特集
Special Feature

［社会インフラシステムにおけるサイバーセキュリティ―レジリエントで持続可能なデジタル経済社会に向けて―］

2 クラウドファースト時代のサイバーセキュリティ

―サイバーセキュリティのためのマルチステークホルダアプローチ―

応般

石黒正揮　三菱総合研究所

クラウドセキュリティの重要性

「クラウド・ファースト」時代の到来！，企業が情報システムを構築・更新する際に，自前で基盤やアプリケーションを開発するのではなく，クラウドサービスの活用を第一に考えるべきとする動きが進んでいる．米国では，Cloud First の次の戦略（Beyond Cloud First）を策定し☆1，政府におけるクラウド活用を加速している．米政府機関では，セキュリティレベルの最も高い TOP SECRET（最高機密）の要求を満たすシステムとして，Amazon Web Services（AWS）などの外部のパブリッククラウドの採用も進んでいる☆2．

日本政府においては 2018 年にクラウドサービスの利用を第一候補とする「クラウド・バイ・デフォルト原則」が示された☆3．クラウドサービスを利用する国内企業の割合は 6 割を超え，年々増加傾向にあり，クラウド・シフトが鮮明になってきている☆4☆5．クラウドサービスを利用することで，企業は機動的に事業を立ち上げ，低コストでシステムを構築できるなどメリットは大きい．一方で，他のユーザとのシステム資源の共有，クラウド事業者への依存などによりクラウド特有のリスクへの対応が課題になる．政府の重点政策に掲げられる**経済安全保障法制の検討においては，電力や情報通信などの基幹インフラの安全性・信頼性の確保のため，クラウドの導入においては，国の審査の義務付けが挙げられている**☆6．このような背景から，本稿では，クラウド特有のリスクやそれらに対するセキュリティ対策の考え方についてポイントをまとめ，今後の課題と取り組み策について展望する．

クラウドシステムのリスクの特徴

クラウドは，利用者が必要なときに，必要な分だ

☆1 米国ホワイトハウス FEDERAL CLOUD, COMPUTING STRATEGY, https://www.whitehouse.gov/wp-content/uploads/2019/06/Cloud-Strategy.pdf

☆2 AWS Secret Region, GovCloud Region 等.

☆3 「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」

☆4 情報通信白書令和 2 年版では，クラウド利用企業は 2019 年に 64.7%に達し，クラウド基盤サービス市場は，17 年から 23 年までの年平均成長率（実績および予測）は 25.4%.

☆5 クラウドは，もはや情報系だけの世界にとどまるものではなく，セーフティクリティカルな自動車の制御系などにも持ち込む動きが活発化している．ARM 社が立ち上げた開発プロジェクト SOAFEE（Scalable Open Architecture For Embedded Edge）では，リアルタイム制御や機能安全への対応など，自動車特有の要件を満たす次世代ソフトプラットフォームを，オープンソースで提供することを目指す．SOAFEE のソフト基盤はクラウド側と車載側にそれぞれ存在し，アプリケーションはクラウド側のコンテナ形式で開発・検証することになる．

☆6 経済安全保障法制に関する提言骨子（基幹インフラの安全性・信頼性の確保）.

け計算リソース（サーバ，ストレージ，ネットワークなど）を動的に確保し，ネットワークを介して利用することができるシステムである．そのため，以下のような特性に留意が必要になる：

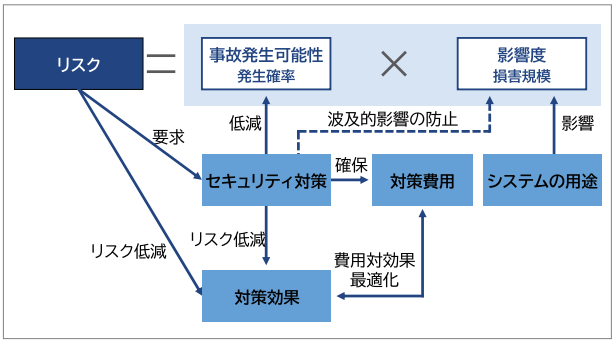
- 他の利用者とリソースを共有する
- 他事業者によりサービスとして基盤を提供される
- ネットワークを介して動的に提供される

クラウド提供者は，一般的にはセキュリティに関して高い能力を持つため，利用者は，提供されるクラウドサービスの高いセキュリティレベルを享受することができる．しかし，セキュリティ事故などにより，**最終的な損害や責任を負うのはクラウド利用者自身であり，対外的な信用が失墜するなどのレピュテーションリスクなどすべてのリスクをクラウド提供者に委ねられるわけではないことに留意**しなければならない．クラウドにおけるリソース共有や開発運用の協業などにおけるセキュリティ対策においては，「何が具体的なリスクなのか」を十分に把握した上，それに対応して対策を講じるリスクベースアプローチが有効である．図 -1 は，リスクと対策等の基本要素の関係を概念的に示したものである．

リスクの大きさは，事故発生の可能性（頻度・確率）とその影響度（被害の大きさ）の積となる．つまり，事故発生の確率が高いほど，または，その影響度が大きいほど，リスクは大きくなる．リスクを低減するためには，事故発生の確率を低減するか，または，その影響度を低減することが必要である．影響度は，扱う情報の機密性や利用業務の重要度によってある程度決まるため，扱う情報や業務を変えない限り，対策により低減できる程度は限られる☆7．したがって，通常は，システムや組織の脆弱性の低減により事故発生の確率を低減することがセキュリティ対策の主眼となる．

特に，クラウドの場合，提供者と利用者は協業関係にあることを前提として，両者の役割分担と責任関係を明確化して，クラウド利用者が実施すべき対策を実現するとともに，クラウド提供者が実施すべき対策についても要件化し，SLA 等を含む契約や評価・監査などを行うパートナとの協力を通じて実効性を確保することが重要である．

クラウドの特徴に応じたリスクを分類整理すると表 -1 のようになる．



■図 -1　リスクの構造と対策の関係

☆7 ただし，障害の波及的連鎖を防止することで，影響度を抑えるような対策はある．

■表 -1　クラウドのリスク分類

リスク	リスクの概要
共有リスク	計算リソースを共有することで，他利用者への攻撃の間接的影響等
協業リスク	クラウド利用者と提供者が他者への依存に伴うコントロール喪失等
技術リスク	仮想化，オーケストレーション，分散システムなど技術の複雑化に伴う脆弱性等
法制度リスク	国内外の法制度に伴う制約や，法執行に伴う影響など
組織リスク	クラウド利用者，提供者などの組織管理，内部犯行などの影響

■表 -2　リスク分類ごとのリスク具体例

リスク分類	リスク具体例
共有リスク	リソース集約の影響 H01，共同利用者からの影響 H03，リソース枯渇 H04
協業リスク	サービスエンジンの侵害 H06, クラウド内の DDoS 攻撃 M11，技術ロックイン L12，ガバナンス喪失 L13, サプライチェーン障害 L14,EDoS 攻撃 L15, 不正な探査 L17, データ保護 L20, 通信インフラ障害 M22, 機能サポートの制限 M23, ストレージへの攻撃 M26
技術リスク	仮想／物理の不整合 H02, 隔離の失敗 H05, 管理インタフェースの悪用 M08, データ転送路の不備 M09, 暗号鍵の喪失 L16, ID 管理の負担 M24
法制度リスク	電子的証拠開示 L18, 各国司法の相違 L19, ライセンス L21
組織リスク	内部不正・特権の悪用 M07, 不完全なデータ削除 M10, 脆弱性管理不備 M25

クラウドのセキュリティを確保するためにはこれらのリスクについて組織に応じて体系的，網羅的に脅威を洗い出し対策を講じることが求められる．

クラウドリスクの具体例

クラウドのリスクについては，欧州ネットワーク・情報セキュリティ機関（ENISA）や日本セキュリティ監査協会（JASA）などにより整理されている．そこで挙げられるリスクを含む形で，上記のリスク分類に応じて主なリスクを列挙すると表 -2 の通り整理できる．X01 から X21（X はリスクのレベルで H:High, M:Middle, L:Low の 3 段階）は ENISA, JASA により提示されたリスクで，M22 ～ M26 は本稿で追加したものである．また，複数のリスク区分に該当するリスク事例は，そのうち一方のみに記載している．

■表 -3　クラウドのステーホルダ分類

ステークホルダ	概要
クラウド利用者	クラウドを利用したアプリケーションの開発・運用・利用する．
クラウド提供者	クラウド基盤を提供する．
クラウドパートナ☆8	クラウド利用者，提供者に対して，構築運用支援・監査等を行う．

☆8 国際標準 ISO/IEC17789 で定義されている，クラウド利用者とクラウド事業者が協業するパートナのことで，クラウド デベロッパ，クラウド監査人，クラウドブローカなどが含まれる．

クラウドのセキュリティを確保するためには，これらのクラウド特有のリスクを認識し，当該組織にとっての具体的なリスクを特定し，通常のセキュリティ対策を強化することが求められる．

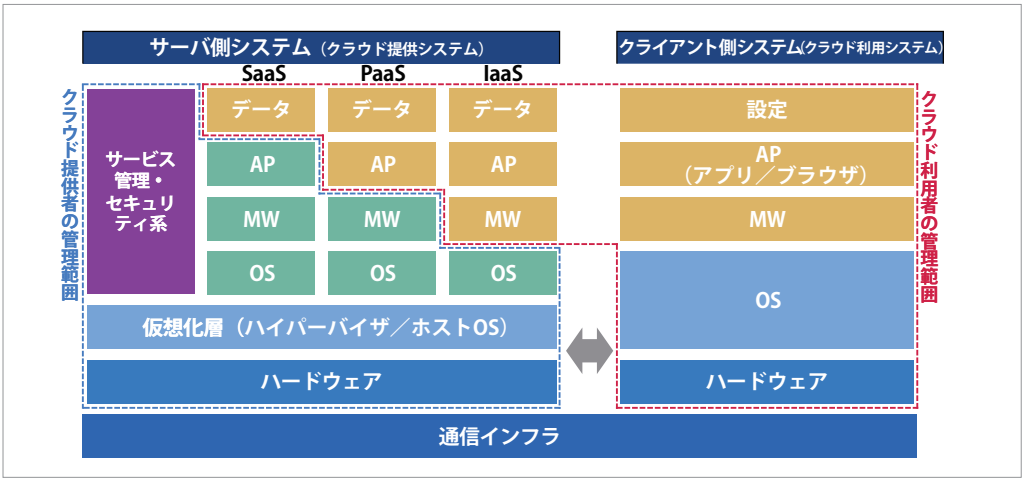
ステークホルダの責任分担

クラウドシステムは多様なステークホルダにより構築・運用される．クラウドシステム全体としてのセキュリティを確保するためには，ステークホルダについて責任範囲を明確にして，それぞれの責任を果たすために開発から運用に至るセキュリティ管理策を講じることが求められる．

ステークホルダを大きく分類すると表 -3 の通りである．

クラウドシステムの構成と責任範囲を示したものが図 -2 である．

クラウド提供者は，提供する基盤サービスの種類（SaaS/PaaS/IaaS）に応じて提供するシステムレイヤまで責任を負う．対して，クラウド利用者はクライアント側システムとサーバ側システムのうち，クラウド提供システムの上位にあるシステムの開発・運用について責任を負う．なお，ISO/IEC 27017:2015 においては，クラウドの 3 つのサービス種別に応じて，利用者と提供者は，下表の項目のいずれに責任を持つか，明確に定義しなければならないと規定している．たとえば，ID 管理システ



■図 -2　クラウドシステムの構成と責任分界

ムの保守は，ID 管理システムに脆弱性や更新がないか確認し対応することなどを意味する．このような要件も考慮してステークホルダ間の責任関係を契約で縛ることも必要である（表 -4）．

クラウド利用事業者とクラウド基盤提供事業者との間では以下のような要求事項を契約に含めることなどが挙げられる．

• SLA（Service Level Agreement）

提供されるクラウドシステムのサービスレベルについて規定するもののことであり，リスク整理表におけるリソース集約の影響，リソース枯渇などのリスクに対策する．サービス稼働率，平均応答時間，サポート項目，要求未達の場合の賠償規定などがある．

• 利用者の規約・禁止事項

利用者の不正行為や不注意などによって被害を受けるリスクに対して，クラウド利用事業者とクラウド関連事業者とで検討し，規約違反の他のクラウド利用者に対してクラウド提供の停止，または賠償請求により実効性を高める措置などを講じる．

• クラウド基盤提供者の体制管理

クラウド提供事業者における内部の不正を防止・抑止するため，ラウド提供システムやメンテナンスシステム等のアクセス特権の管理，情報取扱者の制限，監視・記録による不正行為・操作の抑止，雇用者の契約管理などの要求事項を定める．

• 法的リスクの開示説明

クラウドの所在地の法制度により電子的証拠の開示命令，個人情報の管理規則，輸出管理法令などによるリスクに対処するため，クラウドの所在地における法的リスクの開示を義務づける．

クラウド基盤利用者が，クラウド基盤提供者のセキュリティ対策の妥当性についてチェックすることが困難な場合がある．そのような場合，第三者による専門的な立場から対策の妥当性を保証するための仕組みとしてセキュリティ監査を用いることができる．そのような例として，クラウド情報セキュリティ

■表 -4　クラウド利用者と提供者の責任範囲☆9

区分	利用者	提供者
SaaS	• 収集・処理した顧客データに関するデータ保護法への準拠 • ID 管理システムの保守 • ID 管理システムの管理 • 認証プラットフォームの管理(パスワードポリシーを含む)	• 物理サポート基盤（施設，電力等） • 物理インフラ・セキュリティと可用性確保（サーバ等） • OS パッチ管理と堅牢化 • セキュリティ・プラットフォームの設定（FW 等） • ログ収集とモニタリング
PaaS	• ID 管理システムの保守 • ID 管理システムの管理 • 認証プラットフォームの管理	• 物理サポート基盤（施設，電力等） • 物理インフラ・セキュリティと可用性確保（サーバ等） • OS パッチ管理と堅牢化 • セキュリティ・プラットフォームの設定（FW 等） • ログ収集とモニタリング
IaaS	• ID 管理システムの保守 • ID 管理システムの管理 • 認証プラットフォームの管理 • ゲスト OS パッチの管理と堅牢化 • プラットフォームの設定（FW/IDS 等） • ゲストシステム監視 • ログ収集とモニタリング	• 物理サポート基盤（施設，電力等） • 物理インフラ・セキュリティと可用性確保（サーバ等） • ホストシステム（ハイパーバイザ，仮想 FW など）

☆9　ISO/IEC 27017:2015 抜粋

■表 -5　リスクの区分

意図的区分	概要
意図的脅威	悪意のある攻撃による事故の原因．組織の内部・外部の両方がある．
非意図的脅威	情報システムの不具合や通信インフラの障害など悪意によらない脅威．

■表 -6　技術対策と主なリスクの対応関係

技術的対策	対応する主なリスク
監視・脅威分析	サービスエンジンの侵害，リソースの枯渇，内部不正・特権の乱用，不正な探査・スキャン
脆弱性管理	管理インタフェースの悪用，データ転送路の不備，脆弱性管理の不備，サービスエンジンの侵害
認証・アクセス制御	内部不正・特権の悪用，ガバナンスの喪失，不正な探査・スキャン
ネットワーク防御	リソース枯渇，隔離の失敗，クラウド内の DDoS/DoS 攻撃，不正な探査・スキャン
ストレージ防御	コンテンツやストレージへの攻撃，不完全なデータ削除
構成管理・セキュア開発	サプライチェーンにおける障害，隔離の失敗，サービスエンジンの侵害，管理用インタフェースの悪用，事業者が管理すべき暗号鍵の喪失

監査制度，政府情報システムのセキュリティ評価制度（ISMAP）などがある．

クラウドのセキュリティ対策の全体像

クラウドのリスク対策については，悪意を持った意図的な脅威とそれ以外の非意図的な脅威という観点でも分けられる（表 -5）．

意図的脅威に対する対策は，技術対策と組織対策に分けることができ，それらを組み合わせて対処することが必要である．主な技術対策，組織対策と前述のリスクとの対応関係を整理すると表 -6 のようになる．

このほかに，非意図的脅威に対する対策は主に信頼性の向上，安定性の確保に係るもので，セキュリティ対策と分けて考えることができる．その例としては，単一障害点の解消，正規の利用における負荷の集中・輻輳への対応，リソースの冗長化，動的なリソース確保，ソフトウェアの品質確保などが挙げられるが，本稿はセキュリティに関する特集であり，紙面が限られるため，非意図的脅威については省略する．表 -3 に挙げた技術対策の概要は表 -7 の通りである．

■表 -7　クラウドに適用される主な技術的対策

技術的対策	概要
監視・脅威分析	ネットワーク上の通信，情報システムの操作などのログを監視・分析し，異常や不正な活動を検出する．
脆弱性管理	利用システムの脆弱性の特定と修正により脆弱性対策を迅速に行う．
認証・アクセス制御	ID 認証に基づき，アクセス許可やアカウントの役割（ロール）に応じた認可，特権管理を行う．
ネットワーク防御	ネットワークへの攻撃，不正侵入に対する検知・防御を行う（Firewall, IDS（侵入検知システム）等）．
ストレージ防御	ファイルの改ざん検知，ソフトウェア署名の検証，セキュアブートなどにより，流通・運用時の改ざんを検知する．
構成管理・セキュア開発	暗号などのセキュリティ機能の適切な利用・設定・セキュアコーディングなどの開発技術を適用する．

主な組織対策と概要は表 -8 のようなものが挙げられる．

セキュリティ技術対策の例

セキュリティ技術対策は，表 -1 に示す通り多様である．ここではクラウド・セキュリティにおいて重要な対策例をいくつか紹介する．

監視・脅威分析

近年，組織にネットワークへのマルウェア感染や内部不正のリスクに対して組織内外を問わずセキュリティを強化するゼロトラストセキュリティに注目されている．クラウドにおいては，リソースの共有リスク，事業者の協業リスクがあるため，ネットワークの監視・脅威分析はより重要である．クラウド利用者側としては，クラウド提供者側から提供される仮想マシンの監視・脅威分析用のツールを用いるか，IaaS, PaaS を利用するシステムにおいては，セキュリティイベントの記録管理・分析システム（SIEM）等や不正侵入検知システムなどのツールをホスト上で稼働させることで対応することができる．たとえば，AWS では，クラウドのインフラストラクチャ，システム，アプリケーション，さらにはビジネス指標について，カスタムダッシュボードを構築し，アラームを設定し，アプリケーションのパフォーマンスや信頼性に影響する問題を警告するための異常検知機能として Amazon CloudWatch anomaly detec-

■表 -8　主な組織的対策

組織対策	対策概要
リスクアセスメント	組織におけるリスクの洗出し・評価に基づきセキュリティ対策プロセスを確立する．
ポリシー策定	リスクアセスメントに基づき，組織全体として一貫性を持った方針を規定する．
体制構築	経営層が意思決定を行えるよう，CISO☆10 のリーダシップのもと，開発・運用に必要な予算と体制を構築する．

☆10 Chief Information Security Officer（情報セキュリティ最高責任者）

tion が提供されている．この CloudWatch のメトリクス（監視指標）の異常検出を有効にすると，過去のデータに機械学習アルゴリズムが適用されて，メトリクスの正常時の想定値としてのモデルが作成され，正常な状態から外れる状態や不正な挙動を検知することが可能になる

脆弱性管理

IaaS, PaaS, SaaS およびクラウド事業者が開発するシステム全体に渡り役割分担を明確にして脆弱性管理を行わなければならない．クラウド提供事業者は，クラウドサービスに影響し得る技術的脆弱性を管理し，クラウド利用者が必要とする脆弱性情報を利用者に提供しなければならない．脆弱性の情報源としては，脆弱性対策情報ポータルサイト（Japan Vulnerability Notes；JVN）や NIST NVD（National Vulnerability Database）などがある．また，業界ごとに設置されるセキュリティ情報共有組織 ISAC の活用も有効である．脆弱性を予防管理する技術としては，OWASP Top 10 のような脅威事例に基づく開発ガイドラインや脆弱性検証ツールの利用や，サプライチェーンのおけるソフトウェア部品の情報を管理する SBOM（Software Bill of Material）などの活用が有効である．

近年，サプライチェーンやソフトウェアアップデート機能を介して，不正ソフトウェア，ハードウェアを組込まれる脅威が高まっていることから，脆弱性における不正機能の悪意の意図性を評価する手法[☆11] が重要になると考えられる．

今後の課題と取り組み策

クラウド・セキュリティは，多様なステークホルダとの協業におけるリスクに対するセキュリティの確保が重要である．それらの管理策は十分に成熟しておらず，今後以下のような取り組みが重要となる．

- **マルチステークホルダ・セキュリティガバナンス（サプライチェーン・セキュリティ）**
  クラウド基盤利用者，クラウド基盤提供者，クラウドパートナなどさまざまなステークホルダとの協業において顧客に対する責任主体，ステークホルダ間の責任境界の明確化，役割分担を規定するガイドライン，取引契約書テンプレートを整備する．
- **セキュリティ・アシュアランスの確保**
  セキュリティ対策や技術検証などに関する協業者間や顧客・消費者に対する説明責任を確保する．そのためには経済産業省のサイバーフィジカルセキュリティフレームワークなどのベースを利用し，プロセスや検証結果などのエビデンス（根拠情報）に基づく客観的，体系的な説明を果たすためのガイドライン，モデル事例（アシュアランス・ケース）を整備する．**ここで重要なことは，然るべきセキュリティ対策を実施するだけではなく，利用者，取引相手などに対して然るべき対策を実施していることの説明責任を果たすことで信頼を獲得することである．セキュリティ対策とその説明責任を果たすことは同一ではない．**
- **脅威情報の蓄積・共有と管理策の向上**
  コンテナなど仮想化技術やリソース共有に係る脅威は常に変化しているため，最新の脅威情報の蓄積・共有および脅威に対する管理策，技術対策のガイドラインを整備する．

（2022 年 1 月 5 日受付）

■石黒正揮（正会員） masa@mri.co.jp

博士（情報科学）．東京大学大学院理学系研究科情報科学専攻修士課程修了．2000 年 SRI International（スタンフォード研究所）客員研究員．現在，（株）三菱総合研究所サイバーセキュリティ戦略グループ．専門は，サイバーセキュリティ，ディジタル・エンジニアリング，AI/ 数理データ解析，リスク評価，日米欧アジアにおけるセキュリティ政策・技術戦略，セキュリティ経済学．

☆11 三菱総合研究所、不正機能評価スコアリングシステム（Vulnerability Maliciousness Scoring System）