Expand - Collapse

- Sec01-02-05サイバーセキュリティ対策相談対応の手引き（メモ）
  - 【2018年7月3日】内容は、2016年7月5日のもの
  - 1. 体系的で特に有用な情報提供元【抽出中】
  - 2. 問合せ事例
  - 3. FAQ候補
  - 4. 脆弱性情報の届出
  - 5. 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。
  - 6. 情報セキュリティに関する基礎知識
    - 6.1. 情報セキュリティ 10 大脅威（個人）
      - 6.1.1. 【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
      - 6.1.2. 【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
      - 6.1.3. 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

Expand - Collapse

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、そもそも間違えないようにする設計）が重要

- 6.1.4. 【対策】情報セキュリティ 10 大脅威（個人）
- 6.1.5. 【対策】情報セキュリティ 10 大脅威（組織）
- 6.1.6. 【対策】注目すべき脅威や懸念

⊟ 7. 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。

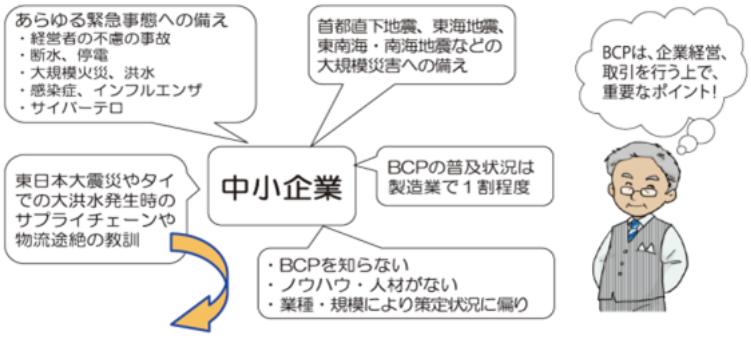
⊟ * 情報セキュリティ対策は

- > 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

⊟ 8. 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復旧を可能とするため、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

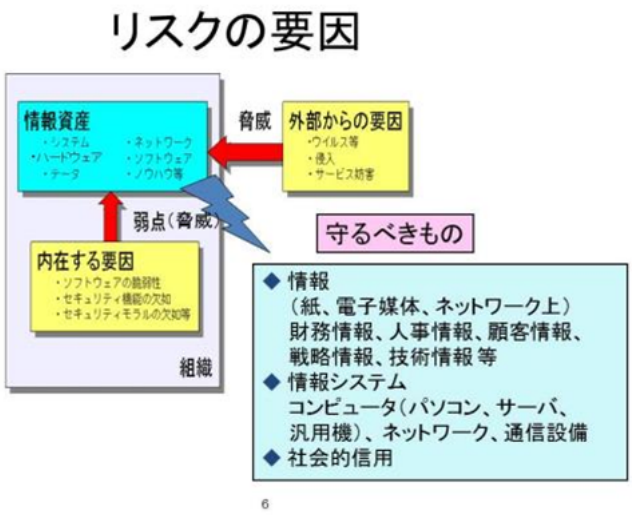
⊟ 何のためにBCPを策定するのか？

⊟ セキュリティインシデント対応はBCPの１つ

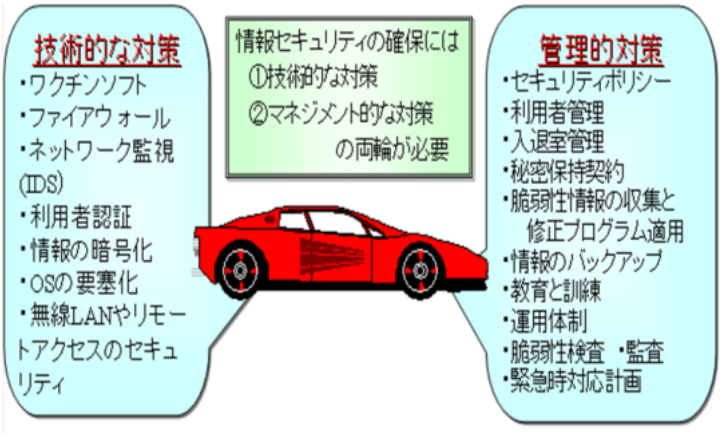
- BCPとは、企業が緊急事態（自然災害、大火災、感染症、テロ、、、）に遭遇した場合において、事業資産（人・もの（情報及び設備）・金）の損害を最小限にとどめつつ、中核となる事業の継続あるいは早期普及を可能とするため、平時に行うべき活動、当該緊急非常時における事業継続のための方法、手段などをあらかじめ取り決め、それを文書化したもの。
- 情報セキュリティポリシー（基本方針、対策基準）は、人的・物的被害の防御、軽減が主眼の「防災計画」の１つ
- インシデント対応は、被災後の事業の継続・早期復旧を視野に入れたBCPの１つ

Expand - Collapse

- 9. 情報セキュリティ対策の概念
  - 9.1. リスクの要因



  - 9.2. 情報セキュリティにおけるさまざまな対策



  - 9.3. 情報セキュリティ対策の意義
    - * 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
  - 9.4. 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

Expand - Collapse

- > 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

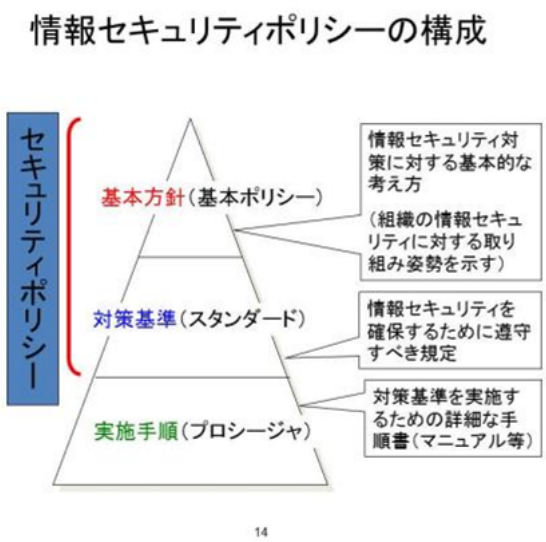
* 管理的情報セキュリティ対策

- > 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

10. 情報セキュリティポリシー、実施手順

10.1. 情報セキュリティポリシーの構成



10.2. 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。

Expand - Collapse

- > 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。

⊟ 10.3. 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

⊟ 10.4. 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

⊟ 10.5. 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

⊟ 10.6. 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

⊟ 10.7. 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

Expand - Collapse

- > 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

10.8. 情報セキュリティマネジメントの規格や標準

10.8.1. 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

- * 「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。

10.8.2. 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

- * 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。

10.9. 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。

Expand - Collapse

- * 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。

⊟

⊟ 10.9.1. 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。

⊟ 10.9.2. 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）
- * (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。

⊟ 11. 「情報セキュリティ管理基準（平成20年改正版）」
- 別途

- 12. 「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）」
- 13. 人材育成
- 14. 個人情報保護

Expand - Collapse

- 15. 中小企業に特化した情報セキュリティ対策の相談対応
- 16. 情報セキュリティ関連法規
- 17.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）
  - 【2016年7月時点】
  - 概要
    - * 「ここからセキュリティ！」のサイト内情報を検索・選択しやすいように、1ページ内に全リンクを表示し、その内容によってレベル表示をし、また必要に応じで内容の解説を加えたもの。
    - * 検索の際はWebブラウザの検索機能を利用してください。
    - * 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
  - 17.1. 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
    - * 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
  - 17.2. 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）

Expand - Collapse

- * http://www.is702.jp/special/1542/partner/12_t/

17.3. 被害にあったら

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

17.3.1. 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

17.3.2. 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）

- * 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

17.3.3. 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】

Expand - Collapse

- > 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/

17.3.4. ワンクリック請求（料金画面が消えない・料金請求された）

- * 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)
- >

17.3.5. 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/

17.3.6. 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）

- * 【×】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

17.4. 対策する

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

Expand - Collapse

- 17.4.1. 対策の基本（まずはここから！）
  - * 企業における対策の基本
    - * 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】

Expand - Collapse

- * 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）

Expand - Collapse

- > 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】
- * 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%
- > 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
- > 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

Expand - Collapse

- > 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

⊟ 17.4.2. 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)

⊟ 17.4.3. 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)

⊟ 17.4.4. 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】

Expand - Collapse

- > 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

17.4.5. 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】

- * 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

17.4.6. 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】

Expand - Collapse

- > 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

⊟ 17.4.7. 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

Expand - Collapse

- * 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) 【LE 【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/

⊟ 17.4.8. 標的型攻撃メール

- * 標的型攻撃への対策(総務省) 【LEVEL1】【詳細】

Expand - Collapse

- > 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
- * 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/

⊟ 17.4.9. 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】

Expand - Collapse

- > 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

17.4.10. 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】

Expand - Collapse

- * 【×】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

Expand - Collapse

- > 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
- * 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 ～

Expand - Collapse

- * [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

- サブトピック 5

17.5. 教育・学習

17.5.1. 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)【動画】
  - * 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）【動画】

Expand - Collapse

- * 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）【動画】
- * 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）

Expand - Collapse

- > 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)

Expand - Collapse

- * 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）

17.5.2. 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）【LEVEL1】
  - * http://jp.norton.com/identity-theft-primer/article
  - >【●】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】【詳細】
  - * http://www.microsoft.com/ja-jp/security/family-safety/childsafety-internet.aspx
  - >【●】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
  - > 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）【LEVEL1】【簡易】
  - * http://www.mcafee.com/japan/home/security/news/049.html
  - >【●】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）【LEVEL1】【詳細】
  - * http://www.mcafee.com/japan/home/security/news/048.html

Expand - Collapse

- > 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）【LEVEL1】
- * http://www.mcafee.com/japan/home/security/news/044.html
- > 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）【LEVEL1】【詳細】
- * http://www.mcafee.com/japan/home/security/news/041.html
- > 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）
- * http://www.mcafee.com/japan/home/security/news/029.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）
- * http://www.mcafee.com/japan/home/security/news/default.asp
- * ⇒セキュリティニュースへリダイレクト「
- * http://www.mcafee.com/japan/home/security/news/
- > 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）【LEVEL0】【簡易】
- * http://www.is702.jp/manga/1964/partner/12_t/
- > 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）【LEVEL0】【簡易】
- > ひろしとアカリのセキュリティ事情「脆弱性対策はなぜ必要なの？」（トレンドマイクロ）【LEVEL0】【簡易】
- * http://www.is702.jp/manga/1964/partner/12_t/
- > Windows 10を安全に使うためのヒント（トレンドマイクロ）【LEVEL0】【簡易】
- *
- > 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）【LEVEL0】【簡易】
- * http://www.is702.jp/manga/1812/partner/12_t/?cm_re=article-_-threat-_-is702&_ga=1.114917703.196970070.1431999093
- > 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）【LEVEL0】【簡易】
- * http://www.is702.jp/special/1801/partner/12_t/?cm_re=article-_-threat-_-is702&_ga=1.122710603.196970070.1431999093
- > 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）【LEVEL0】【簡易】
- * http://www.is702.jp/manga/1766/partner/12_t/?cm_re=article-_-threat-_-is702&_ga=1.86140504.196970070.1431999093
- > 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）【LEVEL0】【簡易】
- * http://www.is702.jp/manga/1753/partner/12_t/?cm_re=article-_-threat-_-is702&_ga=1.55705195.196970070.1431999093
- > 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）【LEVEL0】【簡易】
- * http://www.is702.jp/manga/1744/partner/12_t/?cm_re=pickupbnr-_-threat-_-is702&_ga=1.70522259.2099996290.1431312366
- > 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）【LEVEL0】【簡易】
- * http://www.is702.jp/manga/1735/partner/12_t/?cm_re=article-_-threat-_-is702&_ga=1.108461954.1038327157.1416213751
- > 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）【LEVEL0】【簡易】
- * http://www.is702.jp/manga/1731/partner/12_t/?cm_re=article-_-threat-_-is702&_ga=1.176544421.1038327157.1416213751
- > 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）【LEVEL0】【簡易】
- * http://www.is702.jp/manga/1728/partner/12_t/?cm_re=article-_-threat-_-is702&_ga=1.117216902.1038327157.1416213751
- > 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）【LEVEL0】【簡易】
- * http://www.is702.jp/manga/1709/partner/12_t/
- > 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）【LEVEL0】【詳細】
- * http://www.is702.jp/special/1705/partner/12_t/?cm_re=article-_-threat-_-is702&_ga=1.83359382.1038327157.1416213751
- > 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）
- * http://www.is702.jp/special/1680/partner/12_t/
- > 【×】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）
- * http://is702.jp/special/1478/partner/12_t/
- > 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）
- * http://is702.jp/special/1457/partner/12_t/
- > 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）
- * http://is702.jp/special/1391/partner/12_t/
- > 「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）【LEVEL2】【詳細】
- * http://is702.jp/special/1293/partner/12_t/?cm_re=pickupbnr-_-threat-_-is702f

Expand - Collapse

- > 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）
- * http://is702.jp/special/967/partner/12_t/
- > セキュリティ対策の基礎知識（トレンドマイクロ）
- * https://is702.jp/download/security_basic.pdf
- > スマホからの情報漏洩に気をつけて！（トレンドマイクロ）
- * http://is702.jp/special/1301/partner/12_t/

⊟ * ●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）
- > 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）
- > 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「鉄壁の守り」（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）

Expand - Collapse

- > 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）

⊟ 17.5.3. 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)【動画】
- * 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）【動画】
- * 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/

Expand - Collapse

- > 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-【動画】
- * 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】【オンライン版】【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】

Expand - Collapse

- * 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-【動画】
- * 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

Expand - Collapse

- > 【●】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
- * 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】

Expand - Collapse

- * 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#
- > 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）【LEVEL0】【詳細】
- * 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）
- * 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）
- * http://www.is702.jp/special/1739/partner/12_t/?cm_re=pickupbnr-_-threat-_-is702&_ga=1.75887381.1038327157.1416213751
- > 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）
- * http://www.is702.jp/special/1650/partner/12_t/?cm_re=article-_-threat-_-is702&_ga=1.198511151.1462668070.1409299553
- > 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）
- * http://www.is702.jp/special/1637/partner/12_t/?cm_re=article-_-threat-_-is702&_ga=1.198639919.1462668070.1409299553
- > 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）
- * http://www.is702.jp/special/1593/partner/12_t/?cm_re=pickupbnr-_-threat-_-is702&_ga=1.208867473.2039373246.1395716218
- > 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）
- * http://is702.jp/special/967/partner/12_t/
- > 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）
- * https://is702.jp/download/security_basic_lesson.pdf
- > 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）
- * http://is702.jp/special/951/
- > 危険！パスワードの使い回し（マカフィー）
- * http://mcafee.com/japan/home/security/news/019.asp
- > 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）
- * http://www.mcafee.com/japan/home/security/news/041.html

⊟ * 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）

Expand - Collapse

- > 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)

⊟ 17.5.4. 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）

Expand - Collapse

- * 「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）

17.6. セキュリティチェック

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

17.6.1. 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「だまされレベル」チェック（トレンドマイクロ）

Expand - Collapse

- > 何が「個人情報」？理解度チェック（トレンドマイクロ）

- 17.6.2. 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）
- 17.6.3. 試験・資格
  - * "iパス"IT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）

- 17.7. 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
    - > 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

Expand - Collapse

- > 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
- > 「企業における情報システムのログ管理に関する実態調査」報告書
- > IPAテクニカルウォッチ「増加するインターネット接続機器の不適切な情報公開とその対策」
- > 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
- > 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
- > 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)
- > 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

* JNSA
- > 2015年度 情報セキュリティ市場調査報告書（速報版）
- > 2014年度 情報セキュリティ市場調査報告書

Expand - Collapse

- > 2015年 情報セキュリティインシデントに関する調査報告書【速報版】
- > コンシューマ向けIoTセキュリティガイド
- > 2015セキュリティ十大ニュース
- セキュリティデバイド広がる懸念
- > Challenge PKI Project

* JPCERT/CC
- > インシデント調査のための攻撃ツール等の実行痕跡調査に関する報告書
- > インターネット定点観測レポート(2016年 1～3月)
- > IPv6セキュリティテスト検証済み製品リスト
-
- > JPCERT/CCセキュリティインシデント年表
-
- > HTML5を利用したWebアプリケーションのセキュリティ問題に関する調査報告書
- > Java アプリケーション脆弱性事例解説資料
- > 法人におけるSNS利用に伴うリスクと対策
- > インシデント報告対応四半期レポート
- > 制御システム用ソフトウエアの脆弱性対策に有効なCERT_Cコーディングルールの調査
- > Weekly Report

* フィッシング協議会
- > フィッシング報告状況
- > フィッシングレポート2015
- ―進む対策、利用者としてできること―
- > フィッシングレポート2014
- ―急増する不正送金とフィッシング―

* IBM
- > Tokyo SOC Report

* シマンテック
- > ２０１５年インターネットセキュリティ脅威レポートのハイライト
- > シマンテック「ノートンモバイルアプリ調査」
- > シマンテックインテリジェンスレポート
- > インターネットセキュリティ脅威レポート
- > 人気モバイルデバイスのセキュリティ比較
- > スレットエクスプローラー
- > ノートンオンラインファミリーレポート

* トレンドマイクロ
- > 標的型サイバー攻撃最新動向調査データ・実例からとらえる「攻撃のトレンド」
- > 国内標的型サイバー攻撃分析レポート 2016年版
- > マイナンバーのセキュリティを９割以上の個人ユーザが不安視
- > ２０１５年年間セキュリティラウンドアップ：情報と金銭を狙ったサイバー犯罪の矛先が法人に
- > ２０１５年第３四半期セキュリティラウンドアップ：見ただけで感染する「正規サイト汚染」の脅威
- > ２０１５年第２四半期セキュリティラウンドアップ：標的型メールによる「気づけない攻撃」が多数発覚
- > ２０１５年第１四半期セキュリティラウンドアップ 新旧手法を脅威拡散に利用する攻撃者：不正広告の台頭とマクロ型の復活
- > パスワードの利用実態調査2014
- > 組織におけるセキュリティ対策実態調査2014
- > セキュリティデータベース

* マイクロソフト
- > セキュリティ インテリジェンス レポート
- > 脅威レポート: ルートキット
- > マルウェアの進化と脅威の状況-10年間の振り返り

* マカフィ―
- > McAfee_Labs_2016年の脅威予測
- > モバイルセキュリティ：McAfee 消費者動向レポート
- > In the Dark 重要産業が直面するサイバー攻撃
- > 脆弱性情報
- > McAfee脅威レポート

17.8. （情報セキュリティ　FAQ）
- * https://www.ipa.go.jp/security/faq/faq.html

Expand - Collapse

- * 【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
- > https://www.ipa.go.jp/security/topics/alert20080909.html

- 18. 参考サイト
- 19. セキュリティ関連機関