（音楽分野）

（別冊１）

令和８・９・10 年度
「コンテンツ文化の戦略的・総合的国際発信事業（音楽分野）」委託業務
仕様書

１．業務名

令和８・９・10 年度「コンテンツ文化の戦略的・総合的国際発信事業（音楽分野）」委託業務（以下「本業務」という。）

２．業務の背景・目的

我が国のアニメ、ゲーム、映像、音楽等のコンテンツは、世界中の人々を魅了し、世界市場の中でも高く評価されている、我が国の誇るべき財産である。コンテンツ産業の海外売上は半導体産業、鉄鋼産業の輸出額を超え、2023 年には約 5.8 兆円規模に達しており、政府はコンテンツ産業を基幹産業と位置付け、2033 年に海外売上を現在の約 4 倍となる 20 兆円とする目標を設定している。経済的価値を裏打ちするのは芸術性であり、更なる高みに向けた取組を戦略的に後押しすることが必要である。

これらの各コンテンツ分野の共通の課題として、個社や作品ごとの情報発信はあるものの、業界全体としての戦略に基づく発信や他のコンテンツ分野との連携、いわば「日本コンテンツ」としての発信が十分にできているとは言えない状況にあり、政府が主導することによって一丸となった情報発信を行うことが必要となっている。

このような背景から、令和７年度補正予算により、文化庁文化芸術活動基盤強化基金補助金「クリエイター等育成支援（マンガ等コンテンツの次世代のデジタル配信プラットフォームの構築に向けたコンソーシアム創出等）」が措置され、独立行政法人日本芸術文化振興会（以下「振興会」という。）に令和５年度に造成された文化芸術活動基盤強化基金へ交付された。

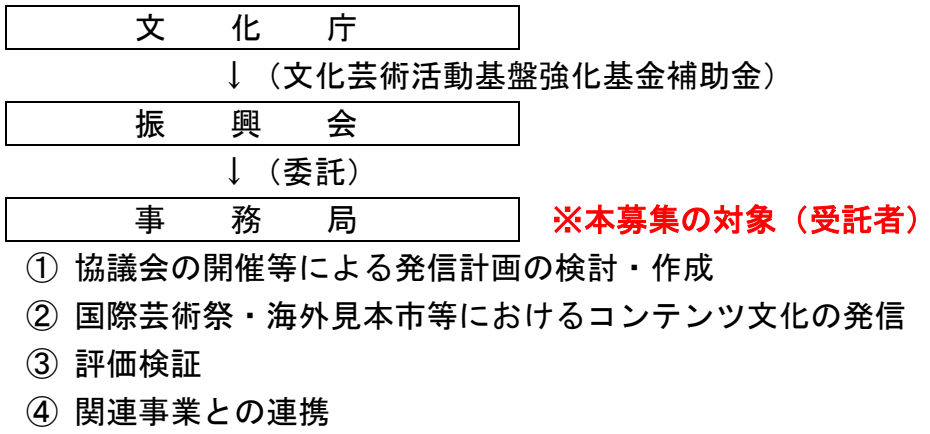
本業務は、上記の課題意識のもと各コンテンツ分野において日本全体としての戦略を定め、世界的な評価形成が行われる主要な国際芸術祭・見本市等において戦略的・総合的に発信し、ひいては我が国コンテンツの芸術性に対する評価を一層高めていくことを目的とする。

３．業務の概要

（１）業務の概要

上記の目的意識のもとコンテンツ文化の戦略的・総合的国際発信を行うため、振興会から委託を受けた受託者は事務局を設置し、①協議会の開催等による発信計画の検討・作成、②国際芸術祭・海外見本市等におけるコンテンツ文化の発信、③事業効果検証の実施等を行う。

（２）事業スキーム



４．履行期間

契約締結日から令和 11 年 9 月 30 日まで。

５．業務内容

受託者は、以下の各業務を実施するための適切な事務局体制を整えた上で、文化庁、振興会及び関係団体・機関等との十分な連携を図りながら実施すること。

本項目は、必要最低限の業務内容を示すものであり、これらを効果的かつ効率的に実施するための提案・実施を妨げるものではなく、自由提案とする。

（委託上限額：全体３億円）

① 協議会の開催等による発信計画の検討・作成

戦略的・総合的に我が国のコンテンツ文化（音楽分野）の海外発信を行うため、コンテンツ関係企業・機関や関係省庁等が有機的に連携する体制を構築し、発信計画を検討・作成する。発信計画は、音楽分野の海外発信における現状認識を整理し、世界的な評価形成が行われる主要な国際芸術祭・見本市における国際的な評価基準となる賞の受賞等も見据えた上で、日本全体としての展開戦略等について国内ステークホルダーと協議の上で策定する。その際、必要に応じて・効果的である場合には他のコンテンツ分野と融合した展開戦略も含めるものとする。

発信計画作成のための手法・体制は問わないが、文化庁や経済産業省、業界統括団体等を含む国内ステークホルダーが調整を行う協議会等を設置・開催することが望ましい。協議会等を設置・開催する場合は、企画提案にあたって、構成員等を具体的に提案すること（受託者決定後に振興会と協議の上決定する）。ただし、受託者が多様なステークホルダーで構成され、協議会等を設置する必要性が低いと振興会が判断する場合は、その限りではない。

発信計画は３年計画を描いた上で年度ごとの計画を盛り込んだものとすること。また、前年度の取組を踏まえ必要に応じ改訂すること。

② 国際芸術祭・海外見本市等におけるコンテンツ文化の発信

①の発信計画を実行に移し、世界的な発信力を有する国際芸術祭・見本市等において発信を行うこと。

具体的には、例えば我が国の優れたコンテンツや若手クリエイター等を戦略的に発信するパビリオン・ブース等の設置・運営等、作品（企画段階を含む）の出品支援や、併設ワークショップ・スクール等への参加・開催、クリエイターと海外関係機関・キーパーソンとのネットワーク構築等を支援すること。

その際、企業が個社又はグループで実施する取組とは異なる、①の発信計画に基づいた国主導による取組となることに留意するとともに、国際的評価を向上させるために真に有効な取組を実施すること。効果的・効率的な実施のため、下記④も踏まえつつ、マンガなどの他のコンテンツ分野との連携等についても検討・実施すること。

③ 評価検証

評価検証の観点から、以下の点について協議会等での議論を経たうえで報告書を毎年作成し、振興会に提出すること。

・①の議論
・②の実施実績
・得られた知見
・得られた課題
・他分野との連携の成果と課題
・戦略的発信に向けた更なる方策案

④ 関連事業との連携

令和７年度補正予算により措置された「クリエイター等育成支援（マンガ等コンテンツの次世代のデジタル配信プラットフォームの構築に向けたコンソーシアム創出等）」においては、本業務のほか、以下の事業を別途実施する予定である。本業務の実施に当たっては、振興会が委託・助成する以下の事業と連携して業務を実施すること。特に、「マンガデジタル配信プラットフォーム構築に向けたコンソーシアムの運営等事業（仮称）」及び「コンテンツ文化の戦略的・総合的発信運営等事業」の各分野に関しては、各受託団体と連絡を密にすること。

・マンガデジタル配信プラットフォーム構築に向けたコンソーシアムの運営等事業（仮称）
・コンテンツ文化の戦略的・総合的発信運営等事業（アニメ分野、ゲーム分野、映像分野）
・コンテンツ制作・発信を支える中核的専門人材育成・確保等
・クリエイターへの対価還元に向けた著作物等データの流通促進に係る環境構築事業

６．受託者に必要な人員等

受託者は本業務の円滑かつ適切な実施のため、必要な体制を整えなければならない。（土日祝日、年末年始を除く）

次に定める人員を確保した上で、上記５．④に記載の各事業の受託事業者や助成対象者及び振興会と

の連絡調整が常時できる体制を整えること。また、業務内容に合った人員配置計画を作成すること。

（１） 業務責任者

ア　受託者は業務全体を統括する業務責任者を定めること。

イ　業務責任者は、業務に必要な知識を有していること。

ウ　業務責任者は、業務を総合的に把握するとともに、従事者に対する適切な助言等を徹底し、業務の適正な履行に努めること。

（２） 従事者

ア　受託者は本仕様を満たすのに十分な従事者を確保すること。なお、業務が停滞又は著しく遅滞していると振興会が判断した場合には、受託者は速やかに従事者を増員し、停滞又は遅滞した状態を解消すること。

イ　従事者はパソコンでワード及びエクセルの操作が問題なく行える者とする。

（３） 服務関係

ア　受託者は、業務開始前に業務体制表（連絡先も含む）を書面にて提出すること。

イ　受託者は、業務上知り得た振興会の業務内容並びに職員及び職員以外の者に関する情報等すべての情報を第三者に漏らさないこと。また、本委託業務以外の如何なる目的にも使用しないこと。業務責任者及び従事者についても同様とする。なお、契約期間満了後、並びに業務責任者及び従事者が本委託業務を離れた後も同様とする。

ウ　受託者は、業務責任者及び従事者に関する一切の責任を負う。

エ　振興会は、業務責任者及び従事者が業務履行上著しく不適切であると判断した場合は、受託者に対し措置を求める。受託者は、業務責任者及び従事者の変更を行うなど、速やかに措置を講ずること。

オ　受託者が本業務の一部を第三者に委任し、又は請け負わせる（以下「再委託」という）場合に、再委託の相手方に同様の措置を講ずるものとする。

７．委託業務完了報告書の提出及び体裁

各年度の終了又は業務が完了した際は、委託業務年度完了報告書を作成し、当該年度終了日若しくは業務完了の日から３０日以内又は委託期間満了の日のいずれか早い日までに振興会へ提出すること。

また、業務が完了した際は、委託業務最終完了報告書を作成し、最終年度にかかる「８．検査」の通知を受けた日から３０日以内に振興会へ提出すること。

８．検査

振興会は、受託者の完了した業務が、契約書及び仕様書記載事項を充たしていることを、振興会、受託者双方の立会いのもとで確認したことをもって検収とする。振興会は受託者より委託業務年度完了報告書の提出を受けた後、委託業務年度完了報告書の内容の審査及び必要に応じて現地調査を行い、受託者の委託業務の実施に要した経費の証憑、帳簿等の調査により支払うべき金額を年度毎に確定し、これを受託者に通知することとする。

また、振興会は受託者より委託業務最終完了報告書の提出を受けた後、委託業務最終完了報告書の内容の審査及び必要に応じて現地調査を行い、受託者の委託業務の実施に要した経費の証憑、帳簿等の調査により支払うべき総額を確定し、これを受託者に通知することとする。

９．契約不適合責任

振興会は、検収が完了した日を起算して１年以内に契約の内容に適合していないものがあることが判明した場合には、受託者の責任及び負担において、直ちに期限を指定して当該契約不適合状態を修補させることとする。

１０．受託者に求める要求要件

本業務は、個人情報管理に高い信頼性を求めることから、受託者はプライバシーマーク又はISO/IEC27001 若しくは JISQ27001 の認証取得事業者であること。本業務の実施に際して情報システムを使用する場合は、政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されているサービスを用いること。ただし、振興会が定める別紙により、当該サービスのセキュリティ対策の実施状況、代替措置等について説明し、振興会が認めた場合には ISMAP 登録外のサービスも可とする。

１１．知的財産権の帰属等

本業務により作成する成果物に関し、著作権法（昭和 45 年 5 月 6 日法律第 48 号）第２１条、第２３条、第２６条の３、第２７条及び第２８条に定める権利を含む全ての著作権を振興会に譲渡し、振興会は独占的に使用するものとする。なお、受託者は振興会に対し、一切の著作者人格権を行使しないものとし、第三者をして行使させないものとする。また、受託者が本業務の成果物に係る著作権を自ら使用し、又は第三者をして使用させる場合、振興会と別途協議するものとする。

・成果物に第三者が権利を有する著作物が含まれている時は、振興会が特に使用を指示した場合を除き、受託者は当該著作物の使用に関して費用の負担を含む一切の手続を行うものとする。なお、この時、受託者は当該著作権者の使用許諾条件につき、振興会の了承を得るものとする。

・本業務の作業に関し、第三者との間で著作権に係る権利侵害の紛争等が生じた場合、当該紛争の原因が専ら振興会の責めに帰す場合を除き、受託者は自らの負担と責任において一切を処理するものとする。なお、振興会は紛争等の事実を知った時は、速やかに受託者に通知するものとする。

１２．再委託

本業務において、再委託を原則として禁止するものとする。ただし、受託者が本業務の一部について、再委託の相手方の商号又は名称、住所、再委託する理由、再委託予定金額、再委託する業務の範囲、再委託の相手方に係る業務の履行能力等について業務計画書に記載し、振興会が了承した場合は、この限りでない。

受託者は、再委託の相手方が行った作業について全責任を負うものとする。また、受託者は再委託の相手方に対して、本仕様書「１１．知的財産権の帰属等」、「１４．秘密保持等」、「１５．情報セキュリティに関する受託者の責任」、「１６．個人情報保護法に関する事項」を含め、本業務の受託者と同等の義務を負わせるものとし、再委託の相手方との契約においてその旨を定めるものとする。

受託者は、再委託の相手方に対して、定期的又は必要に応じて、作業の進捗状況及び情報セキュリティ対策の履行状況について報告を行わせる等、適正な履行の確保に努めるものとする。また、受託者は、振興会が本業務の適正な履行の確保のために必要があると認める時は、その履行状況について振興会に対し報告し、また振興会が自ら確認することに協力するものとする。

受託者は、振興会が承認した再委託の内容について変更しようとする時は、変更する事項及び理由等について記載した申請書を提出し、振興会の承認を得るものとする。

１３．再々委託の履行体制の把握

受託者は、再委託の相手方がさらに再委託を行う等複数の段階で再委託（以下「再々委託」という。）することを原則として禁止するものとする。ただし、再々委託先の住所、氏名、再々委託を行う業務の範囲を事前に書面で振興会に提出し、振興会が了承した場合は、この限りでない。

受託者は、再々委託の相手方が行った作業について全責任を負うものとする。また、受託者は再々委託の相手方に対して、本仕様書「１１．知的財産権の帰属等」、「１４．秘密保持等」、「１５．情報セキュリティに関する受託者の責任」、「１６．個人情報保護法に関する事項」を含め、本業務の受託者と同等の義務を負わせるものとし、再委託の相手方との契約においてその旨を定めるものとする。

受託者は、振興会が承認した再々委託の内容について変更しようとする時は、変更する事項及び理由等について記載した書面を提出し、振興会の承認を得るものとする。

１４．秘密保持等

受託者は、本業務を実施するに当たり、振興会から取得した資料（電子媒体、文書、図面等の形態を問わない。）を含め業務上知り得た情報を、第三者に開示又は本業務以外の目的で利用しないものとする。ただし、次の①から⑤のいずれかに該当する情報は除くものとする。

① 振興会から取得した時点で、既に公知であるもの
② 振興会から取得後、受託者の責によらず公知となったもの
③ 法令等に基づき開示されるもの
④ 振興会から秘密でないと指定されたもの
⑤ 第三者への開示又は本業務以外の目的で利用することにつき、事前に振興会に協議の上、承認を得たもの

受託者は、振興会の許可なく、取り扱う情報を指定された場所から持ち出し、又は複製しないものとする。

受託者は、本業務に関与した受託者の従業員が異動した後においても、機密が保持される措置を講じるものとする。

受託者は、本業務に係る検収後、受託者の事業所内部に保有されている本業務に係る振興会に関する情報を、裁断等の物理的破壊、消磁その他復元不可能な手法により、速やかに抹消するとともに、振興会から貸与されたものについては、検収後１週間以内に振興会に返却するものとする。

１５．情報セキュリティに関する受託者の責任

（１）情報セキュリティポリシー等の遵守

受託者は、「政府機関等のサイバーセキュリティ対策のための統一基準（令和７年度版）」及び「独立行政法人日本芸術文化振興会情報セキュリティポリシー」（以下「セキュリティポリシー等」という。）に従って受託者組織全体のセキュリティを確保すること。「独立行政法人日本芸術文化振興会情報セキュリティポリシー」（以下「振興会情報セキュリティポリシー」という。）は非公開であるが、「政府機関等のサイバーセキュリティ対策のための統一基準（令和７年度版）」等を、必要に応じて参照すること。「振興会情報セキュリティポリシー」については、契約締結後、受託者の求めにより開示する。

（２）情報セキュリティを確保するための体制の整備

(a) 受託者は、セキュリティポリシー等に従い、受託者組織全体のセキュリティを確保するとともに、振興会から求められた当該業務の実施において情報セキュリティを確保するための体制を整備すること。当該体制には、識別・防御・検知・対応・復旧を例とした、準備から事後処理に至る全般的なインシデント対処プロセスを確立していることを含む。

(b) 振興会から求められた本業務の実施において、機密性の確保が求められる情報を取り扱うことを踏まえ、以下の例を参考に、本業務の実施において情報システムを使用する場合に実装すべきセキュリティ機能を定めること。

・主体認証機能
・アクセス制御機能
・権限管理機能
・ログ管理機能
・暗号化
・運用管理機能

(c) 情報システムやアプリケーションプログラムの開発・運用・保守等の情報システムに関する業務の受託者においては、本業務の実施において、以下の対応を行うこと。

・当該情報システムに対して振興会の意図しない変更が行われないことを保証する管理が、一貫した　品質保証体制の下でなされること。また、当該品質保証体制が書類等で確認できること。
・当該情報システムに振興会支給外の端末を接続する場合には、適切な情報セキュリティ対策が講じられた端末を用いること。また、対策の実施状況については、振興会の求めに応じて説明が可能なこと。
・情報システムに導入するソフトウェア等について、導入・構築時のみならず運用・保守期間中に発覚した脆弱性に対処すること。

(d) 受託者は、取り扱う情報の可用性、通信の速度及び安定性、データの保存期間及び方法、データ交換の安全性及び信頼性確保のための方法等を定めて振興会と協議の上、これを実施すること。

(e) 受託者は、自らの資本関係・役員等の情報、本業務の実施場所、本業務に従事する者の所属・専門性（情報セキュリティに係る資格（情報処理安全確保支援士等）・研修実績等）・実績及び国籍に関する情報提供を行うこと。

(f) 受託者は、情報セキュリティに係る業務及び責務の遂行に必要な訓練等を受講した者を、本業務に参加させること。

（g）受託者は、セキュリティポリシー等に従い、情報セキュリティを確保できる環境において、本業務を実施すること。

（３）試験の実施

（a）受託者は、取り扱う情報の格付け及び取扱制限、業務の特性等を踏まえ、以下を例とする情報セキュリティの観点に基づくテストを行うこと。また実施したテストの記録を保存すること。

・想定の範囲外のデータの入力を拒否できるか

・サービス不能攻撃等により情報システムが過負荷状態に陥った場合に処理中のデータは保証されるか、レースコンディションが発生しないか

（b）テストの実施に伴い、運用中の振興会の情報システムに影響を及ぼさないこと。

（c）要機密情報をテストデータとしないこと。

（４）開発環境及び開発工程

ソースコードが不正に変更・消去されることを防ぐために、以下の事項を含むソースコードの管理を適切に行うこと。

（a）ソースコードの変更管理

（b）ソースコードの閲覧制限のためのアクセス制御

（c）ソースコードの滅失、き損等に備えたバックアップの取得

（５）情報セキュリティが侵害された場合の対処

本業務の遂行において、情報セキュリティが侵害され、又はその恐れがある場合には、直ちに振興会に報告し、当該事象の解消に向けた措置を講ずること。これに該当する場合には、以下の事象を含む。

①受託者に提供し、又は受託者によるアクセスを認める振興会の情報の外部への漏洩及び目的外利用

②受託者による振興会のその他の情報へのアクセス

③情報セキュリティが侵害され、又はその恐れがある事象が本業務に係る作業中及び契約に定める契約不適合責任の期間中に発生し、かつその事象が受託者における情報セキュリティ上の問題に起因する場合は、受託者の責任及び負担において次の各事項を速やかに実施すること。

a. 情報セキュリティ侵害の内容及び影響範囲を調査の上、当該情報セキュリティ侵害への対応策を立案し、振興会の承認を得た上で実施すること。

b. 発生した事態の具体的内容、原因及び実施した対応策等について報告書を作成し、振興会へ提出して承認を得ること。

c. 再発防止対策を立案し、振興会の承認を得た上で実施すること。

d. 上記のほか、発生した情報セキュリティ侵害について、振興会の指示に基づく措置を実施すること。

（６）情報セキュリティ監査の実施

本業務の遂行における情報セキュリティ対策の履行状況を確認するために、振興会が情報セキュリティ監査の実施を必要と判断した場合は、振興会がその実施内容（監査内容、対象範囲、実施等）を定めて、情報セキュリティ監査を行う（振興会が選定した事業者による監査を含む。）。

（７）履行状況の確認、改善

(a) 受託者は、本件において講ずる情報セキュリティ対策その他契約の履行状況について、定期的に報告すること。

(b) 受託者は、本業務における情報セキュリティ対策の履行状況について振興会が改善を求めた場合には、振興会と協議の上、必要な改善策を立案して速やかに実施するものとする。

１６．個人情報保護法に関する事項

受託者は、「個人情報の保護に関する法律（平成 15 年法律第 57 号)」又は、当該法律を遵守するために受託者が定めた個人情報保護に関するガイドライン等を遵守し、個人情報を取り扱うこと。

１７．その他

（１）振興会は、受託者による本業務の実施に関し指導監督を行う。

（２）受託者は、本業務の実施に疑義が生じた場合又は本業務の実施に支障が生じた場合には遅滞なく振興会に報告を行わなければならない。

（３）振興会は受託者に対し、本業務の実施状況の報告を求め、必要に応じ改善等の指導及び助言を行うことができるものとする。

（４）受託者は、本業務の事務実施体制の大幅な変更等、本業務の実施に影響を及ぼす事情が生じたときは、速やかに振興会に報告しなければならない。

（５）受託者は、業務により取得した報告書・証憑類等を整理し、本業務が完了した日の属する会計年度の終了後５年間、振興会の要求があったときは、いつでも閲覧に供することができるよう保存しておかなければならない。

（６）振興会は、受託者の業務終了後であっても、業務の実施に疑義が生じたときは、報告を求める場合があるものとする。

（７）仕様書及び契約書に記載されていない事項については、民法その他関係法令に則り、振興会と協議の上決定すること。

別紙　ISMAP管理基準に基づくセキュリティ要件一覧

①全ての要求事項に対して「可否」欄に〇か×を入力すること。×を入力する場合は、「×の場合の代替措置」欄も合わせて記入すること。
②組織としてISO27001を取得している場合は、「ISO27001適用」欄に〇が付いている項目は「可否」欄にISOを入力したうえで確認を省略できる。
③回答・代替措置の内容について、根拠資料の提出を求めることがある。

No.	要件概要	可否	×の場合の代替措置	ISO 27001 適用	ISMAP管理基準		
					管理策番号	要件	管理基準区分
―	―			―	3	情報セキュリティガバナンス	ガバナンス基準
―	―			―		情報セキュリティガバナンスは、組織の情報セキュリティ活動を指導し、管理するシステムである。情報セキュリティの目的及び戦略を、事業の目的及び戦略に合わせて調整する必要があり、法制度、規制及び契約を遵守する必要がある。また、情報セキュリティガバナンスは、内部統制の仕組みによって遂行されるリスクマネジメント手法を通じて、評価、分析及び実施する。	
―	―			―	3.1	情報セキュリティガバナンスのプロセス	
―	―			―	3.1.1	概要	
―	―			―		経営陣は、情報セキュリティを統治するために、評価、指示、モニタ及びコミュニケーションの各プロセスを実行する。さらに、保証プロセスによって、情報セキュリティガバナンス及び達成したレベルについての独立した客観的な意見が得られる。	
1	組織全体として情報セキュリティの対策を確実に遂行するための体制を整備している。また、経営陣は、管理者に対して優先度に即した対応を行わせるなど、重大な情報セキュリティプロジェクトの進捗を管理している。			無	3.1.2	評価	
						評価とは、現在のプロセス及び予定している変更に基づくセキュリティ目的の現在及び予想される達成度を考慮し、将来の戦略的目的の達成を最適化するために必要な調整を決定するガバナンスプロセスである。 “評価”プロセスを実施するために、経営陣は、次のことを行う。	
					3.1.2.1	経営陣は、事業の取組みにおいて情報セキュリティ問題を考慮することを確実にする。 ・経営陣は、管理者に、情報セキュリティが事業目的を十分にサポートし、支えることを確実にさせる。	
					3.1.2.2	経営陣は、情報セキュリティのパフォーマンス結果に対応し、必要な処置の優先順位を決めて開始する。	
					3.1.2.3	経営陣は、管理者に、重大な影響のある新規情報セキュリティプロジェクトを経営陣に付託するようにさせる。	
2	経営陣は、情報セキュリティ戦略及び方針を事業目的に合わせて策定・実施させており、積極的にセキュリティを順守する文化を醸成している。また、リスクマネジメントも適切に行い、必要な投資及び資源の配分を行っている。			無	3.1.3	指示	
						指示は、経営陣が、実施する必要がある情報セキュリティの目的及び戦略についての指示を与えるガバナンスプロセスである。指示には、資源供給レベルの変更、資源の配分、活動の優先順位付け並びに、方針、適切なリスク受容及びリスクマネジメント計画の承認が含まれる。 “指示”プロセスを実施するために、経営陣は次のことを行う。	
					3.1.3.1	経営陣は、その組織のリスク選好を決定する。	
					3.1.3.2	経営陣は、情報セキュリティの戦略及び方針を承認する。 (ア)経営陣は、管理者に、情報セキュリティの戦略及び方針を策定・実施させる。 (イ)経営陣は、管理者に、情報セキュリティの目的を事業目的に合わせて調整させる。	
					3.1.3.3	経営陣は、適切な投資及び資源を配分する。	
					3.1.3.4	経営陣は、管理者に、情報セキュリティに積極的な文化を推進させる。	
3	経営陣は、情報セキュリティの措置状況を必要に応じて確認し、環境の変化を考慮しつつ、組織内部及び外部（法令・規制等も含む）が必要とするセキュリティ要件に常に適合できるようにしている。			無	3.1.4	モニタ	
						モニタは、経営陣が戦略的目的の達成を評価することを可能にするガバナンスプロセスである。 “モニタ”プロセスを実施するために、経営陣は次のことを行う。	
					3.1.4.1	経営陣は、情報セキュリティマネジメント活動の有効性を評価する。 (ア)経営陣は、管理者に、事業の観点から適切なパフォーマンス指標を選択させる。 (イ)経営陣は、管理者に、経営陣が以前に特定した措置の実施及びそれらの組織への影響を含む、情報セキュリティのパフォーマンス成果についてのフィードバックを経営陣へ提供させる。	
					3.1.4.2	経営陣は、内部及び外部の要求事項への適合性を確実にする。	
					3.1.4.3	経営陣は、変化する事業、法制度、規制の環境、及びそれらの情報リスクへの潜在的影響を考慮する。	
					3.1.4.4	経営陣は、管理者に、情報リスク及び情報セキュリティに影響する新規開発案件について、経営陣に対し注意を喚起させる。	
4	経営陣は、事業特性に見合った情報セキュリティのレベルを実践していることを明示している。また、振興会が要求するセキュリティ事項を認識し、組織として対応を行うことができる体制をもっている。			無	3.1.5	コミュニケーション	
						コミュニケーションは、経営陣及び利害関係者が、双方の特定のニーズに沿った情報セキュリティに関する情報を交換する双方向のガバナンスプロセスである。 コミュニケーションの方法の一つは、情報セキュリティの活動及び課題を利害関係者に説明する情報セキュリティ報告書である。 “コミュニケーション”プロセスを実施するために、経営陣は次のことを行う。	
					3.1.5.1	経営陣は、外部の利害関係者に、組織がその事業特性に見合った情報セキュリティのレベルを実践していることを報告する。	
					3.1.5.2	経営陣は、管理者に、情報セキュリティ課題を特定した外部レビューの結果を通知し、是正処置を要請する。	
					3.1.5.3	経営陣は、情報セキュリティに関する規制上の義務、利害関係者の期待及び事業ニーズを認識する。	
					3.1.5.4	経営陣は、管理者に、注意が必要な問題、また、できれば決定が必要な問題について、経営陣へ助言させる。	
					3.1.5.5	経営陣は、管理者に、関連する利害関係者に対し、経営陣の方向性及び決定を支援するためにとるべき詳細な行動を、経営陣の方向性及び決定に沿って説明させる。	

5	必要な情報セキュリティ水準を確保していることを客観的に証明するために、外部機関による監査を行っている。			無	3.1.6	保証	
						保証は、経営陣が独立した客観的な監査、レビュー又は認証を委託するガバナンスプロセスである。これは、望ましいレベルの情報セキュリティを達成するためのガバナンス活動の実行及び運営の遂行に関連した目的及び処置を特定し、妥当性を検証する。 “保証”プロセスを実施するために、経営陣は次のことを行う。	
					3.1.6.1	経営陣は、要求している情報セキュリティ水準に対し、どのように説明責任を果たしているかについて、独立した客観的な意見を監査人等に求める。	
					3.1.6.2	経営陣は、管理者に、経営陣が委託する監査、レビュー又は認証をサポートさせる。	
—	—			—	4.1	マネジメント基準	マネジメント基準
—	—			—		マネジメント基準は、JIS Q 27001:2014を基に、情報セキュリティについて組織を指揮統制するために調整された活動である情報セキュリティマネジメントを確立、導入、運用、監視、維持及び改善するための基準を定める。マネジメント基準は、原則としてすべて実施しなければならないものである。	
—	—			—	4.2	記載内容について	
—	—			—		「情報セキュリティ管理基準」の「マネジメント基準」に同じ。 クラウドサービスにおいては、クラウドサービス利用者の環境等を考慮して、クラウドサービス提供者の管理策等を検討し、実施する必要がある。そのため、クラウドサービス利用者及びクラウドサービス事業者間において、クラウドサービスにおける情報セキュリティリスクとその対応について、情報交換することが非常で重要である。 当該情報セキュリティリスクコミュニケーションについては、クラウドサービスにおいて特に考慮するべき事項として、4.9章に規定する。	
—	—			—	4.3	凡例	
—	—			—		2.3章以降は、以下の構成をとる。 2.3　情報セキュリティマネジメント確立　[27001-4] 2.3.1　組織の役割、責任及び権限　[27001-5.3 / 5.1] 2.3.1.1　トップマネジメントは、情報セキュリティマネジメントに関するリーダーシップ及びコミットメントを発揮する。　[27001-5.1b) / 5.1e) / 5.1f)] その際は、以下を行うこととする。 ・組織のプロセスへ、その組織が必要とする情報セキュリティマネジメント要求事項を統合する ：[27001-X.X.X]は、JIS Q 27001:2014において関連する条項(X.X.X)を示す。	
—	—			—	4.4	情報セキュリティマネジメントの確立 [27001-4.4]	
—	—			—		情報セキュリティマネジメントを確立するために、その基盤となる適用範囲を決定し、方針を確立する。これらをもとに、情報セキュリティリスクアセスメントを実施し、その対応を計画し実施する。それにより、組織が有効な情報セキュリティマネジメントを実施するための基盤作りを行う。	
6	組織は、情報セキュリティマネジメントが有効に行われるように、次の事項を実施している。 ・情報セキュリティ方針・計画等、経営会議等の議事録、内部監査の報告等に経営陣の情報セキュリティマネジメントの意思、判断、指示等を含めている。 ・達成すべきセキュリティの水準として、リスクレベルを経営陣が決定している。 ・内部監査において確認すべき事項に、経営陣が要求する情報セキュリティ要求事項等を含めている。 ・情報セキュリティ方針、リスクアセスメント等の策定、セキュリティ管理策の教育・普及、セキュリティ基準適合の監査、組織内及び経営陣への報告に関わる責任・権限を適切に設定している。 ・経営陣は、管理層がその責任の領域においてリーダーシップを発揮できるよう、管理層の役割を支援している。			○	4.4.1	組織の役割、責任及び権限 [27001-5.3 / 5.1]	
					4.4.1.1	トップマネジメントは、情報セキュリティマネジメントに関するリーダーシップ及びコミットメントを発揮する。　[27001-5.1b) / 5.1e) / 5.1f)] ・組織のプロセスへ、その組織が必要とする情報セキュリティマネジメント要求事項を統合する。 ・情報セキュリティマネジメントがその意図した成果を達成することを確実にする。 ・情報セキュリティマネジメントの有効性に寄与するよう人々を指揮し、支援する。 また、トップマネジメントがリーダーシップ及びコミットメントを発揮していることを以下により確認する。 ・経営会議等の議事録に、トップマネジメントの情報セキュリティマネジメントに関する意思、判断、指示等が記録されていること。 ・情報セキュリティ方針、情報セキュリティ目的及びそれを達成する計画を策定する際に、トップマネジメントの意思、判断、指示等が含まれていること。 ・達成すべきセキュリティの水準として、リスクレベルをトップマネジメントが決定していること。 ・リスクレベルに応じて選択したセキュリティ管理策を実施させる際に、トップマネジメントの意思、判断、指示等が含まれていること。 ・内部監査において確認すべき事項に、トップマネジメントが要求する情報セキュリティ要求事項等が含まれていること。 ・内部監査報告書やそれらに基づく是正処置、マネジメントビュー議事録等に、トップマネジメントの意思、判断、指示等が含まれていること。	
					4.4.1.2	トップマネジメントは、組織の役割について、以下の責任及び権限を割り当て、伝達する。 [27001-5.3] ・情報セキュリティマネジメントを、本管理基準の要求事項として適合させる。 ・情報セキュリティマネジメントのパフォーマンス評価をトップマネジメントに報告する。 また、情報セキュリティマネジメントを本管理基準の要求事項に適合させるために、以下のような責任・権限を割り当てていることを確認する。 ・セキュリティ要求事項を盛り込んだ情報セキュリティ方針等の文書を策定する責任・権限 ・リスクアセスメントにおいて、リスクを運用管理する責任･権限を持つリスク所有者 ・セキュリティ要求事項を満たす管理策を教育、普及させる責任・権限 ・セキュリティ要求事項を満たしているか監査する責任・権限 ・各プロセスの結果及び効果をトップマネジメントに報告する責任・権限 ・各プロセスの結果及び効果を組織内に周知する責任・権限	
					4.4.1.3	トップマネジメントは、管理層がその責任の領域においてリーダーシップを発揮できるよう、管理層の役割を支援する。 [27001-5.1h)] 管理層が、その職掌範囲、組織等において、リーダーシップを発揮できるよう、トップマネジメントは、管理層に、必要な権限を委譲していることを確認する。	

7	組織は、組織内外に存する以下の状況を明確にしている。 ・国際、国内、地方又は近隣地域を問わず、文化、社会、政治、法律、規制、金融、技術、経済、自然及び競争の環境 ・組織の目的に影響を与える主要な原動力及び傾向 ・外部ステークホルダとの関係並びに外部ステークホルダの認知及び価値観 ・統治、組織体制、役割及びアカウンタビリティ ・方針、目的及びこれらを達成するために策定された戦略 ・資源及び知識として見た場合の能力（例えば、資本、時間、人員、プロセス、システム及び技術） ・情報システム、情報の流れ及び意思決定プロセス（公式及び非公式の双方を含む。） ・内部ステークホルダとの関係並びに内部ステークホルダの認知及び価値観 ・組織文化 ・組織が採択した規格、指針及びモデル ・契約関係の形態及び範囲			○	4.4.2	組織及びその状況の理解 [27001-4.1]	
					4.4.2.1	組織は、組織の目的に関連し、かつ、情報セキュリティマネジメントの意図した成果を達成する組織の能力に影響を与える、以下の課題を決定する。[27001-4.1] ・外部の課題 ・内部の課題 これらの課題の決定とは、組織の外部状況及び内部状況の確定のことをいう。外部状況及び内部状況には、以下のようなものが含まれる。 a) 外部状況 ・国際、国内、地方又は近隣地域を問わず、文化、社会、政治、法律、規制、金融、技術、経済、自然及び競争の環境 ・組織の目的に影響を与える主要な原動力及び傾向 ・外部ステークホルダとの関係並びに外部ステークホルダの認知及び価値観	
						b) 内部状況 ・統治、組織体制、役割及びアカウンタビリティ ・方針、目的及びこれらを達成するために策定された戦略 ・資源及び知識として見た場合の能力（例えば、資本、時間、人員、プロセス、システム及び技術） ・情報システム、情報の流れ及び意思決定プロセス（公式及び非公式の双方を含む。） ・内部ステークホルダとの関係並びに内部ステークホルダの認知及び価値観 ・組織文化 ・組織が採択した規格、指針及びモデル ・契約関係の形態及び範囲	
8	組織は、取引先、パートナー、サプライチェーン、グループ企業等、関係省庁等利害関係者からのニーズ及び期待を理解するために、以下を明確にしている。 ・情報セキュリティマネジメントに関連する利害関係者 ・利害関係者からの情報セキュリティに関連する法的及び規制の要求事項並びに契約上の義務			○	4.4.3	利害関係者のニーズ及び期待の理解 [27001-4.2]	
					4.4.3.1	組織は、利害関係者のニーズ及び期待を理解するために、以下を決定する。 [27001-4.2] ・情報セキュリティマネジメントに関連する利害関係者 ・利害関係者の、情報セキュリティに関連する要求事項 利害関係者の要求事項には、法的及び規制の要求事項並びに契約上の義務を含めてもよいが、利害関係者には、以下のようなものが含まれる。 ・組織内で情報セキュリティマネジメントプロセスを推進する役割・権限を持つ人又は組織。例えば、以下のようなものをいう。 -情報セキュリティに関する方針等を策定する人又は組織(トップマネジメント等) -セキュリティ管理策を全組織に徹底させる人又は組織(総務部、情報システム部等) -情報セキュリティ監査を行う人又は組織(監査室等) -組織内の情報セキュリティ専門家 ・取引先、パートナー、サプライチェーン上の関係者 ・親会社、グループ会社 ・当該組織のセキュリティを監督する省庁、政府機関 ・所属するセキュリティ団体、協会	
9	組織は、情報セキュリティマネジメントの適用範囲及び境界を以下の点を考慮して定義している。また、適用範囲の決定は、組織内外の状況に応じて適切に行っている。 ・自らの事業 ・体制 ・所在地 ・資産 ・技術の特徴 ・外部及び内部の課題 ・利害関係者の情報セキュリティに関連する要求事項 ・組織が実施する活動と他の組織が実施する活動との間のインタフェース及び依存関係			○	4.4.4	適用範囲の決定 [27001-4.3]	
						情報セキュリティマネジメントを確立、導入、運用、監視、レビュー、維持及び改善するために、まず適用範囲を明確にし、組織に合った情報セキュリティマネジメントを構築する基盤を整える。	
					4.4.4.1	組織は、情報セキュリティマネジメントの境界及び適用可能性を明確にし、適用範囲を決定する。 [27001-4.3] a) 組織は以下の点を考慮して適用範囲及び境界を定義する。 ・自らの事業 ・体制 ・所在地 ・資産 ・技術の特徴 ・外部及び内部の課題 ・利害関係者の情報セキュリティに関連する要求事項 ・組織が実施する活動と他の組織が実施する活動との間のインタフェース及び依存関係 b) 情報セキュリティマネジメントの目的や目標は、組織の特徴によって異なる。	
						c) 情報セキュリティマネジメントに対する要求事項はそれぞれの組織の事業によって、外部状況、内部状況の双方があり、これらを考慮して適用範囲を定義する。 ・外部状況には、以下のようなものが含まれる。 －国際、国内、地方又は近隣地域を問わず、文化、社会、政治、法律、規制、金融、技術、経済、自然及び競争の環境 －組織の目的に影響を与える主要な原動力及び傾向 －外部ステークホルダとの関係並びに外部ステークホルダの認知及び価値観 ・内部状況には、以下のようなものが含まれる。 －統治、組織体制、役割及びアカウンタビリティ －方針、目的及びこれらを達成するために策定された戦略 －資源及び知識として見た場合の能力（例えば、資本、時間、人員、プロセス、システム及び技術） －情報システム、情報の流れ及び意思決定プロセス（公式及び非公式の双方を含む。） －内部ステークホルダとの関係並びに内部ステークホルダの認知及び価値観 －組織文化 －組織が採択した規格、指針及びモデル －契約関係の形態及び範囲	

10	経営陣は、以下を踏まえた組織の情報セキュリティ方針を確立している。 ・組織の目的に対して適切である。 ・情報セキュリティ目的、又は情報セキュリティ目的を設定するための枠組を含める。 ・必要な情報セキュリティ対応についての言及を含める。 ・情報セキュリティマネジメントの見直しを適宜行う。 組織は、情報セキュリティの目的及びその達成計画を策定している。 目的は、情報セキュリティ方針と整合性があるものとし、測定できるようものとしている。また、リスクマネジメントを考慮に入れている。 計画では、次のことを決定している。 ・実施事項 ・必要な資源 ・責任者 ・達成期限 ・結果の評価方法 経営陣は、上記方針・目的を組織運営と矛盾しないように確立し、その方針を文書として記録し、承認を行っている。			○	4.4.5	方針の確立 [27001-5.2 / 6.2 / 5.1]	
					4.4.5.1	トップマネジメントは、以下を満たす組織の情報セキュリティ方針を確立する。 [27001-5.2] ・組織の目的に対して適切であること。 ・情報セキュリティ目的、又は情報セキュリティ目的を設定するための枠組 ・情報セキュリティに関連して適用する要求事項を満たすことへのコミットメントを含むこと。 ・情報セキュリティマネジメントの継続的改善へのコミットメントを含むこと。 また、情報セキュリティ方針は情報セキュリティマネジメントにおける判断の基盤となる考え方を記載したものであり、組織の戦略に従って慎重に作成する。	
					4.4.5.2	組織は、情報セキュリティ目的及びそれを達成するための計画を策定する。 [27001-6.2] a) 情報セキュリティ目的は、以下を満たすこととする。 ・情報セキュリティ方針と整合していること。 ・（実行可能な場合）測定可能であること。 ・適用される情報セキュリティ要求事項、並びにリスクアセスメント及びリスク対応の結果を考慮に入れること。 b) 情報セキュリティ目的は、関係者に伝達し、必要に応じて更新するとともに、情報セキュリティ目的を達成するための計画においては、以下を決定する。 ・実施事項 ・必要な資源 ・責任者 ・達成期限 ・結果の評価方法	
					4.4.5.3	トップマネジメントは、以下によって、情報セキュリティマネジメントに関するリーダーシップ及びコミットメントを発揮する。 [27001-5.1a)] ・情報セキュリティ方針及び情報セキュリティ目的を確立すること。 ・情報セキュリティ方針及び情報セキュリティ目的は組織の戦略的な方向性と相矛盾しないこと。 また、情報セキュリティ方針は組織に伝えられるように文書化され、しかるべき方法で利害関係者が入手できるようにするとともに、トップマネジメントが情報セキュリティ方針にコミットした証拠を、以下のような記録をもって示す。 ・文書化された情報セキュリティ方針への署名 ・情報セキュリティ方針が議論された会議の議事録 これらはトップマネジメントの責任を明確にするために実施する。	
11	組織は、対処すべきリスクを明確にし、その影響を恒久的に防止又は低減するための機会を設け、具体的な対応計画を立てている。計画立案については、その対応方法が有効であることを確認できるようにしている。			○	4.4.6	リスク及び機会に対処する活動 [27001-6.1]	
					4.4.6.1	リスク及び機会を決定する。 [27001-6.1.1] a) 組織は、外部及び内部の課題、利害関係者の情報セキュリティに関連する要求事項を考慮し、以下のために対処する必要があるリスク及び機会を決定する。 ・情報セキュリティマネジメントが、組織が意図した成果を達成する。 ・望ましくない影響を防止又は低減する。 ・継続的改善を達成する。 当該決定の際、組織は、以下を計画する。 ・決定したリスク及び機会に対処する活動 ・リスク及び機会に対処する活動の情報セキュリティマネジメントプロセスへの統合及び実施方法 ・リスク及び機会に対処する活動の有効性の評価方法 b) リスク及び機会に対処する活動の記録として、具体的な対処計画（実施時期、実施内容、実施者、実施場所、実施に必要な資源などを規定した計画）を作成していることを確認するとともに、当該計画を作成する際、各対処計画が、情報セキュリティマネジメントプロセスの一部として実施されるよう、考慮するとともに、当該対処の有効性を評価する方法（実施状況や実施したことによる効果を評価する方法）を作成していることも確認する。	

12	組織は、リスク受容基準並びにリスクアセスメント実施基準を定めている。 受容基準は組織の価値観、目的、資源を含め、以下を考慮して定めており、アセスメントの結果は、客観的に一貫性及び妥当性がある。 ・原因及び発生し得る結果の特質及び種類、並びにこれらの測定方法 ・発生頻度、結果を考える時間枠 ・リスクレベルの決定方法 ・利害関係者の見解 ・組織に課せられるもの又は策定されるものであること また、情報セキュリティリスクを、以下を考慮のうえ、リスク所有者毎に特定し、それらが発生した場合の結果の分析および、評価を行っている。 ・リスク源 が組織の管理下にあるか否かに関わらず、リスク源又はリスクの原因が明らかでないリスクも特定の対象とする。 ・波及効果及び累積効果を含めた、特定の結果の連鎖を注意深く検討する。 ・何が起こり得るのかの特定に加えて、考えられる原因及びどのような結果が引き起こされることがあるのかを示すシナリオ ・全ての重大な原因及び結果 ・リスク源、影響範囲・結果 なお、リスク対応の優先順位を決定する際には、他者が負うリスクの受容レベルについても考慮するとともに、法令、規制、その他の要求事項についても考慮している。			○	4.4.7	情報セキュリティリスクアセスメント [27001-6.1.2]	
					4.4.7.1	組織は、以下によって、情報セキュリティリスクアセスメントのプロセスを定め、適用する。 [27001-6.1.2a) / 6.1.2b)] a) 以下を含む情報セキュリティのリスク基準を確立し、維持する。 ・リスク受容基準 ・情報セキュリティリスクアセスメントを実施するための基準	
						b) リスク受容基準に、以下を反映するよう、考慮する。 ・組織の価値観 ・目的 ・資源	
						c) リスク受容基準を策定する際には、以下の点を考慮する。 ・原因及び発生し得る結果の特質及び種類、並びにこれらの測定方法 ・発生頻度 ・発生頻度、結果を考える時間枠 ・リスクレベルの決定方法 ・利害関係者の見解 ・リスク基準は、法令及び規制の要求事項、並びに組織が合意するその他の要求事項によって、組織に課せられるもの又は策定されるものもあること。	
						d) 情報セキュリティアセスメントを繰り返し実施した際に、以下の結果を生み出すこと。 ・情報セキュリティリスクアセスメントの結果に、一貫性及び妥当性があること。 ・情報セキュリティリスクアセスメントの結果が比較可能であること。 　なお、情報セキュリティマネジメントにおけるリスクアセスメント手法には、定番といえるものがなく、それぞれの組織に適合したものを選択している場合が多いことから、必要に応じてツールを利用するなどが必要になる。	
					4.4.7.2	組織は、以下によって、情報セキュリティリスクを特定する。 [27001-6.1.2c)] a) 情報セキュリティリスクアセスメントのプロセスを適用し、情報の機密性、完全性及び可用性の喪失に伴うリスクを特定する。 b) リスクを特定する過程において、リスク所有者を特定する。 c) リスクを特定する際には、以下について考慮する。 ・リスク源 が組織の管理下にあるか否かに関わらず、リスク源又はリスクの原因が明らかでないリスクも特定の対象にすること。 ・波及効果及び累積効果を含めた、特定の結果の連鎖を注意深く検討すること。 ・何が起こり得るのかの特定に加えて、考えられる原因及びどのような結果が引き起こされることがあるのかを示すシナリオ ・全ての重大な原因及び結果 ・以下を特定すること。 　－リスク源 　－影響を受ける領域、事象 　－原因及び起こり得る結果 　この段階で特定されなかったリスクは、今後の分析の対象から外されてしまうため、ある機会を追及しなかったことに伴うリスクも含め、リスクの包括的な一覧を作成する。	
					4.4.7.3	組織は、以下によって、情報セキュリティリスクを分析する。 [27001-6.1.2d)] a) 以下の手順によりリスク分析を行う。 ・特定されたリスクが実際に生じた場合に起こり得る結果の分析を行う。 ・特定されたリスクの発生頻度の分析を行う。 ・リスクレベルを決定する。 ・特定した脅威やぜい弱性を基に、以下の点を考慮する。 －セキュリティインシデントが発生した場合の事業影響度 －セキュリティインシデントの発生頻度 －管理策が適用されている場合はその効果 b) リスク分析の際には、以下の点についても考慮する。 ・リスクの原因及びリスク源 ・リスクの好ましい結果及び好ましくない結果 ・リスクの発生頻度 ・リスクの結果及び発生頻度に影響を与える要素 　なお、リスク分析は、状況に応じて、定性的、半定量的、定量的、又はそれらを組み合わせた手法で行うことが可能である。	
					4.4.7.4	組織は、以下によって、情報セキュリティリスクを評価する。 [27001-6.1.2e)] ・リスク分析の結果、決定されたリスクレベルとリスク基準との比較をする。 ・リスク対応のための優先順位付けを行う。 ・リスク評価の結果は今後の改善に利用するため保管する。 　なお、リスク対応の優先順位を決定する際には、より広い範囲の状況を考慮し、他者が負うリスクの受容レベルについて考慮するとともに、法令、規制、その他の要求事項についても考慮する。	

13	組織は、情報セキュリティアセスメントの結果を考慮して、以下に示す情報セキュリティリスク対応の選択肢を選定している。 ・リスクを生じさせる活動を開始又は継続しないと決定することによるリスクの回避 ・ある機会を目的としたリスクの引受け又はリスクの負担 ・リスク源の除去 ・発生頻度の変更 ・結果の変更 ・（契約及びリスクファイナンス を含む）他者とのリスクの共有 ・情報に基づいた意思決定によるリスクの保有 また、選定した情報セキュリティリスク対応の実施に必要な全ての管理策を以下を考慮しつつ決定している。 ・リスクの受容可能レベル ・関連する法令 ・規制や契約上の要求事項 ・その他の社会的責任 加えて、組織は、以下を含む情報セキュリティリスク対応計画を策定している。残留リスクについては定期的に実施状況を踏まえた見直しを行い、経営陣や利害関係者に認識させている。 ・期待される効果を含む、対応選択肢選定の理由 ・情報セキュリティリスク対応計画の承認者及び対応計画の実施責任者 ・対応内容 ・必要な資源 ・費用・労力、制約 ・後日の報告、監視に必要な要求事項 ・対応工程における節目ごとの目標 ・対応時期及び日程 ・残留リスクが生じる場合は、技術的またはコスト的に対応可能になる時期			○	4.4.8	情報セキュリティリスク対応 [27001-6.1.3]	
					4.4.8.1	組織は、情報セキュリティアセスメントの結果を考慮して、適切な情報セキュリティリスク対応の選択肢を選定する。 [27001-6.1.3a)] 情報セキュリティリスク対応の選択肢には、以下が含まれる。 ・リスクを生じさせる活動を開始又は継続しないと決定することによるリスクの回避 ・ある機会を目的としたリスクの引受け又はリスクの負担 ・リスク源の除去 ・発生頻度の変更 ・結果の変更 ・（契約及びリスクファイナンス を含む）他者とのリスクの共有 ・情報に基づいた意思決定によるリスクの保有 　さらに、リスク対応の評価や改善に役立てるため、どの選択肢を選んだ場合も、その理由を明確にし、記載する。	
					4.4.8.2	組織は、選定した情報セキュリティリスク対応の実施に必要な全ての管理策を決定する。 [27001-6.1.3b)] 　リスク対応のための方針を決めた上で、管理策の目的（管理目的）及び管理策について検討する。以下を考慮しつつ、対応による効果と対応に必要な費用及び労力のバランスを取り、適切な情報セキュリティ対応の選択肢を選定する。 ・リスクの受容可能レベル ・関連する法令 ・規制や契約上の要求事項 ・その他の社会的責任 　なお、具体的な管理策の選定においては、管理目的に対応した「管理策基準」から適切なものを選択するが、「管理策基準」はすべてを網羅しているわけではないので、組織の事業や業務などによってその他の管理策を追加してもよい 。	
					4.4.8.3	組織は、管理策が見落とされていないことを検証する。 [27001-6.1.3c)] 　必要な管理策の見落としがないか、管理策基準を参照するが、管理策基準に示す管理目的及び管理策以外の管理目的及び管理策が必要になった場合、他の管理目的及び管理策を追加することができる。	
					4.4.8.4	組織は、情報セキュリティリスク対応計画を策定する。 [27001-6.1.3e)] a)情報セキュリティリスク対応計画には、以下を含む。 ・期待される効果を含む、対応選択肢選定の理由 ・情報セキュリティリスク対応計画の承認者及び対応計画の実施責任者 ・対応内容 ・必要な資源 ・費用・労力、制約 ・後日の報告、監視に必要な要求事項 ・対応工程における節目ごとの目標 ・対応時期及び日程	
						b) 責任及び権限について 　情報セキュリティマネジメントにおいては最終的な承認をトップマネジメントが行っていることがほとんどであり、責任がトップマネジメントに集中している。 一方で、情報セキュリティリスクアセスメント及びリスク対応については、責任及び権限を持つリスク所有者が、責任及び権限を持つ。 リスク所有者は、トップマネジメント、又はトップマネジメントから任命され、責任及び権限が委譲された者であることが多いことから、情報セキュリティマネジメントにおいて、トップマネジメント及びリスク所有者が、どのような責任を持つかについて明確にする。	
					4.4.8.5	組織は、リスク所有者から、情報セキュリティリスク対応計画について承認を得、かつ、リスク所有者に、残留している情報セキュリティリスクを受け入れてもらう。 [27001-6.1.3f)] すべてのリスクについて管理目的や管理策を選択した時点で、残留リスクについて明確にし、今後の対応計画を作成する。計画の作成においては以下の点について考慮する。 ・技術的に対応可能になる時期 ・コスト的に対応可能になる時期 　残留リスクについては、定期的に見直しを行い、必要に応じて、対応の対象とするとともに、リスク対応後の残留リスクについては、リスク所有者のほか、経営陣やその他の利害関係者に認識させることを考慮する。 　また、リスク所有者の責任を明確にするために、承認された会議の議事録を正しく保管する。	

—	—			—	4.5	情報セキュリティマネジメントの運用 [27001-8]	
14	組織は、情報セキュリティマネジメントの確立、実施、維持及び継続的改善に必要な資源（人、組織、設備、システム、費用等）を決定し、提供している。			○	4.5.1	資源管理 [27001-7.1 / 5.1]	
					4.5.1.1	組織は、情報セキュリティマネジメントの確立、実施、維持及び継続的改善に必要な資源を決定し、提供する。 [27001-7.1] 管理目的を満たすためには、継続的に管理策を実施するとともに、人員の増加、システムの増加などの環境の変化に対応するために、適切な時期に適切に提供できるよう、経営資源を確保する。	
					4.5.1.2	トップマネジメントは、情報セキュリティマネジメントに必要な資源が利用可能であることを確実にするため、以下のような資源を割り当てる。 [27001-5.1c)] ・情報セキュリティマネジメントの各プロセスに必要な人又は組織 ・情報セキュリティマネジメントの各プロセスに必要な設備、装置、システム ・上記に必要な費用	
15	経営陣は、情報セキュリティマネジメントの重要性を組織内に伝達し、協力体制及び連絡を明確に行うための体制を構築している。 情報セキュリティマネジメントに関連する業務及び影響のある業務を特定したうえで、役割を明確にした業務分掌を以下の点を考慮して作成している。随時見直しを行いつつ、業務が円滑に行えるようにしている。 ・役職名 ・業務内容 ・担当者の責任範囲 ・業務に必要な知識 ・業務に必要な資格 ・業務に必要な経験 また、教育・訓練を行い、必要なスキルを取得させている。教育・訓練はその計画を事前に策定し、経営陣の承認を得たうえで実施し、確認のテストや結果の評価を行っている。 加えて、各自は、情報セキュリティマネジメントにおけるそれぞれの役割、役割を実行するための業務と手順を認識しており、これらは文書で随時確認することができる。			○	4.5.2	カ量、認識 [27001-7.2 / 7.3 / 5.1]	
					4.5.2.1	トップマネジメントは、有効な情報セキュリティマネジメント及びその要求事項への適合の重要性を伝達する。 [27001-5.1d)] トップマネジメントは情報セキュリティマネジメントについて責任を負うが、実施においては組織全体の協力が必要であることを、情報セキュリティ方針と共に関係者に伝える。 また、組織が同じ規定に従って同じ判断ができるように、情報分類等の基準を策定するが、個人情報のように組織によって解釈が一部異なる情報の場合は、一般的な考え方に加え、自社の考え方を明確にした上で、関係者に伝える。	
					4.5.2.2	組織は、組織の情報セキュリティパフォーマンスに影響を与える業務をその管理下で行う人（又は人々）に必要な力量を決定する。 [27001-7.2a)] 情報セキュリティマネジメントに関係する業務及び影響のある業務を特定し、役割を明確にした業務分掌を作成する。これらの業務分掌においては以下の点を明確にする。 ・役職名 ・業務内容 ・担当者の責任範囲 ・業務に必要な知識 ・業務に必要な資格 ・業務に必要な経験 知識や資格、経験などは環境や目的の変化によって変更される可能性があるため、最新の情報となるように随時見直しを行う。	
					4.5.2.3	組織は、適切な教育、訓練又は経験に基づいて、組織の情報セキュリティパフォーマンスに影響を与える業務をその管理下で行う人（又は人々）が力量を備えられるようにする。 [27001-7.2b)] 適用される処置には、例えば、現在雇用している人々に対する教育訓練の提供、指導の実施、配置転換の実施などがある（教育や訓練などが間に合わないと判断される場合には相応の力量を有した要員の雇用が、また、社内業務との関連が少ない業務においては外部委託などがある。）。	
					4.5.2.4	組織は、必要な力量を身に着けるための処置をとり、とった処置の有効性を評価する。 [27001-7.2c)] 必要な力量を身に着けるための処置としては、教育訓練が重要である。教育は「必要な知識を得させる」、訓練は「必要なスキル及び経験を得させる」ために実施する。教育の内容は一般的な脅威やぜい弱性などの知識だけではなく、業務上のリスクについてなど、組織の特徴を反映した内容を盛り込むなど、実効性のある内容となるようにする。 教育及び訓練を実施した結果、必要な力量が持てたかどうかを確認するために、以下を実施する。 ・知識の確認テスト ・スキルの実習テスト ・チェックリストなどによるベンチマーク 実施結果については記録し、要員選択の客観性を確保する。	
					4.5.2.5	組織は、力量を常に把握し、その証拠として、適切な文書化した情報を組織が定めた期間保持する。 [27001-7.2d)] 教育、訓練については以下を検討し、定期的に実施する。 ・教育・訓練基本計画 ・教育・訓練実施計画 ・確認テスト又は評価報告 教育や訓練の一部を免除する場合は、それがどの技能や経験、資格に当てはまるかを明確にし、それぞれの担当者について調査し、一覧にする。資格については有効期限などを明確にし、更新する。	
					4.5.2.6	組織の管理下で働く人々は、情報セキュリティ方針を認識する。 [27001-7.3a)] 情報セキュリティの活動について、組織が定めた目的と重要性について、情報セキュリティ方針の通達や教育の一環として周知徹底することによって、管理策がなぜ実施されているのかについての関係者の理解を深める。	
					4.5.2.7	組織の管理下で働く人々は、情報セキュリティパフォーマンスの向上によって得られる便益を含む、情報セキュリティマネジメントの有効性に対する自らの貢献を認識する。 [27001-7.3b)] 以下の点について組織の管理下で働く人々に伝えることによって、各人の役割及び情報セキュリティマネジメントの有効性に対する自らの貢献を明確にする。 ・情報セキュリティマネジメントにおけるそれぞれの役割 ・役割を実行するための業務と手順（異常を検知した場合の報告手順も含む。） ・これらが記載された文書の所在	
					4.5.2.8	組織の管理下で働く人々は、情報セキュリティマネジメントの要求事項に適合しないことの意味を認識する。 [27001-7.3c)]	

16	内部（経営陣、管理者、一般従業員等）及び外部（取引先、グループ会社、関係省庁等）とのコミュニケーションを行う際は、以下を考慮している。 ・コミュニケーションの内容（何を伝達するか。） ・コミュニケーションの実施時期 ・コミュニケーションの対象者 ・コミュニケーションの実施者 ・コミュニケーションの実施プロセス			○	4.5.3	コミュニケーション [27001-7.4]	
					4.5.3.1	組織は、情報セキュリティマネジメントに関連する内部及び外部のコミュニケーションを実施する必要性を決定する。 [27001-7.4] a) 内部及び外部のコミュニケーションを実施する際は、以下を考慮することとする。 ・コミュニケーションの内容（何を伝達するか。） ・コミュニケーションの実施時期 ・コミュニケーションの対象者 ・コミュニケーションの実施者 ・コミュニケーションの実施プロセス	
						b) 内部コミュニケーションでは、以下に示すような者と、適宜及び定期的なコミュニケーションを実施する。 ・トップマネジメント ・情報セキュリティマネジメントを本管理基準の要求事項に適合させる権限者 ・情報セキュリティマネジメントのパフォーマンスをトップマネジメント又は組織内に報告する権限者 ・組織内の従業員	
						c) 外部コミュニケーションでは、以下に示すような者と、必要に応じて、コミュニケーションを実施する。 ・取引先、パートナー、サプライチェーン上の関係者 ・親会社、グループ会社 ・当該組織のセキュリティを監督する省庁、政府機関 ・所属するセキュリティ団体、協会	
17	組織は、計画通りに情報セキュリティ目的を達成するための施策を実施していることを示すため、以下の内容を文書化している。 ・管理策の実施状況 ・管理策の有効性 ・管理策を取り巻く環境の変化 これらの情報は、組織内でレビューされ、適切に行われているかを判断できるようにしている。 また、外部委託を行うプロセスについても管理している。			○	4.5.4	情報セキュリティマネジメントの運用の計画及び管理 [27001-8.1]	
					4.5.4.1	組織は、情報セキュリティ要求事項を満たすため、リスク及び機会に対処する活動を実施するために必要なプロセスを計画し、実施し、かつ管理する。 [27001-8.1]	
					4.5.4.2	組織は、情報セキュリティ目的を達成するための計画を実施する。 [27001-8.1]	
					4.5.4.3	組織は、計画通りに実施されたことを確信するために、文書化した情報を保持する。 [27001-8.1] 文書化した情報に、以下の情報が集められているかどうかを確認する。 ・管理策の実施状況 ・管理策の有効性 ・管理策を取り巻く環境の変化 また、これらの情報を把握し判断する体制を構築する。	
					4.5.4.4	組織は、計画した変更を管理し、意図しない変更によって生じた結果をレビューし、必要に応じて、有害な影響を軽減する処置をとる。 [27001-8.1]	
					4.5.4.5	組織は、外部委託するプロセスを決定し、かつ、管理する。 [27001-8.1]	
18	組織は、定期的、重大な変更が提案された場合または重大な変化が生じた場合のいずれかにおいて、情報セキュリティリスクアセスメントを実施している。 また、組織は、情報セキュリティリスク対応計画を以下を考慮しつつ実施しており、効果測定を行うための予算化もしている。 ・管理策の導入及び運用にかかる費用、人員、作業工数、技術 ・セキュリティインシデント発生時の一時対応にかかる費用 ・その他のリスク対応にかかる費用			○	4.5.5	情報セキュリティリスクアセスメントの実施 [27001-8.2 / 8.3]	
					4.5.5.1	組織は、以下のいずれかの場合において、情報セキュリティリスクアセスメントを実施する。 [27001-8.2] ・あらかじめ定めた間隔 ・重大な変更が提案された場合 ・重大な変化が生じた場合	
					4.5.5.2	組織は、情報セキュリティリスク対応計画を実施する。 [27001-8.3] 情報セキュリティリスク対応計画の実施においては、明確にされた個々の責任について全うしていることを確認するための方策を講じる。	
					4.5.5.3	トップマネジメントは、情報セキュリティリスク対応計画のために十分な経営資源を提供する。 情報セキュリティリスク対応計画には相応の経営資源が必要になるところ、以下の点について考慮する。 ・管理策の導入及び運用にかかる費用、人員、作業工数、技術 ・セキュリティインシデント発生時の一時対応にかかる費用 ・その他のリスク対応にかかる費用 運用においては管理策の効果測定などを実施するために必要な経営資源について考察し、予算化する。	
—	—			—	4.6	情報セキュリティマネジメントの監視及びレビュー [27001-5.1 / 8.2 / 9 / 10.2]	
19	組織は、以下を実施し、情報セキュリティマネジメントの適切性、妥当性及び有効性を継続的に改善を行っている。 ・定期的な情報セキュリティリスクアセスメント ・定期的な情報セキュリティ内部監査 ・トップマネジメントによる定期的なマネジメントレビュー 経営陣は、改善のための役割、責任及び権限を割り当て、促進させている。			○	4.6.1	有効性の継続的改善 [27001-10.2 / 8.2 / 9.2 / 9.3 / 5.1]	
					4.6.1.1	組織は、以下を実施し、情報セキュリティマネジメントの適切性、妥当性及び有効性を継続的に改善する。 [27001-10.2 / 8.2 / 9.2 / 9.3] ・定期的な情報セキュリティリスクアセスメント ・定期的な情報セキュリティ内部監査 ・トップマネジメントによる定期的なマネジメントレビュー 継続的改善においては、これまで実施してきた管理策だけはなく、環境の変化に伴う新たな脅威やぜい弱性についても不適合を検出し処置する。	
					4.6.1.2	トップマネジメントは、継続的改善を促進する。 [27001-5.1g)] 4.6.1.1.を実施するための、役割、責任及び権限を割り当て、実施するよう関係者に伝達する。	

20	組織は、情報セキュリティパフォーマンス及び情報セキュリティマネジメントの有効性を継続的に評価し、以下を決定している。 ・必要とされる監視及び測定の対象（情報セキュリティプロセス及び管理策を含む。） ・妥当な結果を確実にするための、監視、測定、分析及び評価の方法（比較可能で再現可能な結果を生み出す方法とする。） ・監視及び測定の実施時期及び頻度 ・監視及び測定の実施者 ・監視及び測定の結果の、分析（因果関係、相関関係を含む）及び評価の時期及び頻度 ・監視及び測定の結果の、分析及び評価の実施者 ・分析及び評価の結果に応じた対応措置 ・分析及び評価の結果の報告頻度 組織は、定期的に内部監査を実施し、本マネジメント基準の要求事項及び組織自体が規定した要求事項に適合しているかを確認している。 内部監査を行うために、基本計画書において対象範囲、目的、管理体制及び期間又は期日についてを、実施計画において実施時期や実施場所、実施担当者及びその割当て及び詳細な監査の手法についてをあらかじめ定めている。予定通り実施されたことを証明するためにも、実施報告書を作成している。 監査計画においては、以下の内容を含む監査基準及び監査範囲を明確にしている。 ・目的、権限と責任 ・独立性、客観性と職業倫理 ・専門能力 ・業務上の義務 ・品質管理 ・監査の実施方法 ・監査報告書の形式 また、監査人の選定は、監査基準に従い、以下の点を考慮している。 ・外観上の独立性 ・精神上の独立性 ・職業倫理と誠実性 なお、監査結果は、関連する管理層に報告している。			○	4.6.2	パフォーマンス評価 [27001-9]	
					4.6.2.1	組織は、情報セキュリティパフォーマンス及び情報セキュリティマネジメントの有効性を継続的に評価し、以下を決定する。 [27001-9.1] ・必要とされる監視及び測定の対象（情報セキュリティプロセス及び管理策を含む。） ・妥当な結果を確実にするための、監視、測定、分析及び評価の方法（比較可能で再現可能な結果を生み出す方法とする。） ・監視及び測定の実施時期及び頻度 ・監視及び測定の実施者 ・監視及び測定の結果の、分析（因果関係、相関関係を含む）及び評価の時期及び頻度 ・監視及び測定の結果の、分析及び評価の実施者 ・分析及び評価の結果に応じた対応措置 ・分析及び評価の結果の報告頻度	
					4.6.2.2	組織は、あらかじめ定めた間隔で内部監査を実施する。 [27001-9.2a) / 9.2b)] a) 内部監査を実施する際は、以下を確認する。 ・以下に適合していること。 －情報セキュリティマネジメントに関して、組織自体が規定した要求事項 －本マネジメント基準の要求事項 ・情報セキュリティマネジメントが有効に実施され、維持されていること。	
						b) 内部監査は、管理策の有効性を総合的に確認するために定期的に実施し、計画及び結果について以下の文書で管理する。 ・内部監査基本計画 ・内部監査実施計画 ・内部監査報告書 基本計画書では対象範囲、目的、管理体制及び期間又は期日について、実施計画では実施時期や実施場所、実施担当者及びその割当て及び詳細な監査の手法についてあらかじめ決める。予定通り実施されたことを証明するためにも、実施報告書を作成する。	
						c) 適合性の監査においては、以下の項目を対象に含む。 ・関連する法令又は規制の要求事項 ・情報セキュリティリスクアセスメントなどによって特定された情報セキュリティ要求事項	
						d) 情報セキュリティマネジメントが有効に実施され、維持されていることの監査においては、以下の項目を対象に含む。 ・管理策の有効性及び維持 ・管理策が期待通りに実施されていること。	
					4.6.2.3	組織は、頻度、方法、責任及び計画に関する要求事項及び報告を含む、監査プログラムの計画、確立、実施及び維持する。 [27001-9.2c)] 監査プログラムでは、関連するプロセスの重要性及び前回までの監査の結果を考慮する。 監査は一度にすべての適用範囲について実施するだけではなく、範囲の一部のみを対象とする場合もあり、毎回の監査の目的を明確にし、適切な監査計画を実施することが重要であることから、監査プログラムの作成においては、以下の点を考慮する。 ・監査の目的と重点目標 ・対象となる監査プロセスの状況と重要性 ・対象となる領域の状況と重要性 ・前回までの監査結果	
					4.6.2.4	組織は、監査基準及び監査範囲を明確にする。[27001-9.2d)] 監査プログラムでは全体的な監査の日程だけではなく、以下の内容について含める。 ・監査の基準（以下の内容も含む。） －目的、権限と責任 －独立性、客観性と職業倫理 －専門能力 －業務上の義務 －品質管理 －監査の実施方法 －監査報告書の形式 ・監査の範囲 ・監査の頻度又は時期 ・監査の方法（個別の情報セキュリティ監査基準を作成し、内部監査、外部組織による監査のいずれにおいても、品質の高い監査を実施できるように準備を整える。）	
					4.6.2.5	組織は、監査プロセスの客観性及び公平性を確実にする監査員の選定及び監査の実施を行う。 [27001-9.2e)] 監査人の選定においては監査基準に従い、以下の点を考慮する。 ・外観上の独立性 ・精神上の独立性 ・職業倫理と誠実性 なお、内部の監査員の場合は、自らが従事している業務については自身で監査しないように、他の担当者を割り当てる。	
					4.6.2.6	組織は、監査の結果を関連する管理層に報告することを確実にする。 [27001-9.2f)]	
					4.6.2.7	組織は、監査プログラム及び監査結果の証拠として、文書化した情報を保持する。 [27001-9.2g)] 監査手順に以下の内容を反映させるとともに、文書化し、お互いのコミュニケーションのために活用する。 ・監査の計画・実施に関する責任及び要求事項 ・結果報告・記録維持に関する責任と要求事項 要求事項については監査品質を確保するための必須条件であり、責任者と監査人が同じ目的をもって監査を実施する。	

21	経営陣は、定期的に、以下の点を考慮したマネジメントレビューを基本計画書、実施計画書、実施報告書等の文書を用いて行っている。 ・前回までのマネジメントレビューの結果として、行った処置の状況 ・情報セキュリティマネジメントに関連する外部及び内部の課題の変化 ・以下に示す内容を含めた、情報セキュリティパフォーマンスに関するフィードバック -不適合及び是正処置 -監視及び測定の結果 -監査結果 -情報セキュリティ目的の達成 ・利害関係者からのフィードバック ・情報セキュリティリスクアセスメントの結果及び情報セキュリティリスク対応計画の状況 ・継続的改善の機会 また、マネジメントレビューの結果を改善策に反映するために、以下の活動を実施し、改善策を検討している。結果は文書化して保存している。 ・情報セキュリティマネジメントの有効性の改善 ・情報セキュリティリスクアセスメント及び情報セキュリティリスク対応計画の更新 ・情報セキュリティマネジメントに影響を与える可能性のある内外の事象を考慮の上での手順及び管理策の修正 ・必要となる経営資源の特定 ・パフォーマンス測定方法の改善			○	4.6.3	マネジメントレビュー [27001-9.3]	
					4.6.3.1	トップマネジメントは、あらかじめ定めた間隔で、マネジメントレビューする。 [27001-9.3] あらかじめ定められた間隔でマネジメントレビューを実施するために、以下の点について考慮するとともに、文書化する。 ・マネジメントレビュー基本計画 ・マネジメントレビュー実施計画 ・マネジメントレビューのための実施報告 基本計画書では目的及び実施時期について、実施計画では詳細な監査の手法についてあらかじめ決める。	
					4.6.3.2	トップマネジメントは、マネジメントレビューにおいて、以下を考慮する。 [27001-9.3] ・前回までのマネジメントレビューの結果とった処置の状況 ・情報セキュリティマネジメントに関連する外部及び内部の課題の変化 ・以下に示す内容を含めた、情報セキュリティパフォーマンスに関するフィードバック -不適合及び是正処置 -監視及び測定の結果 -監査結果 -情報セキュリティ目的の達成 ・利害関係者からのフィードバック ・情報セキュリティリスクアセスメントの結果及び情報セキュリティリスク対応計画の状況 ・継続的改善の機会 また、これらの情報を構成することが予想される活動及び事象を記録し、必要に応じて報告するとともに、緊急性が高いものについてはあらかじめ定義しておき、誰もが同じ判断をできるように基準を定める。	
					4.6.3.3	マネジメントレビューからのアウトプットには、継続的改善の機会及び情報セキュリティマネジメントのあらゆる変更の必要性に関する決定を含める。 [27001-9.3] マネジメントレビューの結果を改善策に反映するために、以下の活動を実施し、改善策を検討する。 ・情報セキュリティマネジメントの有効性の改善 ・情報セキュリティリスクアセスメント及び情報セキュリティリスク対応計画の更新 ・情報セキュリティマネジメントに影響を与える可能性のある内外の事象を考慮の上での手順及び管理策の修正 ・必要となる経営資源の特定 ・パフォーマンス測定方法の改善 なお、改善策の立案においては、情報セキュリティリスク対応の選択肢を選択した際の記録を参考にする。	
					4.6.3.4	組織は、マネジメントレビューの結果の証拠として文書化した情報を保持する。 [27001-9.3] マネジメントレビューの結果は次回のマネジメントレビューに活用されるため、実施内容と結果が分かるように具体的に記録する。	
—	—			—	4.7	情報セキュリティマネジメントの維持及び改善 [27001-10]	
22	組織は、不適合をリスクアセスメント、内部監査、マネジメントレビュー等における結果を複合的に考察することにより検出し、不適合を是正するために以下の措置を行っている。 ・その不適合を管理し、是正するための処置 ・その不適合によって起こった結果への対処 ・以下についてあらかじめ文書化したうえで、それに基づく実施 －不適合の再発防止を確実にするために選択した処置の必要性の評価 －必要な是正処置の決定 －必要な是正処置の実施 －実施した処置の記録 －実施した是正処置のレビュー ・不適合の性質、措置、是正処置の結果の記録			○	4.7.1	是正処置 [27001-10.1]	
					4.7.1.1	組織は、不適合が発生した場合、不適合の是正のための処置を取る。 [27001-10.1a)] a) 是正措置 を取る際は、以下を実施する。 ・その不適合を管理し、是正するための処置 ・その不適合によって起こった結果への対処 ・是正処置を手順どおりに実施するために、以下について文書化する。 －不適合の再発防止を確実にするために選択した処置の必要性の評価 －必要な是正処置の決定 －必要な是正処置の実施 －実施した処置の記録 －実施した是正処置のレビュー	
						b) 不適合は以下の活動によって検出される。 ・定期的な情報セキュリティリスクアセスメント ・定期的な情報セキュリティ内部監査 ・定期的なマネジメントレビュー ・不適合を手順どおりに検出するために、以下について文書化する。 －情報セキュリティマネジメントに対する不適合の特定 －情報セキュリティマネジメントに対する不適合の原因の決定 なお、単一の活動だけでは判断できない場合もあるので、複合的な結果の考察から不適合を検出する。	
					4.7.1.2	組織は、不適合が再発又は他のところで発生しないようにするため、その不適合の原因を除去するための処置をとる必要性を評価する。 [27001-10.1b)] 必要性を評価する際は、以下を実施する。 ・その不適合のレビュー ・その不適合の原因の明確化 ・類似の不適合の有無、又はそれが発生する可能性の明確化	

					4.7.1.3	組織は、必要な処置を実施する。 [27001-10.1c)]	
					4.7.1.4	組織は、とった全ての是正処置の有効性をレビューする。 [27001-10.1d)]	
					4.7.1.5	組織は、必要な場合には、情報セキュリティマネジメントの変更を行う。 [27001-10.1e)]	
					4.7.1.6	組織は、是正処置は、検出された不適合のもつ影響に応じたものとする。 [27001-10.1]	
					4.7.1.7	組織は、是正処置の証跡として、以下の文書化した情報を保持する。 [27001-10.1f) / 10.1g)] ・不適合の性質及びとった処置 ・是正処置の結果	
—	—			—	4.8	文書化した情報の管理 [27001-7.5]	
23	組織は、情報セキュリティマネジメントが必要とする以下の情報を文書化している。 ・情報セキュリティ方針 ・情報セキュリティ目的 ・情報セキュリティリスクアセスメントのプロセス ・情報セキュリティリスク対応のプロセス ・情報セキュリティリスクアセスメントの結果 ・情報セキュリティリスク対応計画 ・パフォーマンス測定の結果			○	4.8.1	文書化の指針 [27001-7.5.1]	
					4.8.1.1	組織は、情報セキュリティマネジメントが必要とする以下の情報を文書化する。 [27001-7.5.1] ・情報セキュリティ方針 ・情報セキュリティ目的 ・情報セキュリティリスクアセスメントのプロセス ・情報セキュリティリスク対応のプロセス ・情報セキュリティリスクアセスメントの結果 ・情報セキュリティリスク対応計画 ・パフォーマンス測定の結果 　これらの内容についてはどの文書に記載されていてもかまわないが、その内容を知る必要がある担当者には必ず伝わるように構成するとともに、知る必要性のない者が閲覧できないことを確実にする。	
24	組織は、文書管理手順を策定したうえで、以下を行うことによって、文書化した情報を作成及び更新している。 ・適切な識別情報の記述（例えば、表題、日付、作成者、参照番号） ・適切な形式（例えば、言語、ソフトウェアの版、図表）及び媒体（例えば、紙、電子媒体）の選択 ・適切性及び妥当性に関する、適切なレビュー及び承認 ・文書化した情報のライフサイクルの定義や、それに応じた処理ができるような手順の策定 ・文書を発行する前における、適正性のレビュー及び承認 ・必要に応じた、文書の更新及び再承認 ・廃止文書の誤使用の防止 ・廃止文書を何らかの目的で保持する場合における、廃止文書であることが分かる適切な識別情報の記述 ・法的及び規制の要求事項及び環境の変化に従い、定めた頻度での更新 なお、文書化した情報の管理は以下を確実にするためである。 ・文書化した情報が、必要なときに、必要なところで、入手可能かつ利用に適した状態であること。 ・文書化した情報が十分に保護されていること（例えば、機密性の喪失、不適切な使用及び完全性の喪失からの保護）。 ・文書化した情報の配付、アクセス 、検索及び利用 ・文書化した情報の読みやすさが保たれることを含む、保管及び保存 ・文書化した情報の変更の管理（例えば、版の管理） ・文書化した情報の保持及び廃棄			○	4.8.2	文書の作成・変更及び管理 [27001-7.5.2 / 7.5.3]	
					4.8.2.1	組織は、以下を行うことによって、文書化した情報を作成及び更新する。 [27001-7.5.2] ・適切な識別情報の記述（例えば、表題、日付、作成者、参照番号） ・適切な形式（例えば、言語、ソフトウェアの版、図表）及び媒体（例えば、紙、電子媒体）の選択 ・適切性及び妥当性に関する、適切なレビュー及び承認 ・文書化した情報のライフサイクルの定義や、それに応じた処理ができるような手順の策定 ・文書を発行する前における、適正性のレビュー及び承認 ・必要に応じた、文書の更新及び再承認 ・廃止文書の誤使用の防止 ・廃止文書を何らかの目的で保持する場合における、廃止文書であることが分かる適切な識別情報の記述 ・法的及び規制の要求事項及び環境の変化に従い、定めた頻度での更新 　また、これらのすべての活動が文書管理に反映されているか、またその活動が業務に大きな障害を与えていないかなどを考慮し、適切な文書管理手順を策定する。	
					4.8.2.2	組織は、以下のことを確実にするために、情報セキュリティマネジメントで要求された文書化した情報を、管理する。 [27001-7.5.3] ・文書化した情報が、必要なときに、必要なところで、入手可能かつ利用に適した状態であること。 ・文書化した情報が十分に保護されていること（例えば、機密性の喪失、不適切な使用及び完全性の喪失からの保護）。 ・文書化した情報の配付、アクセス 、検索及び利用 ・文書化した情報の読みやすさが保たれることを含む、保管及び保存 ・文書化した情報の変更の管理（例えば、版の管理） ・文書化した情報の保持及び廃棄 　また、情報セキュリティマネジメントの計画及び運用のために組織が必要と決定した文書は、外部から入手したものであっても、必要に応じて、特定し、管理する。	
—	—			—	4.9	情報セキュリティリスクコミュニケーション	
—	—			—		利害関係者間の有効なコミュニケーションは、意思決定に大きな影響を与えることがある。情報セキュリティリスクコミュニケーションは、意思決定者とその他の利害関係者（クラウドサービス利用者及びクラウドサービスの提供にかかわる委託先を含む。）との間で情報セキュリティリスクに関する情報を交換、共有し、リスクを管理する方法に関する合意を得る。	

25	リスクコミュニケーション計画を以下の２つに分けて策定し、文書化している。 ・通常運用のためのリスクコミュニケーション計画 ・緊急事態のためのリスクコミュニケーション計画 リスクコミュニケーション計画は、意思決定者とその他の利害関係者（クラウドサービス利用者及びクラウドサービスの提供にかかわる委託先を含む。）との間でどのようにコミュニケーションを図るかに留意し、以下の内容について含めている。 ・適切な利害関係者の参画による、効果的な情報交換／共有 ・法令、規制及びガバナンスの要求事項の順守 ・コミュニケーション及び協議に関するフィードバック及び報告の提供 ・組織に対する信頼を醸成するためのコミュニケーションの活用 ・危機又は不測の事態発生時の利害関係者とのコミュニケーションの実施			無	4.9.1	リスクコミュニケーションの計画	
					4.9.1.1	リスクコミュニケーション計画を策定する。 リスクコミュニケーション計画は、以下の２つに分けて策定し、文書化する。 ・通常運用のためのリスクコミュニケーション計画 ・緊急事態のためのリスクコミュニケーション計画 リスクコミュニケーション計画は、意思決定者とその他の利害関係者（クラウドサービス利用者及びクラウドサービスの提供にかかわる委託先を含む。）との間でどのようにコミュニケーションを図るかに留意し、以下の内容について含める。 ・適切な利害関係者の参画による、効果的な情報交換／共有 ・法令、規制及びガバナンスの要求事項の順守 ・コミュニケーション及び協議に関するフィードバック及び報告の提供 ・組織に対する信頼を醸成するためのコミュニケーションの活用 ・危機又は不測の事態発生時の利害関係者とのコミュニケーションの実施	
26	リスクに関する論議、その優先順位の決定及び適切なリスク対応、並びにリスク受容を行い、主要な意思決定者と利害関係者（クラウドサービス利用者及びクラウドサービスの提供にかかわる委託先を含む。）の協調を得る仕組みを、以下を踏まえたうえで確定している。 ・リスクマネジメントの枠組みの主要な構成要素、及びその後に行うあらゆる修正の適切な伝達 ・枠組み、その有効性及び成果に関する適切な内部報告 ・適切な階層及び時期に利用可能な、リスクマネジメントの適応から導出される関連情報の提供 ・内部の利害関係者との協議のためのプロセス また、リスクコミュニケーションは、次の点を達成するために、リスクマネジメントプロセスのすべての段階で継続的に実施している。 ・組織のリスクマネジメント結果の保証を提供する ・リスク情報を収集する ・リスクアセスメントの結果を共有しリスク対応計画を提示する ・意思決定者と利害関係者（クラウドサービス利用者及びクラウドサービスの提供にかかわる委託先を含む。）の相互理解の欠如による情報セキュリティ違反の発生及び結果を回避又は低減する ・意思決定を支援する ・新しい情報セキュリティ知識を入手する ・他の組織と協調しすべてのインシデントの結果を低減するための対応計画を立案する ・意思決定者及び利害関係者（クラウドサービス利用者及びクラウドサービスの提供にかかわる委託先を含む。）にリスクについての責任を意識させる ・セキュリティ意識を改善する			無	4.9.2	リスクコミュニケーションの実施	
					4.9.2.1	リスクコミュニケーションを実施する仕組みを確定する。 リスクに関する論議、その優先順位の決定及び適切なリスク対応、並びにリスク受容を行い、主要な意思決定者と利害関係者（クラウドサービス利用者及びクラウドサービスの提供にかかわる委託先を含む。）の協調を得る仕組みを確定する。この仕組みでは次の事項を確実にする。 ・リスクマネジメントの枠組みの主要な構成要素、及びその後に行うあらゆる修正の適切な伝達 ・枠組み、その有効性及び成果に関する適切な内部報告 ・適切な階層及び時期に利用可能な、リスクマネジメントの適応から導出される関連情報の提供 ・内部の利害関係者との協議のためのプロセス 仕組みには、適切な場合には、多様な情報源からのリスク情報について、まとめ上げるプロセスが含まれ、また、リスク情報の影響の受けやすさを考慮する必要がある場合もある。なお、この仕組みを設ける場として、委員会がある。	
					4.9.2.2	リスクコミュニケーションを実施する。 リスクコミュニケーションは、次の点を達成するために、リスクマネジメントプロセスのすべての段階で継続的に実施する。 ・組織のリスクマネジメント結果の保証を提供する ・リスク情報を収集する ・リスクアセスメントの結果を共有しリスク対応計画を提示する ・意思決定者と利害関係者（クラウドサービス利用者及びクラウドサービスの提供にかかわる委託先を含む。）の相互理解の欠如による情報セキュリティ違反の発生及び結果を回避又は低減する ・意思決定を支援する ・新しい情報セキュリティ知識を入手する ・他の組織と協調しすべてのインシデントの結果を低減するための対応計画を立案する ・意思決定者及び利害関係者（クラウドサービス利用者及びクラウドサービスの提供にかかわる委託先を含む。）にリスクについての責任を意識させる ・セキュリティ意識を改善する リスクコミュニケーションの実施においては、組織内の適切な広報又はコミュニケーション部門と協力し、リスクコミュニケーション関連の全タスクを調整して行う。	
―	―			―		**情報セキュリティのための方針群**	管理策基準
27	経営陣及び管理者は、情報セキュリティのための方針群を定義、承認及び発行を行い、関係者に伝達している。また、これらの方針群の有効性を確認する機会を定期的または重大な変更時に設けている。			無	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：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。	
					5.1.1	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する。 (脚注）管理層には、経営陣及び管理者が含まれる。ただし、実務管理者（administrator）は除かれる。	
					5.1.2	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する。	
―	―			―	6	**情報セキュリティのための組織**	
28	・クラウドサービスに関する情報セキュリティの役割及び責任の所在を明示している。 ・クラウドサービス事業者の所在地、及び振興会のデータが保管される可能性のある国々及びその法管轄を明示している。 ・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ている。。 ・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んでいる。			無	6.1	内部組織	
					6.1	管理目的：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。	
					6.1.1	全ての情報セキュリティの責任を定め、割り当てる。	
					6.1.1.13.PB	クラウドサービスに関する情報セキュリティの役割及び責任の所在を明示すること。	
					6.1.2	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。	
					6.1.3	関係当局との適切な連絡体制を維持する。	
					6.1.3.3.PB	クラウドサービス事業者は、クラウドサービス利用者に、クラウドサービス事業者の組織の地理的所在地、及びクラウドサービス事業者がクラウドサービス利用者のデータを保管する可能性のある国々及びその法管轄を通知する。	
					6.1.4	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。	

					6.1.5	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。	
29	・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、適切なセキュリティ対策を採用している。 ・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、適切なセキュリティ対策を実施している。			無	6.2	モバイル機器及びテレワーキング	
						管理目的：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。	
					6.2.1	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。	
					6.2.2	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。	
30	・クラウドサービス利用者及びクラウドサービス事業者の両者は、クラウドサービスの利用における情報セキュリティの共同責任について、文書化し、公表し、伝達し、実装している。 ・クラウドサービス事業者の情報セキュリティ管理策及び責任を明示している。			無	6.3.P	クラウドサービス利用者及びクラウドサービス事業者の関係	
					6.3.P	管理目的：情報セキュリティマネジメントのための、クラウドサービス利用者及びクラウドサービス提供者間の共同責任の関係を説明するた	
					6.3.1.P	クラウドサービス利用者及びクラウドサービス事業者の両者は、クラウドサービスの利用における情報セキュリティの共同責任について、文書化し、公表し、伝達し、実装する。	
					6.3.1.1.PB	クラウドサービス事業者の情報セキュリティ管理策及び責任が明示されていること。	
—	—			—	7	**人的資源のセキュリティ**	
31	・関連する法令、規制及び倫理に従い、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、全ての従業員候補者についての経歴などの確認を行っている。 ・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ている。			無	7.1	雇用前	
					7.1	管理目的：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。	
					7.1.1	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う。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う。	
					7.1.2	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。	
32	・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ている。 ・組織の全ての従業員、及び必要に応じて契約相手は、職務に関連する組織の方針及び手順について、また、事業所内でデータを適切に取り扱うための、適切な教育及び訓練を受けている。 ・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ている。			無	7.2	雇用期間中	
					7.2	管理目的：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。	
					7.2.1	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。	
					7.2.2	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、また、定めに従ってその更新を受ける。	
					7.2.2.19.PB	事業所内でデータを適切に取り扱うための教育及び訓練を行っていること。	
					7.2.3	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。	
33	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、遂行させている。			無	7.3	雇用の終了及び変更	
					7.3	管理目的：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。	
					7.3.1	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。	
—	—			—	8	**資産の管理**	
34	・情報、情報に関連するその他の資産及び情報処理施設を特定する。また、これらの資産の目録を、作成し、維持している。 ・クラウドサービス事業者の資産目録において振興会のデータ等を明確に特定し、管理している。 ・利用者がクラウドサービスに保管するデータを暗号化したうえで利用者が安全に扱えるようにするか、利用者自身がデータの暗号化を利用してデータを安全に扱えるようにする手段を提供するかのいずれかに対応している。 ・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、実施している。 ・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ている。 ・クラウドサービス事業者の領域上にあるクラウドサービス利用者の資産は、クラウドサービス利用の合意の終了時に、時機を失せずに返却または除去している。			無	8.1	資産に対する責任	
					8.1	管理目的：組織の資産を特定し、適切な保護の責任を定めるため。	
					8.1.1	情報、情報に関連するその他の資産及び情報処理施設を特定する。また、これらの資産の目録を、作成し、維持する。	
					8.1.1.6.PB	クラウドサービス事業者の資産目録は、クラウドサービス利用者のデータ及びクラウドサービスの派生データを明確に特定する。	
					8.1.2	目録の中で維持される資産は、管理する。	
					8.1.2.7.PB	利用者がクラウドサービスに保管するデータを暗号化したうえで利用者が安全に扱えるようにするか、利用者自身がデータの暗号化を利用してデータを安全に扱えるようにする手段を提供するかのいずれかに対応すること。	
					8.1.3	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。	
					8.1.4	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。	
					8.1.5.P	クラウドサービス事業者の領域上にあるクラウドサービス利用者の資産は、クラウドサービス利用の合意の終了時に、時機を失せずに返却または除去する。	
35	・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、分類している。 ・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、実施している。 ・振興会がクラウドサービス上でデータを取り扱う際に、データをその重要性や秘匿性等に応じて分類し、それに応じた取り扱いを行えるようにするための手順を開示している。 ・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、実施している。			無	8.2	情報分類	
					8.2	管理目的：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。	
					8.2.1	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。	
					8.2.2	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。	
					8.2.2.7.PB	クラウドサービス事業者は、クラウドサービス利用者が扱う情報及び関連資産を当該利用者が分類し、ラベル付けするためのサービス機能について文書化し、開示する。	
					8.2.3	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。	

36	・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ている。 ・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ている。 ・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ている。			無	8.3 8.3 8.3.1 8.3.2 8.3.3	媒体の取扱い 管理目的：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。 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。 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。 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。	
―	―			―	9	**アクセス制御**	
37	・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、レビューしている。 ・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、利用者に提供している。			無	9.1 9.1 9.1.1 9.1.2	アクセス制御に対する業務上の要求事項 管理目的：情報及び情報処理施設へのアクセスを制限するため。 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。 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。	
38	・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ている。 ・振興会にクラウドサービス利用に必要なユーザーの登録及び登録削除の機能及び仕様を提供している。 ・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ている。 ・クラウドサービスのユーザのアクセス権を管理する機能及び仕様を提供している。 ・特権的アクセス権の割当て及び利用を、制限し、管理している。 ・振興会の管理者認証に、十分に強固な認証技術を提供している。 ・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ている。 ・振興会がクラウドサービスを利用する際の秘密認証情報の管理手順を提供している。 ・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ている。 ・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、また、変更に合わせて修正している。			無	9.2 9.2 9.2.1 9.2.1.6.PB 9.2.2 9.2.2.8. 9.2.3 9.2.3.11.PB 9.2.4 9.2.4.9.PB 9.2.5 9.2.6	利用者アクセスの管理 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。 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。 クラウドサービス事業者は、クラウドサービス利用者が扱う情報及び関連資産を当該利用者が分類し、ラベル付けするためのサービス機能について文書化し、開示する。 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。 クラウドサービスのユーザのアクセス権を管理する機能及び仕様を提供すること。 特権的アクセス権の割当て及び利用は、制限し、管理する。 クラウドサービス事業者は、特定したリスクに応じて、クラウドサービスの管理能力にあわせたクラウドサービス利用者の管理者認証に、十分に強固な認証技術（例えば、多要素認証機能）を提供する。 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。 クラウドサービス事業者は、秘密認証情報を割り当てる手順、及びユーザ認証手順を含む、クラウドサービス利用者の秘密認証情報の管理手順について、情報を提供する。 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。 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、また、変更に合わせて修正する。	
39	秘密認証情報の利用時に、組織の慣行に従うことを、利用者に要求している。			無	9.3 9.3 9.3.1	利用者の責任 管理目的：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。 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。	
40	・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、制限している。 ・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、及びデータへのアクセスを制限できるようアクセス制御を提供している。 ・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ている。 ・強い認証及び識別情報の検証が必要な場合には、パスワードに代えて、暗号による手段、スマートカード、トークン、生体認証などの認証方法を用いている。 ・パスワード管理システムは対話式とし、良質なパスワードを利用している。 ・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、厳しく管理している。 ・プログラムソースコードへのアクセスは、制限している。			無	9.4 9.4 9.4.1 9.4.1.8.PB 9.4.2 9.4.2.2.B 9.4.3 9.4.4 9.4.5	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：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。 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。 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、及びデータへのアクセスを制限できるようアクセス制御を提供すること。 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。 強い認証及び識別情報の検証が必要な場合には、パスワードに代えて、暗号による手段、スマートカード、トークン、生体認証などの認証方法を用いること。 パスワード管理システムは、対話式とすること、また、良質なパスワードを確実にするものとする。 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。 プログラムソースコードへのアクセスは、制限する。	
41	・クラウドサービス利用者のクラウドサービス上の仮想環境を、他のクラウドサービス利用者及び認可されていない者から保護している。 ・クラウドコンピューティング環境における仮想マシンを、事業上のニーズを満たすため、要塞化している。			無	9.5.P 9.5.P 9.5.1.P 9.5.2.P	共有化された仮想環境におけるクラウドサービス利用者のデータのアクセス制御 管理目的：共有化されたクラウドコンピューティング上の仮想環境における情報セキュリティを確実にするため。 クラウドサービス利用者のクラウドサービス上の仮想環境は、他のクラウドサービス利用者及び認可されていない者から保護する。 クラウドコンピューティング環境における仮想マシンは、事業上のニーズを満たすため、要塞化する。	

41	・仮想マシンを設定する際には、適切に要塞化し(例えば、クラウドサービスを実行するのに必要なポート、プロトコル及びサービスのみを有効とする）、利用する各仮想マシンに適切な技術的管理策(例えば、マルウェア対策、ログ取得）を実施している。			###	9.5.2.1. PB	仮想マシンを設定する際には、適切に要塞化し(例えば、クラウドサービスを実行するのに必要なポート、プロトコル及びサービスのみを有効とする）、利用する各仮想マシンに適切な技術的管理策(例えば、マルウェア対策、ログ取得）を実施すること。	

—	—			—	10	**暗号**
42	・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、実施している。 ・クラウドサービス利用者に、当該利用者が処理する情報を保護するために暗号技術を利用する機能を提供し、または、暗号技術を利用する環境についての情報を提供している。 ・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ている。 ・クラウドサービス利用者に、当該利用者の管理する情報の暗号化に用いる暗号鍵を当該利用者が管理する機能を提供し、または、当該利用者が暗号鍵を管理する方法についての情報を提供している。			無	10.1	暗号による管理策
					10.1	管理目的：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。
					10.1.1	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。
					10.1.1.9.PB	クラウドサービス利用者に、当該利用者が処理する情報を保護するために暗号技術を利用する機能を提供し、または、暗号技術を利用する環境についての情報を提供する。
					10.1.2	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。
					10.1.2.20.PB	クラウドサービス利用者に、当該利用者の管理する情報の暗号化に用いる暗号鍵を当該利用者が管理する機能を提供し、または、当該利用者が暗号鍵を管理する方法についての情報を提供する。
—	—			—	11	**物理的及び環境的セキュリティ**
43	・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、用いている。 ・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ている。 ・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、適用している。 ・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、適用している。 ・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、適用している。 ・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を管理している。また、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している。			無	11.1	セキュリティを保つべき領域
					11.1	管理目的：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。
					11.1.1	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。
					11.1.2	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。
					11.1.3	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。
					11.1.4	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。
					11.1.5	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。
					11.1.6	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、管理する。また、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。
44	・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、保護している。 ・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ている。 ・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ている。 ・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、正しく保守している。 ・装置、情報又はソフトウェアは、事前の認可なしでは、構外に持ち出していない。 ・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ている。 ・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。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、検証している。 ・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を遅滞なく確実に行っている。 ・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仕組みを整備している。 ・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ている。			無	11.2	装置
					11.2	管理目的：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。
					11.2.1	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。
					11.2.2	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。
					11.2.3	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。
					11.2.4	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。
					11.2.5	装置、情報又はソフトウェアは、事前の認可なしでは、構外に持ち出さない。
					11.2.6	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。
					11.2.7	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。
					11.2.7.4.PB	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を遅滞なく確実に行うこと。
					11.2.8	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仕組みを整備する。
					11.2.9	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。 （脚注）クリアデスクとは、机上に書類を放置しないことをいう。また、クリアスクリーンとは、情報をスクリーンに残したまま離席しないことをいう。

―	―			―	12	**運用のセキュリティ**
45	・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としている。 ・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している。 ・振興会がクラウドサービスを利用する中で、情報セキュリティに悪影響を及ぼす可能性のある変更を行う場合、振興会にその情報を提供している。 ・要求された主要なシステム資源の使用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、将来必要とする容量・能力を予測している。 ・全資源の容量を監視し、資源の枯渇によるインシデント発生を防いでいる。 ・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、分離している。 ・クラウドコンピューティング環境の、管理のための操作手順を定義し、文書化し、監視している。 ・操作マニュアル等を、振興会に提供できる。操作マニュアル等には重要な操作（システムの稼働に影響を与える操作など）がある場合、その操作手順を含む。			無	12.1	運用の手順及び責任
					12.1	管理目的：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。
					12.1.1	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とする。
					12.1.2	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、管理する。
					12.1.2.11.PB	クラウドサービス事業者は、クラウドサービス利用者の情報セキュリティに悪影響を及ぼす可能性のあるクラウドサービスの変更に関する情報を、クラウドサービス利用者に提供する。
					12.1.3	要求された主要なシステム資源の使用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、将来必要とする容量・能力を予測する。
					12.1.3.9	全資源の容量を監視し、資源の枯渇によるインシデント発生を防ぐこと。
					12.1.4	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、分離する。
					12.1.5.P	クラウドコンピューティング環境の、管理のための操作手順を定義し、文書化し、監視する。
					12.1.5.1.PB	クラウドサービス事業者は、重要な操作及び手順に関する文書を、それを求めるクラウドサービス利用者に提供する。
46	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ている。			無	12.2	マルウェアからの保護
					12.2	管理目的：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。
					12.2.1	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する。
47	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、検査している。			無	12.3	バックアップ
					12.3	管理目的：データの消失から保護するため。
					12.3.1	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。
48	・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ている。 ・振興会に、ログ取得機能を提供している。 ・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ている。 ・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ている。 ・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を、単一の参照時刻源と同期している。 ・クラウドサービス利用者に、クラウドサービス事業者のシステムで利用するクロックに関する情報及びクラウドサービス利用者がクラウドサービスのクロックにローカルクロックを同期させる方法についての情報を提供している。 ・クラウドサービス利用者は、利用するクラウドサービスの操作を監視する機能を有している。			無	12.4	ログ取得及び監視
					12.4	管理目的：イベントを記録し、証拠を作成するため。
					12.4.1	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。
					12.4.1.1	クラウドサービス事業者は、クラウドサービス利用者に、ログ取得機能を提供する。
					12.4.2	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。
					12.4.3	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。
					12.4.4	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る。
					12.4.4.4.PB	クラウドサービス事業者は、クラウドサービス利用者に、クラウドサービス事業者のシステムで利用するクロックに関する情報及びクラウドサービス利用者がクラウドサービスのクロックにローカルクロックを同期させる方法についての情報を提供する。
					12.4.5.P	クラウドサービス利用者は、利用するクラウドサービスの操作を監視する機能を有する。
49	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ている。			無	12.5	運用ソフトウェアの管理
					12.5	管理目的：運用システムの完全性を確実にするため。
					12.5.1	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。
50	・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ている。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ている。さらに、それらと関連するリスクに対処するために、適切な手段をとっている。 ・提供するクラウドサービスに影響を及ぼす可能性のあるぜい弱性情報を振興会が利用できるようにしている。 ・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、実施している。			無	12.6	技術的ぜい弱性管理
					12.6	管理目的：技術的ぜい弱性の悪用を防止するため。
					12.6.1	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する。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。
					12.6.1.18.PB	クラウドサービス事業者は、提供するクラウドサービスに影響を及ぼす可能性のある技術的ぜい弱性の管理についての情報を、クラウドサービス利用者が利用可能となるようにする。
					12.6.2	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。
51	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、合意している。			無	12.7	情報システムの監査に対する考慮事項
					12.7	管理目的：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。
					12.7.1	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、合意する。

—	—			—	13	**通信のセキュリティ**
52	・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、制御している。 ・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、また、ネットワークサービス合意書にもこれらを盛り込んでいる。 ・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ている。 ・仮想ネットワークを設定する際には、クラウドサービス事業者のネットワークセキュリティ方針に基づき、仮想ネットワークと物理ネットワークの設定の整合性を検証している。			無	13.1	ネットワークセキュリティ管理
					13.1	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。
					13.1.1	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。
					13.1.2	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、また、ネットワークサービス合意書にもこれらを盛り込む。
					13.1.3	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する。
					13.1.4.P	仮想ネットワークを設定する際には、クラウドサービス事業者のネットワークセキュリティ方針に基づき、仮想ネットワークと物理ネットワークの設定の整合性を検証する。
53	・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ている。 ・情報転送に関する合意では、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、取り扱っている。 ・電子的メッセージ通信に含まれた情報は、適切に保護している。 ・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、文書化している。			無	13.2	情報の転送
					13.2	管理目的：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。
					13.2.1	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る。
					13.2.2	情報転送に関する合意では、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、取り扱う。
					13.2.3	電子的メッセージ通信に含まれた情報は、適切に保護する。
					13.2.4	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、文書化する。
—	—			—	14	**システムの取得、開発及び保守**
54	・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ている。 ・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ている。 ・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、保護している。 ・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			無	14.1	情報システムのセキュリティ要求事項
					14.1	管理目的：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。
					14.1.1	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る。
					14.1.2	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する。
					14.1.3	アプリケーションサービスのトランザクションに含まれる情報は、次の事項を未然に防止するために、保護する。 ・不完全な通信 ・誤った通信経路設定 ・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
55	・ソフトウェア及びシステムの開発のための規則を、組織内において確立し、開発に対して適用している。 ・クラウドサービス事業者は、開示方針に反しない範囲で、セキュリティを保つための開発手順及び慣行についての情報を提供している。 ・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ている。 ・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、試験している。 ・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っている。また、全ての変更は、厳重に管理している。 ・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ている。 ・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、適切に保護している。 ・組織は、外部委託したシステム開発活動を監督し、監視している。 ・セキュリティ機能（functionality）の試験は、開発期間中に実施している。 ・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ている。			無	14.2	開発及びサポートプロセスにおけるセキュリティ
					14.2	管理目的：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。
					14.2.1	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、開発に対して適用する。
					14.2.1.13.PB	クラウドサービス事業者は、開示方針に反しない範囲で、セキュリティを保つための開発手順及び慣行についての情報を提供すること。
					14.2.2	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する。
					14.2.3	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、試験する。
					14.2.4	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。また、全ての変更は、厳重に管理する。
					14.2.5	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する。
					14.2.6	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、適切に保護する。
					14.2.7	組織は、外部委託したシステム開発活動を監督し、監視する。
					14.2.8	セキュリティ機能（functionality）の試験は、開発期間中に実施する。
					14.2.9	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する。

56	試験データは、注意深く選定し、保護し、管理している。			無	14.3	試験データ
					14.3	管理目的：試験に用いるデータの保護を確実にするため。
					14.3.1	試験データは、注意深く選定し、保護し、管理する。
—	—			—	15	**供給者関係**
57	・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、文書化している。 ・組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、情報、情報処理施設及び移動が必要なその他のものの移行の管理、並びにその移行期間全体にわたって情報セキュリティが維持されることの確実化を含めている。 ・振興会がクラウドサービスを選定する際に、サービス上で取り扱われる振興会のデータに対して、国内法以外の法令が適用された結果、振興会の意図しないまま振興会以外の者がアクセスするリスクを考慮にいれている。なお、必要に応じて委託業務の実施場所及び契約に定める準拠法・裁判管轄を指定している。 ・関連する全ての情報セキュリティ要求事項を確立し、組織の情報に対して、アクセス、処理、保存若しくは通信を行っている、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ている。 ・自らが実行する適切な情報セキュリティ対策を、振興会に明解に提供している。 ・供給者との合意には、情報通信技術（以下「ICT」という。）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ている。			無	15.1	供給者関係における情報セキュリティ
					15.1	管理目的：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。
					15.1.1	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、文書化する。
					15.1.1.14.B	組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、情報、情報処理施設及び移動が必要なその他のものの移行の管理、並びにその移行期間全体にわたって情報セキュリティが維持されることの確実化を含める。
					15.1.1.16.B	当該事業者が提供するサービス上で取り扱われる情報に対して国内法以外の法令及び規制が適用された結果、クラウドサービス利用者の意図しないまま当該利用者の管理する情報にアクセスされ、又は処理されるリスクを評価して外部委託先を選定し、必要に応じてクラウドサービス利用者が扱う情報が取り扱われる場所及び契約に定める準拠法・裁判管轄を指定する。
					15.1.2	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する。
					15.1.2.18.PB	クラウドサービス事業者は、クラウドサービス事業者とクラウドサービス利用者の間に誤解が生じないように、クラウドサービス事業者が実行する適切な情報セキュリティ対策を、合意の一環として定める。
					15.1.3	供給者との合意には、情報通信技術（以下「ICT」という。）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。
58	・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、監査している。 ・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）を管理している。			無	15.2	供給者のサービス提供の管理
					15.2	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。
					15.2.1	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。
					15.2.2	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）を管理する。
—	—			—	16	**情報セキュリティインシデント管理**
59	・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ている。 ・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ている。 ・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ている。 ・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ている。 ・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ている。 ・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ている。 ・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、適用している。 ・クラウドサービス事業者は、クラウドサービス利用者と、クラウドコンピューティング環境内の潜在的なディジタル形式の証拠、又はその他の情報の要求に対応する手順を合意している。			無	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
					16.1	管理目的：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。
					16.1.1	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する。
					16.1.2	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。
					16.1.3	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する。
					16.1.4	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。
					16.1.5	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。
					16.1.6	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る。
					16.1.7	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、適用する。
					16.1.7.13.PB	クラウドサービス事業者は、クラウドサービス利用者と、クラウドコンピューティング環境内の潜在的なディジタル形式の証拠、又はその他の情報の要求に対応する手順を合意する。

―	―			―	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**
60	・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ている。 ・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、維持している。 ・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ている。			無	17.1	情報セキュリティ継続
					17.1	管理目的：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。
					17.1.1	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する。
					17.1.2	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、維持する。
					17.1.3	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する。
61	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、導入している。			無	17.2	冗長性
					17.2	管理目的：情報処理施設の可用性を確実にするため。
					17.2.1	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。
―	―			―	18	**順守**
62	・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、最新に保っている。 ・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ている。 ・知的財産権の順守に対応するためのプロセスを確立している。 ・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ている。 ・振興会に、クラウドサービスに蓄積する記録の保護方法について、情報を提供している。 ・プライバシー及び個人識別情報（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行っている。 ・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ている。 ・クラウドサービス利用者に、適用する協定、法令及び規則を順守していることをレビューするため、クラウドサービス事業者が実装した暗号による管理策の記載を、提供している。			無	18.1	法的及び契約上の要求事項の順守
					18.1	管理目的：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。
					18.1.1	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、最新に保つ。
					18.1.2	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する。
					18.1.2.1	知的財産権の順守に対応するためのプロセスを確立していること。
					18.1.3	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する。
					18.1.3.13.PB	クラウドサービス事業者は、クラウドサービス利用者に、クラウドサービスの利用に関して、クラウドサービス事業者が収集し、蓄積する記録の保護について、情報を提供する。
					18.1.4	プライバシー及び個人識別情報（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行う。
					18.1.5	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。
					18.1.5.7.PB	クラウドサービス利用者に、適用する協定、法令及び規則を順守していることをレビューするため、クラウドサービス事業者が実装した暗号による管理策の記載を、提供する。
63	・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ている。 ・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ている。 ・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ている。			無	18.2	情報セキュリティのレビュー
					18.2	管理目的：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。
					18.2.1	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する。
					18.2.2	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する。
					18.2.3	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する。