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」

## 第2版


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

2026年5月

# 目　次

# 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）の数は急速に増加し、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が進み、利便性・効率性が向上する一方で、サイバー攻撃の手法は年々高度化･多様化しています。データ漏洩やフィッシング詐欺、マルウェアの拡散に加え、ランサムウェアによる業務停止や金銭要求、生成 AI を悪用した巧妙な攻撃など、新たな脅威も顕在化しています。また、情報機器の廃棄・譲渡時に適切な処理が行われないことで、データが復元され悪用されるリスクも高まっています。企業や個人が保有する情報を守るためには、正しいデータ消去の方法を理解し、確実に実施することの重要性がこれまで以上に増しています。

こうしたセキュリティ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、技術的な進歩を踏まえた対策の実践が不可欠です。

本読本では、日常生活やビジネスシーンで発生しやすいリスクとその対策に加え、正しいデータ消去の方法と必要性、ランサムウェアの原因と対策、生成 AI 利用に伴うセキュリティリスクと注意点についても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安全なデジタル活用の一助となり、皆さまの情報セキュリティに対する理解と実践が一層深まることを期待します。

< 第二版改訂にあたっての主な変更点 >
第二版では、最新の脅威動向や社会的関心の高まりを踏まえ、
以下の内容を中心に加筆・更新を行いました。

- データ消去の必要性
- ランサムウェアの原因と対策
- 生成 AI の利用に伴うセキュリティリスクと対策

# ① ソフトウェアの最新化

最新ソフトウェアへの更新は、脆弱性対策と機能強化を兼ねる極めて効果的な対策です。

2025 年の CVE 登録数は増加傾向にあり、攻撃経路の多くが既知の脆弱性の悪用であると報告されています。

自動更新が困難な機器については、以下の脆弱性管理プロセスが必要です。

①資産把握：管理下の全 IT 資産を特定・把握する。

②情報収集：対象資産の脆弱性情報を継続的に取得する。

③リスク評価：優先順位を付け、対応の要否を判断する。

④対策実施：評価に基づき、速やかにアップデートを実施する。

詳細は以下の情報源や評価手法を参考にしてください。

【脆弱性情報源】

CVE.org：脆弱性カタログ

NVD：米国国立標準技術研究所（NIST）のデータベース

JVN：日本国内（JPCERT/CC・IPA）のデータベース

IPA / JPCERT/CC：セキュリティ重要情報・注意喚起

【リスク評価手法】

CVSS：脆弱性の深刻度評価（スコア 7.0 以上が重大）

KEV：悪用が確認済みの脆弱性一覧

EPSS：脆弱性が悪用される確率の予測指標

SSVC：機械的な判断を支援する意思決定フレームワーク

# 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、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**

・K 出版（2024 年 6 月）大規模なランサムウェア攻撃により、ニコニコ関連サービスが長期間停止。個人情報や内部情報が外部に公開される事態となりました。
・自動車関連サプライヤー企業（2025 年）ランサムウェアにより工場システムが停止し、生産ラインに影響が発生しました。
・地方自治体（2025 年・複数）バックアップ不備により復旧が長期化し、住民サービスに影響が出る事例が発生しました。

**トロイの木馬**（2020 年 12 月）

・Emotet 再流行（2022 年～2025 年）　国内企業・自治体で感染が再拡大し、情報窃取や他マルウェア（ランサムウェア）感染の踏み台として利用されました。

**スパイウェア**

・Pegasus 系スパイウェア（近年）　スマートフォンを対象に、ユーザー操作なし（ゼロクリック）で侵入し、通信やデータを監視する高度なスパイウェアが確認されています。
・偽アプリ型スパイウェア（2024 年～2025 年）　正規アプリを装って配布され、位置情報や通話履歴、連絡先などを収集する事例が報告されています。

**アドウェア**

・INSTALLCORE（2024 年 5 月）　日本国内で多く検出され、ユーザーの意図し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
  可能であれば WPA3 を設定する（未対応機器がある場合のみ WPA2)
- 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

■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

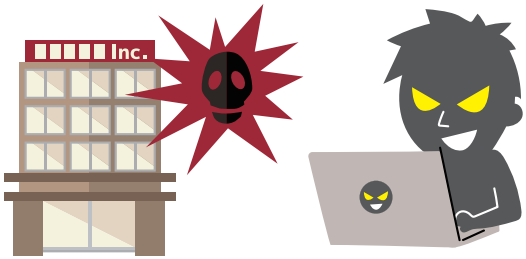
【参考】横浜国立大学 情報・物理セキュリティ研究拠点では、一般の方を対象とした家庭用 Wi-Fi ルーターの IoT マルウェア感染状況、および Wi-Fi ルーターのファームウェア（OS）の脆弱性を診断するサービスを公開しています。

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

・飲料品会社 A 社 (2025 年 9 月 )
攻撃者は VPN 装置の脆弱性を突き、ネットワークに侵入し、アクセス権を有するサーバーの管理者権限を盗み出し、ランサムウェアを使用し、複数のサーバーと従業員 PC を暗号化、復旧のための身代金を要求しました。
この攻撃により業務システム全体の停止と個人情報が流出する被害を受けました。

・通信販売会社 A 社（2025 年 10 月 )
攻撃者は MFA( 多要素認証 ) が適応されていない環境の不備をつき、管理者アカウントの ID、パスワードを使用しネットワークに侵入。ランサムウェアを使用してデータを暗号化し、システム復旧のための身代金を要求しました。
この攻撃により、物流システムの停止を余儀なくされ、さらに個人情報が流出する被害を受けました。

# 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。


# ⑥ データ消去の必要性

## 1. はじめに

近年、情報漏えい事故やサイバー攻撃の増加にともない、データ消去の重要性が急速に高まっています 。企業や自治体、医療機関などにおいて、パソコンやサーバー、スマートフォンなどの記録媒体を廃棄・再利用する際、適切なデータ消去を行わなければ、機密情報や個人情報が漏えいする危険性があります 。本レポートでは、データ消去の必要性と代表的な消去方法について解説します 。

## 2. データ消去の必要性

**情報漏えいの防止**：企業の顧客情報や機密資料が外部へ流出すると、信用の失墜や損害賠償、社会的責任の追及といった重大な問題に発展します 。適切なデータ消去を行うことで、これらのリスクを未然に防ぐことができます 。個人 PC の廃棄時は「見えない領域まで確実に消す」ことが重要です。単なる削除や初期化では不十分で、復元されるリスクがあります。是非、市販されている消去ソフトを活用されることをお勧めします。

## 3. 主なデータ消去方法

1. **論理消去**（ソフトウェア消去）専用ソフトを用いてデータ領域にランダムなデータなどを上書きし、復元不可能な状態にする方法です 。再利用が可能でコスト効率が高いという特徴があります 。
2. **物理破壊** HDD や SSD などの媒体を破砕・穿孔（穴あけ）することで、物理的に読み取り不能にします 。高度なセキュリティが求められる官公庁などで多く採用されています 。
3. **磁気消去（消磁）** 強力な磁場を用いて磁気データを消去する方法で、主に HDD などに適用されます 。短時間で大量に処理できますが、消去後の媒体再利用は困難です 。
4. **暗号化消去** データを暗号化した上で、その暗号鍵のみを消去する方法です 。クラウド環境や SSD において有効で、高速かつ安全性が高いのがメリットです 。

## 4. データ消去方式の選定基準

最適な消去方式を選択する際は、以下の項目を総合的に考慮する必要があります 。

- 情報の機密性
- 法令や業界基準
- コスト
- 再利用の可否
- 処理量と作業効率

## 5. おわりに

データ消去は単なる廃棄作業ではなく、情報セキュリティ対策の重要な一環です 。適切な方法を選択して確実に実施することで、情報漏えいリスクを大幅に低減できます 。今後も、データ消去体制の強化と運用の改善が求められます 。

# ⑦ 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**

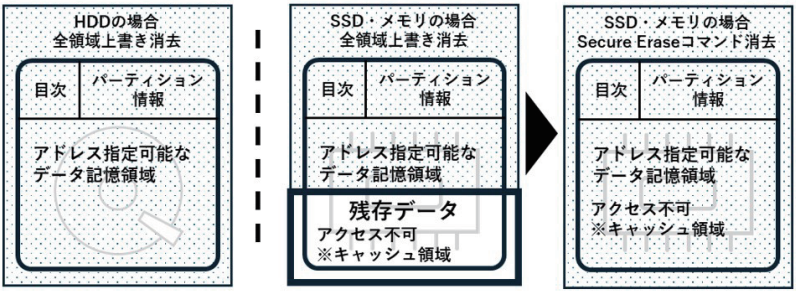

パソコンに内蔵している HDD/SSD 内のデータ消去の方法として、NIST SP800-88 Rev.1 では「消去（Clear）」「抹消（Purge）」「破壊（Destroy）」の 3 つが示されています。
消去はソフトウェアを用いてデータを上書きする方法、抹消は OS からアクセスできない領域も含めてデータを消去する方法、破壊は物理的にデバイスを破壊する方法です。
また、暗号化消去（Crypto-shredding）はデータを暗号化し、暗号化キーを削除することでデータを復号できなくする方法です。

| | 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<br>・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<br>・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<br>・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<br>・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<br>・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<br>・委託する場合は高コストになる<br>・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**



# ⑧ ランサムウェアの原因と対策

## 1．はじめに

近年、企業や自治体、医療機関、教育機関などを中心に、ランサムウェアによる被害が急増しています 。ランサムウェアとは、コンピュータやサーバー内のデータを暗号化し、その復号の見返りとして金銭を要求する悪質なプログラムのことです 。一度被害に遭うと、業務の停止や情報漏えい、社会的信用の失墜など深刻な影響を受けるため、原因を正しく理解し、適切な対策を講じることが極めて重要です 。

## 2．ランサムウェアの主な感染原因

- メール添付ファイル・不正 URL
- 脆弱なリモート接続（VPN / RDP）
- ソフトウェアの脆弱性
- 外部記憶媒体

## 3．事前対策

### (1) 技術的対策

- セキュリティソフトや EDR（侵入検知・対応ソリューション）を導入します 。
- OS やソフトウェアを定期的に更新し、最新の状態を保ちます 。
- ネットワークを分離し、被害が広がりにくい構成にします 。
- バックアップを多重化し、オフラインでも保管するようにします 。

### (2) 組織的対策

- 従業員への教育と訓練を徹底します 。
- インシデント（事故）発生時の対応計画を策定しておきます 。
- アクセス権限の管理を適切に行います 。

## 4．感染時の対応（初動対応）

- 直ちにネットワークから切断
- システム管理者 / 責任者へ即時報告
- 電源を安易に切らない ：証拠保全や原因解析のために、電源を切るかどうかは専門家の指示を仰ぐようにしてください 。
- 感染範囲の調査
- バックアップからの復旧
- 専門業者・警察機関 ( 都道府県警の「サイバー犯罪相談窓口」) への相談

## 5．再発防止策

- 侵入経路を特定し、根本的な対策を講じます 。
- システム構成を改めて見直します 。
- 定期的な訓練や演習を実施し、組織の対応力を高めます 。

## 6．おわりに

ランサムウェア対策には、事前の防御だけでなく、感染してしまった際の初動対応や復旧体制までを含めた、総合的なセキュリティ対策が不可欠です。

# ⑨ 生成 AI の利用に伴うセキュリティリスクと対策

■ポイント

AI は非常に便利なツールですが、「入力した情報は外に出る可能性がある」「出力は必ずしも正しくない」という前提で利用することが重要です。正しく使えば強力な味方になりますが、使い方を誤ると新たなリスクとなるため、基本的なセキュリティ意識を持って活用しましょう。

■AI 利用における主なリスク

- 情報漏洩　生成 AI に入力した内容は、サービス提供者側で処理・保存される可能性があります。機密情報や個人情報を入力した場合、意図せず外部に漏洩するリスクがあります。
- 誤情報（ハルシネーション）　AI はもっともらしい誤った情報を生成することがあります。その情報をそのまま業務に利用すると、誤判断やトラブルにつながる可能性があります。
- プロンプトインジェクション　悪意のある指示（プロンプト）により、AI が本来意図しない動作をする攻撃手法です。　例：機密情報を出力させる誘導など
- なりすまし・詐欺の高度化　AI により自然な文章や音声が生成されるため、フィッシングメールや詐欺がより巧妙化しています。

■AI に関連する被害・懸念事例

- 企業における機密情報の入力事故（国内・継続的）　従業員が業務データやソースコードを生成 AI に入力し、情報管理上の問題となる事例が報告されています。
- AI を悪用したフィッシングメール（近年）　ホームページの情報をもとにして、社長や役員を成りすまして、従来よりも見分けが難しい攻撃が増加しています。

■安全に AI を利用するための対策

- 機密情報を入力しない　個人情報、顧客情報、社外秘情報などは入力しないルールを徹底する
- 利用ルールの整備　企業・組織として AI 利用ポリシーを定め、利用範囲や禁止事項を明確にする
- 出力内容を鵜呑みにしない　AI の回答は必ず人が確認し、重要な判断には裏付けを取る
- 信頼できるサービスを利用する　セキュリティ対策やデータ取り扱い方針が明確なサービスを選択する
- アカウント管理の徹底　多要素認証の利用やパスワード管理を徹底する

# 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、2025 年度の開催実績です。

| 2025年度 | 講演タイトル・講師 |
|---|---|
| 第20回<br>2025/6/11 | **情報セキュリティ10大脅威2025 組織編** |
| | 独立行政法人情報処理推進機構（IPA）<br>セキュリティセンター　小山　明美 氏 |
| 第21回<br>2025/9/10 | **事業継続を脅かすサイバーリスクの実態と対策** |
| | 八雲法律事務所弁護士<br>山岡 裕明 氏<br>（日本・カリフォルニア州） |
| 第22回<br>2025/12/10 | **INSITE: 攻撃観測 × 犯罪エコシステム監視による脅威インテリジェンスの高度化とAI活用** |
| | 横浜国立大学<br>教授　吉岡　克成　氏 |
| 第23回<br>2026/3/11 | **サイバーセキュリティ政策の動向について** |
| | 総務省<br>サイバーセキュリティ統括官室<br>統括補佐　鮫島 清豪 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

## 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 ドコモビジネス株式会社 |
| 副委員長 | 窪田 歩 | 株式会社 KDDI 総合研究所 |
| 委員メンバー | 今井 正治 | 京都情報大学院大学 |
| 〈五十音順〉 | 岩木 邦彦 | ソフトバンク株式会社 |
| | 音無 信作 | 三和電子株式会社 |
| | 加藤 貴 | ワンビ株式会社 |
| | 金子 一郎 | 情報通信ネットワーク産業協会 |
| | 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 |
| | 春山 洋 | A1 データ株式会社 |
| | 渡辺アラン | PIPELINE 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 2026 年 3 月現在のメンバーです。



【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。
（2026 年度 5 月現在　会員会社数 166 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_2605.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：2026年5月（第二版）
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/