(第 2 版: 2011/6/10)

1. 目的

この「情報セキュリティ基本方針」(以下、「本方針」という。)は、株式会社サニー技研(以下、「弊社」という。)が保有する情報資産の機密性、完全性及び可用性を維持するため、弊社が実施する情報セキュリティマネジメントについて基本的な事項を定めるものである。

2. 定義

(1) ネットワーク: コンピュータ等を相互に接続するための通信網、その構成機器(ハードウエア及びソフトウエア)をいう。

(2) 開発システム: コンピュータ、ネットワーク及び記録媒体で構成され、情報処理を行う仕組みをいう。

(3) 情報セキュリティ: 情報資産の機密性、完全性及び可用性を維持することをいう。

(4) 『情報セキュリティポリシー』: 「情報セキュリティ基本方針(本方針)」と「情報セキュリティ対策基準(スタンダード)」と「情報セキュリティ実施手順(プロシージャ)」の 3 つの階層で策定・管理される文書及び規定をいう。

(5) 機密性: 情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

(6) 完全性: 情報が破壊、改ざん又は消去されていない状態を確保することをいう。

(7) 可用性: 情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

3. 適用範囲(システム)

本方針が対象とする情報資産は、次のとおりとする。

(1) ネットワーク、開発システム及びこれらに関する設備、電磁的記録媒体

(2) ネットワーク及び開発システムで取り扱う情報(これらを印刷した文書を含む。)

(3) 開発システムの仕様書及びネットワーク図等のシステム関連文書

4. 対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

(1) 部外者の侵入、不正アクセス、ウイルス攻撃、サービス不能攻撃等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去等

(2) 情報資産の無断持出し、無許可ソフトウエアの使用等の規定違反、プログラム上の欠陥、操作ミス、故障等の非意図的要因による情報資産の漏えい・破壊・消去等

(3) 地震、落雷、火災等の災害によるサービス及び業務の停止等

5. 情報セキュリティ対策

上記 4 の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

(1) 組織体制: 弊社の情報資産について、情報セキュリティマネジメントを推進する全社的な組織体制を確立する。

(2) 情報資産の分類と管理: 弊社の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティマネジメントを実施する。

(3) 物理的セキュリティ: サーバ等、開発システム室等、通信回線等及び社員等のパソコン等の管理について、物理的な対策を講じる。

(4) 人的セキュリティ: 情報セキュリティに関し、社員等が遵守すべき事項を定めるとともに、十分な教育

及び啓発を行う等の人的な対策を講じる。

(5) 技術的セキュリティ：コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

(6) 運用

開発システムの監視、『情報セキュリティポリシー』の遵守状況の確認、外部委託を行う際のセキュリティ確保等、『情報セキュリティポリシー』の運用面の対策を講じる。また、情報資産への侵害が発生した場合等に迅速かつ適切に対応するため、緊急時対応計画を策定する。

6. 法的又は規制要求事項への対応

(1) 個人情報保護：弊社は、個人情報保護法に準じて個人情報を管理する。

(2) 機密情報管理：弊社は、不正競争防止法に準じて顧客および弊社の秘密情報を管理する。

(3) 著作権保護：弊社は、著作権法に準じて著作物を管理する。

7. 秘密保持契約

弊社は、顧客との秘密保持契約事項に準じて情報を管理する。

8. 情報セキュリティ監査及び自己点検の実施

『情報セキュリティポリシー』の遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

9. 「情報セキュリティ対策基準(スタンダード)」の策定

上記の情報セキュリティ対策等を実施するために、具体的な遵守事項及び判断基準等を定める「情報セキュリティ対策基準(スタンダード)」を策定する。なお、本方針以外の文書は機密情報とし非公開とする。

10. 「情報セキュリティ実施手順(プロシージャ)」の策定

「情報セキュリティ対策基準(スタンダード)」に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた「情報セキュリティ実施手順(プロシージャ)」を策定する。なお、本方針以外の文書は機密情報とし非公開とする。

11. 社員等の遵守義務及び罰則

(1) 社員、非常勤社員、派遣社員、及び協力会社(以下「社員等」という。)は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって本方針及び「情報セキュリティ対策基準(スタンダード)」を遵守する。

(2) 社員等は、本方針を維持するため策定された「情報セキュリティ実施手順(プロシージャ)」に従う。

(3) 社員等は、情報セキュリティに対する事故及び弱点を報告する責任を有する。

(4) 社員等が、故意に弊社の情報資産の保護を危うくする行為をした場合は、就業規則の罰則規定に従い、懲戒又は法的処分の対象となる。

12. 『情報セキュリティポリシー』の見直し

情報セキュリティ監査及び自己点検の結果、『情報セキュリティポリシー』の見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合に『情報セキュリティポリシー』を見直す。

以上