クラウドにおける
セキュリティサービスの
効果的な管理のガイドライン

Acknowledgements

Initiative Lead
Kai Chen

Key Contributors
Renato Jose
Delatorre Zhenyu
Wang
Xinmei Shi
Zhiliang Zhang
Yixin Jin
Bin Luo
Heng
Liang
Theo Dimitrakos
Sabri Khemissa
Vani Murthy
Andrea Knoblauch
Atul Bahl
Diego Fernandez

CSA Staff
Hing-Yan Lee
Haojie Zhuang
Victor Chin
Courtney Keogh
Jane Chow

日本語版提供に際しての告知及び注意事項

本書「クラウドにおけるセキュリティサービスの効果的な管理のガイドライン」は、Cloud Security Alliance (CSA)が公開している「Guideline on Effectively Managing Security Service in the Cloud」の日本語訳です。本書は、CSA ジャパンが、CSA の許可を得て翻訳し、公開するものです。原文と日本語版の内容に相違があった場合には、原文が優先されます。
翻訳に際しては、原文の意味および意図するところを、極力正確に日本語で表すことを心がけていますが、翻訳の正確性および原文への忠実性について、CSA ジャパンは何らの保証をするものではありません。
この翻訳版は予告なく変更される場合があります。以下の変更履歴（日付、バージョン、変更内容）をご確認ください。

変更履歴

日付	バージョン	変更内容
2019 年 9 月 17 日	日本語版 1.0	初版発行

日本語版作成に際しての謝辞

「クラウドにおけるセキュリティサービスの効果的な管理のガイドライン」の日本語訳は、CSA ジャパンの「CCM/STAR ワーキンググループ」に参加するメンバーを中心とした、CSA ジャパン会員の有志により行われました。
作業は全て、個人の無償の貢献としての私的労力提供により行われました。なお、企業会員からの参加者の貢献には、会員企業としての貢献も与っていることを付記いたします。
以下に、翻訳に参加された方々の氏名および所属先（企業会員からの参加の場合のみ）を記します。（氏名あいうえお順・敬称略）

伊賀　誠
勝見　勉
成川　達也
満田　淳
諸角　昌宏

要旨

クラウドサービスプロバイダとクラウドサービスカスタマは、セキュリティ責任共有モデルに基づき、Iaas、Paas、Saasといった異なるサービスモデルにおけるそれぞれ特有のセキュリティ責任を分担します。さらに、クラウドプラットフォームにSecurity-as-a-Service (SecaaS)を提供するクラウドセキュリティサービスプロバイダが分担する場合もあります。それぞれのセキュリティ責任を満たすために定義されたセキュリティ特性と機能があります。本書は、サードパーティのセキュリティ製品とサービスを使用してCCMに基づくクラウドのコントロールを実現する方法に関するガイダンスを提供します。セキュリティ機能をサポートするための実用的な模範ケースを示すため、附属書Aは、市販のセキュリティ製品およびサービスを使ったケーススタディを提供します（ベンダーは参照されていません)。 *（訳注： 本文書には附属書Aは存在しないが原文をそのまま訳して記述。）*

1 概要

1.1 この文書の背景

セキュリティ責任共有モデルはよく知られています。すべての主要なクラウドサービスプロバイダ (CSP) は、セキュリティ責任共有についてのホワイトペーパーまたは声明を公開し、クラウドの提供における役割と責任について説明しています。実際には、同じ責任共有のコンセプトであっても、それぞれのCSPでは解釈や実装が異なります。セキュリティの責任を果たすためにCSP向けに開発されたクラウドセキュリティ標準や仕様は多くありますが、クラウド利用者にとっては、セキュアなクラウドサービスの設計、展開、運用は依然として困難です。この文書では、クラウド利用者に、さまざまなクラウドサービスモデルでのセキュアなクラウドサービスの設計、展開、運用方法のわかりやすいガイダンスを提供します。いくつかの標準とベストプラクティス[1,2,3,4]が、さまざまな側面からクラウド利用者にとって価値あるガイダンスを提供しており、これらは役に立つ参考資料です。

1.2 この文書の使いかた

この文書は、クラウドサービスの利用を予定している組織向けのガイダンスを提供します。クラウドでのサービスシステムを構築したり既存システムをクラウドに移行することを計画する際に、この文書を利用します。このガイダンスは、これらの組織がサービスシステムの安全な運用を確保し、自組織および CSP のセキュリティ責任、その責任を引き受けるために提供すべきセキュリティ保証機能、存在するギャップ、ギャップに対処するために関連する機能をどのように開発するかについて明確に理解するのに役立ちます。この文書は、クラウドプラットフォームのセキュリティ保証システムを構築するCSPや、クラウドサービスセキュリティインテグレータ、クラウドサービスカスタマも利用できます。
この文書は、プライベートクラウド、パブリッククラウド、ハイブリッドクラウド、コミュニティクラウドに適用されます。

1.3 用語集

CSP:クラウド サービス プロバイダー
O&M:運用管理

1. Cloud Customer Architecture for Securing Workloads on Cloud Services, **https://www.omg.org/cloud/deliverables/CSCC-Cloud-Customer-Architecture-for-Securing-Workloads-on-Cloud-Services.pdf**.
2. Cloud Computing Security for Tenants, **https://acsc.gov.au/publications/protect/Cloud_Computing_Security_for_Tenants.pdf**.
3. ISO/IEC 27018:2014 — Information technology — Security techniques —Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors.
4. Software Defined Perimeter for Infrastructure as a Service, **https://cloudsecurityalliance.org/artifacts/sdp-for-iaas/**

2 CSP,セキュリティサービスプロバイダ、クラウドカスタマのセキュリティの役割と責任

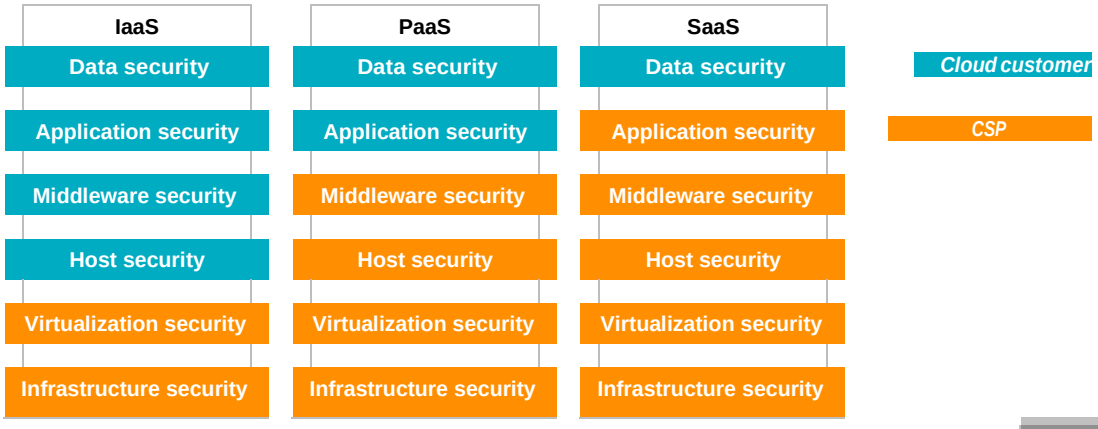
2.1 セキュリティ責任共有モデル

クラウドでのセキュリティは、その責任がCSP とカスタマの間で共有されることがよく知られています。責任共有モデルを理解するには、クラウドコンピューティングの3つの異なる階層モデルを理解する必要があり、多くの組織において、クラウドコンピューティング戦略を構築するにあたりこれらのサービスを組み合わせて利用しています。クラウドコンピューティングの3つの異なる階層モデルとは、Software as a Service (SaaS)、Platform as a Service (PaaS)、Infrastructure as a Service (IaaS) です。それぞれのモデルで、ベンダーとカスタマ間のセキュリティ責任区分が大きく異なっています。

Microsoft Azure,[5] Amazon AWS,[6] Huawei.[7]といった主要な CSP は、セキュリティ責任共有モデルを説明するホワイト ペーパーを公開しています。

ここでは、下に示すセキュリティ責任共有の図を作成するために、ガートナーのセキュリティ責任共有モデル8を参照しています。図2−1は、IaaS、PaaS、SaaSクラウドモデルのセキュリティ責任分界点を示しています。責任分界点が段階的に上に移動しています。IaaSにおいては、CSP側の管理が最も少なく、カスタマにはそれを補うセキュリティ責任が委ねられます*（訳注：mostはleastの間違いと思われる）*。SaaSにおいては、カスタマ側の管理が最も少なく、CSPが大部分のセキュリティ責任を負います。

図 2-1 クラウドサービスごとの CSP とクラウド利用者のセキュリティ責任範囲



5. Shared Responsibilities for Cloud Computing, Microsoft Azure, **https://gallery.technet.microsoft.com/Shared-Responsibilities-81d0ff91**.
6. AWS Shared Responsibility Model, **https://aws.amazon.com/compliance/shared-responsibility-model**.
7. Huawei Cloud Security Whitepaper, **https://static.huaweicloud.com/upload/files/pdf/20171123/20171123171541_66845.pdf**.
8. Staying Secure in the Cloud Is a Shared Responsibility, Gartner, **https://www.gartner.com/doc/3277620/staying-secure-cloud-shared-responsibility**.

2.2 CSP およびクラウド利用者の共通セキュリティ責任

CSPおよびクラウド利用者のセキュリティ責任のいくつかは、すべてのクラウドサービスモデルで共通です。わかりやすいようにここに列記されており、各サービスモデルで繰り返されません。

2.2.1 CSP の共通セキュリティ責任

- インフラストラクチャの物理的セキュリティ。次にあげる項目を含むがこれらに限定されるものではない。機器の設置場所の選択、電力供給保証、冷却設備、火災、水、ショック、盗難に対する保護、監視。（セキュリティ要件の詳細については、関連するセキュリティ標準を参照。)
- コンピューティング、ストレージ、ネットワークのハードウェアセキュリティ。
- DDoS防御 やファイアウォールなどの基本的なネットワークセキュリティ。
- バックアップやリカバリなどのクラウドストレージセキュリティ。
- テナントリソースの隔離や仮想化リソース管理など、クラウドインフラストラクチャの仮想化のセキュリティ。
- テナントの ID 管理とアクセス制御
- テナントによるクラウドリソースへの安全なアクセス
- インフラストラクチャのセキュリティ管理、運用監視、緊急対応
- インフラストラクチャのための、サービス継続性保証計画および災害復旧計画の策定とリハーサル

2.2.2 クラウド利用者の共通セキュリティ責任

- サービスシステムのユーザーアイデンティティ管理とアクセス制御
- データセキュリティ(欧州のGDPRでは、クラウド利用者がデータを管理し、データセキュリティに責任を負います。CSPはデータを処理するだけなので、データ管理者によって与えられたセキュリティ責任を負います。)
- ハードウェア、ソフトウェア、アプリケーションシステム、デバイスの権限を含むクラウドサービスにアクセスする端末のセキュリティ管理。

2.3 IaaS

IaaS サービスモデルでは、クラウド利用者は CSP からコンピューティング、ストレージ、ネットワークインフラストラクチャの提供を受け、独自のサービスシステムを構築します。したがって、カスタマはシステムセキュリティの責任の大部分を負います。CSP は、クラウドデータセンタのインフラストラクチャと基本的なリソースのセキュリティに責任を負います。

2.3.1 CSP のセキュリティ責任

CSP は、セクション 2.2.1 で定義されている共通セキュリティ責任を負います。

2.3.2 クラウド利用者のセキュリティ責任

クラウド利用者は、セクション 2.2.2 の責任に加えて次に挙げるセキュリティ責任を負います:

- CSP が提供するインフラストラクチャのセキュリティ保証機能—クラウド利用者は、CSP のサービス内容や合意したセキュリティ責任を確認することができます。また、第三者が発行したセキュリティ証明書の提供をCSPに依頼できます。必要に応じて、カスタマはCSPのセキュリティ保証機能を現場で確認できます。
- データ転送のセキュリティ
- 仮想ネットワークのセキュリティ
- オペレーティング システム (OS) やデータベースのセキュリティなどの、プラットフォーム層のセキュリティ
- アプリケーションシステムのセキュリティ
- セキュリティ設定、セキュリティ管理、システムリソースの監視
- 事業継続保証計画及び災害復旧計画の策定とリハーサル
- インフラストラクチャのセキュリティ設定、管理、運用監視、緊急対応

2.4 PaaS

PaaS サービスモデルでは、CSP はクラウド利用者にコンピューティング、ストレージ、ネットワークインフラストラクチャ、およびサービスアプリケーションシステムの開発と展開をサポートする OS やデータベースなどのプラットフォームサービスを提供します。セキュリティ責任は次に説明するとおりです。.

2.4.1 CSP のセキュリティ責任

CSP の共通セキュリティ責任のほかに、CSP は次に挙げる責任も負います:

- インフラストラクチャのセキュリティ設定、管理、運用監視、緊急対応
- 仮想ネットワークのセキュリティ
- OS やデータベースのセキュリティなど、プラットフォーム層のセキュリティ
- アプリケーションシステムのセキュリティ

2.4.2 クラウド利用者のセキュリティ責任

クラウド利用者は、セクション 2.2.2 の責任に加えて次に挙げるセキュリティ責任を負います:

- CSP が提供するインフラストラクチャのセキュリティ保証機能—クラウド利用者は、CSPのサービス内容や合意したセキュリティ責任を確認することができます。また、第三者が発行したセキュリティ証明書の提供をCSPに依頼できます。必要に応じて、カスタマはCSPのセキュリティ保証機能を現場で確認できます。
- プラットフォームのセキュリティ設定、管理、監視
- 必要な時にネットワークを監査するための CSP との合意書
- サービスアプリケーションシステムのセキュリティ
- 事業継続保証計画及び災害復旧計画の策定とリハーサル
- サーバーレスアーキテクチャのセキュリティ

2.5 SaaS

SaaS サービスモデルでは、CSP はアプリケーションと基盤となるコンポーネントのセキュリティを提供します。カスタマは、データセキュリティとエンドポイントデバイスの保護に責任を負います。

2.5.1 CSP のセキュリティ責任

2.4.1 でのCSP のセキュリティ責任要件のほかに、CSP は次に挙げる責任も負います:

- プラットフォームのセキュリティ設定、管理、稼働監視、緊急対応
- サービスアプリケーションシステムのセキュリティ

2.5.2 クラウド利用者のセキュリティ責任

クラウド利用者は、セクション 2.2.2 の責任に加えて次に挙げるセキュリティ責任を負います:

- CSP が提供するインフラストラクチャのセキュリティ保証機能—クラウド利用者は、CSPのサービス内容や合意したセキュリティ責任を確認することができます。また、第三者が発行したセキュリティ証明書の提供をCSPに依頼できます。必要に応じて、カスタマはCSPのセキュリティ保証機能を現場で確認できます。
- サービスアプリケーションシステムのセキュリティ設定、管理、監視
- セキュアなアクセス

2.6 サードパーティのセキュリティサービスプロバイダの役割

クラウド コンピューティング業界の急速な発展に伴い、サードパーティのセキュリティサービスプロバイダは、クラウド サービスセキュリティ保証においてますます重要な役割を果たしています。これらのセキュリティサービスプロバイダは、ビジネス契約や合意に基づいて、CSPまたはクラウド利用者のセキュリティ責任の一部分を引き受けます(責任の移転)。

クラウドコンピューティングサービスの普及に伴い、クラウドコンピューティングプラットフォームは、単にクラウド利用者の複数のサービスシステムを載せるだけのものではなくなりました。クラウド サービスの安全かつ信頼性の高い運用は、国の社会的および経済的な安定性に重要な影響を及ぼします。そのため、政府や業界団体は、CSPが提供するクラウドサービスプラットフォームや、クラウド利用者が構築したアプリケーションシステムのセキュリティを監視し、カスタマにガイダンスを提供する必要があります。このプロセスには、専門的なサード パーティのセキュリティサービスプロバイダから提供されるセキュリティ認証、監査、および検査サービスが必要です。

組織のセキュリティ機能はそれぞれ異なります。そのため、サービスシステムをクラウドに移行する場合、クラウドサービスプラットフォームのセキュリティ責任共有モデルに基づくセキュリティソリューションの設計、計画、展開に苦労しています。したがって、専門的なサードパーティサービスプロバイダからのコンサルティング、統合、構築サービスを必要としていると考えられます。さらに、クラウドプラットフォームや、その上に展開されたシステムのセキュリティ脆弱性のスキャンと修正など、システムがクラウドで稼働した後のセキュリティ管理と保守・運用サービスも必要になることでしょう。

3 クラウドセキュリティ保証機能の技術的要件と実装ガイド

この章では、クラウドサービスシステムのセキュリティ保証に関する技術要件について説明し、既存のセキュリティ技術、製品、サービスに基づく実装ガイドを提供します。また、セクション2「CSP、セキュリティサービスプロバイダ、クラウド利用者のセキュリティの役割と責任」に従って、CSPおよび顧客がさまざまなクラウドサービスモードで提供する必要があるセキュリティ保証テクノロジ、製品、サービスについても説明します。

3.1 異なるクラウドサービスモードにおけるセキュリティ技術の責任分担

図 3-1 CSP とクラウド利用者間のセキュリティ責任

Category	Major Security Technology Requirement	IaaS	PaaS	SaaS
Infrastructure security	Physical and network security	CSP	CSP	CSP
Virtualization security	Virtualization platform, virtual storage, and API security	CSP	CSP	CSP
	Virtual network	Cloud customer	CSP	CSP
Host security	Antivirus, intrusion prevention, host security hardening, and patch management of OS, firmware updates	Cloud customer	CSP	CSP
Middleware security	Container, API, database, and resource management platform security	Cloud customer	CSP	CSP
Application system security	Web vulnerability scanning, web tamper protection (WTP), anti-DDoS, application firewall, Identity and access management (IAM), and API security, DLP solutions	Cloud customer	Cloud customer	CSP
Data security	Data transmission and storage security, integrity protection, backup, and recovery	Cloud customer	Cloud customer	Cloud customer
Security management	Network audit, network behavior management, traffic control management, key and certificate management, IAM, database audit, cloud log audit, host security management	Cloud customer / CSP	Cloud customer / CSP	Cloud customer / CSP
Security O&M	Security operations center (SOC), security situation awareness (SSA), web vulnerability scanning, system vulnerability scanning, security event monitoring, baseline configuration check, and security audit	Cloud customer / CSP	Cloud customer / CSP	CSP

Cloud customer

CSP

3.2 クラウドサービスシステムのセキュリティ技術要件と実装方法

3.2.1 インフラストラクチャセキュリティ

3.2.1.1 物理セキュリティ

セキュリティ技術要件:

- 環境セキュリティには、関連する物理的ダメージの脅威と物理的アクセスのリスクに対する保護が必要です。デバイスセキュリティには、システム、建物、関連するインフラの保護が必要です。

実装ガイド:

- 自然災害（洪水や地震など）や不可抗力によるサービスの中断やデータの損失を防ぐために、総合的な物理的セキュリティ対策、管理、リスク制御を実装します。
- インフラ保護には、物理的な場所の選択、物理アクセス制御、盗難 / 損傷 / 落雷 / 火災 / 水 / 湿気 / 静電気に対する保護、温湿度制御、電源、電磁気の保護が含まれます。
- 物理セキュリティの実装ガイドの詳細については、TIA-942 Telecommunications Infrastructure Standard for Data Centers [9] を参照してください。

3.2.1.2 ネットワーク セキュリティ

セキュリティ技術要件:

- ネットワーク境界保護に対して、システムはクラウドネットワークに出入りする情報をフィルタリングし、管理ネットワークの最大トラフィックとクラウドコンピューティングプラットフォームのユーザあたりのネットワーク接続数を制限し、管理ネットワークへの管理者のアクセスを制御します。サービスネットワークと管理ネットワークの不当なリンクを検出してブロックします。システムは、境界管理デバイスの管理対象インタフェース上のアクセス制御リスト（ACL）もしくはトラフィックフローポリシーを自動的に更新し、悪意のある仮想マシン（VM）を隔離し、DDoS攻撃から防御し、トラフィックを監視し、攻撃と境界への侵入を検知します。

- ネットワーク通信セキュリティに対して、システムは、データ送信の機密性、完全性保護、および信頼できるアクセス保護を可能にするために、異なるセキュリティレベルのエリア間の安全な送信をサポートする必要があります。クラウドコンピューティングリソースにアクセスする前に、ユーザを認証および認可することができます。インターネットを介したクラウドコンピューティングプラットフォームの物理ネットワークへの直接アクセスは禁止されています。信頼できるサードパーティのセキュリティ製品へのアクセスを可能にするために、オープンインタフェースを提供する必要があります。

実装ガイド:

- ファイアウォール、IDS/IPS、トラフィック制御、セキュリティゲートウェイ、DDoS対策デバイスなどのセキュリティデバイスは、セキュリティの構成とセキュリティゾーンの区分に基づき、セキュリティゾーンの境界に配置されます。セキュリティポリシーは、ネットワーク境界を保護するためにセキュリティゾーンを管理するように設定されています。さらに、コアスイッチとボーダーセキュリティデバイスは冗長モードで配置され、ロードバランサも配置されます。このアプローチにより、主要なネットワークデバイスは、ピーク時のサービス要求を満たすために冗長なサービス処理機能を可能にします。
- セキュリティアクセスプラットフォームは、すべてのユーザがVPNを通じてリソースにアクセスできるように、ユーザとクラウドコンピューティングリソースの間にVPNシステムを展開するように構築されています。暗号化された通信はデータ伝送の機密性と完全性を保護します。 VPNおよびアクセス認証管理システムは、データの改ざんやデータの盗聴を防ぐために、リモートアクセスおよびリモートアクセスユーザーに暗号化されたデータ転送を提供するために導入されています。
- 著者は、VPNに代わるものとして Software Defined Perimeter（SDP）アーキテクチャを展開することを強く推奨します。SDPは、ネットワークへのオールオアナッシングアクセス制御のような従来のVPN製品の制限を克服しながら、VPNの利点（メッセージの機密性と完全性）を提供することができます[4]。

3.2.2 仮想化セキュリティ

3.2.2.1 仮想化プラットフォームのセキュリティ

セキュリティ技術要件:

- 仮想化プラットフォームセキュリティの場合、プラットフォームはAPIセキュリティとVM/コンテナのテナント分離をサポートする必要があります。仮想化プラットフォーム上のリソースデータの完全性と機密性を保証するためにセキュリティ強化が必要です。

4. Software Defined Perimeter for Infrastructure as a Service, **https://cloudsecurityalliance.org/artifacts/sdp-for-jaas/**
Infrastructure as a Service のための Software Defined Perimeter, **https://cloudsecurityalliance.org/artifacts/sdp-for-iaas/**

実装ガイド:

- API セキュリティのポリシー設定がサポートされています。クラウド利用者がサードパーティのセキュリティ製品にアクセスしたり、クラウドプラットフォーム上のサードパーティのセキュリティサービスを選択したりできるように、オープンインタフェースまたはセキュリティサービスを提供する必要があります。
- 仮想化レイヤセキュリティ技術を用いて、仮想化リソースの分離、クラウドプラットフォームのセキュリティ強化、VPC、VDC、セキュリティグループなど、クラウド仮想化環境のセキュリティを確保します。
- クラウドプラットフォームの安全な運用管理を可能にし、クラウド環境におけるネットワークの脅威と脆弱性に対処するために、Security information and event management（SIEM）、セキュリティコンプライアンス管理、脆弱性管理を強化する必要があります。
-

3.2.2.2 仮想ネットワークセキュリティ

セキュリティ技術要件:

- マルチテナントネットワークサービス*（訳注：マルチテナント環境におけるネットワークサービスについて触れていると解釈する）*の安全な分離が必要です。ネットワークリソースとネットワークトポロジは、集中的に更新および監視できる必要があります。システムはDDoS攻撃に対する防御を提供する必要があります。セキュリティレベルの異なるエリア間の通信中は、安全な伝送がサポートされる必要があります。

推奨される実装ソリューション:

- クラウドプラットフォーム上のすべてのアプリケーションを保護するために、総合的なネットワーク境界セキュリティ保護ソリューションを提供します。クラウドシステムネットワークの安全で信頼性の高い運用を保証するために、システムネットワークを複数の独立したセキュリティゾーンに分割し、各セキュリティゾーンの機能に基づいてさまざまな保護対策を選択してください。基幹末端トラフィック（north-south traffic）と末端間トラフィック（east-west traffic）の間の安全な分離は、通常のネットワーク通信とネットワークを介して送信される情報のセキュリティを確保するために実装します。
- マルチテナントの仮想ネットワークリソースは、スイッチVLANおよびファイアウォールの隔離設定後に、仮想ローカルエリアネットワーク（VLAN）/仮想拡張LAN（VXLAN）およびVPCを通じて隔離されます。さらに、ネットワークリソースの過剰使用を防ぐために、クォータとQoSがスイッチまたは仮想スイッチに設定されます。安全なアクセスプラットフォームは、VPNシステム、アクセス認証管理システム、モバイルセキュリティ管理システム、およびファイアウォールシステムを展開するために構築します。このプラットフォームは、データの改ざんやデータの盗聴を防ぐために、リモートアクセスユーザーにリモートアクセスと暗号化されたデータ転送を提供します。
- SDPはVPNの代替としてリモートアクセスを実現します。SDPアーキテクチャにより、組織は攻撃対象面を減らし、生産性を高め、組織間のコラボレーションを促進しながら、オンプレミスのインフラストラクチャ、クラウドインフラストラクチャ、ユーザの全体をカバーする集中型のポリシー駆動型ネットワークセキュリティプラットフォームを構築できます[5]。

- ウイルス対策ゲートウェイは、ウイルス対策機能を提供するために設置します。ゲートウェイは、HTTP、FTP、電子メールなどの一般的なアプリケーションプロトコルに基づいてウイルスを検出し駆除します。ウイルスが、インターネットアクセスやリモート運用管理を介してクラウドプラットフォームにアクセスするのを防止したり、クラウドプラットフォーム上で拡散するのを効果的に防止します。
- ファイアウォールにより、マルチテナント間と、同じテナントの異なるサービス間でアクセス制御ポリシーを柔軟に設定します。
- 侵入防止システム（IPS）が出入り口に配置され、基幹から末端（north-south）および末端間（east-west）の侵入を防ぐためにトラフィックを詳細に検出します。IPS は、アプリケーショントラフィックの詳細な分析と検出も行います。IPS は、攻撃機能のナレッジベースとユーザルールを利用して、リアルタイムで大量のネットワークトラフィックにおけるウイルス、攻撃、悪用を効果的に検出してブロックします。さらに、ネットワークアプリケーション層を保護するために、ネットワーク内に分散されているさまざまなトラフィックを管理します。
- 機密データの誤用や漏洩を検出して防止するために、データ漏洩/検出防止（DLP）を配備します。
- トラフィックベースのDDoS攻撃（UDPフラッドやTCP SYNフラッドなど）、アプリケーションベースのDDoS攻撃（CC、DNSフラッド、低速接続枯渇など）、DoS攻撃（LAND、ティアドロップ、Smurfなど）、不正なプロトコル攻撃（IPフロー、TCP packet without flag、FIN bit with no ACK bit、クリスマスツリーなど）を検知して防御するために、インターネットの出口にDDoS対策デバイスを導入します。

5. Software Defined Perimeter for Infrastructure as a Service, **https://cloudsecurityalliance.org/artifacts/sdp-for-iaas/**

3.2.2.3 仮想ストレージのセキュリティ

セキュリティ技術要件:

- データの盗難を防ぎ、データのセキュリティを確保するために、異なるVM上のユーザーデータは仮想化層で分離します。システムはデータロケーションとホームロケーションを管理し、バックアップとサービスの継続性をサポートします。

実装ガイド:

- 仮想化環境でデータストレージのセキュリティを確保するために、データ分離、アクセス制御、データの信頼性、残余情報保護(residual information protection)を使用します。
- データの盗難を防ぎ、データのセキュリティを確保するために、異なるVM上のユーザーデータは仮想化層で分離します。
- ハイパーバイザーは、VMが割り当てられたスペースにのみアクセスするようにして、複数のVMのハードディスク上の分離を実現します。
- ボリュームストレージのセキュリティ： システムは各ボリュームのアクセスポリシーを指定します。指定されたボリュームにアクセスできるのは、権限を与えられたユーザだけです。ボリュームはお互いに分離されます。
- 残余情報の保護： データ拡張技術をデータストレージに適用すると、システムはストレージプールを複数の小さなデータブロックに分割し、これらのデータブロックを使用してRedundant Array of Independent Disks（RAID）グループを構築します。これにより、データをストレージプール内のすべてのハードディスクに均等に分散させることができ、リソース管理はデータブロック単位で実装されます。
- VM やボリュームが削除されると、システムはリソースを再利用し、小さいデータブロックのリンクリストがリソースプールに解放されます。これらの小さなデータブロックは、ストレージリソースが再利用されると再編成されます。そのため、再割り当てされた仮想ディスクから元のデータを復元する可能性が低くなり、それが残余情報の保護に役立ちます。
- システムがリソースを回収すると、データのセキュリティを確保するために論理ボリュームの物理ビットをフォーマットすることができます。
- データセンターの物理ディスクが交換された後、システム管理者はデータ漏洩を防ぐためにディスクを消磁または物理的に破壊します。
- 一方向性ハッシュアルゴリズムは、イメージとスナップショットデータの完全性を保証するために使用されます。
- 保存データの信頼性保証：信頼性メカニズムを採用しています。ハードディスクなどの記憶装置に障害が発生してもデータが失われたりサービスが影響を受けたりしないように、バックアップデータのコピーが1つ以上保存されます。

3.2.3 ホストセキュリティ

クラウドホストセキュリティ保護： ホストセキュリティサービスモジュールはクラウドプラットフォーム上で事前に準備されており、Security as a Service （SECaaS）として必要に応じて購入および使用できます。通信事業者やユーザは、外部のシステムやリソースを購入する必要がなく、ホストセキュリティサービスを迅速に展開し、セキュリティ機能を開発できます。

セキュリティ技術要件:

- ホストウイルス対策および悪意のあるコードの防止
- ホスト侵入検知と防御
- ホストセキュリティの強化とパッチ管理

3.2.3.1 ホストウイルス対策

実装ガイド:

- ウイルス対策エンジンは、VMとサーバのスキャン結果をキャッシュして共有し、スキャン効率を向上させるために増加した部分のみのスキャンを実行します。さらに、ローカルのウイルス対策エンジンはエクストラネットに接続せずにウイルス対策効果を高め、ローカルの仮想化環境を最適化することができます。

3.2.3.2 ホスト侵入防止

セキュリティ技術要件:

- 一般的なDoS攻撃、バッファオーバーフロー攻撃、バックドア型トロイの木馬、外部システムからのWeb攻撃を検出して防止します。クラウドホストのシステムとアプリケーションの脆弱性は、外部からの攻撃から保護されます。

実装ガイド:

- クラウドホストのセキュリティ保護コンポーネントとして、クラウドホストがリソースプール内の任意のホストマシンに移動した場合、クラウドホストファイアウォールは安定した効果的な保護ポリシーを提供します。ファイアウォールは、クラウドホストから他のクラウドホストへのアクセスも制御します。顧客のサービス要件に基づいて、IPアドレス、ポート、プロトコル、方向に基づいてクラウドホスト間のファイアウォールに対してきめ細かいアクセス制御ポリシーが作成され、セキュリティゾーンのセキュリティ標準に基づいてクラウドホストにまとめて配信されます。

3.2.3.3 ホストセキュリティ強化

実装ガイド:

- 脆弱性、安全でないユーザーアカウントやパスワード、不適切な構成と操作、安全でないサービスは、ウイルス、トロイの木馬、ワームの形で潜在的なセキュリティ上の脅威をもたらします。脆弱性を狙ったハッカーの攻撃を防ぐために、次のOSのセキュリティ強化方法を提供します:
  - 未使用の通信ポートを無効にする
  - 不要なサービスプロセスを無効にする
  - システムアクセス許可を制限する
  - アカウントの権利を厳密に管理する
  - セキュリティログ監査機能を有効にする
  - SANS、NIST、OS開発者自身によるベストプラクティスに従って、OSとデータベースを強化する
- OSセキュリティには、コンピューティング環境のID認証、アクセス制御、セキュリティ監査、仮想化セキュリティ、データの機密性と完全性、データのバックアップとリカバリ、イメージとスナップショットのセキュリティ、オブジェクトセキュリティの再利用、侵入検知、悪意のあるコードの防止などの仮想リソースに対するセキュリティ強化が必要です。

3.2.4 ミドルウェアセキュリティ

3.2.4.1 コンテナセキュリティ

セキュリティ技術要件:

- 基盤となる物理インフラストラクチャ（コンピューティング、ネットワーク、ストレージ）とマネージャのセキュリティを確保する必要があります。コンテナリポジトリは適切に保護され、適切なアクセス制御が設定されている安全な場所に配置する必要があります。

実装ガイド:

- セキュリティ機能は、コンテナ内で実行されているアプリケーション/タスク/コードに基づいて開発されています。場合によっては、脆弱なソフトウェアがコンテナ内で実行される可能性があり、それによってOSや他のコンテナからのデータが危険にさらされる可能性があります。ネットワークやイメージ/コンテナを含むコンテナ環境は安全に設定する必要があります。

3.2.4.2 APIセキュリティ

セキュリティ技術要件:

- システムは、APIライフサイクルとセキュリティポリシー管理、APIリクエスト管理、IAM、バックグラウンドサービスによるAPIリクエストの有効性検証、および監視とログデータのセキュリティ分析をサポートする必要があります。

実装ガイド:

- API認証：システムにアクセスするユーザが認証済みユーザであることを確認することが目的です。この機能は、実際のユーザ、コンピューターシステム、APIが提供する機能を使用する必要があるアプリケーションに適用できます。OpenAPI認証では、サードパーティのアプリシステム、アプリ開発者、アプリユーザー、システム管理者など、ユーザーロール間の関係を考慮する必要があります。
- APIセキュリティ監視：システムは、API呼び出し回数、遅延、エラー率などの指標の監視を可能にしなければなりません。
- APIログと監査：
  - APIライフステータス管理の操作ログやアプリ購入(subscription)ログなど、管理プレーンのログは記録する必要があります。
  - 支払いや課金に用いられるAPIの呼び出しなど、データプレーン上での重要なAPIの呼び出しログは、サービス提供者によって記録される必要があります。

- データプレーン上での一般的なAPIの呼び出しログは、大きな割合を占めており、実際の状況に基づいて記録されるべきです。

- APIデータセキュリティ：機密データや個人データの漏洩は、顧客を失い、サービスに影響を与え、個人のプライバシーを漏洩することがあります。そのため、API開発において、機密情報や個人データの保護は、伝送中のデータ保護と安全なデータ保存を含め、優先事項です。
- APIデータ伝送のセキュリティ：伝送中の機密データや個人データのセキュリティを確保するために、システムは通常伝送されたコンテンツの暗号化、つまり、HTTPSを使用します。
- APIセキュリティポリシー管理：セキュリティポリシー管理によって、ユーザはAPIを変更し、APIの動作を監視することができ、APIアクセスの競合制御、パフォーマンス、セキュリティ機能を強化できます。
- APIセキュリティ分析：API呼び出しログは、潜在的な侵入操作を検出し防御するために分析されます。

3.2.4.3 データベースセキュリティ

データベース監査により、コア・データベースに入出力されたトラフィックをパケットフィールド・レベルで解析することができ、操作内容を完全に復元し、操作の詳細な出力結果を提供することができます。このようにして、全てのアクセスは管理者に視覚的方法で示され、それによりデータベースは管理され、データの脅威を迅速に検出して処理することができます。
データベースの監査は以下の機能を持っています：イベント前のセキュリティリスクの評価、リアルタイムな動作監視、きめ細かなプロトコル解析と双方向の監査、Webサービスの監査、アプリケーションの3つの層の関連性の監査、柔軟な監査ルール、豊富なアラーム方法、効率的な動作の検索、レポートシステム、実際のシナリオのセッションベースの再生。

3.2.4.4 リソース管理プラットフォームのセキュリティ

セキュリティ技術要件：

- システムは、コードのセキュリティテストと欠陥の修正をサポートするべきです。
- システムは、セキュリティ強化をサポートするべきです。
- システムは、攻撃行動を監視し、アラームを発生させるべきです。攻撃を検出した場合、システムは、IPアドレス、攻撃の種類、目的、時間を記録します。
- システムは、悪意のあるコードを検出して処理するべきです。
- システムは、管理ネットワークへの管理者のアクセスを制御し、不当なリンクを検出してブロックする必要があります。
- コードの開発段階で、ソフトウェアコーディングのベストプラクティスが強制される必要があります。
- より望ましいのは、サードパーティベンダーによってコードが監査/検証されることです。
- システムは、イメージに基づいて作成され、コンテナに配備され、自動的に拡張されるインスタンスを動的に有効にするべきです。これらのインスタンスが不要になった場合は、それらを無効にし、アプリケーションスタックを破壊しないようにします。
- 実行中のシステムにパッチを適用すべきではありません。代わりに、それらを新しい正式なバージョンに置き換えます。
- システムは、マルチテナント間でサービスリソースを安全に分離する必要があります。テナントは、自身のサービスリソースにのみアクセスして操作することができます。
- システムはマルチテナントのデータを安全に分離するべきです。テナントは、自身のデータにのみアクセスして操作することができます。
- テナントは、データのバックアップ、データのエクスポート、データリセットの権限を定義し設定することができます。

実装ガイド：

- リソース管理プラットフォームは、許可されていないイベントと不審なイベントを評価、検知、対処し、クラウド環境のコンプライアンス状況を監視し、セキュリティパッチの適用を管理します。SIEM、セキュリティコンプライアンス管理、脆弱性管理は、クラウドプラットフォームの安全な運用と管理を可能にするために強化されるべきです。
- 仮想化レイヤーは、ホストと他のVMからVMを分離します。従来のセキュリティ保護装置は、VM間の悪意ある攻撃を防ぐことはできないので、仮想化レイヤーのセキュリティ要件を満たすことができません。仮想化レイヤーのセキュリティ技術は、クラウド仮想化環境のセキュリティを確保するために使用します。技術的対策は、仮想リソースの分離、クラウドプラットフォームのセキュリティ強化、VPC、VDC、セキュリティグループを含め、仮想化プラットフォームで実装します。

3.2.5 アプリケーションシステムのセキュリティ

セキュリティ技術要件：

- システムは、ユーザ管理ID認証、アカウント管理、ロール認証、APIアクセスのセキュリティ、サービス管理プレーンの分離、Webセキュリティ、行動の監査をサポートするべきです。クラウドセキュリティサービスプロバイダは、Web攻撃防御、クラウドWAF、クラウドWTP、二要素認証サービスを提供します。

実装ガイド：

- IAM：アプリケーションシステムプラットフォームは、アプリケーションユーザに対し、管理ID認証、アカウント管理、ロール認証、APIアクセスセキュリティ、サービス管理プレーンの分離を実施する必要があります。
- ウェブコードのセキュリティ保護：ウェブコードのセキュリティメカニズムは、入力と出力の有効性チェックや、認証、権限、セッション、Webサービス、インジェクションの脆弱性を防ぐための対策などをサポートします。このシステムはまた、Web経由でのリソースへのユーザアクセスを制御し、リモートからのWebアクセスを安全に伝送することをサポートしています。
- ウェブ攻撃防御：ウェブ攻撃防御機能は、イベント前の検出、イベント中の保護、イベント後の分析をカバーする総合的なWebセキュリティ・ライフサイクル・ソリューションを実装するために開発します。クラウドの監視は、イベントの前にユーザのウェブサイトの脆弱性を監視するために使用し、ゼロデプロイメント（zero-deployment)クラウド保護ソリューションは、イベント中に使用します。
- DDoS攻撃とCC攻撃に対する防御：DDoS攻撃防御には2つの種類があります。一つはローカルに配置された専用の保護装置で、大量のトラフィックによるDDoS攻撃から直接守ることができます。DDoS攻撃のトラフィックがローカルの保護制限値を超えた場合、問題を解決するために専門のセキュリティサービスプロバイダが提供するクラウドスクラビングセンターを使用することができます。対DDoS/CCアルゴリズムは、DDoS攻撃の可用

性の問題を解決し、安定的な運用が出来るようにSSAシステムを強化するために使用します。

- WAFシステム：ルールベースの保護は、SQLインジェクション、クロスサイトスクリプティング、OSコマンドインジェクション、リモートファイルインクルード、ローカルファイルインクルード、ディレクトリトラバーサル、HTTPプロトコル違反、WebShell攻撃を含む既知の多くの攻撃に対して、正確かつきめ細かな防御を提供します。このアプローチは、ウェブサイトを保護します。
- システム：Webページがハッカーやスタッフによって不正に変更された場合、WTPソフトウェアは、ウェブサイトが通常稼働出来るように、リアルタイムに変更されたWebページを復元することができます。また、このソフトウェアは改ざんイベントに関する情報を記録しており、セキュリティ部門による調査の際に証拠として使用することができます。

3.2.6 データセキュリティ

セキュリティ技術要件：

- データのセキュリティは重要です。鍵または機密データ（静的および動的）は保護されなければなりませんし、データ漏洩や破損のリスクは、クラウド上のサービスシステムの信頼性とセキュリティを確保するために最小化されなければなりません。ネットワーク伝送の間、データの完全性、機密性、有効性が、中断、複製、改ざん、偽造、傍受、監視されないようにしなければなりません。

実装ガイド：

- データの漏洩を防ぐために、データが保存時および伝送時に暗号化される必要があります。クラウドは、異なるテナント間のデータの分離と安全な共有を保証すべきです。伝送セキュリティ、データストレージセキュリティ、災害復旧やバックアップ、その他の技術的手段は、データのセキュリティを強化するために使用します。データベース監査システムは、データベースサーバへのアクセスの動作を監査します。データの分離、アクセス制御、データの信頼性、残余情報保護は、仮想化環境でのデータストレージセキュリティを確保するために使用します。利用者が鍵へのアクセスを保持できる方が望ましいです。
- データ伝送のセキュリティ：HTTPSは機密データを含むページに使用され、SSL / TLSベースの伝送経路は、システム管理者が管理システムにアクセスするために使用します。ユーザがVMにログインする際、SSHとRDPが採用されます。利用者がリモートクラウドの運用管理システムにアクセスする際、SSL VPNが使用されます。暗号化プロトコルを使用してログインすることは、暗号化伝送およびID認証を可能とし、データが正しいクライアントとサーバに送信される事を保証し、伝送中のデータの盗難を防ぎ、データの完全性を保証します。HTTPS証明書は更新し管理することができます。IaaSモードのテナントによって配備されたアプリケーションプラットフォームシステムは、自身で証明書を生成し管理するか、もしくはCSPから証明書管理サービスを購入することができます。アプリケーションプラットフォームはまた、CSPストレージとデータ送受信する際のHTTPSのように、クライアントとしての暗号化を有効にすることもあります。Webアプリケーショ

ンが、狙いを定めた攻撃者（インターネットからアクセス可能な機密データを扱うアプリケーションにとっての一般的な脅威モデル）の対象となる可能性がある場合は、よく知られた暗号モジュールによるTLSサービスを使用することを強くお勧めします。

- データストレージセキュリティ：IaaSモードの利用者によって配備されたアプリケーションプラットフォームシステムは、自身で鍵を生成し管理するか、もしくはCSPから鍵管理サービスを購入することができます。鍵/認証資格情報の機密データは可逆的に暗号化され、パスワードは非可逆的に暗号化されます。このアプローチは、データがファイル、データボリューム、システムボリュームに保存される際に、データのセキュリティを保証します。
- データの完全性の検証：システムは、完全性の検証が必要な鍵/機密データサービスのシナリオを特定します。データは保存中に電子的に署名され、データが使用される前に完全性チェックが行われます。
- データのバックアップと復元機能：ミドルウェアセキュリティのモジュールの中のデータベースセキュリティおよびインフラストラクチャセキュリティのための災害復旧およびバックアップ対策を参照してください。

3.2.7 セキュリティマネジメント

3.2.7.1 ネットワーク監査

セキュリティ技術要件：

- クラウドの利用者が異常な操作により、または異常なサービスのためにホストを使用してネットワーク性能に影響を与える場合は、監査に備えてネットワーク資源の利用を記録し元に戻すために、技術的な機能を整えるべきです。

実装ガイド：

- リアルタイムトラフィックの中でコンテンツを記録(restore)するには、ネットワーク監査システムを、インターネットおよびイントラネットの境界点にあるコアスイッチにオフラインモードで配備し、トラフィックをモニタリングします。システムは、HTTP, SMTP, POP3, RDP, FTP, NFSといった数多くの汎用アプリケーションプロトコルのトラフィックを識別し、その内容と挙動に関する監査記録を保持(restore)し、セキュリティリスクを適時に検出するとともにネットワーク資源の利用を最適化します。さらに装置はトラフィック分析機能を提供し、運用管理担当者がネットワーク帯域の利用状況を把握して解析し、問題を発見してネットワークを最適化することに貢献します。

3.2.7.2 ネットワーク挙動管理

セキュリティ技術要件：

- 利用者が機微情報をネットワーク経由で送信し、フォーラムの中で不適切な発信をし、監督者が禁ずる行為を行った場合は、ネットワーク資源の使用状況とネットワークの挙動を記録し保存(restore)するために、技術的な機能を構築するべきです。

実装ガイド：

- オンラインの挙動管理メカニズムをセキュリティゾーンの境界に配置します。セキュリティ管理センターが中央から挙動を管理し、規則違反が確認されたらアラームを発します。CASBを利用することで、クラウドアプリの可視性、リスクインテリジェンス、データガバナンス、利用者挙動分析(UBA)、許可されたクラウドアプリに対するポリシー適用が可能になります。また無許可のクラウドアプリについては、リアルタイムUBA、データセキュリティ、脅威に対する保護を実施するとともに、クラウドアプリを適法に利用するためのクラウドデータの暗号化やトークナイゼーションを提供します。

3.2.7.3 トラフィック制御の管理

セキュリティ技術要件：

- クラウドのインターネット領域にあるWebサーバはWebサイトを運用します。ある一定の時

間内に、巨大な量の通常のアクセス要求が起こり、単一ホストでは大量の同時リクエストを迅速に、信頼性を保って、セキュアに処理することができない可能性があります。クラウド上の主要なアプリケーションであるWebサイトでは、システムは、単一障害点（Single Point of Failures, SPOFs）によって起こるサービス停止リスクを除去しなければなりません。同様に、エクストラネット領域で運用されるOAシステムは、ホストの過負荷やサーバのSPOFsによって引き起こされるリスクに直面しています。

実装ガイド：

- コアスイッチにアプリケーションロードバランサーをバイパスモードで配置して第2層から第7層までのレイヤーにフローコントロールを提供します。この方式により、大量データトラフィックとネットワーク過負荷の問題を的確に捉え、SPOFsにより生じるデータトラフィックのロスを防止します。ロードバランサは複数の間欠接続型ロードバランスアルゴリズム、ポーリング、重みづけラウンドロビン(WRB)、コネクション最小化、最短レスポンス時間等を備え、また、IPキープアライブ、一貫性クッキー、QOSクッキー、QoS URL、QoSホストネームといった継続型ロードバランスアルゴリズムをサポートしています。

3.2.7.4 鍵と証明書

セキュリティ技術要件

- システムは、管理者(admin)のネットワークデバイス(仮想化ネットワーク上のデバイスを含む)のログインアドレスを制限し、デバイスのログイン失敗を管理し、それらのネットワークデバイスの管理者のアイデンティティを認証するために2要素以上の多要素認証を用います。同時に、リモート管理用デバイスの安全な転送を実装し、特権コマンドを制限し、管理者権限を最小化し、ログ記録と監査レポートをサポートします。

実装ガイド：

- クラウドプラットフォーム、セキュリティ対策装置、ネットワークデバイス、サーバ、ストレージ資源のアカウント、認証、認可、監査は中央で管理します。システムは運用管理権限の管理と包括的ログ管理を提供し、グラフィックターミナル、キャラクター端末、データベースアプリケーション、ファイル転送をサポートします。また、リアルタイムのビデオ監視とスクリーン録画を提供して、削除やリスタートといったハイリスクの操作を適時にブロックします。システムはまた、携帯電話型トークンもしくはハードウェアトークンとパスワードによる強力な2要素認証を実装し、システムの当者と特権アカウントのセキュリティを確保します。

3.2.7.5 アイデンティティ認証管理プラットフォーム

セキュリティ技術要件：

- システム利用者のアイデンティティは統一した方式で管理します。サービス管理部署によって、各個人はいくつかのタイプまたはグループに分類され、モジュールに対する異なるアクセス権を付与されます。アクセス権は、一般ユーザ、システムアドミン、セキュリティアドミン、監査アドミンといった役割（ロール）に基づいて設定されます。

実装ガイド：

- 統合されたネットワーク管理システム(NMS)を配備し、資源とシステムの運転の設定、操作、管理を行います。

3.2.7.6 データベース監査

セキュリティ技術要件：

- データセキュリティは重要です。クラウド上のサービス用システムの信頼性とセキュリティを確実にするために、重要なもしくは機微なデータ(静的であれ動的であれ)を保護し、データ漏洩のリスクと損害は最小限にしなければなりません。データベース監査システムは、データベースサーバへのアクセスにおける振る舞いを監査するのに用います。

実装ガイド：

- データベース監査システムには、様々な機能が備わっています。そこには静的監査、リアルタイムモニタリングとリスクコントロール、リアルタイム監査、双方向監査、監査ルール、振舞検索、関連性監査、監査レポート、セキュリティイベント調査、監査目標管理、警告管理、システム設定管理などを含んでいます。データベース監査システムは、データフローのミラーリングにより、すべてのデータベースへのアクセスを監査できます。
- データベース監査システムは、データベース操作における規則違反を検知するのに役立ちます。データベース監査システムは、ネットワーク上のデータを収集、分析、同定し、ネットワークからデータベースにアクセスする全ての操作をリアルタイムでモニターし、ユーザが定義するコンテンツに関するキーワードをサポートし、ユーザが指定するプロトコルのモニタリングを行い、ユーザが指定するポートのモニタリングを行い、それらによりデータベース操作に関するコンテンツのモニタリングと識別を実施します。
- 権限/許可外のデータベースアクセスに対して、データベース監査システムは、複数の方式によるアラームを適時に報じることができ、権限/許可外のデータベースアクセスの全プロセスを記録(restore)することができます。これはセキュリティイベントを、その全プロセスに亘って正確にトレースし特定するのに役立ち、データベースのセキュリティを確かなものにします。統合分析と包括的かつシステマティックなレポーティングの機能により、データベース監査システムは、データベースアクセスの包括的セキュリティ分析レポートをユーザに提供できる。

3.2.7.7 クラウドログ監査

セキュリティ技術要件：

- ログ監査システムは、システム内の構成要素のセキュリティ監査の仕組みを中央で管理するために配備されています。ログ監査システムは、監査記録をセキュリティ監査ポリシーに基づいて分類し、それに対応するセキュリティ監査の仕組みを時間帯ごとに機能させもしくは機能停止させ、監査記録の保存、管理、問合せを行います。ログ監査システムはまた、セキュリティ監査人について厳格なアイデンティティ認証を行い、監査人がセキュリティ監査のための操作を行う際に、特定のコマンドやインタフェースだけを用いるように管理します。

実装ガイド：

- ログモニタリング：ログモニタリングシステムは、最新のログリストやシステムのリスク状態といった、受信したイベントの状態をリアルタイムでモニタリングします。また、デバイスの稼働中のパラメータをモニターして、デバイスとネットワークの状態を判断します。さらに、ログトラフィックやシステムリスクやその他の変化傾向のリアルタイムおよびグラフィカルモニタリングもサポートします。
- ログ管理：ログ管理システムは、複数のログのフォーマットを統一された方式で管理します。SNMP、Syslogその他のログインタフェースを用いて、管理対象のログ情報を収集します。ログ情報は、次に、管理、分析、アラームレポートのために、統一されたフォーマットに変換されます。ログ管理システムは、自動的にログデータを関連付け、分類し、またデータストレージ、バックアップ、リカバリ、削除、インポート・エクスポートといった操作をサポートします。下位の管理センターのログデータは、中央集中管理のために、上位の管理センターに送られることがあります。
- セキュリティイベント分析：中央集中方式の監査では、複数のセキュリティイベントを統合することができ、統合された監査結果に基づいてユーザごとに特別のレポートを提供できます。レポートはすべてのネットワーク状況を包括的に反映し、またカギとなるポイントに光を当てることで理解が容易になります。
- ログ管理システムは、パケットフィルタログ、プロキシログ、侵入攻撃イベント、ウイルス侵入イベントの統計を収集し、解析し、分析レポートを作成します。ログ管理システムは、統計的分析を、デバイスの稼働状況および管理操作に基づくセキュリティデバイスの管理情報に組み入れます。また、アクセスのトラフィック、侵入攻撃、メールフィルタリングログ、ソースアドレス、ユーザアクセス管理ログといった複数の要素に基づいた統計的分析も提供します。さらに、侵入攻撃のログは、侵入攻撃イベント、ソースアドレス、攻撃対象ホストに基づいて分析し、傾向分析チャートを生成することもできます。

3.2.7.8 ホストのセキュリティ管理（踏み台（Bastion）ホスト）

セキュリティ技術要件：

- クラウドプラットフォームは、中央管理型で統一されたアクセス管理ポリシーを備える必要があり、それはアイデンティティ認証と認可、操作履歴監査、ユーザ利用記録が可能であり、それにより、不正な操作や許可の悪用や運用管理要員の誤操作による、実運用システムへのインパクトを防止できるものである必要があります。操作記録は、誤動作の回復やトラブルシューティングに利用することができます。

実装ガイド：

- 運用管理用の踏み台ホストを管理用区域内に配備し、クラウドプラットフォーム、セキュリティ装置、ネットワークデバイス、サービス、ストレージ資源に対するアカウント管理、認証、認可、監査を実施できるようにします。このシステムは運用管理の権限管理と包括的なログ監査機能を備え、グラフィックターミナル、キャラクター端末、データベースアプリケーション、ファイル転送をサポートします。このシステムはまた、リアルタイムのビデオ監視とスクリーン録画を提供して、削除や再起動といったハイリスクの操作を適時にブロックします。踏み台ホストは運用管理ログの監査目的で配備することもできる。

3.2.8 セキュリティの運用管理

3.2.8.1 SOC

セキュリティ技術要件：

- セキュリティ管理プラットフォームの全体的アーキテクチャを計画し、次の事項の設計を行うようにします：コンプライアンス分析、イベント処理、脆弱性分析、脅威インテリジェンス、イベント相関分析およびイベント処理機能。

実装ガイド：

- SOCは状況把握機能（大画面ディスプレイ）、脆弱性管理、SIEM、脅威インテリジェンス、イベント処理モジュールを備えています。ユースケースを描くには、GSCのようなセキュリティ集中管理の機能や訓練が役に立ちます。*（訳注：GSCはGlobal Service Centerの略と判断してこの訳とした。）*

3.2.8.2 SSA

セキュリティ技術要件:

- クラウド利用者のサービスシステムのセキュリティを確保するために、超大容量のデータに対する*（訳注： 想定を超える量のデータのことを意味していると解釈）*クラウドセキュリティ監視システム、すなわちSSAシステムは、定期的に大量のクラウドアプリケーションの脆弱性を自動的にチェックすることで、クラウドシステムのセキュリティ問題をできるだけ早く検知することを保証し、クラウドシステムのセキュリティ管理およびサービス機能を改善できるようにします。SSAシステムは、安全で信頼できるクラウド運用をサポートするための優れたクラウド環境も構築できます。

実装ガイド:

- 継続的なサービス品質監視は、サイトが利用可能であり、サービスを正常に提供できることを保証するために、クラウド上のすべての重要なサイトおよびアプリケーションに実装されています。さらに、定期的なWebサイトセキュリティ監視サービスがこれらのサイトおよびアプリケーションに提供され、ネットワークセキュリティの問題やイベントを迅速に検出し特定します。ネットワークセキュリティ問題とイベント検出機能には、Webサイトの脆弱性検出、Webサイトの可用性監視、Webサイトのトロイの木馬監視、Webサイトのリンク監視、Webサイトのセキュリティイベント監視、Webサイトの機微情報の監視、ネットワークホスト監視があります。

3.2.8.3 ウェブ脆弱性スキャン

セキュリティ技術要件:

- 脆弱性スキャンシステムは、特定のWebサーバのセキュリティ上の脆弱性をスキャンすることによって検出し、タイムリーなセキュリティ保護を提供するために、クラウドプラットフォーム上に展開されます。

実装ガイド:

- ウェブ脆弱性スキャンシステムは、SQLインジェクション、コマンドインジェクション、CRLFインジェクション、LDAPインジェクション、XSSクロスサイトスクリプト、パストラバーサル、情報漏えい、URLリダイレクト、ファイルインクルージョン、アプリケーションプログラム、ファイルアップロード（Webサイトの悪意のあるコードの検出とダークチェーンの検出）などのWebアプリケーションの脆弱性を検出するのに役立ちます。システムはまた、脆弱性を検証し、ウェブサイトのセキュリティを監視し、そして死活状態を検出します。

3.2.8.4 システム脆弱性スキャン

システム技術要件:

- 脆弱性スキャンシステムは、特定のVMまたは物理マシンのセキュリティ脆弱性（侵入攻撃などの攻撃を開始する際に悪用される）をスキャンして検出し、タイムリーなセキュリティ保護を提供するためにクラウドプラットフォームに展開されます。

実装ガイド:

- 脆弱性スキャンシステムは、ファイアウォールおよび侵入検知システムと連携します。 ネットワークをスキャンすることで、プラットフォーム管理者はセキュリティ設定と実行中のアプリケーションサービスを知り、タイムリーにセキュリティ上の脆弱性を検出し、ネットワークのリスクレベルを客観的に評価することができます。
- スキャン結果に基づいて、プラットフォーム管理者はシステム内のネットワークセキュリティの脆弱性とエラー設定を修正し、ハッカーの攻撃から防御できます。これには、脆弱性スキャン、分析、修正、監査、リスクアラーム、ポリシー管理、統計分析を含みます。

3.2.8.5 セキュリティイベント監視

セキュリティ技術要件:

- システムは、プライベートクラウド上のすべてのオンライン情報システムをスキャンし、さまざまなシステムのための基本的なデータ証跡を提供するために、すべてのシステムに配備された監視デバイスおよびプライベートクラウドシステムに配備されたローカル監視エンジンを動的に振り分けることができます。

実装ガイド:

- 継続的なサービス品質監視は、サイトが利用可能であり、サービスを正常に提供できることを保証するために、クラウド上のすべての重要なサイトおよびアプリケーションに実装されます。さらに、定期的なWebサイトセキュリティ監視サービスがこれらのサイトおよびアプリケーションに配置され、ネットワークセキュリティの問題やイベントを迅速に検出し特定します。

3.2.8.6 ベースライン設定のチェック

セキュリティ技術要件:

- クラウド上には、多数のサーバ、ストレージデバイス、ネットワークデバイス、セキュリティデバイスが配備されています。これらのデバイスの設定ファイルには、弱いパスワード、バックドア、危険なポートなどのセキュリティ上の脅威が含まれている可能性があります。セキュリティ設定チェックシステムは、クラウドプラットフォーム上のサーバ、ストレージデバイス、ネットワークデバイス、セキュリティデバイスの設定ファイルを自動的にチェックし、セキュリティ上の脅威を検出し、タイムリーにユーザに通知します。CASBソリューションは、セキュリティやコンプライアンスに影響を与える設定の変更に対するリアルタイムの対応など、これらの機能の多くをサポートできます。

実装ガイド:

- セキュリティ設定チェックシステムは、次の項目に関するセキュリティベースラインチェックをサポートしています:
  - Windows Server 2012、Windows Server 2008、Windows Server 2003、Windows 7、Linux RH 5以降、CentOS 5以降、SUSE Enterprise 9などのOS
  - Huawei、Cisco、Juniper、その他のベンダーのネットワークデバイスとセキュリティデバイス
  - Oracle 9i、MySQL、SQL Server、Informixなどのデータベース
  - Tomcat、IIS、WebSphere、Apache、BINDなどのミドルウェア

3.2.8.7 セキュリティ監査

セキュリティ技術要件:

- ログ監査システムは、システム内のコンポーネントのセキュリティ監査メカニズムを集中管理するために導入されます。ログ監査システムは、セキュリティ監査ポリシーに基づいて監査レコードを分類し、対応するセキュリティ監査メカニズムを時間セグメントごとに有効または無効にし、監査レコードを格納、管理、検索します。また、セキュリティ監査人に対して厳格なID認証を行い、監査人が特定のコマンドまたはインタフェースを介してのみセキュリティ監査操作を実行できるようにします。

実装ガイド:

- ログ監視：最新のログリストやシステムリスク状況など、受信したイベントの状況をリアルタイムに監視します。また、デバイスやネットワークの状況を判断するために、デバイスの実行中のパラメータを監視します。ログトラフィック、システムリスク、その他の変

化の傾向をリアルタイムでグラフィカルに監視することを備えています。

- ログ管理：システムは複数のログフォーマットを統一的に管理します。管理対象オブジェクトに関するログ情報を収集するには、SNMP、Syslog、その他のログインタフェースが使用されます。その後、ログは管理、分析、アラームレポートのために統一フォーマットに変換されます。システムは、ログデータを自動的に解析および分類し、データの保存、バックアップ、回復、削除、インポート、エクスポート操作をサポートします。分散ログカスケード管理（Distributed log cascading management）もサポートされています。下位の管理センターのログデータを上位の管理センターに送信して一元管理できます。
- セキュリティイベント分析：集中監査はさまざまなセキュリティイベントを統合し、統一された監査結果に基づいてカスタマイズされたレポートをユーザに提供できます。レポートは、全体的なネットワークセキュリティステータスを包括的に反映しており、強調表示されている重要なポイントを使用して簡単に理解できます。システムは、パケットフィルタリングログ、プロキシログ、侵入攻撃イベント、ウイルス侵入イベントに関する統計情報を収集して分析し、分析レポートを生成します。デバイスの稼働状態とデバイス管理操作に基づいて、セキュリティデバイス管理情報の統計分析を実行します。また、アクセストラフィック、侵入攻撃、メールフィルタリングログ、送信元アドレス、ユーザアクセス制御ログなど、複数の条件に基づく統計分析もサポートされています。さらに、侵入攻撃イベント、送信元アドレス、攻撃を受けたホストに基づいて侵入攻撃ログを分析し、さまざまな傾向分析チャートを生成できます。システムは、複数の種類の監査レポートをテーブルまたはチャートに生成できます。ユーザはInternet Explorerを使用して監査結果にアクセスしてエクスポートできます。ログレポートをスケジュール通りに生成し、レビュー用に自動的に保存するか、電子メールを介して特定の受信者に自動的に送信するようにシステムを設定し、プロセスベースのセキュリティ監査を有効にすることができます。
- 運用管理セキュリティ監査：運用管理要員の行動、ネットワークデバイスとシステムリソースの異常な使用、重要なシステムコマンドの使用など、システム内の重要なセキュリティイベントが監査されます。監査記録には、イベントの日付、イベントの時刻、イベントの種類、サブジェクトID、オブジェクトID、結果を含める必要があります。さらに、記録データを分析して監査レポートを生成します。監査プロセスは、予期しない中断から保護されるべきであり、監査記録は、予期しない削除、変更、上書きから保護されるべきです。クラウドプラットフォームでは、利用者は、SECaaS拡張機能を通じて自分のリソースに関連する監査情報を収集して表示することができます。

3.3 サードパーティのセキュリティサービスプロバイダが提供するセキュリティ保証機能

2.6のサードパーティセキュリティサービスプロバイダの役割では、サードパーティセキュリティサービスプロバイダはCSPおよび利用者にセキュリティサービスを提供し、取引契約を通じてサービスの購入者にセキュリティ保証機能を提供できます。3.1と3.2は、クラウドベース方式で展開された特定のサービスシステムのセキュリティ保証システムのためのセキュリティ技術要件と対応する実装手段に関する提案を示しています。これらのセキュリティ機能はCSPまたは利用者によって提供されるべきですが、実際にはサードパーティのセキュリティサービスプロバイダが配備、実装、管理、保守することができます。

サードパーティは、別々の製品またはサービス、あるいはパッケージを通して、さまざまなセキュリティサービスを提供できます。以下に例を示します:

- 状況把握（Situation awareness）：超大容量のデータに対するクラウドセキュリティ監視システムは、定期的に大量のクラウドアプリケーションの脆弱性を自動的にチェックし、クラウドシステムのセキュリティ問題をできるだけ早く検知し、クラウドシステムのセキュリティ管理とセキュリティ管理を向上させることができます。
- Webコードのセキュリティ保護：入力および出力の正当性チェック、認証、許可、セッション、Webサービス、インジェクションの脆弱性を防止するための対策を含む、Webコードのセキュリティメカニズムがサポートされています。システムはまた、ウェブを介したリソースへのユーザアクセスを制御し、リモートウェブアクセスの安全な通信をサポートします。
- WAFシステム：ルールベースの保護は、SQLインジェクション、クロスサイトスクリプティング、OSコマンドインジェクション、リモートファイルインクルード、ローカルファイルインクルード、ディレクトリトラバーサル、HTTP違反、WebShell攻撃などの既知の多くの攻撃に対して正確かつ詳細な防御を提供します。
- WTPシステム：このサービスは、ウェブサイトのファイルをリアルタイムで復元してウェブサイトの正常な運営を保証し、改ざんされたイベントに関する情報を記録します。
- SOC：統合管理プラットフォームはさまざまなセキュリティサービスを統合し、WTP、クラウドホスト保護、クラウド型踏み台、クラウドWAF、ログ監査、データベース監査、状況把握などのサービスプラットフォームを提供します。