# 適用宣言書

【Ver.1.1.0】

制定:　　2020年8月1日

改訂:　　2020年9月26日

Thinkings株式会社

| 大項目 | 中項目 | 小項目 | 内容 （ISO/IEC 27001:2013 附属書A 規定） | 適用 | 適用理由（除外の場合、除外理由） |
|---|---|---|---|---|---|
| | 管理目的及び管理策 | | | － | |
| 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:<br>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。 | － | 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、関連する法令及び規則に従って規定するため。 |
| | | 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公表し、通知しなければならない。 | ○ | 情報セキュリティ指針を従業員及び関連する外部関係者に宣言及び通知し、当社のセキュリティを理解させるため |
| | | 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。 | ○ | 情報セキュリティのための方針が、引き続き適切な内容で維持するため |
| 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:<br>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。 | － | 目的:組織内の情報セキュリティを管理するため。 |
| | | 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責任を定め、かつ、割り当てなければならない。 | ○ | 組織内の情報セキュリティ体制を確立するため。 |
| | | 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、分割しなければならない。 | ○ | 認可されていない又は意図しない変更、その他、誤用の危険性を低減するため。 |
| | | 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。 | ○ | 有事の際に、迅速な連絡を行うため。 |
| | | 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。 | ○ | 最新のセキュリティ情報の収集と対応を行えるようにするため。 |
| | | 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関わらず、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。 | ○ | プロジェクトに対する情報セキュリティの取り組みを確実にするため |
| | A.6.2 | モバイル機能及びテレワーキング | 目的:<br>モバイル機器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 | － | 目的:モバイルコンピューティング及びテレワーキングの設備を用いるときの情報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り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。 | ○ | 外部組織のリスクを管理し、セキュリティを維持するめ。 |
| | | 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。 | ○ | 遠隔地からの作業に関して、セキュリティを確保するため。 |
| A.7 | 人的資源のセキュリティ | | | － | |
| | A.7.1 | 雇用前 | 目的:<br>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。 | － | 目的:従業員、契約相手及び第三者の利用者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とともに、盗難、不正行為、又は施設の不正使用のリスクを低減するため。 |
| | | 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、関連のある法令、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、事実上の要求事項、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、契約相手及び第三者の利用者の契約におけるリスクを低減するため |

| 大項目 | 中項目 | 小項目 | 内容 （ISO/IEC 27001:2013 附属書A 規定） | 適用 | 適用理由（除外の場合、除外理由） |
|---|---|---|---|---|---|
| | | 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、契約相手及び第三者の利用者に、当社が求めるセキュリティ要求事項を確実に順守させるため。 |
| | A.7.2 | 雇用期間中 | 目的<br>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。 | － | 目的：従業員、契約相手及び第三者の利用者の、情報セキュリティの脅威及び諸問題、並びに責任及び義務に対する認識を確実なものとし、通常の業務の中で組織の情報セキュリティ基本方針を維持し、人による誤りのリスクを低減できるように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。 | ○ | 従業員、契約相手及び第三者の利用者に、当社が求めるセキュリティ要求事項を確実に順守させるため。 |
| | | 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、関連する場合には、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なず、また、定めに従ってそれを更新しなければならない。 | ○ | 従業員、契約相手及び第三者の利用者に、情報セキュリティの責任及び義務を認識させ、当社が求めるセキュリティ要求事項を確実に順守させるため。 |
| | | 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きを備えなければならない。 | ○ | 従業員、契約相手及び第三者の利用者に、セキュリティ違反に対する懲戒の認識とその手続きを確実にするため。 |
| | A.7.3 | 雇用の終了及び変更 | 目的：<br>雇用の終了及び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 | － | 目的：従業員、契約相手及び第三者の利用者の組織からの離脱又は雇用の変更を所定の方法で行うことを確実にするため。 |
| | | 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、遂行しなければならない。 | ○ | 従業員、契約相手及び第三者の利用者の雇用の終了又は変更による情報漏えいを防止するため。 |
| A8. | 資産の管理 | | | － | |
| | A.8.1 | 資産に対する責任 | 目的：<br>組織の資産を特定し、適切な保護の責任を定めるため。 | － | 目的：組織の資産の適切な保護を達成し、維持するため。 |
| | | 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。 | ○ | 守るべき情報資産を明確にするため。 |
| | | A.8.1.2 資産の管理責任 | 目録で維持される資産は、管理されなければならない。 | ○ | 守るべき情報資産の管理責任を明確にするため。 |
| | | 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。 | ○ | 情報資産の機密性を確実にするため。 |
| | | 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全てを返却しなければならない。 | ○ | 従業員及び外部の利用者の雇用の終了又は変更による資産の返却漏れをなくすため。 |
| | A.8.2 | 情報の分類 | 目的：<br>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確実にするため。 | － | 目的：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の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。 | ○ | 重要な情報資産の取り扱いを確実にするため。 |
| | | A.8.2.2 情報の分類ラベル付け | 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。 | ○ | 重要な情報資産の取り扱いを確実にするため。 |
| | | 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。 | ○ | 情報の取り扱いにおける認可されていない開示、改ざん、除去、又は破壊、並びに誤用を防止するため。 |
| | A.8.3 | 媒体の取扱い | 目的：<br>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。 | － | 目的：資産の認可されていない開示、改ざん、除去、又は破壊、並びにビジネス活動の中断を防止するため。 |
| | | 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。 | ○ | 取り外し可能な媒体における認可されていないアクセス及び持ち出し、紛失、盗難、漏洩等のセキュリティ事故を防止するため。 |

| 大項目 | 中項目 | 小項目 | 内容 （ISO/IEC 27001:2013 附属書A 規定） | 適用 | 適用理由（除外の場合、除外理由） |
|---|---|---|---|---|---|
| | | 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。 | ○ | 媒体の処分から情報漏えいを防止するため。 |
| | | A.8.3.3 物理的媒体の配送 | 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。 | ○ | 配送中による不正アクセス、紛失、破損を防止するため。 |
| 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:<br>情報及び情報処理施へのアクセスを制限するため | － | 目的:情報へのアクセスを制御するため。 |
| | | A.9.1.1 アクセス制御方針 | アクセス制御方針は、業務上及び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。 | ○ | 情報への認可されていないアクセスを防止するため。 |
| | | A.9.1.2 ネットワーク及びサービス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。 | ○ | 利用することを特別に認可したサービスへのアクセスだけを、利用者に提供すること。 |
| | A.9.2 | 利用者アクセスの管理 | 目的:<br>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、認可されてないアクセスを防止するため。 | － | 目的:情報システムへの、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。 | ○ | 社内・社外の利用者登録/削除を確実にするため |
| | | 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を許可及び無効化するために、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。 | ○ | 社内・社外の利用者アクセス権の提供を確実にするため |
| | | 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。 | ○ | システム特権ユーザの不正利用を防止するため |
| | | 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。 | ○ | 秘密認証情報（パスワード/生態認証情報等）の漏洩を防止するため。 |
| | | 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た間隔でレビューしなければならない。 | ○ | 不必要なアクセス権限の発生を防止するため。 |
| | | 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なず、また、変更に合わせて修正しなければならない。 | ○ | 従業員、契約相手及び第三者の利用者の契約の終了又は変更による不要アカウントの削除を確実にするため。 |
| | A.9.3 | 利用者の責任 | 目的:<br>利用者に対して、自らの認証情報を保護する責任をもたせるため。 | － | 目的:認可されていない利用者のアクセス、並びに情報及び情報処理設備の損傷又は盗難を防止するため。 |
| | | 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。 | ○ | 社内・社外の秘密認証情報の管理を徹底させるため。 |
| | 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:<br>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。 | － | 目的:<br>オペレーティングシステムへの、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への認可されていないアクセスを防止するため。 |
| | | 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、認可されていないアクセスを防止するため。 |
| | | 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。 | ○ | 脆弱なパスワード管理によるシステムへの、認可されていないアクセスを防止するため。 |

| 大項目 | 中項目 | 小項目 | 内容 （ISO/IEC 27001:2013 附属書A 規定） | 適用 | 適用理由（除外の場合、除外理由） |
|---|---|---|---|---|---|
| | | 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システムユーティリティへの認可されていないアクセスを防止するため。 |
| | | 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管理を確実にするため |
| A.10 | 暗号 | | | － | |
| | A.10.1 暗号による管理策 | | 目的:<br>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。 | － | 目的:暗号手段によって、情報の機密性、真正性又は完全性を保護するため。 |
| | | 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、真正性又は完全性を維持するため。 |
| | | A.10.1.2 鍵管理 | 暗号鍵の利用、保護、有効期間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。 | ○ | 暗号鍵の漏洩を防止するため。 |
| 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:<br>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。 | － | 目的:組織の施設及び情報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。 | ○ | 当社施設及び情報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.11.1.2 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。 | ○ | 組織の施設及び情報に対する認可されていない物理的アクセスを防止するため。 |
| | | 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。 | ○ | 外部及び環境の脅威による損傷及び業務停止等を防止するため。 |
| | | 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。 | ○ | セキュリティを保つべき領域での物理的／論理的な不正アクセス及び損傷、妨害を防止するため。 |
| | | 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物理的な保護及び指針を設計し、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作業に関する物理的な保護及び指針を設計し、適用すること。 |
| | | 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。 | ○ | 受渡場所からの不正アクセス及び情報漏えいを防止するため。 |
| | A.11.2 装置 | | 目的:<br>資産の喪失、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 | － | 目的:資産の損失、損傷、盗難又は劣化、及び組織の活動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、又は保護しなければならない。 | ○ | 装置の損失、損傷、盗難又は劣化、及び組織の活動に対する妨害を防止するため。 |
| | | 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。 | ○ | 支援ユーティリティの損傷、又は劣化による装置停止を防止するため。 |
| | | 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。 | ○ | 通信ケーブル及び電源ケーブルの配線から、傍受又は損傷を防止するため。 |
| | | 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とするために、正しく保守しなければならない。 | ○ | 装置の可用性及び完全性を継続的に維持するため。 |
| | | 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。 | ○ | 持ち出しによる損失、損傷、盗難事故を防止するため。 |

| 大項目 | 中項目 | 小項目 | 内容 （ISO/IEC 27001:2013 附属書A 規定） | 適用 | 適用理由（除外の場合、除外理由） |
|---|---|---|---|---|---|
| | | 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。 | ○ | 構外での利用による損失、損傷、盗難事故を防止するため。 |
| | | 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。 | ○ | 装置の処分又は再利用から情報漏えいを防止するため |
| | | A.11.2.8 無人状態にる利用者装置 | 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から認可されていないアクセス及び情報漏えいを防止するため |
| | | 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。 | ○ | 書類及び取外し可能な記録媒体等の紛失及び盗難を防止するため。 |
| A.12 | 運用管理 | | | － | |
| | A.12.1 運用の手順及び責任 | | 目的:<br>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 | － | 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。 | ○ | 業務を正確、かつ、セキュリティを保った運用を行うため。 |
| | | 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。 | ○ | 情報処理設備及びシステム変更を確実にするため。 |
| | | 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なず、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。 | ○ | システムの容量・能力不足から業務停止を防止するため。 |
| | | 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。 | ○ | 開発施設、試験施設、及び運用施設に対する認可されていないアクセス又は変更に関するリスクを低減するため。 |
| | A.12.2 マルウェアからの保護 | | 目的:<br>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。 | － | 目的:ソフトウェア及び情報の完全性を保護するため。 |
| | | 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、利用者に適切に意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。 | ○ | マルウェアによるリスクを低減するため。 |
| | A.12.3 バックアップ | | 目的:<br>データの消失から保護するため | － | 目的:情報及び情報処理設備の完全性及び可用性を維持するため。 |
| | | 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。 | ○ | 情報の可用性を維持するため。 |
| | A.12.4 ログ取得及び監視 | | 目的:<br>イベントを記録し、証拠を作成するため。 | － | 目的:認可されていない情報処理活動を検知するため。 |
| | | 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。 | ○ | 認可されていない情報処理活動を検知し、追跡を行い原因を追究するため。 |
| | | 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。 | ○ | ログ情報の改ざん及び消失を防止するため。 |
| | | 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。 | ○ | 担当者の作業を追跡できるようにするため |
| | | 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内のクロックは、単一の参照時刻源と同期させなければならない。 | ○ | 関連するログ情報の完全性を維持するため。 |
| | A.12.5 運用ソフトウェアの管理 | | 目的:<br>運用システムの完全性を確実にするため。 | － | 目的:システムファイルのセキュリティを確実にするため。 |
| | | 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手順を実施しなければならない。 | ○ | 適切な運用システムに関わるソフトウェアを導入し、管理を確実にするため |

| 大項目 | 中項目 | 小項目 | 内容 （ISO/IEC 27001:2013 附属書A 規定） | 適用 | 適用理由（除外の場合、除外理由） |
|---|---|---|---|---|---|
| | A.12.6 | 技術的脆弱性管理 | 目的:<br>技術的脆弱性の悪用を防止するため。 | － | 目的:公開された技術的ぜい弱性の悪用によって生じるリスクを低減するため。 |
| | | A.12.6.1 技術的脆弱性の管理 | 利用中の情報システムの技術的脆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、そのような脆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。 | ○ | 公開された技術的脆弱性への迅速な対応を行うため。 |
| | | 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策定し、また、実施しなければならない。 | ○ | 不正なソフトウェア及び勝手なソフトウェアのインストールを制御するため |
| | A.12.7 | 情報システムの監査に対する考慮事項 | 目的:<br>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 | － | 目的:情報システム監査手続の有効性を最大限にするため、及び情報システム監査手続への/からの干渉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、慎重に計画され、合意されなければならない。 | ○ | 情報システム監査手続の有効性を最大限にするため、及び情報システム監査手続への/からの干渉を最小限にするため。 |
| 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:<br>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。 | － | 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基盤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。 | ○ | ネットワークにおける情報の保護、及びネットワークを支える基盤を保護するため。 |
| | | 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のセキュリティ機能、サービスレベル及び管理上の必要項を特定し、確実に提供させるため |
| | | A.13.1.3 ネットワークの領域分割 | 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。 | ○ | ネットワークを利用した認可されていないアクセスを防止するため。 |
| | A.13.2 | 情報の転送 | 目的:<br>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。 | － | 目的:組織内部で交換した及び外部と交換した、情報及びソフトウェア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。 | ○ | 情報交換による情報漏えいを防止するため。 |
| | | A.13.2.2 情報転送に関する合意 | 合意では、組織と外部組織との間の業務情報の情報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。 | ○ | 外部組織との情報交換における情報漏洩のリスクを低減するため。 |
| | | 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による誤送信及び盗聴を防止するため。 |
| | | 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必要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。 | ○ | 組織内の情報セキュリティ要求事項を順守させるため。 |
| 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:<br>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を含む | － | 目的:セキュリティは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。 |
| | | A.14.1.1 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。 | ○ | 情報システムの取得、開発及び保守におけるセキュリティ要求事項の漏れをなくすため。 |
| | | 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経由するアプリケーションサービスに含まれる情報の不正行為、契約紛争、認可されていない開示及び改ざんから保護するため。 |

| 大項目 | 中項目 | 小項目 | 内容 （ISO/IEC 27001:2013 附属書A 規定） | 適用 | 適用理由（除外の場合、除外理由） |
|---|---|---|---|---|---|
| | | 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、不完全な通路、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または再生。 | ○ | 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、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、認可されていない複製又は再生を未然に防止するため。 |
| | 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:<br>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。 | － | 目的:業務用ソフトウェアシステムのソフトウェア及び情報のセキュリティを維持するため。 |
| | | 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の開発ための統一した方針を確立し、セキュリティ配慮を確実にするため |
| | | 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。 | ○ | システム変更の正確な実装を行うため |
| | | A.14.2.3 オペレーティングプラットフォーム変更後の業務用ソフトウェアの技術的レビュー | 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。 | ○ | オペレーティングシステムの変更による利用規約違反を防止するため。 |
| | | 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なず、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による使用許諾違反又はサポート外とならないため |
| | | A.14.2.5 セキュリティに配慮したシステム構築の原則 | セキュリティ配慮したシステムの設計（engineering)するための原則を確立し、文書化、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。 | ○ | セキュリティ配慮したシステム設計を確実にするため |
| | | A.14.2.6 セキュリティ配慮した開発環境 | 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。 | ○ | セキュリティに配慮した開発環境を確立し、適切に保護するため |
| | | 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。 | － | 開発は委託していない |
| | | 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（fuctionality)の試験は、開発期間中に実施しなければならない。 | ○ | 実装後のセキュリティ上の脆弱の検出を起こらないようにするため |
| | | 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。 | ○ | 本番環境におけるシステム障害のリスクを低減するため。 |
| | A.14.3 | 試験データ | 目的:<br>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、注意深く選択し、保護し、管理しなければならない。 | ○ | 試験データの管理を確実にするため |
| A.15 | 供給者管理 | | | － | |
| | A.15.1 | 供給者関係における情報セキュリティ | 目的:<br>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。 | － | |
| | | A.15.1.1 供給者関係のための情報セキュリティ方針 | 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。 | ○ | セキュリティ要求事項を特定し、供給者との合意を確実にするため |
| | | 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 | ○ | セキュリティ要求事項を特定し、供給者との合意を確実にするため |
| | | 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を取扱うための要求事項をふくめなければならない。 | ○ | 再委託先及び製品のサプライチェーンに関するリスクを低減するため |
| | A.15.2 | 供給者のサービス提供の管理 | 目的:<br>供給者との合意に沿った、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。 | － | 目的:第三者の提供するサービスに関する合意に沿った、情報セキュリティ及びサービスの適切なレベルを確保し、維持するため。 |
| | | A.15.2.1 供給者が提供するサービスの監視及びレビュー | 組織は、供給者によるサービス提供を常に監視、レビュー、及び監査しなければならない。 | ○ | セキュリティ要求事項が順守されていることを確実にするため。 |

| 大項目 | 中項目 | 小項目 | 内容 （ISO/IEC 27001:2013 附属書A 規定） | 適用 | 適用理由（除外の場合、除外理由） |
|---|---|---|---|---|---|
| | | A.15.2.2 供給者が提供するサービス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。 | ○ | 委託業者との契約変更を確実にするため。 |
| 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：<br>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り組み方法を確実にするため。 | － | 目的：情報システムに関連する情報セキュリティの事象及び弱点を、時機を失しない是正処置を講じることができるやり方で連絡することを確実にするため。 |
| | | 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しなければならない。 | ○ | 情報セキュリティインシデントへの対応を確実にするため。 |
| | | 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、できるだけすみ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を確実にするため。 |
| | | 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、また、報告するように要求しなければならない。 | ○ | セキュリティ弱点の報告を確実にするため |
| | | 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、評価し、情報セキュリティインシデントとして分類すべきかどうかについて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を識別し、対応を確実にするため |
| | | 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、文書化され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への対応を確実にするため。 |
| | | 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、将来のインシデントの発生の可能性又は影響を低減するために用いなければならない。 | ○ | 情報セキュリティインシデントから予防策を講じるため |
| | | 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、取得及び保護のための手順を定め、適用しなければならない。 | ○ | 情報セキュリティ事故の証拠を保全するため。 |
| 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：<br>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。 | － | 目的：情報システムの重大な故障又は災害の影響からの事業活動の中断に対処するとともに、それらから重要な業務プロセスを保護し、さらに、事業活動及び重要な業務プロセスの時機を失しない再開を確実にするため。 |
| | | 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（adverese 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。 | ○ | 情報システムの重大な故障又は災害の影響からの事業活動の中断に対処するとともに、それらから重要な業務プロセスを保護し、さらに、事業活動及び重要な業務プロセスの時機を失しない再開を確実にするため。 |
| | | A.17.1.2 情報セキュリティ継続の実施 | 組織は、困難な状況のもと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、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。 | ○ | 情報システムの重大な故障又は災害の影響からの事業活動の中断に対処するとともに、それらから重要な業務プロセスを保護し、さらに、事業活動及び重要な業務プロセスの時機を失しない再開を確実にするため。 |
| | | A.17.1.3 情報セキュリティ継続を検証、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、困難な状況のもとで妥当かつ有効で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。 | ○ | 事業継続計画が最新で効果的なものであることを確実にするため |
| | A.17.2 冗長性 | | 目的：<br>情報処理施設の可用性を確実にするため。 | － | 目的：<br>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。 | ○ | 情報処理設備の可用性を維持するため |

| 大項目 | 中項目 | 小項目 | 内容 （ISO/IEC 27001:2013 附属書A 規定） | 適用 | 適用理由（除外の場合、除外理由） |
|---|---|---|---|---|---|
| A.18 | 順守 | | | － | |
| | A.18.1 | 法的及び契約上の要求事項の順守 | 目的:<br>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、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。 | － | 目的:法令、規則又は契約上のあらゆる義務、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識別 | 各情報システム及び組織について、全ての関連する法令、規制お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。 | ○ | 法令、規則又は契約上のあらゆる義務、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.18.1.2 知的財産権（IPR） | 知的財産権及び権利関係のあるソフトウェア製品を利用に関連する、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。 | ○ | 知的財産権に対する違反を防止するため。 |
| | | 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。 | ○ | 証拠の記録を保全するため。 |
| | | A.18.1.4 プライバシー及び個人情報を特定できる情報（PII）の保護 | プライバシー及びPII（個人情報）の保護は、関連する法令、規制、及び適用がある場合には、その要求に従って確実にしなければならない。 | ○ | 個人データ及び個人情報の管理を確実にするため。 |
| | | 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、法令及び規制要求事項を順守して用いなければならない。 | ○ | 関連するすべての協定、法令及び規制に順守するため。 |
| | A.18.2 | 情報セキュリティのレビュー | 目的:<br>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 | － | 目的:組織のセキュリティ方針及び標準類へのシステムの順守を確実にするため。 |
| | | 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。 | ○ | 組織内の情報セキュリティにおける問題点及び懸念点、改善事項の有無を確認するため。 |
| | | 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。 | ○ | 当社のセキュリティ順守事項における現場の順守状況をチェックするため。 |
| | | 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。 | ○ | 情報システムに対するセキュリティ順守状況をチェックするため。 |

| 大項目 | 中項目 | 小項目 | クラウドサービスカスタマ | 適用 | 適用理由（除外の場合、除外理由） |
|---|---|---|---|---|---|
| | 管理目的及び管理策 | | | | |
| 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:<br>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。 | | |
| | | A.5.1.1 情報セキュリティのための方針群 | クラウドコンピューティングのための情報セキュリティ方針を、クラウドサービスカスタマのトピック固有の方針として定義することが望ましい。<br>クラウドサービスカスタマのクラウドコンピューティングのための情報セキュリティ方針は、組織の情報及びその他の資産に対する情報セキュリティリスクの需要なレベルと矛盾しないものとすることが望ましい。 | ○ | 情報セキュリティ指針を従業員及び関連する外部関係者に宣言及び通知し、当社のセキュリティを理解させるため |
| 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:<br>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 | クラウドサービスカスタマは、クラウドサービスプロバイダと、情報セキュリティの役割及び責任の適切な割り当てについて合意し、割り当てられた役割及び責任は、合意書に記載することが望ましい。<br>クラウドサービスカスタマは、クラウドサービスプロバイダの顧客支援・顧客対応機能との関係を特定し、管理することが望ましい。 | ○ | 組織内の情報セキュリティ体制を確立するため。 |
| | | A.6.1.3 関係当局との連絡 | クラウドサービスカスタマは、クラウドサービスカスタマ及びクラウドサービスプロバイダが併せて行う操作に関連する関係当局を特定することが望ましい。 | ○ | 有事の際に、迅速な連絡を行うため。 |
| A.7 | 人的資源のセキュリティ | | | | |
| | A.7.2 | 雇用期間中 | 目的<br>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.7.2.2 情報セキュリティの意識向上、教育及び訓練 | クラウドサービスカスタマは、関連する従業員及び契約者を含む、クラウドサービスビジネスマネージャ、クラウドサービス実務管理者、クラウドサービスインテグレータ及びクラウドサービスユーザのための意識向上、教育及び訓練のプログラムに次の事項を追加することが望ましい。<br>クラウドサービスに関する情報セキュリティの意識向上、教育及び訓練のプログラムは、経営陣及び監督責任者（事業単位の経営陣及び監督責任者を含む）に提供することが望ましい。このことは、情報セキュリティ活動の有効な協調を支援する。 | ○ | 従業員、契約相手及び第三者の利用者に、情報セキュリティの責任及び義務を認識させ、当社が求めるセキュリティ要求事項を確実に順守させるため。 |
| A8. | 資産の管理 | | | | |
| | A.8.1 | 資産に対する責任 | 目的:<br>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 | クラウドサービスカスタマの資産目録には、クラウドコンピューティング環境に保存される情報及び関連資産も記載することが望ましい。目録の記録では、例えばクラウドサービスの特定など、資産を保持している場所を示すことが望ましい。 | ○ | 資産の適切な管理のため |

| 大項目 | 中項目 | 小項目 | クラウドサービスカスタマ | 適用 | 適用理由（除外の場合、除外理由） |
|---|---|---|---|---|---|
| | A.8.2 | 情報の分類 | 目的:<br>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確実にするため。 | | |
| | | A.8.2.2 情報の分類ラベル付け | クラウドサービスカスタマは、採用したラベル付けの手順に従って、クラウドコンピューティング環境に保持する情報及び関連資産にラベル付けをすることが望ましい。適用可能な場合には、クラウドサービスプロバイダが提供する、ラベル付けを支援する機能が採用できる。 | ○ | 重要な情報資産の取り扱いを確実にするため。 |
| 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:<br>情報及び情報処理施へのアクセスを制限するため | | |
| | | A.9.1.2 ネットワーク及びサービスサービスへのアクセス | クラウドサービスカスタマの、ネットワークサービス利用のためのアクセス制御方針では、利用するそれぞれのクラウドサービスへの利用者アクセスの要求事項を定めることが望ましい。 | ○ | 利用することを特別に認可したサービスへのアクセスだけを、利用者に提供するため |
| | A.9.2 | 利用者アクセスの管理 | 目的:<br>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、認可されち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 | 追加の実施手引きなし | | |
| | | A.9.2.2 利用者アクセスの提供 | 追加の実施手引きなし | | |
| | | A.9.2.3 特権的アクセス権の管理 | クラウドサービスカスタマは、クラウドサービス実務管理者に管理権限を与える認証に、特定したリスクに応じ、十分にセキュアな認証技術を用いることが望ましい。 | ○ | システム特権ユーザの不正利用を防止するため |
| | | A.9.2.4 利用者の秘密認証情報の管理 | クラウドサービスカスタマは、パスワードなどの秘密認証情報を割り当てるための、クラウドサービスプロバイダの管理手順が、クラウドサービスカスタマの要求事項を満たすことを検証することが望ましい。 | ○ | 秘密認証情報（パスワード/生態認証情報等）の漏洩を防止するため。 |
| | 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:<br>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 | クラウドサービスカスタマは、クラウドサービスにおける情報へのアクセスを、アクセス制御方針に従って制限できること、及びそのような制限を実現することを確実にすることが望ましい。これには、クラウドサービスへのアクセス制限、クラウドサービス機能へのアクセス制限、及びサービスにて保持されるクラウドサービスカスタマデータへのアクセス制限を含む。 | ○ | 情報及びアプリケーションシステム機能への認可されていないアクセスを防止するため。 |
| | | A.9.4.4 特権的なユーティリティプログラムの使用 | ユーティリティプログラムの利用が許可されている場合には、クラウドサービスカスタマは、クラウドコンピューティング環境において利用するユーティリティプログラムを特定し、クラウドサービスの管理策を妨げないことを確実にすることが望ましい。 | ○ | 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システムユーティリティへの認可されていないアクセスを防止するため。 |

| 大項目 | 中項目 | 小項目 | クラウドサービスカスタマ | 適用 | 適用理由（除外の場合、除外理由） |
|---|---|---|---|---|---|
| A.10 暗号 | | | | | |
| | A.10.1 暗号による管理策 | | 目的:<br>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 | クラウドサービスカスタマは、リスク分析によって必要と認められる場合には、クラウドサービスの利用において、暗号による管理策を実施することが望ましい。その管理策は、クラウドサービスカスタマ又はクラウドサービスプロバイダのいずれが供給するものであれ、特定したリスクを低減するために十分な強度を持つものであることが望ましい。<br>クラウドサービスプロバイダが暗号を提供する場合は、クラウドサービスプロバイダが提供するすべての情報をレビューし、その機能について次の事項を確認することが望ましい。 | ○ | 情報の機密性、真正性又は完全性を維持するため。 |
| | | A.10.1.2 鍵管理 | クラウドサービスカスタマは、各クラウドサービスのための暗号カ鍵を特定し、鍵管理手順を実施することが望ましい。<br>クラウドサービスプロバイダが、クラウドサービスカスタマが利用する鍵管理機能を提供する場合には、クラウドサービスカスタマは、クラウドサービスに関連する鍵管理手順について、次の情報を要求することが望ましい。<br>クラウドサービスカスタマは、自らの鍵管理を採用する場合又はクラウドサービスプロバイダの鍵管理サービスとは別のサービスを利用する場合、暗号の運用のための暗号カギをクラウドサービスプロバイダが保存し、管理することを許可しないことが望ましい。 | ○ | 暗号鍵の漏洩を防止するため。 |
| A.11 物理的及び環境的セキュリティ | | | | | |
| | A.11.2 装置 | | 目的:<br>資産の喪失、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.11.2.7 装置のセキュリティを保った処分又は再利用 | クラウドサービスカスタマは、クラウドサービスプロバイダが、資源のセキュリティを保った処分又は再利用のための方針及び手順を持つことの確認を要求することが望ましい。 | ○ | 装置の処分又は再利用から情報漏えいを防止するため |
| A.12 運用管理 | | | | | |
| | A.12.1 運用の手順及び責任 | | 目的:<br>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.12.1.2 変更管理 | クラウドサービスカスタマの変更管理プロセスは、クラウドサービスプロバイダによるあらゆる変更の影響を考慮することが望ましい。 | ○ | 情報処理設備及びシステム変更を確実にするため。 |
| | | A12.1.3 容量・能力の管理 | クラウドサービスカスタマは、クラウドサービスで提供される合意した容量・能力が、クラウドサービスカスタマの要求を満たすことを確認することが望ましい。<br>クラウドサービスカスタマは、将来のクラウドサービスの性能を確実にするため、クラウドサービスの使用を監視し、将来必要となる容量・能力を予測することが望ましい。 | ○ | 適切な能力を確保するため |

| 大項目 | 中項目 | 小項目 | クラウドサービスカスタマ | 適用 | 適用理由（除外の場合、除外理由） |
|---|---|---|---|---|---|
| | A.12.3 バックアップ | | 目的:<br>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 | クラウドサービスプロバイダがクラウドサービスの一部としてバックアップ機能を提供する場合は、クラウドサービスカスタマは、クラウドサービスプロバイダにバックアップの仕様を要求することが望ましい。また、クラウドサービスカスタマは、その仕様がバックアップに関する要求事項を満たすことを検証することが望ましい。<br>クラウドサービスプロバイダがバックアップ機能を提供しない場合は、クラウドサービスカスタマが、バックアップ機能の導入に責任を負う。 | ○ | 情報の可用性を維持するため。 |
| | A.12.4 ログ取得及び監視 | | 目的:<br>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 | クラウドサービスカスタマは、イベントログ取得の要求事項を定義し、クラウドサービスがその要求事項を検証することが望ましい。 | ○ | 認可されていない情報処理活動を検知し、追跡を行い原因を追究するため。 |
| | | A.12.4.3 実務管理者及び運用担当者の作業ログ | 特権的な操作がクラウドサービスカスタマに移譲されている場合は、その操作及び操作のパフォーマンスについてログを取得することが望ましい。クラウドサービスカスタマは、クラウドサービスプロバイダが提供するログ取得機能が適切かどうか、又はクラウドサービスカスタマがログ取得機能を追加して実装すべきかを決定することが望ましい。 | ○ | 担当者の作業を追跡できるようにするため |
| | | A.12.4.4 クロックの同期 | クラウドサービスカスタマは、クラウドサービスプロバイダのシステムで使用するクロックの同期について、情報を要求することが望ましい。 | ○ | 関連するログ情報の完全性を維持するため。 |
| | A.12.6 技術的脆弱性管理 | | 目的:<br>技術的脆弱性の悪用を防止するため。 | | |
| | | A.12.6.1 技術的脆弱性の管理 | クラウドサービスカスタマは、クラウドサービスプロバイダに、提供を受け継クラウドサービスに影響しうる技術的ぜい弱性の管理に関する情報を要求することが望ましい。クラウドサービスカスタマは、自らが管理に責任を持つ技術的ぜい弱性を特定し、それを管理するプロセスを明確に定義することが望ましい。 | ○ | 公開された技術的脆弱性への迅速な対応を行うため。 |
| 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:<br>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.13.1.3 ネットワークの分離 | クラウドサービスカスタマは、クラウドサービスの共有環境においてテナントの分離を実現するためのネットワークの分離に関する要求事項を定義し、クラウドサービスプロバイダがその要求事項を満たしていることを検証することが望ましい。 | ○ | ネットワークを利用した認可されていないアクセスを防止するため。 |
| 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:<br>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を含む | | |
| | | A.14.1.1 セキュリティ要求事項の分析及び仕様化 | クラウドサービスカスタマは、クラウドサービスにおける情報セキュリティ要求事項を定め、クラウドサービスプロバイダの提供するサービスがこの要求事項を満たせるか否か評価することが望ましい。<br>この評価のために、クラウドサービスカスタマは、クラウドサービスプロバイダに情報セキュリティ機能に関する情報の提供を要求することが望ましい。 | ○ | 情報システムの取得、開発及び保守におけるセキュリティ要求事項の漏れをなくすため。 |

| 大項目 | 中項目 | 小項目 | クラウドサービスカスタマ | 適用 | 適用理由（除外の場合、除外理由） |
|---|---|---|---|---|---|
| | 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:<br>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 | クラウドサービスカスタマは、クラウドサービスプロバイダが適用しているセキュリティに配慮した開発の手順及び実践に関する情報を、クラウドサービスプロバイダに要求することが望ましい。 | ○ | ソフトウェア及びシステムの開発ための統一した方針を確立し、セキュリティ配慮を確実にするため |
| A.15 供給者管理 | | | | | |
| | A.15.1 | 供給者関係における情報セキュリティ | 目的:<br>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。 | | |
| | | A.15.1.1 供給者関係のための情報セキュリティ方針 | クラウドサービスカスタマは、クラウドサービスプロバイダを供給者の一つとして、供給者関係のための情報セキュリティの方針に含めることが望ましい。これはクラウドサービスプロバイダによるクラウドサービスカスタマデータへのアクセスおよびクラウドサービスカスタマデータの管理に関するリスクの低減に役立つ。 | ○ | セキュリティ要求事項を特定し、供給者との合意を確実にするため |
| | | 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 | クラウドサービスカスタマは，サービス合意書に記載されている，クラウドサービスに関連する情報セキュリティの役割及び責任を確認することが望ましい。これらには次のプロセスが含まれ得る。 | ○ | セキュリティ要求事項を特定し、供給者との合意を確実にするため |
| | | A.15.1.3 ICTサプライチェーン | （追加の実施の手引なし） | | |
| 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:<br>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り組み方法を確実にするため。 | | |
| | | A.16.1.1 責任及び手順 | クラウドサービスカスタマは，情報セキュリティインシデント管理についての責任の割当てを検証し，それがクラウドサービスカスタマの要求事項を満たすことを確認することが望ましい。 | ○ | 情報セキュリティインシデントへの対応を確実にするため。 |
| | | A.16.1.2 情報セキュリティ事象の報告 | クラウドサービスカスタマは，クラウドサービスプロバイダに，次に示す仕組みに関する情報を要求することが望ましい。 | ○ | 情報セキュリティ事象の報告を確実にするため。 |
| | | A.16.1.7 証拠の収集 | クラウドサービスカスタマ及びクラウドサービスプロバイダは，クラウドコンピューティング環境内で生成される，ディジタル証拠となり得る情報及びその他の情報の提出要求に対応する手続について合意することが望ましい。 | ○ | 情報セキュリティ事故の証拠を保全するため。 |

| 大項目 | 中項目 | 小項目 | クラウドサービスカスタマ | 適用 | 適用理由（除外の場合、除外理由） |
|---|---|---|---|---|---|
| A.18 順守 | | | | | |
| | A.18.1 法的及び契約上の要求事項の順守 | | 目的:<br>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、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識別 | クラウドサービスカスタマは，関連する法令及び規制には，クラウドサービスカスタマの法域のものに加え，クラウドサービスプロバイダの法域のもの もあり得ることを考慮することが望ましい。<br>クラウドサービスカスタマは，その事業のために必要な，関係する規制及び標準に対するクラウドサービスプロバイダの順守の証拠を要求することが望ましい。第三者の監査人が発行する証明書を，この証拠とする場合がある。 | ○ | 法令、規則又は契約上のあらゆる義務、及ぴ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.18.1.2 知的財産権（IPR） | クラウドサービスに商用ライセンスのあるソフトウェアをインストールすることは，そのソフトウェアのライセンス条項への違反を引き起こす可能性がある。クラウドサービスカスタマは，クラウドサービスにライセンスソフトウェアのインストールを許可する前にクラウドサービス固有のライセンス要求事項を特定する手順をもつことが望ましい。クラウドサービスが弾力性がありスケーラブルで，ライセンス条項で認められる以上のシステム又はプロセッサコアでソフトウェアが動作する可能性がある場合について，特に注意を払うことが望ましい。 | ○ | 知的財産権に対する違反を防止するため。 |
| | | A.18.1.3 記録の保護 | クラウドサービスカスタマは，クラウドサービスカスタマによるクラウドサービスの利用に関連して，クラウドサービスプロバイダが収集し，保存する記録の保護に関する情報を，クラウドサービスプロバイダに要求することが望ましい。 | ○ | 証拠の記録を保全するため。 |
| | | A.18.1.5 暗号化機能に対する規制 | クラウドサービスカスタマは，クラウドサービス の利用に適用する暗号による管理策群が，関係する合意書，法令及び規制を順守していることを検証することが望ましい。 | ○ | 関連するすべての協定、法令及び規制に順守するため。 |
| | A.18.2 情報セキュリティのレビュー | | 目的:<br>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。 | | 目的:組織のセキュリティ方針及び標準類へのシステムの順守を確実にするため。 |
| | | A.18.2.1 情報セキュリティの独立したレビュー | クラウドサービスカスタマは，クラウドサービス のための情報セキュリティ管理策及び指針の実施状況がクラウドサービスプロバイダの提示どおりであることについて，文書化した証拠を要求することが望ましい。その証拠は，関係する標準への適合の証明書である場合もある。 | ○ | 組織内の情報セキュリティにおける問題点及び懸念点、改善事項の有無を確認するため。 |
| | CLD.6.3 クラウドサービスカスタマとクラウドサービスプロバイダとの関係 | | 目的:情報セキュリティマネジメントに関してクラウドサービスカスタマとクラウドサービスプロバイダ との間で共有し分担する役割及び責任について，両者間の関係を明確にするため。 | | |
| | | CLD.6.3.1 クラウドコンピューティング環境における役割及び責任の共有及び分担 | クラウドサービスカスタマは，クラウドサービスの利用に合わせて方針及び手順を定義又は追加し，クラウドサービスユーザにクラウドサービスの利用における自らの役割及び責任を意識させることが望ましい。 | ○ | 役割責任を明確にするため |
| | CLD.8.1 資産に対する責任 | | | | |
| | | CLD.8.1.5 クラウドサービスカスタマの資産の除去 | クラウドサービスカスタマは，その資産の返却及び除去，並びにこれらの資産の全ての複製のクラウドサービスプロバイダのシステムからの削除の記述を含む，サービスプロセスの終了に関する文書化した説明を要求することが望ましい。<br>この説明では，全ての資産を一覧にし，サービス終了が時機を失することなく行われるよう，サービス終了のスケジュールを文書化することが望ましい。 | ○ | 確実な情報の削除のため |

| 大項目 | 中項目 | 小項目 | クラウドサービスカスタマ | 適用 | 適用理由（除外の場合、除外理由） |
|---|---|---|---|---|---|
| | CLD.9.5 | 共有する仮想環境におけるクラウドサービスカスタマデータのアクセス制御 | 目的クラウドコンピューティングにおける共有する仮想環境利用時の情報セキュリティリスクを低減するため。 | | |
| | | CLD.9.5.1 仮想コンピューティング環境における分離 | （追加の実施の手引なし） | | |
| | | CLD.9.5.2 仮想マシンの要塞化 | クラウドサービスカスタマ及びクラウドサービスプロバイダは，仮想マシンを設定する際には，適切な 側面からの要塞化（例えば，必要なポート，プロトコル及びサービスだけを有効とする。）及び利用する各仮想マシンへの適切な技術手段（例えば，マルウェア対策，ログ取得）の実施を確実にすることが望ましい。 | ○ | システムの確実な保護のため |
| | CLD.12.1 | 運用の手順及び責任 | | | |
| | | CLD.12.1.5 実務管理者の運用のセキュリティ | クラウドサービスカスタマは，一つの失敗がクラウドコンピューティング環境における資産に回復不能な損害を与えるような重要な操作の手順を文書化することが望ましい。 | ○ | ミスによる情報の消去等を防ぐため |
| | | CLD.12.4.5 クラウドサービスの監視 | クラウドサービスカスタマは，クラウドサービスプロバイダに，各クラウドサービスで利用可能なサービス監視機能に関する情報を要求することが望ましい。 | ○ | 監視機能による安全管理のため |
| | CLD.13.1 | ネットワークセキュリティ管理 | | | |
| | | CLD.13.1.4 仮想及び物理ネットワークのセキュリティ管理の整合 | （追加の実施の手引なし） | | |

| 大項目 | 中項目 | 小項目 | クラウドサービスプロバイダ | 適用 | 適用理由（除外の場合、除外理由） |
|---|---|---|---|---|---|
| | 管理目的及び管理策 | | | | |
| 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:<br>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。 | | |
| | | A.5.1.1 情報セキュリティのための方針群 | クラウドサービスプロバイダは，クラウドサービ スの提供及び利用に取り組むため，次の事項を考慮し，情報セキュリティ方針を拡充することが望ましい。 | ○ | 情報セキュリティ指針を従業員及び関連する外部関係者に宣言及び通知し、当社のセキュリティを理解させるため |
| 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:<br>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 | クラウドサービスプロバイダは，そのクラウドサービスカスタマ，クラウドサービスプロバイダ及び供給者と，情報セキュリティの役割及び責任の適切 な割当てについて合意し，文書化することが望ましい。 | ○ | 組織内の情報セキュリティ体制を確立するため。 |
| | | A.6.1.3 関係当局との連絡 | クラウドサービスプロバイダは，クラウドサービスカスタマに，クラウドサービスプロバイダの組織の地理的所在地，及びクラウドサービスプロバイダが，クラウドサービスカスタマデータを保存する可能性のある国を通知することが望ましい。 | ○ | 有事の際に、迅速な連絡を行うため。 |
| A.7 | 人的資源のセキュリティ | | | | |
| | A.7.2 | 雇用期間中 | 目的<br>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.7.2.2 情報セキュリティの意識向上、教育及び訓練 | クラウドサービスプロバイダは，クラウドサービスカスタマデータ及びクラウドサービス派生データを適切に取り扱うために，従業員に，意識向上，教育及び訓練を提供し，契約相手に同様のことを実施するよう要求することが望ましい。これらのデータには，クラウドサービスカスタマの機密情報，又は クラウドサービスプロバイダによるアクセス及び利用について，規制による制限を含む，特定の制限が課されたデータを含む可能性がある。 | ○ | 従業員、契約相手及び第三者の利用者に、情報セキュリティの責任及び義務を認識させ、当社が求めるセキュリティ要求事項を確実に順守させるため。 |
| A8. | 資産の管理 | | | | |
| | A.8.1 | 資産に対する責任 | 目的:<br>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 | クラウドサービスプロバイダの資産目録では，次のデータを明確に識別することが望ましい。<br>－クラウドサービスカスタマデータ<br>－クラウドサービス派生データ | ○ | 資産の適切な管理のため |
| | A.8.2 | 情報の分類 | 目的:<br>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確実にするため。 | | |
| | | A.8.2.2 情報の分類ラベル付け | クラウドサービスプロバイダは，クラウドサービ スカスタマが情報及び関連資産を分類し，ラベル付けするためのサービス機能を文書化し，開示することが望ましい。 | × | 情報資産の分類、ラベル付けの機能については提供していないため |

| 大項目 | 中項目 | 小項目 | クラウドサービスプロバイダ | 適用 | 適用理由（除外の場合、除外理由） |
|---|---|---|---|---|---|
| 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:<br>情報及び情報処理施へのアクセスを制限するため | | |
| | | A.9.1.2 ネットワーク及びサービスサービスへのアクセス | （追加の実施の手引なし） | － | |
| | A.9.2 | 利用者アクセスの管理 | 目的:<br>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、認可されち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 | クラウドサービスカスタマのクラウドサービスユーザによるクラウドサービスへのアクセスを管理するため，クラウドサービスプロバイダは，クラウドサービスカスタマに利用者登録・登録削除の機能及びそれを利用するための仕様を提供することが望ましい。 | ○ | 利用者の管理のため |
| | | A.9.2.2 利用者アクセスの提供 | クラウドサービスプロバイダは，クラウドサービスカスタマのクラウドサービス実務管理者がその役割を行えるように，クラウドサービスカスタマが特定するリスクに応じた，十分に強い認証技術を提供することが望ましい。例えば，クラウドサービスプロバイダは，多要素認証機能を提供し，又は第三者の多要素認証メカニズムを利用可能とすることができる。 | ○ | 利用者が適切にアクセスできるようにするため |
| | | A.9.2.3 特権的アクセス権の管理 | クラウドサービスプロバイダは，クラウドサービスカスタマのクラウドサービス実務管理者がその役割を行えるように，クラウドサービスカスタマが特定するリスクに応じた，十分に強い認証技術を提供することが望ましい。例えば，クラウドサービスプロバイダは，多要素認証機能を提供し，又は第三者の多要素認証メカニズムを利用可能とすることができる。 | ○ | 特権ユーザによる不正行為を制御するため |
| | | A.9.2.4 利用者の秘密認証情報の管理 | クラウドサービスプロバイダは，秘密認証情報を割り当てる手順，及び利用者認証手順を含む，クラ ウドサービスカスタマの秘密認証情報の管理のための手順について情報を提供することが望ましい。 | ○ | 秘密認証情報（パスワード/生態認証情報等）の漏洩を防止するため。 |
| | 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:<br>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 | クラウドサービスプロバイダは，クラウドサービスへのアクセス，クラウドサービス機能へのアクセス，及びサービスで保持するクラウドサービスカスタマデータへのアクセスを，クラウドサービスカスタマが制限できるように，アクセス制御を提供する ことが望ましい。 | ○ | 情報及びアプリケーションシステム機能への認可されていないアクセスを防止するため。 |
| | | A.9.4.4 特権的なユーティリティプログラムの使用 | クラウドサービスプロバイダは，クラウドサービス内で利用される全てのユーティリティプログラムのための要求事項を特定することが望ましい。<br>クラウドサービスプロバイダは，認可された要員だけが，通常の操作手順又はセキュリティ手順を回避することのできるユーティリティプログラムを利用できるように厳密に制限し，そのようなプログラムの利用を定期的にレビューし，監査することを確実にすることが望ましい。 | ○ | 当社内で特権的ユーティリティプログラムの使用があるため |

| 大項目 | 中項目 | 小項目 | クラウドサービスプロバイダ | 適用 | 適用理由(除外の場合、除外理由) |
|---|---|---|---|---|---|
| A.10 暗号 | | | | | |
| | A.10.1 暗号による管理策 | | 目的:<br>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 | クラウドサービスプロバイダは，クラウドサービスカスタマに，クラウドサービスプロバイダが処理する情報を保護するために，暗号を利用する環境に関する情報を提供することが望ましい。クラウドサービスプロバイダは，また，クラウドサービスカスタマ自らの暗号による保護を適用することを支援するためにクラウドサービスプロバイダが提供する能力についても，クラウドサービスカスタマに情報を提供することが望ましい。 | ○ | 情報の機密性、真正性又は完全性を維持するため。 |
| | | A.10.1.2 鍵管理 | (追加の実施の手引なし) | − | |
| A.11 物理的及び環境的セキュリティ | | | | | |
| | A.11.2 装置 | | 目的:<br>資産の喪失、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.11.2.7 装置のセキュリティを保った処分又は再利用 | クラウドサービスプロバイダは，資源(例えば，装置，データストレージ，ファイル，メモリ)のセキュリティを保った処分又は再利用を時機を失せずに行うための取決めがあることを確実にすることが望ましい。 | ○ | 装置の処分又は再利用から情報漏えいを防止するため |
| A.12 運用管理 | | | | | |
| | A.12.1 運用の手順及び責任 | | 目的:<br>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.12.1.2 変更管理 | クラウドサービスプロバイダは，クラウドサービスに悪影響を与える可能性のあるクラウドサービスの変更について，クラウドサービスカスタマに情報を提供することが望ましい。次の事項は，クラウドサービスカスタマが，当該変更が情報セキュリティに与える可能性のある影響を特定するのに役立つ。<br>クラウドサービスプロバイダは，ピアクラウドサービスプロバイダに依存するクラウドサービスを提供する際には，クラウドサービスカスタマに，ピアクラウドサービスプロバイダによって行われた変更を通知する必要がある場合がある。 | ○ | 情報処理設備及びシステム変更を確実にするため。 |
| | | A12.1.3 容量・能力の管理 | クラウドサービスプロバイダは，資源不足による情報セキュリティインシデントの発生を防ぐため，資源全体の容量・能力を監視することが望ましい。 | ○ | 適切な能力を確保するため |

| 大項目 | 中項目 | 小項目 | クラウドサービスプロバイダ | 適用 | 適用理由（除外の場合、除外理由） |
|---|---|---|---|---|---|
| | A.12.3 バックアップ | | 目的:<br>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 | クラウドサービスプロバイダは，クラウドサービスカスタマに，バックアップ機能の仕様を提供することが望ましい。その仕様には，必要に応じ，次の情報を含めることが望ましい。<br>クラウドサービスプロバイダは，クラウドサービスカスタマにバックアップにアクセスさせるサービスを提供する場合には，仮想スナップショットなどの，セキュリティを保った，他のクラウドサービス カスタマから分離したアクセスを提供することが望ましい。 | ○ | 情報の可用性を維持するため。 |
| | A.12.4 ログ取得及び監視 | | 目的:<br>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 | クラウドサービスプロバイダは，クラウドサービスカスタマに，ログ取得機能を提供することが望ましい。 | ○ | 認可されていない情報処理活動を検知し、追跡を行い原因を追究するため。 |
| | | A.12.4.3 実務管理者及び運用担当者の作業ログ | （追加の実施の手引なし） | | |
| | | A.12.4.4 クロックの同期 | （追加の実施の手引なし）クラウドサービスプロバイダは，クラウドサービスカスタマに，クラウドサービスプロバイダのシステムで使用しているクロックについて，及びクラウドサービスカスタマがそのクロックをクラウドサービスのクロックに同期させる方法について，情報を提供することが望ましい。 | ○ | 関連するログ情報の完全性を維持するため。 |
| | A.12.6 技術的脆弱性管理 | | 目的:<br>技術的脆弱性の悪用を防止するため。 | | 目的:公開された技術的ぜい弱性の悪用によって生じるリスクを低減するため。 |
| | | A.12.6.1 技術的脆弱性の管理 | クラウドサービスプロバイダは，提供するクラウドサービスに影響し得る技術的ぜい弱性の管理に関する情報をクラウドサービスカスタマが利用できるようにすることが望ましい。 | ○ | 公開された技術的脆弱性への迅速な対応を行うため。 |
| 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:<br>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.13.1.3 ネットワークの分離 | クラウドサービスプロバイダは，次の場合においてネットワークアクセスの分離を確実に実施することが望ましい。<br>必要な場合には，クラウドサービスプロバイダは， クラウドサービスプロバイダが実施している分離 を，クラウドサービスカスタマが検証することを助けることが望ましい。 | ○ | ネットワークの混在を防ぐため |
| 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:<br>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を含む | | |
| | | A.14.1.1 セキュリティ要求事項の分析及び仕様化 | クラウドサービスプロバイダは，クラウドサービスカスタマが利用する情報セキュリティ機能に関する情報をクラウドサービスカスタマに提供することが望ましい。この情報は，悪意をもつ者を利する可能性のある情報を開示することなく，クラウドサービスカスタマには役立つものであることが望ましい。 | ○ | 情報システムの取得、開発及び保守におけるセキュリティ要求事項の漏れをなくすため。 |

| 大項目 | 中項目 | 小項目 | クラウドサービスプロバイダ | 適用 | 適用理由（除外の場合、除外理由） |
|---|---|---|---|---|---|
| | 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:<br>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 | クラウドサービスプロバイダは，開示方針に合致する範囲で，適用しているセキュリティに配慮した開発の手順及び実践に関する情報を提供することが望ましい。 | ○ | ユーザに対する安心の提供のため。 |
| A.15 | 供給者管理 | | | | |
| | A.15.1 | 供給者関係における情報セキュリティ | 目的:<br>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。 | | |
| | | A.15.1.1 供給者関係のための情報セキュリティ方針 | （追加の実施の手引なし） | | |
| | | 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 | クラウドサービスプロバイダは，クラウドサービスカスタマとの間で誤解が生じないことを確実にするために，合意の一部として，クラウドサービスプロバイダが実施する，クラウドサービスカスタマに関係する情報セキュリティ対策を特定することが望ましい。<br>クラウドサービスプロバイダが実施する，クラウドサービスカスタマに関係する情報セキュリティ対策は，クラウドサービスカスタマが利用するクラウドサービスの種類によって異なることがある。 | ○ | セキュリティ要求事項を特定し、顧客との合意を確実にするため |
| | | A.15.1.3 ICTサプライチェーン | クラウドサービスプロバイダがピアクラウドサービスプロバイダのクラウドサービスを利用する場合，情報セキュリティ水準を自身のクラウドサービスカスタマに対するものと同等又はそれ以上に保つことを確実にすることが望ましい。<br>クラウドサービスプロバイダは，サプライチェーンでクラウドサービスを提供する場合は，供給者に対して情報セキュリティ目的を示し，それを達成するためのリスクマネジメント活動の実施を要求することが望ましい。 | ○ | サプライヤを適切に管理するため |
| 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:<br>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り組み方法を確実にするため。 | | |
| | | A.16.1.1 責任及び手順 | クラウドサービスプロバイダは，クラウドサービスカスタマとクラウドサービスプロバイダとの間の，情報セキュリティインシデント管理に関する責任の割当て及び手順を，サービス仕様の一部として定めることが望ましい。<br>クラウドサービスプロバイダは，クラウドサービスカスタマに，次のことを含む文書を提供することが望ましい。 | ○ | 情報セキュリティインシデントへの対応を確実にするため。 |
| | | A.16.1.2 情報セキュリティ事象の報告 | クラウドサービスプロバイダは，次の仕組みを提供することが望ましい。<br>−クラウドサービスカスタマが，情報セキュリティ事象をクラウドサービスプロバイダに報告する仕組み<br>−クラウドサービスプロバイダが，情報セキュリティ事象をクラウドサービスカスタマに報告す る仕組み<br>−クラウドサービスカスタマが，報告を受けた情報セキュリティ事象の状況を追跡する仕組み | ○ | 情報セキュリティ事象の報告を確実にするため。 |

| 大項目 | 中項目 | 小項目 | クラウドサービスプロバイダ | 適用 | 適用理由（除外の場合、除外理由） |
|---|---|---|---|---|---|
| | | A.16.1.7 証拠の収集 | クラウドサービスカスタマ及びクラウドサービスプロバイダは，クラウドコンピューティング環境内で生成される，ディジタル証拠となり得る情報及びその他の情報の提出要求に対応する手続について合意することが望ましい。 | ○ | 情報セキュリティ事故の証拠を保全するため。 |
| A.18 順守 | | | | | |
| | A.18.1 法的及び契約上の要求事項の順守 | | 目的:<br>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、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識別 | クラウドサービスプロバイダは，クラウドサービスカスタマにクラウドサービスに適用される法域を知らせることが望ましい。<br>クラウドサービスプロバイダは，関係する法的要求事項（例えば，PII 保護のための暗号化）を特定することが望ましい。この情報は，また，求められたときに，クラウドサービスカスタマに提供することが望ましい。<br>クラウドサービスプロバイダは，適用法令及び契約上の要求事項について，現在の順守の証拠をクラウドサービスカスタマに提供することが望ましい。 | ○ | 法令、規則又は契約上のあらゆる義務、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.18.1.2 知的財産権（IPR） | クラウドサービスプロバイダは，知的財産権の苦情に対応するためのプロセスを確立することが望ましい。 | ○ | 知的財産権に対する違反を防止するため。 |
| | | A.18.1.3 記録の保護 | クラウドサービスプロバイダは，クラウドサービスカスタマによるクラウドサービスの利用に関連して，クラウドサービスプロバイダが収集し，保存する記録の保護に関する情報を，クラウドサービスカスタマに提供することが望ましい。 | ○ | 証拠の記録を保全するため。 |
| | | A.18.1.5 暗号化機能に対する規制 | クラウドサービスプロバイダは，適用される合意書，法令及び規制の順守をクラウドサービスカスタマがレビューするために，実施している暗号による管理策の記載を提供することが望ましい。 | ○ | 関連するすべての協定、法令及び規制に順守するため。 |
| | A.18.2 情報セキュリティのレビュー | | 目的:<br>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 | クラウドサービスプロバイダは，クラウドサービスプロバイダが主張する情報セキュリティ管理策の実施を立証するために，クラウドサービスカスタマに文書化した証拠を提供することが望ましい。<br>個別のクラウドサービスカスタマの監査が現実的でない場合，又は情報セキュリティへのリスクを増加させ得る場合，クラウドサービスプロバイダは，情報セキュリティがクラウドサービスプロバイダの方針及び手順に従って実施され，運用されているこ との独立した証拠を提供することが望ましい。この証拠は，契約の前に，クラウドサービスの利用が見込まれる者に利用できるようにしておくことが望ましい。クラウドサービスプロバイダが選択した独立した監査は，それが十分な透明性が確保されていることを条件として，クラウドサービスカスタマがも つクラウドサービスプロバイダの運用に対するレビューへの関心を満たすものであることが一般に望ましい。独立した監査が現実的でないとき，クラウドサービスプロバイダは，自己評価を行い，クラウドサービスカスタマにそのプロセス及び結果を開示することが望ましい。 | ○ | 組織内の情報セキュリティにおける問題点及び懸念点、改善事項の有無を確認するため。 |

| 大項目 | 中項目 | 小項目 | クラウドサービスプロバイダ | 適用 | 適用理由（除外の場合、除外理由） |
|---|---|---|---|---|---|
| | CLD.6.3 | クラウドサービスカスタマとクラウドサービスプロバイダとの関係 | 目的：情報セキュリティマネジメントに関してクラウドサービスカスタマとクラウドサービスプロバイダ　との間で共有し分担する役割及び責任について，両者間の関係を明確にするため。 | | |
| | | CLD.6.3.1 クラウドコンピューティング環境における役割及び責任の共有及び分担 | クラウドサービスプロバイダは，自らの情報セキュリティの能力，役割及び責任を文書化し伝達することが望ましい。さらに，クラウドサービスプロバイダは，クラウドサービスの利用の一部としてクラウドサービスカスタマが実施及び管理することが必要となる情報セキュリティの役割及び責任を，文書化し伝達することが望ましい。 | ○ | 顧客にサービスの安全性を提供するため |
| | CLD.8.1 | 資産に対する責任 | | | |
| | | CLD.8.1.5 クラウドサービスカスタマの資産の除去 | クラウドサービスプロバイダは，クラウドサービス利用のための合意の終了時における，クラウドサービスカスタマの全ての資産の返却及び除去の取決めについて，情報を提供することが望ましい。<br>資産の返却及び除去についての取決めは，合意文書の中に記載し，時機を失せずに実施することが望ましい。その取決めでは，返却及び除去する資産を特定することが望ましい。 | ○ | 情報の確実な削除のため |
| | CLD.9.5 | 共有する仮想環境におけるクラウドサービスカスタマデータのアクセス制御 | 目的：クラウドコンピューティングにおける共有する仮想環境利用時の情報セキュリティリスクを低減するため。 | | |
| | | CLD.9.5.1 仮想コンピューティング環境における分離 | クラウドサービスプロバイダは，クラウドサービスカスタマデータ，仮想化されたアプリケーション，オペレーティングシステム，ストレージ及びネットワークの適切な論理的分離を実施することが望ましい。目的は次のとおりである。<br>マルチテナンシのクラウドサービスでは，クラウ ドサービスプロバイダは，異なるテナントが使用する資源の適切な分離を確実にするために情報セキュリティ管理策を実施することが望ましい。<br>クラウドサービスプロバイダは，提供するクラウドサービス内でクラウドサービスカスタマの所有するソフトウェアを実行することに伴うリスクを考慮することが望ましい。 | ○ | 顧客同士の混在を防ぐ確実なサービスの分離のため |
| | | CLD.9.5.2 仮想マシンの要塞化 | クラウドサービスカスタマ及びクラウドサービスプロバイダは，仮想マシンを設定する際には，適切な 側面からの要塞化（例えば，必要なポート，プロトコル及びサービスだけを有効とする。）及び利用する各仮想マシンへの適切な技術手段（例えば，マルウェア対策，ログ取得）の実施を確実にすることが望ましい。 | ○ | 安全性の確保のため |

| 大項目 | 中項目 | 小項目 | クラウドサービスプロバイダ | 適用 | 適用理由（除外の場合、除外理由） |
|---|---|---|---|---|---|
| | CLD.12.1 | 運用の手順及び責任 | | | |
| | | CLD.12.1.5 実務管理者の運用のセキュリティ | クラウドサービスプロバイダは，要求するクラウドサービスカスタマに，重要な操作及び手順を文書化して提供することが望ましい。 | ○ | 顧客が確実にサービスを利用できるようにするため |
| | | CLD.12.4.5 クラウドサービスの監視 | クラウドサービスプロバイダは，クラウドサービ スカスタマが，自らに関係するクラウドサービスの操作の特定の側面を監視できるようにする機能を提 供することが望ましい。例えば，クラウドサービス が，他者を攻撃する基盤として利用されていないか， 機微なデータがクラウドサービスから漏えいしてい ないかを監視し検出する。適切なアクセス制御によって，監視機能の利用のセキュリティを保つことが 望ましい。この機能は，当該クラウドサービスカスタマのクラウドサービスインスタンスに関する情報へのアクセスだけを許可することが望ましい。<br>クラウドサービスプロバイダは，クラウドサービ スカスタマにサービス監視機能の文書を提供するこ とが望ましい。<br>監視は，12.4.1 に記載されたイベントログと矛盾しないデータを提供し，かつ，SLA の条項の適用を支援することが望ましい。 | ○ | サービスの確実な提供のため |
| | CLD.13.1 | ネットワークセキュリティ管理 | | | |
| | | CLD.13.1.4 仮想及び物理ネットワークのセキュリティ管理の整合 | クラウドサービスプロバイダは，物理ネットワークの情報セキュリティ方針と整合の取れた，仮想ネットワークを設定するための情報セキュリティ方針 を定義し文書化することが望ましい。クラウドサービスプロバイダは，設定作成に使用する手段によらず，仮想ネットワークの設定が情報セキュリティ方針に適合することを確実にすることが望ましい。 | ○ | ネットワークのトラブルを防止するため |