NKサイバーセキュリティワークショップ

IACS UR E27の要件説明

29 May 2024

日本海事協会　機関部
電気・制御部門

01. 使用者（人）の識別及び認証

コンピュータシステムは、直接又はインターフェースを介してシステムにアクセス可能なすべての使用者（人）を識別及び認証するものでなければならない。

■ 概要

システムにアクセス可能なすべての人を識別及び認証する

識別	各使用者を区別すること
認証	使用者が本人であることを証明すること

■ 目的

認められていない人からのアクセスから保護するため

■ 対策

すべての使用者（人）を識別及び認証する機能
例｜アカウント機能

■ 補完的対策

例｜物理的なセキュリティ対策
あらかじめ決められた人員が管理する鍵で操作できない構造とする

■ ポイント

・システムの用途によって、使用者（人）をどの程度識別する必要があるかを検討する。例えば、PLCのみのコンピュータシステムに対して、人間一人ひとりを識別及び認証する機能は不要である。

02. アカウントの管理

ClassNK

コンピュータシステムは、権限を有する使用者によるすべてのアカウントの管理（アカウントの追加、有効化、変更、無効化及び削除を含む）をサポートする機能を提供するものでなければならない。

■ 概要

すべてのアカウントを管理する

■ 目的

システムの使用者を適切に管理するため

■ 対策

すべてのアカウント（追加、有効化、変更、無効化及び削除）を管理する機能

■ 適用

例｜物理的なセキュリティ対策
鍵管理などによって対策されている場合は適用外

■ ポイント

・アカウント機能を実装する必要がないシステムには不要。

https://hatenachips.blog.fc2.com/blog-entry-220.html

03. 識別子の管理

ClassNK

コンピュータシステムは、使用者、グループ及び役割による識別子の管理をサポートする機能を提供するものでなければならない。

■ 概要

使用者、グループ及び役割によって識別子を管理する

識別子	自分自身が誰であるかを示すもの（例：ユーザー名）

■ 目的

使用者の権限を適切に割り当てるため

■ 対策

使用者、グループ及び役割による識別子の管理をサポートする機能
例｜グループアカウントの作成機能

■ 適用

例｜物理的なセキュリティ対策
鍵管理などによって対策されている場合は適用外

■ ポイント

・グループアカウントの作成機能の実装を強制するものではない。使用者に不要な権限を割り当てられないことが重要

https://hatenachips.blog.fc2.com/blog-entry-220.html

04. 認証コードの管理

ClassNK

コンピュータシステムは、次に掲げる機能を提供するものでなければならない。

●認証コードの内容の初期化　●インストール時における全てのデフォルト認証コードの変更

●全ての認証コードの変更／更新　●保存・伝送される全ての認証コードの不正開示及び変更からの保護

■ 概要

認証コードを管理する

認証コード	使用者が自身の身元を証明するための情報

知識情報
パスワード等

所持情報
ICカード等

生体情報
指紋等

■ 目的

認証コードの機密性を確保するため

■ 対策

認証コードを管理する機能

例｜認証コードがパスワードの場合

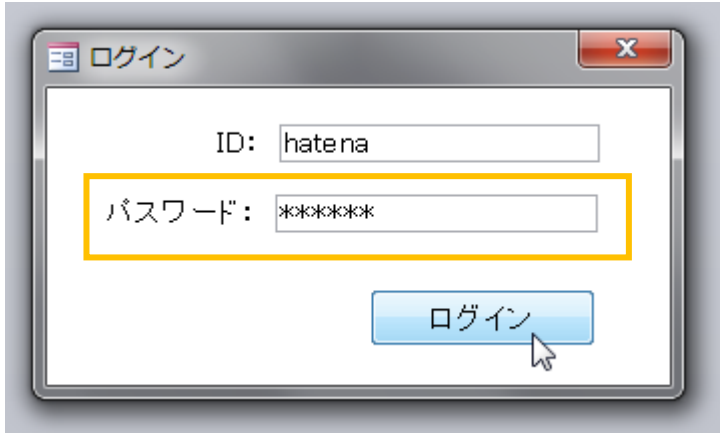
●パスワードの初期化　●初期パスワードの変更

●パスワードの変更　●パスワードの暗号化

■ 適用

例｜物理的なセキュリティ対策

鍵管理などによって対策されている場合は適用外



https://hatenachips.blog.fc2.com/blog-entry-220.html

05. 無線アクセスの管理

コンピュータシステムは、無線通信をするすべての使用者（人、ソフトウェアプロセス又はデバイス）を識別及び認証する機能を提供するものでなければならない。

■ 概要

無線通信をする使用者を識別および認証する

使用者（人）
人間

ソフトウェア
プロセス
プログラム

デバイス
スマートフォン

■ 目的

サイバー攻撃のリスクがある無線通信下でのセキュリティを強化するため

■ 対策

無線通信をする使用者を識別及び認証する機能
例｜IEEE802.1X

■ 適用

例｜無線通信しない場合は適用外

■ ポイント

無線通信はタブレット端末での状態監視などが該当する。この場合、ソフトウェアプロセス及びデバイスに対しても識別及び認証が求められる点に留意する。

06. パスワードによる認証の強度

コンピュータシステムは、パスワードの設定を、最短の長さ及び文字の種類の多様性に基づいて、強化する機能を提供するものでなければならない。

■ 概要

パスワードの設定を、最短の長さ及び文字の種類の多様性に基づいて、強化する

■ 目的

攻撃者によるパスワードの推測を難しくするため

■ 対策

パスワードの設定を強化する機能

■ 補完的対策

例｜多要素認証
認証方法を2要素以上とし、認証の強度を上げる

■ ポイント

・本会は、パスワードの最短の長さ及び文字の種類の多様性に関する基準値を設定しない。コンピュータシステムに基づいて供給者により決定される。

07. 認証時のフィードバック

ClassNK

コンピュータシステムは、認証プロセス中のフィードバックを、明確でないものにしなければならない。

■ 概要

認証プロセス中のフィードバックを、明確でないものとする

■ 目的

認証コードを特定し難くするため

■ 対策

認証プロセス中のフィードバックを不明瞭とする機能
例｜認証コードがパスワードの場合
入力中のパスワードを非表示にする

■ 適用

例｜認証コードがない場合は適用外

■ ポイント

・アカウント機能を実装する必要がないシステムには不要。

https://hatenachips.blog.fc2.com/blog-entry-220.html

08. 権限付与の実施

すべてのインターフェースにおいて，使用者（人）に，職務分離及び最小特権の原則に従って権限を割り当てられるものでなければならない。

■ 概要

使用者（人）は「職務分離」と「最小特権」という2つの重要な原則に従って、権限を割り当てられる

職務分離	一人が全ての権限を持つことを防ぐ原則
最小特権	必要最小限の権限だけを持つという原則

■ 目的

使用者に対して権限を適切に割り当てるため

■ 対策

職務分離及び最小特権の原則に従って権限を割り当てることをサポートする機能

例｜アクセス制御リストによって権限を管理する

■ 補完的対策

例｜物理的なセキュリティ対策

あらかじめ決められた人員が管理する鍵で操作できない構造とする

09. 無線の使用の管理

コンピュータシステムは、一般に受け入れられるセキュリティに関する業界の慣行に従って、システムへの無線接続の認可、監視及び使用制限を実施する機能を提供するものでなければならない。

■ 概要

一般に受け入れられるセキュリティに関する業界の慣行に従って、システムへの無線接続の認可、監視及び使用制限を実施する

認可	特定のリソースや機能へのアクセスを許可又は拒否すること

■ 目的

サイバー攻撃のリスクが高い無線通信下での使用に関するセキュリティをより強化する

■ 適用

例｜無線通信をしない場合は適用外

■ 対策

システムへの無線接続の認可、監視及び使用制限を実施する機能

例｜WPA2-PSK認証の場合

- SSID及び暗号キーによって認証することで、ネットワークへのアクセスを制御（認可）
- PC画面等によって、接続された機器の一覧を確認する（監視）
- MACアドレスフィルタリングにより、特定のMACアドレスを持つ機器のネットワークへのアクセスを制限する（使用制限）

10. 可搬式及び携帯用デバイスの使用の管理

可搬式及び携帯用デバイスの使用に対応したコンピュータシステムは、次に掲げる機能を含むこと。
a) 可搬式及び携帯用デバイスの使用は、設計上許可されたものだけに制限すること。
b) 可搬式及び携帯用デバイスへ／からのコード及びデータの転送を、制限すること。

■ 概要

システムが可搬式又は携帯用デバイスと接続する場合、デバイスを管理する

可搬式及び携帯用デバイス	リムーバブルメディア等

■ 目的

可搬式又は携帯用デバイス経由でマルウェアに感染するリスクを低減するため

■ 対策

可搬式及び携帯用デバイスの使用制限及び転送制限の機能
例｜ホワイトリスト形式

■ 補完的対策

例｜ポートをブロッカーによりブロックする
例｜可搬式及び携帯用デバイスを使用する前に、専用のハードウェアによりマルウェアスキャン及びクリーンアップを行う

■ 補完的対策

例｜可搬式及び携帯用デバイスの使用に対応していない場合は適用外

11. モバイルコード

コンピュータシステムは、Javaスクリプト、ActiveX及びPDFのようなモバイルコードの使用を制御するものでなければならない。

■ 概要

モバイルコードの使用を制御する

モバイルコード	ネットワーク経由で自動的にダウンロード及び実行されるプログラム

■ 目的

自動実行によるマルウェア感染防止のため

■ 対策

モバイルコードの使用を制御する機能

例｜

・ブラウザを削除する

・ポリシーの設定でモバイルコードの動作を禁止する

■ 適用

例｜Webアクセス（クライアント）機能がない場合、モバイルコードが自動的にダウンロードされないため、非適用となる

■ ポイント

「対策」や「適用」の通り、Webアクセス機能がなければ、インターネットからのデータやコードの自動受信は行われないため、モバイルコードが自動的にダウンロードされることは防がれる

12. セッションロック

コンピュータシステムは、設定可能な無操作時間の経過後又は手動によるセッションロックの有効化後に、更なるアクセスを防止することが可能なものでなければならない。

■ 概要

自動または手動いずれかの方法によりセッションをロックできる

セッションロック	システムを一定時間操作しない場合にセッションをロックすること

■ 目的

無操作時間中にセッションが悪用されるリスクを低減するため

■ 適用

例｜HMIを介したセッションを使用しない場合は適用外となる

■ 対策

自動または手動いずれかのセッションロックの機能

■ ポイント

船舶の運航に直接影響を及ぼすシステムについては、自動によるセッションロックにより可用性を損なう可能性があります。

13. 監査可能な事象

コンピュータシステムは、少なくとも次に掲げる事象について、セキュリティに関連する監査記録を作成するものでなければならない：アクセス制御、オペレーティングシステムの事象、バックアップ及び復元の事象、設定の変更、通信の喪失

■ 概要

セキュリティに関する重要な事象の監査記録を作成する

監査記録	セキュリティに関連する記録（ログ）

■ 目的

監査する必要がある重要な事象の発生を記録するため。サイバー攻撃などのインシデントが発生した際、適切な監査記録を通して原因分析を行う。

■ 補完的対策

例｜外部の監視システムにより、監査記録を作成する

■ 対策

監査記録を作成する機能

例｜

アクセス制御	ログイン試行の成否、アクセス権限の変更
OSの事象	OSに関連する記録（起動／停止など）
バックアップ及び復元の事象	データのバックアップ及び復元に関する記録
設定の変更	セキュリティ及びネットワーク設定など
通信の喪失	ネットワーク接続の中断や喪失など

14. 監査用の記憶容量

コンピュータシステムは、監査記録の記憶容量を、ログ管理に関する一般に認識された推奨に従って割り当てる機能を提供できるものでなければならない。監査の仕組みは、当該容量を超過する可能性を下げるように実装されなければならない。

■ 概要

監査記録の記憶容量を超過する可能性を下げるように実装する

■ 目的

十分な量の監査記録を補完するため

■ 補完的対策

例｜リムーバブルメディア等の外部記憶媒体への書き出し機能

■ 対策

必要な期間にわたって監査記録を適切に保管できる記憶容量

■ 適用

例｜外部の監視システムが監査記録を作成する場合は、適用外となる。

■ ポイント

・本会は、記憶容量に関する基準値を設定しない。コンピュータシステムに基づいて供給者により決定される。

15. 監査プロセスの不具合への対応

コンピュータシステムは、監査プロセスの不具合発生時に、不可欠なサービス及び機能の喪失を防ぐ機能を提供するものでなければならない。

■ 概要

・監査プロセスの不具合発生時に、不可欠なサービス及び機能の喪失を防ぐ

■ 目的

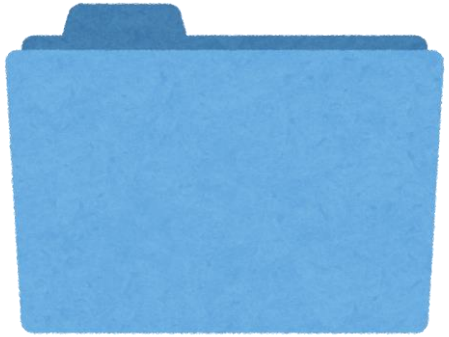
不可欠なサービス及び機能の喪失するリスクを防止するため

■ 対策

・監査プロセスの不具合発生時に、不可欠なサービス及び機能の喪失を防ぐ機能
例｜監査に関わる機能と不可欠な機能を分離する

■ 適用

例｜外部の監視システムが監査記録を作成する場合は、適用外となる。



16. 日時の記録

コンピュータシステムは、監査記録に日時を記録するものでなければならない。

■ 概要

監査記録に日時を記録する

■ 目的

監査が必要となる事象がいつ発生したか等、タイムラインを作成するため

■ 対策

日時を記録する機能
例｜タイムスタンプ（リアルタイムクロックICやシステムクロック等）

■ 適用

例｜外部の監視システムが監査記録を作成する場合は、適用外となる。

■ ポイント

・日時の記録については、他のシステムと同期せず独立した機能とすることで差し支えない。本会としては、システム同士で日時を同期せずとも、十分な監査記録を作成することは可能であるという考えである。

17. 通信の完全性

コンピュータシステムは、伝送される情報の完全性を保護するものでなければならない。
注）無線ネットワークには、暗号化の仕組みが採用されなければならない。

■ 概要

伝送される情報の完全性を保護する

■ 目的

伝送される情報が不当に変更、削除及び破壊されるリスクを防止するため

■ 対策

情報の受信側が情報の改ざんを検証する機能
例｜
・受信データと送信データに相違がある場合、送信元にデータの再送を要求する機能
・受信データと送信データとの相違が続いた場合、警報を発する機能

■ 適用

例｜スタンドアロン型の場合は適用外

■ ポイント

・TCP/IP通信においても規定される要件。シリアル通信の場合は、チェックサムなどでも可。
・無線通信を使用する場合、より強度の高い仕組みとして、暗号技術アルゴリズムを採用しなければならない。

18. 悪意のあるコードからの保護

コンピュータシステムは、悪意のあるコードや不正なソフトウェアによる影響を防止、検知及び低減するための適切な保護手段を実行する機能を提供できるものでなければならない。また、保護の仕組みを更新する機能を有するものでなければならない。

■ 概要

悪意のあるコードや不正なソフトウェアによる影響を防止、検知及び低減するための適切な保護手段を実行する

■ 目的

マルウェアによるリスクを最小化するため

■ 補完的対策

例｜外部のセキュリティデバイスを実装する

■ ポイント

・マルウェアを防止・検知及び低減するものとして、ファイアウォール等の外部のセキュリティデバイスが一般的である。

■ 対策

マルウェアによる影響を防止、検知及び低減するための適切な保護手段を実行する機能

例｜

・ホワイトリスト制限等（防止機能）
・マルウェアスキャン等（検知機能）
・感染端末の隔離等（低減機能）

■ 適用

例｜Windowsベースではない独自のOSにおいて、マルウェアが確認されていない場合は、適用外となる可能性が高い

19. セキュリティ機能の検証

コンピュータシステムは、セキュリティ機能のあるべき動作の検証をサポートし、また、保守中に発生した異常を報告する機能を提供するものでなければならない。

■ 概要

・セキュリティ機能の動作の検証する
・保守中に発生した異常を報告する

■ 目的

X編4章（UR E27）で要求されるセキュリティ機能をシステムに実装し、その機能が要求を満たすための動作が正常に実行していることを確認するため

■ 対策

・セキュリティ機能の検証機能
・保守中に発生した異常を報告する機能

■ ポイント

・これらの機能は、所有者がシステムを保守する際に利用される。統合者がメンテナンスプランを作成するために、この機能に関する記載を「コンピュータシステムの保守・検証手順書」へ含める必要がある。

20. あらかじめ決定した出力

コンピュータシステムは、攻撃により通常の動作を維持できなくなった場合に、出力をあらかじめ指定した状態に設定する機能を提供するものでなければならない。あらかじめ指定した状態とは、次に掲げるものとすることができる。

● 非使用時の状態　●最後の既知の値、又は●固定値

■ 概要

攻撃により通常の動作を維持できなくなった場合に、出力をあらかじめ指定した状態に設定する

非使用時の状態	電源がオフの状態
最後の既知の値	インシデント発生前に出力していた値
固定値	あらかじめ設定された値

■ 目的

機能不全に陥った場合に特定の状態や値を維持することで、システム及び運航の安全性を一時的に確保するため。

■ 対策

・指定した状態へ設定する機能

21. 情報の機密性

コンピュータシステムは、読取りに関して明示的な承認が求められる情報について、保管時であるか伝送中であるかにかかわらず、機密性を保護する機能を提供するものでなければならない。
注：無線ネットワークの場合、伝送中のすべての情報の機密性を保護するために、暗号化の仕組みが採用されなければならない。

■ 概要

読取りに関して明示的な承認が求められる情報について、保管時であるか伝送中であるかにかかわらず、機密性を保護する

読み取り	データベース等から情報を取得すること
明示的な承認	ある使用者に対して、管理者がアクセス等の権限を付与すること

■ 目的

許可された人のみアクセスが可能となる情報の機密性を確保するため

■ 対策

読み取りに関して明示的な承認が求められる情報の機密性を保護する機能

・保管時に情報の機密性を保護する機能

例｜使用者の認証及び認可などのアクセス権に関わる機能や情報を暗号化する機能等

・伝送中に情報の機密性を保護する機能

例｜通信を暗号化する機能。また、一対一での有線接続は、伝送中の機密性の確保につながる。

22. 暗号の使用

暗号を使用する場合、コンピュータシステムは一般に受け入れられるセキュリティに関する業界の慣行及び推奨に従って、暗号アルゴリズム、鍵の長さ及び仕組みを使用するものでなければならない。

■ 概要

・推奨された暗号アルゴリズム、鍵の長さ、仕組みを使用する

暗号アルゴリズム	データを暗号化及び復号化する等、暗号化の手順や規則のこと
鍵の長さ	鍵を校正するビット数
鍵の仕組み	鍵の生成及び管理方法のこと

■ 目的

暗号技術を活用し情報の完全性及び機密性を確保するため

■ 対策

・一般に受け入れられるセキュリティに関する業界の慣行及び推奨に従った暗号技術
例｜ISO/IEC 19790、NIST SP800-57
・「電子政府における調達のために参照すべき暗号のリスト」https://www.cryptrec.go.jp/list.html
・「暗号鍵管理システム設計指針（基本編）」
https://www.ipa.go.jp/security/crypto/guideline/ckms.html

■ 適用

例｜暗号技術を使用する必要がない場合は、適用外となる。

23. 監査ログへのアクセス

コンピュータシステムは、権限を有する人及び／又はツールによる読取り専用での監査ログへのアクセスの機能を提供するものでなければならない。

■ 概要

権限を有する人及び／又はツールが監査ログへ読取り専用でアクセスできる

権限を有する人	監査ログの閲覧を認可された人
権限を有するツール	機能の利用を認可されたプログラム等 例｜SIEM（セキュリティ情報イベント管理）

■ 目的

監査ログの不正利用（閲覧／改ざん）を防止するため

■ 対策

・閲覧権限を有する人及び／又はツールが監査ログに読取り専用でアクセスする機能

■ 適用

例｜監査記録（監査ログ）の作成機能が実装されていない場合は、適用外となる。

24. サービス拒否攻撃からの保護

コンピュータシステムは、DoS事象発生中にも、不可欠な機能を維持するための最小限の機能を提供するものでなければならない。

■ 概要

DoS事象発生中にも、不可欠な機能を維持する

DoS（Denial of Service）	サーバー等に対して大量の情報を送信することで、システムが正常に動作しなくなる攻撃手法

■ 目的

DoS攻撃による不可欠な機能の停止を防止するため

■ 補完的対策

例｜外部のセキュリティ機器により、アクセス可能なIPアドレスに制限をかける

■ 対策

・DoS事象発生中にも、不可欠な機能を維持するための最小限の機能を提供する仕組み

例｜

・通信処理プロセスの優先順位を低くする

・アクセス可能なIPアドレスに制限をかける

■ ポイント

ネットワークの容量が過剰に使用される及びコンピュータのリソースが過剰に消費される等、過負荷に基づくDoS事象を考慮する必要がある。

25. リソースの管理

ClassNK

コンピュータシステムは、リソースを使い果たさないように、セキュリティ機能によるリソースの利用を制限する機能を提供するものでなければならない。

■ 概要

セキュリティ機能によるリソースの利用を制限する

■ 目的

セキュリティ機能によってリソースが不足することを防ぐため

■ 補完的対策

例｜十分なリソースを確保する

■ 対策

リソースの利用を制限する機能

ウイルス対策ソフトのスキャン	システムの稼働時間外でスキャンする。リソースの空容量が一定値を下回った場合スキャンを停止する等
セキュリティログの長期保存	ログを書き出す際に残存容量を確認し、不足しそうな場合は、警報を発する。リングバッファ方式に変更する。
ネットワーク帯域の圧迫	帯域制御により、通信量を制御する

26. システムのバックアップ

コンピュータシステムは、通常の運用に影響することなく、重要なファイルの識別及び場所特定並びに使用者レベル及びシステムレベルでの情報（システム状態に関する情報を含む）のバックアップ 実施をサポートするものでなければならない。

■ 概要

・重要なファイルをバックアップする

・バックアップは通常の運用に影響しない

■ 目的

復旧すべき重要なファイルを確実にバックアップする

■ 対策

復旧すべき重要なファイルをバックアップする機能

・バックアップ動作の通常機能への影響は最小限に

・復旧すべきファイルはシステムごとに決定

■ 補完的対策

例｜予備品との交換（システムそのもの、CDやDVDなどのインストールディスク等）

■ 適用

本要件の目的は、ファイルが改ざんされたり、システムがダウンした場合の復旧です。しかし、プログラムがハードウェアに直接書き込まれている場合、例えば専用の治具を使わないと書き換えられない状況では、バックアップは不要になることがあります。

27. システムの復旧及び再構成

コンピュータシステムは、混乱又は故障の後、既知の保護された状態に復旧及び再構成される機能を提供するものでなければならない。

■ 概要

サイバーインシデントによる混乱又は故障の後、既知の保護された状態に復旧及び再構成される

■ 目的

サイバーインシデントが発生した後、以前の状態へ素早く復旧及び再構成する

■ 補完的対策

例｜予備品との交換（システムそのもの、CDやDVDなどのインストールディスク等）

■ 対策

・リカバリ機能

・システムパラメータがデフォルト又は安全な値であること
・セキュリティに関する重要なパッチが再インストールされること
・セキュリティに関する設定が再確認、再設定されていること
・システム文書及び操作手順が使用可能な状態であること
・アプリケーション及びシステムソフトウェアが安全な設定で再インストールされること
・バックアップデータから情報が復元されていること

28. 代替電源

既存のセキュリティ状態又は文書化された縮退モードに影響することなく、代替電源へ及び代替電源から切り替える機能を提供するものでなければならない。

■ 概要

・セキュリティ機能の動作の検証する

・保守中に発生した異常を報告する

■ 目的

一時的に電源が喪失された場合においても、システムのセキュリティを確保するため

■ 対策

既存のセキュリティ状態又は文書化された縮退モードに影響することなく、代替電源へ及び代替電源から切り替える機能

■ 補完的対策

例｜コンピュータシステムを二重化した上で、一方を代替電源から供給する

■ ポイント

本要件は、システムに対して、代替電源への切り替えを要求するものではなく、「目的」に示す通り、セキュリティ機能によって電源切替えを妨げられないようにするための要件である。

29. ネットワーク及びセキュリティ構成設定

コンピュータシステムのトラフィックは、供給者によって提供される指針にて推奨されるネットワーク及びセキュリティ構成に従って設定される機能を提供するものでなければならない。コンピュータシステムは、現在用いられているネットワーク及びセキュリティ構成の設定へのインターフェースを提供するものでなければならない。

■ 概要

コンピュータシステムのトラフィックは供給者によって提供される指針にて推奨されるネットワーク及びセキュリティ構成に従って設定される機能を実装する

■ 目的

供給者が推奨するネットワークやセキュリティ構成に設定できるようにするため

■ 対策

供給者によって提供される指針にて推奨されるネットワーク及びセキュリティ構成に従って設定できる機能（パラメータの設定等）

例｜

・IPアドレス 、サブネットマスクの設定機能

・セキュリティ機能などに関するパラメータ設定機能

30. 最小限の機能性

次に掲げるもののインストール、可用性及びアクセス権は、システムが提供する機能の厳格な要求に限られなければならない。
・オペレーティングシステムソフトウェアのコンポーネント、プロセス及びサービス
・ネットワークサービス、ポート、プロトコル、ルート及びホストへのアクセス並びにすべてのソフトウェア

■ 概要

不要な機能はインストールしない、利用可能な状態にしない、アクセス可能としない

■ 目的

余計なセキュリティホールの発生を抑制するため

■ 対策

システムの機能、設定情報を最小限にする仕組み

例｜使用しないポートはブロックし必要なポートのみを開放する

■ ポイント

ここでの要件は、システムの機能は必要最小限に保たれる必要があるという原則である。

特にWindowsやLinuxなど汎用的なOSによるシステムである場合には、多くのビルトインサービスが含まれている可能性があり、あらかじめ削除される必要がある。