2009 年 11 月
（2009 November）

クラウドコンピューティング
Cloud Computing

情報セキュリティに関わる利点、リスクおよび推奨事項
Benefits, risks and recommendations for information security

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

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。

本文書は、ENISA の「Emerging and Future Risk programme（新興および将来のリスクに対応するための計画）」を背景として作成されている。

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

貢献者のリスト

本文書は産業界、学術機関および政府機関の専門家を始めとする、選択された、クラウドの専門知識を持つグループから寄せられた情報やコメントを基に、ENISA の編集者が編纂したものである。

本文書は、特に明記しない限り ENISA の編集者の見識を示したものであり、（本文書の作成に）参加した専門家による意見を必ずしも反映させたものではない。

Alessandro Perilli	Virtualization.info (Independent Analyst)
Andrea Manieri	Ingegneria Informatica
Avner Algom	The Israeli Association of GRID Technologies
Craig Balding	Cloudsecurity.org
Dr. Guy Bunker	Bunker Associates
John Rhoton	Independent Consultant
Matt Broda	Microsoft
Mirco Rohr	Kaspersky
Ofer Biran	IBM
Pete Lindstrom	Spire Security
Dr Peter Dickman, Engineering Manager	Google Inc.
Philippe Massonet	Reservoir Project, CETIC
Raj Samani	Information Systems Security Association, UK
Simon Pascoe	British Telecom
Srijith K. Nair, Theo Dimitrakos	The BEinGRID Project, British Telecom
Dr Simone Balboni	University of Bologna
Various	National Health Service (NHS) Technology Office, UK
Various	RSA
Various	Symantec, Symantec Hosted Services

法的情報に関する貢献者

Dr. Paolo Balboni	Baker & McKenzie – Tilburg University
Kieran Mccorry	Hewlett Packard
W. David Snead, P.C.	Attorney and Counselor

エグゼクティブサマリー

本文書の主な結論は、セキュリティの視点から見た場合、クラウドの規模の経済と融通性は、味方であると同時に敵でもあるということである。大量に集約されたリソースとデータは、攻撃者にとって恰好の標的であるが、クラウドをベースにした防御はより強力であり、拡張性があり、費用対効果も優れている。本文書は、クラウドコンピューティングを利用する上でのセキュリティリスクと利点についての評価（informed assessment）を可能にするものであり、クラウドコンピューティングの潜在ユーザ・既存ユーザに対して、セキュリティのガイダンスを提供している。

クラウドコンピューティングは、*新たな技術*ではなく、コンピューティングリソースを配布するための、新たな方法である。データの格納・処理からソフトウェアに至るまでのコンピューティングサービス（電子メールの扱いを含む）は、現在、制約を受けることなく、必要に応じて即座に利用することができる。我々は今、緊縮経営の時代を迎えているため、コンピューティングサービスのこの新たな経済モデルは、地に根を下ろし、全世界的な巨大投資がなされてきている。IDC の分析によると、2009 年における世界のクラウドサービスの規模は、ほぼ 174 億ドルに達すると見込まれており(1)、2013 年には、442 億ドルまでに成長すると予想されている。この予想には、2008 年に 9 億 7100 万ユーロであった欧州市場の規模が、2013 年には、60 億 500 万ユーロに拡大するとの見込みも含まれている。(2)。

本文書の主な結論は、セキュリティの視点から見た場合、クラウドの規模の経済と融通性は、味方であると同時に敵でもあるということである。大量に集約されたリソースとデータは、攻撃者にとって恰好の標的であるが、クラウドをベースにした防御はより強力であり、拡張性があり、費用対効果も優れている。本文書は、クラウドコンピューティングを利用する上でのセキュリティリスクと利点についての評価（informed assessment）を可能にするものであり、クラウドコンピューティングの潜在ユーザ・既存ユーザに対して、セキュリティのガイダンスを提供している。

セキュリティの評価は、次の 3 つのユースケースシナリオに基づいている：1) 中小企業のクラウドコンピューティングサービスへの移行、2) サービスの障害耐性(resilience)に対するクラウドコンピューティングの影響、3) 電子政府におけるクラウドコンピューティング（例、e ヘルス）。

この新たな経済モデルは、以下の点で、技術的変化の要因ともなっている：

規模：コモディティ化および経済的効率性への誘導によって、サービス提供に必要なハードウェアリソースの大量集約化が導かれた。その結果、コンピューティングサービスの提供に必要なすべての種類のリソースに関して、規模の経済が助長された。

アーキテクチャ：リソースの最適利用には、基盤となるハードウェアから抽出されるコンピューティングリソースが必要となる。ハードウェアおよびソフトウェアリソースを共有する個別利用者は、自身のデータを保護するために、論理的な隔離メカニズムに依存している。コンピューティング、コンテンツの格納および処理は、大規模分散される。コモディティのグローバル市場では、顧客から可能な限り近い場所でコンテンツを送受信する末端分散ネットワークが必要となる。このグローバルなサービス提供

および冗長性というものは、リソースが、通常、物理的にも論理的にも大量に一括管理されていることを意味している。

> そのような状況であるにもかかわらず、政府機関および中小企業の双方は、それが正式なポリシーであるかないかにかかわらず、多くの従業員がクラウドをベースとしたサービスを使用することになるであろうという現実に直面している。

多くの中小企業にとって、費用の削減と柔軟性をもたらすクラウドコンピューティングへの移行は抗いがたい流れである。ただし、本文書の一環として実施した調査の結果（Survey – An SME Perspective on Cloud Computing参照）によれば、クラウドに移行する中小企業の主な懸念は、彼らの情報の機密性と、インフラストラクチャ関連のインシデントへの彼らの責任である。

政府機関も IT 関連の費用削減と職務実行能力の拡大のために、クラウドコンピューティングの使用に興味を示している。たとえば、米国政府の GSA（General Services Administration：一般調達局）は、クラウドコンピューティングサービスのポータルサイトを提供している(3)。政府機関においても、国民の個人情報を安全に処理しなければならないといった観点から、クラウドコンピューティングのインフラストラクチャにおいては、乗り越えなければならないハードルは高い。更に、多くの電子政府のアプリケーションのクラウドへの移行を妨げる、法律や規則に関する障壁も存在する。そのような状況であるにもかかわらず、政府機関および中小企業の双方は、それが正式なポリシーであるかないかにかかわらず、多くの従業員がクラウドをベースとしたサービスを使用することになるであろうという現実に直面している。

クラウドコンピューティングが、その技術によって約束された最大能力に到達するためには、確固たる情報セキュリティを提供しなければならない。本文書では、具体的なシナリオを基に、ネットワークと情報のセキュリティ、およびデータの保護とプライバシーにとって、クラウドコンピューティングが何を意味しているのかを説明している。本文書では、クラウドコンピューティングによって提供されるセキュリティ上の利便性と、そのリスクについて考察する。また、本文書では、（クラウドの）技術、ポリシーおよび法律に関わる事項を取り扱う。そして、最も重要なこととして、リスクに対応し、利便性を最大限に引き出すための、具体的な提言を示す。

最後に、クラウドコンピューティングとは、サービスとしてのアプリケーション／ソフトウェア（SaaS）、サービスとしてのプラットフォーム（PaaS）、およびサービスとしてのインフラストラクチャ（IaaS）を含む、いくつかの異なるサービス種別を指し示す場合があるという点に注意することが重要である。関連するリスクと利便性は、モデルごとに異なるため、サービスを契約する際の重要な考慮事項も、それぞれに異なる。以下の各節では、クラウドモデルごとに適用されるリスクや利便性に相違がある場合は、それらの区別に努めている。

主要な推奨事項

クラウド利用者に対する保証

クラウド利用者には、利用者とプロバイダの双方が直面するリスク（例、DDoS 攻撃等）を緩和するために、プロバイダが健全なセキュリティプラクティスに従っているという保証が必要である。業務上、健全な判断を下し、セキュリティ認証を維持または取得するために、この保証が必要である。保証の必要性の初期の兆候として、多くのクラウドプロバイダに監査の要求が殺到するという点がある。

このような事由により、本文書における推奨事項の多くは、保証の提供／取得に使用することができる標準的な質問リストとして提供されている。

チェックリストに基づく文書によって、以下の項目を実施するための手段が、クラウド利用者に提供されることになる：

1. クラウドサービスを採用する際のリスクの評価；
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；
4. 保証に関するクラウドプロバイダの負荷の低減。

このセキュリティチェックリストでは、セキュリティ要件のすべての側面（法律上の問題点、物理的セキュリティ、ポリシー上の問題点および技術的な問題点を含む）を取り扱う。

法的な推奨事項

クラウドコンピューティングに関連する法的な問題点の多くは、目下のところ、契約内容の評価（すなわち、複数のプロバイダが提供するサービスの比較時）または交渉により解消されている。クラウドコンピューティングでは、契約交渉ではなく、市場で提供されている様々な契約内容からの選択がごく一般的である（契約内容の評価）。ただし、将来的なクラウドサービスの利用者には、契約内容の交渉が可能なプロバイダを選択する機会が与えられるかもしれない。

従来のインターネットサービスとは異なり、クラウドコンピューティングの性質上、標準的な契約条項に関して、追加的なレビューが必要になる場合がある。契約書の関係者は、セキュリティ違反の通知、データの転送、派生成果物の作成（creation of derivative works）、管理策の変更（change of control）、および法執行機関によるデータアクセスといった点に関する各々の権利や義務に、特に注意を払うべきである。クラウドでは、重要な内部インフラストラクチャを外部委託することができ、そのインフラストラクチャが使えなくなった場合、その影響が広範囲に及ぶ可能性がある。したがって、関係者は、法的責任の割り当て（関係者によるクラウドの利用方法を考慮した場合の）、またはインフラストラクチャに対する責任の割り当てにおいて、法的責任に関する標準的な制限が反映されているか否かを慎重に判断すべきである。

法的な判例や規制によって、クラウドコンピューティングに特化したセキュリティ問題に対処できるようになるまでは、クラウドプロバイダと利用者は共に、セキュリティリスクに効果的に対処することが

できる契約条項の策定を目指すべきである。

欧州委員会に対する法律的な推奨事項

本文書では、欧州委員会が以下の項目を調査し、明確にするよう提言する：

- Data Protection Directive（データ保護指令）、および Article 29 Data Protection Working Party による推奨事項に関連する、いくつかの課題
- データのセキュリティ違反に関する、クラウドプロバイダから利用者への通知義務
- 電子商取引指令（eCommerce Directive）第 12～15 条に基づく中間責任の免責条項が、クラウドプロバイダにどのように適用されるか
- 全加盟国に共通する、必要最低限のデータ保護規格、およびプライバシー認証スキームを、最適にサポートする方法

調査に関する推奨事項

本文書では、クラウドコンピューティング技術のセキュリティを向上させるために、優先的に調査すべき分野を推奨している。以下に、すべての調査分野のリストから抽出した、優先的な調査が必要であると考えられる分野と、いくつかの例を示す。

クラウドにおける信頼の構築

- セキュリティ違反に関する報告形式が異なることによる影響
- クラウド内外の End-to-End でのデータの機密性
- より高い保証を提供するクラウド、仮想プライベートクラウド等

組織を跨ぐ大規模システムにおけるデータの保護

- フォレンジックスおよび証拠収集メカニズム
- インシデント対応 － 監視と追跡可能性
- データの保護とプライバシーを含む関連規制の国家間の相違

大規模なコンピュータシステムのエンジニアリング

- リソース隔離メカニズム － データ、処理、メモリ、ログ等
- クラウドプロバイダ間の相互運用性
- クラウドコンピューティングの障害耐性(resilience)。いかにしたらクラウドの障害耐性(resilience)を高めることができるか？

セキュリティ上の主な利点

したがって、セキュリティに同じ金額を投資しても、より適切な保護を調達することができる。このセキュリティ対策には、フィルタリング、パッチ管理、仮想マシンやハイパーバイザの強化等、あらゆる種類の防御策が含まれる。大規模化による他の利点としては、複数のロケーション、末端ネットワーク（目的地により近い場所でのコンテンツの配信または処理）、インシデントや脅威管理に対するタイムリーな対応等が含まれる。

大規模化による利点とセキュリティ：簡単に言うと、あらゆる種類のセキュリティ対策は、システムの規模が大きいほど、より低コストで実装することができる。したがって、セキュリティに同じ金額を投資しても、より適切な保護を調達することができる。このセキュリティ対策には、フィルタリング、パッチ管理、仮想マシンやハイパーバイザの強化等、あらゆる種類の防御策が含まれる。大規模化による他の利点としては、複数のロケーション、末端ネットワーク（目的地により近い場所でのコンテンツの配信または処理）、インシデントや脅威管理に対するタイムリーな対応等が含まれる。

市場での差別化要因となるセキュリティ：

リソース集約化の利点：リソースの集約化は、セキュリティ上のデメリットがあることは間違いないが[リスクの項参照]、低コストでの物理的境界の構築や、リソース単位での物理的アクセス制御を実現できること、ならびに、様々なセキュリティ関連プロセスを容易にかつ低コストで適用できる等の明らかな利点がある。

多くのクラウド利用者にとって、セキュリティは優先すべき検討事項である。多くのクラウド利用者が、機密性、完全性、障害耐性(resilience)に関するプロバイダの評判、およびプロバイダによって提供されるセキュリティサービスの内容をもとに、調達に関する選択を行っている。これは、クラウドプロバイダにとっても、セキュリティプラクティスを強化させるための、強力な推進力となっている。

マネージドセキュリティサービスのための標準化されたインターフェース：大規模なクラウドプロバイダは、マネージドセキュリティサービスプロバイダに対して、標準化されたオープンインターフェースを提供することができる。これにより、セキュリティサービスの、オープンでかつ迅速に利用可能な市場が形成される。

リソースの迅速かつ洗練されたスケーリング：クラウドプロバイダが防御策に対して、フィルタリング、トラフィックの形成、認証、暗号化等のためのリソースを動的に再配分することができる能力は（例、DDoS 攻撃に対するもの）、障害耐性(resilience)における明らかな利点である。

監査と証拠収集：クラウドコンピューティングでは、（仮想化を使用する場合）インフラストラクチャをオフラインにせずに、専用の仮想マシンのフォレンジックイメージを、利用量に応じた支払いで提供することができ、このことは、フォレンジック分析のためのダウンタイムの低減にもつながる。また、パフォーマンスを低下させることなく、広範囲のログの記録ができる、費用対効果の高いログ用ストレージも提供することができる。

よりタイムリーで有効かつ効率的なアップデートおよびデフォルトシステム：クラウド利用者によって使用されるデフォルト仮想マシンイメージやソフトウェアモジュールは、最新のパッチや細かく調整されたプロセスに従ったセキュリティ設定等により、あらかじめ強化したり、最新の状態にすることができる。IaaS クラウドサービスの API でも、仮想インフラストラクチャのスナップショットを定期的に取得して基準(baseline)と比較することが可能である。また、パッチモデルに依存する従来型のクライアントベースのシステムよりも、一つの均質なプラットフォームの方がより迅速に、何度でもアップデートを展開できる。

リソース集約化の利点：リソースの集約化は、セキュリティ上のデメリットがあることは間違いないが[リスクの項参照]、低コストでの物理的境界の構築や、リソース単位での物理的アクセス制御を実現できること、ならびに、様々なセキュリティ関連プロセスを容易にかつ低コストで適用できる等の明らかな利点がある。

セキュリティ関連の主なリスク

隔離の失敗：複数テナントおよびリソースの共有は、クラウドコンピューティングを定義付ける特徴である。このリスク分野には、ストレージ、メモリ、ルーティング、および異なるテナント間での評判を隔離するメカニズムの不備も含まれる（例、いわゆるゲストホッピング攻撃等）。ただし、リソース隔離メカニズムに対する攻撃（例、ハイパーバイザに対するもの等）は、まだ少なく、攻撃者にとって、従来の OS に対する攻撃をしかけることと比較しても、難易度がより高いという点は、考慮されるべきである。

本文書で識別された、最も重大なクラウド特有のリスクは、以下の通りである：

ガバナンスの喪失：クラウドインフラストラクチャの使用に際し、クラウド利用者は必然的に、クラウドプロバイダ（CP）に対し、セキュリティに影響を及ぼす可能性がある多くの問題に対する制御を委譲することになる。同時に、SLA では、クラウドプロバイダ側によるそのようなサービス提供の責任が提示されず、結果としてセキュリティ防御に隙が生じることがある。

ロックイン：現状では、データ、アプリケーションおよびサービスのポータビリティを保証できるツール、手順、標準データフォーマットもしくはサービスインターフェースは提供されていない。このような状況が、クラウド利用者にとって、あるプロバイダから別なプロバイダへ移行したり、データやサー

ビスを自組織の IT 環境に戻したりすることを困難にしているともいえる。このような場合、サービス提供に関して特定のクラウドプロバイダに依存することになる（特に、最も基本的な要素であるデータのポータビリティが確保されていない場合）。

隔離の失敗：複数テナントおよびリソースの共有は、クラウドコンピューティングを定義付ける特徴である。このリスク分野には、ストレージ、メモリ、ルーティング、および異なるテナント間での評判を隔離するメカニズムの不備も含まれる（例、いわゆるゲストホッピング攻撃等）。ただし、リソース隔離メカニズムに対する攻撃（例、ハイパーバイザに対するもの等）は、まだ少なく、攻撃者にとって、従来の OS に対する攻撃をしかけることと比較しても、難易度がより高いという点は、考慮されるべきである。

コンプライアンスに関するリスク：（たとえば、業界標準や規制要件などの）認証を取得するための投資は、クラウドへの移行に際して、リスクに晒される可能性がある　：

- クラウドプロバイダが、関連する要件に適合していることに対する証拠を提供できない場合
- クラウドプロバイダが、クラウド利用者による監査を許可していない場合

場合によってはパブリッククラウドインフラストラクチャを使用することが、ある種の適合性が達成されないことを意味することもある。（例、PCI DSS(4)等）

管理用インターフェースの悪用：パブリッククラウドプロバイダの顧客管理インターフェースは、インターネット経由でアクセス可能であり、（従来のホスティングプロバイダよりも）大規模なリソースへのアクセスを可能にする。したがって、特にリモートアクセスやウェブブラウザ関連の脆弱性と組み合わさった場合に、リスクが増大する。

データ保護：クラウドコンピューティングには、クラウド利用者やプロバイダが遭遇するデータ保護関連のリスクが複数存在する。たとえば、クラウド利用者（データ管理者としての役割において）にとって、クラウドプロバイダによるデータの扱い方を効果的にチェックし、データが合法的に扱われていることを保証することが困難な場合がある。この問題は、たとえば連携しているクラウド間で、複合的なデータ転送を行う場合に深刻化する。一方、クラウドプロバイダの中には、自身が行っているデータの取扱に関する情報を提供するところもある。また、クラウドプロバイダの中には、自身のデータ処理およびデータセキュリティ活動、ならびに実施中のデータ制御について認証サマリーを提供するところもある（例、SAS70 認証）。

セキュリティが確保されていない、または不完全なデータ削除：クラウド関連のリソースを削除するよう要請があった場合、ほとんどのオペレーティングシステムでなされるようには、データが完全に消去されるとは限らない。適切な、または、タイムリーなデータ削除は、対象データのコピーが複数あり、それらのすべてが手元にないために、あるいは破壊すべきディスクに他の顧客のデータが保存されているために、不可能な（顧客の立場からは望ましくない）場合がある。したがって、複数のテナントが存在する場合でハードウェアリソースを再利用する場合は、専用のハードウェアを使用する場合よりも高いリスクを顧客が抱えることになる。

悪意ある内部関係者：通常、発生する可能性が低いが、悪意ある内部関係者によってもたらされる可能性のある被害は、はるかに重大であることが多い。クラウドのアーキテクチャは、たとえば、クラウドプロバイダのシステムアドミニストレータやマネージドセキュリティサービスのプロバイダなど、非常にリスクの高い役割を必要とする。

留意事項：上記のリスクは、重大性の高い順に羅列したものではない。これらリスクは、リスクアセスメント時に識別された、クラウドコンピューティングに特化した最も重大なリスクの数項目に過ぎない。クラウドコンピューティングを使用することでもたらされるリスクは、デスクトップベースのシステム等の従来のソリューションに留まるうえで生じるリスクと比較検討されるべきである。このような活動を促進するために、本文書では、クラウドコンピューティングで想定されるリスクと従来のシステム環境におけるリスクを対比させている。

クラウドの利用者からクラウドプロバイダへのリスクの移転は多くの場合に可能であり、そして場合によってはそれが賢明ではあるが、*すべてのリスクを移転することができるわけではない*ことに注意してほしい。仮に、リスクがビジネスの失敗、評判や法的意味における深刻な被害を引き起こした場合、その他の関係者がこの被害を補償することは困難または不可能である。最終的に、責務を外部委託することはできても、説明責任を外部委託することはできない。

目次

対象読者

クラウドコンピューティングは、IT を提供するオンデマンドサービスモデルであり、多くの場合、仮想化と分散コンピューティング技術をベースとしている。クラウドコンピューティングのアーキテクチャは、以下の特徴を持っている：

- 高度に抽象化されたリソース
- 即時的な拡張性とフレキシビリティ
- 即時的なプロビジョニング
- リソースの共有（ハードウェア、データベース、メモリ等）
- 通常、「利用量に応じた支払い」の「サービスオンデマンド」
- （たとえば、WS API による）計画的な管理

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）。
- 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、意識向上イニシアティブ等を決定するため）。
- 個人または市民（これらのアプリケーションの消費者向けバージョンを利用する場合のコストと利益を評価できるようにするため）。

クラウドコンピューティング ― 実用的な定義

以下は、本文書の目的において使用するクラウドコンピューティングの実用的な定義である。これは、最終的な定義付けではない。この定義の参考出典（根拠）は、(5)、(6)および(54)で確認することができる。

クラウドコンピューティングは、IT を提供するオンデマンドサービスモデルであり、多くの場合、仮想化と分散コンピューティング技術をベースとしている。クラウドコンピューティングのアーキテクチャは、以下の特徴を持っている：

- 高度に抽象化されたリソース
- 即時的な拡張性とフレキシビリティ
- 即時的なプロビジョニング
- リソースの共有（ハードウェア、データベース、メモリ等）
- 通常、「利用量に応じた支払い」の「サービスオンデマンド」
- （たとえば、WS API による）計画的な管理

クラウドコンピューティングには、以下の三つのカテゴリーがある：

- **サービスとしてのソフトウェア（SaaS）**とは、第三者プロバイダによって提供されるオンデマンド型のソフトウェアであり、通常は遠隔で設定可能なインターネットを介して利用できる。オンラインでのワードプロセシングや表計算ツール、CRM サービス、Web コンテンツの配布サービス（Salesforce CRM、Google Docs 等）などがある。
- **サービスとしてのプラットフォーム（PaaS）**では、遠隔で展開・設定可能な API を使用し、クラウド利用者が新たなアプリケーションを開発することができる。このプラットフォームには、開発ツール、設定管理や展開用のプラットフォームが含まれる。たとえば、Microsoft Azure、Force および Google App エンジンなどがある。
- **サービスとしてのインフラストラクチャ（IaaS）**では、サービス API を経由して制御できる仮想マシンやその他の概念的なハードウェアおよびオペレーティングシステムを提供する。たとえば、Amazon EC2 や S3、Terremark Enterprise Cloud、Windows LiveSkydrive や Rackspace Cloud などがある。

クラウドはまた、以下のように分類することもできる：

- **パブリック（クラウド）**：誰でも利用することができ、すべての組織が加入できる。
- **プライベート（クラウド）**：サービスは、クラウドコンピューティングの原則に従って構築されるが、プライベートネットワーク内部でのみアクセスできる。

– **パートナー（クラウド）**：明確に限定された数の関係者にのみ、プロバイダによって提供されるクラウドサービス。

通常、クラウド関連のサービス、費用、責任および保証は、以下の図のように様々である。

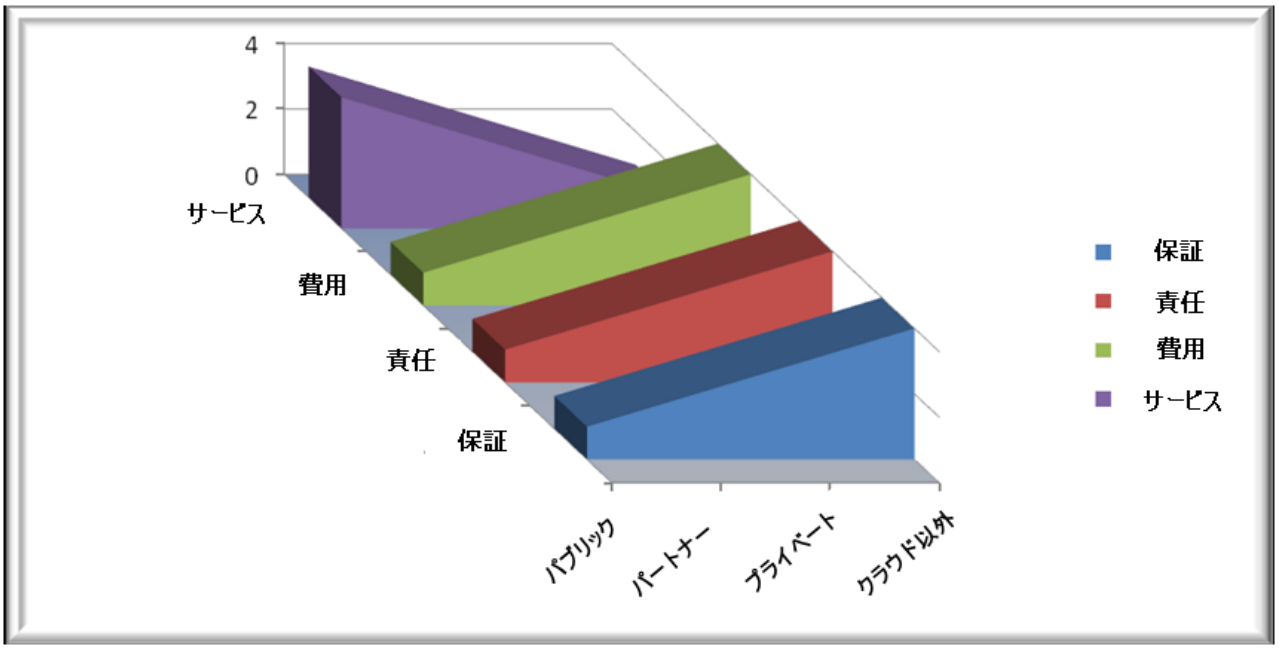


図 1：パブリック、パートナーおよびプライベートクラウドの特徴

既存の文献に関する調査

本文書の編集に当たり、我々は、クラウドセキュリティのリスクと緩和に関する既存の文献を調査し、その結果をどこに当てはめることによって、最大限の付加価値を得ることができるかについて考えた。それらの文献には、クラウドコンピューティングにおける重要分野に関するセキュリティガイダンス（Cloud security Alliance (55)）クラウドキューブモデル：セキュアなコラボレーションのためのクラウド構造の選択（Jericho Forum (56)）およびクラウドコンピューティング関連のセキュリティリスクのアセスメント（Gartner (57)）が含まれる。

1. クラウドコンピューティングによるセキュリティ上の利点

簡単に言うと、あらゆる種類のセキュリティ対策は、システムの規模が大きいほど、より低コストで実装することができる。したがって、セキュリティに同じ金額を投資しても、より適切な保護を調達することができる。

クラウドコンピューティングがもたらす経済面、技術面、アーキテクチャ面および環境保全的面での利点について書かれている、まるで熱帯雨林にある多くの貴重な資源のような資料については繰り返すまでもない。しかしながら、我々の専門家グループのメンバーによる直接的な経験や、「現実世界」から伝わってくる最新のニュースによれば、クラウドコンピューティングがもたらすセキュリティリスクに関する調査は、クラウドコンピューティングがもたらす具体的なセキュリティ上の利点についてのレビューとのバランスを取らなければならない。クラウドコンピューティングは、セキュリティと障害耐性(resilience)を向上させる大きな可能性を秘めている。以下に、クラウドコンピューティングが主に、どのような形で利点をもたらすかについて記述する。

大規模化による利点とセキュリティ

簡単に言うと、あらゆる種類のセキュリティ対策は、システムの規模が大きいほど、より低コストで実装することができる。したがって、セキュリティに同じ金額を投資しても、より適切な保護を調達することができる。このセキュリティ対策には、フィルタリング、パッチ管理、仮想マシンやハイパーバイザの強化、人材の確保、管理および身元調査、ハードウェアやソフトウェアの冗長性、強力な認証、効率的な役割ベースのアクセス制御および ID 管理連携ソリューション等、あらゆる種類の防御策が含まれる。これらは、防御に関与する様々なパートナー間の連携による、ネットワーク効果を向上させている。大規模化がもたらすその他の利点には、以下のようなものがある：

- **複数のロケーション**：クラウドプロバイダの多くは、デフォルトで複数のロケーションにコンテンツを複製することができる経済的リソースを確保している。これによって冗長性と不具合からの独立性が増し、形にとらわれない、所定レベルの災害復旧が提供される。
- **末端ネットワーク**：ネットワークの末端に近い位置でのデータの格納、処理および配布は、サービスに対する信頼性と品質の全体的な向上をもたらし、ローカルネットワーク関連の問題が全ネットワークに副次的な悪影響をもたらす可能性を低下させる。
- **タイムリーな対応**：**インシデントに対しては**大きく向上：適切に運用されている大規模システムでは、たとえば、新たなマルウェアの出現が早期に検出される等の理由により、より効果的で効率のよいインシデント対応能力を構築できる。
- **脅威の管理**：クラウドプロバイダは、特定のセキュリティ脅威を扱う専門家を雇用することができる傍ら、小規模企業は、僅かな数の「万能選手」しか採用することができない。

市場での差別化要因となるセキュリティ

多くのクラウド利用者にとって、セキュリティは優先すべき検討事項である[An SME perspective on Cloud Computing の調査参照]。利用者は、従来型のシステム環境における調達以上に、機密性、完全性、障害耐性(resilience)に関するプロバイダの評判、およびプロバイダによって提供されるセキュリティサービスの内容をもとに、調達に関する選択を行っている。これは、クラウドプロバイダにとっても、セキュリティプラクティスを強化し、セキュリティ面で競い合うための、強力な推進力となっている。

マネージドセキュリティサービスのための標準化されたインターフェース

> 防御関連のリソースをオンデマンドで動的に拡大する能力は、障害耐性(resilience)における明らかな長所である。更に、すべてのシステムリソースをスケーリングすることなく、あらゆる種類のリソースを個別に、かつ詳細にスケーリングすることができれば、サービスに対する要求が突然ピークに達した場合（ただし、悪意のある行為によるものではないこと）でも、低コストで対応することができる。

大規模なクラウドプロバイダは、顧客にサービスを提供するマネージドセキュリティサービス（MSS）プロバイダに対して、標準化されたオープンインターフェースを提供することができる。これにより、セキュリティサービスにおいて、オープンでかつ迅速に利用可能な市場が形成され、利用者は、より簡単で、より少ない設置費用で、プロバイダを切り替えられるようになる。

リソースの迅速かつ洗練されたスケーリング

オンデマンドで迅速にスケーリングできるクラウドリソースのリストには、たとえば、ストレージ、CPU 時間、メモリ、Web サービスのリクエストと仮想マシンインスタンスが含まれており、リソースの消費に対する詳細な制御のレベルは、技術が成熟するにつれて向上している。

クラウドプロバイダは、攻撃を受ける可能性が高い場合、あるいは、実際に攻撃を受けている場合、（たとえば、DDoS 攻撃に対する）防御策に対する支援を強化する目的で、フィルタリング、トラフィックの形成、暗号化等のためのリソースを動的に再配分する可能性がある。このような動的なリソース再配分能力と適切なリソース最適化手法を組み合わせることによって、クラウドプロバイダは、合法的なホストサービスが使用するリソースの可用性に対する、いくつかの攻撃による影響を抑えられる可能性があり、また、そのような攻撃に対応するセキュリティ防御策のためにリソース使用が増加することによる影響を抑えられる可能性がある。ただし、これを実現するには、クラウドプロバイダが、自律的なセキュリティ防御策、リソースの管理および最適化を適切に調整することが必要である。

防御関連のリソースをオンデマンドで動的に拡大する能力は、障害耐性(resilience)における明らかな長所である。更に、すべてのシステムリソースをスケーリングすることなく、あらゆる種類のリソースを個別に、かつ詳細にスケーリングすることができれば、サービスに対する要求が突然ピークに達した場合（ただし、悪意のある行為によるものではないこと）でも、低コストで対応することができる。

監査および証拠収集

IaaS は、オンデマンドによる仮想マシンのクローニング(cloning)をサポートしている。セキュリティ違反の発生が疑われる場合、顧客は、稼動中の仮想マシンや仮想コンポーネントのイメージを取得し、オフラインでのフォレンジック分析を僅かなダウンタイムで実施することができる。ストレージをあらかじめ用意しておくことで、複数のクローンを生成し、調査時間短縮のために、分析活動を並行して実施することができる。これにより、セキュリティインシデントの事後分析が改善され、攻撃者を追跡して、脆弱性にパッチを適用できる確率が高まる。ただし、クラウド利用者が訓練を受けたフォレンジック分析の専門家にアクセスできることが前提となる（本文書執筆中の時点では、これは、標準的なクラウドサービスではない）。

> また、パッチモデルに依存する従来型のクライアントベースのシステムよりも、一つの均質なプラットフォームの方が、より迅速に、何度でもアップデートを展開できる。

また、IaaS は、費用対効果の高いログ用ストレージを提供することができるため、パフォーマンスを低下させることなく、広範囲のログを記録することができる。「利用量に応じた支払い」のクラウドストレージは、ログ監査用のストレージの費用の透明性を高める一方で、将来的な監査ログの要件にも容易に対応することができるよう、調整が可能である。これにより、発生と同時にセキュリティインシデントを特定するプロセスの、効率性を高めることができる(7)。

よりタイムリーで有効かつ効率的なアップデートおよびデフォルトシステム

顧客によって使用される仮想マシンイメージやソフトウェアモジュールは、最新のパッチや細かく調整されたプロセスに従ったセキュリティ設定等により、あらかじめ強化したり、最新の状態にすることができる。更に、IaaS クラウドサービスの API でも、仮想インフラストラクチャのスナップショットを定期的に取得して基準(baseline)と比較することが可能である（たとえば、ソフトウェアファイアウォールのルールが変更されていないことを保証するために）(8)。また、パッチモデルに依存する従来型のクライアントベースのシステムよりも、一つの均質なプラットフォームの方が、より迅速に、何度でもアップデートを展開できる。その結果、PaaS や SaaS モデルでは、アプリケーションは組織外の環境でも使用することができるよう強化される傾向にあり、組織内の同等のソフトウェア（存在する場合）よりもポータビリティが高く、より堅牢である傾向にある。また、脆弱性の残る可能性を最小限に抑えるために、中央集約的な方法で、定期的にアップデートやパッチが適用される傾向にある。

監査や SLA により導かれるより有効なリスクマネジメント

SLA 関連の様々なリスクシナリオが現実となった場合の不利益や、セキュリティ違反によってもたらされる可能性のある評判への影響（市場での差別化要因となるセキュリティの項参照）を定量化する必要性によって、既存のものよりも更に厳格な内部監査およびリスクアセスメント手順を策定するための動機付けがなされている。クラウドプロバイダに対し課せられる頻度の高い監査によって、これまで検出

されていなかったリスクが浮上する傾向がある点で、厳格な内部調査やリスクアセスメントを実施するのと同様の効果が得られる。

リソースの集約化がもたらす利点

リソースの集約化は、セキュリティ上のデメリットがあることは間違いないが[リスクの項参照]、低コストでの物理的境界の構築や、リソース単位での物理的アクセス制御を実現できること、ならびに、包括的なセキュリティポリシーや管理策を、より容易にかつ低コストで、データ管理、パッチ管理、インシデント管理およびメンテナンスプロセスに適用できる等の明らかな利点がある。このような利点により、顧客に対してどの程度の還元がなされるかは、場合によって変化する。

2. リスクアセスメント

ユースケースシナリオ

クラウドコンピューティングのリスクをアセスメントするために、本文書では、以下の三つのユースケースシナリオを分析した。

- クラウドコンピューティングに対する中小企業の見解
- サービスの障害耐性(resilience)に対するクラウドコンピューティングの影響
- クラウドコンピューティングと電子政府（e ヘルス）

便宜上、本書では、中小企業におけるユースケースシナリオの完全版（付録 II 参照）、および障害耐性(resilience)と e ヘルスシナリオのサマリー（付録 III 参照）を刊行した。

クラウドコンピューティングのリスクをアセスメントするために、本文書では、以下の三つのユースケースシナリオを分析した。

- クラウドコンピューティングに対する中小企業の見解
- サービスの障害耐性(resilience)に対するクラウドコンピューティングの影響
- クラウドコンピューティングと電子政府（e ヘルス）

この選択は、欧州におけるクラウド市場が、新たなビジネスの立ち上げや、既存のビジネスモデルの発展にも大きな影響を与えるとの予測を基になされている。EU の産業界は、主に中小企業で構成されているため（EU の情報筋によれば、中小企業の割合は 99% (9)）、中小企業に注目するのは意味がある。そのような状況ではあるが、本文書では、政府機関や大企業に特化したいくつかのリスクや提言も含めることとした。

中小企業に関するシナリオは、「An SME Perspective on Cloud Computing」という調査の結果に基づいており、クラウドコンピューティング関連のプロジェクトや投資を検討、計画または実施している企業のためのロードマップを意味するものでは**ない**。
使用事例として中規模企業を採用したのは、充分なレベルの IT、法律およびビジネスの複雑性を、アセスメントにおいて保証するためである。その目的は、考えられるすべての情報セキュリティリスクを露呈させることにある。それらのリスクの一部は、中規模企業に特化したものであり、その他のリスクは、クラウドコンピューティング環境に移行するに際し、零細規模や小規模の企業も直面する可能性のある一般的なリスクである。
また、このシナリオは、特定のクラウド利用者やプロバイダの現実を完全に再現することを目的としているものではないが、シナリオに含まれているすべての要素は、近い将来、多くの組織で起こり得るものである。

リスクアセスメントプロセス

リスクのレベルは、想定される悪影響に対してマッピングされた、インシデントシナリオの発生可能性を基に予測されている。インシデントシナリオの発生可能性は、一定の発生可能性で脆弱性につけ込む脅威によって示される。

それぞれのインシデントシナリオの発生可能性および事業影響は、本文書の編纂に尽力頂いた専門家グループからの、集団経験に基づく助言をもとに、決定されたものである。適切な根拠に基づいて発生可能性を提供できないと判断した場合、その値は N/A としている。多くの場合、発生可能性の予測は、検討中のクラウドモデルまたはアーキテクチャに依存している。

下記の表は、インシデントシナリオに関連する事業影響を基準に、この発生可能性を対照させたものである。その結果発生するリスクは、リスク受容基準をもとに評価可能な 0 から 8 までの尺度で判定する。このリスク尺度は、例えば、次のように、シンプルなリスク全般の等級付けに使用することもできる。

- 低リスク： 0～2
- 中リスク： 3～5
- 高リスク： 6～8

	インシデントシナリオの発生可能性	きわめて低い（ほとんど発生しない）	低い（まず発生しない）	中程度（発生の可能性がある）	高い（発生の可能性が高い）	きわめて高い（頻繁に発生する）
事業影響	きわめて低い	0	1	2	3	4
	低い	1	2	3	4	5
	中程度	2	3	4	5	6
	高い	3	4	5	6	7
	きわめて高い	4	5	6	7	8

リスクレベルの予測は、ISO/IEC27005:2008 (10)に基づいている。

3. リスク

リスクは、常に全体的なビジネスの機会およびリスクレベルとの関連で理解されるべきである。時には、リスクはビジネス機会によって相殺される場合がある。

下記の点は、以下で説明されるリスクに関連して、留意すべきものである：

- リスクは、常に全体的なビジネスの機会およびリスクレベルとの関連で理解されるべきである。時には、リスクはビジネス機会によって相殺される場合がある。
- クラウドサービスは、複数のデバイスによりアクセス可能な、利便性の高いストレージであるばかりでなく、利便性のより高い通信を実現し、複数ポイントを即座に組み合わせて使用することができる等、重要な利点を備えている。したがって、比較分析では、複数の異なる場所（組織内対クラウド等）にデータを格納する際のリスクの比較だけでなく、組織内に格納された組織内データ（例、表計算データ等）が他の者に送付される場合のリスクと、クラウド内に格納されている表計算データを関係者間で共有する際のセキュリティ問題との比較も必要となる。したがって、クラウドコンピューティングを使用することでもたらされるリスクは、デスクトップベースのシステムなどの従来のソリューションに留まるうえで生じるリスクと比較検討されるべきである。
- 多くの場合、リスクのレベルは、検討中のクラウドアーキテクチャの種類によって大きく異なる。
- クラウド利用者は、クラウドプロバイダにリスクを移転することができ、そのリスクは、サービスがもたらす費用便益と対比して考慮されるべきである。ただし、*すべてのリスクを移転できるわけではない*。仮に、リスクがビジネスの失敗、評判や法的意味における深刻な被害を引き起こした場合、その他の関係者がこの被害を補償することは困難または不可能である。
- 本文書におけるリスク分析は、クラウド技術に適用されるものである。特定のクラウドコンピューティングサービスや企業に適用されるものでもない。本文書は、プロジェクトに特化した組織的なリスクアセスメントにとってかわることを意味するものでもない。
- リスクレベルは、クラウド利用者の観点から示したものである。したがって、クラウドプロバイダの視点で考慮されている箇所は、その旨を明示的に記載している。

したがって、クラウドコンピューティングを使用することでもたらされるリスクは、デスクトップベースのシステムなどの従来のソリューションに留まるうえで生じるリスクと比較検討されるべきである。

下記の図は、リスクの確率とその影響の配分を示したものである。

確率

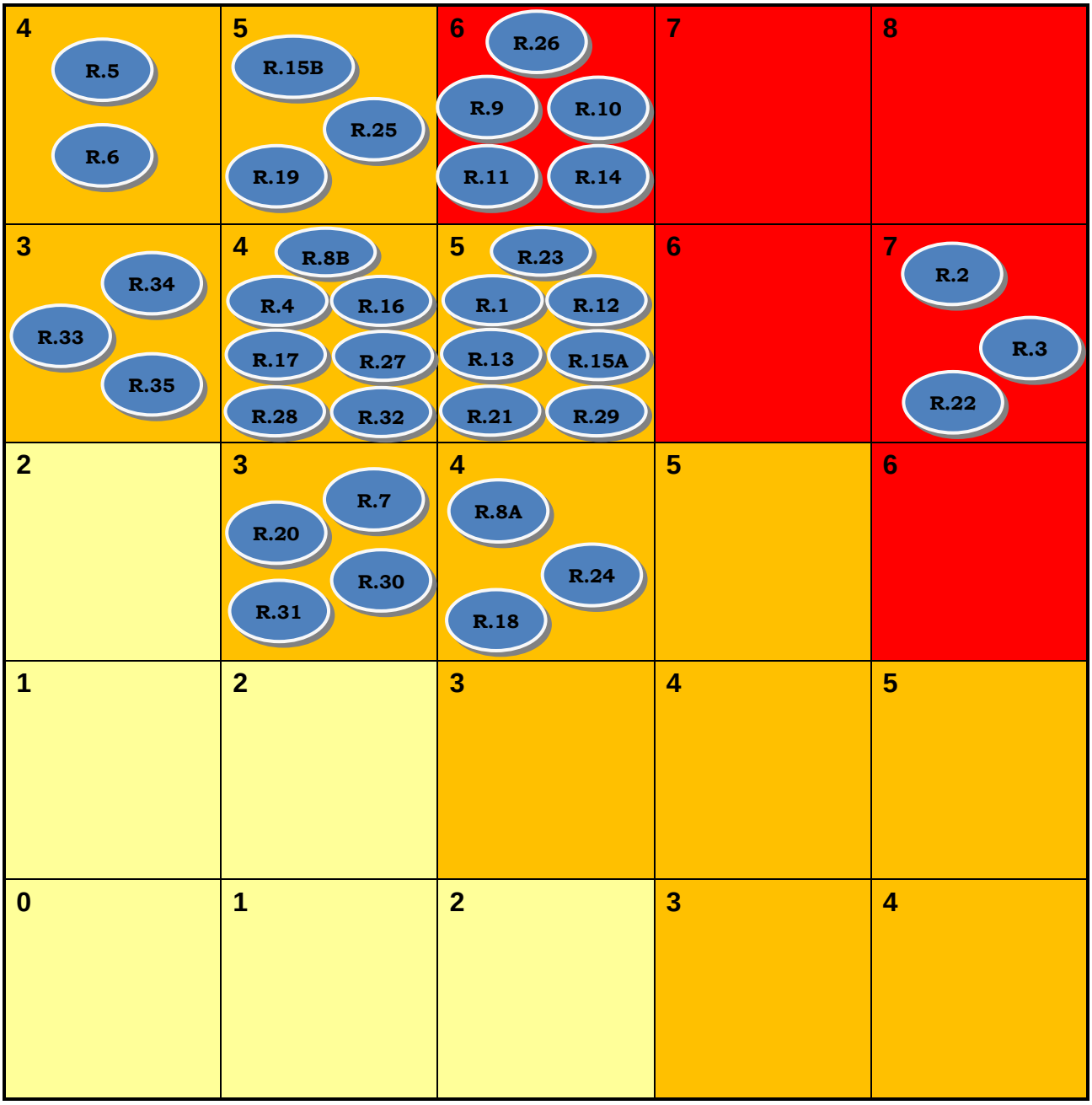


図 2：リスクの配置

アセスメント時に識別されたリスクは、次の三つのカテゴリーに分類される。

- ポリシーおよび組織的リスク
- 技術的リスク
- 法律的リスク

ただし、*すべてのリスクを移転できるわけではない*。仮に、リスクがビジネスの失敗、評判や法的意味における深刻な被害を引き起こした場合、その他の関係者がこの被害を補償することは困難または不可能である。

表に示したリスクには、次のようなものを含む。

- 確率レベル
- 影響レベル
- 脆弱性への参照
- 影響を受ける資産への参照
- リスクレベル

更に、意味がある箇所では、クラウドコンピューティング関連のリスクと標準的な IT アプローチにおけるリスクを比較するための、「相対確率」と「相対的な影響」のセルを追加した。ただし、選択したすべてのリスクが高位であるため、相対的なリスクについては含めていない。

ポリシーと組織関連のリスク

R.1. ロックイン

確率	高	相対確率：高
影響	中	相対的な影響：同等
脆弱性	V13. 技術とソリューションにおける標準の欠如 V46. プロバイダの選定不備 V47. サプライヤの冗長化（SUPPLIER REDUNDANCY）の欠如 V31. 利用規約の完全性と透明性の欠如	
影響を受ける資産	A1. 企業の評判 A5. 個人の秘密データ A6. 個人データ A7. 個人データ（重要） A9. サービス提供 ― リアルタイムによるサービス A10. サービス提供	
リスク	高	

現状では、データおよびサービスのポータビリティを保証できるツール、手順、標準データフォーマット、もしくはサービスインターフェースは提供されていない（いくつかのイニシアティブは存在するが。例、(58)参照）。このような状況により、顧客があるプロバイダから別のプロバイダへ移行したり、デ

ータやサービスを組織内の IT 環境とクラウド間で移行することが非常に困難になっている。更に、クラウドプロバイダには、顧客のサービスやデータのポータビリティを（直接的または間接的に）阻止するためのインセンティブを設けているところもある。

このようにサービスの提供を特定のクラウドプロバイダに依存していると仮定した場合、そのプロバイダのコミットメントにもよるが、万一、クラウドプロバイダが倒産した場合には、壊滅的なビジネス上の失敗につながる可能性があり、（R.5 参照）、また、コンテンツやアプリケーションの別なプロバイダへの移行が（資金面または時間面で）非常に高価となる、あるいは、不十分な警告（早期の警告でない）しか与えられない、といったことが起きてくる。

クラウドプロバイダの買収（R.6）においても、プロバイダのポリシーや、利用規約などの拘束力を持たない同意が、突然変更になる可能性が高まるため、上記と同様の影響がもたらされる可能性がある。

ロックインの範囲やその性質は、クラウドの種類によって異なる点に注意することが重要である。

SaaS のロックイン

- 通常、顧客のデータは、SaaS プロバイダによって設計された、独自のデータベーススキーマに格納されている。ほとんどの SaaS プロバイダは、データレコードを読み出す（そして「エクスポート」する）ための、API コールを提供している。ただし、このプロバイダが、既製のデータ「エクスポート」ルーチンを提供していない場合、顧客が、自身でデータを抽出し、別のプロバイダへ「インポート」することができるよう、ファイルに書き込むプログラムを開発する必要がある。データのエクスポートとインポートには、たとえば XML のような共通ベースとなるファイル形式も存在するが、ビジネスレコードの構造に関しては、正式な合意事項は無いに等しいことを留意しなければならない（例えば、ある SaaS プロバイダの顧客レコードには、他のプロバイダと異なるフィールドが含まれる場合がある）。新しいプロバイダは、費用交渉を経て、この問題を解決してくれることもある。ただし、データを組織内の IT 環境に戻す場合は、クラウドプロバイダがルーチンを提供してくれない限り、必要となるあらゆるデータマッピングに対応するインポートルーチンを顧客側で作成する必要がある。顧客は、重要な移行計画を決定する前に、この点を評価するため、クラウドプロバイダにとっては、データのポータビリティをなるべく容易に、かつ完全で費用対効果が高くなるように実現することが、長期的なビジネス上の関心事項となっている。

- アプリケーションのロックインは、最も明示的なロックインの形式である（尤も、これはクラウドサービスに限定されるものではない）。通常、SaaS プロバイダは、対象とする市場のニーズに合わせて調整される、カスタムアプリケーションを開発する。大規模なユーザを持つ SaaS 利用者が別の SaaS プロバイダに移行する際には、末端利用者の経験にも影響が及ぶため（例、再トレーニングが必要になる等）、多額の移行費用が発生し得る。利用者が、プロバイダの API と直接やり取りするプログラムを開発した場合（例、他のアプリケーションとの統合のため）、新しいプロバイダの API を考慮し、このプログラムも書き換える必要が出てくるであろう。

PaaS のロックイン

PaaS のロックインは、API レイヤ（すなわち、プラットフォームに特化した API コール）およびコンポーネントレベルの双方で発生する。たとえば、PaaS プロバイダは、非常に効率的なバックエンドのデータ格納を提供することができる。この場合、顧客は、プロバイダによって提供されるカスタム API を使用してプログラムを開発する他に、バックエンドのデータ格納と互換性のある方法で、データへアクセスするルーチンをプログラミングしなければならない。この場合のプログラムは、互換性がある API が提供されるように見えても、データへのアクセスモデルが異なる場合もあるため、必ずしも PaaS プロバイダ全体にわたるポータビリティが実現されている訳ではない（たとえば、リレーショナル対ハッシング）。

クラウドインフラストラクチャの使用に際し、利用者は必然的に、クラウドプロバイダ（CP）に対し、セキュリティに影響を及ぼす可能性がある多くの問題に対する制御を委譲することになる。たとえば、利用規約によって、ポートスキャン、脆弱性のアセスメント、および侵入テストが禁止されることが考えられる。また、顧客側の強化手順とクラウド環境との間で矛盾が生じる場合もある（R.20 参照）。その一方で、SLA では、クラウドプロバイダ側によるそのようなサービス提供の責任が提示されず、結果としてセキュリティ防御に隙が生じることがある。

更に、クラウドプロバイダは、自身が提供するのと同じ保証（すなわち、合法的にサービスを提供する等）を提供することができない第三者（未知のプロバイダ）に、サービスを外部委託する、または、下請け契約を結ぶことができる。あるいは、クラウドプロバイダによる管理の変更に伴い、提供されるサービスの諸条件が変更される場合がある。

- API レイヤにおける PaaS のロックインは、プロバイダが異なると、提供される API も異なるために発生する。
- PaaS のロックインは、クラウド環境において、安全に運用できるよう、「標準的な」ランタイムが大きくカスタマイズされていることが多いため、ランタイムレイヤで発生する。たとえば、Java のランタイムには、セキュリティ上の理由から削除または修正された、「危険な」呼び出しが含まれる場合がある。これらの相違を理解し、考慮することの責任は、利用者側の開発者にある。
- PaaS も、SaaS と同様にデータのロックインに悩まされるが、互換性のあるエクスポートルーチンを作成する責任は、顧客側に、完全に課せられることになる。

IaaS のロックイン

IaaS のロックインは、消費される特定のインフラストラクチャサービスによって変化する。たとえば、クラウドストレージを使用する顧客は、互換性のない仮想マシンのフォーマットの影響を受けることは

ない。

- 一般的に IaaS コンピューティングのプロバイダは、ハイパーバイザベースの仮想マシンを提供する。ソフトウェアや VM のメタデータは、ポータビリティのためにバンドルされている（通常は、プロバイダのクラウドに含まれている）。したがって、プロバイダ間での移行は、OVF (11)などのオープンスタンダードが採用されるようになるまでは、容易ではない。

- IaaS ストレージプロバイダの提供するサービスは、単純な鍵／値に基づくデータ格納から、ポリシーに基づいたファイルベースの格納まで、様々である。機能は大きく変化し得るため、格納の意味合いも大きく異なる。ただし、特定のポリシー機能（たとえば、アクセス制御）へのアプリケーションレベルの依存は、顧客が選択できるプロバイダの範囲を限定してしまう可能性がある。

- データのロックインは、IaaS ストレージサービスでは明らかな懸念事項である。クラウド利用者が、より多くのデータをクラウドストレージに詰め込もうとするため、クラウドプロバイダがデータのポータビリティを提供しない限り、データのロックインが進行することになる。

すべてのプロバイダに共通している点は、クラウドプロバイダの「銀行に預金者が殺到する」シナリオが現実化する可能性である。このシナリオでは、クラウドプロバイダの財政状況に信頼の危機的状況が生じたと仮定し、それ故、早い者勝ちでコンテンツの排出または引き出しが一斉に起こることが想像される。したがって、プロバイダが、ある一定期間内に「引き出す」ことができる「コンテンツ（データやアプリケーションプログラム）」の量を制限した場合には、一部の顧客はデータやアプリケーションを使用することが全くできなくなる可能性がある。

R.2. ガバナンスの喪失

確率	非常に高	相対確率：高
影響	非常に高（組織による） （IaaS：非常に高、SaaS：低）	相対的な影響：同等
脆弱性	V34. 役割と責任の不明確性 V35. 役割定義の適用の不備 V21. クラウド外の契約上の義務または責任のクラウドへの適用 V23. 複数利害関係者間で矛盾する SLA 条項 V25. 利用者に監査または認証の証明書が提供されない問題 V22. クラウドをまたがるアプリケーションに潜在する相互依存性 V13. 技術とソリューションにおける標準の欠如 V29. 複数の司法管轄権を跨るデータ格納とそれに対する認識の欠如 V14. ソースコードエスクロー（預託）契約の欠如 V16. 脆弱性診断プロセスに関する管理の欠如 V26. クラウドのインフラに適用できる認証スキームの欠如 V30. 司法管轄権に関する情報の欠如 V31. 利用規約の完全性と透明性の欠如 V44. 不明確な資産の管理責任	
影響を受ける資産	A1. 企業の評判 A2. 顧客の信頼 A3. 従業員の忠誠心と経験 A5. 個人の秘密データ A6. 個人データ A7. 個人データ（重要） A9. サービス提供 ― リアルタイムによるサービス A10. サービス提供	
リスク	高	

クラウドに移行中の組織の中には、競争相手より優位に立つため、または、業界標準や法的要件に適合するために認証を取得する目的で、莫大な投資を行っているところもある（例、PCI DSS）。

クラウドインフラストラクチャの使用に際し、利用者は必然的に、クラウドプロバイダ（CP）に対し、セキュリティに影響を及ぼす可能性がある多くの問題に対する制御を委譲することになる。たとえば、利用規約によって、ポートスキャン、脆弱性のアセスメント、および侵入テストが禁止されることが考えられる。また、顧客側の強化手順とクラウド環境との間で矛盾が生じる場合もある（R.20 参照）。その一方で、SLA では、クラウドプロバイダ側によるそのようなサービス提供の責任が提示されず、結果としてセキュリティ防御に隙が生じることがある。更に、クラウドプロバイダは、自身が提供す

るのと同じ保証（すなわち、合法的にサービスを提供する等）を提供することができない第三者（未知のプロバイダ）に、サービスを外部委託する、または、下請け契約を結ぶことができる。あるいは、クラウドプロバイダによる管理の変更に伴い、提供されるサービスの諸条件が変更される場合がある。ガバナンスと制御の喪失は、組織の戦略に重大な影響をもたらし、結果としてその組織に課せられているミッションや目的を達成する能力にも重大な影響をもたらす可能性がある。また、ガバナンスと制御の喪失は、セキュリティ要件への不適合、データの機密性、完全性、可用性の欠如、パフォーマンスとサービス品質の低下、コンプライアンスの課題の生成等をもたらす可能性がある（R.3 参照）。

R.3. コンプライアンスの課題

確率	非常に高（PCI、SOX に依存）	相対確率：高
影響	高	相対的な影響：同等
脆弱性	V25. 利用者に監査または認証の証明書が提供されない問題 V13. 技術とソリューションにおける標準の欠如 V29. 複数の司法管轄権を跨るデータ格納とそれに対する認識の欠如 V26. クラウドのインフラに適用できる認証スキームの欠如 V30. 司法管轄権に関する情報の欠如 V31. 利用規約の完全性と透明性の欠如	
影響を受ける資産	A20. 認証	
リスク	高	

クラウドに移行中の組織の中には、競争相手より優位に立つため、または、業界標準や法的要件に適合するために認証を取得する目的で、莫大な投資を行っているところもある（例、PCI DSS）。このような投資は、クラウドへの移行に際してリスクに晒される可能性がある：

> リソースの共有は、あるテナントによる悪意の行動が、別のテナントの評判にも影響を及ぼすことがあることを意味する。

- クラウドプロバイダが、関連する要件に適合していることに対する証拠を提供できない場合
- クラウドプロバイダが、クラウド利用者による監査を許可していない場合

場合によってはパブリッククラウドインフラストラクチャを使用することが、ある種の適合性が達成されないことを意味することもある。このような場合、クラウドによってホストされているサービスが、それらの適合性を必要とするサービスのために使用できないことも意味している。たとえば、EC2 では、クラウド利用者が、自身のプラットフォームにおいて PCI との適合性を達成することを強く求められる旨を説明している。したがって、EC2 でホストされるサービスは、クレジットカードの処理のためには使用できない。

R.4. 他の共同利用者の行為による信頼の喪失

確率	低
影響	高
脆弱性	V6. リソース分離の欠如 V7. 不信の伝播に対する隔離の欠如 V5. ハイパーバイザの脆弱性
影響を受ける資産	A1. 企業の評判 A5. 個人の秘密データ A6. 個人データ A7. 個人データ（重要） A9. サービス提供 ― リアルタイムによるサービス A10. サービス提供
リスク	中

リソースの共有は、あるテナントによる悪意の行動が、別のテナントの評判にも影響を及ぼすことがあることを意味する。たとえば、スパムメールの送信、ポートスキャンまたはクラウドインフラストラクチャを使用した悪意のコンテンツの提供等は、以下のような事態を招く可能性がある：

― 攻撃者だけでなく、インフラストラクチャを使用しているその他の無実のテナントを含む、所定範囲の IP アドレスがブロックされる。

― 隣接するテナントの活動によるリソースの押収（隣接するテナントが召喚される）。

影響としては、サービス提供の低下やデータ喪失、組織の評判の低下問題が考えられる。

R.5. クラウドサービスの終了または障害

確率	N/A	
影響	非常に高	相対的な影響：高
脆弱性	V46. プロバイダの選定不備 V47. サプライヤの冗長化（SUPPLIER REDUNDANCY）の欠如 V31. 利用規約の完全性と透明性の欠如	
影響を受ける資産	A1. 企業の評判 A2. 顧客の信頼 A3. 従業員の忠誠心と経験 A9. サービス提供 ― リアルタイムによるサービス A10. サービス提供	
リスク	中	

新たな IT 市場の場合と同様に、競争圧力、不適切なビジネス戦略、財政支援の欠如等により、プロバイダがビジネスから撤退したり、あるいは、少なくとも、彼らが提供するサービスのポートフォリオを再

構築せざるを得ない状況に追い込まれる可能性がある。換言すれば、短中期間において、いくつかのクラウドコンピューティングサービスが終了となる可能性がある。

クラウド利用者に対するこのような脅威による影響は容易に理解することができる。何故ならば、このような脅威が、サービス提供のパフォーマンスの低下やサービスの品質の低下に加え、投資の損失をも生み出す可能性があるからである。

更に、クラウドプロバイダに外部委託されたサービスにおける不具合は、クラウド利用者が自身の顧客に対して果たすべき義務や責任を遂行する能力にも重大な影響を及ぼす可能性がある。したがって、クラウドプロバイダの顧客は、プロバイダの過失をベースとした契約上の、および複雑な責任に晒される可能性がある。クラウドプロバイダによる過失は、顧客側の従業員に対する顧客の責任問題にもつながる可能性がある。

R.6. クラウドプロバイダの買収

確率	N/A	
影響	中	相対的な影響：高
脆弱性	V31. 利用規約の完全性と透明性の欠如	
影響を受ける資産	A1. 企業の評判 A2. 顧客の信頼 A3. 従業員の忠誠心と経験 A4. 知的財産 A5. 個人の秘密データ A6. 個人データ A7. 個人データ（重要） A8. 人材データ A9. サービス提供 ― リアルタイムによるサービス A10. サービス提供	
リスク	**中**	

クラウドプロバイダの買収は、戦略の変更の可能性を増加させ、法的な拘束力を持たない同意事項（例、ソフトウェアインターフェース、セキュリティ関連投資、非契約のセキュリティ管理策等）をリスクに晒す場合がある。これにより、セキュリティ要件に適合することが不可能となり得る。最終的な影響は、組織の評判、顧客または患者の信頼、従業員の忠誠心や経験といった重要な資産への損害があり得る。

R.7. サプライチェーンにおける障害

確率	低	相対確率：高
影響	中	相対的な影響：高
脆弱性	V31. 利用規約の完全性と透明性の欠如	

	V22. クラウドをまたがるアプリケーションに潜在する相互依存性 V46. プロバイダの選定不備 V47. サプライヤの冗長化（SUPPLIER REDUNDANCY）の欠如
影響を受ける資産	A1. 企業の評判 A2. 顧客の信頼 A5. 個人の秘密データ A6. 個人データ A7. 個人データ（重要） A9. サービス提供 ― リアルタイムによるサービス A10. サービス提供
リスク	中

クラウドコンピューティングのプロバイダは、第三者に対し、自身の「生産」工程における特殊なタスクを外部委託することがある。そのような場合、クラウドプロバイダのセキュリティレベルは、それぞれの関係者のセキュリティレベルと、第三者に対するクラウドプロバイダの依存レベルに依存することが考えられる。

そのような場合、クラウドプロバイダのセキュリティレベルは、それぞれの関係者のセキュリティレベルと、第三者に対するクラウドプロバイダの依存レベルに依存することが考えられる。

「生産」工程における中断や破損、または、関係者間の責任の調整の欠如は、顧客の要求に対する不適合、SLA に対する違反、連鎖的に発生するサービスの不具合等を引き起こし、ひいてはサービスの利用不可、データの機密性、完全性、可用性の喪失、経済的および評判上の喪失等を招く可能性がある。

ここで掲げる重要な例では、（クラウドプロバイダが）第三者によるシングルサインオンや ID 管理サービスに決定的に依存する部分を取り扱っている。この場合、第三者が提供するサービスの中断や、クラウドプロバイダによる当該サービスへの接続における中断、セキュリティ手順における脆弱性等によって、クラウド利用者の可用性や機密性だけではなく、クラウドが提供するサービスすべてが侵害される可能性がある。

通常、契約における透明性の欠如は、システム全体の問題となる可能性がある。したがって、プロバイダがどの主要 IT サービスを外部委託しているかを明言していない場合（頻繁に代わるため、プロバイダが契約者のリストを開示することは現実的ではないが）、顧客は、自分達が直面しているリスクを適切に評価する立場にはない。このような透明性の欠如が、プロバイダに対する信頼度を失墜させる可能性がある。

技術関連のリスク

R.8. リソースの枯渇（リソース割当の過不足）

確率	A. 顧客に対し、追加的な機能を提供できない：中	相対確率：N/A
	B. 現在、契約中の機能を提供できない：低	相対確率：高
影響	A. 顧客に対し、追加的な機能を提供できない：低／中 （例、クリスマス時等）	相対的な影響：N/A
	B. 現在、契約中の機能を提供できない：高	相対的な影響：同等
脆弱性	V15. リソースの使用に関する不正確なモデリング V27. クラウドのインフラに対する投資またはリソース割当の不足 V28. リソースの利用上限制限ポリシーの欠如 V47. サプライヤの冗長化（SUPPLIER REDUNDANCY）の欠如	
影響を受ける資産	A1. 企業の評判 A2. 顧客の信頼 A10. サービス提供 A11. アクセス制御／認証／権限付与（root／管理者対その他）	
リスク	中	

クラウドサービスは、オンデマンドサービスである［クラウドコンピューティング － 実用的な定義参照］。リソースは統計的な予測に従って割り当てられるため、クラウドサービスで使用するすべてのリソースの割り当てにおいては、計算されたリスクレベルというものが存在する。リソースの使用に関する不正確なモデリング（共通リソース割り当てアルゴリズムは、公平性を欠く傾向にある）、または、クラウドのインフラに対する投資またはリソース割当の不足は、クラウドプロバイダの視点から以下のような事態を招く可能性がある：

- サービス利用不可：特定のリソースを集中的に使用する特別仕様のアプリケーションシナリオに不備が起きた場合（すなわち、CPU／メモリによる集中的な数値演算またはシミュレーション（例、株価の予測等））。
- アクセス制御の侵害：場合によっては、リソースの枯渇等により、システムが「フェイルオープン」状態に陥る可能性がある［参考：CWE-400：非制御リソース消費 － リソースの枯渇 (12)］；
- 経済的損失および評判の低下：顧客の要求に対応することができないため；
- リソースのニーズに関する不正確な予測によってもたらされる予想に反する結果；

– インフラストラクチャの肥大化：リソースの過剰な提供による経済的損失や収益性の喪失。

クラウド利用者の視点に立った場合、プロバイダの選定不備やサプライヤの冗長化（SUPPLIER REDUNDANCY）の欠如は、以下のような事態を招くことがある：

– サービス利用不可：リアルタイムおよびそうでない両方のサービス提供の失敗（またはパフォーマンスの低下）；

– アクセス制御システムの侵害：データの機密性と完全性を危険に曝す；

– 経済的損失および評判の低下：顧客の要求に対する不適合、SLA に対する違反、連鎖的に発生するサービスの不具合等が原因。

リソースは統計的な予測に従って割り当てられるため、クラウドサービスで使用するすべてのリソースの割り当てにおいては、計算されたリスクレベルというものが存在する。

注：このようなリスクは、DDoS 攻撃（R.15 参照）や、一部のクラウドプロバイダシステムにおける不適切なアプリケーション間の隔離によるアプリケーションの誤動作の結果であることも考えられる。

R.9. 隔離の失敗

確率	低（プライベートクラウドの場合） 中（パブリッククラウドの場合）	相対確率：高
影響	非常に高	相対的な影響：高
脆弱性	V5. ハイパーバイザの脆弱性 V6. リソース分離の欠如 V7. 不信の伝播に対する隔離の欠如 V17. 内部（クラウド）ネットワークへの偵察行為が発生する可能性 V18. 共同利用者からの覗き見の可能性	
影響を受ける資産	A1. 企業の評判 A2. 顧客の信頼 A5. 個人の秘密データ A6. 個人データ A7. 個人データ（重要） A9. サービス提供 – リアルタイムによるサービス A10. サービス提供	
リスク	**高**	

複数のテナント化とリソースの共有は、クラウドコンピューティングの環境を定義付ける二つの特徴で

ある。計算能力、ストレージおよびネットワークは、複数のユーザ間で共有される。このクラスのリスクには、ストレージ、メモリ、ルーティング、および共有されるインフラストラクチャを使用する異なるテナント間での評判を隔離するメカニズムの不備が含まれる（例、いわゆるゲストホッピング攻撃、同じテーブルに格納されている複数顧客のデータを開示する SQL インジェクション攻撃、サイドチャネル攻撃等）。

このクラスのリスクには、ストレージ、メモリ、ルーティング、および共有されるインフラストラクチャを使用する異なるテナント間での評判を隔離するメカニズムの不備が含まれる（例、いわゆるゲストホッピング攻撃、同じテーブルに格納されている複数顧客のデータを開示する SQL インジェクション攻撃、サイドチャネル攻撃等）。

このインシデントシナリオが現実となる確率は、検討中のクラウドモデルよって変わることに留意すること。この確率は、プライベートクラウドでは低く、パブリッククラウドの場合に、高（中）を示す可能性が高い。

また、この影響としては、価値あるデータや機密データの損失、クラウドプロバイダやそのクライアントに対するサービスの中断や評判の失墜等が考えられる。

R.10. クラウドプロバイダ従事者の不正－特権の悪用

確率	中（従来型システムより低）	相対確率：低
影響	非常に高（従来型システムより高）	相対的な影響：高（集合型の場合） 相対的な影響：同等（単独顧客の場合）
脆弱性	V34. 役割と責任の不明確性 V35. 役割定義の適用の不備 V36. 「知る必要性」原則の不適用 V1. AAA の脆弱性 V39. システムまたは OS の脆弱性 V37. 物理的なセキュリティ手順の不備 V10. 暗号化状態でのデータ処理が不可能であること V48. アプリケーションの脆弱性またはパッチ管理の不備	
影響を受ける資産	A1. 企業の評判 A2. 顧客の信頼 A3. 従業員の忠誠心と経験 A4. 知的財産 A5. 個人の秘密データ	

	A6. 個人データ A7. 個人データ（重要） A8. 人材データ A9. サービス提供 － リアルタイムによるサービス A10. サービス提供
リスク	高

クラウドプロバイダ従事者による悪意の行動は、全データの機密性、完全性、可用性、IP およびすべてのサービスに影響を与える可能性があるため、組織の評判、顧客の信頼および従業員の経験等にも間接的な影響がもたらされる。クラウドアーキテクチャでは、非常に高いリスクを伴う特定の役割が不可欠であるため、クラウドコンピューティングでは、このようなリスクを考慮することが特に重要である。このような役割の例には、クラウドプロバイダのシステム管理者や監査者、侵入検知関連の報告やインシデント対応を扱うマネージドセキュリティサービスプロバイダ等が含まれる。クラウドの利用が増えるに従って、クラウドプロバイダの従業員も犯罪組織の標的にされる確率が高まる（金融サービス業のコールセンターの従業員(13)、(14)の証言も得られている）。

R.11. 管理用インターフェースの悪用（操作、インフラストラクチャアクセス）

確率	中	相対確率：高
影響	非常に高	相対的な影響：高
脆弱性	V1. AAA の脆弱性 V4. 管理用インターフェースへのリモートアクセス V38. 設定ミス V39. システムまたは OS の脆弱性 V48. アプリケーションの脆弱性またはパッチ管理の不備	
影響を受ける資産	A1. 企業の評判 A2. 顧客の信頼 A5. 個人の秘密データ A6. 個人データ A7. 個人データ（重要） A9. サービス提供 － リアルタイムによるサービス A10. サービス提供 A14. クラウドサービスの管理用インターフェース	
リスク	中	

パブリッククラウドプロバイダの顧客管理インターフェースは、インターネット経由でアクセス可能であり、（従来のホスティングプロバイダよりも）大規模なリソースへのアクセスを可能にする。したがって、特に、リモートアクセスやウェブブラウザ関連の脆弱性と組み合わさった場合に、リスクが増大する。

パブリッククラウドプロバイダの顧客管理インターフェースは、インターネット経由でアクセス可能であり、（従来のホスティングプロバイダよりも）大規模なリソースへのアクセスを可能にする。したがって、特に、リモートアクセスやウェブブラウザ関連の脆弱性と組み合わさった場合に、リスクが増大する。これには、多数の仮想マシンを制御する顧客用インターフェースが含まれるが、最も重要なことは、クラウドシステム全体のオペレーションを制御するクラウドプロバイダ用のインターフェースも含まれているということである。当然のことながら、このようなリスクは、プロバイダがセキュリティ関連の投資を増額することによって緩和することができる。

R.12. データ転送途上における攻撃

確率	中	相対確率：高（一部のデータ）
影響	高	相対的な影響：同等
脆弱性	V1. AAA の脆弱性 V8. 通信路暗号の脆弱性 V9. アーカイブおよび転送中のデータの暗号化の強度不足または未実施 V17. 内部（クラウド）ネットワークへの偵察行為が発生する可能性 V18. 共同利用者からの覗き見の可能性 V31. 利用規約の完全性と透明性の欠如	
影響を受ける資産	A1. 企業の評判 A2. 顧客の信頼 A4. 知的財産 A5. 個人の秘密データ A6. 個人データ A7. 個人データ（重要） A8. 人材データ A23. バックアップまたはアーカイブデータ	
リスク	中	

分散型アーキテクチャであるクラウドコンピューティングは、従来型のインフラストラクチャよりも多くのデータを転送できることを示している。たとえば、複数分配されたマシンイメージ、複数の物理マシンに分配されたイメージ、クラウドインフラストラクチャとリモートウェブクライアント間等で同期化する目的で、データが転送されなければならない。更に、データセンターでのホスティングの利用の多くは、VPN に類似したセキュアな接続環境を利用して実現されているが、これは必ずしもクラウドの流れに従うものではない。

盗聴、なりすまし、介入者攻撃、サイドチャネルやリプレイ攻撃等は、脅威をもたらす可能性のあるソースとして考慮されるべきである。

また、クラウドプロバイダが機密性または機密保持に関する条項を提供しない場合や、これらの条項が提供されていても、「クラウド」内を巡回する顧客の機密情報や「ノウハウ」を保護するのに十分ではない場合がある。

R.13. データ漏えい（アップロード時、ダウンロード時、クラウド間転送）

確率	中（N/A）
影響	高
脆弱性	V1. AAA の脆弱性 V8. 通信路暗号の脆弱性 V17. 内部（クラウド）ネットワークへの偵察行為が発生する可能性 V18. 共同利用者からの覗き見の可能性 V10. 暗号化状態でのデータ処理が不可能であること V48. アプリケーションの脆弱性またはパッチ管理の不備
影響を受ける資産	A1. 企業の評判 A2. 顧客の信頼 A3. 従業員の忠誠心と経験 A4. 知的財産 A5. 個人の秘密データ A6. 個人データ A7. 個人データ（重要） A8. 人材データ A12. クレデンシャル A13. ユーザディレクトリ（データ） A14. クラウドサービスの管理用インターフェース
リスク	**中**

これらは前項のリスクと同様だが、クラウドプロバイダとクラウド利用者との間でデータを転送する際に適用される。

R.14. セキュリティが確保されていない、または不完全なデータ削除

確率	中	相対確率：高
影響	非常に高	相対的な影響：高
脆弱性	V20. 機密性の高いメディアのサニタイゼーション（記録の抹消）	
影響を受ける資産	A5. 個人の秘密データ A6. 個人データ A7. 個人データ（重要） A12. クレデンシャル	
リスク	**中**	

クラウド利用者のリソースを、経済的な影響を与えるような悪質な方法で、他の利用者が使用するシナリオがいくつか存在する。

プロバイダが変更になると、リソースの縮小や物理的なハードウェアの再割り当て等が行われ、データが、セキュリティポリシーで規定されている寿命以上に長く利用可能となる場合がある。これは、データを完全に消去するには、他のクライアントのデータも格納されているディスクを破壊するしかないため、セキュリティポリシーによって規定されている手順を実施することが不可能な場合があるためである。クラウド関連のリソースを削除するよう要請があった場合、ほとんどのオペレーティングシステムでなされるようには、データが完全に消去されるとは限らない。データを完全に消去する必要がある場合には、特別な手順に従わなければならないが、これは標準 API によってサポートされていない可能性がある。

効果的な暗号化が使用されていれば、リスクのレベルは低くなると考えられる。

R.15. DDoS 攻撃（分散サービス運用妨害攻撃）

確率	顧客：中	相対確率：低
	プロバイダ：低	相対確率：N/A
影響	顧客：高	相対的な影響：高
	プロバイダ：非常に高	相対的な影響：低
脆弱性	V38. 設定ミス V39. システムまたは OS の脆弱性 V53. フィルタリングリソースの不備または設定ミス	
影響を受ける資産	A1. 企業の評判 A2. 顧客の信頼 A9. サービス提供 － リアルタイムによるサービス A10. サービス提供 A14. クラウドサービスの管理用インターフェース A16. ネットワーク（接続等）	
リスク	中	

R.16. EDoS 攻撃（経済的な損失を狙ったサービス運用妨害攻撃）

確率	低
影響	高
脆弱性	V1. AAA の脆弱性 V2. ユーザプロビジョニングの脆弱性 V3. ユーザプロビジョニング削除の脆弱性

	V4. 管理用インターフェースへのリモートアクセス V.28 リソースの利用上限制限ポリシーの欠如
影響を受ける資産	A1. 企業の評判 A2. 顧客の信頼 A9. サービス提供 ― リアルタイムによるサービス A10. サービス提供
リスク	中

クラウド利用者のリソースを、経済的な影響を与えるような悪質な方法で、他の利用者が使用するシナリオがいくつか存在する。経済的な影響としては、以下のものが挙げられる：

- ID の窃盗：攻撃者は、自身の利益のために、または顧客に経済的な損失を負わせるために、アカウントと顧客のリソースを利用する。
- クラウド利用者は、有料リソースの使用について有効な制限を定めておらず、悪意の行動以外でも、予期せぬリソースの負荷を体験することがある。
- 攻撃者は、クラウド利用者に割り当てられたリソースを枯渇させるために、公共チャネルを使用する。たとえば、クラウド利用者が HTTP リクエストを送るたびに料金を支払う場合、DDoS 攻撃が効果的である。

EDoS は、経済的リソースを破壊する。最悪の場合、顧客の破産や重大な経済的影響をもたらす。

注：一般的な資産である「お金」については、リストでは言及していない。

R.17. 暗号鍵の喪失

確率	低	相対確率：N/A
影響	高	相対的な影響：高
脆弱性	V11. 不適切な鍵管理手順 V12. 鍵生成：乱数生成器への低エントロピーの入力	
影響を受ける資産	A4. 知的財産 A5. 個人の秘密データ A6. 個人データ A7. 個人データ（重要） A8. 人材データ A12. クレデンシャル	
リスク	中	

これには、悪意の関係者に対する秘密鍵（SSL、ファイルの暗号化、顧客の秘密鍵等）やパスワードの開示、それらの鍵の喪失や破壊、あるいは、認証の不正使用やデジタル署名による否認防止の不正使用がある。

R.18. 不正な探査またはスキャンの実施

確率	中	相対確率：低
影響	中	相対的な影響：低
脆弱性	V17. 内部（クラウド）ネットワークへの偵察行為が発生する可能性 V18. 共同利用者からの覗き見の可能性	
影響を受ける資産	A1. 企業の評判 A2. 顧客の信頼 A9. サービス提供 ― リアルタイムによるサービス A10. サービス提供	
リスク	中	

不正な探査またはスキャンは、ネットワークマッピングと共に、考慮中の資産に対する間接的な脅威である。これらは、ハッキング行為のための情報収集に利用できる。これによる影響には、サービスやデータの機密性、完全性および可用性の喪失等が考えられる。

R.19. サービスエンジンの侵害

確率	低
影響	非常に高
脆弱性	V5. ハイパーバイザの脆弱性 V6. リソース分離の欠如
影響を受ける資産	A5. 個人の秘密データ A6. 個人データ A7. 個人データ（重要） A8. 人材データ A9. サービス提供 ― リアルタイムによるサービス A10. サービス提供
リスク	中

クラウドアーキテクチャはそれぞれ、極めて特殊なプラットフォーム ― すなわち、物理的なハードウェアリソース上にあり、様々な抽象レベルで顧客リソースを管理しているサービスエンジン ― に依存している。たとえば、IaaS クラウドの場合、このソフトウェアの構成要素がハイパーバイザであることがある。サービスエンジンは、クラウドプラットフォームのベンダーや、場合によってはオープンソースコミュニティによって開発、サポートされている。これは、クラウドコンピューティングプロバイダによって、更にカスタマイズされ得る。

> クラウドプロバイダは、顧客が実施しなければならない最低限の活動を明確にするために、明確な責任の分担を決定しなければならない。

その他のソフトウェアレイヤと同様、サービスエンジンのプログラムにも脆弱性が存在する可能性があり、攻撃の対象となったり、思わぬ不具合に見舞われることがある。攻撃者は、仮想マシンの内部（IaaS クラウド）、ランタイム環境（PaaS クラウド）、アプリケーションプール（SaaS クラウド）やサービスエンジンの API からハッキングして、サービスエンジンを侵害することができる。

サービスエンジンのハッキングは、異なる顧客環境の分離を曖昧にするのに役立ち（牢獄破りのごとく）、内部に格納されているデータへアクセスし、見えない形で内部の情報を監視・改変することができ（顧客環境内のアプリケーションと直接対話することなく）、また、サービス運用妨害を引き起こすために、割り当てられたリソースを減少させることもできる。

R.20. 利用者側の強化手順と、クラウド環境との間に生じる矛盾

確率	低
影響	中
脆弱性	V31. 利用規約の完全性と透明性の欠如 V23. 複数利害関係者間で矛盾する SLA 条項 V34. 役割と責任の不明確性
影響を受ける資産	A4. 知的財産 A5. 個人の秘密データ A6. 個人データ A7. 個人データ（重要）
リスク	**中**

クラウド利用者は、責任不履行が自身のデータやリソースを更なるリスクに晒すことになるという点を認識し、その責任を負わなければならない。

クラウドプロバイダは、顧客が実施しなければならない最低限の活動を明確にするために、明確な責任の分担を決定しなければならない。顧客が自身の環境を保護することに失敗した場合、プロバイダがリソースを隔離するために必要な手続きを取らなかった場合には、クラウドプラットフォームが脆弱になる可能性がある。したがって、クラウドプロバイダは、隔離メカニズムの更なる明確化を図り、顧客が自身のリソースを保護できるよう、ベストプラクティス指針を提供すべきである。

クラウド利用者は、責任不履行が自身のデータやリソースを更なるリスクに晒すことになるという点を認識し、その責任を負わなければならない。中には、顧客のデータのセキュリティを保証するためのすべての活動を、クラウドプロバイダが責任を持って、実施していると勘違いしているケースもある。顧客によるこのような勘違いや、クラウドプロバイダによる明確な説明の不足が原因で、顧客のデータが不必要なリスクに晒されてしまうといったケースがある。したがって、クラウドの利用者は、自身の責任の範囲を認識すると共に、それを遵守することが不可欠である。

クラウドプロバイダは、その性質上、サーバ上の仮想化を通じて、あるいは、顧客が共通のネットワー

クを共有する形で、複数テナント環境を提供することを業務としている。多くの顧客が共同利用するということは、通信のセキュリティに関する顧客の要件もそれぞれに異なる可能性が高く、このような要件の相違から生じる対立を、クラウドプロバイダは避けることができない。

たとえば、二人の顧客が従来型のネットワークインフラストラクチャを共有している場合を考える。一方の顧客が、SSH 以外のすべてのトラフィックを遮断するようネットワークファイアウォールを設定したいと思っており、もう一方の顧客は、ウェブサーバファームを稼働していて、HTTP と HTTPS による通過を必要としている場合、どちらに軍配が上がるだろうか？　これと同様の問題が、適合性要件を主張し合い、対立する顧客間でも持ち上がっている。この種の課題は、テナント数や彼らの要件の格差が増す程、悪化の一途を辿る。したがって、クラウドプロバイダは、これらの課題にテクノロジー、ポリシーおよび透明性を通じて対応する姿勢を取らなければならない。

法的なリスク

R.21.　証拠提出命令と電子的証拠開示

確率	高
影響	中
脆弱性	V6.　リソース分離の欠如 V29.　複数の司法管轄権を跨るデータ格納とそれに対する認識の欠如 V30.　司法管轄権に関する情報の欠如
影響を受ける資産	A1.　企業の評判 A2.　顧客の信頼 A5.　個人の秘密データ A6.　個人データ A7.　個人データ（重要） A9.　サービス提供 ― リアルタイムによるサービス A10.　サービス提供
リスク	**高**

法執行機関や民事訴訟による証拠提出命令により物理的なハードウェアを没収された場合(15)、ストレージの集中化やテナントによる物理的なハードウェアの共有は、多くの顧客のデータが、開示したくない相手に開示されるリスクを負うことを意味している(16)、(17)、(18)。

それと同時に、長距離型のハイパーバイザへの移行が係争中である場合、一国の政府機関が「クラウド」を没収するのは不可能であろう。

R.22. 司法権の違いから来るリスク

確率	非常に高
影響	高
脆弱性	V30. 司法管轄権に関する情報の欠如 V29. 複数の司法管轄権を跨るデータ格納とそれに対する認識の欠如
影響を受ける資産	A1. 企業の評判 A2. 顧客の信頼 A5. 個人の秘密データ A6. 個人データ A7. 個人データ（重要） A9. サービス提供 ― リアルタイムによるサービス A10. サービス提供
リスク	**高**

顧客のデータは複数の司法管轄域で保存される場合もあり、その一部は高いリスクに晒される可能性がある。仮にデータセンターがリスクの高い国に設置されている場合（例、法体制が十分ではない、法的なフレームワークおよび執行が不透明な国、警察権力が独裁的な国、国際的な取り決めを遵守しない国等）、サイトは地元当局によって襲撃されたり、データまたはシステムが強制的に開示・没収される可能性がある。我々は、法執行機関による証拠提出命令が、すべて容認できないと言っている訳ではなく、その中には容認できないものも存在し、（稀ではあるが）ハードウェアの合法的な没収が、データの格納法如何によって、法執行機関が要求している以上に多くの顧客に影響を及ぼす可能性があることに留意する必要があることを言及しているだけである(19)、(20)。

R.23. データ保護に関するリスク

確率	高
影響	高
脆弱性	V30. 司法管轄権に関する情報の欠如 V29. 複数の司法管轄権を跨るデータ格納とそれに対する認識の欠如
影響を受ける資産	A1. 企業の評判 A2. 顧客の信頼 A5. 個人の秘密データ A6. 個人データ A7. 個人データ（重要） A9. サービス提供 ― リアルタイムによるサービス A10. サービス提供
リスク	**高**

クラウドコンピューティングは、クラウド利用者やプロバイダに対し、いくつかのデータ保護関連のリスクをもたらす。

- クラウド利用者（データ管理者としての役割において）にとって、クラウドプロバイダが実行するデータの処理方法を効果的にチェックし、データが合法的に扱われていることを保証することが困難な場合がある。クラウドプロバイダが、外部処理の役割において個人データの処理を実行していたとしても、個人データの処理に関して主要な責任を有するのは顧客であることを明確にしておかなければならない。データ保護に関する法律を遵守できない場合、国によっても異なるが、データ管理者に対して行政上、民事上、刑事上の処分が下されることになる場合がある。この問題は、たとえば、連携しているクラウド間で複合的なデータ転送を行う場合に深刻化する。一方、クラウドプロバイダの中には、自身が担っているデータ処理に関する情報を提供するところもある。また、クラウドプロバイダの中には、自身のデータ処理およびデータセキュリティ活動、ならびに実施中のデータ制御について認証サマリーを提供するところもある（例、SAS70 認証プロバイダ）。
- クラウドプロバイダからデータ管理者に対して通知されないデータセキュリティ違反が発生することがある。
- クラウド利用者は、クラウドプロバイダによって処理されるデータをコントロールできないかもしれない。これは、たとえば、（連携しているクラウドプロバイダ間で）複合的なデータ転送を行う場合に多発する問題である。
- クラウドプロバイダは、顧客（すなわち、データ管理者）から合法的でない方法で収集されたデータを受け取ることもある。

R.24. ライセンスに関するリスク

確率	中	相対確率：高
影響	中	相対的な影響：高
脆弱性	V31. 利用規約の完全性と透明性の欠如	
影響を受ける資産	A1. 企業の評判 A9. サービス提供 ― リアルタイムによるサービス A20. 認証	
リスク	中	

インスタンス毎に課金されるといったライセンス条件や、オンラインでのライセンスの確認は、クラウド環境では使用できないことがある。たとえば、インスタンス毎に課金されるソフトウェアの場合、新たなマシンのインスタンスが作成されるたびに課金されるため、同一期間内に同じ数のマシンを使用していた場合でも、他のソフトウェアに比べてクラウド利用者のライセンス費用は飛躍的に増大すること

がある。PaaS や IaaS の場合は、クラウド内部で、独自の成果物が発生する可能性がある（新しいアプリケーションやソフトウェア等）。すべての知的財産と同様、適切な契約条項によって保護されていなければ、この独自の成果物がリスクに晒される可能性がある（付録 I ― クラウドコンピューティング ― 法律上の重要な問題点、知的財産の項を参照）。

クラウドに特化していないリスク

一連のリスク分析では、クラウドコンピューティングに特化していない以下の脅威を識別したが、典型的なクラウドベースのシステムのリスクを評価する際には、これらの脅威も慎重に考慮すべきである。

R.25. ネットワークの途絶

確率	低	相対確率：同等
影響	非常に高	相対的な影響：高
脆弱性	V38. 設定ミス V39. システムまたは OS の脆弱性 V6. リソース分離の欠如 V41. 事業継続計画および災害復旧計画の欠如、不備、テストの未実施	
影響を受ける資産	A9. サービス提供 ― リアルタイムによるサービス A10. サービス提供	
リスク	中	

最も高いリスクの一つは！ 一度に数千人の顧客が影響を被ることである。

R.26. ネットワークの管理（ネットワークの混雑、接続ミス、最適でない使用）

確率	中	相対確率：同等
影響	非常に高	相対的な影響：高
脆弱性	V38. 設定ミス V39. システムまたは OS の脆弱性 V6. リソース分離の欠如 V41. 事業継続計画および災害復旧計画の欠如、不備、テストの未実施	
影響を受ける資産	A1. 企業の評判 A2. 顧客の信頼 A3. 従業員の忠誠心と経験 A9. サービス提供 ― リアルタイムによるサービス A10. サービス提供 A16. ネットワーク（接続等）	
リスク	高	

R.27. ネットワークトラフィックの改変

確率	低
影響	高
脆弱性	V2. ユーザプロビジョニングの脆弱性 V3. ユーザプロビジョニング削除の脆弱性 V8. 通信路暗号の脆弱性 V16. 脆弱性診断プロセスに関する管理の欠如
影響を受ける資産	A1. 企業の評判 A2. 顧客の信頼 A5. 個人の秘密データ A6. 個人データ A7. 個人データ（重要） A9. サービス提供 ― リアルタイムによるサービス A10. サービス提供
リスク	中

R.28. 特権の（勝手な）拡大

確率	低	相対確率：低
影響	高	相対的な影響：高（クラウドプロバイダ）
脆弱性	V1. AAA の脆弱性 V2. ユーザプロビジョニングの脆弱性 V3. ユーザプロビジョニング削除の脆弱性 V5. ハイパーバイザの脆弱性 V34. 役割と責任の不明確性 V35. 役割定義の適用の不備 V36. 「知る必要性」原則の不適用 V38. 設定ミス	
影響を受ける資産	A5. 個人の秘密データ A6. 個人データ A7. 個人データ（重要） A8. 人材データ A11. アクセス制御／認証／権限付与（root／管理者対その他） A13. ユーザディレクトリ（データ）	
リスク	中	

R.29. ソーシャルエンジニアリング攻撃（なりすまし）

確率	中	相対確率：同等
影響	高	相対的な影響：高
脆弱性	V32. セキュリティ意識の欠如 V2. ユーザプロビジョニングの脆弱性 V6. リソース分離の欠如 V8. 通信路暗号の脆弱性 V37. 物理的なセキュリティ手順の不備	
影響を受ける資産	A1. 企業の評判 A2. 顧客の信頼 A3. 従業員の忠誠心と経験 A4. 知的財産 A5. 個人の秘密データ A6. 個人データ A7. 個人データ（重要） A8. 人材データ A11. アクセス制御／認証／権限付与（root／管理者対その他） A12. クレデンシャル	
リスク	中	

R.30. 運用ログの喪失または改ざん

確率	低	相対確率：低
影響	中	相対的な影響：同等（顧客）
脆弱性	V52. ログの収集および保存に関するポリシーの欠如または手順の不備 V1. AAA の脆弱性 V2. ユーザプロビジョニングの脆弱性 V3. ユーザプロビジョニング削除の脆弱性 V19. 法的対応体制の不備 V39. システムまたは OS の脆弱性	
影響を受ける資産	A21. 運用ログ（クラウド利用者およびクラウドプロバイダ）	
リスク	中	

R.31. セキュリティログの喪失または改ざん（フォレンジック捜査の操作）

確率	低	相対確率：低
影響	中	相対的な影響：同等（顧客）
脆弱性	V52. ログの収集および保存に関するポリシーの欠如または手順の不備 V1. AAA の脆弱性	

	V2. ユーザプロビジョニングの脆弱性 V3. ユーザプロビジョニング削除の脆弱性 V19. 法的対応体制の不備 V39. システムまたは OS の脆弱性
影響を受ける（情報）資産	A22. セキュリティログ
リスク	中

R.32. バックアップの喪失、盗難

確率	低	相対確率：低
影響	高	相対的な影響：同等（顧客）
脆弱性	V37. 物理的なセキュリティ手順の不備 V1. AAA の脆弱性 V2. ユーザプロビジョニングの脆弱性 V3. ユーザプロビジョニング削除の脆弱性	
影響を受ける資産	A1. 企業の評判 A2. 顧客の信頼 A5. 個人の秘密データ A6. 個人データ A7. 個人データ（重要） A8. 人材データ A9. サービス提供 ― リアルタイムによるサービス A10. サービス提供 A23. バックアップまたはアーカイブデータ	
リスク	中	

R.33. 構内への無権限アクセス（装置その他の設備への物理的アクセスを含む）

確率	非常に低	相対確率：低
影響	高（影響を極めて高くするには標的型攻撃を行う（特定のマシンを狙う等）それ以外の影響は高である。	相対的な影響：高
脆弱性	V37. 物理的なセキュリティ手順の不備	
影響を受ける資産	A1. 企業の評判 A2. 顧客の信頼 A5. 個人の秘密データ A6. 個人データ A7. 個人データ（重要） A8. 人材データ	

	A23. バックアップまたはアーカイブデータ
リスク	中

クラウドプロバイダは、リソースを大規模なデータセンターに集約しているため、物理的な境界制御が強化されている可能性が高いが、それらの制御が侵害された場合の影響は大きい。

R.34. コンピュータ設備の盗難

確率	非常に低	相対確率：低
影響	高	相対的な影響：高
脆弱性	V37. 物理的なセキュリティ手順の不備	
影響を受ける資産	A5. 個人の秘密データ A6. 個人データ A7. 個人データ（重要） A8. 人材データ A17. 物理的なハードウェア	
リスク	中	

R.35. 自然災害

確率	非常に低	相対確率：低
影響	高	相対的な影響：高
脆弱性	V41. 事業継続計画および災害復旧計画の欠如、不備、テストの未実施	
影響を受ける資産	A1. 企業の評判 A2. 顧客の信頼 A5. 個人の秘密データ A6. 個人データ A7. 個人データ（重要） A8. 人材データ A9. サービス提供 ー リアルタイムによるサービス A10. サービス提供 A23. バックアップまたはアーカイブデータ	
リスク	中	

一般的に、クラウドプロバイダがデフォルトで複数の冗長的なサイトやネットワークパスを提供しているため、自然災害によるリスクは従来型のインフラストラクチャよりも低い。

4. 脆弱性

以下の脆弱性リストは、包括的なものではないが、本文書で実施した分析の目的を果たすのに十分なレベルで詳述されている。このリストは、一般的な情報セキュリティ上の脆弱性と、クラウドに特化した脆弱性の両方をまとめている。

V1. AAA の脆弱性

認証、認可、課金管理（AAA）が不適切なシステムでは、以下の状況により、通常、リソースに対する不正アクセスや特権の（勝手な）拡大、リソースの悪用やセキュリティインシデントに対する追跡不能が助長される可能性がある：

- クラウドアクセスクレデンシャルが、クラウド利用者によって安全に保管されていない；
- 不適切な役割の割り当てが行われている；
- クレデンシャルが一過性のマシンに格納されている。

更に、クラウドでは、企業のアプリケーションがインターネット上で公開されているため、パスワードに基づいた認証への攻撃（トロイの木馬を使用して企業のパスワードを盗もうとするなど）のインパクトは絶大である。したがって、クラウドのリソースへのアクセスを許可するにあたっては、パスワードに基づく認証だけでは不十分となり、より強力な認証、または、二要素認証が必要となるであろう。

V2. ユーザプロビジョニングの脆弱性

- 顧客は、プロビジョニングプロセスを制御することができない。
- 顧客の ID は、登録時に適切に検証されていない。
- クラウドシステムの構成要素（時間およびプロファイルコンテンツ）間の同期に遅延が発生する。
- 同期のとれていない ID のコピーが、複数作成される。
- クレデンシャルは、盗聴や再生に対して脆弱である。

V3. ユーザプロビジョニング削除の脆弱性

失効に時間を要するため、回収されたクレデンシャルが有効のままである。

V4. 管理用インターフェースへのリモートアクセス

論理的には、たとえば、応答と要求時の脆弱な認証を通じて、末端マシンの脆弱性により、クラウドインフラストラクチャ（単一顧客またはクラウドプロバイダ）が悪用される。

V5. ハイパーバイザの脆弱性

ハイパーバイザレイヤへの攻撃は非常に魅力的である：事実、ハイパーバイザは、物理的なリソースや、ハイパーバイザ上で稼働する仮想マシンを全面的に制御しているため、この層における脆弱性は特に重

大である。ハイパーバイザを悪用することは、すべての仮想マシンを悪用することと同義である。ハイパーバイザの下層部への攻撃というコンセプトの証明が、初めて King らによる論文(21)に著されており、筆者らは、仮想マシンをベースにしたルートキットの考え方を紹介している。当時、最も一般的なハイパーバイザで特定された脆弱性がいくつか存在し（例、(22)および(23)）、その時点では、管理者権限なしで悪用することが可能であったが、執筆当時、それらの脆弱性のうち、パッチ処理がなされていないものは、一つもなかった。

ハイパーバイザの脆弱性を利用することによって可能となる典型的なシナリオは、「ゲストからホストへの回避（guest to host escape）」と呼ばれるもので、その一例としては、最近、発見され、参考文献(24)で紹介された VM ウェアの脆弱性である、「クラウドバースト（Cloudburst）」がある。もう一つのシナリオは、「VM ホッピング（VM hopping）」と呼ばれ、攻撃者がある標準的な手法を利用して仮想マシンをハッキングし、ハイパーバイザの脆弱性を利用して、同一のハイパーバイザ上で稼働する他の仮想マシンの制御を奪うものである。詳しくは、「*Empirical Study into the Security Exposure to Hosts of Hostile Virtualized Environments*（好ましくない仮想環境のホストが抱えるセキュリティ問題に関する実証的研究）」(25)を参照されたい。

V6.　リソース分離の欠如

ある顧客によるリソースの利用は、別の顧客によるリソースの利用にも影響を与え得る。IaaS クラウドコンピューティングのインフラストラクチャの多くは、物理的なリソースが複数の仮想マシン、すなわち複数の顧客によって共有されるアーキテクチャ設計に依存している。

ハイパーバイザのセキュリティモデルにおける脆弱性は、これら共有されるリソースへの不正アクセスの原因になる可能性がある。たとえば、顧客 1 と顧客 2 の仮想マシンは、SAN の内部の同じ共有 LUN（論理ユニット番号）に保存される仮想ハードドライブを備えている。顧客 2 は、自身の仮想マシンに顧客 1 の仮想ハードドライブをマッピングして、内部のデータを閲覧したり、使用することが可能となるかもしれない。IaaS クラウドで使用されるハイパーバイザは、クラウドプロバイダが所有権管理、および顧客に公開するプロビジョニングや報告用インターフェースを開発するために利用できる、多彩な API を提供している。したがって、ハイパーバイザのセキュリティモデルや「管理用のインターフェース」に脆弱性が存在する場合には、顧客の情報に不正アクセスされる可能性がある。同時に、このレベルの脆弱性は、クラウド設備内にある資産を操作する機会を攻撃者に与えるばかりではなく、サービス運用妨害（攻撃）を誘発したり（例、稼働中の仮想マシンをシャットダウンする）、データを漏えいさせたり（例、データをコピーし、クラウドの仮想マシンの外部へ転送する）、データを侵害したり（例、仮想マシンを改変した複製マシンで置き換える）、直接的な経済損害を与えたりする（例、仮想マシンを多数複製し、立ち上げる）可能性がある。また、クラウド**上で物理サーバの所在を割り出し、そこに同居すること（攻撃）に対する管理の不備（または欠如）や**クロスサイドチャネル攻撃に関する脆弱性（(26)参照）は、リソースの隔離に重大なリスクをもたらし得る。たとえば、顧客 1 と顧客 2 でリソースの使用が独立していない場合、顧客 1 は顧客 2 のリソースをマッピングすることができてしまう。これは、たとえば、顧客 1 が自身のリソースの可用性のパターンの変化を測定する一方で、顧客 2 に対して管理されたリソースローディング（投入）を行うことにより可能となる。

ある文献の中で、Craig Gentry 氏は、このアルゴリズムの完璧なまでに合理的で単純な適用事例である、暗号化されたキーワードでの Web 検索を実行した場合、計算時間が約 1 兆規模で高まると予測した。これは、将来的に、データの格納以外の活動を行うクラウド利用者は、クラウドプロバイダを信用するしかないことを意味する

最終的に、サービス品質（QoS）や分散型リソーススケジューリング（DRS）製品等に関する利用規約（ToS）やより詳述なサービスレベルアグリーメント（SLA）を作成するツールが不足している場合、ある顧客によるクラウド施設の独占的な利用が可能となり、他の顧客にサービス運用妨害やパフォーマンスの低下による影響を与えることになる。

V7.　不信の伝播に対する隔離の欠如

ある顧客の活動が、他の顧客の評判に影響をもたらす。

V8.　通信路暗号の脆弱性

通信路暗号の脆弱性から、たとえば、MITM 攻撃、認証の不備、自署の証明書の容認等を通じて、転送中のデータが盗聴される可能性が懸念される。

V9.　アーカイブおよび転送中のデータの暗号化の強度不足または未実施

転送中のデータ、アーカイブやデータベースに格納されているデータ、マウントされていない仮想マシンイメージ、フォレンジックイメージやデータ、格納されている機密ログやその他のデータの暗号化に不備があると、それらのデータがリスクに晒される。当然のことながら、鍵管理を実装するための費用［V11］や処理費用は、導入されるビジネスリスクを考慮し、そのリスクに対応するように設定しなければならない。

V10.　暗号化状態でのデータ処理が不可能であること

格納されているデータの暗号化は難しくはないが、準同型暗号(27)が近年発展しているにもかかわらず、データ処理時に暗号化を維持できる商用システムの出現可能性は少ない。ある文献の中で、Bruce Schneier 氏は、このアルゴリズムの完璧なまでに合理的で単純な適用事例である、暗号化されたキーワードでの Web 検索を実行した場合、計算時間が約 1 兆規模で高まると予測した。これは、将来的に、データの格納以外の活動を行うクラウド利用者は、クラウドプロバイダを信用するしかないことを意味する。

V11.　不適切な鍵管理手順

クラウドコンピューティングのインフラストラクチャでは、様々な種類の鍵を管理し、格納する必要がある。例としては、転送中のデータを保護するセッション鍵（例、SSL 鍵等）、ファイル暗号化鍵、クラウドプロバイダを識別するペア鍵、顧客を識別するペア鍵、認証トークンや失効認証書 (29)等がある。仮想マシンには、固定的なハードウェアインフラストラクチャが備わっておらず、また、クラウドベー

スのコンテンツは地理的に分散されている傾向があるため、クラウドインフラストラクチャの鍵に対して、ハードウェアセキュリティモジュール（HSM）ストレージなどの標準的な管理策を適用するのは更に困難である。たとえば：

- HSM は、（窃盗、盗聴や改ざん等から）強力かつ物理的に保護されている。しかし、（たとえば、地理的に分散され、数多く複製される）クラウドのアーキテクチャで使用する複数の箇所に HSM を分散させるのは非常に困難である。さらに、（HSM が標準的にサポートする）PKCS#10 等の鍵管理規格や PKCS#11 (30)等の関連規格は、分散システムとのインターフェースとしての標準化されたラッパー（wrapper）を提供していない。
- ユーザとクラウド鍵ストレージ間の通信チャネルおよびリモートの相互認証メカニズムの使用によるセキュリティの低下のため、公共のインターネットを経由してアクセス（間接的も含む）可能な鍵管理インターフェースは、更に脆弱である。
- 自身を認証する必要がある新たな仮想マシンは、ある種の秘密を使用してインスタンス化されなければならない。このような秘密の配布によって、拡張性の問題が浮上する可能性がある。ペア鍵を発行する認証局の迅速な拡張は、リソースがあらかじめ決定されていれば容易に達成することができるが、階層的な認証局における動的で計画外の拡張では、新たな認証局（登録や認証、新たなコンポーネントの認証や新たなクレデンシャルの配布等）の生成においてリソースのオーバーヘッドが生じるため、その達成は困難である。
- 分散型アーキテクチャでの鍵の失効を行う費用も高価である。既知の時間の制約によりリスクの大きさが決定されるため、鍵の効果的な失効には、鍵の状態（通常は認証書）を確認するアプリケーションが不可欠である。これを実現するための分散メカニズムは存在するが（(31)と(32)を参照）、クラウドの異なる部分が同等レベルのサービスを受け、異なるレベルのリスクと向き合うことがないよう保証するのは困難である。OCSP などの中央集約化されたソリューションは高価であり、CA や CRL が密接に関連付けられていない限り、リスクを必ずしも低減させない。

V12. 鍵生成：乱数生成器への低ーエントロピーの入力

仮想化技術および不足した入力デバイスの組み合わせである標準的なシステムイメージは、その（鍵生成）システムが、物理的な RNG（Cloud Computing Security (33)参照）よりもかなり低いエントロピーしかもてないことことを意味している。これはまた、乱数を生成するために使用されるエントロピーソースが類似しているため、ある仮想マシン上の攻撃者が別の仮想マシン上で生成された暗号鍵を推測できる可能性があることを意味している。この問題の解決は決して難しくはないが、システム設計の段階で考慮されていない場合には、重大な結果を招く可能性がある。

V13. 技術とソリューションにおける標準の欠如

標準が欠如しているということは、プロバイダにデータがロックインされる可能性があることを意味する。これは、プロバイダが業務を停止した場合に、重大なリスクとなる。

これにより、マネージドセキュリティサービスや FIM のような外部セキュリティ技術の使用が禁止され

ることがある。

多くのプロバイダが顧客に対し、あらかじめリソースを確保することを許可していても、リソース提供アルゴリズムは、以下の理由で失敗する可能性がある：

リソースの使用に関する不正確なモデリング。これは、オーバーブッキング状態やオーバープロビジョニング状態（ひいては、クラウドプロバイダ側のリソースの浪費）につながる可能性がある。

V14. ソースコードエスクロー（預託）契約の欠如

ソースコードエスクロー（預託）契約の欠如は、PaaS または SaaS プロバイダが倒産した場合に、サービスの利用者が保護されないことを意味する。

V.15. リソースの使用に関する不正確なモデリング

クラウドサービスは、統計に則って提供されるため、リソースの枯渇に対し特に脆弱である。多くのプロバイダが顧客に対し、あらかじめリソースを確保することを許可していても、リソース提供アルゴリズムは、以下の理由で失敗する可能性がある：

- リソースの使用に関する不正確なモデリング。これは、オーバーブッキング状態やオーバープロビジョニング状態（ひいては、クラウドプロバイダ側のリソースの浪費）につながる可能性がある。有名なリソース配分アルゴリズムには、Token Bucket (34)、Fair Queuing (35)、Class Based Queuing (36)等がある。これらのアルゴリズムは、公平性を欠く傾向にある（例として(37)参照）。
- 何らかの異常によりリソース配分アルゴリズムに不具合が生じた場合（例、コンテンツの配送における範囲外のニュースイベント等）。
- リソースの分類が不適切であったことが原因でジョブ分類またはパケット分類を使用するリソース配分アルゴリズムに不具合が生じた場合。
- 全体的なリソース提供における不具合（一時的なオーバーロードとは別）。

V16. 脆弱性診断プロセスに関する管理の欠如

ポートスキャンや脆弱性テストへの制限は重大な脆弱性であり、顧客にインフラストラクチャの構成要素のセキュリティを確保する責任を課すような利用規約と組み合わさった場合、重大なセキュリティ問題となる。

V17. 内部（クラウド）ネットワークへの偵察行為が発生する可能性

クラウド利用者は、内部ネットワーク内の別の利用者に対して、ポートスキャンや他のテストを実施することができる。

V18. 共同利用者からの覗き見の可能性

リソース分離の欠如を突いたサイドチャネル攻撃によって、攻撃者は、どのリソースをどの顧客が共有しているかを判断することができる。

V19. 法的対応体制の不備

クラウドには、法的対応体制を向上させる可能性があるが、多くのプロバイダは、これを実現するための適切なサービスや利用規約を提供していない。たとえば、SaaS プロバイダは、一般的に、コンテンツにアクセスするクライアントの IP ログに対して、アクセスを提供していないであろう。IaaS プロバイダは、最近の仮想マシンやディスクイメージ等のフォレンジックサービスを提供しない可能性がある。

V20. 機密性の高いメディアのサニタイゼーション（記録の抹消）

物理的なストレージリソースを複数のテナントが共有することは、たとえば、ディスクが別のテナントによって使用されていたり、特定できなかったり、あるいは、手順が用意されていない等の理由で、メディアを物理的に破壊することができない場合に、データのライフサイクル終了時に適用されるデータ破壊ポリシーが適用できなかったりするため、機密性の高いデータが漏えいする可能性があることを意味する。

V21. クラウド外の契約上の義務または責任のクラウドへの適用

クラウド利用者は、サービス規約の中で彼らに割り当てられている責任に気付いていないことが多い。アーカイブの暗号化などの活動に対する責任は、クラウドプロバイダに帰属すると勘違いされる傾向にある。これは、関係者双方で交わした契約の中で、そのような責任をクラウドプロバイダが負うことはないことが明示的に記載されている場合であっても、起こりうる。

V22. クラウドをまたがるアプリケーションに潜在する相互依存性

サービスサプライチェーンの中に相互依存性（内部／外部クラウドにおける相互依存性）が潜在し、関係する第三者、請負業者、または顧客企業と、サービスプロバイダとの間で通信が途絶した場合に、クラウドプロバイダのアーキテクチャが、クラウドによって提供されている業務に継続的に対応しないこと。

V23. 複数利害関係者間で矛盾する SLA 条項

SLA の条項と、その他の約定、または別のプロバイダとの条項の間に矛盾が生じている可能性がある。

V24. SLA 条項に含まれる過剰なビジネスリスク（クラウドプロバイダにとって）

SLA は、技術的不備による実際のリスクに備え、プロバイダ側に過剰なビジネスリスクを課すことがある。顧客の視点からは、SLA には顧客に不利益をもたらす条項が含まれている場合がある。たとえば、知的財産の分野であれば、SLA では、クラウドインフラストラクチャに格納されているあらゆるコンテンツに対する権利を、クラウドプロバイダが有する旨を規定している場合がある。

V25.　利用者に監査または認証の証明書が提供されない問題

クラウドプロバイダは、監査や認証によって、顧客に保証を提供することはできない。

たとえば、クラウドプロバイダによっては、オープンソースのハイパーバイザや組織のためにカスタマイズしたハイパーバイザ（例、Xen (38)）を使用する場合があり、いくつかの組織（例、米国政府機関）にとって必須要件であるコモンクライテリア(39)認証を取得していない場合もある。

本文書では、認証と脆弱性レベルの間に直接的な関連があると言っている訳ではないことに留意されたい（認証製品のプロテクションプロファイルやセキュリティターゲットに関する十分な情報を入手していないため）。

V26.　クラウドのインフラに適用できる認証スキームの欠如

クラウドに特化した管理策は存在しない。つまり、セキュリティの脆弱性が見過ごされる可能性があることを意味している。

V.27.　クラウドのインフラに対する投資またはリソース割当の不足

インフラストラクチャへの投資には時間がかかる。仮に予測モデルに不備があれば、クラウドプロバイダのサービスは長期間提供不能となり得る。

V.28.　リソースの利用上限制限ポリシーの欠如

顧客やクラウドプロバイダに、リソースに制限をかけるためのフレキシブルで設定可能な方法がない場合は、リソースの使用が予測できないと問題に発展する可能性がある。

V29.　複数の司法管轄権を跨るデータ格納とそれに対する認識の欠如

末端ネットワークによる配送データのミラーリングや、データの格納場所についてのリアルタイム情報をクラウド利用者が利用できない冗長化ストレージにおいては、相当なレベルの脆弱性が誘発される。特に、ストレージの司法管轄域に関して明確な情報が提供されていない場合、企業は知らずに規則違反を侵す可能性がある。

V30.　司法管轄権に関する情報の欠如

データは、強制的な差し押さえに対して無力で、リスクの高い司法管轄域に格納・処理される可能性がある。このような情報がクラウド利用者に対して提供されない場合、それを阻止する手段を講じることができない。

V31.　利用規約の完全性と透明性の欠如

クラウドに特化していない脆弱性

本文書におけるリスク分析において、クラウドコンピューティングには特化していない以下の脆弱性を識別したが、典型的なクラウドベースのシステムを評価する際には、これらの脆弱性も慎重に考慮すべきである。

V32. セキュリティ意識の欠如

クラウド利用者は、クラウドへ移行した時に直面する可能性があるリスク、特に、制御の喪失、ベンダーのロックイン、クラウドプロバイダリソースの枯渇等、クラウド特有の脅威から生じるリスクについて認識していない。このようなセキュリティ意識の欠如が、これらのリスクを緩和するために講じるべき活動を認識していないクラウドプロバイダにも影響を及ぼす可能性がある。

V33. 身元調査プロセスの欠如

規模の関係で、クラウドプロバイダの中には、非常に高い特権を持つ役割が存在することがあるため、このような役割を果たす担当者のリスクプロファイルについての調査が行われない、または調査に不備がある場合、重大な脆弱性となる。

V34. 役割と責任の不明確性

これらの脆弱性は、クラウドプロバイダ組織内の役割や責任の帰属が不適切であることを示している。

V35. 役割定義の適用の不備

クラウドプロバイダ内で、役割の分離に失敗した場合、過剰な特権を持つ役割を生じさせ、それが、非常に大規模なシステムを脆弱にする可能性がある。たとえば、誰一人、クラウド全体へのアクセス特権を与えられるべきではない。

V36. 「知る必要性」原則の不適用

これは、役割と責任に関する脆弱性の特異なケースである。関係者には、不必要なデータへのアクセス権を与えるべきではない。そのような権限が与えられている場合、不要なリスクを招くことになる。

V37. 物理的なセキュリティ手順の不備

この中には、以下の項目が含まれる：

- 物理的な境界における制御の欠如（入室時におけるスマートカード認証等）
- 盗聴に対して脆弱な、重要資産に対する、電磁的シールドの欠如

V38. 設定ミス

このクラスの脆弱性には、セキュリティベースラインや強化手順の不適切な適用、人為的なエラーや訓練を受けていない管理者等が含まれる。

V39.　システムまたは OS の脆弱性

V40.　信頼できないソフトウェア

V41.　事業継続計画および災害復旧計画の欠如、不備、テストの未実施

V42.　資産目録の欠如、不備、不正確性

V43.　資産分類の欠如、不備、不足

V44.　不明確な資産の管理責任

V45.　プロジェクト要件定義の不足

この中には、セキュリティや法律への適合性要件に関する考慮不足、システムユーザやアプリケーションユーザの関与欠如、不明確または不適切なビジネス要件等が含まれる。

V46.　プロバイダの選定不備

V47.　サプライヤの冗長化（SUPPLIER REDUNDANCY）の欠如

V48.　アプリケーションの脆弱性またはパッチ管理の不備

このクラスの脆弱性には、アプリケーションプログラムのバグ、プロバイダと顧客間におけるパッチ適用手順の矛盾、テストされていないパッチの適用、ブラウザの脆弱性等が含まれる。

V49.　リソースの消費に関する脆弱性

V50.　プロバイダによる NDA 違反

V51.　データ喪失に対する責任（クラウドプロバイダ）

V52.　ログの収集および保存に関するポリシーの欠如または手順の不備

V53.　フィルタリングリソースの不備または設定ミス

5. 資産

資産	前述の各要素に対する説明、または参照先	オーナー（関係者、または関係組織）	認識される価値（非常に低－低－中－高－非常に高）
A1. 企業の評判		クラウド利用者	非常に高
A2. 顧客の信頼	苦情申立人が評価し得るもので、誠意が含まれる	クラウド利用者	非常に高
A3. 従業員の忠誠心と経験		クラウド利用者	高
A4. 知的財産		クラウド利用者	高
A5. 個人の秘密データ	（欧州のデータ保護指令の定義通り）	クラウドプロバイダ／クラウド利用者	非常に高（在宅ケアシステムを使用している者に関する情報も含まれるため）
A6. 個人データ	（欧州のデータ保護指令の定義通り）	クラウドプロバイダ／クラウド利用者	中（運用上の価値）／高（喪失した場合の価値）
A7. 個人データ（重要）	欧州のデータ保護指令において個人データの範疇に含まれている全データ、および、組織または企業によって重要と判断または分類されるデータ	クラウドプロバイダ／クラウド利用者	高（運用上の価値）／高（喪失した場合の価値）
A8. 人材データ	データ保護要件以外に、運用上の見地から関係するデータ	クラウド利用者	高
A9. サービス提供 －リアルタイムによるサービス	時間が重視されるサービスで、ほぼ 100%に近い可用性レベルが必要	クラウドプロバイダ／クラウド利用者	非常に高
A10. サービス提供		クラウドプロバイダ／クラウド利用者	中
A11. アクセス制御／認証／権限付与（root／管理者対その他）		クラウドプロバイダ／クラウド利用者	高
A12.クレデンシャル	システムにアクセスする患者および担当者のもの	クラウド利用者	非常に高

A13. ユーザディレクトリ（データ）	これが適切に機能しなければ、誰もアクセスできない	クラウド利用者	高
A14. クラウドサービスの管理用インターフェース	クラウドを通じて提供されるすべてのサービスを管理する管理用インターフェース（ウェブベースまたはリモートシェル等）	クラウドプロバイダ／クラウド利用者	非常に高
A15. 管理用インターフェース API		クラウドプロバイダ／クラウド利用者／EuropeanHealth	中
A16. ネットワーク（接続等）	内部および外部クラウドの接続を含む	クラウドプロバイダ／クラウド利用者	高
A17. 物理的なハードウェア		クラウドプロバイダ／クラウド利用者	低（損失程度に依存）／中（十分に保護されていない状態で盗難にあった場合、重大となる可能性あり）
A18. 物理的な建物		クラウドプロバイダ／クラウド利用者	高
A19. クラウドプロバイダアプリケーション（ソースコード）		クラウドプロバイダ／クラウド利用者	高
A20. 認証	ISO、PCI DSS 等	クラウドプロバイダ／クラウド利用者	高
A21. 運用ログ（クラウド利用者およびクラウドプロバイダ）	これらログは、ビジネスプロセスを維持、最適化するため、および、監査目的で使用	クラウドプロバイダ／クラウド利用者	中
A22. セキュリティログ	セキュリティ違反の証拠やフォレンジック解析時に有効	クラウドプロバイダ／クラウド利用者	中
A23. バックアップまたはアーカイブデータ		クラウドプロバイダ／クラウド利用者	中

6. 推奨事項および重要なメッセージ

本節では、主要な推奨事項や重要なメッセージを記している：

- 情報セキュリティ確保のためのフレームワークは、質問形式の標準的なチェックリストであり、情報セキュリティに関する保証の取得（クラウド利用者によって）や保証の提供（クラウドプロバイダによって）を目的として使用することができる。
- 法律関連の推奨事項
- 研究に関する推奨事項

情報セキュリティ確保のためのフレームワーク

はじめに

本文書で最も重要な推奨事項の一つは、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。

> 本節の推奨事項では、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。

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。

本節の推奨事項では、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。

> 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。

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。

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）

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

[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。

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。

SaaS (Software as a Service)

利用者	プロバイダ
ー 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 ー ID 管理システムの維持管理 ー ID 管理システムのマネジメント ー 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）	ー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） ー 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、ストレージ、ネットワーク帯域等） ー 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） ー 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） ー システムの監視 ー 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） ー ログの収集およびセキュリティの監視

PaaS (Platform as a Service)

利用者	プロバイダ
ー ID 管理システムの維持管理 ー ID 管理システムのマネジメント ー 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）	ー 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） ー 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、ストレージ、ネットワーク帯域等） ー 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） ー 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） ー システムの監視

	ー 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） ー ログの収集およびセキュリティの監視

IaaS (Infrastructure as a Service)

利用者	プロバイダ
ー ID 管理システムの維持管理 ー ID 管理システムのマネジメント ー 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） ーゲスト 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） ー 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） ー ゲストシステムの監視 ー 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） ー ログの収集およびセキュリティの監視	ー 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） ー 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、ストレージ、ネットワークの帯域等） ー ホストシステム（ハイパーバイザ、仮想ファイアウォール等）

（（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：

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（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 のトップ 10 参照(40)）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。

> 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。

- 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(41)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。

メソドロジー

本文書の主だった節は、ISO/IEC 27001/27002 (42)、(43)および BS25999 (44)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 (45)等、上記以外の規格も追加される予定である。

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。

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、最終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。

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？

情報セキュリティ確保のための要件

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

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？

運用上のセキュリティ

外部プロバイダとの金銭的契約（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？

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 (46)、SANS Checklist (47)、SAFECode (48)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？

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？

ネットワークアーキテクチャの管理策

- DDoS 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 (49)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）？

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？

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？

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？

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？

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。

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？

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？

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？

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？

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？

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？

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）？

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。

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？

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？

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？

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？

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 ― 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？

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？

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）？

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？

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？

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。

クラウド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？

法律関連の推奨事項

現在、クラウドコンピューティング関連の法律問題のほとんどは、クラウド利用者による、契約書、利用規約、ユーザライセンス同意書（ULA）および SLA 等の評価によって解消されるであろう。しかしながら、クラウド市場で提供されている様々な契約の中から一つを選択する中小規模組織と、契約条項を交渉できる立場にある大企業とを区別することが重要である。本文書における法律的な分析では、より一般的と考えられる､クラウド市場で提供されている様々な契約や SLA 等をアセスメントする中小規模組織の視点を採用している。これは、クラウドコンピューティングのビジネスモデルが、外部委託のビジネスモデルとは異なるためである。クラウドコンピューティングでは、いくつかの利点を利用者にもたらすために、低コストのサービス提供による規模の経済に依存するが、これは、顧客のニーズに合わせて微細に調整されたサービスとは対照的である。しかし、大規模な組織も、契約交渉の際に、同様の検討事項を適用できる。類似のインターネット技術に関連する過去の経験則からも、クラウドコンピューティング関連のセキュリティリスクを評価するためのガイダンスがクラウド利用者とプロバイダに提供されるが、これらのリスクを評価する際には、両者がクラウドコンピューティング特有の性質を考慮する必要がある。

共通の基盤は多々あるが､クラウドコンピューティングの性質が故に､特定の標準契約条項については､追加的な確認が必要となることが考えられる。セキュリティ違反の通知、データの転送、派生成果物の作成（creation of derivative works）、管理策の変更（change of control）、および法執行機関によるデータアクセスといった点に関する各々の権利や義務に、特に注意を払うべきである。クラウドでは、重要な内部インフラストラクチャを外部委託することができ、そのインフラストラクチャが使用できなくなった場合には、その影響が広範囲に及ぶ可能性がある。したがって、関係者は、法的責任の割り当て（関係者によるクラウドの利用方法を考慮した場合の）、またはインフラストラクチャに対する責任の割り当てにおいて、法的責任に関する標準的な制限が反映されているか否かについて、注意を払うべき

である（**責務の範囲**の項参照）。

法的な判例によって、クラウドコンピューティングに特化したデータセキュリティに関連した懸念事項が明らかになるまでは、クラウドプロバイダと利用者は共に、リスクに効果的に対処するための契約条項の策定を目指すべきである。

以下は、顧客が、クラウドサービスの SLA、ToU、ULA、その他の合意を評価する際に、特に注意を払うべき分野をまとめたものである：

1. **データの保護**：実施されるべき処理を管理する、十分なレベルの技術的セキュリティ対策および組織的な対策を提供できる処理者を選択し、それらの対策への適合を保証することに関して、注意を払うべきである。
2. **データセキュリティ**：契約条項がこれらの義務に対応していない場合に、クラウドプロバイダまたは利用者のいずれかが規制や司法関連の対策の対象となる、必須のデータセキュリティ対策に注意を払うべきである。
3. **データの転送**：クラウドプロバイダの占有するクラウド内部、そのクラウド外部および欧州経済圏の内外におけるデータの転送方法に関して、どのような情報がクラウド利用者に提供されるかに注意を払うべきである。
4. **法執行機関によるアクセス**：法執行機関によるデータへのアクセスに関して、各国では独自の制約や要件が設けられている。クラウド利用者は、データが格納・処理される司法管轄域に関して、プロバイダから提供される情報に注意を払い、その司法管轄域に起因するあらゆるリスクを評価すべきである。
5. **機密性と守秘義務**：本件に関する義務については、再確認すべきである。
6. **知的財産**：IaaS や PaaS の場合、クラウドインフラストラクチャを利用して創造された独創的作品を含む知的財産を格納することもあり得る。クラウド利用者は、提供されるサービスの品質が低下することなく（例、バックアップは、適切なサービスレベルを提供する上で必要な要素となり得る）、契約によって知的財産や独創的な作品に関する彼らの権利が最大限に配慮されることを確認するべきである。
7. **リスクの割当と責任の範囲**：両当事者が契約書上の各自の義務を再確認する場合、両者は、当該契約義務の相手方による違反に対する金銭的補償条項または補償義務を含めることによって、両者に対する重大なリスクに発展し得る義務を強調すべきである。更に、責任の制限を規定する標準的な条項は、慎重に評価されるべきである。
8. **管理策の変更**：管理策が変更になった場合や、契約を撤回する可能性がある場合等に、クラウドプロバイダが、契約義務を継続的に遵守する能力に関する透明性。

本文書に記載されている法律関連の推奨事項は、概して、クラウド利用者の立場から表現されている。

欧州委員会に対する法律関連の推奨事項

本文書では、欧州委員会が以下の項目を調査し、明確にするよう提言する：

1. データ保護指令（Data Protection Directive）、および Article 29 Data Protection Working Party による推奨事項に関連するいくつかの課題によって、明確化が必要であることが示される。特に：

2. どのような状況において、クラウドプロバイダが共同管理者（Joint Controller）として識別されるか；

3. あるクラウドプロバイダから別のプロバイダへ、または組織のクラウド内において、データが転送されている場合、欧州経済圏外の国々におけるデータ処理にもデータ保護指令のセクション 25(2) が適用されるか。[2]

4. 適切なレベルのデータ保護が保証されていない欧州経済圏外の国々とデータを送受信する際のデータへの影響。

5. データ保護指令が起草されて以後の技術の進歩、特に、説明責任に基づく法律的な手法（例、Galway Project (51)で提案されている）を踏まえて、「データの転送」の概念を再検討すべきかどうか。

6. クラウドプロバイダに、彼らの顧客に対してデータのセキュリティ違反を通知する義務があるかどうか、また、その顧客が末端利用者に対してどのような情報を提供すべきか。これは、セキュリティ違反を捜査すべきという旨を契約条項に盛り込むことによっても実現でき、より実効性が高まることを意味する。たとえば、違反の報告に関する法制は、施行が困難であり、透明性を阻害する可能性がある。

7.電子商取引指令（第 12～15 条）の中間債務免除条項がどのようにクラウドプロバイダに適用されるかを、加盟国が明らかにする必要があるかどうか。

8. クラウドに格納されているデータに対する様々な公共機関の要求を統制する法律に関する加盟国間の相違、特に、敷地内（自宅または職場）に格納されている個人データおよびクラウド内に格納されている個人データに対する政府からの要求に対する保護のレベルの相違。

説明責任の概念に基づき、必要最低限のデータ保護規格およびプライバシー認証スキームを最適にサポートする方法。その方法は、全世界、または少なくとも全 EU 加盟国において、共通である。

法律関連の五つの問題点については、付録Iで更に詳しく説明している。

[2] 2009 年に改訂された電子プライバシー指令（http://register.consilium.europa.eu/pdf/en/09/st03/st03674.en09.pdf）では、加盟国に対して、セキュリティ違反の通知方式を導入するよう要求している。この方式は、電気通信ネットワークや電気通信サービスに適用できるが、クラウドコンピューティングサービス等の情報社会サービスには適用されない。

調査関連の推奨事項

クラウドコンピューティング技術のセキュリティを向上させるために優先的に調査すべき分野として、以下を推奨する：

クラウドにおける信頼の確立

- クラウドのための認証プロセスと規格：一般的には、クラウドに特化したガバナンス規格の規定に対して認証が可能なクラウドコンピューティングのセキュリティライフサイクル規格（COBIT (52)、ITIL (53)等）
- クラウドコンピューティングにおけるセキュリティの測定方法(metrics)；
- セキュリティに対する投資対効果（ROSI）：クラウドコンピューティングの測定はセキュリティに対する投資対効果測定の正確性を向上させる可能性がある
- セキュリティ違反に関する報告形式が異なることによる影響；
- 適切なレベルのセキュリティを維持しながら、透明性を向上させる技術：
  * タグ付け（例、場所のタグ付け、データの種類によるタグ付け、ポリシーのタグ付け等）
  * プライバシー保護付きデータプロベナンスシステム（例、システムを通じた End-to-End でのデータ追跡等）
- クラウド内外の End-to-End でのデータの機密性：
  * 暗号化された検索（長期）
  * 暗号化の処理方式（長期）
  * クラウド内のソーシャルアプリケーション用の暗号化ツールおよび機密性を確保するためのツール
  * クラウドにおけるトラステッドコンピューティング（例、仮想マシンのスタックのための信頼できる起動シーケンス等；
- より高い保証を提供するクラウド、仮想プライベートクラウド等；
- クラウドベースの信頼の、クライアントベースのデータやアプリケーションへの拡大。

組織を跨る大規模システムにおけるデータの保護

以下の分野は、クラウドコンピューティングに関する更なる調査が必要な分野である：

- データの破壊とライフサイクルの管理
- 完全性の検証 － クラウドにおけるバックアップおよびアーカイブとそのバージョン管理
- フォレンジックスおよび証拠収集メカニズム
- インシデント対応 － 監視と追跡可能性
- 論争解決と証拠の規則

- データの保護とプライバシーを含む関連規制の国家間の相違点
  * 複数の国家間に跨るクラウドインフラストラクチャの円滑な機能を促進するための法的手段
  * 司法管轄域の違いによる問題を緩和するための自動化された手段

大規模なコンピュータシステムのエンジニアリング

- 大規模な分散コンピュータシステムにおける階層的なセキュリティ；
- クラウドにおけるセキュリティサービス ― セキュリティ技術の非境界化およびクラウドに対する従来型のセキュリティ境界制御技術の採用（例、HSM、ウェブフィルタ、ファイアウォール、IDS 等）；
- リソース隔離メカニズム ― データ、処理、メモリ、ログ等；
- クラウドプロバイダ間の相互運用性；
- あるクラウドプロバイダから別のプロバイダへ仮想マシン、データおよび仮想マシン上のセキュリティ設定を移行する際のポータビリティ（ベンダーのロックインを防止するための）、ならびに、仮想マシンのバックアップの状態やセッションおよび仮想マシンの長距離ライブ移行の維持；
- クラウドにデータ、アプリケーション、システム全体を供給するためのインターフェースの標準化 ―すべての OS において、対応するクライアントインターフェースを開発できるようにするために必要；
- 規模毎のリソース（帯域幅や CPU 等）の提供と割当（融通性）；
- クラウドプラットフォーム内での拡張性のあるセキュリティ管理（ポリシーや運用手順）：
  * セキュリティおよびデータ保護ポリシーの自動実施；
  * プロバイダによるセキュリティが確保された運用プロセス ― ガバナンスプロセスの実施；
- クラウドコンピューティングの障害耐性(resilience) ― クラウドの障害耐性(resilience)を向上させる方法：
  * クライアント側におけるクラウドアーキテクチャの使用（末端ネットワーク、P2P 等）
    - 複数のクライアントネットワークの統合；
    - クライアントベースの冗長性およびバックアップ；
  * クラウド連携(bursting)とクラウドにおける世界規模での障害耐性(resilience)。

調査関連の推奨事項のための有効な情報源は他に、2009 年 12 月に刊行されるPROCENT（Priorities of Research on Current & Emerging Network Technologies）報告書がある。
http://www.enisa.europa.eu/act/res/technologies/procent参照。

用語と略語

AAA	Authentication, Authorization and Accounting（認証、認可および課金管理）。
AD	Active Directory（アクティブディレクトリ）。
API	Application Programming Interface（アプリケーションプログラミングインターフェース ー ソフトウェア供給者により公開されたインターフェースの仕様）。
ARP	Address Resolution Protocol (2)（アドレス解決プロトコル）。
Asset（資産）	セキュリティ分析における保護の対象。
Availability（可用性）	システムが、その機能を実行することができる時間の割合。
BS	British Standard（英国工業規格）。
CA	Certification Authority（認証局）。
CC	Common Criteria（コモンクライテリア）。
Confidentiality（機密性）	アクセス権限を付与された者のみが情報にアクセスできるという保証（ISO 17799）。
Co-residence	クラウド利用者によるハードウェアまたはソフトウェアリソースの共有。
CP	Cloud Provider（クラウドプロバイダ）。
CRL	Certification Revocation List（認証取消リスト）。
CRM	Customer Relationship Management（顧客関係の管理）。
Data Controller（データ管理者）	個人データを処理する目的や方法を、単独または共同で決定する、自然人、法人、公共機関、政府機関、または、その他の機関。この場合、処理する目的や方法は、国家またはコミュニティの法律や規則により決定され、データ管理者やそれを指名するための特定基準は、国家またはコミュニティの法律によって指定される。
Data Processor（データ処理者）	データ管理者に代わって個人データを処理する自然人、法人、公共機関、政府機関、または、その他の機関。
Data Subject（データ主体）	誰からデータを集め、誰のためにそのデータが処理されるのかの情報から識別された、あるいは、識別可能な自然人（EU 指令 95/46/EC 参照）。
DDoS	Distributed Denial of Service（分散サービス運用妨害）。
De-provision（ユーザプロビジョニング削除）	リソース使用の解除を行う、または一連のユーザ群に対するリソース使用を禁止するプロセス。
Edge network（末端ネットワーク）	本文書では、データの最終送付先に近い位置でデータを処理・格納できるネットワーク化されたコンピュータの意。
EDoS	Economic Denial of Service（経済的な損失を狙ったサービス運用妨害）。
Escrow（エスクロー）	明確に定義された特定の条件が満たされた場合に、リソースへのアクセスが

	許可されている第三者によるリソースの格納。
FIM	Federated Identity Management（ID 管理連携）。
Guest OS（ゲスト OS）	仮想環境で稼働している OS で、クラウド利用者の管理下にあるもの。
Host OS（ホスト OS）	複数の guest OS を稼働させている、クラウドプロバイダの OS。
HSM	Hardware Security Module（ハードウェアセキュリティモジュール）。
Https	TLS または SSL を使用した Http 接続。
Hypervisor（ハイパーバイザ）	ホストコンピュータ上で、複数の OS を同時に稼働できるコンピュータソフトウェアまたはハードウェアプラットフォームの仮想化ソフトウェア。
IDS	Intrusion Detection System（侵入検知システム）。
Integrity（完全性）	データの格納時または転送時に、悪質な意図をもって、あるいは、偶発的にデータが改変されていないというデータ特性。
IP	Internet Protocol（インターネットプロトコル）。
IPS	Intrusion Protection System（侵入防止システム）。
ISO	International Organization for Standardization（国際標準化機構）。
LDAP	Lightweight Directory Access Protocol（軽量ディレクトリアクセスプロトコル）。
MAC	Media Access Control（メディアアクセスコントロール：IP プロトコルにおけるネットワークノードのアドレス）。
MITM	Man In The Middle（マン・イン・ザ・ミドル攻撃。攻撃の一種）。
MSS	Managed Security Service（マネージドセキュリティサービス）。
NIS	Network and Information Security（ネットワークと情報のセキュリティ）。
NIST	National Institute of Standards and Technology（米国国立標準技術研究所）。
Non-repudiation（否認防止）	係争中の関係者が、文書または契約書の有効性を否認または異議申し立てすることができない特性。
OCSP	Online Certificate Status Protocol（オンライン証明書状態プロトコル）。
OS	Operating System（オペレーティングシステム）。
OTP	One-time password（ワンタイムパスワード：認証トークンの一種）。
OVF	Open Virtualization Format（オープン仮想化フォーマット）。
Perimeterisation	資産または資産グループに対するアクセス制御。
Port scan（ポートスキャン）	どのポートが開いており、どんなサービスが提供されているかを判断するためのネットワークホストの探査。
Protection Profile（プロテクションプロファイル）	情報システム製品群について、ベンダーの主張を立証するためのセキュリティ評価基準を定めた文書（コモンクライテリアで使用されている用語）。
Provision	The issuing of a resource（リソースの発行）。

PV LAN	Private VLAN（プライベート仮想化 LAN）。
QoS	Quality of service（サービスの品質）。
RBAC	Role-Based Access Control（役割ベースのアクセス制御）。
Resilience（障害耐性）	（故意でない、意図的に、あるいは自然に生じた）障害に遭遇した場合でも、許容できるレベルのサービスを提供および維持するシステムの能力。
ROI	Return on Investment（投資に対する見返り）。
ROSI	Return on Security Investment（セキュリティ投資に対する見返り）。
RPO	Recovery Point Objective（目標復旧地点）。
RTO	Recovery Time Objective（目標復旧時間）。
RTSM	Real-Time Security Monitoring（リアルタイムセキュリティ監視）
Security Target（セキュリティターゲット）	製品のセキュリティ属性に関するベンダーの主張を立証するためのセキュリティ評価基準を定めた文書（コモンクライテリアで使用されている用語）。
Service engine（サービスエンジン）	クラウドサービスの提供に責任を負うシステム。
Side channel attack（サイドチャネルアタック）	システムの物理的実装から得た情報に基づいた攻撃。（例、タイミング情報、電力消費、電磁的漏えいや音に至るまで、システムに侵入するために悪用され得る余分な情報源となり得る。）。
SLA	Service Level Agreement（サービスレベルアグリーメント）。
SSL	Secure Socket Layer（セキュアソケットレイヤ：ウェブサーバとブラウザ間のトラフィックの暗号化に使用される）。
Subpoena（証拠提出命令）	本文書では、証拠を差し押さえするための法的権限。
TLS	Transport Layer Security（トランスポート層のセキュリティ：ウェブサーバとブラウザ間のトラフィックの暗号化に使用される）。
ToU	Term of Use（利用規約）。
UPS	Uninterruptable Power Supply（無停電電源装置）。
VLAN	Virtual Local Area Network（仮想 LAN）
VM	Virtual Machine（仮想マシン）。
VPC	Virtual Private Cloud（仮想プライベートクラウド）。
VPN	Virtual Private Network（仮想プライベートネットワーク）。
Vulnerability（脆弱性）	データへの不正アクセス、破壊、開示、改ざんおよびサービス運用妨害等、資産に悪影響をもたらす可能性がある状況や事象。
XML	Extensible Mark-up Language（拡張マークアップ言語）。

参考文献

1. **IDC** *Cloud Computing 2010 – An IDC Update*, Frank Gens, Robert P. Mahowald, Richard L. Villars, Sep. 2009 – Doc #TB20090929, 2009
2. *Western European Software-as-a-Service Forecast*, 2009 - 2013, David Bradshaw, Apr. 2009 – Doc # LT02R9, 2009
3. **General Services Administration US-GSA** [Online] http://www.gsa.gov/Portal/gsa/ep/contentView.do?pageTypeId=8199&channelId=24825&P=&contentId=28477&contentType=GSA_BASIC
4. **PCI Security Standards Council** [Online] https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml
5. **NIST** [Online] http://csrc.nist.gov/groups/SNS/cloud-computing/index.html
6. **Wikipedia** [Online] http://en.wikipedia.org/wiki/Cloud_computing
7. **Craig Balding** *cloudsecurity.org* [Online] http://cloudsecurity.org/2008/07/21/assessing-the-security-benefits-of-cloud-computing/
8. **SUN-Project Kenai** [Online] http://kenai.com/projects/suncloudapis/pages/HelloCloud#Examining_the_Virtual_Data_Center
9. **EC – European Commission** [Online] http://ec.europa.eu/enterprise/policies/SME/small-business-act/index_en.htm
10. **ISO/IEC.ISO/IEC 27001:2008** *Information technology – Security Techniques – Information security risk management; Annex E: Information security risks assessment approaches*, 2008
11. **Wikipedia** [Online] http://en.wikipedia.org/wiki/Open_Virtualization_Format
12. **MITRE** [Online] http://cwe.mitre.org/data/definitions/400.html
13. **BBC** [Online] http://news.bbc.co.uk/2/hi/uk_news/scotland/glasgow_and_west/6089736.stm
14. **www.retailresearch.org** [Online] http://www.retailresearch.org/reports/fightinternalfraud.php
15. **NY Daily News** [Online] http://www.nydailynews.com/gossip/2009/08/23/2009-08-23_outted_blogger_rosemary_port_blames_model_liskula_cohen_for_skank_stink.html
16. **Enterprise Storage Forum** [Online] http://www.enterprisestorageforum.com/continuity/news/article.php/3800226
17. **Electronic Discovery Navigator** [Online] http://www.ediscoverynavigator.com/statutesrules/
18. **Find Law** http://technology.findlaw.com [Online] http://technology.findlaw.com/articles/01059/011253.html
19. **CBS 11 TV** [Online] http://cbs11tv.com/local/Core.IP.Networks.2.974706.html
20. **WIRED** *www.wired.com/* [Online] http://www.wired.com/threatlevel/2009/04/company-caught/
21. **Samuel T King, Peter M Chen, Yi-Min Wang, Chad Verbowsk, Helen J Wang, Jacob R Lorch** *Subvirt: Implementing malware with virtual machines*. 2006
22. **Secunia** [Online] http://secunia.com/advisories/37081/

23. – [Online] http://secunia.com/advisories/36389/
24. **Kortchinsky, Kostya** *http://www.immunityinc.com* [Online] http://www.immunityinc.com/documentation/cloudburst-vista.html
25. **Ormandy, Tavis** [Online] http://taviso.decsystem.org/virtsec.pdf
26. **Thomas Ristenpart, Eran Tromer, Hovav Shacham, Stefan Savage** [Online] http://people.csail.mit.edu/tromer/papers/cloudsec.pdf
27. **Gentry, Craig** [Online] http://delivery.acm.org/10.1145/1540000/1536440/p169-gentry.pdf?key1=1536440&key2=6166986521&coll=GUIDE&dl=GUIDE&CFID=60359435&CFTOKEN=10086693
28. **Schneier, Bruce** [Online] http://www.schneier.com/blog/archives/2009/07/homomorphic_enc.html
29. **www.spywarewarrior.com** [Online] http://www.spywarewarrior.com/uiuc/ss/revoke/pgp-revoke.htm
30. **RSA Laboratories, PKCS#11** [Online] http://www.rsa.com/rsalabs/node.asp?id=2133
31. **Jun Zhou, Mingxing He** [Online] http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=4716141
32. **Clulow, Tyler Moore and Jolyon** [Online] http://people.seas.harvard.edu/~tmoore/ifipsec-pres.pdf
33. **Andrew Bechere, Alex Stamos, Nathan Wilcox** [Online] http://www.slideshare.net/astamos/cloud-computing-security
34. **Wikipedia** [Online] http://en.wikipedia.org/wiki/Token_bucket
35. – [Online] http://en.wikipedia.org/wiki/Fair_queuing
36. – [Online] http://en.wikipedia.org/wiki/Class-based_queueing
37. **Devera, Martin** [Online] http://Luxik.cdi.cz/~devik/qos/htb/old/htbtheory.htm
38. **Open Source Xen Community** http://xen.org/[Online]
39. **Common Criteria Recognition Agreement (CCRA)** http://www.commoncriteriaportal.org/[Online]
40. **OWASP** [Online] http://www.owasp.org/index.php/ OWASP_Top_Ten_Project
41. – [Online] http://www.owasp.org/index.php/Category:OWASP_Guide_Project
42. **27001:2005, ISO/IEC** *Information technology – Security techniques – Information security management systems – Requirements*
43. **27002:2005, ISO/IEC** *Information technology – Security techniques – Code of practice for information security management*
44. **Group, BSI** BS 25999 Business Continuity
45. **NIST** *Special Publication 800-53, Revision 2 Recommended Security Controls for Federal Information Systems*
46. **OWASP** [Online] http://www.owasp.org/index.php/Main_Page
47. **SANS Institute** [Online] http://www.sans.org/reading_room/whitepapers/securecode/a_security_checklist_for_web_application_design_1389?show=1389.php&cat=securecode
48. **Software Assurance Forum for Excellence in Code (SAFECode)** [Online] http://www.safecode.org

49. **IEEE Standards Association** [Online] http://standards.ieee.org/getieee802/download/802.1Q-2005.pdf
50. **The European Privacy Seal** [Online] https://www.european-privacy-seal.eu/
51. **EDRI – European Digital Rights** [Online] http://www.edri.org/edri-gram/number7.2/international-standards-data-protection
52. **ISACA** [Online] http://www.isaca.org/Content/NavigationMenu/Members_and_Leaders1/COBIT6/COBIT_Publications/COBIT_Products.htm
53. **Office of Government Commerce (OGC)** [Online] http://www.itil-officialsite.com/home/home.asp
54. **Luis M. Vaquero, Luis Rodero-Merino, Juan Caceres, Maik Lindner** *A Break in the Clouds: Towards a Cloud Definition*
55. **Cloud Security Alliance**, Security Guidance for Critical Areas of Focus in Cloud Computing, April 2009, http://www.cloudsecurityalliance.org/guidance/csaguide.pdf
56. **Jericho Forum**, *Cloud Cube Model: Selecting Cloud Formations for Secure Collaboration, April 2009, http://www.opengroup.org/jericho/cloud_cube_model_v1.0.pdf*
57. **Gartner**, *Assessing the Security Risks of Cloud Computing*, June 2008, http://www.gartner.com/DisplayDocument?id=685308
58. **Data Liberation Front**, Google, http://www.dataliberation.org/

付録 I ー クラウドコンピューティング ー 法律上の重要な問題点

I. すべてのシナリオに共通の、法律上の重要な問題点は、以下五つである：

1. データの保護
   a. 可用性と完全性
   b. 必要最低限の標準または保証
2. 機密性
3. 知的財産
4. 業務上の過失
5. 外部委託サービスおよび管理の変更

II. 本文章で取り上げている問題点の多くは、クラウドコンピューティングに特化したものではない。事実、クラウドコンピューティングサービスの利用者は、クラウドコンピューティングによってもたらされるセキュリティリスクの法律的分析を行う際の基礎として、他のインターネットサービスに適用されている法律的分析を利用することが有効であると認識するであろう。以前の分析の繰り返しにならないように、本文書では、以前のインターネット技術に適用されていた分析のなかで、クラウドコンピューティングセキュリティにおいて、新たな法律上の課題や重大な変化がもたらされるであろう部分に焦点を置いている。

III. クラウドサービスの潜在的な顧客は、データ保護に関連する問題に強い懸念を抱くことであろう。したがって、本文書では、これらの問題点を中心に、より詳細なレベルで法律的分析を行っている。

IV. 本文書では、五つの重要な法律上の問題点を取り上げているが、すべてのシナリオ、およびクラウドコンピューティングに関するすべての議論に共通するテーマは、クラウドコンピューティングプロバイダが、極めて詳細で製品に特化した契約やその他の契約や情報開示を行う必要性と、利用者がこれらの契約や関連文書を慎重に検討する必要性である。クラウド利用者とプロバイダの双方は、クラウドコンピューティング関連の法律上の問題点の多くが、SLA によって解消される、または、解消には至らなくても緩和されるケースが多いため、サービスレベルアグリーメント（SLA）にも細心の注意を払うべきである。

V. 法律的な詳細に入る前に、クラウドプロバイダの顧客の種類（民間から公共団体）や規模（中小から大企業）が様々であるが故に、どの程度交渉できる立場にいるかについても、それぞれに異なることに留意する必要がある。クラウドプロバイダと顧客の関係が、契約内容によって規制されることが多いため、法律的な観点から考えると、この問題は、とても重要である。現状では、具体的な規定が欠如しているため、相互の役割や義務が標準的な一般条件として組み込まれるか、クラウドプロバイダによって一方的に起案され、修正なしに顧客が単純にこれを容認するか、あるいは、特別な同意事項が交渉されることになる。

VI. 以下の表は、クラウド利用者とプロバイダとの間で交渉される契約や合意事項に関して、三つの可能性についてまとめたものである。

クラウドプロバイダ	クラウド利用者
A）大企業 － **契約条項を交渉できる能力が高い**	中小企業 － **契約条項を交渉できる能力は弱い**
B）クラウド利用者とプロバイダ双方が、**契約条項を交渉できる能力**を持つ	
C）中小企業 － **契約条項を交渉できる能力は弱い**	大企業または公共機関 － **契約条項を交渉できる**

A、B、C のどのケースに該当するかによって、本章第 I 項で特定された問題点への対処方法が大きく変わる可能性がある。

VII. クラウド市場で提供されている様々な契約の中から一つを選択する中小規模組織と、契約条項を交渉できる立場にある大企業とを区別することが重要である。クラウドコンピューティングによる主な経済利益は、クラウドコンピューティングが即座に、あるいは、利用量に応じた支払いで調達できる、集団／商品サービス傾向にあるという事実からきていることが予見される（例、ケース A の場合：大手クラウドプロバイダ － 中小企業顧客）。これがサービスや法律関連の条件の標準化にもつながる。したがって、本文書における法律的分析では、これらの問題について、クラウド市場で提供されている様々な契約や SLA 等を評価している中小企業の視点から説明している。

そのような状況であるにもかかわらず、クラウドコンピューティングのサービスが、大顧客、すなわち、大企業や公共機関（例、ケース B の場合）のためにオーダーメイドされる場合も発生するかもしれない。このような場合、特定顧客向けの契約となることが想定される。ケース C は、それ程一般的ではない。ケース C では、ケース B の場合と同様に交渉の余地がある。ただし、大企業は、契約交渉をする際、同じようなことを考えがちである。このような理由により、本文書では、可能な場所では、交渉に関する推奨事項を含めた。

仮に、顧客が特定のプロバイダと契約条件を交渉できなかった場合でも、顧客は、*クラウド市場で提供されている他のサービスから自由に選択できる。したがって、中小企業の場合、特定の契約条項の推奨事項をクラウド市場で提供されているサービスの選択という観点から理解すべきである。*

VIII. 以下の分析結果は、第 VI 項で説明した三つの異なる交渉シナリオを通じて、どのようにこれら五つの法律上の重要な問題点に対応していくかを明らかにしている。

1. データの保護

本章では、クラウドコンピューティングサービスで頻繁に取り沙汰されるデータ保護関連の法律上の問題点を扱い、個人データ処理に係る個人の保護及び当該データの自由な移動に関する欧州議会指令95/46/ECおよび理事会の指令（1009 年 10 月 24 日）[3]（以下「データ保護指令」と称す）で使用されている表現をベースにした、ガイダンスの提供を目的としている。ただし、このような問題点は、データ保護指令を施行する国法によって直接統制されることになるため、クラウドコンピューティングサービスの顧客は、適用可能な国法に基づいて、これらの問題点を再吟味することが望ましい。

用語集

以下の定義は、個人データ処理に係る個人の保護及び当該データの自由な移動に関する欧州議会指令95/46/EC および理事会の指令（1995 年 10 月 24 日）（以下「データ保護指令」と称す）に規定されている。

個人データ（Personal Data）とは、特定された、または、特定可能な自然人（「データ主体」）に関連するすべての情報を指す。識別可能な人物とは、直接または間接的に、特に識別番号や身体的、心理的、精神的、経済的、文化的、あるいは、社会的なアイデンティティ（独自性、個性）に特化した一つ以上の要素を参照することによって識別することができる者である。

機密性の高いデータ（Sensitive Data）とは、人種、種族、宗教、哲学やその他の信仰、政治的意見、所属政党、労働組合、宗教組織、哲学的、政治的または労働党員としての資質等を開示させるような個人データに加え、健康状態やセックスライフを暴露するような個人データを指す。

個人データの処理（Processing）とは、自動的な手法であるなしにかかわらず、個人データに対して行われる収集、記録、組織化、格納、適応または改変、検索、相談、使用、転送による開示、配布またはその他の方法による利用、調整または結合、遮断、削除または破壊等の操作を指す。

データ管理者（Controller）とは、個人データを処理する目的や方法を、単独または共同で決定する、自然人、法人、公共機関、政府機関、または、その他の機関を示す。この場合、処理する目的や方法は、国家またはコミュニティの法律や規則により決定され、データ管理者やそれを指名するための特定基準は、国家またはコミュニティの法律によって指定される。

データ処理者（Processor）とは、データ管理者に代わって個人データを処理する自然人、法人、公共機関、政府機関、または、その他の機関を指す。

[3] 指令 95/46/EC の公式文書および本指令の施行状況は、
http://www.ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm から入手できる。

問題点の定義

1.1. クラウドプロバイダによって提供されるサービスは、一般的に、電子メール、メッセージング、デスクトップ、プロジェクト管理、給与計算、経理と財務、CRM、営業管理、カスタムアプリケーションの開発、カスタムアプリケーション、遠隔治療、および顧客への請求から成るため、個人データ（機密データを含む）の処理が行われると考えられる。このようなデータの所有者（データ主体）はかなりの数になるであろう（例、職員、クライアント、サプライヤ、患者および、より一般的に、ビジネスパートナー）。

1.2. 個人データは間違いなく処理されるとの前提で、データ保護指令がどんな時に適用されるかを正確に理解することは重要である。セクション 4 では、「1. 各加盟国は、以下の場合、個人データの処理に関して、この指令に従って、国内法を適用するものとする：(a) 加盟国の領土内で、データ管理者によって確立された活動内容に基づき、データが処理される場合； 複数の加盟国の領土内に、同じデータ管理者が確立されている場合、確立された内容が、該当する国内法をベースにした義務に適合していることを保証するのに必要な対策を講じられなければならない； (b) データ管理者が加盟国の領土内に確立されてはいないが、国際公法の効力によって、その加盟国の法律が適用される場所に所在している場合； (c) データ管理者が、（欧州）共同体の領土内に確立されておらず、個人データを処理する目的で、自動化されている、いないにかかわらず、当該加盟国内に位置している装置を使用する場合（ただし、そのような装置が、（欧州）共同体の領土を介した輸送目的のみに使用される場合を除く）。」と謳われている。

1.3. データ保護指令のセクション 4 では、以下のように分析されている：

a) データ管理者が確立されている場所が、データ保護指令の適用される地域である場合；
b）個人データを処理する場所やデータ主体の居住地は、データ保護指令の適用と関連しない。

1.4. データ保護指令は、データ管理者がEU圏内に確立されている場合に適用される。また、データ管理者がEU圏内に確立されていない場合でも、個人データを処理するための装置がEU圏内に位置する場合（例、加盟国の領土内に位置し、個人データの格納およびリモート処理を行うデータセンター、コンピュータ、ターミナル、サーバ）で、かつ、そのような装置が、共同体の領土を介した輸送目的のみに使用されない場合にも、データ保護指令が適用される。[4]

1.5. データ保護指令が適用されると決まれば、次に問うべき質問は以下の通りである：
誰がデータ管理者で、誰がデータ処理者であるか？ クラウドプロバイダの顧客が個人データを処理する目的や手法を決定する場合には、この顧客がデータ管理者であり、クラウドプロバイダ

[4] 装置の確立および使用、データ保護指令の適用決定因子に関する詳しい説明は、オンラインソーシャルネットワーキングおよび検索エンジンに関するデータ保護作業グループの意見第 29 条、すなわち、それぞれ、オンラインソーシャルネットワーキングに関する意見 5/2009 および検索エンジンに関連するデータ保護問題に関する意見 1/2008 参照のこと。
(http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2009_en.htm)

が顧客の代わりに個人データを処理する場合、このプロバイダが外部処理者となる[5]。実際に、データ処理者であるか、またはデータ管理者であるかの区分は、従事すべき役割や義務、関連する責任に至るまで全く異質である。本文書の分析では、クラウドプロバイダの顧客がデータ管理者であり、クラウドプロバイダが外部処理者であることを前提としている。

1.6. データ保護指令に示されているデータ管理者の主な役割と義務は以下の通りである：

a）公平性、合法性、終局性、適切性、均衡性、必要性およびデータの最小化の原則に則って個人データを処理すること（データ保護指令セクション 6）。

b）データ保護指令 95/46 の第 7 条a.項が適用されるデータ主体から明瞭な同意を得ること[6]。

c）データ主体に必要な情報を提供したのちに、個人データを処理すること（データ保護指令セクション 10）。

d）データ主体に対し、データ保護指令セクション 12 で規定されている権利を保証すること。例として、データ主体と関連のあるデータが処理されているか否かを確認できること、データを処理する目的、関連するデータの分類、データが開示される受領者または受領者の分類に関する情報を得ること、データ保護指令の規定に違反した方法で処理されたデータを修正、消去または遮断すること、等（データ保護指令セクション 12）。

e）偶発的な喪失、改ざん、不正な開示またはアクセス、および、その他すべての違法な形でのデータ処理がなされないように、個人データを保護するための適切な技術的および組織的なセキュリティ対策を実装すること（データ保護指令セクション 17）。

f）実施されるべき処理を管理する技術的セキュリティ対策および組織的な対策に関して、十分な保証を提供できる処理者を選択すると共に、それらの対策への適合も保証すること。

g）データ主体が、データの転送に関し、あらかじめ明確な同意を示している場合またはデータ保護指令セクション 26 に規定されるその他の条件（例、標準的な契約条項、又は、データが米国に転送される場合には、セーフハーバーの原則）が該当する場合に限り、データ保護指令セクション 25 (2)で謳われている､適切なレベルの保護が保証されない第三国への個人データの転送を許可すること。

---

5 「外部者」は、データ管理者の企業/組織外の人物がデータ処理者となる、特別な場合を意味する。

6 データ保護指令 95/46 の第 7 条では、以下の通り記述されている：
加盟国は、以下の各項に該当する場合に限り、個人データを処理するよう規定しなければならない：
a） データ主体が、明確な意思表示をした場合、
b） データ主体が当事者である契約の履行のために、または、契約を取り交わす前に、データ主体の要求により措置を講じる上で、処理が必要な場合、
c） データ管理者が対象となる法的義務を遵守するために処理が必要な場合、
d） データ主体の重要な利益を保護するために処理が必要な場合、
e） 公益のために実施されるタスク、または、データ開示の対象となる、正当な権限を与えられたデータ管理者または第三者が職務遂行のために行うタスクの達成のために、処理が必要な場合、あるいは、
f） データ開示の対象となる、データ管理者または第三者により追求される正当な利益のために、処理が必要な場合（ただし、データ保護指令第 1 条(1)で規定される、保護が必要なデータ主体の基本的な権利および自由を守ることが、そのような利益よりも優先される場合を除く）。

1.7. データ管理者（本分析では、クラウド利用者）は、データ処理に関するすべての必須情報を、データ主体（クラウド利用者のエンドユーザ）に提供すべきである。クラウド利用者は、データ保護指令に基づき、自身の顧客に対し、クラウドプロバイダへの移転に関する状況、クラウドプロバイダ（すなわち、外部処理者）の品質および移転の目的を通知するよう義務付けられている。事実、上記 1.1.のサービスを具体化することは、このようなデータを、EU内またはEU経済圏外の国（第三国）に在住している可能性のある第三者[7]（すなわち、クラウドプロバイダ）に通信または転送する行為を意味する[8]。これらの国々では、データ保護指令セクション 25(2)項が意味するところの、個人データに対する適切なレベルの保護が提供されない可能性がある。したがって、データ保護指令の対象となるデータを収集する者は、当該データの使用や転送に関して、このデータ保護指令が適用されることを理解していることが重要である。この点について、現時点ではまだクラウドコンピューティングに従事していないデータ管理者は、EU経済圏外でデータの処理および転送が行われることに関して、データ主体からインフォームドコンセント（状況をよく説明して相手の同意を得ること）を得ることが推奨される。現在、クラウドコンピューティングに従事しているデータ管理者は、この同意が取り付けられていること、および、この同意の中で、データの処理や転送の性質や範囲が適切に説明されていることを保証することが推奨される。代替手段の一つとしては、セクション 26 に記載されている手続きの一つを利用することである（例、標準的な契約条項またはセーフハーバーの原則、データが米国に転送される場合およびクラウドプロバイダが当該プログラムに参加している場合）。実際、二番目の方法は、データ主体によって随時、取り消すことができるため、データ主体の同意に基づきデータを転送することによって、何らかの利点がもたらされることがある。

1.8. 委員会により、データ保護指令のセクション 25(2)項が適用されることを明示することが推奨される。この項は、あるクラウドコンピューティングプロバイダから別のプロバイダにデータが転送される場合や、ある組織のクラウド内でデータが転送される場合で、そのクラウドが、EU 経済圏外のある司法管轄域を含む、複数の司法管轄域に跨って存在している場合に発生しうる、EU 経済圏外の国におけるデータ処理に対して適用される。

1.9. データ処理に関与しているすべての関係者（データ主体、データ管理者および処理者）は、データ保護指令、および関連規則（EU加盟諸国において施行されているデータ保護指令は、この規則に準じている）で明らかにされている、データ処理に関するそれぞれの権利や義務の把握に努めるべきである[9]。更に、これら関係者は、人権と基本的な自由に関する欧州条約第 8 条に規定される、他人に邪魔されない生活を送る権利についても理解するべきである。この際、関係する国々

---

[7] いくつかの国の国内法では（例、ドイツ連邦のデータ保護法）、「転送」や「第三者」と言った用語が、法的な意味合いを持つ法律用語として定義されている。ここでは、そのような意味でこれらの用語を使用している訳ではない。

[8] 残念ながら、データの転送に関する公式な定義は存在しないようである。ただし、データ保護指令 95/46/EC のセクション 4 の記述によると、法律上の観点から見た場合、領土を介したデータ転送であれば問題ないと考えることができる。例えば、データが英国から米国へ転送される場合、そのデータがアイスランド、グリーンランドおよびカナダに張り巡らされたネットワークを経由したとしても、法律の観点からは問題ないと思われる。

[9] 個人データ処理に係る個人の保護に関する指令 95/46 の実施状況については、次の URL で確認することができる＜http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm#italy＞。

は、条約に署名したか、国内法を制定して実現可能としている。

1.10. データ保護指令を適切に適用するには、データの可用性と完全性が鍵となり、これらはデータセキュリティ対策の議論を先導する。ここには不可避的な交換条件が存在する。データのセキュリティを強化することによって、その可用性が低下する傾向にある。したがって、クラウドプロバイダの顧客は、クラウドプロバイダが備えているセキュリティ対策や保証されているデータの可用性を細部まで吟味したいと思うであろう。多くの欧州諸国には、データのセキュリティに関する必須の要件が存在することに留意しなければならない。クラウドプロバイダの顧客は、それらのセキュリティ対策が確実に実施されていることを確認しなければならない。場合にもよるが（eヘルスや、可能性としては、機密性の高いデータや財政関連のデータが処理される場合の障害耐性(resilience)のシナリオ等）、データの格納、データの通信や転送、データの災害からの復旧時や前方への転送時に、より厳しいデータセキュリティ対策が実施されることを顧客が求めることもある。

1.11. 単一のデータ管理者として分類された顧客（クラウド利用者）が、データ主体との関連で個人データの処理に責任を負う組織となることを、この時点で明らかにしなければならない。この顧客は、このデータが、外部処理者としての役割においてクラウドプロバイダによって処理される場合にも、データに対する責任を負うことになる。このデータ保護指令を遵守できない場合、国によって異なるが、データ管理者が行政上、民事上、刑事上の処分を受ける可能性がある。このような処分は、EU 加盟諸国で施行されているデータ保護指令 95/46/EC のベースとなる関連規定として詳しく記述されている。

問題点の処理

1.12. 前項で論じた問題点は、すべて契約との関連で扱うことができる。データ保護指令のセクション 7 および 10 に適合する方法で個人データが収集されていることを保証する傍ら（すなわち、データ主体に、事前に正式に通知し、同意を得る（セクション 7 で要求されれば））、クラウド利用者は、クラウドプロバイダとの間で交わされた契約におけるデータ保護に関する条項の存在を探すべきである。この条項には、関係者の役割や義務も記載すべきである。クラウド利用者は、このような条項を評価する際に、以下の項目を考慮すべきである：

a）クラウド利用者は、EU データ保護指令の規定においてはデータ管理者として分類されており、また公平性、合法性、（データの）最終的状態等に法的責任を有しており、データ保護指令の規定を顧客が遵守できるように支援する条項を追求すべきであることを念頭に置くべきである。

b）クラウドプロバイダは、データ保護指令のセクション 12 に基づき、データ主体の権利を効果的に保証できるように、データ管理者と協力すべきである。

c）クラウドプロバイダは、データ保護指令のセクション 17 に規定する適切なセキュリティ対策を機能させると共に、データセキュリティ関連の違反を直ちにデータ管理者に通知し、その問題が速やかに解決されるよう協力すべきである。

d）データ保護指令のセクション 25(2)項で謳われている、適切なレベルの保護が保証されない第三国への個人データの転送の可能性は、提案される転送について、データ主体から事前に明確な同意を得るか、セクション 26 の規定に従って他の方策により実施されるものとする（例、標準的な契約条項または、セーフハーバーの原則、データが米国に転送される場合およびクラウドプロバイダが当該プログラムに参加している場合）。クラウドコンピューティングは、データ転送から構成されることも念頭に置くべきである。この問題を契約上扱うのは困難であろう。したがって、本文書では、この問題を欧州委員会が扱うよう提言する。

1.13. ケース A の場合（「導入」セクションの 4 番目の段落を参照）、大規模なクラウドプロバイダと複数の小規模顧客とが契約条項を交渉することが不可能であるため、データ保護条項を含む契約は、クラウドプロバイダによって起草される点に注意していただきたい。したがって、潜在的な顧客は、クラウドプロバイダによる合法的なデータ処理についての十分な保証、および契約上の損害に対する十分な補償が提供されるか否かを判断するために、その条項を慎重に分析すべきである。

1.14. ケース B および C の場合（「導入」セクションの 4 番目の段落を参照）、データ保護の条項は、交渉の対象になる。それに加えて、付録や SLA において、セキュリティ対策が扱われることもある。セキュリティ関連の問題を扱う場合、関係者は、扱うべきすべてのセキュリティ対策を詳述することができない場合もあることに留意すべきである。これは、IT セキュリティが新たな問題を扱う終わりのない競争であるためで、契約書の条項もそれに合わせて自在に策定する必要がある。

1.15. ケース B および C の場合（交渉する可能性がある高い価値の契約）、データ保護関連条項に違反があった場合、契約上の損害に対する適切な賠償について交渉することも、顧客には推奨される。最後に、クラウドプロバイダ側の違反が著しい場合、この違反が、一方的に契約を解消できる事例のリストに含まれる可能性がある。

1.16. クラウドプロバイダが欧州経済圏外の国に所在しており、その国において適切なレベルのデータ保護が提供されない場合は、データ主体の同意を得てデータを転送するよりも、データ保護指令のセクション 26（例、標準的な契約条項またはセーフハーバーの原則、データが米国に転送される場合およびクラウドプロバイダが当該プログラムに参加している場合）に基づく手続きを実施する方が推奨される（サブセクション 1.7 で指摘した通りの理由で）。ただし、加盟国の領土内におけるデータ転送も問題なしでは実施し得ない点を強調しなければならない。事実、個人データが、加盟国内を自在に流通することができるにもかかわらず、法律は各国共通ではない。法律が共通でないという問題は、遵守および責任問題において、明らかな困難を生み出す可能性がある。したがって、本文書では、欧州委員会に対して、欧州における必要最低限のデータ保護要件の標準化に向けた措置を講じるよう提言する。これは、データ保護指令が現在、改訂中であるという事実からも特に重要である。また、加盟国に共通の必要最低限のデータ保護規格をベースにしたデータ保護認証スキームも、非常に有用性が高い。

2. 機密性

問題点の定義

2.1. 機密性の問題は、本書で考察しているシナリオでも取り沙汰されている。事実、秘密情報や「ノウハウ」が、クラウド内で処理される可能性がある。クラウドプロバイダやクラウドのセキュリティ違反による任意の通信が原因で発生した情報の流出が、顧客のビジネスやサービスを危険に曝すこともある。ここで（データを）処理するには、通常、暗号化されていない形式のデータが必要であるため、演算的な操作を施すデータと、改ざんされないような方法で格納・転送されるデータをはっきりと区別することが重要である。

2.2. ノウハウの概念とそれを保護することができる方法を十分に考慮することが有効である。

ノウハウとは、秘密であり、実質的で、任意の形式で識別される情報の本体、と定義されている[10]。「秘密」とは、ボディとしてのノウハウパッケージ、または、その要素の正確な構築または組み立てが、一般的には知られていない、または容易にアクセスできないことを意味している。「識別されている」とは、機密性および実在性の基準を満たすことを検証できる方法で、ノウハウが説明または記録されていることを意味する。これらの目的において、「実質的な」は、ノウハウが、以下の全部または一部分について重要である情報を含んでいることを意味する：

I 製造プロセス、または、

ii 製品またはサービス、または、

iii 製品またはサービスの開発に関連する情報で、重要ではない情報は除外される。

2.3. このようなシナリオに適用できる欧州の規定は見当たらない。上記の定義のようなノウハウに関する欧州の規定では、情報の転送や利用に関するライセンシングおよび活動に主に適用される。

問題点の処理

2.4. 規定を念頭に置き、研究結果や顧客とプロジェクトに関する情報を含んだ、ノウハウや秘密情報の経済価値を保全するために、本文書では、この点を含む契約条件をクラウド利用者が求めることを推奨する。事実、このような価値を保全するための関係者の役割や責任は、「機密性および守秘義務」関連の条項で特別に扱うべきである。関係者の責務や関連責任の範囲にも、特別な注意を払うべきである。技術関連の付属書は、この問題を扱うのに特に適していると言えよう。

2.5. ケース A の場合、クラウドプロバイダの潜在的な顧客は、クラウドプロバイダが、クラウド内を巡回する顧客の秘密情報やノウハウを保護するために十分な保証を提供するか否かを判断するために、「機密性／守秘義務」関連の条項を慎重に分析すべきである。

[10] 2004 年 4 月 27 日付けで公布された欧州委員会規約(EC)、No. 772/2004 の第 81 条(3)項、『The Treaty to categories of technology transfer agreements』を参照。

2.6. ケースBおよびCの場合、本文書では、機密情報または秘密情報が（一方の当事者によって）開示された場合に他方が被る可能性のある損害を反映する規定を両者が交渉するよう提言する。開示が重大な被害につながる場合、この違反が、被害を被った組織が保有する、一方的に契約を解消できる事例のリストに含まれる可能性がある。

3. 知的財産

問題点の定義

3.1. クラウドコンピューティングシナリオにおいては、知的財産もリスクに晒される可能性がある。

3.2. クラウドプロバイダにサービスを外部委託する組織が、関連法によって知的財産権を保護し、これを行使することができても、全欧州加盟国と同様に、知的財産権の違反は、法的な手続きを踏んだとしても完全に回復されることはない直接的被害をもたらす可能性がある。

3.3. その上、起こりそうにないケースではあるが、クラウドプロバイダと利用者間の対話において、たとえば、BまたはCの場合に可能な交渉フェーズにおいて、知的財産権が発生するような共同結果が生み出される可能性がある（たとえば、データをより適切に扱う技術）。したがって、クラウドコンピューティング関連の活動に従事する前に、誰がこれらの権利を所有するかを決定し、更にこのような権利を有するオブジェクトを両者がどのように活用するかについて決定することが賢明である。

問題点の処理

3.4. 知的財産権は、専用の契約条項、すなわち「知的財産に関連の条項」および「機密性および守秘義務関連の条項」[11]によって規制されるべきである。

3.5. ケースAの場合、クラウドプロバイダの潜在的な顧客は、自身の知的財産の価値とクラウドコンピューティングサービスに関連したリスクを慎重に評価すべきである。評価が終了したならば、顧客は、知的財産を管理する条項を慎重に確認して、クラウドプロバイダが十分な保証を提供し、顧客の情報や資産を保護するための適切なツール（例、データの暗号化等）を提供しているか否かを判断すべきである。クラウド利用者は、提供されるサービスの品質が低下することなく、契約によって知的財産に関する彼らの権利が最大限に配慮されることを確認するべきである（例、バックアップの作成は、適切なサービスレベルを提供する上で必要な要素となり得る）。

3.6. ケースBおよびCの場合、「知的財産に関連の条項」は、上述のパラグラフ3.3.で説明している問題点を扱うための明確なルールを規定するのに十分な詳述さであるべきである。また、クラウド利用者は、知的財産を管理する規定に違反したクラウドプロバイダを罰すべきという条項についての交渉を行うことが望ましい。クラウドプロバイダによる重大な違反は、被害を被った組織が保有する、一方的に契約を解消できる事例のリストに含まれる可能性がある。

[11] 「機密性および守秘義務関連の条項」には、前述の段落2.4.が該当する。

4. 業務上の過失

問題点の定義

4.1. クラウドプロバイダに外部委託したサービスにおける不具合は、顧客（クラウド利用者）が自身の顧客に対する役割と義務を果たす能力に、重大な影響を及ぼすことがある。したがって、クラウドプロバイダの顧客は、プロバイダの過失をベースとした契約上または複雑な責任に晒される可能性がある。

4.2. クラウドプロバイダによる過失は、顧客側の従業員に対する顧客の責任問題にもつながる可能性がある。顧客は、電子メール、メッセージング、デスクトップ、プロジェクト管理、給与サービス等の重要な内部機能を提供する、またはサポートする技術を、クラウドプロバイダに外部委託しているため、クラウドプロバイダによる過失が発覚した場合や、顧客の従業員がこれらの機能、または、これらの機能によって処理されたデータにアクセスできなくなった場合の責任が、顧客に及ぶことになる。

4.3. これと関連した問題で、顧客のクレデンシャルによって認証されてはいるが、実際にはその顧客ではない人物がそのアカウントを使用する非合法活動について、その契約条項に顧客の責任を盛り込むことができるか否かという問題がある。

問題点の処理

4.4. ケース A の場合、顧客は、クラウドプロバイダとって有利に設定されている、責任に関する（標準的な）制限および免責条項を慎重にレビューして、それらが受け入れられるものであるか否かを判断すべきである。

4.5. ケース B および C の場合（すなわち、非常に高い価値の契約が交渉される稀なケースの場合）、本文書では、顧客が上述の問題に関する自己責任を、可能な限りクラウドプロバイダにシフトするよう提言する（ただし、責任をシフトすることによって、高額な費用が発生しない場合）。これは、「責任の制限」および「免責」関連の条項で扱われるであろう。クラウドプロバイダによる重大な違反は、被害を被った組織が保有する、一方的に契約を解消できる事例のリストに含まれる可能性がある。ただし、データ保護指令(1)(1)項により、データ主体にもたらされる損害に対する法的な責任は、如何なる契約条項とも独立して、常にデータ管理者に課せられるという点に留意すべきである。

4.6. 本文書は、電子商取引指令の中間責任の免責条項がクラウドプロバイダにどのように適用されるかについての法的説明が、欧州共同体に対して行われることを推奨している。

5. 外部委託サービスおよび管理の変更

問題点の定義

5.1. 企業とクラウドプロバイダとの間で交わされた契約は、個別事情を重視する契約として定義されることが多い。個別事情を重視する契約とは、関係者が、その組織にとって独特な品質に基づき、契約を選択することである。たとえば、顧客は、掲示されている条件、その評判や専門性、その技術スキルの高さ等で、特定のクラウドプロバイダを選択することができる。その結果、顧客は、クラウドプロバイダが、顧客に対して提供しているサービスの全部または一部を外部委託する現場を確認する気にならないであろう。

5.2. クラウドプロバイダの管理も変更される場合があり、その結果、このクラウドプロバイダによって提供されている諸条件も変更されることがある。

問題点の処理

5.3. ケース A の場合、本文書は、クラウドプロバイダがサービスを外部委託するか否か、および、クラウドプロバイダが外部委託するサービスのパフォーマンスに関連する担保や保証を発行するか否かを、顧客が判断するよう提言する。ただし、クラウドプロバイダによるサービスの外部委託を制限できることを、顧客が期待するよう提言しているわけではない。また、管理に変更があった場合に、クラウドプロバイダがどのような方法で顧客に通知するかを判断するために、契約を再確認することを提言する。顧客は、管理に変更があった場合、契約を解消する権利が契約条項中に含まれているかも考慮できるであろう。

5.4. ケース B および C の場合、顧客は、選択肢の一つとして、クラウドプロバイダがサービスを外部委託する際には、顧客の事前承認を得るよう要求することもできる。そのためには、顧客は、クラウドプロバイダが外部委託しようとしているサービスの種類や、サービスを外部委託する組織の身元に関して通知される必要がある。顧客が外部委託に同意した場合でも、顧客がプロバイダに対して、外部委託するサービスについて担保や保証を発行するよう望む可能性がある。これと同じような理由で、顧客は、管理の変更を承認する機会が与えられ、クラウドプロバイダの管理に変更があった場合には、契約を解消または再交渉することができることを希望するかもしれない。このような選択肢は、企業とクラウドプロバイダの間で交わされる契約条項のうち、「第三者へのアウトソーシング」、「保証と補償」、「管理の変更」または「契約の解消」等の条項で、慎重かつ詳述に記載することができる。繰り返しになるが、これは、関係者の交渉力によって決定される。

結論

セクション 1～3 までのすべての契約条項は、関連する罰則規定を除き、関係者の交渉力次第であるが、標準化に適している。一方、セクション 4 および 5 の契約条項の中身も、関係者の交渉力によるところが大きいが、標準化に適しているとは言えない。

付録 II ー 中小企業におけるユースケースシナリオ

クラウドコンピューティングに関する中小企業の視点

ENISA によるクラウドコンピューティングのセキュリティリスクアセスメント

このシナリオは、本文書で公開されているリスク分析のベースとして使用されたものである。

制約と前提条件

このシナリオの一部は、「クラウドコンピューティングに関する中小企業の視点」の調査結果をベースとしている[REF]。このシナリオは、クラウドコンピューティング関連のプロジェクトや投資を検討、計画または実施している企業のためのロードマップを意味するものでは**ない**。

使用例として中規模企業を選択したのは、充分なレベルの IT、法律およびビジネスの複雑性を、リスクアセスメントにおいて保証するためである。その目的は、考えられる（クラウドコンピューティングにおける）すべての情報セキュリティリスクを露呈させることにある。それらのリスクの一部は、中規模ビジネスに特化したものもあり、その他のリスクは、クラウドコンピューティング環境に移行する際、すべての零細企業、小規模企業および中規模企業が直面する可能性のある一般的なリスクである。

このシナリオは、単一組織の現実を完全に再現することを目的としているものではないが、シナリオに含まれているすべての要素は、多くの組織で頻繁に起こり得るものである。目下のところ、シナリオで解説したような幅広いサービスを提供する単一プロバイダは存在しないが、すべてのサービスは、複数のプロバイダによって網羅されるであろう。

各層（IaaS、PaaS、SaaS）に対するアプリケーションの割当は任意であり、説明のためのもので、提言するものでは**ない**。

シナリオ

CleanFuture 社は、太陽電池関連ビジネスを行っている。この会社は、太陽光発電システム、ソーラーシステムや暖房装置用の主要構成品を製造、販売している。この会社は、製品の主要生産拠点であるドイツに 1999 年に創設された。以来、CleanFuture 社は、年平均 20%増の収益を誇る企業として急成長を続けている。

2003 年に、スペインに支社が開設され、2004 年にはイタリアにも新たな支局が開設された。2005 年には、太陽光反射防止用ガラスの製造ラインをポーランドへ移設することが決定し、2006 年 6 月までに、その工場での最初の製品が製造されている。現在、同社は、米国市場への進出を計画中である。

CleanFuture 社には 93 名の従業員がいる：

- ドイツに 50 名（本社（工場、研究所および支社を含むの 2 拠点））
- ポーランドに 34 名

- スペインに 5 名
- イタリアに 4 名。

また、この会社には不定数の契約職員がいる（10～30 名の暫定職員、営業、コンサルタント、トレーニー等）。

2008～2009 年にかけての競争圧力や、経済・財政情勢の危機等により、CleanFuture 社は、コスト削減および生産性向上のための短期見通し戦略の内部協議を開始した。IT サービスは、大きな向上が期待できる重要な分野として認識された。

IT およびセキュリティの要件が内部的に分析され、以下のような結果が導き出された。

1. IT サービスの様々な要求に対応するためには、更なる自在性や拡張性が必要である（年間を通じた職員数の変化、取り引きするパートナーやサプライヤ数の変化、市場展望の突然の変化、研究機関や大学との提携の可能性、支社／支局の新設、または、営業規模拡大の可能性等）。
2. 高品質の IT サービス（有効性やパフォーマンスという観点）、および、高レベルの情報セキュリティ（可用性、完全性および機密性という観点）が、その会社によって求められている。ただし、そのような高レベルのサービスで内部リソース（IT 部門）を提供するには、特別な専門知識に加えて、ハードウェア、ソフトウェア、IT 関連サポートおよび情報セキュリティに対する資本投資が必要である。
3. 事業継続性や災害復旧能力も向上させる必要がある。
4. ビジネスを支援するための新たなアプリケーションを評価するためのテストベッドや、新たなソリューションやプロジェクトの開発に向けて、開発者がパートナーと共に作業できる協力環境が、ビジネスの有効性や革新に向けた能力の向上という観点から特に重要である。
5. 物理的なシステムから仮想システムへの移行（P2V）プロジェクトは、最終成果の信頼性および有効性に関して、重要なフィードバックをもたらすであろう。

新たな IT 手法により影響を受け得るサービスやアプリケーションとして特定されたものには､以下のようなものがある：

- 電子メールやメッセージング
- デスクトップ（オフィスアプリケーション）
- プロジェクト管理
- 給与計算
- CRM および売上管理
- 経理および財務

－ カスタムアプリケーションの実行、ホスティングおよび開発

－ ID 管理。

外部コンサルタントの協力を得て、組織内部の作業グループは、CleanFuture 社のニーズを満たすためのソリューションとして、クラウドコンピューティング技術を提案した。

次のステップとして、クラウドコンピューティングにおける実現可能性の研究がなされた。会社の役員会に報告書「CleanFuture － クラウドコンピューティングにおける実現可能性の研究：可能性のある実現戦略と関連ビジネス、法律およびセキュリティの懸念」が提出された。

アドホックな作業グループの分析に基づき、この報告書では、特定された IT サービスやアプリケーションを少なくとも三つのクラウドプロバイダに外部委託することが提案された。長期的には、この三つのクラウドプロバイダが、「クラウド連携」を構成することになるが、当面の間は、便宜上、「ID 管理連携（FIM:Federated Identity Management）」ソリューションを通じて三つの独立したプロバイダを使用するのが望ましい。

1. クラウドプロバイダ#1 は、電子メール、メッセージング、デスクトップ環境、プロジェクト管理および給与計算（すなわち、クラウドコンピューティングの SaaS モデル）等のクラウドベースのホスティングサービスを提供する。契約上、データは、アジア、欧州および米国を含む世界各地に設置し、処理することができる。

2. クラウドプロバイダ#2 は、クラウドコンピューティングの PaaS モデルと定義される、カスタムアプリケーションをホスティングするためのクラウドベースのプラットフォームを提供する。このカスタムアプリケーションは、顧客による、太陽電池システムのインストール時の設定、エネルギー生産量（立地条件に依存）および ROI（インストールがなされる国のインセンティブに依存）の計算を支援する「シミュレータ」で構成される。

3. クラウドプロバイダ#3 は、人材、経理と財務、CRM と営業管理およびカスタムアプリケーションの開発（すなわち、クラウドコンピューティングの IaaS モデル）のためのクラウドベースのインフラストラクチャを提供する。短期計画（二年間）では、CleanFuture 社は、PaaS および IaaS プロバイダに外部委託したデータやサービスの事業継続性および災害復旧を取り扱う。これは既存のインフラストラクチャを使用して行われる。SaaS プロバイダは、彼らが提供するサービスのバックアップおよび事業継続性要件に責任を負う。いずれの場合も、二年間は、プロバイダと CleanFuture 社双方によりバックアップサービスが提供される。

中期的な災害復旧計画は、これから定義されるものである。ここでは、以下の二つのオプションを比較する：

I. 小規模のプライベートクラウドを構築し、そのインフラストラクチャの機能やコストを共有するビジネスパートナーを特定する；

II. それぞれのクラウドプロバイダから、事業継続性と災害復旧サービスを購入する。

現在の IT インフラストラクチャが陳腐化すると予想される二年以内に、決定が下されることが予想される。それまでの間、CleanFuture 社は、事業継続性と災害復旧のニーズを満たすために、自社の技術とオンサイトホスティングを利用することになる。

ID 管理

本報告書では、ID 管理が、クラウドサービスへ移行する際のすべての要素に影響を与えるものであると認識している。信頼性や拡張性の理由により、CleanFuture 社は、長期的には、ユーザ認証やアカウント管理を、内部規則に依存するべきでは**ない**。拡張性と回復力を備えた、将来が保証されたソリューションでは、以下のような要素が提供されなければならない：

a. シングルサインオン；

b. シングルサインオフ；

c. 全サービス用のシングル ID ディレクトリ；

d. ID の提供および取り消し用の単一アプリケーション；

e. 認証および署名に使用する暗号鍵の安全な管理；

f. アクセス制御ポリシーの実施（例、XACML の使用等）。すべてのユーザ（職員、パートナー、契約社員）が、会社のセキュリティベースライン要件を遵守することを保証するためのソリューション。これらの要件は、ユーザのプロフィールや承認内容に応じて設定される。必要最低限の要件とは：ウイルス対策ソフトウェアおよび OS の更新である。

本報告書では、異なるソリューションプロバイダで必要な様々なアカウントを、ID の提供と管理サービスから分離する、ID 管理連携（FIM）ソリューションへの移行を提言している。簡単な調査でも、既存のクラウドソリューションのいくつかによって、完全な FIM ソリューションで要求されるインターフェースが提供されることが確認されている。これにより、以下の通り、移行に関する重要な要件が導き出される：

1. 選択されたサービスは、選択された FIM のフレームワークを通じた認証をサポートしなければならない（Liberty/Cardspace + SAML 2.0 を利用した実装）。

2. クラウドにサービスやアプリケーションを移行する前に、CleanFuture 社は、外部パートナーの認証も含めた、すべてのアプリケーションに対するシングルサインオンソリューションを実施すべきである。

3. 鍵管理インフラストラクチャの信頼特性は、慎重に検証すべきである。

4. セキュリティクライアントのヘルスベースラインは、すべてのサービスにアクセスするすべてのクライアントについて定義すべきである。

プロジェクト	フェーズ 1ー2008	フェーズ 2ー2009	フェーズ 3ー2010	フェーズ 4ー2011	フェーズ 5ー2012
物理的なシステムから仮想システムへの移行（P2V）	社内で仮想化プラットフォームを採用し、以下のアプリケーションの物理的なシステムから仮想システムへの移行（P2V）を実施する：CRM、営業管理、カスタムアプリケーション、人材。	フェーズ1のソリューションの信頼性およびパフォーマンスの確認。 財務と経理アプリケーションの P2V 移行。 FIM および鍵管理ソリューションの選択。	フェーズ2のソリューションの信頼性およびパフォーマンスの確認。 FIM SSO ソリューションおよび鍵管理ソリューションへの移行。		
クラウドコンピューティングへの移行プロバイダ#1ーSaaS			クラウドプロバイダ（SaaS）の選択およびプロジェクト管理*アプリケーションの移行。	以下のアプリケーションおよびサービスの移行：電子メール*、メッセージング*、デスクトップ*、給与計算*。	
クラウドコンピューティングへの移行プロバイダ#2ーPaaS	---		クラウドプロバイダ（PaaS）の選択および CRM および営業管理アプリケーションの移行。	PaaS プロバイダの信頼性およびパフォーマンスの検証。カスタムアプリケーション、経理および財務、人材アプリケーションの移行。	PaaS プロバイダの信頼性およびパフォーマンスの検証。 カスタムアプリケーションの開発の移行。
DR および BC パートナーのためのプライベートクラウドの開発			パートナーの識別、プロジェクト要件の定義等。	管理計画の定義等。	プライベートクラウドの稼動。

* これらのアプリケーションまたはサービスは、社内の物理的なシステムから仮想システムへの移行を行わずに、クラウドコンピューティングプロバイダに外部委託されたものであることに留意すること。

既存のセキュリティ管理策

プロバイダ#1（SaaS）およびプロバイダ#2（PaaS）は、以下の項目を含んだ標準セキュリティ管理策の実施を主張している：

- ファイアウォール;

- IDS/IPS（ネットワークベースおよびホストベース）;
- システムの強化および社内における侵入テスト;
- ITIL 準拠のインシデントおよびパッチ管理。

詳しい説明は提供されていない。プロバイダの選択は、プロバイダ#1 およびプロバイダ#2 の評判を基に、CleanFuture 社により行われた。

プロバイダ#3（IaaS）は、様々な標準設定をもとに事前に設定された仮想マシンのインスタンスを提供している。ただし、これらプロバイダは、デフォルトで事前に強化されたインスタンスは提供していない。つまり、すべてのデフォルト設定の見直しを含め、仮想マシンのインスタンスに係るすべてのセキュリティ対策は、顧客が全責任を負うことになる。

プロバイダ#3 では、全職員に対する身元確認（各地域の法律による制約あり）や、生体認証を利用したスマートカードをベースとした物理的なアクセス制御、知る必要に基づいたデータアクセス制御ポリシーを規定している。

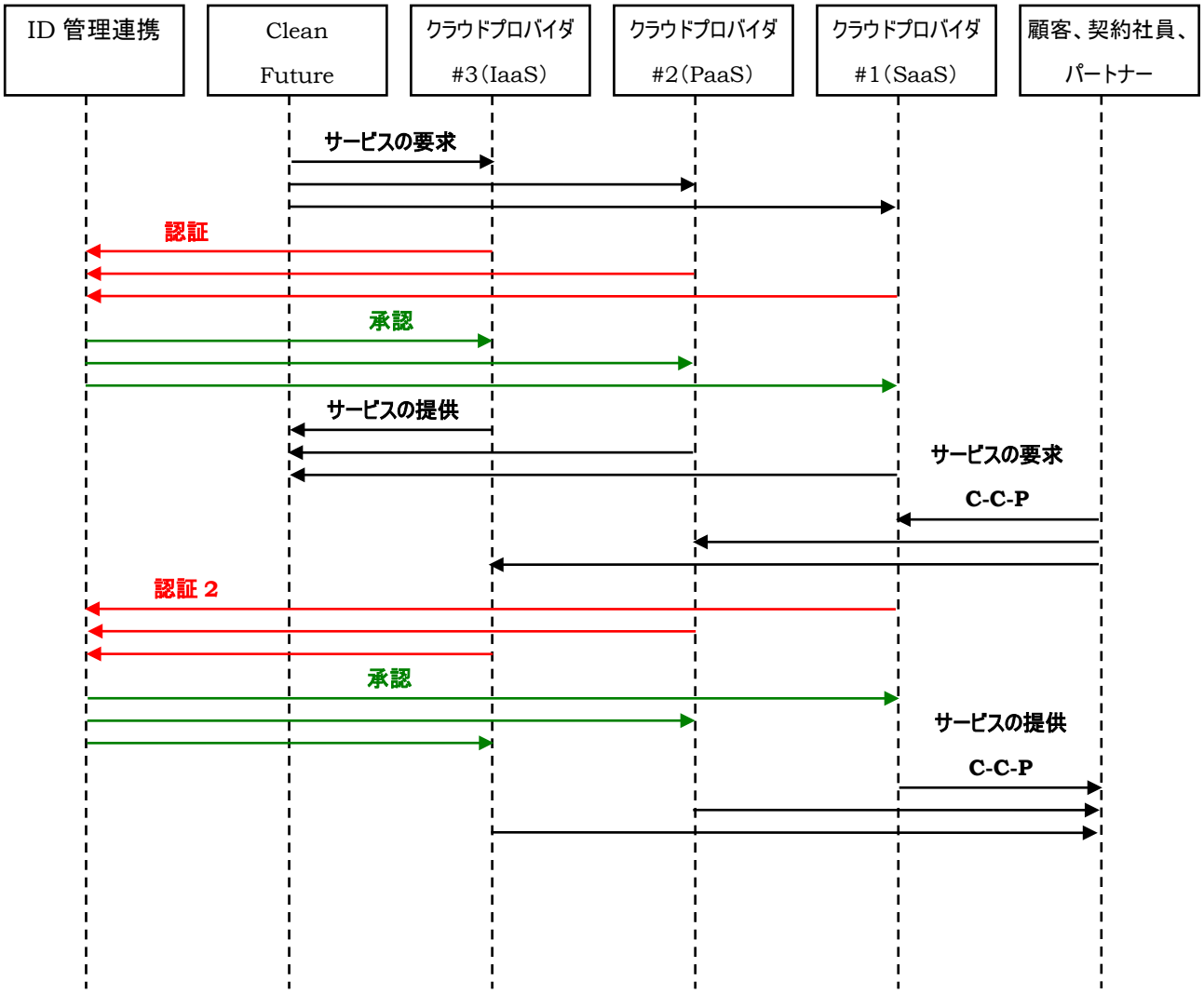
顧客（例、設定アプリケーションを利用）との間を除くすべての接続（IaaS、PaaS、SaaS、IDM 用等）は、暗号化される（VPN または SSH のいずれかを使用）。

すべてのプロバイダが ISO 27001 に適合しているが、いずれのプロバイダも認証の正確な範囲は明らかにしていない。

各プロバイダと締結した SLA には、違反に関する通知条項が盛り込まれている。すべてのプロバイダは、割増料金（支払い済み）のセキュリティ報告機能を提供している。そのような支払い済みの報告には：（顧客の資産に対する）違反未遂、標的型攻撃（企業ユーザ毎、特定のアプリケーション毎、特定の物理マシン毎、外部攻撃に対する内部攻撃の割合、等）、傾向や統計情報、等が含まれる可能性がある。

試みの失敗やインシデントの重大性のスケールに関連した報告の閾値は、顧客のニーズに基づきカスタマイズされる。

データの流れ



付録 III － その他のユースケースシナリオ

以下は、本文書のリスク分析で使用した障害耐性（resilience）および e ヘルスのシナリオを簡潔にまとめたものである。

障害耐性（resilience）のシナリオ

このシナリオでは、以下のようなリスクに直面した際に、クラウドコンピューティングを利用することにより、サービスの障害耐性（resilience）にどのような影響がもたらされるかを探求している：

- 顧客によるリクエストの急増（例、経営危機に直面している期間等）；
- サービス運用妨害攻撃；
- 地域的な自然災害；
- 攻撃用プラットフォームとしてのインフラストラクチャの悪用；
- データ漏えい（悪質または不注意な内部者、もしくはプロセスの破壊）。

2012 年、XK-Ord 社は、購入用ポータルに組み込むことができるウィジェット（Widgets）形式のコンテンツ配布ソリューションと共に、Web サービスインターフェースによるリアルタイムの電子商取引を提供している。

一般的な使用例は以下の通りである：

- 購入用ポータルにおける、商品の価格データや図表のリアルタイム表示；
- 価格の予測および分析に使用する過去のデータ；
- 企業のための受注履歴や在庫管理報告；
- リアルタイムによる外国為替換算および FX 履歴；
- 最新の SOX および EU の独占禁止法に基づく取引報告；
- 更に複雑なアプリケーションで使用する財務データ。

それに加えて、XK-Ord 社は、様々なサービスを管理し、それらをカスタムアプリケーションと組み合わせて使用するための、プラットフォームを提供している。それらのサービス提供を前提として、XK-Ord 社は、以下の項目に対する高い障害耐性（resilience）を要求している：

- 待ち時間 － データ提供の遅延は、価値のある取引を喪失させる可能性がある；
- リクエストの達成 － 例、高い信頼：
  * データベースへのクエリーと結果の表示；
  * Web サーバによる http リクエストへの応答；
  * TCP/IP インフラストラクチャ；
- データの完全性 － データ内のエラーは財政的な喪失を招く可能性がある；
- 機密性と報告 － データには金銭的な価値がある － それ故、支払っていない顧客に開示された場合、XK-Ord 社の金銭上の喪失となる；
- アプリケーションの完全性と脆弱性。

インフラストラクチャ

2011 年に、XK-Ord 社は、コスト、自在性および信頼性の理由により、クラウドインフラストラクチャへ移行した。XK-Ord 社では、コンテンツ配布用の IaaS を提供するクラウドプロバイダ、CumuloNimbus Systems 社を使用している。

- データは、DaaS モデル（サービスとしてのデータベース）を使用して格納されている。
- CRM および請求書発行を含む XK-Ord 社の顧客アカウントの管理は、第二のクラウドプロバイダである Stratocumulus 社によって管理されている。クレデンシャルは、このサービスを使用して XK-Ord 社より発行、検証されており、コンテンツへのアクセス制御は、CumuloNimbus 社のリソースから提供されている。すなわち、Stratocumulus 社は、シングルサインオンを提供する連携 ID プロバイダとして機能している。
- XK-Ord 社の人材管理、給与計算、オフィスデスクトップ用アプリケーションおよび研究開発システムは、XK-Ord 社の敷地内で、XK-Ord 社によって直接管理されている。

ネットワーク

データセンターを使用する場合と比べ、クラウドプロバイダのインフラストラクチャは、総合的な帯域幅、処理能力、メモリおよび格納領域はもとより、即座に上限を測定する能力にもかなりの向上をもたらしている。たとえば、コンテンツ配布地の近くに設置されているルータでは、スケーラブルな仮想メモリ、ログ記録およびパケットフィルタリング用リソースを使用している。IPSec は、ネットワークの一部として実装されている。これらの機能により、DDoS 攻撃に対する障害耐性が著しく向上している。

リソースの管理

- コンテンツの提供は、XK-Ord 社に対して HTTP リクエストベースで課金される。費用は、CumuloNimbus 社が提供するポリシーからの選択に基づいて、その上限が決定される。XK-Ord 社の顧客は、個別の方式による各サービスへの HTTP リクエスト数に応じて課金される。
- プロバイダは、インフラストラクチャ全体を通じて、他のクライアント（必ずしも似ているとは限らない）との共用テナント型リソースを運営している。つまり、異なる顧客によって使用されるリソースの隔離が強力になされていることを意味している。XK-Ord 社は、少額を払うことによって事前にリソースを予約できるオプションを提供しており、それにより、サービスプロバイダおよび XK-Ord 社の全体的な信頼性を向上させている。
- クラウド以外の一般的なインフラストラクチャよりも、利用できるリソース内での利用量は短期間に速いスピードで増加する。そこで更にリソースを追加する（すなわち、クラウドプロバイダ側でのハードウェアの増設は遅い）。特に、DDoS に対する防御は、迅速に増減できるようすると同時に、それに伴うコストやリソースの使用も詳細に定義しなければならない。
- クラウド間の移行をスムーズにするために、標準的な SLA と API が使用される。

セキュリティサービス

XK-Ord 社では、リアルタイムによるセキュリティ監視（RTM）、脆弱性のアセスメントおよびデバイスの管理に、セキュリティサービスプロバイダである BorealisSec 社を利用している。

- BorealisSec 社のスタッフは、VPN 接続を使用し、CumuloNimbus 社のインフラストラクチャ上にホストされている XK のシステムを管理している。
- ログは、CumuloNibus 社のインフラストラクチャ上で収集され、分析のため、VPN を経由して BorealisSec 社の SIEM（セキュリティ情報およびイベント管理）用のプラットフォームへ自動的に転送される。

インシデントが確認された場合には、以下のいずれかの方法が取られるべきである：

* BorealisSec 社の管理者が、直接、インシデントを扱う（自動または手動）、または、
* 問題を解決するために、CumuloNimbus 社のスタッフを割り当てる。

いずれの場合も、インシデントの重大さに基づき、XK-Ord 社と合意した契約に則ってインシデントに対応することとなる。その他、以下の点にも注意する必要がある：

- CumuloNimbus 社の利用規約（ToU）では、プロアクティブなセキュリティテストが禁じられているため、試験環境でのみ脆弱性アセスメントを行うことができる。
- BorealisSec 社は、CumuloNimbus 社の利用規約内で可能な限り、遵守および監査の報告を提供する。
- BorealisSec 社は、クラウドプロバイダの権限外のソフトウェアにパッチを適用する責任を有している。

SLA：XK-Fin -> 顧客

XK-Ord 社は、サービスレベルアグリーメント（SLA）を提供している他の金融データ会社と競争するために、顧客に対して SLA を提供している。XK-Ord 社の SLA は、二社間の依存関係にもかかわらず、CumuloNimbus 社よりも高いレベルの信頼性を提供する可能性がある点に留意する必要がある。これは、XK-Ord 社が、より高いレベルのリスクを容認しようとしているからかもしれない。

ゴール	KPI	値	違約金
サービスの可用性	動作可能時間（%）／月	99.99	10 単位毎に請求額から 20%減額。
待ち時間（注：株式市場でデータが公開されてからの時間を示す）	1 日 100 リクエスト当たりの平均対応時間	1 秒	違反 1 回につき請求額から 5%減額。
管理	リクエストに応答するまでの時間（分）	60 分	違反 1 回につき請求額から 5%減額。
警告	サービスへの違反を顧客に警告するのに要する時間（これは含まれない）	5 分	違反 1 回につき請求額から 5%減額。
不具合からの回復時間	時間	2 時間	違反 1 回につき請求額から 5%減額。

e ヘルスのシナリオ

このシナリオでは、厳格な法的要求事項を遵守する必要があり、国民の否定的な認識に非常に過敏な、大規模政府機関等によるクラウドコンピューティングの利用を探求するものである。この場合、クラウドコンピューティングを利用する際の主な検討事項は、セキュリティやプライバシー関連の問題があまり考慮されていないという国民の認識であろう。これは、「パブリック」クラウドサービスを利用する場合には、特に当てはまる。

EuropeanHealth は、欧州を代表する大規模な政府ヘルスサービスであるが、（それぞれの）*国が提供するヘルスサービスを詳しく説明している訳ではない*。EuropeanHealth は、e ヘルスサービスを提供する公共機関および民間サプライヤで構成されている。EuropeanHealth は、複数の地域に跨る非常に大規模な機関で、約 6 千万人に e ヘルスサービスを提供している。クラウドインフラストラクチャを使用する前は、20 以上の IT サービスプロバイダと 50 か所以上のデータセンターから構成されていた。

具体的なシナリオ

この具体的シナリオでは、持病がある在宅患者の看護と監視を提供する e ヘルスプラットフォームが含まれている。以下に、その一般的なプロセスを詳しく説明する：

1. 監視センターは、在宅の高齢患者を監視し、連絡を取り合うために、家庭用センサを配備する独立したインターネットベースのプラットフォームを使用している。
2. 監視された数値は、患者の基礎データに基づき、異常の有無が分析される。更に特別なサービス（医者、看護師等）が必要か否かは、監視センターで判断される。
3. 患者自身も、外部の e ヘルスサービスプロバイダに対し、自身の情報を提供するかしないかを選択することができる。その場合、プライベート情報は、集約されたデータベースを経由して提供される。
4. 高齢者の能力に適応する、マルチモードのインターフェースを使用して、自宅療養中の高齢者にサービスが提供される。アバターや合成音声が使用できる。

監視されるデータは、専用の患者医療記録サービスを経由して、医師や病院で確認することができる。患者に関する情報は、患者に割り当てられた一意の識別子によってアクセスすることができる。このサービスでは、患者の医療記録や治療に関する文書が提供される。

Gov-Cloud

クラウドインフラストラクチャを利用してこれらのサービスを提供するために、EuropeanHealth は、政府機関によって提供される政府サービス全体向けのクラウドサービスである、Gov-Cloud を利用している。このサービスは、信頼のおけるパートナーのみにより利用され、政府機関のみが管理的なアクセス権を持っているため、ハイブリッドな、プライベートパートナークラウドである（例、行政、ヘルスケア等）。このクラウドでは、インターネットとは物理的に独立している、専用のネットワークインフラストラクチャを使用している。Gov-Cloud は、複数地域でホストされているが、仮想マシンをある場所から別な場所へ移動することもできる。本文書の Gov-Cloud 関連のシナリオに含まれるすべてのサー

ビスは、以下に記述するセキュリティ特性を備えた Gov-Cloud 上で実施される。

たとえば：

- 家庭で稼働するサービスの中には、IaaS を利用したクラウド上で稼働するものがある；
- 監視センターで稼働中のサービスは、IaaS を利用したクラウド上で稼働される；
- 監視されたデータは、DaaS（サービスとしてのデータベース）を利用して、クラウド内にも格納されている。

Gov-Cloud では、カスタマイズされた電子メールサービスを用いて、医師や看護師に対して患者データを安全に転送する手段を提供している（かつては非常に困難であった）。これは、第三機関によって提供されているが、EuropeanHealth によって設計されたものである。

データの保護

EuropeanHealth が収集したすべてのデータは、以下の要件を満たさなければならない：

- データ（機密性の高い個人情報を含む）は、潜在的なリスクがある場合には、転送中および格納中に暗号化されていなければならない（例、携帯用デバイス上のデータ等）。
- データの処理は、欧州データ保護法（例、すべてのオペレーションにおける「データ処理者」の定義等）に準拠しなければならない。
- 国内法では、データ処理に特定の制限を加える場合がある（例、データは常に、データ収集が行われた元の国を離れてはならない）。
- 臨床治療の安全性は、特定のアプリケーションにおいて、最重要視されなければならない；これは、完全性および可用性が、ある場合には「保証」されなければならないことを意味している。
- 機密性の高いデータは、そのライフサイクルで指定された時間に、破壊されなければならない（例、装置の「耐用年数経過後」に、ハードディスクを破壊する場合等）。
- データが格納されているデータセンターの物理的なセキュリティ管理策は、適切に保証されなければならない（現時点では、サプライヤから提出された ISO/IEC27001 に含まれている部分がある）。
- 上級スタッフには、「患者およびサービスを使用するユーザに関する情報」の機密性を確保するために特別な責任が課されている。

法律、規制およびベストプラクティスへの適合

- すべてのサプライヤは、ISO/IEC27001 への適合性を明示しなければならない。認証は要求されないが、その適合性は、自身の情報セキュリティ管理システムと関連ポリシーに関する文書を、彼らが年次的に提出することによって検証される。

- 追加的な認証や監査は、EuropeanHealth 機関が適切なプロバイダを選択する際に役立つ。たとえば、ISO20000（サービス管理）、ISO9001（品質）等が該当するが、義務付けられてはいない。

- 規制またはサービスプロバイダが指定する規格への準拠性監査や適合性に関し、クラウドコンピューティングサービスプロバイダは、彼らのポリシー、手順、システムおよびサービスを監査する権利を認めることが可能で、その意思があることを保証しなければならない。

ガバナンス

基本的なセキュリティ管理策は、Gov-Cloud によって提供される一方で、追加的な管理策は、管理サービスまたは Gov-Cloud の各ユーザが所属する組織内の管理サービス（例、EuropeanHealth）によって任意に提供される。これには、ITIL 等のガバナンス規格が利用されている。

EuropeanHealth は、自組織の部門に特定の技術を採用することを義務付けることはできないが、採用すべき技術を提言することはできる。EuropeanHealth の各部門は、その部門のニーズに最適な技術を自由に実装する権利を有している。

EuropeanHealth は、加盟機関に対し、提言に従っていることを示す文書の提供を求めることができる（例、ラップトップ上にあるすべてのデータが暗号化されていることを示す証明等）。外部サプライヤに関しては、EuropeanHealth のネットワークに接続し、接続状態を維持するために、それらの組織に課せられる特別な要件がある。

アクセス制御と監査証跡

EuropeanHealth は、認証トークンとして、スマートカードを使用し、自組織のアプリケーションやサービスへのシングルサインオン（SSO）を提供している。EuropeanHealth 機関は、その他にも様々な認証方式や目的毎に異なった認証方式を使い分けることができる（すなわち、単一要素、二要素、生体認証等）。Gov-Cloud の第三者機関サプライヤは、スマートカードを使用して、EuropeanHealth の PKI に接続している。

誰が、どの個人データまたは機密性の高い個人データに、どのような目的でアクセスしたかが明確であることを保証するために、監査に関する絶対的要件が存在する。

サービスレベルアグリーメント（SLA）

EuropeanHealth 機関に提供されるすべてのクラウドサービスに関し、SLA は契約として盛り込まれる必要がある。主な内容は、24/7（24 時間週 7 日間）の利用可能性であろう（ただし、サービス、アプリケーション、ホストされるデータの種類に依存する）。

- EuropeanHealth 機関の懸念は、制御を喪失する可能性であろう（例、インフラストラクチャ、サービス、データやプロビジョニング等に対して）。制御の喪失が「ない」ことを証明するクラウドサービスプロバイダの能力は、サービスの利用者が考慮すべき重要な事項である。