ＩＴ資産管理細則

第１章　総 則

第１条（目 的）

この細則は、当社のセキュリティスタンダードに基づき、調達から廃棄までのライフサイクルにおけるＩＴ資産の維持管理に関する手順を定めて、全社的に統一されたセキュリティ対策の実現を容易にし、管理の効率化を図ることを目的とする。

第２条（適用範囲）

当社が保有（レンタル、リースも含む）しているハードウェア、ソフトェウア（内製ソフトウェアは除く）に適用する。内製ソフトウェアについては、別途定める情報システムの開発／保守管理規程に従うものとする。

第３条（定義）

① ハードウェア

ネットワークに接続されているか否かを問わず、当社が保有しているデスクトップＰＣ、ノートＰＣ、サーバ機、ネットワーク機器、プリンター、モデム等周辺機器をいう。

② ソフトウェア

ＯＳ、文書作成/表計算/プレゼンテーション支援のソフトウェア、ウイルス対策ソフトウェア、電子メールソフトウェア、Ｗｅｂブラウザ、圧縮・解凍ソフトウェア、文書閲覧ソフトウェア、暗号化ソフトウェア、業務アプリケーション等をいう。

③ 標準製品

当社のすべての従業員に標準的に導入されるハードウェア、ソフトウェアをいう。

④ 標準外製品

標準製品以外で、業務上の正当な理由があり、特定部署あるいは特定従業員に導入されるハードウェア、ソフトウェアをいう。

第４条（管理枠組み）

１　当社が保有するＩＴ資産のライフサイクルにおける管理項目を明確にする。

① ＩＴ資産の調達・導入に関する手順

② ＩＴ資産の設置・保管・持ち出しに関する手順

③ ＩＴ資産の取扱い・利用に関する手順

④　ＩＴ資産の再利用・廃棄に関する手順

⑤　セキュリティ維持の確認に関する手順

2　当社が保有するＩＴ資産の管理台帳を作成し、新規登録、変更、削除を管理しなければならない。

3　標準製品については、情報システム部が全社一括して管理し、標準外製品については各部署で管理するものとする。

4　ＩＴ資産のセキュリティ維持を定期的に把握し、適切に対処しなければならない。

第２章　調達・導入

第５条（製品の選定）

1　製品選定にあたっては、スペック、サポート、ライセンス、価格等の条件に加え、必要なセキュリティ機能が装備されていることも評価しなければならない。

2　既存の情報システムと問題なく動作できるものを選択しなければならない。

3　製品のセキュリティホール情報やその他の不具合に関する情報の提供、パッチ発行等の対応が悪い製品は、選択してはならない。

第６条（標準製品リストの作成）

1　当社の一般的な業務で使用するクライアント機器については標準製品を定め、標準製品リストを作成しなければならない。

2　すべての従業員は、業務上の正当な理由があり、情報システム部から標準外製品の調達／導入を承認された場合を除き、標準製品リストで定められた製品を調達／導入しなければならない。

3　情報システム部は、標準製品リストを定期的（年一回）に審議し、見直さなければならない。

第７条（標準製品の調達／導入）

1　情報システム部は、標準製品の発注、保守契約、ライセンス、インストールメディア等を一括して管理する。

2　標準製品の調達を行う従業員は、申請書を情報システム部宛に提出しなければならない。

3　情報システム部は、申請を受けた標準製品の発注処理を行い、必要なソフトウェアのインストールと設定、ネットワーク接続の設定、各種ソフトウェアの最新パッチを適用した上で申請者が指定した場所に納品する。製品調達時にインストールされているものや、0S に付属するソフトウェアであっても、標準製品として認められないものは、排除してから納品する。

第８条（標準外製品の扱い）

１　研究、開発、その他業務上の理由で、標準外製品を調達／導入する必要がある従業員は、情報システム部宛に、標準外製品を使用する理由、製品名、製品の種類、管理者等の必要事項を明記し申請を行わなければならない。

２　標準外製品の申請を受けた情報システム部は、申請の妥当性を討議し、結果を申請者および情報セキュリティ委員会に通知する。

３　情報システム部の承認を得て標準外製品の使用を行う従業員は、標準外製品の使用を停止した場合、情報システム部宛に使用停止の報告をしなければならない。

４　標準外製品の調達／導入を行う部署は、自部署の責任において調達／導入の手続きを行い、ライセンス、インストールメディアの管理を厳密に行わなければならない。

５　標準外製品の調達／導入を行う部署は、事前に、既存の情報システムへの影響を検討し、セキュリティ上の安全性を確認し、情報システム部のチェックを受けてから使用しなければならない。

６　情報システム部は、既存の情報システムにセキュリティ上やその他のトラブル発生等の場合、標準外製品の調達／導入を行う部署に対し、当該製品の設定変更や社内ネットワークからの切り離し、当該製品の使用停止等を命じることがある。

第３章　設置・保管・持ち出し

第９条（設置・保管）

１　IT資産は、使用目的、格納される情報の重要度に応じた機密性が確保された場所に設置しなければならない。

２　ノートPC等容易に持ち出しが可能なIT資産は、持ち出されないようチェーンで固定するか、権限のない者がアクセスできないよう、暗号化を行うか、鍵のかかる場所に保管し、鍵は容易に持ち出しが出来ない場所に保管しなければならない。

３　ソフトウェアのインストールメディアは、管理者以外が持ち出せないよう鍵のかかる場所に保管しなければならない。管理者は、再インストールが必要な従業員からの申請により、ライセンス上問題のないインストールメディアを貸し出し、貸し出しの記録を管理しなければならない。

第 10 条（持ち出し）

１　ノートPC等を社外に持ち出すすべての従業員は、格納された情報の機密性に応じて、権限のない者がアクセスできないよう、暗号化を行うことが望ましい。

２　ノートP等を社外に持ち出すすべての従業員は、持ち出したノートPC等を置きっ放しにしたり、置き忘れたりしないよう厳重に注意しなければならない。

第４章　取扱い、利用

第 11 条（メディアの接続）

すべての従業員は、使用している PC に、外部メディアを接続してはならない。

ただし、業務上の必要性があり、部署のセキュリティ責任者の許可を得た場合は、この限りではない。

第 12 条（共有フォルダの利用）

すべての従業員は、個人のローカルフォルダを共有化してはならない。共有が必要な場合は、ファイルサーバー上に共有フォルダを作成し利用しなければならない。

第 13 条（ウイルス対策ソフトウェアの常駐）

すべての従業員は、ウイルス対策ソフトウェアを常駐させなければならない。

第 14 条（パッチの適用）

１　標準製品は情報システム部が、標準外製品は各部門のセキュリティ責任者が、当該製品（ＯＳ、文書作成/表計算/プレゼンテーション支援のソフトウェア、ウイルス対策ソフトウェア、電子メールソフトウェア、Ｗｅｂブラウザ等）に対するパッチ情報を収集し、適切に適用しなければならない。

２　すべての従業員は、情報システム部あるいは部門のセキュリティ責任者から指示されたパッチを速やかに適用しなければならない。正当な理由により、パッチの適用ができない場合、その旨報告の上、指示に従わなければならない。

第 15 条（PC等の保守・修理）

１　PC 等の保守・修理が必要な場合、標準製品は、情報システム部に申請書を提出しその指示に従って修理を依頼しなければならない。情報システム部は、必要に応じて代替品を準備し、貸し出しを行う。

２　標準外製品は、情報システム部の指示に従い、使用部署から直接修理を依頼する。

３　保守・修理を依頼するにあたっては、機密性の高い情報が読み出し可能な状態で保管されていないことを確認した上で修理を依頼しなければならない。故障の状況により、保管されている情報の確認や保護が実施できない場合には、ハードディスク等の情報が保管されている装置を取り外して修理を依頼しなければならない。

４　情報システム部および、標準外製品の保守・修理を依頼した従業員は、外部業者が社内に立ち入って修理を行う場合、『サーバルームに関する標準』、『物理的対策標準』に基づいて対応しなければならない。

第 16 条（従業員の異動に伴うPC等の移設）

１　同職種内で異動する従業員は、使用しているPC等を移設してもよい。

ただし、移動先で必要のないデータは削除しなければならない。

２　異なる職種に異動する従業員は、使用しているPC等を返還し、移動先で新たに使用するPCを調達しなければならない。

第５章　再利用・廃棄

第 17 条（再利用）

機密性の高い情報が保存されている PC 等を再利用する前に、保存されていた情報を、再生できない方法で消去しなければならない。

第 18 条（廃棄）

１　PC等の廃棄を行う者は、情報システム部宛に廃棄申請を提出しなければならない。

２　情報システム部は、機密性の高い情報が保管されたハードディスク等や媒体に保存されたデータの内容を完全に消去し復元できない状態にするか、再生不能な状態に破壊して廃棄しなければならない。

３　PC等の廃棄を行う者は、機密性の高い情報が保管されたハードディスク等を取り外してから、指定された場所に廃棄しなければならない。取り外したハードディスク等は、情報システム部が指定する場所に持ち込まなければならない。

４　機密性の高い情報が保管された媒体の廃棄を行う者は、情報システム部が指定する場所に持ち込まなければならない。

５　機密性の高い情報が保管されているかどうかが確認できない場合には、機密性の高い情報が保管されているものとして取り扱わなければならない。

６　情報システム部は、機密性の高い情報が保管されたバードディク等や媒体の処分を外部業者に委託する場合、情報セキュリティ委員会の承認を得なければならない。外部業者に委託する場合、秘密保持及び、処分依頼品の再利用の禁止を契約文書に含めなければならない。

７　情報システム部は、廃棄されたPC等をだれが利用していたか、そして誰がどのように廃棄処理したのかを記録しなければならない。

第６条　セキュリティ維持の確認

第 19 条（機材の設置・保管）

情報システム部および各部署のセキュリティ責任者は、定期的に、IT 資産管理台帳に記載された IT 資産が、記録された場所に設置され、記録された従業員が利用している等を確認しなければならない。ネットワークに不当なクライアントが接続されていない

第 20 条（システム設定の状況）

情報システム部および各部署のセキュリティ責任者は、定期的に、システム設定の状況を確認し、適切に対処しなければならない。

① ウイルス対策ソフトウェアが常駐されているか
② IIS などの不要なサービスが開いていないか
③ ローカルディスクが共有化されていないか
④ 必要のない外部メディア等が接続されていないか
⑤ 不適切なユーザプロファイルはないか

第 21 条（ソフトウェアのインストール状況）

情報システム部および各部署のセキュリティ責任者は、定期的に PC 等にインストールされているソフトウェアを確認し、適切に対処しなければならない。

① ウイルス対策ソフトウェア等必須のソフトウェアがインストールされているか
② ライセンス上の問題はないか

第 22 条（パッチおよびセキュリティに関わる設定の適用）

情報システム部および各部署のセキュリティ責任者は、定期的にセキュリティパッチおよびセキュリティに関わる設定が、適切に適用されているか確認し、適切に対処しなければならない。

① ＯＳ
② マイクロソフト系 HotFix
③ 文書作成/表計算/プレゼンテーション支援のソフトウェア
④ ウイルス対策ソフトウェア
⑤ 電子メールソフトウェア
⑥ Ｗｅｂブラウザ
等

附 則

第 23 条（施行期目）

この規程は、平成〇年〇月〇日から実施する。

第 24 条（改 正）

この規程の改正は、〇〇の決裁を経て、これを行う。

【参考文献】「情報セキュリティポリシーサンプル(0.92a 版)」
NPO 日本ネットワークセキュリティ協会(JNSA)http://www.jnsa.org/