システム監視に関する標準

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

システム監視に関する標準

１　趣旨

本標準は、当社が利用している情報システムの監視について規定し、システム障害、不正アクセスの兆候、情報の流出、不正利用等をいち早く検知し、それらの原因究明が円滑に行われることを目的とする。

２　対象者

当社の情報システム部に所属するすべての社員を適用対象とする。ただし、これに限らず社内においてサーバ、ファイアウォール、主要なネットワーク機器を管理・運用するすべての者について適用する。

３　対象システム

当社の従業員が業務上、利用するすべてのサーバ、ファイアウォールおよび主要なネットワーク機器

４　遵守事項

４．１　対象システムのログによる監視

（１） 情報システム部は､対象システムに関して次にあげるログを取得すること。なお取得されたログは 24 時間以内に書き換え不能なメディアに転送し、3 年間、安全に保管すること。

取得対象：

① ログオン・ログオフの記録
② サーバのアクセスログ
③ ファイアウォールのログ
④ 主要なネットワーク機器のログ
⑤ システムログ

取得内容：

① アクセス時刻

② 発信元/先アドレスとポート番号
③ アクセス成功/失敗
④ 認証成功/失敗

（2） 情報システム部は、許可された処理だけが実行されていることを確認するために、ログを月 1 回解析すること。解析の結果、以下のような事象が確認された場合、情報セキュリティ委員会に報告すること。
① 連続したアクセスの失敗
② 連続した認証の失敗
③ 大量のデータの送受信
④ 権限外の処理の試み
⑤ ユーザアカウントに関する変更（追加、削除、グループ変更等）
⑥ アクセス権の変更

（3） 情報システム部は（2）の事象が、不正アクセスによってもたらされた疑いがある場合には、『セキュリティインシデント報告、対応標準』に基づいて、原因究明、再発防止計画の作成等、適切な対応を実施しなければならない。

（4） 情報システム部は、（1）で取得するログの時間情報を適切に保ち、ログの証拠としての有効性を高めるため、NTP サーバ等を用いてシステム間の時刻同期をとらなければならない。ただし、その場合、NTP サーバ自身のセキュリティ対策にも十分配慮すること。

４．２　侵入検知システムによる監視

（1） 本社のグローバルゾーンおよび DMZ のネットワークにおいては、ネットワーク監視型侵入検知システムを導入し、不正アクセスの発生状況を常時監視すること。

（2） 本社のグローバルゾーンおよび DMZ 上に設置されているサーバにおいては、ホスト監視型侵入検知システムを導入し、不正アクセスの発生状況を常時監視すること。

（3） 情報システム部は、シグネチャベースの侵入検知システムを用いる場合は、

最新のシグネチャにアップデートされた状態を維持しなければならない。

（４） 情報システム部は（１）、（２）の監視によって、不正アクセスの兆候が検知された場合には、『セキュリティインシデント報告、対応標準』に基づいて、速やかに対応しなければならない。

（５） 情報システム部は、侵入検知システムのログを月 1 回分析し、結果を情報セキュリティ委員会に報告しなければならない。

（６） 情報システム部は、侵入検知システムのログを 24 時間以内に書き換え不能なメディアに転送し、3 年間、安全に保管すること。

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。