ISO27001管理策 ISO27001附属書A「管理目的及び管理策」より			当社の取り組み状況
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 管理目的・選択理由：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。	「情報セキュリティ方針」を定め、ホームページに公開している。
A.5.1.2	情報セキュリティのための本方針群のレビュー	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。	「情報セキュリティ基本方針」およびこれに基づく活動について、年に1度のマネジメントレビューにより、妥当性、有効性を評価している。
A.6　組織セキュリティのための組織			
A.6.1　内部組織 管理目的・選択理由：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。			
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。	情報セキュリティ委員会を中心とする情報セキュリティ活動の組織、体制、責任について、「ISMSマニュアル」に定めている。
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，分離しなければならない。	「業務分掌規程」や「職務権限規程」にもとづき、情報資産への責任範囲やアクセス権限を分離している。
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。	「ISMSマニュアル」に明記している。
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。	同上
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。	プロジェクト遂行のための各業務手順書を作成し、情報セキュリティの要求事項を満たすようにしている。
A.6.2　モバイル機器及びテレワーキング 管理目的・選択理由：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。	「職場環境における業務手順書」にモバイル端末の利用上の注意を定めている。
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。	同上
A.7　人的資源のセキュリティ			
A.7.1　雇用前 管理目的・選択理由：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。	関連する法令、規制及び倫理に従って行っている。また、この確認は、事業上の要求事項、社内規程等のルールに従い行っている。
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。	従業員、契約相手と契約する際は、必ず「情報セキュリティ基本方針」を周知し、「機密保持誓約書」または機密保持条件を明文化した契約書を締結している。
A.7.2　雇用期間中 管理目的・選択理由：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。	経営陣は「情報セキュリティ方針」を公開し、全ての従業員、役員、利害関係者に情報セキュリティについて要求をしている。 「ISMSマニュアル」に経営陣の役割について明記している。
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なければならない。	従業員及び当社事業所内に常駐する人員の、受入れ時には「情報セキュリティ基本方針」、ISMSの仕組み、職場環境のルール等を教育している。また、定期的に全社勉強会を実施している。

ISO27001管理策 ISO27001附属書A「管理目的及び管理策」より			当社の取り組み状況
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。	「情報セキュリティ基本方針」並びに各種手順書に対し違反した場合の懲戒について、「就業規則」に定めている。
A.7.3　雇用の終了又は変更 管理目的・選択理由：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，その従業員又は契約相手に伝達し，かつ，遂行させなければならない。	雇用終了または契約終了時には、貸与資産の返却、機密保持誓約書への署名をしてもらい、雇用終了後または契約終了後もなお有効な責任及び義務が存在することを伝えている。
A.8　資産の管理			
A.8.1　資産に対する責任 管理目的・選択理由：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。	「情報資産シート」に情報資産を特定し、定期的に更新している。
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。	「情報資産シート」に管理責任者を明記している。
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。	「職場環境における業務手順書」等、各手順書に明記している。
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。	雇用、契約終了時には、貸与物品等の返却、退職後の守秘に関する誓約書を提出している。
A.8.2　情報の分類 管理目的・選択理由：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。			
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，分類しなければならない。	「情報資産シート」に、法的要求事項，価値，重要性等の観点から情報資産価値を評価し、分類している。
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。	「ISMS文書管理手順書」に基づき、情報資産の分類をしている。
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。	分類された資産価値に応じて、適切な管理策を講じている。
A.8.3　媒体の取扱い 管理目的・選択理由：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。			
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。	記憶媒体の保管、利用方法、廃棄等について手順を定めている。
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。	記憶媒体の廃棄について、手順を定めている。外部業者に委託する場合は秘密保持及び処分依頼品の再利用の禁止を契約文書に含めている。
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しなければならない。	記憶媒体の移動について、手順を定めている。
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 管理目的・選択理由：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。	アクセス制御方針を定め、各業務ごとに利用者を区分し、適切なアクセス権限を設定している。
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。	許可されたネットワーク以外へは通信できないよう設定している。
A.9.2　利用者アクセスの管理 管理目的・選択理由：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。			

ISO27001管理策 ISO27001附属書A「管理目的及び管理策」より			当社の取り組み状況
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。	アクセス制御方針を定め、手順書に基づき登録、削除を行っている。
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しなければならない。	同上
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。	同上
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しなければならない。	指紋認証やパスワード設定をしており、パスワードは定期的に変更している。
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。	権限設定は定期的に見直しを実施している。
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。	従業員の採用・異動・退職の際には権限、パスワードの変更を行っている。
A.9.3　利用者の責任 管理目的・選択理由：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。	パスワードの取り扱いについて、手順書に定めている。
A.9.4　システム及びアプリケーションのアクセス制御 管理目的・選択理由：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。	アクセス制御方針、業務分掌に基づきアクセス権限を設定している。
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。	システム及びアプリケーションへのアクセスは情報セキュリティ方針に基づき定められた手順に従っている。
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。	パスワードポリシーが設定できる場合はパスワードを定期的に変更するするよう設定する。指紋認証登録の場合はパスワードを不要としている。
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はシステム管理者、またはその指示を受けた者のみとしている。
A.10　暗号			
A.10.1 暗号による管理策 管理目的・選択理由：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。	暗号化通信を利用する場合を手順書に定めている。
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しなければならない。	クラウドサービスの暗号化に用いる鍵は、商用電子証明書を利用、保護および有効期限を管理している。
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 管理目的・選択理由：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。	事務所内の執務室、会議室区画は社員証カードにより入退室管理をし、書庫は情報資産の重要性にあわせ施錠管理をしている。
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。	・事務所ビルはテナントごとにセキュリティカードで入退室管理がされ、執務室、会議室区画は社員証カードで入退室管理をしている。 ・データセンターの入退館は、当社のあらかじめ登録された者のみとし、それ以外の者の入退館には登録者が同伴することとしている。
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。	同上

ISO27001管理策 ISO27001附属書A「管理目的及び管理策」より			当社の取り組み状況
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。	自然災害や悪意のある脅威等について、リスクアセスメントを実施し、結果に基づいた対応策を講じている。
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。	・セキュティを保つべき領域での作業を手順書に定めている。 ・セキュリティを保つべき領域に当社以外の者が入室する場合は、退室するまで、当社の者が同伴している。
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。	宅配などの荷物の受け渡しは、入退室管理区域外としている。やむを得ない場合は、上記のとおり。
A.11.2 装置 管理目的・選択理由：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。	自然災害や悪意のある脅威等について、リスクアセスメントを実施し、結果に基づいた対応策を講じている。
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。	同上
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。	同上
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，正しく保守しなければならない。	定期的に実施するよう手順書に定めている。
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。	全ての情報資産は構外持ち出し禁止とし、やむを得ず持ち出す場合は上職者の許可を得ることとしている。
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。	持ち出し可能な端末はルールに従い利用している。
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。	保存されている情報を消去している。特に、廃棄する場合は、残存データを完全に消去してから廃棄している。外部委託する場合は秘密保持契約や消去証明書を受領している。
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。	不正操作や盗み見等の脅威について、リスクアセスメントを実施し、結果に基づいた対応策を講じている。
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。	クリアデスク、クリアスクリーン方針に基づき管理策を講じている。
A.12　運用のセキュリティ			
A.12.1 運用の手順及び責任 管理目的・選択理由：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。	情報処理設備の運用、操作手順等は各業務について、文書化され、利用可能としている。
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。	システム、装置等の構成変更時は、手順に従い、責任者の承認を得て変更し、記録管理している。
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。	利用状況等を監視し、必要とする容量・能力を予測し調整するよう手順を定めている。
A.12.1.4	開発施設、試験施設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又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。	アクセス制御方針に基づき、開発環境，試験環境、運用環境へのアクセスを制限している。
A.12.2 マルウェアからの保護			

ISO27001管理策 ISO27001附属書A「管理目的及び管理策」より			当社の取り組み状況
管理目的・選択理由：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。	不正アクセスの監視、OS等のアップデートなど予防のための策を講じている。
A.12.3 バックアップ 管理目的・選択理由：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。	データベースのバックアップは手順に基づき、定期的に取得している。また、重要な情報資産のバックアップは遠隔地に保管している。
A.12.4 ログ取得及び監視 管理目的・選択理由：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。	ログファイルは分類し、保存・管理を行っている。
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。	保存したログファイルは、許可された者のみアクセス可能とし、ログは一定期間保管している。
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。	システムにて取得可能なログはシステムで取得し、それ以外は作業記録を作成している。
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。	NTPサーバを利用し、システム装置の時刻を標準時に合わせている。
A.12.5 運用ソフトウェアの管理 管理目的・選択理由：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。	新システムを導入する場合はリスクアセスメントを実施し、重要な変更を行う場合は変更による影響やセキュリティについて検討し、変更計画を立てている。
A.12.6 技術的ぜい弱性管理 管理目的・選択理由：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。	情報システムの技術的脆弱性の情報を得たら、直ちにパッチ適用等、適切な処置をとることとしている。
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。	新システムを導入する場合、標準実装以外のソフトウェアを実装する場合の手順を定めている。
A.12.7 情報システムの監査に対する考慮事項 管理目的・選択理由：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。	内部監査計画の際には業務負担を考慮し、監査対象部門とのスケジュールの合意をしている。
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 管理目的・選択理由：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。	ネットワークは、セグメントを分割し、各情報資産へのアクセスを制御し管理している。また、不正アクセスを不正侵入検知ツールにより監視している。
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。	新システムの導入や外部委託の場合はリスクアセスメントを実施し、情報セキュリティレベルを確認している。
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。	アクセス制御方針に基づき、アクセス制御している。
A.13.2 情報の転送 管理目的・選択理由：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。			

ISO27001管理策 ISO27001附属書A「管理目的及び管理策」より			当社の取り組み状況
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。	・メール誤送信ツールを利用している。 ・電子メールの自動転送設定は禁止としている。業務上必要な場合は手順に従い必要な承認を得ている。
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。	顧客や委託先との秘密保持契約、または業務委託契約を締結している。
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。	メール誤送信ツールを利用している。
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件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。	秘密保持契約書は社内共通の雛形を利用している。
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 管理目的・選択理由：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に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。	システム受入時にはセキュリティ要求事項を満たすことを試験により確認している。また、セキュリティ要求事項は「標準観点」として文書化している。
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。	第三者サービスを利用する際はセキュリティ管理、サービス定義、サービスレベル等を確認し、契約を行っている。
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	VPN通信、暗号化等の対策を講じている。インターネットを経由した接続の場合、HTTPS接続等の接続先の正当性を確認する手段を用いた接続としている。
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 管理目的・選択理由：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。	ソフトウェア及びシステム開発は情報セキュリティに考慮した手順書に従い行っている。
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，正式な変更管理手順を用いて管理しなければならない。	システム、装置等の構成変更時は、手順書に従い、行っている。
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。	システム、装置に重要な変更を行う場合は変更による影響やセキュリティについて検討し、変更計画を立てている。
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。	ソフトウェアは当社指定、または許可されたものに限定している。
A.14.2.5	セキュリティに配慮したシステム構築の原則	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。	システム開発は情報セキュリティに考慮した手順書に従い行っている。
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，適切に保護しなければならない。	アクセス制御方針に基づき、開発環境へのアクセスを制限している。
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。	委託先の、品質管理、セキュリティ管理状況”、“再委託先の管理状況”について確認し、必要に応じて、是正、改善、改良の為の打ち合わせを実施している。
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。	システム開発の各レビューでセキュリティ事項に関するレビューを行っている。

ISO27001管理策 ISO27001附属書A「管理目的及び管理策」より			当社の取り組み状況
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。	新規システム導入時には選定レビュー、試験を実施。システムの改定・更新版の受入れ時には設計レビュー、試験、リリースレビューを手順書に基づき、実施している。
A.14.3 試験データ 管理目的・選択理由：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。	試験で使用するデータ、環境は保護し、管理している。
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 管理目的・選択理由：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。	第三者サービスを利用する際はセキュリティ管理、サービス定義、サービスレベル等を確認し、契約を行っている。
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。	外部委託先との契約の際は必ず機密保持契約を結んでいる。
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。	システム開発業務委託時には、再委託に関して情報セキュリティ要件を満たすように契約を結んでいる。
A.15.2 供給者のサービス提供の管理 管理目的・選択理由：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。	外部委託、外部サービスを利用する場合、年に1度、監査を行っている。
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。	同上
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 管理目的・選択理由：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報告から是正完了までの手順を定めている。
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。	情報セキュリティインシデントを発見した場合の報告の手順を定めている。
A.16.1.3	情報セキュリティ弱点の報告	組織の情報システム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。	情報セキュリティの弱点を発見した場合の報告の手順を定めている。
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レベル・事象の評価の手順を定めている。
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・事象への対応手順を定めている。
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。	・過去の情報セキュリティインシデントの類似事象の有無を確認し、是正計画を作成している。
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。	法的措置が取られる可能性が生じた場合には、関連法令又は事件の審理が行われている特定の法廷の規則に定められた証拠に関する規定に適合させている。
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			

ISO27001管理策 ISO27001附属書A「管理目的及び管理策」より			当社の取り組み状況
A.17.1 情報セキュリティ継続 管理目的・選択理由：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。	事業継続に影響を与える災害、重大な障害に対しては、情報セキュリティ委員会と事業継続委員会が連携し、情報セキュリティを確保することにしている。
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。	事業継続に影響を与える災害、重大な障害に対しては、情報セキュリティ委員会と事業継続委員会が連携し、手順を文書化している。
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の管理策を検証しなければならない。	事業継続に影響を与える災害、重大な障害に対しては、情報セキュリティ委員会と事業継続委員会が連携し、情報セキュリティ管理策を検証している。
A.17.2 冗長性 管理目的・選択理由：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。	システム導入に際しては、複数の情報処理施設での運用を実施している。
A.18　順守			
A.18.1 法的及び契約上の要求事項の順守 管理目的・選択理由：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。	年1回法令改正等の状況を調査し、ISMSの観点で各業務に対する影響の可能性を確認し、対応を検討している。
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。	知的財産権のあるソフトウェアの取扱いについては、法令，規制及び契約上の要求事項を順守している。
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，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。	組織の記録については、消失、破壊、改ざんから保護するよう、各手順書に従い取り扱っている。
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。	関連法規に従って個人情報を保護し、各手順書に反映し運用している。
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。	暗号化機能は、関連する全ての協定、法令及び規制を順守している。
A.18.2 情報セキュリティのレビュー 管理目的・選択理由：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。	ISMS外部審査、内部監査を実施している。
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。	年1回管理策有効性評価を実施している。
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守に関して，定めに従ってレビューしなければならない。	定期的な脆弱性診断や日常監視によりレビューを実施している。