社内ネットワーク利用標準

0.92a 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(0.92a 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(0.92a 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

ネットワーク利用標準

１　趣旨

本標準は、機密保持及び情報資産の保護、有効活用を目的に社内ネットワークの利用管理を行う。利用者は、業務目的以外の理由で、社内ネットワーク及びインターネットを利用してはならない。

２　対象者

社内ネットワークにコンピュータを接続し、社内ネットワーク及びインターネットを利用するユーザ。

３　対象システム

社内ネットワークに接続し、社内ネットワーク及びインターネットへの通信を行うコンピュータ及びシステムを対象とする。

４　遵守事項

４．１　社内ネットワーク及びインターネットの業務目的以外の利用禁止

（１） 社内ネットワークは、会社の情報資産であり、電子メールやＷｅｂサイトの利用などにおいて、業務目的以外の使用を禁止する。インターネットの利用についても同様である。

（２） 情報セキュリティ委員会の許可無く、社内ネットワーク上に、電子メールサーバや、Web サーバ、FTP サーバなどを構築してはならない。

（３） 他人の利用者ＩＤを用いて、社内ネットワーク及び、社外のネットワーク、インターネット上のサイトへアクセスしてはならない。

（４） ネットワーク利用者は、故意もしくは不注意を問わず、社内ネットワーク及び社外ネットワーク、インターネット上のサーバに対して、許可されたアクセス権限以上のアクセスを行ってはならない。

４．２　ネットワークを利用した機密情報の送受信

（１） ネットワーク利用者は、当社の事業に関わる情報や、顧客や従業員のプライバシーに関わる情報などの機密性の高い社内の情報が社外へ漏洩することを防ぐために、ファイルのアップロードや社外へ送信を行ってはならない。

（２） 出所が不明なファイルや内容に確証の持てないファイルをダウンロードや実行してはならない。

（３） 業務上やむを得ず機密情報を社外へ送信もしくは受信する場合は、情報セキュリティ委員会の指示に従い、内容に応じて暗号化、電子署名などの処置を施さなければならない。

４．３　インターネットで利用可能なサービス

（１） ネットワーク利用者は、インターネットの利用において、電子メール及び Web 閲覧以外を使用してはならない。情報セキュリティ委員会は、上記のサービス以外利用できないようなアクセス制御を実施する。

（２） 暗号通信を用いたインターネットへのアクセスは、情報セキュリティ委員会の承認を得たサイトのみ許可するものとする。

（３） Web サービスの利用については、『Web サービス利用標準』を遵守すること。

（４） ネットワーク利用者は、社内ネットワークに接続した PC において、自社の電子メールサービス以外の電子メールサービスを利用してはならない。やむを得ず、社外の電子メールサービスを利用しなければならない時は、情報セキュリティ委員会の承認を得ること。

４．４　社内ネットワークで利用可能なサービス

（１） 電子メールの利用において、本社サーバゾーンにて管理する電子メールサーバを利用しなければならない。その他の電子メールの利用については、『電子メール利用標準』を遵守しなければならない。

（２） インターネット上のサーバに Web ブラウザを用いてアクセスする場合は、必ず、本社サーバゾーンにて管理する Proxy サーバを使用しなければならない。

（３） 本社サーバゾーンにて管理されるシステム（経営、経理、受発注システム、イントラネットサーバ）へのアクセスは、許可された利用者以外利用してはならない。

（４） 各部門サーバは、他部門ネットワーク及び他部門の者が利用する IP アドレスからのアクセスを拒否しなければならない。他部門からのアクセスが業務上必要な場合には、本社サーバゾーンに設置され、アクセス制御可能なイントラネットサーバを利用しなければならない。

（５） 専用線や INS を使用した場合は、Web サービスのプロトコルと電子メールのプロトコル以外を利用してはならない。本社サーバゾーンに配置された重要サーバへのアクセスは、許可されたユーザが許可されたアクセスに限って許可するものとする。

（６） 各部のセキュリティ担当者は、社内ネットワークで利用するサービスを情報セキュリティ委員会に届けなければならない。情報セキュリティ委員会は、届けられた利用サービスにおいて、業務上不必要と判断できるサービスは禁止することができる。また、届けられた利用サービス以外が使用されていないかどうかを検査できるものとする。

（７） 業務上やむを得ず機密情報について、ネットワークを介して扱う場合は、情報セキュリティ委員会の指示に従い、内容に応じて暗号化、電子署名などの処置を施さなければならない。

（８） ネットワーク利用者は、社内ネットワークにおいて、ネットワークモニターなどの、ネットワーク上を流れるパケットを盗聴できる機器及びソフトウェア使用してはならない。但し、情報セキュリティ委員会が承認した調査及び監視目的のネットワークＩＤＳやネットワークモニターなどの利用はできることとする。

（９） ネットワーク利用者は、社内ネットワークサーバへのアクセス用のＩＤ及

びパスワード、証明書は適切に管理しなければならない。特にパスワードの選択および使用については、『ユーザ認証に関する標準』に基づいたものを利用しなければならない。

４．５　社内ネットワークへの接続時の注意事項

（１）　自宅や、他組織のネットワークへ接続した PC は、ウイルス検査とセキュリティ検査を実施し、異常が発見されなかったことを部のセキュリティ担当者が確認した後でなければ、社内ネットワークに接続してはならない。

（２）　ネットワーク利用者は、与えられたＩＰアドレス以外のＩＰアドレスを使用してはならない。

（３）　ネットワーク利用ユーザは、社内ネットワークに接続中のコンピュータを、情報セキュリティ委員会の許可の無い電話回線、携帯電話、PHS、無線ＬＡＮ、専用線などを利用して、社外のネットワークへ接続してはならない。

４．６　監視方針

（１）　我社は、社内から社外、及び社内から社内に対する全ての通信に対して、次の監視を行う。

- 社外への通信権限の有無
- 許可されたサービスの通信状態
- 許可されていない通信先への接続、接続先ＵＲＬ
- 電子メールの本文、添付ファイルの内容
- ダウンロードするファイルの種類
- ウイルスチェック

（２）　情報セキュリティ委員会は、本社サーバゾーンに配置した重要サーバや社内ネットワークへの許可されないアクセス、インターネットへの不審なアクセス等を監視するために IDS を導入する。

（３）　監視内容の決定、追加、変更は情報セキュリティ委員会の承認を得なければならない。監視により、許可されていない通信を検知したシステム管理者及びネットワーク利用ユーザは、情報システム部門長に報告しなければならない。システム管理者及びネットワーク利用ユーザは、監視によって

知りえた情報を情報システム部門長への報告以外に漏洩してはならない。

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　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。

7　公開事項

本標準は対象者にのみ公開するものとする。

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。

用語集
社内ネットワーク
電子メール
Web サービス
ネットワーク利用者
コンピュータ

IDS
サイト
アクセス権限
ファイルのアップロード
ダウンロード
Web 閲覧
アクセス

リンク
『Web サービス利用標準』
『電子メール利用標準』
『ユーザ認証に関する標準』