4.インターネット利用に関する標準

0.9 版

---------- 取扱注意事項 ----------

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「外部接続に関する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. 既存のネットワークにおける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 作成サンプルポリシー」を明記して下さい。営利目的でも非営利目的の区別はありません。
   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などマスコミ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

インターネット利用に関する標準

趣旨

我社は機密保持及び、社内環境の保護、情報資源の有効活用を目的に、インターネットの利用管理を行う。

利用者は、業務目的以外の理由でインターネットを利用してはならない。

対象者

- 社内からインターネットを利用する全ての者
- インターネットを使用して、社内から社外への通信を行う機器及び情報システムの管理者

対象システム

- 社内からインターネットを使用して通信を行うシステム

遵守事項

設定方針

社内システムをインターネットに接続する際には、 Firewall 等の機器を用いて社内システムを適切に保護しなければならない。

社内システムのネットワーク構造は、NAT や Proxy 等の機器を用いて外部へ公開されることを防がなければならない。

優先度の高いサービスは、帯域制御等を用いて常に利用可能とならなければならない。

全社的に社内から社外に対して許可されるサービスは、情報管理責任者が決定する。

Telnet や Ping、TraceRoute など、社外のシステムへセキュリティ侵害を実施できるようなサービスは利用できない。

一般利用方針

私的利用を行ってはいけない。

業務上必要と認められた利用者しか利用できない。

機密性のある社内の情報を社外へ送信してはならない。

社外の掲示板やニュースグループ等公的な場で意見を表明するときは、我社の宣伝活動や他社の中傷を行ってはならない。

他の利用者 ID を用いて身分を隠してはならない。

電子メール利用方針

社内の電子メールを社外のメールサーバへ転送してはならない。
暗号メールを使用してはならない。
機密情報を社外へ送信してはならない。
不用意にメールアカウントを外部へ公開してはならない。
添付ファイルにウィルスが内在することの可能性を考慮しなければならない。

暗号メールを使う必要がある場合の例外

利用者は、特に部門長が認める場合において、暗号メールを使用することができる。この場合、利用者は、S/MIME を使用しなければならない。

Web 利用方針

SSL 等の暗号通信を行ってはいけない。
信頼できないサイトへアクセスしてはならない。
署名のない ActiveX や Java、JavaScript、VBScript などのコードを実行してはならない。
Cookie の設定は OFF にしておかなければならない。

SSL 等を使う必要がある場合の例外

特に部門長が認める場合において、SSL の通信を行うことができる。この場合、利用者は、利用目的、対象サーバ、利用期間等を明らかにしなければならない。

ActiveX や Java、および Script などの例外

署名がない場合や、信頼できるサイトに登録されていない場合でも、システム管理者より周知があった場合には実行してもよい。

ファイル転送利用方針

社内の情報が社外へ漏洩することを防ぐため、ファイルのアップロードを行ってはならない。
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してはならない。
大きなサイズのファイルをダウンロードするときは、他の利用者への影響を考慮しなければならない。
PassiveFTP を用いなければならない。

鍵管理方針

認証局の証明書運用規定について、事前に承認が得られていなければならない。
秘密鍵は、システム管理者へ預託しなければならない。
証明書の有効期限が切れる一定期間前に、更新手続きを実施しなければならない。
証明書や秘密鍵は、文書の保存期間中適切に管理されなければならない。
鍵を紛失または盗難等で安全性を保証できなくなった場合は、速やかに無効化手続きを実施しなければならない。

対象者別方針

情報セキュリティ委員会

権限：

サービスの種類を決定・変更に関して承認できる。
違反者に対して懲罰を適用できる。

責任：

委員会を開催して利用に関する状況を把握しなければならない。
障害発生時に適切な対応の指示を出さなければならない。

情報システム部門長

権限：

情報セキュリティ委員会が委任した事項について、判断を下すことができる。

責任：

システム管理者からの報告をうけて適切に対処する。（自分で解決するか、もしくは、情報セキュリティ委員会へ報告）

システム管理者

権限：

情報セキュリティ委員会の承認を得た内容にしたがって、設定および変更ができる。

責任：

違反者を発見した場合には、情報システム部門長へ報告する。
セキュリティホールの情報について、常に収集を行い必要に応じて利用者へ周知しなければならない。

利用者

権限：

業務上必要な範囲において、ネットワーク資源を活用することができる。

責任：

我社の方針について、教育を受け、その内容を理解し、契約を結ばなければならない。

ブラウザのセキュリティレベルを適切に設定しなければならない。

OS およびソフトウェアについて、最新のパッチをあてなければならない。

利用者管理方針

人事システムに登録されている利用者に対して、アカウントおよびアクセス権の登録、変更、削除を行うことができる。

利用者情報は、常に最新の状態を維持しなければならない。

ログ管理方針

我社は、障害や不正が発生した場合に、その原因を究明し、違反者の特定をするためにログ取得、管理を行う。

取得したログは、定期的に利用頻度、サービス毎、時間毎などの分析結果を公表する。

ログおよびバックアップ媒体は、改ざん、破壊や、権限のない参照から保護されなければならない。

取得されたログは、定期的にバックアップ媒体に記録しなければならない。

バックアップ媒体は、３年間保管しなければならない。

Firewall

許可された通信については、パケットのヘッダ情報が記録されなければならない。

許可されない通信については、すべてのパケット情報を記録しなければならない。

Proxy、NAT

すべての通信について、パケットのヘッダ情報が記録されなければならない。

DHCP を利用している場合には、MAC アドレス情報もあわせて記録さ

れなければならない。

障害対応方針

利用者が障害を検知した場合には、速やかにシステム管理者に報告する。
システム管理者は、情報システム部門長へすみやかに報告する。
システム管理者は、障害復旧した・しないにかかわらず、利用者に対して１時間以内に周知する。その時点で復旧していない場合には、復旧時に再度周知を行う。

監視方針

我社は、社内から社外に対する全ての通信に対し、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
・ウィルスチェック

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。
システム管理者は、監視によって知り得た情報を、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。

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。

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ことがある。罰則の適用については罰則に関する標準に従う。

公開事項

本標準は対象者にのみ公開するものとする。

改定

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すること。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すること。
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すること。