# ハイブリッドクラウドのセキュアな接続要件

CSAJC cloud security alliance SM Japan Chapter

CSA cloud security alliance®

ハイブリッドクラウドセキュリティワーキンググループの恒久的かつ公式の場所は次のURLを参照してください
https://cloudsecurityalliance.org/research/working-groups/hybrid-cloud-security

# Acknowledgments

## Lead Authors:

Zou Feng
Narudom Roongsiriwong

## Key Contributors:

David Chong
Rolando Marcelo Vallejos Michael
Roza
Geng Tao

## CSA Global Staff:

Hing-Yan Lee
Claire Lehnert Ekta
Mishra AnnMarie
Ulskey

**ハイブリッドクラウドセキュリティワーキンググループ(WG)について**

企業が急速に発展し、情報技術（IT）インフラが常に多様化する中であっても、多くのクラウド利用者は単一のパブリック/プライベートクラウドや従来のオンプレミスを発見します。それらのデータセンターは、コスト、パフォーマンス、スケーラビリティ、セキュリティ、耐障害性、規制および互換性に関するサービス要件を満たすことができなくなってきています。企業は、そのニーズに合わせてハイブリッドクラウド環境やサービスを選択することが多くなっています。ハイブリッドクラウドは、様々なクラウドと従来のITインフラを活用し、ユーザのサービス要件に応じて体系的にメリットを提供するものです。しかし、ハイブリッドクラウドは様々なリスクをもたらすため、セキュリティに関して異なる課題が持ち込まれます。このWGは、ハイブリッドクラウドのセキュリティリスクと対策を明らかにし、ユーザがリスクを特定し、低減できるようにすることを目的としています。このほか、このWGは、ハイブリッドクラウドガバナンス、ハイブリッドクラウド脅威プロファイル、ハイブリッドクラウドセキュリティ評価に関する提案も行い、ユーザとクラウドサービスプロバイダの両者がセキュアなハイブリッドクラウドソリューションを選択・提供できるように導き、セキュリティ計画と実施を促進することを意図しています。

# 日本語版提供に際しての告知及び注意事項

本書「ハイブリッドクラウドのセキュアな接続要件」は、Cloud Security Alliance (CSA)が公開している「Secure Connection Requirements of Hybrid 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 |
|---|---|---|
| 2022年6月14日 | 日本語版1.0 | 初版発行 |



# CSAジャパン成果物の提供に際しての制限事項

日本クラウドセキュリティアライアンス(CSAジャパン)は、本書の提供に際し、以下のことをお断りし、またお願いします。以下の内容に同意いただけない場合、本書の閲覧および利用をお断りします。

1.　責任の限定
CSAジャパンおよび本書の執筆・作成・講義その他による提供に関わった主体は、本書に関して、以下のことに対する責任を負いません。また、以下のことに起因するいかなる直接・間接の損害に対しても、一切の対応、是正、支払、賠償の責めを負いません。
(1)　本書の内容の真正性、正確性、無誤謬性
(2)　本書の内容が第三者の権利に抵触しもしくは権利を侵害していないこと
(3)　本書の内容に基づいて行われた判断や行為がもたらす結果
(4)　本書で引用、参照、紹介された第三者の文献等の適切性、真正性、正確性、無誤謬性および他者権利の侵害の可能性

2.　二次譲渡の制限
本書は、利用者がもっぱら自らの用のために利用するものとし、第三者へのいかなる方法による提供も、行わないものとします。他者との共有が可能な場所に本書やそのコピーを置くこと、利用者以外のものに送付・送信・提供を行うことは禁止されます。また本書を、営利・非営利を問わず、事業活動の材料または資料として、そのまま直接利用することはお断りします。
ただし、以下の場合は本項の例外とします。
(1)　本書の一部を、著作物の利用における「引用」の形で引用すること。この場合、出典を明記してください。
(2)　本書を、企業、団体その他の組織が利用する場合は、その利用に必要な範囲内で、自組織内に限定して利用すること。
(3)　CSAジャパンの書面による許可を得て、事業活動に使用すること。この許可は、文書単位で得るものとします。
(4)　転載、再掲、複製の作成と配布等について、CSAジャパンの書面による許可・承認を得た場合。この許

可・承認は、原則として文書単位で得るものとします。

3.　本書の適切な管理

(1)　本書を入手した者は、それを適切に管理し、第三者による不正アクセス、不正利用から保護するために必要かつ適切な措置を講じるものとします。

(2)　本書を入手し利用する企業、団体その他の組織は、本書の管理責任者を定め、この確認事項を順守させるものとします。また、当該責任者は、本書の電子ファイルを適切に管理し、その複製の散逸を防ぎ、指定された利用条件を遵守する(組織内の利用者に順守させることを含む)ようにしなければなりません。

(3)　本書をダウンロードした者は、CSAジャパンからの文書(電子メールを含む)による要求があった場合には、そのダウンロードしまたは複製した本書のファイルのすべてを消去し、削除し、再生や復元ができない状態にするものとします。この要求は理由によりまたは理由なく行われることがあり、この要求を受けた者は、それを拒否できないものとします。

(4)　本書を印刷した者は、CSAジャパンからの文書(電子メールを含む)による要求があった場合には、その印刷物のすべてについて、シュレッダーその他の方法により、再利用不可能な形で処分するものとします。

4.　原典がある場合の制限事項等

本書がCloud Security Alliance, Inc.の著作物等の翻訳である場合には、原典に明記された制限事項、免責事項は、英語その他の言語で表記されている場合も含め、すべてここに記載の制限事項に優先して適用されます。

5.　その他

その他、本書の利用等について本書の他の場所に記載された条件、制限事項および免責事項は、すべてここに記載の制限事項と並行して順守されるべきものとします。本書およびこの制限事項に記載のないことで、本書の利用に関して疑義が生じた場合は、CSAジャパンと利用者は誠意をもって話し合いの上、解決を図るものとします。

その他本件に関するお問合せは、info@cloudsecurityalliance.jp までお願いします。

# 日本語版作成に際しての謝辞

「ハイブリッドクラウドのセキュアな接続要件」は、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を記します。（氏名あいうえお順・敬称略）

高橋　久緒, CISSP, RISS, PMP
松浦　一郎, CISSP, CISM, CDPSE
満田　淳
諸角　昌宏

# 目次

# 1. はじめに

米国標準技術局（NIST）は、ハイブリッドクラウドインフラストラクチャを、独自性のあるクラウドインフラストラクチャ（プライベート、コミュニティ、パブリック）の組み合わせであると定義しています。しかしそれらは、データやアプリケーションの移植容易性を実現する標準化された技術や独自の技術によって結合されています（例えば、クラウド間の負荷分散のためのクラウドバーストなど）。[1]

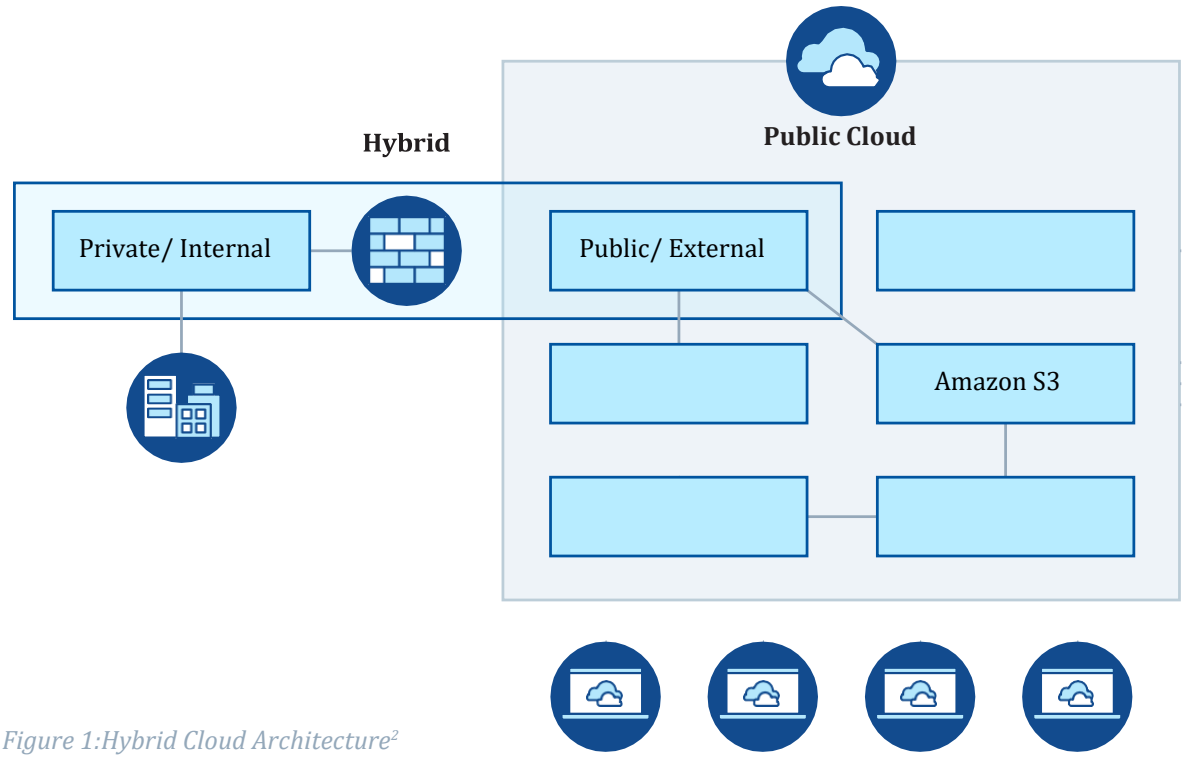



*Figure 1:Hybrid Cloud Architecture*[2]

ハイブリッドクラウド環境は、クラウドサービス利用者（CSC）のニーズに応じて、異なるワークロードを実行するための多様なリソースを企業に提供します。一方、企業はパブリッククラウドを通じて、革新的なサービスを迅速に利用し、インターネットアプリケーションを展開し、最適なパフォーマンスを提供できます。同時に、プライベートクラウドのセキュリティと信頼性を利用して、ローカルデータセンターでコアアプリケーションを実行できます。そのため、ハイブリッドクラウドは、両者の長所を活かせるエンタープライズ・クラウド・モデルとして不可欠なものとなっています。

このハイブリッド展開は、多様なコネクテッドエコシステムを形成しています。クラウド間を流れるデータやアプリケーションは、AWS、Microsoft、Googleなどのクラウドサービスプロバイダ（CSP）がそれぞれ独自に管理するため、セキュリティ上の新たな課題となっています。
このユニークで複雑な状況をうまくセキュアにするために、企業は、境界、伝送、ストレージおよび管理の4つの分野で、クロスクラウドなセキュリティ能力を開発し、採用する必要があります。

本書は、CSA Cloud Controls Matrix （CCM）のハイブリッドクラウドへの適用について説明するものです。

[1] https://csrc.nist.gov/publications/detail/sp/800-145/final
[2] https://dzone.com/articles/5-causes-why-hybrid-cloud-is-becoming-the-new-norm

# 2. クロスクラウドセキュリティ機能

クロスクラウドセキュリティは、4つの要素で構成されています：

1. クロスクラウド境界セキュリティ
2. クロスクラウド通信セキュリティ
3. クロスクラウドストレージセキュリティ
4. クロスクラウド管理セキュリティ

クロスクラウド境界セキュリティ：プライベートクラウドとパブリッククラウドの物理的・論理的境界のセキュリティ、および越境するアクセス動作のセキュリティを確保します。越境保護対策、境界を越えたアクセス制御機構、インターフェースセキュリティなどを含みます。

クロスクラウド通信セキュリティ：ホスト、コンテナ、アプリケーション、データなどの要素のクロスクラウド伝送または移行において、ネットワーク接続のセキュリティ、通信伝送の機密性と完全性、伝送前後のセキュリティポリシーの一貫性などのセキュリティを確保することができます。

クロスクラウドストレージセキュリティ：ハイブリッドクラウドのシナリオにおいて、ストレージ制御、暗号化、バックアップと復元のセキュリティなどを確保します。

クロスクラウド管理セキュリティ：統合ID認証、権限管理、統合O&M（Operations and Maintenance）、運用セキュリティなどの統合管理により、複数のクラウド間でセキュリティを確保します。

## 2.1 クロスクラウド境界セキュリティ

### 2.1.1 境界防御

- パブリッククラウドとプライベートクラウドの境界にアクセス制御ポリシーを設定し、ハイブリッドクラウドの境界に出入りするデータを制御して不正なアクセスを防止します。
- パブリッククラウドとプライベートクラウドの境界にセキュリティ保護メカニズムを設け、不正なネットワーク接続やネットワーク侵入を検知し、悪意のあるコードを防止します。

### 2.1.2 アクセス制御

> - 境界の外からのアクセスは、認証と認可の後にのみ許可されるようにします。
> - 境界内にあるクラウドサービスに対するユーザのアクセス権を制御します。
> - 他のユーザのリソース（ストレージなど）へのアクセスを禁止します。
> - 生データ（プライバシー保護要件に基づく匿名化されていないデータ）へのアクセスを禁止します。

### 2.1.3 インターフェースセキュリティ

- 厳格なACLルールを設定し、そのルールを満たしたアプリケーションのみが、対応するインターフェースにアクセスできるようにします。
- インターフェースは、不正なアクセスを防ぐためにアクセス認証の仕組みを持つ必要があります。
- インターフェースを呼び出す際には、認証クレデンシャルを使用してアクセスの有効性を確認します。
- インターフェースアクセス接続は、セキュアな暗号化アルゴリズムに基づき暗号化される必要があります。
- インターフェースの入力を検証することで、SQLインジェクションやスクリプトインジェクション攻撃から防御します。
- インターフェース要求数、インターフェース呼び出し遅延、インターフェースエラー情報など、リアルタイムかつ可視化されたインターフェース監視を提供します。
- 異なるサービスレベルやユーザーレベルに基づいて要求頻度を制御します。トラフィックコントロールの時間単位は、秒、分、時、日のいずれでも構いません。
- IPアドレスやアカウントのホワイトリストやブロックリストを設定し、IPアドレスやアカウントからのインターフェースへのアクセスを許可または拒否します。
- リーキーバケット、カウンタ、トークンバケットなど複数のフロー制御アルゴリズムをサポートし、詳細なフロー制御を秒単位で実現します。
- カスタムトラフィックコントロールポリシーをサポートします。

## 2.2 クロスクラウド通信セキュリティ

### 2.2.1 ネットワーク接続

- パブリッククラウドとプライベートクラウドにファイアウォールを配備します。ファイアウォールのアクセスポリシーを設定し、指定したルールに合致するパケットのみを許可します。その他の不特定多数のトラフィックをデフォルトでブロックします。
- パブリッククラウドとプライベートクラウドにまたがる仮想ネットワークとアプリケーションセキュリティグループを適切かつ一貫性をもって構成します。
- パブリッククラウドとプライベートクラウド間のネットワークトラフィックを監視し、例外を検出した場合は直ちにアラームを上げ、DoS/DDoS攻撃を防止します。
- プライベートクラウドとパブリッククラウドをVPNまたはDirect Connectで接続し、高速、低レイテンシー、安定性およびセキュアなネットワーク通信を確保します。
- サービスネットワークと管理ネットワークは互いに分離します。
- 攻撃の種類、攻撃時間、攻撃トラフィックなど、ネットワーク攻撃の行動を記録します。
- ルールが適切であることを確認するために定期的なレビューを行います。冗長または使われなくなったルールは削除されるべきです。
- 確立された暗号アルゴリズムとセキュリティ標準を採用します。
- 異なるクラウドプラットフォームを接続するために必要な相互運用性を検討します。

### 2.2.2 通信伝送

- HTTPS や TLS などのセキュアな伝送プロトコルを使用してチャネルを暗号化し、クロスクラウド伝送時にデータ、アプリケーション、API、イメージの機密性と完全性を確保します。
- VM、コンテナ、アプリケーション、データがクラウド間で移行する際に、セキュリティポリシーを自動的に再展開します。

- アプリケーションとデータのクロスクラウド移行時に、セキュリティポリシーの自動展開をサポートします。
- 確立された暗号アルゴリズムとセキュリティ標準を採用します。カスタムアルゴリズムの使用は、堅牢性に欠け、相互運用性に問題が生じる可能性があるため、控えます。

# 2.3 クロスクラウドストレージ＆コンピュート・セキュリティ

## 2.3.1 データストレージ

- データの機密性と情報の分類に基づき、適切なストレージと暗号化のオプションを提供します。これは、要件に応じて、ディスク、ファイル、テーブルストレージ、データベースの各レベルで適用されます。
- CSP は、ストレージの暗号化に使用される鍵を管理する機能を CSC に提供するものとします。キーマネージメントシステム（KMS）を考えてみましょう。
- 暗号化期間を設定し、鍵によって暗号化されるデータ量と、鍵が漏洩する危険性がある期間を減らします。
- データを単一のデータセンター内に格納するのではなく、複数のストレージボリュームに分散して格納します。不正アクセスや改ざんを防ぐために、暗号化技術やその他の技術的手段を用いて、クラウドストレージ全体のデータを保護します。

## 2.3.2 コンピュート・リソース

- パブリッククラウドとプライベートクラウドにまたがる、統一された一貫性のあるエンドポイント保護します。
- VMやコンテナなどの関連コンポーネントを対象に、パブリッククラウドとプライベートクラウドで統一された一貫性のあるパッチ管理を可能にします。
- パブリッククラウドとプライベートクラウドにまたがって、一貫したVMとコンテナのセキュリティ強化を適用します。
- 組織として効果的かつ総合的に管理できるように、上記のための統一されたレポートを作成します。
- 適切なデータ保管時暗号化コントロールを行う必要があります。ディスクの暗号化は、VMを保護するための最低限のものです。
- 鍵やシークレットを保管・管理するためのKMSを検討します。

## 2.3.3 バックアップとリストア

- クロスクラウドの事業継続・災害復旧計画を策定します。
- ファイル、電子メール、データベース、VM、OSなど、複数のデータタイプのバックアップ保護をサポートします。これは、Security as a Service（SaaS）/ Platform as a Service（PaaS）プラットフォーム上のクラウドサービスにおけるデータのバックアップを含めることができます。
- データ保持の要件は、バックアップとリストアの手法の一部として考慮されるべきです。アプリケーションとデータを複数のストレージボリュームに分散し、最も事故が起こる前の状態での迅速な復旧を可能にします。
- バックアップ中にネットワークや機器に障害が発生した場合、障害箇所から確実にデータをバックアップします。
- オンプレミスとクラウドのリソース間でデータを同期させ、単一障害点を排除し、迅速なアクセスを確保します。

- バックアップは強力な暗号化（256ビットAESなど）を使用して暗号化する必要があります。
- バックアップとリカバリのパフォーマンスを向上させるために、ハードウェア暗号化の選択を検討してください。
- 鍵やシークレットを保管・管理するためのKMSを検討します。
- バックアップや災害復旧（DR）時にそのデータ整合性を検証するために、整合性チェック技術を使用します。
- 効率的なデータリカバリをサポートするために必要な技術やツールを選択する際には、RTO（Recovery Time Objective）とRPO（Recovery Point Objective）の要件を考慮します。
- クロスクラウドデータDRにより、CSPの重大な障害を回避し、データの利便性と安定性を確保します。
- リカバリプロセスの効率性と有効性を確保するために、人員の訓練とDRシナリオを実施します。
- RTOとRPOの目標に対するDRトレーニングシナリオの有効性を測定します。

# 2.4 クロスクラウド管理セキュリティ

## 2.4.1 アイデンティティ認証

- パブリッククラウドとプライベートクラウドで統一されたID認証を行います。
- パスワード認証、電子証明書認証、二要素認証など、複数のセキュリティ認証モードをサポートします。
- 管理者は、単純なパスワードや長期間固定されたパスワードによるアカウント漏えいを防ぐため、強度の異なるパスワードポリシーを設定する必要があります。
- 企業ポリシーや標準に基づき、パスワードの複雑さの要件を実施します。例えば、ユーザアカウントのパスワードは、文字、数字、特殊記号を含む8文字以上である必要があります。
- ポリシーに基づきパスワードの紛失や忘却をリセットします。
- 認証クレデンシャル（パスワードや秘密鍵など）は、セキュアな暗号化アルゴリズムを用いて暗号化し、保存する必要があります。

## 2.4.2 認可マネジメント

- ロール制御ポリシーに基づき、ユーザまたはユーザグループの権限を作成、削除、変更することができます。
- パブリッククラウドとプライベートクラウドの統一的な役割制御ポリシーをサポートします。
- データ、アプリケーション、サービスに応じたアクセス制御権の設定など、きめ細かな認可をサポートします。
- アカウントは最小権限原則に基づき認可されるべきです。
- パブリッククラウドとプライベートクラウドは、同じユーザグループの権限を持つ必要があります。

## 2.4.3 キーマネージメント

- 統一された一貫性のある暗号化管理ポリシーを作成し、クラウド全体の暗号化および鍵管理を管理します。これらのポリシーは、鍵管理のライフサイクルとその様々なフェーズに対応しています。
- ハードウェアセキュリティモジュール（HSM）と鍵管理ソフトウェアを含む、マネージドクラウド鍵管理サービスの利用を検討してください。複数のクラウド間での互換性を検討します。
- データ分類、セキュリティ、またはコンプライアンス要件（CSP が管理する鍵または顧客が管理する 鍵など）に基づき、鍵を所有すべき者を慎重に検討します。
- 鍵やシークレットのガバナンス、サポート、使用に責任を持つ当事者について、役割と責任を明確に定義します。
- 鍵の漏洩を疑うに足る十分な理由がある場合、または鍵のライフサイクルが終了した場合は、直ちに鍵を交換してください。
- 詳しくは、下記「*クラウドサービスにおける鍵管理について」を参照してください*3。

## 2.4.4 O&M マネジメント

- クラウドリソースの作成、クエリ、変更、削除など、パブリッククラウドとプライベートクラウド上のリソースの統合管理をサポートします。
- パブリッククラウドとプライベートクラウド上のパフォーマンスモニタリングデータの統一的なクエリと表示をサポートします。
- 現在のアラーム情報の集計、閲覧、表示、保持およびエクスポートに関する一元管理をサポートします。
- O&Mログの保存期間と、ログに記録する必要のあるメトリクス/フィールドを設定します。
- ログに含まれる機密情報を難読化します。
- ログアクセス制御ポリシーを設定し、ログの改ざんを防止します。

### 2.4.5 オペレーションズ・マネジメント

- パブリックおよびプライベートクラウド上のセキュリティイベントやアラームを記録し、分析することができます。
- パブリッククラウドとプライベートクラウド上のセキュリティイベントやアラームの共有と関連付けをサポートします。
- 物理マシン、クラウドホストのOS、クラウドホストのオープンポート、ミドルウェア、データベース、Webサービス、サービスアプリケーション、クラウドセキュリティデバイスなど、パブリック／プライベートクラウド上のユーザの資産情報の一元管理をサポートします。理想的には、O&Mチームが組織のIT資産を完全に可視化できるような、一枚板を作成することです。
- パブリックおよびプライベートクラウド上の悪意のあるアクセス行動やコードセキュリティの検出ポリシーを統一的に管理し、提供します。
- リスクベースのアプローチに基づき、セキュリティの脆弱性を効果的に管理するための脆弱性管理フレームワークを確立します。
- これには、パブリックおよびプライベートクラウドのセキュリティ脆弱性情報を、定められた期間内に特定、評価、分類、是正することが含まれます。
- 脅威に関する情報を一元管理し、その知識を情報と資産の保護に総合的に活用できるようにします。
- セキュリティの自動化とプレイブックを検討し、O&M 全体の生産性と効率性を向上させ、より価値の高いタスクに集中できるようにします。
- ユーザとデータのプライバシーを保護するために、各ユーザまたは機能ユニットが自分の情報のみを照会できるように、統一された測定クエリインターフェースを提供します。

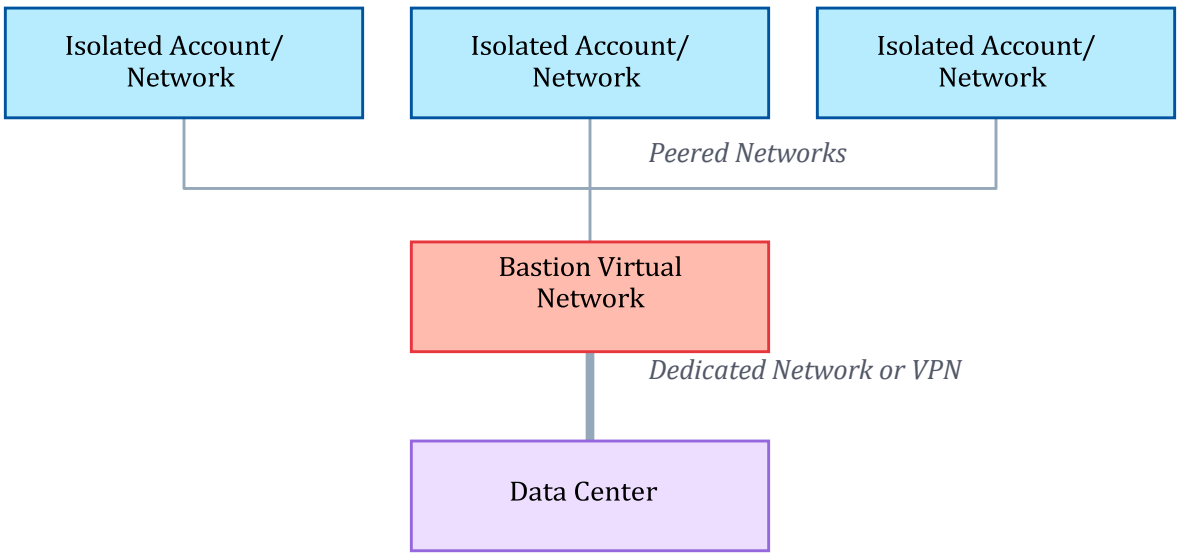
[3] https://cloudsecurityalliance.org/artifacts/key-management-when-using-cloud-services/

# 3. セキュアコネクションの実践

## 3.1 Bastion仮想ネットワーク

クラウドセキュリティアライアンスの「*Security Guidance for Critical Areas of Focus in Cloud Computing v4.0*」では、「ハイブリッド接続は、両方のネットワークのセキュリティを効果的にフラット化すべきではない」と述べています。2つのネットワーク間には、ルーティング、アクセス制御、さらにはファイアウォールや追加のネットワークセキュリティツールを介して分離を強制する必要があります。ハイブリッドクラウド接続のためのアーキテクチャは、「Bastion」または「トランジット」仮想ネットワークです。

> - 複数の異なるクラウドネットワークを、1つのハイブリッド接続でデータセンターに接続します。クラウド管理者は、ハイブリッド接続専用の仮想ネットワークを構築し、指定されたBastionネットワークを通じて他のあらゆるネットワークをピアリングします。
> - セカンドレベルネットワークは、Bastionネットワークを通じてデータセンターに接続し、互いに会話することができず、分離されています。また、ハイブリッド接続に出入りするトラフィックをさらに保護するために、Bastionネットワークに異なるセキュリティツール、ファイアウォールルールセット、アクセスコントロールリストを配備することができます。




# 4. CCM適用範囲

Cloud Controls Matrix（CCM）は、CSAのベストプラクティスに沿ったクラウドコンピューティングのためのサイバーセキュリティコントロールフレームワークであり、クラウドセキュリティとプライバシーのデファクトスタンダードと考えられています。
CCMのバージョン4 は前バージョン(v3.0.1) から大幅にアップグレードされており、追加開発や既存のコントロールの更新により、要求事項が大幅に増加しています。

この文書が対象とするクロスクラウドセキュリティ機能は、CCM v.4 コントロールドメインの関連コントロールを参照し、以下のように実装することができます。

- クロスクラウド境界セキュリティ：アプリケーションとインターフェースセキュリティ（AIS）、暗号化、鍵管理（CEK）、脅威と脆弱性管理（TVM）。
- クロスクラウド通信セキュリティ：暗号、暗号化、鍵管理（CEK）、相互運用性と移植容易性（IPY）、データセンターセキュリティ（DCS）。
- クロスクラウドストレージセキュリティ：インフラストラクチャと仮想化セキュリティ（IVS）、事業継続マネジメントとオペレーショナル・レジリエンス（BCR）。
- クロスクラウド管理セキュリティ、アイデンティティとアクセス管理（IAM）、ロギング＆モニタリング（LOG）、セキュリティインシデント管理、Eディスカバリ、およびクラウドフォレンジック（SEF）。

# 参照


Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing v4.0, July 2017, https://cloudsecurityalliance.org/artifacts/security-guidance-v4/.

Cloud Security Alliance, Cloud Controls Matrix v4.0, 2021, June 2021, https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/.

Cloud Security Alliance, Cloud Controls Matrix v3.01, August 2019, https://cloudsecurityalliance.org/artifacts/security-guidance-v4/.

Cloud Security Alliance, Key Management in Cloud Services, November 2020, https://cloudsecurityalliance.org/artifacts/key-management-when-using-cloud-services/.

NIST, SP 800-145, The NIST Definition of Cloud Computing, September 2011, https://csrc.nist.gov/publications/detail/sp/800-145/final.

ISO/IEC、17788:2014、Information technology — Cloud computing — Overview and vocabulary, 2021,https://www.iso.org/standard/60544.html


# 用語集

**Bastion** – プロビジョニングされた仮想ネットワーク内のすべての VM にセキュアなリモートデスクトッププロトコル（RDP）および Secure Shell（SSH）接続を提供するプラットフォーム
https://docs.microsoft.com/en-us/azure/bastion/bastion-overview

**クロスクラウド機能** – セキュアなデータ共有を促進する統合データ管理プラットフォームは、クロスクラウド管理を行う必要があります。このプラットフォームは、データがクラウド間で自由に移動できるようにすることで、組織に実信頼できる唯一のソースを提供します。クロスクラウド互換性により、マルチクラウドでの運用効率を向上させます。
https://www.cloudbolt.io/blog/driving-operational-efficiency-in-multi-cloud-with-cross-cloud- management/

# 頭字語

| | |
|---|---|
| ACL | アクセスコントロールリスト |
| AES | Advanced Encryption Standard |
| CCM | Cloud Control Matrix |
| CSC | クラウドサービス利用者 |
| CSP | クラウドサービス提供者 |
| DDoS | 分散型サービス拒否攻撃 |
| DoS | サービス拒否攻撃 |
| DR | 災害復旧 |
| EU | 欧州連合 |
| HTTPS | Hypertext Transfer Protocol Secure |
| IaaS | Infrastructure as a Service |
| IP | Internet Protocol |
| ISO/ IEC | 国際標準化機構／国際電気標準会議 |
| NIST | 米国国立標準技術研究所 |
| O&M | オペレーション＆メンテナンス |
| OS | オペレーティングシステム |
| PaaS | Platform as a Service |
| RDP | Remote Desktop Protocol |
| RPO | Recovery Point Objective |
| RTO | Recovery Time Objective |
| TLS | Transport Layer Security |
| SaaS | Software as a Service |
| SDP | Software-Defined Perimeter |
| SQL | Structured Query Language |
| SSH | Secure Shell |
| VM | 仮想マシン |
| VPN | 仮想プライベートネットワーク |
| ZTNA | ゼロトラストネットワークアクセス |

# 付録1– クラウドのデプロイメント・モデル

## NIST定義[4]

**NISTのプライベートクラウド**: クラウドのインフラストラクチャは、複数の利用者（例：事業組織）から成る単一の組織の専用使用のために提供されます。その所有、管理、運用は、その組織、第三者、もしくはそれらの組み合わせにより行われ、存在場所としてはその組織の施設内または外部となります。

**NISTのコミュニティクラウド**: クラウドのインフラストラクチャは共通の関心事（例えば任務、セキュリティの必要、ポリシー、法令順守に関わる考慮事項）を持つ、複数の組織からなる成る特定の利用者の共同体の専用使用のために提供されます。その所有、管理、運用は、共同体内の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、存在場所としてはその組織の施設内または外部となります。

**NISTのパブリッククラウド**: クラウドのインフラストラクチャは広く一般の自由な利用に向けて提供されます。その所有、管理、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ます。その存在場所はそのクラウドプロバイダの施設内となります。

**NISTのハイブリッドクラウド**: 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（プライベート、コミュニティ、パブリック）の組み合わせです。各クラウドは独立の存在ですが、標準化された、あるいは固有の技術で結合され、データとアプリケーションの移植容易性を実現しています（例えば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）。

## ISO定義[5]

**パブリッククラウド**: クラウドサービスプロバイダがリソースを管理し、クラウドサービスをあらゆるクラウドサービス利用者が潜在的に利用できるようにするクラウド展開モデルです。企業、学術機関、政府機関、またはそれらの組み合わせによって所有、管理、運営されている可能性があります。それはクラウドサービスプロバイダの施設内に存在します。特定のクラウドサービス利用者に対する実際の利用可能性は、管轄の規制により制限される場合があります。パブリッククラウドは、境界が非常に広く、クラウドサービス利用者のパブリッククラウドサービスへのアクセスには、ほとんど制限がありません。

**プライベートクラウド**: クラウドサービスを単一のクラウドサービス利用者が独占的に使用し、そのクラウドサービス利用者がリソースを管理するクラウド展開モデルです。プライベートクラウドは、組織または第三者が所有、管理、運営し、存在場所としてはその組織の施設内または外部となります。また、クラウドサービス利用者は、その利益のために他者へのアクセスを認可することができます。プライベートクラウドは、利用者を一つの組織に限定し、プライベートクラウドの周囲を狭く管理する境界を設定しようとします。

**コミュニティクラウド**: クラウドサービスが、互いに共通の要件と関係を持つ特定のクラウドサービス利用者の集合体を排他的にサポートし、共有され、この集合体の少なくとも1つのメンバによってリソースが制御されるクラウド展開モデルです。

[4] https://csrc.nist.gov/publications/detail/sp/800-145/final
[5] https://www.iso.org/standard/60544.html

コミュニティ内の1つまたは複数の組織、第三者、またはそれらの組み合わせによって所有、管理、運営され、オンプレミスまたはオフプレミスに存在する可能性があります。パブリッククラウドがオープンであるのに対して、コミュニティクラウドはプライベートクラウドよりも参加者が広く、共通の関心事を持つクラウドサービス利用者グループに限定されています。これらの共通の関心事には、ミッション、情報セキュリティ要件、ポリシー、コンプライアンスへの配慮が含まれますが、これらに限定されるものではありません。

**ハイブリッドクラウド**: 少なくとも2つの異なるクラウド展開モデルを使用するクラウド展開モデルです。関係するデプロイメントがユニークな存在であることに変わりはありませんが、相互運用性、データの移植容易性、およびアプリケーションの移植容易性を可能にする適切なテクノロジによって結びつけられています。ハイブリッドクラウドは、組織または第三者が所有、管理、運営し、オンプレミスまたはオフプレミスに存在することができます。ハイブリッドクラウドは、2つの異なる環境間の相互作用が必要でありながら、適切な技術でリンクされている状況を表しています。このように、ハイブリッドクラウドが設定する境界は、その2つのベースデプロイメントを反映しています。