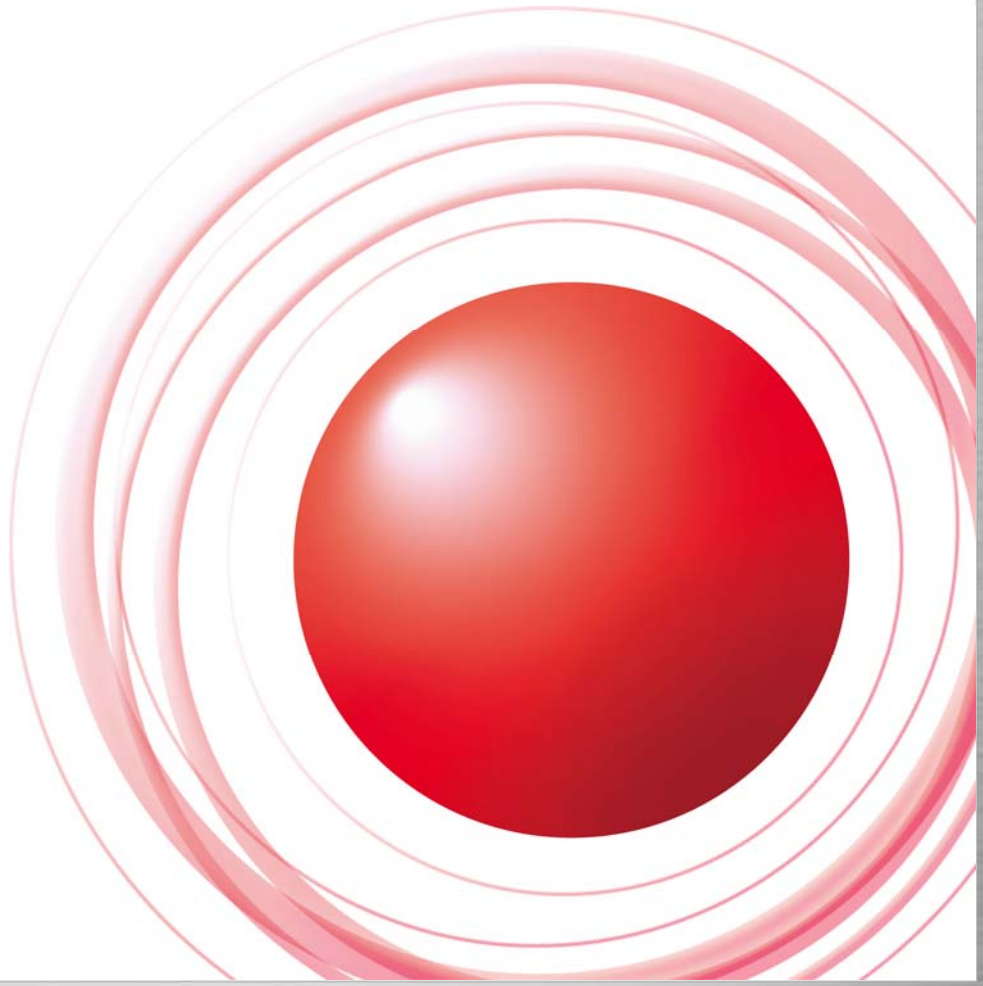
セキュリティ動向2010（2）
クラウドセキュリティ管理の現状と動向

IIJ Internet Initiative Japan



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

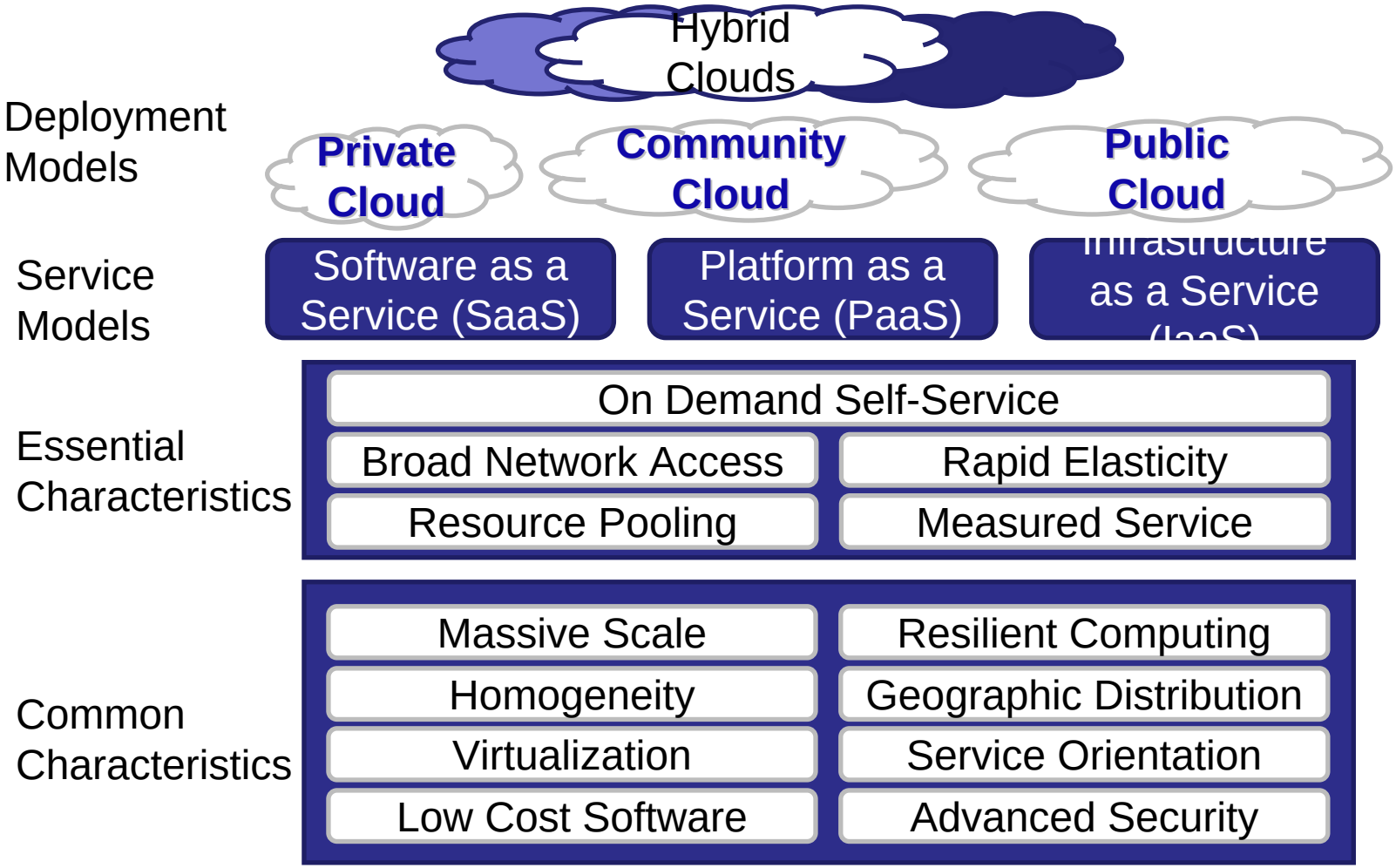
クラウドのイメージ

- 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

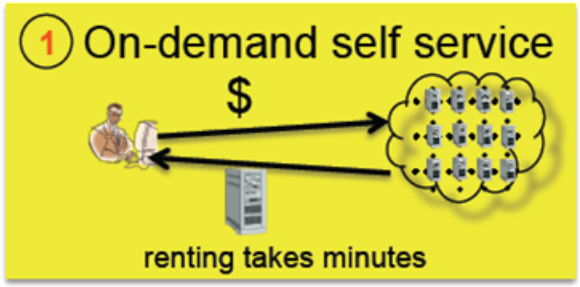
- NISTによるクラウドの定義

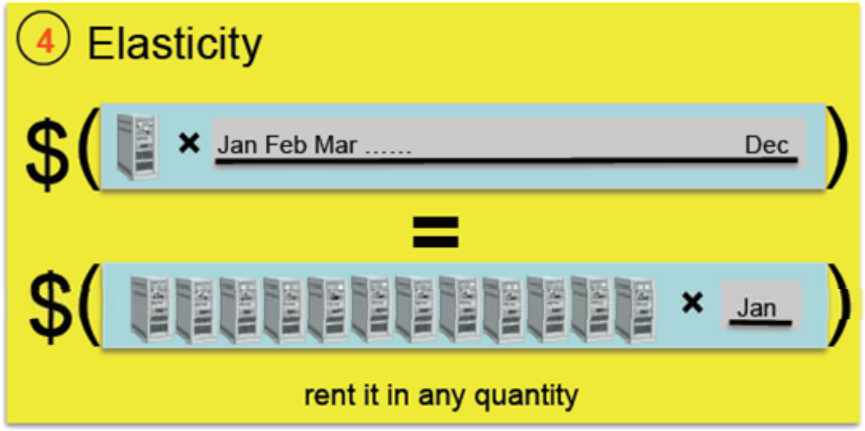


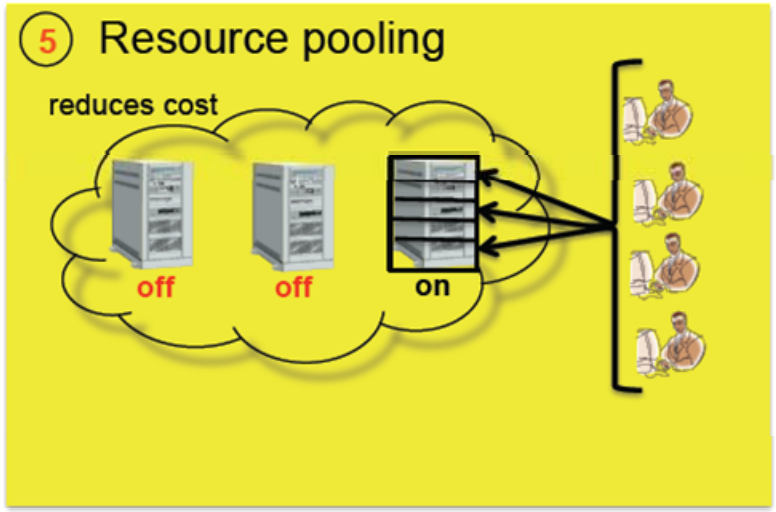
NIST “Cybersecurity and Standards Acceleration to Jumpstart Adoption of Cloud Computing” より引用

概念としてのクラウド

- 5つの性質



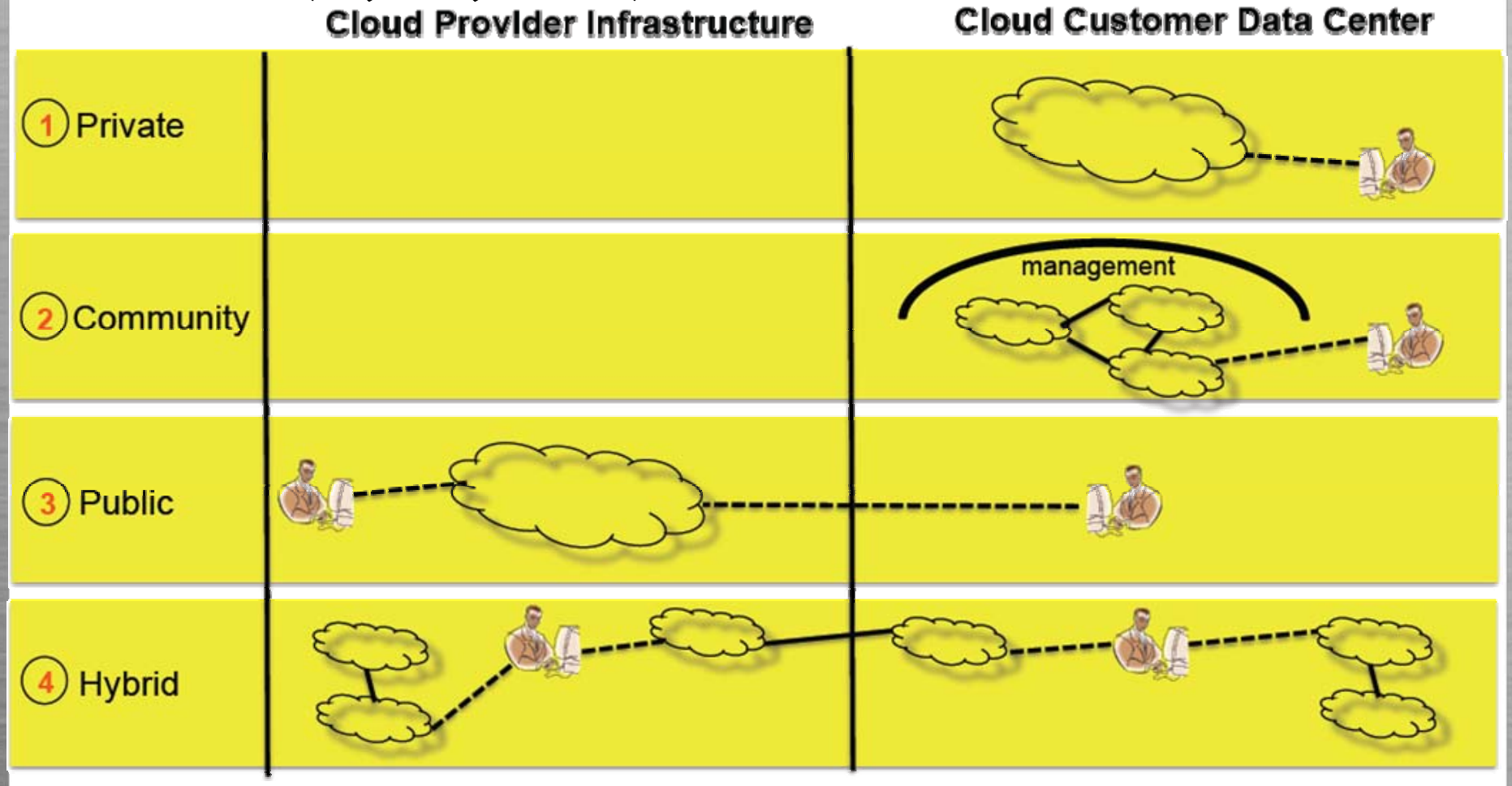




NIST “Cybersecurity and Standards Acceleration to Jumpstart Adoption of Cloud Computing” より引用

概念としてのクラウド

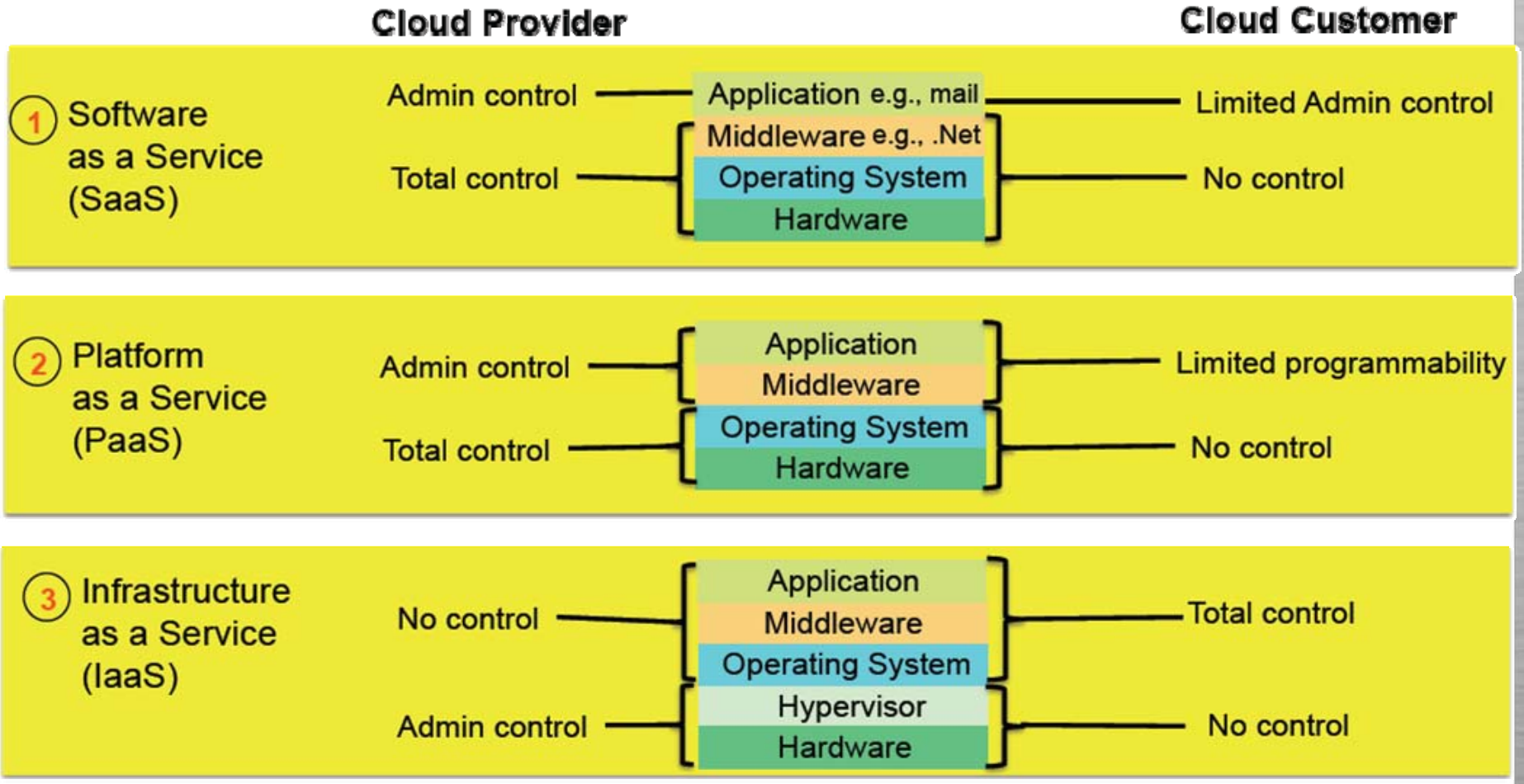
- ４つのデリバリーモデル



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



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

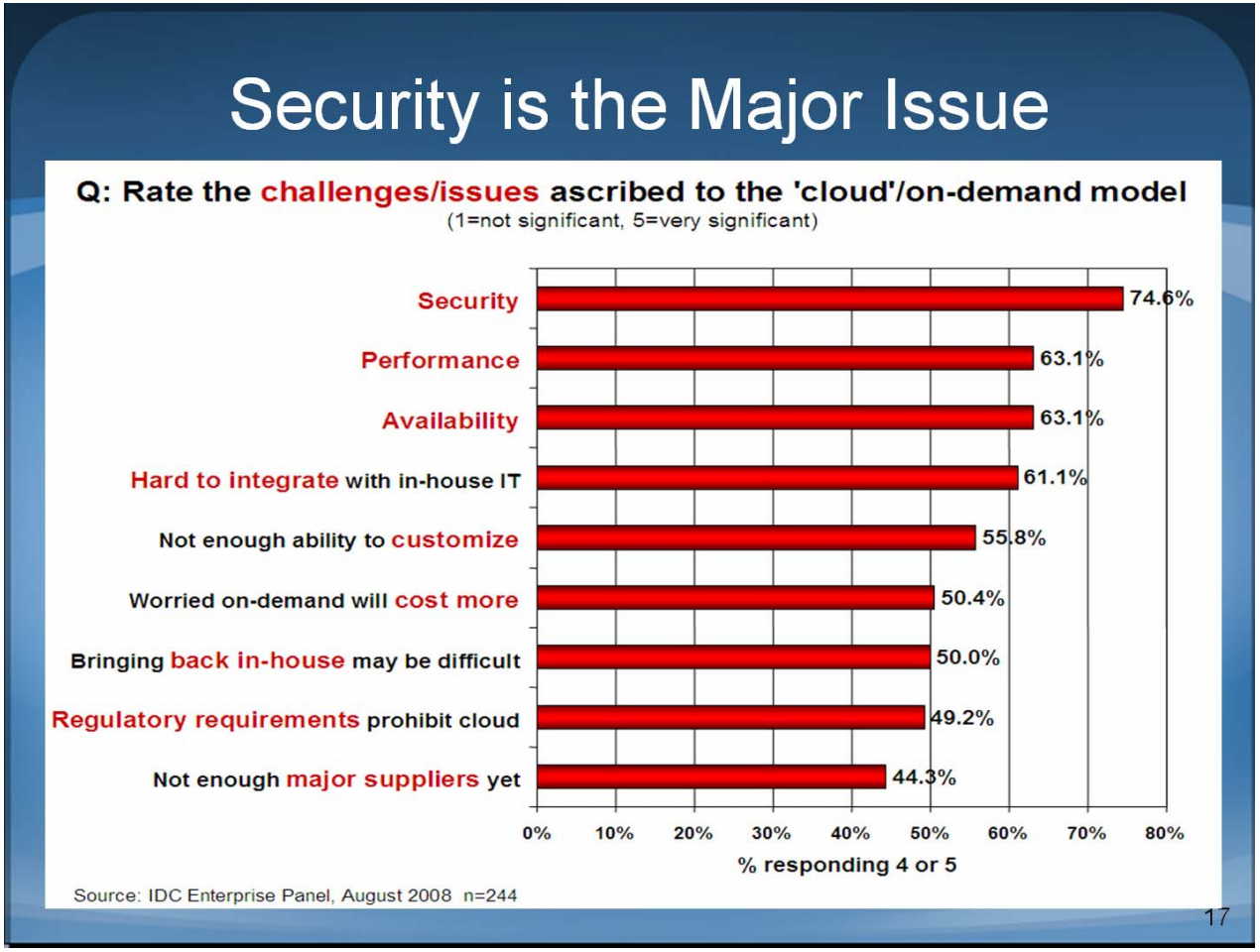
利用が進むにつれ見えてきた現実

- 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

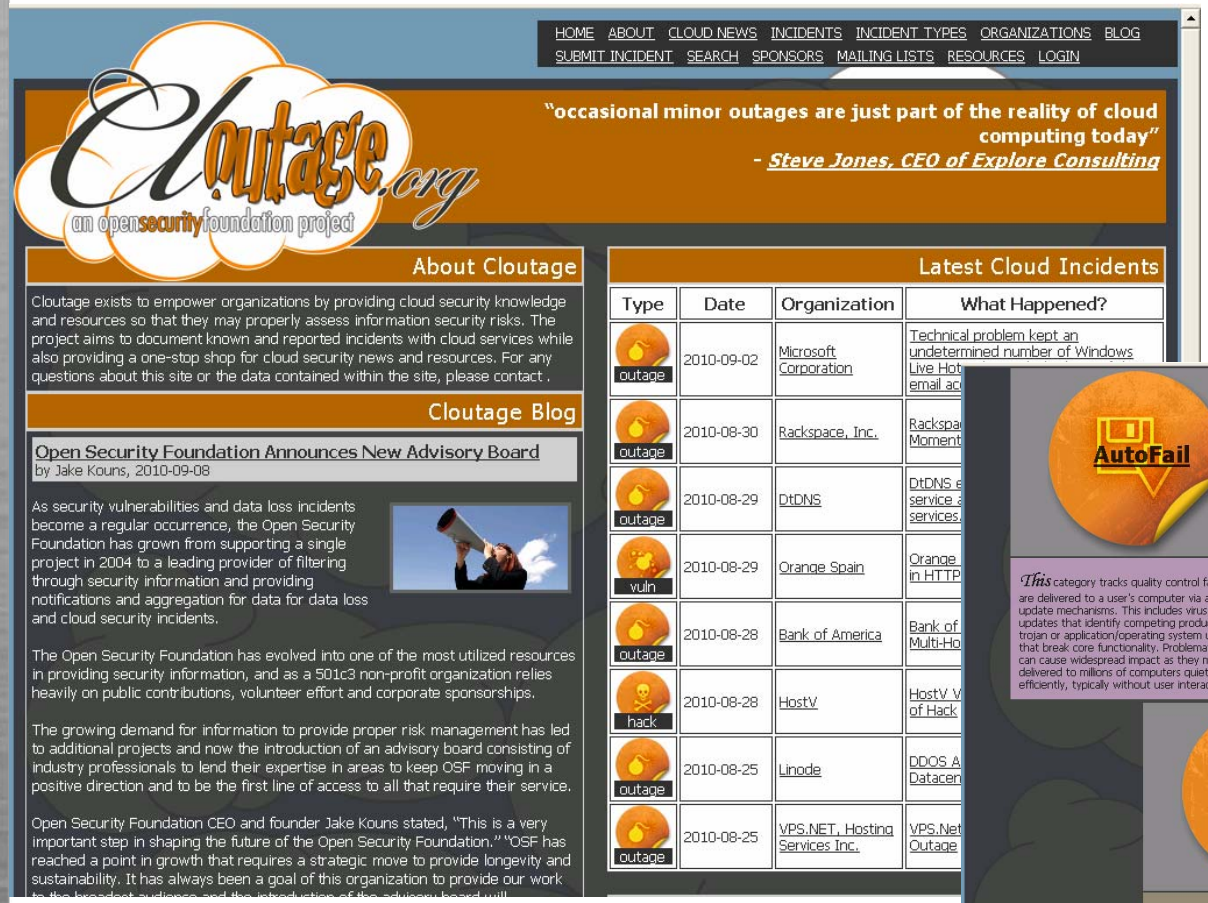
- クラウドー番の心配事は「セキュリティ」

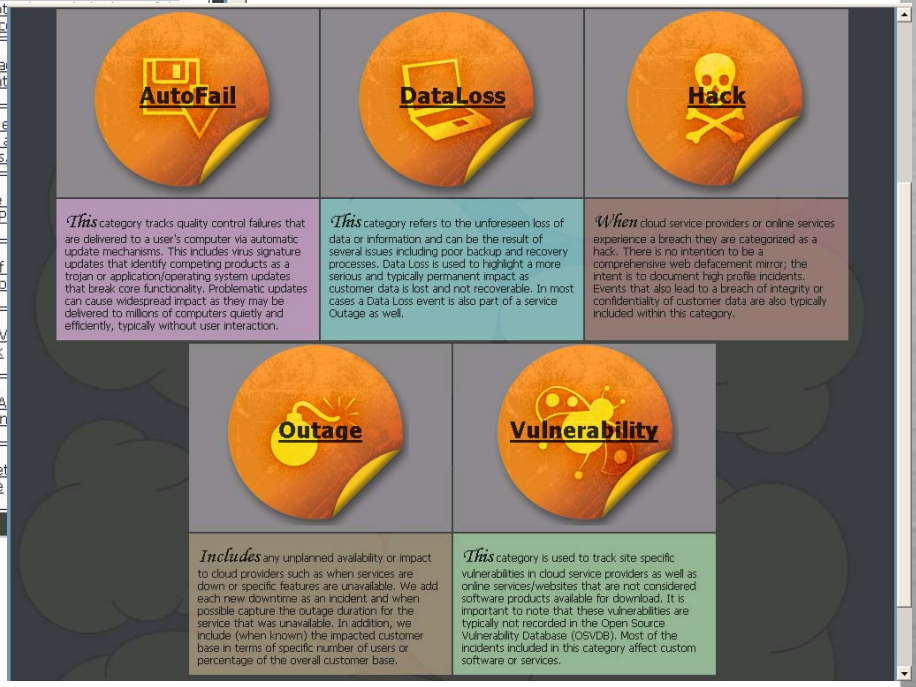


NIST “Cybersecurity and Standards Acceleration to Jumpstart Adoption of Cloud Computing” より引用

クラウドインシデント事例

- 様々なインシデントも発生

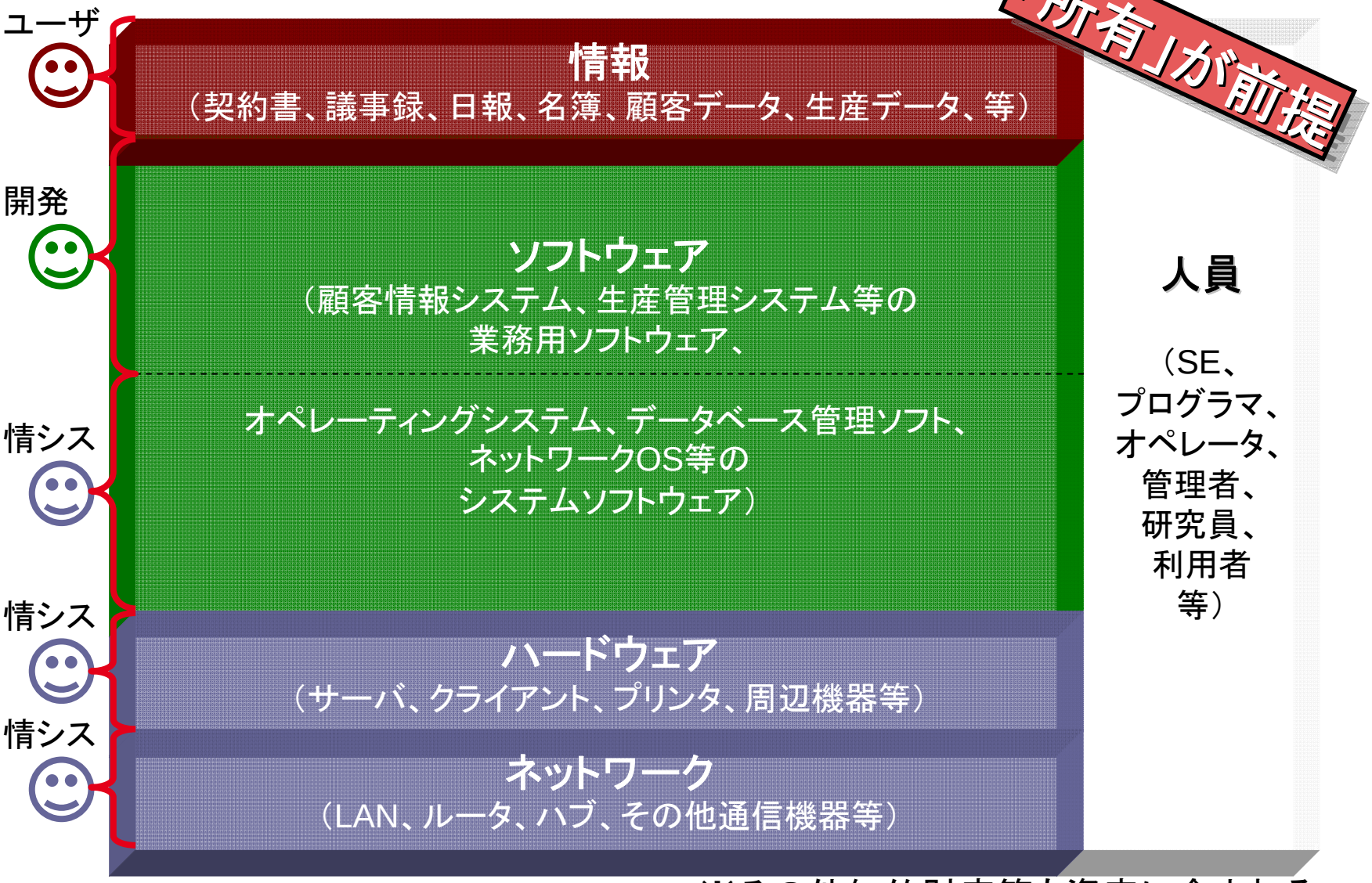




Cloutage.org http://cloutage.org/ より引用

クラウドになると管理はどう変わるのか

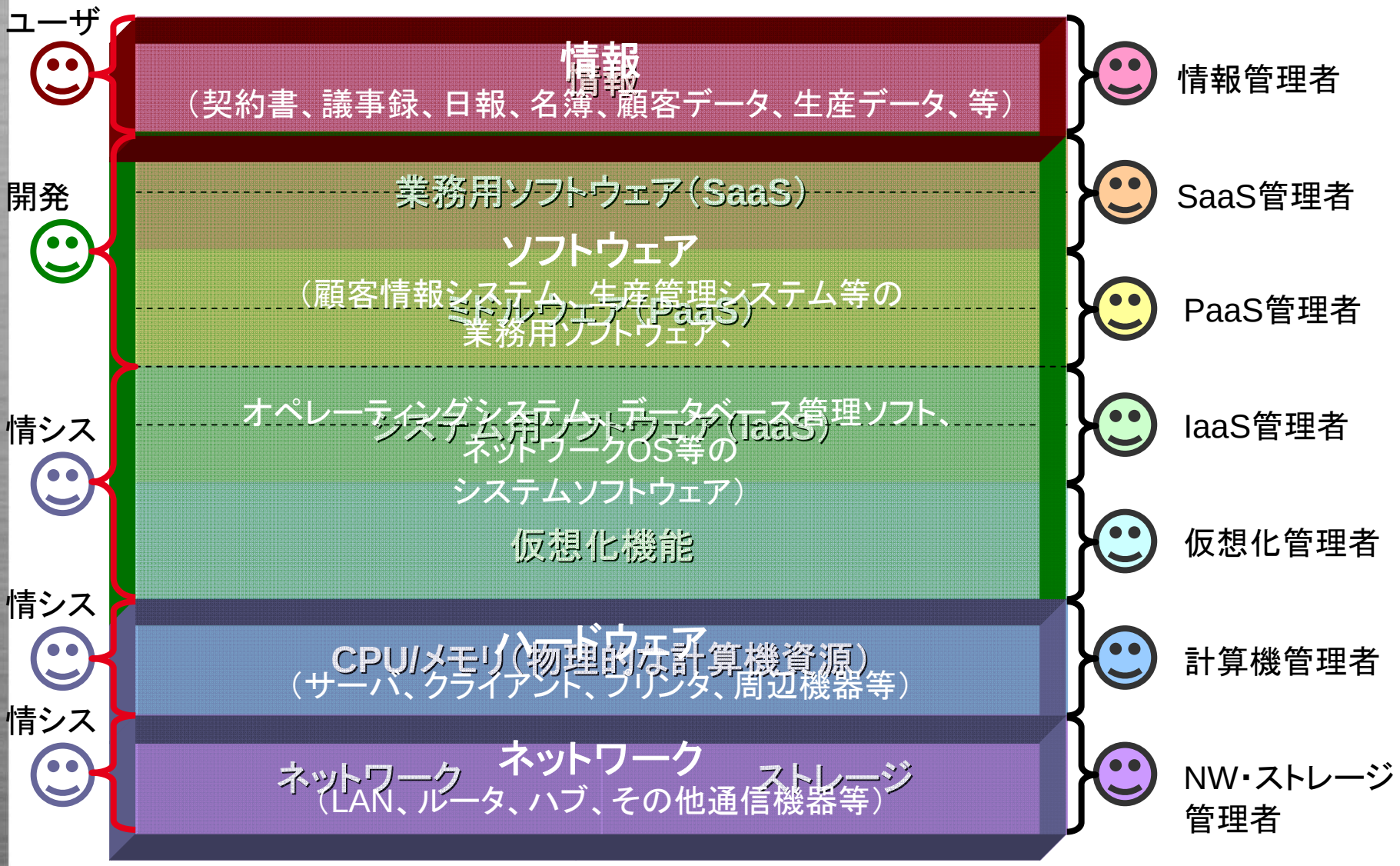
従来型の資産管理領域（ISO27000等）



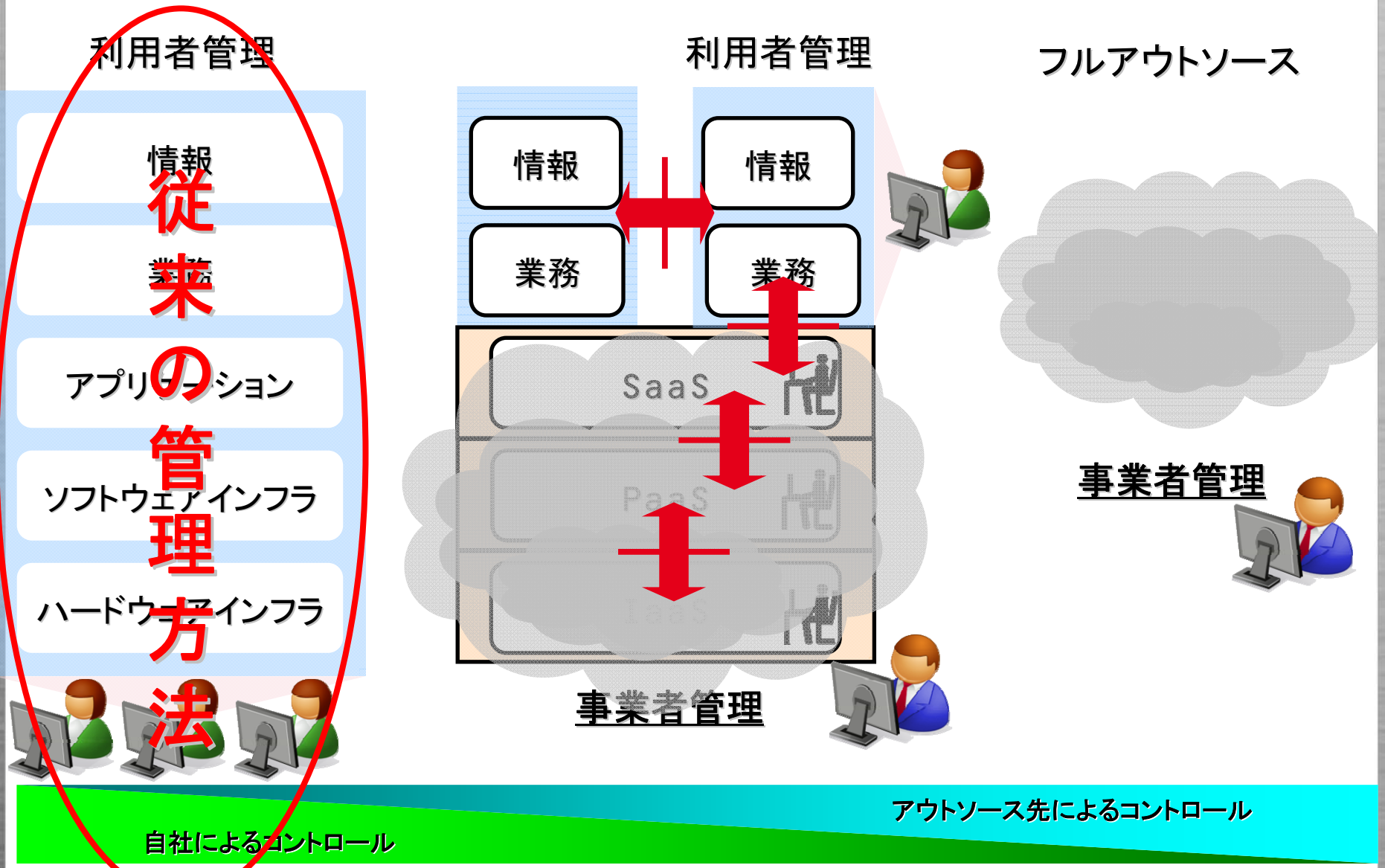
※その他知的財産等も資産に含まれる

クラウドの管理構造

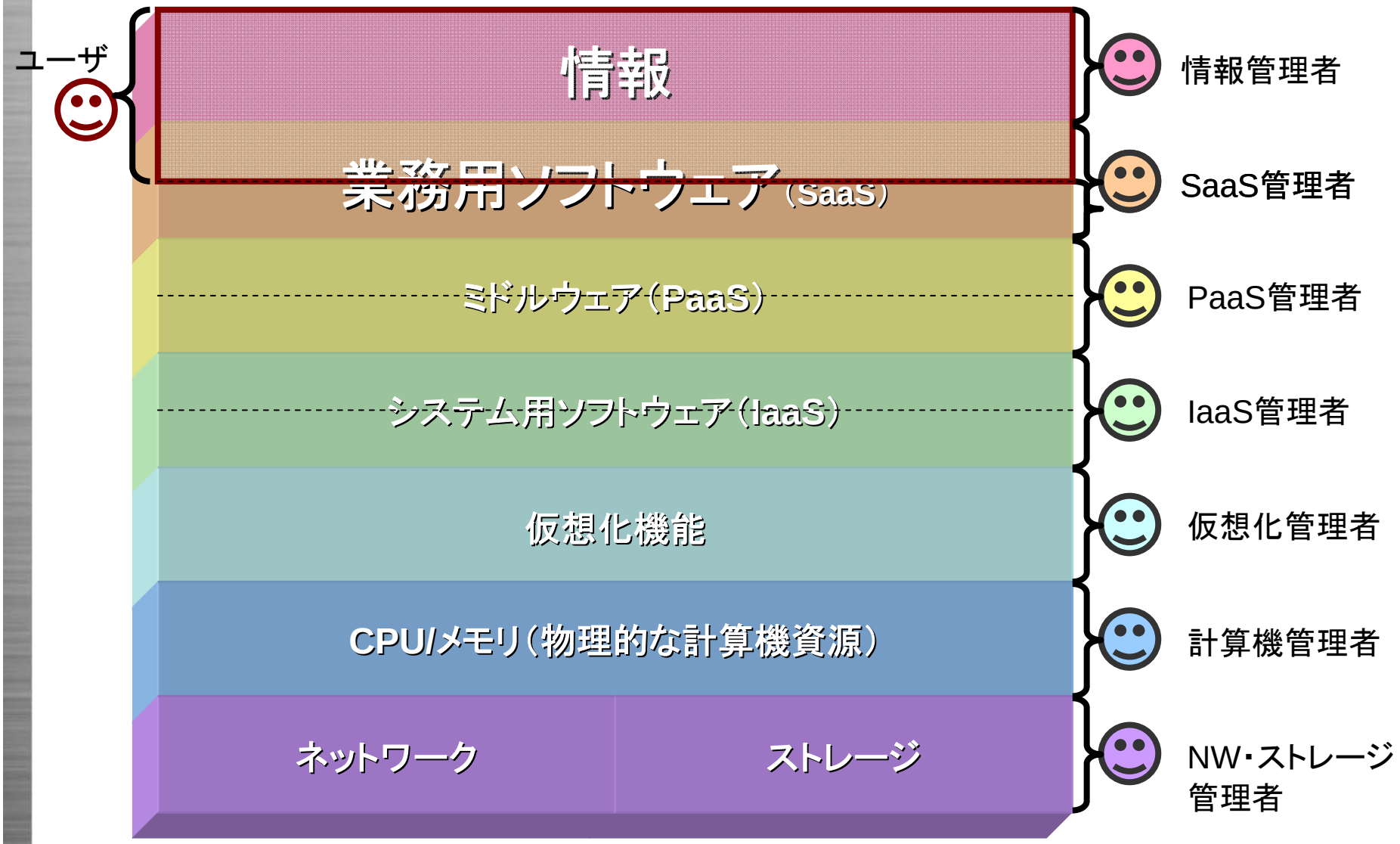
重なると・・・？



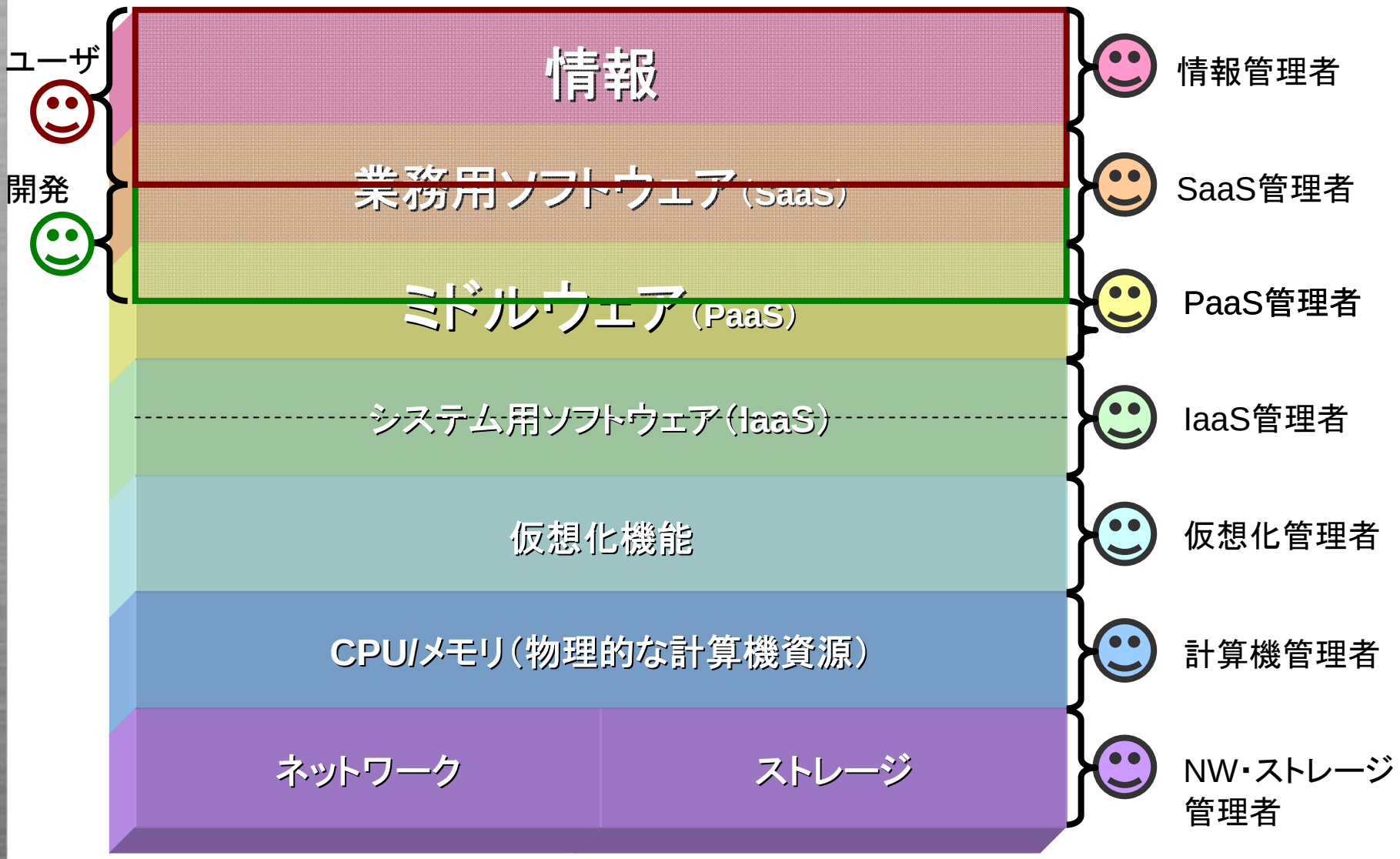
従来との管理領域の違い



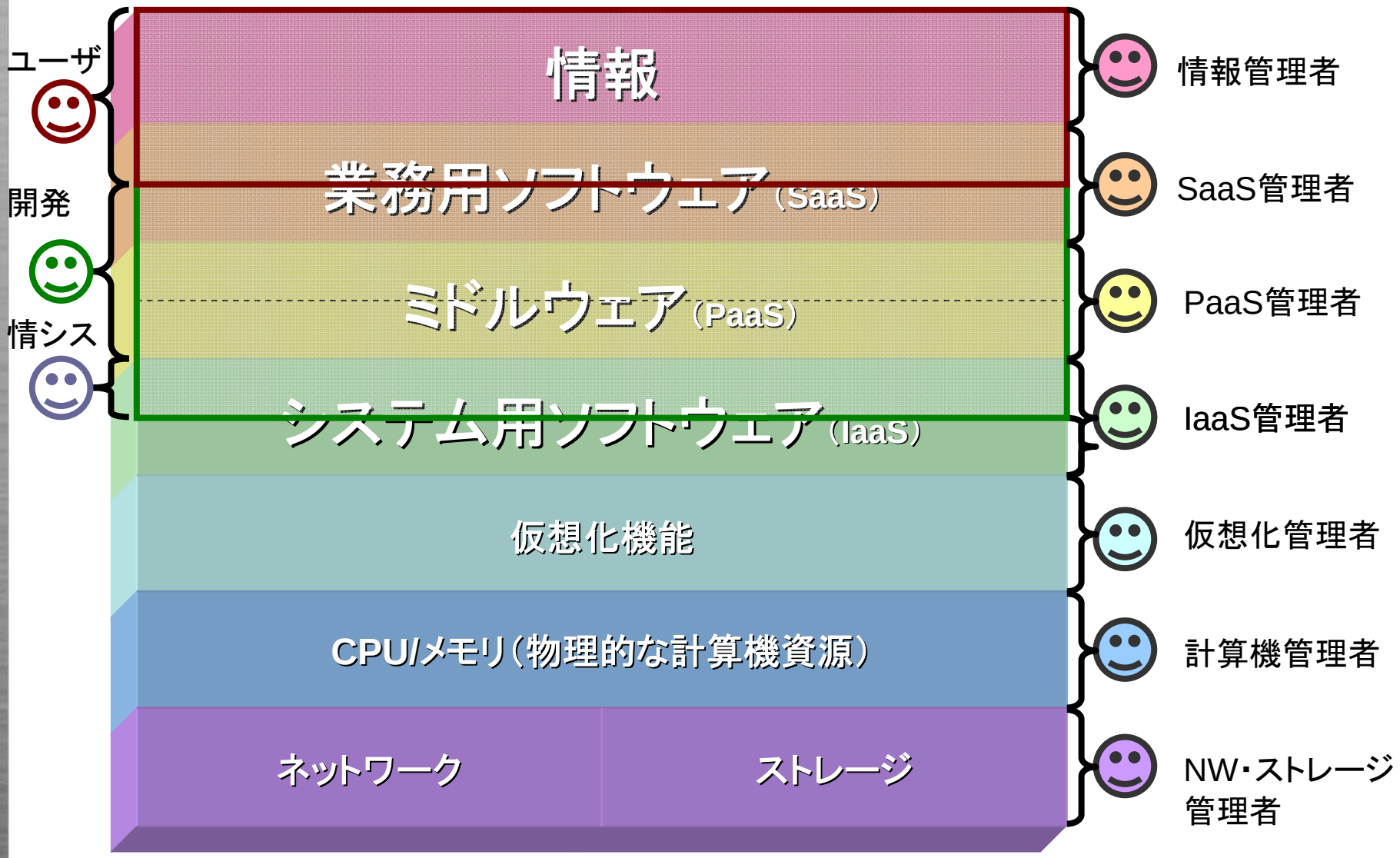
SaaSの管理責任分界点



PaaSの管理責任分界点



IaaSの管理責任分界点



概念的には

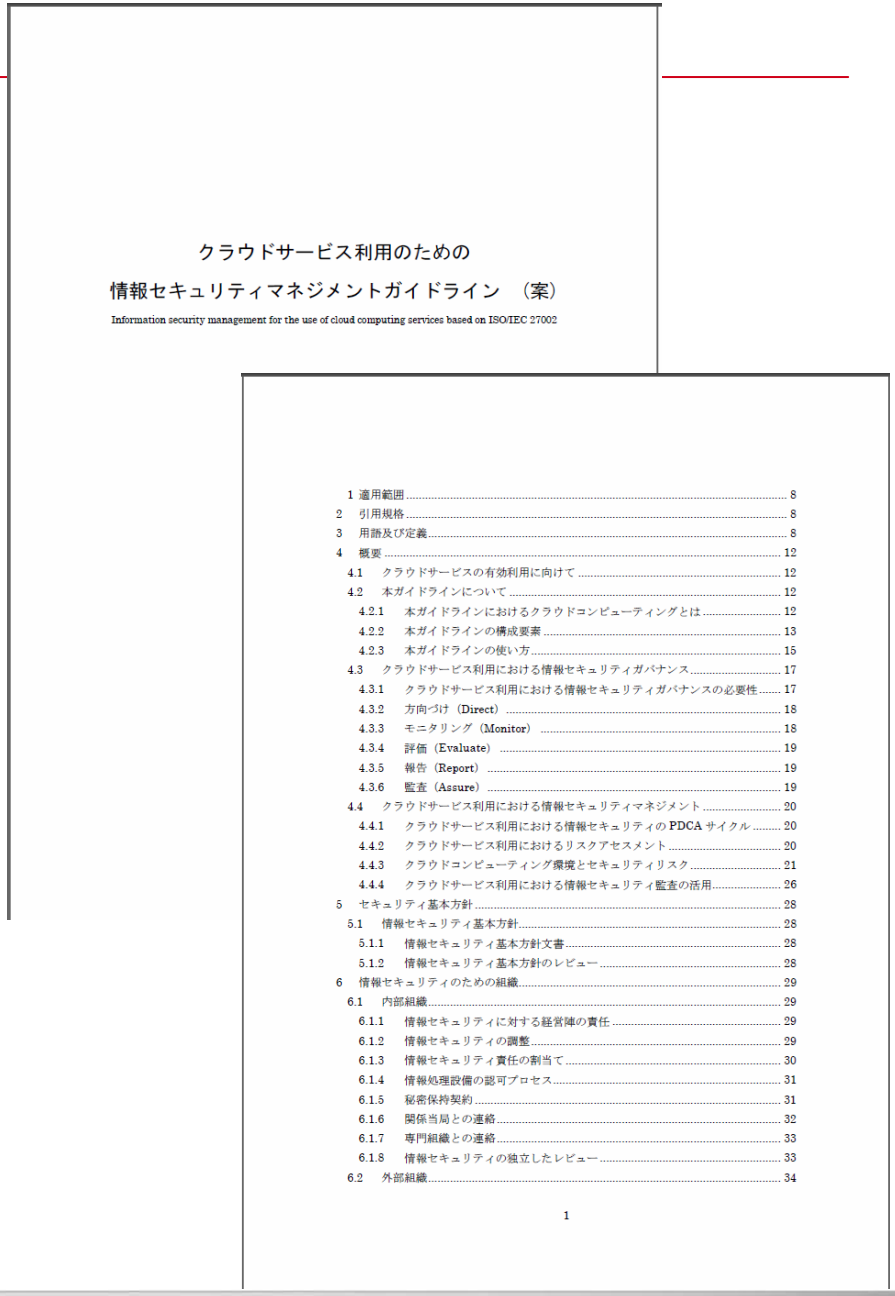
- 事業者と利用者で管理領域を分担している
- 利用/提供するサービスによって管理領域が異なる
- セキュリティ対策に関しても、事業者が対応すべき領域と利用者が対応すべき領域がある

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

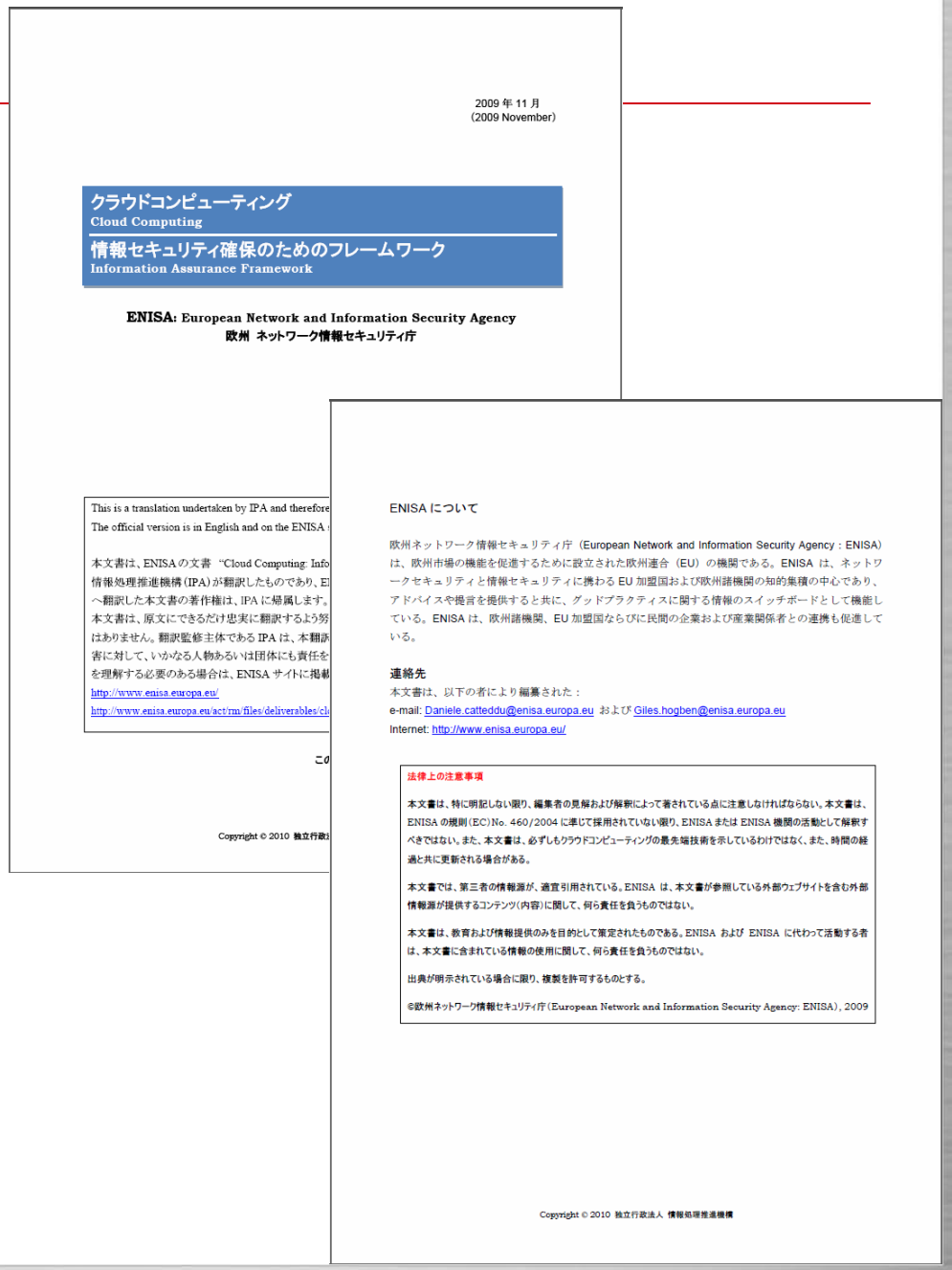
1

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



2009 年 11 月
(2009 November)

クラウドコンピューティング
Cloud Computing

情報セキュリティ確保のためのフレームワーク
Information Assurance Framework

ENISA: European Network and Information Security Agency
欧州 ネットワーク情報セキュリティ庁

This is a translation undertaken by IPA and therefore
The official version is in English and on the ENISA

本文書は、ENISA の文書 "Cloud Computing: Info
情報処理推進機構（IPA）が翻訳したものであり、EI
へ翻訳した本文書の著作権は、IPA に帰属します。
本文書は、原文にできるだけ忠実に翻訳するよう努
はありません。翻訳監修主体である IPA は、本翻訳
害に対して、いかなる人物あるいは団体にも責任を
を理解する必要のある場合は、ENISA サイトに掲載
http://www.enisa.europa.eu/
http://www.enisa.europa.eu/act/rm/files/deliverables/cl

Copyright © 2010 独立行政

ENISA について

欧州ネットワーク情報セキュリティ庁（European Network and Information Security Agency：ENISA）は、欧州市場の機能を促進するために設立された欧州連合（EU）の機関である。ENISA は、ネットワークセキュリティと情報セキュリティに携わる EU 加盟国および欧州諸機関の知的集積の中心であり、アドバイスや提言を提供すると共に、グッドプラクティスに関する情報のスイッチボードとして機能している。ENISA は、欧州諸機関、EU 加盟国ならびに民間の企業および産業関係者との連携も促進している。

連絡先
本文書は、以下の者により編纂された：
e-mail: Daniele.catteddu@enisa.europa.eu および Giles.hogben@enisa.europa.eu
Internet: http://www.enisa.europa.eu/

法律上の注意事項

本文書は、特に明記しない限り、編集者の見解および解釈によって著されている点に注意しなければならない。本文書は、ENISA の規則（EC）No. 460/2004 に準じて採用されていない限り、ENISA または ENISA 機関の活動として解釈すべきではない。また、本文書は、必ずしもクラウドコンピューティングの最先端技術を示しているわけではなく、また、時間の経過と共に更新される場合がある。

本文書では、第三者の情報源が、適宜引用されている。ENISA は、本文書が参照している外部ウェブサイトを含む外部情報源が提供するコンテンツ（内容）に関して、何ら責任を負うものではない。

本文書は、教育および情報提供のみを目的として策定されたものである。ENISA および ENISA に代わって活動する者は、本文書に含まれている情報の使用に関して、何ら責任を負うものではない。

出典が明示されている場合に限り、複製を許可するものとする。

©欧州ネットワーク情報セキュリティ庁（European Network and Information Security Agency: ENISA）, 2009

Copyright © 2010 独立行政法人 情報処理推進機構

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

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、事業者と利用者で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

IIJ Internet Initiative Japan

ご清聴ありがとうございました

Ongoing Innovation