

1. ソフトウェア/ハードウェアの購入及び導入標準

0.91 版

----- 取扱注意事項 -----

特定非営利活動法人日本ネットワーク・セキュリティ協会（JNSA）のセキュリティポリシーワーキンググループにて作成した「情報セキュリティポリシーサンプル」（以下、ポリシーサンプル）をご参照、ご利用される場合、以下の事項に従ってください。

1. 公開の目的

- 1-1. セキュリティポリシーを作成する際の参考
- 1-2. 既存のセキュリティポリシーとの比較によるレベル向上
- 1-3. 既存のセキュリティレベルの大きな把握

2. ご利用にあたっての注意事項

- 2-1. ポリシーサンプルの著作権は、NPO 日本ネットワークセキュリティ協会（JNSA）に属します。
- 2-2. ポリシーサンプルへのリンクは、JNSA 事務局（sec@jnsa.org）への一報をもってフリーです。ただしリンクには必ず JNSA サイトのトップページ(<http://www.jnsa.org/>)を指定してください
- 2-3. ポリシーサンプルの全文もしくは一部を引用する場合には、必ず引用元として「JNSA セキュリティポリシーWG 作成ポリシーサンプル」を明記して下さい。営利目的、非営利目的の区別はありません。

ポリシーサンプルの全部あるいは一部をそのまま、ご使用いただく場合：

【出典】「情報セキュリティポリシーサンプル(0.91 版)」

NPO 日本ネットワークセキュリティ協会(JNSA) <http://www.jnsa.org/>

ポリシーサンプルを一部加工して、ご使用いただく場合：

【参考文献】「情報セキュリティポリシーサンプル(0.91 版)」

NPO 日本ネットワークセキュリティ協会(JNSA) <http://www.jnsa.org/>

- 2-4. ポリシーサンプルを利用したことによって生ずるいかなる損害に関しても JNSA は一切責任を負わないものとします。
- 2-5. 本ポリシーサンプルを報道、記事など、メディアで用いられる場合には、JNSA 事務局にご一報ください。

3. ご意見等連絡先

ポリシーサンプルに関するご意見・ご感想・ご質問等がありましたら、JNSA 事務局まで E-Mail にてご連絡ください。ただし勧誘、商品広告、宗教関連、チェーンメールの E-Mail はお断りします。

また、E-Mail にファイルを添付する場合は、添付するファイルをアンチウイルスソフトウェア等で予め検査を行ってください。

URL : <http://www.jnsa.org> E-Mail : sec@jnsa.org

1 . ソフトウェア / ハードウェアの購入及び導入標準

1 . 1 趣旨

本標準は、当社の業務で使用するソフトウェア / ハードウェアの標準製品を定めて運用管理することにより、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、管理の効率化を図り、導入時の設定ミス等を防止することを目的とする。

1 . 2 対象者

本標準は、業務で使用するソフトウェア / ハードウェアの購入 / 導入を行うすべての従業員と、情報システム部、情報セキュリティ委員会のメンバーを対象とする。

1 . 3 対象システム

本標準は、当社の業務で使用するために購入 / 導入する、ソフトウェア / ハードウェア (PC、ネットワーク機器、OS、アプリケーションソフトウェア等) を対象とし、顧客に納品されるものは対象外とする。

本標準は、ハードウェアのうち、情報 (機器の設定等を含む) を保管できるものを対象とする。

1 . 4 遵守事項

1 . 4 . 1 標準製品リストの作成

(1) 情報セキュリティ委員会は、当社の一般的な業務で使用する以下の標準製品を定め、標準製品リストを作成し、すべての従業員に通知しなければならない。

- ・ PC
 - デスクトップ PC、ノート PC、サーバ機等
- ・ ネットワーク機器
 - ルータ、スイッチングハブ等
- ・ 必須導入のソフトウェア
 - OS、OS に付随するユーティリティ
 - 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

- ウィ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
- 業務アプリケーション
- ・ 選択して導入されるソフトウェア
 - 暗号化ソフトウェア
 - 圧縮・解凍ソフトウェア
 - 文書閲覧ソフトウェア

- (2) すべての従業員は、業務上の正当な理由があり、セキュリティ委員会から標準外製品の購入 / 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購入 / 導入しなければならない。
- (3) 情報セキュリティ委員会は、標準製品を決定するにあたり、必要なセキュリティ機能、スペックを備え、サポート、ライセンス条件、価格、などの条件が適切であることを評価しなければならない。さらに、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。
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、標準製品に指定してはならない。
- (4) 情報セキュリティ委員会は、標準製品リストを定期的(年一回)に審議し、変更が生じた場合には、速やかにすべての従業員に通知しなければならない。
- (5) 情報システム部は、セキュリティ上の問題やその他のトラブルを防止するために、標準製品の適切な設定を検証して決定し、設定ミスを防止するために、設定マニュアルを作成しなければならない。

1 . 4 . 2 標準製品の購入 / 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) 標準製品の購入を行う従業員は、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、必須導入ソ

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。製品購入時にインストールされているものや、OS 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。

- (4) 情報システム部は、購入処理を行った製品を管理台帳に登録しなければならない。
- (5) 情報システム部は、各部署からの申請により、再インストール等のためにライセンス上問題のないインストールメディアの貸し出しをする。情報システム部は貸し出し記録を作成し、管理しなければならない。

1 . 4 . 3 標準外製品の購入 / 導入

- (1) 研究、開発、その他業務上の理由で、標準外製品を購入 / 導入する必要がある従業員は、情報セキュリティ委員会宛に、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セキュリティ委員会は、申請の妥当性を討議し、結果を申請者に通知する。
- (3) 情報セキュリティ委員会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、情報セキュリティ委員会宛に使用停止の申請をしなければならない。
- (4) 情報セキュリティ委員会は、使用許可を行った標準外製品を情報システム部に通知し、情報システム部は、標準外製品を管理台帳に登録しなければならない。
- (5) 情報セキュリティ委員会は、標準外のネットワークソフトウェアに対して使用許可を行った場合、セキュリティ関連の情報収集担当者に通知しなければならない。また、当該製品の使用者から使用停止の申請があった場合も通知しなければならない。

- (6) 情報セキュリティ委員会は、標準外のネットワークソフトウェアに対して使用許可を与えない場合、情報システム部を通じて、社内ネットワークから切り離れた、独立の環境を構築して業務上の要求が達成できるよう指導しなければならない。
情報システム部は、社内ネットワークから切り離れた環境で使用されていることを、3ヶ月を超えない期間毎に、使用部署には通知せず確認しなければならない。独立の環境を使用している部署は、その環境が不要になった場合、速やかに情報システム部に通知しなければならない。
- (7) 標準外製品の購入 / 導入を行う部署は、自部署の責任において購入 / 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。
- (8) 標準外製品の購入 / 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。
- (9) 情報セキュリティ委員会は、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が発生した場合、標準外製品の購入 / 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。

1 . 4 . 4 ネットワーク機器の購入 / 導入について

- (1) 情報システム部は、本社内のグローバルゾーン、DMZ、サーバーゾーン、各フロアゾーンのフロア SWHUB までのエリアに設置するネットワーク機器（ルータ、スイッチングハブ等）の購入 / 導入を行い、許可無く各部署にて購入 / 導入を行ってはならない。
- (2) 情報システム部は、『ネットワーク構築基準』に基づき、主要なネットワーク機器の導入を行わなければならない。
- (3) (1) で指定する以外のエリアに設置するために、各部署にてネットワーク機器を購入する場合も、標準製品として指定されている製品を使用することが望ましい。各部署にて購入した製品は、管理台帳に登録するため、情報システム部に申請しなければならない。購入した製品は、自部署にて

管理するものとする。

1.4.5 管理台帳の作成/管理

- (1) 情報システム部は、申請された情報を元に PC やネットワーク機器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。
- (2) 管理台帳には、標準製品、標準外製品の両方を登録しなければならない。

1.5 例外事項

業務都合等により本標準の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

1.6 罰則事項

本標準の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については罰則に関する標準に従わなければならない。

1.7 公開事項

本標準は対象者にのみ公開するものとする。

1.8 改訂

・本標準は、平成××年××月××日に情報セキュリティ委員会によって承認され、平成××年××月××日より施行する。

・本標準の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本標準は、定期的（年1回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。