明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

クラウドのセキュリティ対策と国際標準化の最新動向

July 10, 2012

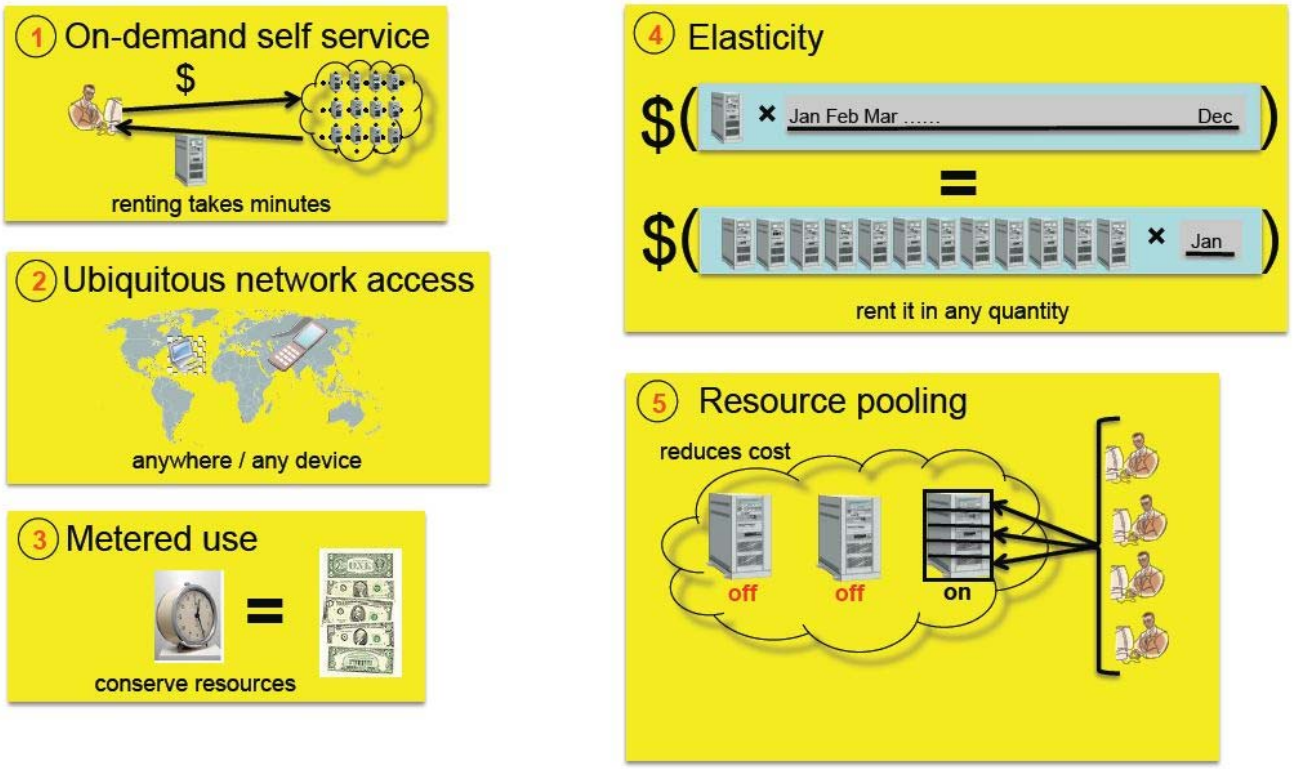
情報セキュリティ大学院大学
後藤　厚宏 goto@iisec.ac.jp

アジェンダ

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

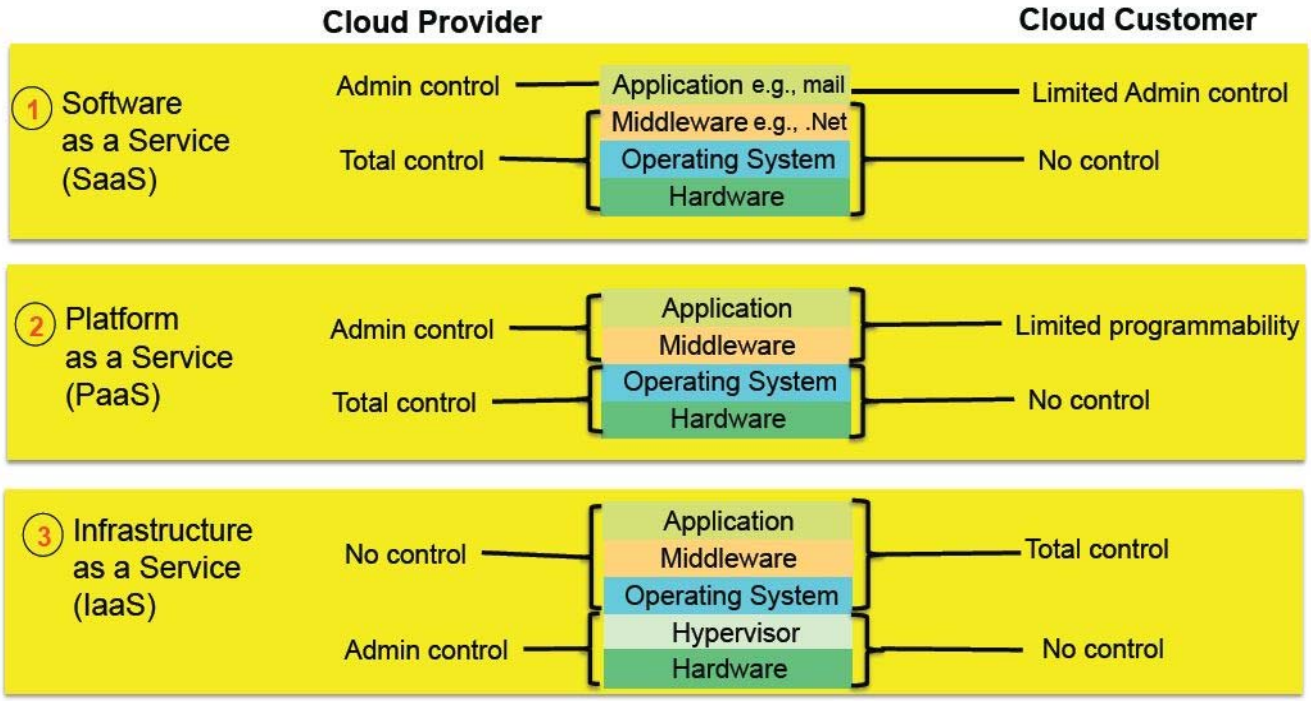
- クラウドサービスシステムの視点
- クラウドとセキュリティ課題
- クラウドセキュリティの取り組み技術例
- クラウド国際標準化動向
- 米国政府のクラウド導入とセキュリティ戦略
- クラウド国際標準化動向（インタークラウドとGICTF）
- まとめ

クラウドに必要な5要素



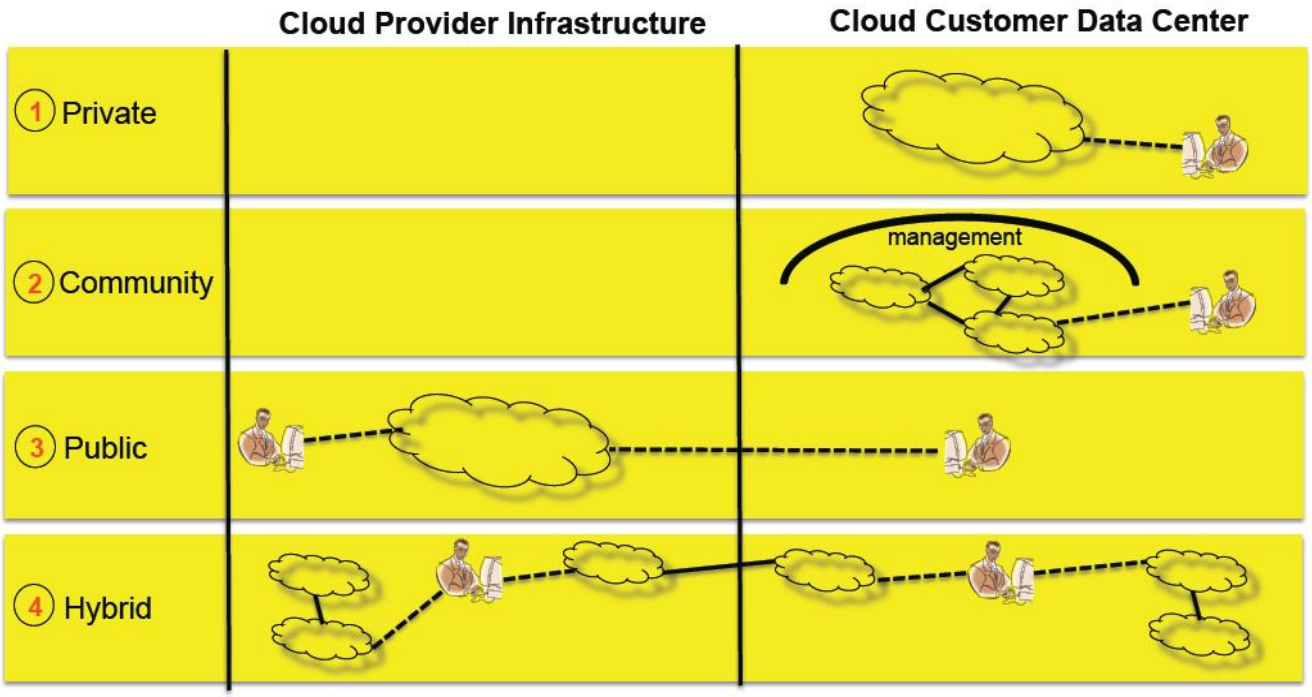
"Cybersecurity and Standards Acceleration to Jumpstart Adoption of Cloud Computing (SAJACC)" より転載

3種類のデプロイメントモデル



NIST cloud computing FORUM & WORKSHOP
"Cybersecurity and Standards Acceleration to Jumpstart Adoption of Cloud Computing (SAJACC)" より転載

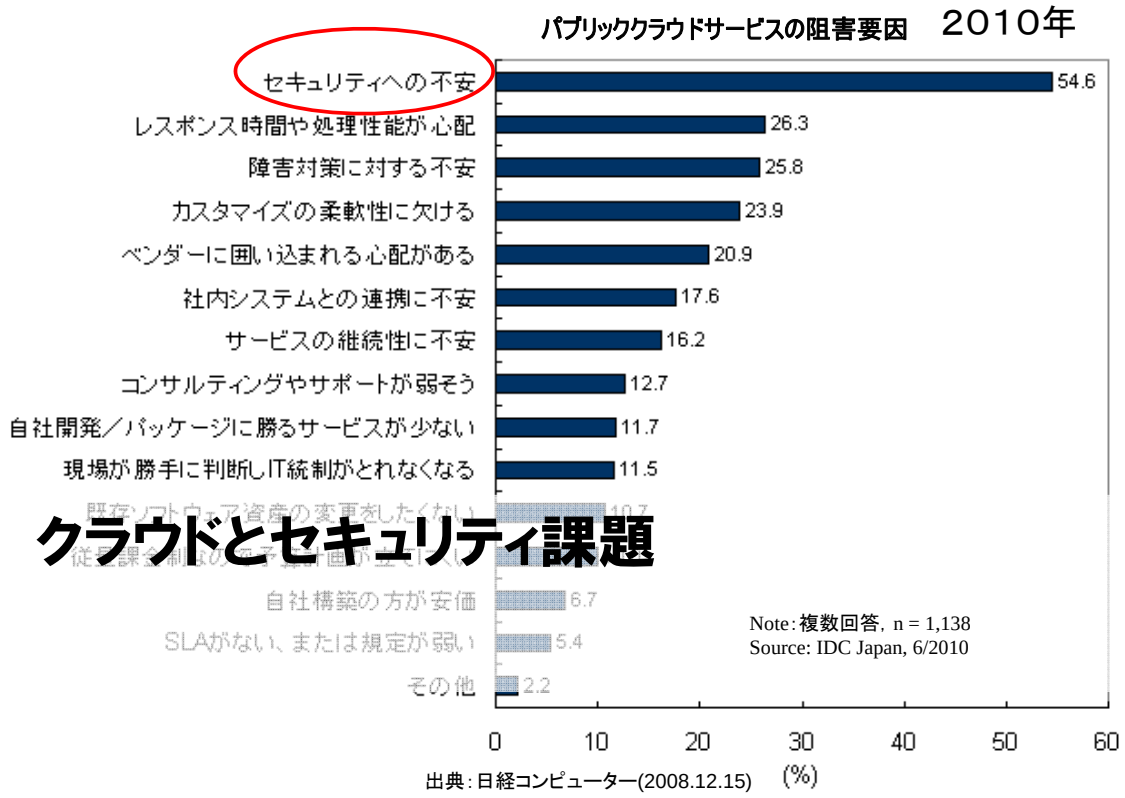
4種類のデリバリモデル



NIST cloud computing FORUM & WORKSHOP
"Cybersecurity and Standards Acceleration to Jumpstart Adoption of Cloud Computing (SAJACC)" より転載

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

クラウドとセキュリティ課題



出典：日経コンピューター(2008.12.15)

Confidentiality　秘匿性

- クラウドに機微なデータを格納しても大丈夫？　(i.e. データの制御権を手放すことへの不安)
- クラウドプロバイダ自身、顧客のデータを覗き見したりしないか？

Integrity　完全性、保全性

- クラウドプロバイダーが正しく計算機処理をしているって、どうやって確かめられる？
- クラウドプロバイダーは勝手に私のデータを改竄したりしない？

A malicious insider with root level access

Availability　可用性

- クラウドプロバイダがDDoS攻撃に晒されても、我々顧客の重要システムは大丈夫？
- クラウドプロバイダが事業を放棄したらどうなるの？

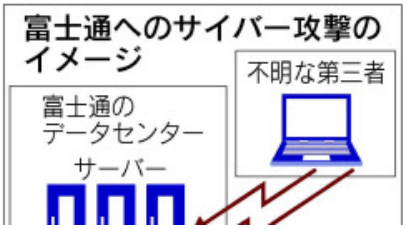
日本経済新聞　小 中 大　印刷

富士通のサーバーに攻撃　クラウドの安全対策急務

2011/11/11 3:08 | 日本経済新聞　電子版

富士通が地方自治体向けにクラウドコンピューティングで提供する電子申請サービスがサイバー攻撃を受けた。ネットワークを通じてシステム機能を提供するクラウドサービスを提供するIT(情報技術)企業が攻撃されると顧客への被害が一気に拡大するリスクが表面化した。富士通などIT企業はクラウドの安全対策の強化が求められそうだ。

富士通によると同社のデータセンターにある電子申請システムのサーバーに対し、30余りのIPアドレスから処理しきれない大量のアクセスが繰り返される「DoS(サービス停止)攻撃」があった。富士通のサービスを利用して電子申請サイトを提供している福島、千葉、静岡、福岡など各県で9日午後から10日朝にかけ



Privacy issues 大量データに関わるプライバシー問題

- クラウドには大量の利用者データが蓄積されているけど、そのデータをデータマイニングすると我々利用者のプライバシー情報が取り出されてしまうのでは？

Increased attack surface　攻撃されやすくなるのでは？

- 企業の外にあるクラウドにデータを置いて計算機処理をしていると、クラウドと企業間を結ぶ通信回線が恰好の標的になったりしない？
- クラウドプロバイダーの従業員がフィッシング詐欺にあったりしない？

Auditability and forensics　監査と鑑識

- データが組織の外のクラウドに置かれると監査が難しくなるのでは？
- 利用者がデータをローカルに持たないと、鑑識も難しくなる

Legal and transitive trust issues 法律と信用移行

- 制度や法規制の遵守は誰が責任をもつの？
- クラウドプロバイダが他のクラウドに第三者委託をしているとき、データは大丈夫？

クラウドセキュリティの取り組み技術例

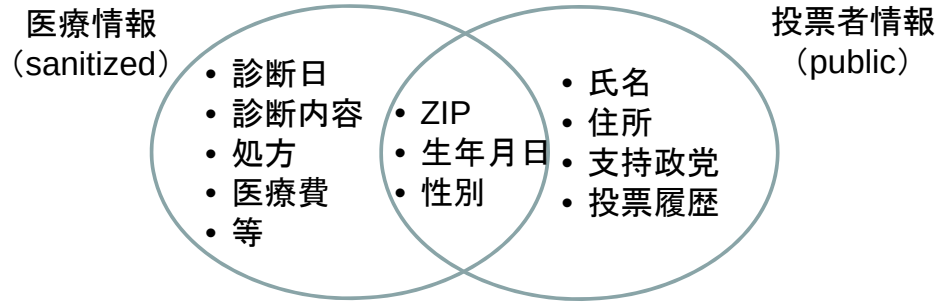
クラウドセキュリティ技術マップ

プライバシ保護データマイニング（PPDM）

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- PPDM: Privacy Preserved Data Mining
  - ●匿名化の方法：データベースに雑音を加える方法
  - ●暗号化の方法：データを暗号化して、そのまま処理
- 匿名化の方法
  - ●Microdata（生の個別データ）をsanitized（実名を隠す、電話番号を隠す）

  ⇒ “Link attacks” の脅威（公開データからプライバシー情報を推測できる可能性あり）
    - ◆有名な例：Massachussetts州知事の医療情報が公開情報から特定可能（6人が知事と同じ生年月日、うち3人が男、内一人が同じZIP）



プライバシ保護データマイニング（PPDM）

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- プライバシーを守るための匿名化
  - ●ExplicitなID（氏名など）は削除
  - ●医療情報のようなsensitiveデータは、分析の対象（削除や変換できない）
  - ●個人特定が可能なデータ（Quasi ID: 生年月日、性別、ZIPなど）をどうするか？
- k-匿名性（k-anonymity）
  - ●個人を他のk-1人に紛れさせる
  - ●公開された 個別データにおいて、Quasi IDが同じ値の個人は少なくとも “k”人存在することを保証 ⇒ link attackでも個人特定の確立は 1/k

	誕生日	性別	ZIP
グループ1	*/1/79	人	5****
	*/1/79	人	5****
（削除）	1/10/44	女	90210
グループ2	*/*/8*	男	022**
	//8*	男	022**

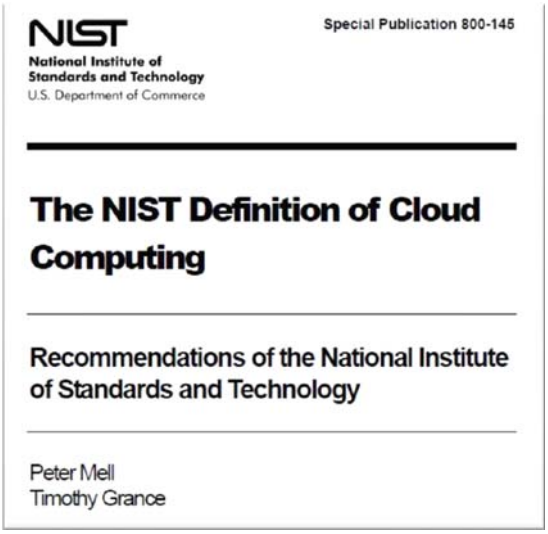
2-anonymity

①リファレンスモデル、ガイドライン議論状況

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■ リファレンスモデルの策定
- ●クラウドは幅広い技術要素、ビジネス要素を含む
- ●**米国立標準技術研究所NIST**が大きく貢献

■ ユースケースの議論⇒標準化が必要な要件の整理
- ●ITU-T, ISO/IEC JTC1
- ●米国、欧州、韓国、日本等の主要な団体



NIST Special Publication 800-145
Sept. 2011

①リファレンスモデル、ガイドライン議論状況

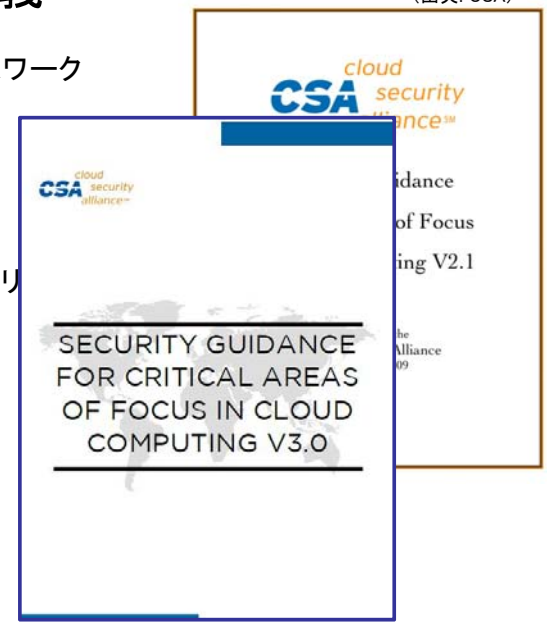
明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

CSA（Cloud Security Alliance）のセキュリティに関する取り組み

・14分野のベストプラクティスを定義

1. クラウドコンピューティングのアーキテクチャフレームワーク
2. ガバナンスとエンタープライスリスク管理
3. リーガルと電子開示
4. コンプライアンスと監査
5. 情報ライフサイクル管理
6. ポータビリティと相互運用性
7. 伝統的なセキュリティー事業継続性ディザスタリカバリ
8. データセンター運用管理
9. 事故に対する対応、通知、回復
10. アプリケーションセキュリティー
11. 暗号化と鍵管理
12. アイデンティティとアクセス管理
13. 仮想化
14. Security as a Service ← V3.0で追加

（出典: CSA）



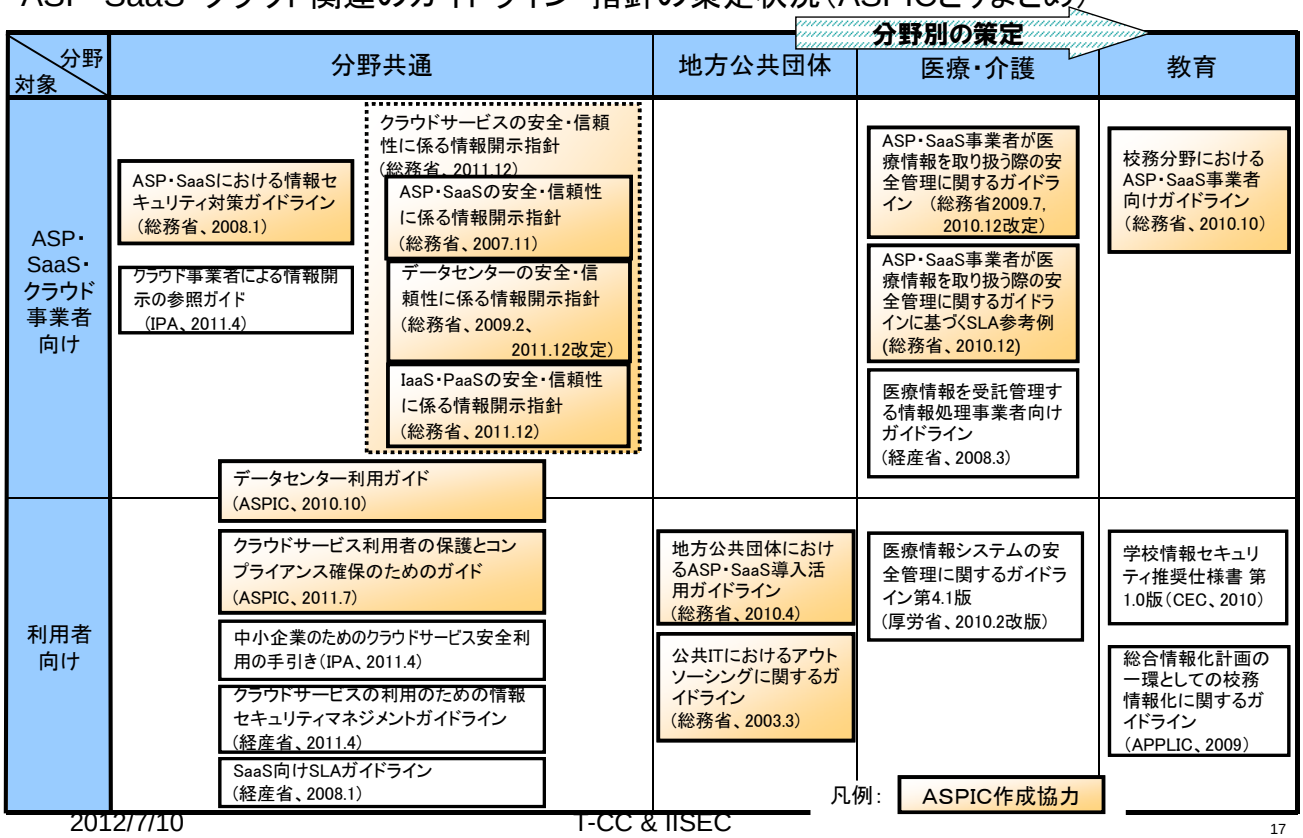
Nov 2011

Ver 1.0はASPICが翻訳しインプレスR&Dからの出版

①リファレンスモデル、ガイドライン議論状況

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

ASP・SaaS・クラウド関連のガイドライン・指針の策定状況（ASPICとりまとめ）



参考：日本でのクラウド標準化活動インデックス

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- 一般社団法人情報通信技術委員会　TTC（⇒ITU-T）
  http://www.ttc.or.jp/j/std/committee/ag/cloud/
- 情報処理学会　情報規格調査委員会　（⇒ ISO）
  http://www.itscj.ipsj.or.jp/index.html
- GICTF（Global Inter-Cloud Technology Forum）:
  http://www.gictf.jp
- DMTF 日本支部
  http://dmtf.org/jp
- SNIA日本支部
  http://www.snia-j.org/
- ASP・SaaS・クラウド コンソーシアム　ASPIC
  http://www.aspicjapan.org/
- 情報処理推進機構　IPA
  http://www.ipa.go.jp
- 他