf>
* 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【IPA】
  + <https://www.ipa.go.jp/security/keihatsu/shiori/management/03_casestudy.pdf>
    - 従業員の情報持ち出し
    - 退職者の情報持ち出し、競合他社への就職
    - 従業員による私物PCの業務利用と Winnyの利用による業務情報の漏洩事故
    - ホームページへの不正アクセス
    - 無許可の外部サービスの利用
    - 委託した先からの情報漏えい
    - 在庫管理システム障害の発生
    - 無線LANのパスワードのいい加減な管理
    - IT管理者の不在
    - 電子メール経由でのウイルス感染
* 初めての情報セキュリティ対策のしおり（IPA) 【LEVEL1】【冊子体】【容易】【中小】
  + <http://www.ipa.go.jp/security/antivirus/documents/09_hazimete.pdf>
* 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【IPA】【LEVEL0】【詳細】【冊子】【中小企業】
  + <http://www.ipa.go.jp/security/keihatsu/shiori/management/01_guidebook.pdf>
* 出社してから退社するまで中小企業の情報セキュリティ対策実践手引き（JNSA) 【LEVEL2】【チェックシート】
  + <http://www.jnsa.org/result/2010/chusho_security_tebiki_110330.pdf>
* 【●】小規模企業必見！　あなたの会社、セキュリティ対策は大丈夫？（トレンドマイクロ）【LEVEL1】【詳細】【チェックリスト】
  + <http://is702.jp/special/789/>

### 中小企業経営者向け

# 問合せ事例

## 東京都中小企業サイバーセキュリティ相談Webフォーム

* 東京都公式ホームページへようこそ
  + <http://www.metro.tokyo.jp/>
  + 分野からさがす⇒[経済・産業](http://www.metro.tokyo.jp/URBAN/keizai.htm)
    - 中小企業支援⇒[緊急中小企業支援対策](http://www.sangyo-rodo.metro.tokyo.jp/chushou/)
      * 商工⇒[サイバーセキュリティ](http://www.sangyo-rodo.metro.tokyo.jp/chushou/shoko/cyber/)
        + [相談窓口](http://www.sangyo-rodo.metro.tokyo.jp/chushou/shoko/cyber/soudan/index.html)⇒ホームページ：[東京都共同電子申請・届出サービス](http://www.shinsei.elg-front.jp/tokyo/navi/procInfo.do?govCode=13000&procCode=10002956)

[東京都電子申請 中小企業サイバーセキュリティ対策相談](http://www.shinsei.elg-front.jp/tokyo/navi/procInfo.do?govCode=13000&procCode=10002956)

[中小企業サイバーセキュリティ対策相談](https://www.shinsei.elg-front.jp/tokyo/uketsuke/dform.do?id=1461031266630)

中小企業サイバーセキュリティ対策相談申し込み内容の入力

* + <http://www.sangyo-rodo.metro.tokyo.jp/chushou/shoko/cyber/soudan/index.html>

## セキュリティ侵害の実態

* 「個人情報漏えい」原因の比率上位5位（2013年　NPO日本ネットワーク協会）
  + ・誤操作34.9%
  + ・管理ミス32.3%
  + ・紛失・置忘れ14.3%
  + ・盗難5.5%
  + ・不正アクセス4.7%
* 個人情報漏えい媒体、経路（2013年　NPO日本ネットワーク協会）
  + ・紙媒体58.7％
  + ・USB等記憶媒体25.9％
  + ・電子メール5.5％
  + ・インターネット5.0％

## 中小企業の現状から

### 情報セキュリティ対策の必要性を認識していない

* + 被害にあった場合、影響が如何に大きいかを認識させる⇒事例に基づいた被害と対策の必要性の認識が必要。
  + セキュリティ対策は、
    - IT化、デジタル化は
      * 業務の効率化、ITを使ったサービスの向上
      * ITを活用するために、セキュリティ対策を実施
        + （自動車を運転するために、自動車保険に入る）
    - セキュリティ侵害
      * 機密性（個人情報、取引先の情報、知的財産）、預金残高
      * 完全性（Webページ、帳簿類）
      * 可用性（業務システム、サービスシステム）
      * ⇒経済的損失、社会的信用の喪失⇒事業存続、事業継続の危機
    - 費用対効果を考える
      * 対策に要する費用と、侵害にあった場合の被害の大きさを比較する
      * 自動車任意保険、火災保険のようなもの。また、自動車の検問レーダーとかも

### システムをベンダーに任せて開発もしくは導入、運用している

* + セキュリティ対策を明確にした調達仕様書作成のスキル習得が必要

### 効果的な情報セキュリティ対策の方法がわからない

* + 認識すること
    - 断片的な対策では、セキュリティホールはなくならない
    - 内部職員による故意もしくは過失によるセキュリティ侵害は全体の80％以上
    - どれだけお金を掛けても脆弱性はゼロにはならない
    - リスク（脅威×資産価値×脆弱性）の高いものから順次対策を講ずる
  + 守るべき情報資産を洗い出して、管理的、技術的、人的、物理的対策の個別の対策の検討方法をレクチャー⇒情報セキュリティマネジメントシステム（ISMS）に準拠した情報セキュリティ対策の考え方

## 経済的損失⇒社会的信用の喪失、組織存立の危機

### ネットバンキングのセキュリティ対策

* ネットバンキング利用者がすべきセキュリティー対策とは
  + <http://www.nikkeibp.co.jp/article/column/20140604/400921/>
* 突然、ネットバンキングの残高がゼロに！？
  + <http://www.is702.jp/special/1748/partner/12_t/?cm_re=article-_-threat-_-is702&_ga=1.76536469.1038327157.1416213751>
* 脅威
  + 預金が勝手に別口座に送金される被害
* 脆弱性
  + フィッシング詐欺
    - 金融機関を装った偽のメールを利用者に送って、実在するネットバンキングのログインページを装う偽サイトに誘導
  + 利用者のパソコンをスパイウエアに感染させて、情報を奪うというもの。
    - 具体的には、正規のネットバンキングのサイトにアクセスすると、偽のポップアップ画面が表示され、そこに乱数表や合言葉などを入力させるのだ。また、パソコン内の個人情報やキーボードなどで入力した文字を犯人に転送するスパイウエアを使って、利用者に気付かれないように盗み出す手口もある。IDやパスワードなどを盗み取る
* 具体的対策
  + OSのアップデートを忘れずに行う。セキュリティーのサポートが行われなくなったOS（Windows XPなど）は使わない。
  + ソフトウエアを最新状態にする。JavaやAdobe Reader、Webブラウザーなどのアップデートは更新案内に従い、速やかに行う。
  + ウイルス対策ソフトを利用し、自動更新にする。
  + 心当たりのないメールは開かない。銀行がメールでIDやパスワードなどについて問い合わせることはない。
  + 怪しいサイトへのアクセスは避ける。
  + 金融機関のサイトを「お気に入り」に登録し、そこからアクセスする。メールに張り付けてあるアドレスからはアクセスしない。
  + 取引銀行のセキュリティー対策ツール（1回限りで使い捨てのワンタイムパスワード、ソフトウエア・キーボード、ウイルス対策ソフトなど）を積極的に利用する。
  + ワンタイムパスワードをメールで受け取る場合、ネットバンキングで利用しているパソコンとは別の機器・端末（携帯電話等）のメールアドレスで受信する。
  + 銀行のサイトにアップされている注意喚起情報を確認する。
  + 預金残高をこまめにチェックする。
  + 「怪しい」と思ったら、金融機関に電話などで問い合わせる。
* 教訓
  + セキュリティー対策は面倒でなおざりにしがちな人もいるかもしれないが、被害にあってから後悔しても遅い。
  + どんな資産
    - 金、情報（預かった情報、自社の機密情報）、機器
  + どんな情報セキュリティを確保するか
    - 機密性（権限のない人に見られない）、完全性（改ざんされない）、可用性（Wewbサービス等が継続できる）、否認防止（やった行為を言い逃れない）、説明責任（きちんと対策をしている）
  + ⇒事前のルール決め、対応策を明文化、ルールの遵守
    - 事業継続計画、情報セキュリティ基本方針、対策基準、実施手順を定める
    - 各手順を就業規則と同様に遵守するよう指導する

## フィッシング詐欺

## 「ウイルスに感染している」という画面が表示されるようになった

* アドウェアの可能性
  + リンクをクリックしたり、表示の電話番号に電話しない。無視する
* ウイルスワクチンソフトからのメッセージ
  + ウイルスを削除する

## OS コマンドインジェクション・SQLインジェクション等の防止

* 脅威
  + 情報の流出
    - 非公開情報（個人情報等）の漏えい等
  + •情報の改ざん
    - データベースに蓄積された情報（商品価格やパスワード等）の改ざん等
  + •データの破壊
    - 蓄積されたデータの消去やデータベーステーブル自体の破壊等
  + •サーバの乗っ取り
    - ストアドプロシージャを利用したサーバの不正操作等
* 対策
  + SQLを用いてデータベースを扱うWebアプリケーションは、SQL注入を許さないようにする必要がある。SQL注入攻撃対策のうち、まずは実装における対策について

## インシデント発生

### ネットワークに繋がりにくい、サーバの反応が悪い

* いつから？頻度は？どのような時に症状を感じるか？

### PCの調子が悪い

* ハード、ソフトの障害か、情報セキュリティ侵害かを切り分ける
* いつから？頻度は？どのような時に症状を感じるか？
* 何台で起こってる？
* 症状が始まった頃に何かしたか？
  + システム変更、新しいソフトのインストール
  + 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
  + その他考えられること

### ウイルスに感染したみたい

* 被害の拡大防止
  + システムをネットワークから切り離し、電源を落とす等の処置を行って、使用を中止する。
* 応急措置
* 原因調査
  + なぜ情報セキュリティ侵害が起きたか？
* 原状復旧
  + 安全なシステムディスクでシステムの再立ち上げを行い、感染したウイルスに合った適切な修復を行う。
  + なお、ウイルスの種類によっては、対処方法が異なりますので、必ずシステム管理者に連絡してその指示に従って、システムの復旧を行って下 さい。
* 恒久的対策
  + ルールの策定、遵守
  + 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

### ランサムウェアを使った詐欺・恐喝

* 悪意のあるプログラムによって、PC内のファイルが閲覧・編集できない形に暗号化され、ファイル復元の身代金として、利用者が金銭を要求される被害
* 原因
  + メールに添付されたランサムウェアに感染したファイルを実行してしまった。
  + 乗っ取られたWebサイトにアクセスして、ランサムウェアに感染してしまった。
* 予防
  + マルウェアに感染しないようにする対策
    - 不審なメールを開かない
      * 信頼できる人からのメールであることを確認（差出人の偽装注意）
    - 偽サイトへのアクセスに注意
      * 標的型メールでの不正サイトへの誘導に注意
    - 水飲み場型攻撃に注意
      * 標的組織が信頼してよく閲覧するWebサイトを改ざんして、標的となる組織からのアクセスの場合のみ攻撃する場合もあり発見しづらいことも多い
        + ⇒内部に侵入されることが前提での対策（サーバ、PCレベル）
  + 被害にあっても復旧できるように⇒事業継続計画（BCP）の対策と同様
    - 定期的なフルバックアップとバックアップ媒体をオフラインに
    - 日々の差分バックアップ
  + 情報セキュリティポリシーを順守する
* 応急措置
  + マルウェアに感染した場合の対応
    - 感染端末のネットワークからの切り離し
* 通報、原因調査
  + 犯罪行為に相当すると思われるので管轄の警察署に連絡
  + 金銭を支払っても復旧できる可能性は低い
  + なぜ情報セキュリティ侵害が起きたか？
* 原状復旧
  + マルウェアの除去
  + ディスクのバックアップからの復元
* 恒久的対策
  + ルールの策定、フールプルーフ対策、フェールセーフ対策、ルールの遵守、監査

## システム運用管理をしている客のシステムが、ランサムウェアに感染して、ファイルが読めなくなった

* 事業継続計画（BCP）に従う

## 水飲み場攻撃とは

* 脅威の概要
  + 標的組織がよく閲覧するWebサイトを改ざんし、閲覧した端末を不正プログラムに感染させる。
  + ブラウザの未知の脆弱性を悪用した攻撃（ゼロデイ攻撃）の場合もあり、未然防止は困難。
  + 不正プログラムを遠隔操作して内部侵入を繰り返し、重要情報の窃取・破壊等を実施。
  + ＜最近の事例＞
    - •2013年8月～9月中央省庁や大手企業の少なくとも20機関を狙った標的型サイバー攻撃（標的組織のIPアドレスからのサイト閲覧者だけが感染するもの）が発生
* 主な対策
  + 感染の未然防止は困難であるため、組織内部へ侵入されることを前提に内部対策を実施。
  + 内部対策としては、以下が挙げられる。
    - •内部に侵入した攻撃を早期検知して対処
    - •侵入範囲の拡大の困難度を上げる
    - •外部との不正通信を検知して対処
  + ＜統一基準群（平成26年度版）における対策事項＞
    - •6.2.4項標的型攻撃対策等

## 標的型メール攻撃とは

* 脅威の概要
  + 特定の組織を狙って職員等になりすましたメールを送付し、添付ファイルやURLを開かせることによって不正プログラムに感染させる。
  + 不正プログラムを遠隔操作して内部侵入を繰り返し、重要情報の窃取・破壊等を実施。
  + ＜最近の事例＞
    - •2012年11月一部の独立行政法人が「なりすましメール」による不正プログラムに感染し、情報漏えいした可能性があることが判明
* 主な対策
  + 不審なメールを検出する仕組みの整備、対応能力を向上する（SPFの検証、教育・訓練、等）。
  + 感染防止を目的とした入口対策のほか、遠隔操作による攻撃の早期検知等を目的とした内部対策を実施する。
  + ＜統一基準群（平成26年度版）における対策事項＞
    - •6.2.4項標的型攻撃対策•6.2.1項ソフトウェアに関する脆弱性対策•7.2.1項電子メール等

## 偽サイトを開設された

* ユーザ
  + 実被害
    - 例）金を振り込んだが商品が送られてこない、商品が送られてきても偽ブランド品だった
  + 事後措置
    - 不正競争防止法に抵触する可能性⇒相談：警視庁サイバー犯罪対策課、届出：所轄の警察署へ
  + 予防策
* 正規サイト運営者

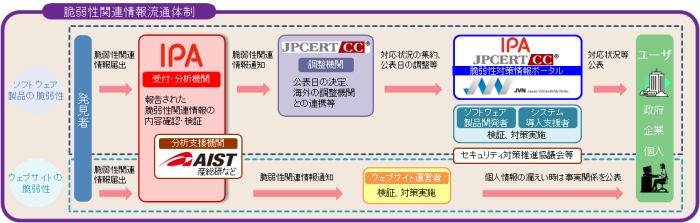
## 偽サイトにアクセスしてしまった

* インシデント

## スマホ等のセキュリティ対策は？

* 脅威
  + 端末を紛失した場合に悪用される
    - 電話の発信、着信
    - SMSの送信、受信
    - 記録されている電話帳のデータを全て見る、編集する
    - 記録されている写真、動画データを見る
    - メールの送信、受信
    - アプリの起動によるソーシャルメディアへの勝手なアクセス
    - 買い物、オンラインバンキング、金融資産の売却など
    - ICカードに登録されているカードが不正利用される
  + SIMを抜き取り悪用される
    - •契約している電話番号による電話の発信、着信
    - •インターネット回線の使用
    - •ネットを介して行うことができる電話会社のサービスの申し込みなど、契約内容の変更
  + SDカードを抜き取られ情報を搾取される
  + マルウェアに感染
    - 電話帳やメールなど様々な個人情報が抜き取られる
    - 意図せずSMS(ショートメッセージサービス)を送る
    - 通話が盗聴される
    - 外部から遠隔操作され犯罪に使われる
* 予兆、侵害緊急対応
  + ウイルスに感染
    - IPAへ
  + 盗難、セキュリティ侵害
    - 管轄の警察署へ
* 予防対策
  + 盗難に遭っても被害を拡大させないために
    - スクリーンロック機能を設定する
    - 各種サービスの認証は、できれば2段認証を利用する
  + SIMカードロック機能を設定
  + ICカードロック機能を設定（利便性は悪くなるが）
  + SDカードに機密情報を置かない
    - もしくは、データを暗号化する
  + FreeのWifi接続は気を付ける
    - 特に、パスワードを要求しない公衆無線LANへの接続は避ける
  + ウイルスに感染しないために
    - セキュリティソフトやセキュリティ対策サービスの導入
      * 危険なアプリのダウンロードをブロック
      * 既にインストールされている危険なアプリを特定し、削除
      * ワンクリック詐欺、フィッシング詐欺サイトなど悪質なサイトへのアクセスをブロック
      * 迷惑な着信およびSMS メッセージを遮断(電話機能があるもの)
      * 紛失時の端末ロック、遠隔地からのデータの削除、GPS による端末の所在地特定
    - 不審なメール、標的型メールにあるURLをクリックしない、添付ファイルを開かない
    - 脆弱性を下げるために
      * 信用できないアプリをインストールしない
        + Google Playストア以外からダウンロードしない
      * アプリが要求するアクセス許可を必ず確認する
        + 必要なさそうな権限を要求するアプリは気をつける
      * OS及びアプリは、できるだけ最新版に更新する
      * 携帯電話会社（キャリア）のセキュリティ対策サービスを利用する
        + ドコモ:あんしんスキャン   
          (<https://www.nttdocomo.co.jp/service/safety/docomo_anshin_scan/>)
    - 個人情報が流出しないように
      * SNS等で個人情報を公開する範囲に気を付ける
  + 原状復帰のため
    - 定期的なバックアップ（アプリ、データ、各種設定）
  + 【案内サイト】I Love スマホ生活
    - <http://www.ipa.go.jp/security/keihatsu/smartphone.html>

# 脆弱性情報の届出



# サイバーセキュリティとは

* サイバーとは
  + インターネットが形成する仮想空間（サイバースペース）
* サイバー攻撃とは、
  + コンピューターシステムやネットワークを対象に、破壊活動やデータの窃取、改ざんなどを行うこと。
  + 特定の組織や企業、個人を標的にする場合や、不特定多数を無差別に攻撃する場合がある。
* サイバーセキュリティとは
  + サイバー攻撃に対する防御行為。コンピューターへの不正侵入、データの改竄や破壊、情報漏洩、コンピューターウイルスの感染などがなされないよう、コンピューターやコンピューターネットワークの安全を確保すること。
* サイバーセキュリティ基本法において、
  + 電子的方式、磁気的方式その他人の知覚によっては認識することができない方式により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。）が講じられ、その状態が適切に維持管理されていること。

# 情報セキュリティに関する基礎知識

## 情報セキュリティ 10 大脅威（個人）

### 【一覧】情報セキュリティ 10 大脅威（個人）

* インターネットバンキングやクレジットカード情報の不正利用
* ランサムウェアを使った詐欺・恐喝
  + 悪意のあるプログラムによって、PC内のファイルが閲覧・編集できない形に暗号化され、ファイル復元の身代金として、利用者が金銭を要求される被害
* 審査をすり抜け公式マーケットに紛れ込んだスマートフォンアプリ
* 巧妙・悪質化するワンクリック請求
* ウェブサービスへの不正ログイン
* 匿名によるネット上の誹謗・中傷
* ウェブサービスからの個人情報の搾取
* 情報モラル不足に伴う犯罪の低年齢化
* 職業倫理欠如による不適切な情報公開
* インターネットの広告機能を悪用した攻撃

### 【一覧】情報セキュリティ 10 大脅威（組織）

* 標的型攻撃による情報流出
* 内部不正による情報漏えいとそれに伴う業務停止
* ウェブサービスからの個人情報の搾取
* サービス妨害攻撃によるサービスの停止
* ウェブサイトの改ざん
* 脆弱性対策情報の公開に伴い公知となる脆弱性の悪用増加
* ランサムウェアを使った詐欺・恐喝
* インターネットバンキングやクレジットカード情報の不正利用
* ウェブサービスへの不正ログイン
* 過失による情報漏えい

### 情報セキュリティ対策の基本

* ソフトウェアの更新
* ウイルス対策ソフトの導入
* パスワード・認証の強化
* 設定の見直し
* 脅威・手口を知る
  + （リスクの大きさに応じた対策：リスク＝情報の資産価値×脅威の大きさ×脆弱性）
  + ⇒どれだけお金をかけてもリスクは０にならない。如何に効率的、効果的に対策を講ずるかを考える。脆弱性の最大の要因は人。ITスキルを高めるとともに、管理的対策としてルールを定め、技術的対策は、フールプルーフ（ヒューマンエラー（利用者が行う誤った操作）が起こっても、危険な状況にならないようにするか、そもそも間違った操作が出来ないようにする設計）が重要

### 【対策】情報セキュリティ 10 大脅威（個人）

* インターネットバンキングやクレジットカード情報の不正利用
  + •OS・ソフトウェアの更新
  + •ウイルス対策ソフトの導入
  + •事例や手口を知る
  + •二要素認証等の強い認証方式の利用
* ランサムウェアを使った詐欺・恐喝
  + 悪意のあるプログラムによって、PC内のファイルが閲覧・編集できない形に暗号化され、ファイル復元の身代金として、利用者が金銭を要求される被害
  + PC利用者
    - •定期的なバックアップ（PCだけではなく、共有サーバーも）
    - また、復元できるかの事前の確認
    - •OS・ソフトウェアの更新
    - •ウイルス対策ソフトの導入・更新
    - •メールの添付ファイル・リンクのURLを不用意に開かない
  + スマートフォン利用者
    - •ウイルス対策ソフトの導入・更新
* 審査をすり抜け公式マーケットに紛れ込んだスマートフォンアプリ
  + スマートフォン利用者
    - •信頼できるアプリかどうかを確認
    - •アクセス権限の確認
    - •OSやアプリは最新版を利用
    - •ウイルス対策ソフトの導入
* 巧妙・悪質化するワンクリック請求
  + ウェブサービスの利用者
    - •怪しいソフトウェアは利用しない
    - •怪しいサイト・メールは開かない
    - •事例・手口の情報収集
  + ※購入の意思がないのであれば金銭を要求されても、慌てず請求に応じない
* ウェブサービスへの不正ログイン
  + ウェブサービス利用者
    - •推測されにくく、長いパスワードを設定する
    - •パスワードを使い回さない
    - •二要素認証等の強い認証方式の利用
    - •ログイン履歴の確認
  + ウェブサービス提供ベンダー
    - •安全なウェブサービスの提供
    - •複雑なパスワード設定を要求（少ない文字数や記号無しの拒否等）
    - •二要素認証等の強い認証方式の提供
    - •セキュリティ対策の徹底
* 匿名によるネット上の誹謗・中傷
* ウェブサービスからの個人情報の搾取
  + ウェブサービス運営者
    - •セキュアなウェブサービスの構築
    - （登録する個人情報も必要最低限に）
    - •OS・ソフトウェアの更新
    - •WAF・IPSの導入
  + ウェブサービス利用者
    - •不要な情報は極力サイトに登録しない
* 情報モラル不足に伴う犯罪の低年齢化
* 職業倫理欠如による不適切な情報公開
* インターネットの広告機能を悪用した攻撃

### 【対策】情報セキュリティ 10 大脅威（組織）

* 標的型攻撃による情報流出
  + ウイルスを添付したメールや、不正なWebサイトへ誘導するためのURLを記載したメール
  + チェックリスト
    - □送信者の名前やアドレスが見慣れないものである。
    - □組織内の話題なのに、外部のメールアドレスから届いている。
    - □フリーのメールアドレスから届いている。
    - □添付ファイルを開くよう、記載URLをクリックするよう不自然に誘導している。
    - □「緊急」などと急がせて、メールの内容を吟味させまいとしている。
    - □送信者の署名が無いか曖昧である。
    - □送信者の名前や組織名として、架空のものを名乗っている。
    - □受信者が信頼しそうな組織になりすまし、ウェブでの公開情報を送付してくる。
    - □上記以外で不審な箇所がある。
  + 経営者層
    - •問題に迅速に対応できる体制の構築
    - •対策予算の確保と継続的な対策実施
  + システム管理者
    - •情報の取扱い・保管状態の確認
    - •システム設計対策・アクセス制限
    - •ネットワーク監視・分離
  + セキュリティ担当部署
    - •セキュリティ教育の実施
    - •情報の保管方法ルール策定
    - •サイバー攻撃に関する情報共有
  + 従業員・職員
    - •セキュリティ教育の受講
    - •OS・ソフトウェアの更新
    - •ウイルス対策ソフトの導入・更新
* 内部不正による情報漏えいとそれに伴う業務停止
  + 組織
    - •情報取扱ポリシー作成および周知徹底・機密保護に関する誓約
    - •資産の把握・体制の整備
    - •情報の取扱教育の実施
    - •重要情報の管理・保護
    - •アカウント、権限の管理・定期監査
    - •システム操作の記録・監視
  + サービス利用者
    - •情報の管理が適切かを確認
* ウェブサービスからの個人情報の搾取
  + ウェブサービス運営者
    - •セキュアなウェブサービスの構築
    - （登録する個人情報も必要最低限に）
    - •OS・ソフトウェアの更新
    - •WAF・IPSの導入
  + ウェブサービス利用者
    - •不要な情報は極力サイトに登録しない
* サービス妨害攻撃によるサービスの停止
  + 個人・組織
    - •OS・ソフトウェアの更新
      * 踏み台にならないため、利用している機器も含めて管理
  + 組織
    - •DDoS攻撃の影響を緩和するISP等によるサービスの利用
    - •通信制御（DDoS攻撃元をブロック等）
    - •システムの冗長化等の軽減策
    - •サイト停止時の代替サーバーの用意
* ウェブサイトの改ざん
  + ウェブサイト運営者
    - •OS・サーバーソフトウェアの更新
    - •サーバーソフトウェアの設定の見直し
    - •ウェブアプリケーションの脆弱性対策
    - •アカウント・パスワードの適切な管理
    - •信頼できないサーバーソフトウェアを利用しない
    - •改ざん検知ソフトウェアの利用
  + ウェブサイト利用者
    - •OS・ソフトウェアの更新
    - •ウイルス対策ソフトの導入
* 脆弱性対策情報の公開に伴い公知となる脆弱性の悪用増加
  + システム管理者
    - •担当するシステムの把握・管理の徹底
    - •継続的な脆弱性対策情報の収集
    - •脆弱性発見時の対応手順の作成
    - •ソフトウェアの更新または緩和策
    - •ネットワークの適切なアクセス制限
  + ソフトウェア利用者
    - •利用しているソフトウェアの把握
    - •定期的な脆弱性情報の収集
    - •ソフトウェアの更新または緩和策
  + ソフトウェア開発ベンダー
    - •製品に組み込まれているソフトウェアの把握・管理の徹底
    - •継続的な脆弱性対策情報の収集
    - •脆弱性発見時の対応手順の作成
    - •情報を迅速に展開できる仕組みの整備
* ランサムウェアを使った詐欺・恐喝
  + 悪意のあるプログラムによって、PC内のファイルが閲覧・編集できない形に暗号化され、ファイル復元の身代金として、利用者が金銭を要求される被害
  + PC利用者
    - •定期的なバックアップ（PCだけではなく、共有サーバーも）
    - また、復元できるかの事前の確認
    - •OS・ソフトウェアの更新
    - •ウイルス対策ソフトの導入・更新
    - •メールの添付ファイル・リンクのURLを不用意に開かない
  + スマートフォン利用者
    - •ウイルス対策ソフトの導入・更新
* インターネットバンキングやクレジットカード情報の不正利用
  + •OS・ソフトウェアの更新
  + •ウイルス対策ソフトの導入
  + •事例や手口を知る
  + •二要素認証等の強い認証方式の利用
* ウェブサービスへの不正ログイン
  + 攻撃者が不正に入手したIDやパスワードでログインを試みる
* 過失による情報漏えい
  + ルールの明文化と遵守
  + フールプルーフ
    - ヒューマンエラー（利用者が行う誤った操作）が起こっても、危険な状況にならないようにするか、そもそも間違った操作が出来ないようにする設計

### 【対策】注目すべき脅威や懸念

* サポートの終了したソフトウェアを継続使用する危険性
  + 最新版への移行を
  + 移行できない場合はリスク緩和策
    - •ネットワークに繋がっていない環境で利用する、等
    - •ただし、脆弱性が解消される訳ではないため、早急な移行を
  + 組織においては計画的な移行を
    - •互換性の問題により移行できないケースを想定し、以下を考慮
      * 特定の製品やバージョンに依存しない
      * ソフトウェア製品のライフサイクル
* 証明書の導入・設定不備や検証不備に起因する脅威と対策
  + 事業者が注意すべきこと
    - 認証局発行でない自己署名証明書をルート証明書にインストールするソフトウェアを開発・配布しない
    - 秘密鍵を他者に配布することで動作するソフトウェアを開発・配布しない
    - 証明書に関する問題が発見された場合、速やかに脆弱性情報を公開すると共に、更新プログラム等の解決策を提供
  + 利用者として注意すべきこと
    - 最新情報の収集に努め、更新プログラム等が提供された場合、早急に適用する
    - 不審なソフトウェアはインストールしない
* マイナンバーの管理・運用の重要性
  + 個人として注意すべきこと
    - 趣旨と提示範囲の理解
      * •マイナンバーは、法令に定められた社会保障・税・災害対策の行政手続のためのみに提示、等制度の趣旨と開示範囲が決まっている
    - 保存・送信する場合
      * •PC等に電子化して保存する場合は、情報自体を暗号化し、端末操作にパスワード入力や指紋認証等の本人確認を必須となるように設定
      * •メール等のネットワーク経由で送信する場合、暗号化や改ざん防止を
  + 事業者が注意すべきこと
    - 特定個人情報の取扱いに関するガイドラインを遵守
      * •法令に定められた利用制限、厳重な管理、提供・収集の制限を実施
    - 継続的なセキュリティ対策の見直し・実施
    - 業種別の個別のガイドラインへの遵守も
      * •金融業務にかかわる事業者や行政機関・地方公共団体等

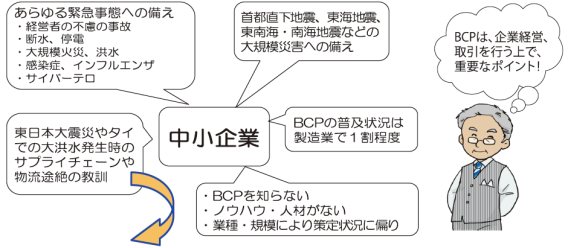
# サービス提供と情報セキュリティ対策

* 提供するサービスの迅速化と一層の充実等
  + - （政府情報システムの整備及び管理に関する標準ガイドライン実務手引書より）
  + インターネットの普及に伴い行政サービスの24時間365日提供に対する要請が高まる中、即時性が要求される申請等や提供するサービス内容の多様化・複雑化等に対応するために、業務手続の標準化と徹底した電子化の推進、情報セキュリティ上の要件を満たす前提での外部委託の活用、手続の統合による共通の情報システムの活用等を検討する。
* 情報セキュリティ対策は
  + サービスの向上を図るために、情報資産（保有情報（媒体に依らず）、情報機器、情報システム）に対する情報セキュリティ上のリスクを低減させる

# 事業継続計画（BCP）とセキュリティインシデント対応

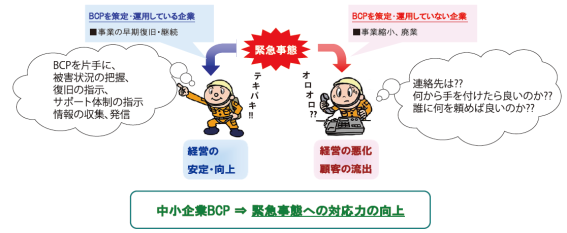
## BCPとは

* BCPとは、企業が緊急事態（自然災害、大火災、感染症、テロ、、、）に遭遇した場合において、事業資産（人・もの（情報及び設備）・金）の損害を最小限にとどめつつ、中核となる事業の継続あるいは早期普及を可能とするため、平時に行うべき活動、当該緊急非常時における事業継続のための方法、手段などをあらかじめ取り決め、それを文書化したもの。



## BCPはなぜ必要か？

* 企業が被災し、復旧が遅れ、事業継続が出来なくなると、①サプライチェーンの分断、②働く場の喪失、③事業の廃止、倒産といった事態に陥る可能性がある
* また、被害が甚大であれば、産業集積そのものが喪失したり、地域の雇用や経済に大きな影響が出ることとなり、被災地以外に影響が波及することにもなる



## 何のためにBCPを策定するのか？

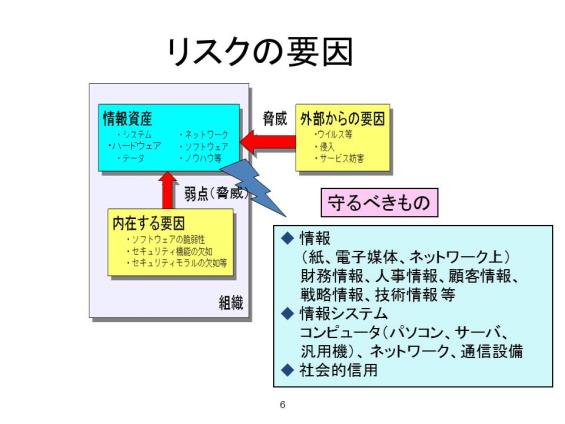


## セキュリティインシデント対応はBCPの１つ

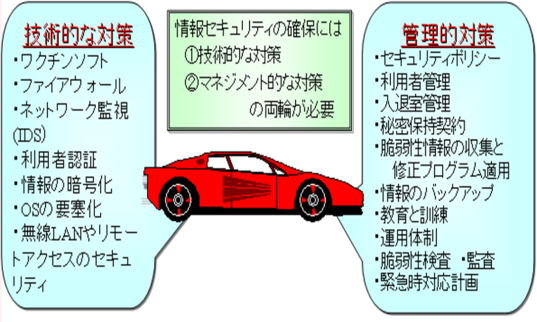
* BCPとは、企業が緊急事態（自然災害、大火災、感染症、テロ、、、）に遭遇した場合において、事業資産（人・もの（情報及び設備）・金）の損害を最小限にとどめつつ、中核となる事業の継続あるいは早期普及を可能とするため、平時に行うべき活動、当該緊急非常時における事業継続のための方法、手段などをあらかじめ取り決め、それを文書化したもの。
* 情報セキュリティポリシー（基本方針、対策基準）は、人的・物的被害の防御、軽減が主眼の「防災計画」の１つ
* インシデント対応は、被災後の事業の継続・早期復旧を視野に入れたBCPの１つ

# 対策の概念

## リスクの要因



## 情報セキュリティにおけるさまざまな対策



## 情報セキュリティ対策の意義（参照：NDL）

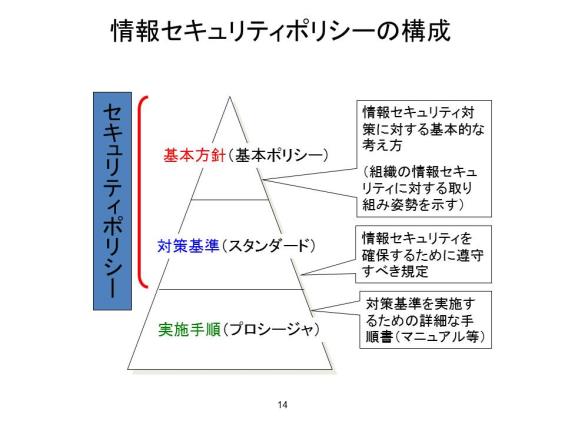
* 情報セキュリティ対策は目的ではない。サービスを向上させるため、サービスを継続するために情報セキュリティ対策を実施する
  + 組織のサービスの改善・向上を図るために必要な情報セキュリティのための措置（完全性・可用性の確保）
  + 組織が公開する権利を有しない情報の機密性を確保（機密性の確保）
  + 職員が館内外の情報資産に係る情報セキュリティを損なわないように（職員によるセキュリティ侵害
  + 行為）
  + 職員以外の者による館内外の情報資産に係る情報セキュリティの侵害に加担する結果にならないように（踏み台）
* セキュリティ侵害のリスクがあるから、サービスを提供しないのは本末転倒
  + 職員のITリテラシが低いから、職員の業務効率化に繋がるサービスの利用を制限するのも本末転倒

## 情報セキュリティ対策のポイント（私見）

* 人的情報セキュリティ対策
  + 背景
    - 情報漏洩は、内部の人間が引き起こす割合が約8割で、外部からの悪意ある攻撃による割合は2割程度
    - 内部の人間の認識不足や不注意をいかに解決するか
    - 誤操作、管理ミス、紛失・置き忘れ、故意や悪意によるもの
  + 情報セキュリティリテラシは、情報リテラシの１つ
  + 一般利用者
    - ITパスポート試験レベル（知識レベル１：社会人の常識レベルの情報リテラシ）
  + システム構築・運用担当者
    - 応用情報技術者試験レベル（知識レベル３）
    - 情報セキュリティマネジメント試験レベル（知識レベル３）
* 技術的情報セキュリティ対策
  + 企画・設計段階で、情報資産のリスクに応じた情報セキュリティ対策の要件を定義する
    - 情報セキュリティ対策は、情報システム構築の１つの要件
  + 要件定義が不明確のまま、構築すると、運用段階で、対処療法的な対策は膨大な費用が掛かる。
    - 未知の脆弱性への対応は、運用段階で
    - 設計・開発及び運用を外部委託するためには、発注者として、仕様書の段階で非機能要件の１つである情報セキュリティ対策を明確に記載  
      ⇒そのためには、情報セキュリティ対策を含め、システム設計・構築を外部委託するためのスキルが必要
  + 自前の情報セキュリティ対策に不安（脆弱性を低減できない等）がある場合、クラウドサービスの活用も有効
    - 情報セキュリティ対策の費用対効果、サービス向上、業務の効率化の観点からも、社会全般での普及が進んでいる
  + 信頼性設計（設計段階での考慮の一例）
    - フォールトレランス
      * システムの一部で障害が起こっても、全体でカバーして機能停止を防ぐ
    - フォールトアボイダンス
      * 個々の機器の障害が起こる確率を下げて、全体として信頼性を上げる
    - フェールセーフ
      * システムに障害が発生したとき、安全側に制御する方法
    - フェールソフト
      * システムに障害が発生したとき、障害が起こった部分を切り離すなどして最低限のシステムの稼働を続ける方法（縮退運転）
    - フォールトマスキング
      * 機器などに故障が発生したとき、その影響が外部に出ないようにする方法（冗長化等）
    - フールプルーフ
      * ヒューマンエラー（利用者が行う誤った操作）が起こっても、危険な状況にならないようにするか、そもそも間違った操作が出来ないようにする設計
* 管理的情報セキュリティ対策
  + 情報セキュリティマネジメントシステム（ISMS）に準拠した情報セキュリティポリシー（基本方針、対策基準）、実施手順の策定と確実な運用が重要
  + まず、情報資産（情報、情報機器、ソフトウェア）のリスクアセスメントを実施
    - （抜け道が多い、費用対効果が悪い対策にならないように）
      * どれだけ対策をしてもリスクは０にはならない。残留リスクに対して許容可能かを評価する
      * リスク（情報資産の価値×脅威×脆弱性）の高いものを優先投資
  + サービスの向上、維持を阻害させない情報セキュリティポリシー、実施手順の策定
    - 過度な情報セキュリティ管理により、新しいサービスの創造ができない、作業効率が悪い等の事象の回避。
      * 情報セキュリティ管理に関する事項のうち、適正水準よりも過度となっている部分について、要件の緩和を検討する。
    - 職員のITリテラシに合わせた情報セキュリティ対策で、はなく、まず、ITリテラシを高めることにより、適切な情報セキュリティ対策に対する意識を高める
* 物理的情報セキュリティ対策

# 情報セキュリティポリシー、実施手順

## 情報セキュリティポリシーの構成



## 情報セキュリティポリシー（基本方針）

* 情報セキュリティに関する組織の基本的な態度【NDL例】
  + 組織は、情報セキュリティを重視し、その保障に努める。
  + 組織は、館のサービスの改善を図るために必要な情報セキュリティのための措置を講ずる。
  + 組織は、利用者情報、利用情報及び館が公開する権利を有しない情報の機密性を確保する。
  + 組織は、職員が館内外の情報資産に係る情報セキュリティを損なうことのないよう措置する。
  + 組織は、職員以外の者による館内外の情報資産に係る情報セキュリティの侵害に加担する結果となることのないよう措置する。

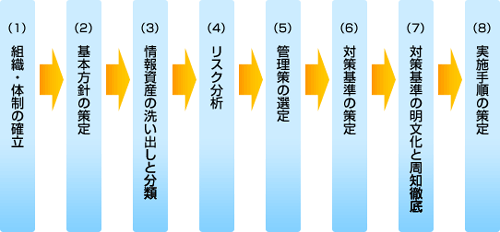
## 情報セキュリティポリシー（対策基準）

* 情報セキュリティ対策の実施【NDL例】
  + 人的セキュリティ対策
    - 情報セキュリティに関する権限及び責任を定め、情報セキュリティポリシーの内容を周知徹底するなど、職員の教育及び啓発を行う。
  + 物理的セキュリティ対策
    - 情報システム関係機器が設置された施設への不正な立入りを防止するなど、情報資産を危害、妨害等から物理的に保護する。
  + 技術的セキュリティ対策
    - 情報資産を外部からの不正なアクセスから保護する等のため、情報資産へのアクセス制御、ネットワーク管理、コンピュータウィルス対策等の技術的な対策を行う。
  + 運用に関するセキュリティ対策
    - 情報システムの監視、情報セキュリティポリシーの実施状況の確認等運用面における対策及び情報セキュリティ緊急事態に対応する危機管理対策を行う。
  + 具体的な対策基準
    - 別途

## 情報セキュリティ実施手順

* 情報セキュリティ対策指針
  + 「情報セキュリティ対策基準」の小項目毎に対応し、更に詳細な管理策（サブコントロールレベル）を示す
* 情報資産リスクマネジメント実施手順
  + 情報資産のリスクアセスメント、リスク対応に関する分析手法、リスク対応策を定めたもの。
  + 機密性・完全性・可用性の視点からリスクアセスメントを行い、必要なリスク対応手順を示す。
* 情報セキュリティ実施手順（一般職員向け）
* 情報セキュリティ実施手順（システム管理者向け）
* 各部課の情報セキュリティ実施手順

## 情報セキュリティマネジメントシステム（ISMS）構築手順



* ISMSの適用範囲を決定する
* 基本方針文書を策定する
* リスクアセスメントの体系的な取り組み方法を策定する
* リスクを識別する
* リスクアセスメントを行う
* リスク対策を行う
* 管理目的と管理策を選択する
* 各部課の実施手順に選択した管理策を反映させる
* 残留リスクを承認し、ISMSの実施を許可する

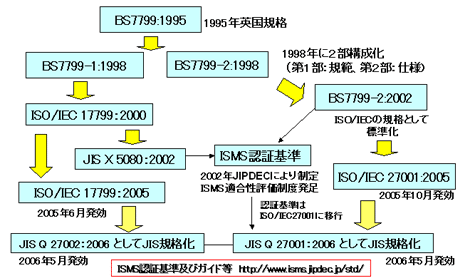
## ISMSとPDCAサイクル

* 情報セキュリティポリシーの策定
* リスクアセスメント
* リスクへの対応  
  管理策の導入と運用
* 情報セキュリティの評価
* 情報セキュリティマネジメントの規格や標準

## 脅威・対策・脆弱性・リスクの関係

* 脅威（内部・外部）
  + サービス妨害の脅威
  + 侵入しての何らかの行為が行われる脅威
    - セキュリティ侵害の事前調査
    - 権限取得及び侵入される可能性
    - 不正実行
      * 機密性を損なう可能性
      * 完全性を損なう可能性
      * 可用性を損なう可能性
    - 再度侵害を受ける可能性
  + 真正性が損なわれる脅威
  + 説明責任を果たせなくなる脅威
* 脅威への対策
  + 人的セキュリティ対策
  + 物理的セキュリティ対策
  + 技術的セキュリティ対策
  + 運用に関するセキュリティ対策
* 対策後の脆弱性
  + セキュリティホールとも呼ぶ
  + 人的、物理的、技術的、運用での対策の設計、構築、運用時の情報セキュリティ上の欠陥、不具合、ミス
* 脆弱性を突かれるリスク
  + 脆弱性が残された状態で情報セキュリティ侵害を受ける可能性
  + 例えば、クラウドコンピューティングの利用のリスクへの対応⇒対策
    - 回避
      * 利用によって生じると考えられるリスクを検討した結果、利用をやめる場合。クラウドコンピューティングサービスを利用しないため、これによるリスクは発生しない
    - 低減・軽減
      * データセンタの場所が国内であって、利用者がシステム監査を実施可能であるサービスを選定し、システム監査の条項を含む契約を結ぶことができるベンダーを選定する場合。適切な運用管理が行われているか否かを確認し、問題があれば改善等を要求し、リスクを低減する
    - 移転・共有
      * 何らかの問題が発生し損害が発生した場合には、賠償責任をベンダーが負うことについて、契約に明記し、その損害をカバーする場合等
    - 受容
      * 既に適切な対策が実施されており、残存リスクが小さいと判断される場合に、残存リスクがあることを承知した上で、特別に新たな対策を取らないことを意思決定した上で、利用する場合
  + 明確にしておくべき事項
    - 既知のリスクとその属性（予想される頻度、潜在的な影響及び対応）
      * リスクが影響する資源
      * リスクに対応する組織の力
      * 現状におけるリスクをコントロールする活動の状況
  + リスクに関する理解の促進
  + リスクのモニタリングと対応策の見直し
  + リスク顕在時の対応
    - 予兆の検出
    - 対応の準備
    - リスクの顕在化時（インシデント発生時）の対応
  + リスク対応結果の評価とその後の対応

## 情報セキュリティマネジメントの規格や標準



### 情報セキュリティマネジメントの実践のための規範JIS Q 27002:2006

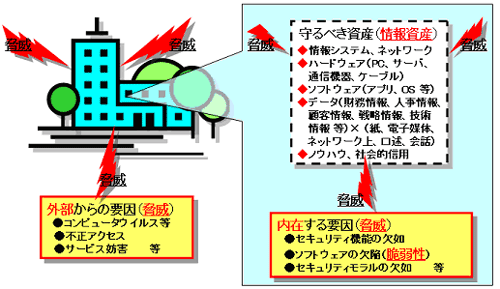
* 「Information technology - Security techniques - Code of practice for information security management（ISO/IEC17799）」という国際標準です。
* 2000年に初めて国際標準化され、2005年に改訂されたこの規格は、2006年5月に「情報技術－セキュリティ技術－情報セキュリティマネジメントの実践のための規範（JIS Q 27002:2006）」としてJIS化されました。
* この規格は、情報セキュリティ対策を行う際の Code of Practice（ = 実践規範）を記したものであり、ベストプラクティスとして様々な管理策が記載されています。
* 組織は、これらの管理策から自社にあったものを適宜、取捨選択できます。

### 情報セキュリティマネジメントシステム - 要求事項JIS Q 27001:2006

* 組織のISMS構築、運用に関する第三者認証のための要求事項を記したISMS認証の規格が、「ISO/IEC27001:2005 Information technology - Security techniques - Information security management systems - Requirements」です。
* この規格も2006年5月に「JIS Q 27001:2006 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム - 要求事項」としてJIS化されました。

## リスクマネジメント

* 対策基準では、
  + 基本方針の内容を受けて具体的なルール、いわゆる「管理策」を記述します。
  + 「管理策」は、情報セキュリティ上のリスクを減らすための対応策のことで、非常に多くのものがありますが、これらは「技術的対策」と「管理的対策（人的対策・組織的対策・物理的(環境的)対策を含む）」に大別されます。
* 対策基準を策定する際には、
  + 多くの管理策の中から、(1)何を自社にとって最適な管理策として選ぶか、そしてそれを(2)どのようにわかりやすく記載するか、というのが大きなポイントとなります。
  + それぞれの組織が抱えるリスクは、その組織の状況によって異なるため、実効性のある対策を選択するためには、リスクアセスメントを行う必要があります。
* リスクアセスメントとは、
  + 守るべき対象である情報資産で発生する可能性のある脅威と、脅威の発生確率や発生した場合の影響度等を評価する方法のこと。



### 情報資産の格付け

* 機密性についての格付の定義
  + 機密性３情報
    - 行政事務で取り扱う情報のうち、秘密文書に相当する機密性を要する情報
  + 機密性２情報
    - 行政事務で取り扱う情報のうち、秘密文書に相当する機密性は要しないが、漏えいにより、国民の権利が侵害され又は行政事務の遂行に支障を及ぼすおそれがある情報
  + 機密性１情報
    - 公表済みの情報、公表しても差し支えない情報等、機密性２情報又は機密性３情報以外の情報
  + なお、機密性２情報及び機密性３情報を「要機密情報」という。
* 完全性についての格付の定義
  + 完全性２情報
    - 行政事務で取り扱う情報（書面を除く。）のうち、改ざん、誤びゅう又は破損により、国民の権利が侵害され又は行政事務の適切な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報
  + 完全性１情報
    - 完全性２情報以外の情報（書面を除く。）
  + なお、完全性２情報を「要保全情報」という。
* 可用性についての格付の定義
  + 可用性２情報
    - 行政事務で取り扱う情報（書面を除く。）のうち、その滅失、紛失又は当該情報が利用不可能であることにより、国民の権利が侵害され又は行政事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報
  + 可用性１情報
    - 可用性２情報以外の情報（書面を除く。）
  + なお、可用性２情報を「要安定情報」という。
  + また、要機密情報、要保全情報及び要安定情報を「要保護情報」という。

### ITセキュリティマネジメントのための手法（JIS TR X 0036-3:2001）

* (1)ベースラインアプローチ
  + 既存の標準や基準をもとにベースライン（自組織の対策基準）を策定し、チェックしていく方法。簡単にできる方法であるが、選択する標準や基準によっては求める対策のレベルが高すぎたり、低すぎたりする場合がある
* (2)非形式的アプローチ
  + コンサルタント又は組織や担当者の経験、判断によりリスクアセスメントを行う。
  + 短時間に実施することが可能であるが、属人的な判断に偏る恐れがある
* (3)詳細リスク分析
  + 詳細なリスクアセスメントを実施。情報資産に対し「資産価値」「脅威」「脆弱性」「セキュリティ要件」を識別し、リスクを評価していく。
  + 厳密なリスク評価が行えるものの多大な工数や費用がかかる
* (4)組合せアプローチ
  + すべての情報資産に詳細なリスク分析を行うのは時間と費用がかかりすぎて現実的ではありません。
  + その組織を守るためのベースライン（基本）となる管理策の組み合わせを決め、その上でよりリスクの高いシステムを保護するために、詳細リスク分析を追加することにより、組織がリスク分析に用いる費用を削減でき、より精度の高いリスク分析を行うことが可能になります。
  + リスク評価は「リスクの重大さを決定するために、算定されたリスクを、与えられたリスク評価基準と比較するプロセス」と定義されていますが、「与えられたリスク評価基準」とは、どこかの基準に書いてあるものではなく、経営者により判断された評価基準です。
  + リスクへの対応は、つまりは、経営的判断により行われます。

# 「情報セキュリティ管理基準（平成20年改正版）」

* <http://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Management_Standard.pdf>

## 構成

* 「マネジメント基準」
  + 情報セキュリティマネジメントの確立
  + 情報セキュリティマネジメントの導入と運用
  + 情報セキュリティマネジメントの監視およびレビュー
  + 情報セキュリティマネジメントの維持および改善
  + 文書管理および記録の管理
* 「管理策基準」
  + セキュリティ基本方針
  + 情報セキュリティのための組織
  + 資産の管理
  + 人的資源のセキュリティ
  + 物理的及び環境的セキュリティ
  + 通信及び運用管理
  + アクセス制御
  + 情報システムの取得、開発及び保守
  + 情報セキュリティインシデントの管理
  + 事業継続管理
  + 順守

## マネジメント基準

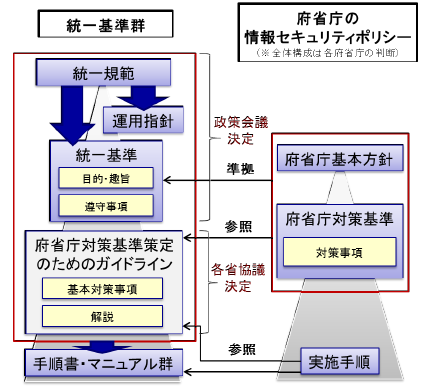
* 情報セキュリティマネジメントの確立
  + 適用範囲の定義
    - 情報セキュリティマネジメントの適用範囲及び境界を定義する
  + 基本方針の策定
    - 情報セキュリティ基本方針を策定する
    - 経営陣は情報セキュリティ基本方針にコミットする
  + リスクアセスメント
    - リスクアセスメントに対する組織の取り組み方を定義する
    - リスクを特定する
    - リスクを分析し、評価する
    - 経営陣はリスク受容基準及びリスクの受容可能レベルを決定する
  + 管理策の選択
    - リスク対応のための選択肢を特定し、評価する
    - リスク対応のための管理目的及び管理策を選択する
    - 残留リスクについて経営陣の承認を得る
    - 情報セキュリティマネジメントを導入し運用することについて経営陣の許可を得る
* 情報セキュリティマネジメントの導入と運用
  + リスク対応計画
    - リスク対応計画を策定する
    - リスク対応計画を実施する
    - 経営陣はリスク対応計画の実施のために十分な経営資源を提供する
  + 管理策の実施
    - 管理目的を満たすために管理策を実施する
    - 選択した管理策または一連の管理策の有効性をどのように評価するか、また評価の結果をどのように活用するかを定義する
  + 情報セキュリティマネジメントの運用管理
    - 情報セキュリティマネジメントの運用を管理する
    - 情報セキュリティマネジメントのための経営資源を管理する
    - 迅速にセキュリティイベントを検知でき、セキュリティインシデントに対応できるための手順及びそのための管理策を実施する
  + 教育、訓練、意識向上及び力量
    - 経営陣は情報セキュリティ基本方針に適合することの重要性を組織に伝える
    - 情報セキュリティマネジメントに影響がある業務に従事する要員に必要な力量を決定する
    - 必要な力量が持てるように教育・訓練するか、的確な要員の雇用など他の処置をとる
    - 教育・訓練、意識向上に関して有効性を評価する
    - 教育、訓練、技能、経験及び資格についての記録を維持する
    - 関連する要員すべてが、情報セキュリティについての活動が持つ意味と重要性とを認識する
    - 関連する要員すべてが、情報セキュリティマネジメントの目的の達成に向けて自分はどのように貢献できるかを認識する
* 情報セキュリティマネジメントの監視及びレビュー
  + 有効性の継続的改善
  + 監視及びレビューの準備
  + 管理策の有効性評価
  + 情報セキュリティマネジメントの継続性評価
* 情報セキュリティマネジメントの維持及び改善
  + 改善策の導入
  + 是正処置
  + 予防処置
* 文書管理及び記録の管理
  + 文書化
  + 文書管理
  + 記録の管理

## 「管理策基準」

* セキュリティ基本方針
  + 情報セキュリティ基本方針
* 情報セキュリティのための組織
  + 内部組織
  + 外部組織
* 資産の管理
  + 資産に対する責任
  + 情報の分類
* 人的資源のセキュリティ
  + 雇用前
  + 雇用期間中
  + 雇用の終了又は変更
* 物理的及び環境的セキュリティ
  + セキュリティを保つべき領域
  + 装置のセキュリティ
* 通信及び運用管理
  + 運用の手順及び責任
  + 第三者が提供するサービスの管理
  + システムの計画作成及び受入れ
  + 悪意のあるコード及びモバイルコードからの保護
  + バックアップ
  + ネットワークセキュリティ管理
  + 媒体の取扱い
  + 情報の交換
  + 電子商取引サービス
  + 監視
* アクセス制御
  + アクセス制御に対する業務上の要求事項
  + 利用者アクセスの管理
  + 利用者の責任
  + ネットワークのアクセス制御
  + オペレーティングシステムのアクセス制御
  + 業務用ソフトウェア及び情報のアクセス制御
  + モバイルコンピューティング及びテレワーキング
* 情報システムの取得、開発及び保守
  + 情報システムのセキュリティ要求事項
  + 業務用ソフトウェアでの正確な処理
  + 暗号による管理策
  + システムファイルのセキュリティ
  + 開発及びサポートプロセスにおけるセキュリティ
  + 技術的ぜい弱性管理
* 情報セキュリティインシデントの管理
  + 情報セキュリティの事象及び弱点の報告
  + 情報セキュリティインシデントの管理及びその改善
* 事業継続管理
  + 事業継続管理における情報セキュリティの側面
* 順守
  + 法的要求事項の順守
  + セキュリティ方針及び標準の順守並びに技術的順守
  + 情報システムの監査に対する考慮事項

# 「政府機関の情報セキュリティ対策のための統一基準群（平成26年度版）」

* 「政府機関の情報セキュリティ対策のための統一規範」
  + <http://www.nisc.go.jp/active/general/pdf/kihan26.pdf>
* 「政府機関情報セキュリティ対策統一基準の策定と運用等に関する指針」
  + <http://www.nisc.go.jp/active/general/pdf/unyou26.pdf>
* 「政府機関の情報セキュリティ対策のための統一基準（平成26年度版）」
  + <http://www.nisc.go.jp/active/general/pdf/kijyun26.pdf>
* 「府省庁対策基準策定のためのガイドライン」
  + <http://www.nisc.go.jp/active/general/pdf/guide26.pdf>

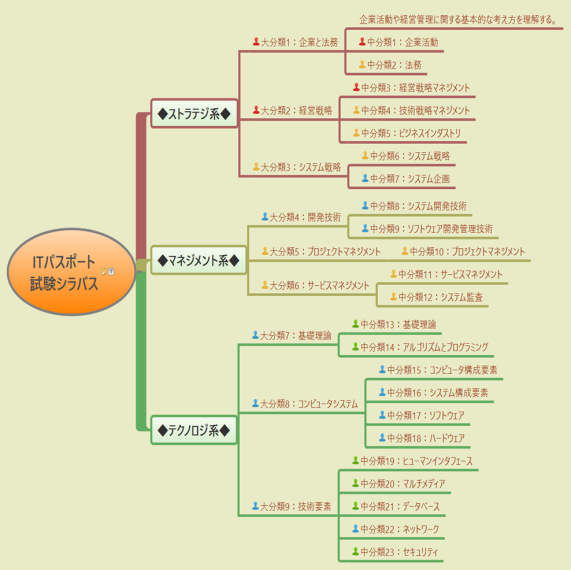


* 「重要インフラの情報セキュリティ対策に係る第３次行動計画」
  + <http://www.nisc.go.jp/active/infra/pdf/infra_rt3.pdf>
* 「新・情報セキュリティ人材育成プログラム」
  + <http://www.nisc.go.jp/active/kihon/pdf/jinzai2014.pdf>
* 情報セキュリティ小冊子（イラストを用いてわかりやすい）
  + <http://www.nisc.go.jp/active/general/pdf/kyozai-booklet.pdf>
  + 「政府機関の情報セキュリティ対策のための統一基準（平成26年度版）」の遵守事項のうち、一般職員が普段の業務を行うに当たり、情報セキュリティ対策を適切に遵守するための主要事項について、テーマ及びユースケースごとに整理したもの

## 

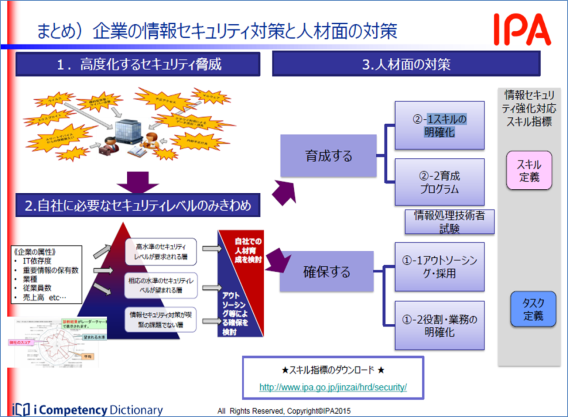
# 人材育成

## ITパスポート試験シラバス

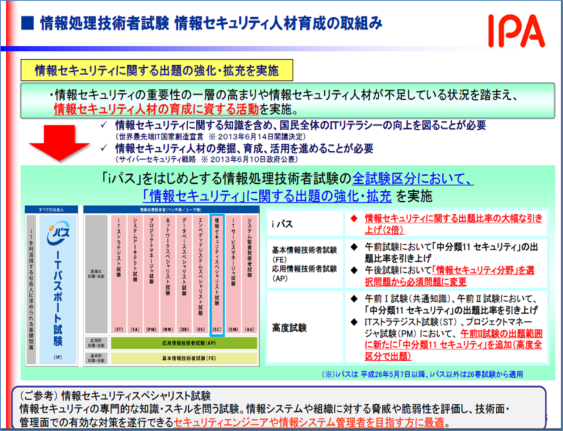


* 情報処理技術者試験のレベル１で、社会人の常識とされる
* システムを使ったサービスの提供者、利用者が知っておくべき基礎知識
* 範囲は網羅的
* 内容は用語の意味を知っていればいい程度

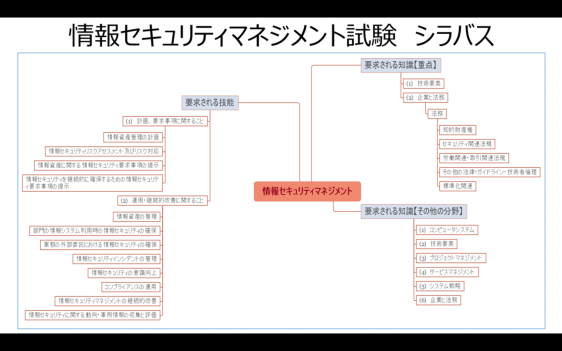
## まとめ）企業の情報セキュリティ対策と人材面の対策



## 情報処理技術者試験　情報セキュリティ人材育成の取り組み



## 情報セキュリティマネジメント試験　シラバス



## 情報セキュリティマネジメントタスクプロフィール

* 情報システムの利用部門において、
* 情報セキュリティリーダとして、部門の業務遂行に必要な情報セキュリティ対策や組織が定めた情報セキュリティ諸規程（情報セキュリティポリシを含む組織内諸規程）の目的・内容を適切に理解し、
* 情報及び情報システムを安全に活用するために、情報セキュリティが確保された状況を実現し、維持・改善する。

## 情報セキュリティ人材の職種

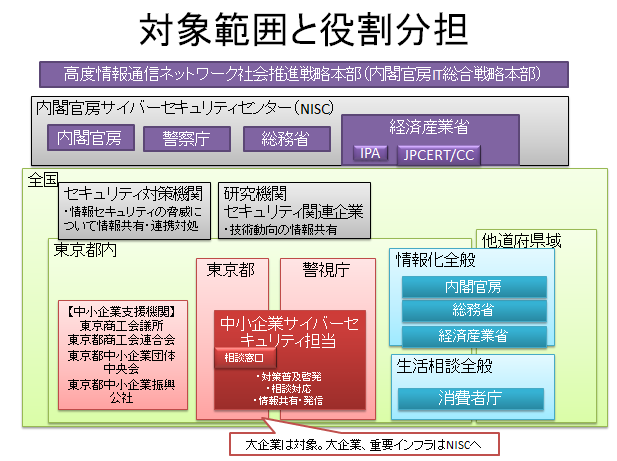
* 平成24年度に「情報セキュリティ人材の育成指標等の策定事業」（経済産業省）によって検討されたスキル標準等の見直し案の方針を受けて作成した 「情報セキュリティ強化対応CCSF」に基づくITSS、UISS、ETSS視点の人材モデル
* コンサルタント
  + 情報リスクマネジメント
    - すべてのインダストリに共通する組織ガバナンスと情報リスクマネジメント（事業継続管理、情報セキュリティマネジメント等）、コンプライアンスの領域における、競争・サービスの差別化の源泉となる専門知識を活用し解決策を提示する。"
* ITアーキテクト
  + セキュリティアーキテクチャ
    - ビジネスおよびIT上の課題を分析し、セキュリティ要件として再構成する。システム属性、仕様を明らかにし、情報システムの安全性や信頼性をセキュリティ面から実現する上で最適なアーキテクチャを設計する。設計したアーキテクチャがビジネス及びIT上の課題に対するソリューションを構成することを確認するとともに、後続の開発、導入が可能であることを確認する。"
* セキュリティアドミニストレータ
  + 情報セキュリティアドミニストレータ
    - 【ミッション】情報セキュリティ戦略やポリシー・ルール策定等を推進する。
    - 【活動内容】セキュリティの活動領域として以下を実施する。
      * ●事業戦略策定・情報セキュリティ戦略の策定
      * ●セキュリティ・セキュリティ方針の策定"
  + ISセキュリティアドミニストレータ
    - 【ミッション】IS戦略と情報セキュリティ戦略との相互連携を図る。情報セキュリティ戦略やポリシーを企画・計画に落とし込み、実装（ないしはその指示）・提供・維持・管理を行う。
    - 【活動内容】セキュリティの活動領域として以下を実施する。
      * ● IT基盤構築・維持・管理・品質統制フレームワークの運営 （各プロジェクトに対するガバナンスの実施）・ IS導入計画の策定
      * ●セキュリティ・セキュリティ基準の策定・セキュリティ事故と対応の分析・セキュリティ対応の見直し"
  + インシデントハンドラ
    - 【ミッション】情報セキュリティインシデントについて、インシデントの発生を検知・受付し、適切に判断・対応することで、被害を極少化する。
    - 【活動内容】セキュリティの活動領域として以下を実施する。
      * ●IS運用・セキュリティ管理"
* セキュリティマネージャ
  + 組込みセキュリティ
    - 製品に関するリスク対応の観点に基づき、機能安全を含む製品のセキュリティの側面から、企画・開発・製造・保守などにわたるセキュリティライフサイクルを統括する責任者。"
* 情報セキュリティマネジメント
  + 情報システムの利用部門において、情報セキュリティリーダとして、部門の業務遂行に必要な情報セキュリティ対策や組織が定めた情報セキュリティ諸規程（情報セキュリティポリシを含む組織内諸規程）の目的・内容を適切に理解し、情報及び情報システムを安全に活用するために、情報セキュリティが確保された状況を実現し、維持・改善する。

# 個人情報保護

* 法の趣旨
* 改正個人情報保護法（2015年6月）
  + 「匿名加工情報」とは、特定の個人を識別できないよう加工し、かつ個人情報を復元できないデータ。
  + この匿名加工情報は、個人情報を提供した本人の同意がなくても他社にデータを提供できる枠組み
  + 、「匿名加工情報は個人情報取得の際の利用目的にとらわれることなく、第三者に提供しなくても自社で利用できる」←匿名加工情報は個人情報ではない
  + 課題
    - 匿名加工情報は「匿名データ」ではない
    - 匿名化技術
      * 暗号法
        + データを暗号化
      * 摂動法
        + データに雑音を加えたり、データの一部を消したりして構造を変え。個人の特定を防ごうとするもの

# サイバーセキュリティ相談窓口の業務

## 中小企業に特化した情報セキュリティ対策の相談対応方針



### 中小企業の現状

* 組織の意識と対策
  + 情報セキュリティ対策の必要性の認識が低い
    - 被害にあった場合、影響が如何に大きいかを認識させる⇒事例に基づいた被害と対策の必要性の啓発。
  + システムをベンダーの言いなりで開発もしくは導入、運用
    - セキュリティ対策を明確にした調達仕様書のためのスキル教育の方法をレクチャー
  + 情報セキュリティ対策の方法がわからない
    - 守るべき情報資産を洗い出して、管理的、技術的、人的、物理的対策の個別の対策の検討方法をレクチャー⇒情報セキュリティマネジメントシステム（ISMS）に準拠した情報セキュリティ対策の考え方
* セキュリティ担当での調査
  + ターゲット分類は？
    - 組織規模
      * 従業員１名から９９９名
    - 業種別
      * 重要インフラ（社会インフラ）
      * 製造業、サービス業
    - 職種
      * 経営者、管理者、一般職員
    - 意識レベル
      * 意識がない⇒啓発から
      * 意識がある⇒具体的な対策から
    - システム・セキュリティ管理者の有無
      * 情報セキュリティマネジメント試験レベルの担当者
    - システムの内部調達・外部委託別
      * 要件定義はどちらでも
      * 外部委託は、調達仕様書が作成できるスキルの有無
      * 内部調達は、情報セキュリティ
      * スペシャリストレベルのスキルを持った設計開発者
  + 対策は？
    - 人的
    - 物理的
    - システム的
    - 管理的
  + 事例は？
    - 一般的な事例
    - 小企業での事例
    - 中企業での事例
    - 大企業とどう違う？

### 中小企業への支援

* 普及啓発
  + 対策の必要性、対策概要、具体的な対策
    - システムを使った事業の実施、創業のためには、情報セキュリティ対策が必要である
    - セキュリティ対策は、費用でなく、システム構築の一要件であり将来への投資であることを理解してもらう
  + 啓発内容の例
    - セキュリティ侵害の事例
      * 脅威の事例
      * リスクの事例
    - セキュリティ対策の事例
      * 費用対効果の高い対策とは
      * システムを構築する際の対策
      * 情報セキュリティ侵害があった時の対策
* 対策の概要
  + セキュリティ対策の普及啓発
    - ⇒啓発用Webページ、セミナー等の案内
      * 連携機関でのセミナー開催予定
      * 他機関でのセミナー開催予定
  + セキュリティの予防対策
    - システム化構築のPDCAサイクル
      * 脆弱性を低減するシステム企画・設計構築
      * セキュリティ侵害が発生したときに、速やかに対応できる運用、保守
    - 過剰、過小な対策を防ぐ提案
      * ⇒情報セキュリティ対策を含めたBCPの策定を提案
      * ⇒情報セキュリティに特化した対策はISMSの体系に沿った対策を提案
    - 重大事象を優先的に対策
      * 重要の情報資産は何か
      * 重要な情報資産への頻度の高い脅威の洗い出し
      * 脅威に対する脆弱性の度合い
      * 脆弱性を低減させる対策は？
  + セキュリティ侵害の事象発生（インシデント）の可能性あり
    - 段階
      * セキュリティ侵害の予兆段階
      * セキュリティ侵害の発生
    - 案内先
      * 犯罪の可能性
      * 一般的な不正アクセス、ウイルス感染
      * 高度な技術的対策が必要な事象

### 相談対応フロー

* 相談受付の基本的な考え方
  + セキュリティ侵害の予兆、事象発生時は、所管の窓口を案内
  + 対策として何をしたらいいかの相談は、外部のIT活用セミナー、セキュリティセミナーを案内
  + ⇒どこを参照？
* 相談を受け付ける対象
  + 重要インフラ⇒NISC
  + 従業員1000名以上⇒？
  + 都以外⇒？
  + 中小事業者、小規模事業者⇒受付
  + 個人⇒受付
* 相談内容種別毎の案内先
  + FAQにある内容⇒FAQに沿って回答
  + セキュリティ対策の普及啓発⇒今後、情報源を整理する
    - ⇒啓発用Webページ、セミナー等の案内
      * 連携機関でのセミナー開催予定
      * 他機関でのセミナー開催予定
  + セキュリティの予防対策（事前対策）⇒今後情報源を整理する
    - 外部のIT活用セミナー、セキュリティセミナーを案内⇒
    - 情報化のPDCAサイクルでのセキュリティ対策⇒
    - 過剰、過小な対策を防ぐ、ISMS、BCPの明文化
    - 重大事象を優先的に対策
  + セキュリティ侵害の事象発生（インシデント）の可能性あり
    - 段階
      * セキュリティ侵害の予兆段階
      * セキュリティ侵害の発生
    - 案内先
      * **一般的なトラブル**
        + **消費生活全般に関する苦情や問合せ**
        + **☎消費者ホットライン**

**188番（いやや！）**

**0570-064-370**

* + - * + **平日バックアップ相談【国民生活センター】**

**03-3446-1623**

* + - * **犯罪の可能性**
        + **サイバー犯罪に係る電話相談窓口**

**警視庁　サイバー犯罪対策課**

**03-3431-8109**

[**http://www.keishicho.metro.tokyo.jp/kurashi/cyber/index.html**](http://www.keishicho.metro.tokyo.jp/kurashi/cyber/index.html)

* + - * + **サイバー犯罪の届出**

**警視庁**

**03-3581-4321（交換）**

**管轄地域を確認し、管轄の警察署名への転送を依頼する**

* + - * + サイバー犯罪に関する情報提供

<https://www.keishicho.metro.tokyo.jp/anket/jiken_cyber.html>

Webフォームによる情報提供

緊急性のある事件・事故等の情報提供（殺害予告や犯行予告、生命の危機に関わるもの）は、110番

* + - * **一般的な情報セキュリティ相談**
        + **⇒IPAセキュリティセンター　情報セキュリティ安心相談窓口**

**可能な限り公開されているFAQを参照**

[**https://www.ipa.go.jp/security/anshin/#01**](https://www.ipa.go.jp/security/anshin/#01)

* + - * + [**https://www.ipa.go.jp/security/anshin/**](https://www.ipa.go.jp/security/anshin/)
        + **E-mail** [**anshin@ipa.go.jp**](mailto:anshin@ipa.go.jp)
        + **☎ 03-5978-7509**
      * 届出：ウイルスの届出
        + <https://www.ipa.go.jp/security/outline/todokede-j.html>
        + 03-5978-7518
        + [virus@ipa.go.jp](mailto:virus@ipa.go.jp)
      * 届出：不正アクセスに関する届出
        + <https://www.ipa.go.jp/security/ciadr/index.html>
        + 03-5978-7518
        + [crack@ipa.go.jp](mailto:crack@ipa.go.jp)
      * インシデント報告の届出
        + インシデント（インターネットに接続されたシステムを運用する際に発生したセキュリティ上の問題として捉えられる事象）の報告、相談
        + JPCERT/CCによる攻撃元サイトの停止などの対応の依頼の受け付け窓口
        + <http://www.jpcert.or.jp/form/>
        + 03-3518-2177
        + Webフォームでの相談
      * 脆弱性関連情報の届出
        + <http://www.ipa.go.jp/security/vuln/report/index.html>
        + [vuln-info@ipa.go.jp](mailto:vuln-info@ipa.go.jp)
        + Webフォームでの届出
      * J-CRAT／標的型サイバー攻撃特別相談窓口
        + <http://www.ipa.go.jp/security/tokubetsu/index.html>
        + [tokusou@ipa.go.jp](mailto:tokusou@ipa.go.jp)
        + 標的型攻撃メールと思われるメールを受信した場合は、各所属組織で決められた連絡先（システム担当部署や、セキュリティインシデント対応部署）へ連絡し、あわせて「標的型サイバー攻撃特別相談窓口」にご連絡ください。

# 情報セキュリティ関連法規

## サイバーセキュリティ基本法

## 不正アクセス禁止法

* アクセス制御機能，不正アクセス行為，不正アクセス行為を助長する行為

## 個人情報保護法

* 個人情報保護に関するガイドライン，特定個人情報の適正な取扱いに関するガイドライン，マイナンバー法施行令（行政手続における特定の個人を識別するための番号の利用等に関する法律施行令），JIS Q 15001，プライバシーマーク，OECD プライバシーガイドライン（プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告），プライバシー影響アセスメント（PIA），プライバシーフレームワーク，オプトイン，オプトアウト，第三者提供，匿名化手法（サンプリング，k-匿名化）

## 刑法

* 不正指令電磁的記録に関する罪（ウイルス作成罪）
* 電子計算機使用詐欺罪
* 電子計算機損壊等業務妨害罪
* 電磁的記録不正作出及び供用罪
* 支払用カード電磁的記録不正作出等罪

## その他のセキュリティ関連法規

* 電子署名及び認証業務等に関する法律（認定認証事業者，電子証明書）
* プロバイダ責任制限法
* 特定電子メール法

## 知的財産権

* 著作権法
* 産業財産権法
  + 不正競争防止法

## 労働関連・取引関連法規

* 労働基準法
* 労働者派遣法
* 男女雇用機会均等法
* 公益通報者保護法
* 労働安全衛生法
* 下請法
* インターネットを利用した取引
  + 特定商取引法
  + 電子消費者契約法

## その他の法律・ガイドライン・技術者倫理

* IT 基本法，e-文書法（電磁的記録），電子帳簿保存法），コンプライアンス，情報倫理・技術者倫理

## 知的財産計画2016

* 知財侵害関連の施策

# ここからセキュリティ！ 情報セキュリティ・ポータルサイト（IPA）【相談事例集作成候補】

* 凡例
  + 【LEVEL0】経営者, 【LEVEL1】一般, 【LEVEL2】システム運用管理者, 【LEVEL3】システム開発者向け

## ここからセキュリティ！ 情報セキュリティ・ポータルサイト

* <http://www.ipa.go.jp/security/kokokara/>
* 官民ボード全体会議メンバーが提供する情報
  + <http://www.ipa.go.jp/security/kokokara/board/index.html>

## トップページ

* <http://www.ipa.go.jp/security/kokokara/>
* スマートフォン利用の注意
  + マンガで学ぶサイバーセキュリティ 内閣サイバーセキュリティセンター(NISC)
  + <http://www.nisc.go.jp/security-site/files/CSmanga_JPN.pdf>
  + I love スマホ生活　スマホを安全に使うための6項目IPA
    - <http://www.ipa.go.jp/security/keihatsu/love_smartphone_life/mini_book/>
* ウイルス（マルウェア）
  + ウイルス感染を目的としたばらまき型メールに引き続き警戒をIPA
    - <http://www.ipa.go.jp/security/txt/2015/12outline.html>
  + 日本国内にも拡散中！巧妙で深刻なウイルス付き迷惑メールに注意　トレンドマイクロ
    - <http://www.is702.jp/special/1921/partner/12_t/>
* 標的型攻撃
  + 標的型攻撃メール対策のしおり　IPA
    - <http://www.ipa.go.jp/security/antivirus/documents/10_apt.pdf>
  + 【？】サイバー攻撃 : 標的型攻撃とは、APTとは　シマンテック
    - <http://www.symantec.com/ja/jp/theme.jsp?themeid=apt_insight#hyouteki>
* 不正アクセス
  + 侵入の手法と対処 警察庁
    - <http://www.npa.go.jp/cyberpolice/server/elearning/05/03/inp/01/contents2.html>
  + 不正アクセスによる被害と対策　総務省
    - <http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/admin/04.html>
* フィッシング詐欺
  + マンガでわかるフィッシング詐欺対策 5ヶ条フィッシング対策協議会
    - <https://www.antiphishing.jp/phishing-5articles.html>
  + あなたのお金が狙われている？！ネット詐欺の手口と対処法をクイズで確認＿トレンドマイクロ
    - <http://www.is702.jp/special/1725/partner/12_t/>
* 動画
  + 注目動画
    - 転落へのクリック～え？まさか犯罪者に～警察庁
      * <http://www.npa.go.jp/cyber/video/index.html>
  + 職場で見る
    - そのメール本当に信用してもいいんですか？　-標的型サイバー攻撃メールの手口と対策-\_\_IPA
      * <https://www.youtube.com/watch?v=duGNXcEEToU>
  + 家庭で見る
    - インターネットの危険から子供を守るのは保護者のあなた！政府インターネットテレビ
      * <http://nettv.gov-online.go.jp/prg/prg12149.html>
  + こどもと見る
    - ネットトラブル防止啓発動画\_ネットトラブルから自分を守ろう！～被害者にも加害者にもならないために～ネットトラブルから子どもを守る協働会議
      * <http://www.hyogo-c.ed.jp/~board-bo/netdouga/index.html>
* 新着情報
* セキュリティ点検ツール
  + クイズで判定新社会人が持つべきセキュリティの心構え（トレンドマイクロ）
    - <http://www.is702.jp/special/1542/partner/12_t/>

## 被害にあったら

* <http://www.ipa.go.jp/security/kokokara/accident/index.html>

### ウイルス（マルウェア）に感染したら

* サーバがウイルスに感染してしまった(警察庁) 【LEVEL1】【事例】
  + <http://www.npa.go.jp/cyberpolice/case/case21.html>
* パソコンがウイルスに感染してしまった(警察庁) 【LEVEL1】【事例】
  + <http://www.npa.go.jp/cyberpolice/case/case04.html>
* 【なし】コンピュータウイルス関連 FAQ　駆除・修復方法(IPA)
  + <http://www.ipa.go.jp/security/virus/faq/qa_top.html#4>
* 主なワクチンベンダー(IPA) 【LEVEL2】【窓口】
  + <http://www.ipa.go.jp/security/antivirus/vender.html>
* コンピュータウイルスに関する届出について(IPA) 【LEVEL2】【窓口】
  + <http://www.ipa.go.jp/security/outline/todokede-j.html>
* システムが感染しました - どうすればよいですか?(シマンテック) 【LEVEL2】【低】
  + <http://www.symantec.com/ja/jp/security_response/infected_systems.jsp>
* 「もしも」に備える処方箋～ウイルスが見つかったとき～(トレンドマイクロ) 【LEVEL1】【パンフレット】
  + <http://is702.jp/special/330/partner/12_t/>
* USBメモリで広まるウイルス～感染してしまったら？感染しないためには？～(トレンドマイクロ) 【LEVEL2】【有用】
  + <http://is702.jp/special/331/partner/12_t/>
* おかしいと思ったときの対処法(トレンドマイクロ) 【LEVEL2】【有用】
  + <http://is702.jp/special/577/partner/12_t/>
* PCがウイルスに感染していないかスキャンする(マイクロソフト) 【LEVEL3】【技術】
  + <http://www.microsoft.com/security/scanner/ja-jp/default.aspx>
* 万が一ウイルスに感染した場合の対処方法(マカフィー) 【LEVEL2】【低】
  + <http://www.mcafee.com/japan/mcafee/support/infection2006/infection1_1.asp>

### 不正アクセス（サーバーが攻撃された・ウェブページを書き換えられた）

* 脆弱性情報を適切に共有するために(不正アクセス行為防止WGセキュリティ･ホール攻撃対策の取組SWG) 【LEVEL3】【施策】
  + <http://www.npa.go.jp/cyber/kanminboard/siryou/sec_hole/partnership.html>
* @police DoS攻撃を受けて、サーバが利用不能になった(警察庁) 【LEVEL1】【事例】
  + <http://www.npa.go.jp/cyberpolice/case/case08.html>
* @police サーバがクラックされ、ページが書き換えられた(警察庁) 【LEVEL1】【事例】
  + <http://www.npa.go.jp/cyberpolice/case/taisho06.html>
* @police 侵入の手法と対処(警察庁) 【LEVEL1】【事例】
  + <http://www.npa.go.jp/cyberpolice/server/elearning/05/03/inp/01/contents2.html>
* @police サービス不能攻撃の手法と対処(警察庁) 【LEVEL1】【事例】
  + <http://www.npa.go.jp/cyberpolice/server/elearning/05/04/inp/01/contents2.html>
* ウェブサイト改ざんに関する注意喚起(IPA) 【LEVEL2】
  + <http://www.ipa.go.jp/security/topics/20091224.html>
* 不正アクセスに関する届出について(IPA) 【LEVEL2】
  + <http://www.ipa.go.jp/security/ciadr/index.html>
* 対応依頼および情報提供の受け付け(JPCERT/CC) 【LEVEL2】
  + <http://www.jpcert.or.jp/form>

### 情報漏えい（情報の紛失・流失・盗難）

* パソコンのハードディスクの中身がインターネット上に公開された(警察庁) 【LEVEL1】【事例】
  + <http://www.npa.go.jp/cyberpolice/case/case23.html>
* 掲示板に個人情報を書き込まれた(警察庁) 【LEVEL1】【事例】
  + <http://www.npa.go.jp/cyberpolice/case/case03.html>
* 会社の顧客情報が流出した(警察庁) 【LEVEL1】【事例】
  + <http://www.npa.go.jp/cyberpolice/case/case11.html>
* サーバのセキュリティ・ホールから不正アクセスをされた(警察庁) 【LEVEL1】【簡易】
  + <http://www.npa.go.jp/cybersafety/Virus/virus5.html>
* 自組織内の機密情報が、ファイル共有ソフトにより流出した(警察庁) 【LEVEL1】【事例】
  + <http://www.npa.go.jp/cyberpolice/case/case26.html>
* 組織内で管理する個人情報がスタッフによって外部へ流出した(警察庁) 【LEVEL1】【事例】
  + <http://www.npa.go.jp/cyberpolice/case/case16.html>
* ウェブページに自分の私的な性的画像が掲載されている(警察庁) 【LEVEL1】【簡易】
  + <http://www.npa.go.jp/cybersafety/Homepage/homepage11.html>
* 営業秘密侵害罪に係る刑事訴訟手続における被害企業の対応の在り方について(経済産業省) 【LEVEL2】【難解】
  + <http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/111216sankou5.pdf>
* 情報漏えい発生時の対応ポイント集(IPA) 【LEVEL2】【冊子体】
  + <http://www.ipa.go.jp/security/awareness/johorouei/>
* 個人情報の盗難を防止するために(マカフィー)【LEVEL1】【冊子体】
  + <http://jp.mcafee.com/ja/local/docs/IDTheft_eguide_JP.pdf>
* もしや、個人情報漏れ！？　そのときあなたがすべきことは？(トレンドマイクロ)【LEVEL2】
  + <http://is702.jp/special/1000/partner/12_t/>

### ワンクリック請求（料金画面が消えない・料金請求された）

* 身に覚えのない料金請求をされた(警察庁) 【LEVEL1】【事例】
  + <http://www.npa.go.jp/cyberpolice/case/case24.html>
* ワンクリック詐欺に注意(総務省) 【LEVEL1】【事例】
  + <http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/case/14.html>
* 【注意喚起】ワンクリック請求に関する相談急増！(IPA)【LEVEL2】
  + <http://www.ipa.go.jp/security/topics/alert20080909.html>
* クリックしただけで料金請求された場合の対応方法について(IPA) 【LEVEL2】
  + <http://www.ipa.go.jp/security/ciadr/oneclick.html>
* 「しまった！」と思ったら･･･ワンクリック詐欺の対処法、教えます(トレンドマイクロ)
  + <http://is702.jp/special/298/partner/12_t/>【LEVEL2】
* スマートフォンでも注意が必要！あなたを狙うワンクリック詐欺にご用心(トレンドマイクロ)

### 迷惑メール（スパムメール）

* 迷惑メールが来たがどうすれば良いか(警察庁) 【LEVEL1】【事例】
  + <http://www.npa.go.jp/cyberpolice/case/case05.html>
* 宣伝・広告のメールがたくさん届いて迷惑である(警察庁) 【LEVEL1】【FAQ】
  + <http://www.npa.go.jp/cybersafety/Case/Case3.html>
* チェーンメールが届いた(警察庁) 【LEVEL1】【簡易】
  + <http://www.npa.go.jp/cybersafety/Mail/mail2.html>
* 自社組織のドメイン名に詐称された迷惑メールをばらまかれた(警察庁) 【LEVEL1】【事例】
  + <http://www.npa.go.jp/cyberpolice/case/case18.html>
* おかしいと思ったときの対処法(トレンドマイクロ) 【LEVEL1】【簡易】
  + <http://is702.jp/special/581/partner/12_t/>
* 受け取りたくない、読みたくない！迷惑メールの対処法、教えます(トレンドマイクロ)っ【LEVEL2】
  + <http://is702.jp/special/1009/partner/12_t/>

### フィッシング詐欺・なりすまし（銀行やカード会社を騙るメール・送信元のアドレスを偽るメール）

* 【×】インターネットバンキング利用者の金融情報を狙った新たな犯行手口の発生について(警察庁)【広報資料】
  + <http://www.npa.go.jp/cyber/warning/h24/121026.pdf>
* フィッシング詐欺に遭った(警察庁) 【LEVEL1】【簡易】
  + <http://www.npa.go.jp/cyberpolice/case/case10.html>
* ID・パスワードを盗まれて「なりすまし」に遭った(警察庁) 【LEVEL1】【簡易】
  + <http://www.npa.go.jp/cyberpolice/case/case25.html>
* 自分のメールアドレスを騙ったメールが送付されている(警察庁) 【LEVEL1】【FAQ】
  + <http://www.npa.go.jp/cybersafety/Mail/mail3.html>
* 金融機関や企業等からID・パスワード等の個人情報を問い合わせるメールが届いた(警察庁) 【LEVEL1】【FAQ】
  + <http://www.npa.go.jp/cybersafety/Phishing/phishing1.html>
* 金融機関や企業等を装った偽のホームページを見つけた(警察庁) 【LEVEL1】【FAQ】
  + <http://www.npa.go.jp/cybersafety/Phishing/phishing2.html>
* ウイルスを使った新しいフィッシング詐欺に注意！(IPA)【LEVEL2】【広報資料】
  + <http://www.ipa.go.jp/about/press/pdf/111005press2.pdf>
* STOP!フィッシング詐欺　フィッシング詐欺に気づいたら(フィッシング対策協議会) 【LEVEL2】【ポータル】
  + <https://www.antiphishing.jp/stop_phishing/kiduitara.html>
* 銀行などを装った「フィッシング詐欺」にご注意ください！(TCA) 【LEVEL2】【窓口案内】
  + <http://www.tca.or.jp/information/phishing.html>
* 詐欺の被害者になったと思われる場合にすべきこと(マイクロソフト) 【LEVEL3】
  + <http://www.microsoft.com/ja-jp/security/online-privacy/phishing-scams.aspx#Victim>

## 対策する

* <http://www.ipa.go.jp/security/kokokara/measure/>

### 対策の基本（まずはここから！）

* 企業における対策の基本
  + 脆弱性対策に関する情報や対策に関するアドバイス(官民ボード不正アクセス行為防止WGセキュリティ･ホール攻撃対策の取組SWG) 【LEVEL3】【FAQ】
    - <http://www.npa.go.jp/cyber/kanminboard/siryou/sec_hole/vuln_solution.html>
  + 情報システムに対する技術的なセキュリティ対策(官民ボード不正アクセス行為防止WGセキュリティ･ホール攻撃対策の取組SWG) 【LEVEL3】【難解】
    - <http://www.npa.go.jp/cyber/kanminboard/siryou/sec_hole/technical_sec.html>
  + 遠隔制御不正プログラムに感染しないために!!!(警察庁) 【LEVEL0】【簡易】
    - <http://www.npa.go.jp/cyberpolice/topics/?seq=10204>
  + ノートパソコンのセキュリティ対策(警察庁) 【LEVEL0】【簡易】
    - <http://www.npa.go.jp/cyberpolice/server/elearning/12/04/inp/01/contents2.html>
  + 持ち運び可能なメディアや機器を利用する上での危険性と対策(総務省) 【LEVEL0】【ポータル】【容易】
    - <http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/staff/11.html>
  + 外出先で業務用端末を利用する場合の対策(総務省) 【LEVEL0】【ポータル】【容易】
    - <http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/staff/10.html>
  + 「 ウェブサイトが改ざんされないように対策を！ 」～サーバーやパソコンのみならず,システム全体での対策が必要です～(IPA) 【LEVEL2】【広報資料】
    - <http://www.ipa.go.jp/security/txt/2013/06outline.html>
  + 初めての情報セキュリティ対策のしおり(IPA) 【LEVEL1】【冊子体】【容易】【中小】
    - <http://www.ipa.go.jp/security/antivirus/documents/09_hazimete.pdf>
  + 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(IPA) 【LEVEL1】【冊子体】【容易】【中小】
    - <http://www.ipa.go.jp/security/keihatsu/shiori/management/01_guidebook.pdf>
  + 【●】情報セキュリティの脅威に対する対策(JPCERT/CC) 【LEVEL2】【容易】【中小】
    - <http://www.jpcert.or.jp/magazine/security/illust/part1.html>
  + 【×】情報セキュリティインシデントへの対応(JPCERT/CC)
    - <http://www.jpcert.or.jp/magazine/security/illust/part2.html#sec01>
  + 【●】出社してから退社するまで中小企業の情報セキュリティ対策実践手引き(JNSA) 【LEVEL2】【チェックシート】
    - <http://www.jnsa.org/result/2010/chusho_security_tebiki_110330.pdf>
  + 在宅勤務における情報セキュリティ対策ガイドブック(JNSA) 【LEVEL2】【冊子】
    - <http://www.jnsa.org/result/2011/zaitaku_guide.pdf>
  + 情報セキュリティ製品・サービス検索サイト(JNSA) 【LEVEL2】【ポータル】
    - <http://www.jnsa.org/JNSASolutionGuide/IndexAction.do;jsessionid=96959367D7BC41A8365344DF1405965F>
  + Heartbleed～OpenSSLの脆弱性～ (シマンテック) 【LEVEL3】【技術】【PPT】
    - <http://www.symantec.com/content/ja/jp/enterprise/images/outbreak/Heartbleed_vulnerability.pdf>
* 子どもを守るための対策
  + キッズ・パトロール ハッピィ星「セキュリティ対策編」(警察庁) 【LEVEL1】【子ども向け】【紙芝居】
    - <http://www.npa.go.jp/cyberpolice/kids/game/game10.html>
  + ご存知ですか？フィルタリング(総務省) 【LEVEL1】【子ども向け】【冊子】
    - <http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/pdf/leaflet.pdf>
  + フィルタリングを利用しましょう～子どもたちがケータイを利用する際の注意点～(EMA) 【LEVEL1】【ビデオ】【都庁環境で内容確認できず】
    - <http://www.ema.or.jp/education/pr/index.html>
  + 【×】インターネット安全教室(マイクロソフト)
    - <http://www.microsoft.com/ja-jp/security/family-safety/iss/iss.aspx>
  + お子様にオンライン セキュリティの基本を教える(マイクロソフト) 【LEVEL1】【保護者向け】
    - <http://www.microsoft.com/ja-jp/security/family-safety/cyberbullying.aspx>
  + 【×上記と同じ？】サイバーいじめからお子様を守る(マイクロソフト) 【LEVEL1】【保護者向け】
    - <http://www.microsoft.com/ja-jp/security/family-safety/cyberbullying.aspx>
  + 親子で安全対策！～ネット犯罪から子供を守る～(マカフィー) 【LEVEL1】【保護向け】【詳細】
    - <http://www.mcafee.com/japan/home/security/news/003.asp>
  + 「ネットいじめ」から子供を守ろう！(マカフィー) 【LEVEL1】【保護者向け】【詳細】
    - <http://www.mcafee.com/japan/home/security/news/021.asp>
  + ネットに潜むストーカーの実態(シマンテック) 【LEVEL2】【保護者向け】【詳細】【字が小さい】
    - <http://jp.norton.com/cyberstalking/article>
  + インターネットの危険からお子さまを守る\_保護者が知っておくべき脅威とその対策 (トレンドマイクロ) 【LEVEL1】【保護者向け】【詳細】
    - <http://www.is702.jp/special/1532/partner/12_t/>
* 家庭で行う対策
  + 個人情報を狙った偽の入力画面に注意(官民ボード質的・量的把握SWG) 【LEVEL1】【冊子体】【容易】【中小】
    - <http://www.npa.go.jp/cyber/kanminboard/siryou/report_netbank.pdf>
  + インターネットバンキングに係る不正送金事犯に関連する不正プログラム等の感染端末の特定及び駆除について(警察庁) 【LEVEL2】【詳細】
    - <http://www.npa.go.jp/cyber/goz/index.html>
  + 遠隔制御不正プログラムに感染しないために!!!(警察庁) 【LEVEL2】【広報】
    - <http://www.npa.go.jp/cyberpolice/topics/?seq=10204>
  + 【●】@policeセキュリティ講座(警察庁) 【LEVEL1】【体系的】【Javascript】
    - <http://www.npa.go.jp/cyberpolice/pc/elearning/index.html>
  + 【●】基本的な対策(総務省) 【LEVEL1】【体系的】【詳細】【事例】
    - <http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/security01/index.html>
      * 【事例列挙、、、】
      * 基礎知識
      * 一般利用者の対策
      * 企業・組織の対策
        + 【●】組織幹部のための情報セキュリティ対策

<http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/executive/index.html>

* + - * + 【●】社員・職員全般の情報セキュリティ対策

<http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/staff/index.html>

* + - * + 【●】情報管理担当者の情報セキュリティ対策

<http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/admin/index.html>

* + - * + 【●】事故・被害の事例

<http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/case/index.html>

* + - * 用語辞典
        + http://www.soumu.go.jp/main\_sosiki/joho\_tsusin/security/glossary/01.html
  + 【●】日常における情報セキュリティ対策(IPA) 【LEVEL1】【体系的】【概要】
    - <http://www.ipa.go.jp/security/measures/everyday.html>
  + 一般家庭における無線LANのセキュリティに関する注意(IPA) 【LEVEL2】【詳細】
    - <http://www.ipa.go.jp/security/ciadr/wirelesslan.html>
  + ネット銀行を狙った不正なポップアップに注意！(IPA) 【LEVEL1】【詳細】【広報】
    - <http://www.ipa.go.jp/security/txt/2012/12outline.html>
  + 【●】これだけはやろう!セキュリティ対策(IPA) 【LEVEL1】【簡易】
    - <http://www.ipa.go.jp/security/personal/base/index.html>
  + 【●】「SNSにおけるサービス連携に注意！」～あなたの名前で勝手に使われてしまいます～(IPA) 【LEVEL1】【詳細】【冊子体】【広報（保存版）】
    - <http://www.ipa.go.jp/security/txt/2012/10outline.html>
    - <http://www.ipa.go.jp/files/000016698.pdf>
  + 「STOP. THINK.CONNECT」とは(JPCERT/CC) 【LEVEL1】【簡易】【冊子体】
    - <https://www.antiphishing.jp/pdf/about_StopThinkConnect.pdf>
  + SNSの安全な歩き方～セキュリティとプライバシーの課題と対策(JNSA) 【LEVEL1】【冊子体】
    - <http://www.jnsa.org/result/2012/SNS-WG_ver0.7.pdf>
  + 【●】情報セキュリティ製品・サービス検索サイト(JNSA) 【LEVEL1】【ポータル】
    - <http://www.jnsa.org/JNSASolutionGuide/IndexAction.do;jsessionid=96959367D7BC41A8365344DF1405965F>
  + PC遠隔操作事件を次の安全対策に活かそう(マカフィー) 【LEVEL1】【簡易】
    - <http://mcafee.com/japan/home/security/news/026.asp>
  + インターネット通信を安全に利用するために(トレンドマイクロ) 【LEVEL1】【簡易】
    - <http://is702.jp/special/1250/partner/12_t/>
  + パソコンを新しくしたら、これだけはやっておこう(トレンドマイクロ) 【LEVEL1】【簡易】
    - <http://is702.jp/special/1101/partner/12_t/>
  + 家族でパソコンを共有するときの注意点と安全対策は？(トレンドマイクロ) 【LEVEL1】【簡易】
    - <http://is702.jp/special/1039/partner/12_t/>
  + 【●】パソコンを安心して使うために。(マイクロソフト) 【LEVEL0】【冊子３】【簡易】
    - <http://www.microsoft.com/ja-jp/security/resources/books.aspx>
  + 安全性の高いパスワードの作成 (マイクロソフト) 【LEVEL1】【簡易】
    - <http://www.microsoft.com/ja-jp/security/online-privacy/passwords-create.aspx>
* モバイル機器のセキュリティ（スマートフォン・携帯電話など）
  + Wi-Fi利用者向け 簡易マニュアル～安全なWi-Fi利用に向けて～(総務省) 【LEVEL1】【冊子】【簡易】
    - <http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/cmn/wi-fi/Wi-Fi_manual_for_Users.pdf>
  + 携帯電話・スマートフォン・タブレット端末の注意点(総務省) 【LEVEL1】【簡易】
    - <http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/security02/14.html>
  + あなたのスマートフォンの情報セキュリティは大丈夫ですか？(内閣官房情報セキュリティセンター) 【LEVEL1】【ポータル】【簡易】
    - <http://www.nisc.go.jp/security-site/smartphone/index.html>
  + スマホにおける新たなワンクリック請求の手口に気をつけよう！(IPA) 【LEVEL1】【広報】
    - <http://www.ipa.go.jp/security/txt/2013/05outline.html>
  + 公式マーケット上の不正なアプリに注意！～不正なアプリをインストールしないために～(IPA) 【LEVEL1】【広報】
    - <http://www.ipa.go.jp/security/txt/2013/03outline.html>
  + I loveスマホ生活　レイとランのスマホ事情(IPA) 【LEVEL0】【マンガ】【簡易】
    - <http://www.ipa.go.jp/security/keihatsu/love_smartphone_life/comics/04.html>
  + I loveスマホ生活　スマホを安全に使うための6項目(IPA) 【LEVEL0】【マンガ】【簡易】
    - <http://www.ipa.go.jp/security/keihatsu/love_smartphone_life/mini_book/index.html>
  + スマートフォンのセキュリティ<危険回避>対策のしおり(IPA) 【LEVEL1】【冊子】【詳細】
    - <http://www.ipa.go.jp/security/antivirus/documents/08_smartphone.pdf>
  + スマートフォン（スマホ）ご利用にあたっての注意事項(TCA) 【LEVEL1】【冊子】【一覧】
    - <http://www.tca.or.jp/mobile/img_1/%E3%82%B9%E3%83%9E%E3%83%BC%E3%83%88%E3%83%95%E3%82%A9%E3%83%B3%E3%81%AB%E9%96%A2%E3%81%99%E3%82%8B%E3%83%AA%E3%82%B9%E3%82%AF%EF%BC%88%E3%83%AD%E3%82%B4%E6%8C%BF%E5%85%A5%EF%BC%892.pdf>
  + ケータイ・インターネットの歩き方１「入門編」別添「スマートフォン編」 (モバイルコンテンツ審査・運用監視機構) 【LEVEL1】【簡易】
    - [http://ema-edu.jp/howtowalk01/text\_sp.html](http://ema-edu.jp/howtowalk01/text_sp.html#howto_sp_3)
  + 安全なWi-Fiの利用のヒント(トレンドマイクロ) 【LEVEL1】【詳細】
    - <http://www.is702.jp/special/1572/partner/12_t/?cm_re=article-_-threat-_-is702&_ga=1.35379362.2039373246.1395716218>
  + スマホやタブレットを取り巻く脅威と、対策のキホン (トレンドマイクロ) 【LEVEL1】【詳細】
    - <http://www.is702.jp/special/1515/partner/12_t/?cm_re=pickupbnr-_-threat-_-is702>
  + スマホ向け迷惑メールの撃退方法！ (トレンドマイクロ) 【LEVEL1】【詳細】
    - <http://is702.jp/special/1362/partner/12_t/>
  + スマホからの情報漏洩に気をつけて！盗難・紛失に伴うセキュリティリスクに備えよう(トレンドマイクロ) 【LEVEL1】【詳細】
    - <http://is702.jp/special/1301/partner/12_t/>
  + 人気アプリ、LINEを安全に利用するために(トレンドマイクロ) 【LEVEL1】【詳細】
    - <http://is702.jp/column/1266/partner/12_t/>
  + 見逃していませんか？インストール時の画面表示を確認して、危険なアプリを回避しよう(トレンドマイクロ)
    - <http://is702.jp/special/1211/partner/12_t/>
  + スマートフォンのセキュリティ対策(トレンドマイクロ) 【LEVEL1】【詳細】
    - <http://is702.jp/special/991/partner/12_t/>
  + あなたのケータイは大丈夫？　携帯電話、スマートフォンのセキュリティ対策(トレンドマイクロ) 【LEVEL1】【詳細】
    - <http://is702.jp/special/888/partner/12_t/>
  + スマートフォンでも急増中！ ワンクリック詐欺 (マカフィー) 【LEVEL1】【簡易】
    - <http://www.mcafee.com/japan/home/security/news/034.asp>
  + 待望のスマホやタブレットを安全に楽しもう！(マカフィー) 【LEVEL1】【簡易】
    - <http://www.mcafee.com/japan/home/security/news/028.asp>
  + 【●】モバイル セキュリティを実践するための10 の秘訣(マカフィー) 【LEVEL1】【冊子】【簡易】
    - <http://images.mcafee.com/ja-jp/advicecenter/pdf/MobileeGuide_Jan2012.pdf>
      * 端末を暗証番号（PIN）またはパスワードでロックする
      * 信頼できる提供元以外からアプリをインストールしない
      * データをバックアップする
      * システムを常に最新の状態にする
      * 端末のハッキングを防ぐ
      * オンライン バンキング サイトやショッピング サイトを閉じる場合には必ずログアウトする
      * 未使用時には無線、位置情報サービス、BLUETOOTHを無効にする
      * 携帯メールや電子メールで個人情報を送信しない
      * 不要なメールにあるリンクや添付ファイルをクリックしない
      * 携帯端末用のセキュリティアプリをインストールする
  + スマートフォンで急増するマルウェアの脅威　(マカフィー) 【LEVEL1】【簡易】
    - <http://www.mcafee.com/japan/home/security/news/027.asp>
      * まずマルウェアを知る
      * 安全性を確認する
      * 信頼できる所から購入する
      * アクセス許可リストを確認する
      * ウイルス対策ソフトを導入する
  + 偽広告モジュールを使用した多数の不審なアプリをGoogle Play上で確認(マカフィー) 【LEVEL1】【事例】【簡易】
    - <http://www.mcafee.com/japan/security/mcafee_labs/blog/content.asp?id=1366>

### ウイルス対策

* MacOSにもウイルス対策が必要 (官民ボード 質的把握SWG)
* 遠隔制御不正プログラムに感染しないため に!!!(警察庁)
* 感染予防策 (警察庁)
* ウイルス対策(総務省)
* ウイルス感染を目的としたばらまき型メールに引き続き警戒を (IPA)
* ウイルスを検出したと音声で警告してくるウェブサイトにご注意！ (IPA)
* ウイルス対策のしおり (IPA)
* コンピュータウイルス対策基準(IPA)
* 「 濡れ衣を着せられないよう自己防衛を！」～ 踏み台として悪用されないために～(IPA)
* 「 ウイルスの ゴールをゆるすな た よれるキーパー セキュリティ」(IPA)
* 「どうして偽セキュリティ対策ソフトがインストールされるの？」～基本的な対策を知って、慎重にネットサーフィンしよう～(IPA)
* 遠隔操作マルウェア事件から学ぶべきこと(JNSA)
* ウイルスやワーム攻撃 からコンピュータを保護する方法(マカフィー)
* マルウェアやトロイの木馬 の脅威からの防護(マカフィー)
* 金銭を狙うウイルスの最新手口と対処法（トレンドマイクロ）
* 知らない間にウイルス感染！？ネットの危険はどこからやってくる？（トレンドマイクロ）
* マクロ型ウイルスに注意
* メールを悪用した標的型攻撃の手口と対策（トレンドマイクロ）
* IT担当者向け、ウイルス検出時の対処法（トレンドマイクロ）
* スマホウイルスに注意！　だましの手口と対策ポイントをチェック(トレンドマイクロ)
* 私物USBメモリを会社に持ち込んでいませんか!? USBメモリ経由のウイルスの感染を防ぐ4つのポイント (トレンドマイクロ)
* 警告が表示されても焦りは禁物！？凶悪化する偽セキュリティソフトと新たな脅威ランサムウェアの対処法 (トレンドマイクロ)
* インターネット接続していなければ、ウイルスの心配 無用？(トレンドマイクロ)
* 危険なのはアダルトサイトだけではない。本当にあっ たウイルス・スパイウェア感染(トレンドマイクロ)
* マルウェア対策を強化し てコンピューターを保護する方法(マイクロソフト)

### 不正アクセス対策

* 脆弱性の対策には
* 脆弱性対策に関する情報や対策に関するアドバイス(官民ボード不正アクセス行為防止WGセキュリティ･ホール攻撃対策の取組SWG)
* 情報システムの技術的なセキュリティ対策
* 情報システムに対する技術的なセキュリティ対策(官民ボード不正アクセス行為防止WGセキュリティ･ホール攻撃対策の取組SWG)
* 侵入の手法と対処(警察庁)
* 無線LANでの対策(警察庁)
* 不正アクセスに遭わないために(総務省)
* 不正アクセス対策のしおり(IPA)
* 無線LAN＜危険回避＞対策のしおり(IPA)
* ウェブサイトの脆弱性検出ツール「iLogScanner」(IPA)
* 注意喚起 深刻且つ影響範囲の広い脆弱性などに関する情報(JPCERT/CC)

### 情報漏えい

* 個人情報管理編(警察庁) 【LEVEL0】【事例】【簡易】
  + <http://www.npa.go.jp/cyberpolice/pc/elearning/begin/05/index.html>
* 廃棄するパソコンやメディアからの情報漏洩 (総務省) 【LEVEL1】【簡易】
  + <http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/staff/09.html>
* 【●】営業秘密を適切に管理するための導入手順 ～はじめて営業秘密を管理する事業者のために～(経済産業省) 【LEVEL2】【冊子】【詳細】【管理手順】
  + <http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/120105sankou4.pdf>
* Winnyによる情報漏えいを防止するために(IPA) 【LEVEL3】【詳細】【技術】
  + <http://www.ipa.go.jp/security/topics/20060310_winny.html>
* 【●】情報漏えい対策のしおり(IPA) 【LEVEL1】【冊子】【詳細】【網羅的】
  + <http://www.ipa.go.jp/security/antivirus/documents/05_roei.pdf>
    - 企業(組織)の情報資産を、許可なく、持ち出さない
    - 企業(組織)の情報資産を、未対策のまま目の届かない所に放置しない
    - 企業(組織)の情報資産を、未対策のまま廃棄しない
    - 私物(私用)の機器類(パソコンや電子媒体)やプログラム等のデータを、許可なく、企業(組織)に持ち込まない
    - 個人に割り当てられた権限(\*3)を、許可なく、他の人に貸与または譲渡しない
    - 業務上知り得た情報を、許可なく、公言しない
    - 情報漏えいを起こしたら、自分で判断せずに、まず報告
* 【●】暗号化による<情報漏えい>対策のしおり(IPA) 【LEVEL1】【冊子】【詳細】【網羅的】
  + <http://www.ipa.go.jp/security/antivirus/documents/12_crypt.pdf>
    - 例えば電子メールの暗号化
    - 例えば、「紛失・置き忘れ」「盗難」対策の暗号化
    - 例えば、無線ＬＡＮを安全に利用するための暗号化
    - 例えば、会社の外と中との通信を安全に利用するための暗号化
* はじめての暗号化メール(Thunderbird編)(JPCERT/CC) 【LEVEL2】【冊子】【詳細】【網羅的】
  + <https://www.jpcert.or.jp/magazine/security/pgpquick.html>
* インターネットでのプライバシー保護(マイクロソフト) 【LEVEL2】【詳細】
  + <http://www.microsoft.com/ja-jp/security/online-privacy/prevent.aspx>
* 個人情報を保護するための10のヒント(マカフィー) 【LEVEL2】【簡易】
  + <http://home.mcafee.com/advicecenter/Default.aspx?id=ad_itp_1ttpypiai>
* 個人情報の盗難を防止するために(マカフィー) 【LEVEL1】【冊子】
  + <http://jp.mcafee.com/ja/local/docs/IDTheft_eguide_JP.pdf>
* 個人情報窃盗犯やハッカーはホーム ユーザを狙っている(マカフィー) 【LEVEL1】【詳細】
  + <http://home.mcafee.com/advicecenter/Default.aspx?id=ad_fis_itahthc>
* 他人に見られたくないデータ、消し忘れていませんか？(トレンドマイクロ) 【LEVEL1】【詳細】
  + <http://is702.jp/special/1050/partner/12_t/>
* 気づかぬうちに流出しているかも！？個人情報は自分で守ろう(トレンドマイクロ) 【LEVEL1】【詳細】
  + <http://is702.jp/special/854/partner/12_t/>
* 個人情報の窃取について：入門編（シマンテック）【LEVEL1】【詳細】【読みづらい】
  + <http://jp.norton.com/identity-theft-primer/article>

### ワンクリック請求（料金画面が消えない・料金請求された）【LEVEL1】【詳細】

* ワンクリック詐欺に注意(総務省) 【LEVEL1】【詳細】
  + <http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/security01/06.html>
* 身に覚えのない請求などの防止(IPA) 【LEVEL1】【リスト】【2005年】
  + <http://www.ipa.go.jp/security/personal/protect/oneclick.html>
* スマートフォンでもワンクリック請求に注意！(IPA) 【LEVEL1】【詳細】【広報】
  + <http://www.ipa.go.jp/security/txt/2012/02outline.html>
* ワンクリック詐欺(不正ポップアップ)への対策(トレンドマイクロ)
  + <http://jp.trendmicro.com/jp/threat/solution/detail/oneclick/index.html>
  + 「セキュリティ情報」へリダイレクト【LEVEL1】【ニュース】
  + <http://www.trendmicro.co.jp/jp/security-intelligence/index.html>
* 【●】そのクリック、ちょっと待って！巧妙化するワンクリック詐欺の手口(トレンドマイクロ) 【LEVEL1】【詳細】
  + <http://is702.jp/special/842/partner/12_t/>
    - 騙しサイトへと誘導する「エサ」が多様化
    - 誘導用のサイトを見つけやすくする
    - Webサイトを転々とたらい回しして誘導
    - 見えづらい利用規約
    - 個人情報が特定されたかのように錯覚させられる
    - スパイウェアやウイルスのインストール
    - ワナ・その7　パソコン以外にも脅威は潜んでいる
    - ワンクリック詐欺にひっかからないためには

### パスワード

* IDやパスワードを使い回すことの危険性(官民ボード 質的把握SWG) 【LEVEL1】【概要】【PDF】
  + <http://www.npa.go.jp/cyber/kanminboard/siryou/report_id_pass.pdf>
* ID･パスワード編 自分で気を付けること(警察庁)【都庁で確認不可】
  + <http://www.npa.go.jp/cyberpolice/pc/elearning/09/03/3-1.html>
* 安全なパスワード管理(総務省) 【LEVEL1】【詳細】
  + 国民のための情報セキュリティサイト内のページ：企業組織の対策
  + <http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/staff/01.html>
* メールが他人に読まれている？(総務省) 【LEVEL1】【詳細】
  + 国民のための情報セキュリティサイト内のページ：一般利用者の対策
  + <http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/case/05.html>
* 「 全てのインターネットサービスで異なるパスワードを！」(IPA) 【LEVEL1】【詳細】【広報】【2013年】
  + <http://www.ipa.go.jp/security/txt/2013/08outline.html>
* 「IDとパスワードを適切に管理しましょう 」(IPA) 【LEVEL1】【詳細】【広報】【2010年】
  + <http://www.ipa.go.jp/security/txt/2010/03outline.html>
* 「良い」パスワードを設定し、定期的に変更する(JPCERT/CC)
  + <http://www.jpcert.or.jp/magazine/security/illust/part1.html#sec03>
  + 【●】「情報セキュリティの脅威に対する対策」ページ内【LEVEL1】【詳細】
    - <http://www.jpcert.or.jp/magazine/security/illust/part1.html#sec03>
    - •全般
      * 1.ソフトウェアを最新版に更新する
      * 2.ウィルスパターンファイルを常に最新の状態に保つ
      * 3.「良い」パスワードを設定し、定期的に変更する
      * 4.使用しない PC をネットワークにつないでおかない
      * 5.スクリーンをパスワードでロックする
    - •web
      * 1.Webブラウザのセキュリティ設定を確認し、安全な設定でアクセスする
      * 2.安全であることが確認できない、web サイトにはアクセスしない
    - •電子メール
      * 1.電子メールの添付ファイルに注意する
      * 2.HTML 形式のメールに注意する
      * 3.電子メールに署名をする
      * 4.電子メールは必要に応じて暗号化する
* インターネット取引におけるID・パスワードの使いまわしによる不正使用被害にご注意ください(日本クレジット協会) 【LEVEL1】【詳細】
  + <http://www.j-credit.or.jp/customer/attention/unauthorized.html>
    - ID・パスワードを使いまわさないためには
* パスワードの約束事(シマンテック) 【LEVEL1】【詳細】
  + <http://jp.norton.com/dos-donts-passwords/article>
    - たとえば、「I want to go to England.」というフレーズなら、各単語の 1 文字目を取り、さらに「to」を「2」に置き換えると、「iw2g2e」という文字列ができます。次に、利用するウェブサイトの最初と最後の文字をこのパスワードに加えます。たとえば、Symantec.com のパスワードなら、上記の文字列に S と c を加え、「Siw2g2ec」とします。これで、シマンテックのウェブサイトで使用する固有かつ複雑なパスワードの出来上がりです。
* ひろしとアカリのセキュリティ事情　ファイルにパスワードをかけて保存する方法･･･(トレンドマイクロ) 【LEVEL1】【詳細】
  + <http://www.is702.jp/manga/1708/partner/12_t/?cm_re=article-_-threat-_-is702&_ga=1.177140645.1038327157.1416213751>
* 【●】パスワードの使いまわしに注意！　より強固なパスワードの作り方と安全な管理術をマスターしよう (トレンドマイクロ) 【LEVEL1】【詳細】
  + <http://is702.jp/special/1382/partner/12_t/>
    - パスワードの使い回しが連鎖的な不正アクセスの要因に！？
    - 破られにくいパスワードの設定と管理のポイント
    - アカウントをより安全に管理するには？
* これで忘れない、盗ませない！安心のパスワード管理術(トレンドマイクロ) 【LEVEL1】【詳細】
  + <http://is702.jp/special/882/partner/12_t/>
* 安全性の高いパスワードの作成 (マイクロソフト) 【LEVEL1】【詳細】
  + <http://www.microsoft.com/ja-jp/security/online-privacy/passwords-create.aspx>
* 不正ログインを防ぐための“パスワード管理術”(マカフィー) 【LEVEL1】【概要】
  + <http://www.mcafee.com/japan/home/security/news/036.asp>
* 強力なパスワードの技術 (マカフィー) 【LEVEL1】【詳細】
  + <http://home.mcafee.com/advicecenter/Default.aspx?id=ad_itp_tfsp>

### フィッシング詐欺・なりすまし

* インターネットバンキングに係る不正送金事案への対策について(警察庁) 【LEVEL1】【簡易】【広報】
  + <http://www.npa.go.jp/cyber/warning/h25/130501.pdf>
* インターネットバンキング利用者の金融情報を狙った新たな犯行手口の発生について(警察庁) 【LEVEL1】【簡易】【広報】【実例】
  + <http://www.npa.go.jp/cyber/warning/h24/121026.pdf>
* 私の名前で誰かがメールを(総務省) 【LEVEL1】【簡易】【事例】
  + <http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/case/02.html>
    - 「国民のための情報セキュリティサイト」内
* インターネットバンキングで情報が盗まれた(総務省) 【LEVEL1】【簡易】【事例】
  + <http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/case/16.html>
* フィッシング (Phishing)対策(IPA) 【LEVEL1】【簡易】【2004年】
  + <http://www.ipa.go.jp/security/personal/protect/phishing.html>
* なりすましメール撲滅に向けたSPF(Sender Policy Framework)導入の手引き(IPA) 【LEVEL3】【技術】【2004年】
  + <http://www.ipa.go.jp/security/topics/20120523_spf.html>
* インターネットバンキング利用時の勘所を理解しましょう！(IPA) 【LEVEL2】【詳細】【広報】【2004年】
  + <http://www.ipa.go.jp/security/txt/2013/09outline.html>
    - 従来手口、ワンタイムパスワードを破る新たな手口、対策の詳細説明
* パスワード ぼくだけ知ってる たからもの(IPA) 【LEVEL2】【詳細】【広報】【2011年】
  + <http://www.ipa.go.jp/security/txt/2011/06outline.html>
* 【●】フィッシング対策ガイドライン 2016 年度版(フィッシング対策協議会) 【LEVEL3】【詳細】【技術】【冊子】
  + <http://www.antiphishing.jp/report/pdf/antiphishing_guide.pdf>
* 【●】利用者向けフィッシング詐欺対策ガイドライン(フィッシング対策協議会) 【LEVEL1】【詳細】【冊子】
  + <http://www.antiphishing.jp/report/pdf/consumer_antiphishing_guideline.pdf>
* STOP!フィッシング詐欺 被害にあわないための５カ条(フィッシング対策協議会) 【LEVEL1】【リスト】
  + <https://www.antiphishing.jp/stop_phishing/gokajou.html>
* フィッシング対策の心得(フィッシング対策協議会) 【LEVEL1】【概要】【事例】
  + <https://www.antiphishing.jp/consumer/attention.html>
* フィッシングに関するFAQ(JPCERT/CC) 【LEVEL1】【概要】【FAQ】
  + <http://www.jpcert.or.jp/ir/faq.html>
    - フィッシング（phishing）とは何ですか？
    - フィッシングには、どのような危険があるのですか？
    - フィッシングサイトに重要な情報を入力しないようにするためには、どうすればよいですか？
    - フィッシングサイトに重要な情報を入力してしまったのですが、どうすればよいですか？
    - JPCERT/CC はフィッシングに対してどのような活動を行っているのですか？
    - フィッシングサイトを発見したのですが、どうすればよいですか？
* アクティビティ、関心事項、ニュース イベントを対象としたフィッシング詐欺(マイクロソフト) 【LEVEL1】【詳細】
  + <http://www.microsoft.com/ja-jp/security/online-privacy/phishing-interests.aspx>
  + 「セーフティとセキュリティ センター」内ページ【LEVEL1】【詳細】【ポータル】
    - <https://www.microsoft.com/ja-jp/security/default.aspx>
* フィッシング詐欺メール メッセージ、リンクまたは電話を識別する方法(マイクロソフト) 【LEVEL1】【詳細】
  + <http://www.microsoft.com/ja-jp/security/online-privacy/phishing-symptoms.aspx>
  + 「セーフティとセキュリティ センター」内ページ
* フィッシング詐欺 － 騙されない方法(マカフィー) 【LEVEL1】【詳細】
  + <http://home.mcafee.com/advicecenter/Default.aspx?id=ad_itp_phntgc>
* 【×】フィッシング対策は万全ですか？(マカフィー)【都庁環境で表示できず】
  + <http://jp.mcafee.com/ja/local/html/identity_theft/hooked_by_phishing_scam.asp>
* スピアフィッシング: スポーツではなく詐欺(シマンテック) 【LEVEL1】【詳細】
  + <http://jp.norton.com/spear-phishing-scam-not-sport/article>
* 【●】5つのコツでフィッシング詐欺を回避しよう(トレンドマイクロ) 【LEVEL1】【容易】
  + <http://www.is702.jp/special/1580/partner/12_t/?cm_re=article-_-threat-_-is702&_ga=1.6477361.2039373246.1395716218>
* 実録・Facebookアカウント乗っ取り被害：覚えのないメッセージが友人へ (トレンドマイクロ) 【LEVEL1】【詳細】【事例】
  + <http://blog.trendmicro.co.jp/archives/7300>
* 日本人を標的にしたマスターカードを偽るフィッシングサイトを大量確認(トレンドマイクロ) 【LEVEL1】【詳細】【事例】
  + <http://blog.trendmicro.co.jp/archives/6474>
* ネットの詐欺に要注意！巧妙化するフィッシング詐欺の手口(トレンドマイクロ) 【LEVEL1】【詳細】
  + <http://is702.jp/special/1130/partner/12_t/>

### 標的型攻撃メール

* 標的型攻撃への対策(総務省) 【LEVEL1】【詳細】
  + <http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/staff/05.html>
    - 「国民のための情報セキュリティサイト」内　企業・組織の対策
* 【●】標的型攻撃メール対策のしおり(IPA) 【LEVEL1】【詳細】【冊子】
  + <http://www.ipa.go.jp/security/antivirus/documents/10_apt.pdf>
* 標的型サイバー攻撃の事例分析と対策レポート(IPA) 【LEVEL1】【詳細】【広報】【2012年】
  + <http://www.ipa.go.jp/security/fy23/reports/measures/>
* 情報窃取を目的として特定の組織に送られる不審なメール(IPA) 【LEVEL1】【内容なし】【広報】
  + <http://www.ipa.go.jp/security/virus/fushin110.html>
  + •標的型サイバー攻撃の特別相談窓口
    - J-CRAT／標的型サイバー攻撃特別相談窓口【LEVEL1】【窓口紹介】【広報】
      * <http://www.ipa.go.jp/security/tokubetsu/index.html>
      * 03-5978-7599
      * [tokusou@ipa.go.jp](mailto:tokusou@ipa.go.jp)
      * 自分のメールアカウント、または自組織のメールシステムから標的型攻撃メールが送られた場合
      * 自分の名前や組織を騙る標的型攻撃メールが見つかった場合
      * 標的型攻撃メールの見分け方
        + •メールの受信者に関係がありそうな送信者を詐称する
        + •添付ファイルや本文中のURLリンクを開かせるため、件名・本文・添付ファイルに細工が施されている
        + （業務に関係するメールを装ったり、興味を惹かせる内容や、添付ファイルの拡張子を偽装するなど）
        + •ウイルス対策ソフトで検知しにくいマルウェアが使われる
      * 一般には次のような件名、本文から構成される事例が多く見られます（NCCICの標的型メール攻撃に関するアドバイザリに一部IPAで加筆）。
        + •社内の連絡メールを装うもの（ファイルサーバのリンクを模すケースを含む）
        + •関係省庁や、政府機関からの情報展開を模すもの（連絡先、体制、会見発表内容など）
        + •メディアリリース
        + •合併や買収情報
        + •ビジネスレポート/在庫レポート/財務諸表
        + •契約関連
        + •技術革新情報
        + •国際取引
        + •攻撃者に関する情報
        + •自然災害
        + •ウェブなど公開情報を引用したもの
        + •政府/業界イベント
        + •政府または産業における作業停止
        + •国際的または政治的なイベント
* 「標的型攻撃について」(JPCERT/CC) 【LEVEL1】【詳細】
  + <http://www.jpcert.or.jp/research/targeted.html>
  + 標的型攻撃についての調査【LEVEL1】【詳細】【2008年】
    - http://www.jpcert.or.jp/research/2007/targeted\_attack.pdf
* 電子メールソフトのセキュリティ設定について(JPCERT/CC) 【LEVEL1】【詳細】【2008年】
  + <http://www.jpcert.or.jp/magazine/security/mail/index.html>
* 深刻化する標的型攻撃への対策(マカフィー) 【LEVEL1】【詳細】
  + <http://www.mcafee.com/japan/security/apt.asp>
  + Security Connectedの紹介
* 【●】サイバー攻撃への備えはできていますか？(トレンドマイクロ) 【LEVEL1】【詳細】
  + <http://is702.jp/special/1055/partner/12_t/>
  + サイバー攻撃の魔の手は個人ユーザにも及ぶ
  + 対策1　OS（基本ソフト）やアプリケーションソフトは最新版を使う
  + 対策2　セキュリティソフトを適切に運用する
  + 対策3　不審なメールやファイル、ウェブサイトに近づかない
* 【●】サイバー攻撃、標的型攻撃への対策(トレンドマイクロ) 【LEVEL1】【ポータル】【詳細】
  + <http://jp.trendmicro.com/jp/threat/solution/detail/cyberattack/>
  + セキュリティ情報ポータル
* 決意を持った敵対者と標的型攻撃(マイクロソフト) 【LEVEL1】【詳細】
  + <http://blogs.technet.com/b/jpsecurity/archive/2012/06/20/3504843.aspx>
  + 日本のセキュリティチーム【LEVEL2】【ポータル】【詳細】
    - <https://blogs.technet.microsoft.com/jpsecurity/>

### 迷惑メール

* メール編　自分で気を付けること(警察庁) 【LEVEL1】【簡単】
  + <http://www.npa.go.jp/cyberpolice/pc/elearning/04/03/inp/01/contents2.html>
* 迷惑メールへの対応 (総務省) 【LEVEL1】【詳細】
  + <http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/security02/10.html>
  + 国民のための情報セキュリティサイト内　一般利用者の対策
* 添付ファイルを開いたらウイルスに感染！？迷惑メールの最新手口と3つの回避術(トレンドマイクロ) 【LEVEL1】【詳細】
  + <http://www.is702.jp/special/1761/partner/12_t/?cm_re=article-_-threat-_-is702&_ga=1.123381323.196970070.1431999093>
  + 反応したら餌食に！？
  + 受信者をだますテクニックが巧妙に
  + 3つの迷惑メール回避術
* スマホ向け迷惑メールの撃退方法！ (トレンドマイクロ) 【LEVEL1】【詳細】
  + <http://is702.jp/special/1362/partner/12_t/>
* 受け取りたくない、読みたくない！迷惑メールの対処法、教えます(トレンドマイクロ) 【LEVEL1】【詳細】
  + <http://is702.jp/special/1008/partner/12_t/>
* 迷惑メール(スパムメール)対策(トレンドマイクロ) 【LEVEL1】【詳細】
  + <http://jp.trendmicro.com/jp/threat/solution/detail/spam/index.html>
  + セキュリティ情報 ポータル　へ　リダイレクト
    - <http://www.trendmicro.co.jp/jp/security-intelligence/index.html>
* 受信トレイにスパムを受信しないようにする(マイクロソフト) 【LEVEL1】【詳細】
  + <http://www.microsoft.com/ja-jp/security/online-privacy/spam-prevent.aspx>
  + オンラインでのプライバシーとセーフティ内
* 迷惑メールのリスクを軽減する(マカフィー) 【LEVEL1】【詳細】
  + <http://home.mcafee.com/advicecenter/Default.aspx?id=ad_spam_rsr>
* デマ メールの受信を避ける方法(マカフィー) 【LEVEL1】【詳細】
  + <http://home.mcafee.com/advicecenter/Default.aspx?id=ad_spam_htarhe>
* 迷惑メールから未成年を保護(マカフィー) 【LEVEL1】【詳細】
  + <http://home.mcafee.com/advicecenter/Default.aspx?id=ad_fis_pytas>
* スパムよスパム、とんでいけ(シマンテック) 【LEVEL1】【詳細】
  + <http://jp.norton.com/spam-spam-go-away/article>

### ガイドライン等

* 公的機関
  + 【●】国家公務員のソーシャルメディアの私的利用に当たっての留意点(総務省) 【LEVEL1】【詳細】【スライド】
    - <http://www.soumu.go.jp/main_content/000235662.pdf>
  + 改正公職選挙法（インターネット選挙運動解禁）ガイドライン(総務省/インターネット選挙運動等に関する各党協議会) 【LEVEL1】【詳細】【冊子】
    - <http://www.soumu.go.jp/main_content/000222706.pdf>
  + 【×】サイバーセキュリティ2014（案）(内閣官房情報セキュリティセンター)
    - <http://www.nisc.go.jp/conference/seisaku/dai39/pdf/39shiryou0502.pdf>
    - ⇒最新版
    - 【●j】重要インフラの情報セキュリティ対策に係る第３次行動計画の見直しに向けたロードマップ（案）【LEVEL1】【詳細】【冊子】
      * <http://www.nisc.go.jp/conference/cs/dai07/pdf/07shiryou02.pdf>
  + 地方公共団体における情報システムセキュリティ要求仕様モデルプラン(地方自治情報センター) 【LEVEL1】【詳細】【ポータル】
    - 【×】　<http://www.lasdec.or.jp/cms/12,28369,84.html>
    - <https://www.j-lis.go.jp/lasdec-archive/cms/12,28369,84.html>
* 教育機関向け
  + 教育分野におけるクラウド導入に対応する情報セキュリティに関する手続きガイドブック(総務省) 【LEVEL1】【詳細】【冊子】
    - <http://www.soumu.go.jp/main_content/000417633.pdf>
  + 教育分野におけるICT利活用推進のための情報通信技術面に関するガイドライン（手引書）2013 小学校版(総務省) 【LEVEL1】【詳細】【冊子】
    - <http://www.soumu.go.jp/main_content/000218505.pdf>
  + 教育分野におけるICT利活用推進のための情報通信技術面に関するガイドライン（手引書）2013 中学校・特別支援学校版(総務省) 【LEVEL1】【詳細】【冊子】
    - <http://www.soumu.go.jp/main_content/000218507.pdf>
  + 大学における営業秘密管理指針作成のためのガイドライン(経済産業省) 【LEVEL1】【詳細】【冊子】【平成16年】
    - 【×】<http://www.meti.go.jp/press/20110331002/20110331002-2.pdf>
    - <http://www.meti.go.jp/policy/innovation_corp/tlo2/0600608himitu-sisin.pdf>
* 個人ユーザー向け
  + インターネットバンキングの不正送金にあわないためのガイドライン(フィッシング対策協議会) 【LEVEL1】【詳細】【冊子】
    - <https://www.antiphishing.jp/report/pdf/internetbanking_guideline.pdf>
  + 【●】フィッシング対策ガイドライン 2016 年度版(フィッシング対策協議会) 【LEVEL2】【詳細】【冊子】【最新版】
    - <http://www.antiphishing.jp/report/pdf/antiphishing_guide.pdf>
  + 【●】利用者向けフィッシング詐欺対策ガイドライン(フィッシング対策協議会) 【LEVEL1】【詳細】【冊子】【最新版】
    - <http://www.antiphishing.jp/report/pdf/consumer_antiphishing_guideline.pdf>
  + スマートフォンの安全な利活用のすすめ～スマートフォン利用ガイドライン～(JNSA) 【LEVEL2】【詳細】【冊子】【最新版】
    - <http://www.jnsa.org/result/2012/surv_smap.html>
      * <http://www.jnsa.org/result/2012/smap_guideline_v1.0.pdf>
  + 【×】オンラインゲームガイドライン（JOGA）【都庁環境で閲覧できず】
    - <http://www.japanonlinegame.org/pdf/JOGAonlinegameguideline.pdf>
  + 【×】スマートフォンゲームアプリケーション運用ガイドライン（JOGA）
    - <http://www.japanonlinegame.org/pdf/JOGA130405.pdf>
  + インターネット上での取引時における本人なりすましによる不正使用防止のためのガイドライン（日本クレジット協会）【LEVEL1】【詳細】【広報】
    - <http://www.j-credit.or.jp/download/120402_news.pdf>
  + お子様のインターネット利用に関する年齢別ガイドライン（マイクロソフト）【LEVEL1】【詳細】
    - <http://www.microsoft.com/ja-jp/security/family-safety/childsafety-age.aspx>
* 事業者向け
  + 【●】Wi-Fi提供者向け セキュリティ対策の手引き(総務省) 【LEVEL1】【簡易】【冊子】
    - <http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/cmn/wi-fi/Wi-Fi_manual_for_AP.pdf>
  + テレワークセキュリティガイドライン第３版(総務省) 【LEVEL1】【簡易】【冊子】
    - <http://www.soumu.go.jp/main_content/000199491.pdf>
  + 【●】サイバーセキュリティ経営ガイドライン(経済産業省) 【LEVEL1】【詳細】【冊子】
    - <http://www.meti.go.jp/press/2015/12/20151228002/20151228002.html>
  + 【●】事業継続計画策定ガイドライン(経済産業省) 【LEVEL1】【詳細】【冊子】
    - <http://www.meti.go.jp/policy/netsecurity/docs/secgov/2005_JigyoKeizokuKeikakuSakuteiGuideline.pdf>
  + 情報セキュリティ報告書モデルガイドライン(経済産業省) 【LEVEL1】【詳細】【冊子】
    - <http://www.meti.go.jp/policy/netsecurity/docs/secgov/2007_JohoSecurityReportModelRevised.pdf>
  + 【●】情報セキュリティ管理基準（平成２８年改正版）(経済産業省) 【LEVEL1】【詳細】【冊子】
    - <http://www.meti.go.jp/press/2015/03/20160301001/20160301001.html>
  + 個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン(経済産業省) 【LEVEL2】【詳細】【冊子】【平成21年】
    - <http://www.meti.go.jp/policy/it_policy/privacy/kojin_gadelane.htm>
  + 営業秘密管理指針　平成27年1月改訂(経済産業省)
    - <http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/20150128hontai.pdf>
  + 技術流出防止指針(経済産業省) 【LEVEL2】【詳細】【冊子】【平成27年】
    - <http://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html#bousi>
    - 営業秘密　～営業秘密を守り活用する～
      * <http://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html>
      * 営業秘密・秘密情報の管理について知りたい
        + 「秘密情報の保護ハンドブック　～企業価値向上に向けて～」

<http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf>

* + - * 秘密情報の管理のうち、情報セキュリティ面について知りたい
        + 組織における内部不正ガイドライン

企業等の組織内部者の不正行為による情報流出等を防止するための対策を示したガイドラインです。

* + - * + 5分でできる！情報セキュリティポイント学習オンライン版

2種類の企業分野と3種類の職位別の事例をもとにセキュリティ対策を学習するツールです。

* + - * + 5分でできる！自社診断オンライン版

25の質問に回答することで情報セキュリティ対策の現状把握が行えるツールです。

* + - * 技術流出対策について知りたい
      * 各種データ・資料等
  + 情報セキュリティガバナンス導入ガイダンス(経済産業省) 【LEVEL2】【詳細】【冊子】【平成21年】
    - <http://www.meti.go.jp/policy/netsecurity/downloadfiles/securty_gov_guidelines.pdf>
  + アウトソーシングに関する情報セキュリティ対策ガイダンス(経済産業省)
    - <http://www.meti.go.jp/press/20090630007/20090630007-4.pdf>
  + IoT開発におけるセキュリティ設計の手引き（IPA) 【LEVEL3】【詳細】【広報】
    - <http://www.ipa.go.jp/security/iot/iotguide.html>
      * IoT開発におけるセキュリティ設計の手引き（84ページ、3.62MB）【LEVEL3】【詳細】【冊子】
        + <http://www.ipa.go.jp/files/000052459.pdf>
  + 職場の情報セキュリティ管理者のためのスキルアップガイド（IPA) 【LEVEL2】【詳細】【ポータル】【iコンピテンシ・ディクショナリ】
    - <http://www.ipa.go.jp/jinzai/hrd/security/index.html>
  + 情報セキュリティ早期警戒パートナーシップガイドライン(IPA) 【LEVEL2】【詳細】【ポータル】
    - <http://www.ipa.go.jp/security/ciadr/partnership_guide.html>
  + 【●】IT製品の調達におけるセキュリティ要件リスト活用ガイドブック(IPA) 【LEVEL2】【詳細】【冊子】
    - <https://www.ipa.go.jp/files/000038924.pdf>
  + 『標的型メール攻撃』対策に向けたシステム設計ガイド(IPA) 【LEVEL2】【詳細】【ポータル】
    - <http://www.ipa.go.jp/security/vuln/newattack.html>
      * 『高度標的型攻撃』対策に向けたシステム設計ガイド(全130ページ、15.5MB）
        + <http://www.ipa.go.jp/files/000046236.pdf>
      * 『標的型メール攻撃』対策に向けたシステム設計ガイド(全70ページ、5.6MB）
        + <http://www.ipa.go.jp/files/000033897.pdf>
  + セキュリティ担当者のための脆弱性対応ガイド (IPA) 【LEVEL2】【詳細】【ポータル】
    - <http://www.ipa.go.jp/security/fy22/reports/vuln_handling/index.html>
      * セキュリティ担当者のための脆弱性対応ガイド(全22ページ、989KB） 【LEVEL2】【詳細】【冊子】
        + <http://www.ipa.go.jp/files/000011568.pdf>
      * 企業等における脆弱性対策に関する実態調査報告書(全72ページ、977KB） 【LEVEL2】【詳細】【冊子】
        + <http://www.ipa.go.jp/files/000011588.pdf>
      * 組込みソフトウェアを用いた機器におけるセキュリティ（改訂版）(全22ページ、912KB）【LEVEL2】【詳細】【冊子】
        + <http://www.ipa.go.jp/files/000011577.pdf>
  + 組込みシステムのセキュリティへの取組みガイド(IPA) 【LEVEL2】【詳細】【ポータル】
    - <http://www.ipa.go.jp/security/fy22/reports/vuln_handling/index.html>
      * 組込みソフトウェアを用いた機器におけるセキュリティ（改訂版）(全22ページ、912KB）【LEVEL2】【詳細】【冊子】
        + <http://www.ipa.go.jp/files/000011577.pdf>
  + 委託関係における情報セキュリティ対策ガイドライン(IPA) 【LEVEL2】【詳細】【ポータル】
    - <http://www.ipa.go.jp/security/fy20/reports/sme-guide/index.html>
    - 中小企業の情報セキュリティ対策に関する研究会報告書（全28ページ、412KB）
      * <http://www.ipa.go.jp/files/000014020.pdf>
    - 中小企業の情報セキュリティ対策ガイドライン（全8ページ、80KB）
      * <http://www.ipa.go.jp/files/000014017.pdf>
      * 別冊1：委託関係における情報セキュリティ対策ガイドライン（全10ページ、333KB）
        + <http://www.ipa.go.jp/files/000014018.pdf>
      * 別冊2：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（全49ページ、803KB）
        + <http://www.ipa.go.jp/files/000014023.pdf>
      * 別冊3-1：5分でできる自社診断シート（全2ページ、156KB）
        + <http://www.ipa.go.jp/files/000014022.pdf>
      * 別冊3-2：5分でできる！自社診断パンフレット（全8ページ、2.67MB）
        + <http://www.ipa.go.jp/files/000014021.pdf>
  + 生体認証導入・運用のためのガイドライン(IPA) 【LEVEL2】【詳細】【ポータル】
    - <http://www.ipa.go.jp/security/fy18/reports/bio_sec/index.html>
    - 生体認証導入・運用のためのガイドライン（全18ページ、430KB） -【2007年】
      * <http://www.ipa.go.jp/files/000013804.pdf>
    - 生体認証利用のしおり（全12ページ、2.43MB） - 【冊子】
      * <http://www.ipa.go.jp/files/000013803.pdf>
  + 【●】安全なウェブサイト運営にむけて ～ 企業ウェブサイトのための脆弱性対応ガイド ～(IPA) 【LEVEL1】【詳細】【ポータル】
    - <http://www.ipa.go.jp/security/fy24/reports/vuln_handling/index.html>
      * [脆弱性対応ガイド]安全なウェブサイト運営にむけて ～ 企業ウェブサイトのための脆弱性対応ガイド ～
      * [報告書]「情報システム等の脆弱性情報の取扱いに関する研究会」2012年度報告書
      * [ハンドブック]「脆弱性ハンドブック」刊行
      * [ダウンロード]公開資料のダウンロード
  + ウェブサイト運営者のための脆弱性対応ガイド(IPA) 【LEVEL2】【詳細】【ポータル】【2009年】
    - <http://www.ipa.go.jp/security/fy19/reports/vuln_handling/>
  + ウェブサイト構築事業者のための脆弱性対応ガイド(IPA)【2009年】
    - <http://www.ipa.go.jp/security/fy20/reports/vuln_handling/>
  + 【●】組織における内部不正防止ガイドライン(IPA) 【LEVEL1】【詳細】【ポータル】【2015年】
    - <http://www.ipa.go.jp/security/fy24/reports/insider/index.html>
    - 組織における内部不正防止ガイドライン（日本語版） 第3版ガイドライン（日本語版）（PDFファイル） (2.59MB) 【LEVEL1】【詳細】【冊子】
      * <http://www.ipa.go.jp/files/000044615.pdf>
    - 第3版の主な改訂内容ガイドライン（日本語版）（PDFファイル） (293KB)
      * <http://www.ipa.go.jp/files/000044616.pdf>
    - 【●】内部不正チェックシート（日本語版） Ver.2.0内部不正チェックシート（日本語版）（Excelファイル） (33.3KB)
      * <http://www.ipa.go.jp/files/000040902.xlsx>
    - Guidelines for the Prevention of Internal Improprieties in Organizations Ver3.0
      * <http://www.ipa.go.jp/files/000045873.pdf>
    - （組織における内部不正防止ガイドライン 第3版の英語版）ガイドライン（英語版）（PDFファイル） (2.3MB)
      * <http://www.ipa.go.jp/files/000045873.pdf>
    - 内部不正対策ソリューションガイド
      * <http://www.jnsa.org/result/2013/surv_acci/index.html>
  + “セキュアな自動車”に向けて「自動車の情報セキュリティへの取組みガイド」(IPA) 【LEVEL1】【詳細】【ポータル】
    - <http://www.ipa.go.jp/security/fy24/reports/emb_car/index.html>
    - 自動車の情報セキュリティへの取組みガイド（全55ページ、1.74MB） -
      * <http://www.ipa.go.jp/security/fy24/reports/emb_car/documents/car_guide_24.pdf>
    - 2012年度 自動車の情報セキュリティ動向に関する調査 報告書（全28ページ、1.23MB） -
      * <http://www.ipa.go.jp/security/fy24/reports/emb_car/documents/car_report_24.pdf>
  + 【●】中小企業における組織的な情報セキュリティガイドライン(IPA) 【LEVEL1】【詳細】
    - <http://www.ipa.go.jp/security/manager/know/sme-guide/sme-security_guidline.html>
    - 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[1,090KB]
      * <http://www.ipa.go.jp/files/000014950.pdf>
  + 高度サイバー攻撃(APT)への備えと対応ガイド～企業や組織に薦める一連のプロセスについて(JPCERT/CC) 【LEVEL3】【詳細】【2016年】
    - <http://www.jpcert.or.jp/research/apt-guide.html>
    - <http://www.jpcert.or.jp/research/20160331-APTguide.pdf>
  + エンタープライズロール特権ID管理解説書（第1版）(JNSA) 【LEVEL3】【詳細】【2016年】
    - <http://www.jnsa.org/result/2016/idm_pum/index.html>
  + エンタープライズロール管理解説書（第3版）(JNSA) 【LEVEL3】【詳細】【2016年】
    - <http://www.jnsa.org/result/2016/idm_guideline/index.html>
  + 内部不正対策ソリューションガイド(JNSA) 【LEVEL3】【詳細】【2014年】
    - <http://www.jnsa.org/result/2013/surv_acci/index.html>
    - <http://www.jnsa.org/result/2013/surv_acci/naibufusei_solguide.pdf>

## 教育・学習

### 一般向け

* http://www.ipa.go.jp/security/kokokara/study/index.html
* 初めてのスマホ特集
  + マンガで学ぶサイバーセキュリティ（NISC) 【LEVEL1】【冊子】
    - <http://www.nisc.go.jp/security-site/files/CSmanga_JPN.pdf>
  + 【●】スマートフォン利用者の方へ（内閣サイバーセキュリティセンター）【LEVEL1】【簡易】【ポータル】
    - <http://www.nisc.go.jp/security-site/smartphone/index.html>
  + モバイル通信利用上の注意（総務省）【LEVEL1】【簡易】【ポータル】【子ども向け】
    - <http://www.soumu.go.jp/joho_tsusin/kids/mobile/caution/index.html>
  + キミはどっち？ -パソコン・ケータイ・スマートフォン 正しい使い方-（IPA)【都庁で閲覧できず】
    - <http://www.youtube.com/watch?v=k2VT6x4wBSk>
  + 大丈夫？あなたのスマートフォン -安心・安全のためのセキュリティ対策-（IPA) 【都庁で閲覧できず】
    - <https://www.youtube.com/watch?v=AhiUC7X3VSg>
  + あなたの書き込みは世界中から見られてる -適切なSNS利用の心得-（IPA) 【都庁で閲覧できず】
    - <https://www.youtube.com/watch?v=tVZSuGkmnGQ>
  + Iラブスマホ生活～レイとランのスマホ事情～（IPA）【LEVEL0】【詳細】【ポータル】【マンガ】
    - <http://www.ipa.go.jp/security/keihatsu/love_smartphone_life/comics/index.html>
  + ケータイ・インターネットの歩き方1「入門編」別添「スマートフォン編」（EMA）【LEVEL0】【詳細】【ポータル】【マンガ】
    - <http://ema-edu.jp/howtowalk01/text_sp.html>
  + スマホを狙う不正アプリの最新事情（トレンドマイクロ）【LEVEL1】【詳細】
    - <http://www.is702.jp/special/1938/partner/12_t/>
  + ひろしとアカリのセキュリティ事情「スマホアプリ導入時は公式マーケットを利用しよう」（トレンドマイクロ）【LEVEL1】【詳細】
    - <http://www.is702.jp/manga/1919/partner/12_t/>
      * 【●】4コマ漫画一覧【LEVEL0】【簡易】
        + <http://www.is702.jp/manga/list/partner/12_t/>
  + 小・中学生向け インターネットあんしんガイド【スマホ＆タブレット編】（トレンドマイクロ）【LEVEL0】【詳細】
    - <http://is702.jp/download/partner/12_t/?cm_mmc=Corp-_-DL-_-702>
      * 登録により各種資料ダウンロード可
  + スマホからの情報漏洩に気をつけて！（トレンドマイクロ）【LEVEL1】【詳細】
    - <http://is702.jp/special/1301/partner/12_t/>
  + LINEのセキュリティ新機能を知っていますか？　楽しく、利用するための5つのヒント（トレンドマイクロ）【LEVEL1】【詳細】
    - <http://www.is702.jp/special/1679/partner/12_t/?cm_re=article-_-threat-_-is702&_ga=1.75813781.1038327157.1416213751>
  + フォロワー数を増やせます!?～TwitterやFacebookユーザを狙う詐欺サイトに注意～（トレンドマイクロ）【LEVEL1】【簡易】
    - <http://is702.jp/column/1473/partner/12_t/?cm_re=article-_-threat-_-is702>
  + SNSでのやりとりがストレスに！？インターネット上のつながりを見直して、安全、快適なコミュニケーションを（トレンドマイクロ）【LEVEL1】【詳細】
    - <http://is702.jp/special/1372/partner/12_t/>
  + 4つのポイントでセキュリティを強化！ LINEとの上手な付き合い方（トレンドマイクロ）【LEVEL1】【簡易】【2013年】
    - <http://is702.jp/special/1332/partner/12_t/>
  + 無防備な無料Wi-Fiに迫るセキュリティの脅威（マカフィー）
    - <http://www.mcafee.com/japan/home/security/news/default.asp>
    - セキュリティニュースコラム【RSS】
* 小学生向け
  + キッズ・パトロール（警察庁）
  + これだけはやっておきたい3つの情報（じょうほう）セキュリティ対策（たいさく）（総務省）
  + 犯罪（はんざい）に注意しよう（総務省）
  + マナーを守って使おう（総務省）
  + SNS（エスエヌエス）を使うときの注意（総務省）
  + モバイル通信利用上の注意（総務省）
  + キミはどっち？ -パソコン・ケータイ・スマートフォン 正しい使い方-【動画】（IPA)
  + ケータイ・インターネットの歩き方～子どもが安心・安全につかうために～（EMA）
  + インターネットをあんぜんにたのしく使おう（シマンテック）
  + 小・中学生向け インターネットあんしんガイド【スマホ＆タブレット編】（トレンドマイクロ）
  + ～あんしんセキュリティ教室～ 親子で学ぶセキュリティ！（トレンドマイクロ）
  + トレンド教授のパソコン安心授業（トレンドマイクロ）
  + インターネット安全教室（マイクロソフト）
  + トラブル対策編 迷惑メール いらないよっ！（ヤフー！きっず）
  + マナー基礎編 カメラでとっちゃえ！（ヤフー！きっず）
* 中高生向け
  + 出会い系サイトへのアクセスは絶対にNO!（警察庁）
  + ココロノスキマ（警察庁）
  + アクセスの代償～あなたの知らないネットの裏側～（警察庁）
  + @policeセキュリティ講座（警察庁）
  + 出会い系サイトは絶対にNO!興味本位のそのサイト、犯罪被害への第一歩（警察庁）
  + そのサイト、誰かがあなたを狙ってる!（警察庁）
  + どんな危険があるの？(総務省)
  + インターネットの安全な歩き方(総務省)
  + オンラインゲームの注意点（総務省）
  + マンガで学ぶサイバーセキュリティ（NISC)
  + iPhone人気に便乗していると考えられる手口にご注意を（IPA)
  + その秘密の質問の答えは第三者に推測されてしまうかもしれません（IPA)
  + チョコっとプラスパスワード（IPA)
  + 「個人間でやりとりする写真や動画もネットに公開しているという認識を！」～スマートフォンの不正アプリによる性的脅迫被害に注意～（IPA)
  + オンラインゲームを楽しむ前にチェックしておきたい３つのセキュリティポイント（IPA)
  + Iラブスマホ生活～レイとランのスマホ事情～（IPA）
  + ケータイ・インターネットの歩き方1「入門編」別添「スマートフォン編」（EMA）
  + ケータイ・インターネットの歩き方3「著作権編」ショート・ビデオ集 （EMA）
  + ケータイ・インターネットの歩き方5「情報発信の仕方編」（EMA）
  + ケータイの使い方について一緒に考えよう（EMA）
  + 斉羽（さいば）家のセキュライフ！更新プログラムで PC を安全に!（マイクロソフト）
  + 10万円以上の被害も！ スマホの「ワンクリック詐欺」、実情が明らかに（マカフィー）
  + 危険が増大！ネット上の音楽や動画（マカフィー）
  + 要注意！FacebookやTwitterに届く"怪しい"メッセージ（マカフィー）
  + オンラインゲームに仕掛けられた悪質なワナ（マカフィー）
  + ひろしとアカリのセキュリティ事情「アカウントリスト攻撃ってなに？」（トレンドマイクロ）
  + スマホを狙う不正アプリの最新事情（トレンドマイクロ）
  + ひろしとアカリのセキュリティ事情「スマホアプリ導入時は公式マーケットを利用しよう」（トレンドマイクロ）
  + ひろしとアカリのセキュリティ事情「うまい話には・・・」（トレンドマイクロ）
  + あなたの情報が盗み見られる！？公衆Wi-Fiを利用する時に知っておくべき３つのこと（トレンドマイクロ）
  + オンラインゲームを安全に楽しむための５つのポイント（トレンドマイクロ）
  + 無断コピーや勝手な投稿がトラブルの火種に！？　インターネット上でトラブルを避ける3つのポイント（トレンドマイクロ）
  + 小・中学生向け インターネットあんしんガイド【スマホ＆タブレット編】（トレンドマイクロ）
  + 実録!あたなのパソコンが盗み見られる！！（トレンドマイクロ）
  + トレンド教授のパソコン安心授業（トレンドマイクロ）
  + スマホからの情報漏洩に気をつけて！（トレンドマイクロ）
  + 知っておきたい!!セキュリティの話（シマンテック）
  + SNS利用上の注意
    - SNS（エスエヌエス）を使うときの注意（総務省）
    - SNS利用上の注意点（総務省）
    - SNSやプロフでのいじめ（総務省）
    - SNSなどへの写真掲載による意図しない利用者情報の流出（総務省）
    - 「SNSの友達申請に注意！」～Facebookで乗っ取り被害に遭わないために～（IPA）
    - SNSにおけるサービス連携に注意！ 」～あなたの名前で勝手に使われてしまいます～（IPA）
    - SNSにひそむワナ！（IPA）
    - ソーシャルメディアとうまくつきあおう！！（EMA）
    - ひろしとアカリのセキュリティ事情「Facebookのタグ付け設定を承認制にしよう」（トレンドマイクロ）
    - ひろしとアカリのセキュリティ事情「SNS、友人リクエストの承認は慎重に」（トレンドマイクロ）
    - あなたの顔写真がネット掲示板に！？ネットで情報を公開し過ぎることに要注意（トレンドマイクロ）
    - ひろしとアカリのセキュリティ事情「日頃のツケ」（トレンドマイクロ）
    - LINEのセキュリティ新機能を知っていますか？　楽しく、利用するための5つのヒント（トレンドマイクロ）
    - フォロワー数を増やせます!?～TwitterやFacebookユーザを狙う詐欺サイトに注意～（トレンドマイクロ）
    - SNSでのやりとりがストレスに！？インターネット上のつながりを見直して、安全、快適なコミュニケーションを（トレンドマイクロ）
    - 4つのポイントでセキュリティを強化！ LINEとの上手な付き合い方（トレンドマイクロ）
    - 人気アプリ、LINEを安全に利用するために（トレンドマイクロ）
    - Facebookユーザもターゲットに　危険なメッセージから身を守る4つのポイント（トレンドマイクロ）
    - 安易な利用がトラブルに発展！？　SNSに潜む危険な罠（トレンドマイクロ）
    - 今だから知っておきたい Twitter、Facebookのマナー入門（トレンドマイクロ）
    - 気軽なコミュニケーションには、こんな落とし穴が！？　覚えておきたい、SNSのマナーとリスク（トレンドマイクロ）
    - あなたのLINEが乗っ取られたら!? 安心して使うための予備知識（マカフィー）
    - 出来心がトラブルに！ SNSの「炎上」を防ぐには（マカフィー）
    - 子供の「LINE」利用。親子で話し合ってルールを決めよう！ （マカフィー）
    - 要注意！ FacebookやTwitterに届く “怪しい”メッセージ （マカフィー）
    - TwitterやFacebookで共有される短縮URL･･･そのリンク先は安全？（マカフィー）
    - 狙われているFacebook「フェイスブック」の個人情報～ユーザー急増により高まるリスク～（マカフィー）
    - Facebookで簡単に検索されてしまう、あなたの個人情報（マカフィー）

### ホームユーザ向け

* ●基本を学ぶ
  + 青少年のインターネット利用環境づくりハンドブック(内閣府) 【LEVEL1】【詳細】【冊子】【要申込み】
    - <http://www8.cao.go.jp/youth/youth-harm/koho/handbook/index.html>
  + どんな危険があるの？(総務省) 【LEVEL1】【詳細】【ポータル】
    - <http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/risk/index.html>
    - 「国民のための情報セキュリティサイト」「基礎知識」内
  + インターネットの安全な歩き方(総務省) 【LEVEL1】【詳細】【ポータル】
    - <http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/privacy/index.html>
    - 「国民のための情報セキュリティサイト」「基礎知識」内
  + スマートフォン利用者の方へ（内閣サイバーセキュリティセンター）【LEVEL1】【詳細】【ポータル】
    - <http://www.nisc.go.jp/security-site/smartphone/index.html>
    - 「みんなでしっかりサイバーセキュリティ」内
  + ワンクリック請求の被害に備えシステム保護の設定を（IPA) 【LEVEL1】【詳細】【広報】
    - <http://www.ipa.go.jp/security/txt/2015/10outline.html>
  + iPhone人気に便乗していると考えられる手口にご注意を（IPA) 【LEVEL1】【詳細】【広報】【事例】
    - <http://www.ipa.go.jp/security/txt/2015/09outline.html>
    - （1）相談事例1（iPhoneがもらえるというメッセージが表示された）
    - （2）相談事例2（ウイルスに感染しているという警告が表示された）
  + その秘密の質問の答えは第三者に推測されてしまうかもしれません（IPA) 【LEVEL1】【詳細】【広報】
    - <http://www.ipa.go.jp/security/txt/2015/07outline.html>
  + 「利便性 となり合わせの 危険性」(IPA)
    - <http://www.ipa.go.jp/security/txt/2015/01outline.html>
    - （1）スマートフォンのセキュリティ事案
    - （2）クラウドサービスのセキュリティ事案
    - （3）インターネットバンキングのセキュリティ事案
    - （4）日頃から意識したいセキュリティ対策
      * スマートフォンに関する被害を防ぐために
      * クラウドサービスからの思わぬ情報漏えい被害を防ぐために
      * インターネットバンキングの不正送金被害やウイルス感染を防ぐために
  + メールの添付ファイルの取り扱い 5つの心得（IPA)【2005年】
    - <http://www.ipa.go.jp/security/antivirus/attach5.html>
  + Winnyによる情報漏えいを防止するために（IPA) 【LEVEL2】【詳細】【2011年】
    - <http://www.ipa.go.jp/security/topics/20060310_winny.html>
  + 【●】不正アプリの被害に遭わないように（IPA）【LEVEL1】【詳細】【2013年】【ポータル】
    - 夏休みにおける情報セキュリティに関する注意喚起
    - <http://www.ipa.go.jp/security/topics/alert250807.html>
    - 1．システム管理を担当されている方へ～ 夏休みなどの長期休暇前の対策について ～
    - 2．企業でパソコンを利用される方へ～ 長期休暇明け等の対応について ～
    - 3．ご家庭でパソコンを利用される方へ～ ウイルス感染やワンクリック請求の被害等に遭わないように ～
    - 4．スマートフォン、タブレットを利用される方へ～ 不正アプリの被害に遭わないように ～
  + 電子メールソフトのセキュリティ設定について(JPCERT/CC) 【LEVEL1】【詳細】【2011年】
    - <https://www.jpcert.or.jp/magazine/security/mail/index.html>
  + 知っておきたい!!セキュリティの話（シマンテック）【LEVEL2】【詳細】【ポータル】
    - <http://jp.norton.com/portal-security/promo>
  + 個人情報の窃取について：入門編（シマンテック）
  + お子様にオンライン セキュリティの基本を教える（マイクロソフト）
  + お子様のインターネット利用に関する年齢別ガイドライン（マイクロソフト）
  + スマートフォンやタブレット、もっと快適に使おう！～基礎編～（マカフィー）
  + 油断大敵！ 詐欺・迷惑電話につけ込まれないためのキホン（マカフィー）
  + 改めて見直そう！個人情報　流出「させない」「してしまったら」（マカフィー）
  + 捨てたパソコンやデバイスから個人情報が流出!?（マカフィー）
  + 知っておきたい、Windows 8 の安全性を活かす8つのヒント！（マカフィー）
  + 待望のスマホやタブレットを安全に楽しもう！（マカフィー）
  + ひろしとアカリのセキュリティ事情「スマホアプリ導入時は公式マーケットを利用しよう」（トレンドマイクロ）
  + ひろしとアカリのセキュリティ事情「OSやソフトのサポート期限を確認しよう」（トレンドマイクロ）
  + Windows 10を安全に使うためのヒント（トレンドマイクロ）
  + ひろしとアカリのセキュリティ事情「鉄壁の守り」（トレンドマイクロ）
  + 初心者の安全ネット利用の心得３カ条（トレンドマイクロ）
  + ひろしとアカリのセキュリティ事情「のれんに腕押し」（トレンドマイクロ）
  + ひろしとアカリのセキュリティ事情「案の定・・・」（トレンドマイクロ）
  + ひろしとアカリのセキュリティ事情「うまい話には・・・」（トレンドマイクロ）
  + ひろしとアカリのセキュリティ事情「かわいいのがお好き」（トレンドマイクロ）
  + ひろしとアカリのセキュリティ事情「その場しのぎ」（トレンドマイクロ）
  + ひろしとアカリのセキュリティ事情「今流行りの」（トレンドマイクロ）
  + ひろしとアカリのセキュリティ事情「穴は穴でも」（トレンドマイクロ）
  + 2015年、ネットの脅威はどうなる？　私たちがセキュリティで今年注意すべきこと（トレンドマイクロ）
  + マークのびっくりエピソード ～ネットのふるまい、あなたは大丈夫？～（トレンドマイクロ）
  + 2014年私たちがセキュリティで注意したいこと（トレンドマイクロ）
  + パソコンやスマホの処分後に情報漏えい!?データ消去の基本を知ろう（トレンドマイクロ）
  + 偽セキュリティソフトに感染してしまうのはなぜ？脆弱性対策の必要性を知ろう（トレンドマイクロ）
  + 今さら聞けないセキュリティの基礎用語　5つの重要キーワードをおさらい！（トレンドマイクロ）
  + 「脆弱性」っていったい何だ？そのリスクを理解し、万事に備える（トレンドマイクロ）
  + 実録!あたなのパソコンが盗み見られる！！（トレンドマイクロ）
  + セキュリティ対策の基礎知識（トレンドマイクロ）
  + スマホからの情報漏洩に気をつけて！（トレンドマイクロ）
* ●家族と学ぶ
  + お子様が安全に安心してインターネットを利用するために保護者ができること（政府）
  + 家族で考えようサイバー犯罪対策（警察庁）
  + 書き込みやメールでの誹謗中傷やいじめ（総務省)
  + ケータイ・インターネットの歩き方～子どもが安心・安全につかうために～（EMA）
  + 家族で話そうケータイ・スマホのルール 「フィルタリングサービス」動画（電気通信事業者協会)
  + 親子で,もう決めましたか？ケータイ・スマートフォンのルール。（電気通信事業者協会)
  + 子どものスマートフォン課金トラブルを防ぎましょう（日本オンラインゲーム協会）
  + 家族のためのインターネットセキュリティガイド（シマンテック）
  + ゲーム機のネット利用に落とし穴！？保護者が知っておくべきセキュリティ事情（トレンドマイクロ）
  + 親子で学ぶインターネットのセキュリティ【前篇】（トレンドマイクロ）
  + 親子で学ぶインターネットのセキュリティ【後篇】（トレンドマイクロ）
  + お子様にオンライン セキュリティの基本を教える（マイクロソフト）
  + お子様がより安全にソーシャル Web サイトを使用できる方法（マイクロソフト）
  + インターネット上の有害で誤った情報についてお子様に教えます（マイクロソフト）
  + お子様のオンライン保護: 保護者ができる 4 つの方法（マイクロソフト）
  + 子供の｢LINE｣利用。親子で話し合ってルールを決めよう！（マカフィー）
  + どうする?ネット社会に生きる子供のセキュリティ教育（マカフィー）
  + おとなも再確認しよう！　インターネット利用時の注意
  + 消えた残高～インターネットバンキングに潜む罠～（警察庁)
  + 便利で安全なオンライン手続きのため公的個人認証サービスを利用しましょう！（総務省)
  + 一般利用者が安心して無線LANを利用するために（総務省)
  + マンガで学ぶサイバーセキュリティ（NISC)
  + 「 その警告表示はソフトウェア購入へ誘導されるかも知れません 」IPA)
  + 一般家庭における無線LANのセキュリティに関する注意（IPA)
  + 亜衣のiパスエピソード【フィッシングにはご用心編】（IPA)
  + オンラインバンキングの正しい画面を知って、金銭被害から身を守りましょう！（IPA)
  + “ただ乗り”を するなさせるな 無線LAN（IPA)
  + マンガでわかるフィッシング詐欺対策 5ヶ条（フィッシング対策協議会)
  + ネット選挙で有権者を襲う5つのリスク（JNSA)
  + オンラインゲームガイドライン（JOGA）
  + インターネット上でのクレジットカード情報の管理にご注意ください！（日本クレジット協会）
  + あなたのクレジットカード情報を狙う犯罪行為にご注意ください！（日本クレジット協会）
  + オンラインゲームのトラブルにご注意を（日本クレジット協会）
  + ID・パスワードの使いまわしにご注意（日本クレジット協会）
  + STOP!フィッシング詐欺 フィッシング詐欺って何？(フィッシング対策協議会)
  + オンラインショッピングについて（JCB）
  + インターネット犯罪対策ハンドブック（シマンテック）
  + ひろしとアカリのセキュリティ事情「アカウントリスト攻撃ってなに？」（トレンドマイクロ）
  + 知らぬ間に私生活や行動がダダ漏れ！？話題の“IoT”で注意したい3つのこと（トレンドマイクロ）
  + ひろしとアカリのセキュリティ事情「 捨て身の覚悟」（トレンドマイクロ）
  + ひろしとアカリのセキュリティ事情「 意固地な性格」（トレンドマイクロ）
  + ひろしとアカリのセキュリティ事情「モテ期到来？」（トレンドマイクロ）
  + あなたの情報が盗み見られる！？公衆Wi-Fiを利用する時に知っておくべき３つのこと（トレンドマイクロ）
  + 突然,ネットバンキングの残高がゼロに！？古いパソコンを使い続けるリスクとは（トレンドマイクロ）
  + 家族をサイバー犯罪から守る！一家の大黒柱が知るべきセキュリティ5カ条（トレンドマイクロ）
  + 脆弱性対策は万全？休暇の前に見落としがちなソフトの更新設定をチェック！（トレンドマイクロ）
  + 購入した品物が届かない！？ネット詐欺の最新動向と対策のポイント（トレンドマイクロ）
  + 動画でチェック！いまどきのインターネット脅威とその対策（トレンドマイクロ）
  + ネットバンキングを安心して利用する５つのヒント\_認証情報の漏えいを防ぐのがカギ（トレンドマイクロ）
  + 「偽サイト」の特徴を知り、トラブルを回避しよう（トレンドマイクロ）
  + 動画で見る ネットバンキングの不正送金被害の実態（トレンドマイクロ）
  + オンライン銀行の不正送金被害が急増！アカウント情報を狙う新たな詐欺手口と対策を知ろう（トレンドマイクロ）
  + あなたのメールやSNSが乗っ取られたらどうする？安全なアカウント管理の実践法をマスターしよう！（トレンドマイクロ）
  + インターネット詐欺への備えは万全ですか？だましの最新手口と回避法を覚えよう （トレンドマイクロ）
  + 無断コピーや勝手な投稿がトラブルの火種に！？　インターネット上でトラブルを避ける3つのポイント（トレンドマイクロ）
  + インターネット通話を安全に利用するために（トレンドマイクロ）
  + 無防備では危ない！あなた無線LANは安全ですか？（トレンドマイクロ）
  + ゆりか先生のセキュリティひとくち講座「クレジットカード情報を入力するその前に！注意する 5 つのポイント」（マイクロソフト）
  + あなたも“カモ”に!? 増え続ける偽サイト・フィッシング詐欺 ～前編～（マカフィー）
  + あなたも“カモ”に!? 増え続ける偽サイト・フィッシング詐欺 ～後編～（マカフィー）
  + 10万円以上の被害も！ スマホの「ワンクリック詐欺」、実情が明らかに（マカフィー）
  + 便利だけど危険も!?無線LANの安全な利用法とは（マカフィー）
  + フィッシング対策は万全ですか？（マカフィー）
  + 無防備な無料Wi-Fiに迫るセキュリティの脅威（マカフィー）
  + 自分が加害者にも!? スパムメールの被害を防げ（マカフィー）
  + 年末年始に注意が必要な12のオンライン詐欺（マカフィー）
  + 考えてみよう！ カップル間のデジタルプライバシー（マカフィー)
  + 危険が増大！ネット上の音楽や動画（マカフィー）
  + 要注意！FacebookやTwitterに届く"怪しい"メッセージ（マカフィー）
  + ホリデーシーズンは、携帯、電子メール、Webを標的とした新たな脅威が出現（マカフィー）
  + Facebookで簡単に検索されてしまう、あなたの個人情報（マカフィー）
  + セキュリティとモラルのガイドブック（セキュリティ対策推進協議会）

### 中小企業向け・より大きな企業・組織向け

* <http://www.ipa.go.jp/security/kokokara/study/company.html>
* 特集　新入社員向け
  + @policeセキュリティ講座 パソコンユーザ向け基礎講座・応用講座（警察庁）【LEVEL1】【体系的】
    - <http://www.npa.go.jp/cyberpolice/pc/elearning/index.html>
  + @policeセキュリティ講座 システム/ネットワーク管理者向け基礎講座（警察庁）【LEVEL1】【体系的】
    - <http://www.npa.go.jp/cyberpolice/server/elearning/index.html>
  + 見えない悪意（警察庁）【LEVEL1】【ビデオ】
    - <http://www.npa.go.jp/cyber/video/index.html>
    - 警察庁　サイバー犯罪対策：情報セキュリティ対策ビデオ
  + 【●】「営業秘密」を管理して会社を守り、強くしよう！（経済産業省）【LEVEL0】【冊子】【経営者】
    - <http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/eigyouhimitsupanfu.pdf>
  + そのメール本当に信用してもいいんですか？　-標的型サイバー攻撃メールの手口と対策-（IPA)【都庁で閲覧できず】
    - <https://www.youtube.com/watch?v=duGNXcEEToU>
  + 3つのかばん-新入社員が知るべき情報漏えいの脅威-（IPA) 【都庁で閲覧できず】
    - <https://www.youtube.com/watch?v=FljLaQA-cRU>
  + 【●】5分でできる！情報セキュリティポイント学習（IPA) 【LEVEL0】【チェック】【2012年】
    - <http://www.ipa.go.jp/security/vuln/5mins_point/index.html>
  + 【●】初めての情報セキュリティ対策のしおり（IPA) 【LEVEL0】【詳細】【冊子】【新入社員】
    - <http://www.ipa.go.jp/security/antivirus/documents/09_hazimete.pdf>
  + 【●】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(IPA)　 【LEVEL0】【詳細】【冊子】【中小企業】
    - <http://www.ipa.go.jp/security/keihatsu/shiori/management/01_guidebook.pdf>
  + 【●】情報漏えい対策のしおり 企業（組織）で働くあなたへ７つのポイント!!（IPA) 【LEVEL0】【詳細】【冊子】
    - <http://www.ipa.go.jp/security/antivirus/documents/05_roei.pdf>
  + 新入社員等研修向け情報セキュリティマニュアル Rev2（JPCERT/CC) 【LEVEL1】【詳細】【冊子】
    - <http://www.jpcert.or.jp/magazine/security/newcomer.html>
      * 新入社員等研修向け情報セキュリティマニュアル Rev3
        + <http://www.jpcert.or.jp/magazine/security/newcomer-rev3_20140326.pdf>
  + 従業員一人ひとりが気をつけるべきこと 標的型サイバー攻撃の対策をクイズでチェック（トレンドマイクロ）【LEVEL1】【クイズ】
    - <http://www.is702.jp/special/1931/partner/12_t/>
  + ひろしとアカリのセキュリティ事情「SNSで仕事がらみの投稿は慎重に」（トレンドマイクロ) 【LEVEL0】【簡易】
    - <http://www.is702.jp/manga/1905/partner/12_t/>
  + 社会人として最低限備えたいセキュリティのお作法（トレンドマイクロ）【LEVEL0】【簡易】
    - <http://www.is702.jp/special/1593/partner/12_t/?cm_re=pickupbnr-_-threat-_-is702&_ga=1.208867473.2039373246.1395716218>
  + 私物のスマホやアプリを勝手に仕事で利用していませんか？（トレンドマイクロ) 【LEVEL0】【簡易】
    - <http://www.is702.jp/special/1650/partner/12_t/?cm_re=article-_-threat-_-is702&_ga=1.198511151.1462668070.1409299553>
  + 恐怖のウイルスうっかり感染物語（トレンドマイクロ）【確認できず】【2009年】
    - <http://is702.jp/special/596/>
  + ネット上での“公私のけじめ”とは？（トレンドマイクロ) 【LEVEL0】【簡易】
    - <http://www.is702.jp/special/1823/partner/12_t/?cm_re=article-_-threat-_-is702&_ga=1.182152679.196970070.1431999093>
  + ひろしとアカリのセキュリティ事情「意外な盲点」（トレンドマイクロ) 【LEVEL1】【簡易】
    - <http://www.is702.jp/manga/1778/partner/12_t/?cm_re=article-_-threat-_-is702&_ga=1.81445335.196970070.1431999093>
  + 会社でやってはいけない5つのこと（トレンドマイクロ) 【LEVEL1】【簡易】
    - <http://www.is702.jp/special/1739/partner/12_t/?cm_re=pickupbnr-_-threat-_-is702&_ga=1.75887381.1038327157.1416213751>
  + 危険！パスワードの使い回し（マカフィー）【LEVEL1】【詳細】
    - <http://mcafee.com/japan/home/security/news/019.asp>
* 中小企業向け
  + @policeセキュリティ講座 パソコンユーザ向け基礎講座・応用講座（警察庁）【LEVEL1】【体系的】
    - <http://www.npa.go.jp/cyberpolice/pc/elearning/index.html>
  + @policeセキュリティ講座 システム/ネットワーク管理者向け基礎講座（警察庁）【LEVEL1】【体系的】
    - <http://www.npa.go.jp/cyberpolice/server/elearning/index.html>
  + 見えない悪意（警察庁）【LEVEL1】【ビデオ】
    - <http://www.npa.go.jp/cyber/video/index.html>
    - 警察庁　サイバー犯罪対策：情報セキュリティ対策ビデオ
  + 【●】「営業秘密」を管理して会社を守り、強くしよう！（経済産業省）【LEVEL0】【冊子】【経営者】
    - <http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/eigyouhimitsupanfu.pdf>
  + 組織の情報資産を守れ！ -標的型サイバー攻撃に備えたマネジメント-【都庁で閲覧できず】
    - <https://www.youtube.com/watch?v=qlcIBHlUKd0>
  + 【注意喚起】組織のウイルス感染の早期発見と対応を（IPA) 【LEVEL3】【詳細】
    - <http://www.ipa.go.jp/security/ciadr/vul/20150610-checklog.html>
  + 【●】5分でできる！情報セキュリティポイント学習（IPA) 【LEVEL0】【ダウンロード版】
    - <http://www.ipa.go.jp/security/vuln/5mins_point/index.html>
    - <http://www.ipa.go.jp/security/vuln/5mins_point/105_themes.html>
    - 経営者、管理者、一般社員
  + 小規模企業のための情報セキュリティ対策（IPA)
    - <http://www.ipa.go.jp/security/manager/know/tool/library.html>
      * 【●】中小企業のためのセキュリティツールライブラリ一覧　内
        + <http://www.ipa.go.jp/security/manager/know/tool/library.html>
        + 「現状把握」「対策・立案」「効果測定」「改善・見直し」
        + 「初級」「中級」「上級」
  + 初めての情報セキュリティ対策のしおり（IPA) 【LEVEL1】【冊子体】【容易】【中小】
    - <http://www.ipa.go.jp/security/antivirus/documents/09_hazimete.pdf>
  + 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(IPA)　 【LEVEL1】【冊子体】【容易】【中小】
    - <http://www.ipa.go.jp/security/keihatsu/shiori/management/01_guidebook.pdf>
  + 情報漏えい対策のしおり 企業（組織）で働くあなたへ７つのポイント!!（IPA) 【LEVEL1】【冊子】【詳細】【網羅的】
    - <http://www.ipa.go.jp/security/antivirus/documents/05_roei.pdf>
  + マイナンバー対応のための情報ポータル（企業向け）（JNSA) 【LEVEL1】【ポータル】
    - <http://www.jnsa.org/mynumber/>
  + 出社してから退社するまで中小企業の情報セキュリティ対策実践手引き（JNSA) 【LEVEL2】【チェックシート】
    - <http://www.jnsa.org/result/2010/chusho_security_tebiki_110330.pdf>
  + ひろしとアカリのセキュリティ事情「SNSで仕事がらみの投稿は慎重に」（トレンドマイクロ) 【LEVEL0】【簡易】
    - <http://www.is702.jp/manga/1905/partner/12_t/>
  + 標的型サイバー攻撃の段階的手口を徹底解説 感染の“連鎖”を早期に断ち切る対策とは（トレンドマイクロ) 【LEVEL3】【詳細】
    - <http://www.trendmicro.co.jp/jp/trendpark/apt/201507-01/20150804021316.html>
  + 私物のスマホやアプリを勝手に仕事で利用していませんか？（トレンドマイクロ) 【LEVEL0】【簡易】
    - <http://www.is702.jp/special/1650/partner/12_t/?cm_re=article-_-threat-_-is702&_ga=1.198511151.1462668070.1409299553>
  + 便利なクラウドを安全に利用するコツ（トレンドマイクロ) 【LEVEL1】【詳細】
    - <http://www.is702.jp/special/1524/partner/12_t/>
  + 【●】小規模企業必見！　あなたの会社、セキュリティ対策は大丈夫？（トレンドマイクロ）【LEVEL1】【詳細】【チェックリスト】
    - <http://is702.jp/special/789/>
  + 恐怖のウイルスうっかり感染物語（トレンドマイクロ）【LEVEL1】【詳細】【2009年】
    - <http://is702.jp/special/596/>
  + 【●】経営者必読！企業の個人情報漏えい対策（トレンドマイクロ）【LEVEL1】【詳細】
    - <http://is702.jp/special/291/>
    - 社内のあちらこちらに個人情報が無造作に置かれていませんか？
    - 大企業だけの問題ではない「個人情報漏えい」
    - 自社が保有する個人情報を把握・管理できていますか？
    - 欠かせない、社員の「意識付け」
    - 企業における個人情報漏えい防止策
  + 危険！パスワードの使い回し（マカフィー）【LEVEL1】【詳細】
    - <http://mcafee.com/japan/home/security/news/019.asp>
* 経営者
  + 【●】企業の情報セキュリティ対策（警察庁）【LEVEL0】【パンフレット】【ポータル】
    - <http://www.npa.go.jp/cyber/pamphlet/>
  + 必要な情報セキュリティ対策（総務省）
    - <http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/executive/03.html>
      * 【●】国民のための情報セキュリティ対策ページ　企業・組織の対策【LEVEL0】【詳細】【ポータル】
  + 個人情報取扱事業者の責務（総務省）【LEVEL0】【詳細】
    - <http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/executive/05.html>
  + 情報セキュリティポリシーの導入と運用（総務省）【LEVEL0】【詳細】
    - <http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/admin/12.html>
  + 秘密情報の保護ハンドブック～企業価値向上に向けて～（経済産業省）【LEVEL2】【詳細】【冊子】
    - <http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf>
  + 「営業秘密」を管理して会社を守り、強くしよう！（経済産業省）【LEVEL0】【冊子】【経営者】
    - <http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/eigyouhimitsupanfu.pdf>
  + 営業秘密の不正な持ち出しは犯罪です！（経済産業省）【LEVEL1】【詳細】【PPT】
    - 【×】 <http://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret-hanzai.htm>
    - <http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/slide6-ver_10.pdf>
  + 組織の情報資産を守れ！ -標的型サイバー攻撃に備えたマネジメント-【都庁で閲覧できず】
    - <https://www.youtube.com/watch?v=qlcIBHlUKd0>
  + 職場の情報セキュリティ管理者のためのスキルアップガイド（IPA) 【LEVEL2】【詳細】【ポータル】【iコンピテンシ・ディクショナリ】
    - <http://www.ipa.go.jp/jinzai/hrd/security/index.html>
  + サーバソフトウェアが最新版に更新されにくい現状および対策（IPA) 【LEVEL2】【詳細】【冊子】
    - <http://www.ipa.go.jp/security/technicalwatch/20140425.html>
    - 「サーバソフトウェアが最新版に更新されにくい現状および対策」～中長期的な視点からウェブサイトの組織的な管理を～
      * <http://www.ipa.go.jp/files/000038393.pdf>
      * 1．サーバソフトウェアのバージョン調査
      * 2．組織的なウェブサイト管理のあり方
      * 3．組織的なウェブサイト管理のケーススタディ
  + 経営者・マネジメント層向け「 組織内部の不正行為にはトップダウンで、組織横断の取り組みを 」（IPA) 【LEVEL2】【詳細】【広報】【2014年】
    - <http://www.ipa.go.jp/security/txt/2014/03outline.html>
  + あなたの組織が狙われている！－標的型攻撃 その脅威と対策－ （IPA動画チャンネル)【都庁で確認できず】
    - <http://www.youtube.com/watch?v=NTOF4XcI8j0>
  + 【●】5分でできる！情報セキュリティポイント学習（IPA) 【LEVEL0】【ダウンロード版】
    - <http://www.ipa.go.jp/security/vuln/5mins_point/index.html>
  + 【●】情報セキュリティ読本 四訂版-IT時代の危機管理入門-（IPA) 【LEVEL1】【詳細】【冊子】【2014年】
    - <http://www.ipa.go.jp/security/publications/dokuhon/index.html>
    - 【●】「情報セキュリティ読本　四訂版－IT時代の危機管理入門」教育用スライド資料【LEVEL1】【詳細】【2014年】
      * <http://www.ipa.go.jp/security/publications/dokuhon/ppt.html>
  + 東南アジアの情報セキュリティ －現状と対策について－【動画】（IPA) 【都庁で確認できず】
    - <http://www.youtube.com/watch?v=xdgg_5aZ9hM&list=PLF9FCB56776EBCABB>
  + 今制御システムも狙われている！－情報セキュリティの必要性－【動画】（IPA) 【都庁で確認できず】
    - <http://www.youtube.com/watch?v=NdMs45qBtbA>
  + 【●】イラストでわかるセキュリティ（JPCERT/CC) 【LEVEL0】【イラスト】
    - <http://www.jpcert.or.jp/magazine/security/illust/index.html>
  + CSIRTマテリアル（JPCERT/CC)【LEVEL3】【詳細】
    - <https://www.jpcert.or.jp/csirt_material/>
  + コンピューターセキュリティインシデント対応チーム (CSIRT) のためのハンド ブック（JPCERT/CC)【2003年】
    - <https://www.jpcert.or.jp/research/2007/CSIRT_Handbook.pdf>
  + 【●】情報セキュリティポリシーサンプル改版（1.0版）（JNSA) 【LEVEL1】【詳細】【冊子】
    - <http://www.jnsa.org/result/2016/policy/index.html>
  + マイナンバー対応のための情報ポータル（企業向け）（JNSA)【LEVEL1】【詳細】【ポータル】
    - <http://www.jnsa.org/mynumber/>
  + 話題のセキュリティ問題を考える（JNSA)【LEVEL3】【詳細】
    - <http://www.jnsa.org/secshindan/>
    - 【●】公開資料・報告書をお探しの方【LEVEL3】【詳細】【ポータル】
      * http://www.jnsa.org/result/2016.html
  + スマートフォンの安全な利活用のすすめ（JNSA) 【LEVEL3】【詳細】
    - <http://www.jnsa.org/result/2010/smap_guideline_Beta.pdf>
  + 危険！パスワードの使い回し（マカフィー）【LEVEL1】【詳細】
    - <http://mcafee.com/japan/home/security/news/019.asp>
  + 脆弱性を狙った攻撃の現状と巧妙な手口(シマンテック）【LEVEL1】【詳細】
    - <http://www.symantec.com/ja/jp/page.jsp?id=banking_topic_vol2>
  + 【●】実録：標的型攻撃(シマンテック）【LEVEL1】【詳細】【事例】
    - <http://www.symantec.com/ja/jp/theme.jsp?themeid=apt_casestudy01>
  + 標的型サイバー攻撃の段階的手口を徹底解説 感染の“連鎖”を早期に断ち切る対策とは（トレンドマイクロ) 【LEVEL2】【詳細】
    - <http://www.trendmicro.co.jp/jp/trendpark/apt/201507-01/20150804021316.html>
  + あなたの不用意な行動が組織を危険に！？標的型攻撃の被害に遭わないためにできること（トレンドマイクロ）【LEVEL1】【詳細】
    - <http://is702.jp/special/1430/partner/12_t/>
  + 【●】経営者必読！企業の個人情報漏えい対策（トレンドマイクロ）【LEVEL0】【詳細】
    - 「ウチの会社は大丈夫」と言い切れますか？
    - <http://is702.jp/special/291/>
  + 実録!あなたのパソコンが盗み見られる！！（トレンドマイクロ）【LEVEL0】【ビデオ】
    - <http://is702.jp/special/967/partner/12_t/>
  + ウイルステロ事件真犯人は誰だ!?（トレンドマイクロ）【LEVEL0】【ビデオ】
    - <http://is702.jp/special/770/partner/12_t/>
  + あなたの会社の「ガンブラー対策」は大丈夫？　ガンブラー攻撃が招いた会社存続の危機！（トレンドマイクロ）【LEVEL0】【詳細】
    - <http://is702.jp/special/694/>
  + 環境変化,脅威の変化に伴い求められる組織内のセキュリティ教育とは？（トレンドマイクロ）【LEVEL0】【詳細】
    - <http://is702.jp/special/1241/partner/12_t/>
* 一般社員・職員
  + 見えない悪意（警察庁）【LEVEL1】【ビデオ】【都庁で確認できず】
    - <http://www.npa.go.jp/cyber/video/index.html>
    - 情報セキュリティ対策ビデオ紹介
      * 第１部　「戻れない」アクセス
      * 第２部　ふたり「だけ」の秘密
      * 第３部　「無料」の償い
  + サイバー犯罪事件簿３～NET SPY ネットスパイ～（警察庁）【LEVEL1】【ビデオ】【都庁で確認できず】
    - <http://www.npa.go.jp/cyber/video/index.html>
  + 電子メールの誤送信（総務省) 【LEVEL1】【詳細】
    - <http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/staff/04.html>
    - 「国民のための情報セキュリティサイト」「企業・組織の対策」内
  + バックアップ（総務省）【LEVEL1】【詳細】
    - <http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/staff/07.html>
    - 「国民のための情報セキュリティサイト」「企業・組織の対策」内
  + 外出先で業務用端末を利用する場合の対策（総務省) 【LEVEL1】【詳細】
    - <http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/staff/10.html>
    - 「国民のための情報セキュリティサイト」「企業・組織の対策」内
  + そのメール本当に信用してもいいんですか？　-標的型サイバー攻撃メールの手口と対策-（IPA) 【LEVEL1】【ビデオ】【都庁で確認できず】
    - <https://www.youtube.com/watch?v=duGNXcEEToU>
  + インターネットサービス利用時の情報公開範囲の設定に注意！(IPA) 【LEVEL1】【詳細】【広報】【2013年】
    - <http://www.ipa.go.jp/security/txt/2013/10outline.html>
  + 企業でパソコンを利用される方へ～長期休暇明けの対応について～（IPA) 【LEVEL1】【詳細】【2013年】
    - [http://www.ipa.go.jp/security/topics/alert250807.html#](http://www.ipa.go.jp/security/topics/alert250807.html)
  + 5分でできる！情報セキュリティポイント学習（IPA) 【LEVEL0】【ダウンロード版】
    - <http://www.ipa.go.jp/security/vuln/5mins_point/index.html>
  + 新入社員等研修向け情報セキュリティマニュアル Rev2（JPCERT/CC) 【LEVEL1】【詳細】【冊子】
    - <http://www.jpcert.or.jp/magazine/security/newcomer.html>
  + 電子メールソフトのセキュリティ設定について(JPCERT/CC) 【LEVEL1】【詳細】【2011年】
    - <https://www.jpcert.or.jp/magazine/security/mail/index.html>
  + マイナンバー対応のための情報ポータル（企業向け）（JNSA) 【LEVEL1】【ポータル】
    - <http://www.jnsa.org/mynumber/>
  + 出社してから退社するまで中小企業の情報セキュリティ対策実践手引き 改訂版（JNSA) 【LEVEL2】【チェックシート】
    - <http://www.jnsa.org/result/2013/chusho_sec/data/chusho_security_tebiki_20140331.pdf>
  + ひろしとアカリのセキュリティ事情「SNSで仕事がらみの投稿は慎重に」（トレンドマイクロ) 【LEVEL0】【簡易】
    - <http://www.is702.jp/manga/1905/partner/12_t/>
  + ネット上での“公私のけじめ”とは？（トレンドマイクロ)
  + ひろしとアカリのセキュリティ事情「意外な盲点」（トレンドマイクロ)
  + 会社でやってはいけない5つのこと（トレンドマイクロ)
  + 私物のスマホやアプリを勝手に仕事で利用していませんか？（トレンドマイクロ)
  + 知っておきたい旬のセキュリティキーワードを解説（トレンドマイクロ）
  + 社会人として最低限備えたいセキュリティのお作法（トレンドマイクロ）
  + 実録!あなたのパソコンが盗み見られる！！（トレンドマイクロ）
  + インターネットセキュリティ対策基礎講座（トレンドマイクロ）
  + 知っておきたいWindows7のセキュリティ機能（トレンドマイクロ）
  + 危険！パスワードの使い回し（マカフィー）
  + 捨てたパソコンやデバイスから個人情報が流出!?（マカフィー）
* システム管理者
  + JDWP（Java Debug Wire Protocol）に対する探索行為の検知について（警察庁）
  + @policeセキュリティ講座（警察庁）
  + ユーザ権限とユーザ認証の管理（総務省）
  + クラウドサービスを利用する際の情報セキュリティ対策（総務省）
  + 廃棄するパソコンやメディアからの情報漏洩（総務省）
  + SQLインジェクションへの対策（総務省）
  + 脆弱性診断士（プラットフォーム）スキルマップ＆シラバス（日本セキュリティオペレーション事業者協議会)
  + 職場の情報セキュリティ管理者のためのスキルアップガイド（IPA)
  + 【注意喚起】組織のウイルス感染の早期発見と対応を（IPA)
  + 複合機やウェブカメラ、情報家電などにも適切なアクセス制限を（IPA)
  + 複合機等のオフィス機器をインターネットに接続する際の注意点（IPA)
  + ウェブサイト改ざんの脅威と対策（IPA)
  + ファジング活用の手引き～製品出荷前に機械的に脆弱性をみつけよう～（IPA)
  + ファジング実践資料（テストデータ編）（IPA)
  + 組込み製品の脆弱性対策に～知ってみようファジング～【動画】（IPA)>
  + 組込み製品の脆弱性が及ぼす影響～製品開発企業はどうすれば～【動画】（IPA)
  + JPEG テスト支援ツール iFuzzMaker（IPA)
  + 安全なウェブサイトの作り方改訂第7版（IPA)<
  + ウェブ健康診断仕様 （IPA)
  + 安全なウェブサイトの作り方 セキュリティ実装チェックリスト（IPA)
  + 暗号技術に関するe-Learning教材（IPA)
  + 脆弱性体験学習ツール AppGoat （IPA)
  + サーバソフトウェアが最新版に更新されにくい現状および対策（IPA)
  + 大企業・中堅企業の情報システムのセキュリティ対策～脅威と対策～（IPA)
  + 安全なSQLの呼び出し方 （IPA)
  + 夏休みなどの長期休暇前の対策について（IPA)
  + セキュリティ担当者のための脆弱性対応ガイド （IPA)
  + 情報漏えいを防ぐためのモバイルデバイス等設定マニュアル～安心・安全のための暗号利用法～実践編（IPA)
  + 情報漏えいを防ぐためのモバイルデバイス等設定マニュアル～安心・安全のための暗号利用法～解説編（IPA)
  + 高度サイバー攻撃への対処におけるログの活用と分析方法（JPCERT/CC)
  + 改ざんされたVPNサーバから攻撃ツールScanboxに誘導（JPCERT/CC
  + 情報セキュリティポリシーサンプル改版（1.0版）（JNSA)
  + オープンソースとの付き合い方再考（JNSA)
  + 話題のセキュリティ問題を考える（JNSA)
  + エンタープライズロール管理解説書（第1版）（JNSA)
  + デジタル証明書と暗号への攻撃の実態～ケーススタディによる～（JNSA)
  + スマートフォンの安全な利活用のすすめ（JNSA)
  + 標的型サイバー攻撃の段階的手口を徹底解説 感染の“連鎖”を早期に断ち切る対策とは（トレンドマイクロ)
  + IT担当者向け、ウイルス検出時の対処法（トレンドマイクロ）
  + 便利なクラウドを安全に利用するコツ（トレンドマイクロ)
  + 小規模企業必見！　あなたの会社、セキュリティ対策は大丈夫？（トレンドマイクロ）
  + ソフトの「寿命」はいつまで？「サポート終了」に注意しよう！（トレンドマイクロ）
  + 深刻化する標的型攻撃への対策 (マカフィー）
  + 話題のウイルス解説(マカフィー）
  + 脆弱性を狙った攻撃の現状と巧妙な手口(シマンテック）
  + 人気モバイルデバイスのセキュリティ比較(シマンテック）
  + 「標的型攻撃」に備える(シマンテック）

### OSのアップデート（サポート終了関連情報を含む）

* 平成26年4月のサポート終了後にWindows XPを使用することの危険性（官民ボード実態把握WG質的把握SWG）
* ウィンドウズXP等のサポート終了、複合機等のインターネットへの接続に関する注意喚起（総務省）
* ソフトウェアを最新に保とう（総務省）
* Windows Server 2003のサポート終了に伴う注意喚起（IPA）
* サイバー攻撃の被害回避のため、サポートが終了したXP等Microsoft 製品の移行を（IPA）
* 「あなたのパソコンは4月9日以降、大丈夫？ 」～使用中パソコンの判別方法、乗り換えプランを紹介～（IPA）
* Windows XPのサポート終了に伴う注意喚起（IPA）
* Windows XPのサポートが終了したらどうなるの？（IPA）
* ウイルス対策ソフトが入っていれば、Windows XPのサポートが終了してもウイルス感染は大丈夫？（IPA)
* パソコンはこのままで他のWindowsにバージョンアップ出来るの？（IPA)
* まだ使えるからこのまま使っていたい。（IPA)
* インターネットに繋がなければこのまま使ってても大丈夫？（IPA)
* 「Windows XPのサポート終了」について（IPA)
* Windows XP サポート終了について考える（JNSA)
* 「XP」を使っているなら、今すぐ”応急措置”を！（マカフィー）
* WindowsXP、まもなくサポート終了！（マカフィー）
* 知っておきたい、Windows 8 の安全性を活かす8つのヒント！（マカフィー）
* Windows XP/Office 2003をご利用のお客様へ　サポート終了の重要なお知らせです。（マイクロソフト)
* Windows XPとOffice 2003のサポートが終了します。（マイクロソフト)
* 突然、ネットバンキングの残高がゼロに！？古いパソコンを使い続けるリスクとは（トレンドマイクロ）
* Windows XP サポート終了後のウイルスバスターの対応について（トレンドマイクロ）
* 古いパソコンを使い続けるとどうなるの！？　OSやソフトウェアの「サポート終了」ってどういう意味？ （トレンドマイクロ）
* ソフトの「寿命」はいつまで？　「サポート終了」に注意しよう！（トレンドマイクロ）
* レガシーOSやセキュリティ対策が難しいシステムを守るには？（トレンドマイクロ）
* Windows 8のセキュリティ機能を活用しよう（トレンドマイクロ）

## セキュリティチェック

* <http://www.ipa.go.jp/security/kokokara/quiz/index.html>

### クイズに挑戦

* 小学生向け
  + インターネットものしりクイズ（総務省)
  + モバイル通信ものしりクイズ（総務省)
  + Mr.トレンドのセキュリティクイズ（トレンドマイクロ）
  + クイズにチャレンジ(マカフィー）
* 中高生向け
  + 入門講座 初心者編テスト（警察庁）
  + 基礎講座 メール編テスト・Web編テスト（警察庁）
  + 基礎講座 常時接続編テスト・フィルタリング編テスト（警察庁）
  + 基礎講座 セキュリティ対策編テスト（警察庁）
  + 応用講座 メール編テスト・Web編テスト（警察庁）
  + 応用講座 常時接続編テスト・ID･パスワード編テスト（警察庁）
  + 情報セキュリティ自己診断チェックリスト（NISC)
  + 「STOP. THINK. CONNECT. 立ち止まって、考えて、ネットを楽しむためのクイズ」（STC普及啓発WG事務局)
  + STOP!フィッシング詐欺フィッシング詐欺対策力診断（フィッシング対策協議会)
  + サイバー犯罪についてのクイズ: リスクの評価（シマンテック）
  + そのクリック、大丈夫ですか！？　セキュリティの常識をクイズでチェック！（トレンドマイクロ）
  + あなたのお金が狙われている？！ネット詐欺の手口と対処法をクイズで確認（トレンドマイクロ）
  + セキュリティの常識をクイズで確認！（トレンドマイクロ）
  + セキュリティ常識力検定（トレンドマイクロ）
  + Mr.トレンドのセキュリティクイズ（トレンドマイクロ）
  + 夏休み“スマホの安全”ドリル(マカフィー）
  + クイズにチャレンジ(マカフィー）
* 社会人向け
  + デジタルフォレンジッククイズ（警察庁）
  + 基礎講座 サイバーセキュリティ概論テスト（警察庁）
  + 基礎講座 サーバ構築編テスト（警察庁）
  + 基礎講座 攻撃と侵入への対処編テスト（警察庁）
  + 応用講座 ファイアウォール編テスト（警察庁）
  + クイズで学ぶ情報セキュリティ対策（経済産業省/JNSA）
  + 新入社員等研修向け情報セキュリティクイズ（JPCERT/CC)
  + 情報セキュリティ理解度セルフチェック（JNSA)
  + 従業員一人ひとりが気をつけるべきこと
  + 標的型サイバー攻撃の対策をクイズでチェック
  + （トレンドマイクロ）
  + ＜クイズで判定＞それ\_やってもいいことですか？
  + 新社会人が持つべきセキュリティの心構え
  + （トレンドマイクロ）
  + ビジネスシーンでのセキュリティ意識診断（トレンドマイクロ）
  + ＜クイズで判定＞ あなたのセキュリティレベルは？　インターネット犯罪に巻き込まれないために【前編】（トレンドマイクロ)
  + ＜クイズで判定＞ あなたのセキュリティレベルは？　インターネット犯罪に巻き込まれないために【後編】（トレンドマイクロ）
  + ＜フィッシング詐欺サイト＞ あなたの「だまさレベル」チェック（トレンドマイクロ）
  + 何が「個人情報」？理解度チェック（トレンドマイクロ）

### 安全性を診断しよう

* インターネット利用上（りようじょう）の注意　自己診断（じこしんだん） （総務省)
* モバイル通信（つうしん）利用上（りようじょう）の注意　自己診断（じこしんだん） （総務省)
* 営業秘密管理チェックシート（経済産業省）
* 組織の情報セキュリティ対策自己診断テスト ～ 情報セキュリティ対策ベンチマーク ～（IPA)
* 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（IPA)
* Androidアプリの脆弱性の学習・点検ツール AnCoLe（IPA)
* 5分でできる！情報セキュリティ自社診断（IPA)
* MyJVNバージョンチェッカ（IPA)
* ウェブ健康診断仕様（IPA)
* 「やられたかな？その前に」ガイド・問診票（日本セキュリティオペレーション事業者協議会)
* 制御システムセキュリティ自己評価ツール「J-CLICS」（JPCERT/CC）
* 制御システムセキュリティ自己評価ツール「J-CLICS STEP2」（JPCERT/CC）
* マイナンバーの安全管理措置チェックシート（JNSA)
* パスワードのチェック ? パスワードは強力か?（マイクロソフト）
* セキュリティアセスメントツール（トレンドマイクロ）

### 試験・資格

* ITパスポート試験（IPA)
* 情報セキュリティスペシャリスト試験（IPA)
* ネットワーク情報セキュリティマネージャー（NISM）資格について (TCA)
* 情報セキュリティ教育事業者連絡会（JNSA)
* 情報セキュリティ対策 中小企業向け指導者育成セミナー（JNSA)

## データ＆レポート

* <http://www.ipa.go.jp/security/kokokara/report/index.html>
* 官民ボード
  + スマートフォン利用における脅威とその対策とは（技術調査SWG）
  + MacOSにもウイルス対策が必要(官民ボード 質的把握SWG)
  + IDやパスワードを使い回すことの危険性(官民ボード 質的把握SWG)
  + 「脆弱性情報を適切に共有するために」
  + 脆弱性情報を受付けし関係者にお知らせする制度について　（不正アクセス行為防止WGセキュリティ･ホール攻撃対策の取組SWG）
  + 「脆弱性の対策には」
  + 脆弱性対策に関する情報や対策に関するアドバイス（不正アクセス行為防止WGセキュリティ･ホール攻撃対策の取組SWG）
  + 「情報システムの技術的なセキュリティ対策」
  + 情報システムに対する技術的なセキュリティ対策について（不正アクセス行為防止WGセキュリティ･ホール攻撃対策の取組SWG）
* 警察庁
  + 平成２７年おける出会い系サイト及びコミュニティサイトに起因する事犯の現状と対策について
  + 平成２７年における不正アクセス行為の発生状況等の公表について
  + Microsoft SQL Server を標的とするアクセスの増加について
  + 平成２７年上半期の出会い系サイト及びコミュニティサイトに起因する事犯の現状と対策について
  + 平成２６年中の出会い系サイト及びコミュニティサイトに起因する事犯の現状と対策について
  + 産業制御システムで使用されるPLCの脆弱性を標的としたアクセスの観測について
  + 平成２７年中のサイバー空間をめぐる脅威の情勢について
  + 携帯電話販売店に対するフィルタリング推奨状況等実態調査
  + Bash の脆弱性を標的としたアクセスの観測について（第３報）
  + 金融機関等のフィッシングサイトの増加について
  + 不正アクセス行為対策等の実態調査調査報告書
  + 平成２７年中のインターネットバンキングに係る不正送金事犯の発生状況等について
  + インターネット観測結果等
  + インターネット定点観測
  + 警察白書
* 総務省
  + ウェブサービスに関するID・パスワードの管理・運用実態調査結果
  + スマートフォン安心安全強化戦略の概要
  + 平成２７年度青少年のインターネット・リテラシー指標等
  + 青少年のインターネット利用と依存傾向に関する調査結果報告書
  + ICT成長戦略～ICTによる経済成長と国際社会への貢献～
  + 世界最先端IT 国家創造宣言
  + パーソナルデータの利用・流通に関する研究会\_報告書
  + 情報通信白書
  + グリッド関連サービスにおけるプライバシー・個人情報保護に関する調査研究報告書
* 経済産業省
  + 平成２７年度「情報セキュリティ監査企業台帳（2015.10.8版）」
  + 平成２７年度「システム監査企業台帳（2015.10.8版）」
  + 模倣品・海賊版対策の総合窓口に関する年次報告（２０１５年版）
  + 不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況
  + 人材を通じた技術流出に関する調査研究 報告書
  + 情報処理実態調査
  + 「営業秘密の管理実態に関するアンケート調査」結果概要（速報版）
  + 経産省の情報セキュリティ対策,情報セキュリティ人材が担う役割,ITパスポート試験 等
  + 近事の技術流出事例への対処と技術流出の実態調査について
* 内閣サイバーセキュリティセンター（NISC）
  + サイバーセキュリティ戦略
  + 第６回「日・ASEAN情報セキュリティ政策会議」の結果
  + 情報セキュリティ政策会議：政府の情報セキュリティ予算について
  + 情報セキュリティ人材の必要性について
* NICT
  + nicterWeb ～サイバー攻撃の観測情報～
  + 次世代暗号≪ペアリング暗号≫－世界記録と安全性－
  + 次世代暗号≪ペアリング暗号≫－実用化に向けて－
* IPA
  + 企業のCISOやCSIRTに関する実態調査2016
  + 営業秘密管理・保護システムに関するセキュリティ要件調査
  + 内部不正による情報セキュリティインシデント実態調査
  + 情報セキュリティ人材の育成に関する基礎調査
  + 標的型サイバー攻撃の事例分析と対策レポート
  + IPAテクニカルウォッチ「標的型攻撃メールの例と見分け方」
  + 情報セキュリティ技術動向調査
  + デジタル複合機のセキュリティに関する調査報告書
  + オンライン本人認証方式の実態調査
  + 重要インフラのサイバーセキュリティを向上させるためのフレームワーク
  + 自動車や家電など製品のセーフティ設計・セキュリティ設計に関する実態調査結果
  + 「暗号利用環境に関する動向調査」報告書
  + 「医療機器における情報セキュリティに関する調査」報告書
  + 攻撃者に狙われる設計・運用上の弱点についてのレポート
  + 「２０１５年度中小企業における情報セキュリティ対策に関する実態調査」報告書>
  + 「情報セキュリティ10大脅威 2015」
  + ２０１４年度情報セキュリティ事象被害状況調査\_報告書
  + 「２０１４年度情報セキュリティの倫理に対する意識調査」報告書
  + 「２０１４年度情報セキュリティの脅威に対する意識調査」報告書
  + コンピュータウイルス・不正アクセスの届出状況および相談状況 [2015年第2四半期（4月～6月）］
  + ソフトウェア等の脆弱性関連情報に関する届出状況 [2015年第2四半期（4月～6月）]
  + 不正アクセス被害の届出状況について
  + 情報セキュリティ白書2015
  + IPA テクニカルウォッチ「ウェブサイトにおける脆弱性検査手法の紹介（ウェブアプリケーション検査編）
  + IPA テクニカルウォッチ 脆弱性を悪用する攻撃への効果的な対策についてのレポート
  + 脆弱性検査と脆弱性対策に関するレポート
  + 脆弱性対策情報データベース
  + 脆弱性を利用した新たなる脅威に関する調査(報告書)

## （情報セキュリティ　FAQ）

* <https://www.ipa.go.jp/security/faq/faq.html>
* 【注意喚起】ワンクリック請求に関する相談急増！パソコン利用者にとっての対策は、まずは手口を知ることから！
  + <https://www.ipa.go.jp/security/topics/alert20080909.html>

# 参考サイト

## 中小企業経営者向け

* 情報セキュリティ上の脅威が事業経営に与える影響：事例：情報システム関連の事件・事故
  + <http://www.ipa.go.jp/security/manager/know/meaning/sample.html>
* 中小企業向け情報セキュリティ対策
  + 5分でできる！自社診断シート・パンフレット
  + 自社診断シート
    - <http://www.ipa.go.jp/files/000027129.pdf>
  + 自社診断パンフレット
    - <http://www.ipa.go.jp/files/000027130.pdf>
* 情報セキュリティ対策のしおり
  + <http://www.ipa.go.jp/security/antivirus/shiori.html>
    - 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
      * <https://www.ipa.go.jp/security/keihatsu/shiori/management/02_checklist.pdf>
    - 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
      * <https://www.ipa.go.jp/security/keihatsu/shiori/management/03_casestudy.pdf>
    - クラウドサービス安全利用のすすめ（～中小企業のみなさん　自社のIT環境の改善のためにクラウドサービスの導入を検討するときは、安全についての確認もしっかり実施しましょう！～）（2011年11月）【LEVEL0】【冊子体】【中小】
      * <https://www.ipa.go.jp/security/cloud/cloud_tebiki_handbook_V1.pdf>
* 「2015年度 中小企業における情報セキュリティ対策に関する実態調査」報告書について
  + <https://www.ipa.go.jp/security/fy27/reports/sme/>

## IoT開発におけるセキュリティ設計の手引き

* <https://www.ipa.go.jp/files/000052459.pdf>
* IoTは、中小企業においても大きなビジネスチャンスであり、先行して取り組むことが期待される
* 開発段階での対応
  + 新たに脆弱性を作り込まないこと
    - セキュアプログラミング技術の適用やコーディング規約の利用によって、新たな脆弱性を作り込まないようにする。ハードウェアに生じる脆弱性の対策（例えば、物理的な攻撃への対策）も考慮する
  + 既知の脆弱性を解消すること
    - 既知の脆弱性が存在しないか確認する。この際には、IPAが提供する脆弱性対策情報データベース「JVN-iPedia」の活用も可能
  + 残留している脆弱性を検出・解消すること
    - 製品出荷前の脆弱性検査として、各種のテスト（既知の脆弱性検査、ソースコード検査、ファジングによる未知の脆弱性検出）を実施し、残留している脆弱性を検出・出荷までに解消する
  + 製品出荷後の脆弱性の新たな発見に備えること
    - 製品出荷後の脆弱性の発見に備えて、ソフトウェア（ファームウェア）の更新機能を実装すべき
* 運用段階での対応
  + 継続的な脆弱性対策情報の収集
    - 出荷した製品自体、製品開発に利用した外部のソフトウェア部品において、新たな脆弱性が検出・発見されていないか、継続的な脆弱性対策情報の収集が必要
  + 脆弱性対策情報（更新ソフトウェアを含む）の作成
    - 新たな脆弱性が検出・発見された場合、脆弱性対策情報（脆弱性の概要、深刻度、影響を受ける範囲、想定される影響、対策等）を作成
    - 対応に時間がかかる場合は、回避策（例えば、製品の特定の機能をオフにして脆弱性の影響を受けないように抑止する）を準備
  + 脆弱性対策情報の利用者への通知
    - 脆弱性対策情報が作成できたら、速やかに、確実に利用者に通知すること。
    - 遠隔操作によって自動的に更新ソフトウェアを適用する方法も検討
    - 利用者における更新ソフトウェアの適用が困難な製品の場合やハードウェアの脆弱性の場合、IoTの製品分野によっては、リコールを実施し、製品を一旦回収してアップデート・改修作業を実施する可能性についても、考慮しておく必要がある

## 内閣サイバーセキュリティセンター（NISC）

* NISC
  + <http://www.nisc.go.jp/>
  + [みんなでしっかりサイバーセキュリティ]
    - <http://www.nisc.go.jp/security-site/index.html>
  + 情報セキュリティハンドブック
    - <http://www.nisc.go.jp/security-site/files/handbook1-0131.pdf>
  + マンガで学ぶサイバーセキュリティ
    - <http://www.nisc.go.jp/security-site/files/CSmanga_JPN.pdf>

### 高度情報通信ネットワーク社会推進戦略本部（IT総合戦略本部）

* <http://www.kantei.go.jp/jp/singi/it2/>

### 国家安全保障会議

* <http://www.kantei.go.jp/jp/singi/anzenhosyoukaigi/index.html>

### 警察庁

* 警察庁セキュリティポータルサイト@police
  + <http://www.npa.go.jp/cyberpolice/>
* サイバー犯罪対策
  + <http://www.npa.go.jp/cyber/>
* インターネット安全・安心相談
  + <http://www.npa.go.jp/cybersafety/>
* @police - パソコンユーザ向けカリキュラム
  + <http://www.npa.go.jp/cyberpolice/pc/elearning/index.html>

### 総務省

* 国民のための情報セキュリティサイト【LEVEL0】【ポータル】【容易】
  + <http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/index.html>
* 電子署名・認証
  + <http://www.soumu.go.jp/main_sosiki/joho_tsusin/top/ninshou-law/law-index.html>

### 外務省

* 日本の安全保障政策
  + <http://www.mofa.go.jp/mofaj/gaiko/page22_000407.html>

### 経済産業省

* 情報セキュリティ政策
  + <http://www.meti.go.jp/policy/netsecurity/>
  + 経営者向けセキュリティ関連コンテンツ一覧
    - <http://www.meti.go.jp/policy/netsecurity/secdoc/mng_contents.html>
      * 情報セキュリティガバナンス導入ガイダンス【経営者向け】【基準・ガイド】
        + <http://www.meti.go.jp/policy/netsecurity/downloadfiles/securty_gov_guidelines.pdf>
  + 運用者向けセキュリティ関連コンテンツ一覧
    - <http://www.meti.go.jp/policy/netsecurity/secdoc/ope_contents.html>
  + 開発者向けセキュリティ関連コンテンツ
    - <http://www.meti.go.jp/policy/netsecurity/secdoc/dev_contents.html>
* 経済産業省 情報セキュリティ政策ポータル
  + <http://www.meti.go.jp/policy/netsecurity/docs.html>
    - クラウドサービス利用のための情報セキュリティマネジメントガイドライン
      * <http://www.meti.go.jp/policy/netsecurity/downloadfiles/cloud_security_guideline.pdf>
* サイバーセキュリティ経営ガイドライン
  + <http://www.meti.go.jp/press/2015/12/20151228002/20151228002.html>
    - （４）サイバーセキュリティ対策フレームワーク構築（PDCA）と対策の開示
      * 経営ガイドラインの各項目
        + PDCAサイクルの実施と改善
      * 項目の実現に有効な
      * 技術的対策項目
        + ISMSの導入やセキュリティ監査の実施によるPDCAサイクルの実施により、現状のセキュリティ対策の改善点を洗い出し、将来の改善計画を立案し実行していくこと。
    - 対策をしないことのリスクや対策を実施する効果
      * 環境や事業の変化に合わせて、対策の点検や改善を継続していない場合、新たな脅威に対抗できなくなる恐れがある。
    - 参考ガイド、文献、ツール類
      * 【制度】
        + JIPDEC『情報セキュリティマネジメントシステム（ISMS）適合性評価制度』
        + JIPDEC『サイバーセキュリティマネジメントシステム（CSMS）適合性評価制度』
        + 経済産業省『情報セキュリティ監査制度』
      * 【ツール】
        + IPA『情報セキュリティ対策ベンチマーク』

### JPCERTコーディネーションセンター

* <https://www.jpcert.or.jp/>
* Japan Vulnerability Notes
  + <http://jvn.jp/>
* 高度サイバー攻撃(APT)への備えと対応ガイド～企業や組織に薦める一連のプロセスについて
  + <https://www.jpcert.or.jp/research/apt-guide.html>
* 高度サイバー攻撃への対処におけるログの活用と分析方法
  + <https://www.jpcert.or.jp/research/apt-loganalysis.html>
* 経営者が知っておくべきセキュリティリスクと対応について【LEVEL3】【難解】
  + https://www.jpcert.or.jp/research/aptrisk.html

### 防衛省

* <http://www.mod.go.jp/>

## 東京都

## 警視庁

* 情報セキュリティ広場
  + <http://www.keishicho.metro.tokyo.jp/kurashi/cyber/index.html>
  + 大阪府警
    - サイバー犯罪対策
      * <https://www.police.pref.osaka.jp/index.html#a%3Dajax%252Fseikatsu.html%26b%3D%252Fajax%252Fseian%252Fhigh_tech.html%26c%3D>

## 中小企業庁

* 中小企業BCP策定運用指針
  + <http://www.chusho.meti.go.jp/bcp/>
  + 中小企業BCPの策定促進に向けて　～中小企業が緊急事態を生き抜くために～
    - <http://www.chusho.meti.go.jp/bcp/2012/download/24fyBCP.pdf>
* 経営サポート「技術革新・IT化支援・省エネ対策」
  + <http://www.chusho.meti.go.jp/keiei/gijut/index.html>
  + 第3章　中小企業のＩＴ 化推進の支援策
    - <http://www.chusho.meti.go.jp/keiei/gijut/it_03.html>
    - 中小企業のＩＴ化支援
      * (1) IT活用に対する意識向上と人材の育成
        + 1)セミナー・研修の実施
        + 2)ＩＴアドバイザーの育成
      * (2) ＩＴ化に関するアドバイス・コンサルティング
      * (3) ITシステム導入に対する支援
    - 中小企業のＩＴ化のための基盤整備
      * (1) 共通基盤的ソフトウェア等の整備
        + 1)新たなビジネスモデルの開発と商業分野の活性化
        + 2)ものづくりとITの融合の支援
      * (2) IT推進のための情報提供
      * (3) 中小企業が電子商取引を促進するための機能の整備
        + 1)電子認証システムの整備・啓発・普及
        + 2)セキュリティーの確保と消費者の保護

○セキュリティー対策の普及

○「オンラインマーク制度」の普及

* + - * + 3)政府調達の電子化と対応の円滑化
        + 4)売掛債権等の流動化に向けたインターネットの活用
        + 5)インターネットによる中小株式会社の計算書類開示を支援
        + 6)中小企業の電子商取引を促進するための制度の検討
    - 中小企業のＩＴ化のための連携促進
      * (１) ネットワーク組織化の推進

## IPA

### 全体

* 情報セキュリティ対策
  + <https://www.ipa.go.jp/security/measures/>
* 「2015年度 中小企業における情報セキュリティ対策に関する実態調査」報告書について
  + <https://www.ipa.go.jp/security/fy27/reports/sme/>

### 基本情報

* 教育・学習（企業・組織向け）｜ここからセキュリティ！ 情報セキュリティ・ポータルサイト
  + <http://www.ipa.go.jp/security/kokokara/study/company.html>
* 5分でできる！情報セキュリティポイント学習(ダウンロード版)
  + <http://www.ipa.go.jp/security/vuln/5mins_point/105_themes.html>
* 個人情報の利活用と保護に関するハンドブック
  + <http://www.ppc.go.jp/files/pdf/personal_280229sympo_pamph.pdf>
* 情報セキュリティ：脆弱性関連情報の取扱い：知っていますか？脆弱性
  + <http://www.ipa.go.jp/security/vuln/vuln_contents/>
* 情報セキュリティ10大脅威 2016
  + <https://www.ipa.go.jp/security/vuln/10threats2016.html>
* 情報セキュリティ対策のしおり
  + <http://www.ipa.go.jp/security/antivirus/shiori.html>

### 情報セキュリティ啓発（IPA）

* IT社会を、守る、育てる
  + <http://www.ipa.go.jp/security/keihatsu/pr2012/>
* 情報セキュリティ・ポータルサイト「ここからセキュリティ」
  + <http://www.ipa.go.jp/security/kokokara/>
* 情報セキュリティ白書
  + <http://www.ipa.go.jp/security/publications/hakusyo/2015.html>
* 対策のしおり
  + <http://www.ipa.go.jp/security/antivirus/shiori.html>
* 映像で知る情報セキュリティ
  + <http://www.ipa.go.jp/security/keihatsu/videos/index.html>
* パスワード －もっと強くキミを守りたい－
  + <http://www.ipa.go.jp/security/keihatsu/munekyun-pw/>
* チョコっとプラスパスワード
  + <http://www.ipa.go.jp/chocotto/pw.html>
* I Love スマホ生活
  + <http://www.ipa.go.jp/security/keihatsu/smartphone.html>
* 情報セキュリティ対策支援サイトiSupport
  + <http://www.ipa.go.jp/security/isec-portal/index.html>
* 情報漏えい発生時の対応ポイント集
  + <http://www.ipa.go.jp/security/awareness/johorouei/index.html>
* 5分でできる情報セキュリティポイント学習
  + <http://www.ipa.go.jp/security/vuln/5mins_point/index.html>
* ひろげよう情報モラル・セキュリティコンクール
  + <http://www.ipa.go.jp/security/vuln/5mins_point/index.html>
* サイバーセキュリティのひみつ
  + <http://www.ipa.go.jp/security/keihatsu/security-himitsu/>
* 漏れたら大変！個人情報
  + <http://www.ipa.go.jp/security/kojinjoho/comment.html>
* 情報セキュリティ読本
  + <http://www.ipa.go.jp/security/publications/dokuhon/index.html>
* インターネット安全教室
  + <http://www.ipa.go.jp/security/keihatsu/net-anzen.html>
* 【情報セキュリティ対策】中小企業向け講習能力養成セミナー
  + <http://www.ipa.go.jp/security/keihatsu/sme/index.html>

### セキュリティ設定共通化手順SCAP概説（IPA）

* <http://www.ipa.go.jp/security/vuln/SCAP.html>
  + SCAP（Security Content Automation Protocol：セキュリティ設定共通化手順）
  + IPAセキュリティセンターが開発した情報セキュリティ対策の自動化と標準化を目指した技術仕様

### サイバー情報共有イニシアティブ（J-CSIP（ジェイシップ））（IPA）

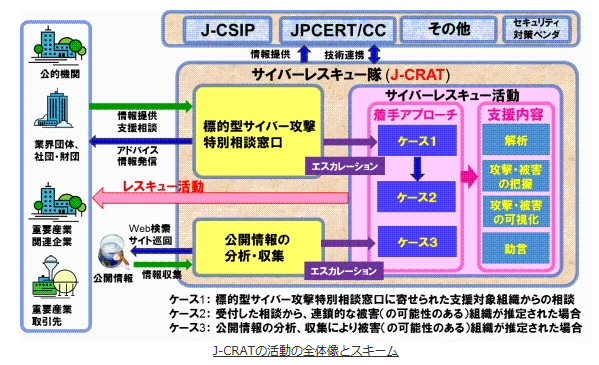
* <http://www.ipa.go.jp/security/J-CSIP/index.html>
* サイバーセキュリティと経済　研究会　中間とりまとめの公表について（経済産業省）
  + <http://www.meti.go.jp/committee/kenkyukai/shoujo/cyber_security/report01.html>
* J-CRAT／標的型サイバー攻撃特別相談窓口
  + <http://www.ipa.go.jp/security/tokubetsu/index.html>

### 情報セキュリティスキル強化についての取り組み（IPA）

* <http://www.ipa.go.jp/jinzai/hrd/security/index.html>
* 情報セキュリティ強化対応スキル指標
  + <http://www.ipa.go.jp/files/000041104.xlsx>
* IT人材における情報セキュリティの育成ニーズ・課題調査（最終報告書・概要版）
  + <http://www.ipa.go.jp/files/000039526.pdf>
* IT人材における情報セキュリティの育成ニーズ・課題調査（最終報告書・詳細版）
  + <http://www.ipa.go.jp/files/000039527.pdf>
* ITのスキル指標を活用した情報セキュリティ人材育成ガイド（冊子）
  + <http://www.ipa.go.jp/files/000039528.pdf>

## サイバーレスキュー隊J-CRAT（ジェイ・クラート）：IPA

* <https://www.ipa.go.jp/security/J-CRAT/>
* IPAは、標的型サイバー攻撃の被害拡大防止のため、2014年7月16日、経済産業省の協力のもと、相談を受けた組織の被害の低減と攻撃の連鎖の遮断を支援する活動としてサイバーレスキュー隊（J-CRAT：Cyber Rescue and Advice Team against targeted attack of Japan）を発足させた。

****

# セキュリティ関連機関

## 日本セキュリティオペレーション事業者協議会（ISOG-J）

* 「やられたかな？その前に〜『やられてる！』と思ったら〜」
  + <http://isog-j.org/output/2015/Yararetakana-Guide-20151014.pdf>

## ノートン

* 情報漏洩の原因を徹底解析！原因と結果から学ぶ意識改革
  + <https://japan.norton.com/leakage-cause-1462>

## トレンドマイクロ

* IS702
  + <http://www.is702.jp/>

## ＠IT

* Security & Trust : 企業ネットワークセキュリティのためのノウハウ＆情報フォーラム - ＠IT
  + <http://www.atmarkit.co.jp/ait/subtop/security/>
* その「セキュリティ教育」、本当に効果ありますか？
  + ています。標的型攻撃への対策自体は、国内でも2008年ごろから検討されていたのですが、やはり2015年に起きた日本年金機構での情報漏えい事件が引き金となり、一気に関心が高まったようです。そこで最近は各組織で「標的型メール攻撃訓練」が盛んに行われています。
  + しかし、こうしたセキュリティ教育・訓練は、単に行えば済むというものではありません。その「目的」や「効果」について、事前にしっかり認識した上で実施する必要があります。事実、国内外で現状のセキュリティ教育・訓練の問題点を指摘した複数の報告もなされています。実効的なセキュリティ教育・訓練が求められているといえるでしょう。
  + <http://www.atmarkit.co.jp/ait/articles/1604/11/news026.html>
* 「新人にはまずセキュリティを教えよう」関連記事
  + サイバーセキュリティ教育を多様なレイヤーの人に届けるプロジェクトが発足
    - Hack＋Academyで「Hackademy」、経営層向けの説明のコツも　有志によるサイバーセキュリティ教育プロジェクト「Hackademyプロジェクト」を解説（2016/4/8）
    - <http://www.atmarkit.co.jp/ait/articles/1604/08/news059.html>
  + 「セキュリティ人材」って、何ですか？――本当に必要なセキュリティ教育を考える
    - セキュリティ教育現場便り（1）　「セキュリティ人材」とは、一体どのような人材を指すのでしょう？ セキュリティ教育に現場で携わってきた筆者が、今求められる人材育成について考えます（2016/1/19）
    - <http://www.atmarkit.co.jp/ait/articles/1601/20/news007.html>
  + グーグル新入社員はコードを書く前にセキュリティ教育を受ける
    - RSA Conference Japan 2008　「脆弱性は変わっていないが、われわれを取り巻く世界は大きく変化している」米グーグルのスコット・ペトリ氏はこのように語り、従来とは異なるセキュリティ対策が求められると述べた。（2008/4/25）
    - <http://www.atmarkit.co.jp/news/200804/25/google.html>

## 一般社団法人 電気通信事業者協会（TCA）

* 銀行などを装った「フィッシング詐欺」にご注意ください！
  + <http://www.tca.or.jp/information/phishing.html>

# 消費者庁

* キャンペーンTOP
  + <http://www.caa.go.jp/adjustments/internet_trouble/>
  + インターネット通販トラブル
    - <http://www.caa.go.jp/adjustments/internet_trouble/internet.html>
  + 口コミトラブル
    - <http://www.caa.go.jp/adjustments/internet_trouble/mouth.html>
  + サクラサイトトラブル
    - <http://www.caa.go.jp/adjustments/internet_trouble/sakura.html>
  + オンラインゲームトラブル
    - <http://www.caa.go.jp/adjustments/internet_trouble/online.html>
  + 決済について
    - <http://www.caa.go.jp/adjustments/internet_trouble/payment.html>
  + リンク集
    - <http://www.caa.go.jp/adjustments/internet_trouble/link.html>

# 東京商工会議所

* 「中小・小規模事業者の情報セキュリティ対策の強化に向けた意見」（2014年4月14日）で参照された情報元
  + 【首相官邸】日本再興戦略』改訂2015
    - <https://www.kantei.go.jp/jp/singi/keizaisaisei/>
  + 「グローバル情報セキュリティ調査®2016（日本版）」
    - <http://www.pwc.com/jp/ja/advisory/press-room/press-release/2015/information-security-survey151107.html>
  + 【IPA】サイバーセキュリティ経営ガイドライン
    - <http://www.meti.go.jp/press/2015/12/20151228002/20151228002.html>
  + 【総務省】情報通信白書平成27年度版
    - <http://www.soumu.go.jp/johotsusintokei/whitepaper/index.html>

# Tcyss会議

## 第1回会議より（4月25日）

* 情報共有、情報交換、情報提供
  + Office365を活用した場の設置（Microsoft）
  + 何をすべきかを明確にしてから（東京都）
    - Q&A集を作る
  + 走りながら発信する場ができればいい（警視庁）
    - SNSを活用して情報が共有できる場ができ、セミナーの案内等ができることが望ましい
  + 情報セキュリティ対策情報の共有と発信が必要（東商）
  + Webで各セキュリティ関連の情報への案内はどうするか？（Microsoft）
    - リンク先は今後調整したい（Microsoft）
* 啓発活動が必要
  + PCの被害に遭ったことさえわからないレベルもある。（IIT）
    - 情報搾取型で、ランサムウェアはすぐ気が付く（マカフィ）
  + 産業交流会がある（東京都）
  + 「2015年度 中小企業における情報セキュリティ対策に関する実態調査」（IPA）
  + 啓発ビデオ、5分でできるチェックシートがある。今年、見直す予定（IPA）
  + リスク管理の必要性を刷り込む必要がある（東商連合会）
    - スポットセミナーを各地域で。
  + アウトリーチが必要（砂原）
    - VTRなどを活用して、「無関係」ではいられないと気付かせる
* 教育すべきこと
  + あるべき姿を見せていくことが重要（トレンドマイクロ）
  + トップ、経営者じ向けて、対策のモチベーションに繋がることが重要（ISO-G）
    - これをやればビジネスに有利になるとか
    - ステークホルダーが集まっているので、知恵を絞りあって
    - 中小企業では何が問題か？
      * 対策は、組織（管理）、人、もの、技術
        + 技術的対策は大企業ではできている
        + 中小への技術的対策は、ウイルス対策だけでなく
* 認定制度は
  + 対策の必須数項目が出来ていれば認定、だめならセミナーへとか（Microsoft）
  + Web ベースの認定書、診断シートは、国全体の対策として行っている（IPA）
  + 中小企業は、複数の大手の下請けになる。大手ごとにチェック項目が違う認定は避けるべき⇒共通の認定制度であるべき（ISO-G）
  + また、認定制度とリンクして、中小が集まったセキュリティ保険も（ISO-G）
  + 東京だけでなく、全体で認定を（マカフィ）
* 具体的な対策
  + 中小の規模に応じたシステムモデルイメージの提示（手塚）
    - セキュリティ対策の常識
    - パターンを既製品として提示
  + 押し付けでなく、事前に対策をすることがインセンティブになるように（高橋）
    - 平時、緊急時は、ポータルへ行けばわかるように

# 文献

## NDLアーカイブ

* 情報通信技術の進展とサイバーセキュリティ（平成26年度　科学技術に関する調査プロジェクト）
  + <http://dl.ndl.go.jp/search/searchResult?searchWord=%E6%83%85%E5%A0%B1%E9%80%9A%E4%BF%A1%E6%8A%80%E8%A1%93%E3%81%AE%E9%80%B2%E5%B1%95%E3%81%A8%E3%82%B5%E3%82%A4%E3%83%90%E3%83%BC%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3&featureCode=all&filters=2%3A1&viewRestrictedList=0>

# 情報セキュリティ関連文書

## NISCサイバーセキュリティ戦略本部

* + <http://www.nisc.go.jp/conference/cs/index.html>
  + 重要インフラの情報セキュリティ対策に係る第３次行動計画の見直しに向けたロードマップ
    - <http://www.nisc.go.jp/active/infra/pdf/ciip_roadmap2016.pdf>
  + サイバーセキュリティ戦略～世界を率先する強靭で活力あるサイバー空間を目指して～
    - <http://www.nisc.go.jp/active/kihon/pdf/cyber-security-senryaku-set.pdf>

# 情報システムの整備と運用管理を調達する際の情報セキュリティ対策として考慮すべき要件

## 「政府情報システムの整備及び管理に関する標準ガイドライン実務手引書」より

* 別紙「情報システム整備と運用時のセキュリティ考慮事項（中山）.doc」

# 東京都の取り組み【公開情報】

## 東京都の行政改革 - 総務局行政改革推進部のホームページ - | ＩＴ・業務改革

* 東京都サイバーセキュリティ基本方針(PDF 124KB)
  + <http://www.soumu.metro.tokyo.jp/02gyokaku/pdf/security/151027policy.pdf>

## 高度情報化推進の取り組み

* 情報システム部は、ＩＴを利活用した都民サービスの向上・業務の効率化に取り組むとともに、区市町村等と連携した電子自治体の構築や地域情報化の推進を行うなど、東京都全体の高度情報化の推進を担っています。
* また、こうした高度情報化を支える庁内ネットワーク及び共通基盤システムなどの保守・運用管理、技術支援、ＩＴ人材の育成などを行っています。
* 平成２２年３月には、都の情報セキュリティポリシー等に基づく対策をより確実に実施するべく、ＩＳＯ規約に基づくＩＳＭＳ（情報セキュリティマネジメントシステム）の認証を受け、セキュリティ対策のさらなる改善に恒常的に取り組んでいます。
* 詳しくは高度情報化推進の取り組み
  + <http://www.soumu.metro.tokyo.jp/13it/jigyougaiyou.html>

# 情報セキュリティマネジメント試験（シラバス）

## 

# 情報処理技術者試験（シラバス）

## 基礎

## 応用

# 情報セキュリティ想定事例集

相談事例によるFAQ作成に先駆けて、各機関が提供している事例を集めて体系的にまとめる。

## 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（IPA）

* <https://www.ipa.go.jp/security/keihatsu/shiori/management/03_casestudy.pdf>
  + 従業員の情報持ち出し
  + 退職者の情報持ち出し、競合他社への就職
  + 従業員による私物PCの業務利用と Winnyの利用による業務情報の漏洩事故
  + ホームページへの不正アクセス
  + 無許可の外部サービスの利用
  + 委託した先からの情報漏えい
  + 在庫管理システム障害の発生
  + 無線LANのパスワードのいい加減な管理
  + IT管理者の不在
  + 電子メール経由でのウイルス感染
* NEC提案資料
  + 金銭搾取
    - マルウェアやフィッシングによる不正送金
    - データを暗号化して複合のために強迫による金銭要求
  + 政治的主張（ハクティビスト）
    - DoS攻撃により、Webサービスの停止
    - マルウェア、クロスサイトスクリプティング等により、Webページの改ざん
  + IoTを経由した重要インフラのサービス停止
  + SNSと密接に関わるサイバー攻撃
    - SNSを使った特定ターゲットへの攻撃予告、協力者募集、攻撃ツールの流布
    - ゼロディ攻撃
    - APT攻撃
* 内閣官房NISC「情報セキュリティ小冊子」（実際の事例）
  + 「政府機関の新人研修資料がインターネット上に流出していたことがわかった。資料には「機密性２」と記されていた。（2015年3月：政府機関）
  + リサイクルショップで購入したワープロ内部に、政府機関において作成したと思われる個人情報を含む職務上の情報が残存しているとの情報提供があった。（2012年5月）
  + パソコン２台が動画再生ソフト「GOMプレーヤー」をアップデートした際にウイルスに感染していたことが判明した。（2014年2月：○○病院）
  + パソコンにおいて、入力した全ての文字情報が「百度（バイドゥ）」のサーバに送信される日本語入力ソフト（BaiduIME）がインストールされていた。（2013年12月：政府機関、○○大学など）