クラウドサービス提供基準

目次

１．クラウドサービス提供における情報セキュリティ基本方針

１．１．組織的取組に関する基本的な方針

１．１．１　クラウドサービス情報セキュリティ方針の作成

クラウドサービスを顧客に提供するにあたって、目標とする情報セキュリティに対する組織的取組についての方針、役割、責任等を定めた文書を作成すること。
文書には、次の事項に関する記載を含める。

a）クラウドサービス提供における情報セキュリティの定義、目的及び適用範囲
b）クラウドサービス提供事業者としての情報セキュリティの重要性についての考え方
d）体制の構築と情報資産保護への取組の姿勢
　1）法令、規制等の遵守
　2）教育・訓練の実施
　3）事件・事故の予防と対応への取組
　4）管理責任者や従業員の義務
f）見直し及び改善への取組の姿勢

作成した方針は、経営陣の承認を経て、サービス提供に関連する組織に配布すること。

１．１．２ クラウドサービス情報セキュリティ方針の変更

クラウドサービス情報セキュリティ方針を定めた文書は、定期的又はクラウドサービスの提供に係る重大な変更や不適合が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。
方針の改定にあたっては、経営陣の承認を経て実施し、サービス提供に関連する組織に通知すること。

１．１．３ 文書の保護

クラウドサービス情報セキュリティに関する基本的な方針を定めた文書を、不正な開示や変更から保護すること。

２．クラウドサービス提供を目的とした組織

２．１．組織体制

２．１．１　クラウドサービス提供の役割と責任

クラウドサービスを顧客に提供するにあたって、以下の役割と責任を担う組織体制を確立

すること。

① クラウドサービスのサービスレベルの維持管理

② クラウドサービスの情報セキュリティの確保

２．１．１　クラウドサービス運用管理責任者

クラウドサービスを顧客に提供するにあたって、サービスレベル、情報セキュリティの両面にわたって、運用管理責任を担う人員を配備する。

経営陣は、人員・資産・予算等のリソース面で運用管理責任者に対して積極的な支援・支持を行うこと。

２．１．２　クラウドサービスシステム一覧

運用管理責任者は、クラウドサービスに関連して保有、提供するシステム、アプリケーション及びクラウドサービスの一覧を作成し、サービスレベルおよび情報セキュリティに関する責任の所在を定めること。

一覧には、プライバシーに関する責任も含めること。

2．１．3.　情報資産の特定

システム一覧をもとにして、クラウドサービスにおいて取り扱いの対象となる情報資産の一覧を作成する。

2．１．4.　個人情報の識別

システム一覧をもとにして、個人を特定できる情報を処理するシステム、アプリケーション、クラウドサービスを識別する。

2．１．5.　情報資産の管理

情報資産の管理、バックアップ及び復元といった情報資産に関連する運用に責任をもつ要員を定める。

２．１．６　相反する職務と責任の分離

クラウドサービスに関連する資産に対する、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、相反する職務及び責任の範囲は、分離すること。

許可されていない状態又はモニタリングされていない状態で、単独で資産に対してアクセス、修正又は使用ができないようにする。

作業を開始することと、その作業を認可することとは分離する。

２．１．７　リスク管理方針

クラウドサービスに対する情報セキュリティ等の侵害が、事業、業務、情報資産、顧客及びサプライチェーンへもたらす脅威に対するリスクを管理する。
リスク管理方針は、定期的又はクラウドサービスの提供に係る変更が生じた場合に見直すこと。

２．１．８　情報セキュリティリスクの評価・分析・対応

クラウドサービスの提供を脅かす情報セキュリティリスクを評価・分析し、対策を講じること。
対策の立案にあたっては、資産、システム、アプリケーション、個別のクラウドサービスの重要度を特定し、重要度に応じた保護・防御機能を検討する。
クラウドサービス固有のサイバーセキュリティ上の脅威を識別し、予防・検知・回復・追跡するための機能を実装する。
個人を特定できる情報の処理に関連するシステム、アプリケーション、又はクラウドサービスが個人情報保護に与える影響を評価する。

２．１．９　テスト、トレーニング及びモニタリング

情報セキュリティに関連するテスト、トレーニング及びモニタリングを計画し、継続的に実施すること。また、当該計画をレビューし、情報セキュリティの基本方針に適合しているかを確認し、必要に応じて見直すこと。

２．１．10　苦情管理

クラウドサービスに関連する情報セキュリティ管理に対する従業員からの気づき、苦情、懸念又は質問を受付、対応するための仕組みを設けること。

２．２．モバイル機器及びテレワーキング

２．２．１　モバイル機器の利用方針

モバイル機器を業務で用いることによって生じるリスクを管理するために、モバイル機器の利用方針を策定し、その方針を実施するために必要な情報セキュリティ対策を講じること。

２．２．２　テレワーキングでの情報保護

テレワーキングでアクセス、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情報セキュリティ対策を実施すること。

３．サプライチェーンに関する管理

３．１．サプライチェーン事業者間の合意

３．１．１　リスク対策と文書化

クラウドサービスを顧客に提供するにあたって、当社が利用するサプライチェーン事業者（クラウドコンピューティングプロバイダ）と当社との間で合意された情報セキュリティリスク対策及びサービスレベルを文書化すること。
文書化された情報セキュリティ対策およびサービスレベルをサプライチェーン事業者によって確実に実施されることを契約及びSLAの締結によって担保すること。

３．１．２　サービスの監視

サプライチェーン事業者が提供するクラウドサービスを定常的に監視もしくはレビューし、運用に関する記録及び報告を継続的に実施すること。
サプライチェーン事業者に起因する情報セキュリティインシデント及びサービスレベルに関する問題点について、ログ記録等によりレビュー・監査できるようにすること。

３．１．３　リスク評価とレビュー

サプライチェーン事業者が提供するシステム、システムコンポーネント、クラウドサービスに関連するサプライチェーン関連のリスクを評価及びレビューすることについて、サプライチェーン事業者と合意し文書化すること。
リスク評価のプロセスには、脆弱性管理を含めること。

３．１．４　関連情報の保護

システム、システムコンポーネント、クラウドサービスに関するサプライチェーン関連情報を保護することについて、サプライチェーン事業者と合意し文書化すること。

３．１．５　セキュリティ侵害の通知

サプライチェーンにおけるセキュリティ侵害の発生に関する通知について手順を確立し、

サプライチェーン事業者と合意し文書化する。

３．１．６ 変更管理

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に伴う、サプライチェーン事業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、手順及び対応策の保守及び改善を含む）を管理することについて、サプライチェーン事業者と合意し文書化すること。

３．１．７　改ざん防止

システム、システムコンポーネント、クラウドサービスに対する改ざん防止プログラムを実装し、情報資産の完全性を保証することについて、サプライチェーン事業者と合意し文書化すること。

３．１．８　システム又はシステムコンポーネントの検査

改ざんを検出して情報資産の完全性を保護するために、システム、システムコンポーネント又はクラウドサービスを検査することについて、サプライチェーン事業者と合意し文書化すること。

３．１．９　システムコンポーネントの信頼性

偽造されたシステムコンポーネントがシステムやクラウドサービスに侵入することを検出及び防止する手段を実装することについて、サプライチェーン事業者と合意し文書化すること。

３．１．１０　システムコンポーネントの廃棄

データ、ドキュメント、ツール又はシステムコンポーネントを廃棄する方法を確立するとともに、廃棄方法についてサプライチェーン事業者と合意し文書化すること。

３．２．サプライチェーン事業者の選定

３．２．１．選定基準

顧客に提供するクラウドサービスの業務要件を勘案し、サプライチェーン事業者の選定基準をあらかじめ設定しておくこと。

３．２．2. 再委託

サプライチェーン事業者がサービスの一部を再委託することについて、許可するかしないか、許可する場合の条件についてあらかじめ定めておくこと。

４．情報資産の管理

４．１．情報資産に対する責任

４．１．１．情報資産の管理責任者

クラウドサービス提供において取り扱う情報資産に関して管理責任者を定めるとともに、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にすること。

４．１．２．クラウドサービス利用終了における手続き

クラウドサービス利用者がクラウドサービスの利用を終了するにあたり、クラウドサービス上に保存された情報を処理する方法についてあらかじめ利用者と合意し、文書化しておくこと。

４．１．３．バックアップ

データ、ソフトウェア及びシステムのバックアップは、利用者と合意されたバックアップ方針に従って定期的に実施し、バックアップ内容を検査すること。また、事業者は、利用者にバックアップ手段を提供すること。

４．１．４．サービスの目的との整合性

サービスの目的や提供機能の範囲を逸脱したサービス及び機能をサポートしていることが判明した場合、潜在的なセキュリティ脅威を検知するため、情報資産が想定又は目的から逸脱して使用されていないかを確認すること。

４．２．情報の分類

４．２．１．情報資産目録

情報資産の価値及び法的要求（個人情報の保護等）等に基づき、重要性の観点から情報資産を分類した上で、情報資産目録を作成し、維持すること。
情報資産の分類方法と各情報資産の管理責任者を定め文書化すること。

４．２．２．データの識別

クラウドサービス上に存在する、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から派生したデータを明確に識別すること。

４．２．３．情報資産の取扱い

情報資産の取扱いに関する手順は、クラウドサービスの特性を考慮したうえで、情報分類の体系に従って策定し、実施すること。
情報資産の分類ごとに、安全な取扱い手順（取得・入力・移送・送信・利用・加工・保管・バックアップ・廃棄・消去）を定めること。

４．３．本基準の遵守、点検及び監査

４．３．１．点検・レビュー

各情報資産の管理責任者は、自らの責任範囲における全ての情報セキュリティ対策が、本基準に則り正しく確実に実施されるか、定期的にレビュー及び見直しを行うこと。
また、情報セキュリティのための方針及び本基準に則して、システムや提供するクラウドサービスが、定めに従って技術的に順守されていることをレビューすること。
運用管理責任者はレビュー及び見直しの方法をあらかじめ定めておく。レビューは、毎年実施することが望ましい。

４．３．２　監査

クラウドサービスの提供に用いるシステムが、本基準の要求を遵守していることを確認するため、定期的に検証・監査すること。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、実施すること。

４．４．アクセス管理

４．４．１．アクセス制御方針

業務及び情報セキュリティの要求事項に基づいてアクセス制御方針を確立し、文書化し、レビューすること。また、情報及びシステム機能へのアクセスは、アクセス制御方針に従って、制限すること。

４．４．２．アクセス制御機能

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利用者データへのアクセスを、利用者が制限できるようにアクセス制御機能を提供すること。
アクセス制御機能の提供には、以下を含めること。

① 利用者の実務管理者が必要に応じて特権アクセス権限の管理を行えるように、利用者が直面するリスクに応じた強固な認証機能を提供する。
② 秘密認証情報を割り当てる手順及び利用者が秘密認証情報を管理する手順(ユーザ認証手順を含む)について、利用者に情報を提供する。

４．４．３．ユーティリティプログラムの使用

システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用は、制限し、厳しく管理すること。
なお、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。

４．４．４． プログラムソースコードへのアクセス

プログラムソースコードへのアクセスは、定められた特定の要員と方法に制限すること。

４．４．５． アクセス制御となりすまし対策

利用者及びシステム管理者等のアクセスを管理するために、適切な認証方法、特定の場所や装置からの接続を認証する方法等によって、アクセス制御及びなりすまし対策を行うこと。
認証に ID・パスワードを用いる場合は、以下を規定すること。

① ID・パスワードの生成規則と運用管理方法（パスワードの有効期限など）
② ID･パスワード等の認証情報は、文字列ではなくハッシュ値を保存すること

高い機密性、完全性が求められるサービスでは、記憶情報・所有情報を組み合わせた多要素認証を採用すること。

４．５．構成管理

４．5．１．　構成管理のポリシーと手順

構成管理を実施する目的と方針を定義し、構成管理を実施するための手順を策定すること。

４．5．２．　ベースライン構成

システムの最新のベースライン構成を把握・文書化すること。
ベースライン構成には、システムコンポーネント（PC、サーバ、ネットワークコンポーネント、インストールされているソフトウェアパッケージ・OS 等の現在のバージョンとパッチ情報、設定項目等）、ネットワークの接続形態及びシステム構成内のそれらのコンポーネントの論理的な配置に関する情報を含む。

４．5．３．　構成変更管理

ベースライン構成の対象となるシステムに対する変更が必要となる際には、変更内容をレビューし、セキュリティへの影響を考慮した上で変更を許可すること。また、変更に関する関連の活動を監査し、レビューすること。
稼働中のシステムに対して変更を実施する前に、それらの変更をテストし、結果を承認して文書化する。

４．5．４．　変更に対するアクセス制限

システムに対する変更に関して、物理的／論理的なアクセス制限を定義すること。

４．5．５．　システム設定基準

セキュリティ運用上の要求事項に基づいて、システムに最適な設定が施された段階で、システムに導入されている製品の設定項目を把握し、文書化すること。

４．5．６．　ソフトウェアの使用制限

契約上の取り決めと著作権法に従ってソフトウェアと関連ドキュメントを管理する。
ソフトウェアと関連ドキュメントが使用許諾の範囲（ライセンスの種類、数）において使用されているかどうかをモニタリングし、それらが複製されないようにすること。

４．5．７．　クラウドサービス利用者によるソフトウェアのインストール

利用者によるソフトウェアのインストールを管理するためのポリシーを確立するとともにポリシーが遵守されていることをモニタリングすること。
利用者がインストールしたソフトウェアが許可されていない場合、アラートを発効する仕組みを設けるのが望ましい。

４．5．８．　重要情報の保管場所

重要情報の保管場所と、重要情報が処理・保存されるシステムコンポーネントを特定し、文書化すること。また、個人を特定できる情報がどのように処理されているかについて文書化すること。

５．従業員に係る情報セキュリティ

５．１．雇用前

５．１．１．　雇用契約

雇用形態に関わらず、雇用予定の従業員に対して、機密性・完全性・可用性に係る情報セキュリティ上の要求及び責任の分界点を提示・説明するとともに、この要求等に対する明確な同意をもって雇用契約を締結すること。

５．２．雇用期間中

５．２．１．　教育・訓練

全ての従業員に対して、情報セキュリティポリシーに関する意識向上のための適切な教育・訓練を実施すること。

５．２．２．　教育のフィードバック

組織のトレーニング結果を情報セキュリティ責任者にフィードバックすること。

５．２．３．　契約違反

従業員が、情報セキュリティポリシー又はクラウドサービス提供上の契約に違反した場合の対応手続を備えること。

５．３．雇用の終了又は変更

５．３．１． アクセス権・資産の取扱い

従業員の雇用が終了又は変更となった場合のアクセス権や情報資産等の扱いや返却について、実施すべき事項や手続、確認項目等を明確にすること。

６．情報セキュリティインシデントの管理

６．１．情報セキュリティインシデント及び脆弱性の報告

６．１．１． インシデントの報告

従業員に対し、情報セキュリティインシデント（サービス停止、情報の漏えい・改ざん・破壊・紛失、ウイルス感染等）もしくはその兆候を発見した場合に、できるだけ速やかに定められた報告窓口に報告がなされるよう手順を定めること。
報告を受けた後に、迅速に効果的な対応ができるよう、インシデント取り扱いの責任体制及び手順を確立すること。

６．１．２． 当社とクラウドサービス利用者間の報告

クラウドサービス提供事業者である当社とクラウドサービス利用者間で、以下の報告の仕組みを設けること。

① クラウドサービス利用者が検知した情報セキュリティ事象を当社に報告する仕組み
② 当社が情報セキュリティ事象をクラウドサービス利用者に報告する仕組み
③ クラウドサービス利用者に対して、当社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

６．１．３． インシデントの評価と分類

従業員からの報告、クラウドサービス利用者からの報告連絡、当社における検知事項など、受け付けた情報セキュリティ事象を評価し、インシデントの重大さに応じて対応を行うための手順を確立すること。

インシデントの評価及び決定の結果は、以後の参照及び検証のために詳細に記録すること。

６．１．４． フィードバック

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を、情報セキュリティインシデントが将来起こる可能性又はその影響を低減するために用いること。

６．１．５． 証拠の収集・取得

インシデントに関連し、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ること。

７．コンプライアンス

７．１．法令と規則の遵守

７．１．１． 関連法規と記録

個人情報(特に要配慮個人情報を含む)、プライバシー情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。

また、クラウドサービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）について、法令、契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理するとともに、利用者から求められたときには提供できるようにすること。

７．１．２． 利用可否の明示

クラウドサービスを利用しようとする者に対して、利用しようとしているシステムが当社の管理下にあること、あらかじめ認可された目的以外のアクセスは許可されないこと等について、警告文を画面表示する等の方法によって警告を行う。

７．１．３． ソフトウェア製品

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こと。

ソフトウェア製品の使用許諾条件等について、利用者に予め周知し、ライセンス契約違反とならないようにすること。

７．１．４． 不正アクセス・流出からの保護

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、記録を保護すること。
また、利用者によるクラウドサービスの利用に関連して、事業者が収集し、保存する記録の保護に関する情報を、利用者に提供すること。
保存した記録の暗号化又はデジタル署名に用いた暗号鍵及び暗号プログラムは、記録類を保存している期間中、確実に記録の復号が可能になるよう保管する。
電子的記憶媒体を選択する場合は将来の技術変化によって読出しができなくなることを防ぐために、定められた保管期間を通じてデータにアクセスできること（媒体及び書式の読取り可能性）を確実にするための手順を確立する。

７．１．５． 暗号化

暗号化機能を用いる際には、関連する法令及び規制を順守するとともに、利用者が法令及び規制の順守状況について確認できるようにすること。

８．ユーザサポートの責任

８．１．クラウドサービス利用者への責任

８．１．１． 責任

クラウドサービスの提供に支障が生じた場合には、その原因がサプライチェーン事業者（クラウドコンピューティングプロバイダ等）に起因するものであったとしても、利用者と直接契約を結ぶ事業者として、当社の責任における一元的なユーザサポートの実施について、合意した内容を文書化すること。

８．１．２． SLO

クラウドサービスを提供する事業者として、当社の責任範囲を SLO 等により文書化し、利用者に明確に示すこと。

８．１．３． 情報提供

クラウドサービスの新規利用又は変更を計画している利用者に向けて情報提供をする際には、当社のガバナンス規定類を順守した上で、利用者が求める統制機能及び能力を有しているかどうか判断できるように努めること。

８．１．４．　クラウドサービス利用者からの苦情対応
提供しているクラウドサービスに対し、利用者からの苦情、懸念又は質問を受け付け、対応するためのプロセスを構築すること。

８．２．保守

８．２．１．　システム保守方針と手順 システム保守の目的、適用範囲、役割、責任、経営のコミットメント、組織間の調整及びコンプライアンスの観点において、システム保守の方針を策定、文書化し、関係する組織に配布すること。

８．２．２．　保守管理 保守に関わる内外の組織と保守の範囲、役割分担を識別しておくこと。
保守契約、保守仕様書及び要求事項に従って、保守を計画、実施、文書化し、記録すること。
保守後に、影響を受けた可能性のあるすべてのセキュリティ対策をチェックして、それらの対策が正しく機能しているかどうかを確認すること及び保守関連情報を記録すること。
保守記録には、下記情報を含む。

1. 保守日時
2. 保守を実施した個人又はグループの名前
3. 実施された保守内容
4. 保守対象のシステムコンポーネント

８．２．３．　保守ツール
システムの保守ツールを承認・管理し、モニタリングするとともに、使用状況をレビューすること。

８．２．４．　保守作業 保守及び診断用ツールは、あらかじめ定められた規定に則って、使用を許可されたものに制限すること。
保守及び診断の実施状況についてモニタリングする。

また、保守及び診断のためのセッションを確立する際には、厳格な認証機能を使用するのに加え、保守及び診断の記録を保管すること。
保守が完了したら、セッションとネットワーク接続を終了すること。

８．２．５．　保守要員　保守要員の認可手順を確立し、認可された保守組織又は要員の一覧を維持すること。

８．２．６．　保守要員による保守
保守要員が付添いなしで保守を行う場合、その要員が必要なアクセス権限を有することを事前に確認すること。また、必要なアクセス権限を持たない要員による保守活動が試行された場合に検知できるようにしておくこと。

８．２．７．　タイムリーな保守 システムコンポーネントに障害が発生した場合、保守サポート契約に基づき、保守サポートが迅速に行われるようにしておくこと。

９．事業継続管理における情報セキュリティ

９．１．情報セキュリティの継続

９．１．１．　情報セキュリティ継続計画の策定と実施
大規模災害発生等における情報セキュリティ及び情報セキュリティ管理の継続のための要求事項を明確にするとともに、プロセス・手順・対策を確立、文書化し、実施、維持すること。また、システムの途絶、侵害、又は不具合が発生した場合に、システムを従前の状態に復旧し、再構成できるように計画すること。
９．１．２．　情報セキュリティ継続の検証、レビュー及び評価
情報セキュリティ継続のための対策が、大規模災害等の下で妥当かつ有効であることを確認するために、組織は、定められた間隔でこれらの対策を検証すること。

１０．その他

１０．１．暗号と認証

１０．１．１．　方針

情報を保護するための暗号利用に関する方針を、策定し、実施すること。
暗号の使用が海外に及ぶ際には、各国の規制、国境を越える暗号化された情報の流れに関する規制及び国内の制約を考慮すること。
方針には、暗号技術として、電子政府推奨している暗号技術以上に強固なものを採用すること。

１０．１．２．　情報提供

クラウドサービスにおいて処理される情報を保護するために暗号を利用する環境について、利用者に情報を提供すること。
また、利用者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、クラウドサービスの一環として実装する機能についても利用者に情報を提供すること。

１０．１．３．　暗号鍵の作成と管理（NIST SP800-34, SC-12）

システム内で使用される暗号鍵を特定し、生成・配布・保管・アクセス・廃棄する手順を定めておくこと。

１０．2．開発プロセスにおけるセキュリティ

１０．２．１．　開発プロセスにおける情報セキュリティへの取組

情報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、文書化、維持し、全てのシステムの実装に対して適用する。

１１．運用における情報セキュリティ

１１．１．運用管理

１１．１．１．　情報セキュリティ監視手順の策定

情報セキュリティ監視（稼働監視、障害監視、パフォーマンス監視等）の実施基準・手順等を定めること。また、クラウドサービスの提供に用いるアプリケーションの運用・管理に関する手順書を作成すること。
運用管理の対象、運用管理の方法（バックアップ、媒体の取扱い、情報セキュリティインシデントへの対応・報告、ログの記録と管理、パフォーマンス監視・評価、システム監査ツールの不正使用の防止等）、運用管理の体制等を明確にする。

１１．１．２．　運用管理端末

運用管理端末に、許可されていないプログラム等のインストールを禁止すること。
運用管理端末は、ウイルス対策ソフトによるリアルタイムスキャン、定期的な完全スキャンを行う。
ウイルス対策ソフトに対して、常に最新のパターンファイルを適用する。

１１．１．３．　稼働・障害監視

クラウドサービスの稼働監視、障害監視、パフォーマンス監視及びセキュリティインシデント監視を行うこと。また、クラウドサービスを利用者に提供する時間帯を定め、サービス時間帯におけるクラウドサービスの稼働率を規定すること。
稼働停止や異常を検知した場合は、利用者に速報すること。
また、原因及び影響を評価・分析して、管理責任者に報告すること。

１１．１．４．　追加報告

稼働停止、障害、パフォーマンス低下、その他の情報セキュリティ事象について、第一報（速報）に続いて、より詳しい分析報告を利用者に対して行うこと。事象発生時はお客様への影響の有無に応じてサポートサイトに掲載する。必要に応じて、利用者側の管理連絡窓口へのメール及び報告書などでの連絡をする。
追加報告には、原因の分析結果や復旧の予測を含める。

１１．１．5.　時刻同期

クラウドサービスを提供するにあたって、当社が利用するサプライチェーン事業者が提供する時刻同期の方法を確認していること。

１１．１．6.　パスワード管理

パスワード管理システムは、対話式とすること、また、良質なパスワードとすること。パスワードの文字数等、パスワードの生成規則については、情報資産の機密度合いやリスクの大きさを考慮して、具体的なルールを定めること。

１１．１．7.　クラウドサービスの変更管理

組織、業務プロセス及びシステムの変更など、情報セキュリティに影響を与える変更を管理すること。

クラウドサービス利用者の情報セキュリティに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、利用者に以下の事項を含む情報を提供すること。 併せて、変更開始と完了の通知を行うこと。

① 変更予定日
② 変更内容
③ 変更内容に関する技術的説明

１１．１．8.　リソース監視

クラウドサービスに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、リソースの利用を監視・調整し、また、将来必要とする容量・能力を予測すること。

潜在的なボトルネックならびに特定の要員へ依存度が高くなる傾向など、情報セキュリティ又はサービスの継続に脅威をもたらすおそれのある要素を識別し、対応を立案する。

事業展開及びシステムに対する要求事項の変化ならびに情報処理の能力について、将来必要とされる容量・能力を予測する。

１１．１．9.　環境の分離

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、開発環境、試験環境および運用環境を互いに分離すること。

１１．１．１0.　マルウェア対策

マルウェアから保護するために、検出、予防及び回復のための対策を実施すること。

マルウェアからの保護の有効性を高めるために、複数の異なる業者及び技術によるマルウェア対策ソフトウェア製品を利用することが望ましい。

１１．１．11. イベントログの取得

利用者の利用状況、例外処理及び情報セキュリティ事象の記録として何を取得するか、取得した記録の保管期間、取得した記録の保管方法、取得した記録のチェック（監査等）方法等を明確にする。

取得することが望ましい情報は以下のとおり。

a）利用者 ID
b）主要な事象の日時及び内容（例：ログオン、ログオフ、下記 c) d)）の事象発生）
c）システムへのアクセスの成功及び失敗した試みの記録
d）特権の利用
e）アクセスされたファイル及びアクセスの種類
f）ネットワークアドレス及びプロトコル

１１．１．12. ログの保護

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すること。

システムログに含まれているデータが改ざん又は削除されると、セキュリティ上、誤った判断をする場合がある。システムログを保護するために、システム管理者の管理外にあるシステムにログを逐次複製するのが望ましい。

１１．１．13. 作業記録

システムの実務管理者及び運用担当者の作業は、記録し、そのログを保護すること。

１１．１．14. ソフトウェア導入

運用システムに関わるソフトウェアの導入を管理するための手順を定めること。

手順には、以下を含めること。

① サポートの失効したソフトウェアを導入することについてのリスクを考慮する。
② ソフトウェアをアップグレードすることを決定する際には、アップグレードに対する事業上及び情報セキュリティ上の要求を考慮に入れる。

ソフトウェア供給者による物理的又は論理的アクセスは、サポート目的で必要なときにのみ、許可すること。また、その活動を監視する。

１１．１．15. 技術的脆弱性

利用中のシステムに関わる技術的脆弱性に関する情報を定期的に入手し、更新すること。

脆弱性に組織がさらされているかどうか、開発段階から脆弱性診断を行うこと等により、導入前にあらかじめ脆弱性対策を実施しておくこと。

検知された脆弱性がもたらすリスクを評価した上で、リスクに見合った対処を実施し、実施の記録を残すこと。

クラウドサービスの提供に用いるアプリケーションについて、開発段階から脆弱性診断を行うこと等により、導入前にあらかじめ脆弱性対策を実施しておくこと。
また、クラウドサービスに影響し得る技術的脆弱性の管理状況に関する情報を利用者が利用できるようにすること。

１１．２．システム及び情報の完全性

１１．２．1.　セキュリティ侵害の検知

システム又はシステムコンポーネントにデータ又は機能を埋め込み、データが盗み出されたり、不適切に変更、削除されたりしたかを検知すること。

１１．２．2.　情報の更新

不要になった情報は削除するとともに削除したことを記録するログ情報等を残すこと。

１１．２．3.　代替情報源

主要な情報源が破損しているか利用できない場合、システム又はシステムコンポーネントが重要な機能又はサービスを実行するためのバックアップ及び冗長を行うことが望ましい。

１１．２．4.　情報の断片化

一度システムに侵入されると、失われた情報を回復する方法は、通常は存在しない。従って、情報を異なる要素に分割し、それらの要素を複数のシステム又はシステムコンポーネントと場所に分散することが望ましい。

１２．アプリケーション

１２．１．アプリケーションの情報セキュリティ対策

１２．１．１．　ウイルス対策

クラウドサービスの提供に用いるアプリケーション（データ・プログラム等）についてウイルス等に対する対策を講じること。
ソフトウェアに対する情報セキュリティ対策として、ソフトウェアの構成管理（ソフトウェアのバージョンが正しいこと、意図しないソフトウェアが存在しないことの確認等）を行う。

１２．１．２．　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すること。

１２．１．３．　アプリケーションサービスのトランザクションの保護

アプリケーションサービスのトランザクションに含まれる情報は、次の事項を未然に防止するために、保護すること。

① 不完全な通信
② 誤った通信経路設定
③ 認可されていないメッセージの変更
④ 認可されていない開示
⑤ 認可されていないメッセージの複製又は再生

１２．１．４．　プラットフォーム変更後のアプリケーションの技術的レビュー

プラットフォームを変更する際には、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、試験すること。

１２．１．５．　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、必要な変更だけに限ることが望ましい。また、全ての変更を厳重に管理すること。

１２．２．データの保護

１２．２．１． バックアップ

利用者のデータ、アプリケーションの管理情報及びシステム構成情報の定期的なバックアップを実施すること。
業務要件、セキュリティ要件等を考慮して、バックアップ方法（フルバックアップ、差分バックアップ等）、バックアップ対象（利用者のデータ、アプリケーション等の管理情報及びシステム構成情報等）、バックアップの世代管理方法、バックアップの実施インターバル、バックアップのリストア方法等を明確にすること。

１２．２．２． バックアップ情報の完全性

利用者のデータ、アプリケーションの管理情報及びシステム構成情報の定期的なバックアップを行うサプライチェーン事業者のサービスに関して、障害及び変更の通知を確認次第、内容の把握と対応を行う。

１２．３．セッション管理

１２．３．１． セッションのライフサイクル管理

通信セッションのライフサイクルの制御(生成、破棄、タイムアウト検知)を行うこと。

１２．３．２． セッションの真正性

通信セッションの真正性を保護すること。
セッションの真正性の保護は、パケットレベルではなくセッションレベルでの通信の保護によって、通信セッションの両端で通信相手の身元及び伝送される情報の有効性に関して信頼の根拠を確立する。
システムは、利用者がログアウトした時点で、もしくはその他のセッションが終了した時点でセッション識別子を無効にする。
システムは、ランダム化を施して、一意のセッション識別子を生成する。また、システムが生成したセッション識別子のみを認める。

１２．３．3． セッションのロック

定められたアイドル時間を経過した場合又は利用者から要求された場合、システムがセッションをロックすることによって以降のアクセスを遮断すること。
なお、認証手順として確立された手順を用いたユーザによってアクセスが再確立されるまで、セッションをロックすること。

参考）

「クラウドサービス提供における情報セキュリティ対策ガイドライン（第３版）」
２０２１年９月 総務省

「組織と情報システムのためのセキュリティおよびプライバシー管理策(NIST SP800-53 Rev.5）」
２０２０年９月 ジョイントタスクフォース

「ISO/IEC 27017」