セキュリティインシデント報告・対応規程

1.0版

セキュリティインシデント報告・対応規程

セキュリティインシデント報告・対応規程

１　趣旨

本規程は、セキュリティインシデントが発生した場合及びセキュリティインシデントの発生と疑われる場合、適切な連絡経路を通じて極力速やかに報告し、定められた手順に従って迅速に対応し、情報システム環境の復旧が速やかになされることと、発生した事態から問題点や改善点などに対する学習を行い、継続的な再発防止が行われることを目的とする。

当社におけるセキュリティインシデントとは次のような事態を指す。

（１）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えい、従業員による情報漏えい、ウイルス・マルウエア感染、DoS 攻撃、記録媒体等の紛失　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

（３）情報資産への脅威

例　建物への侵入　　等

２　対象者

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遂行のため利用するすべてのシステム。

４　遵守事項

経営者の同意・承認の元、未然に防げなかった事態が発生した際に、事態の可及的速やかな収拾と被害や影響範囲を最小にするために、平時からの取組と組織・役割の責任の明確化・伝達方法・事態の評価と対応及び再発防止を含む学習についての取り組みを明確にする。

４．１　平時の準備

(A.16.1.1)

セキュリティインシデントが発生した場合、あるいは発生が疑われる場合は情報セキュリティ委員会に遅滞なく報告がなされ、速やかにセキュリティインシデントの分析、封じ込め、原因の根絶、復旧が可能となるよう、４．２項以降に示す対応について以下の準備作業を行い、関係者に周知・徹底する。

（１）情報セキュリティ委員会は、想定するセキュリティインシデントの具体的な対

応手順を策定する。対応手順には，次の事項を含む。

- 緊急時対応の対応組織の始動、及び終了に関する契機
- 緊急時対応の対応組織の役割、責任の明確化

なお、緊急対応の実行責任者は，緊急時対策に関するすべての判断の権限及び責任をもつものとする。

- 組織の内部及び外部機関との協力関係の明記
- 組織の内外への必要な連絡先の明記

（2）情報セキュリティ委員会は、策定した対応手順でセキュリティインシデントに対応可能となるよう、定期的に訓練を行い、併せて対応手順に問題がないか確認を行い、対応手順に問題があれば是正する。

（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検知に必要な情報セキュリティ対策の導入に向け、情報セキュリティマネジメントを遂行しなければならない。

（4）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　事象の検知、報告と分析

(A.16.1.2)

セキュリティインシデント、あるいは発生が疑われる事象を検知したものは、情報セキュリティ委員会に遅滞なく報告しなければならない。

情報セキュリティ委員会は、報告されたセキュリティインシデントに応じ、策定した対応手順に従い、被害の特定、原因の分析を行う。

なお、策定した対応手順に該当しないセキュリティインシデントの場合、情報セキュリティ委員会は、そのための実行責任者を任命し、対応組織を始動し、被害の特定、原因の分析を行う。

検知したセキュリティインシデント情報、原因の分析状況について、実行責任者のもと、一元的に収集、管理する。

４．３　封じ込め、根絶、復旧

(A.16.1.5)

特定したセキュリティインシデントの原因に基づく対応手順に則り、被害の拡散を防止し、被害箇所の原因の根絶、修復を行い、復旧をする。

なお、セキュリティインシデントに関する情報は、実行責任者のもと、一元的に収集、管理する。以下の情報を管理、記録する。

・セキュリティインシデントの発生状況及び対応状況に関する情報
・自社のビジネス活動再開に関する情報
・顧客及び取引先等利害関係者の影響等に関する情報

４．４　インシデントからの学習

(A.16.1.6)

セキュリティインシデントの対応後、同様のセキュリティインシデントの再発防止、および対応手順の不備等について改善を行う。

（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。

（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。

・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管理した記録から、対応手順の不備、または良かった点を整理し、対応手順を改善しなければならない。また、一連の記録を保管、管理しなければならない。

５　運用確認事項

インシデント発生時における対応方法について、あらかじめ報告及び復旧等に向けた手順を作成しているか確認する。また、インシデント対応実施後に再発防止策、対応手順の改善が行われているか、確認する。

６　例外事項

業務都合等により本規程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

本規程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『人的管理規程』に従う。

８　公開事項

本規程は対象者にのみ公開するものとする。

９　改訂

・本規程は、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。

・本規程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。

・本規程は、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。