クラウドコンピューティングにおけるセキュリティ確保の取り組み

Measures for Ensuring Security in Cloud Computing

高原 清 Takahara Kiyoshi
永井 康彦 Nagai Yasuhiko
受田 賢知 Ukeda Masaharu

クラウドコンピューティングの特徴は，クラウド事業者が提供するネットワーク，サーバ，ストレージなどのITリソースを不特定多数の利用者が共用することにある。複数の利用者が同一ITリソースを使用することにより，情報漏洩や他利用者からの影響などの危惧が生じる。さらに，システムがクラウド事業者の管理下にあることから，自社内では可能だったコンプライアンス確保も課題となる。
日立クラウドソリューション「Harmonious Cloud」は，クラウドに特有のセキュリティの確保に取り組んでいる。

1. はじめに

クラウドコンピューティングの誕生により，IT（Information Technology）システムを「所有」せずに「利用」することが可能となった。クラウドの巨大リソースを不特定多数が共用することによって，効率化の実現からコストの削減がもたらされた。一方でクラウドの利用者数増加に伴い，社会的影響が大きくなったことで，障害時の業務継続や情報セキュリティの確保などが課題になっている。

このような状況から，社会基盤化するクラウドに対し，セキュリティの面で国内外の公的機関や業界団体によるガイドラインなどの制定が進められている。

日立グループは，クラウドサービスの安全・安心を実現するため，これらガイドラインなども踏まえながら，種々の取り組みを行っている。

ここでは，クラウドコンピューティングにおけるセキュリティ確保の取り組みについて述べる。

2. セキュリティの観点からのクラウドの特性

2.1 リソースの共用と独立性

クラウドコンピューティングでは，クラウド事業者が提供するITリソース（ネットワーク，サーバ，ストレージなど）を不特定多数の利用者が共用する。通常，ビジネス向けのクラウドシステムでは，利用する企業（テナント）ごとに，仮想化技術などを用いて相互に独立した環境を提供している（図1参照）。しかし，物理的には同一のITリソースを使用することから，テナント間の「独立性」の強度が，クラウドにおけるセキュリティの最重要項目となる。独立性に関しては，以下のような項目が考えられる。

(1) データの独立性

ほかのテナントによるアクセスから自社のデータが防護されており，使用を終了したストレージ中のデータ消去など，ライフサイクル全体にわたる措置がなされていること

(2) 性能の独立性

あるテナントの処理負荷が，ほかのテナントの性能に影響を与えず，性能負荷の伝播（ぱ）が局所化され，限定されること

一般に，(2) については，多くのクラウドサービスは「ベ

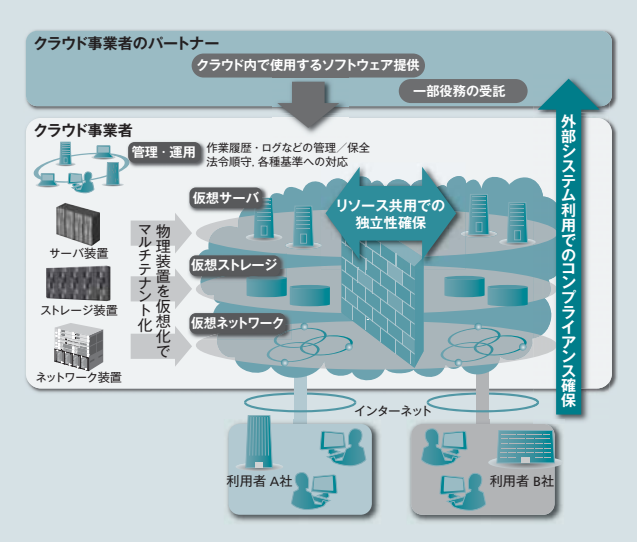


図1 | セキュリティの観点からのクラウドの特性
従来の情報セキュリティに加え，クラウドの特性である共用，社外利用に対し，独立性やコンプライアンスの観点が考慮されなければならない。

ストエフォート」であるとし，処理速度などはクラウド全体の負荷状況に左右されるとしている。しかし，企業活動にとって重要なシステムもクラウドへと移行しようとしている現在では，看過できない要素となっている。

2.2　外部システム利用とコンプライアンス

さらに，クラウドコンピューティングでは，自社内では可能だったコンプライアンス確保も課題となる。情報システムにおける法令・規制・契約を順守するためのコンプライアンスは，システムが自社の管理下にある場合，ログなどの証跡保持，モニタリングの実施などによって確保することが可能である。他方，クラウドにおいては，このような措置はクラウド事業者の中で行われる。このため，利用者がコンプライアンスに関わるような事象を把握し，検証するための手段が必要となる。

これについては，クラウド事業者との間で，証跡（例：作業履歴，ログデータ）の保全やモニタリング項目（例：応答性能，外部からの攻撃数）の計測をSLA（Service Level Agreement）などで規定し，利用者側で捕捉するなどの方法が考えられる。

3.　クラウドセキュリティに関する動向

3.1　国内の動向

上述のとおり，クラウドコンピューティングでは，クラウド独自の特性に応じたセキュリティ対策が必要となっている。クラウドの普及が進む中，公的機関・業界団体などがクラウドセキュリティに関する各種のガイドラインを策定している（**表1**参照）。

総務省による「ASP（Application Service Provider）・SaaS（Software as a Service）における情報セキュリティ対策ガイドライン」は，安全性・信頼性に対する事業者の情報開示を促進することを目的としている。一般財団法人マルチメディア振興センターは，このガイドラインなどを根拠として「ASP・SaaS安全・信頼性に係る情報開示認定制度」を運用している。この認定制度では，事業者やサービスの安全・信頼性に関する情報について開示項目を規定している。外部システムの利用に関し，利用者がその評価を可能とすることを目的とした制度と言える。

経済産業省が策定した「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」では，利用者向け手引き事項，事業者向け要望事項を中心としつつ，事業者が対応すべき要望事項が整理されている。このガイドラインは，情報セキュリティ規格群ISO/IEC 27000シリーズでの標準化に向けて日本から提案され，現在，標準化作業が進められている。

双方のガイドラインに共通する点は，ISO/IEC 27002を基本に，クラウドの特性に応じた管理策の応用を行っていることにある。主な観点として次の三つが挙げられる。

(1) 事業者から利用者へのセキュリティ対策情報の開示
(2) セキュリティ対策責任分担の明確化
(3) 利用者資産や利用サービス状況の利用者への可視化（監視機能の提供）

官公庁調達事案では，以前から内閣官房情報セキュリティセンター（NISC：National Information Security Center）が政府機関の情報セキュリティを全体的・共通的に向上するために「政府機関の情報セキュリティ対策のための統一基準群（管理基準，技術基準）」を発行している。クラウド利用の要件として，最近の改訂で以下の項目などが加えられた。

(1) 海外のデータセンターに情報を保存する場合の留意点
(2) 事業者間の管理責任範囲の明確化

3.2　海外の動向

海外でのクラウドセキュリティに関する動向としては，米国に本拠を置く非営利法人のCSA（Cloud Security Alliance）の活動が挙げられる（詳細は56ページ参照）。

CSAは，日本支部が設立されている。また，独立行政法人情報処理推進機構（IPA：Information-technology Promotion Agency，Japan）は，クラウドセキュリティに関する調査研究，普及啓発，教育，対策・指針策定などを目的に，CSAと相互協力協定を締結している。

欧州では，ENISA（European Network and Information

表1｜国内の主なクラウドセキュリティガイドライン
公的機関・業界団体などからガイドラインが提示されている。

発行省庁	ガイドライン	対象範囲		特徴	備考
		利用対象	適用対象		
総務省	ASP・SaaSにおける情報セキュリティ対策ガイドライン	クラウドサービス事業者	SaaS（ASP）	・ASP/SaaSに焦点 ・ISO/IEC 27002を参考	事業者の情報公開に関する認定制度
経済産業省	クラウドサービス利用のための情報セキュリティマネジメントガイドライン	クラウドサービス事業者（事業者への要望事項を含む）	クラウドサービス全般	・ISO/IEC 27002をベース ・利用者向け:手引き事項 ・事業者向け:要望事項	ISO/IEC 27000シリーズに日本から提案
内閣官房情報セキュリティセンター（NISC）	政府機関の情報セキュリティ対策のための統一基準群（管理基準，技術基準）	政府機関担当者，官公庁調達担当者など	政府機関担当者	・官公庁共通の情報セキュリティ対策の統一基準	2011年版からクラウド利用の観点が追加

注：略語説明　ASP（Application Service Provider），SaaS（Software as a Service），NISC（National Information Security Center）

Security Agency：欧州ネットワーク情報セキュリティ庁）が，「クラウドコンピューティング：情報セキュリティ確保のためのフレームワーク」，「クラウドコンピューティング：情報セキュリティに関わる利点，リスクおよび推奨事項」を発行するなどの活動を行っている。

4. クラウドセキュリティに関する日立グループの取り組み

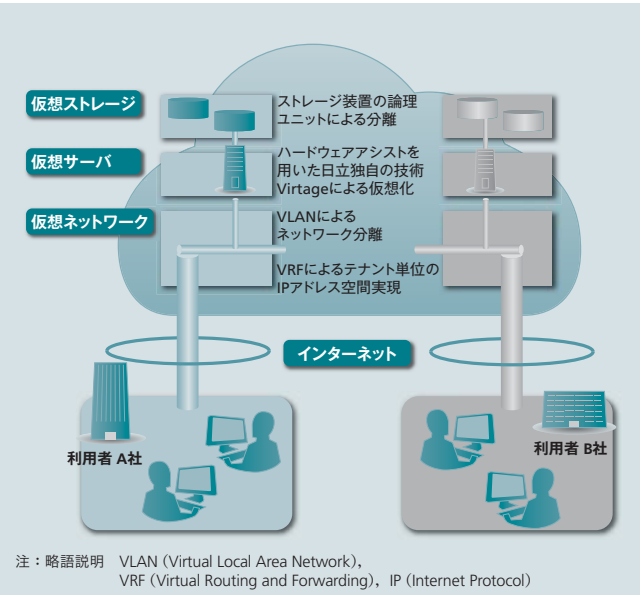
日立クラウドソリューション「Harmonious Cloud」では，「安全・安心」，「スピード・柔軟」，「協創」を中心コンセプトとしている。これらのうち，安全・安心を確立するため，Harmonious Cloudでは，クラウドを支える基盤，データセンター，運用など各面でクラウドセキュリティの確立を図っている。

ここでは，Harmonious Cloudのパブリッククラウドサービスの一つである「プラットフォームリソース提供サービス」〔PaaS（Platform as a Service）/IaaS（Infrastructure as a Service）〕を例として，その具体的な内容を紹介する。

4.1 テナントの独立性の確保

クラウドにおいては利用企業（テナント）間の独立性がセキュリティの重要な要素となる。PaaS/IaaSでは，ネットワーク，サーバ，ストレージの各層において独立性が確保されなければならない。プラットフォームリソース提供サービスでは，日立独自のプラットフォーム技術を用いてテナント間の独立を実装している（**図2**参照）。

性能の独立については，これらに加えて以下の技術を用いて，他のテナントの負荷に影響されずに所定の処理能力を提供できる手段を用意している（**表2**参照）。



注：略語説明　VLAN（Virtual Local Area Network），VRF（Virtual Routing and Forwarding），IP（Internet Protocol）

図2｜プラットフォームリソース提供サービスでのテナント独立性確保
日立グループのプラットフォーム製品が持つ技術を活用し，強力な独立性を確保している。

表2｜プラットフォームリソース提供サービスでの性能の独立性確保技術
重要な企業システムに必要な一定した処理速度の提供を可能とした。

インフラ層	性能の独立技術	内容
ネットワーク	データセンター内ネットワークシェーピング	仮想LANが使用する帯域を確保物理LANの輻輳（ふくそう）を回避
サーバ	Virtageによる物理CPU，I/Oの占有	CPU，I/Oを占有常に一定の処理能力を確保
ストレージ	I/Oパスの占有（計画中）	サーバとストレージ装置間で一定の伝送速度を確保

注：略語説明　CPU（Central Processing Unit），I/O（Input/Output），LAN（Local Area Network）

クラウドの誕生期においては，一時的なITリソースの利用によるコスト削減が求められたが，現在では，基幹システムへの適用が加速している。日立グループは，この目的でのクラウド利用を可能とするため，「リソースの共用」と「テナントの独立」を両立させ，クラウドセキュリティを強固にしたサービスの提供を進めている。

4.2 体系的なクラウドセキュリティへのアプローチ

4.2.1 クラウドセキュリティチェックリストの整備

Harmonious Cloudでは，運用やコンプライアンスへの対応も含めたクラウドセキュリティの確立について，前述の各種ガイドラインなどを参考にしたクラウド全般をカバーする「クラウドセキュリティチェックリスト」の作成および評価を行っている。

クラウドの特性に応じたセキュリティの体系化として，チェックリストの分類軸にはCSAのドメインを採用した。作成当時のCSA V2.1ではRecommendation中心で個々の要件の記載が少なかったことから，経済産業省の「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」と，ENISAのガイドラインに採録された項目をまとめて統合することで，網羅性の確保を図った。さらに，以下の分類を行って確認の便を図っている。

(1) 対象：IaaS／PaaS／SaaS／利用者のいずれに適用されるか。

(2) 施策実装：ITシステムの機能として実装されるか，管理や運用手続きとして実装されるか。

このチェックリストにより，遺漏なくセキュリティ施策が講じられる素地を確立した。

4.2.2 クラウドセキュリティチェックリストの例

CSAにおいてドメイン4として規定されている「コンプライアンスと監査」を例として，チェック観点・内容を紹介する。

顧客によるコンプライアンスは，クラウドサービスの中でも順守されなければならない。これを担保・検証するための監査が必要となる。それを実現するためには，顧客による監査を可能とする以下のような項目を整備することが求められる。

(1) 監査に必要な証跡の提示が可能であること（IaaS/PaaS/SaaS）
(2) クラウドサービスの契約において自社のコンプライアンスを満足するかという検証を行うこと（利用者）

一般に，クラウド事業者はデータセンターのオペレーション，回線確保などを外部に委託している。コンプライアンスに関する項目はクラウド事業者の社内だけではなく，委託先についてもクラウド事業者が統制していることが必要となる（**図3**参照）。そのため，委託先に，自社と同等の統制・監査が可能であることも必要となる。

4.2.3　チェックリストを利用しての施策／評価

プラットフォームリソース提供サービスでは，「コンプライアンスと監査」について，以下のような施策により，顧客が要求する水準でのコンプライアンスの実現を可能としている。
(1) 顧客と日立グループの間での責任範囲，監査および報告方法を明確化し，契約で規定する。
(2) 必要に応じて，日立グループのセキュリティ対策の履行状況を報告する。
(3) システムおよび運用の一部を再委託するものがサービスに含まれる場合，日立グループの責任において管理する。
(4) 情報セキュリティの履行状況を確認する目的で顧客へ提出する報告のうち，顧客自身による確認が必要な情報については，契約で指定された期間にわたって収集し保管する。

このような取り組みは，CSAが規定するすべてのドメインについて実施している。さらに，逐次見直しを行い，継続・反復してセキュリティの水準を高めている。

クラウドセキュリティチェックリストは日立グループ内で共有され，同サービスだけでなく，Harmonious Cloudの各種サービスにおいても活用されている。

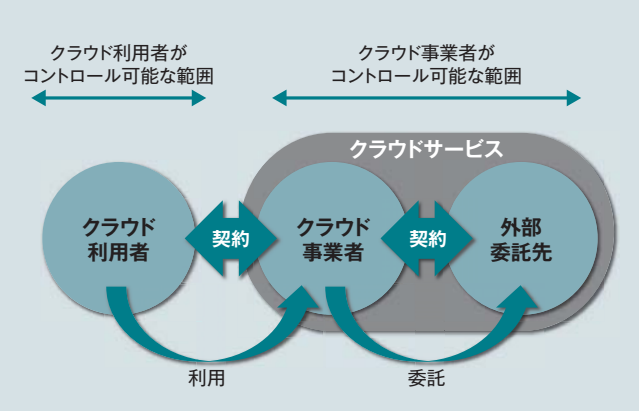


図3｜クラウドにおけるコンプライアンスの範囲
クラウド事業者だけでなく，その先のサードパーティを含めたコンプライアンスの検証が必要となる。

4.3　セキュリティ施策の公開

クラウドサービス提供者がセキュリティに関してどのような施策を行っているかは，利用者にとって重要な情報である。前述の取り組みの詳細については，「『安全・安心クラウド』を実現するための日立のセキュリティの取り組み―日立『プラットフォームリソース提供サービス』(PaaS/IaaS) を例として―」というホワイトペーパーにまとめ，広く一般に公開している。

5.　おわりに

ここでは，クラウドコンピューティングにおけるセキュリティ確保の取り組みについて述べた。

Harmonious Cloudは，これまでの製品提供やシステム開発などの中で日立グループが蓄積してきたセキュリティについてのノウハウを基礎とし，その上にクラウドの特性に応じたセキュリティへの取り組みを行うことで，安全・安心の具現化を図っている。

日立グループは，今後もこの取り組みを継続・発展させることで，安心して使える社会基盤としての役割を担うクラウドの実現をめざしていく。

参考文献など

1) 総務省：ASP・SaaSにおける情報セキュリティ対策ガイドライン，
http://www.soumu.go.jp/main_sosiki/joho_tsusin/policyreports/chousa/asp_saas/pdf/asp_saas_zentai.pdf
2) 経済産業省：クラウドサービス利用のための情報セキュリティマネジメントガイドラインの公表，
http://www.meti.go.jp/press/2011/04/20110401001/20110401001.html
3) 内閣官房情報セキュリティセンター：政府機関の情報セキュリティ対策のための統一基準，
http://www.nisc.go.jp/materials/index.html
4) 勝見：クラウドセキュリティアライアンスとその活動について，情報処理，Vol. 51，No. 12，情報処理学会 (2010.12)
5) 日立製作所：「安全・安心クラウド」を実現するための日立のセキュリティの取り組み―日立「プラットフォームリソース提供サービス」(PaaS/IaaS) を例として―，
http://www.hitachi.co.jp/cloud/solution/paas/platform.html

執筆者紹介


高原 清
1991年日立製作所入社，情報・通信システム社 ITサービス事業部 クラウド本部 クラウドソリューション開発部 所属
現在，Harmonious Cloudのサービス開発に従事
情報処理学会会員


永井 康彦
1985年日立製作所入社，株式会社日立コンサルティング ITコンサルティング&サービス本部 所属
現在，システムセキュリティデザインのコンサルティングに従事
工学博士
情報処理学会会員，電子情報通信学会会員，電気学会会員，日本航空宇宙学会会員


受田 賢知
2001年日立製作所入社，横浜研究所 情報サービス研究センタ サービスイノベーション研究部 所属
現在，クラウドコンピューティングの研究に従事
情報処理学会会員