Ｖ．基準項目

２．システム管理者基準

(1) 管理体制の整備

・システムのセキュリティ方針を確立し、周知・徹底すること。
・システムの管理体制、管理手順を確立し、周知・徹底すること。
・緊急時の連絡体制及び復旧手順を確立し、周知・徹底すること。
・システム管理の業務上知り得た情報の秘密を守ること。
・システム管理者の権限は、業務を遂行する上で必要最小限にすること。
・システム管理者は２人以上かつ必要最小限の管理者で、その業務は定期的に交代すること。
・システム管理者の資格を喪失した者の権限は、速やかに停止すること。

(2) システムユーザ管理

・システムユーザの登録は、必要な機器に限定し、システムユーザの権限を必要最小限に設定すること。
・ネットワークを介して外部からアクセスできるユーザＩＤは、必要最小限にすること。
・ユーザＩＤは、個人単位に割り当て、パスワードを必ず設定すること。
・長期間利用していないユーザＩＤは、速やかに停止すること。
・ユーザＩＤの廃止等の届出があった場合は、速やかに登録を抹消すること。
・パスワードは、当該システムユーザ以外に知らせないこと。
・パスワードのチェックを随時行い、悪いパスワードは、速やかに変更させること。
・パスワードが当該システムユーザ以外に知られた場合又はその疑いのある場合は、速やかに変更させること。
・特権を付与する場合は、当該システムユーザの技術的能力等を考慮すること。
・必要としなくなったシステムユーザの特権は、速やかに停止すること。

(3) 情報管理

・通信経路上の情報は、漏えいを防止する仕組みを確立すること。
・通信経路上で情報の盗聴及び漏えいが行われても、内容が解析できない機密保持機能を用いること。
・通信経路上で情報の改ざんが行われても、検出できるような改ざん検知機能を用いること。
・システム関連のファイルは、システムユーザがアクセスできないように管理すること。
・重要な情報は、削除、改ざん、漏えい等による被害が少なくなるように分散化すること。
・重要な情報を記録した紙、磁気媒体等は、安全な場所に保管すること。

・重要な情報を記録した紙、磁気媒体等を廃棄する場合は、内容が漏えいしない方法で行うこと。
・ファイルのバックアップを随時行い、その磁気媒体等を安全な方法で保管すること。

(4) 設備管理

・すべての機器及びソフトウェアの管理者を明確にすること。
・重要な情報が格納されているか又は重要な処理を行う機器は、許可を与えられた者以外立ち入れない場所に設置し、厳重に管理すること。
・移動可能な機器は、盗難防止策を行うこと。
・システム構成を常に把握しておくこと。
・機器及びソフトウェアを導入する場合は、セキュリティ機能がセキュリティ方針に適合していることをあらかじめ確認してから行うこと。
・機器及びソフトウェアの設定情報がシステムに適合していることを随時確認すること。
・機器及びソフトウェアは、供給者の連絡先及び更新情報が明確なものを利用すること。
・セキュリティ上の問題点が解決済みの機器及びソフトウェアを利用すること。
・外部と接続する機器は、十分なアクセス制御機能を有したものを利用すること。
・システム構成の変更を行う前に、セキュリティ上の問題が生じないことを確認すること。
・ネットワークを介して外部からアクセスできる通信経路及びコンピュータは、必要最小限にすること。
・ネットワークを介して外部からシステム管理を行う場合は、認証機能、暗号機能及びアクセス制御機能を設定すること。
・長期間利用しない機器は、システムに接続しないこと。
・機器及びソフトウェアの廃棄、返却、譲渡等を行う場合は、情報の漏えいを防ぐ対策を行うこと。
・ソフトウェア及びシステムファイルの改ざんが生じていないことを随時確認すること。
・システムが提供するパスワード強化機能は最大限に活用すること。
・ネットワークの負荷状況を監視すること。
・システムの利用形態等に応じて、ネットワークを分離すること。

(5) 履歴管理

・システムのセキュリティ方針に基づいたシステムの動作履歴、使用記録等を記録すること。
・システムの動作履歴、使用記録等を記録する場合は、改ざん、削除、破壊及び漏えいの防止措置を施すこと。
・記録したシステムの動作履歴、使用記録等を随時分析すること。
・記録したシステムの動作履歴、使用記録等は、安全な方法で一定期間保管

すること。

(6) 事後対応

- **異常の連絡を受けた場合又は異常を発見した場合は、速やかに原因を追究すること。**
- **不正アクセスであることが判明した場合は、関係者と協調して被害の状況を把握すること。**
- **関係者と協調して不正アクセス被害の拡大を防止するための処置を行うこと。**
- **事前に確立した復旧手順を遂行し、関係者と協調して不正アクセス被害の復旧に努めること。**
- **不正アクセス被害の原因を分析し、関係者と協調して再発防止策を行うこと。**
- **不正アクセス被害の拡大及び再発を防止するため、必要な情報を経済産業大臣が別に指定する者に届け出ること。**

(7) 情報収集及び教育

- **セキュリティ対策に関する情報を随時収集すること。**
- **収集した情報を分析し、重要な情報については速やかに対応すること。**
- **システムユーザがセキュリティ対策を行う場合に必要な情報を提供すること。**
- **システムユーザに、セキュリティ教育を随時実施すること。**

(8) 監査

- **システム管理者が行う不正アクセス対策の実効性を高めるため、システム監査の報告を受け、必要な措置を講ずること。**