適用宣言書

第1.0版

制定：2023年3月23日

株式会社ツナググループ・ホールディングス

○:適用、×:適用除外

○:実施、未:未実施、ー:適用除外

表A.1ー管理目的及び管理策			適用	実施・未実施	管理策を含めた理由 または 管理策を除外した理由	規定・手順書
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経営陣の方向性 目的:情報セキュリティのための経営陣の方向性及び支持を，事業上の要求事項並びに関連する法令及び規制に従って提示するため。						
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は，これを定義し，管理層が承認し，発行し，従業員及び関連する外部関係者に通知しなければならない。	○	○	情報セキュリティのための経営層の方向性及び支持を、事業上の要求事項、関連する法令及び規則に従って規定するため	A-02 情報セキュリティ方針 B-01 ISMSマニュアル5.2 C-01 情報セキュリティ手順書5.1.1
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，あらかじめ定めた間隔で，又は重大な変化が発生した場合に，それが引き続き適切，妥当かつ有効であることを確実にするためにレビューしなければならない。	○	○	方針に、変化が生じた場合に適切性、妥当性、有効性を維持するため	B-01 ISMSマニュアル8.1 C-01 情報セキュリティ手順書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 目的:組織内で報セキュリティの実施及び運用に着手し，これを統制するための管理上の枠組みを確立するため。						
A.6.1.1	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，割り当てなければならない。	○	○	ISMSの構築・運用を円滑に行うため	B-01 ISMSマニュアル5.3 C-01 情報セキュリティ手順書6.1.1
A.6.1.2	職務の分離	相反する職務及び責任範囲は，組織の資産に対する，許可されていない若しくは意図しない変更又は不正使用の危険性を低減するために，分離しなければならない。	○	○	許可されていない若しくは意図しない変更又は不正使用の危険性を低減するために	各文書の作成／承認 C-01 情報セキュリティ手順書6.1.2
A.6.1.3	関係当局との連絡	関係当局との適切な連絡体制を維持しなければならない。	○	○	情報セキュリティインシデントを時機を失せずに報告するため	A-08 連絡先一覧表 C-01 情報セキュリティ手順書6.1.3
A.6.1.4	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会議，及び情報セキュリティの専門家による協会・団体との適切な連絡体制を維持しなければならない。	○	○	社内からの通知だけではなく、関係するセキュリティ情報を最新に保つため	A-08 連絡先一覧表 C-01 情報セキュリティ手順書6.1.4
A.6.1.5	プロジェクトマネジメントにおける情報セキュリティ	プロジェクト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は，情報セキュリティに取り組まなければならない。	○	○	情報セキュリティリスクがプロジェクトの中で特定及び対処されることを確実にするため	C-01 情報セキュリティ手順書6.1.5
A.6.2 モバイル機器及びテレワーキング 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	モバイル機器の方針	モバイル機器を用いることによって生じるリスクを管理するために，方針及びその方針を支援するセキュリティ対策を採用しなければならない。	○	○	モバイル機器を用いることによって生じるリスクを管理するために	C-01 情報セキュリティ手順書6.2.1
A.6.2.2	テレワーキング	テレワーキングの場所でアクセス，処理及び保存される情報を保護するために，方針及びその方針を支援するセキュリティ対策を実施しなければならない。	○	○	テレワーキングの場所でアクセス，処理及び保存される情報を保護するため	C-01 情報セキュリティ手順書6.2.2
A.7 人的資源のセキュリティ						
A.7.1 雇用前 目的:従業員及び契約相手がその責任を理解し，求められている役割にふさわしいことを確実にするため。						
A.7.1.1	選考	全ての従業員候補者についての経歴などの確認は，関連する法令，規制及び倫理に従って行わなければならない。また，この確認は，事業上の要求事項，アクセスされる情報の分類及び認識されたリスクに応じて行わなければならない。	○	○	従業員候補者について可能な範囲においてセキュリティ上の危険性がないということを確認するため	C-01 情報セキュリティ手順書7.1.1.
A.7.1.2	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及び組織の責任を記載しなければならない。	○	○	雇用する従業員、契約相手との間で情報セキュリティに関する責任の内容を互いの了解を得るため	C-01 情報セキュリティ手順書7.1.2
A.7.2 雇用期間中 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，かつ，その責任を遂行することを確実にするため。						
A.7.2.1	経営陣の責任	経営陣は，組織の確立された方針及び手順に従った情報セキュリティの適用を，全ての従業員及び契約相手に要求しなければならない。	○	○	ISMSの取り組みが、経営陣の経営戦略の一部であることを確実にするため	B-01 ISMSマニュアル5 C-01 情報セキュリティ手順書7.2.1
A.7.2.2	情報セキュリティの意識向上，教育及び訓練	組織の全ての従業員，及び関係する契約相手は，職務に関連する組織の方針及び手順についての，適切な，意識向上のための教育及び訓練を受けなければならず，また，定めに従ってそれを更新しなければならない。	○	○	方針群，セキュリティ要求事項，法的責任及び実務管理や手順の浸透を図るため	B-01 ISMSマニュアル5.1 B-01 ISMSマニュアル7.3 C-01 情報セキュリティ手順書7.2.2
A.7.2.3	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とるための，正式かつ周知された懲戒手続を備えなければならない。	○	○	情報セキュリティ違反を犯した従業員に対して処置をとるため	C-01 情報セキュリティ手順書7.2.3
A.7.3 雇用の終了及び変更 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	雇用の終了又は変更に関する責任	雇用の終了又は変更の後もなお有効な情報セキュリティに関する責任及び義務を定め，その従業員または契約相手に伝達し，かつ，遂行されなければならない。	○	○	従業員の職務変更、退職時における雇用者・従業員の責任を明確にするため	C-01 情報セキュリティ手順書7.3.1
A.8 資産の管理						
A.8.1 資産に対する責任 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	資産目録	情報及び情報処理施設に関連する資産を特定しなければならない。また，これらの資産の目録を，作成し，維持しなければならない。	○	○	全ての資産を明確に認識し、維持管理するため	D-02-01 資産目録 C-01 情報セキュリティ手順書8.1.1.
A.8.1.2	資産の管理責任	目録の中で維持される資産は，管理されなければならない。	○	○	情報資産に対する管理責任者を明確にするため	D-02-01 資産目録 C-01 情報セキュリティ手順書8.1.2
A.8.1.3	資産利用の許容範囲	情報の利用の許容範囲，並びに情報及び情報処理施設と関連する資産の利用の許容範囲に関する規則は，明確にし，文書化し，実施しなければならない。	○	○	資産利用の許容範囲を明確にするため	D-02-01 資産目録 C-01 情報セキュリティ手順書8.1.3
A.8.1.4	資産の返却	全ての従業員及び外部の利用者は，雇用，契約又は合意の終了時に，自らが所持する組織の資産の全てを返却しなければならない。	○	○	退職者が、不正に当社の資産を使用するのを防ぐため	C-01 情報セキュリティ手順書8.1.4
A.8.2 情報分類 目的:組織に対する情報の重要性に応じて，情報の適切なレベルでの保護を確実にするめ。						
A.8.2.1	情報の分類	情報は，法的要求事項，価値，重要性，及び許可されていない開示又は変更に対して取扱いに慎重を要する度合いの観点から，分類しなければならない。	○	○	価値、取扱い等、重要性を明確にするため	C-01 情報セキュリティ手順書8.2.1
A.8.2.2	情報のラベル付け	情報のラベル付けに関する適切な一連の手順は，組織が採用した情報分類体系に従って策定し，実施しなければならない。	○	○	従業員に分類に対応した識別方法とその取扱い方法を明確にするため	C-01 情報セキュリティ手順書8.2.2
A.8.2.3	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分類体系に従って策定し，実施しなければならない。	○	○	情報を認可されていない開示又は不正使用から保護するため	C-01 情報セキュリティ手順書8.2.3
A.8.3 媒体の取扱い 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	取外し可能な媒体の管理	組織が採用した分類体系に従って，取外し可能な媒体の管理のための手順を実施しなければならない。	○	○	媒体の持ち出し、紛失による情報の漏洩を防ぐため	C-01 情報セキュリティ手順書8.3.1
A.8.3.2	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，セキュリティを保って処分しなければならない。	○	○	不必要になった媒体からの情報の漏洩を防ぐため	C-01 情報セキュリティ手順書8.3.2
A.8.3.3	物理的媒体の輸送	情報を格納した媒体は，輸送の途中における，許可されていないアクセス，不正使用または破損から保護しなければならない。	○	○	配送される情報媒体を保護するため	C-01 情報セキュリティ手順書8.3.3

表A.1－管理目的及び管理策			適用	実施・未実施	管理策を含めた理由 または 管理策を除外した理由	規定・手順書
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 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	アクセス制御方針	アクセス制御方針は，業務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，レビューしなければならない。	○	○	アクセス制御に適合する業務上の要求事項を明確にするため	C-01 情報セキュリティ手順書9.1.1
A.9.1.2	ネットワーク及びネットワークサービスへのアクセス	利用することを特別に認可したネットワーク及びネットワークサービスへのアクセスだけを，利用者に提供しなければならない。	○	○	ネットワークサービスへの，認可されていないセキュリティを保護するため	C-01 情報セキュリティ手順書9.1.2
A.9.2 利用者アクセスの管理 目的：システム及びサービスへの，認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	利用者登録及び登録削除	アクセス権の割当てを可能にするために，利用者の登録及び登録削除についての正式なプロセスを実施しなければならない。	○	○	アクセス権の割当てを可能にするため	C-01 情報セキュリティ手順書9.2.1
A.9.2.2	利用者アクセスの提供（provisioning）	全ての種類の利用者について，全てのシステム及びサービスへのアクセス権を割り当てる又は無効化するために，利用者のアクセスの提供についての正式なプロセスを実施しなければならない。	○	○	全ての種類の利用者について，全てのシステム及びサービスへのアクセス権を割り当てる又は無効化するため	C-01 情報セキュリティ手順書9.2.2
A.9.2.3	特権的アクセス権の管理	特権的アクセス権の割当て及び利用は，制限し，管理しなければならない。	○	○	特権が割り当てられた利用者を制御するため	C-01 情報セキュリティ手順書9.2.3
A.9.2.4	利用者の秘密認証情報の管理	秘密認証情報の割当ては，正式な管理のプロセスによって管理しなければならない。	○	○	利用者の認可によって情報システム又はサービスへのアクセスを確実にするため	C-01 情報セキュリティ手順書9.2.4
A.9.2.5	利用者アクセス権のレビュー	資産の管理責任者は，利用者のアクセス権を定められた間隔でレビューしなければならない。	○	○	データ及び情報サービスへのアクセスに対する有効な管理を維持するため	C-02 情報セキュリティ手順9.2.5
A.9.2.6	アクセス権の削除又は修正	全ての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，契約又は合意の終了時に削除しなければならず，また，変更に合わせて修正しなければならない。	○	○	退職者や異動者が、不正に当社の情報へアクセスするのを防ぐため	C-01 情報セキュリティ手順書9.2.6
A.9.3 利用者の責任 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	秘密認証情報の利用	秘密認証情報の利用時に，組織の慣行に従うことを，利用者に要求しなければならない。	○	○	情報システム又はサービスへのアクセスを確実にするため	C-01 情報セキュリティ手順書9.3.1
A.9.4 システム及びアプリケーションのアクセス制御 目的：システム及びアプリケーションへの，認可されていないアクセスを防止するため。						
A.9.4.1	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機能へのアクセスは，アクセス制御方針に従って，制限しなければならない。	○	○	情報及びアプリケーションシステム機能のアクセス権を制御するため	C-01 情報セキュリティ手順書9.4.1
A.9.4.2	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しなければならない。	○	○	認可されていないアクセスの危険性を最小限に抑えるため	C-01 情報セキュリティ手順書9.4.2
A.9.4.3	パスワード管理システム	パスワード管理システムは，対話式でなければならず，また，良質なパスワードを確実とするものでなければならない。	○	○	責任追跡性を維持するため	C-01 情報セキュリティ手順書9.4.3
A.9.4.4	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のできるユーティリティプログラムの使用は，制限し，厳しく管理しなければならない。	○	○	システムユーティリティの使用の制限のため	C-01 情報セキュリティ手順書9.4.4
A.9.4.5	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，制限しなければならない。	○	○	プログラムソースコードの意図しない変更を回避するため	C-01 情報セキュリティ手順書9.4.5
A.10 暗号						
A.10.1 暗号による管理策 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，暗号の適切かつ有効な利用を確実にするため。						
A.10.1.1	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による管理策の利用に関する方針は，策定し，実施しなければならない。	○	○	情報の機密性，真正性及び／又は完全性を保護するため	C-01 情報セキュリティ手順書10.1.1
A.10.1.2	鍵管理	暗号鍵の利用，保護及び有効期限（lifetime）に関する方針を策定し，そのライフサイクル全体にわたって実施しなければならない。	○	○	暗号技術の利用を維持するため	C-01 情報セキュリティ手順書10.1.2
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 目的：組織の情報及び情報処理施設に対する認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	物理的セキュリティ境界	取扱いに慎重を要する又は重要な情報及び情報処理施設のある領域を保護するために，物理的セキュリティ境界を定め，かつ，用いなければならない。	○	○	取扱いに慎重を要する又は重要な情報及び情報処理施設のある領域を保護するため	A-04 レイアウト図 C-01 情報セキュリティ手順書11.1.1
A.11.1.2	物理的入退管理策	セキュリティを保つべき領域は，認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，適切な入退管理策によって保護しなければならない。	○	○	セキュリティを保つべき領域について，認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	C-01 情報セキュリティ手順書11.1.2
A.11.1.3	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セキュリティを設計し，適用しなければならない。	○	○	壁や窓などの破壊により、建物内部への不正な侵入を防ぐため	A-04 レイアウト図 C-01 情報セキュリティ手順書11.1.3
A.11.1.4	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，適用しなければならない。	○	○	自然災害又は人的災害からの損傷を回避するため	C-01 情報セキュリティ手順書11.1.4
A.11.1.5	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，適用しなければならない。	○	○	セキュリティを保つべき領域での監督されていない作業を回避するため	C-01 情報セキュリティ手順書11.1.5
A.11.1.6	受渡場所	荷物の受渡場所などの立寄り場所，及び認可されていない者が施設に立ち入ることもあるその他の場所は，管理しなければならない。また，可能な場合には，認可されていないアクセスを避けるために，それらの場所を情報処理施設から離さなければならない。	○	○	許可されていないアクセスから適切に保護するため	C-01 情報セキュリティ手順書11.1.6

表A.1－管理目的及び管理策			適用	実施・未実施	管理策を含めた理由 または 管理策を除外した理由	規定・手順書
A.11.2 装置 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	装置の設置及び保護	装置は，環境上の脅威及び災害からのリスク並びに認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，保護しなければならない。	○	○	物理的、環境的脅威から装置を保護するため	C-01 情報セキュリティ手順書11.2.1
A.11.2.2	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しなければならない。	○	○	物理的、環境的脅威から装置を保護するため	C-01 情報セキュリティ手順書11.2.2
A.11.2.3	ケーブル配線のセキュリティ	データを伝送する又は情報サービスをサポートする通信ケーブル及び電源ケーブルの配線は，傍受，妨害又は損傷から保護しなければならない。	○	○	物理的、環境的脅威から装置を保護するため	C-01 情報セキュリティ手順書11.2.3
A.11.2.4	装置の保守	装置は，可用性及び完全性を継続することを確実にするために，正しく保守しなければならない。	○	○	装置の可用性・完全性を維持するため	C-01 情報セキュリティ手順書11.2.4
A.11.2.5	資産の移動	装置，情報又はソフトウェアは，事前の認可なしでは，構外に持ち出してはならない。	○	○	持ち出すことのある、資産のセキュリティを確保するため	C-01 情報セキュリティ手順書11.2.5
A.11.2.6	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，構外での作業に伴った，構内での作業とは異なるリスクを考慮に入れて，セキュリティを適用しなければならない。	○	○	構外にある装置の保護、セキュリティを確保するため	C-01 情報セキュリティ手順書11.2.6
A.11.2.7	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ていること，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，検証しなければならない。	○	○	記憶媒体を内蔵した全ての装置について，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ていること，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	C-01 情報セキュリティ手順書11.2.7
A.11.2.8	無人状態にある利用者装置	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しなければならない。	○	○	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ため	C-01 情報セキュリティ手順書11.2.8
A.11.2.9	クリアデスク・クリアスクリーン方針	書類及び取外し可能な記憶媒体に対するクリアデスク方針，並びに情報処理設備に対するクリアスクリーン方針を適用しなければならない。	○	○	取扱いに慎重を要する又は重要な業務情報を保護するため	C-01 情報セキュリティ手順書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 目的：情報処理設備の正確か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	操作手順書	操作手順は，文書化し，必要とする全ての利用者に対して利用可能にしなければならない。	○	○	不注意又は故意によるシステムの不正使用のリスクを低減するため	C-01 情報セキュリティ手順書12.1.1
A.12.1.2	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は，管理しなければならない。	○	○	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の管理を確実にするため	C-01 情報セキュリティ手順書12.1.2
A.12.1.3	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・調整しなければならず，また，将来必要とする容量・能力を予測しなければならない。	○	○	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	C-01 情報セキュリティ手順書12.1.3
A.12.1.4	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，運用環境への認可されていないアクセスまたは変更によるリスクを低減するために，分離しなければならない。	○	○	運用環境への認可されていないアクセスまたは変更によるリスクを低減するため	C-01 情報セキュリティ手順書12.1.4
A.12.2 マルウェアからの保護 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	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，利用者に適切に認識させることと併せて，検出，予防及び回復のための管理策を実施しなければならない。	○	○	マルウェアから保護するため	C-01 情報セキュリティ手順書12.2.1
A.12.3 バックアップ 目的：データの消失から保護するため。						
A.12.3.1	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，検査しなければならない。	○	○	重要な情報及び、ソフトウェア及びシステムイメージの回復を確実にするため	C-01 情報セキュリティ手順書12.3.1
A.12.4 ログ取得及び監視 目的：イベントを記録し，証拠を作成するため。						
A.12.4.1	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，定期的にレビューしなければならない。	○	○	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，証拠を作成するため	C-01 情報セキュリティ手順書12.4.1
A.12.4.2	ログ情報の保護	ログ機能及びログ情報は，改ざん及び認可されていないアクセスから保護しなければならない。	○	○	ログ機能及びログ情報は，改ざん及び認可されていないアクセスから保護するため	C-01 情報セキュリティ手順書12.4.2
A.12.4.3	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，定期的にレビューしなければならない。	○	○	実務管理者が規則を順守して活動していることを監視するため	C-01 情報セキュリティ手順書12.4.3
A.12.4.4	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，単一の参照時刻源と同期させなければならない。	○	○	イベントログの正確さを確実にするため	C-01 情報セキュリティ手順書12.4.4
A.12.5 運用ソフトウェアの管理 目的：運用システムの完全性を確実にするため。						
A.12.5.1	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しなければならない。	○	○	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	C-01 情報セキュリティ手順書12.5.1
A.12.6 技術的ぜい弱性管理 目的：技術的ぜい弱性の悪用を防止するため。						
A.12.6.1	技術的ぜい弱性の管理	利用中の情報システムの技術的ぜい弱性に関する情報は，時機を失せずに獲得しなければならない。また，そのようなぜい弱性に組織がさらされている状況を評価しなければならない。さらに，それらと関連するリスクに対処するために，適切な手段をとらなければならない。	○	○	技術的ぜい弱性に対する効果的な管理プロセスを確立するため	C-01 情報セキュリティ手順書12.6.1
A.12.6.2	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，実施しなければならない。	○	○	利用者によるソフトウェアのインストールを管理しない事による技術的ぜい弱性の悪用を防止するため	C-01 情報セキュリティ手順書12.6.2

表A.1－管理目的及び管理策			適用	実施・未実施	管理策を含めた理由 または 管理策を除外した理由	規定・手順書
A.12.7 情報システムの監査に対する考慮事項 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	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を伴う監査要求事項及び監査活動は，業務プロセスの中断を最小限に抑えるために，慎重に計画し，合意しなければならない。	○	○	業務プロセスの中断のリスクを最小限に抑えるため	C-01 情報セキュリティ手順書12.7.1
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 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	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，制御しなければならない。	○	○	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	C-01 情報セキュリティ手順書13.1.1
A.13.1.2	ネットワークサービスのセキュリティ	組織が自ら提供するか外部委託しているかを問わず，全てのネットワークサービスについて，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特定しなければならず，また，ネットワークサービス合意書にもこれらを盛り込まなければならない。	○	○	ネットワークサービス提供者が合意したサービスを，セキュリティを保って管理するため	C-01 情報セキュリティ手順書13.1.2
A.13.1.3	ネットワークの分離	情報サービス，利用者及び情報システムは，ネットワーク上で，グループごとに分離しなければならない。	○	○	ネットワーク内に保管又は処理される情報を保護するため	C-01 情報セキュリティ手順書13.1.3
A.13.2 情報の転送 目的：組織の内部及び外部に転送した情報のセキュリティを維持するため。						
A.13.2.1	情報転送の方針及び手順	あらゆる形式の通信設備を利用した情報転送を保護するために，正式な転送方針，手順及び管理策を備えなければならない。	○	○	あらゆる形式の通信設備を利用した情報転送を保護するため	C-01 情報セキュリティ手順書13.2.1
A.13.2.2	情報転送に関する合意	合意では，組織と外部関係者との間の業務情報のセキュリティを保った転送について，取り扱わなければならない。	○	○	取引先や外部組織と自社のセキュリティーレベルの相違による情報交換のトラブルを防ぐため	C-01 情報セキュリティ手順書13.2.2
A.13.2.3	電子的メッセージ通信	電子的メッセージ通信に含まれた情報は，適切に保護しなければならない。	○	○	電子的メッセージ通信を保護するため	C-01 情報セキュリティ手順書13.2.3
A.13.2.4	秘密保持契約又は守秘義務契約	情報保護に対する組織の要求を反映する秘密保持契約又は守秘義務契約のための要求事項は，特定し，定めに従ってレビューし，文書化しなければならない。	○	○	情報漏えいの抑止を法的に強制できるようにするため	C-01 情報セキュリティ手順書13.2.4
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 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	情報セキュリティ要求事項の分析及び仕様化	情報セキュリティに関連する要求事項は，新しい情報システム又は既存の情報システムの改善に関する要求事項に含めなければならない。	○	○	セキュリティの不具合又はセキュリティが確保されていない場合に起こると思われる業務上の損傷の可能性を低減するため	C-01 情報セキュリティ手順書14.1.1
A.14.1.2	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の考慮	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，並びに認可されていない開示及び変更から保護しなければならない。	○	○	公衆ネットワークを介してアクセス可能なアプリケーションについて、ネットワークに関連したから情報を保護するため	C-01 情報セキュリティ手順書14.1.2
A.14.1.3	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，保護しなければならない，不完全な通信，誤った通信経路設定，認可されていないメッセージの変更，認可されていない開示，認可されていないメッセージの複製又は再生。	○	○	不完全な通信、誤った通信経路設定、認可されていないメッセージの変更、認可されていない開示、認可されていないメッセージの複製又は再生等を未然に防止するため	C-01 情報セキュリティ手順書14.1.3
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 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	セキュリティに配慮した開発のための方針	ソフトウェア及びシステムの開発のための規則は，組織内において確立し，開発に対して適用しなければならない。	○	○	セキュリティを考慮した開発のため	C-01 情報セキュリティ手順書14.2.1
A.14.2.2	システムの変更管理手順	開発のライフサイクルにおけるシステムの変更は，正式な変更管理手続きを用いて管理しなければならない。	○	○	システム、アプリケーション、製品の完全性を確実にするため	C-01 情報セキュリティ手順書14.2.2
A.14.2.3	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をレビューし，試験しなければならない。	○	○	オペレーティングプラットフォームを変更するときに，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	C-01 情報セキュリティ手順書14.2.3
A.14.2.4	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変更は，抑止しなければならず，必要な変更だけに限らなければならない。また，全ての変更は，厳重に管理しなければならない。	○	○	パッケージソフトウェアの変更は，抑止し，必要な変更だけに限るため	C-01 情報セキュリティ手順書14.2.4
A.14.2.5	セキュリティに配慮したシステムの構築の原則	セキュリティに配慮したシステムを構築するための原則を確立し，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しなければならない。	○	○	セキュリティに配慮したシステムを構築するため	C-01 情報セキュリティ手順書14.2.5
A.14.2.6	セキュリティに配慮した開発環境	組織は，全てのシステム開発ライフサイクルを含む，システムの開発及び統合の取組みのためのセキュリティに配慮した開発環境を確立し，的確に保護しなければならない。	○	○	セキュリティに配慮した開発環境の確立のため	C-01 情報セキュリティ手順書14.2.6
A.14.2.7	外部委託による開発	組織は，外部委託したシステム開発活動を監督し，監視しなければならない。	○	○	実施される作業の質及び正確さを管理するため	C-01 情報セキュリティ手順書14.2.7
A.14.2.8	システムセキュリティの試験	セキュリティ機能（functionality）の試験は，開発期間中に実施しなければならない。	○	○	システムが期待どおりに、かつ、期待した形だけ動作することを確実にするため	C-01 情報セキュリティ手順書14.2.8
A.14.2.9	システムの受入れ試験	新しい情報システム，及びその改訂版・更新版のために，受入れ試験のプログラム及び関連する基準を確立しなければならない。	○	○	セキュリティ要求事項に適切に対処していることを検証するため	C-01 情報セキュリティ手順書14.2.9
A.14.3 試験データ 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	試験データの保護	試験データは，注意深く選定し，保護し，管理しなければならない。	○	○	試験データの不正利用を管理するため	C-01 情報セキュリティ手順書14.3.1

表A.1－管理目的及び管理策			適用	実施・未実施	管理策を含めた理由 または 管理策を除外した理由	規定・手順書
A.15 供給者関係						
A.15.1 供給者関係における情報セキュリティ 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	供給者関係のための情報セキュリティの方針	組織の資産に対する供給者のアクセスに関連するリスクを軽減するための情報セキュリティ要求事項について，供給者と合意し，文書化しなければならない。	○	○	組織の資産に対する供給者のアクセスに関連するリスクを軽減するため	C-01 情報セキュリティ手順書15.1.1
A.15.1.2	供給者との合意におけるセキュリティの取扱い	関連する全ての情報セキュリティ要求事項を確立しなければならず，また，組織の情報に対して，アクセス，処理，保存若しくは通信を行う，又は組織の情報のためのIT基盤を提供する可能性のあるそれぞれの供給者と，この要求事項について合意しなければならない。	○	○	関連する情報セキュリティ要求事項を満たすという義務に関し、供給業者との間に誤解が生じないことを確実にするため	C-01 情報セキュリティ手順書15.1.2
A.15.1.3	ICTサプライチェーン	供給者との合意には，情報通信技術（ICT）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なければならない。	○	○	情報通信技術（ICT）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	C-01 情報セキュリティ手順書15.1.3
A.15.2 供給者のサービス提供の管理 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	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，監査しなければならない。	○	○	供給者が提供するサービスの合意における情報セキュリティの条件の順守を確実にするため	C-01 情報セキュリティ手順書15.2.1
A.15.2.2	供給者のサービス提供の変更に対する管理	関連する業務情報，業務システム及び業務プロセスの重要性，並びにリスクの再評価を考慮して，供給者によるサービス提供の変更（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。）を管理しなければならない。	○	○	供給者が提供するサービスの変更における情報セキュリティの条件を管理するため	C-01 情報セキュリティ手順書15.2.2
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 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	責任及び手順	情報セキュリティインシデントに対する迅速，効果的かつ順序だっ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しなければならない。	○	○	情報セキュリティインシデントに対する迅速，効果的で整然とした対応を確実にするため	C-01 情報セキュリティ手順書16.1.1
A.16.1.2	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しなければならない。	○	○	情報セキュリティ事象の報告手順及びその連絡先を明確にするため	C-01 情報セキュリティ手順書16.1.2
A.16.1.3	情報セキュリティ弱点の報告	組織の情報セキュリティ及びサービスを利用する従業員及び契約相手に，システム又はサービスの中で発見した又は疑いをもった情報セキュリティ弱点は，どのようなものでも記録し，報告するように要求しなければならない。	○	○	情報セキュリティインシデントを防止するため	C-01 情報セキュリティ手順書16.1.3
A.16.1.4	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しなければならない。	○	○	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ため	C-01 情報セキュリティ手順書16.1.4
A.16.1.5	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しなければならない。	○	○	情報セキュリティインシデントに対して、予め準備した手順通りの対応を確実にするため	C-01 情報セキュリティ手順書16.1.5
A.16.1.6	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及び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なければならない。	○	○	再発する又は影響の大きいインシデントを特定するため	C-01 情報セキュリティ手順書16.1.6
A.16.1.7	証拠の収集	組織は，証拠となり得る情報の特定，収集，取得及び保存のための手順を定め，適用しなければならない。	○	○	必要な証拠の特定、収集、取得及び保存のため。また、インシデントの重大さに気が付く前に、必要な証拠を破壊してしまわないため	C-01 情報セキュリティ手順書16.1.7
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 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取り込まなければならない。						
A.17.1.1	情報セキュリティ継続の計画	組織は，困難な状況（adverse situation)(例えば，危機又は災害）における，情報セキュリティ及び情報セキュリティマネジメントの継続のための要求事項を決定しなければならない。	○	○	困難な状況（adverse situation)(例えば，危機又は災害）における，情報セキュリティ及び情報セキュリティマネジメントの継続のため	C-01 情報セキュリティ手順書17.1.,1
A.17.1.2	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対する要求レベルを確実にするための，プロセス，手順及び管理策を確立し，文書化し，実施し，維持しなければならない。	○	○	困難な状況の下で情報セキュリティ継続に対する要求レベルを確実にするため	C-01 情報セキュリティ手順書17.1.,2
A.17.1.3	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策が，困難な状況の下で妥当か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をの管理策を検証しなければならない。	○	○	確立及び実施した情報セキュリティ継続のための管理策が，困難な状況の下で妥当かつ有効であることを確実にするため	C-01 情報セキュリティ手順書17.1.,3
A.17.2 冗長性 目的：情報処理施設の可用性を確実にするため。						
A.17.2.1	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，導入しなければならない。	○	○	情報処理施設について、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るため	C-01 情報セキュリティ手順書17.2.1
A.18 順守						
A.18.1 法的及び契約上の要求事項の順守 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	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ついて，全ての関連する法令，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，明確に特定し，文書化し，また，最新に保たなければならない。	○	○	関連する法令，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するため	C-01 情報セキュリティ手順書18.1.1
A.18.1.2	知的財産権	知的財産権及び権利関係のあるソフトウェア製品の利用に関連する，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しなければならない。	○	○	著作権を侵害しないことを確実にするため	C-01 情報セキュリティ手順書18.1.2
A.18.1.3	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，消去，破壊，改ざん，認可されていないアクセス及び不正な流出から保護しなければならない。	○	○	記録及び情報を消失，破壊及び改ざんから保護するため	C-01 情報セキュリティ手順書18.1.3
A.18.1.4	プライバシー及び個人を特定できる情報（PII）の保護	プライバシー及びPII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しなければならない。	○	○	プライバシー及びPIIの保護の関係する法令、規制、契約事項の要求に従うため	C-01 情報セキュリティ手順書18.1.4

表A.1－管理目的及び管理策			適用	実施・未実施	管理策を含めた理由 または 管理策を除外した理由	規定・手順書
A.18.1.5	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なければならない。	○	○	暗号化した装置を輸出する，または海外に持ち出す運用は現状行っているため。	C-01 情報セキュリティ手順書18.1.5
A.18.2 情報セキュリティのレビュー 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	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）に対する組織の取組みについて，あらかじめ定めた間隔で，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しなければならない。	○	○	取組が引き続き適切、妥当及び有効であることを確実にするため	B-01 ISMSマニュアル5 C-01 情報セキュリティ手順書18.2.1
A.18.2.2	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しなければならない。	○	○	すべてのセキュリティ手順が正しく実行されることを確実にするため	C-01 情報セキュリティ手順書18.2.2
A.18.2.3	技術的順守のレビュー	情報システムを，組織の情報セキュリティのための方針群及び標準の順序に関して，定めに従ってレビューしなければならない。	○	○	ソフトウェア、ハードウェアの設定が決められた通りに実施されているかを確認するため	C-01 情報セキュリティ手順書18.2.3