リスク管理規程

1.0版

リスク管理規程

リスク管理規程

１　趣旨

本規程は、当社を取り巻く状況から派生する課題と、当社の経営課題並びに顧客等利害関係者からの要求事項を考慮し、情報セキュリティに関わる、リスクを防止又は低減する過程を定めることを目的とする。

２　対象者

当社の情報セキュリティ委員会。

３　対象システム

当社が保有するすべての情報資産を対象とする。

４　遵守事項

４．１ リスクアセスメント

当社を取り巻く状況から派生する課題と、経営課題並びに顧客等利害関係者からの要求事項が何なのか、またどこにどのような情報資産が存在し、どのような方法で管理されているかを洗い出す。洗い出された情報資産を機密性、完全性、可用性の観点から重要度の評価を行う。評価の結果、重要と判断された情報資産に対しての脅威や脆弱性は、どのようなものがあるかを洗い出して記述する。

情報資産の評価、洗い出された脅威、脆弱性により、情報資産に関わるリスクを算定する。

リスクアセスメントの過程は、検討された事項や除外の理由などを記録しておく。

４．１．１　組織の状況の確定

当社を取り巻く外部及び内部状況を洗い出す。外部状況としては、法律・規制・技術・自然環境、情報セキュリティ事件・事故の傾向、利害関係者の情報セキュリティに関する要求事項等があり、内部状況としては、経営方針・目標・課題・戦略、組織体制、社会的責任、企業文化、情報システムに関わるプロセス等がある。

洗い出した状況より、当社の情報セキュリティに影響を与える課題を確定する。

４．１．２　情報資産の洗い出しと重要度分析

当社の情報資産が業務の流れの中で、どこにどのような形でどのように利用、保管、管理されているかを洗い出す。情報資産は、関連会社や取引先などにも利用されている場合が多く、情報資産を取り扱う従業員に協力を得て存在を確認する。洗い出された情報資産は、情報資産管理者（情報やデータの持ち主で存在及び利用の責任者）とともに

機密性、完全性、可用性、また流出時の影響度などを考慮し重要度を付け、情報資産台帳に記録する

４．１．３　脅威の洗い出し

脅威の洗い出しにおいては、以下を遵守しなければならない。

（１）重要度付けの結果、重要と判断された情報資産に関する脅威を、従業員の協力・参画の元、情報資産の保存形態、利用形態を考慮して洗い出し、記録する。

（２）脅威の洗い出しにおいて、過去に発生したヒヤリ・ハット、事件・事故、業務遂行上の問題点を考慮して洗い出す。

４．１．４　脆弱性の洗い出し

対象となる情報資産を、保存形態、利用形態を考慮してその脆弱性を洗い出し記録する。

４．１．５　リスクの分析

（１）洗い出された脅威と脆弱性に対し、どのような時にどのような状況でどのような原因でどのようにリスクが発生するのか、発生した場合にどのような影響があるのかを分析する。

（２）分析の際に使用した状況・原因・影響について記録し、除外した部分や除外した理由について記録する。

４．１．６　リスクの特定

（１）分析されたリスクについて、当社に関係すると思われるリスクを特定する。

（２）特定したリスクについて、特定の理由と状況・原因・影響を記録する。

（３）特定に至らなかったリスクについては、至らなかった理由を記録する。

４．１．７　リスクの算定

（１）特定されたリスクに対し、起こり易さと、そのリスクが発生した場合に当社が被る損害（金額・範囲・関係する利害関係者等）について具体的な数値を示して算定を行う。

（２）算定の際に使用した条件・数値等を記録する。

４．２　リスクの対応

（１）アセスメントで洗い出し・分析・特定・算定されたリスクに対して、受容レベルを決定し記録する。

（２）受容レベルを超えるリスクに関してリスク対応の種類より対応を決定し記録す

る。

（3）決定の際に使用された判断材料について記録する。

４．２．１　リスク対応の種類

リスク対応は、以下からひとつ、または複数の組み合わせを選択する。

（1）リスクの回避

リスクを発生させる活動や行動を、開始しない、または継続しないと決定することにより、リスクを回避すること。

（2）リスクテイク

リスクを発生させる活動や行動を、開始しない、または継続しないと決定することにより、リスクを回避すること。

例えばビジネスの機会を追求または増加するためにリスクを取るまたはリスクを増加させること。利益を追求するために市場の拡大などを目ざす場合に、積極的にリスクを取ること。

（3）リスク源の除去

リスク源を取り除く。リスクの原因となっている脅威又は脆弱性を排除・除去すること。

（4）起こりやすさの変更

リスクの起こりやすさを変えること。リスクが発生する確率は同じではなく、少なくなる、または多くなる場所・要因・時間帯など様々な要素があり、これらを考慮してリスクの起こりやすさを変えること。

（5）結果の変更

事前の策により結果を変えること。万が一リスクが発生した場合に、損失をできるだけ小さくなるよう結果を変えること。

（6）リスクの共有

一つまたは複数の他者とリスクを共有すること。万が一リスクが発生した場合に保険などで被害に対する損害賠償などの減額を行うこと。

（7）リスクの保有

十分な情報に基づいた選択と経営者の判断によりリスクを保有する（受け入れる）こと。

４．３　管理策の決定

リスク対応の結果から受容レベル以下になるよう、具体的なセキュリティ管理策を決定し、経営者の承認を得て記録し、対策の流れを記載したリスク対応手順書を作成し関係者への周知・徹底を行う。

５　運用確認事項

リスク管理において、以下が行われていることを確認しなければならない。

（１）本規程に基づき、運用の実施・記録の管理が確実に行われ、管理されている事を定期的に確認する。

（２）情報セキュリティ委員会は、マネジメントサイクルが適切に運用されていることを最低年一回以上は確認し、問題があれば適切な助言や改善策を実施する。

（３）情報セキュリティ委員会は、最低年一回以上、従業員及び経営陣にリスクマネジメントに関する問題についてのアンケート調査を実施する。

（４）新しい脅威の情報を取得した場合は、リスクアセスメントとリスクマネジメントを実施し、新たなリスク対応や管理策がとられ、それらの管理策が周知徹底できているかを確認する。また、その管理策の効果を評価し、必要に応じ管理策の見直しを行う。

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。