企業におけるクラウドの利用とそのリスク

目　　次

主任研究員　海老﨑　美由紀

要　　約

Ⅰ．はじめに

企業におけるクラウドサービスの利用が進み、クラウド障害が発生したときは事業運営に大きな影響を及すようになり、企業はこれまでとは異なる新たなリスクを抱え込んでいる。本稿ではクラウド障害のリスクとその影響について取り上げる。

Ⅱ．拡大するクラウドサービスの利用とリスクの所在

世界のクラウドサービス市場は急速に伸びており、日本においても過半数の企業が利用するようになった。クラウドサービスは複数のサービスの組み合わせで構成されており、近年さらに高度化し複雑になってきている。マルチテナント化によってコスト削減を図っているが、リスクも生じている。サービスレベルアグリーメント（SLA）にて利用者の責任範囲が示されており、障害発生時の補償は往々にして利用料の一定割合のみとされている。

Ⅲ．クラウド障害の発生状況と保険の利用

クラウド障害の多くはハードウェアの不具合やシステムのアップグレード、バグによって引き起こされている。サイバー攻撃を原因とする障害の件数は少ないが、発生すると長期間影響を受ける可能性がある。金額としては事業継続に影響が出たことによる損害が占める割合が高く、情報漏えいを伴った場合はさらに大きな損害となる。また、多くの企業が影響を受けることによって経済全体に影響を与えることにもなる。

損害保険会社のサイバー保険では、サイバー攻撃だけではなく、システムオペレーションミス、システムの管理不備等の過失に起因する事故も対象とし、賠償責任や事故対応費用だけでなく、喪失利益も対象とすることができる。さらに損害保険各社のグループ会社を通じて予防策の提案サービスを行う。

Ⅳ．情報の収集と開示

クラウドサービスのセキュリティについて第三者機関の評価を参考にすることができる。サイバーセキュリティの強化は重要課題であり、公共機関により情報共有が進められている。クラウドサービス提供業者によるクラウド障害の情報開示も行われているが比較可能性に乏しく、最新の情報を利用した質の高い分析・研究が行われることが望まれる。

Ⅴ．おわりに

構造を複雑化させながら急速に拡大するクラウドサービスのリスクは､完全に把握することが難しい。グローバル化が進み、広範な情報収集とリスク分析が進められることが望まれる。想定されるリスクについて防御する対策をとり、保険へのリスクの移転や万が一発生した場合の事後策の検討を進めることが促される。

Ⅰ．はじめに

企業におけるクラウドサービスの利用が進み、自社で開発したシステムではなく、クラウドサービスによって提供されるシステム環境を利用することでシステム開発が容易に、かつ迅速に行えるようになってきた。これまで企業内のシステムは組織の中で閉じられた世界であったが、クラウドサービスの利用を進めることで、システムを企業外部にアウトソースし、外部と密接に関係するようになった。企業の内部と外部が複雑に連携したシステムに依存するようになり、それが障害を起こしたときには、事業運営に大きな影響を及ぼすようになってきている。クラウドサービスを利用する企業はこれまでとは異なる新たなリスクを抱え込んでしまっていることを十分認識しているだろうか。

本稿ではクラウドが障害によりダウンするというリスクとその影響について取り上げる。まずは、クラウドサービスについてリスクの観点から特徴を挙げる。次に、クラウド障害がどの程度発生し、それが企業の収益にどのような影響を与えるのか、オープンにされている統計や調査結果を用いて示す。

新たに生じ増加しつつあるリスクの把握は難しい。社会を支えるインフラとして重要性を増しているクラウドサービスであるからこそ、広範な情報収集や体系的な統計の蓄積、さらに対処法の策定に役立つような分析が今後も進められることが望まれる。

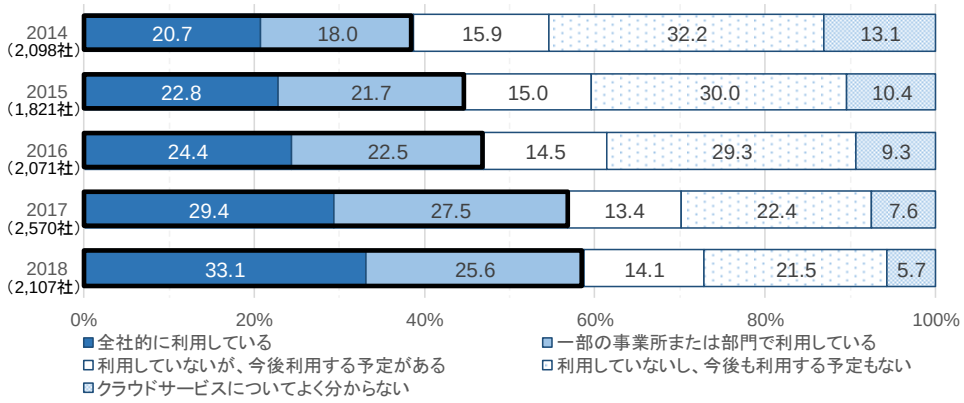
Ⅱ．拡大するクラウドサービスの利用とリスクの所在

１．クラウドサービス利用の拡大

（１）拡大するクラウドサービス市場

クラウド（クラウド・コンピューティング）は、コンピュータの利用形態のひとつであり、クラウドの利用者はインターネットなどのネットワークに接続されたコンピュータ（サーバー）によって提供されるクラウドサービスを使う[1]。世界のクラウドサービス市場は急速に伸びており、2020 年には 3,000 億ドルを突破すると予想され、日本国内市場は 2018 年に 2 兆円弱になったとされる[2]。日本においてもクラウドサービスの利用が拡大し、総務省の調査では2017年に利用している企業が過半数を超えた（《図表Ⅱ-1》参照）。

《図表Ⅱ-1》日本企業によるクラウドサービス利用状況



（出典）総務省「情報通信白書令和元年版」（2019 年）より SOMPO 未来研究所作成（データは総務省「通信利用動向調査」）。

[1] NEC ウェブサイト「クラウドサービスとは？例を交えて解説！初心者にもわかるクラウド入門（第１回　そうか！わかった。クラウドサービス）」<https://jpn.nec.com/cloud/smb/column/01/index.html>（visited Feb. 12, 2020）

[2] MM 総研「2019 年国内クラウドサービス需要動向調査」（2019 年 6 月 11 日）。

（2）企業がクラウドを利用する理由と評価

企業がクラウドサービスを利用する理由として、システムの効率性、セキュリティ水準、技術革新対応力、柔軟性、可用性の高さが挙げられる[3]。2019 年の総務省の調査によると、企業がクラウドサービスを利用する理由として「資産保守体制を社内に持つ必要がないから（41.6%）」、「どこでも、機器を選ばずに同様のサービスを利用できるから（33.8%）」「サービスの信頼性や情報漏えい等へのセキュリティが高いから（31.9%）」、「安定運用、可用性が高くなるから（29.6%）」「災害時のバックアップとして利用できるから（26.2%）」などが上位に挙げられている[4]。企業のクラウドサービス利用が拡大する背景には、IT 人材の確保難や企業間の競争激化からシステム開発の迅速化が求められることなどがあると考えられる[5]。

一方で、クラウドサービスを利用していない国内企業においては、その理由として「必要がない（41.6%）」に続き「情報漏えいなどセキュリティに不安がある（30.1%）」とする割合が大きい[6]。先の利用する理由とは逆となっており、情報セキュリティに関する信頼性の評価は二分されているようである。大手のクラウドサービス提供業者は、自社のクラウドシステムについて高いセキュリティ対策を施しており、一般の企業に比べてセキュリティのレベルは高いと考えられる[7]が、重要なデータをクラウドサービス提供業者に託すことにより不安を抱くのではないかとされる[8]。また、業態によって求められるセキュリティのレベルが異なり、クラウドサービスに求めるセキュリティレベルに差が出るとも考えられる。

2．高度に複合されるシステム

（1）クラウドサービスの種類

クラウドサービスは、提供するサービスの範囲に応じて IaaS、PaaS、SaaS の大きく 3 つに分かれる（《図表Ⅱ-2》参照）。また一般的な分類として、限定されない多数の利用者で共用するパブリッククラウドと、単一の組織専用に提供されるプライベートクラウドがある[9]。本稿では、より企業外部との関連が大きいパブリッククラウドを念頭に置いている。

《図表Ⅱ-2》クラウドの種類

IaaS (Infrastructure as a Service)	利用者に、CPU 機能、ストレージ、ネットワークその他の基礎的な情報システムの構築に係るリソースが提供されるもの。利用者は、そのリソース上にＯＳや任意機能を構築することが可能。
PaaS (Platform as a Service)	IaaS のサービスに加えて、ＯＳ、基本的機能、開発環境や運用管理環境等もサービスとして提供されるもの。利用者は、基本機能等を組み合わせることにより情報システムを構築。
SaaS (Software as a Service)	利用者に、特定の業務系のアプリケーション、コミュニケーション等の機能がサービスとして提供されるもの。業務系のサービス、メールサービスやファイル保管等のコミュニケーション系のサービス等がある。

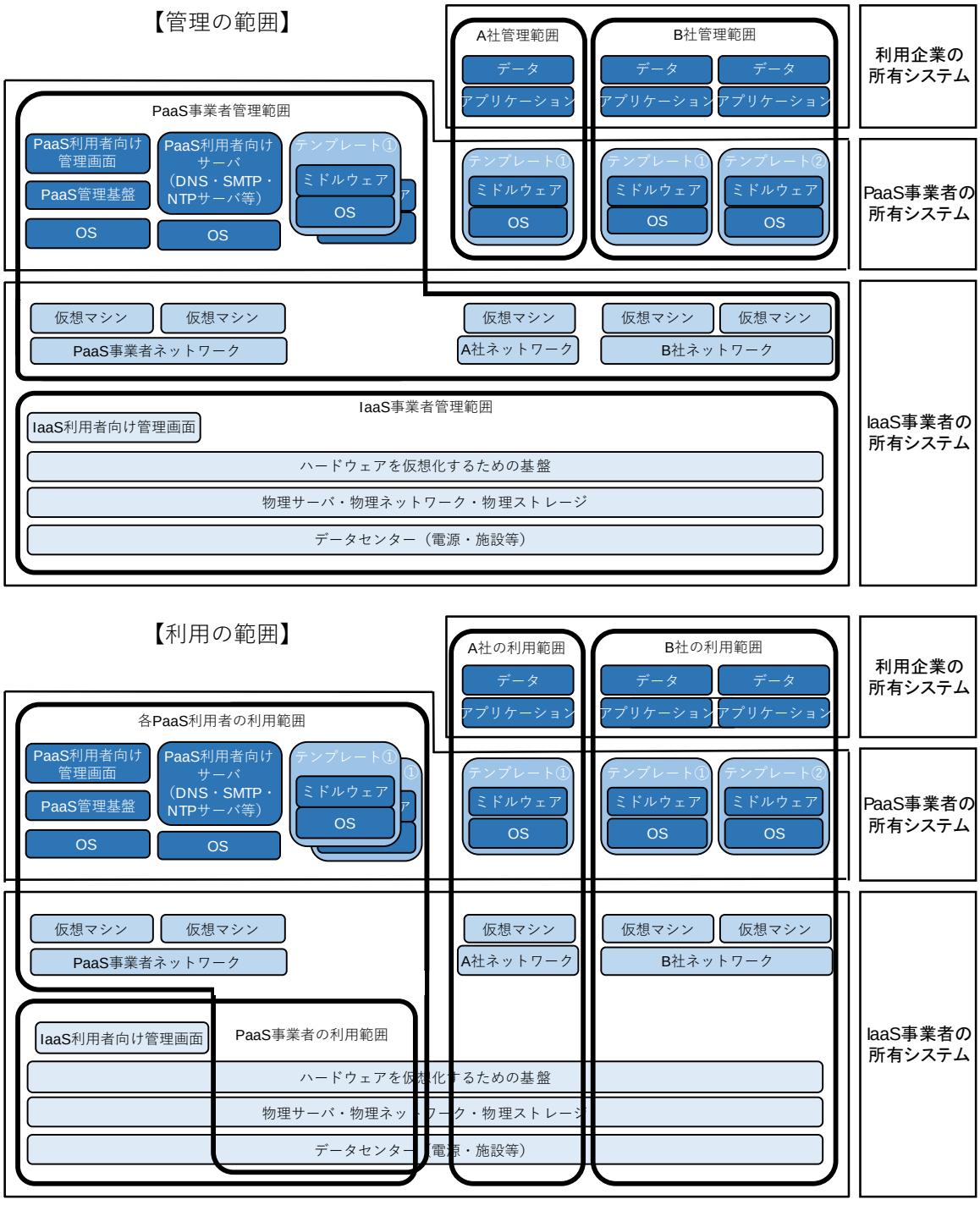
（出典）内閣官房 IT 総合戦略室「政府情報システムにおけるクラウドサービスの利用に係る基本方針」（2018 年 6 月 7 日）より SOMPO 未来研究所作成。

[3] 内閣官房 IT 総合戦略室「政府情報システムにおけるクラウドサービスの利用に係る基本方針」（2018 年 6 月 7 日）。
[4] 総務省「情報通信白書令和元年版」（2019 年）。
[5] マイナビニュース「AWS、長崎社長が IT 人材育成に向けた教育プログラムについて説明」（2018 年 9 月 3 日）。
[6] 回答割合はずっと小さくなるが、セキュリティに続いて「クラウド導入に伴う既存システムの改修コストが大きい（17.0%）」、「ネットワークの安定性に対する不安がある（16.1%）」がクラウドを利用しない理由として上位に挙がっている。
[7] クラウドサービスには、外部から脆弱性を攻略されるといった類のサイバー攻撃について、提供者側がシステムの OS や Web サービスなどのプログラムを自動的にアップデートすることにより脆弱性が解消されるというメリットがある。
[8] KPMG コンサルティング、「マルチクラウド時代のリスクマネジメント入門」（2019 年 3 月）。
[9] 金融情報システムセンター「金融機関におけるクラウド利用に関する有識者検討会報告書」（2014 年 11 月）。

（２）複数のサービスの組み合わせで構成されるクラウド

クラウドサービスの一つの特徴として、全体が複数のサービスの組み合わせで構成されていることがある。物理サーバ、物理ネットワーク、物理ストレージやそれらのハードウェアを仮想化するための基盤、仮想マシン、OS、管理基盤、ミドルウェア、それらの管理画面などから構築されており、往々にして異なる複数の業者が提供するサービスを組み合わせて利用される。《図表Ⅱ-3》はPaaSを例にしたモ

《図表Ⅱ-3》クラウドサービスの構成と利用・管理の範囲（PaaSを例にしたモデル）



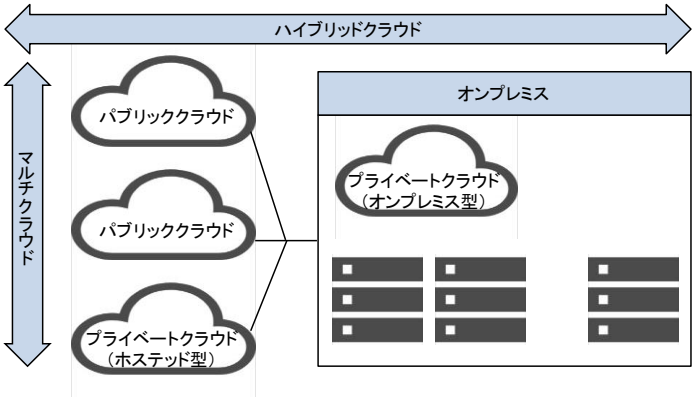
（出典）JASAクラウドセキュリティ推進協議会「エンタープライズクラウド選定ガイド、クラウド選びで困ったら要求仕様作成と提案書評価のための基礎知識」（2016年１月）よりSOMPO未来研究所作成。

デルであり、利用企業、ミドルウェアを提供する PaaS 事業者、インフラを提供する IaaS 事業者がそれぞれ所有する資産の範囲、管理範囲、利用範囲を示している。上段が責任の範囲を示す管理範囲であり、下段が利用範囲である。利用企業が利用する範囲の中に自社の管理範囲と PaaS 事業者の管理範囲および IaaS 事業者の管理範囲がある一方で、PaaS 事業者が所有する範囲の中にも利用企業の管理範囲が存在する。

（3）マルチクラウド・ハイブリッドクラウド

単体のクラウドでも複数のサービスが組み合わされていることを（2）でみたが、近年、クラウドの利用の高度化、複雑化はさらに進んでいる。異なる業者が提供する複数のクラウドを併用するマルチクラウド、自社のオンプレミス[10]のシステムと併用するハイブリッドクラウドへと、クラウドの構成はますます複雑になってきている[11]（《図表Ⅱ-4》参照）。提供業者やシステムが異なれば、リスクに対応する技術も異なり、異なるリスクマネジメント手法を組み合わせて利用することになる。

《図表Ⅱ-4》ハイブリッド・クラウドとマルチクラウド



（出典）IBM Cloud Blog、「マルチクラウドとは何か」<https://www.ibm.com/blogs/solutions/jp-ja/what-is-multicloud/>（visited Feb. 5, 2020）より SOMPO 未来研究所作成。

このように、クラウドサービスの利用により企業の内部と外部が複雑に連携したシステムに依存するようになってきており、これまでと異なるリスクを企業は抱えるようになってきた。

《BOX 1》シャドーIT

クラウドサービスを利用して比較的容易にシステム開発を行うことが可能になってきたことが、新たなリスクを生む要因となっている。システム化やシステムを提供する外部業者の選定・利用は、従来は IT 部門によって行われてきたが、近年はユーザー部門によって進められることが多くなっている。ユーザー部門によるクラウドサービス利用については IT 部門に申請を行うなど、システムを管理する一定のしくみが作られることが多い。しかし、組織の中で多くの部門がクラウドサービスを利用し、その案件数も多くなるため、利用されているクラウドサービスが IT 部門ですべて管理できているとは言えない状況が生じている。従業員個人でも名刺管理などの SaaS を気軽に利用でき、組織として管理されない、いわゆる「シャドーIT」が企業内で増殖しつつあることが懸念される[12]。

[10] オンプレミスとは、サーバやアプリケーションなどの IT システムを、利用する企業の管理する設備内に設置し運用することを指す。自社運用ともいう。（IDCFronrier「クラウド・データセンター用語集」<https://www.idcf.jp/words/on-premises.html>（visited Feb. 26, 2020））。またプライベートクラウドには、自社で構築し所有・管理を行うオンプレミス型とクラウド提供業者から提供を受けるホステッド型がある。

[11] IT 調査会社ガートナーは、「今後 5～10 年でほとんどのデータセンターのアーキテクチャは、オンプレミスの物理／仮想マシン、クラウドの仮想マシン、コンテナ、サーバレス、PaaS を含む「ハイブリッド」になると予測している。」（ビジネス＋IT、「ハイブリッド・クラウドのセキュリティ対策をガートナーが解説、CWPP とは何か？」（2018 年 9 月 6 日））。

[12] オラクル、KPMG「オラクルと KPMG によるクラウドの脅威レポート、クラウド利用促進によるサイバーセキュリティ戦略への影響」（2018 年）。

３．リスクの観点から見たクラウドサービスの特徴

２．でみたように、クラウドサービスは高度に複合されたシステムであるが、その特性である「マルチテナント（複数の利用者による共同利用）[13]」、「アウトソーシング（管理の委託）」、「サプライチェーン（複数のサービスの組み合わせ構造）」はリスクを考える上で重要なポイントとなる。

（１）マルチテナント

パブリッククラウドではシステムのリソースを複数の利用者でシェアする、マルチテナントであることによってコスト削減を図る、という点がひとつの利点とされている。一方で、このマルチテナント化がクラウドのリスクを増幅させる働きをするとされる。欧州ネットワーク情報セキュリティ機関（ENISA）がクラウド上のさまざまなリスクを列挙するレポート[14]を発行している。その中でマルチテナントであることによるリスクとして、①特定の利用者が高い負荷がかかる処理を実施した場合、リソースが枯渇するリスク、②1 つの機器を共有している複数の利用者のデータの隔離が失敗するリスクの２つを挙げている。

また、《図表Ⅲ-1》の Amazon 東京リージョンの例に見るように、マルチテナントであることから障害が発生した際に数多くの利用者、サービスが影響を受ける。

（２）アウトソーシング

クラウドサービスによりシステムの全部または一部をアウトソースするからといってリスクマネジメント全般をアウトソースはできない。クラウドサービスを利用する際に結ぶ契約によって、クラウドサービス提供業者と利用者の責任の範囲が定められている。クラウドサービス提供業者は利用者に責任の負担を求めており、例えば、AWS は「責任共有モデル」を掲げ、クラウドサービスに関して顧客と AWS がそれぞれ責任を負う範囲を明示している[15]。クラウドサービスを利用する企業は、クラウドサービスの契約の責任の範囲に従い運用プロセスにおけるリスクマネジメントの責任を担うことになる。《図表Ⅱ-5≫にその分担例を示す。

《図表Ⅱ-5》運用プロセスにおけるリスクマネジメントの責任分担の例

対象プロセス	クラウドサービス提供業者の責任範囲（例）	利用者の責任範囲（例）
稼働監視	● クラウド仮想環境に係る稼働監視	● クラウド側稼働監視結果の定期的確認と切替等の対応 ● 自社設定環境に係る稼働監視
障害検知と対応	● クラウド仮想環境に係る障害検知・復旧対応	● クラウド側障害状況の定期的確認とユーザー告知等の対応 ● 自社設定環境に係る障害検知・復旧対応
ID 管理	● クラウド仮想環境に係る ID 管理	● 自社設定環境に係る ID 管理
変更管理	● クラウド仮想環境に係るバージョン管理、リリース作業等	● 自社設定環境に係るバージョン管理、リリース作業等
災害対応	● 災害時を想定したバックアップ機能の提供	● 災害時を想定したバックアップ環境の設定、切替設定、対応マニュアルの整備
委託先管理	● 委託先の管理	● 委託先（クラウドサービス提供業者）の管理 ● 再委託先の管理（クラウドサービス提供業者発表情報の定期的確認）

（出典）KPMG コンサルティング「マルチクラウド時代のリスクマネジメント入門」（2019 年 3 月）より SOMPO 未来研究所作成。

[13] クラウドサービスは、単体の利用者だけでシングルテナントとして利用することも可能である。その場合は、カスタマイズの自由度が高くなる反面でコストメリットは限定的となる。

[14] ENISA, *"Cloud Computing: Benefits, risks and recommendations for information security"*, Nov. 2009.

[15] AWS ウェブサイト「責任共有モデル」<https://aws.amazon.com/jp/compliance/shared-responsibility-model/>（visited Feb. 12, 2020）。

クラウドサービス提供業者は、SLA の中で、稼働率、遅延時間などの測定可能な指標を使って、提供するサービスとその品質を明文化している[16]。また、多くの標準的な SLA では、基準となる月間稼働率などを定め、実際の稼働率が基準を下回った場合に利用料を減額するといった補償を約束している[17]。三大クラウドサービスの稼働率指標とその補償を比較し《図表Ⅱ-6》に示す。クラウド障害が発生したとき、利用している企業の様々な活動が影響を受けるが、契約書に従い補償されるのは利用料の一部だけとなる[18]。

《図表Ⅱ-6》三大クラウドサービス提供業者の SLA における稼働率指標と補償の例示

クラウド提供業者	サービス	月間稼働率	補　償 (利用料に対し)
AWS	IaaS: Elastic Compute Cloud (EC2)	99.99%未満 99.0%以上 99.0%未満 95.0%以上 95.0%未満	10% 30% 100%
	オブジェクトストレージ: Simple Strage Service (S3)	99.9%未満 99.0%以上 99.0%未満 95.0%以上 95.0%未満	10% 25% 100%
Google Cloud	IaaS: Compute Engine	99.99%未満 99.0%以上 99.0%未満 95.0%以上 95.0%未満	10% 25% 50%
	オブジェクトストレージ: Cloud Storage	99.95%未満 99.0%以上 99.0%未満 95.0%以上 95.0%未満	10% 25% 50%
Microsoft Azure	IaaS: Virtual Machines	99.99%未満 99.0%以上 99.0%未満 95.0%以上 95.0%未満	10% 25% 100%
	オブジェクトストレージ: Disk Storage	99.9%未満 99.0%以上 99.0%未満	10% 25%

（出典）各社 SLA より SOMPO 未来研究所作成。条件が付かない通常の場合を比較した（2020 年 2 月 26 日現在）。

（3）複数のサービスを組み合わせたサプライチェーンとリスクの連鎖

クラウドサービスの一つの特徴として、全体が複数の提供業者が提供するサービスの組み合わせで構成されていることを２．（2）および（3）でみた。それぞれのサービス、提供業者が異なるリスクを有しており、個別の提供業者のリスク評価とともに、それらが複合された全体のリスクを評価する必要があり、クラウドサービスのリスク評価を難しくしている。

さらに、グローバルなネットワークによる障害の連鎖についても触れておきたい。2013 年 2 月にマイクロソフトの Azure クラウドプラットフォームが SSL 証明書の期限切れによりダウンし、約 12 時間にわたって全世界の Azure が停止した[19]。最近では 2018 年 12 月に発生したスウェーデンのエリクソンのソフトの不具合に起因する通信障害は、世界 11 カ国の通信インフラに影響を与えた[20]。

このようにますます高度に複雑化するクラウドサービスが障害を起こしたとき、利用している企業はどのように影響をうけるであろうか。次章では実際の障害の発生状況をみながら確認していきたい。

---

16 ニフクラウェブサイト、クラウドナビ、基礎知識「クラウド選択時の重要な指標。サービス品質保証（SLA）とは？」<https://pfs.nifcloud.com/navi/beginner/sla.htm>（visited Feb. 12, 2020）。

17 2016 年 4 月に発生した Google クラウドプラットフォームの 18 分間（月間稼働率 99.96%と換算される）の障害に対する月間利用料の返金は総額何百万ドルという額となった（OneNeck, *"How Much Downtime Can You Really Afford?"*, 2017）。

18 日本で 2012 年に発生したレンタルサーバのデータ消失事件では、ファーストサーバはサービス利用契約約款に基づいて、サービスの対価として支払われた総額を限度に損害賠償するとしており、親会社のヤフーが 2013 年 3 月期決算でシステム事故関連損失として 12 億円を計上している（ヤフー株式会社「平成 25 年 3 月期 決算短信〔日本基準〕(連結)」および日経 XTECH「データ消失障害のファーストサーバが中間報告「データは復旧不可能」（2012 年 6 月 25 日））。

19 日経 XTECH、「2 月 22 日の Windows Azure 障害、原因は SSL 証明書の期限切れ」（2013 年 2 月 26 日）。Azure は 2016 年 9 月にも世界規模で 2～3 時間の障害を生じている（日経 XTECH、「Azure で世界規模の障害が発生し 2～3 時間後にはほぼ復旧」（2016 年 9 月 16 日））。

20 日本でもソフトバンクの携帯電話が約 4 時間半にわたって通信障害を起こしている（日本経済新聞「エリクソン、シェア 4 割の死角　世界 11 カ国で通信障害」（2018 年 12 月 7 日））。

Ⅲ．クラウド障害の発生状況と保険の利用

１．クラウド障害の発生とその原因

（１）日本で最近発生したクラウド障害事例

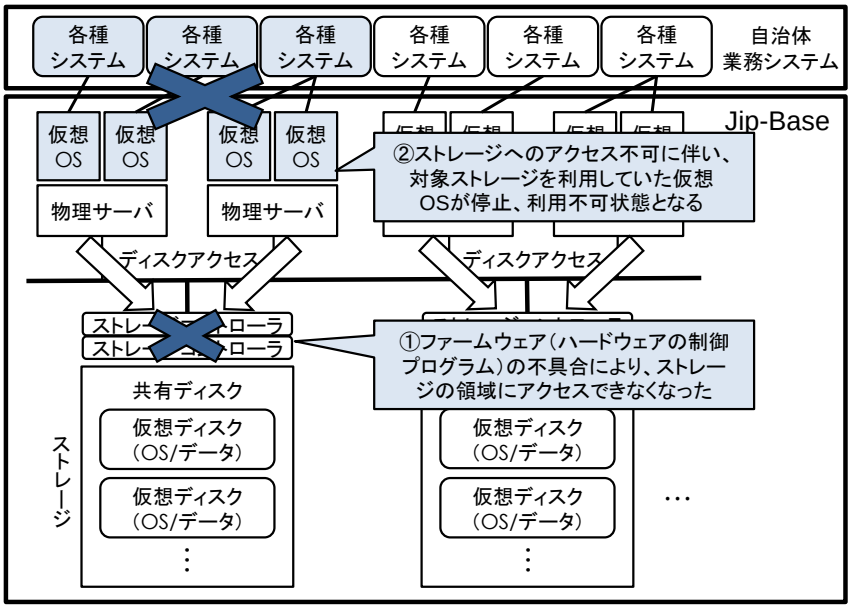
日本においてもクラウドサービスの利用が拡大し高度化する一方で、さまざまな障害の発生が報じられている。《図表Ⅲ-1》に 2019 年に発生した大きな障害を示す。Ⅱ．３．（１）で挙げたクラウドサービスのマルチテナントという特徴により、１つのクラウドサービスがダウンすることによって、数多くの事業やシステムに大きな影響が生じている。《図表Ⅲ-2》には、クラウドが障害を起こした際に、内部でどのようなことが起こっていたかを例示している。クラウドを構成する複数のシステムのサプライチェーンにより、システムの内部で障害が連鎖し、大きな障害に発展した様子が見て取れる。

《図表Ⅲ-1》最近発生したクラウド障害の事例

事　例	概　要
Amazon 東京リージョン （2019 年 8 月）	冷却システムの故障によりオーバーヒート状態となり、一部の仮想サーバ（EC2）および仮想ディスク（EBS）のパフォーマンスが劣化し、リレーショナルデータベース（RDS）等のクラウドサービスに影響を与え、復旧までに約 8 時間を要した。30 社以上のアプリケーションが影響を受け、半日程度ストップを余儀なくされた例もある。複数のアベイラビリティゾーンを利用する冗長化を行っていても影響を受けた。このような障害はこれまでに発生していなかったものの十分に想定される障害とされている。[21]
自治体システム Jip Base （2019 年 12 月）	全国約 50 の自治体で利用しているシステムのストレージ（Dell 製）のファームウェアの故障から障害が発生した。33 の自治体のデータが消失し、介護保険に関する手続きが行えない、教育ネットワークシステムの障害から小中学校の通知表が作成できないなどの影響が 10 日間以上続いた。インフラのみを提供する IaaS であり、クラウドサービス提供業者単独ではクラウドサービス利用者側のシステムまで復旧することは困難とされた[22]。

（出典）SOMPO 未来研究所作成。

《図表Ⅲ-2》自治体システムダウン時の状況（2019 年 12 月）



（出典）日本電子計算機障害発生状況説明資料より SOMPO 未来研究所作成。

[21] 日経 XTECH「ニュース解説　AWS 大障害、ユニクロ・楽天・PayPay など 30 社以上に影響」（2019 年 8 月 23 日）および AWS ウェブサイト「東京リージョン（AP-NORTHEAST-1）で発生した Amazon EC2 と Amazon EBS の事象概要」<https://www.serverworks.co.jp/news/20190823_aws_news.html>（visited Feb. 18, 2020）。

[22] 中野区「12 月 4 日に発生したシステム障害について お詫びと状況のご報告」（2019 年 12 月 14 日）および日本経済新聞「練馬区の小中学校で通知表渡せずシステム障害の影響」（2019 年 12 月 24 日）。

（2）クラウド障害の原因

クラウドサービスの障害の原因はどのようなものだろうか。クラウド障害に関する専門家のレポートに掲げられたクラウド障害を生じる可能性がある事象を≪図表Ⅲ-３≫に示す。※印をつけたものは実際にクラウドサービスのダウンを招いた事象であり、ヒューマンエラーによる誤操作やシステムの不具合などが該当する。この他に、サイバー攻撃や自然災害などが挙げられている。

クラウド障害の発生について体系的に情報収集し原因別に分類した調査は案外少ないが、そのひとつを紹介する。米国でニュースのヘッドラインを飾るようなクラウドサービスの大規模災害のデータを、インターネット検索にて 2009 年から 2015 年の 7 年間分について収集している[23]。この調査データによると、クラウド障害は往々にしてオーバーヒートなどによるハードウェアの不具合や、システムのアップグレード、システムのバグによって引き起こされている。

同調査では数多くのクラウド障害を調査する中で、単一障害点（SPOF：Single Point Of Failure）、システムを構成する要素のうちそこが停止するとシステム全体が停止してしまう部分を探っている。結論として、SPOF としてひとつの点があるのではなく、ハードウェアの冗長性のみならず、障害復旧のチェーンが完全であることが求められる。障害復旧のチェーンとは、故障・異常が検知され、フェールオーバー、すなわち障害発生を回避するための切替えが機能し、そしてバックアップが稼働するということである。このチェーンが完璧に機能することによってようやく障害回避が成功するのである。例えば、2012 年 10 月 22 日に AWS の US-East リージョン[24]で発生したストレージ障害は、故障したデータ収集サーバ 1 台を入れ替えた際に、データ収集サーバの DNS[25]が新しいものにうまく更新されなかっ

《図表Ⅲ-3》クラウド障害を生じる可能性がある事象

不測の障害	● 通常のアップグレードにおいて誤った設定を行ったためにフロントエンドのサーバが利用不能※ ● 通常のメンテナンス作業中にバックアップサーバの容量が不足※ ● 通常のメンテナンス作業中の誤操作による障害が連鎖を起こし内部のトラフィックの過剰負荷が発生※ ● 通常のメンテナンス作業またはアップグレード中の誤操作によりインフラである基盤システムに悪影響※ ● HTTPS の証明書が通常のメンテナンスで更新されず期限切れ※ ● 不適切なアップデートの試行によりバグが発生※ ● ひとつのゾーン内のすべてのサーバの同時一斉再起動※ ● 故意ではない主要クラウドサービス（ストレージなど）の停止※ ● 故意ではない仮想マシンの大量削除
構造的要因	● データサーバが容量不足からクラッシュと再起動を繰り返していることが検知されず、自動検知器がサーバをオフラインに切替え、サーバ容量を失い残りのデータサーバに過剰な負荷が発生※ ● 一次、二次およびバックアップの電源システムの喪失※ ● 分電盤パネルのショート ● ネットワーク機器、ファイルサーバの不具合 ● 自動検知システムにより誤操作がかえって不明確となり、主要システムの大規模な障害に発展
敵対的行為	● 意図的に過剰な負荷をかけたり（DDoS 攻撃）、脆弱性をついたりする攻撃 ● 内部人員による故意の仮想マシンの大量削除 ● 内部人員による故意の主要クラウドサービス（ストレージなど）の停止
施設設備・環境要因	● 雷、洪水、太陽フレア、地震 ● 火災、危険物の爆発 ● 事故による電源の遮断・ネットワークの切断 ● 飛行機やトラックなどの外部からの飛来・突入 ● 電磁パルスによる障害

（出典）Lloyd's, AIR, *"Cloud Down, Impacts on the US economy"*, Emerging Risk Report 2018, Technology より SOMPO 未来研究所作成。※印付きは、実際に過去にクラウドダウンを生じたことがある事例。

[23] Haryadi et al., *"Why Does the Cloud Stop Computing? Lessons from Hundreds of Service Outages"*, 2016.
[24] 現在の US-East-1 リージョン。
[25] 機器を指定するためのしくみ。

たことが引き金となっている。入れ替えられてすでに存在しない古いデータ収集サーバへのアクセスが繰り返され、ストレージサーバのメモリ領域を圧迫したがその異常がなかなか検出されず、多くのストレージサーバが徐々にスタックしていった。スタックしたサーバを切り離し正常なサーバへフェールオーバーして障害に対応しようとするが、多くのサーバがスタックする中でフェールオーバー先が足りなくなっていき、大規模なストレージ障害へと発展した[26]。検知、フェールオーバー、バックアップとうまく連携できなかった例である。回避策が別の障害を生み、障害の連鎖を起こしている。クラウド障害の回避には、複数のシステムの連携がすべてうまくいかなければならないという困難さがある。

さらに同調査では、障害復旧後にクラウドサービスへのアクセスが集中し過剰負荷を生じる可能性もあり注意すべきだとしている。例えば 2014 年 6 月 23 日に Office 365 の Exchange Online が 8 時間 44 分ダウンしたが、復旧後にアクセスが集中し、翌日 6 月 24 日にも 8 時間 20 分ダウンしている[27]。障害復旧後の多数の利用者のアクセスのコントロールがうまくいかず障害につながってしまった例になる。

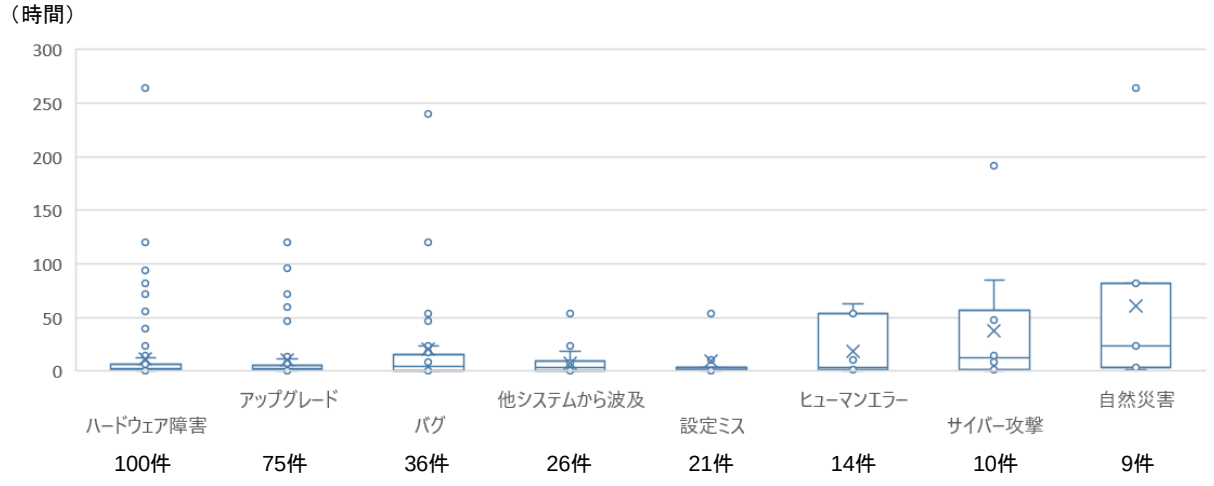
２．クラウド障害の発生状況の分析

（１）クラウド障害の原因別件数と持続時間

クラウド障害の原因別に、件数の分布やどれくらいの時間クラウドがダウンするかという影響の大きさの傾向を見てみよう。１.（２）で紹介した調査のデータが公開されているのでこれを使って統計をとってみる[28]。

《図表Ⅲ-4》は、原因別[29]のクラウド障害の持続時間を箱ひげ図で表したものである。ハードウェアの障害やアップグレード、バグによる障害件数が多くなっている一方で、サイバー攻撃や自然災害による

《図表Ⅲ-4》原因別のクラウド障害持続時間の分布



（出典）Uchicago systems research on Availability, Reliability and Efficiency ウェブサイト, *"CBS: Cloud Bug Study database"*, <https://ucare.cs.uchicago.edu/projects/cbs/> (visited Nov. 22, 2019) より SOMPO 未来研究所作成。

[26] Publickey、「Amazon クラウド、ストレージ障害は潜在バグからメモリリーク発生が原因。きっかけは DNS の変更」<https://www.publickey1.jp/blog/12/amazondns.html> (visited Mar. 3, 2020).
[27] Redmond, *"Microsoft Offers Explanations for Lync and Exchange Service Outages"*, Jun. 6, 2014.
[28] Uchicago systems research on Availability, Reliability and Efficiency ウェブサイト, *"CBS: Cloud Bug Study database"*, <https://ucare.cs.uchicago.edu/projects/cbs/> (visited Nov. 22, 2019).
[29] 1 つの障害が 2 つ以上の原因で発生することがあり、その場合は複数の原因についてそれぞれ 1 カウントとしている。

クラウド障害の件数は比較的少ないが、発生すると障害が長時間持続しがちである。ハードウェア障害は100件と最も多く、その7割が4時間以内に、9割が12時間以内に復旧している。短時間の障害に集中しているので、箱ひげ図のハードウェア障害の箱は平べったく薄くなっている。その箱の上に、ヤフーメールの11日間（2014年11月）[30]および5日間（2013年12月）[31]の2回のダウンを含む12時間を超える障害10件が点々と縦に分散している。サイバー攻撃によるものは10件と少ないが、そのうち7件は8時間を超えており、最長はアップルの開発者サイトの8日間（2013年7月）である[32]。サイバー攻撃による障害はデータの数が少なく障害の時間も長時間から短時間にまばらに分布しているので、箱ひげ図では背の高い箱になっている。

（2）損害額の推定

クラウドサービスがダウンしてしまうと、企業にはどのような損害が生じるだろうか。リスクマネジメントを考えるとき、どの程度のリスクとなるかを知ることは重要である。しかしながら、システム責任者の多くはクラウドがダウンした際のコストを十分に評価できていないとしている[33]。実際に、クラウド障害が発生した際の損害額の調査例はあまり見当たらない。

クラウドサービスそのものではないが、データセンターのダウンを対象とした調査を行った例があり[34]、損害額の推計を行っている[35]。この研究では、2015年の調査時点において、過去1年間に予期しない障害によるダウンを経験した米国所在の63のデータセンターを対象としている。損害額は1件につき合計7万ドルから240万ドルまで大きな幅があり、費目としては事業の中断や喪失利益、生産性の低下など、事業継続に影響が出たことによる損害が大きな割合を占めている（《図表Ⅲ-5》参照）。この調査は米国の企業が対象となっているので、そのまま日本の企業に当てはめることはでき

《図表Ⅲ-5》データセンターの計画外のダウンによる損害額

（単位：ドル）

	平均	最小	最大
事業の中断	255,963	15,750	812,440
喪失収益	208,599	26,591	755,810
最終顧客の生産性低下	138,193	15,600	456,912
IT部門の生産性低下	61,880	6,994	125,600
調査	26,712	877	69,100
復旧	21,177	1,900	58,171
外部コンサルタント等	9,927	1,551	27,600
機器買替	9,478	1,249	67,783
事後処理	8,428	―	36,575
合　計	740,357	70,512	2,409,991

（出典）Ponemon, *"Cost of Data Center Outages"*, Jan 2016 より SOMPO 未来研究所作成。

30 海底ケーブルの切断により通信不能が発生した（ITPro, *"Yahoo Mail outage: Engineers still trying to repair cable"*, Nov. 29, 2014 および Techworm, *"Yahoo Mail Is Back Online After 11 Days Of Outage"*, Dec. 2, 2014.）。

31 データセンターのハードウェアがダウンしメールおよび小企業向けのサイトがダウンした（International Working Group on Cloud Computing Resiliency, *"'Hardware problem' causes partial outage for Yahoo Mail"*, Dec. 9, 2013 および Tumblr, *"An Update on Yahoo Mail"*, Dec. 13, 2013.）。

32 アップルは開発者向けサイトの登録者データへ不正アクセスがあったとして一時的に閉鎖した。後に外部の研究者がアップルにバグがあることを報告するためだったと公表しているが真偽は定かでない（ASCII.jp「「バグ調査だった」アップルサイト侵入者が無実主張」（2013年7月23日））。

33 Veritas が行った世界各国 1,200 社のクラウドサービスを利用している企業のシステム責任者に対するアンケート調査で、60%がクラウドダウンのコストを十分に評価できていないとしている（Veritas, *"Veritas Study Shows that Organizations are Moving to the Cloud Without Evaluating the Impact of a Cloud Outage"*, Mar. 15, 2018.）。

34 Ponemon, *"Cost of Data Center Outages"*, Jan 2016.

35 この調査では、該当するデータセンターのIT関係者に対し、障害対応の行動を確認し、また損害の費目ごとに直接費、間接費に分けておおよその推定額を回答してもらい、インタビューによって確認したうえで、活動基準原価計算（ABC）法により損害額を見積もっている。

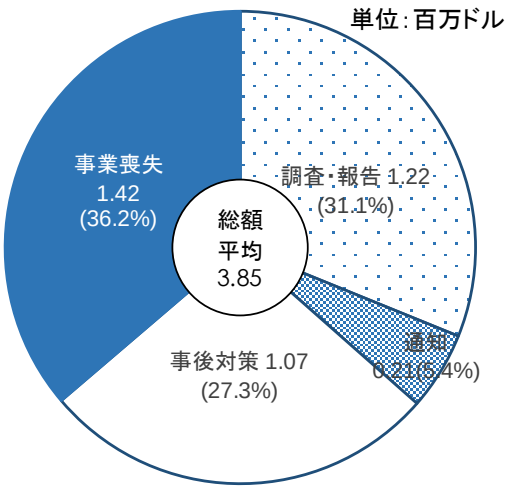
ないかもしれないが、大まかな傾向を示すものとして興味深い。また、これはクラウドサービスではなくデータセンターの調査であるが、同じ研究所が行った情報漏えい事故を対象とした調査[36]では、クラウドサービスの利用によりシステムが複雑化しているとき、コストが通常に比べて平均で 7.6%高いという推計がされているので付記しておく。

クラウド障害が発生すると 1 企業だけでなく複数の企業の事業運営に影響が及び、経済全体にも大きな影響を及ぼすと推測される。クラウド障害により長時間クラウドがダウンしたと想定し、米国経済全体への影響額を推計した研究がある[37]。先のデータセンターの研究は通常発生する平均 1.5 時間程度のダウンを対象としているが、この研究では稀にしか発生しない長時間のダウンによる巨大災害を想定している。米国の上位 3 位までのクラウドサービス提供業者のうち 1 社がサイバー攻撃を受け 3～6 日ダウンした場合、E コマースの事業に影響を与え、総額で 69～147 億ドルの損失を生じると推定している。これが上位 10～15 位のクラウドサービス提供業者 1 社だけであれば、11～21 億ドル程度の損害となる[38]。過去には、実際にこれくらいの期間のクラウド障害が発生しており、また、クラウドサービスを利用する企業の増加に伴って損害額は大きくなる可能性がある。一方で同研究のレポートでは、クラウドサービス提供業者は技術的進歩や管理手法の発達、自動化の進展によって発生確率や損害額の縮小を行う努力を重ねており、過去のデータに基づいた推計ほどに大きな損失に至らない可能性にも言及している。

（3）情報漏えいにより生じる損害

クラウド障害はシステムの不具合やヒューマンエラー、サイバー攻撃を原因として発生するが、このような障害が発生したとき、クラウドのストレージに保存されている個人情報や機密情報が漏えいするリスクがある。情報漏えい事故が発生したときは、（2）でみたような事業中断や障害復旧といった損害とは別に、情報漏えいによる損害が生じる。世界 16 カ国 1,786 件の情報漏えい事故について分析した調査[39]では、1 件の情報漏えい事故につき平均で 385 万ドルのコストがかかると推計しており、（2）のクラウド障害の平均コスト 74 万ドルに比べると、約 5 倍となっている。その内訳は《図表Ⅲ-6》のとおりである。情報漏えいを起こしたときは顧客の乖離が起こり[40]、事業の一部が喪失する。さらに事後対策や調査・報告のコストもかかる。なお、同調査のレポートで

《図表Ⅲ-6》情報漏えい事故コストの内訳（2019 年）



（出典）Ponemon, IBM Security, *"Cost of a Data Breach Report"*, 2019 より SOMPO 未来研究所作成。

[36] Ponemon, IBM Security, *"Cost of a Data Breach Report"*, 2019.
[37] AIR, Lloyd's, *"Cloud Down, Impacts on the US economy"*, Emerging Risk Report, Technology, 2018.
[38] 推計するにあたり、事業中断による変動費の削減、バックアップ計画の発動による損失削減、期間経過に従い復旧の進捗などを仮定し、業態ごとの事業規模の分布や E コマースへの売り上げ依存割合などに基づき計算を行っている。
[39] 前脚注 35 と同様の手法を採用している。（文献は前脚注 36 に同じ。）
[40] 情報漏えいを起こした際の顧客乖離率は世界平均で 3.9%のところを日本においては 4.3%となっており、世界 16 カ国中 3 番目に高い（前脚注 36 と同じ。）。

は、損害の削減に寄与する要因の分析を行っており、情報漏えい事故対応チームの形成や幅広な対応プランの策定により 1 割程度コストが削減できるとしている。同調査によると、日本では情報漏えい事故 1 件につき約 2 万件の情報が漏えいしており、それに対するコストは 1 事故につき平均 375 万ドル（2019 年）と推計されている。

（4）情報漏えいリスクの推定手法

情報漏えい事故が発生した場合にはどれくらいの損害が生じるのか、それは業種や保有している情報量によって変わってくる。日本ネットワークセキュリティ協会（JNSA）は個人情報の潜在的リスクを把握するための推定手法として想定損害賠償額算定式（JNSA Damage Operation Model for Individual Information Leak：JO モデル）を提案している。これは、日本における情報漏えい事故や判例を調査し、事故の原因や被害者数等の分析を行い、専門家の助言に基づき算定式を策定したもので、実際の判例結果と比較し検算を行っている[41]。この算定式はあくまでも「もし被害者全員が賠償請求したら」という仮定に基づいて潜在的なリスクを推計するものであり、実際支払われる金額を計算したものではないが、自社のリスクの大きさを知る上で参考になると考えられる。

≪BOX 2≫　想定損害賠償額算定式（JO モデル）[42]

◆計算式

損害賠償額 = 漏えい情報価値 × 社会的責任度 × 事後対応評価

= （基礎情報価値 × 機微情報度 × 本人特定容易度）× 社会的責任度 × 事後対応評価

[500] × [$10^{x-1}+5^{y-1}$] × [1, 3, 6] × [1, 2] × [1, 2]

◆入力値の設定

基礎情報価値：一律 500 ポイント

機微情報度：$10^{x-1}+5^{y-1}$ ポイント（複数種類ある場合は計算値が最大となるもの）
漏えいした情報の種類等に従って経済的損失（x）と精神的苦痛（y）それぞれを 1、2、3 の三段階で評価

本人特定容易度：1、3、6 ポイントの三段階で評価

社会的責任度：一般的な場合は 1、医療・金融など個人情報の取扱責任が一般より高い場合は 2 ポイント

事後対応評価：不適切な対応であれば 2、それ以外は 1 ポイント
（事後対応の適切性については行動例が示されている。）

---

41 山田他は 2014 年に発生したベネッセコーポレーションの情報漏えい事故について、JO モデルを用いて損害賠償額を被害人数 1 人あたり 33,000 円、被害人数 4,858 万人であるから総額 1 兆 6,031 億 4 千万円と推計している。これに対し山田他は、情報漏えい事故を起こした企業の特別損失額を分析して新たな計算モデルを提案している。その計算式に従うとベネッセコーポレーションの事故の損害額は 1 人あたり 273 円程度となる。この分析は企業の特別損失をベースにしており、JO モデルの損害賠償額とは厳密には異なる。なお、ベネッセコーポレーションの場合は、特別損失は約 260 億円であり、被害者人数で割ると 535 円となる。JO モデルより山田他の方が実際の値には近いが、今度は過小評価していることになり、さらなる精度向上が課題となる（山田道洋他「個人情報漏洩の損害額の新しい数理モデルの提案」情報処理学会論文誌 Vol.60 No.9 1528-1537（2019 年 9 月））。

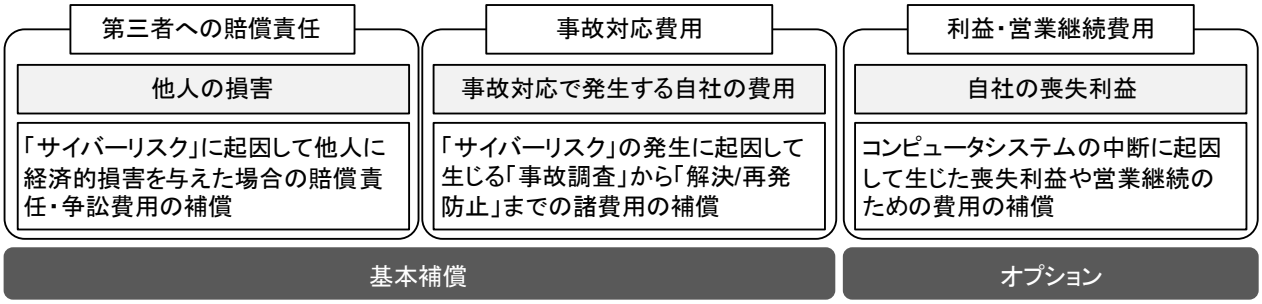
42 日本ネットワークセキュリティ協会、セキュリティ被害調査ワーキンググループ「情報セキュリティインシデントに関する調査報告書、別紙、第 1.0 版」（2017 年 5 月 17 日）。

３．保険サービスの利用

（１）サイバー保険による補償

ここまで、クラウドサービスを利用する際に考慮すべきリスクとその発生状況をみてきたが、クラウド障害によって生じる損害に対して、どのように備えればよいだろうか。損害保険会社がサイバーリスクに対する補償を行う保険としてサイバー保険を提供しているので簡単に内容を紹介しておく。保険会社によって異なる可能性はあるが、一般的にサイバー保険[43]では、外部からの攻撃だけではなく、内部のシステムオペレーションミス、システムの管理不備等の過失に起因する事故も対象となる。また、オプションとして使用人の犯罪行為に起因する事故も補償対象とすることができる。さらに≪図表Ⅲ-７≫に示すように、第三者への賠償責任や事故対応費用だけでなく、オプションとして自社の喪失利益も補償の対象とすることができる。

《図表Ⅲ-7》一般的なサイバー保険の補償内容



（出典）損保ジャパン日本興亜のサイバー保険に関する資料より SOMPO 未来研究所作成。

（２）セキュリティ対策サービス

保険会社は、事故が発生した後に損害に対して保険金を支払うが、グループ会社を通じて発生する前に有効な予防策を提案するサービスも提供している。いったん事故が発生してしまうと保険ではカバーされない損害[44]も生じ、また損害が明確にならないような風評被害など長い期間にわたって事業が影響を受けることになる。したがって、事後の補償を準備しながらも、事前に十分な予防対策を講じることが重要となる。

また、サイバー攻撃などによる被害が生じた場合、サイバー保険に自動で付帯されるサービスによって、調査や広報などの必要な事故対応について、外部の提携専門業者を通じて保険会社が支援を行う。各種対応で発生した費用は、サイバー保険の保険金として支払われるので、個別にセキュリティコンサルタントなどと契約する場合と異なりスピーディにサービス提供を受けられ、緊急対応体制への移行をスムーズに行うことができる。

---

[43] 既存商品（企業向けの火災保険等）でも明示的にサイバーリスクを免責としていないために、サイバーリスクを担保していると解釈される可能性があったが、サイバーリスクについては専用の保険で補償する方向性が固まった（日本経済新聞「サイバー被害は専用保険で　各国損保、既存補償から分離」（2020 年 2 月 4 日））。

[44] 保険では支払われない費用の例として、GDPR 等の法規制によって企業に課せられる課徴金や罰金、サイバー攻撃を仕掛けられ攻撃者から要求される脅迫金やランサムウェアによる身代金、PCI DSS（クレジットカード業界のグローバルセキュリティ基準）の違反によって、カードブランドや加盟店契約会社等から求められる違反費用、ビジネスメール詐欺によって不正な口座に誤って振り込んでしまった費用などがあり、一般的に保険契約上で免責となっている。

Ⅳ．情報の収集と開示

１．クラウドサービスのセキュリティ評価

Ⅲ．ではクラウド障害が発生し、さらに情報漏えいがあった場合に、損害がかなりの高額になる可能性があることをみた。大事なデータやシステムを委託するからには、クラウドサービスは安定的で信頼のおけるものであってほしい。では、クラウドサービスの信頼性をどのように評価すればよいだろうか。

ひとつには専門的な第三者機関が行う評価や認定を参考にすることができる。米国に本部を置く CSA Security, Trust & Assurance Registry（CSA STAR：The Cloud Security Alliance（CSA））では、クラウドサービスのセキュリティコントロールについて登録・公開を行っている[45]。また、クラウドのセキュリティ認証を行う機関として、ルクセンブルグの StarAudit Certification（EuroCloud Europe（ECE））や The European Security Certification Framework（EU-SEC）などがある[46]。

日本では、総務省が「クラウドサービス提供における情報セキュリティ対策ガイドライン」[47]を公表しており、これに則る形で ASP/SaaS/IoT クラウドコンソーシアム（ASPIC）が 2008 年 4 月から「ASP・SaaS の安全・信頼性に係る情報開示認定制度」、2012 年 8 月から「IaaS・PaaS の安全・信頼性に係る情報開示認定制度」を運営している[48]。開示情報には、事業やサービスの概要に加えてリスクマネジメントに関する項目やサービス品質も含まれている。また、情報マネジメントシステム認定センター（ISMS-AC）が 2016 年 8 月より ISO/IEC27017[49]に規定されるクラウドサービス固有の管理策が適切に導入、実施されていることを認証する「ISMS クラウドセキュリティ認証」を行っている。これらの認証は、クラウドサービスに情報を預ける際に当該サービスを評価する一つの指標となる[50]。あわせて、クラウドサービス提供業者がホワイトペーパーなどの形で用意するリスクマネジメントに関する情報開示資料も参考とすることができる。

２．公共機関が収集するサイバーセキュリティ事故情報

サイバーセキュリティに対する取り組みの強化は国際的にも国家としても重要な課題となっている。

サイバーセキュリティに関する情報の共有が、近年、米国を始めとして EU、英国、シンガポール、韓国など諸外国において促進され始めている。特に米国においては、2015 年 2 月の大統領令[51]によって明文化され、業界ガイドラインにより情報セキュリティ事故検知後 72 時間以内に当局へ通知する義務が課されるなど、厳しい規制が引かれている[52]。日本においてはサイバーセキュリティ事故の報告が経済産業省の告示[53]により推奨されている[54]。

---

45 レベル１－自己評価、レベル２－第三者評価、レベル３－連続監視の 3 段階がある（日本情報経済社会推進協会「クラウドサービスに関連する国内外の制度・ガイドラインの紹介」（2019 年 5 月 22 日））。

46 日本情報経済社会推進協会「クラウドサービスに関連する国内外の制度・ガイドラインの紹介」（2019 年 5 月 22 日）。

47 2008 年 1 月公表の「ASP、SaaS における情報セキュリティ対策ガイドライン」と 2014 年 4 月公表の「クラウドサービス提供における情報セキュリティ対策ガイドライン（第 1 版）」を統合し、2018 年 7 月に第 2 版を公表している。

48 2020 年 2 月 24 日現在、日本の ASP・SaaS 提供業者 138 社、IaaS、PaaS 提供業者 7 社が認定を受けている。

49 クラウドサービスに関する情報セキュリティ対策を実施するためのガイドライン規格（ISMS-AC、「ISMS 適合性評価制度、JIS Q 27001:2014（ISO/IEC 27001:2013）対応版」（2020 年 1 月））。

50 2020 年 2 月 24 日現在、158 の組織の機関が登録し、そのうち 149 が公表されている。

51 Executive Order 13691, *"Promoting Private Sector Cybersecurity Information Sharing"*, Feb. 13, 2015.

52 日本サイバーセキュリティ・イノベーション委員会「諸外国におけるサイバーセキュリティの情報共有に関する調査」（2018 年 3 月 9 日）。

53 経済産業省告示第 19 号「ソフトウェア製品等の脆弱性関連情報に関する取扱い規程」（2017 年 2 月 8 日付）。

３．クラウド障害の情報開示と分析・研究

セキュリティに関する情報だけでなく、実際にクラウドサービスにどのような障害が発生してきたかについて、クラウドサービス提供業者が情報公開を行っている。

Google はウェブサイトで自社の 27 種類のクラウドサービスの障害状況を公表[55]しており、2019 年 2 月から 2020 年 1 月の 12 か月間で 73 回[56]の障害を数える。世界各地の状況を一括で表示しており、30 分程度の小さな障害から最長 45 時間半に及ぶコンピュータのダウンまでさまざまである。大きな障害については、その原因や経過を詳細にレポートしている。AWS も過去の障害を公表[57]しているが年 1 回発生するような大規模な障害に限定されており、2011 年から 2019 年の 9 年間に発生した 12 件の障害を挙げている。Azure は過去 90 日間の障害を公表[58]している。

これらのウェブページでは、障害の状況や原因を伝えているが、全般的な発生状況を把握するには一つ一つの障害に関する記述を読みこなしてまとめる必要がある。この他のクラウドサービス提供業者もそれぞれに情報開示を行っているが、情報開示の内容や範囲はバラバラであり、平仄をそろえて比較することが難しい。このような開示情報を拾って集約しているサイト[59]もあるが、情報の網羅性や信頼性を吟味する必要があるだろう。

主要なクラウドサービスについては、大きな障害が生じれば何らかのメディアに取り上げられることになり、それを集約することは可能である。しかしながら、メディアから得られる情報は均一ではなく、突き合わせや内容の咀嚼が必要である。Ⅲ．２．（１）で取り上げた調査は、統一された手法を用い、研究者の目を通してフィルタリングしており、7 年間という期間をカバーする数少ない研究例である。すでに 5 年が経過し状況も変化しており、最新の情報に基づいた質の高い調査が、米国に限らず再び行われることを望みたい。

---

[54] 米国では国家インフラストラクチャ諮問委員会のプロジェクトとして、情報システムの脆弱性に対するオープンで包括的、汎用的な評価手法の確立と普及を目指し、共通脆弱性評価システム（CVSS）が作成され、FIRST（Forum of Incident Response and Security Teams）によって管理・推進されている。この CVSS は脆弱性の深刻度を評価する基準である（情報処理推進機構「共通脆弱性評価システム CVSS 概説」（2018 年 5 月 31 日））。日本では JPCERT（Japan Computer Emergency Response Team）コーディネーションセンターと情報処理推進機構が共同で日本の脆弱性情報データベース（JCN）を管理している。

[55] Google Cloud Platform, *"Incidents Reported in the last 365 days"*, <https://status.cloud.google.com/summary> (visited Feb. 18, 2020).

[56] 同じ日付で発生している障害は 1 つとカウントした。

[57] AWS, *"Post-Event Summaries"*, <https://aws.amazon.com/jp/premiumsupport/technology/pes/> (visited Feb. 21, 2020).

[58] Microsoft Azure, *"Azure status history"*, <https://status.azure.com/en-us/status/history/> (visited Feb. 21, 2020).

[59] たとえば検索エンジンなどのソリューションを提供している elastic のサービス elastic cloud <https://cloud-status.elastic.co/history?page=1> や cloudsquare <https://cloudharmony.com/status> がある。

Ⅴ．おわりに

クラウドサービスは技術的な進歩とともに急速な拡大を遂げている。企業はクラウドサービスを利用することによって、企業の外部と深く連携した複雑なシステムに依存するようになってきている。クラウドサービスには、システムの効率性、セキュリティ水準、技術革新対応力、柔軟性、可用性を高める効果が期待されるが、一方で、新たなリスクも生じている。クラウドサービスを利用するにあたっては、クラウドサービス提供業者と利用者それぞれの責任範囲を認識し、リスクマネジメントを考えていく必要がある。

本稿では、クラウドサービスの障害の発生状況を示す情報や調査研究についていくつか紹介した。クラウド障害の多くはハードウェアの不具合やシステムのアップグレード、バグによって引き起こされている。クラウド障害を回避するにはハードウェアの冗長性のみならず、障害復旧のチェーンが完全であることが求められ、複雑に連携したシステムの難しさがある。クラウド障害は完全に回避することはできず、発生すると企業の事業運営に大きな影響を及ぼす可能性がある。したがって、障害が発生することを前提として事業継続の観点からリスクへの対応を考える必要がある。クラウド障害による事業運営への影響は、業態やクラウドサービスの利用状況によって変わってくると考えられる。利用するクラウドサービスに障害が発生することを想定し、企業ごとに自社の事業内容に即したリスクを認識する必要があるだろう。

また、サイバーセキュリティは国際的に重要課題となっており、国家レベルで情報の収集に取り組み、リスクに対する備えを促している。サイバー攻撃を原因とする障害件数は少ないが、発生すると大規模損害になる可能性がある。クラウド障害は多くの企業が影響を受けることによって経済全体に影響を与えることにもなり、情報漏えいを伴った場合はさらに損害が拡大する。新たな脅威に対してデータの蓄積と分析が必要である。

クラウドサービスの利用者は、システムをアウトソーシングしてもリスクのすべては転嫁されず、自社のリスクを認識し、リスクマネジメントを行っていく必要がある。クラウドサービス提供業者はリスクに関して必要な情報を開示し、利用者の理解と対応を促すよう求められる[60]。クラウドサービス利用者とクラウドサービス提供業者は、クラウドサービスが新たなシステムインフラとして急速に拡大するなかで、リスクマネジメントの面でも連携し、情報を共有し、適切にリスクをコントロールしていく必要がある。損害保険会社としては、万が一損害が生じた際の補償や事後対策のサービス提供を行うに留まらず、事前に行うリスク診断などのサービスをあわせて提供し、総合的なリスクマネジメントを支援していこうとしている。

技術の進歩により構造を複雑化させながら急速に拡大するクラウドサービスのリスクは、完全に把握することが難しいといえるだろう。グローバル化が進み、国内だけでなく海外で発生した事象が国内のクラウドサービスに影響を及ぼす可能性もあり、広範な情報収集とリスク分析が進められることが望まれる。想定されるリスクについて防御する対策をとり、また、保険へのリスクの移転や万が一発生した場合の事後策についてあらかじめ検討しておくことが促される。

---

[60] 総務省は、利用者によるクラウドサービスの比較・評価・選択等に資する情報に対するニーズに対応するため、「クラウドサービスの安全・信頼性に係る情報開示指針」を策定・公表してきた。