８．サーバ等におけるセキュリティ対策標準

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

８．サーバ等におけるセキュリティ対策標準

８．１　趣旨

本標準は各サーバのＯＳを含めたソフト、ハード、及び、運用の規定をし、サーバに格納されている情報の保護を目的とする。

８．２　対象者

当社の全てのサーバ管理者。

８．３　対象システム

本社・営業所・子会社・関連会社を含む当社の従業員が業務上、利用する全てのサーバシステム。

８．４　遵守事項

８．４．１　導入時の規定

（１）サーバ管理者は対象システムの設置場所をサーバルームまたは、それに準ずる安全な場所に設置しなければならない。

（２）サーバ管理者はサーバを設置する際はサーバ設置申請書を作成し、情報セキュリティ委員会で認可を受けなければならない。

（３）サーバ管理者は、サーバの設置申請時にそのシステム構成を明確にしなければならない。情報セキュリティ委員会により、システム構成の不備もしくは、改善要求を受けたとき、サーバ管理者は、直ちにシステム構成の再検討を行わなければならない。

（４）サーバ管理者は情報及び情報システムの正しく安全な運用を確実にするために、管理体制及びサーバ管理者を明確にしなければならない。人的不注意および故意の誤用のリスクを低減するために、サーバ管理者及びオペレータを２名以上任命しなければならない。

（５）サーバ管理者はサーバの設置申請時に運用手順書を作成し、情報セキュリティ委員会へ提出なければならない。
但し、侵害時対応手順が運用手順書に含まれる事。

（６）本標準が適用される以前の既存のサーバについては、３ヶ月以内に本標準に適合するようにしなければならない。３ヶ月以内に、本標準に適合しない場合、情報セキュリティ委員会は情報の公開を強制的に停止させることができる。

８．４．２　環境設定の規定

（１） サーバ管理者はサーバで使用するＯＳ及び、ソフトウェア（ウイルス対策ソフト、脆弱性検査ソフトを含む）は情報セキュリティ委員会が規定したものを使用しなければならない。

（２）サーバ管理者はサーバで使用されるソフトウェアは常に最新のＯＳ、最新のアプリケーション、最新のセキュリティパッチの適用、不要なサービスの削除を常に行わなければならない。

（３）サーバ管理者はＯＳのアクセス制御、ファイルのアクセス制御、アプリケーション、サービスのアクセス制御に関して、厳密にアクセス権を設定しなければならない。

（４）サーバ管理者はユーザー、ＷＥＢアクセスなどに使用する匿名ユーザーアカウントを含む全てのアカウントのアクセス権限に対して、必要最低限のアクセス権限のみ許可しなければならない。

（５）サーバ管理者は、CGI、API などのアプリケーション開発を行う者にリスク分析を実施し、仕様書の段階から、データの入力チェック、内部でのデータの処理プロセス、出力されるデータの妥当性などの、セキュリティ対策の実施を義務づけなければなければならない。

（６）サーバ管理者は、サーバの趣旨、用途に応じた必要最低限のアプリケーション・サービス以外インストールしてはならない。

（７）サーバには、推測困難なパスワードを設定しなければならない。特にサーバ管理者もしくはサーバ管理者に類する権限を持つアカウントのパスワードは、厳重に管理されなければならない。

８．４．３　運用時の規定

（１）　サーバ管理者はサーバで使用されるソフトウェアは常に最新のＯＳ、最新のアプリケーション、最新のセキュリティパッチの適用、不要なサービスの削除を常に行わなければならない。

（２）　サーバ管理者はウイルス対策として常にウイルス定義ファイル、ウイルス対策システムが最新のものとなるよう情報を収集し、更新があった場合は直ちに反映を行い、サーバのウイルスチェックを行わなければならない。

（３）　サーバ管理者はサーバのパスワードを定期的にこれを変更しなければならない。

（４）　サーバ管理者はサーバのログの取得を行わなければならない。

（５）　サーバ管理者は定期的にサーバのログを一定期間分、媒体に保存を行わなければならない。

（６）　サーバ管理者は定期的にログの解析を行わなければならない。

（７）　サーバ管理者は定期的にサーバ内の情報のバックアップを行わなければならない。

（８）　サーバ管理者は定期的に第三者による検査を受けなければならない。

・脆弱性検査ソフトによる最新の脆弱性情報を含む検査
・「サーバ設置申請書」と実際の設置機器との整合性
・不要なアクセス権が存在しない事
・不要サービスの起動が存在しない事
・不要なアカウントが存在しない事
・推測可能なパスワードが設定されていない事

（９） 第三者による検査結果は必ず記録し、一定期間保管しなければならない。

（１０）第三者による検査によりセキュリティの不備が発見された場合は直ちに不備を是正し、不備の内容と対策状況を情報セキュリティ委員会に報告する。

（１１）セキュリティ侵害が発生した場合、セキュリティ侵害時の対応手順に則って対応しなければならない。
また、サーバ管理者は、セキュリティ侵害の状況を、できるだけ速やかに、情報セキュリティ委員会に報告しなければならない。
情報セキュリティ委員会は、前述の報告を受けた後、各行政機関への通報を含めて迅速に対応しなければならない。

（１２）万が一、想定外のセキュリティ侵害が発生し、セキュリティ侵害時の対応手順のみでは状況の改善が見込めない場合、サーバ管理者は即座に情報セキュリティ委員会に報告しなければならない。サーバ管理者は、情報セキュリティ委員会の指示のもと、手順書外の行為を行うことができる。但し、作業実施記録は詳細に記録しなければならない。

（１３）また、実効性を維持するため、適宜更新しつづけなければならない。

８．５　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。

８．６　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。

８．７　公開事項

本標準は対象者にのみ公開するものとする。

８．８　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。