



金融部門でのクラウドの 利用について:

サーベイレポート

2015 年 3 月

© 2015 Cloud Security Alliance – All Rights Reserved

All rights reserved. You may download, store, display on your computer, view, print, and link to the Cloud Security Alliance “Cloud Adoptions Practices & Priorities Survey Report” at <https://cloudsecurityalliance.org/research/surveys/>, subject to the following: (a) the Report may be used solely for your personal, informational, non-commercial use; (b) the Report may not be modified or altered in any way; (c) the Report may not be redistributed; and (d) the trademark, copyright or other notices may not be removed. You may quote portions of the Report as permitted by the Fair Use provisions of the United States Copyright Act, provided that you attribute the portions to the Cloud Security Alliance “Cloud Adoptions Practices & Priorities Survey Report” (2015).

謝辭

Managing Editors / Researchers

John Yeoh
Frank Guanco

Contributors

Mario Maawad Marcos
Willy Leichter
Juan Francisco Losa
Tomas Herranz Medina
Mario Reyes
Maria Luisa Rodriguez
Chenxi Wang

Design/Editing

Texto Graphic Design

Special Thanks

The CSA Financial Services Working Group

Sponsored By



日本語版の提供について

本書「金融部門でのクラウドの利用について: サーベイレポート」は、CSAが公開している「How Cloud is Being Used in the Financial Sector: Survey Report」の日本語訳です。

本書は、原文をそのまま翻訳したものです。また、本書内で参照されている URL 等は、すべて英語版へのリンクとなっております。原文と日本語版の内容に相違があった場合には、原文が優先されます。

また、この翻訳版は予告なく変更される場合があります。以下の変更履歴(日付、バージョン、変更内容)をご確認ください。

変更履歴

日付	バージョン	変更内容
2015 年 4 月 15 日	日本語バージョン 1.0	

本書は、一般社団法人 日本クラウドセキュリティアライアンスの有志により作成されています。

日本クラウドセキュリティアライアンスに関する情報は、以下の URL より参照可能です。

<http://cloudsecurityalliance.jp>

2015 年 4 月 15 日



概要

クラウドインシデントを検出するためのビッグデータ/セキュリティの研究を基にして、Cloud Security Alliance は、クラウドセキュリティのトピックに対する情報技術当局の専門研究や深い専門知識を持った人からの豊富なデータやアドバイスを提供しています。Financial Services Working Group (FSWG)が、Cloud Security Alliance(CSA)の新しいワーキンググループとして創設され、2014 年の CSA EMEA Congress で正式に発表されました。FSWG は、安全なクラウドソリューションが金融業界においてどのように提供され管理されることができるかについての知識とガイダンスを提供するために発足しました。

FSWG の最初の活動の 1 つは、金融部門においてどのようなクラウドソリューションが展開されているかを示すために、その状況図を作成することでした。この目的のため、2014 年 9 月から 10 月まで「金融部門でどのようにクラウドが利用されているか」という調査を行いました。この研究の目的は、金融業界において、ベストプラクティスの採用を可能とすることによって、安全なクラウドサービスを採用するために必要なことを理解することです。これを達成するためには、最初に、クラウドサービスの展開と管理に関する金融業界の主な懸念点を分析することが必要です。これは、クラウドにおけるビジネスプロセスとデータの保護を保証するために、適切な戦略的セキュリティにアプローチすることと同様に、技術的かつ規制的に業界のニーズと要件を含めることです。

この研究では、クラウドソリューションの採用のレベルと金融機関の観点での要件の分析に関心のある 3 つの領域に焦点を当てました。それは、セキュリティの懸念点、クラウドサービスに対するアプローチ、コンプライアンスの懸念点です。

いくつかの重要な結果が、この研究から導き出されました:

- クラウドコンピューティングは、金融部門に普及してきています。そして、プライベートクラウドとパブリッククラウドの融合戦略がほとんどのビジネスにおいて一般的になってきています。
- ほとんどの組織は、一貫したクラウド移行戦略を持っていません。
- データ保護が、金融部門がクラウドに移行する際の最も大きな懸念点となっています。特に、データ保護基準と関連法は、調査回答者にとって「最初に浮かぶこと」になっています。
- 業界の規制は、金融機関がクラウドサービスへの移行を考える際に、特定のセキュリティ対策を実装するためのコンプライアンス要件となっています。

「金融部門においてクラウドがどのように利用されているか」という調査を行うにあたって、Cloud Security Alliance は、金融部門におけるクラウドコンピューティングに対する状況を調べ、安全なクラウドサービスの採用を促進するためのガイダンスを提供しようとしていました。調査から集められたデータおよび導き出された結果は、CSA の Financial Services Working Group が 2015 年の目標と提供物を詳細に検討する機会を提供します。提供された内容は、ワーキンググループに情報提供され、クラウドコンピューティングと金融サービスに関連した懸念点と機会を取り扱うための活動項目を提供することになるでしょう。

目次

謝辞.....	3
概要.....	4
目次.....	6
序論.....	7
調査回答者.....	7
クラウド利用は普及していますが、場当たりの利用に留まっています.....	8
金融機関に対する顧客の影響.....	8
プライベートおよびパブリッククラウド戦略.....	9
クラウドユーザの最前線におけるデータセキュリティの懸念.....	11
コンプライアンス.....	12
暗号化とトークン化.....	13
結果と概要.....	14

序論

私たちは、金融サービス機関の IT とセキュリティの専門家に対して、「金融部門でどのようにクラウドが利用されていますか」という調査を送りました。目標は、以下のトピックに関する議論を進めることでした:

- あなたの会社のクラウドコンピューティングに対するアプローチについて説明してください。
- プライベートクラウドのポリシーについて説明してください。
- クラウドコンピューティングに対する企業のリスクアセスメントはどのようになっていますか?
- クラウドプロバイダからのどのような機能が必要でしょうか?

そして、最後に…

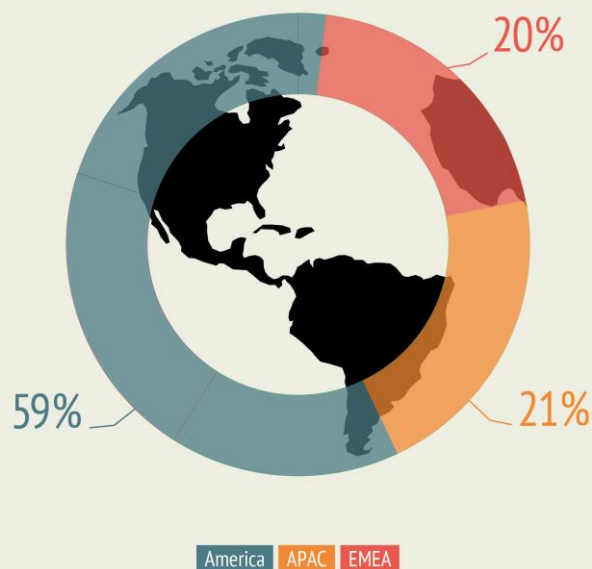
クラウドコンピューティングを採用する主な理由は何でしょうか?

クラウドサービスの採用に対する認識を高める以上に、調査の結果は、金融サービス業界の意思決定者が組織に対してどのようにアクションを取っていくかについての手掛かりを提供します。それは、最も安全なクラウドでサービスを確立し標準化することから、リスクを緩和するために適用するポリシーを知り、ユーザを教育する時にどこにフォーカスを当てるかを理解することです。

調査回答者

調査は 2014 年の第 4 四半期の 13 週間に渡って行われ、世界中から 102 人の回答を得ました。回答者の内訳は、銀行/クレジット・ユニオン (35%)、保険 (13%)、投資 (11%)、政府 (7%)、その他の専門的役割 (34%) でした。回答者は、20 か国に広がっていて、アメリカ地域 (59%)、アジアパシフィック (APAC) 地域 (21%)、ヨーロッパ中東アフリカ (EMEA) 地域 (20%) となっています。組織の規模は、従業員数 1-99 人 (8%)、100-500 人 (12%)、501-1000 人 (3%)、1001-5000 人 (16%)、5,001 人以上 (59%) となっています。一方、回答いただいた企業のクライアント数では、回答者の 26% が顧客数 0-1000 の小さなクライアントで、32% が 100 万人以上の顧客数のクライアントとなっています。

Participants by region



調査回答者の 64%は、組織の C-レベルの幹部社員かマネージャで、役割は以下のようになっています。

- 保証、セキュリティ、監査、リスク(情報システム)管理(38%)
- 情報システム管理、IT 専門家(34%)
- CSO/CISO (15%)
- ネットワーク/エンタープライズ・アーキテクト(7%)
- 事業部門(LOB)のオーナー(2%)
- その他(4%)。

クラウド利用は普及していますが、場当たりの利用に留まっています

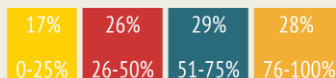
金融機関に対する顧客の影響

クラウドコンピューティングは、顧客がデータをやり取りする方法を変えています。この会社と顧客の間の情報交換は、最終的に金融業界がどのようにビジネスを行うかに影響を与えるでしょう。金融業界におけるクラウドの利用についてもっとよく理解するために、調査の回答者を地域と会社のサイズに従って分類しました。また、調査において、デジタル化された顧客数の割合も尋ねました。この研究において、デジタル化された顧客とは、銀行との取引において少なくとも 50%以上を電子チャネル(すなわち、オンラインバンキング、ATM、モバイル)を通して行っていることを表しています。

このデータは、金融機関の顧客基盤がクラウドコンピューティングへのアプローチにどのような影響を与えるかの状況を調べるための背景を提供しました。当然のことながら、デジタル化した顧客数が少ない企業は、クラウドへの移行は控えめになります - デジタル化した顧客が 25%未満の企業の 19%は、厳格にクラウドに移行しないというポリシーを持っています。対照的に、デジタル化した顧客を 26%以上持っている企業では、クラウドに移行しないというポリシーを持っているのはわずか 3%になります。さらに、クラウド戦略を既に持っている企業は、より多くのデジタル化した顧客数を持っている場合には 38%で、あまりデジタル化していない顧客を持っている場合には 13%になりました。

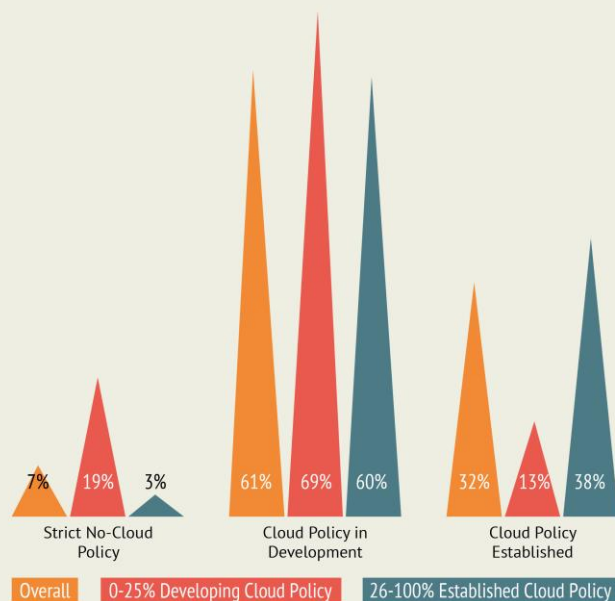
興味深いのは、小企業(500 人以下の従業員)と大企業(5,001 人以上の従業員)は、それぞれ 40%と 35%という最も高いクラウド戦略の採用率を示していました。501-5000 人の従業員がいる企業の 18%だけが、クラウド戦略を持っていました。アメリカ地域は、EMEA や APAC に比べてクラウド戦略を持つことに関して若干遅れをとっています。アメリカの 28%の企業がクラウド戦略を持っているのに対して、EMEA と APAC 地域ではそれぞれ 35%と 41%が既存のクラウド戦略を持っていると回答しました。

Digitalized Customer Base



プライベートおよびパブリッククラウド戦略

Cloud Strategy According to Digitalized Customer Base



金融業界は、まだクラウド採用の初期段階にあります。大部分(金融機関の 61%)が、組織の中でクラウド戦略を開発している段階です。最も一般的な戦略では、プライベート、パブリック、ハイブリッドのクラウド環境をミックスして使用しています。企業が採用する展開モデルは、まさにクラウド戦略の成熟度に関連しています。クラウドポリシーを既に持っている回答者の 9%だけが、プライベートクラウド（訳注：下の図によるとパブリッククラウドと思われます）を主に使用していると報告しました。クラウドを利用している金融系企業は、パブリッククラウドを使用しています。一方、その他の多くの企業は、プライベートクラウドとパブリッククラウドの両方を使用していて、大多数が社内サービスとパブリッククラウド環境を統合しています。クラウド戦略を開発中の企業は、パブリッククラウドを信頼した計画をほとんど立てていません。さらに、企業の 18%は、プライベートクラウドのみのモデルを使用したクラウド開発計画を立てようとしています。そのような計画を持っている企業は、実際にプライベートクラウドのみを使用している企業の倍の割合

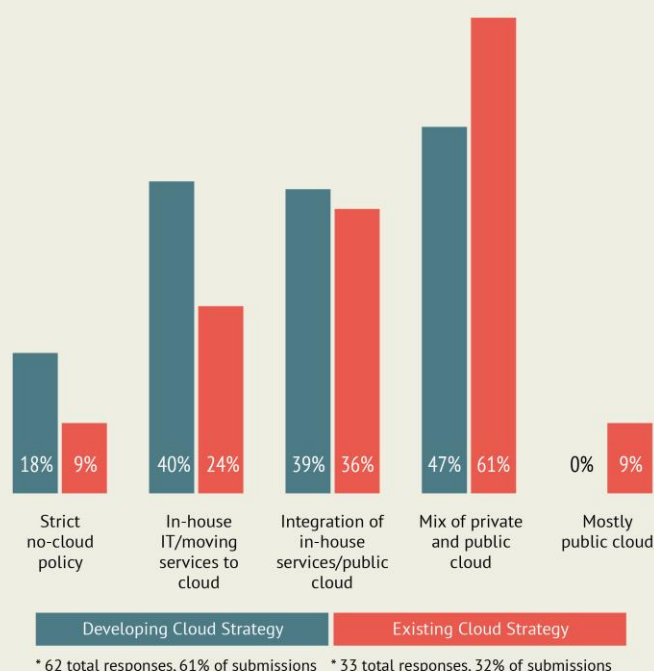
合となっています。これらの 2 つの統計は、クラウドを実際に利用するとき、追加の安心と保障が必要であることとクラウドの信頼に対する成熟度の証拠を示すことが必要であることを示しています。

厳格にプライベートクラウドのみを使用するポリシーを持っている企業に関して、その主な理由は以下になります：

- セキュリティの懸念 (86%)
- コンプライアンスの懸念 (86%)
- プライバシー(79%)
- データの保有と破棄(79%)
- データの格納 (57%)

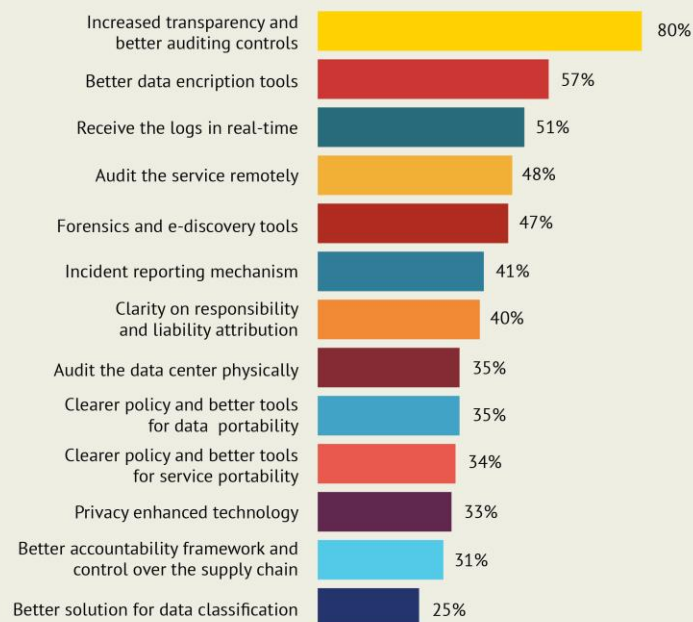
社内 IT、プライベートクラウド、パブリッククラウドのミックスが、最も一般的なクラウドのアプローチであるように、クラウド戦略を既に持っている企業の 70%が、ハイブリッドクラウドからプライベートクラウドとパブリッククラウドのミックス、あるいは、大部分パブリッククラウドに移行したことは興味深い内容になり

Cloud strategy - companies are approaching their cloud strategy



ます。これは、クラウドサービスを採用し、社内 IT に依存しないということに対する信頼が増加しているという別の兆候になります。柔軟なインフラを持ち、プロビジョニングの時間を削減し、総所有コストを減少させ、製品化までの時間を短縮することは、クラウド採用の主な理由になります。

Top Features Desired from Cloud Providers

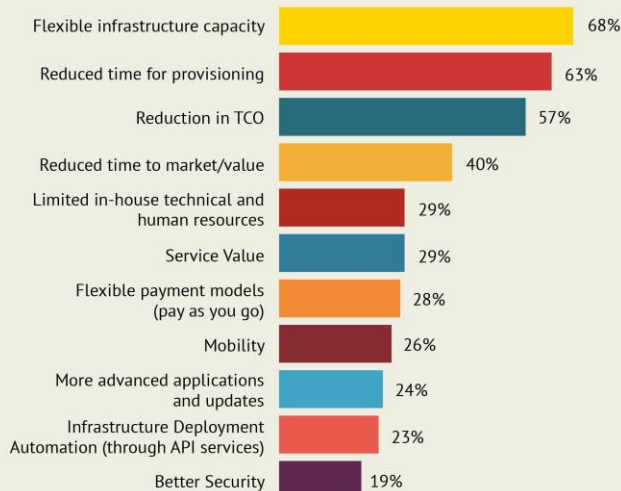


企業がクラウドを採用するかどうかは、クラウドサービスがユーザにとって重要な機能や特徴を提供するかということに大きな関係があります。これらの特徴と機能のいくつかは、セキュリティとコンプライアンスのために必要です。回答者によって報告された最も必要とされる機能は、「透明性の増大と、より良い監査のコントロール」(80%)です。その他の必要とされる機能は、より良いデータ暗号化ツール(57%)、リアルタイムのログ取得(51%)、リモート監査(48%)、フォレンジックと e-ディスカバリツール(47%)となっています。サービス自身、またもっと重要なことは、クラウドプロバイダがこれらの重要な機能にどのように適合しているかということが、特定のクラウドサービスをどのくらい早く採用するかを決定するでしょう。

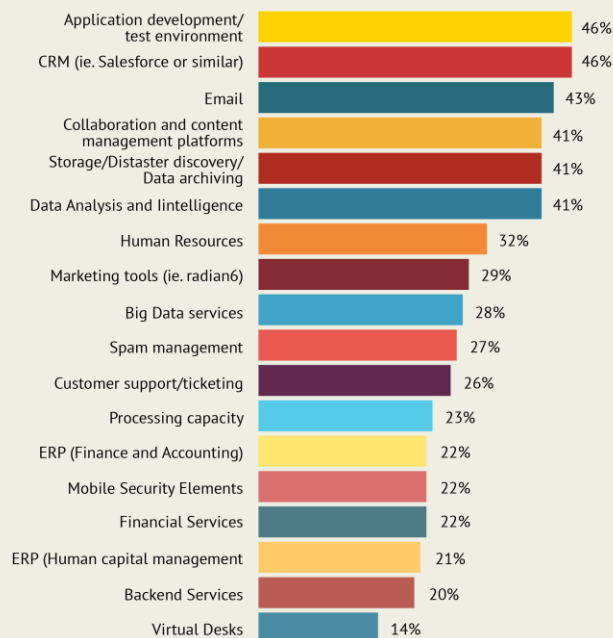
採用されている上位のクラウドサービス/アプリケーションは、現在、組織がクラウドプロバイダのどのようなサービスに力を入れているかについての情報を提供しています。Customer

Relationship Management(CRM)ツール(46%)、アプリケーション開発/テスト環境(46%)、email (43%)というのは、驚くことではありません。コラボレーションプラットフォーム(41%)、ストレージ機能(41%)、データインテリジェンス(41%)もまた、人気のあるクラウドアプリケーションです。1つのクラウドアプリケーションカテゴリが大部分の調査回答者によって採用されているということはありません。これは、ビジネスクラウド市場が実際に成長していることを示しています。

Primary reason for adopting cloud computing



Top Cloud Applications Adopted



クラウドユーザの最前線におけるデータセキュリティの懸念

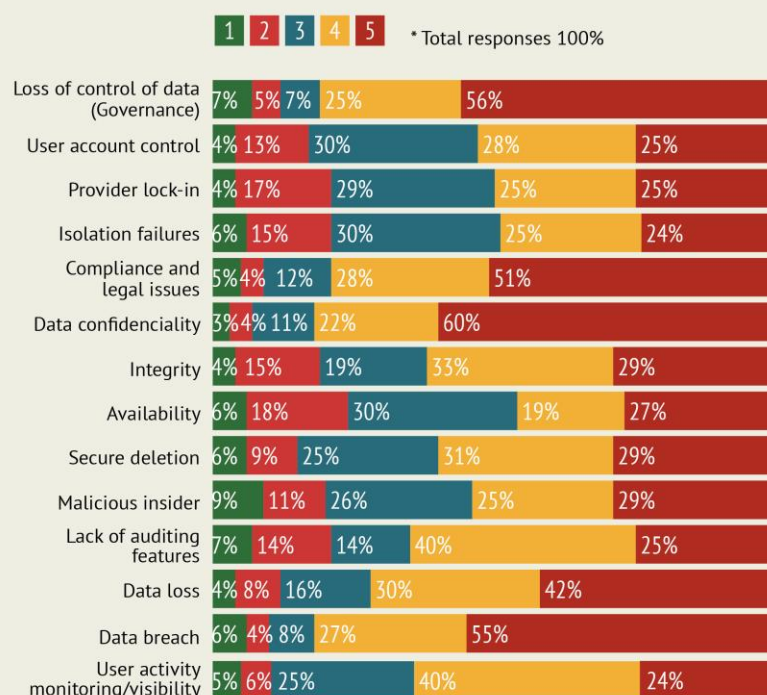
研究結果は、クラウドに関連するセキュリティの問題に対する継続的な懸念を示しています。43%の企業は、クラウドを採用する際に、違反を公に知らせることが最も大きな障害の1つであるとみなしています。13%の企業は、クラウド関連のセキュリティインシデントを報告しました。特に、データセキュリティは、報告されたインシデントにおいて最も一般的に引用された領域でした: データの可用性と漏えいは、クラウドインシデントの50%と報告されています。この内訳は、33%の不正アクセス、25%のマルウェアと他の障害を引き起こす脆弱性、17%のサービス乱用になります。

クラウドを採用しないこととして、回答者が報告した上位の理由は以下です:

- セキュリティの懸念 (100%)
- 規制上の制限(71%)
- 違反を公に知らせることの懸念(43%)

クラウドの採用を妨げている主な障壁である安全上の懸念に関して、よく知られたセキュリティの懸念点のリストにランク付けを行うように回答者にお願いしました。回答者は、1~5のスケールで懸念点の項目にランクを付けました。5が最大の懸念点になります。ここでも、データの機密性とデータのコントロールに関する懸念が最高になりました: 60%の金融機関は、データの機密性が最大のセキュリティの懸念点になるとランク付けしました。次が、データのコントロールの喪失(57%) (訳注: 図では56%となっています)、データ漏えい(55%)となりました。上位5つにランクされた懸念点のうち、唯一データ関連でないものは、法的およびコンプライアンス問題(51%)でした。それぞれの問題は、金融サービス企業がクラウドコンピューティングのパワーをよりよく利用するのを可能にするために、クラウドと技術のプロバイダにそれらの提供を強化する機会を与えています。

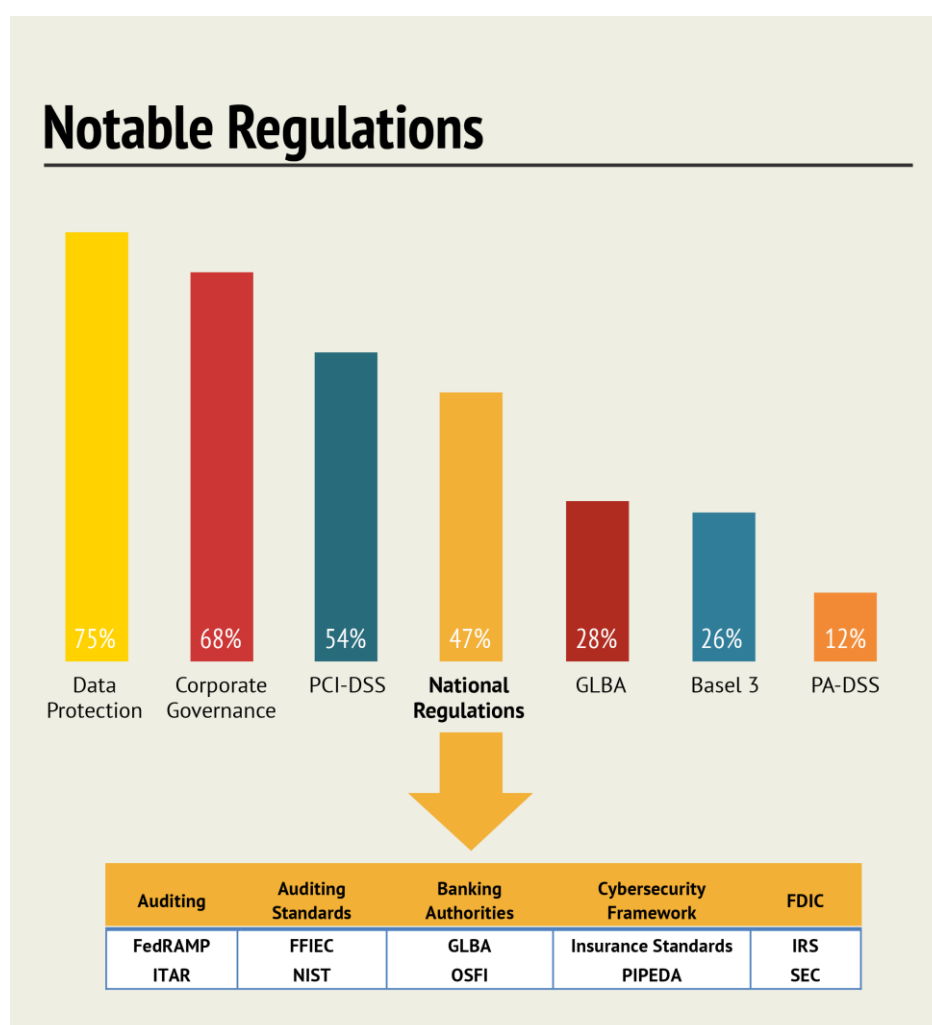
Cloud computing security concerns ranked



コンプライアンス

規制上の制限は、クラウドに移行する企業にとってもう 1 つの大きな障壁です。71%の金融系企業は、コンプライアンスを社内に対するコントロールを保つことの理由と考えており、パブリッククラウドサービスへのデータの移行の理由とは考えていません。調査回答者の 31%は、金融部門のための要件の議論において取締機関とのやり取りを行っていることを示しました。より多くの金融機関は、クラウドへの移行を統治するために特定の規制と規格に従っています。これらの特定の規定要件は、以下を含んでいます:

法規制のコンプライアンスについての更なる洞察を引き出すために、クラウドへの移行にあたってコンプライアンスを達成するのに重要であると考えている具体策をランク付けするように回答者にお願いしました。上位の回答は、マルウェア検出、監査許可、データの暗号化/トークン化になりました。以下に、上位にランク付けされたリストを示します:

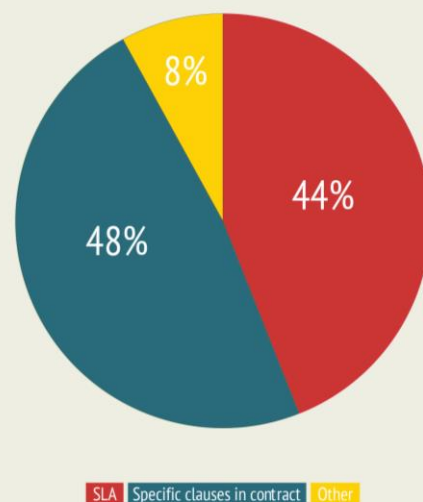


- セキュリティ対策 (マルウェア検出と削除、フォレンジックの用意ができていること、その他)の完全な実装 (66%)
- インシデントのため監査の許可 (57%)。
- 保存データの暗号化 (46%)
- データの暗号化あるいはトークン化(そして、キーを保有するビジネス)(46%)

- インシデントのための罰則条項(42%)
- クラウド上に顧客クライアントデータを置かない(20%)

コンプライアンスは、銀行および金融機関にとって重要な運用上の要件です。したがって、クラウドの採用においては、規定とポリシーのコンプライアンスを維持することを考えなければなりません。研究では、次にあげる手段を通して企業がクラウドプロバイダに対してコンプライアンス保証のアプローチを行っていることがわかりました: 特定の契約条項(48%)、SLA(44%)、監査(8%)。CSA Cloud Controls Matrix は、これらの領域のコンプライアンスのために一般的に使用されるツールです。さらに、コンプライアンスは、18%の金融機関において、社内ポリシー、コードレビュー、クラウド脆弱性のテストのための個別の監査方針に強化されています。

Ensuring compliance by service providers



* 102 total responses, 100% of submissions

暗号化とトークン化

データ保護は、クラウドサービスを考えている企業にとっては共通の懸念点です。したがって、金融機関で必要とされる主要なセキュリティツールとして、暗号化とトークン化機能があります。

クラウドの初期採用者と将来のユーザの両方が、暗号化機能を必要としています。しかしながら、回答者の42%しか、実際にクラウドに対してデータの暗号化ソリューションを実装していません。61%は、暗号化キーの所有権に懸念があると報告しました。重要なデータは機密にしなければならないので、暗号化鍵へのアクセスはデータへのアクセスを意味します。そのようなことから、企業は、鍵をクラウドに置くより、完全にオンプレミスで所有することを好みます。

データの匿名化技術、たとえば、トークン化やマスキングに関して、クラウドに移行するときにそのような対策を行う企業は少ないです(23%)。トークン化とマスキングは、重要な顧客情報、PII、PHI、特定の居住規制を持ったデータを保護するのにしばしば使用されます。

暗号化とトークン化は、社内のコンピューティングの安全とクラウドへの移行の両方のために、金融業界における重要な役割を果たし続けていることがわかります。結果として、展開される数が将来上昇することを期待します。

Encryption and Anonymization



結果と概要

インフラの柔軟性、総所有コストの減少、製品化期間の短縮は、クラウドに移行するためのいくつかの主要な理由になります。クラウドコンピューティングが金融業界の中でますます一般的になるにつれて、企業は適切にクラウドコンピューティングのメリットとリスクを評価する必要があります。この研究では、業界の大部分がクラウドの採用のためのアプローチを固め、協調しようとしています。セキュリティは最大の障壁のまま残っていることがわかりました。この研究の回答者は、より可視性の高さ、ログへの素早いアクセス、データのより良い保護を要求していました。クラウドプロバイダは、これらの要件と特定の業界の規制に対応する方法をさらに理解していくために、金融機関と共に作業していく必要があります。

監査のためのより良いツールとデータ保護がさらに主流になっていくとき、企業はセキュリティとコンプライアンスに対する姿勢を維持しながら、より快適に重要なデータをクラウドに移行したいと感じるでしょう。クラウドプロバイダと企業とのセキュリティ責任の分割に対する適切なガイダンスとより深い理解は、金融部門におけるより広いクラウドサービスの採用につながるより大きな信頼を築き上げるでしょう。

About the Cloud Security Alliance

The Cloud Security Alliance is a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing. The Cloud Security Alliance is led by a broad coalition of industry practitioners, corporations, associations and other key stakeholders. For further information, visit us at <http://www.cloudsecurityalliance.org/>, and follow us on Twitter @cloudsa.

About CipherCloud

CipherCloud, the leader in cloud visibility and data protection, delivers cloud adoption while ensuring security, compliance and control. CipherCloud's open platform provides comprehensive cloud application discovery and risk assessment, data protection – searchable strong encryption, tokenization, data loss prevention, key management and malware detection – and extensive user activity and anomaly monitoring services. CipherCloud has experienced exceptional growth and success with over 3 million of business users, across 11 different industries. The CipherCloud product portfolio protects popular cloud applications out-of-the-box such as Salesforce, Box, Microsoft Office 365, and ServiceNow.

CipherCloud, named as SC Magazine's Best Product of the Year, technology is FIPS 140-2 validated and is backed by premier venture capital firms Transamerica Ventures, Andreessen Horowitz, Delta Partners, and T-Venture, the venture capital arm of Deutsche Telekom. For more information, visit www.ciphercloud.com and follow us on Twitter @ciphercloud.