TOKIO MARINE

リスクマネジメント最前線

2022 | No.14

GAFAM のサービス停止が企業活動に与えるリスクと対策

ビジネスリスク本部　上級主任研究員　城野 崇

専門分野：全社的リスクマネジメント、危機管理広報を含む危機管理、不正・不祥事対策等。公認不正検査士（CFE）。

デジタルトランスフォーメーション（DX）や働き方改革、リモートワークの推進等を背景に、事業・業務の中で情報システムを導入する流れが従来より加速する中、クラウドサービスの利用が企業の業務に急速に浸透している。このクラウドサービス市場ではＧAFAM[1]が提供するサービスへの依存度が高い。一方、GAFAM 等のクラウドサービスを利用できなくなる障害もたびたび発生しており、多くの企業のさまざまな業務・サービスに大きな影響が生じる事態が相次いでいる。

本項では、GAFAM 等のクラウドサービス利用の状況を整理するとともに、それらのサービスで障害が生じるリスク等を分析する。また、クラウドサービスが停止した際に企業が被る影響を踏まえ、企業がとるべき対策についても提案する。

[1] **G**oogle の持ち株会社 Alphabet、**A**pple、**F**acebook を運営する Meta Platforms、**A**mazon、**M**icrosoft の 5 社を指す。

1. GAFAM サービスの浸透

（1）クラウド市場における台頭

デジタル庁は 2022 年 10 月 3 日、「ガバメントクラウド」の調達先として、Microsoft、Amazon Web Service（AWS）、Google、Oracle の日本法人を採択したと発表した。日本の行政機関が共同利用するガバメントクラウドの調達先として国内企業が選定されなかったことは大きく報じられたが、同時に調達先が、世界のクラウド市場を寡占する米系ビッグテック企業（世界的に影響力を有する巨大 IT 企業）であったことに驚きは少なかったといえる。

GAFAM は、それぞれ一般消費者向けの事業、法人向け事業と多角的に事業展開しており、売上高に占める割合の大きい順に主要事業を整理すると図表 1 の通りである。

一言でいえば、Alphabet（Google）および Meta は広告事業主体、Apple はハード事業主体、Amazon は EC 主体、Microsoft はソフト主体の事業構造といえるが、Alphabet、Amazon、Microsoft の 3 社はそれぞれ Google Cloud Platform（GCP）、Amazon Web Service（AWS）、Microsoft Azure のブランドでクラウドサービス事業を急速に成長させており、それぞれ自社の売上高 2 ～ 3 位に成長している。

■ 図表 1 GAFAM の売上高に基づく事業構成

社名	構成比 1 位	構成比 2 位	構成比 3 位
Alphabet/ Google	広告（検索、YouTube 等）	サービス（コンテンツ）	クラウド（GCP）
Apple	ハード（iPhone、iPad、Mac 等）	サービス（金融、コンテンツ）	その他
Meta Platforms/ Facebook	広告	—	—
Amazon	EC・マーケットプレイス	クラウド（AWS）	有料会員サービス
Microsoft	ソフト（Microsoft 365、Windows）	クラウド（Azure）	ハード（Surface、ゲーミング）

（出典： 米 Visual Capitalist の 2022 年調査[2]を基に整理。黄色塗セルはクラウドサービス事業を表す）

また、市場シェアを見ると、2022 年第 3 四半期におけるクラウドサービス事業者の世界市場は、Amazon（34%）、Microsoft（21%）、Alphabet（11%）の 3 社で全体の 3 分の 2 を占めた。日本の公正取引委員会は、クラウドサービス市場の寡占が進む背景について、先行する事業者ほどスケールメリットによるコスト競争力を有する点や、クラウドサービスを利用するのにも技術知識が求められるため事業者ごとに技術者が必要になる点などを指摘[3]している。

（2）企業のクラウド利用動向

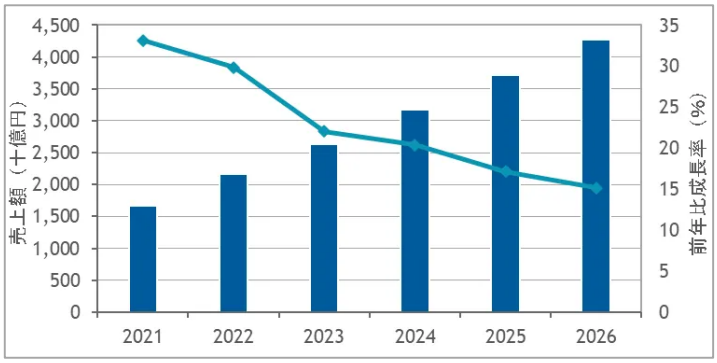
総務省の令和 3 年通信利用動向調査によれば、クラウドサービスを利用している国内企業は、「全社的に利用している」（42.7%）と「一部の事業所又は部門で利用している」（27.7%）を合わせて、全体の 70.4%で過去

[2] Visual Capitalist “How Do Big Tech Giants Make Their Billions?” April 25, 2022
https://www.visualcapitalist.com/how-big-tech-makes-their-billions-2022/

[3] 公正取引委員会「クラウドサービス分野の取引実態に関する報告書」（2022 年 6 月 28 日）
https://www.jftc.go.jp/houdou/pressrelease/2022/jun/220628.html

最高の割合を記録した。また、調査会社 IDC ジャパンは、国内のクラウドサービス市場規模について 2022 年に 2 兆円を超え、今後の成長率は鈍化するとしても右肩上がりで成長するものと予測している（図表２）。

■ 図表２ クラウドサービス市場の売上額予測



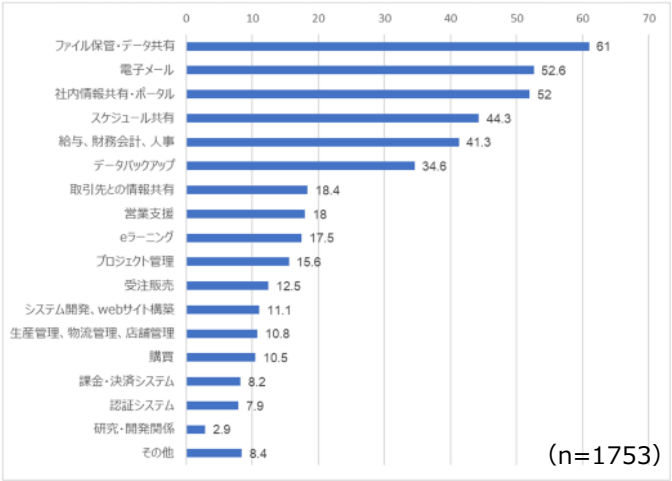
（出典：IDC ジャパンによる国内パブリッククラウドサービス市場予測[4]）

クラウドサービスの利用が進む理由としては、サーバを自社で調達・構築・運用するオンプレミス方式に比べ、次のような利点が評価されていると考えられる。

- 社内に持つべき資産や保守体制を軽くできる
- クラウドサービス事業者が保守・運用を行うため安定運用が可能（自社運用部分を除く）
- 迅速、かつ柔軟にコンピュータ、ネットワーク等の規模・構成を変更できる
- 柔軟に構成を変更できるため最新技術を導入しやすい
- 災害時のバックアップとして利用できる
- 構築コストを低く抑えることができる　　等

国内企業におけるクラウドサービスの用途としては、図表 3 に示すように「ファイル保管・データ共有」「電子メール」「社内情報共有・ポータル」「スケジュール共有」などの一般的な業務ツールとしての利用が上位を占めた。また、「システム開発、web サイト構築」「生産管理、物流管理、店舗管理」などの利用は低いものの、1 割程度の回答がある。

■ 図表３ 国内企業におけるクラウドサービスの用途



（出典：総務省の令和 3 年通信利用動向調査）

[4] IDC ジャパン「国内パブリッククラウドサービス市場予測を発表」（2022 年 9 月 25 日）
https://www.idc.com/getdoc.jsp?containerId=prJPJ49684222

（3）利用されるクラウドサービス

各社が提供する「クラウドサービス」の中で、実際にはどのようなサービスが利用されているのか、ICT 業界で広く用いられている米国の国立標準技術研究所（NIST：National Institute of Standards and Technology）によるクラウドサービス分類を用いて以下のように整理した。図表 4 は各社の代表的なサービス名である。

□SaaS（Software as a Service）

Microsoft 365、Teams、Gmail、Facebook Messenger のように、インターネットを介して直接、ソフトやアプリケーションの形で提供するサービス。ユーザーは通常、これらのシステムがどのようなコンピュータやネットワークで構成・運用されているのか意識する必要がない。

各社のセキュリティ施策によって異なるが、オフィス以外からでもどこでもアクセス・利用できる点を生かして、企業のあらゆる部門において Office ソフトやメールソフト、コミュニケーションツール、ファイル共有の場面で利用されている。災害時などのコミュニケーションツールとして利用するケースも増えている。

□PaaS（Platform as a Service）

Azure App Service、Amazon ECS のように、システム・アプリの開発環境として提供するサービス。コンピュータやネットワーク、OS だけでなく、よく活用されるミドルウェアなどもセットで提供されるため、利用企業が開発環境の整備にかける労力を低減できる。

直接利用するのはシステムの開発や運用部門が多いが、IoT、AI の基盤としても提供され、業務システムやお客様向けシステムの運用の裏側で利用されている場合がある。

□IaaS（Infrastructure as a Service）

Google Compute Engine、Azure Virtual Machines のように、インターネット上に仮想コンピュータやネットワーク、OS を提供するもの。PaaS に比べて、環境を自社で整備しなければならないが、個社事情に合わせて自由に整備できる。

システム部門が仮想コンピュータを用いて自社サーバを柔軟に構築し、その環境でシステム開発・運用を行う。PaaS と同様、業務システムやお客様向けシステムの運用に利用されている場合がある。

■ 図表４ 企業で利用される主なクラウドサービス名

クラウド種別		SaaS	PaaS	IaaS
GAFAMの主要ウェブサービス	Alphabet/Google	・BigQuery ・Ads ・Gmail、Workspace、検索、マップ、YouTube 等	・App Engine ・Cloud Run	・Cloud Storage ・Compute Engine
	Apple	・iCloud App ・Apple Pay、マップ 等	—	—
	Meta Platforms/ Facebook	・Ads ・Facebook、Instagram ・Messenger、WhatApp	—	—
	Amazon	・EC サイト、マーケットプレイス	・ECS ・Lamda	・EC2 ・S3
	Microsoft	・Microsoft 365、Outlook ・Teams ・LinkedIn	・Azure App Service	・Azure Virtual Machines
その他企業のサービス		・Apps on SDPF ・Zoom ・box ・Slack	・Salesforce Platform ・SDPF プラットフォームサービス	・SDPF クラウド/サーバー ・IBM Cloud 等

（出典：各社のウェブサイトを基に弊社整理）

要すれば、GAFAM のクラウドサービスには、一般従業員や顧客が直接利用するもの（SaaS 型）と、企業がクラウドサービスを活用してシステム・サービスを構築し、従業員や顧客に利用してもらうもの（PaaS 型/IaaS 型）に分かれ、いずれも幅広い場面で利用されている。

2. GAFAM のサービス停止等

前述の通り、企業がクラウドを利用する理由の一つとして、GAFAM の専任チームが運用にあたることで自社での運用と比べても安定運用を期待できることが挙げられる。しかしながら、GAFAM のクラウドサービスが停止した事例は多数存在する。

本章では、クラウドサービスの停止・障害の要因と、主要な障害事例について整理する。

（1）クラウドサービス停止・障害の発生原因

クラウドサービスであっても事業者のデータセンターには物理的なコンピュータやネットワークによりシステムが構築・運用されているため、障害の発生原因としてはオンプレミス型のシステムと同様に、図表 5 のような脅威が想定される。

■ 図表 5 システム障害を引き起こす脅威の例

脅威の類型		脅威の例	クラウドサービスで脅威が生じる範囲	
			①クラウド事業者の範囲で発生	②利用企業の範囲で発生
意図的な要因(サイバー攻撃、犯罪等)		不正侵入、データ改竄・破壊、不正コマンド実行、ウイルス攻撃、サービス不能攻撃(DoS:Denial of Service)、情報漏洩、重要情報の詐取、内部不正 等	○	○
非意図的な要因	偶発的な要因(人為的ミス、機器故障)	操作・設定ミス、プログラム上の欠陥(バグ)、メンテナンス不備、内部・外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥、機器故障 等	○	○
	環境的な要因(災害、疫病)	地震、水害、落雷、火災等の災害による電力設備の損壊、通信設備の損壊、水道設備の損壊、コンピュータ施設の損壊 等	○	―
	他分野の障害からの波及	電力供給の途絶、通信の途絶、水道供給の途絶（相互依存性解析の成果で判明しているもの） 等	○	―

（出典：独立行政法人情報処理推進機構 資料[5]をもとに、弊社がクラウド事業者・利用企業の別を追記）

オンプレミス型と異なるのは、クラウドサービス事業者側の運用・管理責任を有する範囲で生じるものと、利用企業側の責任範囲で生じるものに分けて考えなければならない点である。

まず、クラウドサービス事業者側と、利用企業側の双方で生じる可能性があるのが「意図的な要因」「偶発的な要因」の脅威である。例えば、クラウドサービス事業者の操作ミスで障害が発生した場合は、クラウドサービス事業者が復旧対応を行うことになり、利用企業側が停止・障害自体の復旧にあたることは難しい。復旧を待つか、代替手段により業務を実施する必要がある。逆に、利用企業側の操作ミスで障害が発生する場合もあり、その際は通常のシステム障害と同様、利用企業側が自社の責任で対応する必要がある。

一方、クラウドサービス事業者側でのみ生じるものは、実際のデータセンターが物理的に影響を受ける「環境的な要因」や「他分野の障害からの波及」である。これらの要因による障害に対してはクラウドサービス事業者が復旧対応を行うこととなり、利用企業側が停止・障害自体の復旧にあたることは難しい。

（2）GAFAM のサービスが停止した障害事例

図表 6 は GAFAM のサービスが停止し、企業等の業務・サービスに具体的な影響が生じた主要な障害事例を抜粋したものである。

それぞれの障害の要因について、報道では不詳のものもあるが、前項の脅威類型でいう「偶発的な要因」「環境的な要因」「他分野の障害からの波及」が大半であり、SaaS 型、PaaS 型、IaaS 型のいずれにおいてもサー

[5] 独立行政法人情報処理推進機構（IPA)「システム障害事例の分析により得られた教訓の共有～教訓を活用して情報システムの類似障害を削減～」（2017 年）

ビスそのものや一部機能に支障が出た事例が報じられている。クラウドサービスが停止したことで、利用企業がビジネスの一環として顧客向けに提供しているアプリやサービス、ウェブサイトが停止した事例や、社内業務ツールが利用できなくなった事例が明らかになっている。また、報道では直接言及されなかったものの、IaaS 等に依存して運用している基幹システム等があれば同様に停止した可能性がある。

ただし、これらの事例においては、最長でも 10 時間程度で復旧しており限定的な影響ではある。

なお、AWS の場合、特別の条件がなければ稼働率の SLA（Service Level Agreement：サービス目標）は 99.99%とされている。これは、裏返せば利用時間の 0.01%は稼働しないおそれがあるということであり、年間 365 日（8760 時間）のうちの 1 時間弱（0.876 時間＝約 52 分）の停止が発生しても想定の範囲内ともいえる。

■ 図表 6 GAFAM のクラウドサービスにおける主な障害事例

企業	時期	内容
Alphabet/ Google	2022 年 7 月	・ 英国のデータセンターで、40℃を超える猛暑により冷却系が故障。データセンターの一部を停止したところ、Cloud Storage や BigQuery などのサービスに影響が出た。英ネット銀行のアプリが一時的に利用できなくなった。
	2021 年 11 月	・ Google 内のネットワーク設定変更に不備があり、App Engine などのクラウドサービスに障害が発生。これらを利用するポケモン Go や Spotify などのサービスが停止した。
	2020 年 12 月	・ アカウントのログイン認証サービスで障害が発生し、ログインが必要な Gmail や Google ドライブなど Google のサービスをすべて利用できなくなった。1 時間程度で復旧。
	2020 年 3 月	・ Cloud 関連のアクセスを制御するシステムに異常が生じ、Compute Engine や Cloud Storage などのサービスが 10 時間程度利用できなくなった。
Meta Platforms/ Facebook	2021 年 10 月	・ サーバのアドレスを指定する DNS 設定を誤り、Facebook や Instagram、WhatsApp のサービスに 6 時間程度アクセスできなくなった。
Amazon	2021 年 12 月	・ AWS の米国東部リージョンで大規模障害が発生。Lamda や API Gateway など様々なサービスが利用できなくなり、ゲーム会社のネットワークサービスなどで障害が発生。 ・ AWS の米国西部（北カリフォルニア）リージョンと米国西部（オレゴン）リージョンでネットワーク障害が発生。映像配信サービス、ウェブ会議システムなどが利用できなくなった。
	2021 年 9 月	・ AWS のネットワーク機器障害に起因して大規模な輻輳が発生。 ・ AWS Direct Connect を利用する都市銀行のアプリや証券会社のサイト、携帯電話会社の決済サービス、航空会社のチェックインサービス等が繋がりにくくなった。
	2021 年 2 月	・ 東京リージョンで冷却システムへの電力供給が適切に行われず仮想マシンの処理能力が低下。気象庁のウェブサイトが接続できない状況になった他、一部のソーシャルゲームや暗号資産取引所でサービス提供が不能になった。
	2020 年 10 月	・ 東京リージョンのネットワーク大規模障害により EC2 を利用するサービスに影響が出た。EC2 を利用する QR 決済アプリなどが一時的に利用できなくなった。
Microsoft	2022 年 12 月	・ Outlook や Teams、Skype に繋がりにくい状況が 4 時間程度続いた。電話システムに Teams を活用している JETRO では外部からの電話が繋がりにくい状況が生じた。
	2022 年 7 月	・ 内部データベースの更新で不具合が発生し、Teams や Microsoft365、関連するサービスが 7 時間程度利用できなくなった。
	2021 年 2 月	・ Virtual Machines などで障害が発生し、鉄道会社のアプリやウェブサイトが利用できなくなった。

（出典： 各種報道を基に弊社作成）

（3）障害が長期化した他社事例

前項の障害事例では、サービス停止は数時間程度にとどまったものが多いが、GAFAM 以外では、影響が長期化した事例もある。

2019 年 12 月、国内 IT ベンダーが自治体向けに提供する IaaS で、ストレージのファームウェアでトラブルが生じ、全国 53 の自治体・団体の業務システムが稼働できず、ウェブサイトの閲覧や住民票、戸籍、印鑑証明書の発行ができないなど、業務が中断した。IaaS としての復旧に数日かかったほか、一部自治体のデータが復元できず、全面復旧までに 1 ヶ月以上を要した。

また、クラウドサービスをめぐる事例ではないものの、2022 年 7 月に発生した KDDI の通信ネットワーク障害においては、合計約 80 時間の通信障害が継続している。

（4）「リージョン」と「アベイラビリティゾーン」を踏まえたリスク分析

Amazon、Google、Microsoft のクラウドサービスの停止・障害の影響範囲を適切に分析するためには、クラウドサービスのデータセンターにおける「リージョン」と「アベイラビリティゾーン」の構造を把握する必要がある。事業者ごとに用語が異なる場合があるが、考え方や構造はおおむね共通している。

□リージョン

クラウドサービスのデータセンター群を設置する地域のことをいう。

リージョン同士は、地理的に離れている上に、ネットワークなど物理的に分離されて設計しており、大手 3 社の場合、利用者はリージョンを選んで利用できる。

例えば、AWS は世界 30 リージョンを展開しており、アジアパシフィックエリアにおけるリージョンは、東京、シンガポール、ソウル、大阪、ムンバイ、ジャカルタ、香港、北京、寧夏の 9 リージョンが設けられており、これらリージョンは複数が同時に物理的な損傷を受けたりしないよう、地理的に分離されている。アジアパシフィック以外にも北米、南米、欧州、中東、アフリカなどのエリアごとに、それぞれリージョンが設けられている。

■ 図表 7 AWS のリージョンとアベイラビリティゾーン

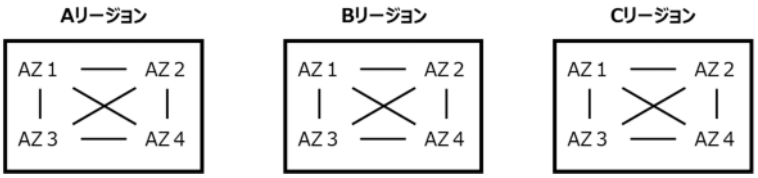
（出典： AWS ウェブサイト）

□アベイラビリティゾーン（AZ 可用性ゾーン）

ひとつのリージョンの中に複数配置されている各データセンターを指す。図表 7 は AWS のリージョンの一つ、大阪リージョンには 3 つの AZ で構成されることが確認できる。

図表 8 はリージョンと AZ の関係を模式図で示したもので、AZ１～AZ４の一つ一つが AZ（データセンター）を示しており、数キロ以上離れた３～４つの AZ が高速回線で連結されてリージョンを構成している。AZ 同士は高速回線で繋がれているため、AZ をまたいだデータやリソースの連携は実施しやすい。

■ 図表 8 AWS のリージョンと AZ のイメージ



（出典：弊社作成）

それぞれの類型について、一つの AZ で脅威が生じた場合に当該 AZ では停止・障害が生じるが、他のリージョンや AZ を用いて冗長化している場合の影響の有無を整理すると、図表 9 の通りである。

■ 図表 9 リージョン・AZ をまたいだ影響のおそれ

脅威の類型		リージョンをまたいだ影響	AZ をまたいだ影響
意図的な要因(サイバー攻撃、犯罪等)		物理的に分離されているため、他リージョンへの波及は考えにくい。 ※ 例外的に複数のリージョンが攻撃された場合、同時に障害・停止が発生する。	ネットワークで接続されているため、不正コマンド・ウイルスなどの**脅威が他 AZ に波及する可能性がある。**
非意図的な要因	偶発的な要因(人為的ミス、機器故障)	物理的に分離されているため、他リージョンへの波及は考えにくい。 ※ 例外的にリージョン間で同期連携するようなシステムの場合、同時に障害・停止が発生する。	ネットワークで接続されているため、設定ミス・操作ミスなどの**脅威が他 AZ に波及する可能性がある。**
	環境的な要因(災害、疫病)	地理的・物理的に隔絶されているため、他リージョンとの同時障害は発生しにくい。	数キロ程度の距離があるため、同時に損傷する事態は少ないが、**大地震等の広域災害では複数 AZ が同時被災し得る。**
	他分野の障害からの波及	地理的・物理的に隔絶されているため、他リージョンとの同時障害は発生しにくい。 ※ 同一国内などで地理的に近いリージョンが存在する場合、同時に障害・停止が発生する。	数キロ程度の距離があっても**複数 AZ が同一の広域ライフライン事業者に依存する場合は同時障害が生じ得る。**

（出典：独立行政法人情報処理推進機構の脅威の類型を用いて、弊社が影響を整理）

すなわち、各リージョンが完全に独立し、一つのリージョンでの障害が他のリージョンに影響する事態は起こりにくいとされるが、リージョン内の複数の AZ をまたいだ影響は十分生じうると考えるべきである。

実際、前述(2)の GAFAM の主要障害事例でも、単一リージョン全体の障害事例は多いが、リージョンをまたいだ事例は 2021 年 12 月の AWS の障害事例のみを確認している。これは、やや近接している米国西部の２リージョンで、同一のネットワークの混雑により繋がりにくかったことが原因であった。

システム障害以外にも GAFAM の事業撤退によって、企業がサービスを利用できなくなる事態が想定される。この場合、通常数ヶ月～１年程度の猶予をもって撤退・変更が行われることが多い。

事例として、Google は 2022 年 8 月、IoT 端末の管理やデータ分析等を行うための PaaS「Cloud IoT Core」について、競争優位性がないとして 1 年後の 2023 年 8 月に終了することを発表した。これにより利用企業は別サービスへの移行を強いられた。

今後も AWS や GCP、Azure 等のクラウドサービス全体が撤退することは考えにくいとしても、一部の機能・サービスが終了することは常に想定しておく必要がある。

3. 企業としてのリスクと求められる対策

（1）企業に生じる影響

クラウドサービスの障害が生じた場合、それぞれの企業で利用しているクラウドの用途によって、様々な影響を及ぼす。第 1 章 2 項で紹介した令和 3 年通信利用動向調査での用途ごとに、典型的な影響の例を図表 10 に整理した。

■ 図表 10 クラウドの用途ごとに想定される影響

クラウドの用途	想定される影響の例
ファイル保管・データ共有、データバックアップ 取引先との情報共有	● ファイルの共有フォルダを利用できなくなり、業務データの利活用が遅延・停滞する。 ● 取引先からデータを受領できなくなり、発注内容や売上等の重要情報を把握できず、取引を失う。
メール、コミュニケーション、社内情報共有、e ラーニング	● メールやビジネスチャットを利用できなくなり、上司や取引先からの指示・依頼を確認できず業務を遂行できない。取引先に重要な報告を行えない。 ● オンライン会議を社内外と実施することができず、プロジェクトの効率が大きく低下する。 ● 社内ポータルサイトを利用できなくなり、従業員に必要な情報を発信できない。
給与、財務会計、人事	● 人事系システムが利用できなくなり、正しい労働時間や給与の計算ができず業務処理が停滞する。または長時間労働を管理できず、法令違反が生じる。加えて最悪の場合、給与支払いが遅延し労働基準法違反となる ● 財務会計データが利用できなくなり、法定の期日までに財務報告を行えなくなる。
営業支援、プロジェクト管理、スケジュール共有	● 有力な顧客や商談の状況、従業員の行動を把握できず、本来獲得できた取引の売上・利益を逸失する。 ● プロジェクト管理システムが利用できなくなり、解決すべき課題が放置された結果、業務品質が大幅に低下する。または、プロジェクト遂行が遅延する。
受注販売、課金・決済システム	● 顧客が、EC の販売システムや店頭の決済サービスを利用できなくなり、その結果、商品・サービスを販売できない。顧客離れや逸失利益が生じる。
システム開発、web サイト構築、研究・開発関係	● システム開発環境を利用できなくなったことで開発が遅延し、サービス開始時期に間に合わない。逸失利益が生じるほか、状況によっては損害賠償が生じる。 ● IoT システム、AI システム等が作動しない、または障害によりデータが汚損され、期待と反する動作を行ってしまい、外部に損害を与える。
生産管理、物流管理、店舗管理、購買	● 生産・物流・購買等の管理システムが使用できなくなり発注や生産、出荷が遅延・停止し、逸失利益が発生する。 ● 店舗の来店者数や売上高、店舗在庫等の管理システムが使用できなくなり、店舗運営効率が悪化する。逸失利益が発生する。
認証システム	● 物理的な拠点やフロアの認証システムが利用できなくなり、役職員が入構・入室できず業務が遅延・停止する。または、不審者の侵入を防げず、会社資産を窃取される。 ● システム上の認証を行えなくなり必要な業務サービス全般にアクセスできなくなる。上記の影響が幅広く発生する。

（出典：総務省の令和 3 年通信利用動向調査における用途分類を用いて弊社が影響を整理）

（2）求められる対策

上記のような影響を避けるため、クラウドサービス事業者における障害の発生原因（例えば設定ミス 等）に対して、利用する企業側が関与することは難しい。このため、障害が発生したとしてもその影響を極力小さくするための事業継続計画を検討する必要がある。

□ビジネス影響分析（BIA）・被害想定

まず、自社のビジネスの中でクラウドサービスに依存している事業・業務を洗い出し、障害が発生した場合の影響を分析して、その影響の重大性を評価する「ビジネス影響分析」を行う。事業・業務で利用している他社システムが、クラウドサービスに依存している可能性を含めて洗い出す。

このとき、クラウドサービスでの障害リスクは、第２章での事例を踏まえれば、仮に次のように分析できる。ただし自社で契約しているクラウドサービス事業者における契約条件やサービス構成、過去の障害事例等により異なるため、実態に合わせて設定する必要がある。

- 「復旧まで数時間程度」を要する障害が「２～３年に１回」の頻度で発生

このリスクを踏まえ、各事業・業務にどのような影響が生じるかを具体的に分析する（内容の例は図表 10 を参照されたい）。停止したとしても想定の時間程度であれば事業・業務に重大な影響は出ないのか否かを判断する。許容できない重大な影響が出ると判断されるものは「重要事業」「重要業務」であり、事業継続戦略を定める必要がある。

なお、クラウドサービス事業者の利用規約では一般的に、障害が発生した際にも、利用料の返金（またはポイント付与）を行うことはあっても、それ以上の責任は免責としているため、損害や逸失利益をクラウドサービス事業者に賠償請求することはできないという前提に立ち、事業・業務が停止した際の影響を検討しなければならない。

□事業継続戦略

BIA の結果、重要事業・重要業務と判明した事業・業務で利用しているクラウドサービスについては、障害が発生した場合でも影響が小さくなるようなシステム構成または利用形態とするか、システムが停止しても代替手段で事業・業務を継続できることが重要である。戦略の主要な方向性を①②に整理した。

①冗長化による影響の極小化

前述したように、クラウドサービス事業者は障害の影響を単一の AZ 内やリージョン内に留める施策を講じていることから、利用企業としては、一つの AZ で障害が生じたとしても複数 AZ を利用（マルチ AZ 化）したり、または別リージョンを利用（マルチリージョン化）する等、冗長化を行うことで稼働を継続できる可能性を高められる。当然ながら、マルチ AZ 化やマルチリージョン化を行う分、構築コストや運用コストを要する。

さらに、複数のクラウドサービスで冗長化を施す（マルチクラウド化）場合もある。この場合、クラウドサービスごとに必要なスキルが異なることから、例えば AWS と GCP で冗長化する場合には、社内システム部門やベンダーにおいてもそれぞれに対応できる技術者を確保しなければならず、構築コストや運用コストはなおさら大きい。

事業・業務が停止する影響と、事業継続のためのコストを判断して導入されたい。

②代替実施・仮対応

当該クラウドサービスを利用せずに、重要事業・業務を実施する要領を事前に定めておく。図表 11 に整理する主要な代替実施・仮対応の考え方を組み合わせて検討する。代替実施・仮対応は、平常時と異なる手法となるため、手順書の策定や訓練を実施して、いつでも対応できるよう備えておくことが望ましい。また、代替実施・仮対応により業務品質が下がると予見される場合、顧客・取引先へあらかじめ説明し、理解を求めることも必要になる。

■ 図表 11 代替実施・仮対応の考え方

類型	内容
システム外対応	・ クラウドサービスに依存しない Office ソフトや紙の情報・記録様式、電話・口頭・手動操作などの手段により、事業・業務を実施できるようにしておく。
データのバックアップ	・ 重要なデータは当該クラウドサービスとは別の、社内ネットワークやスタンドアロン PC などに定期的に保存しておき、閲覧・利用できるようにしておく。 ・ 重要なデータは定期的に紙で出力しておき、閲覧・利用できるようにしておく。
仮払い	・ 正確な集計・計算が必要な場合でも、前回データ等に基づいて仮払いする。クラウドサービス復旧後、本来の集計・計算を行い、修正する。
副系システムの稼働	・ システムの機能が不可欠である場合、クラウドサービスに依存しない、スタンドアロンまたはオンプレミス型システムを構築しておき、稼働を切り替える。

（出典：弊社作成）

□早期検知・有事対応

①②のような事業継続戦略をとるにあたり、停止・障害が発生した場合にいち早く検知し、対応を行える体制を構築しておくことも重要である。

各クラウドサービス事業者は、自社サービスの稼働状況・障害情報をダッシュボードや SNS などで掲載しているほか、監視のためのクラウドサービスを提供している。これらの情報を活用して、障害発生時にはアラートを得て、対応体制を立ち上げるルールを整備しておくべきである。また、障害が発生している場合は、これら稼働状況・障害情報も正確な情報を反映していないおそれがあることから、第三者が提供する監視サービスを活用できるとなおよい。

□クラウドサービスリストの活用

クラウドサービス事業者が、障害対策を含めて可用性を適切に担保できる体制を備えているかどうかを確認した上で、クラウドサービスを選定する。

冒頭のデジタル庁によるガバメントクラウド調達先選定においては、内閣官房セキュリティセンター等が策定した「政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program：ISMAP」を活用している。これは政府システムの調達先選定のための基準であるが、これに基づき選定されたクラウドサービスリスト[6]が公開されており、民間企業におけるサービス選定でも活用できる。

[6] ISMAP クラウドサービスリスト https://www.ismap.go.jp/csm?id=cloud_service_list

4. おわりに

GAFAM をはじめとしたクラウドサービスは今や大半の企業にとって欠かせない外部リソースとなっているが、一方で、自然災害のように利用企業がコントロールできない事業停止リスクが生じている状況も懸念される。このリスクを適切に把握し、クラウドサービスの導入効果を下げることのないように事業継続戦略を定めておくことが肝要であり、各社の検討において本稿が参考になれば幸いである。

[2022 年 12 月 27 日発行]

To Be a Good Company

東京海上ディーアール株式会社

ビジネスリスク本部　上級主任研究員　城野 崇（専門分野：全社的リスクマネジメント、危機管理広報を含む危機管理、不正・不祥事対策等。
公認不正検査士（CFE））
〒100-0004 東京都千代田区大手町 1-5-1 大手町ファーストスクエア ウエストタワー23F
Tel. 03-5288-6594　Fax. 03-5288-6626 https://www.tokio-dr.jp/