システムリスク管理の基本方針

第１章　総則

（目　的）

第１条　　名寄商工会議所（ 以下、「本所」という。）は、システムに係る外部委託先が提供するサービスを利用して提供する「Yoroca」を継続的・安定的に行ううえで、本所の情報資産に対し、適切な安全対策を実施す ることは重要な要件である。特に、サーバ型前払式支払手段について は、システムに障害が発生した場合には、発行額、回収額、未使用残高の把握ができなくなるおそれや、前払式支払手段の発行の業務が継続 不可能となるなど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。また、サーバ型前払 式支払手段を発行する場合は、自己の発行する前払式支払手段の種類、規模、特性などに応じて、IT と経営戦略を連携させ、企業価値の創出を実現するための仕組みである「IT ガバナンス」を適切に機能させる必要がある。

２ 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や前払式支払手段発行者が損失を被るリスク（ 以下「システムリスク」という。） が存在することを認識し、システム障害が発生することにより前払式支払手段の発行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。

３ 別途定める「情報セキュリティ基本方針」と本方針が有効に機能するよう、役職員がこれに関与し、これを支持しなければならない。

第２章 セキュリティ管理に関する基本方針

（ 情報資産とは）

第２条 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、職員が業務上知り得た利用者情報等を含むものである。

２ これらは本所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本所は損害を被る可能性が大きく、また利用者へ損害を与える場合もある。このため、本所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。

（ 情報資産の分類）

第３条 情報資産は、別途定める「情報機器等管理規程」に基づいて適切に管理しなければならない。

（ 情報資産へのアクセス）

第４条 本所は、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。本所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。

（ 情報資産の私的利用の禁止）

第５条 職員は、本所の情報資産を私的に利用してはならない。

（ 役員による確認）

第６条 役員は、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、本所は定期的にこれらの調査を行い、報告を求める。

（ 本所の意思決定）

第７条 本所の意思決定は、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。

２ 役職員に対して、本方針に違反する行為を命じてはならない。

第３章 情報資産の管理に関する基本方針

（ 情報資産の管理に関する規程の策定）

第８条 情報システムは、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。本所はこのために内部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。

（ 情報資産の管理に関する規程の遵守）

第９条 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。

（ 情報機器等管理責任者の設置）

第１０条 情報システムを適正に管理する責任者として、専務理事を設置する。

第４章 システムリスク管理の基本方針

（ システムリスク管理体制）

第１１条 本所は、情報資産の保護のための統括責任者として事務局次長を選任する。また、情報資産の保護を本所統一的な視点で行うために事務局をシステム管理部門として、必要なシステム管理体制を整備する。

２ 事務局は、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内部規程等を含む。） を確立し、有効に機能させる職務を担う。

（ システムリスク評価）

第１２条 事務局は、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。

（ システムの企画・開発・運用管理）

第１３条 事務局は、システムに関する企画・開発・移行の計画に関し、システムに係る外部委託先に確認し、その内容を承認する手続を実施する職務を担う。

（ 監査体制）

第１４条 監事は、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。

第５章 全職員の参加と義務

（ 職員の義務）

第１５条 すべての職員は、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。

（ セキュリティ教育）

第１６条 本所は、情報資産の保護に関する職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、すべての職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。

（ 本方針に対する違反の検知と対応）

第１７条 本所は、本方針に対する違反を検知した場合、事務局と協力して問題解決にあたり、その原因追究、その再発防止の措置を講じる。

第６章 システムに係る外部委託先に関する方針

（ 委託先の選定）

第１８条 外部委託に関しては、システムに係る外部委託先が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。

（ 契約の締結）

第１９条 システムに係る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。

２ 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、本サービスの利用者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。

（ 安全対策の確認及びモニタリング）

第２０条 事務局次長は、システムに係る外部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。

第７章 情報資産に関する法令の遵守

（ 情報資産に関する法令の遵守）

第２１条 本所及び職員は、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事務局がこれを支援する。