

クラウドセキュリティ部会 活動状況について

2011年11月21日

クラウドセキュリティ部会 部会長

塩崎 哲夫

■ 目的と背景

- 当部会は、クラウドにおけるセキュリティの課題解決・普及を促進する。
- 他部会のテーマ(ソーシャルクラウド基盤技術)や経済産業省(METI)、日本セキュリティ監査協会(JASA)で検討中のガイドライン等を踏まえ、クラウドのセキュリティに関する調査・検討を行う。

■ 活動状況

- 第1回(2011年6月24日)
当部会の設立の背景・趣旨、他部会のテーマ(ソーシャルクラウド基盤技術)について情報共有を行い、今後の活動テーマについてディスカッションを行った。
- 第2回(2011年7月21日)
活動テーマについて、各社の案を持ち寄りディスカッションを行った。当面、ターゲットをIaaSとし、METIのガイドラインの実装及びテスト手順の手引きの作成を検討することとした。
- 第3回(2011年8月25日)
METIのガイドライン10.2章(第三者が提供するサービスの管理)について、各社の実装例・実装案を持ち寄り、ディスカッションを行った。
- 第4回(2011年9月21日)
METIのガイドラインの10.5章(バックアップ)について、各社の実装例・実装案を持ち寄り、ディスカッションを行った。
- 第5回(2011年10月18日)
METIのガイドラインの10.10.1章(監査ログ)について、各社の実装例・実装案を持ち寄り、ディスカッションを行った。

■ METIのガイドライン “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”

- 特に技術に関わりが強い、10章:通信及び運用管理、11章:アクセス制御、12章:情報システムの取得、開発及び保守、14章:事業継続管理 を対象に検討する。

目次構成



・本ガイドラインの箇条5～15は、クラウド利用者がJIS Q 27002（実践のための規範）の箇条5～15の管理策を実施するための補足として活用できる。
・参考として附属書Aは、クラウドサービス利用に係るリスクを例示し、附属書Bは、クラウドサービス利用におけるリスクアセスメントの実施例の一つを示す。

序文

- 0.1 一般
- 0.2 クラウドサービス及び情報セキュリティ
- 0.3 このガイドラインの位置づけ及び構成

- 1 適用範囲
- 2 引用規格
- 3 用語及び定義
- 4 クラウドサービス利用における情報セキュリティガバナンス及び情報セキュリティマネジメント
 - 4.1 クラウドサービス利用における情報セキュリティガバナンス
 - 4.2 クラウドサービス利用における情報セキュリティマネジメント

- 5 セキュリティ基本方針
- 6 情報セキュリティのための組織
- 7 資産の管理
- 8 人的資源のセキュリティ
- 9 物理的及び環境的セキュリティ
- 10 通信及び運用管理
- 11 アクセス制御
- 12 情報システムの取得、開発及び保守
- 13 情報セキュリティインシデントの管理
- 14 事業継続管理
- 15 順守

附属書 A（参考）クラウドサービス利用に係るリスク
附属書 B（参考）クラウド利用におけるリスクアセスメントの実施例

活動成果のご紹介

■ 各社の実装例・実装案の整理 (10.5章「バックアップ」の機能に関して)

「何を」「いつ」「どうやって/どこに」の観点で、利用形態ごとのバックアップの実施内容をマトリクスにして比較。



利用形態

- ・オンプレミス
- ・パブリッククラウド
 - 富士通 FGCP/S5
 - 富士通FIP OVH(オンデマンド仮想環境ホスティング)
- ・プライベートクラウド
 - 日本電気 社内クラウド
- ・OSSクラウド
 - 富士通 Eucalyptus
 - NTTデータ OpenStack

バックアップ形態	いつ	どこ/どこに	パブリッククラウド	プライベートクラウド	Eucalyptus	
サーバー、ネットワークのレイアウト サーバーのスペック情報 (CPU/メモリ/ディスク容量) ネットワークの構成情報 (セグメント情報/FW/アドレス情報)	システム設計/変更時 サーバーの設置 - ネットワーク接続	構成情報を、資料(例:Excelなど)として作成・保存するか、構成管理ソフトウェア(例:Sysmanwalkerなど)を用いて自動収集・保存する	FGCP/S5(富士通) 利用者が作成テンプレートを作成することで、企業固有の仮想システムから仮想システムの構築を行うことができます(利用者のシステム管理者が実施)	オンデマンド仮想環境ホスティング(富士通/OP) 条件等	社内向けクラウドサービス(NEO) 条件等	CLOデータの保存(事業側の運用担当者)
サーバーの構成情報 (OSの基本設定など)	サーバーとネットワークの設定/変更時	OSの標準コマンドまたは専用ソフトウェアを用いて、別のディスク又は外部媒体にバックアップを行う	システムディスク/バックアップ-リスト及び「増設ディスク/バックアップ-リスト」を行うことができます(利用者のシステム管理者が実施)	オンデマンド仮想環境ホスティング(OVHのサブスクリプションサービスとして、富士通製品の機能であるOne Point Only(OPO)を利用し、ディスクを丸ごとバックアップ実施できる機能を提供している。 バックアップ媒体の世代管理(5世代が標準、(契約には、21世代まで実施) バックアップ媒体(Tape、DVD等)は、使用せず。スリージブレイクでのバックアップ。(数年毎書き換えバックアップツールは、毎年毎に換えていく) バックアップデータは、AESで暗号化されており、ネットワーク経路上の脅威を防止 バックアップ情報は、管理者及び利用者向けに作成。(利用者でのバックアップ運用が多い)	日時での差分バックアップがメイン。完全バックアップは利用者で行う。 条件等	Watusデータの保存(事業側の運用担当者) インスタンスのWatusへの登録(利用者のシステム管理者)
ネットワークの構成情報 (FWのルール/DNS設定/NTP設定)	サーバーとネットワークの設定/変更時	コンフィグをファイル出力するなどして保存する	FW/S5/ビルドインサーバのコンフィグ(設定内容)をバックアップ-リストを行うことができます(利用者のシステム管理者が実施) FW/ビルドインサーバのコンフィグバックアップはファイアウォールルールの他、DNS設定やNTP設定の情報もバックアップされます 条件等 コンフィグバックアップやコンフィグリストを実行するには、対象のビルドインサーバが稼働状態。またビルドインサーバ/バックアップ途中やビルドインサーバ/バックアップ中での必要がありませ	個別バックアップ等については特に対応せずお尋ねにて対応してまいります。 条件等	バックアップ媒体の遠隔地保管は、標準では実施せず。データセンター内の別ラックにて保管(顧客との契約により、遠隔地(九州や北海道等)での保管は実施)。 利用者は、クライアント標準データのバックアップ/リストに依存。 バックアップの機能は、ソフトウェア依存には実施せず。 仮想化は、VMwareでの実装が多く、バックアップもVMwareに依存の部分が大きい。(OSSの実装は今後実装予定) 運用中は、5人交替で運用して、事業継続の観点の可用性を確保している。 バックアップ装置自体は、データセンターの自然災害や長時間にバックアップ関連機器の故障はほとんど発生せず。	条件等 バックアップとして動作しているOSは継続しない。 インスタンスとして動作しているOSを最新イメージとし「Watus」に登録できる。 OSイメージとは別に継続ストレージEBSを利用することである。(その場合、EBSのバックアップが必要)
アプリケーションソフトウェア	アプリケーション設計/変更時	開発者が任意に実施する	システムディスク/バックアップ-リスト及び「増設ディスク/バックアップ-リスト」を行うことができます(利用者の開発者が任意に実施する) 条件等 ディスク全体をコピーする機能のため、ファイル/ディレクトリ単位のバックアップ-リストや、差分/増分バックアップ-リストを行うことはできません。 バックアップ-リストを行う仮想マシンは停止状態であればなりません。	個別バックアップ等については特に対応せずお尋ねにて対応してまいります。 条件等	条件等	SOIにあるEBSボリューム(本機ストレージ)のスナップショットを取得する 利用者のシステム管理者が任意に実施する 条件等
業務データ	運用中	開発者が任意に実施する	システムディスク/バックアップ-リスト及び「増設ディスク/バックアップ-リスト」を行うことができます(利用者の開発者が任意に実施する) 条件等 ディスク全体をコピーする機能のため、ファイル/ディレクトリ単位のバックアップ-リストや、差分/増分バックアップ-リストを行うことはできません。 バックアップ-リストを行う仮想マシンは停止状態であればなりません。	個別バックアップ等については特に対応せずお尋ねにて対応してまいります。 条件等	条件等	SOIにあるEBSボリューム(本機ストレージ)のスナップショットを取得する 利用者のシステム管理者が任意に実施する 条件等

活動成果のご紹介

■ 各社の実装例・実装案の整理 (10.5章「バックアップ」の機能に関して)

「何を」「いつ」「どうやって/どこに」の観点で、利用形態ごとのバックアップの実施内容をマトリクスにして比較。

バックアップ手順
標準的なバックアップ手順

何を	いつ	どうやって/どこに	パブリッククラウド		プライベートクラウド	Eucalyptus
			FGCP/S5	OVH	NEC社内向けクラウド	
サーバーの構成情報(OSの基本設定など)	サーバーとネットワークの設定/変更時	OSの標準コマンドまたは専用ソフトウェアを用いて、別のディスク又は外部媒体にバックアップを行う	“システムディスクバックアップ・リスト”及び“増設ディスクバックアップ・リスト”を行うことができます(利用者側のシステム管理者が実施)	オプションサービスとして、富士通製品の機能であるOne Point Copy (OPC) を利用しディスクを丸ごとバックアップ実施できる機能を提供している	日時での差分バックアップがメイン。完全バックアップは利用者によって。バックアップ媒体の世代管理(5世代)が標準。(実際には、21世代まで実施)	Walrusデータの保存(事業者側の運用担当者) インスタンスのWalrusへの登録(利用者側のシステム管理者)

標準的なバックアップ手順

何を	いつ	どうやって/どこ	パブリッククラウド		プライベートクラウド	Eucalyptus
			FGCP/S5	OVH	NEC社内向けクラウド	
サーバーの構成情報(OSの基本設定など)	サーバーとネットワークの設定/変更時	OSの標準コマンドまたは専用ソフトウェアを用いて、別のディスク又は外部媒体にバックアップを行う	“システムディスクバックアップ・リスト”及び“増設ディスクバックアップ・リスト”を行うことができる(利用者側のシステム管理者が実施)	オプションサービスとして、富士通製品の機能であるOne Point Copy (OPC) を利用しディスクを丸ごとバックアップ実施できる機能を提供している	日時での差分バックアップがメイン。完全バックアップは利用者によって。バックアップ媒体の世代管理(5世代)が標準。(実際には、21世代まで実施)	Walrusデータの保存(事業者側の運用担当者) インスタンスのWalrusへの登録(利用者側のシステム管理者)

活動成果のご紹介

■ モデルの作成（クラウド基盤の階層構造）

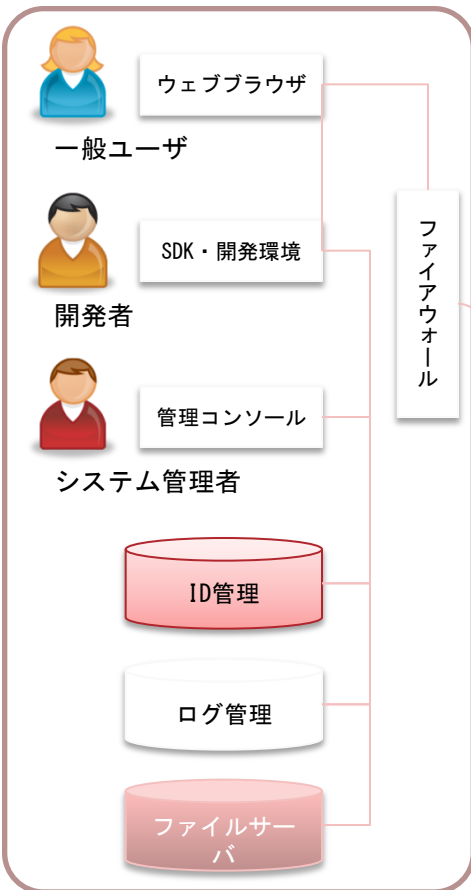
	機能	Eucalyptus	Open Stack	VMware
ノード管理層 ノード(仮想マシン群)を管理する層	稼働中の仮想マシンの管理	Node Controller	Compute Node	調査検討
クラスタ管理層 クラスタ(Availability Zone, アイランド)を管理する層	Networkの管理 仮想マシンIPの払出 どのノードで仮想マシンを立ち上げるかの管理	Cluster Controller	Network Node Scheduler Node	調査検討
クラウド管理層 クラウド全体(リージョン)を管理する層	利用者からの要求を受け付ける 要求を配分する	Cloud Controller	API Node Rabbit MQ	調査検討

上記以外の機能	機能			
データストレージ	仮想マシンにAmazon EBSのようなストレージを提供する	Storage Controller	Volume Node	調査検討
仮想マシンイメージストレージ	仮想マシンのイメージを格納する Amazon S3のようなストレージを提供する	Walrus	Glance	調査検討

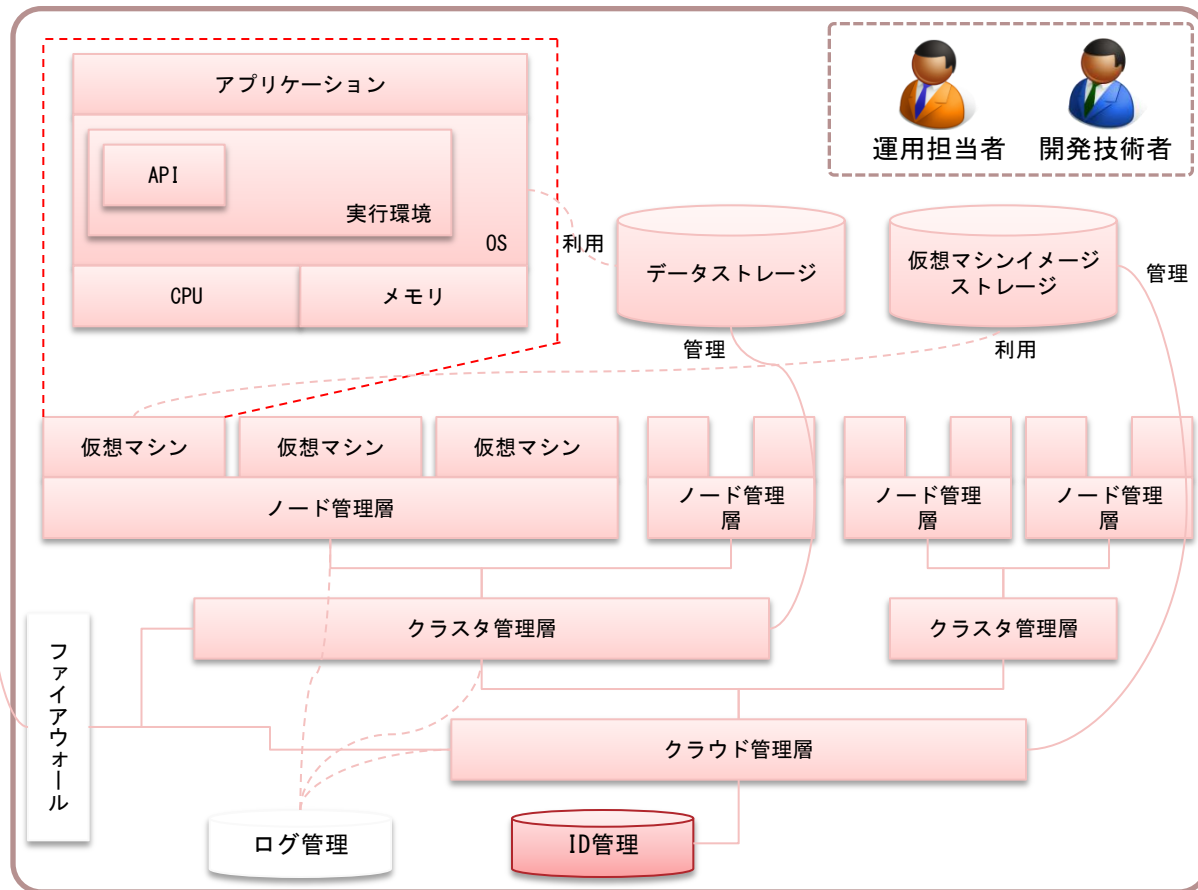
活動成果のご紹介

■ モデルの作成（利用者からみたクラウドシステムの全体構成）

クラウド利用者のIT環境



クラウド事業者（サービス提供者）のシステム環境



■ 登場人物の定義




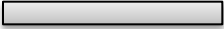

- 一般ユーザ：クラウド利用者のIT環境において、クラウド上で提供される業務アプリケーションやオフィスアプリケーションを利用する。
- 開発者：クラウド利用者のIT環境において、クラウド上の開発環境・実行環境で業務アプリケーションやオフィスアプリケーションを開発・実装する。
- システム管理者：クラウド利用者のIT環境において、クラウド事業者により用意されたポータルサイト等の管理インタフェース等を用いてシステムを管理する。
- 運用担当者：クラウド事業者のシステム環境において、システムの運用管理を行う。
- 開発技術者：クラウド事業者のシステム環境において、システムの機能拡張や新サービスの開発、緊急トラブルへの対応などを行う。

活動スケジュール

■ 今後の予定

第6回会合 2011年11月24日(木), 富士通トラステッドクラウドスクエア(浜松町)

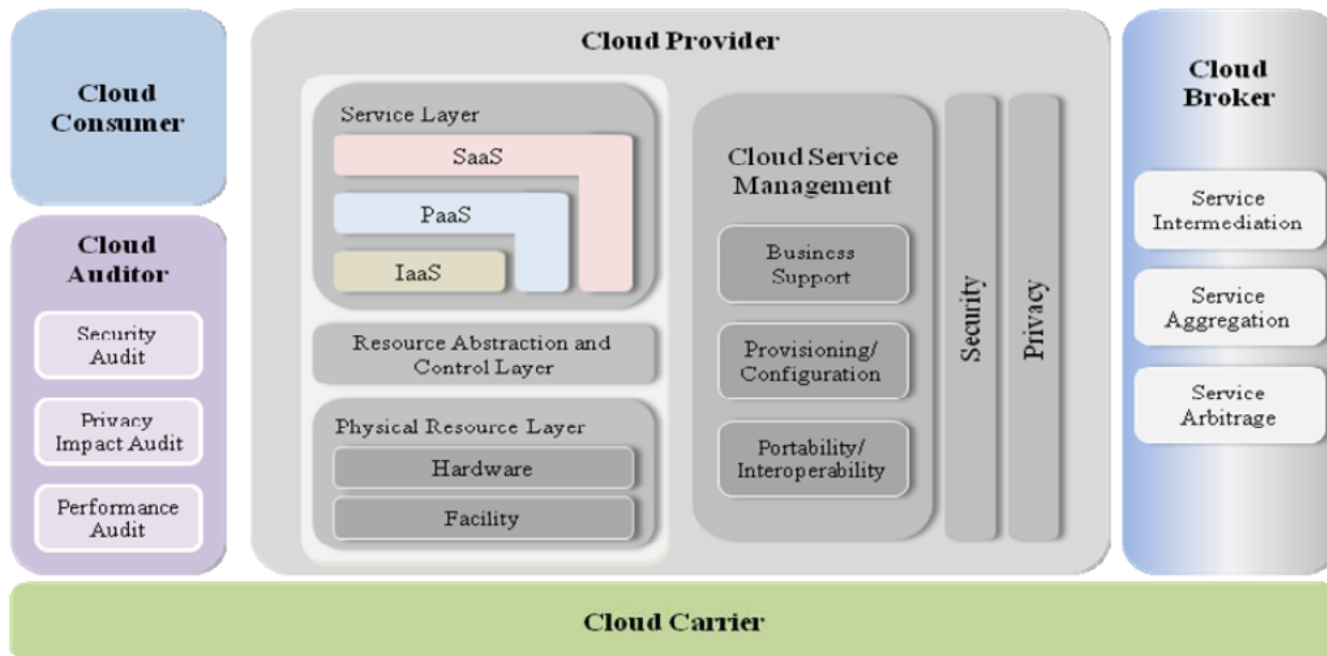
■ 当面のスケジュール

検討項目	2011年度				2012年度	2013年度	
	1Q	2Q	3Q	4Q			
部会 立ち上げ	正式承認 5月▽ メンバー募集 						
テーマ検討 ・調査	活動開始 6月▽ 						
課題抽出・ 技術観点の 検討							
実証検証							
報告書 取りまとめ							

今後の検討テーマと課題

■ 検討テーマ(キーワード)

- 「ソーシャルクラウド基盤技術」におけるセキュリティ
- ハイブリッドクラウド、コミュニティクラウド
- Cloud Broker, Cloud Auditor, Cloud Carrier, ...



出所: NIST <http://www.vsqi.gov.vn/Picture%20Library/NISTCloud%20Computing%20Roadmap.pdf>

■ 課題

- クラウドの運用は、社内機密情報の為、その内容を突っ込んで議論しにくい
- 参加メンバーの偏り...外資系の主なクラウドベンダーの参加も必要と感じる

森 徳行
花館 蔵之
大田原 忠雄
草地 慎太郎
伊藤 求
岩岡 泰夫
小池 晋一
谷川 哲司
川嶋 一宏
望月 貴史
塩崎 哲夫
鈴木 拓也
服部 真
吉田 正敏
宮田 義文
加藤 智之
油井 秀人
小代田 和樹


NECシステムテクノロジー
NTTデータ
トレンドマイクロ
トレンドマイクロ
ニフティ
日本電気
日本電気
日本電気
日立製作所
日立製作所
富士通
富士通
富士通
富士通
富士通
富士通
富士通エフ・アイ・ピー
富士通エフ・アイ・ピー

(オブザーバー)

勝見 勉
河野 省二
永宮 直史

情報処理推進機構
情報処理推進機構
日本セキュリティ監査協会

※敬称略・会社名50音順



FUJITSU

shaping tomorrow with you