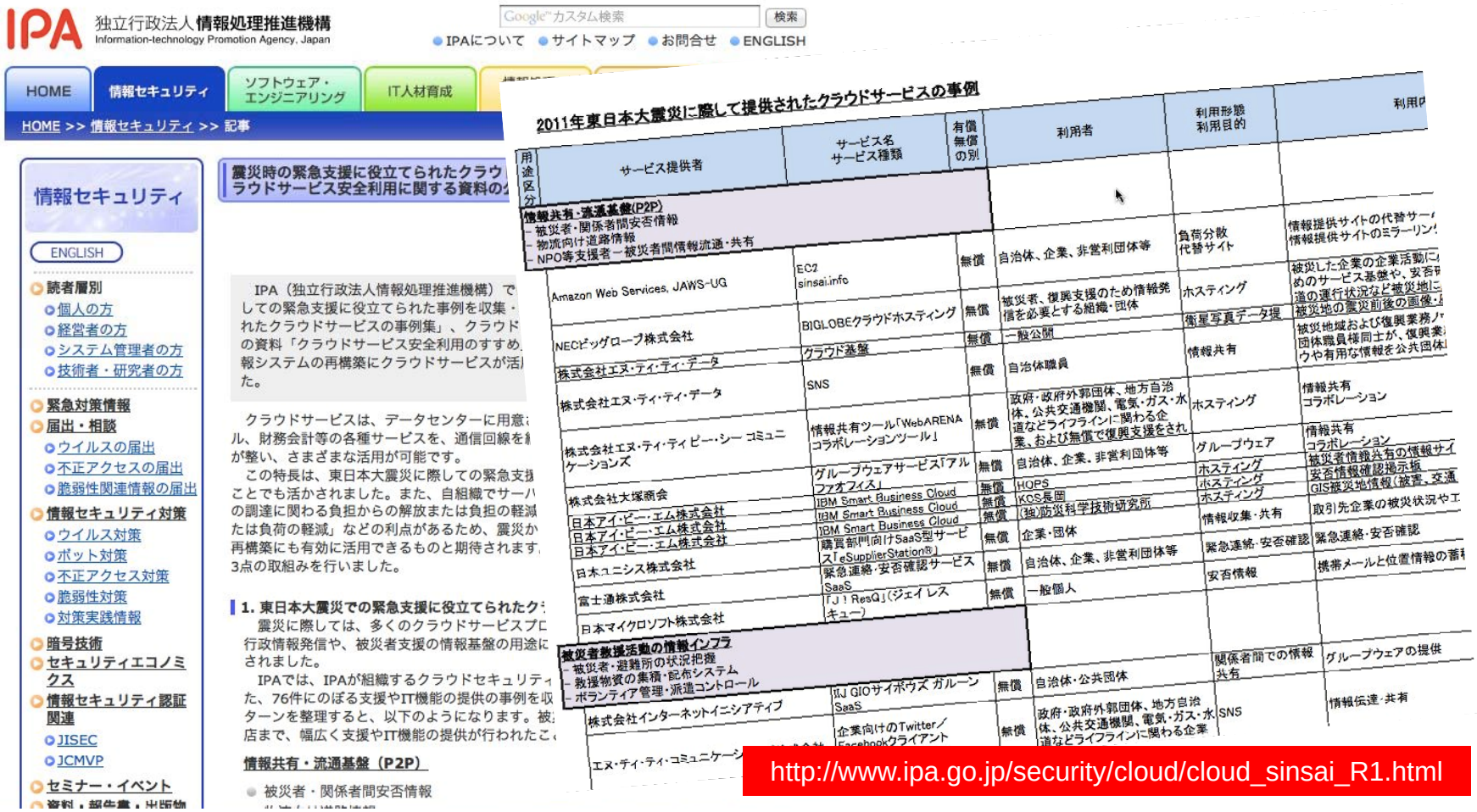
加藤さんのお話に加えて・・・



クラウドコンピューティングにおける セキュリティの考え方と標準化

株式会社ディアイティ セキュリティサービス事業部
河野省二, CISSP <shoji@dit.co.jp>

本日のアジェンダ

- クラウドコンピューティングって安全ですか？
  - クラウドコンピューティングに関する不安
  - クラウドコンピューティングでなにが変わるのか
  - 情報セキュリティマネジメントにおけるクラウドコンピューティング
- クラウドセキュリティの標準化
  - 経産省
    - 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
  - SC27 WG1
    - Standards for Cloud Computing Security and Privacy

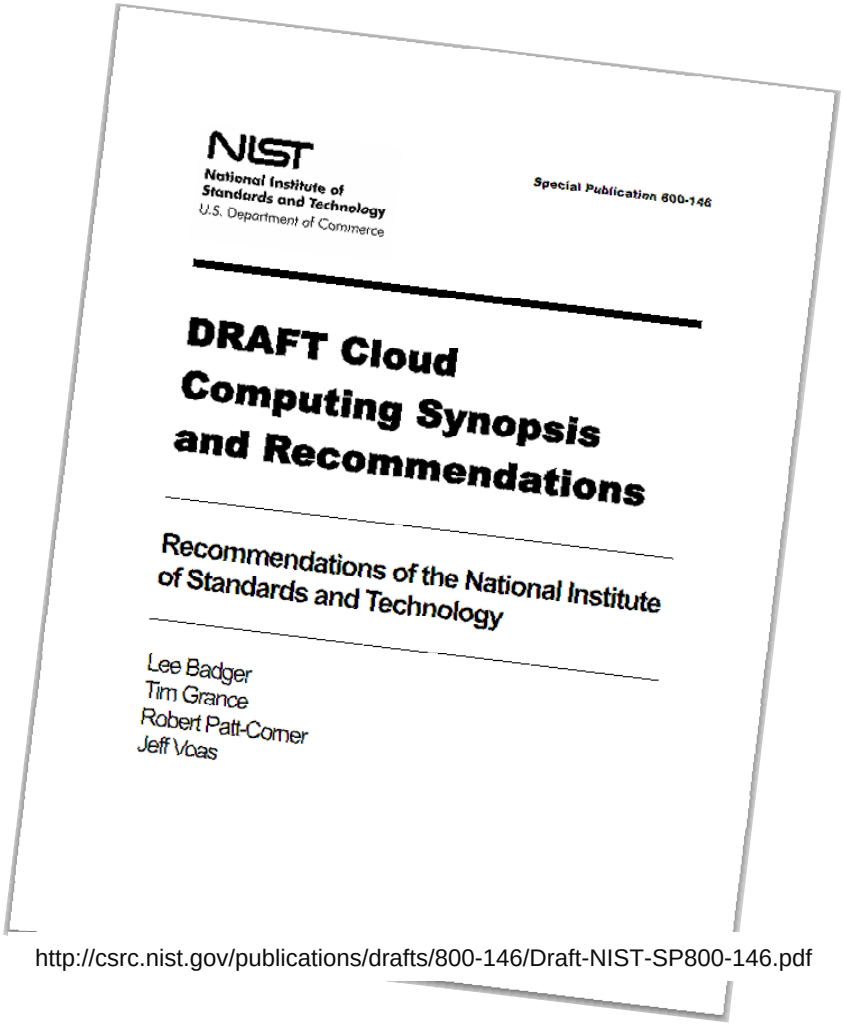
クラウドコンピューティングの特性から見る安全性の確保

クラウドコンピューティングって安全ですか？

クラウドコンピューティングに関する不安

- クラウドに関する様々な不安は以下の3つに分けることができる
  - クラウドのシステム（インフラ）に関するもの
    - 仮想化、分散処理、ネットワーク、端末など
  - クラウドのサービスに関するもの
    - 事業継続、コスト、サービス事業者（組織、社員）など
  - メンタル的なもの
    - 新しいものに対する不安、わからないものに対する不安
- クラウド以前にできてないことは、クラウド以降もできない
  - クラウドになったからといって何でもできるようになるわけではない
  - クラウドに関して正しい情報を入手することがまだまだ難しい

クラウドコンピューティングとは？


NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-146

DRAFT Cloud Computing Synopsis and Recommendations

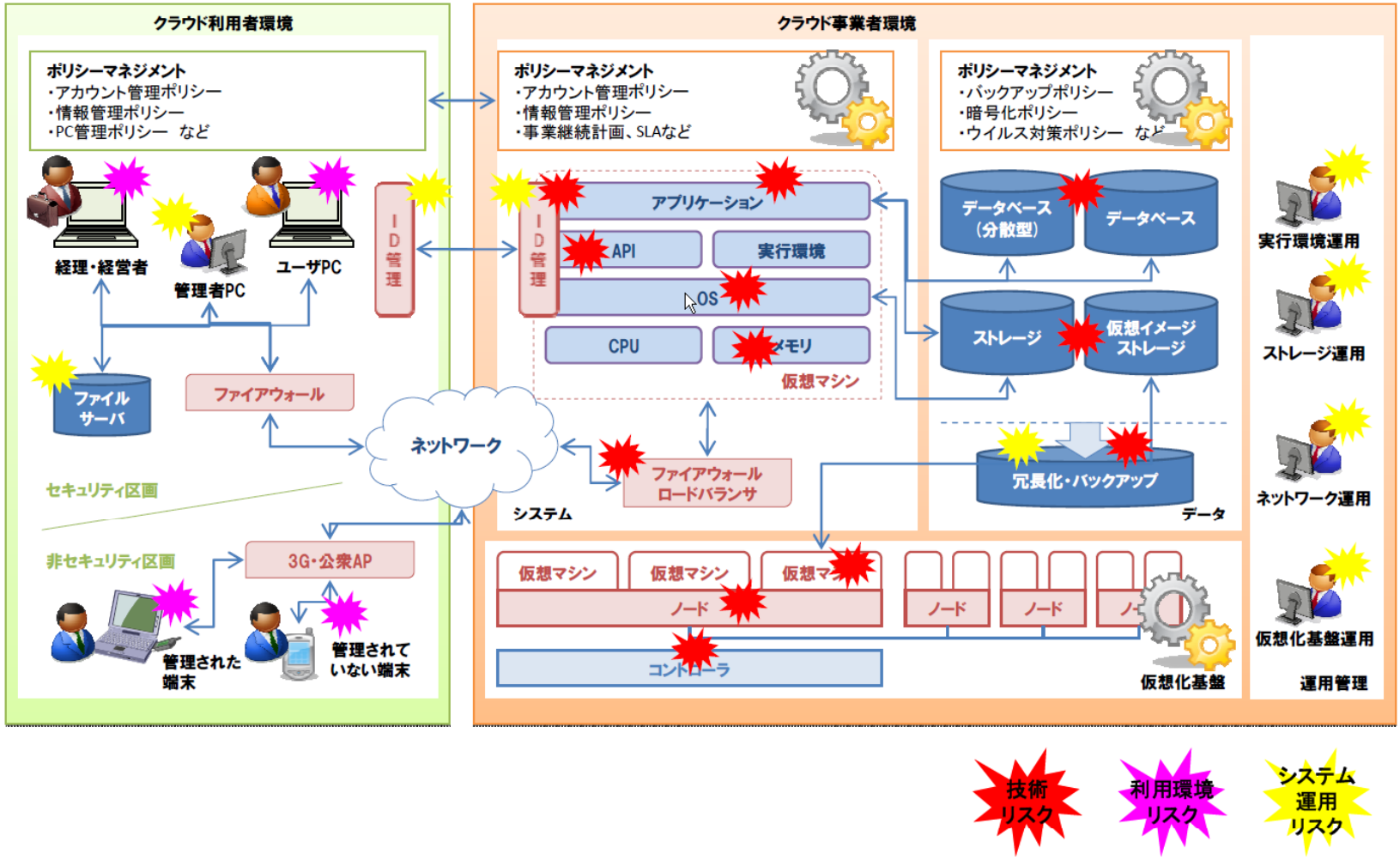
Recommendations of the National Institute of Standards and Technology

Lee Badger
Tim Grance
Robert Patt-Corner
Jeff Voas

http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf

- NIST SP800-146
  - 本質的な特徴
    - On-demand self-service
    - Broad network access
    - Resource pooling
    - Rapid elasticity
    - Measured Service
  - サービスモデル
    - Cloud Software as a Service (SaaS)
    - Cloud Platform as a Service (PaaS)
    - Cloud Infrastructure as a Service (IaaS)

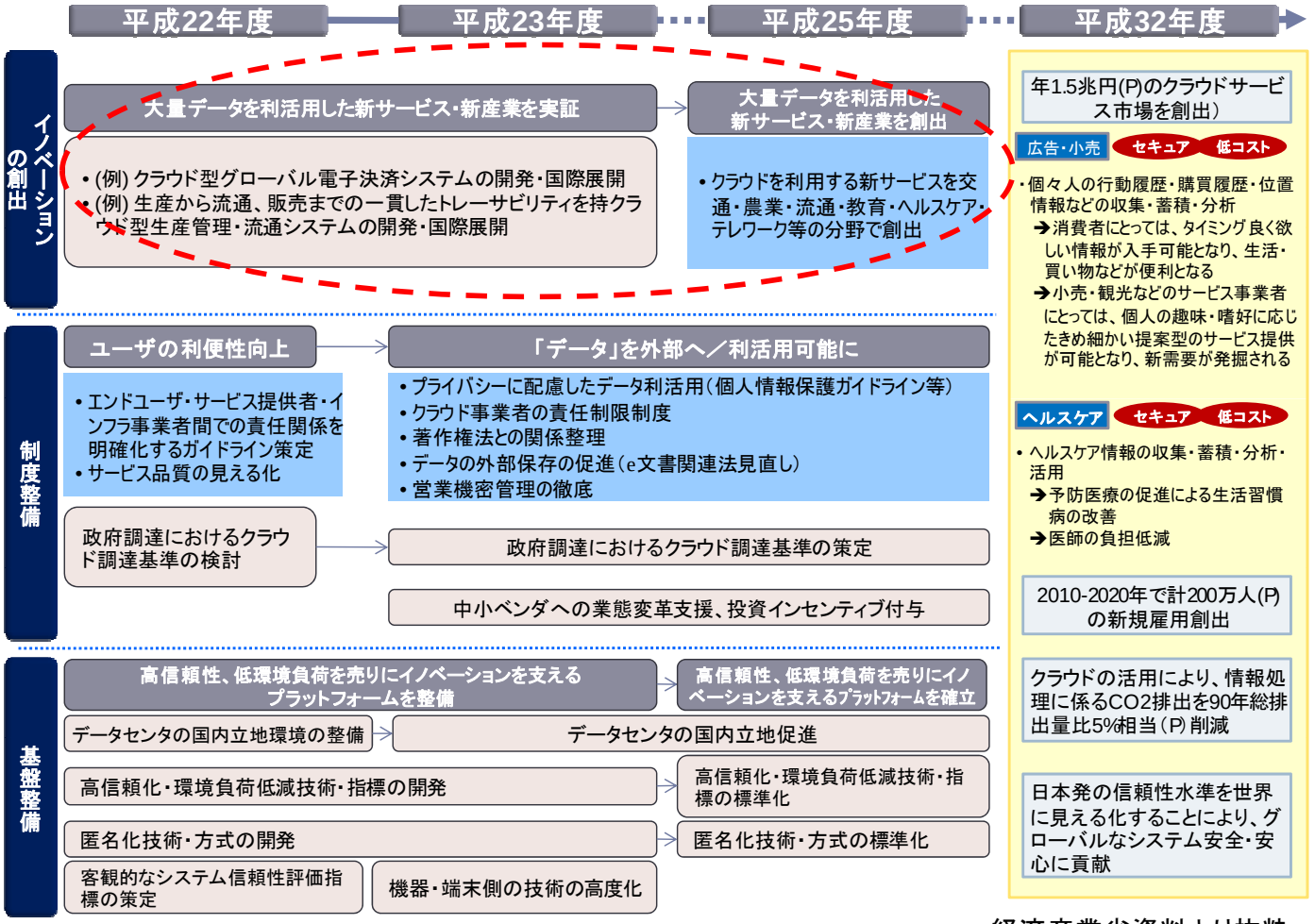
クラウドコンピューティングの環境



リスクマネジメントの基本は崩さずに

- リスクマネジメントの基本は「脅威、ぜい弱性の特定」
  - たとえば、会社でTwitterを使っても良いかを検討するときに「Twitterは安全か？」と考えているだけではダメ
  - クラウドコンピューティングは「サービス」であると考え、サービスとそれをとりまくすべての環境においてリスクアセスメントを行う
- クラウドサービスに向いているか向いていないか？
  - クラウドサービスの信頼性について議論があるが、そもそもバックアップを取らなくても良いシステムなどはない
    - バックアップが取りやすいか？バックアップの必要性がないか？など、サービスの選択を正しく行うための情報収集を行う
  - 手元に（個別に）情報を持たないことの安全性についても考える

情報化推進の方向性とクラウドのあり方



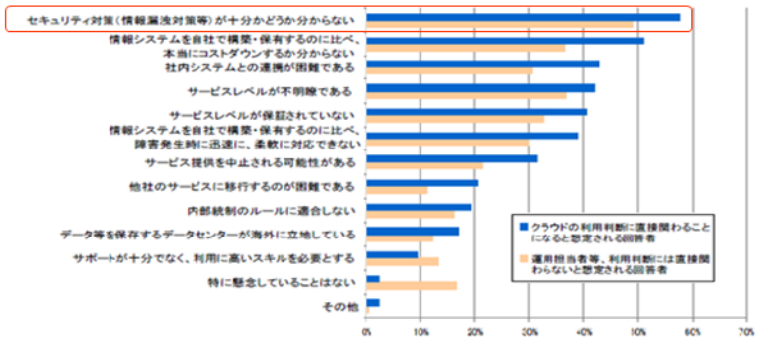
経済産業省資料より抜粋

標準化のためのベースと考え方

クラウドセキュリティの標準化

クラウドセキュリティガイドラインの策定

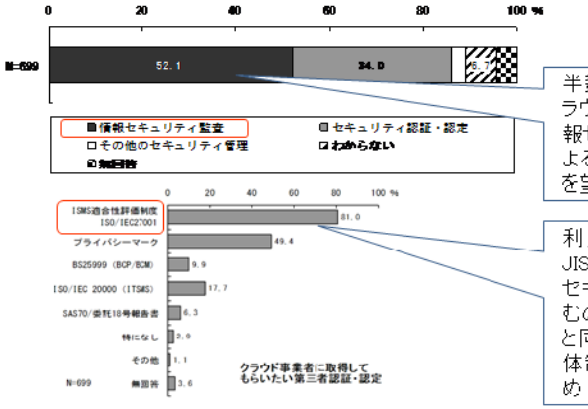
クラウド利用者の不安



＊「高度情報化社会における情報システム・ソフトウェアの信頼性及びセキュリティに関する研究会」（経済産業省2009年3月）

クラウド利用においてセキュリティ上の不安が払拭できていない

クラウド事業者への要求



半数の利用者が、クラウド事業者には情報セキュリティ監査による、具体的な報告を望んでいる

利用者が事業者にJIS Q 27000ベースのセキュリティ管理を望むのは、利用者組織と同様のセキュリティ体制を望んでいるため

＊「クラウドサービスの情報セキュリティ監査に関するアンケート調査報告書」（経済産業省2010年1月）

クラウド利用者はクラウド事業者に、情報セキュリティ監査およびJIS Q 27000ベースのセキュリティ管理を望んでいる。

「情報セキュリティ」および「事業者におけるシステム運用」が見えないことに関する不安を「見える化」する

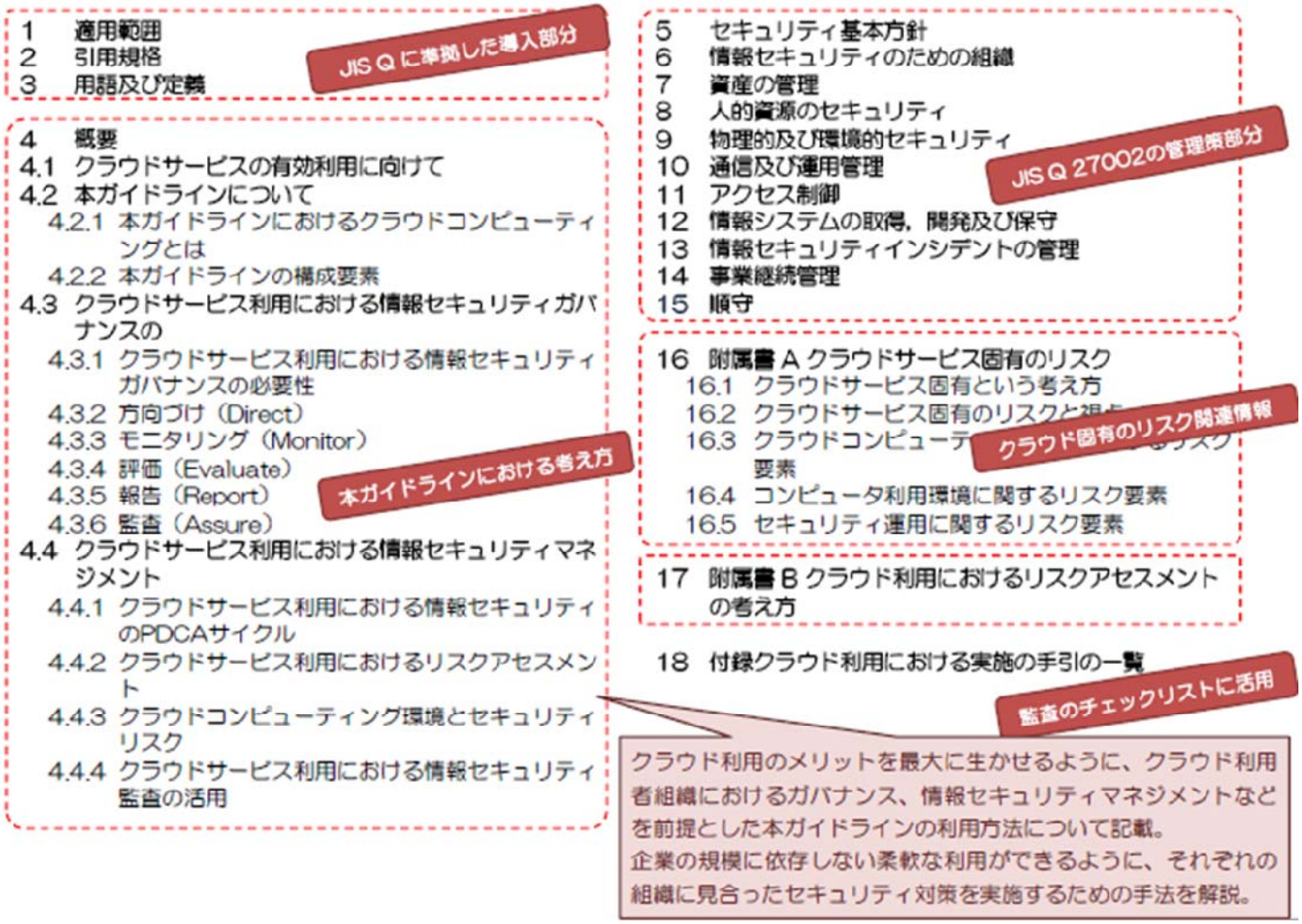
クラウドサービスの利用のための情報セキュリティマネジメントガイドライン

- 利用者における セキュリティリスクの 共通認識の形成
- 事業者選択における 基準として利用できる 対策標準
- 情報セキュリティ監査による 利用者と事業者の 信頼関係の構築

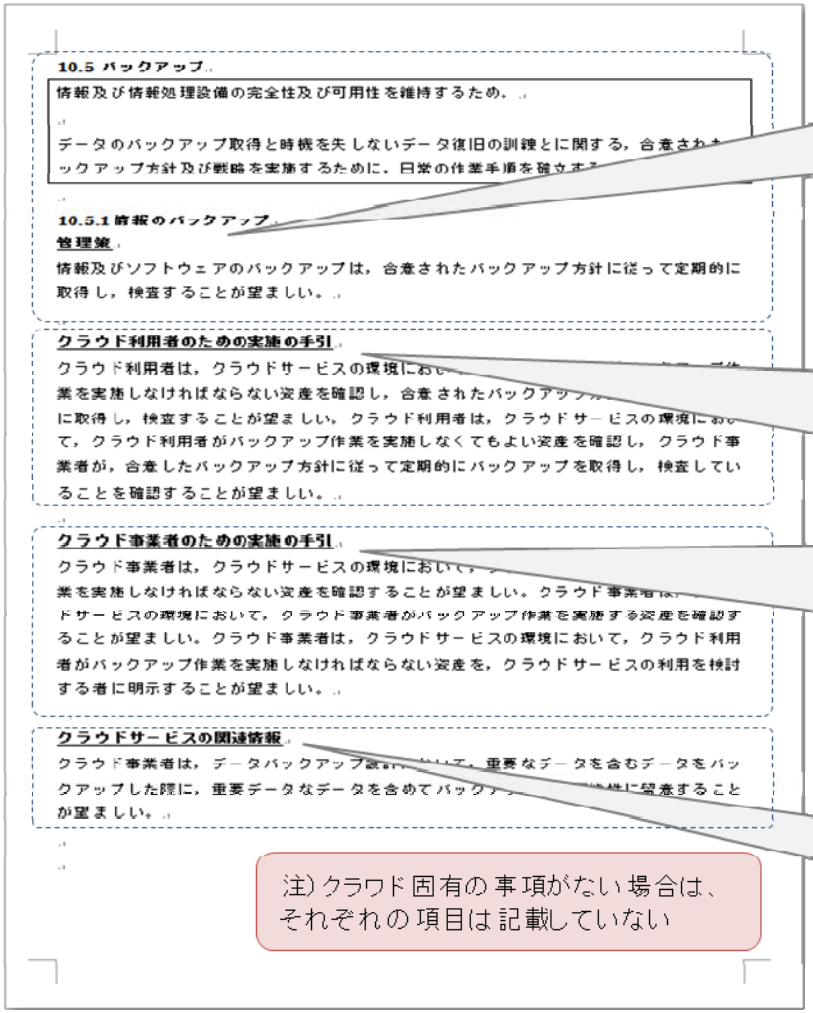
クラウドサービス利用のための情報セキュリティマネジメントガイドライン

- JIS Q 27002をベースにしたガイドライン
  - クラウド利用者が安心してクラウドサービスを利用することが出来るために、システムライフサイクルに応じた「実施の手引」を提供
  - ISMS認証のベースを変えることなくリスクマネジメントを実施できるようにしている
  - 事業者が実施すべき対策についても、利用者への情報提供として記載

マネジメントシステムを活用する



ガイドラインのサンプル



管理策の目的と管理策

- 管理策の目的と管理策は、JIS Q 27002:2006をそのまま引用。
- 情報セキュリティ監査に利用する場合にも、目的を明確にするために利用が可能。

クラウド利用者のための実施の手引

- 管理策を順守するための、クラウド利用者組織における実施事項を記載。
- 実施事項には、クラウドサービス利用組織における、情報システム等の変化に伴うリスクの軽減のためのセキュリティ対策や考え方を記載。

クラウド事業者のための実施の手引

- クラウド利用者組織が管理策を順守するために自ら実施するのではなく、クラウド事業者に実施してもらう必要があるセキュリティ対策事項について記載。
- クラウド事業者を選定する際の選定基準や、情報セキュリティ監査における管理基準として活用が可能。

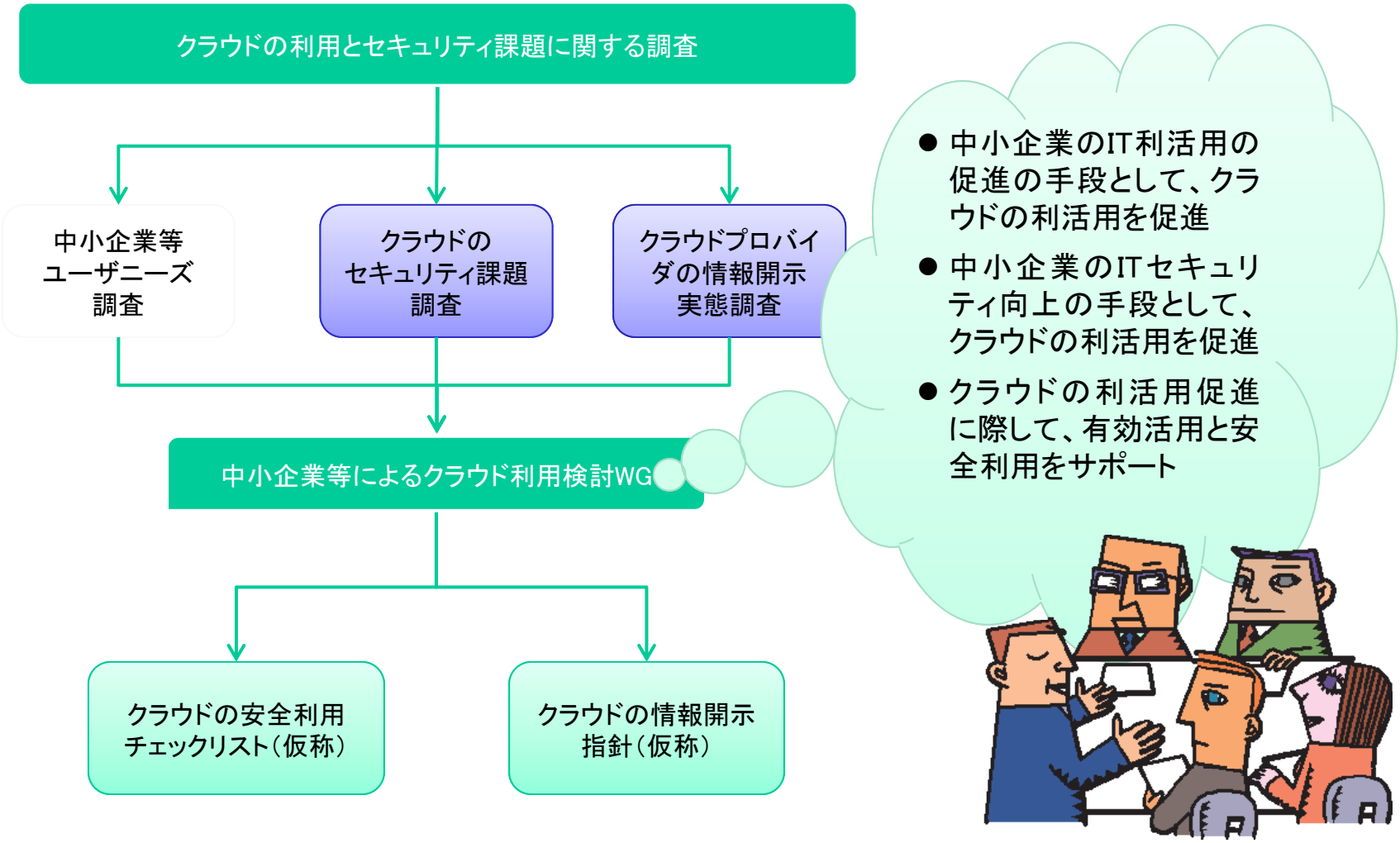
クラウドサービスの関連情報

- 当該項目では、クラウドサービスの形態や環境に特有の、個別の実施事項について記載。

ガイドラインの国際化に向けて

- IS Technical Specification
  - ISOに向けて技術文書として策定中
  - 日本発の取り組みとして、国際化のリードを行う
- スケジュール
  - 2010/10 Study Period start
  - 2011/04 NP vote propose
  - 2011/10 WD start
  - 2012/10 PDTR
  - 2013/xx published

IPA:中小企業等によるクラウド利用検討WG



本資料のお問い合わせは

株式会社ディアイティ

セキュリティサービス事業部

03-5634-7655 / ss-info@dit.co.jp

時間調整ではありません（笑）

クラウドセキュリティ言いたい放題

トークテーマ（その１）

最近気になる、クラウドに関する「思い込みセキュリティ」ってありますか？

こんな思い込みセキュリティが・・・

- SaaSとかPaaSとかIaaSというセキュリティの区分けは成り立たない
  - SPIスタックみたいなものは技術的なカットであって、多くの方が心配してるマネジメント視点（内部の犯罪者、データ管理の問題など）とは異なる
  - 実際のビジネス構造と合っていない視点で論じてもダメ
- 情報が少なすぎる（煽りがほとんど・・・）
  - 利用者が判断できる内容まで専門家が話せていない（たぶん使ったことがないか理解していない）
  - もっと前向きな考えで標準化などに取り組んだほうが良い

トークテーマ（その２）

クラウドサービスの
困ったところってなんですか？

ベンダーとして困ったところ

- 利用者からの要求に応えることはできるが・・・
  - 利用者からの要求に応じてセキュリティ対策をしていると、結果としては使いにくいだけの基板提供となってしまう
  - 一度ハードルを上げたセキュリティを緩和することは難しくなってしまう可能性がある
- 一方、利用者としては
  - 利用者がどこまでやれば良いのかわからないので、どうしてもベンダーに頼ってしまう
  - 事故などの事例がなく、万が一の事故にどのように対応して良いかわからない
  - 情報開示をお互いにしていくのが良いのではないか