６．ネットワーク構築標準

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

目次

６．ネットワーク構築標準

６．１　趣旨

本標準は、当社のネットワーク構築をする際に必要なセキュリティに関して記載するもので、インターネット接続環境、社内ＬＡＮ環境、社内WＡＮ環境においてネットワーク機器及び各種サーバの構築の条件、及び運用・管理の実施方法の遵守事項を規定する。

６．２　対象者

ネットワークを運用・管理する全ての従業員。

６．３　対象システム

インターネット接続環境、社内ＬＡＮ環境、社内WＡＮ環境を対象とする社内ネットワーク（ネットワーク機器及び各種サーバ）

６．４　遵守事項

６．４．１　全般規定

ネットワーク構築の全般規定を以下に示す。

(1) ネットワーク環境は、以下に示す３つの環境とする。

- インターネットと接続をするインターネット接続環境（グローバルアドレスを利用したネットワークとし、グローバルゾーンとＤＭＺの２つとする）
- 社内環境に設置するＬＡＮを利用した社内ＬＡＮ環境（プライベートアドレスを利用したネットワークとし、サーバゾーンと各フロアゾーンと営業所と子会社・関連会社の３つとする）
- 専用線及び公衆回線を利用した社内WＡＮ環境（プライベートアドレスを利用したネットワークとし、自宅と携帯端末との接続を可能にする）

(2) ネットワーク構築のための機器は、以下に示す機器とする。

- ネットワーク機器（ルータ、ハブ、スイッチングハブ（レイヤ３、レイヤ２）、ＬＢ（負荷分散装置）、ＶＰＮ装置等）
- ファイアウォールサーバ
- インターネットサーバ（ＤＮＳサーバ、WWWサーバ、メールサーバ、Ｐｒｏｘｙサーバ、ウィルス対策サーバ、ＦＴＰサーバ等）
- イントラネットサーバ（WWWサーバ、ＬＤＡＰサーバ、ファイルサーバ、プリンタサーバ、ウィルス対策サーバ、業務システムサーバ）

・ 認証サーバ、不正アクセス監視サーバ、運用監視サーバ、時刻同期サーバ

(3)インターネット接続環境に接続する機器は、ルータ、スイッチングハブ、UNIX系サーバとする。（Windows系サーバについては、アプリケーションを利用するため必要な場合に接続をすることができる）。

(4)インターネット接続環境には、不正アクセスを防止するための仕組みを設置し、不正アクセスを検出した場合には速やかにセキュリティ委員会に報告しなければならない

(5)インターネット接続環境には、不正アクセスを監視できる仕組みを設置し、不正アクセスを検出した場合は速やかにセキュリティ委員会に報告し、システム運用部門と共に適切な対策を講じなければならない。

(6) 主要な機器は、ログ採取とネットワーク監視を実施すること。

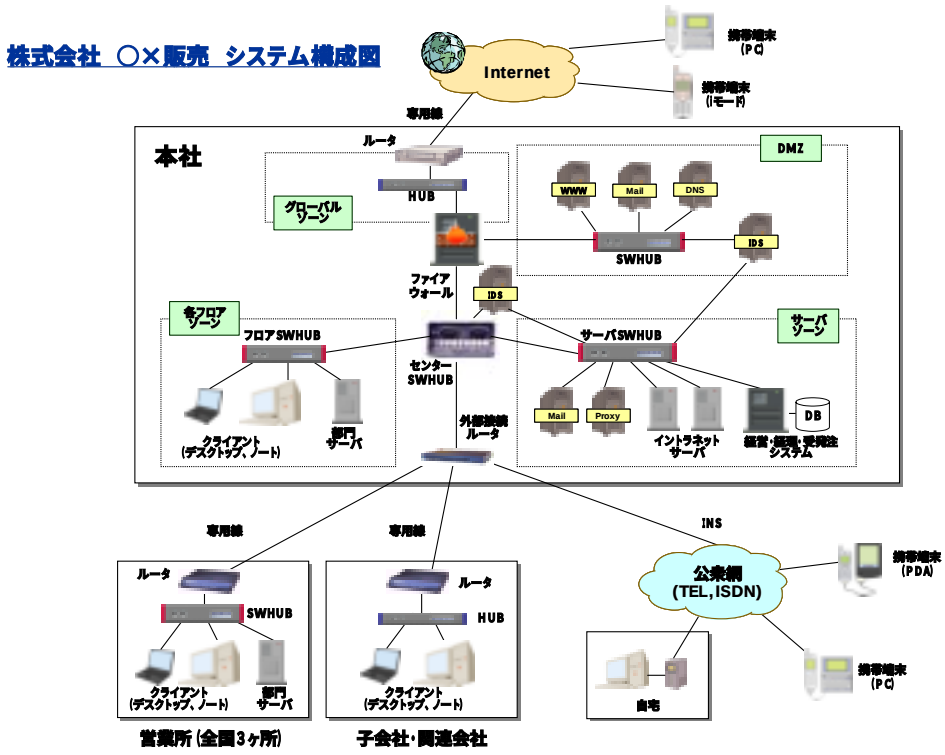
(7) パスワードの設定が可能な機器には、『ユーザ認証に関する標準』に準拠すること。

(8)アクセス制御の設定が可能な機器には、特定の機器からの接続のみ可能な設定をすること

(9) 各機器は、設置場所・接続機器状況・管理者を明確にすること。

(10) 主要なサーバ（インターネットサーバ・イントラネットサーバ）は、サーバルームに構築するサーバ専用セグメントに接続すること。

図６．４－１にシステム構成図を示す。



６．４．２　インターネット接続環境規定

インターネット接続環境の規定を以下に示す。

(1) ネットワーク接続構成

・ルータによるインターネットプロバイダ接続とし、プロバイダ側のネットワークはグローバルアドレスを利用しなければならない。
・プロバイダと当社の境界には、ファイアウォールサーバを設置し、不正アクセスの対策を実施しなければならない。
・インターネット接続環境に接続できる機器は、インターネットサーバとする。
・ファイアォールサーバには、ＤＭＺを用意しインターネットサーバを利用できるようにしなければならない。
・ファイアウォールサーバでは、グローバルアドレスとプライベートアドレスの変換を行うことが望ましい。
・外部へのＷｅｂアクセス及びファイル転送は、Ｐｒｏｘｙサーバを経由すること。
・外部とのメールの送受信は、ウィルス対策サーバを経由し最新のパターンデータでウィルス感染チェックすると共に不正中継対策を実施すること。
・インターネットサーバは、情報セキュリティ委員会が指示するＯＳ及びパッチの適用をし、常に最新のセキュリティ対策を実施しなければならない。

(2) 利用できるサービス

・社外ユーザ向けのWWWサービス（情報公開）
・社内ユーザ向けのWWWサービス（情報収集）
・メールの送受信サービス
・ドメインネームサービス
・ファイル転送サービス
・時刻同期サービス

６．４．３　社内ＬＡＮ環境規定

社内ＷＬＡＮ環境の規定を以下に示す。

(1) ネットワーク接続構成

・ スイッチングハブ（レイヤ３、レイヤ２）とハブを使用し、ビル内のネットワークとする。
・ ネットワークの中心となるネットワーク機器は、サーバルームに設置し、他のネットワーク機器はフロアに設置すること。
・ ネットワークセグメント間は、通信サービス毎のアクセス制限を実施し不正アクセスの対策を実施しなければならない。
・ 主要な場所に設置するネットワーク機器には、ネットワーク監視を実施すること。
・ 接続できる機器は、各種サーバとPCとプリンタとする。
・ 使用するアドレスは、プライベートアドレスを利用すること。

(2) 利用できるサービス

・インターネット（WWWサービス）
・イントラネット（社内各業務システム）
・ファイル共有サービス
・プリンタ共有サービス
・メールの送受信サービス

６．４．４　社内ＷＡＮ環境規定

社内ＷＡＮ環境の規定を以下に示す。

(1) 接続構成

- ルータによる専用回線による専用接続とし、接続先は社内拠点（支店、営業所）及び子会社・関連会社とする。
- ネットワークセグメント間は、通信サービス毎のアクセス制限を実施し不正アクセスの対策を実施しなければならない。
- ネットワーク機器には、ネットワーク監視を実施すること。
- 使用するアドレスは、プライベートアドレスを利用すること。
- 専用線接続が困難な場合においては、情報セキュリティ委員会が認めた場合のみインターネットを利用したＶＰＮ装置を利用した接続を認める。

(2) 利用できるサービス

・インターネット
・イントラネット（社内各業務システム）
・ファイル共有サービス
・メールの送受信サービス

６．４．４　ネットワーク管理規定

ネットワークに設置するネットワーク機器は、以下に示す手順で管理を行う。

(1) 設置許可申請

ネットワーク機器を設置する場合、別途規定する設置許可申請書を情報システム部に提出しなければならない。

(2) システム管理者の決定

ネットワーク機器を設置する場合、管理者を選出しなければならない。選出は、該当ネットワーク機器を管理する部門とし、選出後には情報システム部に文書で報告しなければならない。

(3) 機器の設置

設置するネットワーク機器は、情報セキュリティ委員会からの指示によるセキュリティ対策がされるように設定を行わなければならない。

設置許可申請の受理及び内部審査での合格がされていないネットワーク機器は、ネットワークに設置を認めない。

(4) 審査・設置許可

セキュリティ対策の施されたネットワーク機器は、速やかに情報セキュリティ委員会が実施する内部審査を行わなければならない。 内部審査は、ネットワークを通じた検証について実施することが望ましい。

内部審査で発見された問題点は速やかに処置を行い、再審査を受けて合格するまで処置と審査を継続しなければならない。

内部審査に合格したネットワーク機器は、許可されたネットワークのみ設置することができる。

(5) 監視

設置したネットワーク機器は、情報セキュリティ委員会から指定された外部機関又は内部組織で監視を行わなければならない。 監視の対象は、ネットワークを流れているデータ（通信パケット）とネットワーク機器の稼動状況）とログとする。

(6) 監査の継続と切り離し

設置したネットワーク機器は、設置後も定期・不定期的に監査を実施しなければならない。監査により発見された問題点の程度によっては、情報セキュリティ委員会の判断により、問題点の処置が完了するまでネットワークから切り離なさなければならない。

６．５　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。

６．６　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』に従う。

６．７　公開事項

本標準は対象者にのみ公開するものとする。

６．８　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。