

# 加藤さんのお話に加えて・・・



## 情報セキュリティ

ENGLISH

### 読者層別

- 個人の方
- 経営者の方
- システム管理者の方
- 技術者・研究者の方

### 緊急対策情報

- 届出・相談
  - ウイルスの届出
  - 不正アクセスの届出
  - 脆弱性関連情報の届出

### 情報セキュリティ対策

- ウイルス対策
- ポット対策
- 不正アクセス対策
- 脆弱性対策
- 対策実践情報

### 暗号技術

### セキュリティエコノミクス

### 情報セキュリティ認証関連

- JISEC
- JCMVP

### セミナー・イベント

- 資料、報告書、出版物

## 震災時の緊急支援に役立てられたクラウドサービス安全利用に関する資料の紹介

IPA（独立行政法人情報処理推進機構）での緊急支援に役立てられた事例を収集・れたクラウドサービスの事例集」、クラウドの資料「クラウドサービス安全利用のすすめ、報システムの再構築にクラウドサービスが活かした。

クラウドサービスは、データセンターに用意した、財務会計等の各種サービスを、通信回線を通じて提供し、さまざまな活用が可能です。この特長は、東日本大震災に際しての緊急支援でも活かされました。また、自組織でサーバの調達に関わる負担からの解放または負担の軽減または負荷の軽減などの利点があるため、震災が再構築にも有効に活用できるものと期待されます。3点の取組みを行いました。

**1. 東日本大震災での緊急支援に役立てられたクラウドサービス**  
震災に際しては、多くのクラウドサービスで行政情報発信や、被災者支援の情報基盤の用途に活用されました。

IPAでは、IPAが組織するクラウドセキュリティ、76件にのぼる支援やIT機能の提供の事例を取組を整理すると、以下ようになります。被災者まで、幅広く支援やIT機能の提供が行われたこと。

### 情報共有・流通基盤 (P2P)

- 被災者・関係者間安否情報

## 2011年東日本大震災に際して提供されたクラウドサービスの事例

用途区分	サービス提供者	サービス名 サービス種類	有償 無償 の別	利用者	利用形態 利用目的	利用IP
情報共有・流通基盤(P2P)	被災者・関係者間安否情報 物流向け道路情報 NPO等支援者-被災者間情報流通・共有					
	Amazon Web Services, JAWS-UG	EC2 sinsai.info	無償	自治体、企業、非営利団体等	負荷分散 代替サイト	情報提供サイトの代替サービス 情報提供サイトのエラーリフレクション
	NECビッグロップ株式会社	BIGLOBEクラウドホスティング	無償	被災者、復興支援のための情報発信を必要とする組織・団体	ホスティング	被災した企業の企業活動に ためのサービス基盤や、災害 時の運行状況など被災地に 被災地の震災前後の画像
	株式会社エヌ・ティ・ティ・データ	クラウド基盤	無償	一般公開	衛星写真データ提供	被災地域および復興業務に 関係する関係者同士の、復興業 務に有用な情報を公共団体
	株式会社エヌ・ティ・ティ・データ	SNS	無償	自治体職員	情報共有	情報共有 コラボレーション
	株式会社エヌ・ティ・ティ・データ	情報共有ツール「WebARENA コラボレーションツール」	無償	政府・政府外団体、地方自治 体、公共交通機関、電気・ガス・水 道などライフラインに関わる企 業、および無償で復興支援をされ	ホスティング	情報共有 コラボレーション
	株式会社大塚商会	グループウェアサービス「フル フーズ」	無償	自治体、企業、非営利団体等	グループウェア	被災者情報共有の情報サイ ンボード 安否情報確認掲示板
	日本アイ・ビー・エム株式会社	IBM Smart Business Cloud	無償	HQPS KOS長岡	ホスティング	取引先企業の被災状況や工 場稼働状況
	日本アイ・ビー・エム株式会社	IBM Smart Business Cloud	無償	（防災科学技術研究所）	ホスティング	緊急連絡・安否確認
	日本アイ・ビー・エム株式会社	IBM Smart Business Cloud	無償	企業・団体	情報収集・共有	緊急連絡・安否確認
	日本アイ・ビー・エム株式会社	購買部門向けSaaS型サービス「eSupplierStation」	無償	自治体、企業、非営利団体等	緊急連絡・安否確認	携帯メールと位置情報の番付
	日本ユニシス株式会社	SaaS	無償	自治体、企業、非営利団体等	安否情報	
	富士通株式会社	「J! ResQ」(ジェイレス キュー)	無償	一般個人	安否情報	
	日本マイクロソフト株式会社					
	被災者救援活動の情報インフラ	被災者・避難所の状況把握 救援物資の集積・配布システム ボランティア管理・派遣コントロール				
株式会社インターネットイニシアティブ		「J! GIOサイボウズ ガルーン SaaS	無償	自治体・公共団体	関係者間での情報共有	グループウェアの提供
情報共有・流通基盤 (P2P)	被災者・関係者間安否情報					
	株式会社インターネットイニシアティブ	企業向けのTwitter/ Facebookクライアント	無償	政府・政府外団体、地方自治 体、公共交通機関、電気・ガス・水 道などライフラインに関わる企業	SNS	情報伝達・共有

[http://www.ipa.go.jp/security/cloud/cloud\\_sinsai\\_R1.html](http://www.ipa.go.jp/security/cloud/cloud_sinsai_R1.html)



# 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

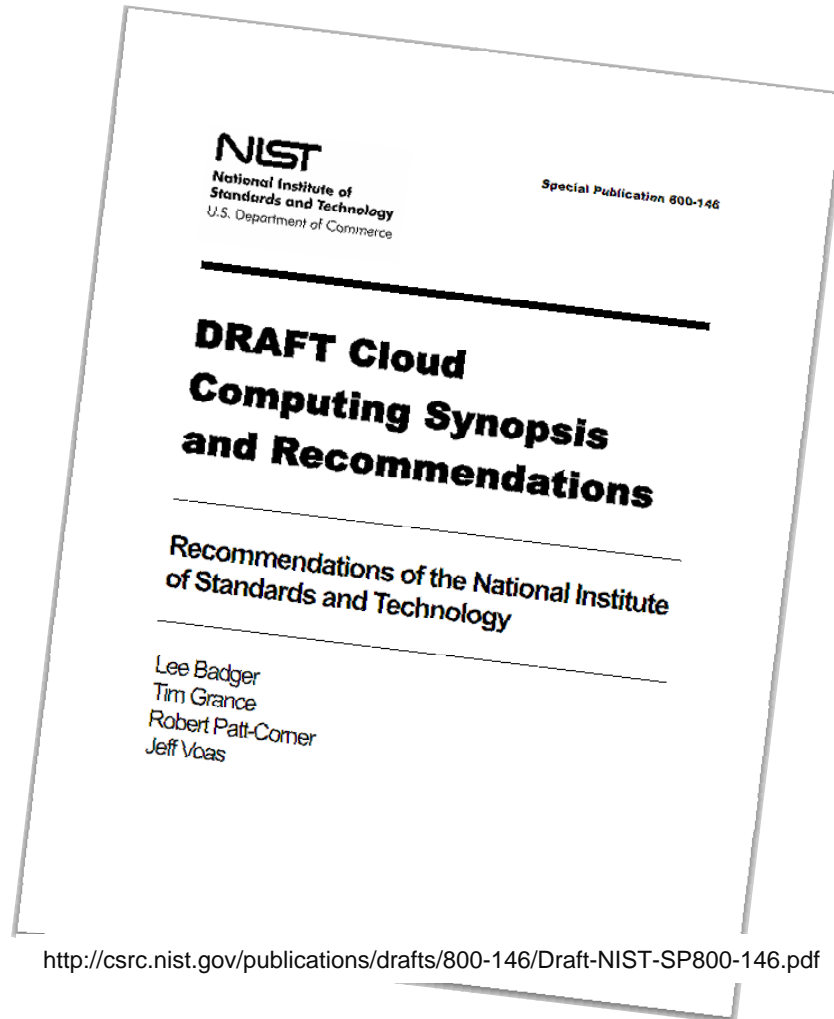
# クラウドコンピューティングって 安全ですか？

# クラウドコンピューティングに関する不安



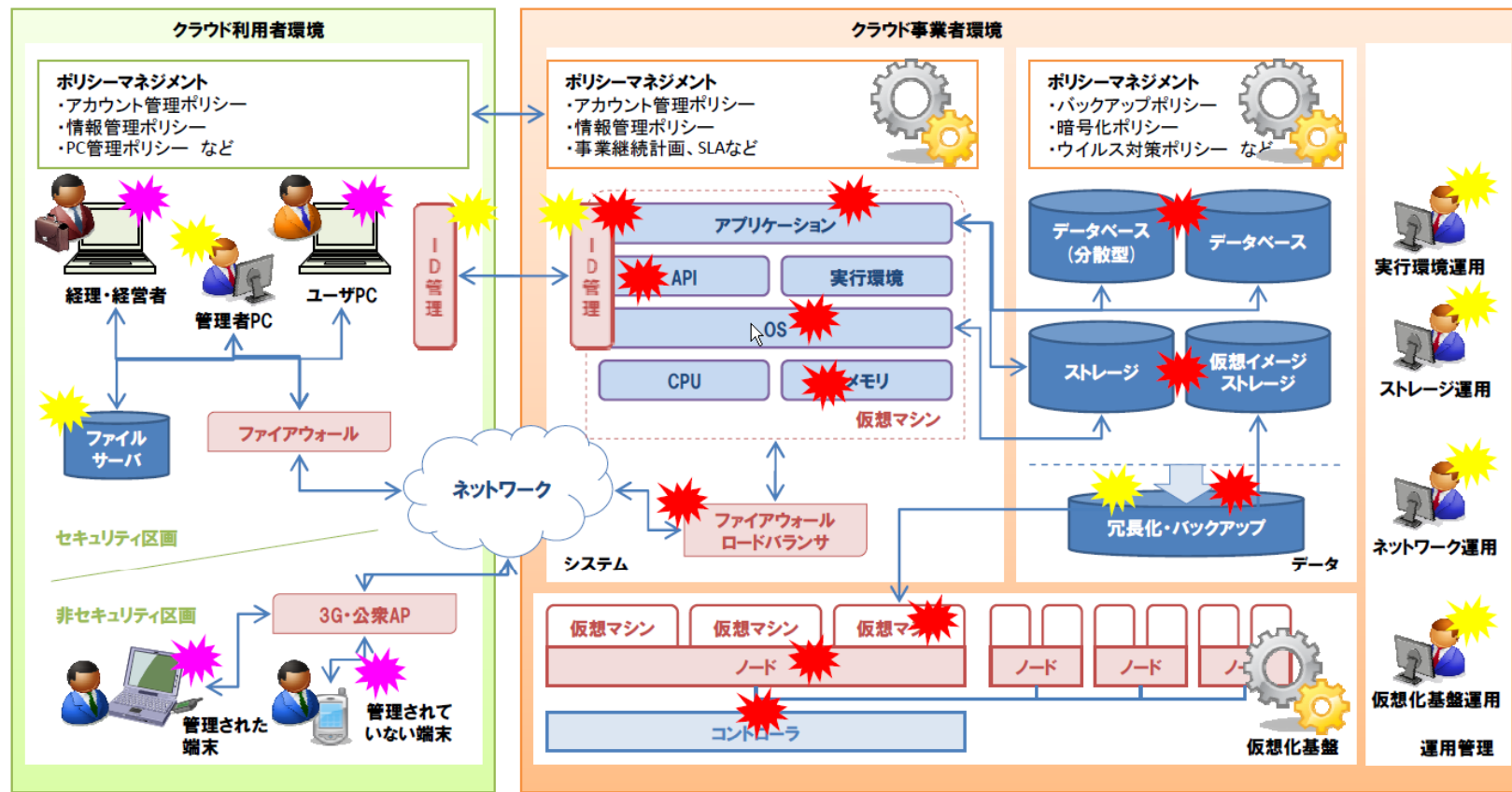
- クラウドに関する様々な不安は以下の3つに分けることができる
  - クラウドのシステム(インフラ)に関するもの
    - 仮想化、分散処理、ネットワーク、端末など
  - クラウドのサービスに関するもの
    - 事業継続、コスト、サービス事業者(組織、社員)など
  - メンタル的なもの
    - 新しいものに対する不安、わからないものに対する不安
- クラウド以前にできてないことは、クラウド以降もできない
  - クラウドになったからといって何でもできるようになるわけではない
  - クラウドに関して正しい情報を入手することがまだまだ難しい

# クラウドコンピューティングとは？



- NIST 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



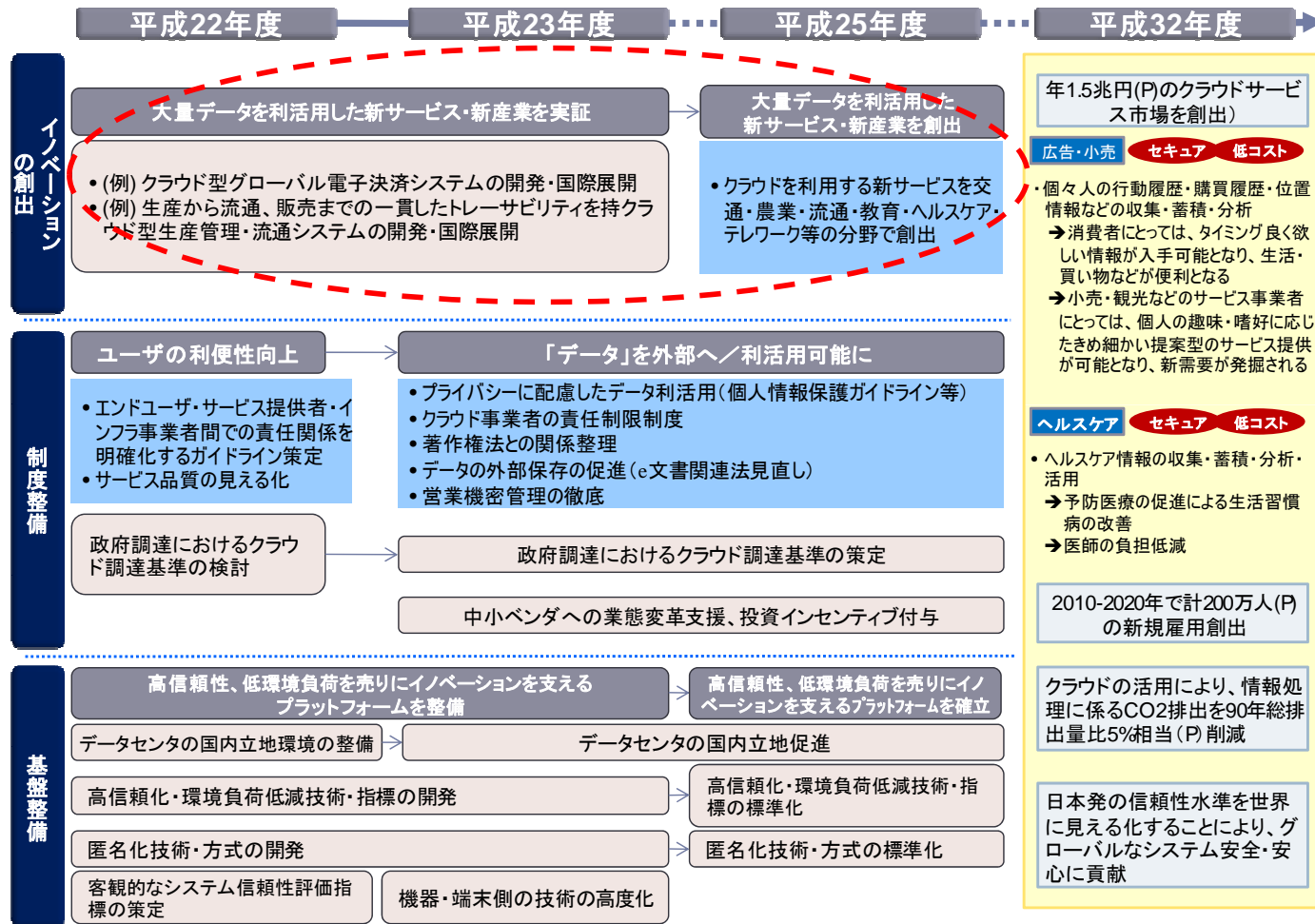
# リスクマネジメントの基本は崩さずに



- 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



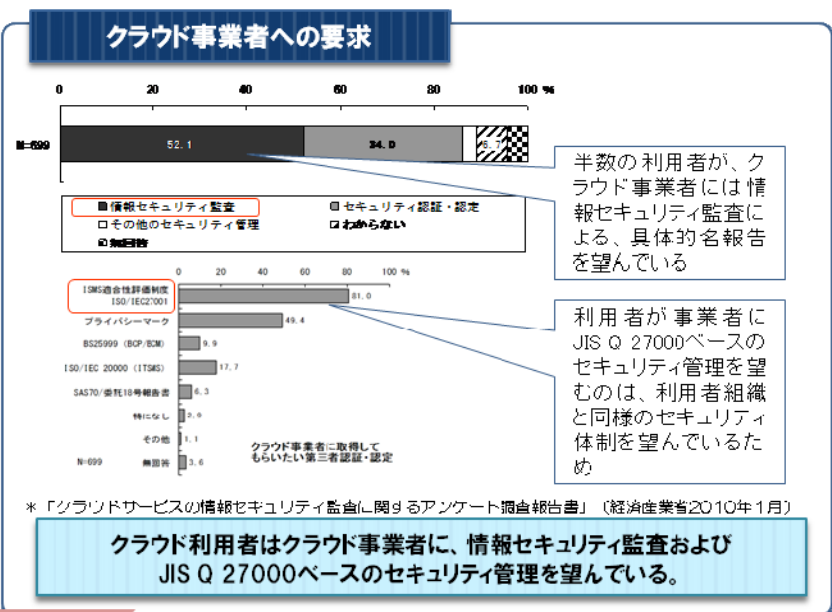
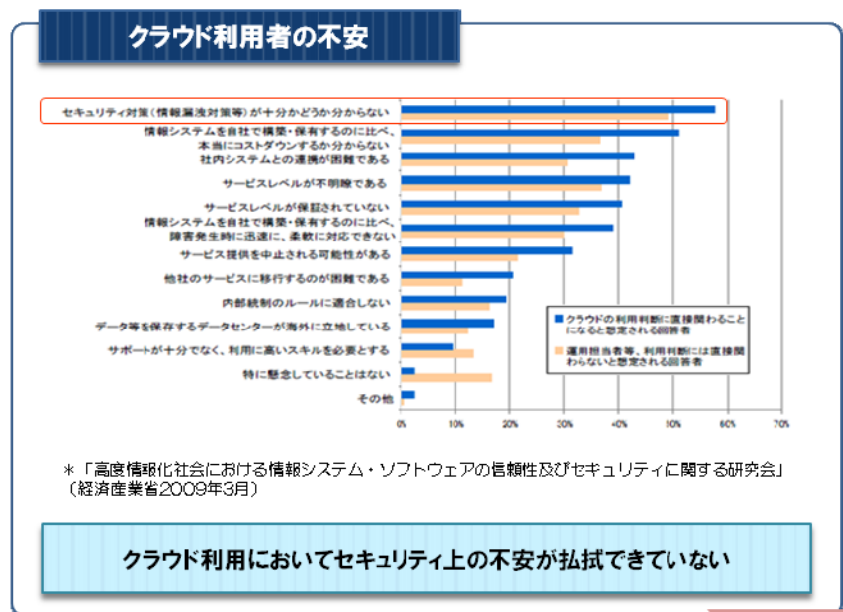
経済産業省資料より抜粋

---

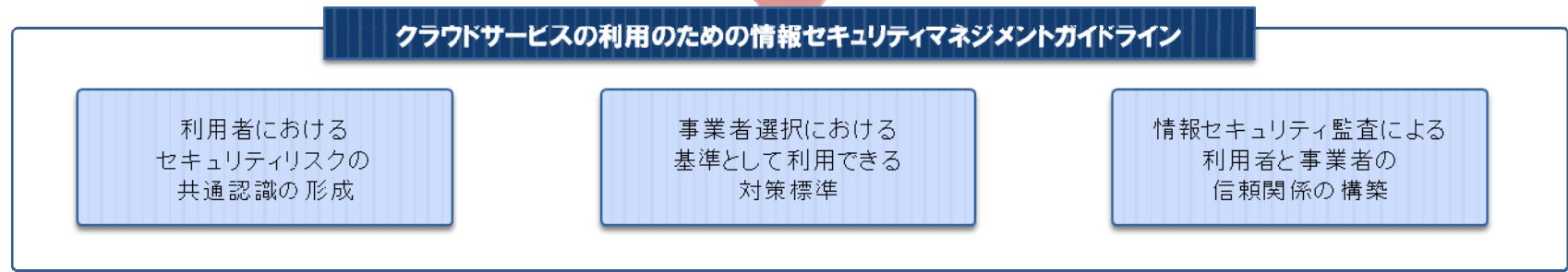
標準化のためのベースと考え方

# 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



「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



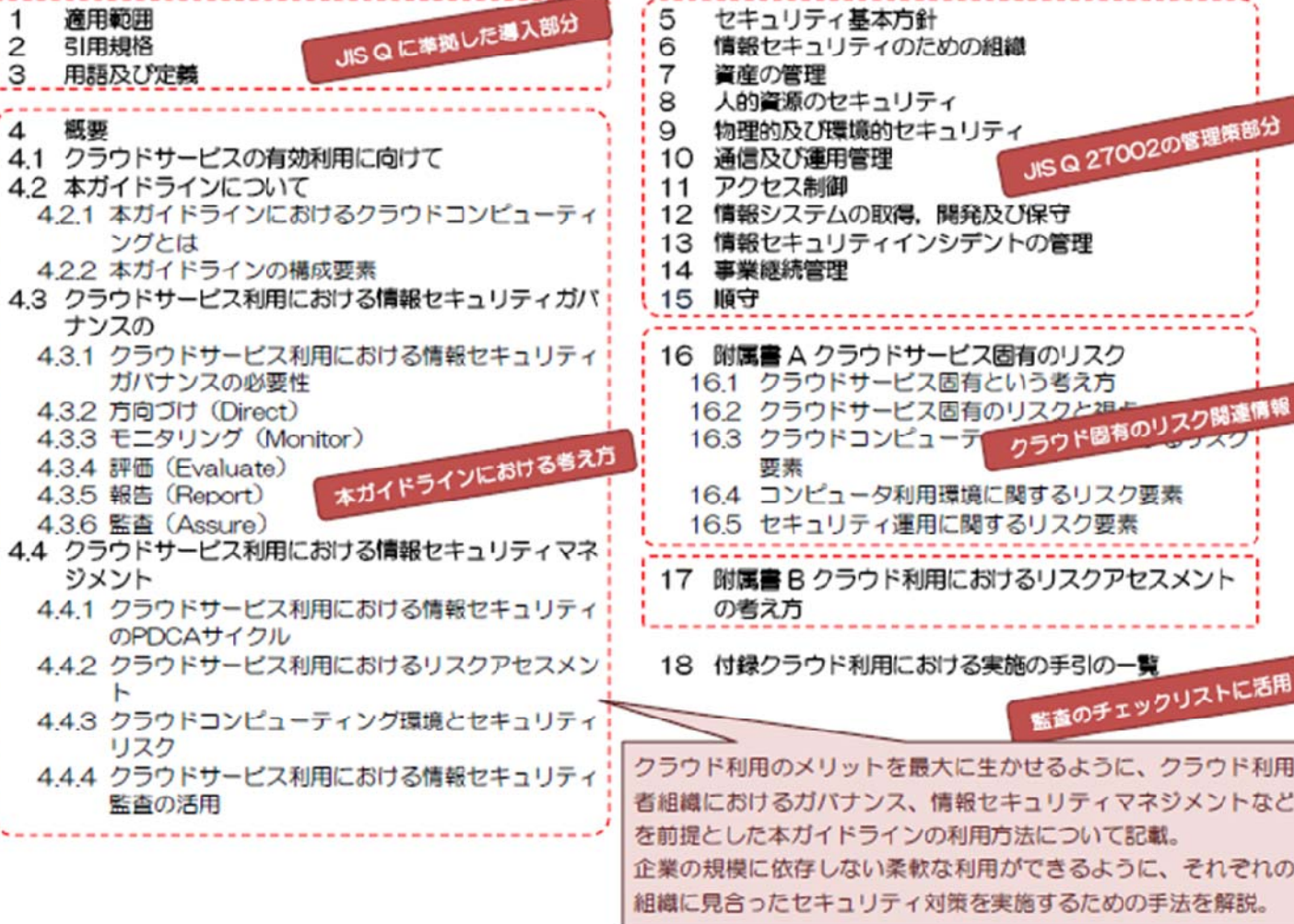
# クラウドサービス利用のための 情報セキュリティマネジメントガイドライン



## • 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、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

**10.5 バックアップ**  
 情報及び情報処理設備の完全性及び可用性を維持するため、...

データのバックアップ取得と時機を失しないデータ復旧の訓練とに関する、合意されたバックアップ方針及び戦略を実施するために、日常の作業手順を確立する...

**10.5.1 情報のバックアップ**  
**管理策**  
 情報及びソフトウェアのバックアップは、合意されたバックアップ方針に従って定期的に取得し、検査することが望ましい。...

**クラウド利用者のための実施の手引**  
 クラウド利用者は、クラウドサービスの環境において、バックアップ作業を実施しなければならない資産を確認し、合意されたバックアップ方針に従って定期的にバックアップを取得し、検査することが望ましい。クラウド利用者は、クラウドサービスの環境において、クラウド利用者がバックアップ作業を実施しなくてもよい資産を確認し、クラウド事業者が、合意したバックアップ方針に従って定期的にバックアップを取得し、検査していることを確認することが望ましい。...

**クラウド事業者のための実施の手引**  
 クラウド事業者は、クラウドサービスの環境において、バックアップ作業を実施しなければならない資産を確認することが望ましい。クラウド事業者は、クラウドサービスの環境において、クラウド事業者がバックアップ作業を実施する資産を確認することが望ましい。クラウド事業者は、クラウドサービスの環境において、クラウド利用者がバックアップ作業を実施しなければならない資産を、クラウドサービスの利用を検討する者に明示することが望ましい。...

**クラウドサービスの関連情報**  
 クラウド事業者は、データバックアップ設計において、重要なデータを含むデータをバックアップした際に、重要データなデータを含めてバックアップ取得に留意することが望ましい。...

注) クラウド固有の事項がない場合は、それぞれの項目は記載していない

**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。

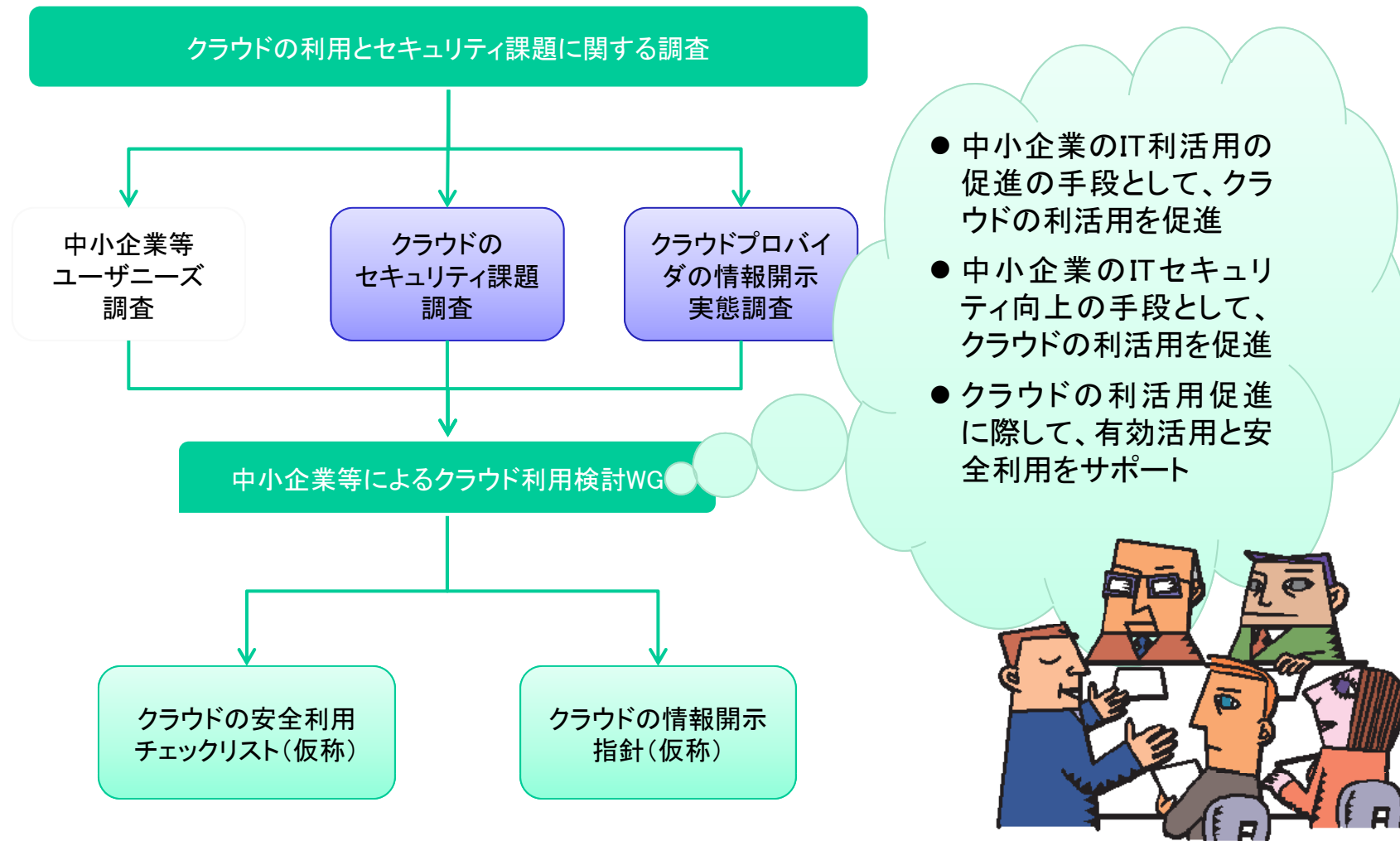
**クラウドサービスの関連情報**

- 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





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](mailto: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別は成り立たない
  - 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