外部公開サーバに関する標準

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

外部公開サーバに関する標準

１　趣旨

本標準は、当社がシステムをインターネットに接続する場合に、ネットワーク犯罪の被害者や加害者、あるいは踏み台になることなく、円滑かつ効率的なビジネスを継続することを趣旨としている。

インターネットへの接続は、当社の業務効率の向上をもたらす反面、インターネット上の脅威にさらされる可能性もある。そのためインターネットへの接続にあたっては接続そのものの企画から、管理、運用まで慎重に行わなければならない。

当社は、外部へ公開する情報、情報システムに関して、セキュリティレベルの維持、向上、管理を趣旨として、以下の外部公開サーバに関する標準を実施する。

２　対象者

下記を本標準の遵守義務対象者とする。

・外部公開サーバの設置申請者
・システムおよびセキュリティ対策の設計者
・情報セキュリティ委員会
・システム構築担当者
・外部公開サーバのシステム管理者、オペレータ
・利用者（パスワード認証不要のアカウント利用者は除く）

３　対象システム

インターネットに接続し、不特定多数のインターネットユーザにＩＰアドレス及び情報を公開する情報システム、情報機器などを対象とする。対象システムの例としては外部公開サーバ（ウェブサーバ、メールサーバ、FTP サーバ、DNS サーバ、プロキシサーバなど）、ルータ、ファイアウォール及び外部公開サーバに情報を提供するデータベースサーバなどがある。

４　遵守事項

本標準の対象者は次に挙げる事項を遵守しなければならない。

なお、遵守事項は前述の対象手順のうち、セキュリティを考慮する上で特に留意が必要であると考えられる手順についてのみ記載しており、また遵守事項の記載順は対象手順の流れに沿うものとする。

４．１　システムおよびセキュリティ対策の設計に関する遵守事項

（１）　外部公開サーバの目的と公開情報の明確化

システムおよびセキュリティ対策の設計者（以下、システム設計者）は、外部公開サーバの設置の目的と当該サーバにて公開される情報を明確にしなければならない。また公開される情報に「顧客情報、プライバシー情報」などを含む場合は、『プライバシーに関する標準』を遵守しなければならない。

（２）　ネットワークの分離

システム設計者は、外部公開サーバと社内ネットワークの境界点にファイアウォールなどのようにアクセス制御が可能で、通信のログが取得できる機器を設置し、内外のネットワークを分離しなければならない。

（３）　リスク分析の実施

システム設計者は、外部公開サーバのセキュリティ設計を行う上で、必ずリスク分析を行わなければならない。リスク分析を行う上で、以下の項目を明確にしなければならない。

・保護・脅威の対象（守るべき情報）
・脅威
・脅威の原因、プロセス
・対策（予防、防御、検査、対応：回復）

（４）　ルータ及びファイアウォールなどによるアクセス制御

システム設計者は、ルータ及びファイアウォールなど、通信のアクセス制御が可能な機器ではアクセス制御に関して設計書を作成し、情報を公開する上で、必要最低限のアクセスのみ許可するようアクセス制御を実施し厳密に管理しなければならない。アクセス制御は、送信元及び送信先アドレスだけ、プロトコル、通信ポートでなく、時間や通信量などの制限も含まれる。これらのアクセス制御は、外部から外部公開サーバセグメントへのアクセス制御のみならず、外部公開サーバセグメントから外部へのアクセス制御も同様に、実施、管理しなければならない。

これらのアクセス制御の設計書は変更時を含めて、情報セキュリティ委員会に報告し、随時検査を受け、承認を得なければならない。システム管理者は、この変更履歴を保管管理しなければならない。

（５） OS、アプリケーション・サービスのアクセス制御

システム設計者は、OS のアクセス制御とアプリケーションとサービスのアクセス制御に関して、設計書を作成し、厳密にアクセス権を設定しなければならない。この設計書は、変更履歴を含めて保管管理しなければならない。

（６） データのアクセス制御

システム設計者は、データのアクセス制御に関して、設計書を作成し、厳密にアクセス権を設定しなければならない。この設計書は保管管理しなければならない。これらのデータには、OS のシステムファイルやアプリケーション、アプリケーション設定ファイルなども含まれる。これらの設計書は、変更履歴を含めて保管管理しなければならない。

（７） アプリケーション開発

システム設計者は、CGI、API などのアプリケーション開発を行う際、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などの、セキュリティ対策の実施を行わなければならない。

（８） 不正アクセス検知システム（IDS）について

システム設計者は、IDS を設置する場合、設計時に以下の作業を行わなければならない。

・適用するシグネチャの選定及び必要なシグネチャの作成
・対応手順の必要なシグネチャの選定と、その対応手順書の作成

（９） 外部公開サーバの推奨プラットホーム

情報システム委員会は、外部公開サーバに関して、推奨プラットホームを規定することが望ましい。システム設計者は外部公開サーバのプラットホームについては、情報セキュリティ委員会が規定する推奨プラットホームを採用することが望ましい。

（１０）設置場所

システム設計者は対象システムの安全な設置場所を検討しなければならない。

安全な設置場所とは、以下の条件を満たす場所を指す。

・施錠されていること
・明示的に許可された者以外の立ち入りが禁止されていること

・ネットワークの盗聴が外部から行えないこと
・監視カメラが設置されていること

（１１）セキュリティ侵害時の対応手順書の作成

システム設計者は、リスク分析で想定されるセキュリティ侵害が発生した場合の対応手順書を設計時に作成しなければならない。対応手順書には以下の項目が含まれていなければならない。

・想定されるセキュリティ侵害の可能性がある事象とその定義
・確認方法
・確認で得られ情報毎の対応方法
・連絡先及び緊急連絡先
・セキュリティ侵害事象の保存方法
・外部公開サーバの運用再開の基準

４．２　設置の申請・設計審査に関する遵守事項

（１）　申請書の提出

外部公開サーバの設置申請者（以下、申請者）は、外部公開サーバの設置の際、必ず情報セキュリティ委員会に「外部公開サーバ設置申請書」を提出し、許可を得なければならない。申請には、申請者の押印だけではなく所属長部長職相当の押印が必要である。

申請を受けた情報セキュリティ委員会は、直ちに審査を開始しなければならない。「外部公開サーバ設置申請書」には次の項目を含まなければならない。

・システム設置の趣旨と扱う情報の内容
・システム構成
・システムの設置場所の住所と組織名称
・システム管理者名とシステムセキュリティ責任者名
・運用開始希望日
・運用管理手順書の添付
・セキュリティ侵害時の対応手順書の添付

（２）　システム構成の明確化

申請者は、外部公開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、申請者及びシステム設計者は、直ちに

システム構成の再検討を行わなければならない。

（３） 管理体制及びシステム管理者の明確化

申請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、管理体制及びシステム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、システム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。

（４） 運用手順書の提出

申請者は、外部公開サーバの設置申請時に運用手順書を情報セキュリティ委員会へ提出なければならない。

（５） セキュリティ侵害時の対応手順書の提出

申請者は、外部公開サーバの設置申請時にセキュリティ侵害時の対応手順書を情報セキュリティ委員会へ提出しなければならない。

（６） 既存の外部公開サーバの申請について

本標準が適用される以前の既存の外部公開サーバについては、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。

４．３　システム構築に関する遵守事項

（１） 提供サービス

システム構築担当者は、外部公開サーバの趣旨、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。

（２） 安全な設定

システム構築担当者は外部公開サーバに、安全な設定を施さなければならない。安全な設定とは、以下の要件を満たすものである。

・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
・不要なプログラムやサービスの削除

（3） パスワード強度

ルータ、サーバなど全てのパスワードが利用できる機器には、パスワードを設定しなければならない。特にシステム管理者もしくはシステム管理者に類する権限を持つアカウントのパスワードは、下記のように厳重に設定されなければならない。

・システム管理者自身が設定する
・８文字以上
・大文字小文字の区別がある場合には大文字を１文字以上含める
・記号が含められる場合には１文字以上含める
・数字が含められる場合には１文字以上含める

４．４　検査に関する遵守事項

・検査実施手順

外部公開サーバは、運用開始前に必ずシステム構築担当者が情報セキュリティ委員会が指定する第三者による検査を受けなければならない。検査には以下の項目を含まなければならない。

・最新の脆弱性情報を含む検査項目
・「外部公開サーバ設置申請書」との整合性
・許可された範囲以外へのアクセスが出来ないこと
・アクセスコントロール定義の確認
・不要なサービス、不要なアカウントが存在しないこと
・推測可能なパスワードが設定されていないこと

検査は、インターネット方向からだけでなく、様々な脅威を想定した方向から実施し、検査に合格するまでは接続試験や検査の目的以外で運用を開始してはならない。また、検査は定期的に実施するが、外部公開サーバが新設された場合及び、ルータ、ファイアウォールの設定変更された場合は随時検査を実施する。検査に不合格になった場合には、１週間以内に対策を行い、再検査を受け、以後これを繰り返す。

４．５　運用に関する遵守事項

（1） セキュリティレベルの維持

システム管理者は、常に最新のセキュリティ情報を入手し、OS 及びインストールされた、アプリケーション・サービスについて、随時、必要な最

新のアプリケーションのバージョン、セキュリティパッチを適用しなければならない。また、これらの履歴は保管管理しなければならない。OS 及びインストールされたアプリケーション・サービスに関するセキュリティホールのうち深刻なものであると判断され、かつセキュリティパッチが公開されていないものについては、別方法のセキュリティ対策の検討し、その施策を実施しなければならない。検討の結果、セキュリティ対策が無いと判断された場合は、速やかに情報セキュリティ委員会に報告し、情報の公開を停止しなければならない。この停止は、対応のセキュリティパッチの適用もしくは別の施策が実施にて、セキュリティ委員会に報告後、解除できる。

（２） 外部公開サーバのアカウント管理

システム管理者は、外部公開サーバの趣旨、用途に応じた、必要最低限のアカウント以外作成してはならない。また、アカウント毎のアクセス権を規定し、必要最低限のアクセス権のみ付与しなければならない。これらのアカウントは更新履歴を含めて、管理しなければならない。パスワードが必要なアカウントについては、適切なパスワード強度を有しなければならない。

（３） パスワード管理

設定されたパスワードには、以下の運用がなされなければならない。

・１ヶ月に一度必ず更新されなければならない

・同じパスワードを異なる機器、異なる時期に使用してはならない

・設定されたパスワードは、システム管理者が責任を持って携行及び保管する手帳類以外には書き留めてはならない

・緊急時（現場に行くことができない場合等）を除いて、システム管理者以外に教えてはならない。

・パスワードを入力する際は、他人に見られないよう注意しなければならない

（４） 運用業務の委任

システム管理者の運用業務はオペレータに委任することができるが、オペレータは運用手順書以外の操作を行ってはならない。

（５） 運用日誌

システム管理者は、次の項目を含んだ運用日誌を作成し一定期間、保管

管理しなければならない。

・システムへのログイン時間とログオフ時間
・システムの設定変更内容
・ログの保存記録
・バックアップ実施記録
・システムエラーの記録とその是正処置

また情報セキュリティ委員会は、定期的に運用日誌を検査し不適切な記載が発見された場合、適切な是正処置をシステム管理者に指導しなければならない。

（6） 入退室管理

システム管理者は、全ての外部公開サーバの設置場所への入退室記録を保管管理しなければならない。これらの機器のディスプレイ及びコンソールは離席時を含めて、システム管理者及び、オペレータ以外操作、目視できないように必ず、ログアウトもしくはパスワードで保護された状態にしなければならない。

（7） リモートメンテナンス

システム管理者は、外部公開サーバの情報及びデータを、ネットワークを利用し更新・メンテナンスを行う必要がある場合は、その手順を明確に規定しなければならない。システム管理者は、リモートからの情報の更新手順書を作成し、リモートメンテナンスを実施する者に配布、徹底させなければならない。

（8） ログの取得について

外部公開サーバのOS 及びアプリケーション監査ログは次の項目を含めなければならない。

・ユーザID
・ログオン及びログオフの日時
・端末のIP アドレスもしくは端末のID
・OS もしくはアプリケーションへのアクセスを試み、成功したものと、失敗したものの記録
・内部エラー

ファイアウォールおよびルータなど通信経路に設置される機器のログは次の項目を含めなければならない。

・アクセス日時
・プロトコル番号
・ソースIP アドレス
・ソースポート
・ディスティネーションポート
・ディスティネイションIP アドレス
・許可しているアクセス及び、許可していないアクセス

（９） ログの保存

ログは、一時的にハードディスクなどの書き換え可能なメディアに保存されていても良いが、２４時間以内に書き換え不能なメディアに転送され厳重に保管されなければならない。一時的にハードディスクなどの書き換え可能なメディアにログを記録する場合には、十分な記憶容量を確保しておき、異常な量の書き込みが発生した場合においても十分に対処できるように備えておかなければならない。ログは、その取得日から３年間は確実にシステムセキュリティ責任者のみが参照できる場所と方法で厳重に保管されなければならない。

（１０）ログの解析

保存されたログは、システムセキュリティ責任者もしくはシステムセキュリティ責任者からに委任を受けたシステム管理者により解析されなければならない。

ログの解析は少なくとも１ヶ月に１回以上定期的に行わなければならず、セキュリティ侵害や、その可能性がある場合は随時行わなければならない。

ログの解析を行う際は以下の点に注意しなければならない。

・許可されていないIP アドレス
・指定時間外のアクセス
・アクセス頻度
・データ量
・度重なるアクセス失敗

（１１）時間の同期

システム管理者は、ログの精度及び、ログの証拠としての信頼性を確保するために、外部公開サーバの時間の同期を行わなければならない。

（１２）外部公開サーバ情報のバックアップ

システム管理者は、対象システムに保存されるデータとシステムの設定情報をそれぞれ一定期間毎にバックアップをとり、保管管理しなければならない。

（１３）セキュリティ侵害時の対応

システム管理者は、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書に則って対応しなければならない。
またシステム管理者は、セキュリティ侵害時の情報を、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。

（１４）想定外のセキュリティ侵害への対応

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書のみでは状況の改善が見込めない場合、システム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。システム管理者は、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。

またシステム管理者は、状況の改善後、作業実施記録を元にセキュリティ侵害時の対応手順書を更新しなければならない。

（１５）セキュリティ侵害時の対応手順書の更新

システム管理者は、セキュリティ侵害時の対応手順書の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。

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。