クラウド事業者が提供するセキュリティ機能の活用

Utilization of Security Functions Provided by Cloud Service Provider

石　川　政　朝

要　約　パブリッククラウドを活用するシステムでは，セキュリティ対策の考え方がオンプレミスとは異なり「責任共有モデル」が一般的である．責任共有モデルとは，クラウド事業者（CSP）と，クラウド利用者のセキュリティに対する責任分担の考え方である．クラウド利用者の責任範囲におけるセキュリティ対策不足や対策不備が，多くのセキュリティ事故の原因になっている．クラウド利用者の責任範囲におけるセキュリティ対策には，CSP が提供するセキュリティ機能の活用，他ベンダーが提供している SaaS の活用と，クラウド向けの他ベンダー製品の活用がある．パブリッククラウドや他ベンダーの SaaS は日々進化しているため，クラウド利用者は，最新の情報を調査した上でセキュリティ対策を検討すべきである．

Abstract　In systems that use public clouds, the concept of security measures is different from on-premises, and a “responsibility sharing model” is common. The responsibility sharing model is the concept of sharing responsibility for security between cloud service provider (CSP) and cloud users. Many security incidents are caused by lack of security measures or inadequate measures within the responsibility of cloud users. Security measures in the responsibilities of cloud users include the use of security functions provided by CSP, the use of SaaS provided by other vendors, and the use of other vendor products for the cloud. Because public clouds and SaaS from other vendors are evolving daily, cloud users should consider security measures after investigating the latest information.

1. はじめに

「クラウドファースト」という言葉が浸透し，IaaS，PaaS および SaaS[*1] 等のクラウドサービスの利用が拡大している．社内システムなどを SaaS に置き換える企業や，システム開発やシステム更改において，IaaS や PaaS を活用する企業も増えている．

Microsoft Azure（以降，Azure）や Amazon Web Services（以降，AWS）に代表されるパブリッククラウドが提供する IaaS や PaaS は，CPU やメモリ，ディスクなどリソースの割り当てや変更を容易に行うことができ，利用した分だけの料金を支払う従量課金システムを採用している．コンピュータリソースを所有せず利用することができるので，クラウド利用者はインフラストラクチャのコストを最適化することができる．システム構築後のリソースの見直しも容易なため，従来のインフラ設計と比べ厳格なリソース見積もりが不要である．また，クラウド利用者の責任範囲におけるセキュリティ対策には，クラウド事業者（Cloud Service Provider：以降，CSP）が提供するセキュリティ機能の活用，他ベンダーが提供している SaaS の活用と，クラウド向けの他ベンダー製品の活用がある．

本稿では，このようなパブリッククラウドが提供する IaaS および PaaS を活用したシステムにおけるセキュリティ対策の考え方を，パブリッククラウド特有の脅威も踏まえて解説し，

CSP が提供するセキュリティ機能を中心に正しくセキュリティ対策を行うことの利点を述べる．2 章でパブリッククラウドのセキュリティの考え方，3 章でセキュリティ事故の事例，4 章でクラウド利用者のセキュリティ対策，5 章でシステムモデル別の具体的な対策について述べる．

2. パブリッククラウドにおけるセキュリティの考え方

Azure や AWS が提供するパブリッククラウドを活用するシステムでは，セキュリティ対策の考え方がオンプレミスとは異なる．本章ではパブリッククラウドのセキュリティの考え方を確認する．

2.1 責任共有モデル

パブリッククラウドにおけるセキュリティの考え方として「責任共有モデル」と言われているものが一般的である．責任共有モデルとは，クラウドサービスを提供しているクラウド事業者（CSP）と，クラウド利用者のセキュリティに対する責任分担の考え方であり，Microsoft や Amazon など多くの CSP が採用している．

CSP は，この責任共有モデルに従って，物理的なデータセンター，物理ネットワーク，仮想サーバを稼働させるハイパーバイザーなどに関する責任を負っている．クラウド利用者は，IaaS では仮想サーバで稼働する OS 以上のセキュリティ対策の責任を負う．責任分界点は，IaaS や PaaS など利用するサービスによって異なり，一般的に図 1 のように説明されている．

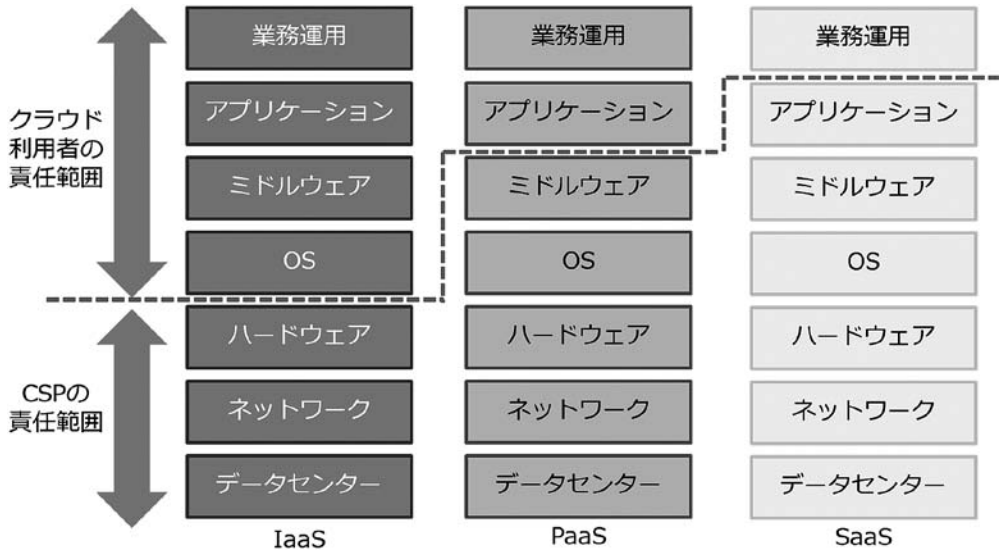

図 1　責任共有モデル イメージ

IaaS を利用したシステムより，PaaS や SaaS を活用したシステムの方が，クラウド利用者の責任範囲は少なくなる．但し，PaaS が提供しているセキュリティ機能（データバックアップ機能や認証/認可機能，データ暗号化機能，ファイアウォール機能，ログ管理機能など）を，クラウド利用者が正しく理解し，設定することが重要となる．

2.2　CSP のセキュリティ対策

前節の責任共有モデルにおける CSP の責任範囲では，CSP 側でセキュリティ対策，維持運用を行っている．CSP は，その実態や状況をクラウド利用者に示すため，認証制度を利用している．ISO/IEC27001[*2] や ISO/IEC27017[*3]，PCI DSS[*4] など多くの国際認証を取得し，その認証情報を公開している．Azure や AWS では，認証制度の無い NIST サイバーセキュリティフレームワーク[*5] に対しても独自に準拠性を確認し公開している．さらに，日本独自の金融機関向けのセキュリティガイドライン FISC 安全対策基準[*6] を始め，各国のガイドラインやフレームワークへの対応も行い，全世界へ情報公開，サービス提供を行っている．

さらに Azure と AWS は，CSP として実施しているセキュリティ対策や維持運用の概要をホワイトペーパーの形で外部へ公開することで，CSP の責任範囲における説明責任を果たしている．

2.3　クラウド利用者のセキュリティ対策

クラウド利用者の責任範囲では，クラウド利用者側でセキュリティ対策を検討し実施しなければならない．但し，パブリッククラウドは仮想化技術を活用し，複数のクラウド利用者を共通の物理環境上で稼働させているため，物理サーバやネットワーク機器，アプライアンスなどの物理機器をパブリッククラウド上に展開することはできない．そのためクラウド上の展開を想定した仮想アプライアンス型のセキュリティ製品[*7] などを活用する．パブリッククラウドでのセキュリティ対策方法は 4 章で述べる．

パブリッククラウドでは，各クラウドサービスを操作するための「管理コンソール」と呼ばれる機能が提供されている．クラウド利用者は，管理コンソールを利用して仮想サーバやデータベース，ファイアウォールなどを構築したり，それらの設定を変更することができる．それゆえ，管理コンソールに対するセキュリティは，パブリッククラウドを利用する際の考慮点として絶対に見落としてはならない．

3.　パブリッククラウドを活用したシステムでの事故事例

パブリッククラウドを活用したシステムは，インターネットを介したサイバー攻撃の標的になることが多い．セキュリティ事故の原因の多くは，クラウド利用者の責任範囲におけるセキュリティ対策不足や対策不備であり，正しくパブリッククラウドを活用していれば防止できていたものである．本章で実際に発生した事故事例を挙げ，5 章にてセキュリティ対策を考察する．

3.1　事故事例 1：管理コンソールへの不正アクセス

パブリッククラウドの管理コンソールのアカウント情報が漏えいし，クラウドリソースが悪用される事故が多く発生している．攻撃者は，管理コンソールへのパスワードクラック[*8] だけでなく，アクセスキーの不正入手も試みている．アクセスキーとは，管理コンソールの操作をプログラム等から行う際の認証情報であり，アクセスキーの漏えいは，管理コンソールの不正アクセスと同じ意味を持つ．GitHub[*9] にアクセスキーを記載したプログラムを不用意に登録したことで，アクセスキーが漏えいし，クラウドリソースを悪用された事故事例が多くみられる．

攻撃者は，不正入手したアクセスキーを使って確保したクラウドリソースを，仮想通貨のマイニングや，他のシステムへの攻撃などに利用する．CSP からの多額の請求連絡を受けるまで，リソースの悪用を認識できていないクラウド利用者も多い．

3. 2　事故事例 2：クラウド環境からの情報漏えい

CSP が提供する IaaS や PaaS の各機能を正しく利用できていないことで事故に繋がるケースが多い．IaaS や PaaS には各種アクセス制御機能が提供されている．しかし，このアクセス制御機能を認知していなかったり，誤った設定をすることで，外部からの不正アクセスを許し情報漏えいに繋がる．攻撃者は，このようなアクセス制御が行われていない箇所を常に検索し続けている．

CSP が提供しているストレージサービスに付属されているアクセス制御機能の未設定や設定不備により不正アクセスされ，機密情報が漏えいした事例が多く報告されている．この被害は長期間，認識できないことで大量の情報漏えいに繋がり，発覚した際には被害額が高額になっているケースも見受けられる．

3. 3　事故事例 3：仮想サーバへの不正アクセス

最後の事故事例として，パブリッククラウド上の仮想サーバへの不正アクセスが挙げられる．パブリッククラウドによっては，仮想サーバをデプロイした際，ファイアウォールのデフォルト設定がインターネットからのリモート接続（RDP や SSH 接続）を許可している場合がある．安易な仮想サーバへのログインパスワードが設定されていると，簡単に不正アクセスを許す．

開発や検証目的で仮想サーバをデプロイした際に簡易パスワードを設定し，不正アクセスされる事故が後を絶たない．不正アクセスされた仮想サーバは，他システムへの攻撃に利用されることが多く，意図せず攻撃に加担していることになる．

4.　パブリッククラウドでのセキュリティ対策方法

パブリッククラウドを活用する場合，責任共有モデルで示されたクラウド利用者の責任範囲におけるセキュリティ対策は，クラウド利用者側で検討し，実装，運用しなければならない．パブリッククラウドでのセキュリティ対策は，オンプレミスで実施する方法とは異なる部分がある．本章では，パブリッククラウドを活用したシステムにおけるセキュリティ対策の方法について解説する．

4. 1　CSP が提供するセキュリティ機能を活用する

パブリッククラウドにおけるセキュリティ対策において，まず優先的に活用すべきは CSP が提供するセキュリティ機能である．CSP はセキュリティ機能を IaaS や PaaS に付属させたり，単体としてサービス提供もしている．付属する機能の中には無料で利用できるものも多い．他のセキュリティ機能（次節以降で述べる他ベンダーが提供する SaaS や仮想アプライアンス製品など）を多く活用した場合，セキュリティ運用がそれぞれで独立しているため運用負荷が高くなる場合がある．そのため，CSP が提供するセキュリティ機能を優先して活用し，運用のサイロ化を防ぐことが推奨される．

無料で利用できるセキュリティ機能としては，ネットワーク分割機能やファイアウォール機能などが代表的なものとして挙げられる．PaaS に付属する機能では，アクセス制御機能や透過暗号機能，ログ取得機能などが無料で提供されており，どのシステムにおいても利用できるセキュリティ機能であるため，これらは積極的に活用すべきである．

有料で提供されているセキュリティ機能としては，WAF（Web Application Firewall）や DDoS（Distributed Denial of Service）対策[*10] など，システム毎に必要性が異なる機能や，高度なセキュリティ対策などがある．これらも PaaS のオプションや付属機能として提供されている．CSP が提供するセキュリティ機能の一部を表 1 に示す．

表 1　CSP が提供する代表的なセキュリティ機能

	ネットワーク分離	アクセス制御	透過暗号機能	WAF	DDoS対策
機能概要	パブリッククラウド上に仮想的なプライベートネットワークを構築することが出来る機能	IaaSやPaaSへの接続元をIPアドレスで限定することによって，不特定な不正アクセスを防ぐことが出来る機能	ストレージへ保管するデータを暗号化することで，ディスクからの情報漏えいを防ぐことが出来る機能	Webアプリケーションにおける脆弱性を狙った攻撃を防ぐことが出来る機能	DDoS攻撃を緩和することが出来る機能．但し，CSPが提供するDDoS対策は低レイヤ（レイヤ4以下）であるものが多いため，高レイヤに対する対策は検討が必要
有料/無料	無料	無料 ※有料の場合あり	無料 ※有料の場合あり	有料	有料 ※一部無料で提供されている機能あり
利用が推奨されるシステム	全てのシステム	全てのシステム	全てのシステム	インターネットに公開されるWebシステム	インターネットに公開されるシステム

Azure や AWS では，IaaS や PaaS を利用したシステム向けにセキュリティに関するベストプラクティスをホワイトペーパー[*11] で公開している．また，CIS[*12]（Center for Internet Security）は，CIS Benchmark と呼ばれる Azure や AWS などのパブリッククラウド向けのセキュリティ設定に関する確認リストを公開している．パブリッククラウドを活用するシステム設計では，セキュリティ要件からの実装検討だけではなく，活用する PaaS が提供している機能や，ホワイトペーパー，CIS Benchmark で推奨されている事項を参考にして検討し，設計および設定することが重要である．

CSP のベストプラクティスや CIS Benchmark の確認リスト内容が設定されているか否かを確認するためのサービスを提供しているベンダーがある．このようなサービスを用いて，パブリッククラウドの設定を確認することは非常に有用である．ファイアウォールなどの設定は，リリース運用や保守における作業で一時的に変更されることもあり，サービスによる設定値確認を定期的に実行し，見直し運用を行うことで，保守作業の戻し漏れや設定誤りなどを検出し，セキュアな環境が維持できる．

4. 2　他ベンダーが提供している SaaS を活用する

CSP 以外の他ベンダーがセキュリティ機能を SaaS としてサービス提供しているものがあり，これらを活用することで運用負荷を減らすことができる．4.1 節で説明した CSP の提供機能を利用した場合，シグネチャ更新などの運用や保守作業を要する部分があるが，他ベンダーが提供する SaaS はそれらまで含めてサービス提供されているものが多い．

他ベンダーが提供するセキュリティ機能の SaaS は，WAF や不正侵入対策（IPS/IDS），DDoS 対策，ゲートウェイ型ウイルス対策など主にネットワークセキュリティ対策であり，シ

ステムの特性に合致するサービスを選んで活用することができる．他ベンダーが提供する主なSaaSを表2に示す．

表2　他ベンダーが提供する代表的なSaaS

	WAF	不正侵入対策（IPS/IDS）	DDoS対策	ゲートウェイ型ウイルス対策
機能概要	Webアプリケーションにおける脆弱性を狙った攻撃を防ぐことが出来る機能	主にOSやミドルウェアなどの脆弱性を狙った攻撃を防ぐことが出来る機能	DDoS攻撃を緩和することが出来る機能．但し，SaaSが提供するDDoS対策は低レイヤ（レイヤ4以下）であるものが多いため，高レイヤに対する対策は検討が必要	ファイル転送などの通信に対して，ネットワーク上でウイルススキャンを行うことで，不正プログラムがサーバに到達する前に防ぐことが出来る機能
CSP提供機能と比較した場合の利点 ※サービスによって異なる	新しい脆弱性への対応（新しいルール作成など）もサービス内に含まれていることが多く，CSP提供機能を利用した場合より運用負荷が少ない．	パブリッククラウドでは標準的に実装されている場合が多い．但し，CSP提供機能よりカスタマイズ機能が優れている場合が多い．	カスタマイズやレポート機能が優れているものがあり，定期的に状態を確認することができる．	CSP提供機能なし
利用が推奨されるシステム	インターネットに公開されるWebシステム	インターネットに公開されるシステム	インターネットに公開されるシステム	インターネットに公開され，不特定多数からのファイルアップロード機能を有するシステム

他ベンダーのSaaSを活用した場合，通信経路はSaaS環境を経由してパブリッククラウド環境に到達する．複数のSaaSを活用したシステムでは通信経路が各SaaSを経由することになり，ネットワークの遅延に繋がる．そのため，複数のSaaSを活用するのではなく，CSPが提供するセキュリティ機能や，次節以降で述べるセキュリティ対策方法と併せた対策を検討するべきである．なお，活用するSaaSによってはHTTPS通信で必要なサーバ証明書の登録が前提[*13]であったり，活用するSaaSのサービスレベルがシステム設計と異なるため全体のサービスレベルが低下したりする場合があるため，事前にサービス仕様の確認を要する．

4.3　クラウド向けの他ベンダー製品を活用する

アプライアンス製品を提供している各ベンダーは，自社製品をパブリッククラウド向けに仮想アプライアンスとして提供している場合があり，この仮想アプライアンスを利用することで，オンプレミス環境で活用しているアプライアンス製品と同様の機能をパブリッククラウド上で継続して利用することができる．AzureやAWSでは，パートナーベンダーが提供している仮想アプライアンスをマーケットプレイス[*14]と呼ばれる機能でデプロイできるようにしており，次世代ファイアウォールや不正侵入対策（IPS/IDS），WAF，ゲートウェイ型ウイルス対策などのセキュリティ対策が仮想アプライアンスを活用することで実装できる．マーケットプレイスから提供されている各製品は，BYOL[*15]（Bring Your Own License）での利用や，ライセンス料金をパブリッククラウドの利用料金に含めることができる製品もある．既に購入済のライセンスを再活用したり，ライセンス料金を従量課金として支払ったり，状況に応じて選択できる．

WAFなど一部のセキュリティ対策は，CSPが提供するセキュリティ機能や，他ベンダーのSaaS，仮想アプライアンスなど実装の選択肢が多い．全ての製品に共通する特徴ではないが，一般的に表3のような特徴がある．これらの特徴を理解し，システムによってどれを活用すべきか検討することを推奨する．

表 3　同じセキュリティ対策の実装形態による特徴

	CSPセキュリティ機能	他ベンダーSaaS	仮想アプライアンス
特徴	・利用開始が容易であり，比較的システム構成への影響が少ない． ・細かい設定変更やチューニングが出来ない機能が多い ・設定変更やポリシー見直し運用作業が必要	・利用開始が容易であり，システム構成への影響が少ない． ・細かい設定変更やチューニングが出来ないサービスが多い ・運用も含めてサービス提供されている	・制限される機能はほぼ無く，細かい設定変更やチューニングが可能 ・設定や運用，定期的なバージョンアップなどの保守作業が必要
コスト感	・他と比較して最も安価	・CSPより高額	・CSPより高額
注意点	・サービスの見直し，機能追加が頻繁に行われている場合が多く，定常的な確認，場合によっては新機能への切り替えを検討する必要がある	・CSPとは異なるベンダーが提供するサービスであるため，サービスレベルやメンテナンス時期などが異なる場合があるため，確認が必要	・ライセンス料が従量課金となっておらず，年間ライセンスを購入する必要のある製品もあるため，事前にライセンスも含め確認が必要

4. 4　仮想サーバに対して従来と同様のセキュリティ対策を行う

仮想サーバにおけるセキュリティ対策は，オンプレミスで構築した物理サーバと同様にウイルス対策や改ざん検知，セキュリティパッチ適用運用などの実施を検討する．また，WAF や IPS/IDS などネットワークにおけるセキュリティ対策もホスト型として製品化され提供されているものがある．ホスト型のセキュリティ対策製品は，仮想サーバに導入して利用するソフトウェアであり，仮想サーバ単位に導入可否を判断できるため，サーバの用途や重要度別に検討することができる．

複数の仮想サーバを構築してセキュリティ対策を行う場合は，オンプレミス環境と同様に統合管理することが望ましい．しかし，統合管理機能を利用するために，管理サーバを別途構築しなければならない製品は多く，システム構成の変更や，仮想サーバの追加を要する．パブリッククラウドでは，管理サーバを容易に構築できるよう，マーケットプレイスからデプロイ可能な製品も存在するが，仮想サーバの追加となることには変わりない．この統合管理機能を SaaS としてサービス提供している製品もある．システムの特性や求められるセキュリティ要件，保護対象となる仮想サーバの台数などに応じて，採用する製品を検討することを推奨する．管理サーバを IaaS で構築（マーケットプレイスからのデプロイを含む）した場合と，SaaS で提供された統合管理機能を利用する場合の一般的な視点での特徴を表 4 に示す．

表 4　管理サーバを IaaS で構築と SaaS 活用の特徴

	管理サーバをIaaSで構築	管理機能にSaaSを活用
特徴	・提供された機能を全て利用することが可能であるが，管理サーバの構築，維持運用（パッチ適用等）作業が必要． ・管理サーバも保護する必要があるため，管理サーバ分のライセンスも購入が必要 ・管理サーバを内部に設置することで，保護対象となる仮想サーバと管理サーバ間の通信は，内部ネットワークで完結	・一部の機能に制限（ログ保管期間など）が設けられている場合があるが，管理サーバの構築，維持運用作業は不要． ・保護対象となる仮想サーバは，インターネット上にある管理機能に接続（通信）する必要があるため，インターネット接続が必要．
コスト感	・1台当たりのライセンス料は割安※	・1台当たりのライセンス料が割高※

※ライセンスの考え方は製品によって異なるが，保護対象となる仮想サーバの台数に応じたライセンスが必要となる製品が多い．
上記表では，保護対象となる仮想サーバ1台当たりのライセンス料で比較

5.　パブリッククラウドを活用したシステムの具体的なセキュリティ対策

本章では，パブリッククラウドを活用したシステムのモデル別に具体的なセキュリティ対策を示す．3 章の事故事例を防ぐためのセキュリティ対策も含まれる．なお，本章で解説しているセキュリティ対策は，2019 年 6 月執筆時点において CSP が提供している機能や他ベンダーの SaaS を活用した対策である．パブリッククラウドや他ベンダーの SaaS は日々進化してい

るため，システム設計の際は，本章の内容を参考として最新の情報を調査した上でセキュリティ対策を検討しなければならない．

5.1　全システム共通のセキュリティ対策

まず，パブリッククラウドを活用した場合，インターネットに公開しているか否かに関係なく，共通して求められるセキュリティ対策がある．3章の事故事例でも挙げられているパブリッククラウドの不正利用に備えたセキュリティ対策である．

3.1節にて記載したような不正アクセスや不正利用に備え，管理コンソールの認証を強化する機能の利用や，管理コンソールへ接続するアカウントに付与する権限の最小化，不正利用を検知できるよう設定変更時の通知設定，利用料金の閾値超過時の通知設定などを施す．また，内部不正も視野に入れ，アカウントを個人に割り当て，各アカウントの操作記録を採取することも有効な対策である．運用や保守作業において一時的にパブリッククラウドの設定を変更することがあるが，作業後の戻し漏れや戻し忘れを検出するため，パブリッククラウドの設定値を定期的に確認する運用も効果がある．その他も含め，パブリッククラウドを活用するシステムに共通して求められるセキュリティ対策を表5に示す．多くの機能は，CSPが提供するものを活用できるが，一部他ベンダーが提供しているサービスで補うものもある．

表5　全てのシステムに求められるセキュリティ対策

分類	#	セキュリティ対策	補足
外部からのサイバー攻撃に対する備え	1	特権ユーザを利用しない	・特権ユーザは無効化し利用しない
	2	ユーザ認証の強化	・管理コンソールの認証は多要素認証を有効にする
	3	最小権限の付与	・管理コンソールのユーザ権限は役割に応じ，必要な権限のみ付与する
	4	アクセスキーの管理	・Azureではサービスプリンシパル，AWSではアクセスキー ・特権ユーザのキーは作成しない ・プログラムへのハードコード，GitHubなどへの登録は要注意
不正利用，操作ミスに対する備え	5	個別ユーザ付与	・ユーザは個人に紐付け，不要なユーザは定期的に確認して削除
	6	操作記録の保管	・各PaaSの操作記録を保管するにはPaaSの設定変更が必要なものもある
	7	設定変更時の通知設定	・クラウドサービスによっては，変更されたことを通知することが可能
	8	コスト超過時の通知設定	・月間の想定クラウド利用料を登録しておくことで，利用料が想定を超過した場合に通知することが可能．不正利用されたことを検知することが可能
	9	定期的な設定確認	・他ベンダーが提供するツールを活用 ・定期的（日次や週次）で実行することで，不正に変更されたことを検知することが可能

5.2　システムモデル別のセキュリティ対策例

前節で示したシステム共通のセキュリティ対策に加え，システムの特性によって個別のセキュリティ対策を施す．本節では，パブリッククラウドを活用したシステムモデルを想定し，そのシステムにおけるセキュリティ対策例を示す．セキュリティ対策例では，セキュリティ対策を解説し，4章で示したどの対策方法が推奨されるかを表形式で示す．システムモデルとして，大量コンテンツの効率的な配信システム，不特定向けの大規模ECサイト，パブリッククラウドと専用線接続利用の3パターンを示す．

5.2.1　システムモデル1：大量コンテンツの効率的な配信システム

ファイルや動画，静的コンテンツなどを大量にインターネット経由で利用者に配信するシステムをパブリッククラウド上に構築する場合，CSPが提供するCDNサービス[*16]（Azure

CDN や Amazon CloudFront）を活用するシステム構成となる．このような効率的にコンテンツ配信するシステムの構成を図 2 と想定し，求められるセキュリティ対策を表 6 に示す．

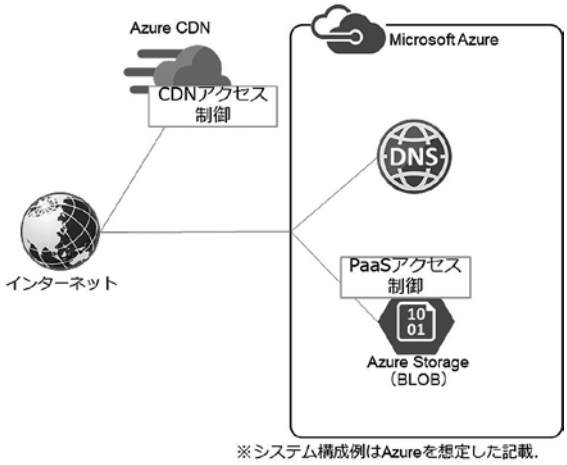

図 2　大量コンテンツの効率的な配信システムのシステム構成例

このような配信システムの場合，全てを PaaS で実装することで，クラウド利用者の責任範囲を少なくすることができる．CDN サービスが外部からのサイバー攻撃への対策（DDoS 対策など）を実施している[*17]ので，クラウド利用者は不正利用や不正アクセスのためのアクセス制御を中心に検討することができる．

CDN へのアクセス制御として，CDN サービスが提供する機能を活用できる．コンテンツを配信する時間帯や配信対象者が限定されている場合は，それらのアクセス制限機能を活用する．さらに，コンテンツが保管されているストレージへの直接アクセスを CDN サービスからのアクセスに限定することで，CDN を回避して接続しようとする不正アクセスも防ぐことができる．

なお，本システムから配信されるコンテンツは，運用者がコンテンツをアップロードする際にウイルスチェックすることを想定しているため，本システム中ではウイルス対策を行っていない．

表 6　大量コンテンツの効率的な配信システムでのセキュリティ対策例

#	セキュリティ対策	推奨する対策方法	サービス名		選定理由
1	CDNアクセス制御	4.1 CSP	Azure	Azure CDN	・サービスが標準機能として提供しているアクセス制御機能は，無料で利用できる場合が多く，十分なアクセス制御が可能であるものが多いため，CSP提供機能を活用する． ・但し，有料のアクセス制御機能が提供されている場合は，有料の機能を併用することも検討する必要あり
			AWS	CloudFront	
2	PaaSアクセス制御	4.1 CSP	Azure	Azure Storage	・サービスが標準機能として提供しているアクセス制御機能は，無料で利用できる場合が多く，十分なアクセス制御が可能であるものが多いため，CSP提供機能を活用する． ・但し，有料のアクセス制御機能が提供されている場合は，有料の機能を併用することも検討する必要あり
			AWS	S3	

5. 2. 2　システムモデル 2：不特定向けの大規模 EC サイト

パブリッククラウドを活用したシステムで最も多いのは，不特定向けにインターネット公開するシステムである．不特定向けの大規模 EC サイトなどは，最も攻撃を受けやすいシステム

である．パブリッククラウドを活用した不特定向け大規模 EC サイトのシステム構成を図 3 と想定し，求められるセキュリティ対策を表 7 に示す．

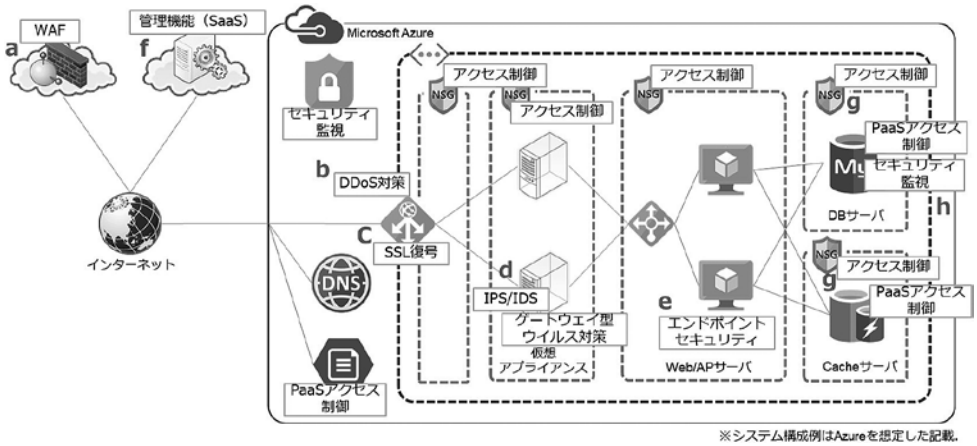

図 3　不特定向け大規模 EC サイトのシステム構成例

不特定向けにインターネット公開しているシステムは，サイバー攻撃のリスクに常に晒されている．セキュリティベンダーが提供している製品や SaaS を活用し，新しい攻撃にも素早く対応できるようにする．

新しい脆弱性を突いた攻撃に対応できるようアプリケーションの前段には WAF を設置し（図 3 の a），サービス妨害への対策として DDoS 対策も利用する（同 b）．SSL/TLS 通信の復号処理はパフォーマンスへの影響を考慮し CSP サービスを活用する（同 c）．IPS/IDS はネットワーク型もしくはホスト型での実装が可能だが，本例では不正プログラムのシステムへの侵入を事前に防ぐことを目的に，ゲートウェイ型ウイルス対策機能を有した仮想アプライアンスを設置する（同 d）．

仮想サーバへのセキュリティ対策は従来のウイルス対策だけではなく，振る舞い検知などもできる製品を活用する（同 e）．本例では 2 台構成で図示しているため統合管理は不要との判断もできるが，大規模 EC サイトを想定しているため，仮想サーバの増減を考慮し統合管理機能が SaaS 提供されている製品を選定する（同 f）．

データベースサービスやキャッシュサービス等の PaaS は仮想ネットワーク[*18] に接続できる機能を提供しているものがある．設定誤りなどでインターネット公開されるリスクが減るため，提供機能を調査し，可能な限り仮想ネットワークに接続すべきである（同 g）．また，データベースサービスなど一部の PaaS には，セキュリティ監視機能（監査機能など）が提供されている．本機能は有料サービスとなる場合もあるが，重要データを保管する PaaS であれば利用の検討を推奨する（同 h）．

CSP はクラウド環境全体に対するセキュリティの管理機能，監視機能をサービスとして提供している．CSP によって提供されている機能が異なる．Azure が提供するサービスでは IaaS や PaaS への脅威の検出，および各設定状況を確認し，対応した方が良い箇所を通知する．AWS が提供するサービスでは IaaS や PaaS への脅威検出，および AWS 上で採取された各種ログを分析し，悪意ある操作の可能性を検出して通知する．パブリッククラウドでは，クラウ

ド利用者には対策が難しいものも多く，このようなセキュリティ管理，監視機能は，有料であってもCSPが提供する機能を活用すべきである．

表7　不特定多数向け大規模ECサイトでのセキュリティ対策例

#	セキュリティ対策	推奨する対策方法	サービス名		選定理由
1	WAF	4.2 他ベンダSaaS	SaaS型WAF		・他ベンダが提供するWAFサービスは専門要員による運用が行われているものが多く，新しい脆弱性にも素早く対応可能であるため，他ベンダSaaSを活用する．
2	DDoS対策	4.1 CSP	Azure	DDoS Protection	・低レイヤのDDoS対策は利用者側で実施することが出来ないため，CSP提供機能を活用する． ・CSPは，標準機能として簡易なDDoS対策を提供している場合が多いが，多機能な有償機能の利用も検討する．
			AWS	AWS Shield	
3	SSL復号	4.1 CSP	Azure	Application Gateway	・暗号化通信の復号は，パフォーマンスへの影響を考慮し，CSP提供機能を活用する．（2019年6月時点では，仮想アプライアンスによる復号処理は，CPU負荷が高くアプリケーションのパフォーマンスに影響を及ぼしてしまう場合が多い）
			AWS	Application LB	
4	アクセス制御	4.1 CSP	Azure	NSG	・サービスが標準機能として提供しているアクセス制御機能は，無料で利用できる場合が多く，十分なアクセス制御が可能であるものが多いため，CSP提供機能を活用する． ・但し，有料のアクセス制御機能が提供されている場合は，有料の機能を併用することも検討する必要あり
			AWS	セキュリティグループ	
5	IPS/IDS ゲートウェイ型ウイルス対策	4.3 他ベンダ製品	仮想アプライアンス		・IPS/IDS機能，ゲートウェイ型ウイルス対策機能は，2019年6月時点でCSPから提供されていない．そのため，他ベンダ製品を仮想アプライアンスで構築する．
6	エンドポイントセキュリティ	4.4 従来の対策	管理機能にSaaSを活用		・複数台の仮想サーバを統合管理できるよう，管理機能がSaaS提供されている製品を活用する．
7	PaaSのアクセス制御	4.1 CSP	Azure	SQL Database, Storageなど	・サービスが標準機能として提供しているアクセス制御機能は，無料で利用できる場合が多く，十分なアクセス制御が可能であるものが多いため，CSP提供機能を活用する． ・但し，有料のアクセス制御機能が提供されている場合は，有料の機能を併用することも検討する必要あり
			AWS	RDS，S3など	
8	セキュリティ監視	4.1 CSP	Azure	Security Centerなど	・CSP以外での実装は難しい監視機能などを提供しているため，CSP提供機能を活用する． ・CSPによって提供機能が異なるため，調査した上で活用を検討する． ・データベースサービスなど重要なデータを保管するPaaSにおいても，個別にセキュリティ監視機能が提供されているため，優先的に活用を検討する．
			AWS	GuardDutyなど	

5.2.3　システムモデル3：パブリッククラウドと専用線接続利用

CSPが提供するアクセス制御機能を利用してインターネットからの接続を全て制限し，専用線接続サービスでイントラネットと接続することで，パブリッククラウドをプライベートクラウドとして利用することができる．既にオンプレミス環境で稼働している社内向けシステムをLift&Shift[*19]方式にてパブリッククラウドへ移行する場合，本モデルが該当する．

このような利用の場合，外部からのサイバー攻撃を受けるリスクは少ないが，アクセス制御機能を正しく設定しなければ想定外のリスクに晒されることになる．パブリッククラウドと専用線接続利用として，社内向けシステムを想定したシステム構成を図4と想定し，求められるセキュリティ対策を表8に示す．

社内向けシステムを構築する場合，まずパブリッククラウド上に仮想ネットワークを作成し，アクセス制御機能を利用してインターネットから仮想ネットワークへの通信を全て制限する．その上で，イントラネット（オンプレミス環境）と専用線で接続する．

PaaSを利用する場合，PaaSも全て仮想ネットワークに接続することを推奨する．仮想ネットワークに接続することができないPaaSの場合は，グローバルIPアドレス単位でのアクセス制限と，暗号化通信を必須とする設定を行う．

IaaSを利用するシステム構成の場合，エンドポイントセキュリティはイントラネットで利用している製品を利用することで，オンプレミスとクラウドの統合管理が可能になる．管理サーバの移行については，クラウド環境への移行計画として検討し，影響の少ないタイミング

で移行すべきである．管理サーバは，移行前であっても移行後であっても，オンプレミス環境とクラウド環境の両方を統合管理することが可能である[*20]．

社内向けシステムであり，インターネットからの接続を制限することで，WAF や IPS/IDS，DDoS 対策などは不要である．

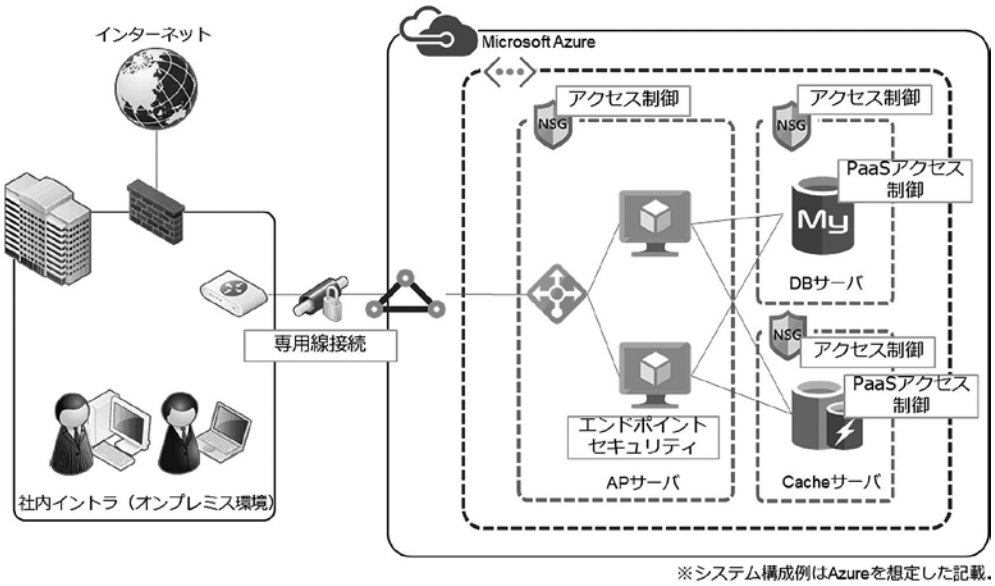

図 4　パブリッククラウドと専用線接続利用のシステム構成例

表 8　パブリッククラウドと専用線接続利用でのセキュリティ対策例

#	セキュリティ対策	推奨する対策方法	サービス名		選定理由
1	専用線接続	4.1 CSPサービス	Azure	Express Route	• オンプレミス環境や社内ネットワークと直接接続するには，CSPが提供するVPN接続か専用線接続サービスを活用する．安定した通信が求められる場合は，専用線接続サービスの活用を検討する．
			AWS	Direct Connect	
2	アクセス制御	4.1 CSPサービス	Azure	NSG	• サービスが標準機能として提供しているアクセス制御機能は，無料で利用できる場合が多く，十分なアクセス制御が可能であるものが多いため，CSP提供機能を活用する． • 但し，有料のアクセス制御機能が提供されている場合は，有料の機能を併用することも検討する必要あり
			AWS	セキュリティ グループ	
3	エンドポイントセキュリティ	4.4 従来の対策	オンプレミスと同製品		• オンプレミスで採用しているエンドポイントセキュリティ製品を利用
4	PaaSのアクセス制御	4.1 CSPサービス	Azure	SQL Database，Storageなど	• サービスが標準機能として提供しているアクセス制御機能は，無料で利用でき，十分なアクセス制御が可能であるものが多いため，CSPサービスを活用する． • 但し，有料のアクセス制御機能が提供されている場合は，有料の機能を併用することも検討する必要あり • 利用するPaaSが，仮想ネットワークに接続可能な機能を有している場合，仮想ネットワークに接続することを強く推奨する．
			AWS	RDS，S3など	

6. お　わ　り　に

パブリッククラウドは，低コストで耐障害性の高いシステム構築を可能にし，従来の調達速度よりはるかに速くリソースを確保できるなど，ビジネスの発展を下支えできるインフラであるため，今後更なる利用拡大が想定される．IaaS だけに注目すると，オンプレミスと同様 OS（Windows や Linux）が稼働しているため，セキュリティ対策なども同様に考えがちだが，パブリッククラウド上では実装方法が異なる．本稿で解説したように，CSP が提供するセキュ

リティ機能を中心に正しくセキュリティ対策を行うことを強く推奨する．

クラウドサービスは成長が速く，様々なサービスや機能が続々とリリースされている．その中にはセキュリティ機能も含まれているため，常に動向を確認し新しい機能の活用を検討するべきである．パブリッククラウドは利用者のコミュニティが形成されており，ブログなどで有識者が解説を公開している．従量課金であり，新機能を検証するだけであれば，数千円程度で利用することもできるため，システム設計をする際には，調査と検証を組み合わせてセキュリティ対策を検討することが望ましい．

なお，システム開発においては，本稿に記載されたインフラ関係のセキュリティ対策以外にも，アプリケーションのセキュアコーディング，セキュリティ対策を維持するための運用などは重要なセキュリティ対策の要素である．セキュリティ対策はシステム全般においてバランス良く実施すべきであることを補足しておく．

最後に，本稿執筆にあたりご協力，ご指導いただいた全ての皆様に深く感謝し，お礼申し上げます．

＊1　IaaS（Infrastructure as a Service）とは，仮想サーバやストレージ，ネットワークなどのリソースをインターネット経由で提供するサービスを指す．また，PaaS（Platform as a Service）は，データベースやアプリケーションサーバ等のミドルウェアレイヤまでをサービスとして提供するサービスであり，SaaS（Software as a Service）は，ソフトウェアやアプリケーションの機能を提供するサービスである．

＊2　ISO/IEC27001 とは，情報セキュリティマネジメントシステム（Information Security Management System 以降，ISMS）を構築・運用し，継続的に改善するための国際規格であり，準拠しているかを認定機関が審査する制度がある．

＊3　ISO/IEC27017 とは，クラウドサービスの提供および利用に関する情報セキュリティ管理策であり，ISO/IEC27001 を補完する国際規格の一つである．

＊4　PCI DSS（Payment Card Industry Data Security Standard）とは，クレジットカード情報および取り引き情報を保護するために国際ペイメントブランド5社が共同で策定したクレジット業界における国際的なセキュリティ基準であり，準拠しているかを認定機関が審査する制度がある．

＊5　NIST サイバーセキュリティフレームワークとは，米国の政府機関である NIST（米国国立標準技術研究所）が発行した「重要インフラのサイバーセキュリティを向上させるためのフレームワーク」のこと．

＊6　FISC 安全対策基準とは，FISC（公益財団法人金融情報システムセンター）が発行した日本の金融機関システム向けのセキュリティ基準である．

＊7　仮想アプライアンスとは，機能を実現するために必要となる全てのものをプリインストール，設定した OS イメージを保持した仮想サーバのことであり，ネットワーク機器やセキュリティ機器などを仮想化技術の上で動作するように設計されたもの．

＊8　パスワードクラック（パスワードクラッキング）とは，他人のパスワードを不正に暴く行為であり，総当たり攻撃（ブルートフォース攻撃）や辞書攻撃（ディクショナリ攻撃），パスワードリスト攻撃など複数の攻撃手法が存在する．

＊9　GitHub とは，ソースコードのバージョン管理システムである Git の仕組みを利用して世界中の人々とソースコードを共有することができるサービスである．設定によりプライベートでの利用も可能である．

＊10　DDoS 対策は，CSP は標準機能として提供している．さらに，PaaS などにオプションとして高機能が付加されている場合もある．

＊11　Azure や AWS では，パブリッククラウドを活用する際のセキュリティのベストプラクティスをホワイトペーパーとして公開している[4][5]．

＊12　CIS（国際インターネット・セキュリティ組織）とは，米国の政府機関と企業，学術機関などが協力して，インターネット・セキュリティ標準化に取り組む団体である．

＊13　WAF や IPS/IDS などの機能を適用する SaaS では，通信の内容のチェックが行われる．SSL/TLS にて暗号化された状態では通信の内容がチェックできないため，復号するためにサーバ証明書を SaaS に登録しなければならない．

＊14　マーケットプレイスとは，CSP が提供する管理コンソール上から，そのパブリッククラウド向けのサービスや製品を販売する場であり，CSP だけではなくパートナーベンダーも様々

な製品を販売している．

＊15 BYOL（Bring Your Own License）とは，既に持っている，もしくは別途購入したライセンスをクラウド環境に持ち込んで利用する形態のこと．

＊16 CDN サービスとは，コンテンツを多くの配布先に対して効率的に配布するための仕組み（Content Delivery Network：CDN）であり，Azure では「Azure CDN」というサービス，AWS では「Amazon CloudFront」というサービスを提供している．

＊17 CSP が提供する CDN サービスなどが実装しているセキュリティ対策については，CSP が公開しているドキュメントを確認することを推奨する．

＊18 仮想ネットワークとは，仮想的に構築されたネットワークのことだが，本稿では CSP が提供する機能を用いてクラウド内に利用者独自に構築したネットワークを指す．

＊19 Lift&Shift とは，オンプレミス環境等で稼働しているシステムをパブリッククラウド環境に移行する方式の一つである．Lift&Shift 方式で移行する場合，まず Lift として IaaS を活用したシステム構成となる．その後，Shift として PaaS を活用していくことで，運用負荷を減らし，セキュリティの責任範囲を縮小していくことができる．

＊20 一部，複数の仮想ネットワークで構成されたクラウド環境の場合，直接通信が行えず，統合管理できない場合がある．

参考文献

［1］ 日本マイクロソフト株式会社，「Azure 定番システム設計・実装・運用ガイド～オンプレミス資産をクラウド化するためのベストプラクティス」，日経 BP 社，2018 年 9 月，初版

［2］ エディフィストラーニング株式会社 竹島 有理，「ひと目でわかる Azure Active Directory 第 2 版」，日経 BP 社，2018 年 10 月，初版第 3 刷

［3］ NRI ネットコム株式会社 佐々木拓郎 林晋一朗 小西秀和 佐藤瞬，「Amazon Web Services パターン別構築・運用ガイド」，SB クリエイティブ株式会社，2016 年 5 月，初版第 4 刷

［4］ Azure セキュリティ ホワイト ペーパー，日本マイクロソフト株式会社，2018 年 11 月 https://docs.microsoft.com/ja-jp/azure/security/security-white-papers

［5］ AWS ホワイト ペーパー，Amazon Web Services, Inc., 2019 https://aws.amazon.com/jp/whitepapers/

※ 上記参考文献に含まれる URL のリンク先は，2019 年 6 月 26 日時点での存在を確認．

執筆者紹介

石 川 政 朝（Masatomo Ishikawa）

ソフトウェア開発会社にて開発業務に従事した後，2004 年に日本ユニシス(株)入社．入社後，大規模金融システムにおけるインフラセキュリティ対策，EC サイトのインフラセキュリティ対策，大規模流通システムのセキュリティ対策などを担当し，2014 年からメガクラウドを活用した複数の案件にセキュリティ対策担当として従事．情報セキュリティ・プロフェッショナル（CISSP）