

対策①



初期認証情報(パスワード等)の変更

初回ログイン時に最初に設定されている認証情報(パスワード等)を強制的に変更させる。

初期パスワードは製造時に設定されているもので、共通のパスワードが用いられていることが多くあります。

これを放置すると外部からの攻撃者による不正アクセスのリスクが高くなります。

このリスクを防ぐために、システム上で初回ログイン時に強制的に変更させる機能を実装することも重要な対策になります。

対策①



初期認証情報(パスワード等)の変更

初回ログイン時に最初に設定されている認証情報(パスワード等)を強制的に変更させる。

初期パスワードは製造時に設定されているもので、共通のパスワードが用いられていることが多くあります。

これを放置すると外部からの攻撃者による不正アクセスのリスクが高くなります。

このリスクを防ぐために、システム上で初回ログイン時に強制的に変更させる機能を実装することも重要な対策になります。

対策②



強力な認証方法を導入

認証を容易に突破されないように強力な認証方法を選択する。

例)

強力なパスワード※を設定する。

2段階認証を実装する。

生体認証を実装する。

※ 英数大文字混合12桁以上など

強いパスワードは非常に有効なセキュリティ対策です。

簡単なパスワードは推測されやすく、不正アクセスのリスクがあります。

長く、文字や数字、記号を組み合わせたパスワードがおすすめです。

また、生体認証や2段階認証を実装することもセキュリティレベルを高めることができます。

対策③



認証情報の適切な管理

パスワード等の認証情報は適切な保管方法を選択して管理する。

例)

- ・端末に平文で保管せずハッシュ化して保存する。
- ・パスワードをメモして保存しない。

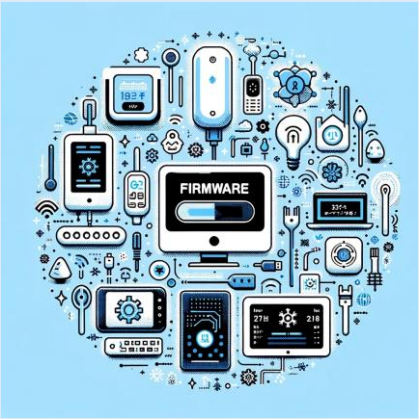
認証情報とは、パスワードやIDのことで、これらは個人を識別しシステムへのアクセスを許可する鍵です。

これらの管理が不十分だと、情報を盗まれたり、悪用される可能性があります。

例えば、IoTデバイスの端末に平文でパスワードを保存するのではなく、ハッシュ化(逆変換が原則不可能で第三者悪用リスクを大幅に減らす)して保管する。

また、パスワードを付箋などに書いて机上に保管するのは極めて危険です。

対策④



ファームウェアの更新 又は パッチの適用

定期的なファームウェア更新とセキュリティパッチ適用を迅速に実施する。

システムやソフトウェアには意図しない弱点や欠陥である脆弱性が日々見つかり、攻撃者はこのような脆弱性を「入り口」として悪用することでサイバー被害が発生します。

ファームウェア更新やセキュリティパッチ適用を定期的の実施することで、攻撃者にとっての「入り口」を塞ぐことができます。

*ファームウェアとは、電子機器に組み込まれたハードウェアを制御するソフトウェアのことを言います。

対策⑤



脆弱性情報の収集

利用しているソフトウェア・システムの脆弱性情報を定期的に収集する。

脆弱性情報の収集は、システムやソフトウェアの弱点を知るために重要です。

この情報を定期的に集めることで、どこが攻撃されやすいかを把握し、適切な修正や保護策を早急に施すことができます。

弱点を早く修正することで、悪意のある攻撃者がその弱点を利用する前に防ぐことが可能となり、情報やシステムの安全を守ることにつながります。

自分たちで情報収集が難しい場合は、契約に含めることも有効な手段です。

対策⑥



ファイアウォールの導入

ファイアウォールをネットワークの境界に設置し、IPアドレスやポートをシステムに必要な最低限のものに制限する。

ファイアウォールは、インターネットからの不正なアクセスを防ぐ壁のようなものです。

特定の「入り口」(ポート)や「住所」(IPアドレス)を制限することで、外部からの危険をブロックし、安全にコンピュータを使用できるようにします。

このように制限を設けることは、不審なアクセスを防ぎ、情報を守る上でとても重要です。

対策⑦



リモートアクセスにおける
VPNの導入

離れたネットワークからアクセスを行う際は、VPN(仮想専用ネットワーク)機能などを用いてセキュリティを確保する。

IoTデバイスは、個人情報や重要データを扱うことが多く、情報保護が重要です。

VPN (仮想プライベートネットワーク)を利用することで、データの通信が暗号化され、盗聴や改ざんのリスクを下げて安全に情報を送受信することができます。

また、近年はVPN機器の脆弱性を狙った攻撃も多発しているためバージョンアップが非常に重要な対策になります。

対策⑧



アクセスログを確認し、不審なアクセスが無いか確認する。

**ネットワーク機器のアクセスログを確認し、
不審なアクセスが無いか確認する**

ネットワークに接続した際、ネットワーク機器にアクセスしたログが残ります。

これを定期的に確認することで、普段と違う不審なアクセスを早く発見できます。

例えば、いつもと違う時間に誰かがシステムを使っていたりすると、攻撃者の可能性があるため調査が必要です。

対策⑨



送受信するデータを暗号化

送受信するデータを暗号化し、第三者が盗聴しても読み取れないように保護する。

データを暗号化することは、手紙に封をするようなものです。

ネット上で情報が盗まれても、その内容の解読を困難にします。

暗号化されたデータは、正しい鍵を持っている人にしか読めません。

暗号化技術は様々あり、解読されている技術もあるため、都度有効な技術を選択する必要があります。

対策⑩



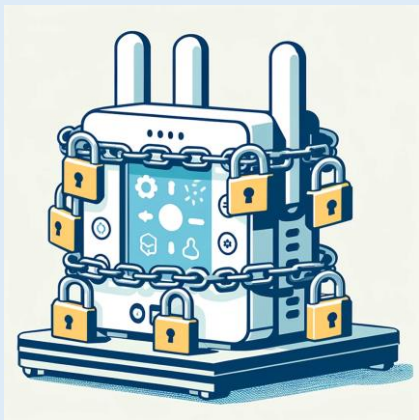
デバイスのストレージ暗号化

データをデバイスに直接保管する場合、
デバイスのストレージを暗号化する。

ストレージの暗号化は、機密性を確保し、不正アクセスから情報を守るために重要です。暗号化はデータを読み取り困難な形式に変換し、盗難や不正利用から保護します。これにより、個人情報や機密データが漏洩するリスクを軽減することができます。

対策

②



デバイスの物理的な
セキュリティの強化

デバイスが物理的に侵入され不正をされないようにセキュリティ対策を強化する。

例)

施錠

監視カメラ

入退管理

IoTデバイスは、家電やセンサーなどインターネットに接続される機器です。

これらのデバイスの物理的なセキュリティ対策が重要で、盗難や破壊から守ることが必須です。

不正にアクセスされたり、物理的に損傷を受けたりすると、情報が漏れたりシステムが乗っ取られるリスクがあります。

そのため、適切な場所に設置し、セキュリティを確保することが、情報保護のために非常に重要です。

対策⑫



資産管理の実施

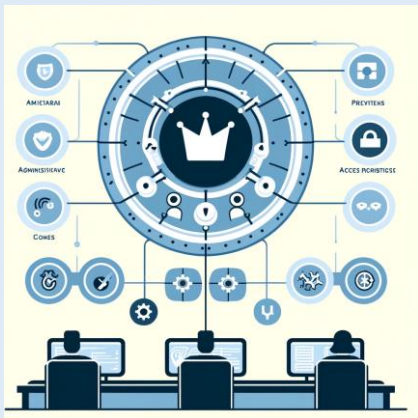
資産台帳を作成し、定期的に資産の棚卸を実施することで資産管理を行う。

資産管理とは、会社のコンピューターやデータなど、重要な資産を把握し管理することです。

これにより、どの資産がどこにあるのか、どれが保護が必要かを分類し、セキュリティ対策を適切に行うことができます。

資産が明確でないと対策漏れが発生し、盗難や不正アクセスのリスクが高まり、重要な情報が漏れる可能性があります。

対策 ⑬



アクセス管理の実施

アクセス管理を実施し、必要な権限を持つユーザーのみがアクセスできるようにする。

アクセス管理は、重要な情報へのアクセスを特定の人だけに限定する仕組みです。これにより、不正なアクセスや情報漏洩を防ぎ、安全を保つことができます。

必要な人だけに権限を設定することが、情報の保護には不可欠です。

対策 ⑭



クラウドサービスの
セキュリティ機能の利用
(不正アクセス検知)

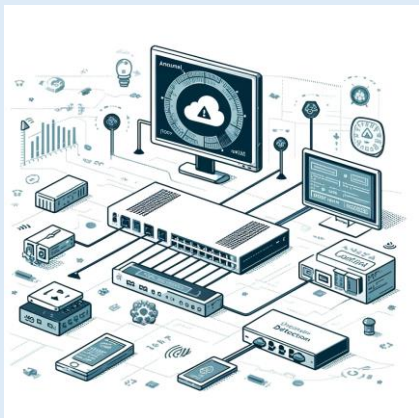
クラウドサービスのセキュリティ機能を活用することで不正アクセスを検知、防止する。

クラウドサービスには、不正なアクセスを見つけて防ぐ機能が備わっています。

これを使うことで、情報が盗まれるのを効果的に防ぐことができます。

安全に情報を管理するために、これらの機能の利用は非常に重要です。

対策 ⑮



ネットワークトラフィック監視

ネットワークのトラフィック(通信量)を監視し、異常発生時にアラートを発報する。

通信の異常を監視し、通常と比較して通信量が増えている(又は減っている)際に気付くことができる仕組みを導入する。

このように通常状態を監視することは、侵入を早く察知し情報を守るために大切です。

対策 ⑬



データ改ざんを検知する。

データの整合性チェックを実施し、データ改ざん時にアラートを発報するシステムを導入する。

IoTデバイスは日常のさまざまな機器がインターネットにつながって情報を送るものです。

これらの機器からのデータが正しいかを確かめ、いたずらに変えられたらすぐに知らせる仕組みは、安全な使い方を守るためにとっても重要です。

対策

⑪



アカウントの棚卸し

定期的にアカウントの棚卸しを実施するとともに、退職者や異動者が現れた場合に即座にアカウントの削除を行う

アカウントの中には強い権限を持ったものも存在し、データの書き換えや削除などできる場合があります。

不要アカウントを逐次削除することで不正利用を最大限防ぎましょう。

加えて消し忘れがないかチェックすることも大切です。

対策 ⑮



公開範囲を限定的にする

クラウドサービスの公開範囲を限定する

クラウドサービスは自社にサーバを設置せずとも利用できるサービスです。

正しく公開範囲を設定しなければ自社の情報が公開されてしまう恐れがあります。

対策 ⑱



権限設定の見直し

**社員に払い出しているアカウントの権限を
都度見直す**

**必要なシステムに必要な人だけがアクセス
できる状況を徹底しましょう。**

**不必要に閲覧・修正が可能な状況であると、
情報漏洩や改ざんのリスクが高まります。**

対策

20



規程やルールを作成・修正

規程の内容を見直し、システム利用に関する制約を設ける。

システム側で制限を強くしすぎると、通常の業務・作業に影響が出る恐れがあります。

システムの新規導入や改修する際は、業務影響も加味し、システム側で制限を強くできない場合は規程やルール等で制限を設けることも重要です。

対策 ②



Webサイトのセキュア化

Webサイトの入力欄で不正なコードを実行できないようにセキュア化する

通常Webサイトを利用している場合、入力フォームに特定のコードを入力することで予期せぬ挙動を行う攻撃が存在します。

実行された場合、同じサーバ上のファイルやパスワードが漏洩してしまったり、公開している内容が書き換えられてしまう可能性があるため、対策が必要です。

対策 ②②



利用できる端末の制限

重要なシステムにおいてアクセスできる端末を制限する。

個人情報など特に重要なファイルを扱うサーバには、より強力なセキュリティを施す必要があります。

特定の鍵を持たせたPC以外からはアクセスを受け付けないなどアカウント以外の制御の方法も検討しましょう

対策

23



セキュリティ教育

システムの利用に当たって Eラーニングを実施する

会計情報に触ることができるユーザに対して倫理教育を実施する。

違反時の罰則がある場合、内容を伝えておくことで抑止力の効果を期待する。