内部統制手法を活用した堅牢なセキュリティサービス

清水 美欧　宮地 均　坂上 武史　碩 正樹

要 旨

クラウドは、その性質上、常にセキュリティの脅威にさらされています。NEC Cloud IaaSは、オペレーションセンターで外部からの脅威に対して監視を行い、セキュリティ確保に努めています。また、専門のセキュリティ組織と連携し、システムの安全性向上を図っており、内部統制対応としてSOC2レポートなどの内部統制保証報告書を取得し、お客様の内部統制監査対応の負荷軽減に貢献しています。

本稿では、NEC Cloud IaaSをシステムの脅威から守る「セキュリティサービス」について紹介します。

KeyWords
クラウド･コンピューティング／内部統制／セキュリティサービス／SOC2／内部統制保証報告書／NEC Cloud IaaS／米国公認会計士協会（AICPA）／ID&アクセス管理

1. はじめに

情報システムの導入・運用コストの軽減を期待することができるコンピュータの新しい利用形態として「クラウド・コンピューティング」（以下、クラウド）が注目されています。

クラウドサービス利用が拡大するにつれ、外部脅威対策やコンプライアンスへの対応が重要になってきています。しかしながら、クラウドサービスの利用においては、クラウドサービス事業者の管理下で他の利用者とコンピュータ資源を共有するため、情報の機密性・完全性・可用性に関わる情報セキュリティ管理の実態が把握しがたいといった問題が生じる可能性があります。

本稿では、NECのクラウド基盤サービスである「NEC Cloud IaaS」がクラウドサービス事業者として実施するセキュリティ対策、内部統制の取り組み、及びクラウド利用者が自らのシステムの内部統制をする支援サービス「セキュリティサービス」について紹介します。

2. NEC Cloud IaaSのセキュリティ対策

（1）セキュリティへの考え方

NEC Cloud IaaSでは、業界団体、標準化団体が発行するセキュリティ規格や基準、クラウドのセキュリティガイドライン（CSA CCM、ISO/IEC27001-27002、FISC安全対策基準、JASA、PCI DSS など）を網羅した独自のクラウドセキュリティ基準を策定・整備しました。この基準をベースとしてNEC Cloud IaaSでは、各サービスが一定のセキュリティ品質を継続的に担保するための取り組みを行っています。

NEC Cloud IaaSでは、規定したセキュリティ方針が遵守されているか検証するために、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診しています。更に、セキュリティの脅威に対して迅速かつ的確に対応するため、社内のセキュリティ専門チームであるCSIRT（Computer Security Incident Response Team）や情報システム部門と情報連携し、各種の脅威・脆弱性情報の早期発見や適切な対処を行っています。

（2）内部統制保証報告書制度への取り組み

クラウド利用者にとって、自らの内部統制を向上させるためには、クラウドサービス事業者がどのような内部統制を実施しているかを理解する必要があります。しかし、クラウド利用者自身が複雑なクラウドの仕組みを確実に理解することは難しく、更にクラウドサービスのセキュリティ強度や信頼性の判断は困難となります。

NEC Cloud IaaSでは、内部統制保証報告書の取得を通じて、自らが構築・運用しているインフラ基盤の内部統制の有効性を、独立した第三者機関により客観的な立場で検証を受けています。これにより、クラウド利用者は直接NEC Cloud IaaSの内部統制の有効性を確認する必要はなく、第三者が保証した報告書を手に入れるだけで、NEC Cloud IaaSの内部統制を評価することができます。

NEC Cloud IaaSは、米国公認会計士協会（American Institute of Certified Public Accountants：AICPA）が定めたSOC報告書（Service Organization Control report）という制度を採用しています。そのうち次の2種類の保証報告書の取得に取り組んでいます（2015年4月より提供予定）。

1）SOC1保証報告書

財務諸表に関わる委託業務の内部統制の保証報告書であり、クラウド利用者の財務諸表監査に利用可能です。

2）SOC2保証報告書

SOC1が財務諸表の信頼性に限定されているのに対し、SOC2はより広範囲なシステムリスクに関わる内部統制の保証報告書です。クラウド利用者が自らの内部統制に利用可能です。

特に、SOC2は、情報セキュリティ全般に関わる内部統制を対象にできるため、利用者にとってNEC Cloud IaaSのセキュリティを評価するのに最適となります。

これらの評価情報は、既存・新規のお客様に対してNDAに基づいて開示されます。

（3）その他の外部認証の取得

NEC Cloud IaaSは、この他にも、外部の認証機関と協力し、NECが構築及び運用しているポリシー、プロセス、及び統制に関する認証を取得しています。

・ISMS（JIS Q 27001）
・プライバシーマーク（JIS Q 15001）

お客様のビジネスシーンで多く活用されるクラウドサービスとして、NEC Cloud IaaSはデータの安全性とプライバシーを保持するため高水準のセキュリティを維持しています。

また、NEC Cloud IaaSでは、最適な基盤運用体制を構築し、アクセス統制や作業のモニタリングなど、運用要員への適切な統制を図る体制を設けています。

更に、独立の内部監査部門を設置し、定期的な監査と改善促進により、セキュリティの統制レベルの向上に取り組んでいます。

3. クラウド利用者の内部統制

NEC Cloud IaaSでは、NECの内部統制システム構築及びセキュリティ専門部隊のノウハウと、エンカレッジ・テクノロジ株式会社と共同開発したID&アクセス管理技術に基づいた、ID&アクセス管理サービスを提供しています。ID&アクセス管理技術は、NEC Cloud IaaSのサービスを提供する基盤システムに実装したもので、そのノウハウを活用したサービスとして、NEC Cloud IaaSを利用する企業・団体のセキュリティ・内部統制を強化することができます。

本サービスは、以下の機能を提供することにより、システム運用者による情報漏えいや不正行為、システムトラブルなどを未然防止することができます。

3.1 ID&アクセス管理（作業証跡管理）

ID&アクセス管理サービスは、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、重要なシステムの操作内容を克明に記録し、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。お客様要員の操作内容を、画面遷移の動画とテキストによりすべて記録します。

本機能は、各個人のシステム操作画面を自動記録し、かつ、オペレーションログなどの操作履歴情報と同時に照合・保管し、それらの記録内容を検索・再生することで内外の監査に活用するとともに、リアルタイムに不正行為を検知・通報するなど、未然にセキュリティインシデントを抑止するものです。この機能を利用することで、不正操作・誤操作に起因するシステムトラブルや情報漏えいなどのセキュリティリスクを低減させ、システム運用操作に対する点検・監査作業をより効率的・実証的に実施することが可能となります。

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のエンカレッジ・テクノロジ株式会社のESS RECを、クラウドサービス用に共同開発したサービスとして提供しています。

機能詳細1：パスワードを知らせずにアクセスを許可

アクセスを許可されたオペレーターが管理対象サーバ

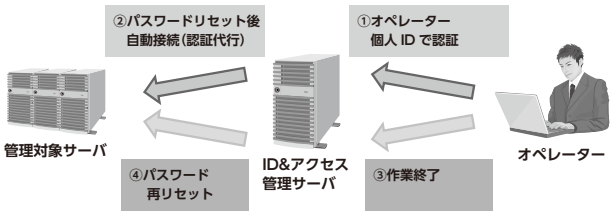

図１　パスワードを知らせずにアクセスを許可

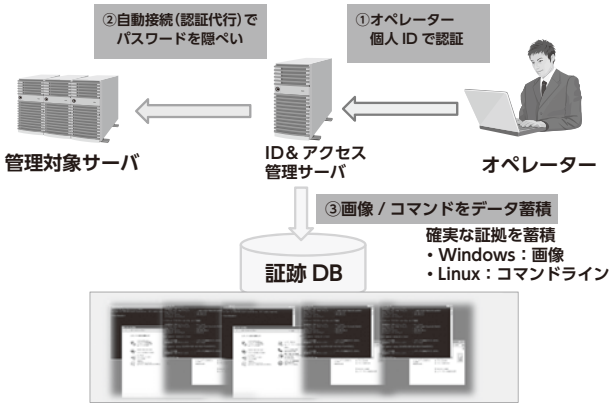

図２　動画・テキストによる詳細な操作記録

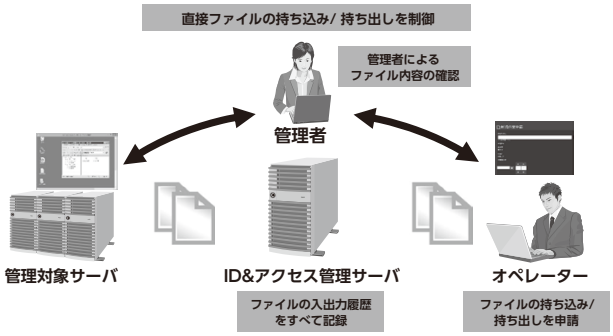

図３　サーバからのファイル入出力制御

にアクセスする場合、ID&アクセス管理のサーバは管理対象サーバのパスワードを毎回自動変更し、変更したパスワードを利用して自動接続を行います。

管理対象サーバにはID&アクセス管理で自動的に割り振られたパスワードのみがセットされており、ID&アクセス管理サーバ経由以外の経路からのアクセスを禁止します（図1）。

オペレーターは許可されたサーバへのアクセスのみが可能であり、許可されたサーバを踏み台にした他サーバへのアクセスを事実上不可能にしています。

詳細機能２：動画・テキストによる詳細な操作記録

システム運用においては、アプリケーションやデータベースへ直接の操作を行うための特別な権限（特権ID）を利用することが避けられないため、権限の濫用や利用者の不注意などによる誤操作がもたらすリスクへの対処が必要となります。

特に高い技術を有する権限者に対する統制が必要です。技術知識の豊富なシステム運用担当者の特権IDの利用に対して有効な統制を行うためには、ITを利用した仕組みを活用するだけではなく、適正な権限の利用や、あるいは利用者の不注意による誤操作が発生した場合でも、すぐに発見できる仕組みの構築に重点を置くことが重要となります。

更に、システム運用業務の作業内容の妥当性を客観的に判断する方法として、詳細な作業記録は有効かつ重要な手立てとなります（図2）。

作業内容・作業結果を綿密に点検・監査することで、正当な理由のない操作や不注意による誤操作を早期に発見し対処できます。

詳細機能３：サーバからのファイル入出力制御

ID&アクセス管理サーバ経由でアクセスする管理対象サーバへのファイルの持ち込み/持ち出しは、すべて管理されます。許可なくファイルを持ち込み/持ち出しすることを防止することで、情報漏えいを防ぐことができます。

オペレーション上必要なファイルの持ち込み/持ち出しは、いったんID＆アクセス管理サーバで管理され、管理者の許可によりファイルを持ち込み/持ち出しすることが可能となります。

持ち込み/持ち出しされたファイルは履歴としてすべて記録されており、オペレーターが管理者の許可なくサーバから機密情報を持ち出すといったリスクを回避することができます（図3）。

詳細機能４：不正ログイン管理機能（ログイン突合）

ID&アクセス管理機能では、セキュリティ機能の強化として不正ログイン管理機能（ログイン突合）があります。本機能はサーバからのログイン履歴を収集し、不正なアクセスの有無を検出する機能となります。これにより、万が一外部からの不正侵入や、許可を得ていない不正アクセスが発生した際の早期検知を行います。

更に、禁止コマンドのアラート機能により、許可された

操作以外のオペレーションが実施されると、即座に検知し管理者にアラートを通報します。これにより、不正操作に対する即時対応が可能であり、許可されたオペレーターの許可されていない操作を即時に発見、対応することが可能となります。

4. むすび

以上、NEC Cloud IaaSのセキュリティ対策と、NEC Cloud IaaS上で構築するお客様システムに内部統制手法を活用した堅牢なシステムの構築を支援するセキュリティサービスに関して紹介しました。

NEC Cloud IaaSは、お客様のシステムに対して統一的な内部統制強化を容易にかつ効率的に実現する機能を提供していきます。

執筆者プロフィール

清水 美欧
サービスデリバリ事業部
主席サービス事業主幹

宮地 均
サービスデリバリ事業部
サービス管理部
エキスパート

坂上 武史
サービスデリバリ事業部
サービス管理部
主任

碩 正樹
サービスデリバリ事業部
サービス管理部
主任

関連URL

NEC Cloud IaaS
http://jpn.nec.com/cloud/service/platform_service/iaas.html

エンカレッジ・テクノロジ株式会社
http://www.et-x.jp/

NEC 技報のご案内

NEC技報の論文をご覧いただきありがとうございます。
ご興味がありましたら、関連する他の論文もご一読ください。

NEC技報WEBサイトはこちら

NEC技報(日本語)　　NEC Technical Journal(英語)

Vol.67 No.2　ICTシステムを担うこれからのクラウド基盤特集

ICTシステムを担うこれからのクラウド基盤特集によせて
NECのクラウド基盤への取り組み

◇ 特集論文

NEC C&Cクラウド基盤　NEC Cloud IaaSのサービス
マルチ環境統合を実現するポータルサービス
多用途環境に対応するハイブリッド型サーバサービス
多様なネットワーク環境を提供するネットワークサービス
内部統制手法を活用した堅牢なセキュリティサービス
クラウド基盤を支えるデータセンターサービス

NEC C&Cクラウド基盤を支える製品、最新技術
運用の自動化によりトータルコストを最適化する「WebSAM vDC Automation」
運用自動化により効率的な管理を実現する統合運用管理基盤
データセンターのTCO削減に貢献するマイクロモジュラーサーバ及び相変化冷却機構
クラウド環境に適した高信頼基盤を提供するiStorage M5000
データ保存に最適な、優れた圧縮効率と高速性を両立するiStorage HSシリーズ
大規模データセンターの管理自動化をサポートするSDN対応製品 UNIVERGE PFシリーズ
省電力を実現する相変化冷却技術・熱輸送技術

NEC C&Cクラウド基盤の将来技術
低コスト・省電力・低フットプリントを実現するアクセラレータ活用技術
スケールアップにより多種多様なコンピューティングを実現するResource Disaggregated Platform
クラウド環境を対象にしたモデルベース設計支援技術
モデルベースでのサイジングと構成管理によりクラウド上のSIを効率化するクラウド型SI
ビッグデータ分析とクラウド ～異常を見抜くインバリアント分析技術～

導入事例
クラウドで遠隔監視保守システムの安定稼働を実現　全国約1,100基のタワーパーキングの安全を支える
ビジネスの中核を担うシステムをNEC Cloud IaaSへ移行　NECのトータルサポート力を評価
クラウド基盤サービスでグループのIT環境を共通化　ITガバナンスのさらなる強化を目指す

◇ NEC Information

C&Cユーザーフォーラム&iExpo2014
Orchestrating a brighter world　世界の想いを、未来へつなげる。
基調講演
展示会報告

NEWS
2014年度C&C賞表彰式典開催

Vol.67 No.2
(2015年3月)

特集TOP