クラウドコンピューティング

のための

セキュリティガイダンス V2.1

Prepared by the
Cloud Security Alliance
December 2009

日本語訳（ベータ版）

はじめに

ここで提供しているガイダンスは、2009年4月に初版をリリースしたCloud Security Allianceの文書である“クラウドコンピューティングのためのセキュリティガイダンスの第2版”である。これらのドキュメントは以下に保管されている。

http:／／www.cloudsecurityalliance.org／guidance／csaguide.v2.1.pdf（本ガイダンス）
http:／／www.cloudsecurityalliance.org／guidance／csaguide.v1.0.pdf (初版)

初版を変更して、キーガイダンスをコアドメインリサーチから切り離した。各ドメインのコアリサーチはそれぞれ別個のホワイトペーパーとしてリリースする。これらのホワイトペーパーおよびリリーススケジュールは、以下のサイトに掲載する。

http:／／www.cloudsecurityalliance.org／guidance／domains／

その他の変更点としては、**ドメイン 3: 法律**および**ドメイン 4: 電子情報開示**をひとつのドメインにまとめた。さらに、**ドメイン 6: 情報ライフサイクル管理**および**ドメイン 14: ストレージ**を一つにまとめ、“データライフサイクル管理”に名称変更した。これにより、ドメイン(現在 13)の番号付けが変更されている。

日本語版にあたって

この日本語翻訳ベータ版は、クラウドセキュリティアライアンス・ジャパンチャプター有志の翻訳を参考にデロイト トーマツ リスクサービス株式会社（以下、DTRS）と有限責任監査法人トーマツが翻訳したものです。

クラウドセキュリティアライアンス・ジャパンチャプターは、翻訳を提供された株式会社日立ソリューションズ　有志一同、マカフィー株式会社　諸角昌宏氏および翻訳をしたDTRS及び有限責任監査法人トーマツに感謝の意を表します。

目次

はじめに 2
序文 5
Cloud Security Alliance の”クラウドコンピューティングのためのセキュリティガイダンス” 第 2 版へようこそ。 5
クラウドコンピューティングの発展が続く中、新たなチャンスと新たなセキュリティ課題の両方が生じている。私たちは、新たなリスクを管理する皆様のビジネスニーズをサポートするためのガイダンスとインスピレーションを提供することを望んでいる。 5
謝辞 6
編集者からのレター 8
セクション I. クラウド・アーキテクチャ 13
ドメイン 1: クラウドコンピューティングのアーキテクチャフレームワーク 14
セクション II. クラウドにおけるガバナンス 33
ドメイン 2: ガバナンスとエンタープライズリスクマネジメント 34
ドメイン 3: 法律と電子証拠開示 39
ドメイン 4: コンプライアンスと監査 41
ドメイン 5: 情報ライフサイクルマネジメント 44
ドメイン 6: 移植性と相互運用性 51
セクション III. クラウドにおける運用 55
ドメイン 8: データセンター運用 58
ドメイン 9: インシデントレスポンス、通知および復旧 61
ドメイン 10: アプリケーションセキュリティ 64
ドメイン 11: 暗号化と鍵管理 67
ドメイン 12: アイデンティティとアクセス管理 70
ドメイン 13: 仮想化 76
参照 78

序文

Cloud Security Allianceの”クラウドコンピューティングのためのセキュリティガイダンス” 第2版へようこそ。

クラウドコンピューティングの発展が続く中、新たなチャンスと新たなセキュリティ課題の両方が生じている。私たちは、新たなリスクを管理する皆様のビジネスニーズをサポートするためのガイダンスとインスピレーションを提供することを望んでいる。

Cloud Security Allianceについては、本ガイダンスの作成で最もよく知られているかもしれないが、今後数カ月にわたり、国際支部、パートナーシップ、新たなリサーチおよびカンファレンス活動を含んだ私たちのミッション促進に関する幅広い活動を見ることができる。私たちの活動は、 www.cloudsecurityalliance.org に掲載されている。

クラウドコンピューティングの安全を確保するための道のりは、グローバルベースの幅広い利害関係者の参加を必要とする長いものである。しかし、私たちが目の当たりにしている進歩は喜んで評価すべきである。新たなクラウドセキュリティソリューションが定期的に現れ、企業は、クラウドサービスプロバイダーと関与するために私たちのガイダンスを使用し、コンプライアンスと信頼性に関する健全で公開された議論が世界中で起こっている。私たちが得た最も重要な勝利は、セキュリティの専門家が、単に現状を守ることに関してだけではなく、未来を安全にすることに積極的に携わっているということである。ぜひ本トピックに関与し続け、私たちと共にこの重要なミッションを完成していただきたい。

よろしくお願いします。

Jerry Archer　　Dave Cullinane　　Nils Puhlmann
Alan Boehme　　Paul Kurtz　　Jim Reavis

謝辞

編集者

Glenn Brunette
Rich Mogull

寄稿者

Adrian Seccombe
Alex Hutton
Alexander Meisel
Alexander Windel
Anish Mohammed
Anthony Licciardi
Anton Chuvakin
Aradhna Chetal
Arthur J. Hedge III
Beau Monday
Beth Cohen
Bikram Barman
Brian O'Higgins
Carlo Espiritu
Christofer Hoff
Colin Watson
David Jackson
David Lingenfelter
David Mortman
David Sherry
David Tyson
Dennis Hurst
Don Blumenthal
Dov Yoran
Erick Dahan
Erik Peterson
Ernie Hayden
Francoise Gilbert
Geir Arild Engh-Hellesvik
Georg Hess
Gerhard Eschelbeck
Girish Bhat
Glenn Brunette
Greg Kane
Hadass Harel
James Tiller
Jean Pawluk
Jeff Reich
Jeff Spivey
Jeffrey Ritter
Jens Laundrup
Jesus Luna Garcia
Jim Arlen
Jim Hietala
Joe Cupano
Joe McDonald
Joe Stein
Joe Wallace
Joel Weise
John Arnold
Jon Callas
Joseph Stein
Justin Foster
Kathleen Lossau
Karen Worstell
Lee Newcombe
Luis Morales
M S Prasad
Michael Johnson
Michael Reiter
Michael Sutton
Mike Kavis

Nadeem Bukhari
Pam Fusco
Patrick Sullivan
Peter Gregory
Peter McLaughlin
Philip Cox
Ralph Broom
Randolph Barr
Rich Mogull
Richard Austin
Richard Zhao
Sarabjeet Chugh
Scott Giordano
Scott Matsumoto
Scott Morrison
Sean Catlett
Sergio Loureiro
Shail Khiya
Shawn Chaput
Sitaraman Lakshminarayanan
Srijith K. Nair
Subra Kumaraswamy
Tajeshwar Singh
Tanya Forsheit
Vern Williams
Warren Axelrod
Wayne Pauley
Werner Streitberger
Wing Ko
Yvonne Wilson

編集者からのレター

最初の”クラウドコンピューティングのためのセキュリティガイダンス”を出版するために、テクノロジー業界の各方面から多様な方々を集めたのがわずか７か月前であることはとても信じがたい。それ以来、この影響力の大きい出版物は、世界中の組織がクラウドコンピューティングサービスと技術の導入の是非、時期および手法に関する決定を行うことに、私たちの期待以上に大いに役立ってきた。しかし、この７カ月間の間で、私たちの知識とクラウドコンピューティング技術は驚くべき速さで進化した。この第２版は、これらの挑戦的な決定を行うために役立つ、新たな、そして更に奥深い知識を提供するようデザインされている。

クラウドコンピューティングの導入は、多くの要素を含む複雑な決定である。本ガイダンスが、導入の際に問うべき質問、現在推奨されているプラクティスおよび避けるべき潜在的な落とし穴を少しでも良く理解するために役に立つことを願う。私たちは、クラウドコンピューティングセキュリティの中核に焦点をあてることにより、しばし不完全で簡素化されすぎた情報が溢れる、分かりにくい展望をより明確にしようと試みてきた。私たちがフォーカスした最初の 15 ドメイン(現在は 13 に統合)は、クラウドコンピューティングセキュリティの議論に背景と具体性を提示する役割を果たしている。それにより、一般化を超えて、より洞察力がある、的を絞った提案をすることができる。

活動を続けるにつれ、クラウドコンピューティングのセキュリティを確保するためのベストプラクティスを発展させ普及させるという私たちのミッションが正しいものであることを信じる業界組織、企業および個人の参加が増えている。彼らの視点や洞察は、バランスのとれた、偏見のない、今後の土台になり続けられる内容を作成する上で不可欠であった。

クラウドコンピューティングは今まだ急速に進化している状況であり、常に最新動向を追う必要がある。ガイダンス第２版では、更に詳細で高い正確性を持った完全な内容に仕上げるため、私たちの大規模で多様なボランティアコミュニティの経験と専門性を活用した。それでもまだ満足すべきではない。セキュリティの専門家が長年行っているように、私たちは、クラウドコンピューティングが業界にもたらす機会のもとで、プロセス、方法および技術を常に進化させ続けなければならない。このことは、私たちがセキュリティ強化と監視機能の有効性や効率性を改善する新たな方法を見つけるための長期的な成功に重要である。

クラウドコンピューティングは、必ずしも現在の環境より安全、あるいは危険であるとは限らない。あらゆる新しい技術と同様に、クラウドコンピューティングは新たなリスクと機会の両方をもたらす。たとえば、クラウドへの参入は、現在のセキュリティ要求に合う、またはそれを超えるために、古いアプリケーションやインフラの再構築を行う機会を提供するだろう。一方で、機密なデータやアプリケーションを新しいインフラに移行するリスクは許容範囲を超えるかもしれない。本ガイダンスの目的は、何を、どこに、どのようにクラウドへ移行するかを厳密に伝えることではなく、あなた自身にて可能な限り安全に移行するための、実践的な提案と鍵となる質問を提供することである。

最後に、Cloud Security Alliance とその編集ワーキンググループを代表して、この新たなガイダンスの作成にあたり、ボランティアとして参加してくださった多くの方々に感謝する。私たちは、彼らが各自のエリアを広げ、かつ改善することに熱心であることに心を動かされ続けた。彼らの努力は、本ガイダンスの内容に大いに真の価値を加えたと信じている。彼らの貢献なくしては本ガイダンスを完成させることはできなかったであろう。

私たちは、本ガイダンスについてのあなた方からのフィードバックを切望している。
もし、本ガイダンスにおいてあなたの役に立った点、または改善すべき点があった場合は、ぜひ Cloud Security Alliance にメンバーとして、または寄稿者として参加してください。

Glenn Brunette
Rich Mogull
編集者

リスクについての編集注記:
何を、いつ、どのようにクラウドへ移行するかの決定

本ガイダンスを通して、私たちは、クラウドコンピューティングを導入する際にリスクを減らすための幅広い提案を行っている。しかし、全ての提案が必ずしも全てのクラウド展開にとって必要なわけでも、現実的なわけでもない。編集にあたり異なるワーキンググループからの情報をまとめるにつれ、起こりうる全てのリスクシナリオに対する完全な提案を提供するのは無理であることが分かった。クリティカルなアプリケーションが、公共のクラウドサービスプロバイダーに移行するには重要すぎるかもしれないのと同時に、低い価値のデータをクラウドベースのストレージに移行する際に、幅広いセキュリティコントロールを適用する必要性は低いか、または全くないかもしれない。
とても多くの異なるクラウド展開オプションが存在するため、１つのセキュリティコントロールのリストで全ての状況をカバーすることはできない。これらのオプションとは、SPI サービスモデル(SPI とは、**S**oftware as a Service, **P**latform as a Service, **I**nfrastructure as a Service のことであり、ドメイン１で説明されている)、パブリック対プライベートの展開、内部対外部のホスティング、および様々なハイブリッドへの置換である。他のセキュリティエリアと同様に、組織は、クラウドへの移行およびセキュリティオプションを選択する際に、リスクベースのアプローチを採用すべきである。以下は、初期のクラウドリスクを評価し、セキュリティ上の決定を通知するのに役立つ簡単なフレームワークである。
このプロセスは完全なリスク評価のフレームワークでもなければ、あなた方の全てのセキュリティ要件を決定する方法でもない。あなた方が資産を様々なクラウドコンピューティングモデルに移行する場合の許容範囲を評価するための簡素な方法に過ぎない。

クラウド展開する資産の特定

簡単に言うと、クラウドでサポートされる資産は一般的に以下の２つに分けられる。

1. データ
2. アプリケーション／機能／プロセス

私たちがクラウドに移行するのは、情報か、トランザクション／処理(機能の一部からアプリケーション全体まで)のどちらかである。

クラウドコンピューティングでは、データとアプリケーションが同じ場所に存在する必要はなく、機能の一部のみをクラウドに移行することさえ可能である。たとえば、Platform as a Service を通して機能の一部をクラウドにアウトソースする一方で、アプリケーションとデータを自分のデータセンタでホスティングすることができる。

クラウドのリスクを評価する第一歩は、どのデータまたは機能についてクラウドへの移行を検討するかを正確に特定することである。その際、仕様変更を防ぐため、クラウドに移行した資産の潜在的な利用法も含めるべきである。データおよびトランザクションの量は予想以上に多くなるものである。

資産の評価

次のステップは、移行を検討するデータまたは機能が、その組織にとってどれほど重要であるかを決定することである。あなたの組織に評価プロセスがある場合を除き、詳細な評価を実施する必要はないが、少なくとも資産がどれほど機密であるか、およびアプリケーション／機能／プロセスがどれほど重要であるかの大体の評価を実施する必要はある。
各資産について、次の質問をしてみよう。

1. その資産が広く一般公開されたり配布されたりした場合、どれほどの被害を受けるか？
2. クラウドプロバイダーの社員がその資産にアクセスした場合、どれほどの被害を受けるか？
3. プロセスまたは機能が外部の人間に操作された場合、どれほどの被害を受けるか？
4. プロセスまたは機能が期待した結果を出さない場合、どれほどの被害を受けるか？
5. 情報／データが予期せず変更された場合、どれほどの被害を受けるか？
6. 資産がある期間利用不可能となった場合、どれほどの被害を受けるか？

基本的に、私たちは、その資産に必要な機密性、完全性および可用性を評価しているのであり、資産の全てまたは一部がクラウドで扱われた場合にどのような影響を受けるかを評価しているのである。潜在的なアウトソーシングプロジェクトを評価するのにとてもよく似ており、異なるのは、クラウドコンピューティングでは内部モデルを含み、幅広い展開オプションがあるということである。

潜在的クラウド展開モデルへの資産のマッピング

ここまでで、私たちは既に資産の重要性を理解しているはずである。次のステップは、どの展開モデルが最適かを決定することである。潜在的なプロバイダーを検討する前に、様々な展開モデル(プライベート、パブリック、コミュニティまたはハイブリッド)およびホスティングシナリオ(内部、外部、または組み合わせ)に潜んでいるリスクを受け入れることができるかどうかを知っておくべきである。

資産について、次のオプションを受け入れることができるかどうかを決定する。

1. パブリック
2. プライベート　内部／社内(on-premise)
3. プライベート　外部(専用または共有のインフラを含む)
4. コミュニティ　ホスティング場所、潜在的なサービスプロバイダーおよび他のコミュニティメンバーを考慮する。
5. ハイブリッド　潜在的なハイブリッド展開を有効に評価するためには、コンポーネント、機能およびデータをどこに置くかについて少なくとも大まかなアーキテクチャを考慮しておく必要がある。

この時点で、あなた方はクラウド移行にあたって安心できるレベル、およびどの展開モデルと場所があなたのセキュリティとリスク要件に合うかを把握できているはずである。

潜在的クラウドサービスモデルとプロバイダーの評価

ここでは、要求されたリスク管理を実施するために、各 SPI レイヤにおいて有するコントロールの度合いに焦点を当てる。もし特定の提案を評価している場合は、この段階で完全なリスク評価に変更するかもしれない。

注目する点は、異なる SPI レイヤにおいてリスク対策を実施するために有するコントロールの度合いとなるだろう。既に具体的な要件(たとえば、規制されたデータの取り扱いなど)がある場合は、それを評価に含むこともできる。

潜在的データフローのスケッチ

具体的な展開オプションを評価する場合、あなたの組織、クラウドサービスおよび利用者／その他のノード間のデータフローを描くべきである。これらのステップの大半はハイレベルなものであっても、最終決断をする前に、データがどのようにクラウドに入ったり出たりするのかを理解することは絶対に不可欠である。

もしまだ特定の提案を検討していない場合は、受け入れ可能リストのどのオプションにおいても、大まかなデータフローを描くべきであろう。これにより、あなたは最終決定を行う際に、リスクのポイントを確認することができるようになる。

結論

この時点で、クラウドへの移行を検討しているデータまたは機能の重要性、リスク許容度(少なくともハイレベルでの)およびどの展開とサービスモデルの組み合わせを受け入れることができるかを理解できたであろう。また、機密情報と運用に関する潜在的な脅威のポイントについて大まかには把握できたであろう。

これらにより、本ガイダンスにある他のセキュリティコントロールを評価するために十分な背景をあなたは得ているであろう。低い価値を有した資産である場合、同じレベルのセキュリティコントロールは不要であり、オンサイト検査、開示可能性および複雑な暗号化スキームのような多くの忠告をスキップすることができる。高い価値を有し、管理された資産は、監査やデータの保有に関する要件を必要とするかもしれない。管理されていないが、高い価値を有した資産の場合は、技術的なセキュリティコントロールに焦点が当てられるかもしれない。

紙面は限られている中、カバーする題材が深く広いこともあり、本ガイダンスにはセキュリティ提言の広範なリストが含まれている。すべてのクラウド展開において、それぞれのセキュリティとリスクコントロールが必要なわけではない。あなたのリスク許容度と潜在的な脅威を事前に評価することにより、あなたの組織における最善のオプションと展開を選択するための背景を得ることができるだろう。

セクション I. クラウド・アーキテクチャ

ドメイン 1: クラウドコンピューティングのアーキテクチャフレームワーク

このドメイン(クラウドコンピューティングのアーキテクチャ・フレームワーク)は、本ガイダンスの他の部分のための概念的なフレームワークを提供する。このドメインの内容は、クラウドコンピューティングを特に IT ネットワークとセキュリティの専門家による視点に基づいて記述することに焦点をあてている。続く 3 つのセクションは、次の観点に基づいてこの見解を定義している:

- 一貫した語彙を提供するため、ガイダンスを通して使用される用語
- クラウド・アプリケーションとサービスを安全に保つためのアーキテクチャ要件および課題
- クラウドサービスとアーキテクチャの分類を説明する参照モデル

このドメインの最後のセクションで、他のドメインの簡潔な概要を述べている。

このドメインで記述されているアーキテクチャ・フレームワークを理解することは、本ガイダンスの他の部分を理解するための重要な第一歩である。このフレームワークは、他のドメインの中で使用される概念と用語の多くを定義している。

クラウドコンピューティングとは何か?

クラウドコンピューティング(”クラウド”という)は、コンピューター環境を別のものに変えてしまう多くの既存技術およびアプローチの発展を述べるための用語で、今も進化し続けている用語である。クラウドによって、アプリケーションと情報資源は、インフラおよびそれを提供するメカニズムから分離される。

クラウドは、連携(コラボレーション)、迅速性、スケーリングおよび可用性を強化し、最適化と効率的なコンピューティングを通して、コスト削減の可能性を提供する。

より詳しく述べると、クラウドとは、コンピューティング、ネットワーク、情報およびストレージリソースのプールで構成されるサービス、アプリケーション、情報およびインフラの集合を利用することを指している。これらのコンポーネントは、迅速に編成、プロビジョニング、実装、閉鎖、拡大・縮小することができ、割り当てと利用というオンデマンドのユーティリティ型のモデルを提供する。

アーキテクチャの観点について、クラウドと既存のコンピューティング・モデルとの類似点および相違点、これらの類似点と相違点がネットワークと情報セキュリティ対策への組織、運用、技術面におけるアプローチに与える影響については大きな混乱が見られる。

現在、学術的な観点、アーキテクトの観点、エンジニアの観点、開発者の観点、管理者の観点、さらに利用者の観点からクラウドを定義しようという試みがある。本ガイダンスでは、IT ネットワークとセキュリティの専門家の特有の観点からの定義に焦点を当て

ている。

クラウドのアーキテクチャがどのようにセキュリティアーキテクチャに影響を与えるかを理解するための鍵は、一般的で簡潔な用語と、クラウドサービスとアーキテクチャを分解し、セキュリティと業務管理のモデル、リスク評価と管理のフレームワーク、そしてコンプライアンス基準へのマッピングを可能にする一貫性のある定義・分類である。

クラウドコンピューティングの構成要素とは？

本ガイダンスの初版では、クラウドコンピューティングに対する米国標準技術局(NIST)の科学者による公開作業の前に書かれた定義を用いていた。

NIST の出版物は一般によく受け入れられている。 本ガイダンスの作成にあたっては、クラウドコンピューティングに対する NIST Working Definition of cloud computing (これを書いている時点ではバージョン 15)と合わせることにより、共通の言葉による一貫性とコンセンサスをもたらし、意味づけよりも使用事例に焦点を当てるようにした。

本ガイダンスが、グローバルな組織において幅広く使用可能で適用可能になるように試みていることは重要である。NIST は米国の政府組織であり、この参照モデルを選択するにあたっては、別の観点や地理的な要素にも配慮するべきである。

NIST は、クラウドコンピューティングを 5 つの基本特性、3 つのクラウドサービスモデルおよび 4 つのクラウド展開モデルにより定義している。それらは、図 1 に視覚化された形で要約され、その後で詳細に説明されている。

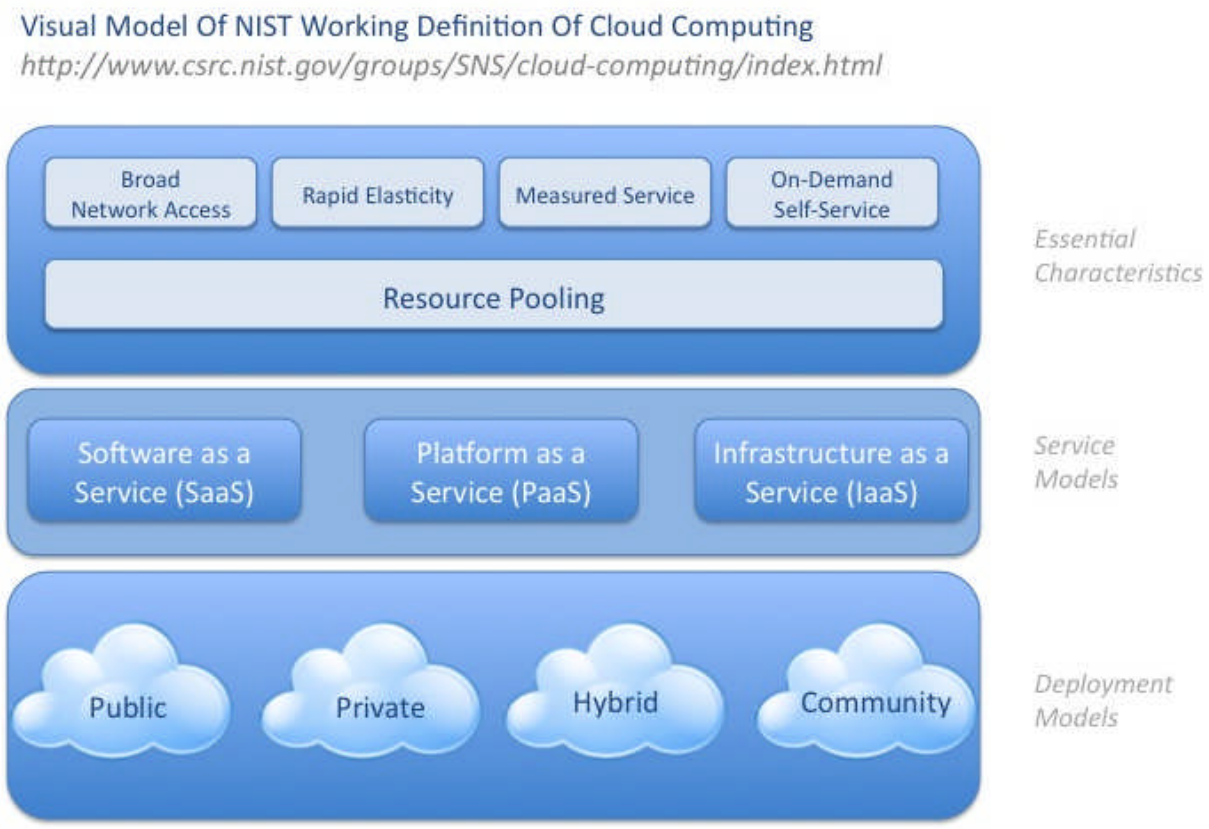


図 1　NIST ビジュアルモデルによるクラウドコンピューティングの定義

クラウドコンピューティングの基本特性

クラウドサービスは、従来のコンピューティングのアプローチとの関係および違いを示す 5 つの基本特性を有している:

- **オンデマンド・セルフサービス**　　利用者は、、サーバタイムやネットワーク・ストレージ等のコンピューティング機能を、サービスプロバイダとの人的なやり取りなしに、必要に応じて自動的に独自に供給することができる。
- **幅広いネットワークアクセス**　　機能はネットワークを通して利用でき、標準的なメカニズムでアクセスできる。これは、従来のサービスやクラウドベースのソフトウエアサービスと同様に、さまざまなシンクライアントあるいはシッククライアント(たとえば、モバイル電話、ラップトップ、PDA)で使うことができる。
- **リソースプーリング**　　プロバイダーのコンピューティング・リソースは、マルチテナントモデルを使用することで複数の利用者に提供されるようにプールされる。これは、異なった物理的リソースや仮想化リソースにダイナミックに割り当てられ、利用者の要求に従って再割り当てされる。ある程度の位置の独立性があり、利用者は、通常、プロバイダーのリソースの正確な場所をコントロールすることや知ることはできない。しかし、より抽象度の高いレベル(たとえば、国、州またはデータセンター)では位置は指定できるかもしれない。リソースの例として

は、ストレージ、プロセシング、メモリ、ネットワーク回線容量および仮想マシン(VM)が含まれる。プライベートクラウドでさえ、同じ組織の異なった部分のリソースをプールする傾向がある。

- **迅速な弾力性**　機能は、素早くスケールアウトするために、迅速かつ弾力性をもって(場合によっては自動的に)プロビジョニングされ、また素早くスケールインするために迅速に解放することができる。利用者にとっては、プロビジョニング可能な機能は、しばしば無限にあるように見え、必要な時に必要な量だけ購入することができる。
- **測定されたサービス**　クラウドシステムは、サービスのタイプ(たとえば、ストレージ、プロセシング、帯域幅、アクティブなユーザアカウント)に適したレベルで抽象化された測定機能を活用することで、自動的にリソースの利用をコントロールし、最適化する。リソースの使用はモニタリング、コントロールおよび報告が可能であり、これはプロバイダーとサービス利用者の両方に透明性を提供する。

クラウドサービスが、しばしば仮想化技術とともに、あるいは、仮想化技術により利用可能にされていることを理解することは重要である。しかし、リソースの抽象化と仮想化技術を結びつける必要はないし、多くの製品では、ハイパーバイザーやオペレーティングシステム(OS)・コンテナによる仮想化は利用されていない。

さらに、マルチテナント型であることは、NIST におけるクラウドの基本特性として挙げられていないが、しばしばそうであると議論されているということに注意すべきである。以下のクラウド展開モデルの記述の後に記載されているマルチテナントのセクションを参照してください。

クラウドサービスモデル

クラウドサービスの展開は、3 つの典型的なモデルと、様々な派生形の組み合わせに分けられる。3 つの基本的な分類は、しばしば"SPI モデル"と呼ばれる。ここで、"SPI"は、それぞれ、Software、Platform、Infrastructure (as a Service)で、以下のように定義される:

- **クラウド Software as a Service (SaaS)**　利用者に提供される機能は、クラウドのインフラ上で動く、プロバイダーが提供するアプリケーションを使用する機能である。アプリケーションは、ウェブブラウザ(例:ウェブベースの email)のようなシンクライアント・インターフェースを通して、さまざまなクライアント・デバイスからアクセス可能である。利用者は、限られたユーザ固有の設定を除き、ネットワーク、サーバ、OS、ストレージ、個々のアプリケーションの機能を含むクラウドインフラの管理およびコントロールを行わない。
- **クラウド Platform as a Service (PaaS)**　利用者に提供される機能は、プロバイダーによってサポートされているプログラミング言語やツールを使用し、利用者が作成したアプリケーションをクラウドのインフラに展開する機能である。利用者は、基本的なクラウドのインフラ、ネットワーク、サーバ、OS およびストレージを管理およびコントロールしないが、展開しているアプリケーションと、場合によってはアプリケーションをホスティングしている環境の設定をコントロールする。

- **クラウド Infrastructure as a Service (IaaS)**　利用者に提供される機能は、処理、ストレージ、ネットワークおよびその他の基本となるコンピューティング資源の割り当てであり、そこで利用者は OS とアプリケーションを含む任意のソフトウェアを展開して動かすことができる。利用者は、基盤となるクラウドのインフラを管理およびコントロールしないが、OS、ストレージ、展開されたアプリケーションおよび場合によっては選択されたネットワーク・コンポーネント(たとえば、ホスト・ファイアウォール)をコントロールする。

NIST モデルおよび本ガイダンスでは、クラウドサービスブローカー、仲介や監視、移送・移植性、ガバナンス、プロビジョニングを提供するプロバイダ、およびインテグレーションサービスに関連した新たなサービスモデルの定義は行わない。また、NIST モデルおよび本ガイダンスでは、さまざまなクラウドプロバイダーと利用者の間の関係についての議論は行わない。

短期的には、イノベーションが迅速なソリューション開発を促すのに伴い、API やインタフェースの開発といった形態で、クラウドサービスのプロバイダーと利用者がクラウドサービスと連携する方法は多様化している。これにより、クラウドサービスブローカーは、総合的なクラウド・エコシステム(生態系)において重要な構成要素になる。

特定の問題をより長期的に解決するための、一般的でかつオープンでありまた標準的な方法が登場する前に、クラウドサービスブローカーは、利用者に代わり、場合によっては互換性のない機能やインターフェースを取り除くであろう。それにより利用者独自のニーズに対して最も効果のあるモデルを活用することができるよう、利用者が流動性や迅速性を得ることができるための意味を与える。

また、クラウドの管理、セキュリティ、相互運用性などを可能にしようとするオープン API および独自の API の両方の開発に関する多くの取り組みにも注意する必要がある。これらの取り組みをいくつか挙げると、Open Cloud Computing Interface Working group、 Amazon EC2 API、VMware の DMTF によって提出された vCloud API、Sun の Open Cloud API、Rackspace API、GoGrid の API 等がある。オープンで標準的な API は、DMTF の Open Virtualization Format (OVF)のような共通のコンテナ形式と同様に、クラウドの移植性と相互運用性に重要な役割を果たすであろう。

現在、多くのワーキンググループやドラフトおよび公開済みの仕様があるが、利用者の要求や市場および経済の原理により、管理が容易で相互運用性のあるものだけに整理されていくだろう。

クラウド展開モデル

利用するサービスモデル(SaaS、PaaS、IaaS)にかかわらず、クラウドサービスには 4 つの展開モデルと、特定の要求に対処するためにそれらから派生した変化形がある:

- **パブリッククラウド**　クラウドインフラは、一般社会や大企業グループに利用可能で、クラウドサービスを販売する組織によって所有される。
- **プライベートクラウド**　クラウドインフラは、1 つの組織のみのために運用さ

れる。組織あるいはサードパーティによって管理が行われ、組織内(on-premise)か、組織外(off-premise)に置かれる。

- **コミュニティクラウド**　クラウドインフラは、いくつかの組織によって共有され、関心事(たとえば、ミッション、セキュリティ要件、政策、またはコンプライアンス問題)を共有した特定のコミュニティをサポートする。組織あるいはサードパーティによって管理が行われ、組織内(on-premise)か、組織外(off-premise)に置かれる。
- **ハイブリッドクラウド**　クラウドインフラは、2 つあるいはそれ以上のクラウド(プライベート、コミュニティ、パブリック)から構成され、それぞれが独自の実体が残るものの、データやアプリケーションの移植性(たとえば、クラウド間のロードバランスのためのクラウドバースティング)を可能にする標準ないしは独自の技術によって結び付けられている。

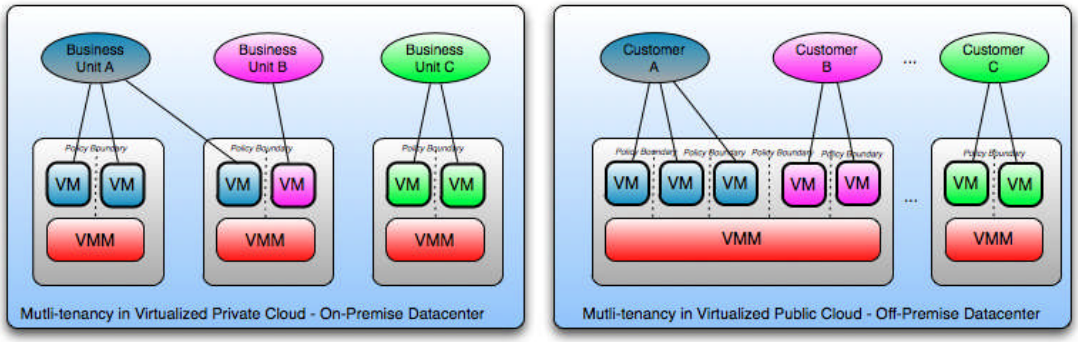
市場の製品と顧客要求の成熟化により、派生したクラウド展開モデルが出現してきていることに注意することは重要である。そのような例として、仮想化プライベートクラウドがある。これは、プライベートあるいは準プライベートな方法でパブリッククラウドインフラを利用して、利用者のデータセンターにある内部リソースを仮想プライベートネットワーク(VPN)を通して相互接続する方法である。

ソリューションを設計するときに用いられるアーキテクチャの考え方は、結果として得られるソリューションに対する将来の柔軟性、セキュリティおよび移行性に対して明確な意味を持っている。経験則からすると、境界のある(perimeterized)ソリューションは、それぞれの 4 つの領域において境界のない(de-perimeterized)ソリューションより有効性が低い。また、同様の理由で、独自のソリューションを用いるか、オープンなソリューションを用いるかの選択については慎重な検討を実施すべきである。

マルチテナント

NIST のクラウドコンピューティングモデルの基本特性には挙げられていないが、CSA は、マルチテナントをクラウドの重要な要素であると認識している。

クラウドサービスモデルにおけるマルチテナントは、異なる利用者層のための、ポリシーに基づいた実施や、区分け、分離、ガバナンス、サービスレベル、支払拒否／請求モデルの必要性を暗示する。パブリッククラウドプロバイダーが提供するサービスは複数の利用者によって利用される。そのような利用者は、実際には複数の異なる組織というよりは、同じ組織内で複数の異なる事業単位でインフラを共有しつつサービスを利用するかもしれない。



Private Cloud of Company XYZ with 3 business units, each with different security, SLA, governance and chargeback policies on shared infrastructure

Public Cloud Provider with 3 business customers, each with different security, SLA, governance and billing policies on shared infrastructure

図 2　マルチテナント

プロバイダーの観点から見ると、マルチテナントは、規模の経済性、可用性、管理、区分け、分離、および効率的な運用を可能にするためのアーキテクチャとデザインへのアプローチであり、多くの異なった利用者に対してインフラ、データ、メタデータ、サービスおよびアプリケーションの共有を促進している。

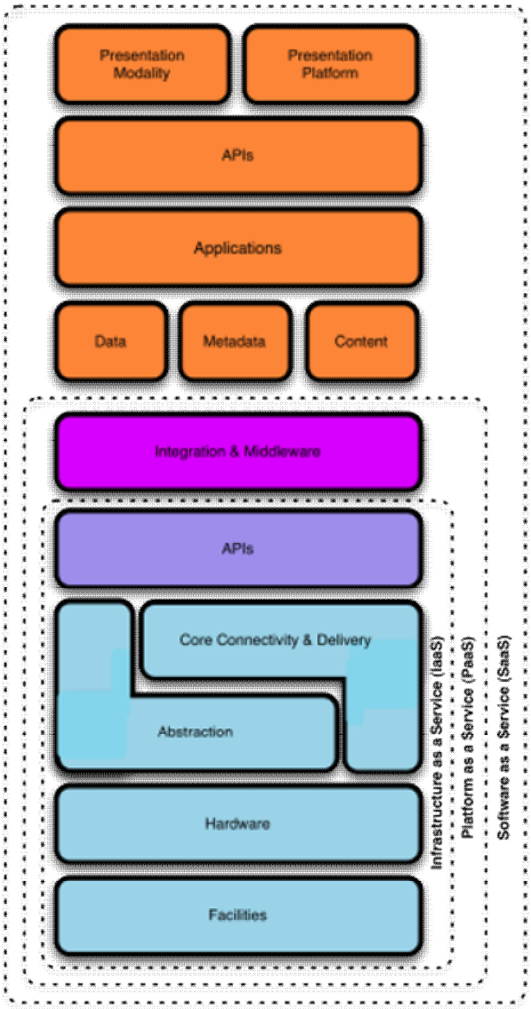


図 3　クラウド参照モデル

また、マルチテナントには、プロバイダーのクラウドサービスモデルごとに異なった定義が可能である。マルチテナントは、上記のインフラ、データベースまたはアプリケーションレベルで説明した機能を可能にするかもしれないからである。例としては、IaaS と SaaS ではマルチテナントの実現方法に違いが見られる点がある。

クラウド展開モデルは、マルチテナントに対して別の重要性を持っている。しかし、プライベートクラウドの場合でさえ、1 つの組織には、サードパーティのコンサルタントや契約者が多数いるかもしれない。また、事業単位ごとに高度に論理的な分離を希望する可能性もある。したがって、マルチテナントの懸念点を常に考慮するべきである。

クラウド参照モデル

クラウドコンピューティングのモデル間の関係と依存性を理解することは、クラウドコンピューティングのセキュリティリスクを理解する上で重要である。IaaS はすべてのクラウドサービスの基盤であり、PaaS は IaaS 上に作られており、SaaS はクラウド

参照モデルの図で説明されているように PaaS 上に作られている。機能が継承されるのと同様に、情報セキュリティの問題とリスクも継承される。商業用クラウドプロバイダーは、その階層化されたサービスモデルにきちんと収まらない可能性があることに注意する必要がある。それでもなお、実世界にあるサービスをアーキテクチャ・フレームワークに関連づけ、セキュリティ分析を必要とするリソースとサービスを理解するために、この参照モデルは重要である。

IaaS は、全体的なインフラのリソーススタックからできている。これは、施設からそこに設置されているハードウェアプラットフォームまでを含んでいる。さらに、IaaS は、機能を抽象化する(あるいはしない)機能と、リソースに対する物理的あるいは論理的な接続性を提供する機能を包含する。つまり、IaaS は、サービスの利用者がインフラに対する管理やその他の相互のやり取りを行うための API を提供する。

PaaS は IaaS の上に位置し、アプリケーション開発用フレームワーク、ミドルウェア機能およびデータベース、メッセージング、キューイングのような機能を統合するためのレイヤを提供している。これにより、開発者は、プログラミング言語とツールがスタックによってサポートされているアプリケーションをプラットフォーム上に構築することができる。

SaaS は、IaaS と PaaS スタックの上に作られ、内包した運用環境を提供している。これは、コンテンツ、プレゼンテーション、アプリケーションと管理機能を含んだ全体的なユーザ環境を提供している。

したがって、それぞれのモデルには統合機能、複雑性対公開性(拡張性)およびセキュリティにおいて重要なトレードオフがあることは明らかである。3 つのクラウド展開モデル間のトレードオフには次のものが含まれる:

- 一般に、SaaS は 3 つのモデルの中で、製品に直接組み込まれた統合機能を最も多く提供し、利用者側の拡張性は最小であり、比較的高いレベルのセキュリティ(少なくともプロバイダー側がセキュリティに対する責任を負う) を提供する。
- PaaS は、開発者にプラットフォーム上で開発者独自のアプリケーションを構築させることを意図している。結果として、利用者がすぐに利用できる機能を削減することで SaaS より拡張性が高い傾向にある。このトレードオフは、セキュリティ機能や能力にも及ぶ。PaaS では、作りこみの機能は完全ではないが、セキュリティのレイヤを追加することに対する柔軟性は高い。
- IaaS は、アプリケーションのような機能をわずかしか提供しないが、拡張性が非常に高い。このことは、一般に、インフラ自身を守るセキュリティ機能や能力はほとんど持っていないということを意味する。このモデルでは、OS、アプリケーションおよびコンテンツがクラウド利用者によって管理され、安全に保たれている必要がある。

セキュリティ・アーキテクチャについての重要なポイントは、クラウドサービスプロバイダーが提供するモデルのレイヤが下に行くほど、利用者が実装あるいは管理しなければならないセキュリティの機能と管理が増大するということである。

SaaS の場合は、サービスとプロバイダーのサービスレベル、セキュリティ、ガバナンス、コンプライアンスおよび法的責任に対して期待される点が、契約上規定され、管理され、強制される。PaaS あるいは IaaS の場合は、プロバイダーには、基本サービスの可用性およびセキュリティを確保するため、プラットフォームおよびインフラのコンポーネントを安全にするための、一部の埋め合わせが期待されるものの、サービスレベル、セキュリティ、ガバナンス、コンプライアンス、および期待される法的責任を管理することは、利用者側のシステム管理者の責任である。どちらの場合においても、実施責任は譲渡／移転できるが、必ずしも説明責任も譲渡／移転できるわけではないということは明確である。

それぞれのクラウド展開モデルについて、スコープや特定の機能を狭めていくか、あるいは各モデル間のサービスや能力をつなげていくと、派生した分類をもたらすかもしれない。たとえば、”Storage as a Service”は IaaS 系の中の一つの形態である。

成長し続けるクラウドコンピューティングソリューションをより広く検討することは、本ガイダンスの範囲外であるが、以下の図で示す OpenCrowd クラウドソリューションの定義・分類は素晴らしい出発点を提供している。OpenCrowd の定義・分類は、これまでに定義したそれぞれのモデルを超えて、さらに増え続ける今日のソリューションを示している。

CSA は、以下に示されているソリューションや会社のいずれに対しても特別な支持をしておらず、今日利用可能な提供サービスの多様性を説明するためにこの図を提示していることに注意すべきである。

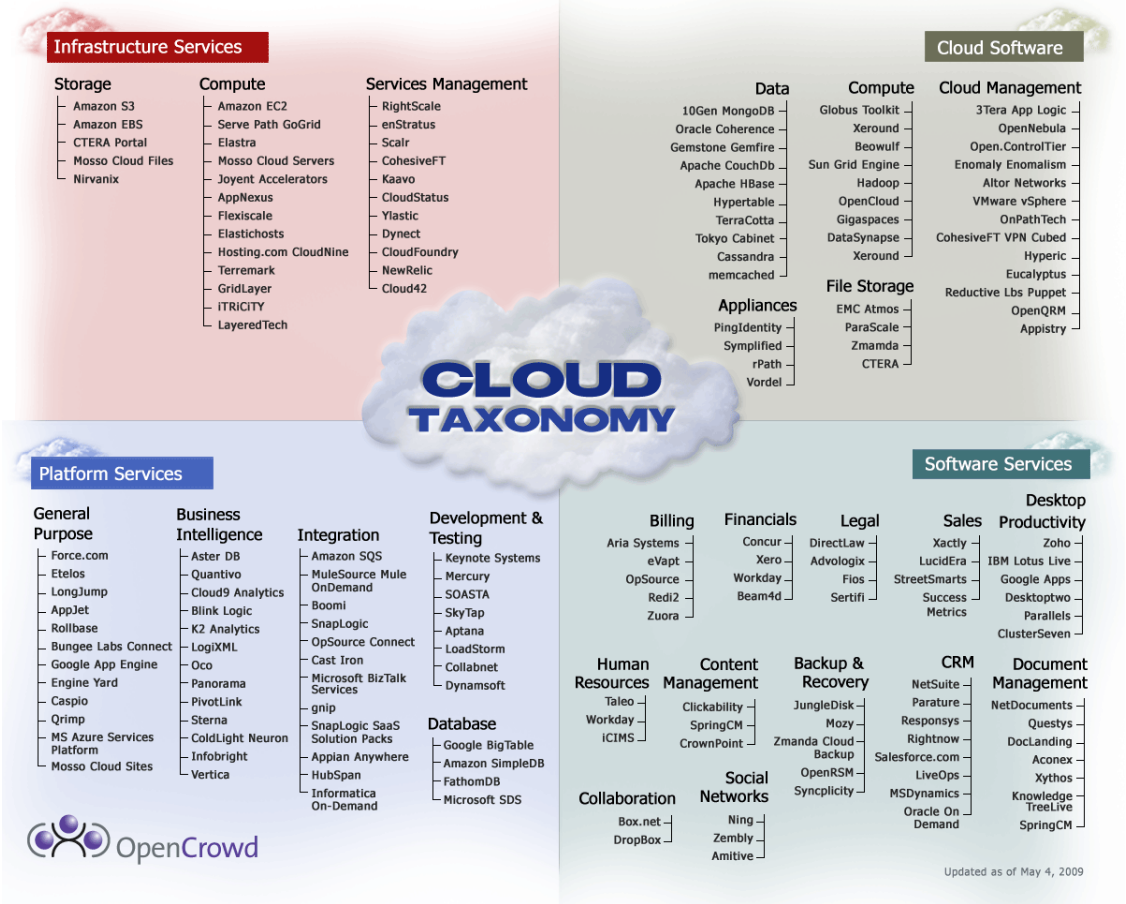


図 4　OpenCrowd 分類学

多くのクラウドコンピューティングのユースケースに関する優れた概要を作成するため、Cloud Computing Use Case Group は、”クラウド利用者およびクラウドベンダーと共にクラウドコンピューティングの一般的な使用事例を定義し、相互作用性、統合の容易さ、および移植性を確保するために、クラウド環境で標準化される必要がある機能および要件を明らかにする”という目的のもと、一般的な事例を説明および定義し、クラウドの利点を説明するため、共同研究を行った。

クラウドセキュリティ参照モデル

クラウドセキュリティ参照モデルは、分類間の関係性を説明し、関連するセキュリティコントロールや懸念事項に応じて分類を定義している。クラウドコンピューティングに初めて取り組む組織や個人は、以下の潜在的な落とし穴や混乱を避けることが重要である:

1. クラウドサービスがどのように展開されるかという概念は、しばしば、それがどこに提供されるかという概念と混同して使われており、混乱を引き起こしている。たとえば、パブリックとプライベートのクラウドが、”外部”と”内部”のクラウドと呼ばれることがあるが、これは全ての状況において必ずしも正確ではない。

2. クラウドサービスの利用形態は、しばしば組織の管理または境界セキュリティ(通常、ファイアウォールの存在によって定義される)の位置に関連して説明されている。セキュリティ境界が、クラウドコンピューティングにおいてどこに位置しているかを理解することは重要である一方、明確な境界が存在するという考えは、時代遅れの概念である。
3. 企業において既に起こっている信頼境界の再境界化および侵害は、クラウドコンピューティングによって増幅され、加速される。ユビキタスな接続性、無定形な情報のやりとりおよび従来の静的なセキュリティコントロールの無効性は、動的な性質を持つクラウドサービスに対応できない。これらはすべて、クラウドコンピューティングに対する新しい考え方を必要としている。Jericho Forum は、多くのケーススタディを含む企業ネットワークの再境界化についての多くの資料を作り出した。

このように、クラウドの展開と利用方法は、資産、リソースおよび情報の物理的な場所に関する”内部”または”外部”か、の状況だけではなく、それらが誰によって利用されているか、そして、誰がポリシーと標準に対するガバナンス、セキュリティおよびコンプライアンスに責任を持つかということも合わせて考慮されるべきである。

このことは、資産、リソースおよび情報が存在する場所が社内(on-premise)であるか社外(off-premise)であるかどうかが、セキュリティおよび組織のリスク管理に影響を与えないということを示しているわけではなく(実際には影響は与える)、リスクは以下のことにも依存するということを強調しているのである：

- 管理される資産、リソースおよび情報のタイプ
- 誰がどのように管理するか
- どのコントロールが選択され、どのように統合されているか
- コンプライアンスの問題

たとえば、Amazon の AWS EC2 で展開される LAMP スタックは、パブリック、社外(off-premise)、サードパーティによって管理される IaaS ソリューションとして分類されるであろう。それは、その中に含まれたインスタンスとアプリケーション／データが、利用者またはサードパーティによって管理される場合においても同様である。また、会社のコントロール、管理、および所有権のもとで Eucalyptus 上に展開された、複数の事業単位に提供されるカスタムアプリケーションスタックは、プライベート、社内(on-premise)、そして、自己が管理する SaaS ソリューションとして分類できる。この 2 つの例は、クラウドの弾力性によるスケーリングとセルフサービス機能を活用している。

以下の表はこれらのポイントをまとめている:

	Infrastructure Managed By[1]	Infrastructure Owned By[2]	Infrastructure Located[3]	Accessible and Consumed By[4]
Public	Third Party Provider	Third Party Provider	Off-Premise	Untrusted
Private/ Community	Or Organization / Third Party Provider	Organization / Third Party Provider	On-Premise / Off-Premise	Trusted
Hybrid	Both Organization & Third Party Provider	Both Organization & Third Party Provider	Both On-Premise & Off-Premise	Trusted & Untrusted

[1] *Management includes: governance, operations, security, compliance, etc...*
[2] *Infrastructure implies physical infrastructure such as facilities, compute, network & storage equipment*
[3] *Infrastructure Location is both physical and relative to an Organization's management umbrella and speaks to ownership versus control*
[4] *Trusted consumers of service are those who are considered part of an organization's legal/contractual/ policy umbrella including employees, contractors, & business partners. Untrusted consumers are those that may be authorized to consume some/all services but are not logical extensions of the organization.*

表 1　クラウドコンピューティング展開モデル

クラウドサービスモデル、展開モデル、リソースの物理的な場所、管理と所有権の特性を見える化するためのもう一つの方法として、以下の図に示した Jericho Forum (www.jerichoforum.org)のクラウドキューブモデルがある。:

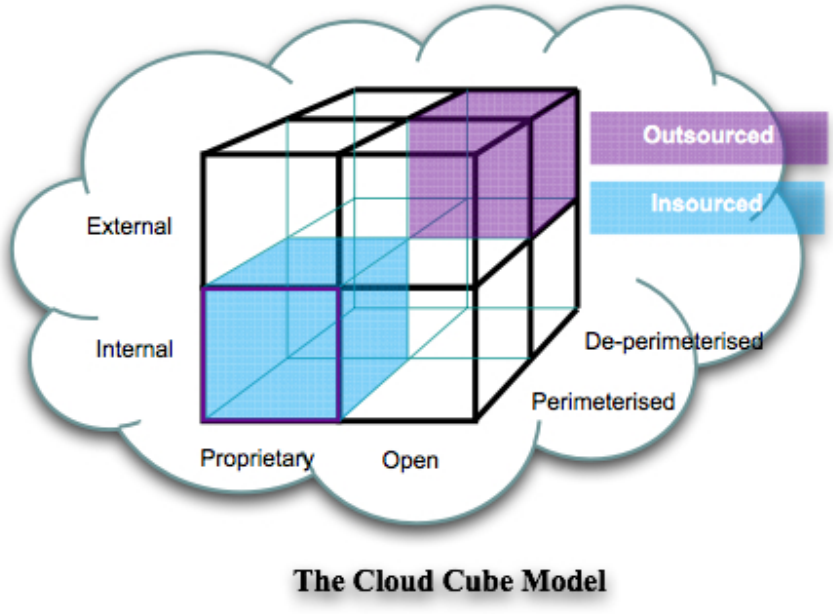


図 5　Jericho クラウドキューブモデル

クラウドキューブモデルは、クラウドが今日提供している利用可能な組み合わせを示し、各クラウドの”構成”および提供方法を区別するための 4 つの評価基準／次元を提示している。これにより、クラウドコンピューティングがセキュリティへのアプローチ方法にどのように影響するかを理解することができる。

また、クラウドキューブモデルは、クラウドモデルを理解すること、また、これをコントロールフレームワークやISO／IEC 27002のような規格にマッピングすることの難しさを浮き彫りにし、”…組織におけるセキュリティ管理を開始し、導入し、維持し、改善するための一連のガイドラインや一般的な原理”を提供している。

ISO／IEC27002 のセクション 6.2 ”外部組織”のコントロール目標は、次のように記載されている。”…組織の情報と情報処理設備のセキュリティは、外部組織の製品やサービスの導入によって削減されるべきではない…”。

このように、3 つのクラウドサービスモデルを安全に保つための方法と責任の違いは、クラウドサービスの利用者が困難な試練に直面していることを意味する。クラウドプロバイダーが、速やかにセキュリティコントロールおよびそれをどの程度利用者に対して実装しているかを公開し、また、利用者が情報セキュリティを維持するためにどのようなコントロールが必要であるかを理解しない限り、誤った意思決定や有害な結果をもたらす可能性が非常に多くなる。

重要な点としては、まず、クラウドサービスをクラウドアーキテクチャモデルに沿って分類する。そうすると、ギャップ分析の実践として、セキュリティ・アーキテクチャにマッピングすることができるようになる。同様に、ビジネス、規制、その他のコンプライアンス要件に対してもマッピングすることができる。結果として、そのサービスの全体的な”セキュリティ”に対する姿勢を特定したり、資産の保証と保護に関する要件にどのようにかかわっているかを特定したりすることできる。

以下の図では、クラウドサービスのマッピングが、どのように対象となるコントロールの一覧と比較することができるかについて例を示している。これは、利用者、クラウドサービスプロバイダーあるいはサードパーティ機関のいずれかが提供するコントロールのうち、どのコントロールが存在し、どのコントロールが存在しないかを特定するためのものである。これは、以下の図が示すように、コンプライアンスのフレームワークあるいは PCI DSS のような一連の要件と比較することができる。

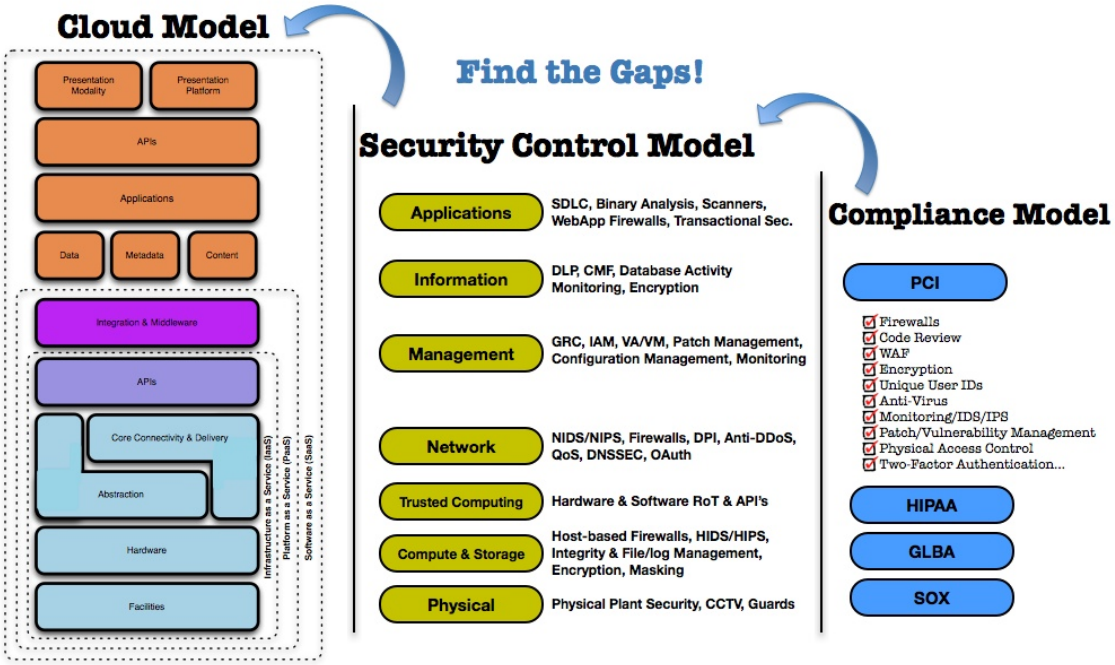


図 6　クラウドモデルをセキュリティコントロールとコンプライアンスモデルにマップする

一度、何らかの規制またはその他のコンプライアンス要件に対してこのギャップ分析を完成させると、リスク評価フレームワークにフィードバックするために行わなければならないことを特定することが容易になる。これは、今度はギャップに、そして最終的にはリスクに対してどのように対処(受容、移転または緩和)するべきか、の決定に役立つ。

クラウドコンピューティングを運用モデルとして使用することは、本質的にコンプライアンスを達成したり妨げたりすることはないということに注意するのは重要である。どのような要件に対しても準拠する能力は、サービス、使用されている展開モデルならびに対象範囲にあるリソースのデザイン、展開や管理によるものである。

上記で示した一般的なコントロールフレームワークの概要に関しては、Open Security Architecture Group のセキュリティアーキテクチャパターン文書の”landscape”、あるいは、NIST800-53 revision3 で推薦されている Security Controls for Federal Information Systems and Organizations のセキュリティコントロールカタログに分かり易い説明がある。

クラウドコンピューティングのためのセキュリティとは何か?

クラウドコンピューティングにおけるセキュリティコントロールは、IT 環境におけるセキュリティコントロールとほとんど変わらない。しかし、使用されているクラウドサービスモデル、運用モデルおよびクラウドサービスの使用を可能にする技術により、クラウドコンピューティングは従来の IT ソリューションと異なったリスクをもたらす可能性がある。
クラウドコンピューティングでは、コントロールは行わないもののものの、説明責任は

維持される。これは、運用の責任が一つまたは複数のサードパーティに委ねられていたとしても同様である。

組織のセキュリティに対する姿勢は、実装されているセキュリティコントロールの成熟度、有効性および完全性によって特徴付けられる。これらのコントロールは、施設(物理的なセキュリティ)からネットワークインフラ(ネットワークセキュリティ)、IT システム(システムセキュリティ)、情報とアプリケーション(アプリケーションセキュリティ)まで複数のレイヤに渡って実装される。さらに、コントロールは、職責の分離や変更管理など、人とプロセスのレベルにも実装される。

本ガイダンスで前述したように、プロバイダーと利用者それぞれが負うセキュリティに関する責任の範囲は、クラウドサービスモデルごとに大きく異なる。例として、Amazon の AWS EC2 infrastructure as a Service は、ハイパーバイザーまでのセキュリティの責任をベンダーが負っている。つまり、ベンダーは物理的なセキュリティ、環境のセキュリティおよび仮想化のセキュリティのみを扱う。そして、利用者は、OS、アプリケーションおよびデータを含む IT システム(インスタンス)に関連したセキュリティコントロールに対して責任を負う。

Salesforce.com のカスタマ・リレーションシップ・マネジメント(CRM)SaaS では状況が逆になる。全体の"スタック"が Salesforce.com によって提供されるため、プロバイダーは物理的および環境のセキュリティコントロールに対して責任を負うだけでなく、インフラ、アプリケーションおよびデータのセキュリティコントロールにも対応しなければならない。このことは、利用者の直接的な運用責任の多くを緩和している。

クラウドコンピューティングの魅力の 1 つは、規模の経済性、再利用および標準化による費用効率の良さである。これらの効率化を実現するため、クラウドプロバイダーは可能な限り多くの利用者にサービスを提供するための十分な柔軟性を保ち、対応可能なマーケットを最大化しようとする。残念ながら、セキュリティをこれらのソリューションに統合することは、しばしば柔軟性を低減させてしまうと認識されている。

この柔軟性の弱さにより、しばしばクラウド環境では従来の IT と同等のセキュリティコントロールを展開することができない。これは、多くの場合、インフラの抽象化や、(特にネットワークレイヤにおいて)良く知られたセキュリティコントロールを統合するための可視性や能力が欠如していることに起因している。

以下の図は、これらの問題を表現している: SaaS 環境においては、セキュリティコントロールとそれらの範囲はサービス契約として取り決められる。サービスレベル、プライバシーおよびコンプライアンスは、すべて契約において法的に対処されるべき問題である。IaaS 提供においては、インフラと抽象化レイヤのセキュリティに対する責任はプロバイダー側にあるが、残りのスタックについては利用者の責任となる。PaaS は、それらの中間で、プラットフォームのセキュリティはプロバイダーの責任であるが、プラットフォーム上に開発されたアプリケーションのセキュリティおよびやそれらのアプリケーションを安全に開発することは利用者側の責任である。

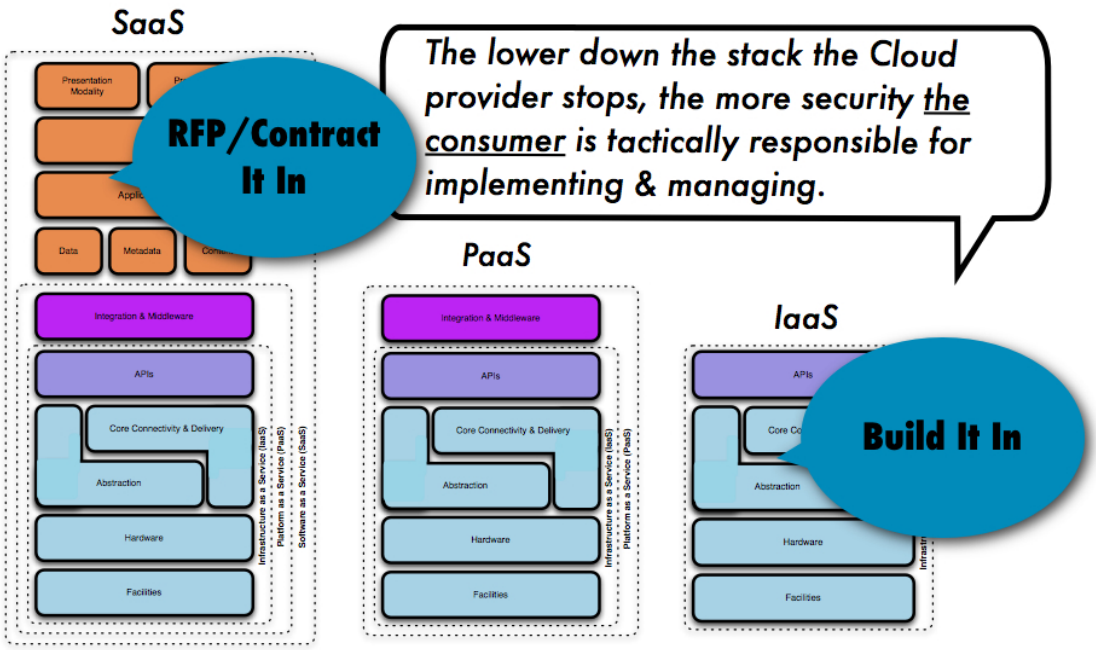


図 7　どのようにセキュリティが統合されるか

サービスモデルおよび展開方法の違いによるインパクトを理解することは、組織のリスクに対する姿勢を管理する上で重要である。

アーキテクチャを超えて：重要なフォーカスエリア

CSA ガイダンスの残りの部分を構成している 12 のドメインは、クラウドコンピューティングにおける懸念点を浮き彫りにし、クラウド環境におけるセキュリティの”痛点”を戦略的、戦術的に扱い、クラウドサービスと展開モデルのどのような組み合わせにも適用できるようにしている。

ドメインは、ガバナンスと運用という 2 つの広義のカテゴリに分割されている。ガバナンスドメインは幅広くクラウドコンピューティング環境における戦略的で政策的な問題を扱っている。一方、運用ドメインは、アーキテクチャにおけるより戦術的なセキュリティの問題と実現方法に焦点を当てている。

ガバナンスドメイン

ドメイン	ガイダンスの内容
ガバナンスとエンタープライズリスクマネジメント	クラウドコンピューティングの導入によりエンタープライズリスクを統治し、測定する組織の能力。合意違反の際の法的な優先権、ユーザ組織によるクラウドサービスプロバイダーのリスクを適切に評価できる能

	力、利用者とプロバイダーの両者に過失がある場合の機密データ保護責任および国際的な境界がこれらの問題にどのように影響するか、などの項目を取り上げている。
法律と電子情報開示	クラウドコンピューティングを利用する際の潜在的な法的問題。このセクションで触れられている問題は、情報およびコンピュータシステムのための保護要件、セキュリティ違反の情報開示法、法的な要求事項、プライバシー要件、国際法などを含む。
コンプライアンスと監査	クラウドコンピューティングを使用する際のコンプライアンスの維持と証明。クラウドコンピューティングが、社内のセキュリティポリシーやその他さまざまなコンプライアンス要件(規制、立法、その他)へのコンプライアンスに与える影響の評価方法に関する問題がここでは議論されている。このドメインは、監査に際してコンプライアンスを証明するためのいくつかの方向性を含む。
情報ライフサイクル管理	クラウドに置かれているデータの管理。クラウド上のデータの認識とコントロールに関する項目や、クラウドにデータを移す際に失われる物理的なコントロールを補償するコントロールについて取り上げている。その他に、データの機密性、完全性および可用性に対する責任の所在についても言及している。
移植性および相互運用性	あるプロバイダーから別のプロバイダーへデータ／サービスを移行する、または社内に戻す能力。プロバイダー間の相互運用性に関わる問題についても論じている。

運用ドメイン

従来のセキュリティ、ビジネス継続性、ディザスタリカバリ	セキュリティ、ビジネス継続性およびディザスタリカバリを実装するために現在使用されている運用プロセスや手続きに対して、クラウドコンピューティングがどのように影響を与えるか。クラウドコンピューティングに起こりうるリスクについて論じ、分析することに焦点を当てている。これは、より優れたエンタープライズリスク

	管理モデルに対する需要についての話し合いや議論が増えることを期待してのことである。さらに、このセクションでは、クラウドコンピューティングをセキュリティリスクの低下に活用できる箇所や、クラウドコンピューティングによりセキュリティリスクが増加してしまう箇所を特定するために役立つ内容にも触れている。
データセンター運用	プロバイダーのデータセンターのアーキテクチャや運用を評価する方法。主に、ユーザが、稼働中のサービスにとって有害である特性や、長期間の安定性の基本となる特性など、一般的なデータセンターの特性を認識することを助けることに焦点を当てている。
インシデント対応、通知および復旧	正確で適切なインシデントの発見、対応、通知および復旧。これは、プロバイダーとユーザの双方のレベルにおいて、正確なインシデントの処理と分析を行うために整備されるべき事項について扱っている。このドメインは、クラウドが、現在のインシデント処理プログラムにもたらす複雑性を理解する手助けとなる。
アプリケーションセキュリティ	クラウド上で稼働している、または開発されているアプリケーション・ソフトウエアの安全性の確保。これは、クラウド上に稼働するようにアプリケーションを移行または設計することが適当であるかについてや、適当である場合は、どのタイプのクラウドプラットフォーム(SaaS、PaaS または IaaS)が、最も適当であるか、などの項目を含む。クラウドに関する幾つかの特定のセキュリティ問題についても取り上げている。
暗号化と鍵管理	適切な暗号化用法と拡張性のある鍵管理の特定。このセクションは、規範的ではないが、それらが必要である理由や、リソースへのアクセスやデータを保護するにあたって発生する問題などに関する、多くの情報を含む。
アイデンティティとアクセス管理	アイデンティティ管理およびアクセス制御を提供するためのディレクトリサービスの

	活用。組織のアイデンティティをクラウドに拡張する際に遭遇する問題にフォーカスしている。このセクションは、クラウドベースのアイデンティティとアクセス管理(IAM)を行う組織の準備状況を評価することについて、洞察を提供する。
仮想化	クラウドコンピューティングにおける仮想化の利用。このドメインでは、マルチテナント、VM による分離、VM 共存、ハイパーバイザーの脆弱性等に関連したリスク項目を扱っている。このドメインでは、仮想化のあらゆる形に対する一般的なサーベイではなく、システム／ハードウェアの仮想化に関わるセキュリティの問題にフォーカスしている。

まとめ

クラウドアーキテクチャがどのようにセキュリティアーキテクチャに影響を与えるかを理解するための鍵は、一般的で簡潔な用語と、クラウドサービスとアーキテクチャを分解し、セキュリティと業務管理のモデル、リスク評価と管理のフレームワーク、そしてコンプライアンス基準にマッピングすることを可能にする一貫性のある定義・分類である。

クラウドコンピューティングを展開する際、アーキテクチャ、技術、プロセスおよび人的資源がどのように変化するか、あるいは現状のままであるかを理解することが重要である。クラウドサービスにおける上位レベルのアーキテクチャの関係性を明確に理解しなくては、より詳細な問題に合理的に対処することは不可能である。

このアーキテクチャ概要は、他の 12 のフォーカスエリアとともに、読者に対してクラウドコンピューティング環境のセキュリティを評価、運用、管理および統制するための確固とした基礎を提供する。

寄稿者: Glenn Brunette, Phil Cox, Carlo Espiritu, Christofer Hoff, Mike Kavis, Sitaraman Lakshminarayanan, Kathleen Lossau, Erik Peterson, Scott Matsumoto, Adrian Seccombe, Vern Williams, Richard Zhou

セクション II. クラウドにおけるガバナンス

ドメイン 2: ガバナンスとエンタープライズリスクマネジメント

クラウドコンピューティング環境における効果的なガバナンスとエンタープライズリスクマネジメントは、組織の総合的なコーポレートガバナンスにおける注意義務の一部として、十分に開発された情報セキュリティガバナンスプロセスから得られる。十分に開発された情報セキュリティガバナンスプロセスは、ビジネス上の拡張性があり、組織を越えて繰り返し可能であり、測定可能であり、持続可能であり、防御可能であり、継続的に改善され、継続的に費用対効果に優れている情報セキュリティ管理プログラムをもたらすはずである。

クラウドコンピューティングにおけるガバナンスとエンタープライズリスクマネジメントの基本的な問題は、効果的な情報セキュリティガバナンス、リスクマネジメントおよびコンプライアンスを維持するための適切な組織構造、プロセスおよびコントロールの識別と実装に関係する。また、組織は、どのようなクラウド展開モデルにおいても、クラウドコンピューティングサービスのプロバイダー、利用者およびサードパーティベンダーを含む情報サプライチェーンに対して、妥当な情報セキュリティを確保するべきである。

ガバナンスに関する推奨事項

√ 要求事項が継続的に満たされていることを保証するため、クラウドコンピューティングの利用により削減されたコストの一部は、プロバイダーのセキュリティ能力の監視の強化、セキュリティコントロールの適用、および継続的で詳細な評価や監査の実施に支払われるべきである。

√ クラウドコンピューティングサービスの利用者とプロバイダーは、サービスや展開モデルに関わらず堅牢な情報セキュリティガバナンスを開発すべきである。情報セキュリティガバナンスは、ビジネスのミッションと情報セキュリティプログラムをサポートするための、利用者とプロバイダーの合意目標を達成するよう、両者が連携して行うべきである。サービスモデルにより、(利用者およびプロバイダーのコントロール適応範囲に基づき)連携して実施する情報セキュリティガバナンスとリスクマネジメントで定義された役割と責任は調整されるかもしれない。一方、展開モデルは、(リスク評価に基づいた)説明責任と期待値を定義するかもしれない。

√ 利用者の組織は、利用を検討するプロバイダーに対するデューデリジェンスの一部として、特定の情報セキュリティコントロールおよびセキュリティガバナンスの構造とプロセスの検討を含めるべきである。プロバイダーのセキュリティガバナンスのプロセスと能力は、利用者の情報セキュリティマネジメントプロセスに対する十分性、成熟度および一貫性の観点で評価されるべきである。プロバイダーの情報セキュリティコントロールは、実証可能なリスクをベースとしたものであり、これらの管理プロセスを明確にサポートしているべきである。

√ 利用者とプロバイダーによる連携したガバナンス構造とプロセスは、サービス

展開の設計や開発の一部として、また、サービスのリスク評価とリスク管理プロトコルの一部として、必要に応じて識別するべきである。そして、それらはサービス契約に含まれるべきである。

√ セキュリティ要件が契約上履行されることを保証するために、セキュリティ部門は、サービスレベルアグリーメントや契約上の義務の制定に加わるべきである。

√ 情報セキュリティ管理のパフォーマンスと有効性を測定するための基準と規格は、クラウドに移行する前に確立されるべきである。組織は、最低でも現在採用している測定基準と、異なる(潜在的に互換性のない)測定基準を使用している可能性があるクラウドに運用を移行する場合に、測定基準がどのように変わるかについて理解し、記録すべきである。

√ 可能な限り、セキュリティの測定基準と規格(特に法律およびコンプライアンスの要件に関連するもの)を、サービスレベルアグリーメントと契約に含めるべきである。これらの規格と測定基準は、記録され実証可能である(監査可能である)べきである。

エンタープライズリスクマネジメントに関する推奨事項

あらゆる新しいビジネスプロセスと同様に、リスク管理のためのベストプラクティスに従うことは重要である。事例は、無難で一時的なデータ処理から極秘情報を扱うミッションクリティカルなビジネスプロセスまで多岐にわたるクラウドサービスの利用方法の中で、個別の利用方法に合ったものを利用するべきである。エンタープライズリスクマネジメントと情報リスク管理の本格的な議論は本ガイダンスの対象外だが、ここでは、既存のリスク管理プロセスに取り入れることができるいくつかのクラウド特有の推奨事項を記載する。

√ 多くのクラウドコンピューティングの展開において、インフラに対する物理的なコントロールが不足する中、リスク管理においては、サービスレベルアグリーメント、契約要求事項およびプロバイダーによるドキュメンテーションが、企業によって所有されている従来のインフラよりも大きな役割を持つ。

√ クラウドコンピューティングのオンデマンド・プロビジョニングやマルチテナントの性質により、従来の形式の監査や調査は利用できない、あるいは、変更されるかもしれない。たとえば、いくつかのプロバイダーは、脆弱性評価とペネトレーションテストを制限しており、また別のプロバイダーは、監査ログとアクティブ監視の可用性を制限している。もし、これらが社内ポリシーで必要とされている場合、代替の評価オプション、特定の契約上の例外事項、あるいはリスク管理要件に見合った代替のプロバイダーを求める必要があるかもしれない。

√ 組織にとって重要な機能に対するクラウドサービスの使用に関して、リスク管理アプローチは、資産の識別と調査、資産に対する脅威と脆弱性と潜在的なイ

ンパクトの識別と分析(リスクとインシデント・シナリオ)、イベント／シナリオの発生可能性の分析、経営者によって承認されたリスク許容レベルと基準および複数のオプション(コントロール、回避、委譲、許可)を持ったリスク対処プランの開発を含めるべきである。リスク対処プランの結果は、サービスアグリーメントに組み入れられるべきである。

√ プロバイダーと利用者の間のリスク評価アプローチは、インパクト分析基準と発生可能性の定義に一貫性を持たせることにより、一致しているべきである。利用者とプロバイダーは、クラウドサービスのためのリスクシナリオを共同で開発すべきである。これは、プロバイダーによる利用者のためのサービスのデザインと、利用者によるクラウドサービスリスクに対する評価に本質的に関連したものであるべきである。

√ 資産在庫は、クラウドサービスでサポートされる資産としてプロバイダーのコントロール下に置かれる。資産の分類や調査の体系は、利用者とプロバイダーの間で一貫しているべきである。

√ ベンダーだけでなく、サービスもリスク評価の対象であるべきである。クラウドサービスの利用および利用される特定のサービスや展開モデルは、組織のリスク管理目標およびビジネス目標と一致しているべきである。

√ プロバイダーがサービスに関して包括的で有効なリスク管理プロセスの実証を行うことができない場合、利用者は、ベンダーの利用および潜在的なリスク管理のギャップを補うための自身の能力を慎重に評価すべきである。

√ クラウドサービスの利用者は、利用者自身の管理者がクラウドサービスに関するリスク許容度を定義したかどうか、およびクラウドサービスを利用することによる残存リスクを受容したかどうかを確認するべきである。

情報リスク管理に関する推奨事項

情報リスク管理は、リスク・エクスポージャーとそれを管理する能力を、データ所有者のリスク許容度に合わせて調整する行為である。このように、情報資産の機密性、完全性および可用性を保護するように設計された情報技術リソースの意思決定を支援するための主要な手段である。

√ IRM を評価するリスク管理フレームワークモデルおよび IRM モデルの有効性を評価するための成熟度モデルを採用する。

√ 情報リスクの意思決定(たとえば、情報の利用、アクセス制御、セキュリティコントロール、場所など)を通知するために必要となるデータを収集するため、適切な契約要件と技術コントロールを確立する。

√ クラウドコンピューティングプロジェクトのための要件を開発する前に、リスク・エクスポージャーを決定するためのプロセスを採用する。エクスポージャーと管理能力を理解するために必要となる情報のカテゴリは一般的なものだが、

集められた実際の証拠の測定基準は、クラウドコンピューティングの SPI モデルの性質に特有のものであり、サービスの観点から収集可能なものに特定される。

√ SaaS を利用するとき、圧倒的多数の情報はサービスプロバイダーによって提供されなければならない。 組織は、SaaS サービスの契約上の義務に分析情報を集めるプロセスを構築するべきである。

√ PaaS を利用するときには、上記の SaaS のような情報収集を組み込み、可能であればコントロールから情報を展開し収集する能力およびコントロールの有効性をテストするための契約条項の作成も含める。

√ IaaS サービスプロバイダーを利用するときには、リスク分析に必要な情報に関する情報の透明性を契約に組み込む。

√ クラウドサービスプロバイダーは、利用者が自らの情報リスク管理要件の実装を支援するための測定基準とコントロールを情報リスク管理の導入に含めるべきである。

サードパーティの管理に関する推奨事項

√ 利用者は、クラウドサービスとセキュリティをサプライ・チェーンのセキュリティ問題として見るべきである。これは、プロバイダーのサプライ・チェーン(サービスプロバイダーとの関係と依存関係)を可能な限り調べ、評価することを意味する。また、これはプロバイダー自身のサードパーティの管理を調べることも意味する。

√ サードパーティサービスプロバイダーの評価は、プロバイダーのインシデント管理、ビジネス継続性、ディザスタリカバリ・ポリシー、プロセスおよび手順を対象とするべきであり、コロケーションとバックアップ施設に対する検討も含むべきである。これには、プロバイダーによる自身のポリシーや手順に従っているかどうかについての内部評価の検討や、この領域におけるコントロールのパフォーマンスや効果に関して意味のある情報を提供するための測定基準に対する評価を含むべきである。

√ 利用者のビジネス継続性とディザスタリカバリ・プランは、プロバイダーのサービスを失った場合、ならびにプロバイダーがサードパーティサービスおよびサードパーティに依存する能力を失った場合のシナリオを含むべきである。この部分のプランのテストは、クラウドプロバイダーと連携して行うべきである。

√ プロバイダーの情報セキュリティガバナンス、リスク管理、コンプライアンス構造およびプロセスは、以下のように包括的に評価されるべきである:

- 施設とサービスのリスクに関する評価やコントロールの不備に関する監査がどのように行われているか、またその頻度はどの程度か、さらにコントロールの不備がどのように緩和されているかに関して明確な文書を

求める。
- プロバイダーが、サービスと情報セキュリティの重要な成功要因が何であると考えているか、主要なパフォーマンス指標(KPI)は何であるか、およびこれらがITサービスと情報セキュリティ管理と比較してどのように測定されるかについて説明を要求する。
- プロバイダーの法律、規制、産業、契約における要件の把握、評価、およびコミュニケーション・プロセスの包括性を検討する。
- 役割、実施責任および説明責任を決定するために、完全な契約または利用規約によるデューデリジェンスを実施する。ローカルの契約規定と外国あるいは州外の法的強制力の評価を含む法的な検討を実施する。
- デューデリジェンス要件が、クラウドプロバイダーとの関係におけるすべての重要な側面を包含しているかどうかを特定する。たとえば、プロバイダーの財政状態、評判(たとえば、リファレンスチェック)、コントロール、主要人員、ディザスタリカバリ・プランとテスト、保険、コミュニケーション能力、下請契約者の使用などである。

寄稿者： Jim Arlen, Don Blumenthal, Nadeem Bukhari, Alex Hutton, Michael Johnson, M
S Prasad, Patrick Sullivan

ドメイン 3: 法律と電子証拠開示

クラウドコンピューティングは、組織と情報との関係に、サードパーティ、つまりクラウドサービスプロバイダーを取り込み、新しい力学を作り出している。このことは、さまざまな情報管理シナリオに対して法律がどのように適用されるかを理解する上で新しい挑戦を生み出している。

クラウドコンピューティングに関連した法的な問題の完全な分析は、機能面、法制面、そして契約面での検討を必要とする。

- 機能面には、参加者や利害関係者に対してクラウドコンピューティングにおける機能とサービスがどのような法的意味を有するかについて特定することが含まれている。
- 法制面には、政府がクラウドコンピューティングサービス、利害関係者および関連するデータ資産に影響を与える法律や規則を管理する方法が含まれている。
- 契約面には、クラウドコンピューティング環境における利害関係者が法律やセキュリティの問題を扱い、対処できるような契約構造、取引条件および実施メカニズムが含まれている。

一般に、クラウドコンピューティングは、3 つの方法で従来のアウトソーシングと区別できる。それは、サービスの時間(オンデマンドで断続的)、サービスプロバイダーのアイデンティティの匿名性、関連するサーバの場所の匿名性である。特に、IaaS と PaaS を考慮する場合、多くの組織化、構成およびソフトウェア開発が利用者によって行われる。したがって、多くの責任をクラウドプロバイダーに移譲することができない。

最近の世界中の法制上あるいは管理上の要件に対するコンプライアンスは、弁護士や技術専門家の間の強い共同作業を必要としている。これは、クラウドコンピューティングにおいて特にあてはまる。それは、従来の社内あるいはアウトソースされたインフラと比べて、クラウドの分散された性質により作られた新しい領域に対する法的リスクの可能性のためである。

米国とヨーロッパ連合(EU)における多数のコンプライアンスの法律と規制は、企業に対して、下請契約者に責任を転嫁するか、あるいは、契約により下請契約者に責任を負わせることを要求している。。

裁判所は今、情報セキュリティ管理サービスが、デジタル情報を証拠として認められるどうかを決定する上で非常に重要であることを理解し始めている。これは、従来の IT インフラの問題でもあるが、クラウドにおいては確立された法的な歴史が不足しているため、クラウドコンピューティングにおいては特に問題である。

推奨事項

√ 利用者とクラウドプロバイダーは、訴訟時の主導権、訴訟開示の検索、誰が鑑定を行うかなど、電子証拠開示に関するお互いの役割と責任について相互に理

解しなければならない。

√ クラウドプロバイダーは、データ(プライマリーデータならびにメタデータやログファイルなどのセカンダリーデータを含む)を正確で信頼できる状態で保管する、という利用者からの要求に対して、情報セキュリティシステムが対応できるということを保証するべきである。

√ クラウドサービスプロバイダーが保管するデータは、そのオリジナルの所有者あるいは管理人の管理下にある場合と同様の保護を受けなければならない。

√ 契約交渉において予期できる関係の終了、または予期できない関係の終了や、資産の適切な回収または安全な処分のための計画を立てる。

√ 契約前のデューデリジェンス、契約期間交渉、契約後の監視、契約終了およびデータ管理の移行は、クラウドサービスクライアントに必要な注意義務の要素である。

√ 国境を越えたデータの流れを制限する地域法へのコンプライアンスを確実にするために、クラウドサービスプロバイダーがどこでデータをホスティングするかを知る必要がある。

√ クラウドコンピューティングサービスを利用する企業は、従業員あるいはクライアントの個人データ、その他の企業の知的財産資産の管理人として、データの所有権を、オリジナルの、信頼できるフォーマットで保有し続けられることを確保するべきである。

√ データ漏洩の疑惑のような多くのセキュリティの問題は、クラウドサービスプロバイダーと利用者の双方の合意を明示しているサービス契約における特定の条項に記載されていなければならない。

√ クラウドサービスプロバイダーと利用者は、召喚、送達およびその他の法的な要求に応じるための統一されたプロセスを持つべきである。

√ クラウドサービス契約は、クラウドサービスの利用者や指定されたサードパーティに対して、サービスプロバイダーのパフォーマンスの監視と、システムの脆弱性に対するテストを行うことを認めなければならない。

√ クラウドサービス契約の当事者は、その契約上の関係が終了した後に、利用者のデータのリカバリに関して予測される問題を見込んでおくようにすべきである。

寄稿者: Tanya Forsheit, Scott Giordano, Francoise Gilbert, David Jackson, Peter McLaughlin, Jean Pawluk, Jeffrey Ritter

ドメイン 4: コンプライアンスと監査

クラウドコンピューティングがシステムまたはビジネスプロセス全体のアウトソースを行うための、実行可能でコスト効果の高い方法として発展する中、組織のセキュリティポリシーやさまざまな規制や法律の要件へのコンプライアンスは、実現が難しく、監査役や調査者への実証は更に困難になるだろう。

組織が応じなければならない情報技術に関わる多くの規制の中で、クラウドコンピューティングを考慮して書かれたものは僅かである。監査役や調査者は、クラウドコンピューティング一般的または特定のクラウドサービスについて詳しくない可能性がある。そのような事情から、クラウド利用者は以下の点を理解するべきである:

- 特定のクラウドサービス利用における規制適用性
- クラウドサービスプロバイダーと利用者の間のコンプライアンス責任の紊乱
- コンプライアンスに必要となる証拠を作成するクラウドサービスプロバイダーの能力
- クラウドサービスプロバイダーと監査役／調査者の間のギャップを塞ぐためのクラウド利用者の役割

推奨事項

√ 法務および契約チームを関与させる。サービスに関するクラウドプロバイダーの標準条項は、あなたのコンプライアンス要件に対応していないかもしれない。したがって、初期の段階から法務および契約に関わる人を関与させて、クラウドサービス契約規定がコンプライアンスと監査義務に対して適切であることを確認することは有益である。

√ 監査をする権利の契約条項を入れる。クラウドと規制環境の両方の動的な性質を考慮すると、利用者は、しばしばクラウドサービスプロバイダーを監査ことが必要になるだろう。特に、利用者が法規制のコンプライアンス責任を持っているサービスでクラウドプロバイダーを使用する場合は、できる限り監査をする権利の契約条項を入れるべきである。時間がたつにつれて、この権利の必要性は減少し、多くの場合適切なクラウドプロバイダーの認証に置き換えられていくだろう。これは、このセクションで後述する ISO／IEC27001 認証のための推奨事項と関連している。

√ コンプライアンスの範囲を分析する。組織が前提としているコンプライアンス規定が、あるアプリケーションとデータにおけるクラウドサービスの利用により影響を受けるかどうかを決定する。

√ データセキュリティに対する規制の影響を分析する。クラウドコンピューティングサービスの潜在的なエンドユーザは、どのアプリケーションとデータをクラウドサービスに移行しようとしているか、そしてそれらがどの程度コンプライアンス規定の対象範囲内にあるかを考慮するべきである。

- √ 関連パートナーとサービスプロバイダーを見直す。これは、サービスプロバイダーとの関係がコンプライアンスに否定的な影響を与えないようにするための一般的なガイダンスである。どのサービスプロバイダーがコンプライアンス規則対象のデータを処理しているかを評価し、次に、それらのサービスプロバイダーによって提供されたセキュリティコントロールを評価することが必要である。いくつかのコンプライアンス規則には、サードパーティベンダーのリスクを評価し管理することに関する特定の規定がある。 非クラウド IT やビジネスサービスと同様に、組織はどのクラウドビジネスパートナーがコンプライアンス規則対象のデータを処理しているかを理解する必要がある。

- √ 契約上のデータ保護責任と関連する契約を理解する。利用者あるいはクラウドサービスプロバイダーのどちらにセキュリティコントロールを展開する責任があるかは、ある程度クラウドサービスモデルによって決まる。IaaS 展開シナリオでは､利用者は SaaS シナリオより大きなコントロールと責任を持っている。セキュリティコントロールの観点からは、これは、IaaS 利用者が法規制のコンプライアンスのために多くのセキュリティコントロールを展開しなければならないことを意味する。SaaS シナリオにおいては、クラウドサービスプロバイダーが、必要なコントロールを提供しなければならない。契約上の観点からは、具体的な要件を理解し、クラウドサービス契約とサービスレベルアグリーメントがそれらに適切に対応していることを確認することは重要である。

- √ プロバイダーのインフラに対する規制の影響を分析する。インフラの領域において、クラウドサービスへの移行は慎重な分析を必要とする。いくつかの法的な要求事項は、特定のクラウドサービスのタイプでは実現が難しい、あるいは不可能なコントロールを規定している。

- √ ポリシーと手順における規制の影響を分析する。データとサービスをクラウドサービスに移行することは、ポリシーと手順に影響を与える可能性が高い。利用者は、規制に関連するポリシーと手順のうちどれを変更しなければならないかを評価すべきである。影響を与えられるポリシーと手順の例は、活動報告、ロギング、データ保有、インシデントレスポンス、コントロールテスト、プライバシーポリシーを含む。

- √ それぞれの要件がどのように満たされているかについて証拠を用意する。多くのコンプライアンス規制と要件に対して、コンプライアンスの証拠を集めることは課題である。クラウドサービスの利用者は、監査ログや活動報告、システム構成のコピー、変更管理レポート、その他のテスト手続の結果を含むコンプライアンス証拠を集めて保存するためのプロセスを開発すべきである。クラウドサービスモデルによっては、クラウドプロバイダーがこの情報の多くを提供する必要がある。

- √ 監査人の資格と選択について、多くの監査人や調査者はクラウドおよび仮想化の課題を熟知していない可能性がある。多くの場合、組織は監査人やセキュリティ調査者を選ぶ際に発言権がないが、もし、意見を言うことができるのであれば､”クラウドに関する認識が高い” 監査人を選定することを推奨する。IaaS、

PaaS、および SaaS という用語を知っているかどうか尋ねることは良い出発点である。

√ プロバイダーは、最低でも SAS 70 Type II を持っているべきである。SAS70 TypeII は、監査人や調査者にとって認識可能な評価基準を提供するが、この監査は、コントロールが記録されたとおり実施されていることを保証するだけであるため、SAS 70 監査の範囲とこれらのコントロールがあなたの要件を満たすかどうかを理解することは同様に重要である。

√ クラウドプロバイダーの ISO／IEC27001／27002 ロードマップを確認する。ミッションクリティカルなサービスを提供することを模索しているクラウドプロバイダーは、情報セキュリティ管理システムとして ISO／IEC27001 認証を採用すべきである。プロバイダーが、ISO／IEC 27001 認証を取得していない場合は、ISO27002 との整合性を示すべきである。

√ ISO／IEC27001／27002 の対象範囲について、Cloud Security Alliance は重要な認証基準が対象範囲から除外されないことを確実にするため、ISO／IEC 27001 認証を取得したクラウドプロバイダーに歩調を合わせるよう業界に呼びかけている。

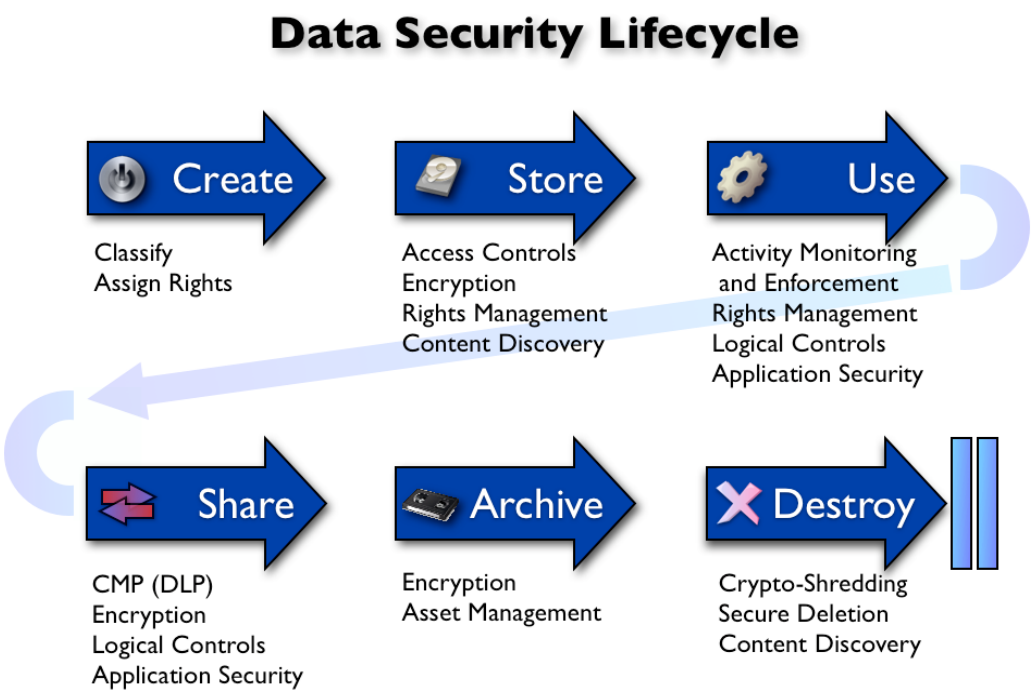
寄稿者: Nadeem Bukhari, Anton Chuvakin, Peter Gregory, Jim Hietala, Greg Kane, Patrick Sullivan

ドメイン 5: 情報ライフサイクルマネジメント

情報セキュリティの主な目標の 1 つは、システムとアプリケーションを動かしている基本的なデータを保護することである。クラウドコンピューティングへ移行するにつれて、データを保護するための従来の方法は、クラウドベースのアーキテクチャに課題を突きつけられている。弾力性、マルチテナント、新しい物理的および論理的アーキテクチャおよび抽象化されたコントロールは、新しいデータセキュリティ戦略を必要とする。また、多くのクラウド展開において、ほんの数年前には思いもよらなかったような方法で、データを外部、あるいはパブリックの環境に移している。

情報ライフサイクルマネジメント

データセキュリティライフサイクルは、セキュリティ関係者の異なったニーズを反映して、情報ライフサイクルマネジメントとは違っている。データセキュリティライフサイクルは、以下の 6 つのフェーズからできている:



クラウドにおけるデータライフサイクルセキュリティに関する主な課題は、以下を含む:

データセキュリティ　機密性、完全性、可用性、信頼性、権限付与、認証、否認防止。

データの場所　すべてのコピーとバックアップを含むデータが、契約、サービスレベ

ルアグリーメントおよび／または規制によって許可された地理的な場所だけに保存されるということが保証されていなければならない。たとえば、電子健診記録を保存するためにヨーロッパ連合において命じられている”コンプライアント・ストレージ”の使用は、データ所有者とクラウドサービスプロバイダーに追加された課題である。

データの残留性あるいは持続性　データは、”破壊された”と判断されるために効果的かつ完全に削除されなければならない。したがって、効果的かつ完全にクラウド上のデータの位置を特定する技術、データを削除／破壊する技術およびデータが完全に削除され復元できない状態になったことを保証する技術が利用可能であり、要求に応じて利用されなければならない。

他のクラウド利用者とのデータの結合　データ、特に極秘／機密データは、利用中、保管中、移動中におけるコントロールが保証されない限り、他の利用者のデータと混合させてはならない。データを混ぜるまたは結合させることは、データセキュリティや地理的な場所についての懸念が浮上した際に問題となる。

リカバリと復元のためのデータバックアップとリカバリスキーム　データ損失、予期しないデータの上書きおよび破壊を防ぐために、データは利用可能で、かつ、クラウドのためのデータバックアップやリカバリスキームは整備され、有効でなければならない。クラウドベースのデータは、バックアップされていてリカバリ可能であると想定してはいけない。

データ開示　法制度は電子情報開示を意識していることから、クラウドサービスプロバイダーやデータ所有者は、法律や規制当局に対して、データを開示することおよび要求されたデータがすべて回収されたことを保証することに重点的に取り組む必要がある。クラウド環境においては、その質問に答えることは非常に難しく、要求された際には管理上、技術上および法律上のコントロールを必要とする。

データ集約と推定　クラウドにデータを置くことにより、機密情報や極秘情報の侵害につながる可能性がある、データ集約と推定に関する追加の懸念が発生する。したがって、データが混合され、および／または集約された結果、保護データ(たとえば、名前や医療情報匿名化されているが、他の情報と照合すると個人が特定可能な医療記録)が漏れた場合、データ所有者およびデータ利害関係者が、データは巧妙な”侵害”から保護されていると確信できるように、実務が機能しなければならない。

推奨事項

- √ 完全性はどのように維持されるか、および完全性の侵害はどのように検知され、利用者に報告されるのかを理解する。この推奨事項は、適切である場合は、機密性についても適用される。

- √ クラウドコンピューティングプロバイダーは、サービスレベルアグリーメントで述べられているとおりに、セキュリティの取組みと手順に関して完全な情報開示(すなわち”透明性”)を提供していることをデータ所有者に保証しなければならない。

- √ データのライフサイクルにわたって使用されるすべてのコントロールについて、必ず明確に識別し、各コントロールについて、データ所有者とクラウドサービスプロバイダーのどちらに責任があるかを明確にする。

- √ データの所在地を知るという基本方針を維持する。ストレージの地理的な場所を知ることができるようにしておき、これをサービスレベルアグリーメントと契約において規定する。国の位置の制限に関する適切なコントロールが定義され、実行されることを確保する。

- √ サードパーティあるいは政府機関によってストレージが押収される可能性がある状況について理解しておく。クラウドプロバイダーとのサービスレベルアグリーメントにおいて、データ所有者の情報が押収された、あるいは、押収されるということが、(可能であれば事前に)データ所有者に通知されることを確かめる。

- √ クラウドコンピューティングサービスプロバイダーに対して、召喚あるいは電子証拠開示令状が出される場合がある。このような場合、プロバイダーが利用者のデータを保管しているのであれば、クラウドサービスプロバイダーは、データ所有者のデータの公開が強制されていることを、データ所有者に知らせなければならない。

- √ データ所有者とクラウドサービスプロバイダーとの契約に、サービスペナルティのシステムを含めるべきである。特に、州や国際データ侵害法(California Senate Bill 1386 あるいは新しい HIPAA データ侵害規則)の影響下にあるデータは、クラウドサービスプロバイダーによって保護されるべきである。

- √ 誰がデータにアクセスすべきであるか、アクセスすべき人にはどのような権利と特権を与えるか、およびこれらのアクセス権をどのような条件のもとで提供するかを決定することは、データ所有者の責任である。データ所有者は、データ所有者の従業員とクラウドサービスプロバイダーの両方に対して”デフォルトはすべて禁止する”というポリシーを維持すべきである。

- √ クラウドサービスプロバイダーは、基本的な方針として、データへのアクセスの禁止を保証する契約上の文言を提供するべきである(すなわち、”デフォルトはすべて禁止する”)。これは、データ所有者の従業員と利用者に対してよりもクラウドサービスの従業員とその利用者に対して特に適用する。

- √ データ所有者の責任は、データ分類を定義、識別することである。データ分類に基づくデータ所有者のアクセス要件を実施するのは、クラウドサービスプロバイダーの責任である。そのような責任は、契約に盛り込まれるべきであり、コンプライアンス上実施され監査されるべきである。

- √ 利用者が情報を開示せざるを得ないとき、データ汚染が起こってはならない。すなわち、データ所有者は、保全命令、召喚、電子証拠開示などに必要となるすべてのデータが完全であり適切に開示されていることを保証する必要がある

だけでなく、他のどのようなデータも影響を受けていないことを保証しなければならない。

√ “内のデータを暗号化する。保管されているデータおよび移動中のデータを暗号化する(参照 ドメイン 11、暗号化および鍵管理)。

√ IT アーキテクチャと抽象化レイヤを通して、信頼境界を特定する。データの不当な開示、変更および破壊を防ぐため、必要であり、かつ適切なセーフガードが講じられている場合においてのみ、サブシステムが信頼境界を越えられるようにする。

√ 利用者を他の利用者から分離するために、プロバイダーがどのような区画化技術を使用しているか理解する。プロバイダーは、提供するサービスのタイプと数に応じてさまざまな方法を使用している可能性がある。

√ データ開示のためにデータセットの”内部”を見ようとする際の、クラウドプロバイダーのデータ検索能力と限界を理解する。

√ 暗号化が、マルチテナントのストレージにおいてどのように管理されているか理解する。すべてのデータ所有者に対して 1 個の鍵であるのか、1 データ所有者あたり 1 個の鍵であるのか、あるいは 1 データ所有者あたり複数の鍵があるのか？異なったデータ所有者が、同じ暗号化鍵を持つことを防ぐためのシステムはあるのか？

√ データ所有者は、クラウドサービスプロバイダーに対して、データ所有者のバックアップデータが他のクラウドサービス利用者のデータと混在しないことを保証するように要求すべきである。

√ クラウドプロバイダーのストレージ破棄プロセスを理解する。データ破壊は、マルチテナント環境では非常に難しい。クラウドサービスプロバイダーは、ストレージが再利用、廃棄および認められているアプリケーション、プロセス、利用者以外からアクセスされる際に、データを読み取り不可能な状態にするための強力なストレージ暗号化を使用するべきである。

√ データの保存および破棄のスケジューリングは、データ所有者の責任である。要求に応じてすべての場所のすべてのデータを破棄することはクラウドサービスプロバイダーの責任である。特に、データ構造の中およびメディア上のスラックにあるすべてのデータを破棄することを特に重要視する必要がある。可能であれば、データ所有者はこの実務を強制し、監査すべきである。

√ 情報の論理的な分離と保護のためのコントロールを理解する。

√ 委託されたデータについて、固有のプライバシーに関する制限事項を理解する。情報をクラウドプロバイダーに預ける前に、あなたは、利用しているクラウドプロバイダーを特定のパートナーとして指定する必要があるかもしれない。

- √ データ保存と破壊に関するクラウドプロバイダーのポリシーとプロセスを理解し、それらが社内の組織的なポリシーと比較してどうであるかを理解する。クラウドプロバイダーにとって、データ保存の保証を示すことは簡単であるかもしれないが、データの破壊については、非常に難しい可能性があることに注意する。

- √ データ漏洩が真剣に受け止められていることを保証するために、クラウドプロバイダーが支払うべきペナルティを交渉する。現実的であれば、利用者はプロバイダーとの契約の一部としてすべての漏洩コストを取り戻すことを模索すべきである。現実的でない場合、利用者は、漏洩コストを取り戻すために保険などの他のリスク移転手段を模索すべきである。

- √ 定期的にバックアップとリカバリのテストを実施し、論理的な分離とコントロールが有効であることを保証する。

- √ クラウドサービスプロバイダーの人員に対するコントロールが実施され、論理的な職務分離が提供されることを確保する。

- √ マルチテナントストレージにおいて、暗号化がどのように管理されているかを理解する。すべての利用者に対して 1 つの鍵であるのか、1 利用者あたり 1 つの鍵であるのか、あるいは 1 利用者あたり複数の鍵があるのか？

ILM フェーズ別のデータセキュリティ推奨事項

本ガイダンスにおける一般的な推奨事項の一部は、他の特定のコントロールと同様に、それぞれのライフサイクルフェーズの内容に沿ってリストされている。クラウドサービスモデル(SaaS、PaaS、IaaS)によって、いくつかの推奨事項は利用者によって実装される必要があり、その他の提案はクラウドプロバイダーによって実装されなければならないことに注意すること。

作成時

- √ 利用可能なデータラベリングと分類の能力を識別する。

- √ エンタープライズデジタル著作権管理(Enterprise Digital Rights Management)は選択肢の一つであるかもしれない。

- √ データのユーザ・タグ付けは、Web 2.0 環境では一般的になりつつあり、データを分類するために利用できる。

保存時

- √ ファイルシステム、DBMS、ドキュメント管理システムなどの中で利用可能なアクセス制御を確認する。

- √ 電子メール、ネットワーク・トランスポート、データベース、ファイルおよびファイルシステムなどのための暗号化ソリューションを確認する。

√ コンテント・ディスカバリ・ツール（しばしば DLP、あるいは Data Loss Prevention と呼ばれる)は、コントロールを必要とするデータを特定し、監査するのに役立てることができる。

利用時

√ ログファイルやエージェントベースのツールを通したアクティビティの監視と制御を確認する。

√ アプリケーションロジックを確認する。

√ DBMS ソリューションの中のオブジェクトレベルコントロールを確認する。

共有時

√ ログファイルやエージェントベースのツールを通したアクティビティの監視と制御を確認する。

√ アプリケーションロジックを確認する。

√ DBMS ソリューションの中のオブジェクトレベルコントロールを確認する。

√ ファイルシステム、DBMS、ドキュメント管理システムなどの中で利用可能なアクセス制御を確認する。

√ メール、ネットワーク通信、データベース、ファイルおよびファイルシステムなどにおける暗号化を確認する。

√ コンテントベースのデータ保護を確認する。

アーカイブ時

√ テープバックアップやその他の長期記憶媒体などにおける暗号化を確認する。

√ 資産管理とトラッキングが行われているか確認する。

破壊時

√ 暗号化シュレディング(Crypto-shredding): 暗号化されたデータに関連したすべての主要な資料の破壊を確認する。

√ ディスク・ワイピングおよび関連した技術を通した安全な削除を確認する。

√ 物理メディアに対する消磁のような物理的な破壊を確認する。

√ 破壊プロセスを確認するための証拠開示手続きを確認する。

寄稿者: Richard Austin, Ernie Hayden, Geir Arild Engh-Hellesvik, Wing Ko, Sergio Loureiro, Jesus Luna Garcia, Rich Mogull, Jeff Reich

ドメイン 6: 移植性と相互運用性

組織は、将来プロバイダーを変えなければならなくなる可能性があることを念頭に置いた上で、クラウドにアプローチしなければならない。あらゆるクラウドプログラムに関し、移植性と相互運用性は、リスク管理とセキュリティ保証の重要な一部として考慮されなければならない。

大きなクラウドプロバイダーは、クラウド上に地理的に冗長性を持たせることができ、うまくいけば単独のプロバイダーで高可用性を提供することができる。それでもなお、最悪のシナリオが起こった場合の影響を最小にするため、基本的なビジネス継続計画を行うことを推奨する。いろいろな会社が、将来、以下に例示するさまざまな理由から、突然クラウドサービスプロバイダーを変更しなければならない緊急の必要性にせまられることになる。

- 契約更新時において、容認できないレベルのコストの増大。
- プロバイダーの営業活動の停止。
- プロバイダーが、許容できる移行計画なしに突然使用中の 1 つ以上のサービスを止める。
- 主要なパフォーマンス指標やサービスレベルアグリーメントの未達成など、許容できないサービス品質の低下。
- クラウド利用者とプロバイダーのビジネス上の紛争。

アーキテクチャにいくつかの簡単な配慮を施しておくことで、このようなシナリオが発生した場合の損害を最小限に抑えることができる。ただし、これらの問題を扱うための手段はクラウドサービスのタイプに依存する。

Software as a Service(SaaS)においては、定義上、クラウド利用者は、新しいソフトウェアアプリケーションを古いもので代用することになる。したがって、アプリケーションの移植性に対してではなく、古いアプリケーションが提供するセキュリティ機能の維持または拡張、およびデータの正常な移行に対して焦点が当てられるべきである。

Platform as a Service(PaaS)においては、移植性を実現するためには、ある程度のアプリケーションの修正が必要となることが予想される。焦点は、アプリケーションの書き換えを最低限にしつつ、セキュリティコントロールを維持、または拡張し、正常なデータの移行を実現することである。

Infrastructure as a Service(IaaS)においては、アプリケーションとデータの両方が新しいクラウドプロバイダーに移行し、稼働できるということに焦点および期待がある。

相互運用性の規格が一般的に不足しており、また、これらの規格に対して市場からの圧力が不足しているため、クラウドプロバイダー間の移行は手間のかかる、手作業によるプロセスになるかもしれない。セキュリティの観点からの主な関心は、環境を変えている間、セキュリティコントロールの一貫性を維持することである。

推奨事項

すべてのクラウドソリューション向け:

- √ クラウドプロバイダーの変更は、事実上すべてのケースにおいて、少なくとも 1 つの当事者にとって否定的なビジネス取引となるものであり、既存クラウドプロバイダーから予期しない否定的な反応を引き起こす可能性がある。これは、ドメイン 3 に概説されている契約上のプロセス、ドメイン 7 で概説されているビジネス継続性プログラムおよびドメイン 2 の全体的なガバナンスの一部として計画されなければならない。

- √ クラウドプロバイダーによってホスティングされるデータセットのサイズを理解すること。データの全体の大きさは、移行の際に、サービスの中断、あるいは予想を超える移行期間の長期化を引き起こすかもしれない。多くの利用者は、大きなデータセットに関しては、宅急便でハードドライブを送る方が、電子的に送信するよりも早いことを発見している。

- √ 内部監査をサポートし、新しいプロバイダーへの移行を容易にするために、個々のコンポーネントのセキュリティコントロールのセキュリティアーキテクチャと設定を文書化する。

IaaS クラウドソリューション向け:

- √ どのように仮想マシン(”VM”という)のイメージを獲得し、新しいクラウドプロバイダーに移植できるかを理解する。新しいクラウドプロバイダーは、異なった仮想化技術を使用している可能性がある。

- √ VM 環境におけるプロバイダー固有の拡張機能を特定し、排除(あるいは少なくとも文書化)する。

- √ クラウドサービスプロバイダーからアプリケーションが移植された後に、VM イメージの適切なデプロビジョニングを実施するためにどのような施策が取らているかを理解する。

- √ ディスクとストレージ装置の廃棄において実施されている施策を理解する。

- √ アプリケーション／データの移行の前に、ハードウェア／プラットフォームへの依存性を理解する。

- √ 既存クラウドプロバイダーに対して、システムログ、トレースログ、アクセスログおよび支払い記録へのアクセスの許可を求める。

- √ もし、新しいサービスの一部または全体が既存のサービスより劣ると判明した場合、既存クラウドプロバイダーのサービスを再開、または延長するための選択肢を明確にする。

√ 新しいプロバイダーには互換性がない、あるいは実装されていないような管理者レベルの機能、インタフェースまたは API があるかどうか特定する。

PaaS クラウドソリューション向け:

√ 可能な限り、標準のシンタックス、オープン API およびオープンスタンダードであるプラットフォームコンポーネントを使用する。

√ 安全なデータ転送、バックアップおよびリストアのために、どのようなツールが利用可能であるかを理解する。

√ PaaS プロバイダーに固有のアプリケーションコンポーネントとモジュールを理解および文書化し、独自のモジュールへの直接的なアクセスを最小化するため、抽象化レイヤを持ったアプリケーションアーキテクチャを開発する。

√ 監視、ログの取得および監査のような基本サービスが、どのように新しいベンダーに移行されるかを理解する。

√ 既存クラウドプロバイダーによって提供されているコントロール機能を理解し、それらが新しいプロバイダーにどのように移行されるかを理解する。

√ 新しいプラットフォームに移行する際、それがアプリケーションのパフォーマンスと可用性に与える影響、およびそれらの影響をどのように測定するかを理解する。

√ サービスやアプリケーションが正しく動作していることを確認するために、移行の前後にどのようにテストを行うかを理解する。テスティングにおけるプロバイダーとユーザの両者の責任を明確化し、文書化する。

SaaS ソリューション向け:

√ 使用可能なフォーマットで、定期的なデータ抽出とバックアップを SaaS プロバイダーを介さずに実施する。

√ メタデータが保存および移行可能かどうか理解する。

√ 実装されているどのようなカスタムツールも、再度開発されなければならないか、新しいベンダーから提供されなければならないことを理解する。

√ 既存のプロバイダーと新しいプロバイダー間でのコントロールの有効性について一貫性を確保する。

√ 法律あるいはコンプライアンスに必要とされる可能性があるログ、アクセス記録、その他の付属情報のバックアップやコピーの移行可能性を確保する。

- √ 管理、監視、レポート用インタフェースおよびそれらの環境間における統合について理解する。
- √ 新しいベンダーから、移行の前にアプリケーションをテストし、評価するための機能は提供されるか？

寄稿者： Warren Axelrod, Aradhna Chetal, Arthur Hedge, Dennis Hurst, Sam Johnston, Scott Morrison, Adam Munter, Michael Sutton, Joe Wallace

セクション III. クラウドにおける運用

ドメイン 7: 従来のセキュリティ、ビジネス継続性および災害復旧

従来の物理的なセキュリティ、ビジネス継続計画(BCP)および災害復旧(DR)から生じた一連の知識は、クラウドコンピューティングとも関連を持ってしている。クラウドコンピューティングの急速な変化と透明性の不足により、従来のセキュリティ、BCP および DR の専門家は､選ばれたクラウドサービスプロバイダーの審査および監視に引き続き従事することが求められる。

私たちの課題は、積極的で力強い方法で、リスクの識別や相互依存性の認識、インテグレーションの実施、リソースの活用に共同で取り組むことである。 クラウドコンピューティングと付随するインフラは、特定のセキュリティ問題を軽減するが、他のセキュリティ問題は増大させる可能性があり、セキュリティの必要性は決してなくなることはない。ビジネスと技術は大きく転換し続けるが、従来のセキュリティ原則は依然として残る。

推奨事項

- √ データが中央に集中することにより、クラウドサービスプロバイダーの内部関係者による不正使用のリスクが重大な懸念となることを念頭に入れておく。
- √ クラウドサービスプロバイダーは、セキュリティのベースラインとして、あらゆる利用者の中で最も厳しい要件を採用することを検討するべきである。厳しいセキュリティ施策は、顧客に否定的な影響を与えない範囲であれば、リスクの軽減と、さまざまな分野の懸念事項について利用者が行う調査の軽減により、長期的には費用対効果が高いことが判明するだろう。
- √ プロバイダーは、職務に関する強固な区画化を行い、従業員の素性調査を実行し、秘密保持契約を要求／強制し、従業員の利用者に関する知識を、職務の実行に必要不可欠な範囲に制限するべきである。
- √ 利用者は、可能な場合クラウドサービスプロバイダー施設の立ち入り点検を実行するべきである。
- √ 利用者は、クラウドサービスプロバイダーの災害復旧と業務継続計画を点検するべきである。
- √ 利用者は、クラウドサービスプロバイダーのインフラにおける物理的な相互依存性を特定するべきである。
- √ セキュリティ、リカバリおよびデータへのアクセスに関する契約上の義務を明確に定義するため、信頼できる定義・分類法が使用されていることを確実にする。

- √ 利用者は、プロバイダーの内部・外部のセキュリティコントロールに関する文書および業界標準の遵守に関する文書を要求するべきである。

- √ 契約関係において、利用者の Recovery Time Objectives(RTOs)が完全に理解、定義され、テクノロジー計画を策定するプロセスに反映されていることを確実にする。技術のロードマップ、ポリシーおよび運用能力によりこれらの要件を満たすことができることを確実する。

- √ 利用者は､プロバイダーの役員会によって承認された BCP ポリシーを持っていることを確認する必要がある。

- √ 利用者は、BCP が有効であることを確認するため、積極的な経営側の支持や、定期的な見直しが行われている証拠を探すべきである。

- √ 利用者は、BCP が BS25999 などの国際的に認識された規格に認証されていること、そして／または、マッピングされていることを確認するべきである。

- √ 利用者は､プロバイダーが､計画の概要とファクトシートが参照できるような、セキュリティと BCP に関するオンラインリソースを提供しているかどうか確認するべきである。

- √ 共有されるデータおよび利用されるコントロールが明確に理解されるよう、クラウドサプライヤーが、会社の Vendor Security Process(VSP)を通して検査されるようにする。 VSP の結果は、リスクが許容できるかどうかに関する意思決定のプロセスと評価に使用されるべきである。

- √ クラウドコンピューティングは変化が激しい一方で比較的未熟な分野であることから、利用者に伝えられていない変化を明らかにするため、より頻繁に上記全ての活動を実施するべきである。

寄稿者: Randolph Barr, Luis Morales, Jeff Spivey, David Tyson

ドメイン 8: データセンター運用

企業と一般利用者向け IT サービスがクラウドに移行するにつれて、クラウドサービスプロバイダーの数は増加し続けている。クラウドコンピューティングのサービス提供を可能にするためのデータセンターも同様に増加している。よく知られたテクノロジーリーダーから新興企業まで、あらゆる種類と規模のクラウドサービスプロバイダーが、IT サービス提供に関するこの有望で新しいアプローチに対して、大規模な投資を行っている。

効率と規模の経済を実現するために IT リソースを共有することは、新しい概念ではない。しかし、伝統的に莫大であったデータセンター運用への投資額を、より広範囲の利用者へ広げた方が、クラウドビジネスモデルは非常に良く働く。歴史的に、データセンターアーキテクチャは、周期的なピーク負荷に対応するため、意図的に大きめに作られている。これは、通常の需要および低い需要の期間においては、データセンターリソースは頻繁に待機の状態か、または長時間遊休状態にあることを意味する。 他方で、クラウドサービスプロバイダーは、競争優位性を獲得し、営業利益率を最大化するため、人的および技術的なリソースの活用を最適化しようとしている。

クラウドサービス利用者にとっての課題は、自己のデータと利益を保護しながら、適切でコスト効率の良いプロバイダーのサービス提供能力をいかに評価するかである。プロバイダーが利用者の利益を最優先に考えていると思い込んではならない。クラウドコンピューティングがその一形態であるところの、一般的な電気通信事業者のサービス提供モデルでは、通常、サービスプロバイダーは、契約上の管理レベルを超えた範囲の利用者データやシステムに対して、コントロールをほとんどまたは全く持たない。これは、確かに正しいアプローチである。しかし、一部のクラウドアーキテクチャでは、利用者のデータの完全性とセキュリティを、利用者が認識した場合には好ましく思わないような勝手な変更が行われる可能性がある。利用者は適切な質問を行い、セキュリティの脆弱性に関する基本的なアーキテクチャと潜在的領域について詳しく知ることで、検討しているサービスについて学習しなければならない。

一部またはすべての IT 運用をクラウドに移行することを決定する際、クラウドサービスプロバイダーが、ドメイン 1 の”クラウドコンピューティングの 5 つの主要な特性”をどのように実装しているか、また、その技術的なアーキテクチャとインフラが、どのようにサービスレベルアグリーメントを満たし、かつセキュリティ懸念に対処する能力についてどのように影響を与えるかを理解することはまず有用である。プロバイダーの独自の技術的なアーキテクチャは、別のプロバイダーの IaaS ストレージサービスの活用など、IT 製品と他のクラウドサービスの組み合わせであるかもしれない。

クラウドサービスプロバイダーによって技術的なアーキテクチャとインフラは異なるかもしれない。 しかし、セキュリティ要件を満たすためには、全てのプロバイダーがシステム、データ、ネットワーク、管理、プロビジョニングおよび人員の包括的な区画化を示すことができなければならない。インフラの各レイヤを隔離するコントロールは、互いに干渉しないように、適切に統合される必要がある。たとえば、管理ツールや不十分な鍵管理により、ストレージ区画化が容易に迂回できるかどうか調査するべきである。

最後に、通常の業務上の変動によるシステムの可用性と性能に関し最も良い予測を行う

ために、クラウドサービスプロバイダーが、リソース平準化とダイナミズムをどのように行っているかを理解するべきである。クラウドコンピューティングにおいては、まだ理論が実践をいくらか上回っていることを忘れてはならない: 多くの利用者が、実際に行われている自動化のレベルについて間違った仮定をしている。提供されたリソースが最大容量に達した際に、利用者に対し追加リソースをシームレスに提供することについてプロバイダーは責任を有している。

推奨事項

クラウドサービスの購入を検討している組織は、そのサービスがどのような種類であれ、どのサービスが契約に含まれ、どのサービスが含まれないかについて、明確に認識することが必要である。ベンダーの選定にあたり検討する必要がある情報の概要と、プロバイダーを適任としそのサービスを組織の要件に対しより適合させるのに役立つ追加的な質問について、以下に記載する。

- √ クラウドサービスプロバイダーがどの認証を保持しているかにかかわらず、利用者または外部のサードパーティによる監査を実施する誓約または許可を得ることは重要である。

- √ クラウド利用者は、ドメイン 1 の”クラウドコンピューティングの 5 つの主要な特性”をクラウドサービスプロバイダーがどのように実装し、その技術的なアーキテクチャとインフラが、サービスレベルアグリーメントを満たすため、セキュリティ懸念に対応する能力にどのように影響を与えているかを理解するべきである。

- √ クラウドサービスプロバイダーによって技術的なアーキテクチャは異なるが、全てのプロバイダーがシステム、ネットワーク、管理、プロビジョニングおよび人員の包括的な区画化を示めさなければならない。

- √ 利用者の業務上の変動を通じて適切なレベルのシステム可用性と性能を最もよく予測するために、クラウドサービスプロバイダーにおいて、どのようにリソース平準化が行われているかを理解すること。可能であれば、クラウドサービスプロバイダーの他のクライアントを見つけ出し、彼らの業務上の変動が利用者としてのあなたの経験に与える影響を評価する。ただし、これはサービスレベルアグリーメントが明確に定義され、測定可能で法的強制力があり、あなたの要件に適していることを確保することの代わりにはならない。

- √ クラウド利用者は、利用するクラウドサービスプロバイダーのパッチ管理ポリシーと手順、およびそれらが利用者の環境にどのように影響を与えるかを理解するべきである。この理解は契約に反映されるべきである。

- √ クラウド環境では、1 人(または 1 社)の利用者のためにポリシーやプロセス、手順、ツールを改善すると、すべての利用者に対するサービス改善につながる可能性があるため、継続的な改善は特に重要である。継続的改善プロセスを標準に持つクラウドサービスプロバイダーを探すべきである。

- √ 技術サポートまたはサービスデスクにより、利用者はプロバイダーの運用をしばしば知ることができる。あなたのエンドユーザーのために円滑で一定の顧客サポートを実現するためには、プロバイダーの顧客サポートプロセス、手順、ツールおよびサポート時間があなたの顧客サポートと確実に適合している必要がある。

- √ ドメイン 7 で示したように、ビジネス継続性と災害復旧を IT の観点から検討し、それらが要員とプロセスにどのように関連するかについて考察するべきである。クラウドサービスプロバイダーの技術的なアーキテクチャでは、たとえばフェイルオーバーについて新規でまだ立証されていない手法が使用されるかもしれない。また、利用者自身のビジネス継続計画は、クラウドコンピューティングの影響と制限に対応しているべきである。

寄稿者: John Arnold, Richard Austin, Ralph Broom, Beth Cohen, Wing Ko, Hadass Harel, David Lingenfelter, Beau Monday, Lee Newcombe, Jeff Reich, Tajeshwar Singh, Andrew Windel, Richard Zhao

ドメイン 9: インシデントレスポンス、通知および復旧

クラウドコンピューティングの性質により、セキュリティインシデント、データ侵害や、その他調査と対応を必要とする事象が発生した場合、誰に連絡をするべきかを特定することがより困難になる。共通の報告義務により求められる、変更に対応するための修正については、標準化されたセキュリティインシデントレスポンスの仕組みを使用することができる。このドメインは、これらのインシデントをどう扱うかについてガイダンスを提供する。

クラウドにおいて導入されたアプリケーションは、必ずしもデータの完全性やセキュリティを念頭に入れて設計されている訳ではないことは、クラウド利用者にとって問題である。 これにより、脆弱性を有したアプリケーションがクラウド環境に導入され、セキュリティインシデントを引き起こす可能性がある。さらに、インフラのアーキキテクチャの不具合、手続きを強化している際に発生したミスおよび単純な見落としにより、クラウドの運用において重大なリスクを引き起こす。もちろん、同様の脆弱性は従来のデータセンター運用に対しても危険を及ぼす。

インシデント対応には、明らかに技術的な専門性が求められるが、プライバシーと法律の専門家も、クラウドのセキュリティに寄与する割合は大きい。彼らは、インシデント対応に関連して、通知、復旧およびその後起こる可能性がある訴訟においても役割を担う。クラウドサービスの利用を検討する組織は、ユーザ契約やプライバシーポリシーの対象ではない従業員によるデータへのアクセスに関する問題に対してどのようなメカニズムが導入されたかを検討する必要がある。一般に、IaaS や PaaS アーキテクチャなどにおける、クラウドサービスプロバイダーによって管理されていないアプリケーションデータは、SaaS プロバイダーのアプリケーションで管理されたデータと異なったコントロールを持っている。

大手のクラウドサービスプロバイダーが SaaS、PaaS および IaaS 機能を提供する場合、その複雑性により、インシデント対応について重大な問題が発生する。そのようなプロバイダーを使用する可能性のある利用者は、その問題を評価し、受容可能なレベルであることを確認しなければならない。プロバイダーを評価するとき、そのプロバイダーは何十万ものアプリケーションインスタンスをホスティングしている可能性があることに注意しておくことが重要である。インシデント監視の観点からは、異質なアプリケーションがあることにより、セキュリティオペレーションセンター(“SOC”という)の責任は広がる。通常 SOC は、侵入検知システムやファイアウォールなどにより発報されるアラートやインシデント指標を監視する。しかし、SOC は外部のインシデントだけでなく、利用者間の活動も監視する必要があるかもしれず、監視しなければならないソースの数と通知の量は、オープンなクラウド環境では飛躍的に増加する可能性がある。

組織は、選択したクラウドサービスプロバイダーにおけるインシデントレスポンス戦略を理解する必要がある。この戦略は、アプリケーションデータへの不正アクセスに対して、インシデントの識別、通知および復旧のためのオプションに対応していなければならない。アプリケーションデータの管理とアクセスは、データの保管場所によって重要性や法的な要求事項が異なり、これが更に問題を複雑にする。たとえば、データがアメリカに保管されている場合は問題とみなされなくても、そのデータがドイツに存在して

いる場合は、そのデータに関してインシデントが発生する可能性がある。このような複雑さが、インシデントの特定を特に困難にしている。

推奨事項

√ クラウド利用者は、サービス展開の前に、何を単なる事象とみなし(たとえば、疑わしい侵入探知アラートなど)、何をインシデントとみなすか(データ侵害など)を明確に定義し、クラウドサービスプロバイダーに伝える必要がある。

√ クラウド利用者は、プロバイダーのインシデントレスポンス活動にほとんど関わらない可能性がある。そのため、事前に用意されたプロバイダーのインシデントレスポンスチームへの連絡経路を利用者が理解することは重要である。

√ クラウド利用者は、プロバイダーがどのインシデント検知ツールやどの解析ツールを使用しているか調査し、自身のシステムと適合していることを確認するべきである。プロバイダー独自のログ形式、または一般的ではないログ形式を使用している場合、共同調査、特に法的な開示手続きや政府の介入に関わる調査において深刻な障害となる可能性がある。

√ アプリケーションおよびシステムが十分に設計および保護されていない場合、そのようなアプリケーションやシステムは、容易に全員のインシデント対応能力を台無しにしてしまう可能性がある。セキュリティインシデントの発生可能性を小さくするためには、システムについて適切なリスク管理を行い、徹底的な防御のための施策を利用することが不可欠である。

√ SOC はインシデントレスポンスに関して、インシデント対応について単一のガバナンスモデルを度々前提とするが、これはマルチテナントのクラウド事業者には不適切である。利用可能なデータソース(アプリケーションログ、ファイアウォールログ、IDS ログなど)を特定して、一般的な分析と警告プラットフォームに結合させる、堅固でよく管理されたセキュリティ情報とイベント管理(SIEM)プロセスは、SOC がクラウドコンピューティングプラットフォームにおけるインシデントを検出するのに有用である。

√ 詳細なオフライン分析をうまく進めるためには、利用者の仮想環境全体、つまり、ファイアウォール、ネットワーク(スイッチ)、システム、アプリケーションおよびデータ、のスナップショットを提供する能力があるクラウドサービスプロバイダーを探すべきである。

√ インシデント被害の拡大を防止するため、ダメージコントロールおよび証拠収集のどちらを優先させるかを検討する必要がある。機密性、完全性、可用性(CIA)の 3 要素を重視した、インシデント被害の拡大防止アプローチは有効である。

√ 復旧では、インシデント前の状態にシステムをリストアできることの重要性、および安全と判断される設定のために 6 カ月から 12 カ月前に戻す必要性が強調

される。法的オプションおよび要件に注意すると、復旧においてインシデントデータを記録するフォレンジックをサポートする必要もあるかもしれない

√ データ侵害の規制で個人のデータと分類されたデータは、侵害が発生した場合の影響を軽減するため、常に暗号化されるべきである。利用者は、ドメイン 11 に示すように、契約上で暗号化要件を規定するべきである。

√ いくつかのクラウドサービスプロバイダーは、固有のアプリケーションを使用する多数の利用者をホスティングする可能性がある。これらのクラウドサービスプロバイダーは、インシデントの影響を特定の利用者に細かく限定するために、アプリケーションレイヤのログフレームワークを検討するべきである。また、これらのクラウドサービスプロバイダーは、アプリケーション・インターフェース(URL、SOA サービスなど)ごとにアプリケーション所有者の登録簿を作成するべきである。

√ アプリケーションレベルのファイアウォール、プロキシおよびその他のアプリケーションログツールは、マルチテナント環境におけるインシデント対応を支援するために現在利用できる重要な機能である。

寄稿者: John Arnold, Richard Austin, Ralph Broom, Beth Cohen, Wing Ko, Hadass Harel, David Lingenfelter, Beau Monday, Lee Newcombe, Jeff Reich, Tajeshwar Singh, Andrew Windel, Richard Zhao

ドメイン 10: アプリケーションセキュリティ

柔軟性、開放性およびパブリックな可用性という長所により、クラウド環境は、アプリケーションセキュリティに関する多くの基本的な前提を覆す。これらの前提のいくつかはよく理解されているものの、多くは理解されていない。このセクションは、クラウドコンピューティングが、アプリケーションのライフタイム(設計から運用、完全な廃棄まで)に渡ってセキュリティにどのように影響を及ぼすかについて記載することを意図している。このガイダンスは、アプリケーション設計者、セキュリティ専門家、業務職員、および技術管理を含む、すべての利害関係者に対して、クラウドコンピューティングアプリケーションにおいてどのようにリスクを軽減し、保証を管理するかについて記載している。

クラウドコンピューティングは、SaaS、PaaS および IaaS の全てのレイヤにわたるアプリケーションにおいて、とりわけ課題である。クラウドベースのソフトウェアアプリケーションは、古典的な DMZ にあるアプリケーションと同様に、厳格な設計を必要とする。 これには、情報の機密性、完全性および可用性の管理に係るすべての伝統的な側面を網羅する深い事前分析が含まれる。

クラウド環境におけるアプリケーションは、以下の主要な側面に影響を与え、そして与えられる:

- **アプリケーションセキュリティアーキテクチャ**　ほとんどのアプリケーションは､他の様々なシステムに依存しているということを考慮しなければならない。クラウドコンピューティングでは、アプリケーションの依存性は、個々のサードパーティサービスプロバイダーごとに異なるほど、大幅に変わり得る。クラウドの特性により、構成管理と進行中のプロビジョニングは、従来のアプリケーション展開よりかなり複雑になる。アプリケーションセキュリティを確保するため、アーキテクチャの変更を必要としている。

- **ソフトウェア開発ライフサイクル(SDLC)**　クラウドコンピューティングは、アプリケーションアーキテクチャ、デザイン、開発、品質保証、ドキュメンテーション、展開、管理、メンテナンスおよび廃棄に至るまで、SDLC の全ての側面に影響する。

- **コンプライアンス**　コンプライアンスは明確にデータに影響するが、アプリケーション(たとえば､プログラムにおいて特定の暗号化機能を実装する方法を規制する)、プラットフォーム(おそらく OS コントロールと設定を規定する)およびプロセス(たとえば、セキュリティインシデントの報告要件として)にも影響を及ぼす。

- **ツールとサービス**　クラウドコンピューティングは、稼働中のアプリケーションの構築と管理に必要なツールとサービスについて、複数の新しい課題をもたらす。これには、開発およびテスト用ツール、アプリケーション管理機能、外部サービスとの連結およびライブラリと OS サービスへの依存が含まれ、これらはクラウドサービスプロバイダーが提供する可能性がある。それぞれに関し、誰が提

供するか、誰が所有するか、誰が運用するか、および誰が責任を負うかについて影響を理解することは重要である。

- **脆弱性**　ウェブアプリケーションに関連してよく立証され、絶え間なく発展し続けている脆弱性だけではなく、クラウドへの展開が増加しつつある、マシン間サービス指向型アーキテクチャ（SOA)アプリケーションに関連する脆弱性も含まれる。

推奨事項

√ ソフトウェア開発ライフサイクル(SDLC)セキュリティは重要であり、クラウドベースの開発において、次の 3 つの主要な違いについて、高いレベルで対応するべきである: 1)アップデートされた脅威と信頼モデル、2) クラウド環境のためにアップデートされたアプリケーション評価ツールおよび 3)アプリケーションのセキュリティアーキテクチャ変更を説明するための SDLC プロセスと品質のチェックポイント。

√ IaaS、PaaS および SaaS は、ソフトウェア開発ライフサイクルにおいて異なった信頼境界を生じさせる。 これらはアプリケーションの開発、テストおよび展開において、考慮されなければならない。

√ IaaS に関しては、信頼できる VM イメージの存在が、成功の鍵の一つである。それが無い場合は、内部ポリシーに合致する VM イメージを、利用者自身が提供することが最も良い代替手段である。

√ DMZ 内のホストシステムを堅牢にするために利用可能な最も良いプラクティスが、VM に適用されるべきである。アプリケーションスタックを支えるのに必要最低限なものにサービスを制限することは適切である。

√ ホスト間通信をセキュアにすることは、必ず実施しなければならない。一般的なデータセンターにおいては、同じハードウェア機器の中でさえ、ホスト間には安全なチャンネルがあると想定することはできない。

√ アプリケーション認証情報と鍵の情報を管理し、保護することは重要である。

√ アプリケーションロギングとデバッグに使用されているファイルは、リモートに保管されているか、場所が不明である可能性があり、また、機密情報である可能性がある。したがって、その管理には、特別な注意が払われるべきである。

√ アプリケーションの脅威モデルに、外部の管理とマルチテナントを考慮する。

- √ エンタープライズサービスバス(ESB)を利用することができるくらい複雑なアプリケーションは、WS-Security などのプロトコルを利用して、直接 ESB をセキュアにする必要がある。PaaS 環境では、ESB を分割する機能は利用できない。

- √ アプリケーションセキュリティプログラムの有効性を評価するための指標を適用するべきである。アプリケーションセキュリティに特化した利用可能な指標として、脆弱性スコアとパッチ適用範囲がある。これらの指標は、アプリケーションコーディングの品質を示すことができる。暗号化されたデータの割合など、間接的なデータを扱う指標は、アプリケーションアーキテクチャの観点から責任のある決断がなされていることを示すことができる。

- √ クラウドサービスプロバイダーは、自身の環境でホスティングされたアプリケーションに対する動態分析ウェブアプリケーションセキュリティツールをサポートしなければならない。

- √ アプリケーション要素を監視から目立たなくしてしまう新しいクラウドアプリケーションアーキテクチャに対して、悪意のある者がどのように反応するかに注意を向けるべきである。ハッカーは、ユーザーコンテクストで稼動するコードなど、目に見えるコードを攻撃する傾向がある。彼らは、インフラを攻撃して、大規模なブラックボックステストを行う傾向がある。

- √ 利用者は、従来の(ネットワーク／ホスト)脆弱性およびアプリケーションの脆弱性を含む、脆弱性評価をリモートで実施する契約上の許可を得るべきである。多くのクラウドサービスプロバイダーは、本物の攻撃と区別することができないこと、および他の利用者に対する潜在的な影響を防ぐことを理由に、脆弱性評価の実施を制限している。

寄稿者: John Arnold, Warren Axelrod, Aradhna Chetal, Justin Foster, Arthur J. Hedge III, Georg Hess, Dennis Hurst, Jesus Luna Garcia, Scott Matsumoto, Alexander Meisel, Anish,Mohammed, Scott Morrison, Joe Stein, Michael Sutton, James Tiller, Joe Wallace, Colin Watson

ドメイン 11: 暗号化と鍵管理

クラウド利用者とプロバイダーは、データの損失と盗用に対して防御する必要がある。今日、個人および企業データの暗号化は強く推薦されており、国によっては法や規制によって強制される場合もある。 クラウド利用者は、データがどこに保管されているとしても保護されるよう、プロバイダーにデータを暗号化することを求める。 同様に、クラウドサービスプロバイダーは、利用者の機密データを保護する必要がある。

鍵管理を行った上での強固な暗号化は、クラウドコンピューティングシステムがデータを保護するために使用するべき主要なメカニズムの 1 つである。暗号化自体は必ずしもデータの損失を防ぐわけではないが、法及び規制における免責条項は、暗号化されたデータの損失は損失ではないと見なす。鍵管理は保護資源へのアクセスを可能にし、暗号化はリソース保護を提供する。

機密性と完全性のための暗号化

クラウド環境は多くのテナントと共有されており、クラウドサービスプロバイダーは、その環境にあるデータに対して特権的にアクセスできる。したがって、クラウドにホスティングされている機密データは、アクセス制御(ドメイン 12 を参照)、契約責任(ドメイン 2、3 および 4 を参照)およびこのセクションで説明する暗号化の組み合わせにより、保護しなければならない。これらのうち暗号化は、クラウドサービスプロバイダーへの依存を最小にする恩恵や、運用上の不履行を検知するにあたっての依存がない恩恵をもたらす。

ネットワーク上で伝送されるデータの暗号化　　インターネットで送信されるクレジットカード番号、パスワードおよび秘密鍵などの多目的に使用される認証情報は、必ず暗号化される必要がある。クラウドサービスプロバイダーのネットワークは、オープンなインターネットより安全であるかもしれないが、クラウドは多くの異なる構成要素で作られており、そして、異なった組織により共有される。したがって、クラウドサービスプロバイダーのネットワークの中であっても、送信中の機密で規制された情報を保護することは重要である。通常、これは SaaS、PaaS および IaaS 環境において同様に容易に実装することができる。

保管データの暗号化　　ディスク上の、または、稼働中の本番データベースのデータを暗号化することは、悪意のあるクラウドサービスプロバイダーや共同テナント、およびいくつかの種類のアプリケーションの悪用から保護できるため、価値がある。長期のアーカイブ保管のために、一部の利用者は、保管データを暗号化した上でクラウドデータ保管ベンダーに送る。 利用者は、暗号化キーを保持および管理し、必要であれば自身の環境で複合する。さまざまなプロバイダーとサードパーティツールを使用して、保管データを暗号化することは IaaS 環境では一般的である。PaaS 環境で保管したデータの暗号化は、プロバイダーが提供する手段または特別なカスタマイゼーションを必要とするため、概してより複雑である。SaaS 環境で保管したデータの暗号化は、クラウド利用者が直接実装することができない機能であり、プロバイダーに要求しなければならない。

バックアップメディアのデータの暗号化　　これにより紛失したメディア、あるいは盗

まれたメディアを不正使用から守ることができる。理想的には、クラウドサービスプロバイダーが利用者に意識させることなく、それを実装する。 しかし、そのような暗号化が行われることを確かめるのは、データの利用者および提供者であるあなたの責任である。 暗号化インフラに関しては、データの寿命についても考慮するべきである。

クラウドサービスプロバイダーに対する新しい攻撃が行われる可能性を考えると、これらの一般的な暗号化の使用を超えて、メモリに保管されているデータを含め、動的なデータを暗号化する手段を更に探求することは当然である。

鍵管理

既存のクラウドサービスプロバイダーは、クラウドベースのアプリケーション開発とサービスをセキュアにするために基本的な暗号化鍵体系を提供するか、またはそのような保護対策をすべて利用者に任せるかもしれない。クラウドサービスプロバイダーは、堅固な鍵管理体系のサポートに向けて進歩しているが、採用に至るまでには多くの障害を乗り越える必要がある。新規の規格が、近い将来、この問題を解決するはずだが、それに向けた作業はまだ進行中である。 クラウドコンピューティングにおける鍵管理に関しては、いくつかの課題がある:

鍵保管のセキュア化　鍵保管はそれ自身、他のあらゆる機密データと同様、保護される必要がある。それらは保管、移動およびバックアップにおいて、保護されなければならない。不適切な鍵保管は暗号化された全データを危険にさらす可能性がある。

鍵保管へのアクセス。　鍵保管へのアクセスは、個々の鍵を必要とするエンティティに明確に制限されなければならない。 また、鍵保管を統制するポリシーが必要であり、そのポリシーでは、アクセス制御を行うために役割の分離を行うべきである。鍵を使用するエンティティとその鍵を保存するエンティティは異なるべきである。

鍵のバックアップと復元可能性。　鍵の損失は、必然的にそれらの鍵が保護するデータの損失を意味する。 これはデータを破壊する効果的な方法であるが、ミッションクリティカルなデータを保護する鍵の不慮の損失は企業にとって打撃を与える。したがって、安全なバックアップとリカバリソリューションが導入されなければならない。

クラウドにおける鍵管理に適用できる、幾つかの規格とガイドラインがある。OASIS Key Management Interoperability Protocol(KMIP)は、クラウドにおける相互運用可能な鍵管理に関する新規の規格である。 IEEE1619.3 規格は、特にストレージ IaaS に関する、ストレージ暗号化と鍵管理をカバーしている。

推奨事項

- √　暗号化を使用して、データ保持とデータ利用を分離する。
- √　データをホスティングするクラウドサービスプロバイダーから鍵管理を隔離し、一連の分離体系を作成する。これは、法的な命令によりデータの提供をせざる

を得ない場合に、クラウドサービスプロバイダーと利用者の両方を対立から守る。

√ 契約に暗号化を規定するときには、関連する既存の業界や政府の規格を順守することを確保する。

√ クラウドサービスプロバイダー施設が役割の管理と職務分離を提供しているか、およびそれらをどのように提供しているかについて理解する。

√ クラウドサービスプロバイダーが鍵管理を行わなければならない場合は、プロバイダーが鍵管理ライフサイクルのプロセスを定義しているかどうか確認する: 鍵がどのように生成、使用、保存、バックアップ、復元、交代、および削除されるか、さらには、すべての利用者に対して同じ鍵が使用されるのか、または各利用者に独自の鍵セットがあるのかどうかを確認する。

√ 規制対象、または機密データが、保管されているときに加え、クラウドサービスプロバイダーの内部ネットワークを移動するときにも暗号化されることを確実にする。これを導入することは、IaaS 環境においてはクラウド利用者の、PaaS 環境においては利用者とプロバイダー共同の、そして SaaS 環境においてはクラウドサービスプロバイダーの責任である。

√ IaaS 環境では、従来の方法により暗号化されているはずの機密情報や鍵に関する資料が、利用中にどのように暴露される可能性があるかを理解する。たとえば、VM スワップファイルやその他の一時的なデータの格納先も、暗号化を行う必要があるかもしれない。

寄稿者: John Arnold, Girish Bhat, Jon Callas, Sergio Loureiro, Jean Pawluk, Michael Reiter, Joel Weise

ドメイン 12: アイデンティティとアクセス管理

エンタープライズアプリケーションのアイデンティティとアクセス制御を管理することは、依然として、今日 IT が直面している重要な課題の 1 つである。企業は、優れたアイデンティティとアクセス管理の戦略がなくても、いくつかのクラウドコンピューティングサービスを利用することができるかもしれない。しかし、長期的には、組織のアイデンティティサービスをクラウドに広げることは、オンデマンドコンピューティングサービスを戦略的に利用するための前提となる。今日明らかに未熟なクラウドエコシステムのアグレッシブな導入が行われている。この導入をサポートするには、その組織のクラウドコンピューティングプロバイダーの能力を理解することと同様に、クラウドベースのアイデンティティとアクセス管理(IAM)を行う組織の準備状況に対する公正な調査が必要である。

クラウドにおける効果的なアイデンティティ管理に不可欠である、下記の主要な IAM 機能について議論する:

- アイデンティティのプロビジョニング／デプロビジョニング
- 認証
- フェデレーション
- 承認とユーザ・プロファイル管理

これらの全てにおいて、コンプライアンスは重要な考慮すべき事項である。

アイデンティティのプロビジョニング:　クラウドコンピューティングサービスを採用する組織にとって、主要な課題の 1 つは、ユーザのプロビジョニングをデプロビジョニングにおける安全でタイムリーな管理である。 さらに、企業内のユーザ管理プロセスに投資をした企業は、それらのプロセスとプラクティスをクラウドに広げようとする。

認証: 組織がクラウドサービスを利用し始めるとき、信頼でき管理が可能な方法でユーザ認証をすることは、重大な必要条件である。組織は、認証情報の管理、厳密認証(通常多要素認証と定義される)、委譲された認証(デレゲーション)およびあらゆる種類のクラウドにわたる信用情報の管理など、認証に関する課題に対処していかなければならない。

フェデレーション:　クラウドコンピューティング環境において、連携したアイデンティティ管理(フェデレーション)は、組織が選択したアイデンティティプロバイダー(IdP)を利用してクラウドサービスのユーザ認証を行う上で重要な役割を果たす。そのような意味で、サービスプロバイダー(SP)と IdP の間でアイデンティティ属性を安全な方法で交換することも、重要な必要条件である。クラウドで連携されたアイデンティティ管理を検討する組織は、否認防止をサポートしながら、アイデンティティライフサイクル管理や、機密性と完全性を担保するための利用可能な認証方法に関するさまざまな課題、およびそれらの課題に対処するソリューションについて理解するべきである。

承認とユーザ・プロファイル管理:　ユーザ・プロファイルとアクセス制御ポリシーの要件は、ユーザが自身の意思でクラウドを利用しているのか(利用者など)、組織のメンバーとして利用しているのか(雇い主、大学、病院、または他の企業など)によって異なる。

SPI 環境におけるアクセス制御の要件は、信頼できるユーザ・プロファイルおよびポリシー情報の作成、それを使用したクラウドサービス内のアクセス制御、およびこれらの監査可能な方法での実施を含む。

アイデンティティプロビジョニングに関する推奨事項

- √ クラウドサービスプロバイダーによって提供されている機能は、現在、企業の要件を満たすために十分でない。 利用者は、クラウドプロバイダー固有のカスタムコネクターの作成など、管理の複雑さをさらに悪化させる独自のソリューションを避けるべきである。

- √ 利用者は、実用的な範囲において、クラウドサービスプロバイダーによって提供された、望ましくは、SPML スキーマで構築された標準コネクタを利用するべきである。あなたのクラウドサービスプロバイダーが現在 SPML を提供しない場合、あなたはそれを要求するべきである。

- √ 利用者は、クラウド内のアプリケーションとプロセスを包含するように、アイデンティティデータに関する信頼できるレポジトリを、変更するか、広げるべきである。

認証に関する推奨事項

クラウドサービスプロバイダーと顧客企業の両方が、認証情報管理と厳密認証に関連する課題を検討し、リスクを適切に低減させる、コスト効率のよいソリューションを実装するべきである。

SaaS と PaaS プロバイダーは、通常アプリケーションかプラットフォームに組み込まれた認証サービスか、企業に委譲する認証(デレゲーション)のどちらかのオプションを提供する。
利用者には、以下のオプションがある:

- √ 企業のための認証。企業は、彼らの Identity Provider(IdP)を通してユーザを認証を行い、フェデレーションにより SaaS ベンダーと信頼関係を構築することを検討するべきである。

- √ 自身の意思でクラウドを利用している個人ユーザのための認証。 企業は、複数のサイトで有効な単一セットの認証情報の使用を可能にするために、Google、Yahoo、OpenID、Live ID などのユーザ中心の認証を使用することを検討するべきである。

- √ 認証を委譲(デレゲーション)するための独自の方法(たとえば、共有の暗号化クッキーなどの方法で信用情報を扱うなど)を要求するあらゆる SaaS プロバイダーは、継続する前に適切なセキュリティ評価により厳密に評価されるべきである。一般的には、オープンスタンダードを使用するべきである。

IaaS に関しては、認証の戦略は既存の企業の機能を利用することができる。

- √ IT 要員にとっては、既存のシステムとプロセスを活用できるため、専用 VPN の確立が、より良いオプションになるだろう。

- √ 専用 VPN トンネルを企業ネットワークあるいはフェデレーションに確立することは、可能な戦略の一つである。専用 VPN トンネルは、アプリケーションが、既存のアイデンティティマネジメントシステム(アイデンティティデータの信頼できるソースを提供する、SSO ソリューションあるいは LDAP ベースの認証など)を活用する場合に適している。

- √ 専用 VPN トンネルが可能でない場合、アプリケーションは、SSL などの標準のネットワーク暗号化と組み合わせて、様々な形式(SAML、WS-Federation など)の認証アサーションを受け入れるように設計されるべきである。このアプローチにより、組織は企業内だけではなく、クラウドアプリケーションにも連携する SSO を導入することができる。

- √ アプリケーションが企業ユーザ以外も対象とする場合、OpenID も一つの選択肢である。しかし、OpenID 認証情報のコントロールは企業外であるため、そのようなユーザに与えられたアクセス権は、適切に制限されるべきである。

- √ クラウドサービスプロバイダーによって実装されたローカル認証サービスは、OATH に準拠するべきである。 OATH に準拠したソリューションで、企業は、1 つのベンダーの認証情報に縛られることを避けることができる。

- √ 技術にかかわらず､厳密認証を可能にするために､クラウドアプリケーションは、SAML などを通して、サービスを利用している企業に認証を委譲(デレゲーション)するための機能をサポートするべきである。

- √ クラウドサービスプロバイダーは、ワンタイムパスワード、生体認証、電子証明書およびケルベロスなど、さまざまな厳密認証オプションをサポートすることを検討するべきである。これは、企業に既存のインフラを使用する新たなオプションを提供する。

フェデレーションに関する推奨事項

クラウドコンピューティング環境では、会社間における認証、シングルサインオン(SSO)または回数を減らしたサインオン、ならびにサービスプロバイダー(SP)とアイデンティティプロバイダー(IdP)間のアイデンティティ属性の交換を可能にする上で、アイデンティティのフェデレーションは鍵である。クラウドでフェデレーションアイデンティティ管理を検討している組織は、アイデンティティライフサイクル管理、認証方法、トークン形式および否認防止に関するさまざまな課題とそれらに対応するための利用可能なソリューションについて理解するべきである。

- √ クラウドサービスプロバイダーを探している企業は、プロバイダーが主要な規格(SAML と WS-Federation)のうち少なくともどちらかをサポートしていることを確認するべきである。 SAML は、広くサポートされているフェデレーション規格として浮上しつつあり、主要な SaaS と PaaS クラウドサービスプロバイダーによってサポートされている。複数の規格へのサポートは、高い柔軟性を可能にする。

- √ クラウドサービスプロバイダーには、異なったアイデンティティプロバイダーから標準のフェデレーション形式を受け入れる柔軟性があるべきである。 しかし、本ガイダンスを書いている現在、ほとんどのクラウドサービスプロバイダーは、単一の規格(SAML1.1 や SAML2.0 など)しかサポートしていない。複数のフェデレーショントークン形式をサポートしたいと考えるクラウドサービスプロバイダーは、何らかのタイプのフェデレーションゲートウェイを実装することを検討するべきである。

- √ 利用者は、Federated Public SSO と Federated Private SSO を比較して評価したいかもしれない。Federated Public SSO は、SAML や WS-Federation などのクラウドサービスプロバイダーの規格に基づいているが、Federated Private SSO は、VPN 上で既存の SSO アーキテクチャを活用する。長期的には、Federated Public SSO が理想的であるが、成熟した SSO アーキテクチャを持っており、クラウド展開の数が限られている組織にとっては、Federated Private SSO の利用は短期的なコストメリットをもたらすかもしれない。

- √ 利用者は、トークンの発行と照合を管理することを目的として、フェデレーションの導入を外部に展開するため、フェデレーションゲートウェイを選ぶかもしれない。この手法により、組織は様々な形式のトークンの発行をフェデレーションゲートウェイに委譲し、フェデレーションゲートウェイはトークンを異なる形式に翻訳する。

アクセス制御に関する推奨事項

クラウドサービス向けの適切なアクセス制御ソリューションの選択または検討には多くの側面があり、下記の事項を考慮する必要がある:

- √ サービスまたはデータの種類に応じた、アクセス制御モデルの適切性を検討する。

- √ ポリシーおよびユーザプロフィール情報の信頼できるソースを特定する。

- √ データに必要なプライバシーポリシーに対するサポートを評価する。

- √ ポリシーとユーザ情報を規定するフォーマットを選択する。

- √ ポリシ管理ポイント(PAP)からポリシ決定ポイント(PDP)にポリシーを転送するメカニズムを特定する。

- √ メカニズムがポリシ情報ポイント(PIP)からポリシ決定ポイント(PDP)にユーザ情報を転送するメカニズムを特定する。
- √ ポリシ決定ポイント(PDP)からの方針決定を要求する。
- √ ポリシ実施ポイント(PEP) で決定した方針を実行する。
- √ 監査に必要な情報を登録する。

IdaaS に関する推奨事項

Identity as a Service は、プライバシー、完全性および可監査性に関する追加の検討事項とともに、内部に実装された IAM と同様のベストプラクティスに従うべきである。

- √ 内部の企業ユーザに関しては、管理人は、ダイレクト VPN、または SAML や厳密認証などの業界基準を通して、クラウドへの安全なアクセスを提供するためのクラウドサービスプロバイダーのオプションを見直さなければならない。クラウドを使用することによるコスト削減は、従業員情報を外部に保存することに付随するプライバシー問題に対応するためのリスク軽減対策コストとバランスをとる必要がある。
- √ パートナーなどの企業外ユーザに関しては、情報所有者は、IAM プロバイダーとのやりとりを SDLC および脅威の評価の中に組み込む必要がある。また、アプリケーションセキュリティ(さまざまなコンポーネント間のやりとり、およびそれによってもたらされる SQL インジェクションやクロスサイトスクリプティングなどの脆弱性)についても検討し、対策を講じる必要がある。。
- √ PaaS 利用者は、プロビジョニング、認証、アクセス制御ポリシーに関するコミュニケーションおよび監査情報に関する規格について、IDaaS ベンダーがどの範囲までサポートするか調べるべきである。
- √ 独自のソリューションは、独自コンポーネントにおける透明性が欠如することにより、クラウド上の IAM 環境に対して重大な危険をもたらす。独自のネットワーク・プロトコル、暗号化アルゴリズムおよびデータ通信は、しばしばより安全が低く、脆弱であり、相互運用可能性が低い。外部化を行う IAM コンポーネントに対してはオープンスタンダードを使用することが重要である。
- √ IaaS 利用者に関しては、仮想サーバを起動するために使用されるサードパーティイメージを、ユーザおよびイメージの信頼性の観点で確認する必要がある。 イメージのライフサイクル管理に提供されるサポートの検討は、あなたの内部ネットワークにインストールされているソフトウェアと同じ原則をもとにして確認しなければならない。

寄稿者: Subra Kumaraswamy, Sitaraman Lakshminarayanan, Michael Reiter,

クラウドコンピューティングのためのセキュリティガイダンス V2.1

Joseph Stein, Yvonne Wilson

ドメイン 13: 仮想化

インフラ、プラットフォームまたはソフトウェアレベルでマルチテナントクラウドにサービスを提供する能力は、しばしば何らかの仮想化を提供し、スケールメリットを作り出すことによって支えられる。しかし、これらの技術の使用により新たなセキュリティ問題をもたらす。 このドメインは、これらのセキュリティ問題について取り上げる。仮想化にはさまざまな形式があるが、圧倒的に一般的なのが、OS の仮想化である。そして、このバージョンにおける本ガイダンスでは、OS の仮想化に焦点をあてる。 バーチャルマシン(VM)技術がクラウドサービスのインフラに使用されている場合、それらの VM システムの区画化および堅牢性に注意をしなければならない。

仮想 OS の管理に関する現在のプラクティスの実態は、デフォルトでセキュリティを提供するプロセスの多くが欠けており、それらを代用することに特別な注意を支払わなければならない。仮想化のコア技術自体はハイパーバイザーおよびその他の管理コンポーネントに対して新たな攻撃対象範囲を作り出すが、より重要であるのは、仮想化がネットワークセキュリティに与える深刻な影響である。現在、VM は、ネットワークよりむしろハードウェアバックプレーンの上で通信を行う。その結果、このトラフィックは、標準のネットワークセキュリティコントロールにとって死角になっており、モニタリングやインラインブロッキングを実行できない。これらのコントロールは、仮想環境で機能するように形式を変える必要がある。

集中されたサービスやレポジトリにおけるデータの混在も懸念事項である。クラウドコンピューティングサービスで提供される集中データベースは、理論上は、膨大な数のさまざまなエンドポイントに分散されたデータのセキュリティを向上させるはずである。しかし、これは同時にリスクの集中化でもあり、漏洩による影響を増加させる。

異なる機密性とセキュリティを有する VM の混在も懸念事項である。クラウドコンピューティング環境では、保護を目的としたネットワークの依存を組み込まない新しいセキュリティアーキテクチャが実現されない限り、セキュリティの最小公倍数がマルチテナント仮想環境におけるすべてのテナントによって共有される。

推奨事項

- √ クラウドサービスプロバイダーが仮想化を使用する場合、どのタイプの仮想化を使用するかを特定する。
- √ 仮想 OS は、階層化されたセキュリティコントロールを提供し、プラットフォームプロバイダーへの依存度を減少させるため、サードパーティのセキュリティ技術によって増補されるべきである。
- √ 内臓されたハイパーバイザーの分離以外に、どのセキュリティコントロール(侵入検出、アンチウイルス、脆弱性スキャンなど)が VM 内部に実装されているか理解する。デフォルトの設定によるセキュリティは、利用可能な業界基準に準拠すること、または上回ることにより、保証されなければならない。

- √ 利用者に公開される管理インターフェース(Web ベース、API など)を保護するために、どのようなセキュリティコントロールが VM の外部に実装されているかを理解する。

- √ クラウドサービスプロバイダーから提供されるあらゆる VM イメージやテンプレートは、その由来と完全性を確認してから使用する。

- √ ハイパーバイザーAPI に組み込まれた VM 特有のセキュリティメカニズムは、従来のネットワークセキュリティコントロールでは不明瞭な、VM バックプレーン上を通過するトラフィックに対して、粒度の細かい監視を提供するために利用されなければならない。

- √ 仮想 OS の管理アクセスとコントロールは重要であり、改ざん不可能なログ収集ツールおよび完全性監視ツールに加え、企業のアイデンティティ管理に統合された厳密認証を含めるべきである。

- √ 利用の種別(たとえば、デスクトップ対サーバ)やステージ(たとえば、開発、本番およびテスト)およびサーバ、ストレージなどの別々の物理的なハードウェアにあるデータの機密性に応じて VM を分離し、セキュリティゾーンを作成することの有効性と実行可能性を調査する。

- √ VM における分離の証拠を提供し、分離違反があった場合にアラートを発報する報告メカニズムを持つようにする。

- √ 規制事項により分離が必要となる可能性がある場合、VM においては、マルチテナントの状況に注意する。

寄稿者: Bikram Barman, Girish Bhat, Sarabjeet Chugh, Philip Cox, Joe Cupano, Srijith K.Nair, Lee Newcombe, Brian O'Higgins

参考文献

A guide to security metrics. SANS Institute, June 2006. http://www.sans.org
Amazon EC2 API -
http://docs.amazonwebservices.com/AWSEC2/2006-10-01/DeveloperGuide/

Amazon Elastic Compute Cloud Developer Guide,
http://docs.amazonwebservices.com/AWSEC2/2009-03-01/DeveloperGuide/

Amazon Simple Queue Service Developer Guide,
http://docs.amazonwebservices.com/AWSSimpleQueueService/2008-01-01/SQSDeveloperGuide/

Amazon Simple Storage Service Developer Guide,
http://docs.amazonwebservices.com/AmazonS3/2006-03-01/

Amazon SimpleDB Developer Guide,
http://docs.amazonwebservices.com/AmazonSimpleDB/2007-11-07/DeveloperGuide/

Amazon web services blog: Introducing amazon virtual private cloud (vpc), Amazon, August 2009.
http://aws.typepad.com/aws/2009/08/introducing-amazon-virtual-private-cloud-vpc.html

Amazon Web Services: Overview of Security Processes, September 2008
An Innovative Policy-based Cross Certification methodology for Public Key Infrastructures.
Casola V., Mazzeo A., Mazzocca N., Rak M. 2nd EuroPKI Workshop. Springer-Verlag LNCS
35. Editors: D. Chadwick, G. Zhao. 2005.

Auditing the Cloud, Grid Gurus,
http://gridgurus.typepad.com/grid_gurus/2008/10/auditing-thecl.
html, October 20, 2008

Azure Services Platform, http://msdn.microsoft.com/en-us/library/dd163896.aspx
Balanced Scorecard for Information Security Introduction", Published: March 06, 2007,
http://technet.microsoft.com/en-us/library/bb821240.aspx

BITS Kalculator and BITS Financial Services Shared Assessments Program (third party provider assessment methodology)

Building Security In Maturity Model, http://www.bsi-mm.com/

Business case for a comprehensive approach to identity and access management, May 2009
https://wiki.caudit.edu.au/confluence/display/CTSCIdMWG/Business+case

Business Roundtable, Principles of Corporate Governance, 2005

Business Roundtable, Statement on Corporate Governance, 1997.

Business Software Alliance, Information Security Governance: Towards a Framework for Action

Centers for Medicare and Medicaid Services Information Security Risk Assessment Methodology

Cloud Computing and Compliance: Be Careful Up There, Wood, Lamont, ITWorld, January 30, 2009

Cloud computing definition, by P. Mell and T. Grance, NIST June 2009.
http://csrc.nist.gov/groups/SNS/cloud-computing/index.html

Cloud Computing is on the Up, but what are the Security Issues?, Mather, Tim, Secure

Computing Magazine (UK), March 2, 2009.

Cloud Computing Use Case Group Whitepaper
-http://www.scribd.com/doc/17929394/Cloud-

Computing-Use-Cases-Whitepaper

Cloud computing use cases whitepaper, August 2009.
http://www.scribd.com/doc/17929394/Cloud-Computing-Use-Cases-Whitepaper

Cloud computing use cases whitepaper, August 2009.
http://www.scribd.com/doc/17929394/Cloud-Computing-Use-Cases-Whitepaper

Cloud computing vocabulary (cloud computing wiki)
http://sites.google.com/site/cloudcomputingwiki/Home/cloud-computing-vocabulary

Cloud Computing: Bill of Rights,
http://wiki.cloudcomputing.org/wiki/CloudComputing:Bill_of_Rights

Cloud Cube Model: Selecting Cloud Formations for Secure Collaboration, Jericho Forum, V 1.0, April 2009

Cloud Security and Privacy – An Enterprise perspective on Risks and Compliance from O'Reilly
- http://oreilly.com/catalog/9780596802776/ -

Cloud Standards Organization - http://cloud-standards.org/

Cloud Storage Strategy, Steve Lesem, July 19, 2009,
http://www.cloudstoragestrategy.com/2009/07/cloud-storage-and-the-innovators-dile

mma.html

Common Configuration Scoring System (CCSS): Metrics for Software Security Configuration

Vulnerabilities (DRAFT), 2009.
http://csrc.nist.gov/publications/drafts/nistir-7502/Draft-NISTIR-7502.pdf

Contracting for Certified Information Security: Model Contract Terms and Analysis (published by the Internet Security Alliance and available at www.cqdiscovery.com)

Contracting for Information Security: Model Contract Terms (published by the Internet Security Alliance and available at www.cqdiscovery.com)

CPMC ClearPoint Metric Catalog, 2009 Online Available:
http://www.clearpointmetrics.com/newdev_v3/catalog/MetricApplicationPackage.aspx

CVSS A Complete Guide to the Common Vulnerability Scoring System, Version 2.0, 2007
Online Available: http://www.first.org/cvss/cvss-guide.html

Data Lifecycle Management Model Shows Risks and Integrated Data Flow, by Ernie Hayden,

Information Security Magazine, July 2009
http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1321704_mem1,00.html

Data Privacy Clarification Could Lead to Greater Confidence in Cloud Computing, Raywood,

Dan, Secure Computing Magazine (UK), March 9, 2009.

Defending Electronic Mail as Evidence—The Critical E-Discovery Questions, Jeffrey Ritter,
(available at www.cqdiscovery.com)

Does Every Cloud Have a Silver Compliance Lining?, Tom McHale, July 21, 2009 Online
Available:http://blog.ca-grc.com/2009/07/does-every-cloud-have-a-silver-compliance-lining/

Encryption of Data At-Rest: Step-by-step Checklist", a whitepaper prepared by the Security
Technical Working Group of the Storage Network Industry Association (SNIA).

ENISA - http://www.enisa.europa.eu/
Fedora Infrastructure Metrics, 2008.

http://fedoraproject.org/wiki/Infrastructure/Metrics

Few Good Information Security Metrics, By Scott Berinato, July 2005 Online Available:
http://www.csoonline.com/article/220462/A_Few_Good_Information_Security_Metrics

Force.com Web Services API Developer's Guide,
http://www.salesforce.com/us/developer/docs/api/index.htm

Global Privacy & Security, Francoise Gilbert, (Aspen Publishing 2009).

GoGrid API - http://wiki.gogrid.com/wiki/index.php/API

GSA to launch online storefront for cloud computing services, August 2009.
http://www.nextgov.com/nextgov/ng_20090715_3532.php

Guidelines for Media Sanitization," NIST's Special Publication 800-88
Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds, T. Ristenpart, et al,

http://blog.odysen.com/2009/06/security-and-identity-as-service-idaas.html

http://blogs.forrester.com/srm/2007/08/two-faces-of-id.html

http://blogs.intel.com/research/2008/10/httpseverywhere_encrypting_the.php

http://code.google.com/apis/accounts/docs/AuthForWebApps.html

http://code.google.com/apis/accounts/docs/OpenID.html

http://csrc.nist.gov/groups/SNS/cloud-computing/index.html

http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf

http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final-errata.pdf

http://csrc.nist.gov/publications/PubsSPs.html

http://en.wikipedia.org/wiki/Statement_on_Auditing_Standards_No._70:_Service_Organizations

http://www.aspeninstitute.org/publications/identity-age-cloud-computing-next-generationinternets-impact-business-governance-socia

http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=kmip

http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

http://www.sas70.com

https://siswg.net/index.php?option=com_docman&task=cat_view&gid=21&Itemid=99999999

Information Security Governance: A Call to Action, National Cyber Security Summit Task Force,Corporate Governance Task Force Report, April 2004.

Information Security Law: Emerging Standard for Corporate Compliance, Thomas Smedinghoff,(ITGP 2008).

ISACA, IT Governance Institute, Control Objectives for Information and related Technology (CobiT), 4.1

ISO/IEC 19011:2002 Guidelines for quality and/or environmental management systems auditing

ISO/IEC 20000-1:2005 Information technology—service management—Part 1: Specification

ISO/IEC 20000-1:2005 Information technology—service management—Part 2: Code of practice

ISO/IEC 21827:2008 Information technology—Systems Security Engineering—Capability Maturity Model (SSE-CMM®)

ISO/IEC 27000:2009 Information technology—Security techniques—Information security management systems—Overview and vocabulary

ISO/IEC 27001:2005 Information technology—Security techniques—Information security management systems—Requirements.

ISO/IEC 27002:2005 Information technology—Security techniques—Code of practice for information security management

ISO/IEC 27005:2008 Information technology—Information security techniques—Information security risk management

ISO/IEC 27006:2007 Information technology—Security techniques—Requirements for bodies providing audit and certification of information security management systems

ISO/IEC 28000:2007 Specification for security management systems for the supply chain

ISO/IEC 38500:2008 Corporate governance of information technology

IT Governance Institute, Board Briefing on Governance, 2nd Edition, 2003

IT Governance Institute, Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition, 2006

ITGI Enterprise Risk: Identify Govern and Manage IT Risk—The Risk IT Framework, Exposure Draft version 0.1 February 2009.

Jericho Forum - http://www.opengroup.org/jericho/ and the Jericho Cloud Cube model http://www.opengroup.org/jericho/cloud_cube_model_v1.0.pdf

Justify Identity Management Investment with Metrics, by Roberta J. Witty, Kris Brittain and Ant Allan, 23 Feb 2004. Gartner Research ID number TG-22-1617.

Managing Assurance, Security and Trust for Services. Online. Available: http://www.masterfp7.eu/

National Association for Information Destruction Inc - http://www.naidonline.org/forms/cert/cert_program_us.pdf

NIST Guidelines for Media Sanitization (800-88) - http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf

NIST Recommended Security Controls for Federal Information Systems (SP800-53)

NIST SP 800-30 Risk Management Guide for Information Technology Systems

OATH- http://www.openauthentication.org

OCEG, Foundation Guidelines Red Book, v1 10/27/2008

OCTAVE-S Implementation Guide, Christopher Alberts, Audrey Dorofee, James Stevens, Carol Woody, Version 1, 2005

OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security

Open Cloud Computing Interface Working Group - http://www.occi-wg.org/doku.php

Open Security Architecture Group - http://www.opensecurityarchitecture.org

OpenCrowd - http://www.opencrowd.com/views/cloud.php

OpenID – http://openid.net

OpenID attribute exchange http://openid.net/specs/openid-attribute-exchange-1_0.htmlOAuth (created by a small group of individuals) http://OAuth.net/

OpenSocial – sharing social networking information http://www.opensocial.org/

ORCM Overcoming Risk And Compliance Myopia, August 2006 Online Available: http://logic.stanford.edu/POEM/externalpapers/grcdoc.pdf

OSAG Security Landscape - http://www.opensecurityarchitecture.org/cms/foundations/osalandscape

OWASP Top Ten Project, http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Princeton Startup Lawyer, "Company Formation-Fiduciary Duties (the basics)", June 17, 2009, http://princetonstartuplawyer.wordpress.com/2009/06/17/company-formation-fiduciary-dutiesthe-basics/

Python Runtime Environment, http://code.google.com/appengine/docs/

Rackspace API - http://www.rackspacecloud.com/cloud_hosting_products/servers/api

Sailing in Dangerous Waters: A Director's Guide to Data Governance, E. Michael Power &Roland L. Trope, (American Bar Association, 2005).

SAML- http://www.oasis-open.org/specs/index.php#saml

Security Guidance for Critical Areas of Focus in Cloud Computing, Version 1, by Cloud Security Alliance, April 2009

Service Level Agreements: Managing Cost and Quality in Service Relationships, Hiles, A.(1993), London:Chapman & Hall

SNIA Encryption of Data At Rest: A Step-by-Step Checklist http://www.snia.org/forums/ssif/knowledge_center/white_papers/forums/ssif/knowledge_center/white_papers/Encryption-Steps-Checklist_v3.060830.pdf

SNIA Introduction to Storage Security http://www.snia.org/forums/ssif/knowledge_center/white_papers/Storage-Security-Intro1.051014.pdf

SNIA Storage Security Best Current Practices http://www.snia.org/forums/ssif/forums/ssif/programs/best_practices/
Storage Security Best Current Practices (BCPs)" by the Security Technical Working Group of SNIA

Sun Project Kenai API - http://kenai.com/projects/suncloudapis
The Committee of Sponsoring Organizations of the Treadway Commission (COSO), Enterprise Risk Management—Integrated Framework (2004).

The Darker Side of Cloud Computing, by Matthew D. Sarrel, PC Mag.com, February 1, 2009

The Force.com Workbook,
http://wiki.developerforce.com/index.php/Forcedotcomworkbook

The Institute of Internal Auditors, Critical Infrastructure Assurance Project, "Information Security Governance: What Directors Need to Know", 2001

The International Grid Trust Federation (IGTF). http://www.igtf.net
United States General Accounting Office, Information Security Risk Assessment Practices of Leading Organizations, 1999.

United States Sentencing Commission, Guidelines Manual
vCloud API - http://www.vmware.com/solutions/cloud-computing/vcloud-api.html
Where We're Headed: New Developments and Trends in the Law of Information Security,

Thomas J. Smedinghoff, Privacy and Data Security Law Journal, January 2007, pps. 103-138

Windows Azure SDK, http://msdn.microsoft.com/en-us/library/dd179367.aspx

Windows Cardspace - http://msdn.microsoft.com/en-us/library/aa480189.aspx

WS-Federation :
http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-specos.html

