2016年7月

クラウドネイティブ時代におけるリスク管理策

企業システムにおいて、クラウドサービスの利用が第一候補として挙がることは珍しくなくなり、業務用パッケージソフトなどはクラウド環境を前提としたものが市場に投入され始めている。

また、IoT[1]やAI[2]、Fintech[3]など注目を集めているサービスやテクノロジーはクラウドを基盤として活用することで、開発期間短縮や柔軟な構成を実現しているものが多い。こうした背景から最近ではシステム構築やアプリ開発において「クラウドネイティブ」という言葉が台頭してきている。

一方でクラウドにおけるインシデント事例も絶えず報告されており、クラウド導入についての懸念点としてセキュリティが上位に挙げられることも少なくない。

本稿ではクラウドのセキュリティについて最新動向を取り上げるとともに、クラウドを利用するうえで考慮すべきリスクとその管理策について解説する。

なお本文中の意見に関する部分については、筆者の私見であることをあらかじめお断りする。

1. クラウドにおけるセキュリティの最新動向

(1) クラウドサービスのインシデント事例

クラウドコンピューティングという概念が提唱され今年で10年が経った。その有益性が認識され利用者が急激に増加する一方で、利用者に大きな影響を与えるインシデントも断続的に発生している（図表1参照）。それらのなかから特徴的な事例について紹介する。

1 Internet of Thingsの略。モノのインターネット。

2 Artificial Intelligenceの略。人口知能。

3 FinanceとTechnologyを組み合わせた造語。ITを利用した金融サービスやそれに関連する技術を総称する。

【図表1】クラウドサービスにおけるインシデント事例

項番	発生事象	影響
1	運用管理ソフトウェアの不具合により誤った設定を投入	数十分間に渡り全世界でサービスの利用が不能
2	正規プロセスに従わず作業を実施してミスが発生	Webやメールなどのデータが消失
3	事業者のサーバを捜査機関が押収	押収されたサーバを利用していた複数ユーザのシステムに影響
4	オンラインストレージ上に数千万人分の個人データの不正アップロード発生	氏名や住所などの個人情報が流出
5	サービスへの新機能追加後に不具合が発生	当該サービスを利用していたアプリやWebサイトが数時間利用不能
6	事業者が倒産	利用者に対し約2週間以内の移行期限
7	データセンターのストレージネットワークにて障害が発生	パフォーマンス低下やデータ消失などが発生
8	ユーザ数拡大に対する設備リソース不足発生	機能停止やパフォーマンス低下などが数週間に渡って継続
9	仮想化ソフトの脆弱性を突く攻撃が発生	数十万台分のサーバデータが消失
10	SaaSについて共有権のバグが発覚	意図しない相手へのファイル共有が発生

出典:公開情報を元にKPMGが作成

- 事例A（図表1の項番1）運用管理用ソフトウェアの不具合によるサービス中断

  クラウド事業者のメンテナンス作業中、運用管理用ソフトウェアが設定内容に不整合を発見したため、自動で作業直前の設定へ戻るよう動作した。ところがこの動作部分のバグにより、直前の設定ではなく必要な情報まで削除した設定が実施されたことで、事業者が異常に気づき回復措置を行うまでの数十分間に渡り全世界でサービスが利用できなくなった。

  不具合が連続したことが要因のインシデント発生であり、極めて稀な事象とは考えられるが、集中制御と自動化が進むクラウドでは、1つの作業トラブルが全世界に影響を及ぼす可能性があることを示した例である。

- 事例B（図表1の項番2）作業ミスによるサーバデータ消失および情報漏えい

  クラウド事業者がメンテナンス作業時に、社内マニュアル記載の手順に従わず作業を行った結果、本番環境とバックアップ双方の顧客データが消失した。さらに顧客データ消失に対するマニュアルが存在せず、動作確認が不十分な復元プログラムを使ってデータ復元を試みたことで、複数の顧客間でデータが混在してしまい、情報漏えいというさらなるインシデントが発生した。

  最終的に事業者側では消失したデータを復旧することはできず、利用者が自らの手元にあるバックアップからの復旧を試みることとなった。事業者内の管理体制と利用者側の自衛措置の必要性が問われることとなった事例である。

• 事例C（図表1の項番3）捜査機関のサーバ押収によるサービス停止

現地の捜査機関により、クラウド事業者に全データセンター停止とサーバなどすべての機材押収が命じられた。当該事業者を利用している一部利用者の不正行為に対する捜査が目的であったが、捜査とは無関係の利用者についてもシステムが利用できなくなるなどの事態に発展した。

クラウドサービスの特徴である複数顧客でのリソース共有のリスクと、現地の法令というリスクが組み合わされ、利用者に深刻な影響を与えた事例である。

(2) クラウドセキュリティにおける評価・認定制度

クラウドサービスのリスク対策やコンプライアンス対応については、多くのクラウド事業者で優先課題として認識されており、事業者によっては取組みの具体的な内容をホワイトペーパー等で公開している。

こうした情報に加えて、第三者による評価・認証制度を利用し、利用者に対してより客観性と信頼性が高い情報を公開するという動きも積極的に行われている。例としてはISO/IEC 27001、PCI DSS、SOC2等の取得や利用、国内外の組織・団体により作られた基準やガイドラインへの準拠等が挙げられる。

そのような状況において注目されているのが、クラウドセキュリティの国際規格として2015年12月に発行されたISO/IEC 27017:2015（以下、「ISO27017」という）である。これは日本の経済産業省が発行したガイドライン[4]がベースとなっており、策定にあたりさまざまな国や組織・団体の議論が反映されている。

ISO27017ではクラウド特有の考慮事項について、利用者と事業者それぞれの立場でどのようなリスク管理を行うべきかが定められており、ISMSに準拠している組織がクラウドに対する追加の管理策として利用することを前提としている。このためISMS導入済みの組織にとっては既存の体制に組み込み易く、加えて2016年夏にISO27017に基づいたISMSクラウドセキュリティ認証が、一般財団法人日本情報経済社会推進協会（JIPDEC）により開始される予定[5]となっていることから、ISMS導入が進んでいる日本国内での早期の普及が期待されている。

2. クラウドサービス利用に関する主なリスクと対策

本章ではクラウドサービスに関するリスクについて、米国国立標準技術研究所（National Institute of Standards and Technology：NIST）が発行したドキュメントを独立行政法人情報処理推進機構（IPA）が日本語訳を行った「SP800-144 パブリッククラウドコンピューティングのセキュリティとプライバシーに関するガイドライン」[6]から、特にクラウド利用者の立場から注意すべきリスクを3つ紹介し、あわせてそのリスクに対する管理策として筆者の私見を述べる。

---

4 経済産業省「クラウドサービス利用のための情報セキュリティマネジメントガイドライン 2013年度版」
http://www.meti.go.jp/press/2013/03/20140314004/20140314004-2.pdf

5 一般財団法人日本情報経済社会推進協会「ISMS適合性評価制度　ISO/IEC 27017に基づくクラウドセキュリティ認証開始のお知らせ」（2015年11月16日）
http://www.isms.jipdec.or.jp/topics/ISO27017_CLS.html

6 独立行政法人情報処理推進機構「セキュリティ関連NIST文書」（2014年5月19日）
http://www.ipa.go.jp/security/publications/nist/

【図表2】クラウドのセキュリティにおける課題

項番	分類	項目
1	ガバナンス	利用者と事業者間の役割と責任不明確
2		正規手続を経ない利用
3	コンプライアンス	データ所在地と適用される法令
4		電子的証拠開示能力
5	信用	内部関係者によるアクセス
6		データ所有権
7		複合型サービス提供形態 （サプライチェーン間の役割と責任の複雑化）
8		情報セキュリティの可視性不足
9		クラウド利用で生じる二次データの侵害
10		事業者内のリスクマネジメント
11	アーキテクチャ	ハイパーバイザに対する攻撃
12		仮想ネットワークの保護
13		仮想マシンイメージの保護
14		クライアント側の保護
15	アイデンティティとアクセスの管理	不十分な認証
16		不十分なアクセスコントロール
17	ソフトウェアの隔離	ハイパーバイザの複雑性
18		マルチテナントに起因する攻撃
19	データの保護	情報集中による高い攻撃価値
20		テナント間のデータ保護
21		不十分なデータ削除
22	可用性	一時的なサービス停止
23		長期的および恒久的サービス停止
24		サービス拒否攻撃（DoS）
25	インシデント対応	モニタリングデータの可用性
26		分析と解決に必要な情報の不足

出典：NIST発行「SP800-144 パブリッククラウドコンピューティングのセキュリティとプライバシーに関するガイドライン」をIPAが日本語に訳した資料を基にKPMGが作成
（http://www.ipa.go.jp/security/publications/nist/）

(1) ガバナンスにおけるリスク

- クラウドの利用に対する組織内ルールが整備されていない状況においては、情報システム部門やコンプライアンス部門などのチェックといった正規プロセスを経ずに事業部門や個人がクラウドを利用し、シャドーIT化してしまう恐れがある。そうした状況を放置してしまうと、情報資産の漏えいなど重大なインシデントを引き起こしかねない。

→ クラウドの利用に関する社内ルールの整備と遵守を徹底すること。その際には社内の利用状況をよく調査し、厳しく禁止するだけではなく業務に不可欠なサービスなどがあれば、うまくコントロールすることも必要である。

加えて技術面からのアプローチとして、CASB[7]などクラウドサービス利用状況の可視化やアクセス制限、ログ記録等を行うことができる製品やサービスも登場しており、先進的な組織における導入事例も報告されている。

- 事業者内のリスク管理体制については直接利用者から確認することは難しく、いざ重大なインシデントが発生してから明らかとなる場合も多い。

また利用者である自組織と事業者間の役割・責任分担を明確にせず、これくらいまでは対応してくれるはずといった、思い込みに基づいたリスク管理は危険である。運用時の脆弱性管理やインシデント発生において、双方の対応が進まないまま、事態のみが進行し、より深刻な影響を及ぼすことが懸念されるためである。

→ 利用するクラウドサービスの選定にあたっては、機能や価格だけではなく、セキュリティやコンプライアンスに対する取組み、第三者による評価・認定の状況等も比較すること。管理策の具体的な内容についてはオープンになっていないことが多いため、必要に応じてNDA契約（Non-Disclosure Agreement：秘密保持契約）を締結して開示を依頼する。また、役割や責任等の具体的な内容については契約時に書面で確認すべきであり、場合によってはSLA（Service Level Agreement：サービス品質保証）による保証を求めることも有効である。

(2) コンプライアンスにおけるリスク

- クラウドサービスのシステム環境は事業者に任せ、利用者側はほとんど意識する必要がないことは、クラウドを利用するうえで大きなメリットである。ただし、データの収集・保存場所がどこの国または地域になるかといった点について考慮を怠ると、適用される法令や規制により想定外の事態が発生することも考えられる。

たとえば、EU域内で収集した住民の個人情報については、十分なデータ保護レベルを確保していない第三国へのデータ移転を禁止する「EUデータ保護指令」という法律が存在し、第三国に分類される日本へデータを転送した場合、この法律に抵触する可能性がある。

一方で事例Cでも紹介したように、法令や司法当局の強い権限によりデータの閲覧や差し押さえが比較的容易に行える国や地域も存在し、自らが当事者でなくとも巻き添えで情報漏えいの危険にさらされることもあり得る。

→ データの保存場所については事業者に対して開示を要求すること。現地の法令については事業者から情報提供を受けられる場合もあるが、最終的なリスクは利用者側が負わざるを得ないため、利用者自身の責任で調査するべきである。法令の変更に対する追従や米国のように州ごとに法令が異なるといった状況に対応するために、外部の調査機関の利用も検討する余地がある。また、無関係な捜査等に巻き込まれた場合の閲覧や差し押さえによる情報漏えいに対する備えとして、データ伝送中および保存中の暗号化も自衛手段として有効である。

クラウドのバックアップ機能等を利用する際には、想定外の場所にデータが保存されないよう、技術仕様については詳細を理解しておく必要がある。

---

7 Cloud Access Service Brokerの略。主にSaaSの利用状況について可視化や制御を行う。

- 訴訟などが発生し、クラウド上のデータ、更新日等のメタデータ、操作変更履歴等が電子的な証拠として開示が必要となる際に、利用しているクラウドサービスが十分な電子的証拠開示能力を有しているかが、訴訟に影響を与えることも考えられる。

  → ログ取得機能や保存期間等、電子的な証拠開示能力について事業者に情報開示を求めること。たとえば法令などで3年間の保存が義務づけられているログについて、1年間の保存能力しか有さない事業者を利用することは大きなリスクとなるため、事業者を変更するか、利用者側で独自にログを保存するなどの代替案が必要となる。

(3) 可用性に対するリスク

- クラウドサービスでは高い信頼性と可用性を実現するため、事業者は設計や運用に対してさまざまな改善を続けているが、サービス停止時間をゼロにすることは難しい。可用性が99.95%とうたわれているサービスについては、年間で4時間程度のダウンタイムが発生する想定である。またメンテナンス作業についても、事業者都合によりスケジュールが決められるため、利用者の業務において不都合な時間帯にシステムが停止する可能性もある。

  → データセンターやリージョンを跨って代替サーバやサービスを準備しておくことで、業務影響を最小限にすることができる。また事例Aで示したような全世界のリージョンが停止するような事態に対しては、通信回線において複数通信キャリアを利用して信頼性と可用性を確保するキャリアダイバーシティのように、複数クラウド事業者を利用するクラウドダイバーシティが有効である。

- クラウド事業者は厳しい競争環境にさらされており、サービスやテクノロジーも日々進化を続けている。そのため一時的な停止ではなく、クラウドサービスの終了や事業者自体の廃業などにより恒久的に利用できなくなるといった事態も想定される。

  → 契約時にサービス終了についての告知期限に関する条文を追加し、契約後も事業者の経営状態の定期的なチェックなどを行い、突如サービスが使えなくなってしまうというリスクは最小限に抑えておくこと。また、利用しているサービスやデータ形式が特定のクラウドサービスに過剰に依存してしまうと、そのサービスの終了が利用者の業務に大きく影響してしまうため、常に代替案を検討しておくことで、そうしたリスクを下げることができる。前述のクラウドダイバーシティも代替案の1つである。

3. まとめ

以下にクラウドセキュリティにおけるポイントをまとめる。

・クラウドサービスの利用者に影響が大きいインシデントは断続的に発生している。

・国際規格制定などクラウドセキュリティ向上のための取組みが進んでおり、事業者選定における評価項目の1つとして活用できる。

・クラウドのリスクは事業者側の取組みも必要だが、利用者側も適切な管理策を取り入れていくことで、よりリスクを低減させることができる。

KPMGコンサルティング株式会社
マネジャー　宮田 高明

KPMGコンサルティング株式会社

東京本社
〒100-0004
東京都千代田区大手町1丁目9番5号
大手町フィナンシャルシティ　ノースタワー
TEL ： 03-3548-5305
FAX ： 03-3548-5306

大阪事務所
〒541-0048
大阪市中央区瓦町3丁目6番5号　銀泉備後町ビル
TEL ： 06-7731-2200

名古屋事務所
〒450-6426
名古屋市中村区名駅3丁目28番12号　大名古屋ビルヂング
TEL ： 052-571-5485

kpmg.com/jp/kc