JFE 技報 No. 28
（2011 年 8 月）p. 42–43

エクサのクラウド「E@CS®」を支えるセキュリティ基盤

Practical Security Infrastructure for EXA Cloud Service “E@CS®”

1. エクサのクラウドサービス「E@CS®」

1.1 エクサクラウドのサービスメニュー

IT 資産を開発・所有せず，サービスとして必要に応じて調達・利用するというクラウドサービスの実用化が進み，さまざまなサービスが利用できるようになってきた。エクサでは，現在，E@CS®（EXA Cloud Service）というブランド名称で，**図 1** に示すさまざまなサービスを開発中である。

エクサのクラウドサービスは，サーバなどの基盤環境を提供する IaaS (Infrastructure as a Service)，アプリケーションサービスを提供する SaaS (Software as a Service)，PC（パーソナルコンピュータ）のデスクトップ環境を提供する DaaS (Desktop as a Service，ThinClient)，およびファシリティ，ネットワーク，運用などからなる共通サービスで構成される。これらのサービスは，インターネットや専用線などを経由して利用できる。

IaaS には，開発・テスト用サーバを提供するサービスと，本番用サーバ向けのホスティング環境を提供するサービスがある。また，SaaS では，IT 資産管理，IT 機器監視，コラボレーション，およびエクサが強みを持つクレジットカードや設備管理などのアプリケーションを提供するサービスを予定している。

1.2 クラウドサービスのメリットと課題

クラウドサービスを利用するユーザー側のメリットは，コンピュータ機器やアプリケーションなどを所有しないことで，その保守や維持に関わるさまざまな作業やコストから解放されることにある。

また，クラウドサービスを提供する側のメリットは，仮想化技術の適用により，1 台の物理マシンの計算機資源（CPU，メモリ，ネットワーク，ストレージなど）を複数の企業向けの仮想マシンで共有させ，その使用を最適化し，効率化することにある。

当然ではあるが，これらメリットを享受するために解決すべき技術課題は少なくない。とくに，次の 2 点の解決が重要である。

(1) 著しいコンピュータハードの性能向上によるコストメリットを享受し続けるため，提供側としても所有することなく，常に最新のハードを利用したい。
(2) コンピュータ資源の仮想化と共有という形態が，新しいタイプのセキュリティ上の問題を引き起こす。一つの物理マシンの資源を複数の企業向けシステムが共用することになり，仮想環境に特化したセキュリティ対策が必要になる。

以下では，これらの課題を解決するためのエクサの取り組みについて述べる。

2. ハイブリッドクラウド〜クラウドでクラウドを造る

エクサのクラウドサービス環境は，クラウドをクラウドで作るというコンセプトで作られている。そのため，クラウド環境は，ハイブリッド的な構成，すなわち複数のクラウド環境を組み合わせて，1 つのクラウド環境のように利用でき，かつクラウド環境内では，さらに仮想マシンと物理マシンの

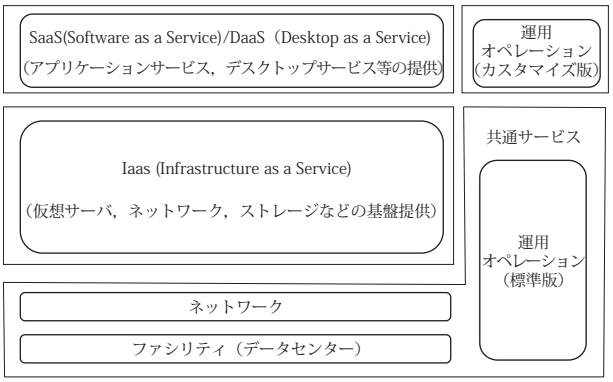

図 1　E@CS® のサービスメニュー
Fig. 1　Service menu of E@CS®

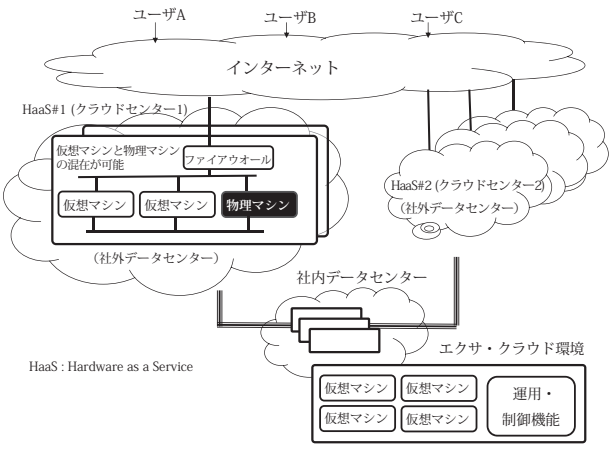

図 2　E@CS® の構成イメージ
Fig. 2　Construct of E@CS®

2011 年 4 月 5 日受付

組み合わせ利用を可能にしている。

エクサのクラウドサービスを構成するサーバは，**図 2** に示すように社内データセンターと社外データセンターに配置されている。

社外データセンターのサーバの実体は，アライアンス先のハードウエア提供サービスベンダーのサーバであり，社内と社外のサーバを，エクサのデータセンターから管理する。社外のサーバは，HaaS（Hardware as a Service) 形式で提供されるため，必要に応じて追加，返却が可能であり，常に時代に合わせて最適の HaaS を利用していくことにより，陳腐化しない競争力のあるハードウエア環境を安価に提供できる。

3. 仮想化セキュリティの実装

3.1 仮想環境における脅威

仮想環境における脅威は，大きく分けて**図 3** に示すように，仮想化に関係なく存在する脅威と，仮想化に関連した脅威がある。仮想化に関係なく存在する脅威は，物理マシンで存在する脅威に等しく，その対策は従来型の対策である。

仮想化に関連した脅威は，仮想化環境の外部に起因する脅威と，その内部に起因する脅威がある。外部に起因する脅威は，仮想環境，すなわちハイパーバイザ（仮想環境を制御する基本ソフトウエア）や仮想マシンに対する外部からのネットワークを介した攻撃などがある。内部の脅威は，ウイルスなどの脆弱性を含んだ旧い仮想マシンが休眠状態にあり，必要な状況が生じて起動され，仮想環境内に，その脆弱性が伝播するような場合などが考えられる。

3.2 セキュリティのコントロールモデル

クラウドサービスのセキュリティコントロールモデルは，サーバやネットワークなどに対する従来の考え方と，仮想環境に対する脅威を封じ込め，かつサービス形態 (IaaS や SaaS) を考慮した新しい考え方の融合になる。つまり，従来

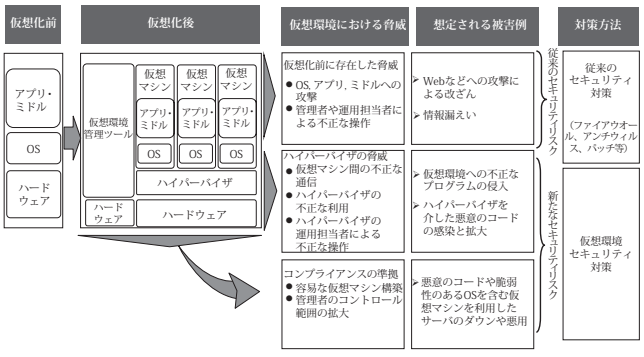

図 3　仮想化環境における脅威と対策

Fig. 3　Menace and measures in the virtualization environment

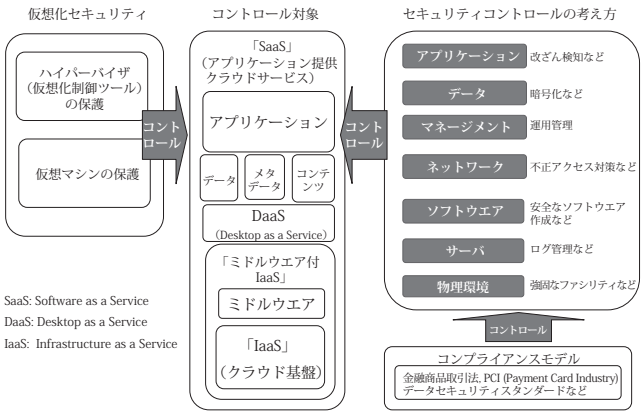

図 4　セキュリティコントロールモデル

Fig. 4　Security control model

のセキュリティの考え方をベースに，クラウド特有の事項を考慮した，より包括的なモデルが必要になる。

セキュリティのコントロールモデルは，一般的にアプリケーション，データ，管理，ネットワーク，ソフトウエア，サーバ，物理環境に分けてセキュリティのコントロールモデルを作る。E@CS® のセキュリティ基盤は，**図 4** に示すように，従来の考え方に，IaaS などのサービス境界線を加味した新しい考え方で作られている。これによって，仮想化と共有をベースにした IaaS 上で，論理的に隔離され，互いに防御された形で仮想マシンを安心して稼動させることができる。

4. おわりに

E@CS® では，仮想化セキュリティの考え方を導入し，仮想環境内のハイパーバイザや仮想マシンを保護するとともに，クラウドサービスのセキュリティコントロールモデルをベースに，必要な対策を実装している。具体的には，IaaS であれば，セキュリティ対策として，仮想マシンの隔離，データの保全性，仮想化環境の脆弱性対策，サービス継続性の確保，ユーザ認証，監査証跡などを実装している。

クラウドサービスを構成する IT 技術要素のスピードは極めて速く，E@CS® は，今後も時代の流れに適した形で，提供サービスの内容を変えて競争力を維持していくことになる。

競争の激しいクラウドサービスの中で，柔軟性を確保するためのハイブリッドという大きな特長と，クラウド時代に適したセキュリティを実装した E@CS® は，お客様に多くのメリットを安価に提供していけると確信している。

〈問い合わせ先〉
エクサ　クラウドサービス事業部　クラウドサービス営業部
TEL：044-540-2109　　E-mail：cloud-sales@exa-corp.co.jp