MCPC　情報セキュリティ読本

「誰でもわかるセキュリティ入門」

DXを推進する
MCPC

モバイルコンピューティング推進コンソーシアム
MCPC セキュリティ委員会

2025年5月

目　次

はじめに …… 1

① ソフトウェアの最新化 …… 2

② マルウェア（ウイルス等）対策 …… 3

③ 安全な無線 LAN の利用 …… 4

④ 標的型攻撃への対策 …… 5

⑤ 悪意のある Web サイトへの対策 …… 6

MCPC 情報セキュリティセミナーのご案内 …… 7

●正しいデータの消去方法 …… 8

●世の中で騒がれているけど何のこと？ …… 10

【用語解説】 …… 12

はじめに

近年、インターネットに接続されたデバイス（IoT: Internet of Things）の数は急激に増加しており、日々進化するテクノロジーとともに社会全体に革新的な変化をもたらしています。

リモートワークやクラウドサービスの活用などで利便性・効率性が進む一方、サイバー攻撃の手法は年々高度化・多様化しており、データ漏洩やフィッシング詐欺、マルウェアの拡散など、様々なセキュリティの脅威が社会や個人の安全を脅かすとともに、これらの潜在的脅威は、企業の存続に影響を与える深刻な問題となり得ます。

こうしたセキュリティのリスクに対処するためには、システムや専門部署による対策だけではなく、ひとり一人のセキュリティ意識の向上とともに、技術的な進歩を反映した対策が不可欠となります。

この読本では、日常の生活やビジネスシーンにおいて発生確率の高いリスク、そしてその対策方法について分かりやすく解説しています。

これらが、企業のセキュリティ強化や個人のデジタル技術活用の一助となり、皆さまの情報セキュリティに対する理解と実践が深まることを期待します。

①ソフトウェアの最新化

最新のソフトウェアは脆弱性の対策に加えて、セキュリティ機能強化も含まれます。アプリケーション、OS、IoT デバイスやルーターなどのアップデートを定期的に確認してソフトウェアを最新に保つのはセキュリティの観点では効果の高い対策です。

公開される脆弱性は年々増加し、2024 年に CVE 登録された脆弱性は 5 万件*1 を超えました。攻撃者が最初に使用する経路の 38% は既知の脆弱性の悪用であるという報告*2 もされています。

自動アップデートは、膨大な脆弱性情報から適切にアップデートするために有効ですが、無条件で適用できない機器に対しては脆弱性管理プロセスが必要です。脆弱性管理のプロセスは以下の手順で行います。

①資産の把握 : 組織が管理する様々な IT 資産を洗い出し、把握します。
②脆弱性情報の収集 : 対象資産の脆弱性情報を継続的に収集します。
③リスク評価 : 対象資産のリスク評価を行い、優先順位を付けます。
④対策の実施 : リスク評価結果に基づき、対策を検討し、実施します。

以下に公開されている脆弱性関連情報源とリスク評価手法の参考になる情報を記載しますので、必要に応じて参照して取り組んでください。

◆ 一般公開されている脆弱性情報（製品ベンダを除く）
- CVE.org：CVE 番号を管理する非営利団体の MITRE 社の脆弱性カタログ
  https://www.cve.org/
- NVD：米国国立標準技術研究所（NIST）が運営する脆弱性データベース
  https://nvd.nist.gov/
- JVN：JPCERT と IPA が運営する脆弱性対策データベース
  https://jvndb.jvn.jp/index.html
- IPA：情報処理推進機構のセキュリティ重要情報
  https://www.ipa.go.jp/security/security-alert/index.html
- JPCERT/CC：情報セキュリティインシデントに関する情報提供機関
  https://www.jpcert.or.jp/at/2024.html

◆ 脆弱性のリスク評価するための代表的な手法
- CVSS：IPA「共通脆弱性評価システム CVSS v3 概説」
  https://www.ipa.go.jp/security/vuln/scap/cvssv3.html
  ※脆弱性のスコア 7.0 以上が重大とされるが膨大 (57.4%) で、実際の攻撃が観測されたのは 4%*3
- KEV：CISA が公開している悪用が確認された脆弱性のカタログ
  https://www.cisa.gov/known-exploited-vulnerabilities-catalog
  ※悪用が確認されているものが 1305 件登録 (2025/3 時点)。
- EPSS : FIRST の EPSS 解説
  https://www.first.org/epss/user-guide
  ※脆弱性が悪用される確率を示す指標。他の指標との併用が必要。
- SSCV：米カーネギーメロン大学によって提案されたフレームワーク
  https://resources.sei.cmu.edu/asset_files/WhitePaper/2021_019_001_653461.pdf
  CISA が米国政府機関の実践用にシンプルなものも提案
  https://www.cisa.gov/sites/default/files/publications/cisa-ssvc-guide%20508c.pdf
  ※決定木に判断情報を入力することで、機械的に意思が示される

*1) https://www.cve.org/ の CVE 登録数をカウント
*2) Mandiant M-Trend2024 https://cloud.google.com/security/resources/m-trends
*3) FIRST The EPSS Model https://www.first.org/epss/model

②マルウェア（ウイルス等）対策

マルウェア（malware）は、「悪意のあるソフトウェア」のことで、コンピュータやネットワークに損害を与えるために開発されたソフトウェアです。ウイルス、ワーム、トロイの木馬、スパイウェア、アドウェア、ランサムウェアなど、さまざまな種類があり、データの盗難、システムの破壊、個人情報の漏洩などを引き起こします。

ウイルスは、他のプログラムに自身をコピーして感染を急速に広げていきます。特に、ランサムウェアは、システムやデータを暗号化し、復号のために身代金を要求し、企業や個人に大きな経済的損失をもたらします。被害の多くは電子メールの添付や不正なウェブサイトにアクセスしてダウンロードするケースが多いです。ランサムウェアの攻撃は、重要なデータを人質に取り、復旧のために高額な身代金を要求するため、被害者にとって非常に深刻な問題となります。

保護するために、もっとも重要なことは、不審な電子メールや Web サイトへのアクセスを避け、ソフトウェアを常に最新の状態に保つことです。定期的なバックアップを行い、重要なデータを安全な場所に保管することも推奨されます。また、信頼性の高いセキュリティソフトウェアを使用し、システムの脆弱性を定期的にチェックすることも重要です。さらに、ユーザー教育を通じて、フィッシング詐欺やソーシャルエンジニアリング攻撃に対する警戒心を高めることも効果的です。

■日本国内でのウイルス、ワーム、トロイの木馬、スパイウェア、アドウェアの被害事例

ランサムウェア

・A セントラルクリニック（2025 年 2 月）
ランサムウェア攻撃を受け、最大約 30 万人分の個人情報が漏洩した可能性があります。
・スーパーマーケットチェーン A 社（2024 年 2 月）
VPN を狙ったランサムウェア攻撃により、最大 778 万 4,999 件の個人情報が閲覧可能な状態になりました。

ワーム

ワーム型ランサムウェアである WannaCry は 2017 年に確認され、その年に世界 150 ヵ国で 23 万台以上のコンピューターが感染しました。海外では WannaCry に感染した影響で病院のシステムが停止し、手術や診察ができなくなった事例も発生しました。

トロイの木馬（2020 年 12 月）

自治体の病院事業局のパソコンがトロイの木馬の一種である「Emotet（エモテット）」に感染し、複数のなりすましメールが送信されるという事態が発生しました。

スパイウェア

スマートフォンに感染する「Exodus」は 2019 年に確認され、OS を乗っ取り、連絡先・写真・ビデオなどの情報へのアクセスや盗聴などを行います。マーケットプレイスに公開されていた複数のアプリが登録していたことがありました。

アドウェア

日本国内でアドウェア「INSTALLCORE」が 2024 年 5 月に多く検出され、ユーザーの望まない広告表示や不審なソフトウェアのダウンロードが確認されました。

③安全な無線 LAN の利用

近年リモートワークの普及により自宅での無線 LAN 利用のために自宅へ Wi-Fi ルーターの設置が増えています。Wi-Fi ルーターは容易に設置することができる反面セキュリティ対策が重要です。

- Wi-Fi ルーターへのログイン用パスワードの設定 購入時に設定されているパスワードから推測されにくい複雑なパスワードに変更する
- Wi-Fi 通信の暗号化 最新のセキュリティ機能に対応した Wi-Fi ルーターを使用する セキュリティの高い WPA2 あるいは WPA3 を設定する
- Wi-Fi ルーターへ最新ファームウエアを適用 定期的にメーカーのホームページを確認して最新のファームウェアが適用されていることを確認するメーカーからファームウェア更新のお知らせを受けた場合は速やかに更新する
- SSID の名称 Wi-Fi ルーターに機器名や自宅の場所、利用者の名前を含む名称は避ける
- SSID の隠蔽 SSID を非公開 (ステルス) 設定することで第三者が Wi-Fi ルーターを容易に検知できない

■Wi-Fi ルーターが悪用された事例

～ Wi-Fi ルーターがボットに感染し、DDoS の踏み台にされた (2024 年 5 月) ～

Wi-Fi ルーターログイン用パスワードが平文でルーター内に保存されており、[Internet 側リモートアクセス制限を許可する] を有効にしている場合にインターネットからの攻撃が可能な状態となり、ログインパスワードが読みだされて Wi-Fi ルーター内にアクセスされ DDoS 用プログラムが組み込まれた。

対策 : 最新のファームウエアを適用

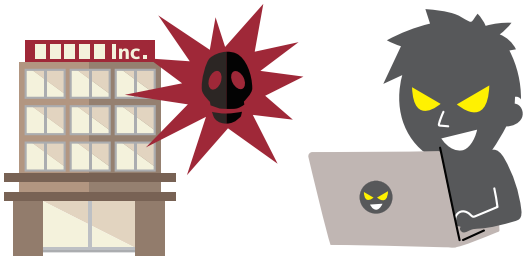
【参考】横浜国立大学 情報・物理セキュリティ研究拠点では、一般の方を対象とした家庭用 Wi-Fi ルーターの IoT マルウェア感染状況、および Wi-Fi ルーターのファームウェア（OS）の脆弱性を診断するサービスを公開しています。

https://1d4fbea64b27a7f05dd5d7ee3e70c10b.ynu.codes/

④標的型攻撃への対策

標的型攻撃は、特定の企業や個人を狙った高度なサイバー攻撃です。攻撃者は、メールや Web サイトを通じてマルウェアを送り込み、機密情報の窃取やシステムの破壊を試みます。

対策としては、不審なメールを開かない、ソフトウェアを最新の状態に保つ、強力なパスワードを設定する、従業員の教育を徹底することが重要です。また、多要素認証の導入や、ネットワークの監視強化も効果的です。さらに、定期的なセキュリティ診断を行い、脆弱性を早期に発見・修正することが求められます。サイバー攻撃の脅威を理解し、最新の対策を行い続けることが、企業全体のセキュリティ意識向上と迅速な対応体制の整備に不可欠です。



■標的型攻撃の例

・A 医療センター（2024 年 5 月）

攻撃者は、フィッシングメールを通じて職員の認証情報を盗み、内部ネットワークに侵入しました。その後、ランサムウェアを使用してシステムを暗号化し、復旧のために身代金を要求しました。この攻撃により、患者の診療記録や個人情報が一時的にアクセス不能となり、医療サービスに大きな影響を与えました。

・A 出版社（2024 年 6 月）

攻撃者はランサムウェアを使用してサーバーに侵入し、動画などのサービスを停止させました。

データを暗号化し、復旧のために身代金を要求しました。この攻撃により、サービスの一時停止を余儀なくされ、ユーザーに多大な影響を与えました。

さらに、攻撃者は内部ネットワークに潜伏し、重要な顧客情報やビジネスデータを窃取しました。

⑤悪意のある Web サイトへの対策

インターネット上には、個人情報の詐取や、パソコンやスマートフォンへのマルウェア感染を狙うなどの悪意を持って構築された危険 Web サイトが多数存在しています。

これらの悪意のある Web サイトは、アドレスを変えて次々と現れるため、危険サイトへのアクセスをブロックするようなセキュリティ対策をすり抜けてしまうケースも多く、利用者自身でも十分な注意を払う必要があります。

悪意のある Web サイトへの誘導は、事業者を装って送信される偽メール、宅配業者の不在通知を装ったショートメッセージ、SNS での拡散など様々な形で行われ、手口も巧妙化しているため、危険だと気づくのが難しくなっています。

このため、どんな場合でも第三者から届いた Web サイトへのリンクは偽物かもしれないとの認識を持ち不用意にアクセスしないことと、ネット銀行など重要なサービスの利用に際しては、スマートフォンにインストールした公式アプリや、自身でブラウザのブックマークに登録したリンクからアクセスするなど、確実に安全と分かる方法でのアクセスを習慣化することを日頃から心掛けましょう。

悪意のある Web サイトによる被害にあわないようにするためにも、脅威事例について知ることは重要です。上述した、偽のメール、ショートメッセージ、SNS などにより危険サイトに誘導されるケースの他、検索サービスの結果に悪意のあるサイトが含まれてしまうケースもあります。また、フィッシングサイトなど、個人情報の詐取を狙うサイトの他、スマートフォンやパソコンへの悪意のあるアプリのインストールを促すサイトや、Web で利用できる無料のファイル変換サービスを装って変換後のファイルにマルウェアを感染させるサイトなど、マルウェア感染を狙う様々な危険サイトも存在します。攻撃者の手口は日々進化し、巧妙化していますので、ニュースで報道される被害事例などにも関心を払い、日々のインターネット利用にも危険が潜んでいることを意識しましょう。

MCPC　情報セキュリティセミナーのご案内

MCPC セキュリティ委員会では、定期的に情報セキュリティセミナーを開催（無料）しています。
ご興味のある方は、以下の QR コード、または URL にアクセスしてください。
以下は、2024 年度の開催実績です。

2024年度	講演タイトル/講師
第15回 2024/6/12	**情報セキュリティ10大脅威2024 組織編**
	独立行政法人情報処理推進機構（IPA） セキュリティセンター 大友 更紗 氏
第16回 2024/10/9	**神奈川県警察本部による講演** 1)身近に迫るサイバー空間の脅威 ～知っておきたいサイバーセキュリティの勘所～ 2)技術情報流出防止について ～技術流出の実態と対策について～
	1) 神奈川県警察 サイバーセキュリティ対策本部 2) 神奈川県警察本部　警備部　外事第一課
第17回 2024/12/11	**攻撃観測と脅威インテリジェンスを融合した サイバー脅威動向把握**
	横浜国立大学 教授　吉岡 克成 氏
第18回 2025/2/12	**フィッシング詐欺の現状**
	JPCERTコーディネーションセンター シニアアナリスト 吉岡 道明 氏
第19回 2025/3/12	**インシデント発生時のセキュリティ・コミュニケーションの要諦**
	日立製作所　デジタルシステム＆サービス統括本部 セキュリティリスクマネジメント本部　セキュリティ戦略企画部 博士（情報学）　加藤 岳久　氏

MCPC 情報セキュリティセミナーはこちらからお申込みください。
https://peatix.com/group/9516863

正しいデータ消去の方法

パソコンの廃棄における情報漏洩リスクを低減するためには、適切な廃棄方法とデータ消去が重要です。日本国内では、メーカーによるリサイクルや家電量販店での回収サービスが一般的です。メーカーのリサイクルサービスでは、公式 Web サイトやカスタマーサービスで詳細を確認し、回収されたパソコンは再資源化施設でデータ破壊や素材の分解が行われます。家電量販店では、新しいパソコン購入時に古いパソコンを回収するサービスを提供しており、データ消去サービスも利用できますが、事前に確認が必要です。

パソコンを廃棄する前にデータを完全に消去することが重要です。OS 標準の削除方法では不十分であり、専門的なツールを使用してデータを消去する必要があります。デバイス廃棄のプロセスは、①利用者からの回収、②データ消去、③廃棄業者への輸送、④最終処分／再資源化のフローを辿ります。各プロセスでのリスクを理解し、適切な対策を講じることが求められます。

データ消去およびデバイスの廃棄工程におけるリスク

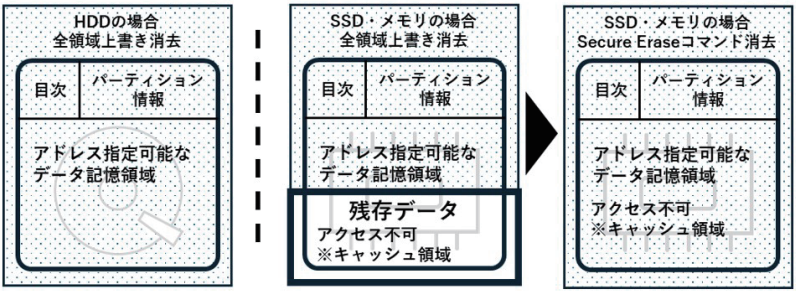
パソコンに内蔵している HDD/SSD 内のデータ消去の方法として、NIST SP800-88 Rev.1 では「消去（Clear）」「抹消（Purge）」「破壊（Destroy）」の 3 つが示されています。
消去はソフトウェアを用いてデータを上書きする方法、抹消は OS からアクセスできない領域も含めてデータを消去する方法、破壊は物理的にデバイスを破壊する方法です。
また、暗号化消去（Crypto-shredding）はデータを暗号化し、暗号化キーを削除することでデータを復号できなくする方法です。

	消去	抹消	破壊
概要	OSで読み書きが可能な領域をアプリケーションで上書き消去する	OSがアクセスできない領域に対してデータの消去をする	ハードウェアを再使用不可能な状態に粉砕溶解する
メリット	・コストが最も抑えられる ・遠隔から消去が可能なツールがある	・データ復元困難な状態にできる ・遠隔から消去が可能なツールがある	・データ復元困難な状態にできる ・電源が入らないデバイス等も消去可能
デメリット	・記憶媒体の性能や容量、上書き回数により消去に時間がかかる場合がある ・LBA(Logical Block Address:)を持たない領域のデータを消去できない場合がある	・ディスクの種類や容量、上書き回数により消去に時間がかかる場合がある ・SecureEraceを用いてもデータの一部が残存する場合がある	・専用の破壊装置が必要、また安全面と騒音への配慮が必要 ・委託する場合は高コストになる ・残存した部品からデータを復元させられる場合もある

データ消去は自社で行うことが望ましく、外部委託する場合は信頼性のある認定業者を選ぶことが重要です。業者の過去の実績や財務状況、技術力を確認し、ISMS などの認証取得状況をチェックします。委託先の現地調査も定期的に実施し、リスクを早期に発見することが求められます。

ISO/IEC 27001:2022 (ISMS)、ISO 14001:2015/AMENDMENT 1:2024 (EMS) などの認証を取得することで、情報セキュリティや環境管理のリスクを低減し、信頼性を向上させることができます。
企業はデータ消去の技術と手法を理解し、適切な消去方法を選択・適用することで、情報漏洩リスクを抑制し、環境への貢献も意識した資源の再利用に取り組むことが重要です。

HDD、SSD・メモリのデータ消去手法



世の中で騒がれているけど何のこと？

①Windows 10 のサポート終了とは何のこと？

- 新たな機能の提供や現行の機能改善、セキュリティアップデート対応などが行われなくなります。
- Windows 10 のサポート終了日は、2025 年 10 月 14 日です。

製品発表のリリース後の Microsoft の製品ライフサイクルポリシーについては、製品、バージョンなどにより異なることがあります。詳しくは、以下のマイクロソフト株式会社の公式リンク先をご参照し、ご購入元、または、Microsoft アカウント担当者にお問合せください。

< ライフサイクルに関する FAQ - 拡張セキュリティ更新プログラム >
https://learn.microsoft.com/ja-jp/lifecycle/faq/extended-security-updates

<2025 年 10 月 14 日 Windows 10、Office 2016 & Office 2019 サポート終了で世界は変化する >
https://www.microsoft.com/ja-jp/biz/smb/win10eos

< 概要 - 製品のサポート終了と廃止 - Microsoft Lifecycle | Microsoft Learn>
https://learn.microsoft.com/ja-jp/lifecycle/overview/product-end-of-support-overview

②終了後はどうなるのかな？

- セキュリティ上のリスクを低減した修正プログラムは配布されません。ただし、特定の製品に対しては延長セキュリティ更新プログラム（ESU）が有償にて提供されることがあります。詳細は以下のマイクロソフト株式会社のリンク先の参考情報をご覧下さるか、購入元へお問合せください。

<Windows 10 Home and Pro>
https://learn.microsoft.com/ja-jp/lifecycle/products/windows-10-home-and-pro

<Windows 10 Enterprise and Education>
https://learn.microsoft.com/ja-jp/lifecycle/products/windows-10-enterprise-and-education

< ライフサイクルに関する FAQ - 拡張セキュリティ更新プログラム >
https://learn.microsoft.com/ja-jp/lifecycle/faq/extended-security-updates

- Windows11 の新機能に特化した、新しいアプリや新しい外部デバイスが使えなく可能性があります。詳細は、ご購入元、アプリの開発メーカー、外部デバイスメーカーにお問合せ下さい。
- Windows Update のサポート（セキュリティアップデート）が受けられないとセキュリティリスクが高まります。
- 追加の個別有償サポート契約（ESU：Extended Security Updates）をMicrosoft 社と締結することも可能です。
- 詳細については、以下のマイクロソフト株式会社のリンク先の参考情報をご覧下さるか、購入元へお問い合わせください。

<Windows 10 の拡張セキュリティ Updates (ESU) プログラム >
https://learn.microsoft.com/ja-jp/windows/whats-new/extended-security-updates

< ライフサイクルに関する FAQ - 拡張セキュリティ更新プログラム >
https://learn.microsoft.com/ja-jp/lifecycle/faq/extended-security-updates

③サポート期間内は何をすればよいのか？

- アプリケーションソフトウェアの更新
  （例：ブラウザやオフィススイートの最新版インストール）
- OS のセキュリティパッチの更新（Windows Update）
- OS のセキュリティパッチ提供期間内のバージョンアップグレード 「PC 正常性チェック アプリ」を利用し、Windows 11 へのアップグレードが可能かどうかをチェック
  例）「スタート」→「設定」→「更新とセキュリティ」と進み、「Windows Update」で確認

④アップグレードの導線はどこかな？

- 必ず公式サイトに自らアクセスしてください。
- 各組織の IT 管理部門の指示 / 手順に従ってください。

<Windows 11 無償アップグレード方法や条件を解説 >
https://www.microsoft.com/ja-jp/biz/smb/column-windows-11-free-upgrade

【用語解説】

頁	用語名	意味
2	CVE登録	CVEとは共通脆弱性識別子 (CVE)を指す。CVE登録とは一般公開されているコンピュータセキュリティの脆弱性リストへの登録を意味します。
3	ウイルス	他のプログラムに感染し、自身をコピーして拡散するマルウェア。
3	ワーム	ワームは、ネットワークを通じて自己複製し、システムに損害を与えるソフトウェアです。ワームは、感染したシステムから他のシステムに拡散し、ネットワーク全体に影響を与えることがあります。ワームは、システムの動作を遅くしたり、ネットワークトラフィックを増加させたりすることがあります。
3	トロイの木馬	トロイの木馬は、正当なソフトウェアに見せかけてシステムに侵入し、悪意のある活動を行うソフトウェアです。ユーザーがトロイの木馬をインストールすると、攻撃者がシステムにアクセスし、データを盗んだり、システムを操作したりすることができます。
3	スパイウェア	スパイウェアは、ユーザーの情報を密かに収集し、第三者に送信するソフトウェアです。これにより、ユーザーのオンライン活動が監視され、個人情報が盗まれる可能性があります。スパイウェアは、ユーザーの許可なしにインストールされることが多いです。
3	アドウェア	アドウェアは、ユーザーのコンピュータに広告を表示するために設計されたソフトウェアです。通常、ユーザーの許可なしにインストールされ、ポップアップ広告やバナー広告を表示します。これにより、ユーザーのブラウジング体験が妨げられることがあります。
3	ランサムウェア	ランサムウェアは、システムやデータを暗号化し、復号のために身代金を要求するソフトウェアです。攻撃者は、ユーザーが身代金を支払うまでデータをアクセス不能にします。ランサムウェアの被害は、企業や個人に大きな経済的損失をもたらすことがあります。
4	WPA2	Wi-Fi暗号化プロトコル。高い安全性を提供する。WPA3はより強固なセキュリティ機能を備えています。
4	WPA3	
4	SSID	Wi-Fiネットワーク名で、非公開設定によりセキュリティ向上が可能です。
4	DDoS	分散型サービス妨害攻撃で、多数のデバイスが標的を一斉攻撃する手法です。
4	踏み台	DDoS攻撃などでWi-Fiルーターやパソコン、IoTデバイスなどが悪用される状態。
5	多要素認証	パスワードに加えて、スマートフォンや指紋などの追加情報を使う認証方法です。
6	フィッシングサイト	実在の企業やサービスを装った偽のWebサイトで、個人情報を不正に取得します。
8	NIST SP800-88 Rev.1	データ消去の方法として「消去（Clear）」「抹消（Purge）」「破壊（Destroy）」の3つを示すガイドラインです。これにより、データ消去の標準的な手法が確立されています。
9	ISO/IEC 27001:2022（ISMS）	情報セキュリティ管理の国際規格です。これにより、組織の情報セキュリティ管理体制が評価されます。
9	ISO 14001:2015/ AMENDMENT 1:2024 (EMS)	環境管理の国際規格です。これにより、組織の環境管理体制が評価されます。
10	ライフサイクルポリシー	製品やサービスのサポート期間や、オブジェクトの保存期間などを定めたポリシーです。

詳細な用語解説いついては、こちらから参照してください。
https://www.mcpc-jp.org/pdf/mcpc_security_2505T.pdf

MCPC セキュリティ委員会　冊子企画・編集メンバー

委員長	鷲尾 諭	NTT コミュニケーションズ株式会社
副委員長	窪田 歩	株式会社 KDDI 総合研究所
委員会メンバー	安達 智雄	日本電気株式会社
	今井 正治	京都情報大学院大学
	岩木 邦彦	ソフトバンク株式会社
	内田 敏晶	三和電子株式会社
	加藤 貴	ワンビ株式会社
	多賀谷 裕	情報通信ネットワーク産業協会
	島本 幸夫	株式会社日立製作所
	華井 克育	モバイルコンピューティング推進コンソーシアム（MCPC）
	濱田 圭	富士通クライアントコンピューティング株式会社
事務局	野村 宏	モバイルコンピューティング推進コンソーシアム（MCPC）

※企画・編集メンバーは 2025 年 3 月現在のメンバーです。

※本冊子に記載されている社名および製品名は、各社の登録商標または商標であり、それぞれの所有者に帰属します。また、本冊の著作権は、MCPC に帰属します。

【MCPC について】
ワイヤレスデータ通信とコンピューティングシステム（モバイルシステム）の普及を促進するために、1977 年我が国を代表する移動体通信会社、コンピュータハードウェア／ソフトウェア会社、携帯電話会社、システムインテグレータなどにより組織化さました。現在、世界をリードするワイヤレステクノロジーにより最先端の IoT・AI ソリューションを追求した飛躍的発展を目指しており、そのための技術課題への対応、運用課題の調査・研究、開発の推進、標準化、相接続製互検証、普及啓発活動、人材育成などの活動を行っています。さらには、米国姉妹組織の USB-IF、Bluetooth SIG などと連携を図りながら、モバイル利活用の IoT･AI ソリューションの市場拡大と利用環境の高度化に務めています。
（2025 年度 3 月現在　会員会社数 162 社）

［総務省後援］ワイヤレスIoTプランナー検定

https://www.mcpc-jp.org/wip-kentei/kentei_msg_kiso/
https://www.mcpc-jp.org/wip-kentei/kentei_cbt_kiso/

本検定資格制度は DX(デジタルトランスフォーメーション) 導入の資格です。
企業、自治体、団体で DX 推進の中核リーダに IoT、5 G、AI などに関する基礎知識を認定します。
このたび、本検定のテキストを第 3 版に改訂いたしました。第 3 版では、最近、急速に注目を浴びている生成 AI に関する記述を充実させ、その他にも GX(グリーントランスフォーメンション)、次世代のオール光ネットワーク、非地上系ネットワークなど新しい技術を取り込んでいます。
このテキストで、検定試験にチャレンジされてはいかがでしょうか！

DXを推進する
MCPC

本冊子ダウンロード用2次元コード
https://www.mcpc-jp.org/pdf/mcpc_security_2505.pdf

MCPC　情報セキュリティ読本　「誰でもわかるセキュリティ入門」

発　行　元：モバイルコンピューティング推進コンソーシアム（MCPC）
【法人番号：9700150005356】
発　行　日：2025年5月（初版）
編 集・制 作：セキュリティ委員会
問合わせ先：MCPC　事務局
〒105-0011　東京都港区芝公園3-5-12 長谷川グリーンビル2F
TEL：03-5401-1935　FAX：03-5401-1937
E-mail：office@mcpc-jp.org　　URL：https://www.mcpc-jp.org/

本冊子の一部あるいは全部について、モバイルコンピューティング推進コンソーシアム（MCPC）に無断で複写・複製・転載することを禁じます