システムリスクに関する基本方針

Ⅰ 経営者の声明

ビジネスを継続的・安定的に行ううえで、会社の情報資産に対し、適切な安全対策を実施することはビジネス上の重要な要件である。システムに障害が発生した場合には、利用者に多大な損害を及ぼすおそれがあることから、特にシステムリスク管理を適切に行う必要がある。

当基本方針はコンピュータシステムのダウンや誤作動等、システムの不備等、サイバーセキュリティ事案により、又はコンピュータが不正に使用されることにより利用者が損失を被るリスク（以下「システムリスク」という。）が存在しうることを認識しシステムに障害が逸生することにより業務に支障を来すおそれがある場合の措置を定め、必要に応じた態勢整備を行うことにより、適切にシステムリスク管理を行うための会社の基本方針であり、システムリスク管理のためのすべての施策は、この基本方針に則って実施する必要がある。

この基本方針が有効に機能するよう、経営者を含め全社員がこれに関与し、これを支持しなければならない。

※セキュリティポリシー

Ⅱ 情報資産

2-1 情報資産とは

情報資産とは、情報と情報システム、並びにそれらが正当に保護され使用され機能するために必要な要件の総称であり、ハードウェア・ソフトウェア、ネットワーク、各種データファイルのみならず、システム開発・運用のために必要な要員やドキュメント、社員が業務上知り得た顧客情報等を含むものである。

これらは会社の重要な資産であり、これらの機密性・完全性・可用性が失われると会社はビジネス上の損害を被る可能性が大きく、また顧客へ損害を与える場合もある。このため、会社はこれらに対する管理者を設置し、さまざまな脅威（故障、災害、誤処理、不正使用、破壊、盗難、漏洩、サイバーセキュリティ事案等）による被害を最小限にするために必要な対策を行う。

2-2 情報資産の分類

情報資産は、機密性・完全性・可用性の視点から重要度を「最重要」、「重要」、「一般」の 3 段階に分類のうえ、適切に管理しなければならない。

2-3 情報資産へのアクセス

会社は、情報資産がその目的に沿って適切に使用されるよう、正当な必要性に基づくアクセスのみを許可する。会社はこのために必要な時間、資源を投入し、ハードウェア・ソフトウェア、ネットワーク、各種の記録媒体等へのアクセスを管理・監視する。

2-4 情報資産の私的利用の禁止

社員は、会社の情報資産を私的に利用してはならない。

2-5 経営者による確認

経営者は、情報資産が適切に管理・保護されていることを確認する必要がある。このため、会社は定期的にこれらの調査を行い、報告を求める。

2-6 会社の意思決定

会社の意思決定は、情報資産の適切な利用と保護に背反するものであってはならない。

すべての管理者は社員に対して、基本方針に違洗い出し、その維持・反する行為を命じてはならない。

※情報資産の管理に関する基本方針

Ⅲ 情報システム

3-1 情報資産の管理に関する規程の策定

情報システムは、当基本方針に準拠し、システムリスク管理のために必要な要件を満足しなければならない。会社はこのために社内規程中にシステム管理の安全対策に関する規程を策定する。

3-2 情報資産の管理に関する規程の遵守

情報システムの構築、運用において、情報資産の管理に関する規程を遵守しなければならない。

3-3 情報資産管理責任者の設置

情報システムを適正に管理する責任者を設置する。

※リスク管理の基本方針

Ⅳ システムリスク管理体制

4-1 全社システム管理

会社は、情報資産の保護のための統括責任者としてシステム管理担当役員を選任する。また、情報資産の保護を全社統一的な視点で行うためにシステム管理部門を設置し、必要なシステム管理体制を整備する。

システム管理部門は、基本方針やシステムの安全対策に関する各種の規定（コンティンジェンシープランの策定及びシステム障害発生時の対応に関する社内規程等を含む。）を確立し、有効に機能させる職務を担う。

4-2 システムリスク評価

システム管理部門は、システムの制限値その他の事項につき、システムリスクを評価する職務を担う。

4-3 システムの企画・開発・運用管理

システム管理部門は、システムに関する企画・開発・移行の計画に関し、その内容を承認する手続を実施する職務を担う。

4-4 監査体制

監査（システム監査）部門・検査部門は、各部門が基本方針及びそれに基づいた取決めや手順を遵守していることを検証する職務を担う。

Ⅴ　全社員の参加と義務

5-1 社員の義務

　すべての社員（派遣社員を含む）は、基本方針並びにセキュリティに関する各種の規程を遵守しなければならない。

5-2 セキュリティ教育

　会社は、情報資産の保護に関する社員の義務を周知徹底し、情報資産を保護するためのセキュリティ水準を維持・向上させるため、すべての社員に対してセキュリティに関する教育を継続的に実施する。

5-3 基本方針に対する違反の検知と対応

　会社は基本方針に対する違反を検知した場合、就業規則における懲戒対象とすることがある。

※外部委託先に関する方針

VI 外部委託

6-1 委託先の選定

　外部委託に関しては、委託対象業務を適正かつ確実に遂行することができる能力を有する者に委託するため、委託先の選定基準、委託契約における考慮事項や外部委託リスクが顕在化したときの対応について明確にする。

6-2 契約の締結

　外部委託に関しては、外部委託先の役職員が遵守すべきルールや必要なセキュリティ要件を記載した契約を締結する。

　委託先が当該業務を適切に行うことができない事態が生じた場合には、当該業務の委託に係る契約の変更又は解除、他の適切な第三者に当該業務を速やかに委託する等、利用者の保護に支障が生じること等を防止するための措置を含む。

6-3 安全対策の確認及びモニタリング

　委託部門においては、委託先において必要な安全対策が確保されていることを確認し、かつ定期的にモニタリングしなければならない。

VII 情報資産に関する法令の遵守

会社及び社員は、職務の遂行において使用する情報資産に関連する法令を遵守し、これに従う。関連する法令の周知は各部門の情報資産管理者がその責任を負い、法務部門がこれを支援する。

株式会社 VIRTUS　PAYMENT

代表取締役 高田　雅旗