2009 年 11 月
（2009 November）

クラウドコンピューティング
Cloud Computing

情報セキュリティ確保のためのフレームワーク
Information Assurance Framework

ENISA: European Network and Information Security Agency
欧州 ネットワーク情報セキュリティ庁

This is a translation undertaken by IPA and therefore is not official translation of ENISA.
The official version is in English and on the ENISA site http://www.enisa.europa.eu/.

本文書は、ENISA の文書 “Cloud Computing: Information Assurance Framework” を独立行政法人情報処理推進機構（IPA）が翻訳したものであり、ENISA による公式の翻訳ではありません。日本語へ翻訳した本文書の著作権は、IPA に帰属します。
本文書は、原文にできるだけ忠実に翻訳するよう努めていますが、完全性、正確性を保証するものではありません。翻訳監修主体である IPA は、本翻訳物に記載されている情報より生じる損失または損害に対して、いかなる人物あるいは団体にも責任を負うものではありません。原文のありのままの内容を理解する必要のある場合は、ENISA サイトに掲載されている原文をお読み下さい。
http://www.enisa.europa.eu/
http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-information-assurance-framework

この文書は下記団体によって翻訳監修されています
IPA 独立行政法人 情報処理推進機構
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

ENISA について

欧州ネットワーク情報セキュリティ庁（European Network and Information Security Agency：ENISA）は、欧州市場の機能を促進するために設立された欧州連合（EU）の機関である。ENISA は、ネットワークセキュリティと情報セキュリティに携わる EU 加盟国および欧州諸機関の知的集積の中心であり、アドバイスや提言を提供すると共に、グッドプラクティスに関する情報のスイッチボードとして機能している。ENISA は、欧州諸機関、EU 加盟国ならびに民間の企業および産業関係者との連携も促進している。

連絡先

本文書は、以下の者により編纂された：
e-mail: Daniele.catteddu@enisa.europa.eu および Giles.hogben@enisa.europa.eu
Internet: http://www.enisa.europa.eu/

目次

対象読者

本文書は、以下の読者を対象としている：

- 企業、特に中小企業（クラウドコンピューティング技術を採用するリスクを評価し、緩和するため）。
- クラウドプロバイダ（自身のクラウドコンピューティングサービスを法や規則へ適合させるプロセスを標準化するため）。
- 欧州の政策立案者（リスクを緩和するための技術を開発するための研究政策を決定するため）。
- 欧州の政策立案者（クラウドコンピューティング技術に対し、適切な政策および経済的インセンティブ、法的措置、意識向上イニシャチブ等を決定するため）。

メソドロジー

本文書の主だった節は、ISO/IEC 27001/27002 および BS25999 規格で規定されている広範な管理策がベースとなっている。各節の詳細内容は、双方の規格に加え、業界のベストプラクティス要件から導出されている。我々は、本文書の全体を通じて、クラウドプロバイダおよび第三者外部委託利用者に関連のある管理策のみを選択した。

2010 年に公開予定の詳細なフレームワークには、NISTSP800-53 等、上記以外の規格も追加される予定である。

1. 情報セキュリティ確保のためのフレームワーク

ENISA のクラウドコンピューティングリスクアセスメントレポートにおける最も重要な推奨事項の一つは、情報セキュリティ確保のためのフレームワーク、すなわち、以下の目的のために設計された、情報セキュリティの確保のための一連の評価基準である：

1. クラウドサービスを採用する際のリスクの評価（「従来の」組織やアーキテクチャを維持することによるリスクと、クラウドコンピューティング環境に移行することによるリスクとの比較）。
2. 複数のクラウドプロバイダが提供するサービスの比較。
3. 選択したクラウドプロバイダから情報セキュリティに関する保証を得ること。第三者サービスプロバイダに対する効果的なセキュリティ関連の質問表を用意することは、クラウド利用者にとって重大なリソースドレイン（資源の消費）となり、クラウドに特化したアーキテクチャに関する専門的知識がなければ、実現が困難である。
4. 保証に関するクラウドプロバイダの負担を低減する。クラウドインフラストラクチャに特化した、極めて重要なリスクが NIS 保証要件において提示されている。クラウドプロバイダの多くは、大多数の利用者が自身のインフラストラクチャやポリシーに対する監査を要求していることを認識している。これは、セキュリティ担当者にとって非常に大きな負担となり得るもので、インフラストラクチャへアクセスする人をも増加させ、セキュリティ上重要な情報の悪用による攻撃を受けるリスク、重要または機密性の高いデータの窃盗のリスクを著しく増大させる。クラウドプロバイダは、このような要求を扱う明確なフレームワークを確立することによって、この問題に対応する必要がある。

このフレームワークでは、組織がクラウドプロバイダに対し、彼らに預託された情報を彼らが十分に保護することを確認するための一連の質問を提供している。

これらの質問は、最低限必要なベースラインが提供されることを目的としているため、組織は、このベースラインに含まれていない、具体的な要件を追加することができる。

同様に、本文書は、クラウドプロバイダ向けの標準回答形式を示すものではないため、その回答は、自由なテキスト形式で行うこととなる。但し、今回の作業のフォローアップとして開発される予定の、より詳細で包括的なフレームワークへ、これらの質問をインプットとすることで、一貫性のある、比較可能な回答セットを用意する計画である。そのような回答セットにより、プロバイダの情報セキュリティ確保の成熟度を測定するための定量的な測定手段（metrics）が提供されるであろう。

前述の測定手段は、エンドユーザ組織が他のプロバイダにそのまま適用でき、容易に比較することができることを狙いとしている。

2. リスクの管理

リスクの多くを組織外のサプライヤに移転することが可能であっても、リスク移転に伴う実際の費用が認識されることはほとんどないことを考慮しておく必要がある。たとえば、クラウド利用者のデータの不正開示をもたらすセキュリティインシデントは、プロバイダにも金銭的な損失をもたらすことがあるが、マイナスの評判や消費者の信頼喪失、法的な罰則の可能性（PCI－DSS）は、末端利用者側に課せられることになる。このような事態により、金銭的リスク（commercial risk）と他のリスクを区別する重要性が認識させられる。このような点で、金銭的リスクを移転することはできても、現実的なリスクは、常に末端利用者側に残されることになる。

リスクアセスメントの結果に対する対応、特にリスクの緩和措置に充てられる金額および出資のタイプは、組織が緩和する必要のあるリスク、および特定のリスク緩和策の実施に伴う機会の喪失および金融貯蓄の減額幅をベースに決定されるべきである。

クラウド利用者も、自組織の状況に特化したリスク分析を自身で実施すべきである。リスク管理／リスクアセスメントの方法論のいくつかは、http://rm-inv.enisa.europa.eu/rm_ra_methods.html から入手することができる。

ビジネス環境および規制環境が変わり、新たなリスクが発生するにつれて、リスクアセスメントは、一時的なイベントとしてではなく、定期的な活動にすべきである。

3. 法的責任の範囲

下の表は、利用者とプロバイダの間で予想される法的責任の範囲をまとめたものである。

	利用者	プロバイダ
コンテンツの合法性	全面的に責任を負う	電子商取引指令の条項およびその解釈をベースにした免責事項を伴う中間的な責任[1]
セキュリティインシデント（データの漏えい、攻撃を実行するためのアカウントの使用を含む）	締結された条件に従って自身の管理下にあるものに対する善管注意義務を果たす責任	自身の管理下にあるものに対する善管注意義務を欠かないという責任
欧州データ保護法の状況	データ管理者	データ処理者（外部）

[1] （電子商取引指令）指令 2000/31/EC の第 12－15 項に含まれる免責事項と併せて、指令 98/48/EC の第 2 項および指令 2000/31/EC の第 2 項に記載されている、「情報社会サービス」の定義を参照のこと。

4. 責務の範囲

セキュリティインシデントに関して、利用者とプロバイダの間に、セキュリティ関連の役割と責務についての明確な定義と理解が必要である。SaaS の提供と IaaS の提供では、その境界は大きく異なり、後者の場合、利用者側により多くの責務が委任される。典型的（合理的）な責務の範囲は、次の表に示した通りである。*どのサービスを使用する場合*でも、*利用者とプロバイダは、次の表で示した各項目について、どちらが責任を負うかを明確にすべきである。*標準的なサービス条項（すなわち、交渉することができない）を利用する場合、クラウド利用者は、何が自己の責務に含まれるかを検証すべきである。

4.1. SaaS (Software as a Service)

利用者	プロバイダ
－ 収集および処理されたクラウド利用者のデータに関するデータ保護法への適合 － ID 管理システムの維持管理 － ID 管理システムのマネジメント － 認証プラットフォームのマネジメント（パスワードポリシーの実施を含む）	－ 物理的サポートインフラストラクチャ（設備、ラック空間、電力、空調、配線等） － 物理的なインフラストラクチャのセキュリティと可用性（サーバー、ストレージ、ネットワーク帯域等） － OS のパッチ管理と強化手順（利用者の強化手順とプロバイダのセキュリティポリシーとの矛盾の有無の確認） － セキュリティプラットフォームの設定（ファイアウォールルール、IDS/IPS のチューニング等） － システムの監視 － セキュリティプラットフォームのメンテナンス（ファイアウォール、ホスト用 IDS/IPS、ウイルス対策、パケットフィルタリング） － ログの収集およびセキュリティの監視

4.2 PaaS (Platform as a Service)

利用者	プロバイダ
― ID 管理システムの維持管理 ― ID 管理システムのマネジメント ― 認証プラットフォームのマネジメント（パスワードポリシーの実施を含む）	― 物理的サポートインフラストラクチャ（設備、ラック空間、電力、空調、配線等） ― 物理的なインフラストラクチャのセキュリティと可用性（サーバー、ストレージ、ネットワーク帯域等） ― OS のパッチ管理と強化手順（利用者の強化手順とプロバイダのセキュリティポリシーとの矛盾の有無の確認） ― セキュリティプラットフォームの設定（ファイアウォールルール、IDS/IPS のチューニング等） ― システムの監視 ― セキュリティプラットフォームのメンテナンス（ファイアウォール、ホスト用 IDS/IPS、ウイルス対策、パケットフィルタリング） ― ログの収集およびセキュリティの監視

4.3 IaaS (Infrastructure as a Service)

利用者	プロバイダ
― ID 管理システムの維持管理 ― ID 管理システムのマネジメント ― 認証プラットフォームのマネジメント（パスワードポリシーの実施を含む） ― ゲスト OS のパッチ、および強化手順の管理（利用者の強化手順とプロバイダのセキュリティポリシーとの矛盾の有無の確認） ― ゲストセキュリティプラットフォームの設定（ファイアウォールルール、IDS/IPS のチューニング等） ― ゲストシステムの監視	― 物理的サポートインフラストラクチャ（設備、ラック空間、電力、空調、配線等） ― 物理的なインフラストラクチャのセキュリティと可用性（サーバー、ストレージ、ネットワークの帯域等） ― ホストシステム（ハイパーバイザー、仮想ファイアウォール等）

– セキュリティプラットフォームのメンテナンス（ファイアウォール、ホスト用 IDS/IPS、ウイルス対策、パケットフィルタリング） – ログの収集およびセキュリティの監視	

（IaaS における）自身のインフラストラクチャのセキュリティに責任を負うクラウド利用者は、以下の点を考慮すべきである：

4.3.1. IaaS におけるアプリケーションのセキュリティ

IaaS アプリケーションプロバイダは、利用者の仮想環境にあるアプリケーションを「ブラックボックス」として扱うため、利用者のアプリケーションの操作や管理にはいっさい関知しない。「スタック」全体、すなわち、利用者のアプリケーション、ランタイムアプリケーションプラットフォーム（.Net、Java、Ruby、PHP 等）は、利用者側のサーバー（すなわち、プロバイダのインフラストラクチャ上）で稼働し、利用者自身によって管理される。このような理由により、利用者が、クラウドで配備したアプリケーションのセキュリティに全責任を負わなければならないことに留意することは極めて重要である。以下は、セキュアアプリケーションの設計およびマネジメントのベストプラクティスに関連する簡単なチェックリストおよび概要説明である：

– クラウドで配備するアプリケーションは、インターネットの脅威モデルに対応する設計でなければならない（VPC（仮想プライベートクラウド）の一環として配備されている場合でも）。

– クラウドで配備するアプリケーションは、一般的な Web の脆弱性（OWASP ガイド参照）から保護するために、標準的なセキュリティ対策を含めた設計とするか、または、それらの対策を組み込まれなければならない。

– クラウド利用者は、アプリケーションを最新の状態に保つ責任を負う。したがって、パッチ適用計画を備えていなければならない（クラウド内のデータへの不正アクセスを模索するマルウェアやハッカーの脆弱性スキャンから遮蔽できるようアプリケーションの防御を確実にするため）。

– クラウド利用者は、AAA（Authentication（認証）、Authorisation（認可）および Accounting（課金管理））のカスタム実装を安易に行うべきではない。というのも、これらは、適切に実装されない場合に脆弱になるからである。

まとめ – 企業用に配備されるクラウドアプリケーションは、ホスト（およびネットワーク（前節参照））、ユーザアクセス、アプリケーションレベルの制御（セキュリティが確保された Web／オンラインアプリケーションの設計に関する OWASP ガイドを参照）のセキュリティ確保のために、いくつもの管理策を施した上で稼働させなければならない。更に、Microsoft、Oracle、Sun 等の多くの主要ベンダーが、セキュリティを確保するための自社製品の設定方法に関する包括的なドキュメントを公開している点にも留意されたい。

5. 留意事項

次節で詳述する一連の質問は、一般的な管理策から抜粋したものである。これは包括的なリストを意図するものではなく、質問によっては、特定の実装に該当しないものもある。このリストは、共通管理策のベースラインとして利用すべきものであり、利用者は、必要に応じて詳細な管理策を求めるべきである。

5.1 政府機関に対する留意事項

本文書に示す管理策は、主にクラウドプロバイダを評価する中小企業を対象としたものである。これらはまた、次のような条件に該当する政府機関にとっても有用である。*使用するクラウドの特徴は、政府機関の情報分類方式に則って、慎重に考慮されるべきである。*

- パブリッククラウドを使用することは（本文書で提示する質問に対し、良い感触の応答が得られたとしても）、低位の保証クラスに分類されたデータを除き、推奨されない。
- 高位の保証クラスに分類されたデータの場合、本文書で提案しているチェックリストは有効であるが、追加的なチェックで補足されるべきである。本文書では、そのような管理策については触れていないが、含まれるべき項目には以下のものがある：
  * プロバイダは、すべてのデータの物理的な位置に関して、透明性の高い情報を提供し、十分な制御を行っているか？　高位の保証クラスに分類されたデータは、格納場所によって（アクセスが）制限されることが多い。
  * プロバイダは、使用されているデータ分類方式に対応しているか？
  * 利用者のリソースが完全に隔離されていることをプロバイダはどのように保証しているか（たとえば、物理的なマシンを共有していない等）？
  * 物理的なマシンがクラウド利用者間で共有されていないと仮定した場合、マシンが再配置される前に、ストレージ、メモリおよびその他のデータの痕跡をどの程度まで完全に消去しているか？
  * プロバイダは、クライアントのアクセスに対し、物理的なトークンをベースとした二要素認証をサポートまたは命じているか？
  * プロバイダは、ISO/IEC 27001 認証を取得しているか？　その認証の範囲は？
  * プロバイダが使用する製品は、コモンクライテリアによる認証を取得しているか？　認証のレベルは？　その製品のプロテクションプロファイルおよびセキュリティターゲットは？

6. 情報セキュリティ確保のための要件

6.1. 人的セキュリティ

IT 担当者に関する質問の多くは、貴組織の IT 担当者や IT に携わるその他の者への質問内容とほぼ同じであろう。ほとんどのアセスメントと同様に、リスクと費用とのバランスが存在する。

- IT 管理者やシステムにアクセス可能な者を採用する際に、どのようなポリシーと手順を実施しているか？　これには、次の項目が含まれるべきである：
  * 採用前調査（身元、国籍または身分、職歴および信用照会先、犯歴、身元調査（高特権的な役割を果たす上級職員に対して）。
- データの格納場所またはアプリケーションが稼動する場所に応じて、異なったポリシーを採用しているか？
  * たとえば、ある領域で採用するポリシーは、別な領域で採用するポリシーと異なる場合がある。
  * プラクティスは、すべての領域において一貫していなければならない。
  * 機密性の高いデータは、ある特定領域に格納し、適切な担当者が配置される場合がある。
- 職員すべてに対し、どのようなセキュリティ教育プログラムを実施しているか？
- 評価を継続的に実施するためのプロセスが存在するか？
  * 実施頻度は？
  * より詳細な面談
  * セキュリティアクセスおよび権限の見直し
  * ポリシーと手順の見直し

6.2. サプライチェーンにおける情報セキュリティの確保

以下の質問は、クラウドプロバイダの業務遂行上のセキュリティにとって重要な幾つかの業務を第三者に下請契約する場合に適用される（たとえば、SaaS プロバイダが、第三者プロバイダに対して、ベースとなるプラットフォームを外部委託する、または、クラウドプロバイダが、マネージドセキュリティサービスを提供するプロバイダに対し、セキュリティサービスを外部委託する、もしくは、オペレーティングシステムの ID 管理に外部プロバイダを使用する、等）。また、第三者がクラウドプロバイダのインフラストラクチャに物理的またはリモートアクセスする場合も含まれる。したがって、これらすべての質問は、外部委託をしている第三者（第 n 者）クラウドサービスプロバイダにも適用されることが考えられる。

- 貴組織の業務遂行上のセキュリティ（可用性を含む）にとって重要な鍵となり、貴組織のサービスデリバリーサプライチェーンのもとで外部委託される、または下請契約されるサービスを定義せよ。
- 貴組織のインフラストラクチャに（物理的に／論理的に）アクセスする第三者（の身元）を保証

するために使用される手順を詳述せよ。

* 外部委託先および下請契約者を監査しているか？その頻度は？

- 外部委託先によって保証される SLA 規定のうち、貴組織が顧客に対して提供している SLA 規定よりも（サービスレベルが）低いものが存在するか？　存在する場合、貴組織では、サプライヤの冗長化 (supplier redundancy)を実施しているか？
- 第三者サービスに求められるサービスレベルの達成および維持を確実にするために、どのような対策が取られているか？
- クラウドプロバイダは、自身のセキュリティポリシーおよび管理策が、（契約に従って）第三者プロバイダにも適用されていることを確認することができるか？

6.3. 運用上のセキュリティ

外部プロバイダとの契約（commercial agreement）には、すべてのネットワーク関連サービスについてのサービスレベルが含まれることが期待される。とはいうものの、末端利用者は、プロバイダとの間の明示的な契約に加えて、不正な開示を防止するための適切な管理策がプロバイダによって導入されていることを確認すべきである。

- 変更管理手順およびポリシーについて詳述せよ。これには、変更の結果として生じるリスクを再評価するためのプロセスを含めると同時に、評価結果を末端利用者が利用できるかどうかを明示すべきである。
- リモートアクセスポリシーを定義せよ。
- プロバイダは、情報システムの文書化された操作手順書を維持管理しているか？
- リスクを低減するための段階的な環境（たとえば、開発環境、テスト環境および運用環境）が存在するか、また、それらの環境は独立しているか？
- 末端利用者のアプリケーションや情報をホスティングするシステムを保護するために採用されているホストおよびネットワーク管理策について記述せよ。これには外部規格による認証（たとえば、ISO/IEC 27001 の認証など）の詳細が含まれるべきである。
- 不正プログラムから保護するために使用される管理策について詳述せよ。
- 配備されているセキュリティ設定は、承認されたモバイル・コードおよび機能の実行のみを許可しているか（たとえば、特定のコマンドのみを実行可能とする）？
- バックアップに関するポリシーおよび手順を詳述せよ。これには、取り外し可能な媒体の管理手順および不要になった媒体を確実に破壊する手法が含まれるべきである（業務上の必要性から、末端利用者が独自のバックアップ戦略を実施したいと考える場合がある。これは、バックアップに対するタイムクリティカルな（スピード重視の）アクセスが必要となる場合に特に関係する）。

監査ログは、調査が必要なインシデントが発生した場合に使用される。また、問題を解決するために使用することもできる。これらの目的のため、末端利用者は、以下の情報を利用することができるという保証が必要になる。

- プロバイダは、監査ログにどのような情報が記録されているか、詳しく述べることができるか？
  * このデータが保存される期間は？
  * 監査ログを分割して、他のクラウド利用者を煩わせることなく、当該利用者／法執行機関だけが利用できるようにし、更に、法廷でも有効なログデータを提供することができるか？
  * 不正アクセスまたは改ざんからログを保護するために、どのような管理策が導入されているか？
  * 監査ログの完全性を確認し、保護するために、どのような手法が使用されているか？
  * 監査ログのレビュー方法は？　記録されたイベントのうち、どれに対して行動を起こすか？
  * システム（複数）の時刻を合わせて、監査ログの正確なタイムスタンプを得るために、どのようなタイムソースが使用されているか？

6.3.1. ソフトウェアのセキュリティ確保

- 使用するオペレーティングシステムおよびアプリケーションソフトウェアの完全性を保護するために使用される管理策を定義せよ。参照している規格も含めよ（たとえば、OWASP、SANS Checklist、SAFECode 等）。
- 新たにリリースされたソフトウェアが目的にかなっているか、あるいはリスク（バックドア、トロイの木馬等）を含んでいないかを、どのように立証するか？　使用する前にこれらをレビューしているか？
- アプリケーションのセキュリティ確保のために、どのような実践規範に従っているか？
- リリースされたソフトウェアに脆弱性が含まれていないことを保証するためのペネトレーションテストを実施しているか？　脆弱性が発見された場合の修正プロセスとして、どのようなプロセスが用意されているか？

6.3.2. パッチマネジメント

- 実施すべきパッチマネジメント手順を詳述せよ。
- パッチマネジメントプロセスが、クラウドを提供するための技術、すなわち、ネットワーク（インフラストラクチャの構成要素、ルータやスイッチ等）、サーバーのオペレーティングシステム、仮想化ソフトウェア、アプリケーションおよびセキュリティのサブシステム（ファイアウォール、ウイルス対策ゲートウェイ、侵入検知システム等）の全階層に対応していることを保証できるか？

6.3.3. ネットワークアーキテクチャの管理策

- DDoS（分散サービス運用妨害）攻撃を緩和するために使用される管理策を定義せよ。
  * 多重防御（ディープパケット分析、トラフィックスロットリング、パケットブラックホーリング等）。
  * （クラウドプロバイダのネットワークから派生する）「内部的な」攻撃や（インターネットや

クラウド利用者ネットワークから派生する）外的な攻撃に対する防御策を備えているか？

- どのレベルの隔離策が使用されているか？
  * 仮想マシン、物理マシン、ネットワーク、ストレージ（たとえば、ストレージエリアネットワーク）、管理用ネットワークおよび管理支援システム等。
- 企業とサービスプロバイダ間の通信が途絶した場合も、アーキテクチャは、クラウドによって提供されている業務に継続的に対応するか（たとえば、末端利用者の LDAP システムに強く依存しているか）？
- クラウドプロバイダが使用する仮想ネットワークインフラストラクチャ（PVLAN/VLAN タギング 802.1q アーキテクチャにおいて）は、ベンダーの規格、および／もしくはベストプラクティスに特化した規格に適合する形でセキュリティの確保がなされているか（たとえば、MAC スプーフィング、ARP ポイゾニング攻撃等が、特定のセキュリティ設定によって回避されているか）？

6.3.4. ホストアーキテクチャ

- プロバイダは、仮想イメージがデフォルトで強化されていることを保証できるか？
- 強化された仮想イメージは、不正アクセスから保護されているか？
- プロバイダは、仮想化されたイメージに認証情報が含まれていないことを確認できるか？
- ホストのファイアウォールは、仮想システムのサービスをサポートするのに必要な、必要最低限のポートのみで動作しているか？
- ホストベースの侵入防止サービス（IPS）を、仮想システム上で稼動させることは可能か？

6.3.5. PaaS － アプリケーションのセキュリティ

一般的に、PaaS サービスプロバイダは、プラットフォームソフトウェアスタックのセキュリティに責任を負い、本文書が提供している提言は、PaaS プロバイダが、自身の PaaS プラットフォームを設計、管理する際に、セキュリティポリシーを考慮したかどうかを判断するための、適切な材料となる。PaaS プロバイダが、どのように自身のプラットフォームのセキュリティを確保しているかといった詳しい情報を取得するのは困難な場合が多い － しかしながら、以下の質問と本文書の他の節の質問を組み合わせることによって、PaaS プロバイダが提供するセキュリティを評価する際の一助となるであろう。

- 複数の利用者が共有するアプリケーションがどのように分離されているかの情報を要求せよ － 封じ込めおよび隔離策の概要が必要である。
- 貴組織のデータへのアクセスが貴組織のユーザおよび貴組織が所有するアプリケーションに限定されることに関して、PaaS プロバイダは、どのような保証を提供することができるか？
- プラットフォームのアーキテクチャは、クラシックな「サンドボックス」とすべきである － プロバイダは、PaaS プラットフォームのサンドボックスが、新たなバグや脆弱性について監視されていることを保証しているか？
- PaaS プロバイダは、（利用者間で再利用可能な）一連のセキュリティ機能を提供できるべきであ

る － これらのセキュリティ機能には、ユーザ認証、シングルサインオン、権限付与（特権管理）および（API を経由して利用可能な）SSL／TLS が含まれているか？

6.3.6. SaaS － アプリケーションのセキュリティ

SaaS モデルは、プロバイダに、末端利用者に提供される一連のアプリケーションすべてを管理するよう命じている。したがって、SaaS プロバイダは、これらのアプリケーションのセキュリティの確保に主な責任を負う。通常、顧客は、運用上のセキュリティプロセス（ユーザおよびアクセス管理）に責任を負う。但し、以下の質問および本文書の他の節の質問を組み合わせることによって、SaaS プロバイダが提供するセキュリティを評価する際の一助となるであろう：

- アドミニストレーションコントロール（administration control）にはどのようなものがあり、これらは他のユーザに対して読み取り／書き込み権限を割り当てるために使用することができるか？
- SaaS のアクセス制御が詳しく定義され、貴組織のポリシーに対応するようカスタマイズすることができるか？

6.3.7. リソースの割当

- リソースが過負荷となった場合（処理、メモリ、ストレージ、ネットワーク）、
  * リソースの提供時に不具合が生じた場合、自身のリクエストに割り当てられた相対的優先順位に関して、どのような情報が与えられるか？
  * サービスレベルや要件の変更に、リードタイムは存在するか？
- どの程度のスケールアップが可能か？　プロバイダは、最短期間内に最大限利用可能なリソースについての保証を提供しているか？
- スケールアップの速度は？　プロバイダは、最短期間内に補助リソースの可用性についての保証を提供しているか？
- リソースの使用における大規模な傾向（たとえば、季節的な影響）を扱うために、どのような手順を用意しているか？

6.4. ID 管理およびアクセス管理

以下の管理策は、クラウドプロバイダの ID およびアクセス管理システム（クラウドプロバイダの管理下にある）に適用される。

6.4.1. 権限付与

- クラウドシステム全体において、全システムにわたる特権を持つアカウントは存在するか？　存在する場合、どの操作（読み取り／書き込み／削除）に対してか？
- 最高レベルの特権を持つアカウントは、どのように認証され、管理されているか？

- 最重要な決定（たとえば、大規模なリソースブロックの割り当ての一斉解除等）は、どのように承認されるか（単独または複数による承認、および、組織内のどの役割によって承認されるか）？
- 高位特権の役割は同じ人物に割り当てられているか？　この割り当てにより、職務の分離や最小権限の原則に違反しないか？
- 役割ベースのアクセス制御（RBAC）を使用しているか？　最小権限の原則を遵守しているか？
- 緊急時において、特例のアクセスを許可するために、管理者の権限および役割に対してどのような変更（存在する場合）が行われるか？
- 利用者に対して、なんらかの「管理者」的な役割が割り当てられているか？　たとえば、利用者側の管理者は、（ベースとなるストレージに対する変更は許可されていないものの）新しいユーザを追加する役割を有するか？

6.4.2. ID の割当

- ユーザアカウントの ID を登録する際に、どのような確認がなされているか？　参照している規格はあるか？　たとえば、電子政府の相互運用性のフレームワーク等は？
  * 要求されているリソースに基づき、ID 確認を異なるレベルで行っているか？
- クレデンシャルの割り当て解除には、どのような手順が用意されているか？
- クレデンシャルは、クラウドシステム全体にわたって一斉に割り当て／解除されているか？　または、地理的に複数の場所に跨って分散しているクレデンシャルを解除する際のリスクは存在するか？

6.4.3. 個人データの管理

- ユーザディレクトリ（たとえば、AD、LDAP）およびそのアクセスに際し、どのようなデータストレージおよび保護管理策が適用されているか？
- ユーザディレクトリのデータは、相互運用性のある形式でエクスポートが可能か？
- クラウドプロバイダ内のクラウド利用者のデータへのアクセスは、必知事項に基づいているか？

6.4.4. 鍵管理

以下は、クラウドプロバイダの管理下にある鍵が対象である。

- クラウドプロバイダの管理下にある鍵を読み／書きするためのセキュリティ管理策が存在するか？　たとえば、強力なパスワードポリシー、独立したシステムに格納されている鍵、ルートの認証鍵用のハードウェアセキュリティモジュール（HSM）、スマートカードに基づく認証、ストレージに対する直接アクセスの遮断、有効期間の短い鍵等。
- これらの鍵を使用して、データに署名したり、データを暗号化する際に適用できるセキュリティ管理策は存在するか？
- 鍵が危殆化した場合に取られる手続きは存在するか？　たとえば、鍵失効リスト等。

- 鍵の失効は、複数サイトで同時に発生する問題に対処できるか？
- クラウド利用者のシステムイメージは保護または暗号化されているか？

6.4.5. 暗号化

- 暗号化は、いくつかの場面で使用することができる － どのような場面で使用されているか？
  * データの送信時
  * データの保管時
  * メモリ上もしくは処理中のデータ
- ユーザ名やパスワード？
- 何を暗号化すべきで、何を暗号化すべきではないかを明確に定義するポリシーが存在するか？
- アクセス鍵は誰が所有しているか？
- 鍵はどのように保護されているか？

6.4.6. 認証

- 高位な保証を要求する業務には、どのような形式の認証が使用されているか？　これには、マネジメントインターフェースへのログイン、鍵生成、複数ユーザアカウントへのアクセス、ファイアウォール設定、リモートアクセス等が含まれる。
  * インフラストラクチャにおける、ファイアウォール等の重要なコンポーネントを管理するために、二要素認証が採用されているか？

6.4.7. クレデンシャルの危殆化または盗難

- 異常を検知する機能を備えているか（特異であり、潜在的に悪質であると思われる IP トラフィック、およびユーザまたはサポートチームの行動を察知する機能）？　たとえば、失敗／成功したログインの分析、特異な時間帯のログイン、複数同時のログイン等。
- クラウド利用者のクレデンシャルが盗まれた場合の規定として、どのような規定が存在するか（検知、失効、活動の証拠）？

6.4.8. クラウド利用者に提供される ID 管理およびアクセス管理システム

以下の質問は、クラウド利用者による使用および管理を目的として、クラウドプロバイダによって提供される ID およびアクセス管理システムに適用される。

6.4.8.1. ID 管理のフレームワーク

- システムは、高位保証（必要な場合には、OTP システム）と低位保証（たとえば、ユーザ名およ

びパスワード）の双方に対して相互運用が可能な連合 IDM インフラストラクチャを許可しているか？

- クラウドプロバイダは、第三者 ID プロバイダとの相互運用が可能か？
- シングルサインオンを組み込む能力があるか？

6.4.8.2. アクセス制御

- クライアントのクレデンシャルシステムは、役割や責任の分割および複数のドメイン（または、複数のドメイン、役割、責任に対する単一の鍵）を許可しているか？
- クラウド利用者システムのイメージに対するアクセスをどのように管理しているか、また、認証鍵や暗号化鍵が、システムイメージ内に含まれていないことをどのように保証しているか？

6.4.8.3. 認証

- クラウドプロバイダは、クラウド利用者に対して自身をどのように識別させているか（すなわち、相互的な認証はあるか？
  * クラウド利用者が API コマンドを送信する時？
  * クラウド利用者が管理インターフェースにログインする時？
- 連合認証メカニズムに対応しているか？

6.5. 資産の管理

クラウドプロバイダの制御下にあるハードウェアおよびソフトウェア（アプリケーション）資産の最新のリストが維持管理されていることを保証することは、重要である。これにより、すべてのシステムに適切な管理策が導入されていることと、そのシステムがインフラストラクチャへのバックドアとして使用できないことに対する確認が可能になる。

* プロバイダは、すべての資産の適切な管理を容易にする自動化されたインベントリ（資産一覧作成）手法を備えているか？
* クラウド利用者が特定の期間にわたって使用した資産リストが存在するか？

以下の質問は、末端利用者が追加的な保護を必要とするデータ（すなわち、機密性が高いとみなされる）を配備している場合に使用される。

- 資産は、機密性や重要度で分類されているか？
  * その場合、プロバイダは、資産分類の異なるシステムを適切に区分する手法を採用しているか？また、セキュリティ分類の異なるシステムを所有する単独利用者のために、それらのシステムを適切に区分する手法を採用しているか？

6.6. データおよびサービスのポータビリティ

以下は、ベンダーのロックインに関するリスクを理解するために、考慮すべき質問集である。

- クラウドからデータをエクスポートするための文書化された手順や API が存在するか？
- ベンダーは、クラウドに格納されているすべてのデータに対し、相互運用可能なエクスポート形式を提供しているか？
- SaaS の場合、使用する API インターフェースは標準化されているか？
- ユーザが作成したアプリケーションを標準的な形式でエクスポートするための規定があるか？
- データを別のクラウドプロバイダにエクスポートできるかどうかテストするための手順があるか ー たとえば、クライアントがプロバイダを変更したい場合に？
- クライアントは、データ形式が共通であることを検証し、別のクラウドプロバイダに移行できるかどうかを検証するため、自身でデータを抽出できるか？

6.7. 事業継続管理

組織にとって、事業継続性の提供は重要である。（障害時の目標復旧時間等の）時間系に関する詳細を盛り込んだサービスレベルアグリーメントを用意することは可能であるが、考慮すべき様々な問題点が残されている。

- プロバイダは、サービスの中断による影響を詳述するための文書化された手法を維持管理しているか？
  * サービスの RPO（目標復旧地点）および RTO（目標復旧時間）はどのように設定されているか？　サービスの重要性に従って詳述せよ。
  * 復旧プロセスにおいて、情報セキュリティ活動が適切に実施されているか？
  * サービスの中断時における末端利用者への通信ラインは何か？
  * サービスの中断時の対応に関するチームの役割と責任は明確に定義されているか？
- プロバイダは、復旧の優先順位を分類しているか、また、復旧時の我々（末端利用者）の相対的優先順位はどうなっているか？　注：分類の例としては、（高／中／低）が考えられる。
- 復旧プロセスに関する依存関係として、どのような関係が存在するか？　サプライヤおよび外部委託パートナーを含めること。
- 主要なサイトが利用不可能な状態に陥った場合、第二サイトへの最小距離はどれくらいが望ましいか？

6.7.1. インシデントマネジメントおよびインシデント対応

インシデントマネジメントおよびインシデント対応は、事業継続管理の一部である。このプロセスのゴールは、予測不可能で、サービスの中断につながる可能性のあるイベントによる影響を、組織が容認できるレベルまで抑えることである。

情報セキュリティインシデントの発生可能性を最小限に留め、マイナスの影響を低減するための組織の能力を評価するためには、クラウドプロバイダには以下の質問をするべきである。

- プロバイダは、インシデントを検知、識別、分析および対応する正式なプロセスを備えているか？
- インシデント対応プロセスが効果的であることを確認するために、プロセスのリハーサルを行っているか？　リハーサル時に、クラウドプロバイダがサポートする組織の利用者すべてが、そのプロセスとインシデント対応時の役割（インシデント発生時および事後分析の双方）を理解していることも保証しているか？
- インシデントの検知機能はどのように構成されているか？
  * クラウド利用者は、システムの異常やセキュリティイベントをプロバイダにどのように報告できるか？
  * クラウドプロバイダは、クラウド利用者が選択した第三者 RTSM（リアルタイムセキュリティ監視）サービスに対して、彼らのシステムに介入する（適切な場合）、または、彼らとインシデント対応能力の調整を行えるようにするために、どのようなファシリティを許可しているか？
  * リアルタイムセキュリティ監視（RTSM）サービスは存在するか？　そのサービスは外部委託されているか？　どのようなパラメータやサービスが監視されているか？
  * セキュリティインシデントに関する定期報告を（要求に応じて）提供しているか？（たとえば、ITIL 定義に従って）
  * セキュリティログが保存されている期間は？　これらのログは安全に保管されているか？　このログへのアクセス権を持っているのは誰か？
  * クラウド利用者は、仮想マシンイメージで、HIPS／HIDS を構築することが可能か？　クラウド利用者の侵入検知・防止システムによって収集された情報を、クラウドプロバイダまたは第三者の RTSM サービスに統合することができるか？
- 重要度はどのように定義されているか？
- エスカレーション手順はどのように定義されているか？　クラウド利用者が関与するのはいつか（関与することがある場合）？
- インシデントの文書化と証拠の収集はどのように行われるか？
- 認証、課金管理、監査の他に、内部者による悪意の行動を防止する（あるいは影響を最小限に留める）ための管理策にはどのようなものが存在するか？
- プロバイダは、クラウド利用者に対し（リクエストに応じ）、仮想マシンのフォレンジックイメージを提供しているか？
- プロバイダは、インシデントの測定方法(metrics)や指標（すなわち、月ごとの検知または報告されたインシデントの数、クラウドプロバイダの下請業者が原因で発生したインシデントの数、および、そのようなインシデントの総数、インシデントの平均対応時間および回復時間等）を収集しているか？

* 上記の項目の中で、プロバイダが一般に公開しているのはどれか？（注：利用者の機密性が損なわれたり、セキュリティ上重要な情報が開示される恐れがあるため、インシデント関連で報告されたすべてのデータが公開されるわけではない。）

- プロバイダは、どのくらいの頻度で災害復旧計画および事業継続計画についてのテストを実施しているか？
- プロバイダは、SLA（サービスレベルアグリーメント）に適合するレベルでデータを収集しているか？
- プロバイダは、ヘルプデスクに対するテストを実施しているか？　たとえば、
  * なりすましに関するテスト（パスワードのリセットを要求している電話の人物が、本当に名乗っている本人かどうか？）、または「ソーシャル・エンジニアリング」と呼ばれる攻撃等。
- プロバイダは、侵入テストを実施しているか？　その頻度は？　侵入テストでは、実際にどのような項目がテストされるのか？ － たとえば、あるイメージから別のイメージを取り出すことができないこと、および、ホストインフラストラクチャにアクセスできないことを確認するために、各イメージのセキュリティ独立性をテストしているか？　このテストでは、クラウドプロバイダの管理・支援システムに、仮想イメージを介してアクセスすることができるか否かについても確認すべきである（たとえば、プロビジョニングおよびアドミンアクセス制御システム等）。
- プロバイダは、脆弱性テストを実施しているか？　その頻度は？
- 脆弱性を修正するプロセスにはどのようなものがあるか（ホットフィックス、再構成、ソフトウェアを最新バージョンに更新する等）？

6.8.　物理的セキュリティ

人的なセキュリティと同様、IT インフラストラクチャが第三者の管理下にあるために、物理的セキュリティにおいても多くの潜在的な問題が存在する － 従来の外部委託のように、複数のクラウド利用者（組織）が物理的セキュリティ侵害の被害を受ける可能性がある。

- ロケーションに関する物理的セキュリティに関して、どのような保証をクラウド利用者に提供できるか？　例を挙げ、遵守している規格（たとえば、ISO/IEC 27001 の第 9 章）を示しなさい。
  * 権限を付与された IT 担当者以外で、IT インフラストラクチャに、つきそい人無しで（物理的に）アクセスできる者は誰か？
    - たとえば、清掃員、マネージャー、「物理的セキュリティ」担当者、契約者、コンサルタント、ベンダー等。
  * アクセス権はどの程度の頻度で見直されているか？
    - アクセス権の取り消しには、最短でどれくらいかかるか？
  * セキュリティリスクアセスメントと周辺環境の評価を定期的に実施しているか？
    - その頻度は？
  * 隣接する建物等を含め、定期的なリスクアセスメントを実施しているか？

* セキュリティが確保された領域にアクセスする（第三者を含む）者を制御または監視しているか？
* 機器のロード、アンロードおよびインストールに関して、どのようなポリシーまたは手順を備えているか？
* インストールする前に、配送品のリスクを検査しているか？
* データセンターにある備品の最新の在庫リストが存在するか？
* ネットワークケーブルは、公共のアクセス領域に設置されているか？
  - 外装されたケーブルまたは導管を使用しているか？
* 不正な機器が設置されていないよう、周辺を定期的に確認しているか？
* 離れた場所で機器を使用しているか？
  - それはどのように保護されているか？
* 担当者は、データセンターにアクセス可能な可搬機器（たとえば、ノート型 PC、スマートフォン等）を使用しているか？
  -それらはどのように保護されているか？
* アクセスカードを制御するために、どのような対策が取られているか？
* 古いメディアやシステムを廃棄する必要がある場合、どのようなプロセスまたは手順を実施しているか？
  -データを上書き？
  -物理的な破壊？
* 機器をあるサイトから別のサイトへ移動する際に、どのような承認プロセスが実施されているか？
  - この作業を行う権限を付与されている担当者（または契約者）をどのように識別しているか？
* 機器の不正な持ち出しを監視するための監査の実施頻度は？
* その環境が、該当する法律および規則を遵守していることを保証するための確認は、どれくらいの頻度で行われているか？

6.9. 環境に関する管理策

- 環境的な問題がサービス中断の原因とならないことを保証するために、どのような手順またはポリシーが設定されているか？
- 火災、洪水、地震等の被害を防ぐために、どのような対策を講じているか？
  * 自然災害が発生した場合、物理的アクセスを保護するために、どのような追加のセキュリティ対策が実施されるか？
  * 主要なサイトおよび二次サイトの双方？

- データセンターの室温と湿度を監視しているか？
  - 空調への配慮または監視をしているか？
- 建物を落雷から保護しているか？
  - 電子・電気通信ラインが含まれているか？
- 停電時に備えて、独立した発電機を備えているか？
  - 給電可能時間は？
  - 適切な燃料供給はあるか？
  - フェールオーバー用発電機はあるか？
  - 無停電電源装置（UPS）の確認頻度は？
  - 発電機の確認頻度は？
  - 複数の給電装置を備えているか？
- すべてのユティリティ（電力、水等）が、貴組織のシステム環境をサポート可能か？
  - そうであることの再評価およびテストの実施頻度は？
- エアコンは、貴組織のシステム環境をサポート可能か？
  - そうであることのテストの頻度は？
- 製造会社が推奨するメンテナンススケジュールに従っているか？
- 承認されたメンテナンスまたは修理担当者のみに、サイトへのアクセスを許可しているか？
  - 担当者の身元確認の方法は？
- 機器を修理に出す場合、まずデータの消去を行っているか？
  - その方法は？

6.10. 法的要求事項

クラウドプロバイダサービスの利用者および潜在的な利用者は、法的枠組みにおけるそれぞれの国家および超国家的義務を考慮すべきであり、それらの義務が適切に遵守されていることを保証すべきである。

利用者がクラウドプロバイダに対して問うべき、法律に関する主な質問は以下の通りである：

- クラウドプロバイダが所在する国は？
- クラウドプロバイダのインフラストラクチャは、同じ国に存在するのか、別の国か？
- クラウドプロバイダは、そのクラウドプロバイダのインフラストラクチャとは別のインフラストラクチャを所有する他の会社を使っているか？
- データが物理的に存在する場所は？
- 契約条件の司法管轄権と、データ自体の司法管轄権は、分割されるか？
- クラウドプロバイダのサービスのいずれかは、下請け契約されるか？

- クラウドプロバイダのサービスのいずれかは、外部委託されるか？
- クラウド利用者（および利用者の顧客）から提供されたデータは、どのように収集、処理および転送されるか？
- 契約が終了した場合、クラウドプロバイダに送信されたデータはどうなるか？