１８．システム維持に関する標準

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

１８．システム維持に関する標準

１８．１　趣旨

本標準は、当社システムのセキュリティレベルを維持するためのパッチ等の適用ルール及びバックアップルールについて規定する。

１８．２　対象者

当社の情報システム部と各システム管理者及び当社システムを利用する全ての社員

１８．３　対象システム

当社の社員が業務上使用する全てのサーバ、クライアント PC、ネットワーク機器

１８．４　遵守事項

１８．４．１　パッチ適用のルール

（１） 弊社システムの管理者及び使用者は、『セキュリティ情報収集及び配信の標準』基づいて情報システム部より配信されたパッチ適用の指示に対して、自分が管理または使用している全てのマシンに対して速やかにパッチを適用しなければならない。

（２） パッチ適用作業によるサービスの停止など他システムへの影響が大きく、速やかに（１）のパッチが適用出来ない場合、システム管理者は情報システム部に連絡しなくてはならない。また、システム管理者はパッチ適用計画を作成し、それに基づいてパッチを適用しなければならない。
（例えば FireWall にパッチを適用するために FireWall を停止しなければならず、その間全ての Web アクセスが出来ないなど）

（３） 情報システム部は社内全てのマシンに対して、（１）のパッチが指示通り適用されているかを確認する事が望ましい。

（４） システムに対して業務上必要となる修正パッチ等を適用する場合、システ

ム管理者は情報システム部に対して適用したいパッチとその理由について報告しなければならない。

１８．４．２　パッチの取得及び配布方法

（１） WindowsOS 関連のパッチは、システム管理者が MicroSoft のホームページよりダウンロードで取得し、クライアント PC 利用者に対してパッチの置き場所を通知する。

（２） UNIXOS のパッチについては、システム管理者が各ベンダーよりダウンロード取得し、サーバの管理者に対してパッチの置き場所を通知する。

（３） 各アプリケーションのパッチに関しては、システム管理者が各ベンダーより取得する。クライアント PC にインストールが必要な場合はシステム管理者が配布する。

（４） ネットワーク機器のパッチににについては情報システム部がベンダーより取得し、ネットワーク管理者にパッチの置き場所を通知する。

１８．４．３　ウィルス定義ファイルの更新

（１） 『ウィルス対策標準』に基づいてウイルス定義ファイルを更新しなければならない

１８．４．４　サーバーのバックアップについて

（１） 業務上重要なサーバー（WWW サーバー、mail サーバー、経営・経理・受発注システムなど）については、そのデータ及び log を定期的にバックアップしなければならない。

（２） パッチの適用など、サーバーのシステムに対して何らかの変更を行う場合、変更後の不具合が発生する可能性がある。その為、サーバーに対して変更を行う前にサーバーのシステムバックアップを取らなければならない。

（３） パッチの適用など、サーバーのシステムに対して何らかの変更を行った場合は、安定動作確認後にサーバーのシステムバックアップを取らなければ

ならない。

（４） バックアップ作業は業務に影響が及ばないように作業時間は十分に配慮しなければならない。

１８．４．５　バックアップ媒体の取り扱いについて

（１） バックアップ媒体はテープとする。

（２） 過去２回分のバックアップデータを保持することが望ましい。

（３） バックアップに使用する媒体は、鍵付きの保管場所に置くなど、サーバ管理者が責任をもって管理しなければならない。

（４） バックアップに使用した媒体の破棄については、『媒体の取り扱いに関する標準』に基づいて処理をしなくてはならない。

１８．４．６　システムの監視について

（１） サーバ管理者及びネットワーク管理者は、システム障害等の兆候をいち早く見つけるために、サーバ及びネットワークの監視を行わなければならない。監視については『システム監視に対する標準』に基づいて行わなければならない。

１８．５　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。

１８．６　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。

１８．７　公開事項

本標準は対象者にのみ公開するものとする。

１８．８　改訂

・本標準は、平成 XXXX 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 XXXX 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。