２２．セキュリティインシデント報告、対応標準

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

２２．セキュリティインシデント報告、対応標準

２２．１　趣旨

本標準は、セキュリティインシデントが発生した場合に迅速に対応し、円滑に事業継続がなされることを目的とする。

また、当社においてセキュリティインシデントとは下記の事態を指す。

①情報セキュリティに対する侵害
例：不正アクセスによる情報漏洩、従業員による情報漏洩、ウイルス感染、
なりすまし、使用不能攻撃、ハードウエア紛失
②システム・ネットワークの故障
例：電源異常、熱暴走、機器破損　等

２２．２　対象者

本社・営業所・子会社・関連会社を含む当社のすべての従業員

２２．３　対象システム

当社の従業員が業務上、利用するすべてのシステム

２２．４　遵守事項

２２．４．１　平時の準備

（１） 従業員は、業務上、利用するすべてのコンピュータについて、『ウイルス対策標準』に基づき、適切にウイルス検査を実行しなければならない。

（２） 従業員は、ノート PC・機密資料等の情報資産を紛失しないように十分、注意しなければならない。

（３） 従業員は、『セキュリティ情報収集および配信標準』に基づいて、日常的にセキュリティ情報を収集し、適切な対策を実施しなければならない。

（４） 情報システム部は、将来起こりうる調査やアクセス制御の監視に役立てるために『監視に関する標準』に基づいて、適切にログを取得しなければならない。

（５） 情報システム部は、将来起こりうるシステムの復旧作業に役立てるために『システム維持に関する標準』に基づいて、適切にバックアップを取得しなければならない。

（６） 情報システム部は、不正アクセスを検知するため、『監視に関する標準』に基づいて、侵入検知システム（IDS）を利用し、適切にシステムおよびネットワークの監視を行わなければならない。

（７） 情報システム部は、重要なシステムに対して UPS を使用し、停電時には自動でシャットダウンを行うように設定しなければならない。

２２．４．２　セキュリティインシデント発生時

（１） 当社ではセキュリティインシデントを被害の深刻度に応じて、以下のようにレベル分けする。従業員はレベルに応じた報告先に対し、速やかに報告し、指示を仰がなければならない。

① レベル１（深刻度：低）
問題の発生原因・被害の範囲とも当社内に限定される場合
＜報告先＞
必須：情報システム部、情報セキュリティ委員会

② レベル２（深刻度：中）
社外の第三者からのセキュリティ侵害により、当社が被害者となる場合
＜報告先＞
必須：情報システム部、情報セキュリティ委員会
任意：警察機関、コンピュータ緊急対応センター（JPCERT)、
情報処理振興事業協会（IPA）

③ レベル３（深刻度：高）
顧客や取引先等の社外に対して、当社が加害者となる場合
＜報告先＞
必須:情報システム部、情報セキュリティ委員会、該当する顧客や取引先、
総務部（広報）

（２） 従業員は、ウイルス感染被害や不正アクセスの被害に気づき次第、対象システムをネットワークから切り離すこと。（１）で定める報告先へは対象システムの切り離し後、報告すること。

（３） 情報セキュリティ委員会は、ログ・IDS の監視レポート・関係者へのヒアリング等に基づいて、速やかに被害状況を把握し、情報セキュリティ委員長の指示のもと、対策にあたらなければならない。

（４） 情報セキュリティ委員会は、被害状況を把握するにあたり、次の事項を確認すること。
①セキュリティインシデントの種類
②被害を受けた日時
③原因と対処方法
③被害の拡大範囲

（５） 情報システム部は、侵害原因が解消された後、速やかにバックアップテープを用いてシステムを正常な状態に復旧しなければならない。

（６） 従業員は、ウイルス感染などが原因で OS,アプリケーションの入れ替えが必要になった場合は、適切なメディアを使用して速やかに再インストールを実施すること。

２２．４．３　再発防止計画

（１） セキュリティインシデントへの対応が完了した後、情報セキュリティ委員会および情報システム部は、２２．４．２（４）で調査した被害状況をもとに再発防止計画を作成しなければならない。再発防止計画作成時には、技術的側面と組織的（制度的）側面の両方に留意すること。

（２） ２２．４．３（１）で作成された再発防止計画は、すべての従業員に周知され、適切に実施されなければならない。

（３） 情報セキュリティ委員会は、セキュリティインシデントの発生から再発防止計画作成までの一連の記録を保管・管理しなければならない。

２２．５　運用の見直し

２２．５．１　訓練計画

（１） 本標準の内容の実効性を担保するため、情報セキュリティ委員会は、定期的にセキュリティインシデント対応訓練を計画し、すべての従業員を対象とした訓練を実施しなければならない。

２２．５．２　訓練の評価

（１）訓練の結果は、情報セキュリティ委員会において、レビュー、改善策の審議を実施しなければならない。

（２）訓練の結果は、改善策とともにすべての従業員に周知されなければならない。

２２．６　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。

２２．７　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。

２２．８　公開事項

本標準は対象者にのみ公開するものとする。

２２．９　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。