適用宣言書

株式会社SDホールディングス

改訂暦表

発行者	監査役　加藤　和昭
承認者	代表取締役社長　大熊基由

版番号	発行年月日	改訂内容
1	2023/3/1	制定
2	2023/8/30	改定
3	2024/8/30	内容確認

A.5	情報セキュリティのための方針群					関連文書
A.5.1	情報セキュリティのための経営陣の方向性					
	管理策	チェック項目	採否:○×	実施:○×	理由	
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、従業員及び外部関係者に通知すること。	○	○	**事業上の要求事項のため。**	ISMSマニュアル 5 情報セキュリティ方針
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、内部監査及びマネジメントレビュー、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すること。	○	○	事業上の要求事項のため。	ISMSマニュアル 5

A.6	情報セキュリティのための組織					関連文書
A.6.1	内部組織 目的:組織内で情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					
	管理策	チェック項目	採否:○×	実施:○×	理由	
A.6.1.1	情報セキュリティの役割及び責任	全ての情報セキュティの責任を定め割り当てること	○	○	事業上の要求事項のため。	**ISMSマニュアル 役割分担表**
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、認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すること	○	○	リスクアセスメント及びリスク対応のプロセスの結果及び結論のため。	**ISMSマニュアル 役割分担表**
A6.1.3	関係当局との連絡	関係当局との適切な連絡体制を維持すること	○	○	事業上の要求事項のため。	**情報セキュリティ管理規程**
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すること。	○	○	事業上の要求事項のため。	**情報セキュリティ管理規程**
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むこと	○	○	リスクアセスメント及びリスク対応のプロセスの結果及び結論のため。	**情報セキュリティ管理規程**

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					関連文書
	管理策	チェック項目	採否:○×	実施:○×	理由	
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すること。	○	○	モバイルコンピューティング及び通信はしていない。	-
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すること。	○	○		-

A.7	人的資源のセキュリティ					関連文書
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					
	管理策	チェック項目	採否:○×	実施:○×	理由	
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、この確認は事業上との要求事項、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うこと	○	○	**人による情報漏えいや不正行為を防ぐため**	**情報セキュリティ管理規程**
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すること。	○	○	人による情報漏えいや不正行為を防ぐため	**情報セキュリティ管理規程**

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。					関連文書
	管理策	チェック項目	採否:○×	実施:○×	理由	
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すること	○	○	従業員、契約相手及び第三者の利用者にセキュリティの適用をするため	情報セキュリティ管理規程
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，及び関係する場合には契約相手は，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，定めに従ってその更新を受けていること	○	○	人による情報漏えいや不正行為を防ぐため	情報セキュリティ管理規程
A.7.2.3	懲戒手続き	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ること	○	○	人による情報漏えいや不正行為を防ぐため	就業規則 情報セキュリティ管理規程

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。					関連文書
	管理策	チェック項目	採否：○×	実施：○×	理由	
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，その従業員又は契約相手に伝達し，かつ，遂行させること	○	○	雇用終了者による情報漏えいや不正行為を防ぐため	**情報セキュリティ管理規程**

A.8	資源の管理					関連文書
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					
	管理策	チェック項目	採否：○×	実施：○×	理由	
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すること。また，これらの資産の目録を，作成し，維持すること	○	○	情報資産を把握しリスクに応じて適切に管理するため	**情報セキュリティ管理規程**
A.8.1.2	資産の管理責任	目録の中で維持される資産は，管理すること。 ※注a) 6.1.2 及び6.1.3 では，情報セキュリティのリスクを運用管理することについて，責任及び権限をもつ人又は主体をリスク所有者としている。情報セキュリティにおいて，多くの場合，資産の管理責任を負う者は，リスク所有者でもある。	○	○	情報資産を把握しリスクに応じて適切に管理するため	情報セキュリティ管理規程
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，実施すること	○	○	情報資産を把握しリスクに応じて適切に管理するため	情報セキュリティ管理規程
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すること。	○	○	情報資産を把握しリスクに応じて適切に管理するため	情報セキュリティ管理規程

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ため。					関連文書
	管理策	チェック項目	採否：○×	実施：○×	理由	
A.8.2.1	情報の分類	情報は，法的要求事項，価値，重要性，及び認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，分類すること	○	○	情報資産を情報漏えいから防ぐと共に完全性及び可用性に配慮するため	**情報セキュリティ管理規程**
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，実施すること	○	○	情報資産を把握しリスクに応じて適切に管理するため	情報セキュリティ管理規程
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，実施すること。	○	○	情報資産を把握しリスクに応じて適切に管理するため	**情報セキュリティ管理規程**

A.8.3	媒体の取扱い 目的：媒体に保存された情報の認可されていない開示，変更，除去又は破壊を防止するため。					関連文書
	管理策	チェック項目	採否：○×	実施：○×	理由	
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すること	○	○	機密情報及び顧客情報の漏洩を防ぐため	情報セキュリティ管理規程
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すること	○	○	機密情報及び顧客情報の漏洩を防ぐため	情報セキュリティ管理規程
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，認可されていないアクセス，不正使用又は破損から保護すること	○	○	情報の適切な取り扱い及び処分を行うため	情報セキュリティ管理規程

A.9	アクセス制御					関連文書
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。					
	管理策	チェック項目	採否：○×	実施：○×	理由	
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，レビューすること。	○	○	適切にアクセス権限を設定し情報漏えいを防ぐため	情報セキュリティ管理規程
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，利用者に提供すること。	○	○	適切にアクセス権限を設定し情報漏えいを防ぐため	情報セキュリティ管理規程

A.9.2	利用アクセスの管理 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。					関連文書
	管理策	チェック項目	採否:○×	実施:○×	理由	
A.9.2.1	利用者登録及び登録解除	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すること	○	○	利用者を識別するため。及び利用権限がないものが使用することを防ぐため。	情報セキュリティ管理規程
A.9.2.2	利用者アクセスの提供	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，利用者アクセスの提供についての正式なプロセスを実施すること	○	○	適切にアクセス権限を設定し情報漏えいを防ぐため	情報セキュリティ管理規程
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，管理すること	○	○	**特権の割り当てを適切に管理するため**	情報セキュリティ管理規程
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，正式な管理プロセスによって管理すること	○	○	利用者を識別するため。及び利用権限がないものが使用することを防ぐため。	情報セキュリティ管理規程
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すること	○	○	アクセス権が適切に割り当てられている状態を確保するため	情報セキュリティ管理規程
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すること	○	○	割当及び削除を適切に管理するため	情報セキュリティ管理規程

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					関連文書
	管理策	チェック項目	採否:○×	実施:○×	理由	
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，利用者に要求すること	○	○	適切に利用し情報漏えいを防ぐため	情報セキュリティ管理規程

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					関連文書
	管理策	チェック項目	採否:○×	実施:○×	理由	
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，制限すること	○	○	不正アクセスを防ぐため	情報セキュリティ管理規程
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すること	○	○	個別の端末を識別するため	情報セキュリティ管理規程
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こと	○	○	正しいパスワードの利用のため	情報セキュリティ管理規程
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，厳しく管理すること	○	○	システムを適切に管理するため	情報セキュリティ管理規程
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，制限すること	○	×	プログラムソースコード（原本）の取扱いを行っていない。	-

A.10 A.10.1	暗号 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。					関連文書
	管理策	チェック項目	採否:○×	実施:○×	理由	
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，実施すること	○	○	お客様の仕様で入ることがあるため	**情報セキュリティ管理規程**
A.10.1.2	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体にわたって実施すること	○	○	ＳＳＨ等の暗号手段によって、情報の機密性、真正性または完全性を保護するため。	情報セキュリティ管理規程

A.11	物理的及び環境的セキュリティ					関連文書
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。					
	管理策	チェック項目	採否：○×	実施：○×	理由	
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，用いること	○	○	セキュリティリスクに見合ったリスク対応をとるため	情報セキュリティ管理規程
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すること	○	○	許可されていないものによる不正アクセスを防ぐため	情報セキュリティ管理規程
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，適用すること	○	○	セキュリティリスクに見合ったリスク対応をとるため	情報セキュリティ管理規程
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，適用すること	○	○	環境の脅威からの保護を防ぐため。	情報セキュリティ管理規程
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，適用すること	○	○	セキュリティリスクに見合ったリスク対応をとるため	情報セキュリティ管理規程
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すこと	○	○	許可されていないものによる不正アクセスを防ぐため	**情報セキュリティ管理規程**

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。					関連文書
	管理策	チェック項目	採否：○×	実施：○×	理由	
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，保護すること	○	○	許可されていないものによる不正アクセスを防ぐため	情報セキュリティ管理規程
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すること	○	○	可用性を確保するため	情報セキュリティ管理規程
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すること	○	○	通信ケーブル及び電源ケーブルを損傷から保護するためめ	情報セキュリティ管理規程
A.11.2.4	装置の保守	装置は，可用性及び完全性を継続的に維持することを確実にするために，正しく保守すること	○	○	完全、可用性を確保するため	情報セキュリティ管理規程
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，構外に持ち出しさせないこと	○	○	資産の移動による不正を防ぐため	情報セキュリティ管理規程
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すること	○	○	構外にある装置（携帯電話、車両）のセキュリティを保護するため	—
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，検証すること。	○	○	情報漏えいを防ぐため	情報セキュリティ管理規程
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すること	○	○	無人運転装置の適切な保護を行うため	情報セキュリティ管理規程
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すること	○	○	情報漏えいを防ぐため	**情報セキュリティ管理規程**

A.12	運用のセキュリティ					関連文書
A.12.1	運用の手順及び責任 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。					
	管理策	チェック項目	採否:○×	実施:○×	理由	
A.12.1.1	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こと。	○	○	システムの変更に伴う可用性を損なわないため	情報セキュリティ管理規程
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を、管理すること。	○	○	システムの変更に伴う可用性を損なわないため	情報セキュリティ管理規程
A12.1.3	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、また、将来必要となる容量・能力を予測すること。	○	○	資産に対する、認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部門責任者は業務を分割し、実施するため採用	情報セキュリティ管理規程
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、分離すること。	○	○	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	情報セキュリティ管理規程

A.12.2	悪意のあるソフトウェア(malware)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。					関連文書
	管理策	チェック項目	採否:○×	実施:○×	理由	
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こと	○	○	ウィルスによる被害を防ぐため	情報セキュリティ管理規程

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。					関連文書
	管理策	チェック項目	採否:○×	実施:○×	理由	
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、検査すること。	○	○	運用障害を防ぐため	情報セキュリティ管理規程 バックアップ実施管理表

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。					関連文書
	管理策	チェック項目	採否:○×	実施:○×	理由	
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、定期的にレビューすること。	○	○	セキュリティ事象時に対応するため	情報セキュリティ管理規程
A.12.4.2	ログ情報の保護	ログ機能及びログ情報は、改ざん及び許可されていないアクセスから保護すること。	○	○	監査証跡の完全性を確保するため	情報セキュリティ管理規程
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、定期的にレビューすること。	○	○	セキュリティ事象時に対応するため	情報セキュリティ管理規程
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、基となる単一の時刻に同期させること。	○	○	セキュリティ事象の時間を正確に把握するため	情報セキュリティ管理規程

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。					関連文書
	管理策	チェック項目	採否:○×	実施:○×	理由	
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すること。	○	○	セキュリティを保つため	情報セキュリティ管理規程

A.12.6	技術的な脆弱性の管理 技術的な脆弱性の悪用を防止するため。					関連文書
	管理策	チェック項目	採否:○×	実施:○×	理由	
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こと。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、適切な手段をとること。	○	○	技術的脆弱性を適切に管理するため	**情報セキュリティ管理規程**
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、実施すること。	○	○	セキュリティを保つため	情報セキュリティ管理規程

A.12.7	情報システムの監査に対する管理策 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。					関連文書
	管理策	チェック項目	採否：○×	実施：○×	理由	
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、合意すること。	○	○	運用システムの監査システムのセキュリティに対するリスクを最小限に抑えるため事前に被監査箇所と監査計画（日程・主監査箇所・方法など）を作成し実施するため	ISMSマニュアル

A.13	通信のセキュリティ					関連文書
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。					
	管理策	チェック項目	採否：○×	実施：○×	理由	
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、制御すること。	○	○	ネットワークに対する不正アクセスを監視するため	情報セキュリティ管理規程
A.13.1.2	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）に盛り込むこと。	○	○	ネットワークサービスのセキュリティを保つため	情報セキュリティ管理規程
A.13.1.3	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こと。	○	○	相互のネットワークを保護するため	情報セキュリティ管理規程

A.13.2	情報の転送 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。					関連文書
	管理策	チェック項目	採否：○×	実施：○×	理由	
A.13.2.1	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こと。	○	○	情報の交換を適切に行うため	情報セキュリティ管理規程
A.13.2.2	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こと。	○	○	文書の交換を適切に行うため	情報セキュリティ管理規程
A.13.2.3	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、適切に保護すること。	○	○	配送中の漏洩を防ぐため	情報セキュリティ管理規程
A.13.2.4	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、文書化すること。	○	○	事業上の要求事項のため。	情報セキュリティ管理規程

A.14	システムの取得、開発及び保守					関連文書
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。					
	管理策	チェック項目	採否：○×	実施：○×	理由	
A.14.1.1	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こと。	○	○	新しい情報システムの購入又は既存のシステムの改善については事前に申請・調査・評価を実施する。受入れ基準を明確にするため	情報セキュリティ管理規程
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・変更から保護すること。	○	○		—
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、保護すること。 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。	○	○	オンライン取引による業務をおこなわないため	—

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。					関連文書
	管理策	チェック項目	採否：○×	実施：○×	理由	
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、開発に適用すること。	○	×	開発時のセキュリティを保つため	情報セキュリティ管理規程
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こと。	○	○	システム変更時のセキュリティを保つため	情報セキュリティ管理規程
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についてレビューし、試験すること。	○	○	ＯＳ不良によるセキュリティリスクを軽減するため	情報セキュリティ管理規程
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改良は、極力避け、必要な変更だけに留めること。又、全ての変更は、厳重に管理すること。	○	○	必要な保守（セキュリティパッチ）の変更だけで対応し、パッケージソフトウェアの変更は禁止とするため	情報セキュリティ管理規程
A.14.2.5	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こと。	○	○	入力データの妥当性を確保するため	情報セキュリティ管理規程
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、適切に保護すること。	○	○	完全性、可用性を確保するため	情報セキュリティ管理規程
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の活動を監督し、監視すること。	○	○		-
A.14.2.8	システムセキュリティの試験	セキュリティ機能の試験は、開発期間中に実施すること。	○	○		-
A.14.2.9	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こと。	○	○	完全性、可用性を確保するため	情報セキュリティ管理規程

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。					関連文書
	管理策	チェック項目	採否：○×	実施：○×	理由	
A.14.3.1	試験データの保護	試験データは、注意して選び、保護し、管理すること。	○	○		-

A.15	供給者関係					関連文書
A.15.1	供給者管理におけるセキュリティ 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。					
	管理策	チェック項目	採否：○×	実施：○×	理由	
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、文書化すること。	○	○	事業上の要求事項のため。	情報セキュリティ管理規程
A.15.1.2	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こと。	○	○	事業上の要求事項のため。	情報セキュリティ管理規程
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ること。	○	○	供給者による情報漏洩を防ぐため	情報セキュリティ管理規程

A.15.2	供給者が提供するサービスの管理 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。					関連文書
	管理策	チェック項目	採否：○×		理由	
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、監査すること。	○	○	第三者が提供するサービスによる情報の漏洩を防ぐため	情報セキュリティ管理規程
A.15.2.2	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、管理すること。	○	○	第三者が提供するサービスによる情報の漏洩を防ぐため	情報セキュリティ管理規程

A.16 情報セキュリティインシデントの管理						関連文書
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。						
	管理策	チェック項目	採否:○×	実施:○×	理由	
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こと。	○	○	情報セキュリティインシデントに迅速に対応するため	情報セキュリティ管理規程
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すること。	○	○	事業活動の中断を防ぐため	情報セキュリティ管理規程
A.16.1.3	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こと。	○	○	事業活動の中断を防ぐため	情報セキュリティ管理規程
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すること。	○	○	情報セキュリティインシデントに迅速に対応するため	情報セキュリティ管理規程
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すること。	○	○	情報セキュリティインシデントに迅速に対応するため	情報セキュリティ管理規程
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こと。	○	○	セキュリティインシデントの未然防止のため	情報セキュリティ管理規程
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、保存のための手順を定め、適用すること。	○	○	セキュリティインシデントの再発防止のため	情報セキュリティ管理規程

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						関連文書
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組み込むため。						
	管理策	チェック項目	採否:○×	実施:○×	理由	
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こと。	○	○	事業活動の中断を防ぐため	情報セキュリティ管理規程
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、維持すること。	○	○	中長期的なリスクを未然に防ぐため	情報セキュリティ管理規程
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こと。	○	○	障害などの対応を迅速に行うため	情報セキュリティ管理規程

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。						関連文書
	管理策	チェック項目	採否:○×	実施:○×	理由	
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、導入すること。	○	○	情報処理に十分な余剰をもたせるため	情報セキュリティ管理規程

A.18	順守					関連文書
A.18.1	情報セキュリティのレビュー 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。					
	管理策	チェック項目	採否：○×	実施：○×	理由	
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、最新に保つこと。	○	○	法令・規制要求事項を遵守するため	法令及びその他一覧
A.18.1.2	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こと。	○	○	法令・規制要求事項を遵守するため	情報セキュリティ管理規程
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こと。	○	○	事故時に記録に基づき事象を適切に追跡するため	ISMSマニュアル 4.3.3
A.18.1.4	プライバシー及び個人を特定できる情報の保護	プライバ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こと。	○	○	個人情報保護の漏洩を防ぐため	情報セキュリティ管理規程
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ること。	○	○		―

A.18.2	法的及び契約上の要求事項の識別 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。					関連文書
	管理策	チェック項目	採否：○×	実施：○×	理由	
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。	○	○	リスクアセスメント及びリスク対応のプロセスの結果及び結論のため。	情報セキュリティ管理規程
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（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。	○	○	各部門責任者は基本方針及び規定類への順守を達成するために適用範囲における全てのセキュリティ手順が正しく実行されることを管理、見直しをするため採用。もし正しく実施されていない場合は原因を特定し、教育・指導を実施する。	ISMSマニュアル 6
A.18.2.3	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。	○	○	リスクアセスメント及びリスク対応のプロセスの結果及び結論のため。	情報セキュリティ管理規程