セキュリティインシデント報告・対応標準

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

セキュリティインシデント報告・対応標準

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、情報システム環境の復旧が円滑に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次の事態を指す。

（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　等

（2）システム・ネットワークの故障、損壊

例：電源異常、熱暴走、天災による機器損壊　等

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

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

４　遵守事項

４．１　平時の準備

（1）　情報セキュリティ委員会は、『セキュリティ教育に関する標準』に基づいて、セキュリティ教育を実施し、従業員のセキュリティ意識の向上に努めなければならない。

（2）　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』に基づいて、適切にウイルス対策を実施しなければならない。

（3）　情報システム部は、『セキュリティ情報収集および配信標準』に基づいて、当社で使用されている製品のセキュリティ情報を収集し、必要なセキュリ

ティ対策を実施することでセキュリティレベルを維持しなければならない。

（4） 情報システム部は、インシデントの検知や原因究明に役立てるために『システム監視に関する標準』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、インシデントを検知するため、『システム監視に関する標準』に基づいて、侵入検知システムを利用し、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。

（6） 情報システム部は、インシデント発生後の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。なお、バックアップは必要に応じて遠隔地にコピーを保管することが望ましい。

（7） 情報システム部は、インシデント発生後のシステムの復旧作業に必要なリソースを検討し、確保しておかなければならない。

（8） 情報セキュリティ委員会は、各システムの復旧優先度を決定しなければならない。復旧優先度の決定は、対象システムにおいて運用される業務の停止許容時間を観点において行う。
（表１参照）

表１

復旧優先度	業務復旧までの許容時間
3	業務が停止することは許されない
2	24時間以内に復旧しなければならない
1	3日以内に復旧しなければならない
0	インシデント発生時は停止してもよい

４．２　セキュリティインシデント発生時

（1） 従業員はインシデントの発生と疑われる事象を発見した場合、速やかに情報セキュリティ委員会もしくはセキュリティ担当者に報告しなければならない。またクライアント PC において、ウイルス感染や不正アクセスの疑いがある場合、発見後ただちに該当するクライアント PC をネットワークから切り離した上で報告しなければならない。

（2） （1）の報告を受けた情報セキュリティ委員会およびセキュリティ担当者は、下記の観点で状況把握し、対応方法を報告者に指示しなければならない。セキュリティ担当者が報告を受けた場合は、対応方法を報告者に指示するとともに下記事項を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。
またセキュリティ担当者のみでの作業が困難である場合は、速やかに情報セキュリティ委員会に申し出て、協力を依頼すること。
＜観点＞
・インシデント発生の真偽
・被害を発見した日時
・被害の拡大範囲
・被害内容
・被害原因
・対応方法

（3） インシデントの発生が確認された場合、情報セキュリティ委員会は速やかに関連する部署（情報システム部、広報担当等)、プロバイダー、外部ベンダー等に連絡し、協力を依頼しなければならない。
また、情報セキュリティ委員会は必要に応じて組織横断的なタスクフォースを設け、状況把握や対応方法の指示にあたることができる。

（4） 情報システム部は、インシデントの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。復旧作業にあたっては、４．１（８）で決定した復旧優先度に従って作業すること。

（5） 従業員は、インシデントの 2 次被害防止のため、OS、アプリケーションの入れ替えやクライアント PC の設定変更等の作業が必要になった場合は、情報セキュリティ委員会の指示に従い､速やかに実施しなければならない。

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、調査結果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側面の両方に留意すること。

（2） 情報セキュリティ委員会は発生したインシデントのうち、以下の要件を満たすものについては、再発防止計画と共に取締役会に報告しなければならない。

＜要件＞

・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

・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

（3） 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。

（4） 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。

４．４　運用の見直し

４．４（1）　訓練計画

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の訓練計画を作成し、従業員参加のもと、訓練を実施しなければならない。

４．４（2）　訓練の評価

・　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し、セキュリティ対策の運用について改善策の審議を実施しなければならない。

・　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。

４．４（3）　インシデント後の見直し

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事後に一連の対応を見直し、運用上の改善点を検討しなければならない。検討の結果、運用変更が必要であると認められた場合、速やかに関係する従業員に周知されなければならない。

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。

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。

8　公開事項

本標準は対象者にのみ公開するものとする。

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。