別表_ソフトウェアのセキュリティ

中項目	目的	対象	管理策	項目	内容	＜対策を実施しない場合の影響の例＞	機密性	完全性	可用性	＜対策の評価＞
1 セキュリティ仕様	システムに関するソフトウェアのセキュリティリスクを適切に管理するため。	アプリケーションソフトウェア、ミドルウェア、ライブラリ、サービス、ドライバ、OS	システムに関するソフトウェアが出荷される際にセキュリティ仕様を明確にすること。また、仕様通りに設計され、脆弱性を含まないよう製造されているか確認すること。環境変化に合わせてセキュリティ仕様を修正できる仕組みを構築すること。仕様を踏まえ、運用も含めた対策を実施すること。	1.1 ソフトウェアのセキュリティ仕様	システムに関するソフトウェアのセキュリティ仕様を明確にすること。必要小限のソフトウェア、ライブラリ、サービスのみ利用し、不要なソフトウェア、ライブラリ、サービスは無効化または削除すること。仕様には、脆弱性が存在しないか、マルウェアの混入や実装上のセキュリティ問題がないかの確認を含めること。また、仕様を踏まえ、システム全体のセキュリティ確保のために、運用も含めた対策を実施すること。	システムに関するソフトウェアの改竄が行われる可能性や、アプリケーションが有する情報が保護できない可能性がある。	情報の漏洩	情報の改竄・消去、ソフトウェアの不正な動作	ソフトウェアの停止	■システムに関する全てのソフトウェアのセキュリティ仕様が実装可能な状態で記述されているか確認する。 ■仕様において、不要なソフトウェア、ライブラリ、サービスの無効化または削除の記載があるか確認する。 ■仕様において、セキュリティ検査が記述されているか確認する。 ■仕様を踏まえ、運用も含めた対策が実施されているか確認する。
				1.2 準拠性の確認	システムに関するソフトウェアは、仕様通りに設計され、コーディングされているか確認するために、設計・コーディング・結合・運用テスト時、出荷時及び設置時などソフトウェアのライフサイクルにしたがって検査を受けること。	システムに関するソフトウェアの改竄が行われる可能性や、ソフトウェアが有する情報が保護できない可能性がある。	情報の漏洩	情報の改竄・消去、ソフトウェアの不正な動作	ソフトウェアの停止	■システムに関する全てのソフトウェアが仕様通りに設計され、製造されていることをテスト手順に従って確認する。 ■テスト手順には適正なテストが実施されるように、必要に応じてツールの利用が推奨されているか確認する。
				1.3 ソフトウェアのセキュリティ仕様の変更	システムに関するソフトウェアのセキュリティ仕様の変更は、正式な変更管理手順を用いて管理すること。ソフトウェアのセキュリティ仕様の重要な変更は、文書化、仕様化、試験、品質管理及び管理された実装からなる正式な手続きに従うこと。	システムに関するソフトウェアのセキュリティの不備が発生する可能性がある。	情報の漏洩	情報の改竄・消去、ソフトウェアの不正な動作	ソフトウェアの停止	■システムに関する全てのソフトウェアが仕様通りに設計され、製造されていることをテスト手順に従って確認する。 ■テスト手順には適正なテストが実施されるように、必要に応じてツールの利用が推奨されているか確認する。
2 ソフトウェアの取得と設置、更新、撤去	システムに関するソフトウェアを適切に管理し、保護するため。それぞれのソフトウェアがシステム全体へ影響を与えないようにするため。	アプリケーションソフトウェア、ミドルウェア、ライブラリ、サービス、ドライバ、OS	システムに関するソフトウェアのライフサイクルにおいて継続的な管理が可能な手順を明確にすること。実施のための要員の認定や実施状況の定期的な確認を行うこと。	2.1 手順の策定	システムに関するソフトウェアの管理手順を明確にすること。ソフトウェアのライフサイクルに関して継続して適切な管理が行われる仕組みを構築すること。	システムに関するソフトウェアの管理不備により、セキュリティの不備が発生する可能性がある。	情報の漏洩	情報の改竄・消去、ソフトウェアの不正な動作	ソフトウェアの停止	■システムに関する全てのソフトウェアがライフサイクルにおいて適切に管理されるように、手順が策定されているか確認する。 ■特にソフトウェアの更新については変更前と変更後で動作に変更がないか確認するための手順が策定されているか確認する。
				2.2 要員の認定	システムに関する全てのソフトウェアの取得と設置、交換、撤去に携わる要員は教育、訓練されていること。認定された要員であることが証明できるような仕組みを構築すること。	ソフトウェアを認可されていない要員がメンテナンスした場合、不適切な対応によりセキュリティの不備が発生する可能性がある。	情報の漏洩	情報の改竄・消去、ソフトウェアの不正な動作	ソフトウェアの停止	■ソフトウェアのメンテナンスに携わる要員については、適切な対応ができるようにマニュアルを作成し、教育、訓練を実施しているか確認する。 ■ソフトウェアのメンテナンスに携わる要員が認定された者であることを示す仕組みが構築されているか確認するか確認する。できれば、その要員以外では作業ができない仕組みとなっているか確認する。
				2.3 定期的な確認	システムに関連するソフトウェアが不正に改竄されたり、必要な更新がなされていることを、定期的に確認すること。	ソフトウェアが不正に改竄されたり、必要な更新がなされていないことが検知できず、事故の発生・被害の増大の可能性がある。	情報の漏洩	情報の改竄・消去、ソフトウェアの不正な動作	ソフトウェアの停止	■ソフトウェアの不正な改竄や置換えを検知するための仕組みが構築されているか確認する。 ■ソフトウェアの必要な更新がされていることを検知するための仕組みが構築されているか確認する。 ■適切な期間で確認がされているか確認する。
3 ソフトウェアアップデート	システム環境を維持するため。不正なソフトウェアのアップデートによってソフトウェアが不正な動作をしないように保護するため。	アプリケーションソフトウェア、ミドルウェア、ライブラリ、サービス、ドライバ、OS	ソフトウェアアップデートを適切かつ確実に実施できる仕組みを構築すること。	3.1 ソフトウェアアップデート手順の策定	システムのソフトウェアアップデートは予め策定した手順に従って実行すること。ソフトウェアアップデートには以下の機能を含めること。 a) アップデート前のソフトウェアバージョン確認機能 b) アップデート適用前の動作評価 c) アップデートのロールバック機能 d) アップデータの検証機能（配布元、データの内容など） e) アップデートの記録機能 f) 設定の維持機能	ソフトウェアの改竄や、アップデート時の不正なプログラムやマルウェア等の混入により、システムの無効化や他のシステムやネットワークの機能に対する影響が発生する可能性がある。 アップデートの実施により、システム障害や他のシステムやネットワークの機能に対する影響が発生する可能性がある。	情報の漏洩	情報の改竄・消去、ソフトウェアの不正な動作	ソフトウェアの停止	■ソフトウェアアップデートの手順か確認する。 ■ソフトウェアアップデートの機能か確認する。 ■ソフトウェアアップデートでの影響を評価・確認する。 ■ソフトウェアアップデートが失敗した際の代替手段か確認する。
				3.2 アップデータの確認	ソフトウェアアップデートに利用するアップデータは正しいものであるか確認する機能を提供すること。	ソフトウェアの改竄や、アップデート時の不正なプログラムやマルウェア等の混入により、システムの無効化や他のシステムやネットワークの機能に対する影響が発生する可能性がある。	情報の漏洩	情報の改竄・消去、ソフトウェアの不正な動作	ソフトウェアの停止	■アップデータの真正か確認する手順か確認する。 ■不正なアップデータを受け付けないか確認する。
				3.3 定期的な確認	システムは、ソフトウェアウェアの不正なアップデートを検知する機能を有すること。不正なアップデートを検知した場合、当該アプリケーションを無効化するか、システムからのデータを無効化する機能を有すること。	アプリケーションの改竄や、アップデート時の不正なプログラムやマルウェア等の混入により、システムの無効化や他のシステムやネットワークの機能に対する影響が発生する可能性がある。	情報の漏洩	情報の改竄・消去、ソフトウェアの不正な動作	ソフトウェアの停止	■管理システムからの定期的な確認機能について確認する。 ■確認機能が正常に動作しているか確認する。
4 認証	システム環境を維持するため。なりすまし等によってシステムが不正な動作をしないように保護するため。	アプリケーションソフトウェア、ミドルウェア、ライブラリ、サービス、ドライバ、OS	システムにおいて予め許可された管理者だけが、認証を受けソフトウェア更新を行うこと。	4.1 システム管理者認証	事業者によって定義された管理者権限に基づき認証されること。管理者識別の認証は暗号等を用いた手段が実装されること。	管理者のなりすましによるソフトウェアの改竄の可能性や、不正な管理者がシステムに接続することによる、他のシステムやネットワークの機能に対する影響が発生する可能性がある。	情報の漏洩	情報の改竄・消去、ソフトウェアの不正な動作	ソフトウェアの停止	■セキュリティ仕様に管理者を一意に認証するための機能について記載されているか確認する。 ■セキュリティ仕様にアクセス制御機能について記載されているか確認する。 ■認証の手順は暗号等を用いて実装されているか確認する。