附属書A　管理目的及び管理策

出典：ISO/IEC27001-2013版(JCSR)にを一部、編集。文責：河東岩夫　平成26年3月31日

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **A.5　情報セキュリティのための方針群** | | | | |
| A.5.1 情報セキュリティのための管理の方向性 | | | 事例 | 改訂の影響：小 |
| 目的：情報セキュリティに関する管理の方向性と支持を、事業上の要求事項、関連する法令・規制に従って提示するため。 | | | | |
| A.5.1.1 旧：A.5.1.1 | 情報セキュリティのための方針群 | 情報セキュリティのための方針群を定義し、管理者の承認をもって発行し、従業員及び関連する外部関係者に伝える。 |  | |
| A.5.1.2 旧：A.5.1.2 | 情報セキュリティのための方針群のレビュー | 情報セキュリティのための方針群は、あらかじめ定められた間隔で又は重大な変化が生じた場合、それが適切で、妥当で且つ有効であることを継続するためにレビューする。 | 情報セキュリティ方針は、マネジメントレビューで1 年に1 回見直すほか、5 年毎に全面改定することにしている。5.1.2 | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **A.6　情報セキュリティのための組織** | | | | |
| A.6.1 内部組織 | | | | 改訂の影響：中 |
| 目的：情報セキュリティの実施、運用を開始し、管理するための管理上の枠組みを組織内に確立するため。 | | | | |
| A.6.1.1 旧：A.6.1.3 | 情報セキュリティの役割及び責任 | 全ての情報セキュリティの責任を定め、割り当てること。 | ISMS の構築に当たり、全社を統括するISMS 管理責任者、各部門でISMS を推進するISMS 推進担当者の役割と権限を定め、社長が任命書を交付した。6.1.1 | |
| A.6.1.2 旧：A.10.1.3 | 職務の分離 | 立場が異なる職務や責任範囲は、組織の資産に対する許可されていない、又は、意図していない変更や不正使用される危険性があるため、職務を分離する。 |  | |
| A.6.1.3 旧：A.6.1.6 | 関係当局との連絡 | 関係当局との適切な連絡体制を維持する。 |  | |
| A.6.1.4 旧：A.6.1.7 | 専門組織との連絡 | 情報セキュリティに関する研究会又は専門的なセキュリティ会議、協会・団体との適切な連絡体制を維持する。 |  | |
| A.6.1.5 旧：N/A | プロジェクトマネジメトにおける情報セキュリティ | プロジェク卜の種類にかかわらず、プロジェクトマネジメントにおいて、情報セキュリティに取り組む。 | 新たな開発プロジェクトの開始に当たり、必要な管理策を特定するために、まずリスクアセスメントを実施した。6.1.5 | |
| A.6.2 モバイル機器及びテレワーキング | | | | 改訂の影響：小 |
| 目的：モバイル機器の利用及びテレワーキングに関するセキュリティを確実にするため。 | | | | |
| A.6.2.1 旧：A.11.7.1 | モバイル機器の方針 | モバイル機器を使用することによって生じるリスクを管理するために、方針及び方針を支援するセキュリティ対策を取る。 |  | |
| A.6.2.2 旧：A.11.7.2 | テレワーキング | テレワーキングの現場でアクセスされ、処理され、保存される情報を保護するために、方針及び方針を支援するセキュリティ対策を取る。 | 当社ではシステム管理者にノートPC を貸与し、自宅に持ち帰らせ、休日でも社内システムに異常があった場合は、自宅から監視、一時対応ができるようになっている。6.2.2 | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **A.7　人的資源のセキュリティ** | | | | |
| A.7.1 雇用前 | | | | 改訂の影響：小 |
| 目的：従業員及び契約相手がその責任を理解し、役割を確実にするため。 | | | | |
| A.7.1.1 旧：A.8.1.2 | 選考 | 全ての従業員の選考対象者について、経歴などの確認は、関連する法規制及び倫理を踏まえて行うこと。  また、この確認は、事業上の要求事項、アクセスさせる情報の分類、認識されたリスクに応じて行うこと。 | 中途採用者の雇用にあたって、履歴書や職務経歴書を取り寄せたが、機微なプライバシーには触れないように配慮した。7.1.1 | |
| A.7.1.2 旧：A.8.1.3 | 雇用条件 | 従業員及び契約相手との雇用契約書には、情報セキュリティに関する各自の責任と組織の責任を記載する。 |  | |
| A.7.2 雇用期間中 | | | | 改訂の影響：小 |
| 目的：従業員及び契約相手が、情報セキュリティの責任を認識し、且つ、その責任を全うすることを確実にするため。 | | | | |
| A.7.2.1 旧：A.8.2.1 | 経営陣の責任 | 経営陣は、組織が確立した方針及び手順に従った情報セキュリティを適用させることを、全従業員及び契約相手に要求する。 |  | |
| A.7.2.2 旧：A.8.2.2 | 情報セキュリティの自覚、教育及び訓練 | 組織の全従業員及び、関係する場合は、契約相手も、職務に関連する組織の方針及び手順についての自覚を即す教育・訓練を受け、定期的な啓発を即す。 | 最近会社で定めたセキュリティルールを守らないものが出てきたので、全社員を集めて手順書教育を実施した。7.2.2 | |
| A.7.2.3 旧：A.8.2.3 | 懲戒手続 | 情報セキュリティ違反を犯した従業員に対して、処置を行うための正式、且つ周知された懲戒手続を備える。 |  | |
| A.7.3 雇用の終了及び変更 | | | | 改訂の影響：小 |
| 目的：雇用の終了又は変更のプロセスの一部として、組織の利益を保護するため。 | | | | |
| A.7.3.1 旧：A.8.3.1 | 雇用の終了又は変更に関する責任 | 雇用の終了又は変更に際しては、引き続き、有効な情報セキュリティに関する責任と義務を定め、対象者となる従業員又は契約相手に伝達し、適用する。 |  | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **A.8　資産の管理** | | | | |
| A.8.1 資産に対する責任 | | | | 改訂の影響：小 |
| 目的：組織の資産を特定し、適切な保護の責任を定めるため。 | | | | |
| A.8.1.1 旧：A.7.1.1 | 資産目録 | 情報及び情報処理施設に関連する資産を特定する。また、これらの資産の目録を作成し、維持する。 | ISMS の構築に当たり、全部署の情報資産の棚卸を行い、情報資産台帳を作成した。8.1.1 | |
| A.8.1.2 旧：A.7.1.2 | 資産の管理責任 (オーナシップ) | 目録で維持される資産は、オーナシップを持たせる。 | 内部監査で、情報資産台帳上で管理責任者が特定されていない情報資産があるとの指摘を受けた。8.1.2 | |
| A.8.1.3 旧：A.7.1.3 | 資産利用の許容範囲 | 情報や情報処理施設及びそれらに関わる資産の利用を許可する範囲を特定し、規則を文書化し、実施する。 |  | |
| A.8.1.4 旧：A.8.3.2 | 資産の返却 | 全従業員及び外部の利用者は、雇用、契約又は合意が終了した時点で、自らが所有する組織の資産を全て返却する。 |  | |
| A.8.2 情報の分類 | | | | 改訂の影響：小 |
| 目的：組織に対する情報の重要性に応じて、情報を適切なレベル分けの下で保護を確実にするため。 | | | | |
| A.8.2.1 旧：A.7.2.1 | 情報の分類 | 法的要求事項、情報の価値、重要性、及び許可されていない開示や変更に対して、取扱いを慎重にする必要性の観点から情報を分類する。 | 重要な帳票類を、「機密」、「部外秘」、「社外秘」に分類することとし、情報ごとにその区分を情報資産台帳に記入した。8.2.1 | |
| A.8.2.2 旧：A.7.2.2 | 情報のラベル付け | 情報のラベル付けに関する一連の手順は、組織が採用した“情報の分類”の体系に従って策定し、実施する。 |  | |
| A.8.2.3 旧：A.7.2.2 | 資産の取扱い | 資産の取扱いに関する手順は、組織が採用した“情報の分類”の体系に従って策定し、実施する。 |  | |
| A.8.3 媒体の取扱い | | | | 改訂の影響：小 |
| 目的：媒体に保存された情報の許可されていない開示、変更、除去又は破壊を防止するため。 | | | | |
| A.8.3.1 旧：A.10.7.1 | 取り外し可能な媒体の管理 | 組織が採用した情報の分類体系に従って、取り外し可能な媒体の管理手順を実施する。 | 当社では記憶媒体を使用した情報流出を防止するため、USB メモリの社内での使用を一切禁止している。8.3.1 | |
| A.8.3.2 旧：A.10.7.2 | 媒体の処分 | 媒体が不要になった場合は、正式な手順を用いて、セキュリティを保ち、処分する。 | 使用済みのCD-R を破砕処理するために、専用のシュレッダーを購入した。8.3.2 | |
| A.8.3.3 旧：N/A | 物理的媒体の輸送 | 情報を格納した媒体は、輸送の途中の、不正アクセス、不正使用、破損から保護する。 | 宅配便で、重要な情報が記録された資料や、媒体を送付するときは、インターネットで配送状況を確認することにしている。8.3.3 | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **A.9　アクセス制御** | | | | |
| A.9.1 アクセス制御に対する業務上の要求事項 | | | | 改訂の影響：やや大 |
| 目的：情報及び情報処理施設へのアクセスを制限するため。 | | | | |
| A.9.1.1 旧：A.11.1.1 | アクセス制御方針 | アクセス制御方針は、業務上、及び情報セキュリティの要求事項に基づいて確立し、文書化し、レビューする。 |  | |
| A.9.1.2 旧：A.11.4.1 | ネットワーク及びネットワークサービスへのアクセス | ネットワーク及びネットワークサービスへのアクセスは、利用することを特別に許可した利用者にのみ提供する。 |  | |
| A.9.2 利用者アクセスの管理 | | | | 改訂の影響：小 |
| 目的：システム及びサービスへの許可された利用者のアクセスを、確実にし、認可されていないアクセスを防止するため。 | | | | |
| A.9.2.1 旧：A.11.2.1 | 利用者登録及び登録抹消 | アクセス権を付与するために、正式な利用者登録と登録抹消のプロセスを実施する。 | 新入社員のために、グループリーダが共通サーバを利用するための「アカウント申請書」を起票し、情報システム部に提出した。9.2.1 | |
| A.9.2.2 旧：N/A | 利用者アクセスの提供(プロビジョニング) | 全ての利用者のタイプについて、利用者の要求に迅速に対応するために、全てのシステム・サービスへのアクセス権を割り当て又は無効化するための、正式な利用者アクセスの提供(プロビジョニング)プロセスを実施する。 |  | |
| A.9.2.3 旧：A.11.2.2 | 特権的なアクセス権の管理 | 特権的な利用者のアクセス権の付与及び利用は、制限し、管理する。 |  | |
| A.9.2.4 旧：A.11.2.3 | 利用者の秘密認証情報の管理 | 秘密認証情報の付与は、正式な管理プロセスによって管理する。 |  | |
| A.9.2.5 旧：A.11.2.4 | 利用者アクセス権のレビュー | 資産の管理責任者(オーナ)は、利用者のアクセス権を定められた間隔でレビューする。 | 情報システム部では共通サーバへのアカウント表を毎年3 月に見直すことになっている。9.2.5 | |
| A.9.2.6 旧：A.8.3.3 | アクセス権の削除又は修正 | 全従業員及び外部の利用者の情報及び情報処理施設に対するアクセス権は、雇用、契約又は合意が終了した時に、削除し、または、変更に合わせて修正する。 |  | |
| A.9.3 利用者の責任 | | | | 改訂の影響：小 |
| 目的：利用者に対して、自らの秘密認証情報を保護する責任をもたせるため。 | | | | |
| A.9.3.1 旧：A.11.3.1 | 秘密認証情報の利用 | 秘密認証情報の利用に際しては、組織の慣行に従うことを、利用者に要求する。 | 社員に貸与しているPC へのログインパスワードを社員間で教えあうことを禁止した。9.3.1 | |
| A.9.4 システム及び業務用ソフトウェアのアクセス制御 | | | | 改訂の影響：小 |
| 目的：システム及びアプリケーションへの、許可されていないアクセスを防止するため。 | | | | |
| A.9.4.1 旧：A.11.6.1 | 情報へのアクセス制限 | 情報及びアプリケーションシステムへのアクセスは、アクセス制御方針に従って、制限する。 |  | |
| A.9.4.2 旧：A.11.5.1 | セキュリティに配慮したログオン手順 | アクセス制御方針で求められている場合には、システム及びアプリケーションへのアクセスは、セキュリティに配慮したログオン手順によって制御する。 |  | |
| A.9.4.3 旧：A.11.5.3 | パスワード管理システム | パスワード管理システムは、インタラクティブ(対話式)で且つ、良質なパスワードを確実にする。 |  | |
| A.9.4.4 旧：A.11.5.4 | 特権的なユーティリティプログラムの使用 | システム及びアプリケーションによる制御を無効にすることができるユーティリティプログラムは、使用を制限し、厳しく管理する。 |  | |
| A.9.4.5 旧：A.12.4.3 | プログラムソースコードへのアクセス制御 | プログラムソースコードへのアクセスは、制限する。 |  | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **A.10　暗号** | | | | |
| A.10.1 暗号による管理策 | | | | 改訂の影響：小 |
| 目的：情報の機密性、真正性及び／又は完全性を保護するために、暗号の適切且つ有効な利用を確実にするため。 | | | | |
| A.10.1.1 旧：A.12.3.1 | 暗号による管理策の利用方針 | 情報を保護するための暗号利用に関する方針を策定し、実施する。 | 社外にノートPC を持ち出す場合は必ずハードディスク単位で暗号化することを基本方針としている。10.1.1 | |
| A.10.1.2 旧：A.12.3.2 | 鍵管理 | 暗号鍵の利用、保護及び有効期間(lifetime)に関する方針を策定し、そのライフサイクル全般にわたって実施する。 |  | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **A.11　物理的及び環境的セキュリティ** | | | | |
| A.11.1 セキュリティを保つべき領域 | | | | 改訂の影響：小 |
| 目的：組織の情報及び情報処理施設に対する許可されていない物理的アクセス、損傷及び妨害を防止するため。 | | | | |
| A.11.1.1 旧：A.9.1.1 | 物理的セキュリティ境界 | 物理的なセキュリティの境界を定め、取扱いが慎重な、又は重要な情報や情報処理施設を有する領域を保護するために用いること。 |  | |
| A.11.1.2 旧：A.9.1.2 | 物理的入退管理策 | セキュリティを保つべき領域は、許可された者だけにアクセスを許すことを確実にするために、適切な入退管理によって保護する。 |  | |
| A.11.1.3 旧：A.9.1.3 | オフィス、部屋及び施設のセキュリティ | オフィス、部屋及び施設に対する物理的なセキュリティを設計し、適用する。 |  | |
| A.11.1.4 旧：A.9.1.4 | 外部及び環境の脅威からの保護 | 自然災害、悪意のある攻撃又は事故に対する物理的な保護を設計し、適用する。 |  | |
| A.11.1.5 旧：A.9.1.5 | セキュリティを保つべき領域での作業 | セキュリティを保つべき領域での作業に関する手順を設計し、適用する。 | 利用者からの注文情報を入力するデータ室は、個人情報保護を確実にするため正社員以外の臨時社員や委託先社員単独での作業を許可していない。11.1.5 | |
| A.11.1.6 旧：A.9.1.6 | 受渡場所 | 荷物の受渡場所のように、立寄り場所や、許可されていない者が施設に立ち入る場所は、管理する。また、可能な場合には、許可されていないアクセスを避けるために、情報処理施設をそれらの場所から隔離する。 | 宅配便の集荷場所はオフィスの入り口近くにあり、業者が集荷・配達に来た場合は、総務担当者にインターホンで連絡の上入室してもらっている。11.1.6 | |
| A.11.2 装置 | | | | 改訂の影響：小 |
| 目的：資産の損失、損傷、盗難又は劣化、及び組織の業務に対する妨害を防止するため。 | | | | |
| A.11.2.1 旧：A.9.2.1 | 装置の設置及び保護 | 装置は、環境上の脅威や、災害のリスク、許可されていないアクセスの機会を低減するように設置し、保護する。 | サーバ室には、サーバ管理者から許可を受けて入室カードを持っている者しか入室できない。11.2.1 | |
| A.11.2.2 旧：A.9.2.2 | サポートユーティリティ | 装置は、サポートユーティリティの不具合による、停電、その他の故障から保護する。 | 停電によるシステム停止に備えて、電力の供給系統を２重化した。11.2.2 | |
| A.11.2.3 旧：A.9.2.3 | ケーブル配線のセキュリティ | データを転送する又は情報サービスをサポートする通信ケーブルや電源ケーブルの配線は、傍受、妨害又は損傷から保護する。 |  | |
| A.11.2.4 旧：A.9.2.4 | 装置の保守 | 装置は、可用性や完全性を継続的に維持することを確実にするために、正しく保守する。 |  | |
| A.11.2.5 旧：A.9.2.7 | 資産の移動 | 装置、情報又はソフトウェアは、事前の許可なしに構外へ持ち出さないこと。 | 営業部員が、部外秘以上のデータが記憶されたノートPC を持ち出す場合は、必ず持ち出し許可申請を行い、上司の承認を得ることをルールとしている。11.2.5 | |
| A.11.2.6 旧：A.9.2.5 | 構外にある装置及び資産のセキュリティ | 構外にある資産に対しては、構内での作業とは異なる、構外での作業に伴うリスクを考慮に入れて、セキュリティを適用する。 |  | |
| A.11.2.7 旧：A.9.2.6 | 装置のセキュリティを保った処分又は再利用 | 記憶媒体を内蔵した全ての装置は、処分又は再利用する前に、全ての取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを消去し、又はセキュリティを保って上書きしていることを確実にするために、検証する。 | ノートPC をリースバックするに当たり、専用ソフトを使ってハードディスクの情報を消去した。11.2.7 | |
| A.11.2.8 旧：A.11.3.2 | 無人状態にある装置 | 利用者は、無人状態にある装置が適切な保護対策を備えていることを確実にする。 | 社員は帰宅時に必ず自ら管理しているPC の電源をオフにすることをルールにしている。11.2.8 | |
| A.11.2.9 旧：A.11.3.3 | クリアデスク・クリアスクリーン方針 | 書類や取外し可能な記憶媒体に対するクリアデスク方針や情報処理設備に対するクリアスクリーン方針を適用する。 | 【事例】自分の机の上を整理・整頓できていない社員に対して、グループリーダが厳重に注意をした。11.2.9 | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **A.12　運用のセキュリティ** | | | | |
| A.12.1 運用の手順及び責任 | | | | 改訂の影響：小 |
| 目的：情報処理設備の正確且つセキュリティを保った運用を確実にするため。 | | | | |
| A.12.1.1 旧：A.10.1.1 | 操作手順書 | (情報処理設備の)操作手順は、文書化し、必要とする全ての利用者が利用可能にする。 |  | |
| A.12.1.2 旧：A.10.1.2 | 変更管理 | 情報セキュリティに影響を与える、組織、業務プロセス、情報処理設備及びシステムの変更を、管理する。 | 運用している情報システムのアクセス権申請の手順を変更することとなり、起案、承認、実施、検査などの手順を踏んで実行した。12.1.2 | |
| A12.1.3 旧：A.10.3.1 | 容量・能力の管理 | 要求されたシステム性能を満たすことを確実にするために、資源の利用を監視・調整し、また、将来必要となる容量・能力を予測する。 |  | |
| A.12.1.4 旧：A.10.1.4 | 開発環境、試験環境及び運用環境の分離 | 開発環境、試験環境及び運用環境は、運用環境への許可されていないアクセスや変更によるリスクを低減するために、分離する。 |  | |
| A.12.2 悪意のあるソフトウェア(malware)からの保護 | | | | 改訂の影響：小 |
| 目的：情報及び情報処理施設がマルウェアから保護されることを確実にするため。 | | | | |
| A.12.2.1 旧：A.10.4.1 | マルウェアに対する管理策 | マルウェアから保護するために、利用者に自覚させることと併せて、検出、予防、回復のための管理を実施する。 | モバイル全PC にウィルス対策ソフトを導入し、もし感染した場合の処置について、集合訓練で周知した。12.2.1  ソフトウェアの受注に当たり、発注元との契約に従い、該当開発部員しか入室できない部屋を作り、その部屋のネットワークも自社のネットワークから切り離した環境を用意した。12.2.6 | |
| A.12.3 バックアップ | | | | 改訂の影響：小 |
| 目的：データの消失から保護するため。 | | | | |
| A.12.3.1 旧：A.10.5.1 | 情報のバックアップ | 情報、ソフトウェア及びシステムイメージのバックアップは、合意されたバックアップ方針に従って定期的に取得し、検査する。 | サーバのバックアップは毎日テープで取得し、サーバ室外の耐火金庫に保存している。  12.3.1 | |
| A.12.4 ログ取得及び監視 | | | | 改訂の影響：小 |
| 目的：イベントを記録し、証拠を作成するため。 | | | | |
| A.12.4.1 旧：A.10.10.1 | イベントログ取得 | 利用者の活動、例外処理、過失及び情報セキュリティ事象を記録したイベントログを取得し、保持し、定期的にレビューする。 | サーバへのアクセスはすべてログを採取し、10 年間保管することとした。12.4.1 | |
| A.12.4.2 旧：A.10.10.3 | ログ情報の保護 | ログ機能及びログ情報は、改ざん及び許可されていないアクセスから保護する。 |  | |
| A.12.4.3 旧：A.10.10.4 | 実務管理者及び運用担当者の作業ログ | システムの実務管理者及び運用担当者の作業は、記録し、そのログを保護し、定期的にレビューする。 |  | |
| A.12.4.4 旧：A.10.10.6 | クロックの同期 | 組織又はセキュリティ領域内の関連する全ての情報処理システムのクロックは、基となる単一の時刻に同期させる。 |  | |
| A.12.5 運用ソフトウェアの管理 | | | | 改訂の影響：小 |
| 目的：運用システムの完全性を確実にするため。 | | | | |
| A.12.5.1 旧：A.12.4.1 | 運用システムに関わるソフトウェアの導入 | 運用システムに関わるソフトウェアの導入を管理するための手順を実施する。 |  | |
| A.12.6 技術的な脆弱性の管理 | | | | 改訂の影響：中 |
| 目的：技術的な脆弱性の悪用を防止するため。 | | | | |
| A.12.6.1 旧：A.12.6.1 | 技術的な脆弱性の管理 | 利用中の情報システムの技術的な脆弱性に関する情報は、時機を失せずに獲得する。  また、そのような脆弱性に組織がさらされている状況を評価する。  さらに、それらと関連するリスクに対処するために、適切な手段をとる。 | 毎月マイクロソフトが発表するWindows に関する脆弱性情報を収集し、どのように対処すべきか検討するミーティングを毎月定期的に開いている。12.6.1 | |
| A.12.6.2 旧：N/A | ソフトウェアのインストールの制限 | 利用者によるソフトウェアのインストールを管理する規則を確立し、実施する。 | 社員がインストールできるソフトウェアのホワイトリストを作成し、それに従ってインストールを許可している。12.6.2 | |
| A.12.7 情報システムの監査に対する管理策 | | | | 改訂の影響：小 |
| 目的：運用システムに対する監査活動の影響を最小限にするため。 | | | | |
| A.12.7.1 旧：A.15.3.1 | 情報システムの監査に対する管理策 | 運用システムの検証に必要な監査は、その要求事項及び監査活動が業務プロセスの中断を最小限に抑えるように慎重に計画し、合意する。 |  | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **A.13　通信のセキュリティ** | | | | |
| A.13.1 ネットワークセキュリティ管理 | | | | 改訂の影響：小 |
| 目的：ネットワークにおける情報の保護、及びネットワークを支える情報処理施設の保護を確実にするため。 | | | | |
| A.13.1.1 旧：A.10.6.1 | ネットワーク管理策 | システム及びアプリケーション内の情報を保護するために、ネットワークを管理し、制御する。 |  | |
| A.13.1.2 旧：A.10.6.2 | ネットワークサービスのセキュリティ | 全てのネットワークサービスについて、組織が提供しているか、外部委託しているかに関わらず、セキュリティ機能、サービスレベル及び管理上の要求事項を決定し、ネットワークサービス・アグリメント(合意書)に盛り込む。 | 社内ネットワークを外部からの不正アクセスから守るため、ファイアウォール以外にどのような設備を導入すべきか専門業者からヒアリングをした。13.1.2 | |
| A.13.1.3 旧：A.11.4.5 | ネットワークの領  域分割 | 情報サービス、利用者、情報システムは、ネットワーク上でグループ毎に分割する。 |  | |
| A.13.2 情報の転送 | | | | 改訂の影響：小 |
| 目的：組織の内部で、或いは外部との間で転送された情報のセキュリティを維持するため。 | | | | |
| A.13.2.1 旧：A.10.8.1 | 情報転送の方針及び手順 | 通信設備のタイプに関わらず、転送した情報を保護するために、正式な転送方針、手順及び管理を備える。 |  | |
| A.13.2.2 旧：A.10.8.2 | 情報転送に関する合意 | (情報の転送に関する)合意では、組織と外部関係者間のビジネス情報の安全な転送について取り扱う。 | 重要情報をFAX 送信するときには、あらかじめ電話でその旨通知し、送信後には再び電話で到着確認している。13.2.2 | |
| A.13.2.3 旧：A.10.8.3 | 電子的メッセージ通信 | 電子的なメッセージを発信する場合、そこに含まれた情報は、適切に保護する。 |  | |
| A.13.2.4 旧：A.6.1.5 | 秘密保持契約又は守秘義務契約 | 情報保護のために組織のニーズを反映した秘密保持契約又は守秘義務契約の要件を特定し、定期的にレビューし、文書化する。 |  | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **A.14　システムの取得、開発及び保守** | | | | |
| A.14.1 情報システムのセキュリティ要求事項 | | | | 改訂の影響：小 |
| 目的：ライフサイクル全体にわたって、情報セキュリティが情報システムの欠くことのできない部分であることを確実にするため。これには、公衆ネットワークを介してサービスを提供する情報システムのための要求事項も含む。 | | | | |
| A.14.1.1 旧：A.12.1.1 | 情報セキュリティ要求事項の分析及び仕様化 | 新しい情報システムの仕様や既存の情報システムの改善要求事項には、情報セキュリティに関する要求事項を含める。 |  | |
| A.14.1.2 旧：A.10.9.1 | 公衆ネットワーク上のアプリケーションサービスのセキュリティ考慮 | 公衆ネットワークを経由するアプリケーションサービスに含まれる情報は、不正行為、契約紛争、や許可されていない開示・変更から保護する。 |  | |
| A.14.1.3 旧：A.10.9.2 | アプリケーションサービスのトランザクションの保護 | アプリケーションサービスのトランザクションに含まれる情報は、次の事項を未然に防止するために、保護する。  不完全な通信、誤った通信経路設定、許可されていないメッセージの変更、許可されていない開示、許可されていないメッセージの複製又は再生。 |  | |
| A.14.2 開発及びサポートプロセスにおけるセキュリティ | | | | 改訂の影響：中 |
| 目的：情報システムの開発サイクルの中で情報セキュリティを設計し、実施することを確実にするため。 | | | | |
| A.14.2.1 旧：N/A | セキュリティに配慮した開発のための方針 | ソフトウェアやシステムの開発規則は、組織内で確立し、開発に適用する。 |  | |
| A.14.2.2 旧：A.12.5.1 | システムの変更管理手順 | 開発のライフサイクルの中で発生するシステム変更は、正式な変更管理手順を用いて管理する。 |  | |
| A.14.2.3 旧：A.12.5.2 | オペレーティングプラットフォーム変更後のアプリケーションの技術的レビュー | オペレーティングプラットフォームを変更するときは、組織の運用又はセキュリティに悪影響がないことを確実にするために、重要なアプリケーションについてレビューし、試験する。 | サーバのOS を変更する際に、OS の下で動くアプリケーションソフトが正常に動作するか事前にテストした。14.2.3 | |
| A.14.2.4 旧：A.12.5.3 | パッケージソフトウェアの変更に対する制限 | パッケージソフトウェアの改良は、極力避け、必要な変更だけに留める。  又、全ての変更は、厳重に管理する。 |  | |
| A.14.2.5 旧：A. 12.2 | セキュリティに配慮したシステム構築の原則 | 安全なシステムを設計するための原則を定め、文書化し、維持し、全ての情報システムの実装に対して適用する。 |  | |
| A.14.2.6 旧：N/A | セキュリティに配慮した開発環境 | 組織は、全ての開発のライフサイクルをカバーするシステム開発とシステムインテグレーションの活動のために、安全な開発環境を構築して、適切に保護する。 |  | |
| A.14.2.7 旧：A.12.5.5 | 外部委託による開発 | 組織は、外部委託したシステム開発の活動を監督し、監視する。 |  | |
| A.14.2.8 旧：N/A | システムセキュリティの試験 | セキュリティ機能の試験は、開発期間中に実施する。 |  | |
| A.14.2.9 旧：A.10.3.2 | システムの受入れ試験 | 新しい情報システム、アップグレード及び新しいバージョンのために、受入れ試験のプログラム及び関連する受け入れ基準を確立する。 | 社内基幹システムのサーバを更改することとなり、あらかじめ定められていた導入・試験手順に従って作業を進めた。14.2.9 | |
| A.14.3 試験データ | | | | 改訂の影響：小 |
| 目的：試験に用いるデータの保護を確実にするため。 | | | | |
| A.14.3.1 旧：A.12.4.2 | 試験データの保護 | 試験データは、注意して選び、保護し、管理する。 | 外部ソフトハウスにソフト開発を委託する場合には、仕様書と試験データを提供するが、運用で使用している生データを試験データとして渡すことは厳禁している。14.3.1 | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **A.15　供給者関係** | | | | |
| A.15.1 供給者管理におけるセキュリティ | | | | 改訂の影響：中 |
| 目的：供給者がアクセスできる組織の資産の保護を確実にするため。 | | | | |
| A.15.1.1 旧：A.6.2.3 | 供給者関係のための情報セキュリティの方針 | 組織の資産に供給者がアクセスするリスクを軽減するために、情報セキュリティの要求事項について、供給者と合意し、文書化する。 |  | |
| A.15.1.2 旧：A.6.2.3 | 供給者との合意に含まれるセキュリティの取り組み | 関連する全ての情報セキュリティ要求事項を確立し、組織の情報にアクセスし、処理し、それを保存し、通信を行う、又は組織の情報のためにITインフラを提供するなどの可能性を有する供給者と合意する。 | 販売店から集めた、加入申込書の電子データ化を、外部の専門会社に委託するに当たり、守秘義務、情報の取り扱い、再委託の禁止、損害賠償事項を明記した契約書を取り交わした。15.1.2 | |
| A.15.1.3 旧：N/A | ICTサプライチェーン | 供給者との合意には、情報通信技術(lCT)サービス及び製品のサプライチェーンに関連する情報セキュリティリスクに対処するための要求事項を含めること。 |  | |
| A.15.2 供給者が提供するサービスの管理 | | | | 改訂の影響：小 |
| 目的：供給者との合意に沿って、情報セキュリティ及びサービス提供について合意したレベルを維持するため。 | | | | |
| A.15.2.1 旧：A.10.2.2 | 供給者のサービス提供の監視及びレビュー | 組織は、供給者のサービス提供を定常的に監視し、レビューし、監査する。 | 当社はインターネットサービス業者にWeb とメールサーバの運用を任せているので、運用状況を年一回報告させている。15.2.1 | |
| A.15.2.2 旧：A.10.2.3 | 供給者のサービス提供の変更に対する管理 | 現行の情報セキュリティの方針群、手順及び管理策の保守及び改善を含む供給者によるサービス提供の変更は、ビジネス情報、システム及び関連プロセスの重要性やリスクの再評価の結果を考慮して、管理する。 |  | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **A.16　情報セキュリティインシデントの管理** | | | | |
| A.16.1 情報セキュリティインシデントの管理及びその改善 | | | | 改訂の影響：小 |
| 目的：セキュリティ事象及びセキュリティ弱点に関する伝達を含む、情報セキュリティインシデントの管理のための、一貫性のある効果的な取組みを確実にするため。 | | | | |
| A.16.1.1 旧：A.13.2.1 | 責任及び手順 | 情報セキュリティインシデントに対し、迅速で、効果的で整然とした対  応を確実にするために、管理層の責任及び手順を確立する。 | あらかじめ、セキュリティ事件発生を想定して、管理者の対応手順を定め、予行演習を行なった。16.1.1 | |
| A.16.1.2 旧：A.13.1.1 | 情報セキュリティ事象の報告 | 情報セキュリティ事象は、適切な管理者への連絡経路を通して、できるだけ速やかに報告する。 | セキュリティに関するヒヤリハットを体験した時、どのような連絡経路で管理者に報告するか決め、社員研修で徹底した。16.1.2 | |
| A.16.1.3 旧：A.13.1.2 | 情報セキュリティ弱点の報告 | システム又はサービスの中で発見した又は疑いがある情報セキュリティ上の弱点は、どのようなものでも記録し、報告するよう、組織の情報システム、サービスを利用する従業員、契約相手に要求する。 |  | |
| A.16.1.4 旧：N/A | 情報セキュリティ事象の評価及び決定 | 情報セキュリティ事象は、これを評価し、情報セキュリティインシデントに分類するか否かを決定する。 |  | |
| A.16.1.5 旧：A.13.2.1 | 情報セキュリティインシデントへの対応 | 情報セキュリティインシデントは、文書化した手順に従って対応する。 |  | |
| A.16.1.6 旧：A.13.2.2 | 情報セキュリティインシデントからの学習 | 情報セキュリティインシデントの分析や解決から得られた知識は、インシデントが将来起こる可能性又は、その影響を低減するために用いる。 |  | |
| A.16.1.7 旧：A.13.2.3 | 証拠の収集 | 組織は、証拠となり得る情報の特定、収集、取得、保存のための手順を定め、適用する。 |  | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **A.17　事業継続マネジメントにおける情報セキュリティの側面** | | | | |
| A.17.1 情報セキュリティ継続 | | | | 改訂の影響：小 |
| 目的：情報セキュリティ継続を組織の事業継続マネジメントシステムに組み込むため。 | | | | |
| A.17.1.1 旧：A.14.1 | 情報セキュリティ継続の計画 | 組織は、困難な状況の下で(adverse situation) (例えば、危機又は災害)情報セキュリティ及び情報セキュリティマネジメントを継続するための要求事項を決定する。 | 東京での大震災に備え、大阪に予備のサーバを設置し、半日以内にシステムを切り替える計画を策定した。17.1.1 | |
| A.17.1.2 旧：A.14.1 | 情報セキュリティ継続の実施 | 組織は、困難な状況の下で情報セキュリティ継続に関する要求レベルを確実にするために、プロセス、手順及び管理策を定め、文書化し、実施し、維持する。 |  | |
| A.17.1.3 旧：A.14.1 | 情報セキュリティ継続の検証、レビュー及び評価 | 確立及び実施した情報セキュリティ継続のための管理が、困難な状況の下で妥当且つ有効であることを確実にするために、組織は、定められた間隔でこれらの管理を検証する。 | 地震発生時にもデータセンタの機能をできるだけ早期に回復させるため、毎年9 月に対策本部の設置、社員の呼集、バックアップデータからの復旧、顧客／業者への連絡等の訓練を実施し、問題点を見直している。17.1.3 | |
| A.17.2 冗長性 | | | | 改訂の影響：やや大 |
| 目的：情報処理施設の可用性を確実にするため。 | | | | |
| A.17.2.1 旧：N/A | 情報処理施設の可用性 | 情報処理施設は、可用性の要求事項を満たすのに十分な冗長性をもって、導入する。 | 顧客にサービスを提供しているサーバの障害に備え、ハードディスクは２重化し、更に遠隔地にバックアップサーバを設置した。これにより許容停止時間内にサービスを開始する計画を立てた。17.2.1 | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **A.18　順守** | | | | |
| A.18.1 情報セキュリティのレビュー | | | | 改訂の影響：小 |
| 目的：情報セキュリティに関連する法的、規制又は契約上の義務に対する違反、及びセキュリティ上のあらゆる要求事項に対する違反を避けるため。 | | | | |
| A.18.1.1 旧：A.15.1.1 | 適用法令及び契約上の要求事項の特定 | 各情報システム及び組織に関する法令、規制及び契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組みを明確に定め、文書化し、最新に保つ。 | 「不正競争防止法」を順守するために、当社としてどのようなことに注意すべきか話し合い、手順書に追加した。18.1.1 | |
| A.18.1.2 旧：A.15.1.2 | 知的財産権 | 知的財産権及び登録商標が存在するソフトウェア製品の利用する場合、法令、規制及び契約上の要求事項の順守を確実にするための適切な手順を実施する。 | 社員に貸与されたPC にインストールされたソフトをモニタすることのできるソフトを導入し、社員の違法インストール(ライセンス違反)を監視している。18.1.2 | |
| A.18.1.3 旧：A.15.1.3 | 記録の保護 | 記録は、法令、規制、契約及び事業上の要求事項に従って、消失、破壊、改ざん、許可されていないアクセス及び公開から保護する。 |  | |
| A.18.1.4 旧：A.15.1.4 | プライパシー及び個人を特定できる情報の保護 | プライパシー及び個人を特定できる情報の保護は、関連する法令及び規制が適用される場合には、その要求に従って確実にする。 | 経済産業省の「個人情報保護ガイドライン」の改訂にともない、当社の個人情報保護手順にどのように影響があるか精査した。18.1.4 | |
| A.18.1.5 旧：A.15.1.6 | 暗号化機能に対する規制 | 暗号化機能は、関連する全ての協定、法令及び規制を順守して用いる。 |  | |
| A.18.2 法的及び契約上の要求事項の識別 | | | | 改訂の影響：小 |
| 目的：組織の方針及び手順に従って情報セキュリティが実施され、運用されることを確実にするため。 | | | | |
| A.18.2.1 旧：A.6.1.8 | 情報セキュリティの独立したレビュー | 情報セキュリティ及びその実施の管理(例えば、情報セキュリティのための管理目的、管理策、方針、プロセス、手順)に関する組織の取組みは、あらかじめ定められた間隔で、又は重大な変化が生じた場合に、独立したレビューを実施する。 |  | |
| A.18.2.2 旧：A.15.2.1 | 情報セキュリティのための方針群及び標準の順守 | 管理者(マネジャー)は、自分の責任の範囲内における情報処理及び手順が、適切な情報セキュリティのための方針群、標準類、及び他の全てのセキュリティ要求事項を順守していることを定期的にレビューする。 | 当部門のグループリーダは、毎週のグループミーティングで、セキュリティ方針が順守されているか、グループ内情報が適切に保護されているか、問題はないかチェックしている。18.2.2 | |
| A.18.2.3 旧：A.15.2.2 | 技術的順守のレビュー | 情報システムは、組織の情報セキュリティのための方針群や基準の順守について、定期的にレビューする。 | システム管理者は、外部からの不正アクセスに備えて、定期的にファイアウォール、ルータ等のネットワーク機器の設定状況を点検している。18.2.3 | |

出典：ISO/IEC27001-2013(日本シーエスアール認証登録機構)\_編集版　文責：河東岩夫　平成26年3月31日

【ISO/IEC27001-2013】の今回の主な改訂点

(1)付属書 SL‐Appendix 3の適用を受けて規格同士の両立性を高めることが主な狙い。

(2)事業の目的に関連した内外の課題を解決することや、さまざまな期待、ニーズに応じるためにISMSを構築する上で反映すべきことを明確に記載。

(3)予防処置はリスクマネジメントそのものでネジメントシステムの計画(PDCA)の段階で扱われるのはあることから、予防処置の要求事項のを削除。