NEC Cloud IaaS

セキュリティホワイトペーパー

（バージョン　2.0　2020 年 11 月 30 日　）

日本電気株式会社

ドキュメント ID：MGD1-0228

目次

本文書について

1. はじめに

NEC Cloud IaaS は、可用性、信頼性、そして拡張性の高いクラウドコンピューティング・プラットフォームを提供します。

次節で後述するように、Infrastructure as a Service（以下「IaaS」といいます）型のクラウドサービスである NEC Cloud IaaS は、ハードウェア、ネットワークといった IaaS を構成するリソースを、利用者間でセキュリティを確保しつつ共有することで、調達コストの抑制や導入期間短縮が可能という特長を有しています。

本文書（以下「ホワイトペーパー」といいます）では、NEC Cloud IaaS のセキュリティへの取組みを説明するとともに、NEC Cloud IaaS を利用する上でセキュリティの考慮ポイントについても紹介しています。また、第三者機関によるセキュリティ評価の結果を参照し、クラウド利用者が注意すべき点についても触れています。

■ホワイトペーパーの目的

このホワイトペーパーは、以下を目的として作成されています。

・NEC Cloud IaaS のセキュリティへの取組みを確認する。

・NEC Cloud IaaS をセキュアに利用するための考慮事項を確認する。

お客様の責任範囲は、使用するサービス、IT 環境、及び関連法令に応じて異なります。

お客様は、セキュリティの目的を達成するために役立つ様々な機能を利用することができます。

NEC Cloud IaaS では、ネットワークセキュリティ、アクセスコントロールなどのセキュリティ機能を提供しています。

■ホワイトペーパーの対象読者

・NEC Cloud IaaS をご利用中の方

・NEC Cloud IaaS の導入をご検討中の方

2. NEC Cloud IaaS とは

NEC Cloud IaaS は、コンピュータ資源（ネットワーク、ストレージ、アプリケーション、サービス）を構成可能にするシェアードリソースプールへの、オンデマンドアクセスを実現するクラウドコンピューティングサービスです。

NEC Cloud IaaS は、多くの異なった利用者に対して、インフラ、データ、メタデータ、サービス及びアプリケーションの共有、区分け、分離の管理を行い（マルチテナント）、規模の経済性と効率的な運用を可能とするアーキテクチャとデザインを採用した IaaS です。

NEC Cloud IaaS では、ハイブリッドクラウド環境をお客様自身がセルフサービスポータルから利用することが可能です。セルフサービスポータルは、様々なクラウド環境や個別システムの運用をまとめて管理する「統合運用管理機能」や、リソースの調達や管理を行う「プロビジョニング機能」を提供しています。

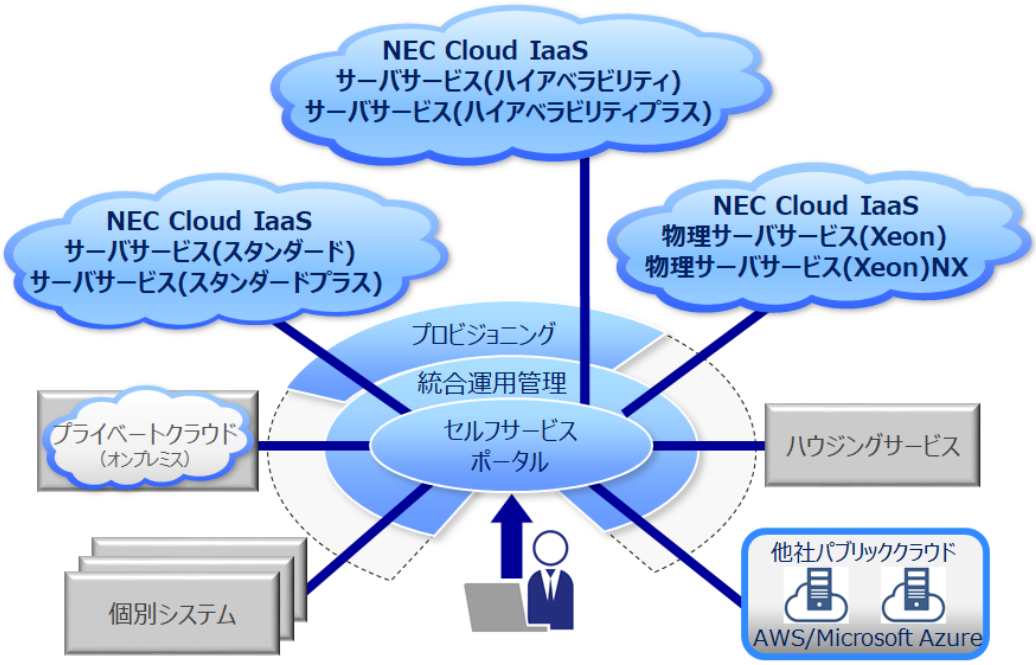


図 1　NEC Cloud IaaS の全体像

3. NEC Cloud IaaS のセキュリティ概要

3.1. セキュリティ方針

NEC では、各種セキュリティの規格、基準等（CCM[1],ISO/IEC 27001[2], ISO/IEC 27002[3],FISC[4],JASA[5],PCI DSS[6],COBIT[7],SOC2[8],CAIQ[9],NIST SP800-171[10] ）に準拠、対応したサービス提供をめざしています。そのため、最新のセキュリティ規格や基準について、関連の業界団体、標準化団体、クラウドのセキュリティガイドラインを参考に、NEC 独自のクラウドセキュリティ基準を策定・整備しました。この基準を NEC Cloud IaaS に適用することで、各サービスが一定のセキュリティ品質を継続的に担保可能とする統制の取り組みを確立しました。後述する通り、NEC Cloud IaaS で規定したセキュリティ方針に準拠していることを保証するために、年に 1 回、国際的に認められた第三者機関による統制評価を受けています。これらの評価情報は、既存・新規のお客様に対して NDA[11]に基づいて開示されます。

3.2. 責任分担の考え

NEC Cloud IaaS の利用においては、お客様と NEC Cloud IaaS 間でセキュリティ対策に関する責任分担が求められます。NEC Cloud IaaS は、ホストオペレーティングシステム、仮想レイヤー、及びサービスが運用されている施設の物理セキュリティ、様々なコンポーネントの操作、管理、及び運用における論理的セキュリティの実行責任を負います。お客様はゲストオペレーティングシステムにおける更新やセキュリティパッチ適用、お客様アプリケーションの管理、及び NEC Cloud IaaS としてご利用になる機能の設定や動作結果の管理を行うことになるため、それらに関するセキュリティ上の実行・管理責任も負うことになります。

お客様の責任範囲は、使用するサービス、IT 環境、及び関連法令に応じて異なります。お客様は慎重にサービスを選択し、その適切な責任を負う必要があります。

お客様とのこの責任分担によって NEC Cloud IaaS は、お客様に必要な業界固有の認証要件等に適合するソリューションの配備を、お客様自ら実施できることを可能とし、柔軟性とお客様側でのコントロール性を提供しています。

3.3. ガバナンスとリスクマネジメント

NEC Cloud IaaS では、情報セキュリティ管理の現場徹底、リスクマネジメントの継続性確保、及び、コンプライアンス遵守を行うために、適切な組織化、プロセス整備、及びリスクコントロールを、ISMS 活動を中心に組織的に行っています。

NEC Cloud IaaS では、サービスを内部的にサポートする委託先関連各社やベンダーに対して、クラウドセキュリティ基準に基づく情報セキュリティ管理を実施しています。

本サービスに係る、データ処理を含む運用業務の一部を以下の法人に再委託をしております。

・**NEC** フィールディング株式会社

また、NEC Cloud IaaS の基盤システムに対する各種の脅威に対して ISMS 活動に基づく定期的なリスク評価を行い、リスクの軽減計画の策定やその実施状況のモニタリングを行っています。

3.4. 各種認証の取得

NEC Cloud IaaS では、クラウドサービスを行う上で重要とされる様々な認証、及び保証を取得しています。

ISO/IEC 20000

国際標準化機構（International Organization for Standardization）によって 2005 年に制定された、IT サービスマネジメントに関する要求事項を規定した国際規格です。
日本では、JIS Q 20000:2007 として日本工業規格となっています。

ISO 9001

国際標準化機構（International Organization for Standardization）によって制定された品質マネジメントシステムに関する要求事項を規定した国際規格です。日本では、JISQ9001 として日本工業規格となっています。

ISO/IEC 27017 （クラウドサービスセキュリティ）

ISO/IEC 27001/JIS Q 27001 認証に加えて、クラウドサービス固有の管理策(ISO/IEC 27017)が 適切に導入、実施されていることを認証するものです。

ISO/IEC 27018 （パブリッククラウドでの個人情報保護）

ISO27018 認証は、ISMS(ISO/IEC 27001/JIS Q 27001)認証のアドオン規格として位置づけられており、ISO27001 単体で実施した各種の対策に加え、個人情報に特化した対策を追加で検討・実施することで、パブリッククラウドにおける個人情報保護体制を構築します。

ISMS（ISO/IEC 27001/JIS Q 27001）

一般的に情報セキュリティの問題として、ホームページの改ざん、ハードウェア/ソフトウェアへのサイバー攻撃や、関係者による情報の漏えいなどが存在しており、個別の対策技術は各種各様であり、必要性と投資効果で個々に実施されているのが現状です。

ISMS とは、問題毎個々の技術対策のほかに、組織のマネージメントとして、自らリスクアセスメントにより必要なセキュリティレベルを決め、プランと戦略を持ち、資源を配分して、情報システムを安全に運用する仕組みが、正しく働いているかどうかを重視します。

組織が保護すべき情報資産について、機密性、完全性、可用性をバランス良く配置し維持し改善することが、情報セキュリティマネージメントシステム（ISMS）の基本コンセプトです。

プライバシーマーク（JIS Q 15001）

個人情報保護を目的とし、様々な企業や組織が個人情報を適切に管理するためのマネジメントシステムの要求事項を定めたものです。

SOC1/SOC2

「SOC2 保証報告書」は、受託会社の IT 統制にかかる内部統制を、第三者機関である独立監査法人が、米国公認会計士協会が公表したガイドに基づき評価した結果をまとめたもので、国際的にも信頼性の高い報告書です。

このガイドは２０１１年５月に公表され、Trust サービス®の「セキュリティ」、「可用性」、「処理のインテグリティ」、「機密保持」、「プライバシー」の 5 原則のうち 1 つ以上を対象に、受託会社監査人が受託会社の内部統制に対してあらかじめ定められた規準を満たすかどうか検証を行い報告するものです。

NEC Cloud IaaS では、ホワイトペーパー発行時点で、「セキュリティ」、「可用性」を対象とした報告書を取得しています。

事業継続マネジメントシステム（ISO/IEC22301）

ISO/IEC22301 は事業継続マネジメントシステム（BCMS）に関する国際規格です。地震・洪水・台風などの自然災害をはじめ、システムトラブル・感染症の流行・停電・火災といった事業継続に対する潜在的な脅威に備えて、効率的かつ効果的な対策を行うための包括的な枠組みを示しています。

NEC Cloud IaaS では、より安全、安心なクラウドサービスの構築、運用を支援するため、今後も、外部認証、保証の取得を拡大していきます。

3.5. セキュリティ設計の原則

NEC Cloud IaaS の開発プロセスは、セキュリティ評価の国際基準である ISO/IEC 15408 を活用した、セキュア開発・運用に従っています。

開発プロセスの各フェーズで、セキュリティの観点から実施すべき事項をセキュリティタスクとして定義し、それらのタスクをガイドラインに沿って実行することで、配備されるソフトウェアは適切なソースコード診断、脆弱性診断を経て実装されます。これらのセキュリティリスク査定は、定期的に実施されます。

さらに、不正プログラムの混入やその攻撃による各種の脅威（情報漏洩や可用性低下）に対抗するために、ウイルス対策ソフトを導入すること、安全なプログラム設定をおこなうこと、不要プロセスを削除すること等をセキュリティポリシーに纏め、同ポリシーに準拠した設計・構築及び運用体制を確立しています。

3.6. 事業継続性管理

NEC Cloud IaaS は、高可用性、耐障害性、災害対策機能を配備する機能をお客様に提供します。

高可用性設計

NEC Cloud IaaS は、回復機能を持つ IT アーキテクチャを配備する機能をお客様に提供します。物理サーバのハードウェア障害時に別物理サーバにて仮想サーバの自動再起動を行います。NEC Cloud IaaS の運用システム（サービス提供のための基盤システム）は、ハードウェアの故障等によるサービス停止リスクに対抗するための各種設計に基づいて、構成・運用されています。

事故への対応

NEC Cloud IaaS は、システムの事故（ハードウェア障害など）に対して、適切なモニタリングを行うことでそれを検出し、可及的速やかに障害からの復旧を行います。障害発生時には、あらかじめお申込みいただいたサービスの内容に基づき、適切な手段によりそれをお客様に伝えます。

災害時対策

NEC Cloud IaaS は、広域災害などサービスを継続できなくなる事態に備えて、遠隔地に退避したお客様のアプリケーションとデータを復旧することのできる環境を提供します。お客様は業務への影響を最小限に、災害時復旧計画を実行することができます。

3.7. 脆弱性管理

NEC Cloud IaaS では、サービスでご利用いただくことになるインターネットに接している IP アドレスに関して、脆弱性を定期的にスキャニングしています（お客様環境にあるファイアウォールやサーバに対してはこのスキャニングを行うことはありません）。これらのスキャニングは、NEC Cloud IaaS のインフラストラクチャの健全性と実行可能性を確認するためで、お客様固有のコンプライアンス要件に適合するために必要なお客様自身の脆弱性スキャニングに置き換わることを意味するものではありません。

お客様は、ご利用中のお客様環境に対して、利用規定に違反しない範囲でスキャニングを実施することができます。なお、スキャニングを行うためには NEC Cloud IaaS に対して事前の連絡が必要です。

3.8. データ管理

NEC Cloud IaaS では、故障等によりストレージデバイスを交換する場合、お客様データの流出を防止するための廃棄プロセスが定義されています。

破棄方法には、上書き消去・磁気消去・物理破壊があり、上書き消去の方法については、NSA（米国家安全保障局）推奨方式や DoD（米国防総省）準拠方式等の消去方式に基づくものもあります。

NEC Cloud IaaS では、これらの技術を用いて、廃棄プロセスの一環としてデータ破棄することができます。

また、個人情報を含む紙媒体については日本国内に保存しています。

4. クラウドサービス利用に関わるリスク

クラウドサービスは、共有化されたコンピュータリソース（サーバ、ストレージ、アプリケーション等）を、利用者の要求に応じて適宜・適切に配分し、ネットワークを通じて提供する情報処理サービスです。

その意味でクラウドサービスは、従来型の類似サービス（ハウジングサービス、ホスティングサービス、またはアプリケーションサービス）と同様の特徴、すなわちデータセンターからネットワークを通じて提供され、ファシリティやコンピュータリソースを他の利用者と共有するという特徴を持っています。クラウドサービスに関わるリスクを検討する場合、従来型の類似サービスにおけるリスクが依然として存在していることに留意してください。

中間者攻撃

クラウドサービスは、一般的に広域ネットワークを介したサービス提供であり、様々な場所から利用できることを前提としています。そのため、１対１の専用接続に比べて中間者攻撃を受けやすくなっています。また、マッシュアップ（複数の異なる提供元の技術やコンテンツを複合させて新しいサービスを形作ること）などによってサービスが構成される場合は、脆弱性の未処置等により、さらに攻撃の機会が増えると考えられています。このような中間者攻撃に対する適時の検知と適切な防御策について、お客様は十分に検討する必要があります。

NEC Cloud IaaS では、盗聴による影響を軽減するために専用線接続サービスや VPN サービスを提供しております。さらに、IDS 機能を利用することで不審なアクセスの試みを検知することができます。

また、NEC Cloud IaaS のセルフサービスポータルは、すべて SSL で暗号化保護し、通信中の傍受リスクを回避しています。

残存データ

クラウドサービスでは、システムメモリ上、またはハードウェア上にお客様データが何らかの原因で残ってしまった場合、安全にこれらが制御され処理されているか可視化できない問題があります。

NEC Cloud IaaS では、これらの残存データの処理に関して適切な管理を行うために、論理的なデータの取り扱い、物理的なデータが記録されている媒体の取り扱いに関して適切な運用規定を設け運用管理を徹底しています。実施している運用内容は第三者機関によって定期的に監査され、必要に応じて改善が実施されます。

仮想化対応

NEC Cloud IaaS は仮想化環境を提供するクラウドサービスです。一般的に仮想化環境においては、CPU やメモリなどの利用について従来の物理的な実行環境と異なる管理が行われることがあります。また、ネットワークやストレージが仮想化される場合についても、同様に単一機器と動作が異なる場合もあり、このことが運用上の制約やリスクを生む可能性があります。お客様のアプリケーションソフトが仮想化環境での利用を前提とした設計が行われていない場合、処理速度の低下やコンピュータリソースの浪費を引き起こす可能性があり、クラウド本来のメリットであるコスト削減に寄与しないという可能性も考えられます。

ライセンス管理

お客様が利用するサードパーティソフトウェアが、クラウドサービスを前提に作成されていないライセンス体系のソフトウェアである可能性があります。ソフトウェアのライセンス体系によっては、クラウドサービスでの利用で権利関係のトラブルに発展する可能性があります。お客様は利用するソフトウェアについて、クラウド環境で利用可能なライセンス体系を持つソフトウェアなのかを、慎重に再確認する必要があります。

クラウド環境では、適切なライセンス管理を行わないと、無意識のうちにライセンス違反を生じさせてしまう可能性があります。

利用するソフトウェアをクラウド環境で利用する際に適用できるのか、或いは見直しや追加契約が必要か、確認する必要があります。例えば、製品によってはオンプレミス環境で利用している既存のライセンスをクラウド環境にそのまま持っていくことができない場合があります。

インシデント管理

インシデント管理には様々なシステム関連情報が必要となります。クラウドサービスでは共有環境での運用上、お客様自ら入手できるシステム情報に制限があるため、お客様制御範囲外でのインシデント検知やその対応が困難になる可能性があります。特に、NEC Cloud IaaS が対応するインシデントやイベントの検知/対応レベルとお客様組織のレベルが合致していないこと等により、お客様側で定めたワークアラウンドが適時にできなかったり、その発生によるお客様ビジネスに対する影響分析が適切にできなかったりする可能性があります。

NEC Cloud IaaS では、お客様のインシデント管理を支援する機能として、セルフサービスポータルから発生したインシデント情報を取得することができます。

マルチテナント

クラウドサービスでは、１つのハードウェア上に複数のテナントが同居することにより、外部からハードウェアを狙った攻撃が実施された場合に、直接の攻撃対象でないほかのテナントにも影響が及ぶ可能性があります。NEC Cloud IaaS では、お客様環境を特定のハードウェアに集約することは行っておらず、どのテナントが同じシステム内で同居しているかを、お客様側で特定、またはコントロールすることはできません。そのため、他のテナントのシステム管理の不備によって引き起こされるリスクについても考慮する必要があります。

例えば、あるテナントへの攻撃やシステム障害が、他のテナントの環境に影響を及ぼす可能性があります。また、他のテナント利用者が不正行為を働く可能性もないわけではありません。

NEC Cloud IaaS では、適切なリソース監視を行っていますが、マルチテナントに起因するリスクを完全に回避することはできません。お客様はこのリスクを軽減するために、適切なサーバ・ネットワーク構成を行う必要があります。

NEC Cloud IaaS では、他テナントからの影響を軽減するため、お客様のリソースを専有するサービスを提供しています。スタンダードサービスの STD-Plus・ホストサーバ専有型や物理サーバサービスを利用することで他テナントの影響を軽減することができます。

DoS 及び DDoS 攻撃[12]

クラウドサービスはネットワーク経由で提供されるため、DoS 及び DDoS 攻撃をされた場合すべてのサービスが停止してしまう可能性があります。お客様は、あらかじめ DoS 及び DDoS 攻撃のリスクに対し、攻撃の防止・軽減を行い、期待通りのアプリケーション可用性を実現しなくてはなりません。

NEC Cloud IaaS では、お客様側で DoS 及び DDoS 攻撃への対抗手段を講じる際に有用となる侵入検知システム（以下 IDS[13] といいます）を提供しています。この IDS を用いたサービスは、後述の通り、DoS 及び DDoS 攻撃のパターンを検出・通報し、お客様側で必要な対処が実行可能となる監視サービスです。

ID 管理

NEC Cloud IaaS のセルフサービスポータルでは、独立した ID 管理を行っています。

そのため、お客様がすでに利用している ID 管理システムに連携し、一元的な ID 管理を実施するためのインターフェースはありません。お客様は、従来からの一貫したセキュリティ対策及び管理を行うにあたって、不正やミスの発生可能性を低くするなど、細心の注意を払った ID 管理を実施する必要があります。

NEC Cloud IaaS では、お客様環境のアクセス制御を強化する機能として、ID&アクセス管理機能を提供しています。ID&アクセス管理機能を利用することにより、お客様環境のリソースへのアクセスを安全にコントロールすることができ、運用担当者の特権 ID の利用に対して有効な統制を実施することができます。

アクセス制御

NEC Cloud IaaS では、共有サービスに最適化したアクセス制御を行っています。それらはお客様組織内であらかじめ定められたアクセスポリシーと異なる場合があり、お客様が独自に固有のアクセス制御を実現する必要がある場合があります。

お客様は NEC Cloud IaaS で提供するアクセス制御に加え、お客様組織内で要求されるアクセス制御を確実に実施する必要があります。

NEC Cloud IaaS では、お客様が様々なアクセス制御を実現するためにファイアウォールやロードバランサーを提供しています。さらに、ID&アクセス管理機能を利用することで特権を持つ運用担当者の作業など重要な作業の記録と蓄積を実施することができます。

5. NEC Cloud IaaS の利用におけるセキュリティ

5.1. サーバのセキュリティ

仮想インスタンスのセキュリティ

仮想インスタンスはお客様によって完全に管理することができます。お客様は、OS へのアクセス権、及びアプリケーションに対して、ルートアクセス権または管理コントロールを有しています。NEC Cloud IaaS は、お客様の仮想インスタンスに対するアクセス権を有しておらず、ゲスト OS にはログインすることができません。

インスタンスの分離

同一の物理マシン上で実行中の様々なインスタンスが、ハイパーバイザーを経由してお互いに分離されています。

インスタンス同士は、利用を許可されたネットワーク以外のアクセス方法を有することはなく、それらがあたかも物理的に分離したホスト上に存在しているかのようにあつかうことができます。

仮想ネットワークについて

NEC Cloud IaaS では、SDN（Software-Defined Networking）の概念を取り込み、レガシーネットワークと OpenFlow ネットワークのハイブリッド環境のネットワーク環境を構築しています。

ネットワークは、サーバ/ストレージ同様、集中制御され、セキュアで柔軟な仮想ネットワーク環境を構成しています。

お客様で作業した記録は、問題が発生した時等の原因調査で利用できるようログ情報として収集し、仮想ネットワーク設定作業の監視を日次で行っています。

グローバル IP アドレス

グローバル IP アドレスは、インターネットに直接接続することが可能な IP アドレスです。NEC Cloud IaaS で利用提供されるグローバル IP アドレスは、日本の IP アドレスとなります。

グローバル IP アドレスの利用では、セキュリティを十分に考慮する必要があります。グローバル IP アドレスをインターネットに公開することで様々な脅威による影響を受ける可能性があります。お客様サイトの改ざんやデータの流出等の被害を受ける可能性があります。また、ウイルスを仕込まれたり、他サイトへの攻撃の踏み台にされるなど加害者とされてしまう可能性もあります。外部からの脅威に対する影響を軽減するために、不必要なサービスを停止し、必要なポートのみアクセス許可する等の安全な設定を行ってください。ポートを開放する場合でも、アクセス元を制限する等、適切な制御と管理が重要です。

NEC Cloud IaaS では、ファイアウォールやロードバランサー、IDS 機能など外部

からの脅威を低減するための機能を提供しています。

プライベート IP アドレス

プライベート IP アドレスは、NEC Cloud IaaS 内のセグメントで利用する IP アドレスです。プライベート IP アドレスは、NEC Cloud IaaS で自動的に割り振ることも、お客様側の指定に従い設定することもできます。

NEC Cloud IaaS では、お客様毎に専用のプライベートネットワーク環境を提供しています。お客様のサーバは、お客様専用の仮想ネットワーク環境（仮想 NIC）を利用することで、他のユーザのネットワーク環境から隔離し、独立したネットワーク環境としてセキュアに利用することができます。

ゾーンについて

NEC Cloud IaaS では、仮想サーバの生成時に物理環境を指定して配置することができます。指定できる物理環境をゾーンと呼んでいます。

ゾーンは仮想サーバ作成時に仮想サーバ毎に指定することで、異なる物理サーバ上に仮想サーバを配置することができ、お客様システムの可用性を向上させることができます。冗長構成を必要とするシステム構成を組む場合、異なるゾーンに仮想サーバを配置することにより、物理障害発生時のお客様システムの影響を少なくすることができます。

ポートスキャニング

お客様による許可のないポートスキャニングは、NEC Cloud IaaS の使用ポリシーに違反します。許可のないポートスキャニングが検出された場合、それは停止されブロックされます。お客様側でお客様システムに対してポートスキャニングを行う場合、事前に NEC Cloud IaaS のポータルからご連絡をお願いします。

第三者によるパケットスニッフィング

実行中の仮想インスタンスが、異なるお客様の仮想インスタンス向けのトラフィックを受信することや傍受することは不可能です。お客様は自らのインターフェースをプロミスキャス・モード（無差別モード）にすることは可能ですが、異なるお客様の仮想インスタンスに対してトラフィックを伝送することはありません。

物理的に同一のホスト上に位置する、同一のお客様によって保有されている２つの仮想インスタンスであっても、通信内容を傍受することはできません。

物理障害発生時について

NEC Cloud IaaS では、物理障害発生時の標準機能として、HA (High Availability) 機能を提供しています。これはスタンダードサービス（STD)、ハイアベイラビリティサービス（HA)、両方で実現しています。万が一特定の物理ホストサーバが使用できなくなった場合、その物理ホストサーバで稼働している仮想サーバは自動的に別の物理ホストサーバに移行して自動的に起動します。これにより、サービスのダウンタイムを最小にすることが可能となっています。

また、ネットワークはすべて冗長化した構成を採っており、ストレージに関してもコントローラの 2 重化、DISK の RAID 構成を行っています。

5.2. セルフサービスポータルのセキュリティ

NEC Cloud IaaS のすべての運用操作は、セルフサービスポータルを介して行われます。セルフサービスポータルへのログインは、ID/パスワードによる認証で行われ、お客様環境に関する運用操作のすべてが可能となるため、推測されにくいパスワードの使用、及び定期的なパスワード変更を推奨しています。

なお、セルフサービスポータルはセキュリティ脆弱性診断/プラットフォーム診断ツールでの検査や、IDS（侵入検知システム）を利用した不正なアクセスの兆候検知など、NEC が定めるセキュリティ基準を満たして公開されます。

図 2　セルフサービスポータル画面例

マルチアカウント

NEC Cloud IaaS では、お客様のセルフサービスポータル上の操作範囲に制限を持たせたアカウントを複数作成することができます。

マルチアカウントで操作範囲の制限を行うことにより、複数人で同一の NEC Cloud IaaS を利用する場合や、協力会社や関連部署にインフラの運用を委託する場合などの利用において、利便性やセキュリティが向上します。

NEC Cloud IaaS のセルフサービスポータル上でお客様に提供するアカウント権限には、次の 3 種類があります。

テナント管理者	セルフサービスポータル利用において、契約時に最初に提供されるアカウントです。お客様は、管理者、運用者のアカウントの作成、管理、すべての機能の閲覧・操作、及び申請に対する承認を、このアカウントで行うことができます。 本アカウント権限は、テナントにおいて全承認権限を持ち、かつ、承認権限を管理者に対して付与（代行承認権限）することができる高権限アカウントです。お客様で適切に利用管理してください。
管理者	テナント管理者から代行承認権限を付与されている管理者向けアカウントです。 セルフサービスポータル利用において、サーバに対する操作（起動、停止、再起動、各種設定など）の申請に対して承認を実施することができるアカウント権限です。
運用者	リソースの作成、変更に対する承認権限はないが、セルフサービスポータルを利用できる運用者向けアカウントです。 セルフサービスポータル利用において、サーバに対する操作（起動、停止、再起動、各種設定など）を行うことができ、課金に関する操作（サーバやストレージの作成等）の申請を行うことができるアカウント権限です。

5.3. 基本監視

NEC Cloud　IaaS では、セルフサービスポータルを通じて、契約しているサーバに対しお客様自ら各種監視項目を設定・変更することができます。CPU の使用率やメモリ使用状況を監視するリソース監視を利用して、通常時の稼働状況とリアルタイムに比較することで、セキュリティ攻撃等の異常検知に役立てることができます。

また同様に、死活、ポート、リソース、ログ、プロセス、ネットワークを監視する仕組みが提供されています。設定した閾値を超えた場合、設定した任意のメールアドレスに対してアラートを通知する仕組みが提供されています。

死活監視では、NEC Cloud IaaS 環境と連携したハウジング環境のサーバに対しても、監視連携することができ、より統合的な運用管理を構成することができます。

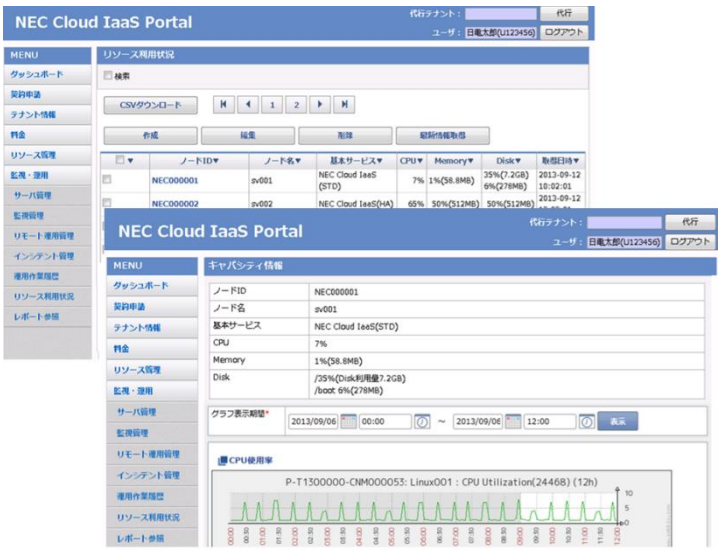


図 3　監視状況画面例

5.4. ファイアウォール機能

NEC Cloud IaaS では、用途に応じた 3 種類のファイアウォールメニュー（仮想ファイアウォール、物理・専用ファイアウォール、物理・共用ファイアウォール）を選択することができます。

広帯域のネットワークを利用するシステムでは、物理・専用、物理・共用ファイアウォールを利用することができます。スループットの目安としては 1Gbps となります。仮想ファイアウォールは、導入が容易であり、セルフサービスポータルから利用契約を行うことにより短時間での導入が可能です。

インターネット接続を利用する場合は、前出の通りインターネット側の接続インターフェースにグローバル IP アドレスが付与されます。ファイアウォールサービスとしては、インターネットと内部ネットワーク間でのフィルタリング、NAT、ルーティング機能を利用することに加え、内部ネットワークのサーバ間に対しての内部ファイアウォー

ルとしても利用可能です。内部ファイアウォールとしての利用では、複数のセグメントに分離したネットワーク構成間の通信を、目的に合わせてアクセス制限する等の柔軟なネットワーク構成を構築することができます。

5.5. IDS 機能

NEC Cloud IaaS では、ネットワークセキュリティサービスとして IDS（侵入検知システム）を利用することができます。IDS は、お客様ネットワークに設置されたファイアウォールを通過するパケットの監視を行います。NEC Cloud IaaS では、IDS を 24 時間週 7 日体制にわたってリモートで監視する運用代行サービスを提供しています。この運用代行サービスは、セキュリティの専門要員による高度な監視運用サービスです。

5.6. ID･証跡管理機能

NEC Cloud IaaS では、お客様システムの運用業務において、データベースへの直接操作やアプリケーションプログラムの変更作業などにおける不正操作に備え、重要なシステム操作を行うお客様要員の操作内容を画面遷移の動画とテキストで克明に記録し、操作内容の定期的な点検監査を実施することができる機能を提供しています。

NEC Cloud IaaS の ID&アクセス管理は、以下の機能があります。

- 管理対象サーバに対する ID/パスワード及びアクセス制御
- 利用者に対する作業申請・承認のワークフロー
- オペレータ作業の記録と蓄積

ID&アクセス管理は不正ログインの防止、作業誤りの特定、不正作業に対する抑止効果があります。本機能は、システム証跡監査ツールとして国内トップベンダーのエンカレッジ・テクノロジ株式会社の ESS AdminGate[14]を、NEC Cloud IaaS のソフトウェアサービスとして提供しています。

5.7. ロードバランサー

NEC Cloud IaaS は、オプションサービスとしてロードバランサー機能を提供しています。ロードバランサーを利用することにより、適切な負荷分散を実現するとともに、フロントエンドの仮想サーバのローカル IP アドレスとポートを隠ぺいすることが可能となります。NEC Cloud IaaS のロードバランサーは以下の機能があります。

・負荷分散機能
・SSL 暗号化・復号化機能

ロードバランサーは、物理・専用、物理・共用、仮想の 3 種類のサービスから選択することができます。

広帯域のネットワークを利用するシステムには、物理・専用、物理・共用ロードバラ

ンサーを利用することができます。スループットの目安としては 1Gbps となります。仮想ロードバランサーは、導入が容易であり、セルフサービスポータルから利用契約を行うことにより、短時間での導入が可能です。お客様は、利用する回線帯域、ファイアウォールの種類に合わせて選択可能です。

5.8. VPN サービス

NEC Cloud IaaS では、SSL-VPN、装置対向 VPN を提供しています。

SSL-VPN は WWW の暗号化などで標準的に用いられている SSL で、仮想回線を暗号化する VPN 技術です。SSL-VPN でアクセスする場合、インターネットに接続されたクライアント端末から SSL-VPN ゲートウェイにアクセスを行い、ユーザ ID/パスワードによるユーザ認証を完了することで、お客様環境内へのアクセスが可能となります。SSL-VPN はセルフサービスポータル利用開始から標準で利用できます。

装置対向 VPN とは、VPN 装置を用いたゲートウェイ型の VPN です。利用者サイトとデータセンター間を VPN 接続する機能として利用できます。データセンター側で用意した装置対向 VPN 機器と、利用者側で用意された装置対向 VPN 機器間で、VPN 通信を行います

データセンター側 VPN 装置としてファイアウォール機器の機能を利用するため、ご利用いただいているファイアウォール種別により、ご利用いただけるメニューが決定します。

利用者側には、指定の対向 VPN 装置を設置いただく必要があります。

5.9. データセンターのセキュリティ

NEC はデータセンターの設計、構築、運用において、長年の経験を有しています。その経験は、NEC Cloud IaaS プラットフォームとデータセンターインフラストラクチャに活かされています。また、NEC Cloud IaaS のデータセンターは、最新鋭のセキュリティ設備（金属探知機、顔認証設備、赤外線センサー）を利用し、専門のスタッフが、建物の入り口とその周辺両方において、物理アクセスを厳密に管理しています。権限を与えられたスタッフは顔認証（NEC の顔検出・顔照合エンジン「NeoFace®」は、米国国立標準技術研究所（NIST）の技術ベンチマークテストにおいて、世界一の精度を獲得しています）と連動した IC カード認証を用いて、データセンターフロアに入場します。すべての訪問者と契約事業者は、事前に入場を許可された者のみ IC カードを発行し入場が許可されます。

NEC Cloud IaaS のデータ保管場所である、神奈川データセンター、神戸データセンターは JDCC（特定非営利活動法人 日本データセンター協会）が制定した、日本国内のデータセンターに求められる信頼性を実現するためのファシリティ内容を定めた基準で、ティア 4（最高レベル）相当の仕様となっております。

※データセンターの詳細については、データセンターのご紹介資料を参照ください

火災検出と鎮火

NEC Cloud IaaS のデータセンターには、自動火災検知装置及び鎮火装置が取り付けられ、火災のリスクを軽減しています（超高感度煙検知設備、窒素ガス消火設備を設置）。

電力

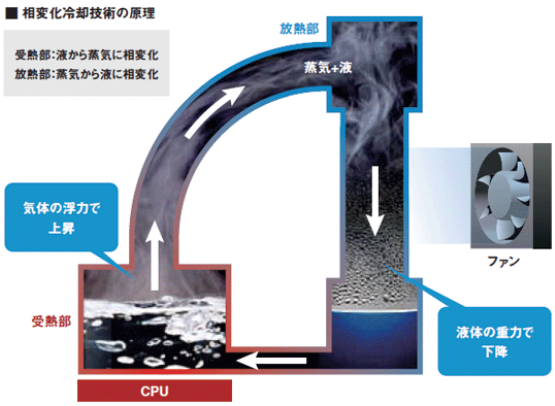
NEC Cloud IaaS のデータセンターの電力システムは、電力会社から本線・予備線による完全冗長化された受電方式を採用し、運用に影響を与えることなく柔軟な電力管理が可能となっています。

電力供給障害時には、非常用発電機を使用して施設全体のバックアップ電力を供給します。非常用発電機は冗長構成で設置され、商用電源停止時に 72 時間を超える連続運転が可能な発電機用燃料を備蓄しています。

また、施設内で重要でかつ不可欠な設備に対しては、無停電電源装置（UPS）を冗長構成で設置、停電時に約 10 分間のバックアップ電力を供給します。

冷却システムと温度

NEC Cloud IaaS のデータセンターでは、NEC が独自に開発してきた「相変化冷却技術」、及び「多段式高効率冷却技術」を利用した最新の空調システムを導入しています。相変化冷却技術とは冷媒が液体から気体に変化（気化）する際に熱エネルギーが移動する現象を利用し、動力を使わずに排熱を行う技術です。



多段式高効率冷却技術とは受熱部を多段に構成し、それを最適化した独自の冷媒流路設計を行うことにより、ラック内での冷却ムラを防ぎ、高い受熱効率を実現する技術です。

ファシリティ管理

NEC Cloud IaaS のデータセンターは、電気、機械、設備の稼働状況をモニタリングし、問題が速やかに特定されるように管理しています。また、予防的メンテナンスを実行し、これらのファシリティ設備が継続的かつ安全に運用するよう保たれています。

6. 関連文章

経済産業省のクラウドサービスセキュリティガイドライン

経済産業省が策定した、クラウドサービス利用に関わるリスク対応のためにクラウド利用者が実施すべき管理策を定めた基準書。正式名は「JIS Q 27002:2006 情報技術―セキュリティ技術ー情報セキュリティマネージマントの実践のための規範」。

利用者におかれましても、よりセキュアな環境構築のために、一度確認されることをお勧めいたします。

http://www.meti.go.jp/press/2013/03/20140314004/20140314004.html

CCM（Cloud Control Matrix）

CCM（Cloud Control Matrix）は、CSA（Cloud security alliance）が制定したクラウドコンピューティングのセキュリティを実現するためのセキュリティコントロールフレームワーク、及び法令、標準、基準へのマッピング情報です。

https://cloudsecurityalliance.org/

http://www.cloudsecurityalliance.jp/ (Japan Chapter)

FISC（The Center for Financial Industry Information Systems）

公益財団法人 金融情報システムセンター（FISC）が策定した「金融機関等コンピュータシステムの安全対策基準・解説書」（以下 FISC 安対基準といいます）は、金融庁が金融機関を検査する際に使用される「金融検査マニュアル」においても、検査官が具体的なシステム検査を行う際に参照するよう指定された金融機関のシステム安全対策基準書です。

https://www.fisc.or.jp/

PCI DSS（Payment Card Industry Data Security Standard）

PCIDSS とは、加盟店・決済代行事業者の皆様が取り扱うカード会員のクレジットカード情報・取引情報を安全に守るために、JCB、American Express、Discover、MasterCard、VISA の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グローバルセキュリティー基準です。

https://www.pcisecuritystandards.org/

7. まとめ

本書は NEC Cloud IaaS のセキュリティへの取組みを説明しています（ホワイトペーパー発行現在）。

セキュリティリスクは常に変化しています。それに合わせて各基準等も改版されており、対策も常に改善が必要です。セキュリティの脅威に対して継続的に取組み、安心、安全のクラウドサービスを NEC Cloud IaaS は提供していきます。

NEC Cloud IaaS 全体のセキュリティ向上のため、セキュリティに高い意識を持ってクラウド環境をご利用いただけますようお願い申し上げます。

---

[1] CCM：クラウドコンピューティングにおけるセキュリティ保証のためにベストプラクティスを推進する非営利団体 Cloud Security Alliance（ CSA :https://cloudsecurityalliance.org/）から提供されている、クラウドコンピューティングのセキュリティコントロールフレームワーク

[2] ISO/IEC 27001：国際標準化機構(ISO)と国際電気標準学会(IEC)が共同で作成する情報セキュリティ規格。組織が保有する情報に関わる様々なリスクを適切に管理し、組織の価値向上をもたらす情報セキュリティマネジメントシステムの国際規格

[3] ISO/IEC 27002：国際標準化機構(ISO)と国際電気標準学会(IEC)が共同で作成する情報セキュリティ規格。企業などの組織における情報セキュリティマネジメントシステムの仕様を定めたもの

[4] FISC：The Center for Financial Industry Information Systems(FISC)とは、公益財団法人 金融情報システムセンター（https://www.fisc.or.jp/）の略称で、金融情報システムの安全確保を目的とし、金融機関における各種の調査、研究を行っている。FISC から金融情報システムに関する安全対策の共通の基準として「金融機関等コンピュータシステムの安全対策規準・解説書」が策定発行されている

[5] JASA：Japan Information Security Audit Association(JASA)とは、特定非営利活動法人 日本セキュリティ監査協会(http://www.jasa.jp/)の略称で、情報セキュリティ監査制度の実施に関する活動を展開している。クラウドのセキュリティに関して「クラウドセキュリティ監査」が策定されている

[6] PCI DSS：Payment Card Industry Data Security Standards（PCI DSS）とは、加盟店やサービスプロバイダにおいて、クレジットカード会員データを安全に取り扱うことを目的として策定された、クレジットカード業界のセキュリティ基準。国際カードブランド 5 社（American Express、Discover、JCB、MasterCard、VISA）が共同で設立した PCI SSC（Payment Card Industry Security Standards Council）によって運用、管理されている

[7] COBIT：COBIT（control objectives for information and related technology）とは、米国の情報システムコントロール協会（ISACA: Information Systems Audit and Control Association）が提供する IT ガバナンスのフレームワーク

[8] SOC2：Service Organization Control 2(SOC2)は、クラウド事業者等のサービス提供会社の受託業務にかかる、セキュリティ、可用性、処理のインテグリティ、機密保持、及びプライバシーの各統制について、米国公認会計士協会（AICPA）の評価基準をもとに公認会計士が実施する内部統制評価報告の総称

[9] CAIQ：Consensus Assessments Initiative Questionnaire （CAIQ）は非営利団体 Cloud Security Alliance（CSA :https://cloudsecurityalliance.org/）から提供されているクラウドセキュリティ要件。CAIQ は、IaaS, PaaS, SaaS においてどのようなセキュリティコントロールが存在するかについて詳細な規準を質問形式で提供している。この質問票(CAIQ)は、クラウド利用者あるいはクラウド監査人が、クラウドプロバイダに対して確認する 140 以上の質問から成る

[10] NIST SP800-171: 米国国立標準技術研究所(以下、NIST)が定めているセキュリティ対策基準
米国の政府機関を中心に「NIST SP800-171」の定めるセキュリティ対策への対応を求める動きが加速しており、今後は米国の他業界や日本国内においても同様の基準を設け、対応を求める動きが広がっていくと見られている

[11] NDA：（Non-Disclosure Agreement）秘密保持契約。営業秘密や個人情報など業務に関して知った秘密を第三者に開示しないことを約す契約

[12] DoS 及び DDoS 攻撃 ：：DoS 攻撃(Denial of Service attack)は、可用性を侵害する攻撃手法で、サーバやネットワークなどのリソース（資源）に意図的に過剰な負荷をかけたり脆弱性をついたりする事でサービスを妨害する。DoS 攻撃の送信元を分散させ、さらに負荷を増大させたものが DDoS 攻撃(Distributed Denial of Service attack)である

[13] IDS：侵入検知システム（IDS: Intrusion Detection System）は、ネットワーク上などへの不正なアクセスの兆候を検知し、通報するシステム

[14] ESS AdminGate：エンカレッジ・テクノロジ株式会社（http://www.et-x.jp/index.html）が提供する、システム管理者による特権 ID の不正行為や情報漏えいなどを未然に防止するソフトウェア製品。ワークフローによる事前申請・承認に基づき、ID・パスワードおよびアクセスを制御し、操作記録を蓄積することができる

改版履歴

版数	作成日	変更内容
1.0	2014.10.31	初版作成
1.1	2015.10.07	3.4　SOC2 保証報告書の取得状況を追記 5.6　ID・証跡管理機能に関する説明を修正
1.2	2015.11.25	5.6　ID・証跡管理機能に関する説明から作業証跡管理機能に関する記述を削除
1.3	2016.06.27	5.9　データセンターのセキュリティ設備の説明を修正 5.9　火災検出と鎮火の説明を修正 5.9　冷却システムの説明を修正
1.4	2017.07.14	3.8　データ管理の説明を追記
1.5	2017.09.20	1.ホワイトペーパーの目的の説明を修正 3.4　各種認証の取得の説明に ISO/IEC27017、ISO/IEC27018、ISO/IEC22301 を追記 4.　中間者攻撃、ライセンス管理、マルチテナント、DoS 攻撃、ID 管理、アクセス制御の説明を修正 DoS 及び DDoS 攻撃の注釈を追加 5.　グローバルアドレスの説明を修正 データセンターのセキュリティの説明を修正 冷却システムの説明を修正
1.6	2018.05.10	3.1 基準等の事例に NIST SP800-171 を追記 3.4 各種認証の取得の説明に ISO/IEC20000、ISO9001 を追記 文末注釈に NIST SP800-171 を追記
1.7	2019.04.04	3.4 各種認証の取得の説明に PCI DSS を追記 誤記、表現などを修正
1.8	2019.11.8	3.4 PCI DSS の記載を削除
1.9	2020.7.6	3.3　データの処理業務を行う再委託先を追記 5.9　データの保管場所の説明を追記
2.0	2020.11.30	2.NEC Cloud IaaS とはにある図 1　NEC Cloud IaaS の全体像を差し替え 5.1　サーバのセキュリティに仮想ネットワークの説明を追記