セキュリティ情報収集及び配信標準

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

セキュリティ情報収集及び配信標準 1
１　趣旨 1
２　対象者 1
３　対象システム 1
４　遵守事項 1
４．１　セキュリティ情報の収集 1
４．２　セキュリティ情報の配布 2
５　例外事項 2
６　罰則事項 3
７　公開事項 3
８　改訂 3

セキュリティ情報収集及び配信標準

１　趣旨

本標準は、社内で使用されている製品のセキュリティ情報を収集し、セキュリティレベルを維持する事を目的とする。

２　対象者

当社の情報システム部

３　対象システム

当社に導入されているすべてのソフトウェアおよびハードウェア
“すべて”➔”識別された”がいいなぁ

４　遵守事項

４．１　セキュリティ情報の収集

（１） 情報システム部は『ソフトウェア/ハードウェアの購入標準』で作成された各管理台帳をもとに、社内システムに導入されている全てのハードウェア及びソフトウェアのセキュリティ情報について、定期的に情報を収集しなければならない。

（２） セキュリティ情報は各ベンダーの Web サイトやサポートページなどから収集する。

（３） 情報システム部門（部門⇔部どっち）はセキュリティ関連のメーリングリスト、セキュリティセミナーなどに参加し情報を収集する。

（４） 収集した情報は、重要性、影響範囲などから下記の様に分類する。
危険度　高：サーバの管理権限の剥奪などにより、業務が停止してしまう、または取引先などに影響を与える可能性があり、即座に対応が必要な情報
中：業務が停止するあるいは取引先などに影響は与えないため、

即座に対応する必要はないが、定期メンテナンス時などに対処する必要がある情報

低：特殊な環境/設定でのみ発生し、社内のシステムには関係がないため、特に対処しなくともよい情報

４．２　セキュリティ情報の配布

（１）　情報システム部は、収集した情報を危険度に応じて関係者に対して報告しなければならない。

危険度　高　：発見次第即座に関係者全員に連絡
連絡方法は基本的にはメールを使用。場合によっては社内放送なども利用する。

中　：週 1 回程度の定例報告を行う。メールにて関係者全員に連絡

小　：週 1 回程度の定例報告を行う。メールにてシステム管理者に連絡

（２）　情報システム部より通知を受けた者は速やかにその指示に従わなければならない。パッチを適用が必要な場合は『システム維持に関する標準』、ウィルス定義ファイルを更新する場合には『ウィルス対策標準』に基づいて行わなければならない。

（３）　情報システム部は、収集した情報を基に以下のものを作成、公開することが望ましい。

- サーバ設置時の OS の適用パッチ一覧
- サーバ設置時に必要となるサービスなどをまとめたセキュリティ設定チェックリスト
- アプリケーションの適用パッチ一覧
- アプリケーションの実装変更

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 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。