VII　進化するテクノロジー

企業組織では今日、進化し続ける多様なテクノロジーが用いられている（例：クラウド、ゼロトラスト・アーキテクチャ(ZTA)、AIやML、およびIoT）。これらのテクノロジーは、組織のアーキテクチャ、インフラストラクチャ、およびオペレーション機能に影響を及ぼし得る。当セクションでは、こうした進化するテクノロジーに関する全般的な情報を提示し、かつ必要に応じて、当ブックレットの先立つセクションにて論じた特定のリスクや統制の原則についても全般的に述べる。

VII.A　クラウドコンピューティング

クラウドコンピューティング環境は、仮想化技術によって実現される。クラウドサービスプロバイダは、仮想化技術を用いて、共有の物理的・仮想的ハードウェア上の複数の顧客を分離している。米国国立標準技術研究所(National Institute of Standards and Technology : NIST)の定義では、クラウドコンピューティングとは「共用の構成可能なコンピューティングリソース（ネットワーク、サーバー、ストレージ、アプリケーション、サービス）の集積に、どこからでも、簡便に、必要に応じて、ネットワーク経由でアクセスすることを可能とするモデルであり、最小限の利用手続きまたはサービスプロバイダとのやりとりで速やかに割当てられ提供されるもの」である[86]。クラウドシステムのもたらす恩恵は多様である。例として、リソースのスケーラビリティや、システムやソフトウェアに対する統制を一貫して実装可能であることが挙げられる。

当ブックレットにおける当セクションの目的上、「クラウドサービスプロバイダ」という語は、クラウドコンピューティングサービスを提供するプロバイダを指して用いられている。また「組織(“entity”)」という語は、クラウドコンピューティングサービスを受ける顧客を指して用いられている。

NISTの定義によれば、「クラウドコンピューティングは、5つの基本的な特徴と3つのサービスモデル、および4つの実装モデルによって構成される」[87]。

VII.A.1　基本的な特徴

NISTの定義によれば、クラウドの実装においては、以下に挙げる５つの「基本的な特徴」すべてが活用されている[88]。ただし、以下の５つの特徴すべてを伴わない環境でも、組織により「クラウドコンピューティング」とみなされているケースもあり得る。NISTは、クラウドコンピューティングの基本的な特徴として、以下の５項目を

[86] NIST SP 800-145、「NISTによるクラウドコンピューティングの定義：米国国立標準技術研究所による推奨」 を参照。
[87] 既出。
[88] 既出。

挙げている。

- **オンデマンド・セルフサービス：**ユーザは、各サービスプロバイダと直接やりとりすることなく、必要に応じて、自動的に、サーバーの稼働時間やネットワークストレージなどのコンピューティング能力を一方的に設定可能である。
- **幅広いネットワークアクセス：**コンピューティング能力は、ネットワークを通じて利用可能、かつ標準的な仕組みで接続可能であり、それによって様々なシンクライアント（thin client）およびシッククライアント（thick client）プラットフォーム（例：モバイルフォン、タブレット、ラップトップコンピュータ、ワークステーション）から利用可能である。
- **リソースの共用：**クラウドサービスプロバイダのコンピューティングリソースは集積され、複数のユーザにマルチテナントモデルを利用して提供される。様々な物理的・仮想的リソースが、ユーザの需要に応じて動的に割り当て・再割り当てされる。ユーザは一般的に、提供されるリソースの正確な所在地を知ることやこれを統制することはできないが、より抽象的なレベルで所在地を特定可能な場合もある（例：国、州、データセンタ）。リソースの例としては、ストレージ、処理能力、メモリ、ネットワーク帯域が挙げられる。
- **迅速な拡張性：**コンピューティング能力は、伸縮自在に割当ておよび提供が可能であり、場合によっては自動的に、需要に応じて即座に拡張や縮小が可能である。ユーザ側からは多くの場合、割当て可能なコンピューティング能力は無尽蔵であり、いつでもどのような量でも調達可能であるように感じられる。
- **計測可能なサービス：**クラウドシステムは、計測能力を利用し（例：ストレージ、処理能力、帯域、実利用中のユーザアカウント数）、サービスの種類に応じてリソースの利用状況を自動的に制御し最適化する。リソースの利用状況は監視され、制御され、かつ報告される。それにより、サービスの利用状況がユーザおよびサービスプロバイダの双方に対して明示される。

VII.A.2 クラウドサービスモデル

クラウドコンピューティングの実装においては、一般的に3つの主要なクラウドサービスモデル[89]が用いられている[90]。各アプリケーションやサービスに最適なアーキテクチャは、組織のニーズに応じて決定される。例として、データ分類、データレジデンシー、サービスやアプリケーションの可用性、ならびに外部サービスおよびデータストアとのインターフェースが挙げられる。

[89] NIST SP 500-316、「クラウドユーザビリティのフレームワーク」を参照。

[90] この他にも様々なクラウドサービスモデルがある（例：サービスとして提供される災害復旧、サービスとして提供されるバックアップ、サービスとして提供されるデスクトップ）。当ブックレットではその目的上、他の多くのサービスのベースラインとして用いられている主要なクラウドサービスモデルに焦点を当てている。

NISTでは、上記の３つのサービス[91]を以下のように示している。

- **サービスの形で提供されるソフトウェア(Software as a service (SaaS))：**SaaSでは、ユーザである組織に対して、クラウドのインフラストラクチャ上で稼働しているアプリケーションが提供される。組織は、アプリケーションそのもの、およびアプリケーションが稼働している環境を制御または管理することはできない。こうしたアプリケーションや環境の例としては、ネットワーク、サーバー、OS、ストレージ、および個々のアプリケーションの機能が挙げられる。当モデルでは一般的に、エンドユーザや組織がクラウドサービスのユーザインターフェースに対して行えるカスタマイズは制限されている。ただし、ユーザに固有のアプリケーションの構成の設定は例外である。
- **サービスの形で提供されるプラットフォーム(Platform as a service (PaaS))：**PaaSでは、ユーザである組織に対して、クラウドサービスプロバイダによってサポートされているプログラミング言語、ライブラリ、サービス、およびツールを用いて、ユーザ組織が開発または取得したアプリケーションを実装する機能が提供される。ユーザ組織は、クラウドのインフラストラクチャ（例：ネットワーク、サーバー、OS、ストレージ）を管理または制御することはできない。一方で、ユーザ組織は、各自が実装したアプリケーション、および場合によりそのアプリケーションをホストする環境の設定を管理することが可能である。
- **サービスの形で提供されるインフラストラクチャ(Infrastructure as a service (IaaS))：**IaaSでは、ユーザである組織に対して、演算機能、ストレージ、ネットワークその他の基礎的コンピューティングリソースを配置する機能が提供され、ユーザ組織はOSやアプリケーションを含む任意のソフトウェアを実装し、実行することが可能である。ユーザ組織は、基盤にあるクラウドインフラストラクチャを管理または制御することはできない。一方で、OS、ストレージ、実装されたアプリケーションを制御することは可能である。またユーザ組織は、各自のクラウドサービスおよびユーザインターフェースをほぼ自在にカスタマイズすることが可能である。

経営層は、クラウドの様々な活用法を選択可能である。ストレージやクラウドへのデータバックアップなど、特定のアプリケーションや処理機能をアウトソーシングすること（SaaSの一部）も可能であるし、自らアプリケーションを開発するという選択肢もあり得る。ただし後者では、OSの提供および維持をクラウドサービスプロバイダに委ねることになる（PaaSの一部）。また、物理的ハードウェアのみをクラウドサービスプロバイダにアウトソーシングし、OSやアプリケーションの維持は自ら行うことを選択することも可能である（IaaSの一部）。

[91] NIST SP 500-316、「クラウドユーザビリティのフレームワーク」を参照。

VII.A.3 クラウド実装モデル

クラウドサービスモデルでは、様々な実装方法が選択可能である。NISTは、以下のような実装モデルを示している[92]。

- **プライベートクラウド：**プライベートクラウドのインフラストラクチャは、複数のビジネスユニットからなる単一の組織の専用使用のために提供される。その所有、管理、および運用は、当該組織、第三者、もしくはそれらの組み合わせにより行われる。またその存在場所はその組織の施設内または外部となる。
- **コミュニティクラウド：**コミュニティクラウドのインフラストラクチャは、共通の関心事（例：任務、セキュリティ要件、ポリシー、法令遵守に関わる考慮事項）を有する、複数の組織からなる特定のコミュニティ（例：政府機関、金融サービス、銀行）の専用使用のために提供される。その所有、管理、および運用は、コミュニティ内の１つまたは複数の組織、第三者、もしくはそれらの組み合わせにより行われる。またその存在場所はそれらの組織の施設内または外部となる。
- **パブリッククラウド：**パブリッククラウドのインフラストラクチャは、一般向けに広く自由な利用を目的として提供される。その所有、管理、および運用は、企業組織、学術機関、政府機関、もしくはそれらの組み合わせにより行われる。またその存在場所はそのクラウドサービスプロバイダの施設内となる。
- **ハイブリッドクラウド：**ハイブリッドクラウドのインフラストラクチャは、2つ以上の異なるクラウドインフラストラクチャ（例：プライベート、コミュニティ、またはパブリック）の組み合わせからなる。各クラウドは独立した存在であるが、標準化された、あるいは固有のテクノロジーで結合され、データおよびアプリケーションの移動を可能にしている（例：クラウド間のロードバランスのためのクラウドバースト）。

ユーザである組織は、様々なオペレーションにおいて、またはクラウド上でのオペレーションの継続性やレジリエンスを増強する目的で、複数のクラウドサービスプロバイダを用いることが可能である。複数のクラウドサービスプロバイダを用いることにより、単一のプロバイダへの依存度を低減させることが可能である。また、より多くの容量が求められる状況下や、事業継続上の目的のために、クラウドバースト[93]機能を活用することも可能である。さらに、クラウドブローカーを用いて、経営層とクラウドサービスプロバイダとの間における、情報に基づいた仲介者の役割を担わせることも可能である。またクラウドブローカーを用いて、ユーザ組織の経営層や従業員の能力を補完することも可能である。

---

92 NIST SP 800-145、「NISTによるクラウドコンピューティングの定義：米国国立標準技術研究所による推奨」を参照。

93 クラウドバーストの目的は、クラウドコンピュータやストレージリソースを、その時点でのサービス需要に応じて動的に割当て・割当て解除することによって、ユーザ組織のデータセンタ内での処理に求められるサービスレベルを維持することである。

VII.A.4 責任の共有

クラウドコンピューティング環境では、ユーザ組織は情報・技術資産や運用に対する様々な統制の管理を、クラウドサービスプロバイダにアウトソーシングする可能性がある。その際には、組織とクラウドサービスプロバイダとの間に締結された契約を慎重にレビューし、共有の責任の分割方法や関連リスクについて理解しておくことが、適切な統制を行う上で重要である。契約には、組織およびクラウドサービスプロバイダの双方に対するサービスレベルの期待や管理上の責任が定められている。組織の内部基準と合致するレベルのセキュリティを維持するためには、クラウドサービスプロバイダが契約に基づいて提供する統制に加えて、さらなる統制が必要となる可能性がある。

経営層は、いずれのサービスモデルや実装モデルを導入するかに応じて、クラウドコンピューティングに関連する共有の責任について理解する必要がある。NISTによれば、「一組織がすべてのコンピューティングリソース[94]やシステムのライフサイクル全体を統制する従来のITシステムと異なり、クラウドサービスプロバイダおよびクラウドユーザは、互いに連携してクラウドベースのシステムを設計し、構築し、実装し、運用する。統制の分割は、両者がクラウドベースシステムを適切に保護する責任を共有することを意味する。」クラウドサービスプロバイダによって、クラウドサービスプロバイダ自身の運用のためにいかなる統制が実行され、一方で組織のコンテンツやアプリケーションのセキュリティを保証するためにいかなるセキュリティ管理が実行され運用されるかを理解しておくことが重要となる。

サービスモデルによって、通常、統制の実行・管理に関して組織とクラウドサービスプロバイダとの間で共有される責任は異なる。サービスモデルや契約内容に応じて、組織とクラウドサービスプロバイダのいずれか、または双方が責任を負うべき統制について以下に示す。

- 基盤となるクラウドインフラストラクチャシステム（例：ネットワーク、サーバー、ストレージ）やソフトウェアの管理。
- ハイパーバイザーに対する制御の管理・実行。
- クラウドプラットフォームリソースの提供および設計。
- ユーザ固有のアプリケーションの構成の設定実行、ユーザアクセスや認証の管理。
- 組織のデータの管理（例：資産の分類や暗号化の実行）。
- クラウドサービスプロバイダのプラットフォーム上に存在するソフトウェアの開発および実装。

---

[94] NIST SP 500-292、「NIST クラウドコンピューティング・リファレンスアーキテクチャ：米国国立標準技術研究所による推奨には、次のように記載されている。「クラウドコンピューティングにおいては、コンピューティングリソースの蓄積とは、組織がクラウドコンピューティングサービスプロバイダから購入するサービスの一群を指す。」

表 5. クラウドコンピューティング環境における共有の責任の例

	オンプレミスの責任	IaaSの責任	PaaSの責任	SaaS(および従来のアウトソーシング)の責任
リスク管理/管理統制	リスク管理戦略	リスク管理戦略	リスク管理戦略	リスク管理戦略
	方針(ポリシー)	方針(ポリシー)	方針(ポリシー)	方針(ポリシー)
	組織	組織	組織	組織
	アプリケーション管理	アプリケーション管理	アプリケーション管理	アプリケーション管理
	IAM/アクセス制御	IAM/アクセス制御	IAM/アクセス制御	IAM/アクセス制御
技術的統制	アプリケーション	アプリケーション	アプリケーション	アプリケーション
	データ	データ	データ	データ
	ランタイム	ランタイム	ランタイム	ランタイム
	ミドルウェア	ミドルウェア	ミドルウェア	ミドルウェア
	OS	OS	OS	OS
	仮想化	仮想化	仮想化	仮想化
	サーバー	サーバー	サーバー	サーバー
	ストレージ	ストレージ	ストレージ	ストレージ
	ネットワーキング	ネットワーキング	ネットワーキング	ネットワーキング
物理的統制	設備	設備	設備	設備

注：クラウドセキュリティアライアンス(the Cloud Security Alliance)の作成した表をもとに、FFIECメンバーは「リスク管理および管理統制(risk management and administrative controls)」の新たな項目を追加した表を作成した。この表は、組織とクラウドサービスプロバイダとの間で、契約に基づき、どのように責任が分割され得るかを示した一例である。濃紺のセルは組織の責任を表し、白いセルはクラウドサービスプロバイダの責任を表す。青色のセルは、組織とクラウドサービスプロバイダのいずれかまたは双方に割り当てられる可能性のある責任の例である。

- 物理的なデータセンタの管理。環境の管理統制（例：冷暖房、火災や洪水からの保護）や、電力、物理的セキュリティ、データ通信接続を含む。
- データアクセスや、ユーザの本人証明の窃取、規定遵守、データ漏洩に関する管理統制の実行。

組織のクラウドコンピューティング環境や用いているサービスモデルに関わらず、クラウドサービスの安全性および健全性、ならびに顧客および組織の機密情報保護に関する全般的な責任は、その組織自身が負う[95]。第三者サービスプロバイダに対する監督に関す

[95] 情報セキュリティ基準(the Information Security Standards)を参照。連邦規則集第12巻第30条付録B(12 CFR 30, appendix B) (OCC)、連邦規則集第12巻第208条付録D-2 (12 CFR 208, appendix D-2)および連邦規則集第12巻第225条付録F(12 CFR 225, appendix F) (FRB)、連邦規則集第12巻第364条付録B(12 CFR 364, appendix B) (FDIC)、連邦規則集第12巻第748条付録A(12 CFR 748, appendix A) (NCUA)。

る詳細については、「ITハンドブック」の「テクノロジーサービスのアウトソーシング」および「情報セキュリティ」の各ブックレットを参照。

VII.A.5　クラウドコンピューティングにおけるリスクの検討

クラウドコンピューティングは、クラウドコンピューティング環境が組織内部で管理されているか、もしくは第三者サービスプロバイダに管理されているかに関わらず、他のテクノロジー環境と同様の脅威や脆弱性、リスクに晒されている。クラウドコンピューティングには、従来のネットワークアーキテクチャで用いられていたものとは異なるセキュリティ管理の設定やプロセスが含まれる。そのため、単に既存のネットワークテクノロジーをクラウドに移すだけでは適切ではない。組織の統制(controls)、方針(policies)、および手続き(procedures)は、クラウドベース環境に有効に移されない可能性がある。クラウド環境におけるセキュリティ管理の実装を補助すべく、特別に設計されたツールがある（例：クラウドアクセスセキュリティブローカー）。

また、テナンシーに関するリスクも考慮する必要がある。アプリケーションやサービスは、シングルテナントまたはマルチテナントの環境に存在し得る。統制に関する要件はテナントによって異なる可能性があり、より高レベルのセキュリティを必要とするテナントもある。仮にテナントの１つで誤用や濫用が行われれば、他のテナントのセキュリティ体制も潜在的に弱体化する可能性がある。また不注意により、もしくは故意にセキュリティ管理を怠れば、同一環境における他のテナントにも悪影響が生じ得る。例として、クラウドサービスプロバイダやテナント１つがDOS攻撃を受ければ、他のテナントにも影響が生じ得る。

第三者保証レビュー（例：SOCレビュー、ペネトレーションテスト、脆弱性評価）を行うことにより、クラウドサービスプロバイダの統制環境、および同プロバイダが統制に関する組織の期待（例：関連法令へのコンプライアンス）を満たすことが可能であるか否かを判断することが可能である。詳細については、FFIECの共同声明[96]を参照のこと。

VII.A.5(a)　アクセス制御に関する考慮事項

「アクセス制御では、クラウドシステム内にある機密性の高いデータや重要なコンピューティングオブジェクトを保護するために、アクセス制御に関する方針の定めるところに基づき、主体(subjects)(例：ユーザ、プロセス)がいかにして対象(objects)にアクセス可能であるかを定める。」[97]クラウドコンピューティングは幅広い選択肢を提供するため、セキュリティに関する考慮事項は、様々なサービスモデルやデリバリーモデル、共有の責任に応じて、複雑なものとなり得る。概して、IaaSに関するアクセス

[96] FFIEC、クラウドコンピューティング環境におけるセキュリティ。

[97] NIST SP 800-210、クラウドシステムのアクセス制御に関する全般的指針を参照。

制御の考慮事項は、PaaSやSaaSにも適用される。またPaaSに関するアクセス制御の考慮事項は、SaaSにも適用される。ただし、そこにはバリエーションも存在する。

アクセス制御システムの設計における問題は、前述したクラウドコンピューティングの基本的な性質、およびデータ共有のリスクと関連している。こうした問題やリスクに関する考慮事項には、クラウド環境における以下の要素に関する考慮事項が含まれる。

- ネットワーク
- ハイパーバイザー
- VM
- API
- マルチテナンシー
- 属性および役割管理
- データの複製および破壊(destruction)

こうした要素について考慮する際には、クラウド環境におけるアクセス制御に関して、以下に挙げる項目についての考慮も必要となる。

- クラウド仮想化によって、アクセス制御やセキュリティ管理に関する懸念は増す。クラウドにおいて作成・変更されたVMの量によって、リスクが複合的になる可能性があるからである。
- アクセス制御では、ネットワークやネットワーク境界、ハイパーバイザー、VM、APIをリスト化し、様々なユーザに対して適切なアクセスレベルを定め、実行する。
- OSメモリーキャッシュ内のデータなど、アプリケーションやデータを漏洩の可能性から保護するために、PaaSプロバイダから提供されるセキュリティおよびプライバシーに関連するアクセス制御。
- SaaSでは、プロバイダ側に所在する、またはプロバイダからアクセス可能であるSaaSシステムや顧客データに対して、プロバイダは不必要または不適切にアクセスすべきでない。
- アクセス制御の設計においては、組織のデータが他の顧客のアプリケーションから適切に分離されたマルチテナンシーの状態が確保されている必要がある。

クラウド環境におけるアクセス制御およびセキュリティに関する詳細については、NISTを参照[98]。また、詳細については「ITハンドブック」の「情報セキュリティ」および「テクノロジーサービスのアウトソーシング」の各ブックレットをも参照。

[98] 既出。

VII.B ゼロトラスト・アーキテクチャ

NISTによれば、ZTAとは「ゼロトラストの原則に基づいた組織向けのサイバーセキュリティアーキテクチャであり、データ侵害を防止し、内部ネットワーク上の水平移動（ラテラルムーブメントlateral movement）を制限するように設計されている。」[99]組織の複雑性が増すにつれて、組織は複数の内部ネットワークや、独自のローカルインフラストラクチャを持つリモートオフィス、リモートやモバイルの環境の端末、およびクラウドサービスを運用するようになる[100]。ペリメータベースのネットワークセキュリティを用いるレガシー手法は、複雑さを増したIT環境にはもはや適さない。例えば、組織のペリメータベースの内部ネットワークセキュリティが完全に有効でなければ、ひとたび境界(perimeter)を突破されると、ネットワーク内部での水平移動を防ぐことが不可能となりかねない。こうした懸念から、ゼロトラストと呼ばれるサイバーセキュリティモデルが生み出された[101]。

ZTAでは、内部ネットワークを含むあらゆるネットワークを信頼できないものとみなしている。ZTAにおいては、システムやユーザは、物理的な場所またはネットワーク上の位置（例：LANやインターネット）に基づく暗黙の信頼を得られない。データリソースへのアクセスが認可されるのは、リソースが必要とされ、かつ接続が確立する前に認証（ユーザとデバイスの両方に対して）が行われた場合のみである。ZTAは、認証や権限付与によるネットワークセグメントの保護よりも、リソースの保護に重点を置いている。暗黙のトラストゾーンに頼ることは最小限にとどめている。さらに、ZTAは、組織が所有するネットワークの境界外における認証手法によって生じる遅延を低減させることをも重視している[102]。

ゼロトラストの設計により、組織は多様なビジネスケースが存在する複雑な状態を安全に保持することが可能となる。その過程では、すべてのアクセス決定およびシステム間のやり取りに対して仮想的方法により情報が与えられる[103]。経営層は、ゼロトラストの原則をアーキテクチャに関連する意思決定に適用するか否か検討することが可能である。ZTAの原則は、以下のとおりである[104]。

- すべてのデータソースおよびコンピューティングサービスをリソースとみなす。
- ネットワーク上の位置に関わらず、すべての通信を保護する。
- 個々の組織リソースへのアクセスは、ネットワーク上の位置、ユーザ、デバイスに関わらず、セッション単位かつ安全な方法で認可する。

---

99 NIST SP 800-207、「ゼロトラスト・アーキテクチャ」。
100 既出。
101 既出。
102 既出。
103 既出。
104 これらの原則は、NIST SP 800-207、「ゼロトラスト・アーキテクチャ」より引用。

- リソースへのアクセスに対する認証および認可は、ユーザおよびデバイスの分析ならびに行動属性（例：ネットワーク上の位置、デバイスの特性、アクセスの日時）により、ベースラインとなるパターンからの逸脱の程度と比較した上で決定される。
- アクセス制御を厳格に行う（例：最小特権や、組織のデジタルリソース周辺の詳細なトラストゾーンを使用）。こうした統制には、データレベルの保護や、頑健なアイデンティティアーキテクチャ、戦略的なマイクロセグメンテーションが含まれる。
- 組織が所有するデバイス、および関連するデバイスの監視を行い、可能な限り最も安全な状態が保持されるよう保証する。また、組織はネットワークトラフィックの検査、監視、および記録を継続的に行うとともに、得られた情報を用いてセキュリティ体制を向上させる。
- アクセス要求およびネットワークトラフィック行動の評価を、接続が開いている間リアルタイムで行い、組織のリソースへのアクセスを継続的に再評価する。

VII.C マイクロサービス

マイクロサービスとは複数のコンテナ(containers)の集まりであり、協同して1つのアプリケーションを構成する。各マイクロサービスは本質的に、通信や認証などの各アプリケーションを構築するために用いられる、独立した建築用ブロックのようなものである。各マイクロサービスはごく小さなアプリケーションであり、互いに緩やかにつながりつつ[105]単一の機能を果たす（例：データベースアクセスやメッセージング）。それらが統合され、集合体として1つのアプリケーションを構成する。様々な組み合わせのやり取り（例：顧客とマイクロサービス、マイクロサービス同士、マイクロサービスとエグレスサービス）からなる通信が行われている間、各々は個別のアイデンティティを有し、相互認証を行う。

各マイクロサービスは通常、1つ(稀に複数)の別個のビジネスプロセスや機能を実行する（例：顧客の詳細情報の格納や商品カタログの表示）。NIST 800-204A[106]では、マイクロサービスについて、大きく分けて以下の2種類の機能が示されている。

- ビジネスロジック。ビジネス関連の機能、コンピューテーション、サービス構

[105] NIST SP 800-204、「マイクロサービスベースのアプリケーションシステムのためのセキュリティ戦略」によれば、「規模の大きなアプリケーションにおいては、アプリケーションを、互いに緩やかに結びついたコンポーネントに分割することで、各コンポーネントに割り当てられた開発チームが独立して開発を進めることが可能になる。それによって、各開発チームは、各々が開発中のコンポーネントに適切である独自の開発プラットフォームやツール、言語、ミドルウェア、ハードウェアを選択することにより、開発を最適化することが可能となる。」

[106] NIST SP 800-204A、「サービスメッシュ・アーキテクチャを用いた安全なマイクロサービスベースのアプリケーションの構築」を参照。

成やインテグレーションロジックを実行する。
- ネットワーク機能。サービス間の通信メカニズムを管理し、基盤となるOSレベルのネットワークスタックの上に構成される。

マイクロサービスソフトウェアは、複雑なアプリケーションが小さな独立したサービスによって構成される形態のアーキテクチャを設計する際に用いられる。これらの小さな独立したサービスは、データや手続き上の要求を相互に交換する。マイクロサービスベースのアプリケーションのアーキテクチャは、固有のスケーラビリティや、実装の機敏性、ツールの可用性を提供するとともに、エラーのない構成や実装を促進する。また、マイクロサービスベースのアプリケーションは、純粋に企業組織のアプリケーションとして実装可能だが、一般的には、サービスベースのアーキテクチャや、APIに基づく通信、およびコンテナベースのインフラストラクチャを含むクラウドネイティブなアプリケーションとして認識されている[107]。

マイクロサービス・インフラストラクチャの実装は、複数のサービスが指定された場所（IPアドレスやポート番号）で動作するよう設定されている点で、レガシーの分散システムとは異なる。マイクロサービスベースのアプリケーションを用いる際には、組織のインフラストラクチャにおける主要な考慮事項[108]として、以下の項目が挙げられる。

- 多数のサービス、および各サービスに関連する多数のインスタンスがあり、かつ動的に位置が変化する。
- 各サービスに関連するインスタンスの数は、オートスケーリングなどの機能を用いる負荷変動に基づいて異なる。
- サービス要求を出している間、サービスを探して見つける機能。こうした機能を実装するための一般的なアプローチは、サービスレジストリを用いる方法である[109]。
- 各マイクロサービスはVMにて実装されるか、またはコンテナとして実装され、動的なIPアドレスを割当てられる。とくにIaaSやSaaSのクラウドサービスにホストされている場合はこれに該当する。
- 同一のサービスに複数のインスタンスがある場合、ロードバランスが必要である。これらのインスタンスにかかる負荷を均等に分配することにより、オーバーロードによるレスポンスの遅延やサービスがクラッシュする事態を避けるためである[110]。

---

[107] NIST SP 800-204、「マイクロサービスベースのアプリケーションシステムのためのセキュリティ戦略」を参照。

[108] NIST SP 800-204A、「サービスメッシュ・アーキテクチャを用いた安全なマイクロサービスベースのアプリケーションの構築」において、主要な考慮事項について論じられている。

[109] サービスレジストリは、マイクロサービスベースのアプリケーションのために新規に作成されたサービスインスタンスが自動的に記録され、オフラインになったサービスインスタンスは消去される仕組みのディレクトリからなる。

[110] NIST SP 800-204A、「サービスメッシュ・アーキテクチャを用いた安全なマイクロサービスベースのアプリケーションの構築」を参照。

- マイクロサービスでは、以下のような様々な機能を活用している[111]。
  - サーキットブレーカー[112]。
  - レート制限やスロットリング。
  - バージョン管理。
  - カナリアリリース[113]。

クラウド環境および規模の大きな企業組織環境におけるマイクロサービスベースのアプリケーション導入が増加するに伴い、包括的かつ継続的に相互連携するサポートサービスを提供するインフラストラクチャが明らかにされつつある[114]。そうしたインフラストラクチャの例が、サービスメッシュやAPIゲートウェイである。マイクロサービス関連のオペレーションにおいては、セキュリティに関してさらなる考慮が必要である[115]。以下にその例を挙げる。

- 多数のマイクロサービスを用いる場合、保護しなければならない相互接続や接続リンクが増加する。保護方法の例として、イングレス/エグレス・コントローラの使用が挙げられる。
- マイクロサービスは、短期的かつプロミスキャス（すなわち、多くの様々なアプリケーションやプラットフォームに用いられる）であるため、安全なサービス検出メカニズムが必要となる。すなわち、作成されたマイクロサービスが正確に記録され、新バージョンに置き換えられたマイクロサービスは削除されることを確認するメカニズムである。
- マイクロサービスが構築される際には、組織の安全および権限付与の方針をサポートする機能が含まれる必要がある。
- マイクロサービスベースのアプリケーションに対する複数のサポートサービス（例：認証、権限付与、セキュリティ監視）は、専用のインフラストラクチャを通じて相互に連携する必要がある。
- ネットワークペリメーターに関するコンセプト(concept)は存在しない。
- あらゆるマイクロサービスは、信頼できるものとして扱ってはならない。

マイクロサービスの性質を詳細に知っておくことで、経営層はセキュリティに関する方針や設定を速やかに定めることが可能であり、それによってあらゆるマイクロサービスを均一かつ持続的に実装することが可能となる。

---

111 既出。

112 サーキットブレーカーを使用すると、マイクロサービスのインスタンスからのレスポンスの失敗に対する閾値が設定され、レスポンスの失敗が閾値を超えた場合（例：サーキットブレーカーが落ちた場合）には、そのインスタンスに対する要求の転送が切断される。

113 カナリアリリースは、マイクロサービスの潜在的な問題に関する早期の警告システムとして役立つ。

114 NIST SP 800-204A、「サービスメッシュ・アーキテクチャを用いた安全なマイクロサービスベースのアプリケーションの構築」を参照。

115 既出。

VII.D 人工知能および機械学習

AIとは、論理的思考や学習、自己改善など、通常人間の知能に関連しているタスクや機能を遂行するシステムの理論および開発を指す。MLはAIのサブセットである。MLでは、AIシステムのコンポーネントを用いて一連の動作(actions)を設計するが、それらは経験を通じて自動的にアルゴリズム上で改善され、かつアルゴリズムを最適化することが可能である。それによって、人間の介入を最小限にとどめながらタスクを遂行することが可能となる。

AIのアルゴリズムでは、大量のデータセットを即座に分析し、複雑なパターンを見出すことが可能であり、それによって、問題解決や、予測や分類を行うことが可能である。AIを用いることにより、経営層は顧客向けの商品やサービスをパーソナライズすることが可能となり、またリアルタイムのデータを分析して将来の顧客行動の予測に役立てることも可能となる。また、AIは、人間がデータ分析を行う際には見落としかねないパターンを見出すことによって、意思決定を向上させることも可能である。循環プロセスおよび意思決定を自動化することによって、人間の介入を減らし、運用上の効率や生産性を向上させること（例：時間や人的コストの削減）が可能である。

組織では、AIをさまざまな活動に用いることが可能である。以下にその例を挙げる。

- 詐欺や違法行為の検知および防止（例：マネーロンダリング防止、アカウント侵害、内部不正）による損失低減。
- サイバーセキュリティ違反の特定、通知、および低減。
- 自動取引（例：アルゴリズム取引）の促進[116]。
- 融資組成プロセスの自動化および増加。顧客信用評価を含む。
- リスク管理およびビジネス上の意思決定。
- セキュリティ管理の強化（例：論理的・物理的アクセスの異常分析や顔認証）。
- 関連法令の遵守。

AIやMLの使用に関しては、多くのリスクがある。AIやMLは、利用可能なデータを大量に扱うが、万一そうしたデータが漏洩すれば、データの悪用や詐欺、財務上の損失、組織の評判への悪影響、消費者への悪影響をもたらすおそれがある。またアルゴリズム開発における作為または不作為によるヒューマンエラーの可能性もあり、それが誤った意思決定につながるおそれもある。さらに、テストや検証が行われなければ、仮に使用方法が適切であったとしても、アルゴリズムの開発や使用の際にバイアスが生じる可能性（意図的であれ非意図的であれ）がある。開発におけるテストや検証についての詳細は、「ITハンドブック」の「開発および取得」ブックレットを参照。

[116] アルゴリズム取引では、企業は一連の段階からなる特定のアルゴリズムを用いてプログラミングされたコンピュータを用いて、取引の機会を見出し、取引のオーダーを実行する。

またAIは、透明性や説明可能性に欠ける可能性がある。すなわち、処理アプローチを辿って監視することが難しく、インプットがいかにしてアウトプットに変換されたのかが不明確になりかねない。こうした説明可能性の欠如ゆえに、AIのアプローチに対する理解が妨げられ、AIによってもたらされた結果に対する信頼性にも影響が生じかねない。さらに、意図せざる結果（例：関連法令に対する違反、組織のリスク許容度を超える結果）がもたらされる可能性も否定できない。

上記に加えて、AIには自身で進化する能力という潜在的リスクもある。こうした能力により、人間の介入なしに、AIが自身の既存の変数や機能を修正する（または新しい変数や機能を導入する）能力が生じる可能性がある。こうした現象は、ダイナミック・アップデートとして知られ、AIに対する監視や独立したレビューを困難にするおそれがある。

VII.E IoT（モノのインターネット）

IoTは、物理的デバイスとの間で、インターネット経由で情報の送受信を行うことが可能なテクノロジーの集合を指す（例：セキュリティシステム、HVACシステム、インテリジェントパーソナルアシスタント、スマートテレビ、その他の電化製品）。こうした物理的デバイスは、従来はIT資産と見なされていなかった。こうしたデバイスは、内蔵されたコンピューティング能力やネットワーク接続、固有の識別子（例：IPアドレス）を用いて、ネットワークを通じたデータの送受信を行うことが可能である。その際、人間同士、または人間とコンピュータとのやり取りは必ずしも必要ではない。IoTは、クラウドコンピューティングやモバイルコンピューティング、ビッグデータ、その他の最新テクノロジーを活用して、機能を提供する。IoTを通じて収集されたデータは、向上した統計モデルやアルゴリズムを通じて、組織の経営層の意思決定に役立てることが可能である。IoTは、腕時計や電話に搭載されたモバイル支払システムから、インターネットに接続された医療機器や家庭用セキュリティデバイスまで、あらゆるセクターにおいて活用されている。

IoTでは、インターネットに接続されたコンピューティングデバイスを用いており、コードの実行が可能であることから、使用に伴うリスクは多い[117]。

- IoTデバイスは、従来のITデバイスとは異なる方法を用いて、物理的世界との間でやり取りを行う。IoTデバイスは、物理的システムに変更を加えることが可能である。しかし、それらの機器の機密性や完全性(integrity)、可用性に関わる操作上の必要条件は、従来のITデバイスにおける一般的なサイバーセキュリティやプライバシーの慣行とは相容れない可能性がある。例として、オンラインやモバイルで

[117] これらのリスクは、NIST IR 8228、「『モノのインターネット(IoT)』のサイバーセキュリティおよびプライバシーに関連するリスク管理に関する検討」から引用した。

のペイメントチャネルに関わるセキュリティ要件は、インテリジェントパーソナルアシスタントデバイスを用いた購買や支払いに関わるセキュリティ要件よりも、厳重であることが多い。

- IoTデバイスの多くは、従来のITデバイスと同様の方法ではアクセスや管理、監視ができない。例として、IoTデバイスのほとんどは、集中管理するための標準化されたメカニズムをサポートしていない。そのため管理者は、IoTデバイスのファームウェアやOS、アプリケーションを完全には管理できない可能性がある。利用できない機能として、ソフトウェアの取得、完全性の検証、インストール、設定、格納、復旧、実行、終了、削除、置換、アップデート、パッチが挙げられる。IoTデバイスの中には、デバイスの使用や管理のためのアプリケーションやヒューマンユーザインターフェースが備わっていないものもある。そうしたインターフェースが備わっている場合でも、従来のITデバイスが通常提供していた機能が提供されない可能性がある。なかには、製造者にしか、パッチのインストールなどのメンテナンスを行うことができないケースもある。
- IoTデバイスのソフトウェアは、停電やネットワーク接続の遮断などの異常事態が起こった場合、自動的に再設定される可能性がある。例として、IoTデバイスのセキュリティ設定が、すべてリセットされて初期設定に戻ってしまう可能性がある。
- IoTデバイスが提供可能である、または現在提供している機能がどのようなものであるかを組織が把握できない可能性がある。IoTデバイスは、製造者が提供したクラウドベースのサービスの処理機能やストレージにデータを送信する。データはクラウドサービスに送られ、同一の場所にある複数のIoTデバイスからのデータが合算される。こうしたクラウドサービスは、IoTデバイスのデータの一部またはすべてへのアクセスを提供可能であり、さらに、監視やメンテナンス、問題解決を目的とした、IoTデバイスへのアクセスやデバイスの管理をも提供可能である。
- デバイスの所有者に関する情報がほとんどまたは全く入手できない可能性がある。説明責任(accountability)が欠如していることにより、個人が自分自身に関する情報のソースを特定したり、そうした情報を修正・削除したりする権限が制限される。また、その他の問題（例：プライバシー）への対処も制限される。
- IoTデバイスによっては、デバイスを廃棄または他者に譲渡した後も、データが利用可能であるおそれがある。
- 組織で用いられるIoTデバイスでは、通常のITプロセスによるインベントリの作成・管理、登録(registered)、プロビジョニングが行えない可能性がある。そうしたデバイスの従来のイテレーションは、ネットワーク機能（例：組織のネットワークに接続してテレビ会議を行う機能を備えたスマートテレビ）を備えていなかった。IoTデバイスでは、従来のIT向けのサイバーセキュリティやプライバシー管理では理解・分析が不可能なプロトコルが用いられる場合が多い。したがって、標準的なネットワークスキャニングデバイスは、IoTデバイス（個人所有のIoTデバイスを含む）を認識できない可能性がある。

IoTデバイスの機能には、一般に知られていないものも多い。したがって、そうした機能や関連リスク、デバイスがアクセス可能なデータについて理解しておくことが重要で

ある。また、IoTデバイスは比較的容易にインストール可能であるため、インストールされたデバイスの数や、使用されている場所を把握しておくことが重要であり、また組織のITAMインベントリプロセスにおいて検討する必要がある。