Open Stack Days Tokyo 2016
S-7

クラウド特化のセキュリティ評価制度の紹介

2016年7月7日

NTTソフトウェア株式会社
クラウド＆セキュリティ事業部
https://www.ntts.co.jp/

NTTソフトウェア

講師略歴と協議会活動

中田　美佐
NTTソフトウェア株式会社
クラウド＆セキュリティ事業部

ISO/IEC 27001等に基づくセキュリティコンコンサルティングや、個人情報保護法・JIS Q 15001に基づく個人情報/パーソナルデータ保護のコンサルティングを提供。
所属組織でクラウド向け開発等を行なっていることから、クラウドセキュリティに関する協議会活動にも参加。

JASA-クラウドセキュリティ推進協議会における活動

監査手続WG、調査WGに参加し、クラウド情報セキュリティ監査制度の初期段階から、制度の構築活動を行なう。その基準となる「情報セキュリティ管理基準」「クラウド情報セキュリティ管理基準」の改正作業にも参加。

■ **特定非営利活動法人　日本セキュリティ監査協会（JASA）**

JASA-クラウドセキュリティ推進協議会
http://jcispa.jasa.jp/

活動内容

質の高い情報セキュリティ監査を通じて、クラウドコンピューティングにおける情報セキュリティに対する懸念を払拭し、わが国でのクラウドコンピューティングの一層の利用を促進するために活動する協議会。日本の有力クラウド事業者、監査法人、セキュリティ有識者らが参加。
経済産業省の委託を受けて、「情報セキュリティ管理基準」をクラウドに適用した「クラウド情報セキュリティ管理基準」の公開や、本基準に基づくクラウド情報セキュリティ監査制度を設立を行なう。今後は国際的な基準化、制度化を目指して運営。

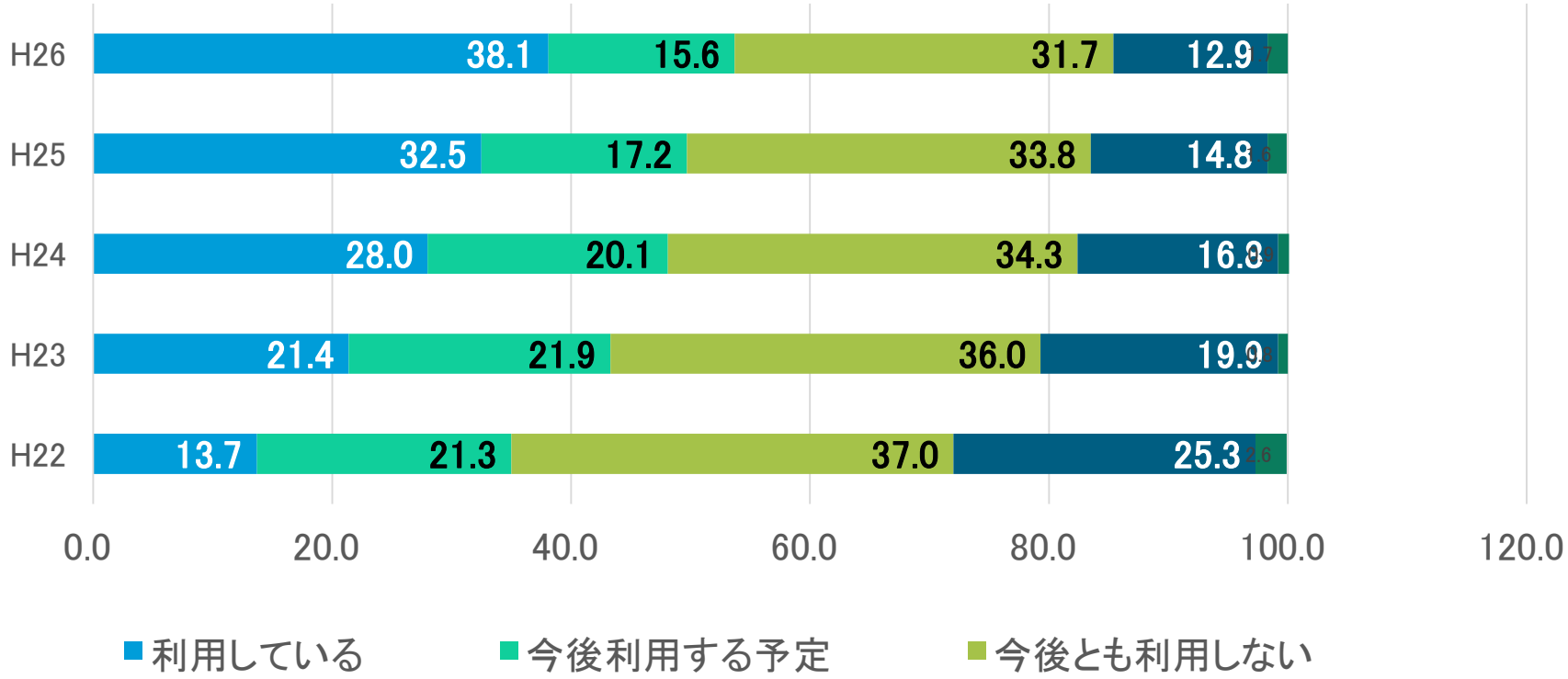
本資料の扱いについて

■本資料の一部は、 JASAの許可を得て、JASA-クラウドセキュリティ推進協議会において、作成された資料を使用しています。
（該当スライドには、  を挿入）

目次

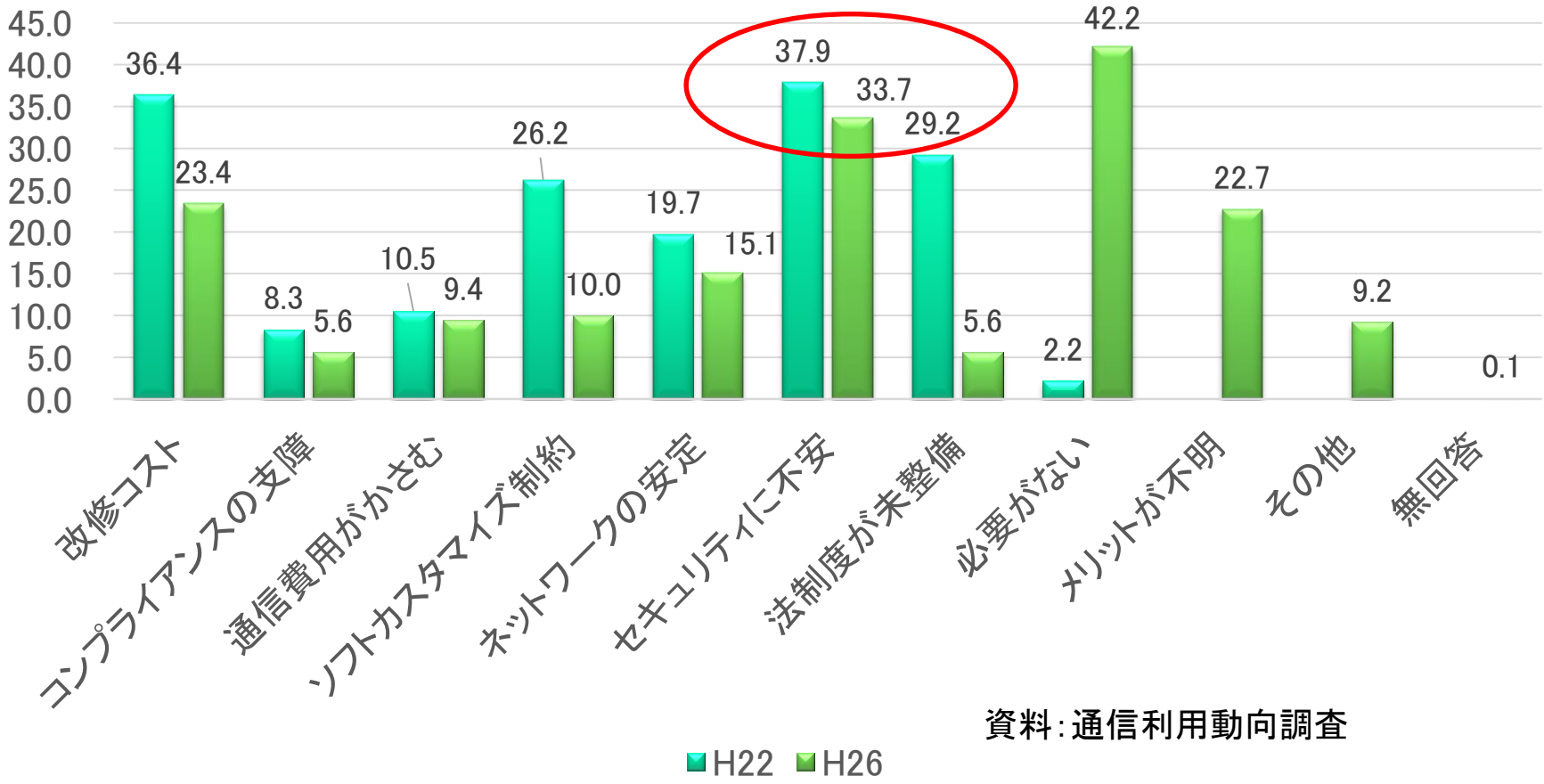
１．はじめに

クラウドサービスの利用動向



資料：通信利用動向調査

クラウドサービスの利用阻害要因



資料：通信利用動向調査

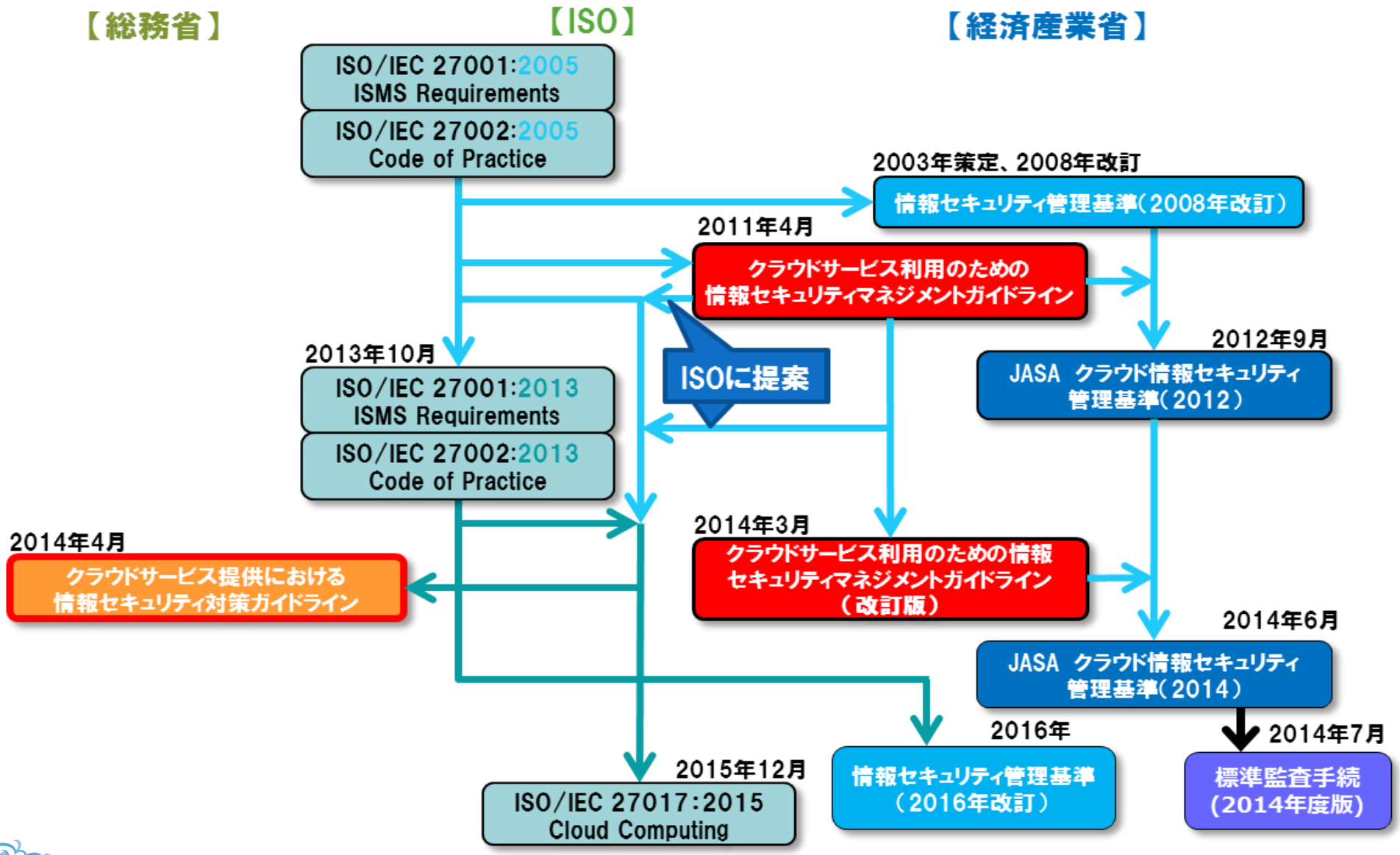
クラウドサービスのセキュリティ検討

- 明確な基準、規格がなく、多くの業界団体等が自主ガイドライン等を検討し、公表してきました

年	団体/ガイドライン	主要国	概要
2009	Open Cloud Manifesto	米	IBMやSun、Cisco、VMware、EMC、SAPなどが署名をしているマニフェスト。
2009	CSA（Cloud Security Alliance）	米 その他	米国eBayやオランダのINGを創設者とする業界団体で、クラウドセキュリティのベストプラクティスの普及活動、教育プログラムを提供するNPO団体。
2009	Jericho Forum	-	2004年1月に業界団体のThe Open Group内に設立された、企業のCISOによるコミュニティ組織。2008年頃から本組織で、クラウドの活用が検討課題となる
2009	ENISA（欧州 ネットワーク情報セキュリティ庁）	EU	2009年にクラウドコンピューティング向けガイドラインを発行 （団体としては2004年設立）

- **標準化**に向けて、日本、米国などが動き出しました

クラウドセキュリティの標準化動向



クラウドサービスのリスク

■**クラウドサービス（パブリック）は、コンピュータ資源を多くの利用者が共有し、オンデマンド、セルフサービスによる、迅速で拡張容易性の高いシステム環境を提供するサービスです。**

■**クラウドサービスのリスクは、他者にシステムの主要な部分を委ねることから発生します。**

- ▸システムの状態をリアルタイムに把握しにくい
- ▸障害の原因が分からないことがある
- ▸説明責任が果たせないか懸念がある

クラウドサービス

オンプレミス

見えない/分らないからこその利用者の不安

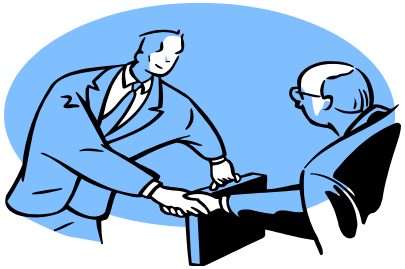
何故、クラウド特化のセキュリティ評価が必要なのか

■クラウドサービスに対する利用者の懸念
（他者にシステムの主要な部分を委ねているのに、）

- システムの状態をリアルタイムに把握しにくい
- 障害の原因が分からない
- 説明責任が果たせない

■クラウドサービスに関わるセキュリティ情報伝達の課題

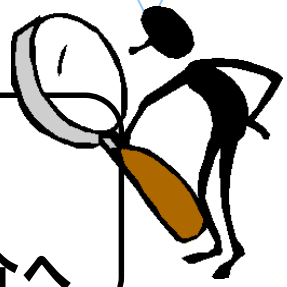
- 利用者には、セキュリティ対策を理解するための基礎知識が必要となる
- クラウド事業者が、多数の利用者に個別に説明することが難しい



クラウドサービス

■必要な「利用者代表の目で確認して、結果を知らせてくれる」仕組みの必要性

- 専門的な知識（クラウド固有のリスクや管理策）
- 公正で的確な評価



クラウド特化のセキュリティ評価制度

2.クラウド情報セキュリティ監査制度の紹介　へ

3. ISO/IEC 27017に基づくISMSクラウドセキュリティ認証の紹介へ

2．クラウド情報セキュリティ監査制度の紹介

クラウドサービスに対する監査の必要性

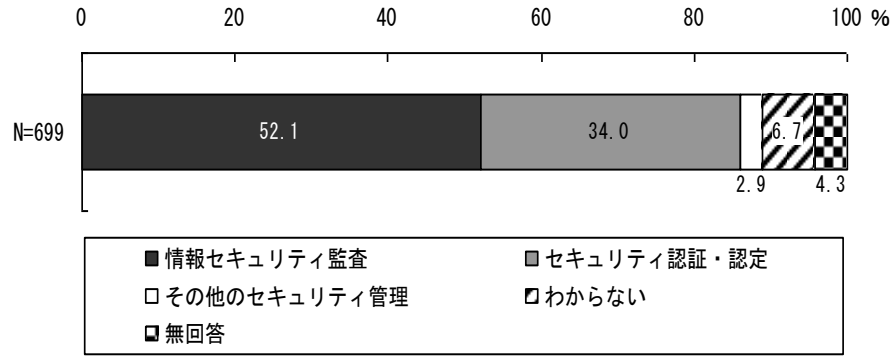
■ 必要な「利用者代表の目で確認して、結果を知らせてくれる」仕組みの必要性

- ▸専門的な知識（クラウド固有のリスクや管理策）がわかる人に任せたい
- ▸公正で的確な評価ができる人に任せたい

■ISO/IEC 27017の要求

- ▸18.2.1　情報セキュリティの独立したレビューの要求
- ▸クラウド事業者が選択する適切で独立した監査は、一般的には、十分な透明性をもった、クラウド事業者の運用をレビューしたいとするクラウド利用者の関心を満たすに足りる手段とする。

保証型監査が必要



出典 「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）

※ ISMS適合性評価制度において認証を受けている企業、もしくはプライバシーマークを取得している企業を中心に2000社を抽出。経営陣、情報システム部門に回答を求めた。有効回答総数は699件

どのような監査が求められるか

一般にみられる内部監査

目的： 自身の対策の有効性確認

水準： 経営者が求める水準

基準： 情報セキュリティ一般

監査人：経営者の期待に応える評価能力

クラウドに必要な監査

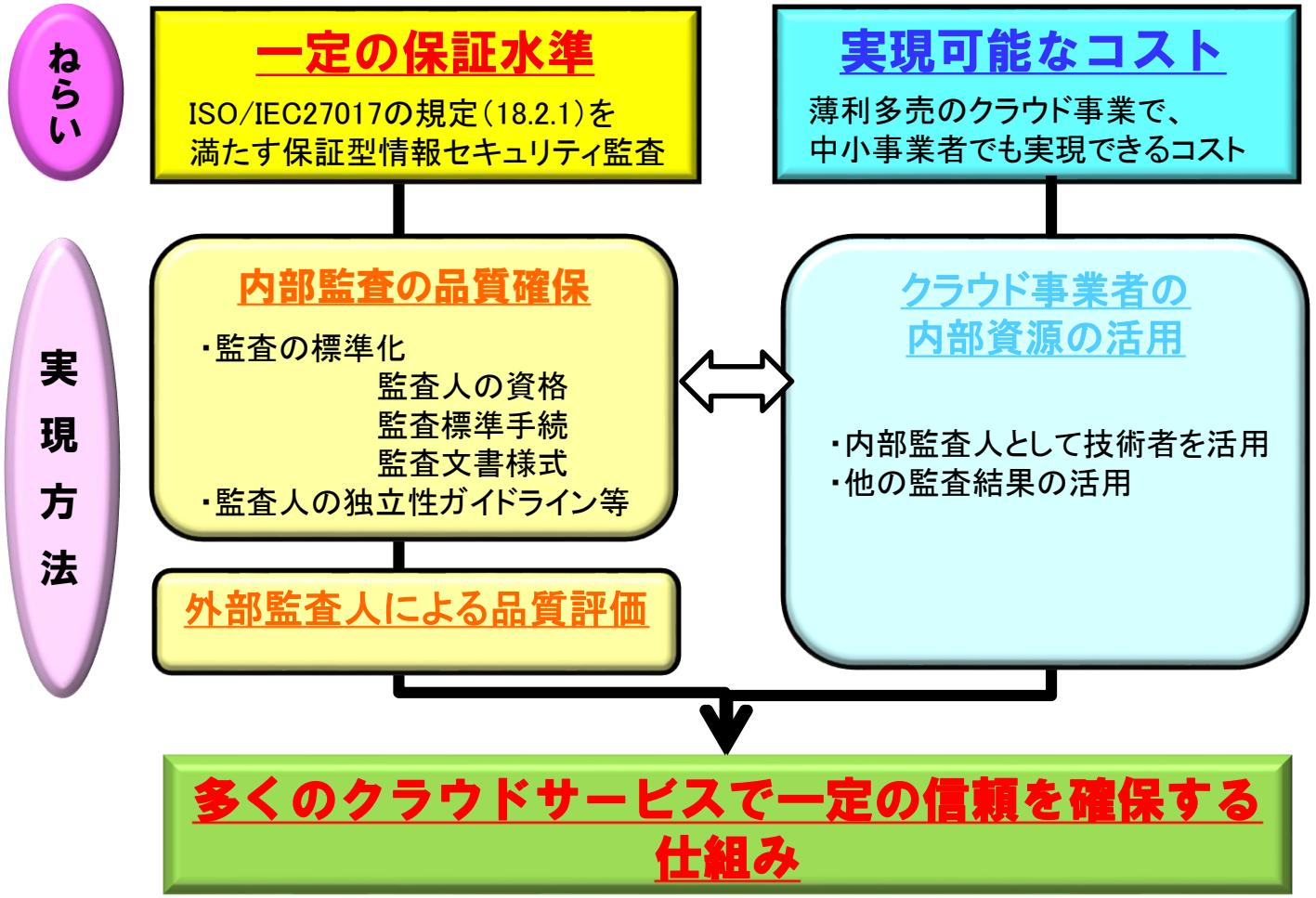
目的： **提供する環境**での
対策の有効性確認

水準： **利用者**が求める水準
・公正さ
・クラウドの知識

基準： **クラウドに特化した**
情報セキュリティ基準
・事業者責任のセキュリティ対策
・利用者への支援
（情報・機能の提供）

監査人：客観的に評価された能力

クラウド情報セキュリティ監査のコンセプト



- SOC等に代表される保証型監査は、費用が高く、実施が容易でない場合が多いです。これを解消しつつ、品質を確保した監査を行なうことを目的にした制度です。

クラウド情報セキュリティ監査制度の特徴

■情報セキュリティ監査制度をクラウドサービスに適用

- ▸情報セキュリティ監査基準を適用
  - – このため、公認情報セキュリティ監査人資格認定制度に基づく監査人を育成（対象は、クラウドサービスに関わる情報セキュリティ技術者）
  - – 内部監査の公正さを確保するために、監査人の独立性ガイドラインを導入し、会員に遵守を求める
- ▸情報セキュリティ管理基準に基づく業態別基準として、クラウド情報セキュリティ管理基準を作成

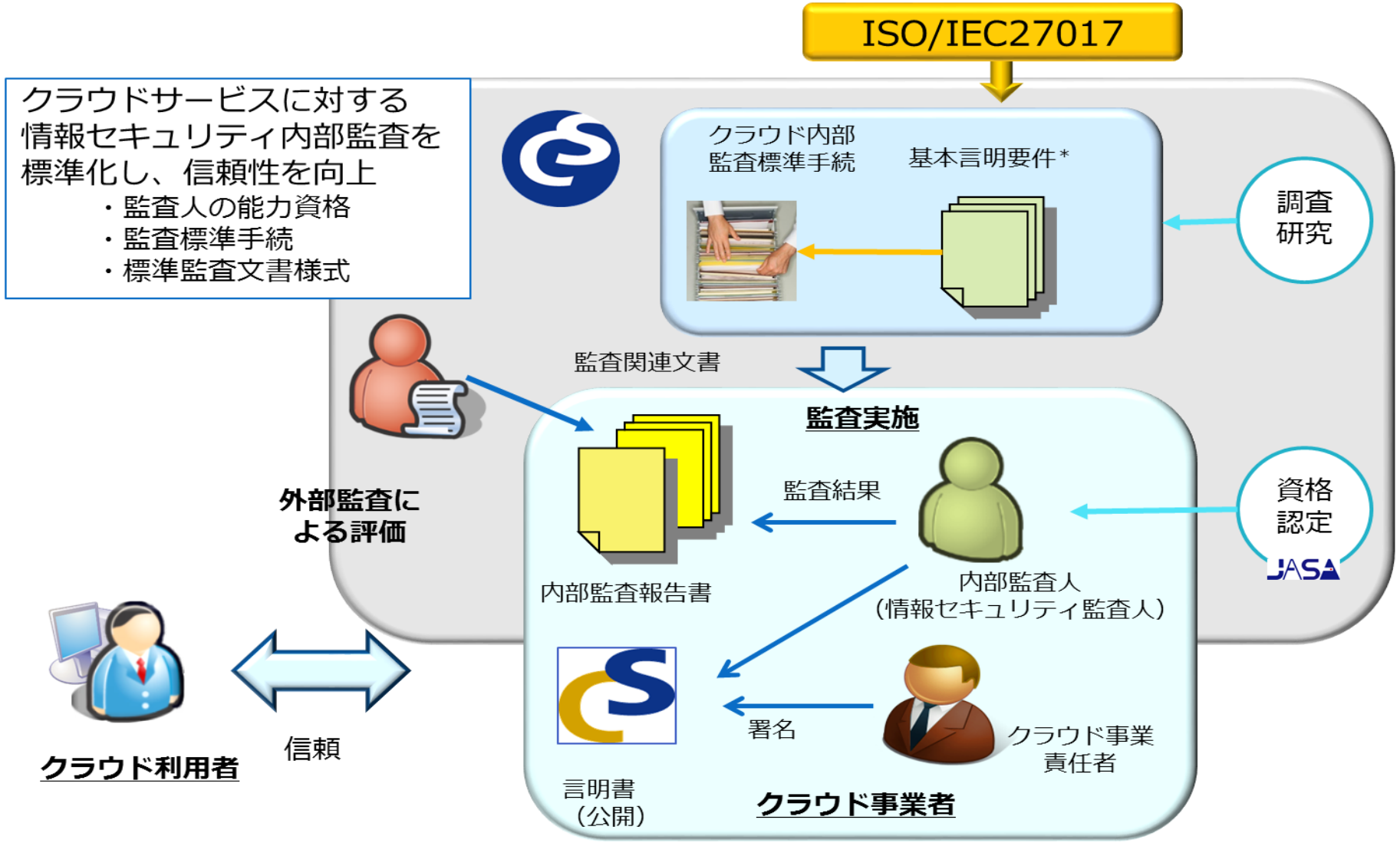
■内部監査を標準化することにより透明性を確保

- ▸事業者として最低限守るべき基本リスク対策と、そのための基本言明要件を定める
- ▸経営者に基本言明を求め、これを監査することで情報セキュリティ対策の有効性を確認。利用者の安心につなげる
- ▸監査標準手続を定め、これに準拠することで内部監査の透明性を確保
- ▸監査関連文書の標準様式を定め、外部チェックの容易さを確保

■外部監査人による内部監査の評価を通じ間接的に保証（ゴールドマーク）

- ▸保証は協議会として行う
- ▸外部監査人評価を行わない場合も、自主申告でシルバーマークとして公開

クラウド情報セキュリティ監査のしくみ



クラウド情報セキュリティ監査制度の効果

■事業者の負担が大幅に軽減

- ▸既往の監査等の情報を活用できるため、監査手続を大幅に削減
- ▸事業者の事情に合わせた柔軟なスケジュールによる社内リソースの活用

■ISO/IEC27017認証の監査に関する要件をクリア

- ▸ISO/IEC27017がクラウド事業者に求めるISMSの内部監査の要件を満たす
  （CSゴールドマーク、CSシルバーマーク共に）

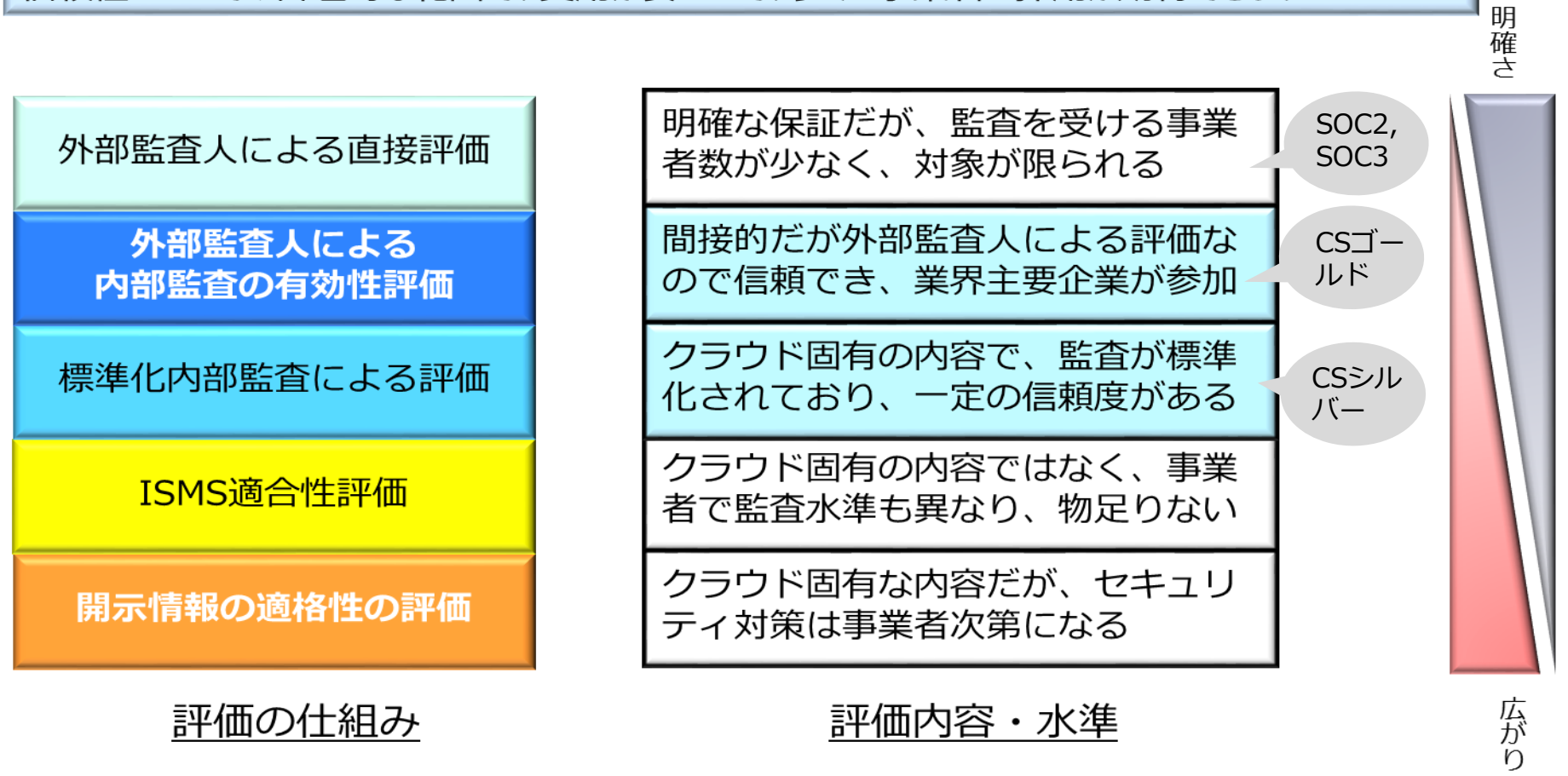
■サービスを対象とした情報セキュリティの信頼性を明示

クラウドサービスのための監査

No		名称	概要	優れた点	考慮点	主体
1	保証型監査	SOC； サービス・オーガニゼーション・コントロール	独立した組織の監査人がクラウド事業者を監査し、報告する方式	完全な公正さ	技術的評価の専門性 費用等負担の大きさ	AICPA； 米国公認会計士協会
2		CSゴールドマーク； クラウド情報セキュティ監査適合監査	事業者の内部監査人が行った監査を、外部の監査人が評価し、その結果に基づいて一定の水準にあると認める方式	技術的評価の高さ 適度な負担-時期、費用	公正さ -監査品質含む	JASA； 日本セキュリティ監査協会
参考	自己評価※	CSシルバーマーク； クラウド情報セキュティ監査自主監査	JASAが定めた標準にしたがって、事業者が行う内部監査	技術的評価の高さ 負担の軽さ -時期、費用、範囲	透明性	JASA； 日本セキュリティ監査協会

クラウド情報セキュリティ監査の位置づけ

クラウド情報セキュリティ監査制度は、クラウドの特徴に適した実用性の高い評価の仕組みです。
信頼性については合理的な範囲で、費用が安いので、多くの事業者の採用が期待できます



３．ISO/IEC 27017に基づくISMSクラウドセキュリティ認証の紹介

ISMSクラウドセキュリティ認証の背景

出展：JIPDEC「ISMSクラウドセキュリティ認証に関する説明会資料」(2015年4月26日)

クラウドサービスの本格的な普及に伴い、クラウドサービスに求められるセキュリティ要求事項を明確化することの重要性を認識。

クラウドサービス向けの国際規格 ISO/IEC 27017 (Code of practice for information security controls based on ISO/IEC 27002 for cloud services)が2015年12月15日に発行された。

このような状況を踏まえ、ISMSに基づき、クラウドサービスの信頼性を保証するISMSクラウドセキュリティ認証を開始する予定。

ISMSクラウドセキュリティ認証の枠組み　-分野別アドオン認証-　(1/2)

２０１６年夏頃、開始予定

出展：JIPDEC「ISMS適合性評価制度クラウドセキュリティ認証の方針」(2015年11月16日)

http://www.isms.jipdec.or.jp/topics/ISO27017_CLS.html

クラウドセキュリティ認証（略称：CLS認証)の枠組みは以下の方針とする。

ISMS（ISO/IEC 27001）認証を前提として、クラウドサービスの情報セキュリティ規格（ISO/IEC 27017）を満たしている組織を認証する仕組みとする。

※これをアドオン認証とよぶ。

ここでは、ISOの枠組みの中で、ISMS（ISO/IEC 27001）認証を前提として、特定の分野固有の規格に準拠していることをアドオン認証という。
（アドオン認証のイメージは、図1・図2を参照）

ISMSクラウドセキュリティ認証の枠組み　–分野別アドオン認証–　(2/2)

出展：JIPDEC「ISMS適合性評価制度クラウドセキュリティ認証の方針」(2015年11月16日)

http://www.isms.jipdec.or.jp/topics/ISO27017_CLS.html

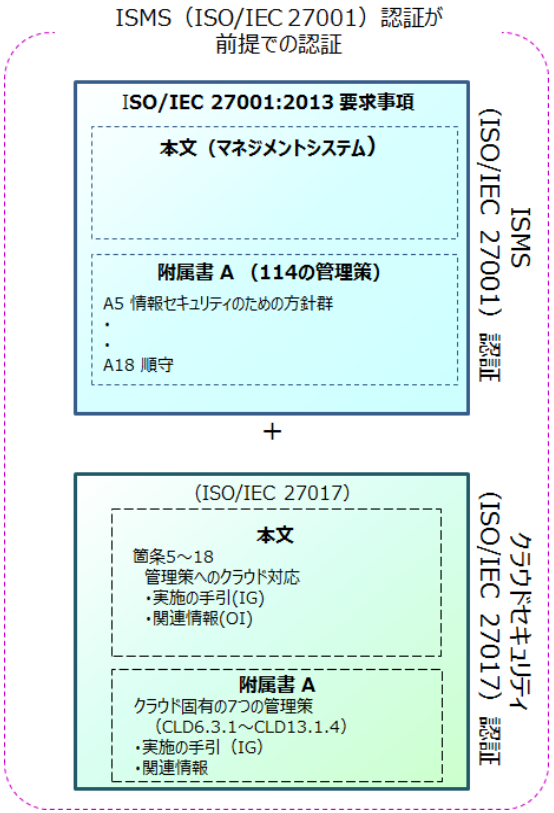


図1 ― 認証制度の枠組み

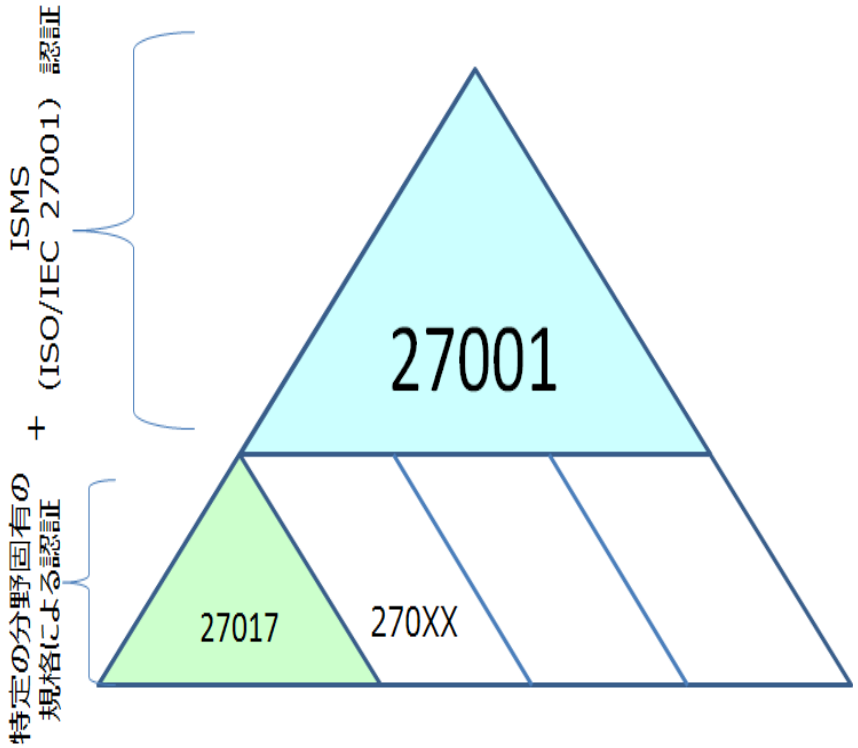


図2　アドオン認証のイメージ

従来の27001
ベースの管理策

＋

クラウド固有の
リスクを考慮した
27017ベースの
管理策

ISO/IEC 27017の概要

- **ISO/IEC 27017:2015**
  - Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services
  - 情報技術－セキュリティ技術－クラウドサービスに関するISO/IEC 27002に基づく情報技術制御の実施標準
  - 2015/12/15発行

- **ISO/IEC 27017:2015は、Cloud Service ProviderとCloud Service Customerの双方に情報セキュリティ管理策の実施要項を提供するガイドラインです。**

- **ISO/IEC 27002に定義された管理策にクラウドサービス固有の管理策を追加しています。**

- **ISO/IEC　27017を認証規格として使用する場合は、管理策の「望ましい」を「しなければならない」と読み替えます。**

ISO/IEC 27017の対象者 （1/2）

- **Cloud Service Provider （CSP） ：クラウドサービスを提供する組織、事業者**
  - IaaS,PaaS,SaaSなどあらゆる形態のクラウドサービスを含む
  - 日本語訳「クラウドサービスプロバイダ」 (クラウド情報セキュリティ管理基準では「クラウドサービス提供者」)
- **Cloud Service Customer （CSC） ：クラウドサービスを利用する組織、事業者**
  - いわゆるクラウドサービスを利用する法人などを想定
  - 日本語訳「クラウドサービスカスタマ」 (クラウド情報セキュリティ管理基準では「クラウドサービス利用者」)
  - 当該組織内の個人ユーザは、Could Service User（クラウドサービス利用者のユーザ）

（例） 他社が提供するクラウド開発環境を利用して、開発したクラウドサービスやアプリケーションを提供する事業者

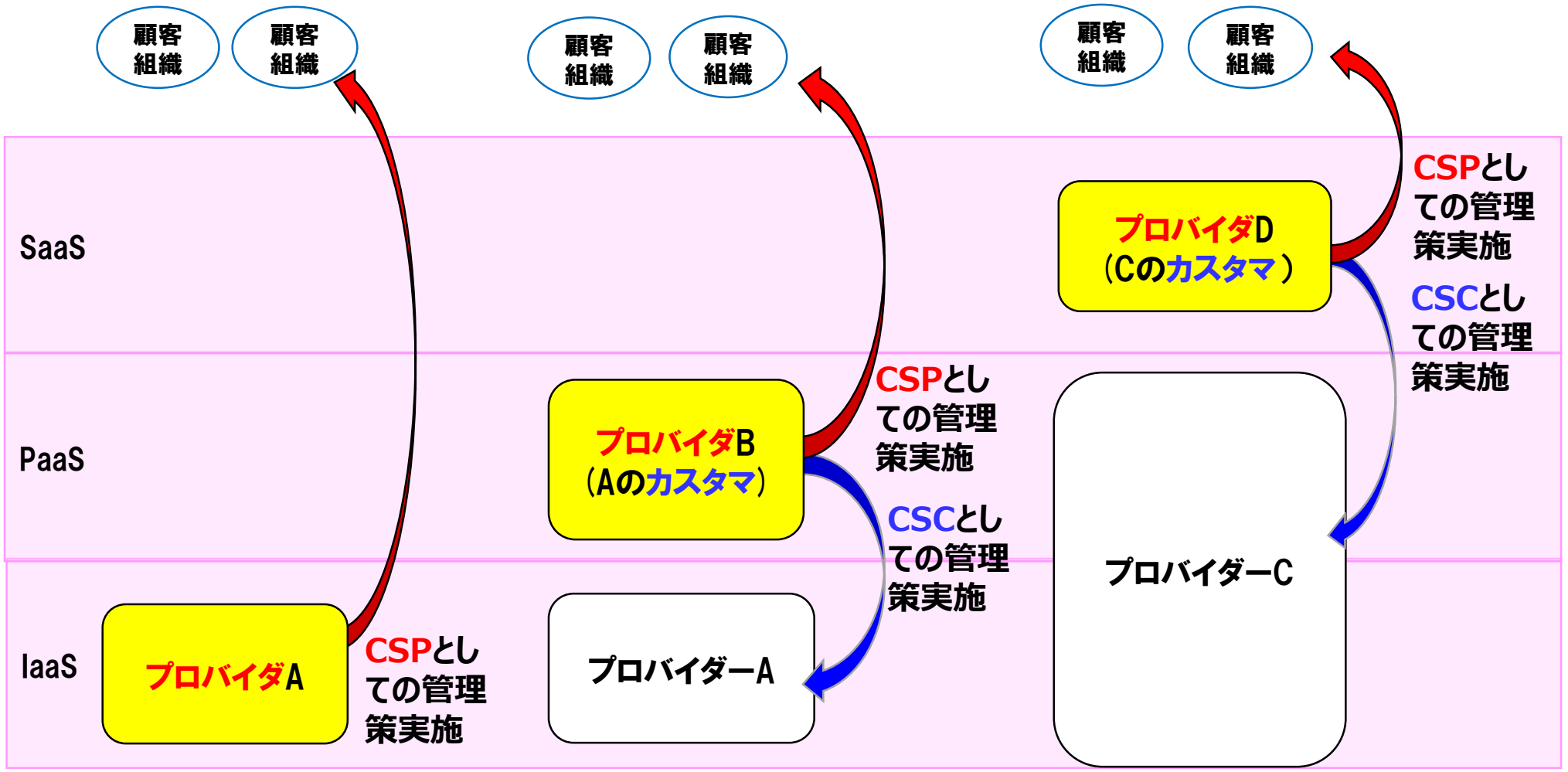
・他社が提供するクラウド開発環境を利用して、：
→CSCの立場から、安全なクラウドサービスを選定、利用し、必要な管理策を実施しているか

・開発したクラウドサービスやアプリケーションを提供
→CSPの立場から、提供するクラウドサービスやアプリケーションに適切な管理策を実施しているか

→ 当該事業者のコンシューマにセキュリティをアピール

ISO/IEC 27017の対象者 （2/2）

■様々なパターンのクラウドサービスのセキュリティを管理します



ISO/IEC 27017の構成

1．適用範囲
2．引用規格
3．定義及び略語
4．クラウド固有の概念

5～18
ISO/IEC 27002と同じ構成

- 情報セキュリティ管理目的
- 管理策

クラウドサービスプロバイダ／カスタマのための
実施の手引き
関連情報

附属書A
（規定）クラウドサービス拡張管理策集

ISO/IEC 27002には無い
クラウドサービス固有の管理策

附属書B
（参考）クラウドコンピューティングの情報セキュリティリスクに関する参考文献

備考 ISO/IEC 27017とクラウド情報セキュリティ監査制度の関係

■ ISO/IEC 27017 18.2.1 情報セキュリティの独立したレビュー の要求

18.2.1 情報セキュリティの独立したレビュー（ISO/IEC 27002管理策タイトル）

管理策(ISO/IEC 27002管理策内容)
情報セキュリティ及びその実施の管理（例えば，情報セキュリティのための管理目的，管理策，方針，プロセス，手順）に対する組織の取組みについて，あらかじめ定めた間隔で，又は重大な変化が生じた場合に，独立したレビューを実施しなければならない。

クラウドサービスのための実施の手引

クラウドサービスカスタマ	クラウドサービスプロバイダ
・・・	・・・クラウドサービプロバイダが選択した独立した監査は，それが十分な透明性が提供されることを条件として，クラウドサービスカスタマがもつクラウドサービスプロバイダの運用に対する関心を満たすために受けいれられる方法であることが望ましい。独立した監査が実現実的でないとき，クラウドサービスプロバイダは、自己評価を行い，クラウドサービスカスタマにそのプロセス及び結果を開示することが望ましい。

← クラウド情報セキュリティ監査制度等にて対応可能

４．おわりに

クラウドセキュリティ評価制度の運用

- 既に複数の企業・サービスにて、クラウド情報セキュリティ監査の適合性監査（外部評価）を実施されています
- ISMSクラウドセキュリティ認証も開始されれば、何らかのクラウドセキュリティ評価に対応しようというクラウド事業者は、更に増えることでしょう

CSゴールドマーク付与企業

No	会員企業名	サービス名	
1	日本マイクロソフト株式会社	Microsoft Azure	PaaS型
2		Office 365	SaaS型
3	東日本電信電話株式会社	フレッツ・あずけ～る、フレッツ・あずけ～るPROプラン	IaaS型
4		Bizひかりクラウド 安心サーバーホスティング	IaaS型

出展： JASA-クラウド情報セキュリティ協議会 CSゴールドマーク取得企業
http://jcispa.jasa.jp/cs_mark_co/cs_gold_mark_co/

クラウドセキュリティの検証

- 自身の開発・提供するクラウドサービスのセキュリティ
- 自身が利用するクラウド環境／サービスのセキュリティ

を検証するために、
各クラウドセキュリティに関する基準・規格、及び評価制度を活用されることを
お勧めいたします。

備考　政府機関向けクラウドサービスの対策に有効

■平成28年度版「政府機関等の情報セキュリティ対策のための統一基準群」の改定（案）にて、クラウドサービスの情報セキュリティ監査、認定・認証制度として、紹介されています。

出展：「「政府機関等の情報セキュリティ対策のための統一基準群」の改定（案）に関する意見の募集」 内閣サイバーセキュリティセンター　政府機関総合対策グループ　平成28年6月13日

「政府機関の情報セキュリティ対策のための統一基準（平成28年度版）（案）」
4.1.4　クラウドサービスの利用
遵守事項
(1) クラウドサービスの利用における対策
(e) 情報システムセキュリティ責任者は、クラウドサービスに対する情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、クラウドサービス及び当該サービスの委託先の信頼性が十分であることを総合的・客観的に評価し判断すること。

政府機関向けクラウドサービスに情報セキュリティ監査／評価が必要になります

「府省庁対策基準策定のためのガイドライン（案）」
遵守事項4.1.4(1)(e)「クラウドサービスに対する情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、・・・判断すること」について
・・・クラウドサービス事業者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等を利用することが考えられる。・・・・なお、参考となる認証には、ISO/IEC 27017 によるクラウドサービス分野におけるISMS 認証の国際規格があり、・・・、これらの国際規格をクラウドサービス事業者選定の際の要件として活用することも考えられる。その他、日本セキュリティ監査協会のクラウド情報セキュリティ監査やクラウドサービス事業者等のセキュリティに係る内部統制の保証報告書であるSOC 報告書（Service Organization Control Report）を活用することも考えられる.

本資３．ISO/IEC 27017に基づくISMSクラウドセキュリティ認証

本資2．クラウド情報セキュリティ監査制度

参考団体・サイト等

- **特定非営利活動法人　日本セキュリティ監査協会　(JASA)**
  JASA-クラウドセキュリティ推進協議会　　http://jcispa.jasa.jp/
  - ▸公開資料　http://jcispa.jasa.jp/documents/
    - ・クラウド情報セキュリティ管理基準
    - ・エンタープライズクラウド選定ガイド クラウド選びで困ったら　～要求仕様作成と提案書評価のための基礎知識～
    - 等

- **一般財団法人　日本情報経済社会推進協会(JIPDEC)**
  http://www.jipdec.or.jp/
  - ▸ISO/IEC 27017に基づくクラウドセキュリティ認証開始のお知らせ
    http://www.isms.jipdec.or.jp/topics/ISO27017_CLS.html

- **経済産業省　情報セキュリティ政策**
  http://www.meti.go.jp/policy/netsecurity/

- **内閣サイバーセキュリティセンター(NISC)**
  http://www.nisc.go.jp/index.html

ご清聴ありがとうございました。