セキュリティ対策標準(概要)

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まかな把握

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版権は、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エ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

セキュリティ対策標準（概要）

1　趣旨

当社は、ネットワークコンピュータ上を流通する情報やコンピュータ及びネットワークなどの情報システム（以下、情報資産）を第4の資産と位置付け、この情報資産を重要な資産とし、保護・管理する「情報セキュリティマネジメント」を実施するために、情報セキュリティポリシーを策定する。

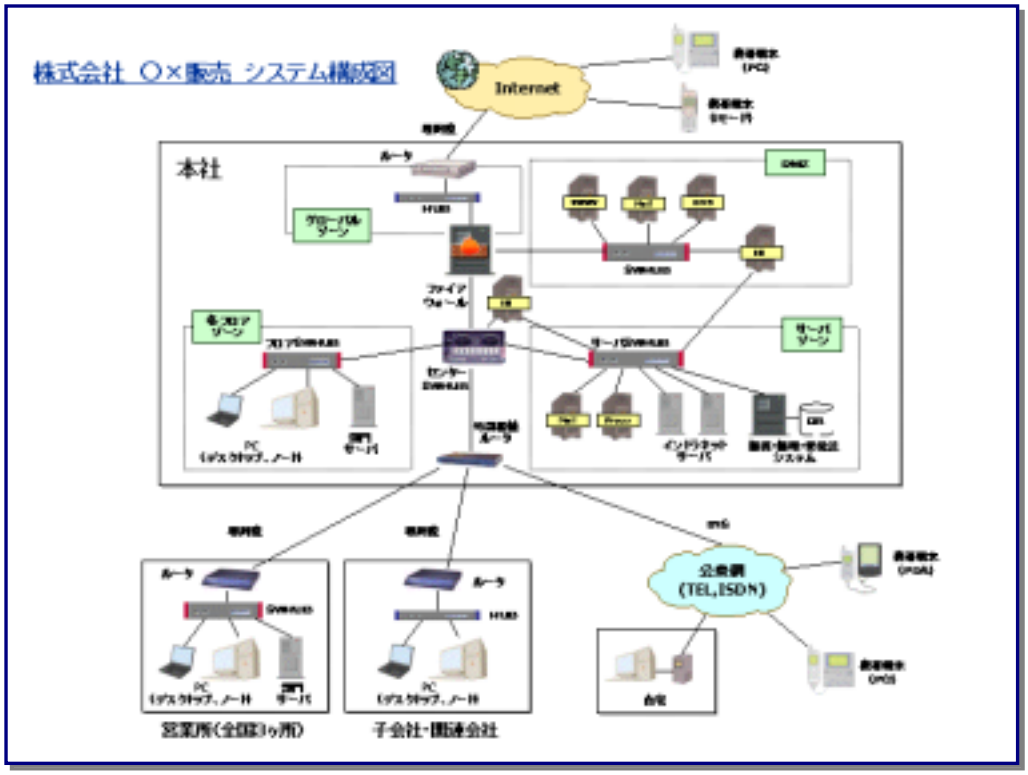
情報セキュリティポリシーは、セキュリティ方針とセキュリティ対策標準とセキュリティ実施手順書の3つの階層に分けて策定・管理する。

セキュリティ対策標準は、セキュリティ方針に従い、情報資産を保護・管理するために遵守すべき事項を可能な限り具体的かつ網羅的に記載したものである。

2　対象範囲

当社のセキュリティ対策標準の適用範囲（対象システム）は、当社の情報資産に関係する人的・物理的・環境的リソースを含むものとする。

当社の対象システムのシステム構成図を下図に示す。



3　適用者

セキュリティ対策標準は、当社のネットワークコンピュータを利用する全ての利用者に適

用する。しかしセキュリティ対策の内容によって適用者が異なるため、各セキュリティ対策標準では適用者を明確に記載するものとする。

当社のセキュリティ対策標準の適用者を、以下に示す。

（1） 当社の経営陣
（2） 当社の従業員
（3） 子会社･関連会社の従業員
（4） 外部委託業者の従業員（派遣社員、アルバイトを含）

4 用語

セキュリティ対策標準で用いられる用語について、以下のように定義する。

(1) セキュリティ方針

セキュリティ方針は、『情報セキュリティポリシー』の最上位に位置する文書であり、当社の情報セキュリティマネジメントにおける方針を記述したものである。

(2) セキュリティ対策標準

セキュリティ対策標準は、方針の下層に位置する文書であり、方針での宣言を受け、項目毎に遵守すべき事項を網羅的に記述する。

(3) セキュリティ実施手順書

セキュリティ実施手順書は、対策標準の下層に位置する文書であり、この文書は、対策標準で記述された文書をより具体的に、配布するべき対象者毎に内容をカスタマイズして記述する。

(4) 情報セキュリティ委員会

当社の情報セキュリティを維持していく組織であり、全社的なマネジメント体制を整える。

(5) 情報システム部

情報システム部は、情報セキュリティ委員会で決定した対策事項を実施及び推進する担当部署で、当社の情報機器の管理責任を有し、当社に関係するセキュリティ情報収集を行い、社内のセキュリティ対策に反映、また従業員から収集した情報を、必要に応じて情報セキュリティ委員会に報告する。

(6) システムセキュリティ責任者

システムセキュリティ責任者は、情報システム部に属し、システム管理者の作業指示･管理を行い、システム管理者同士での作業の「相互牽制」及び「職務の分離」が有効に働くように配慮する。

(7) システム管理者

システム管理者は、情報システム部に属し、システムセキュリティ責任者より与えられた管理作業の責任を有し、管理を依頼された情報機器に対して、セキュリティ対策を実施する現場レベルでの責任者である。

(8) オペレーター

オペレーターは、情報システム部に属し、システム管理者の管理下のもの実質的な作業を行う者である。

(9) セキュリティ担当者

セキュリティ担当者は、情報システム部以外の各部署の部門長によって最低一人は任命され、配置される者であり、部門内におけるセキュリティ推進及び情報収集担当であり、収集した情報は情報システム部へ報告する。

上記以外で、各セキュリティ対策標準で用いられる用語については、別紙1に記載する。

5 セキュリティ対策標準構成

当社の『情報セキュリティポリシー』のセキュリティ対策標準は、そのセキュリティ対策を29の項目に分け策定･管理する。

以下に各セキュリティ対策標準の記載項目（ドキュメントの単位）を示す。

(1) ソフトウェア／ハードウェアの購入及び導入標準
(2) 第三者契約に関する標準
(3) サーバルームに関する標準
(4) 物理的対策標準
(5) 職場環境におけるセキュリティ標準
(6) ネットワーク構築標準
(7) ＬＡＮにおけるＰＣ設置/変更/撤去の標準
(8) サーバ等にセキュリティ標準
(9) ＰＣ等におけるセキュリティ標準
(10) 社内内ネットワーク利用標準
(11) パスワードに関する標準
(12) ウィルス対策標準
(13) 電子メールサービス利用標準
(14) Web サービス使用標準
(15) リモートアクセスサービス利用標準
(16) 媒体の取扱に関する標準
(17) アカウント管理標準
(18) システム維持に関する標準
(19) システム監視に関する標準
(20) プライバシーに関する標準
(21) セキュリティ情報収集及び配信標準
(22) セキュリティインシデント報告･対応標準
(23) 監査標準
(24) セキュリティ教育に関する標準
(25) 罰則に関する標準
(26) スタンダード更新手順
(27) 専用線及び VPN に関する標準
(28) 外部公開サーバに関する標準
(29) プロシージャ配布の標準

各セキュリティ対策標準（スタンダード）では、以下に示す項目の記載をしなければならない。

(1) 趣旨
(2) 対象者
(3) 対象システム
(4) 遵守事項
(5) 例外事項
(6) 罰則事項
(7) 公開事項
(8) 改訂

6 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。

7 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』に従う。

8 公開事項

本標準は対象者にのみ公開するものとする。

9 改訂

・本標準は、平成ＸＸ年ＸＸ月ＸＸ日に情報セキュリティ委員会によって承認され、平成ＸＸ年ＸＸ月ＸＸ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。