

セキュリティ動向2010(2) クラウドセキュリティ管理の現状と動向



2010/11/19
株式会社インターネットイニシアティブ
セキュリティ情報統括室 加藤雅彦

Ongoing Innovation



普及期に入るクラウド

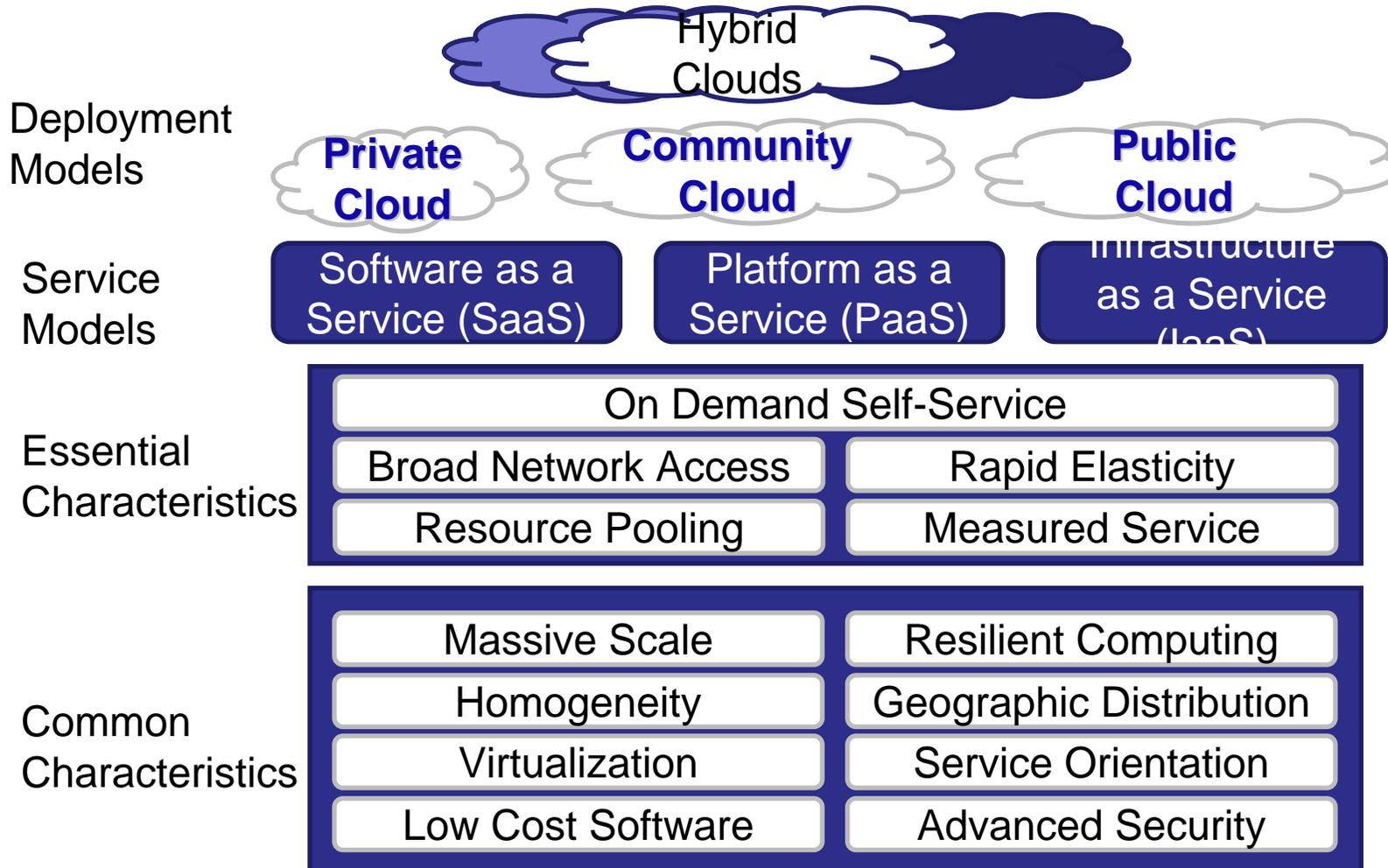
クラウドのイメージ

- クラウドといえば「
」である
 - 「具体的な企業やサービス名」
 - Google / Amazon / Salesforce / Azure …
 - 「サービスモデル」
 - SPIモデル (SaaS, PaaS, IaaS)
 - X as a Service
 - 「何かの性質や特徴」
 - 欲しいときに欲しいだけ使える
 - ネットに繋がればどこからでもアクセスできる
 - 使ったら使っただけ費用を払えばよい

概念としてのクラウド

※NIST: 米国国立標準技術研究所

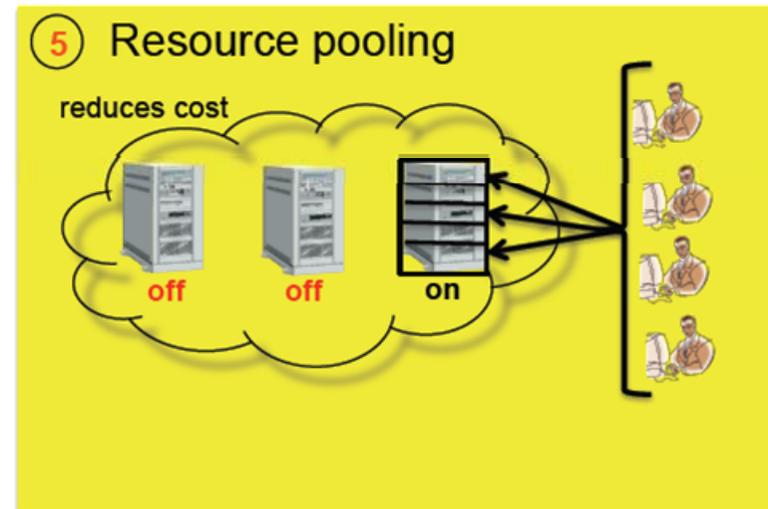
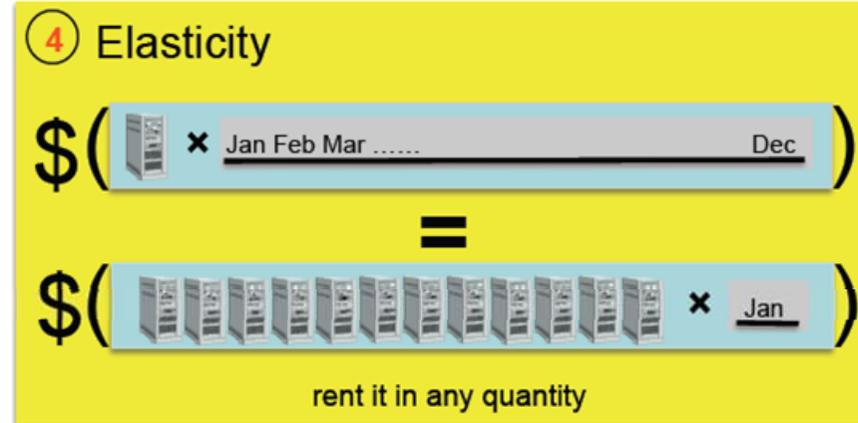
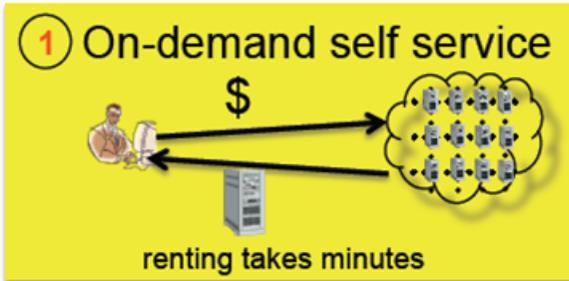
- NISTによるクラウドの定義



NIST "Cybersecurity and Standards Acceleration to Jumpstart Adoption of Cloud Computing" より引用

概念としてのクラウド

- 5つの性質



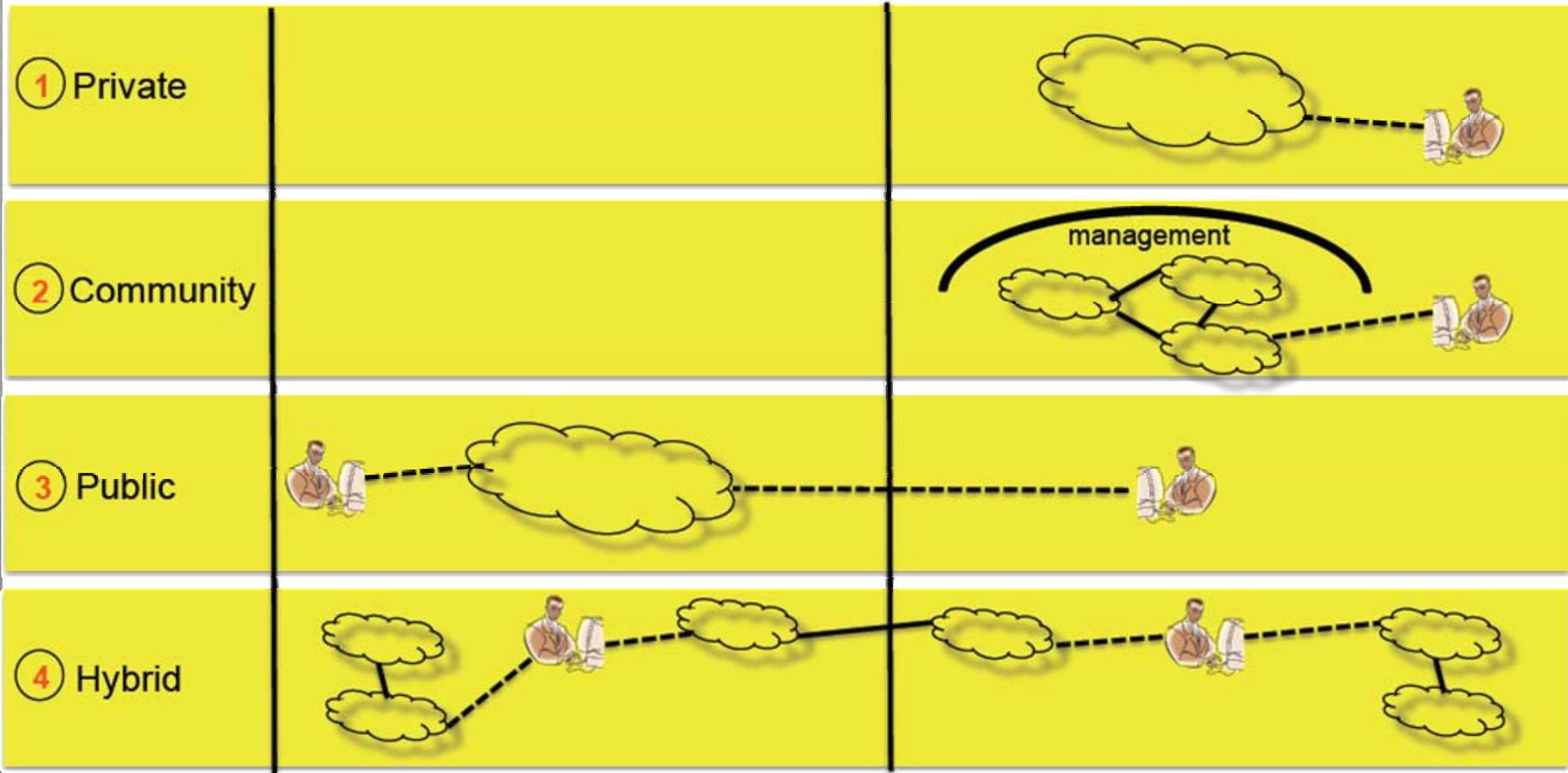
NIST “Cybersecurity and Standards Acceleration to Jumpstart Adoption of Cloud Computing” より引用

概念としてのクラウド

- 4つのデリバリーモデル

Cloud Provider Infrastructure

Cloud Customer Data Center



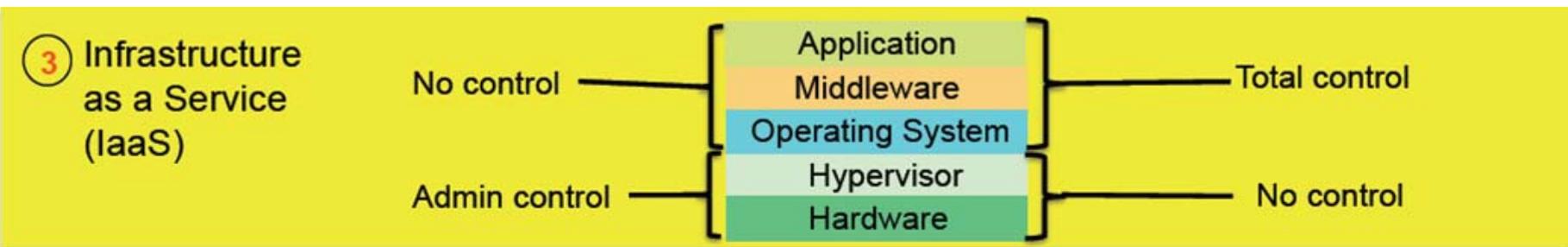
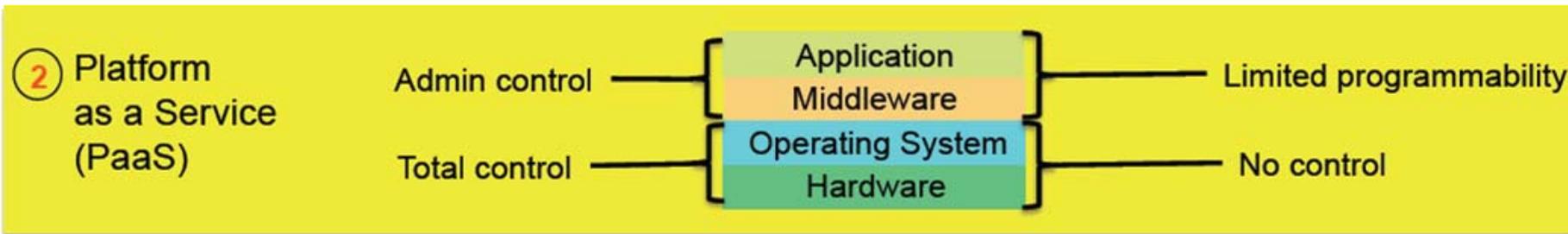
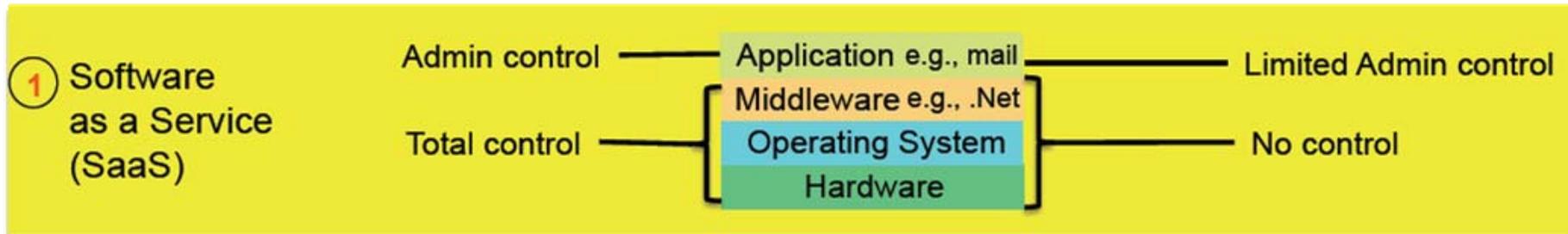
NIST "Cybersecurity and Standards Acceleration to Jumpstart Adoption of Cloud Computing" より引用

概念としてのクラウド

- 3つのデプロイモデル

Cloud Provider

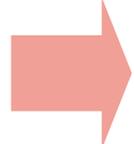
Cloud Customer



NIST “Cybersecurity and Standards Acceleration to Jumpstart Adoption of Cloud Computing” より引用

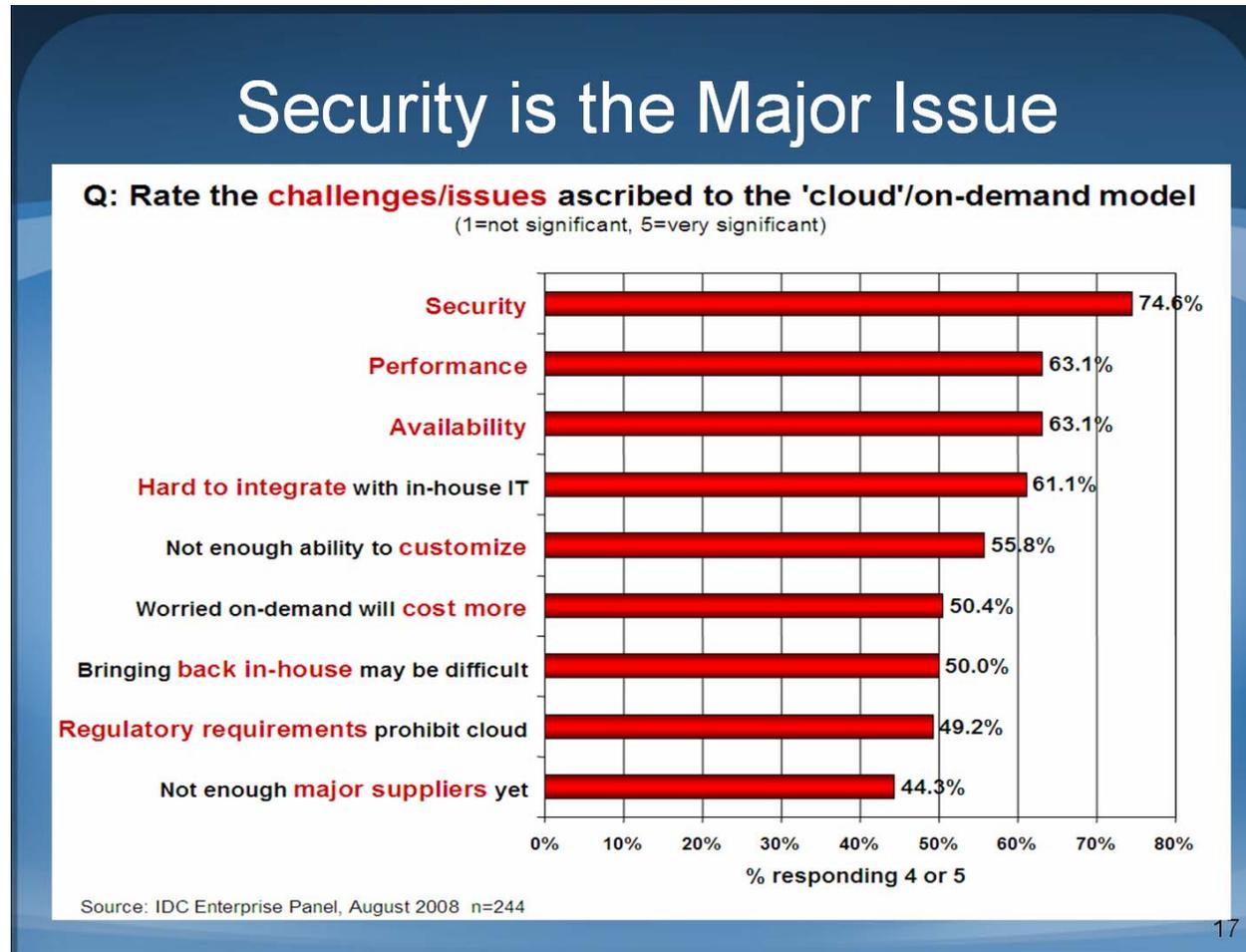
利用が進むにつれ見えてきた現実

- 必ずしも言われているイメージどおりではない
- クラウドのリソースにも限界がある
- クラウドでも(障害により)サービスが止まる
- 従量課金は利用量によってメリットにもデメリットにもなる

 クラウドという
ブラックボックスに対する不安

クラウド利用の課題

- クラウド一番の心配事は「セキュリティ」



NIST “Cybersecurity and Standards Acceleration to Jumpstart Adoption of Cloud Computing” より引用

クラウドインシデント事例

- 様々なインシデントも発生

HOME
ABOUT
CLOUD NEWS
INCIDENTS
INCIDENT TYPES
ORGANIZATIONS
BLOG
SUBMIT INCIDENT
SEARCH
SPONSORS
MAILING LISTS
RESOURCES
LOGIN



Cloutage.org
an open security foundation project

"occasional minor outages are just part of the reality of cloud computing today"
- Steve Jones, CEO of Explore Consulting

About Cloutage

Cloutage exists to empower organizations by providing cloud security knowledge and resources so that they may properly assess information security risks. The project aims to document known and reported incidents with cloud services while also providing a one-stop shop for cloud security news and resources. For any questions about this site or the data contained within the site, please contact .

Cloutage Blog

Open Security Foundation Announces New Advisory Board
by Jake Kouns, 2010-09-08

As security vulnerabilities and data loss incidents become a regular occurrence, the Open Security Foundation has grown from supporting a single project in 2004 to a leading provider of filtering through security information and providing notifications and aggregation for data for data loss and cloud security incidents.

The Open Security Foundation has evolved into one of the most utilized resources in providing security information, and as a 501c3 non-profit organization relies heavily on public contributions, volunteer effort and corporate sponsorships.

The growing demand for information to provide proper risk management has led to additional projects and now the introduction of an advisory board consisting of industry professionals to lend their expertise in areas to keep OSF moving in a positive direction and to be the first line of access to all that require their service.

Open Security Foundation CEO and founder Jake Kouns stated, "This is a very important step in shaping the future of the Open Security Foundation." OSF has reached a point in growth that requires a strategic move to provide longevity and sustainability. It has always been a goal of this organization to provide our work to the broadest audience, and the introduction of the advisory board will

Latest Cloud Incidents

Type	Date	Organization	What Happened?
 outage	2010-09-02	Microsoft Corporation	Technical problem kept an undetermined number of Windows Live Hotmail email accounts
 outage	2010-08-30	Rackspace, Inc.	Rackspace Moment
 outage	2010-08-29	DtDNS	DtDNS e service a services
 vuln	2010-08-29	Orange Spain	Orange in HTTP
 outage	2010-08-28	Bank of America	Bank of Multi-Ho
 hack	2010-08-28	HostV	HostV V of Hack
 outage	2010-08-25	Linode	DDOS A Daterc
 outage	2010-08-25	VPS.NET, Hosting Services Inc.	VPS.Net Outage



AutoFail

This category tracks quality control failures that are delivered to a user's computer via automatic update mechanisms. This includes virus signature updates that identify competing products as a trojan or application/operating system updates that break core functionality. Problematic updates can cause widespread impact as they may be delivered to millions of computers quietly and efficiently, typically without user interaction.



DataLoss

This category refers to the unforeseen loss of data or information and can be the result of several issues including poor backup and recovery processes. Data Loss is used to highlight a more serious and typically permanent impact as customer data is lost and not recoverable. In most cases a Data Loss event is also part of a service Outage as well.



Hack

When cloud service providers or online services experience a breach they are categorized as a hack. There is no intention to be a comprehensive web defacement mirror; the intent is to document high profile incidents. Events that also lead to a breach of integrity or confidentiality of customer data are also typically included within this category.



Outage

Includes any unplanned availability or impact to cloud providers such as when services are down or specific features are unavailable. We add each new downtime as an incident and when possible capture the outage duration for the service that was unavailable. In addition, we include (when known) the impacted customer base in terms of specific number of users or percentage of the overall customer base.



Vulnerability

This category is used to track site specific vulnerabilities in cloud service providers as well as online services/websites that are not considered software products available for download. It is important to note that these vulnerabilities are typically not recorded in the Open Source Vulnerability Database (OSVDB). Most of the incidents included in this category affect custom software or services.

Cloutage.org <http://cloutage.org/> より引用

© 2010 Internet Initiative Japan Inc.

10

クラウドになると管理はどう変わるのか

従来型の資産管理領域 (ISO27000等)

「所有」が前提

ユーザ


情報
(契約書、議事録、日報、名簿、顧客データ、生産データ、等)

開発


ソフトウェア
(顧客情報システム、生産管理システム等の
業務用ソフトウェア、

情シス


オペレーティングシステム、データベース管理ソフト、
ネットワークOS等の
システムソフトウェア)

情シス


ハードウェア
(サーバ、クライアント、プリンタ、周辺機器等)

情シス


ネットワーク
(LAN、ルータ、ハブ、その他通信機器等)

人員

(SE、
プログラマ、
オペレータ、
管理者、
研究員、
利用者
等)

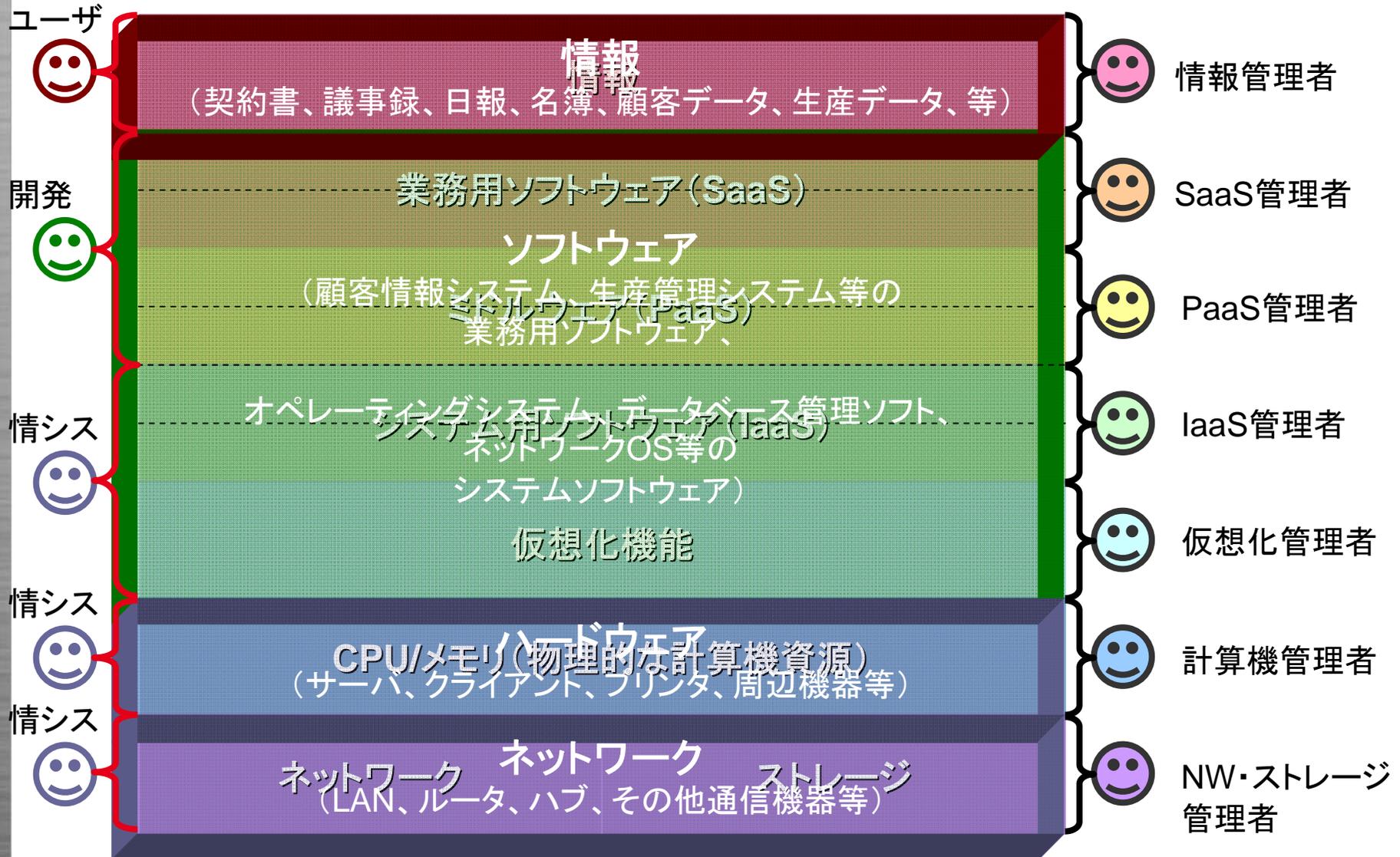
※その他知的財産等も資産に含まれる

クラウドの管理構造

利用が前提



重なると・・・？



従来との管理領域の違い

利用者管理

利用者管理

フルアウトソース

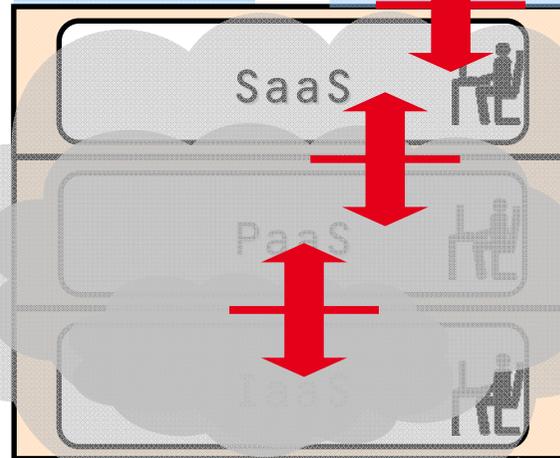
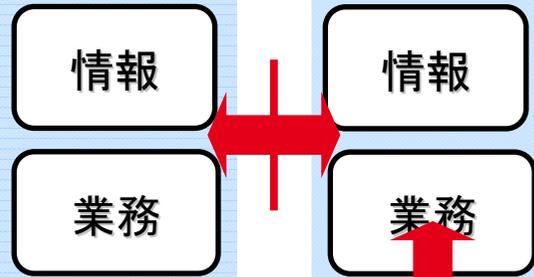
情報
従来

アプリケーション

ソフトウェアインフラ

ハードウェアインフラ

の
管理
方法



事業者管理

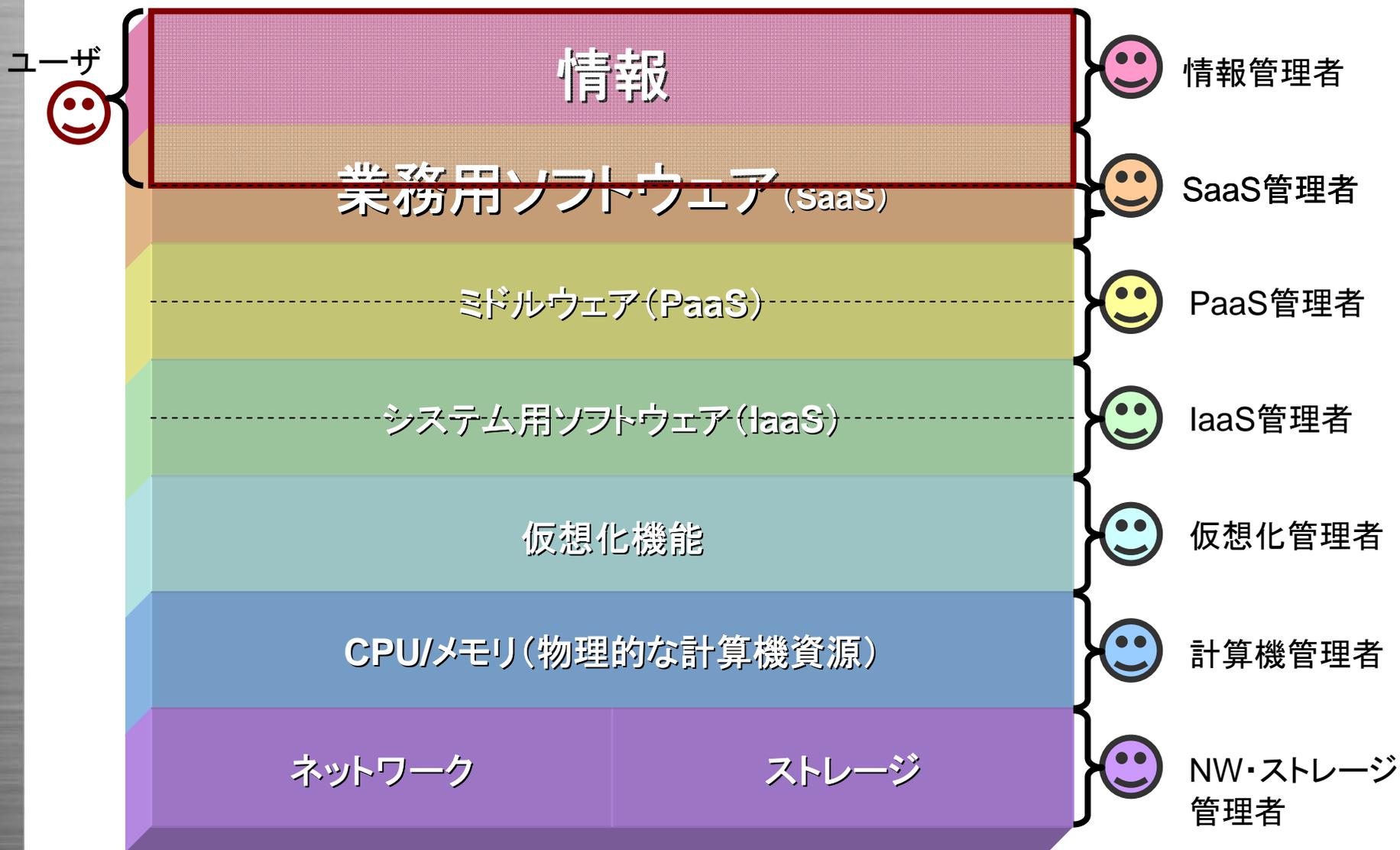
事業者管理



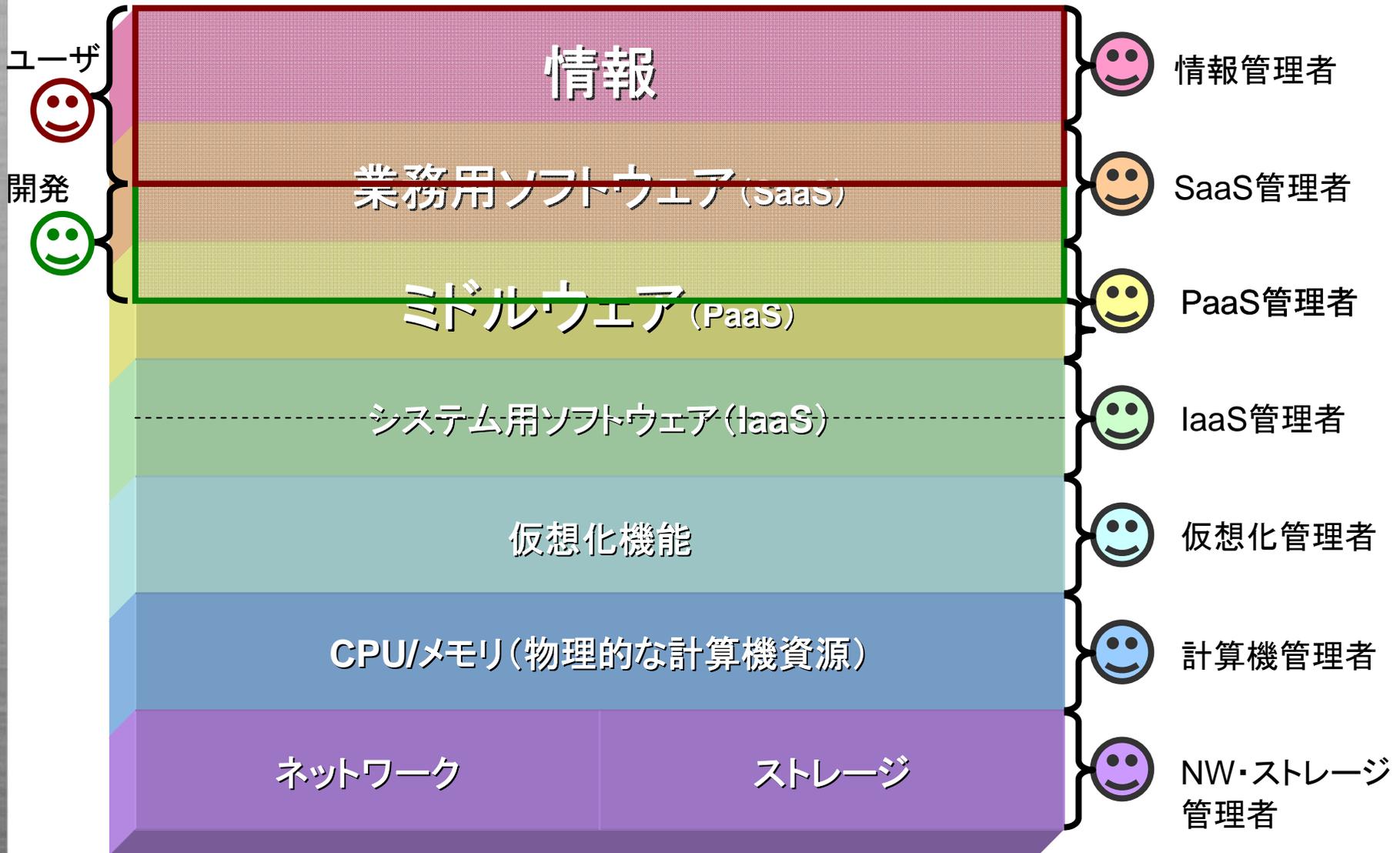
自社によるコントロール

アウトソース先によるコントロール

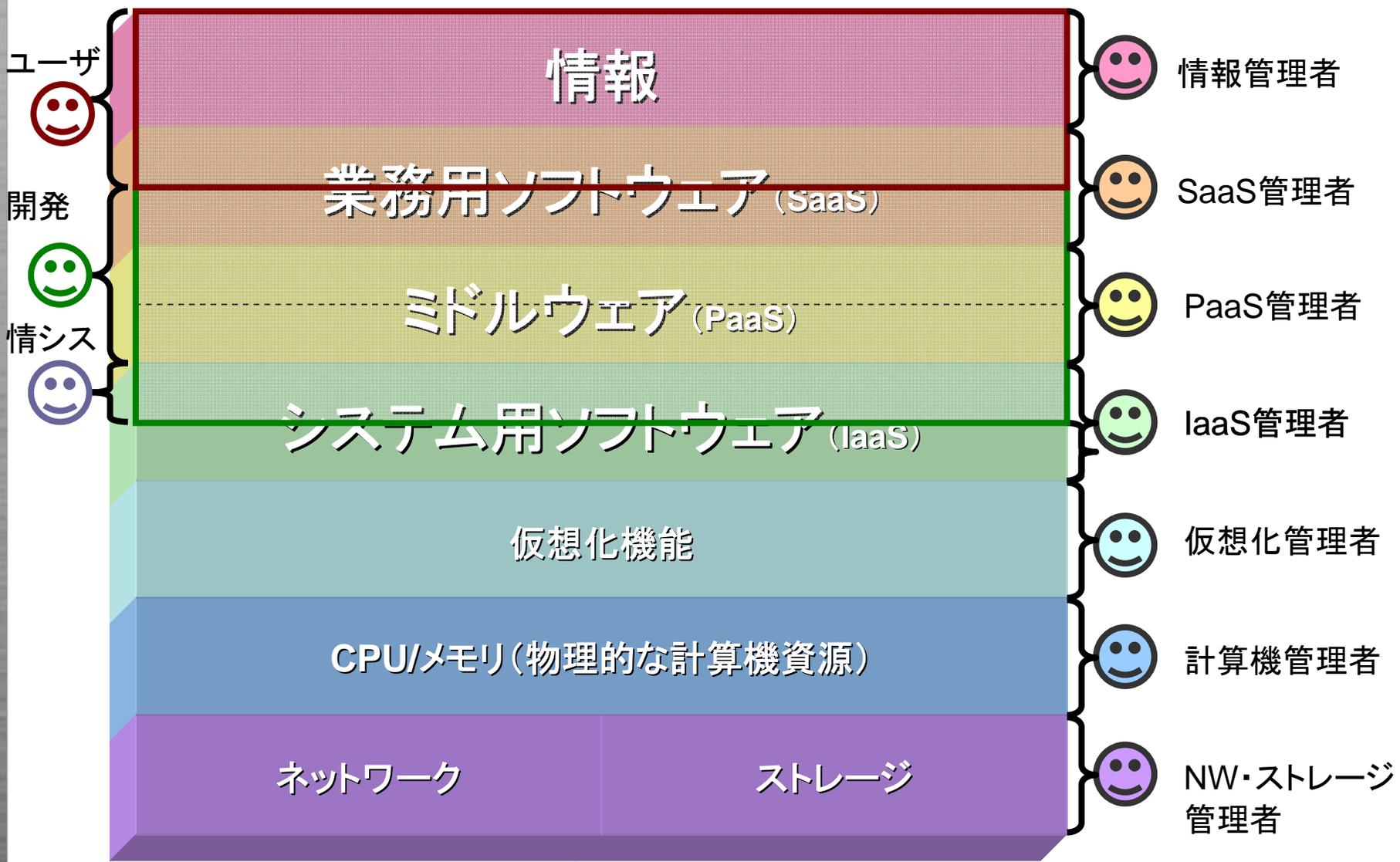
SaaSの管理責任分界点



PaaSの管理責任分界点



IaaSの管理責任分界点



概念的には

- 事業者と利用者で管理領域を分担している
- 利用/提供するサービスによって管理領域が異なる
- セキュリティ対策に関しても、事業者が対応すべき領域と利用者が対応すべき領域がある

 双方合意が取れる基準の必要性

クラウドセキュリティにおける基準策定の国内動向

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(案)
 - 1章 適用範囲
 - 2章 引用規格
 - 3章 用語及び定義
 - 4章 概要
 - 5章～15章 JIS Q27002の管理策
 - 16章 附属書 A クラウドサービス固有のリスク
 - 17章 附属書 B クラウド利用におけるリスクアセスメントの考え方
 - 18章 付録クラウド利用における実施の手引の一覧

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 (案)
Information security management for the use of cloud computing services based on ISO/IEC 27002

1 適用範囲	8
2 引用規格	8
3 用語及び定義	8
4 概要	12
4.1 クラウドサービスの有効利用に向けて	12
4.2 本ガイドラインについて	12
4.2.1 本ガイドラインにおけるクラウドコンピューティングとは	12
4.2.2 本ガイドラインの構成要素	13
4.2.3 本ガイドラインの使い方	15
4.3 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	17
4.3.1 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の必要性	17
4.3.2 方向づけ (Direct)	18
4.3.3 モニタリング (Monitor)	18
4.3.4 評価 (Evaluate)	19
4.3.5 報告 (Report)	19
4.3.6 監査 (Assure)	19
4.4 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	20
4.4.1 クラウドサービス利用における情報セキュリティの PDCA サイクル	20
4.4.2 クラウドサービス利用におけるリスクアセスメント	20
4.4.3 クラウドコンピューティング環境とセキュリティリスク	21
4.4.4 クラウドサービス利用における情報セキュリティ監査の活用	26
5 セキュリティ基本方針	28
5.1 情報セキュリティ基本方針	28
5.1.1 情報セキュリティ基本方針文書	28
5.1.2 情報セキュリティ基本方針のレビュー	28
6 情報セキュリティのための組織	29
6.1 内部組織	29
6.1.1 情報セキュリティに対する経営陣の責任	29
6.1.2 情報セキュリティの調整	29
6.1.3 情報セキュリティ責任の割当て	30
6.1.4 情報処理設備の認可プロセス	31
6.1.5 秘密保持契約	31
6.1.6 関係当局との連絡	32
6.1.7 専門組織との連絡	33
6.1.8 情報セキュリティの独立したレビュー	33
6.2 外部組織	34

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(案)
 - ISO27002をベースとして、クラウド管理に特有な事項を盛り込んだガイドライン
 - 利用者でも事業者でも利用可能なガイドラインとなっている
 - 各管理策に、「クラウド利用者のための実施の手引き」「クラウド事業者のための実施の手引き」「クラウドサービスの関連情報」が記載されている
 - 関連資料として出ている概要を一番最初に、それから4章を次に読むことをお勧めします
 - 5章～をいきなり斜め読みするのはお勧めしません
 - 11/17～12/16 パブリックコメント受付中！
 - ぜひ積極的にご意見ください

情報処理推進機構

● ENISA (European Network and Information Security Agency) による、クラウドのセキュリティに関するガイドラインの翻訳

- 1. 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
- 2. 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
- 3. 項目2の文書に記載のある、35のリスク項目の対訳、53の脆弱性項目の対訳、23の資産項目の対訳



日本クラウドセキュリティアライアンス

- Security Guidance for Critical Areas of Focus in Cloud Computing v2.1 日本語版作業開始

CSAガイドンス ver2.1の翻訳について | LinkedIn - Mozilla Firefox

ファイル(E) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルプ(H)

http://www.linkedin.com/groupItem?view=&gid=2920100&type=member&item=32490006&qid

Google linkedin

NETCRAFT Services Risk Rating Since: Jan 2003 Rank: 39 Site Report [US] LinkedIn Corporation

LinkedIn Account type: Basic Masahiko Katoh Add Connections

Home Profile Contacts Groups Jobs Inbox 2 More Groups

CSAJC cloud security alliance Japan Chapter Cloud Security Alliance, Japan Chapter a subgroup of Cloud Security Alliance

Discussions Members Search More... Start a discussion

CSAガイドンス ver2.1の翻訳について
ガイドンス Ver2.1の翻訳について、JCとして、企画をおこしたいと思います。

Ikuo
Stop Following
できれば、スポンサーのご支援をいただきたいうえで、最終的に合宿(といっても2日間くらいでしょうか)で、きちんとつめられるといいなあ、とおもっているのですが、どんなものでしょう。

それぞれ、すでに翻訳している企画が複数あると聞いておりますが、このスレッドのもとで、この企画への参加希望を募るといのはいかがでしょうか。
29 days ago

Like Comment Follow Flag More

8 comments

Ikuo Takahashi • ボードでは、私は、監訳者付けようといっていたのですが、この方向でいくのであれば、ひとつのアイデアですが

People I'm Following

Ikuo Takahashi commented on: Cloud Security Alliance Congress
9 hours ago • Like • 3 comments

Ikuo Takahashi posted: Cloud Security Alliance Congress
18 hours ago • Like • 3 Comments

See all updates >

Manager's Choice

Group 3: Legal and eDiscovery(法務と電子証拠開示)
Eiji Sasahara, Ph.D., MBA See all >

完了

まとめ

- クラウドの利用が進み、様々な問題点も明らかに
- オンプレミスやフルアウトソースとは異なり、事業者と利用者が管理領域を分担しあう構造
- ベストプラクティスとして国内でもガイドラインが整い始めている状況



ご清聴ありがとうございました

Ongoing Innovation

本書には、株式会社インターネットイニシアティブに権利の帰属する秘密情報が含まれています。本書の著作権は、当社に帰属し、日本の著作権法及び国際条約により保護されており、著作権者の事前の書面による許諾がなければ、複製・翻案・公衆送信等できません。IIJ, Internet Initiative Japan は、株式会社インターネットイニシアティブの商標または登録商標です。その他、本書に掲載されている商品名、会社名等は各会社の商号、商標または登録商標です。本文中では™、®マークは表示しておりません。©2010 Internet Initiative Japan Inc. All rights reserved. 本サービスの仕様、及び本書に記載されている事例は、将来予告なしに変更することがあります。