情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

(ISC)2 Asia-Pacific 2013 受賞者講演

情報セキュリティのガバナンスと監査
-情報セキュリティの透明性・説明責任を高める-

原田　要之助
情報セキュリティ大学院大学教授

2013年9月30日

目次

- ISLAの背景
- クラウドのリスク（情報セキュリティ）への不信
- 情報セキュリティに関する様々な制度について
- 情報セキュリティの透明性と説明責任、利用者と提供者の認識ギャップ
- まとめ

講師のプロフィール

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- 職歴
  - 1977年～1999年　NTT通信網総合研究所
  - 1999年～2009年　情報通信総合研究所の主席研究員
  - 2010年4月より　情報セキュリティ大学院大学教授
- 教育・研修
  - 2005年より　2010年　大阪大学工学部大学院研究科　特任教授（組織のリスクマネジメント担当）
  - 2010年　明治大学商学部兼任講師
  - 2011年　中央大学工学部大学院兼任講師、サイバー大学兼任講師、フェリス女学院大学講師
- 資格
  - CISA(Certified Information Systems Auditor), CISM (Certified Information Security Manager) ,CGEIT（Certified Enterprise Governance of IT）
  - 公認情報セキュリティ主席監査人、公認情報セキュリティ主任監査人
  - 技術士（情報数理）、情報処理技術者（特種、システム監査）、情報処理技術者試験委員
- 委員など
  - ISACA国際本部副会長（2008-2010)、ISACA東京支部元会長(2001～2003)、ISO/IEC SC27国内委員、ISO/IEC WG8の国内幹事、IT Auditのeditor（2011年より）、
  - OPCWの情報セキュリティ監査チームリーダ（2000-2008）
  - 日本ITガバナンス協会理事、システム監査学会理事、JADACのPマーク審査委員会委員
- 学会など
  - JSSM学会、システム監査学会、電子情報通信学会、情報処理学会、経営情報学会、IEEE
- 出版
  - ITリスク学（共立出版），2012
  - リスク社会で勝ち抜くためのリスクマネジメント JRMS2010(JIPDEC)，2010
  - CobiT実践ガイドブック（日経BP），2008
  - 経営革新と情報セキュリティ（日科技連），2011

ISLAの背景

ISLAの背景

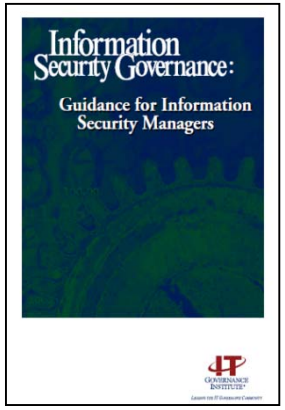
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

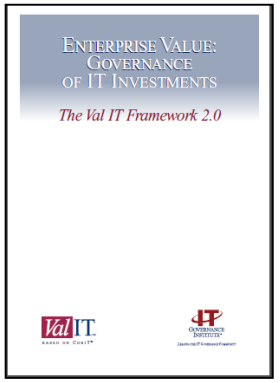
- 監査関係
  - ISACA東京支部(2001-2002)会長　CISAの増加に取組む
  - ISACA国際の活動
    - 1997年　2000年問題の研究会→米国の2000年問題
    - 2006-2008年　情報セキュリティマネジメント委員会
    - 2008-2010年　国際本部副会長
    - 2008-2011年　ISO/IECSC27のISACA代表
  - OPCW(化学兵器禁止機関)
    - OPCWの情報セキュリティ監査チームリーダ
  - ISO/IEC WG8
    - ISO/IEC TR30120　IT AuditのEditor
- 日本セキュリティ監査協会の資格制度立ち上げと認定
  - 10年で1,200名

ISLAの背景

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- ガバナンス関係
  - ISACA国際の活動
    - ガバナンスの啓発と普及
      - 2006年　情報セキュリティガバナンスガイド
      - 2009年　COBIT5に向けた戦略検討
    - ITガバナンス
      - 2008年　VAL-ITフレームワーク
  - ISO/IEC WG6　ITガバナンス委員
- 情報セキュリティガバナンス制度（2011まで）
  - 情報セキュリティガバナンスガイドブック
  - IT-BCP
  - ISO/IEC27014、JIS Q.27014の標準化





クラウドのリスク（情報セキュリティ）への不信

クラウド事業者の事故
リスクは本当にマネージされているのか

- Twitterの不正アクセスによる情報漏洩 、2009年7月
- Google（非公開のドキュメントが共有）、2009年3月
- Danger（Microsoft傘下） データ消失、2009年10月
- Dropbox（パスワードなしで共有）、2011年6月
- salesforce.com（パフォーマンス問題）、2012年7月
- 富士通、館林データセンターが電源障害、2012年7月
- Amazon EC2、電源断によるサービス停止、2012年6月
- （FSのバックアップ削除と情報漏えい問題、2012年6月）
- EvernoteのIDとパスワードの漏えい問題、2013年3月

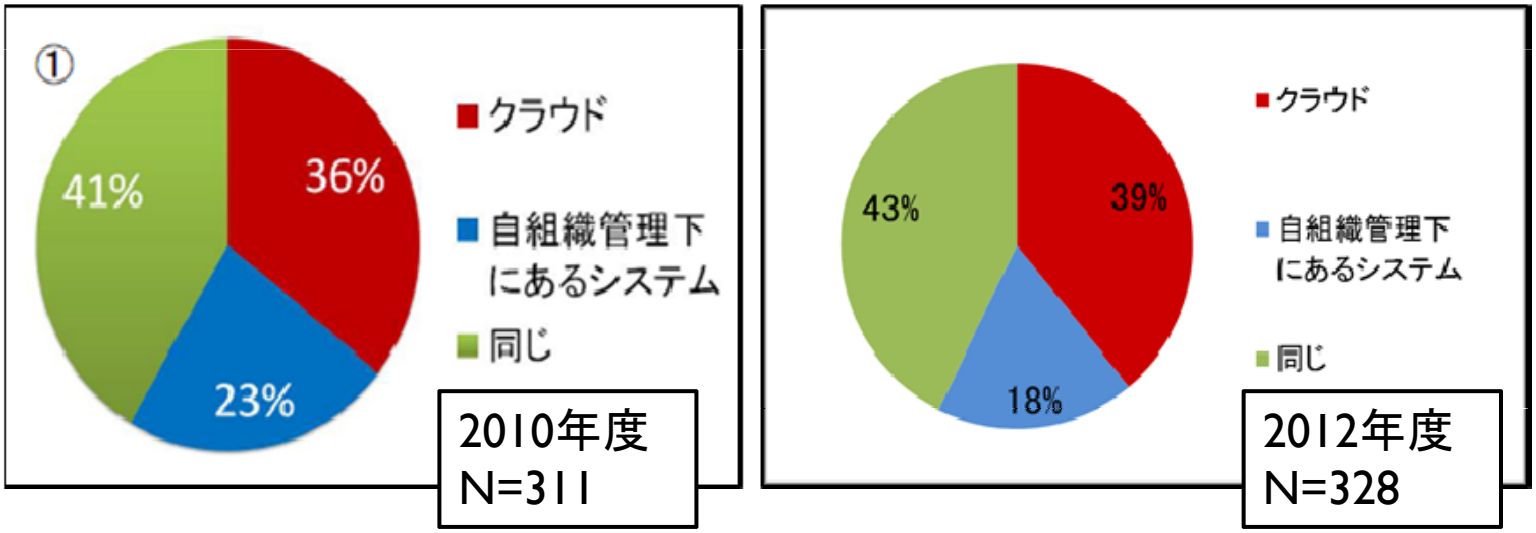
→クラウドに対する認証、監査は？？？

クラウドサービスに対するユーザの意識の現状

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

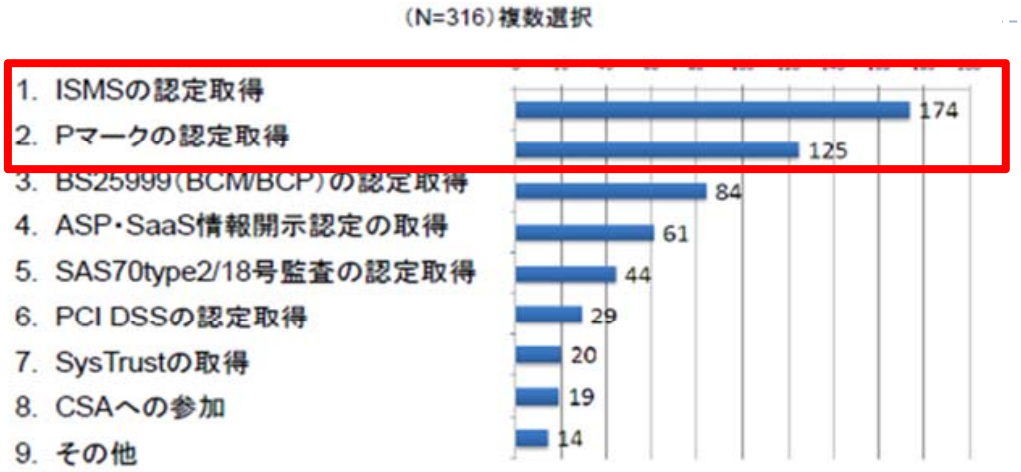
クラウド利用による運用コスト減などのメリットが注目される一方で、セキュリティへの懸念は未だに残っている。

自組織管理下とクラウドのセキュリティ上の脅威の比較



クラウドサービスと第三者認証制度

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



クラウド事業者を選定する材料として
「ISMS認証」、「Pマーク認証」取得を求めているユーザが多い

認証取得事業者(FS社)で事故発生

クラウドサービスと第三者認証制度との検討が必要

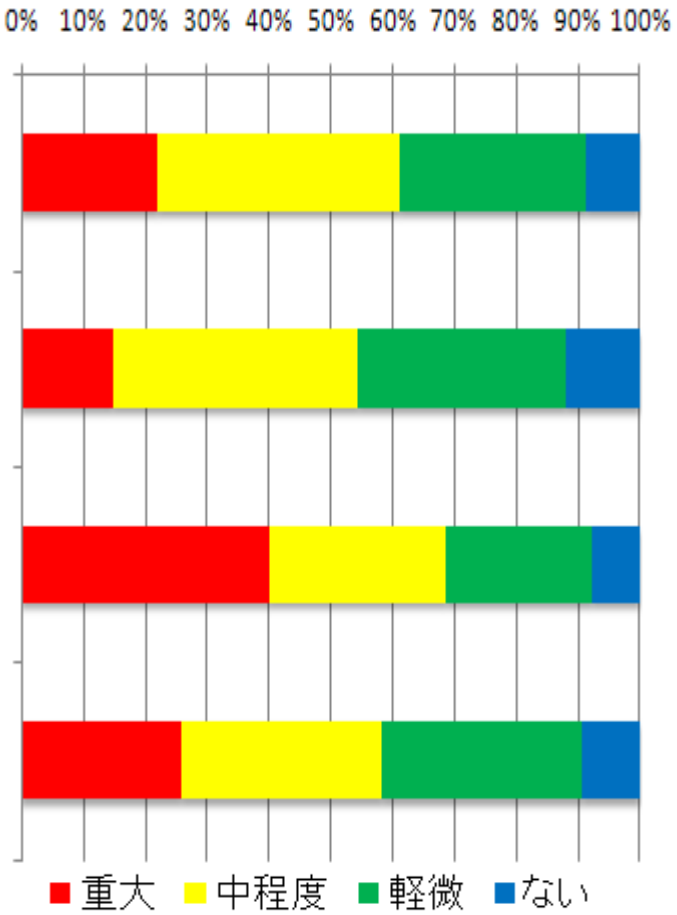
ENISAのリスク評価と日本2010年調査を振り返って②

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

技術的リスク①

リスク	ENISA
RESOURCE EXHAUSTION 事業者のリソース（サーバのCPU能力やストレージの容量）が不足して、その影響を受ける（処理速度が遅い、ファイルが保存できないなど）リスク	Medium
ISOLATION FAILURE リソースを共用する他の利用者の影響で自組織のサービス品質が低下するリスク	High
CLOUD PROVIDER MALICIOUS INSIDER - ABUSE OF HIGH PRIVILEGE ROLES 事業者の内部者によるセキュリティ違反（不正アクセスなど）で自組織の機密情報が見られその事実が分からないリスク	High
MANAGEMENT INTERFACE COMPROMISE 事業者が意図的に、自組織の機密情報を盗み見するリスク	Medium

アンケート結果



・FS事で件は、セキュリティ違反は強く感じていた通りの事件

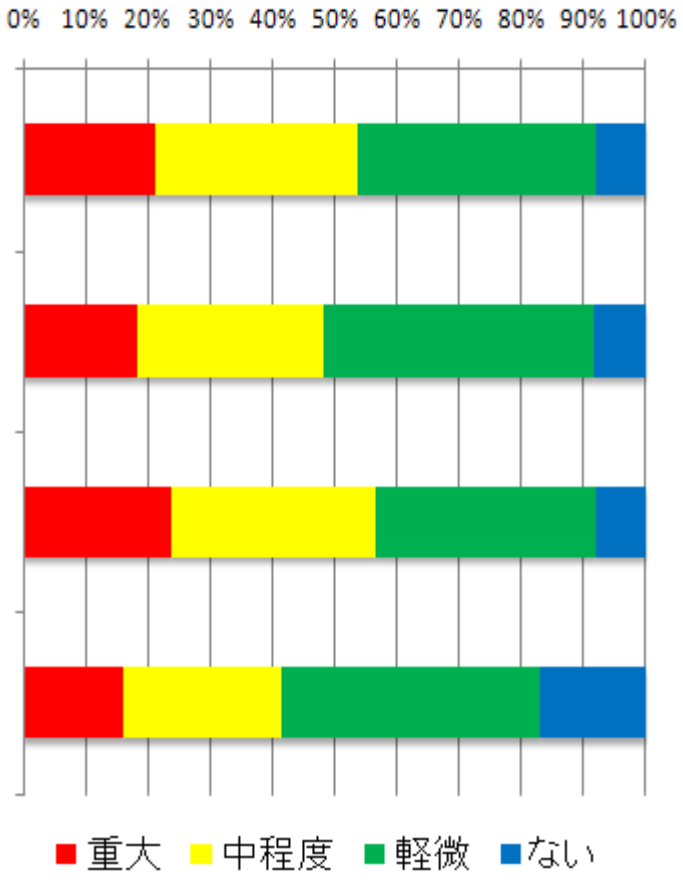
出所：原田、クラウドコンピューティングのリスクとガバナンスに関する調査・研究について、情報処理 Vol.51 No.12 Dec. 2010

ENISAのリスク評価と日本2010年調査を振り返って③

技術的リスク②

リスク	ENISA
INTERCEPTING DATA IN TRANSIT DATA LEAKAGE ON UP/DOWNLOAD, INTRA-CLOUD 事業者へのデータ転送に伴い、機密情報が漏えいするリスク	Medium
INSECURE OR INEFFECTIVE DELETION OF DATA 事業者が不要になったデータを消去しないリスク	Medium
DISTRIBUTED DENIAL OF SERVICE (DDOS) 事業者へのDDoS攻撃でサービスが中断したり品質低下するリスク	Medium
ECONOMIC DENIAL OF SERVICE (EDOS) 事業者を利用して提供している自組織のWebサービスなどへのDDoS攻撃を受けて、増えたアクセスに対する使用料を事業者に請求されるリスク	Medium

アンケート結果



・FS事件では、バックアップを戻した後、機密情報が漏えい事件が起きた

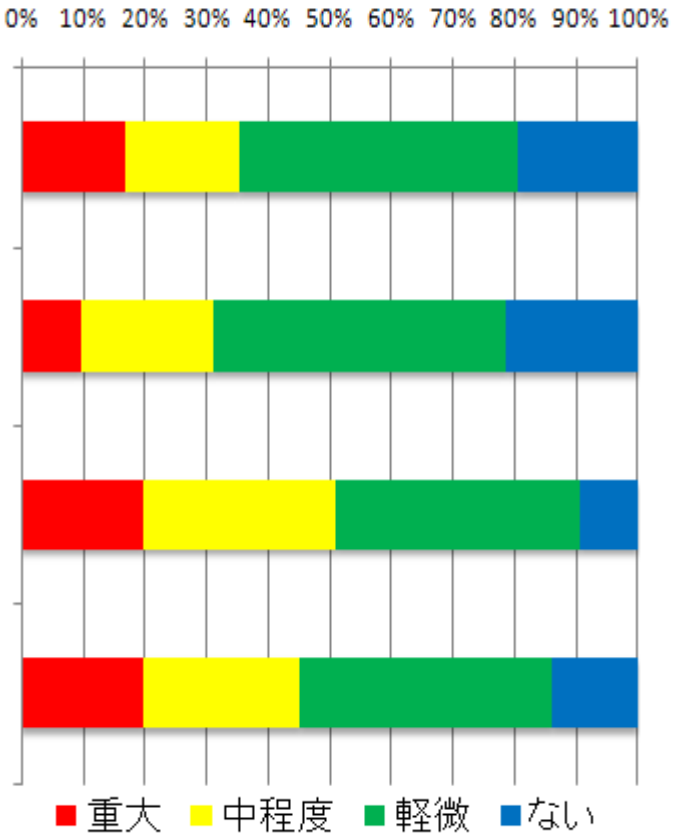
出所：原田、クラウドコンピューティングのリスクとガバナンスに関する調査・研究について、情報処理 Vol.51 No.12 Dec. 2010

ENISAのリスク評価と日本2010年調査を振り返って④

技術的リスク③

リスク	ENISA
LOSS OF ENCRYPTION KEYS 事業者が暗号かぎを紛失して復号できなくなるリスク	Medium
UNDERTAKING MALICIOUS PROBES OR SCANS 事業者が自組織にスキャン（空いているポートを探すなど）するリスク	Medium
COMPROMISE SERVICE ENGINE 事業者の提供するサービスに欠陥や問題があるリスク	Medium
CONFLICTS BETWEEN CUSTOMER HARDENING PROCEDURES AND CLOUD ENVIRONMENT 事業者の提供するセキュリティ水準が低いため、結果として自組織のセキュリティが低くなるリスク	Low

アンケート結果



・FS事件では、事業者のセキュリティ水準の問題点を気付かせてくれた

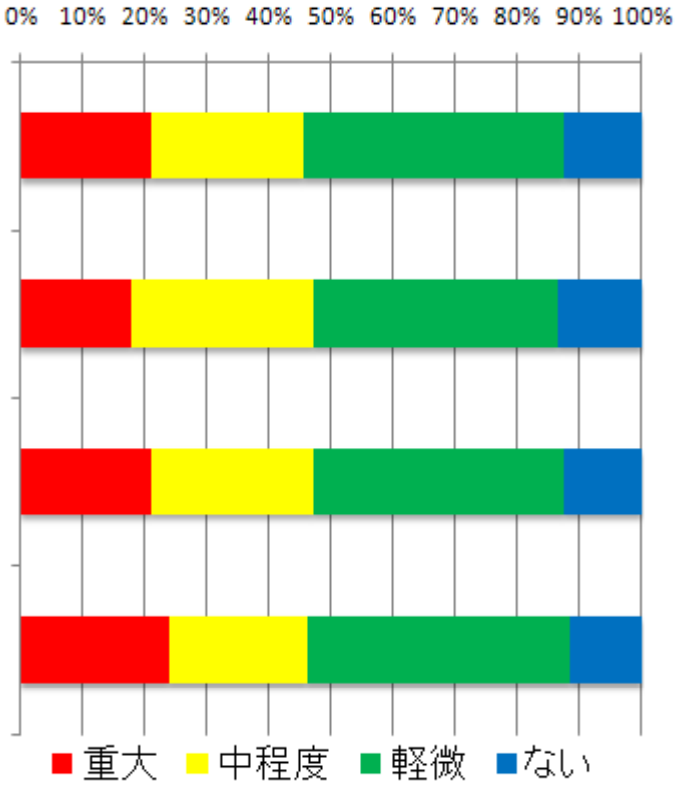
出所：原田、クラウドコンピューティングのリスクとガバナンスに関する調査・研究について、情報処理 Vol.51 No.12 Dec. 2010

ENISAのリスク評価と日本2010年調査を振り返って⑤

共通事項

リスク	ENISA
SOCIAL ENGINEERING ATTACKS 事業者がソーシャルエンジニアリング攻撃を受けて、自組織に関する情報を開示するリスク	Medium
LOSS OR COMPROMISE OF OPERATIONAL LOGS 自組織サービスが取得しているログを紛失したり、漏えいさせるリスク	Low
LOSS OR COMPROMISE OF SECURITY LOGS 事業者が認証などのセキュリティログを紛失したり、漏えいさせるリスク	Low
BACKUPS LOST, STOLEN 事業者がバックアップファイルを毀損させたり、漏えいさせるリスク	Medium

アンケート結果



・FS事件では、事業者のバックアップの問題点を気付かせてくれた

出所：原田、クラウドコンピューティングのリスクとガバナンスに関する調査・研究について、情報処理 Vol.51 No.12 Dec. 2010

クラウドのリスクを振り返って

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- さまざまなリスク(ENISA)は現実化してきている
  - 組織的なリスク
  - 法的なリスク
  - 技術的なリスク
  - 共通のリスク
- リスクは減るよりもますます増えている

↓

- リスクを減らして、安全にクラウドを利用
  - ガバナンスの問題
  - 認証、監査、保証サービスがより重要に

ISMS認証機関の対応

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

2012年	6月20日	（FS社事故発生）
	6月27日	**事実関係の調査を行う旨を公表**
	7月31日	（FS社が第三者委員会調査報告書を公開）
	8月16日	**調査の結果、「マネジメントシステムへの不適合」を理由にISMS認証を一時停止 ⇒ 同20日公表**
	10月12日	**臨時審査の結果、ISMS認証一時停止を解除 ⇒同日公表**

一連の措置・情報公開(※)が行われている

(※) 認証機関ウェブサイトにて
http://www.bsigroup.jp/assessmentandcertification/managementsystem/news/

ISMS認証制度の限界

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

(ii)管理策の問題、(iii)データ復旧手順の不備

バックアップ、復旧手順ともにISMS(JIS Q 27001)の要求　事項に規定されているが、「組織が特定した情報資産に対するリスク評価とそれを低減する管理策の有効性を審査員が判断」

全ての管理策の実施や内容のレベルを保証しているわけではない

適用宣言書は原則として非公開
⇒ユーザが管理策実施の有無と内容を判断することは困難

ISMS認証取得を事業者の安全性の判断として
利用するには限界がある

17 出所：佐藤・原田、クラウドサービスにおける第三者認証制度の考察、情報処理学会研究報告 Vol.2013-EIP-59 No.1 Feb. 2013

Pマーク認証機関の対応

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

2012年11月20日に公表された審議結果

ISMSとは対照的に、対応に関する情報公開が遅れていた。

■Pマークの要求事項(JIS Q 15001)における、個人情報保護マネジメントシステムの適用範囲

→事業の用に供する個人情報

■「事業の用」に供しない例（経産省ガイドライン）

→倉庫業、データセンター（ハウジング、ホスティング）等の事業において、当該情報が個人情報に該当するかどうかを認識することなく預かっている場合に、その情報中に含まれる個人情報

⇒レンタルサーバ内の情報はFS社にとって個人情報に該当しないため、個人情報の滅失事故とは言い切れない。措置なしと判断

→クラウドサービスを利用するPマークの認証企業に問題点を周知

■利用者から個人情報などの重要な情報の修復を依頼されて、データのリカバリを実施したところ、複数の企業の情報が混ざった形で提供することになった。

→個人情報の漏えい事件と認定、ただし、直ちにリカバリを停止し、消去を依頼したため、漏えい範囲は限定的と判断して同様の事故との比較から、注意措置と判断

出所：佐藤・原田、クラウドサービスにおける第三者認証制度の考察、情報処理学会研究報告 Vol.2013-EIP-59 No.1 Feb. 2013

FS社の事故におけるISMS・Pマークの問題

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

事故に対する説明、(限定的な)損害賠償の支払い、
再発防止策の実施がされたが、
一方で下記の問題点が明らかになった。

(i)組織のマネジメントシステムの問題

(ii)管理策の内容の問題

(iii)データ復旧手順の不備

⇒ISMSやPマーク認証を取得しているのであれば、
これらを防止する体制の構築を期待されているはず

ISMSやPマークの制度設計(事後の対応や審査基準等)
に問題はないか？

19 出所:佐藤・原田、クラウドサービスにおける第三者認証制度の考察、情報処理学会研究報告 Vol.2013-EIP-59 No.1 Feb. 2013

ISMS・Pマーク認証制度と事件への対応
ISMS・Pマーク認証制度の限界

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■製造物製品（例：ISO9001等）

マネジメントシステムのみならず、製品の種類ごとに法令や業界基準等により定められている品質基準を遵守する必要有

■情報システム

データと処理する作業が特定されないと対策レベルの具体的一般化が困難。製造物製品と違い、遵守すべき水準が存在する分野は限られている。

⇒例えばIaaSの場合、ユーザが保存しているデータを事業者は認知しない。

ISMS・Pマーク認証制度の限界

 出所：佐藤・原田、クラウドサービスにおける第三者認証制度の考察、情報処理学会研究報告 Vol.2013-EIP-59 No.1 Feb. 2013

情報セキュリティに関する様々な制度

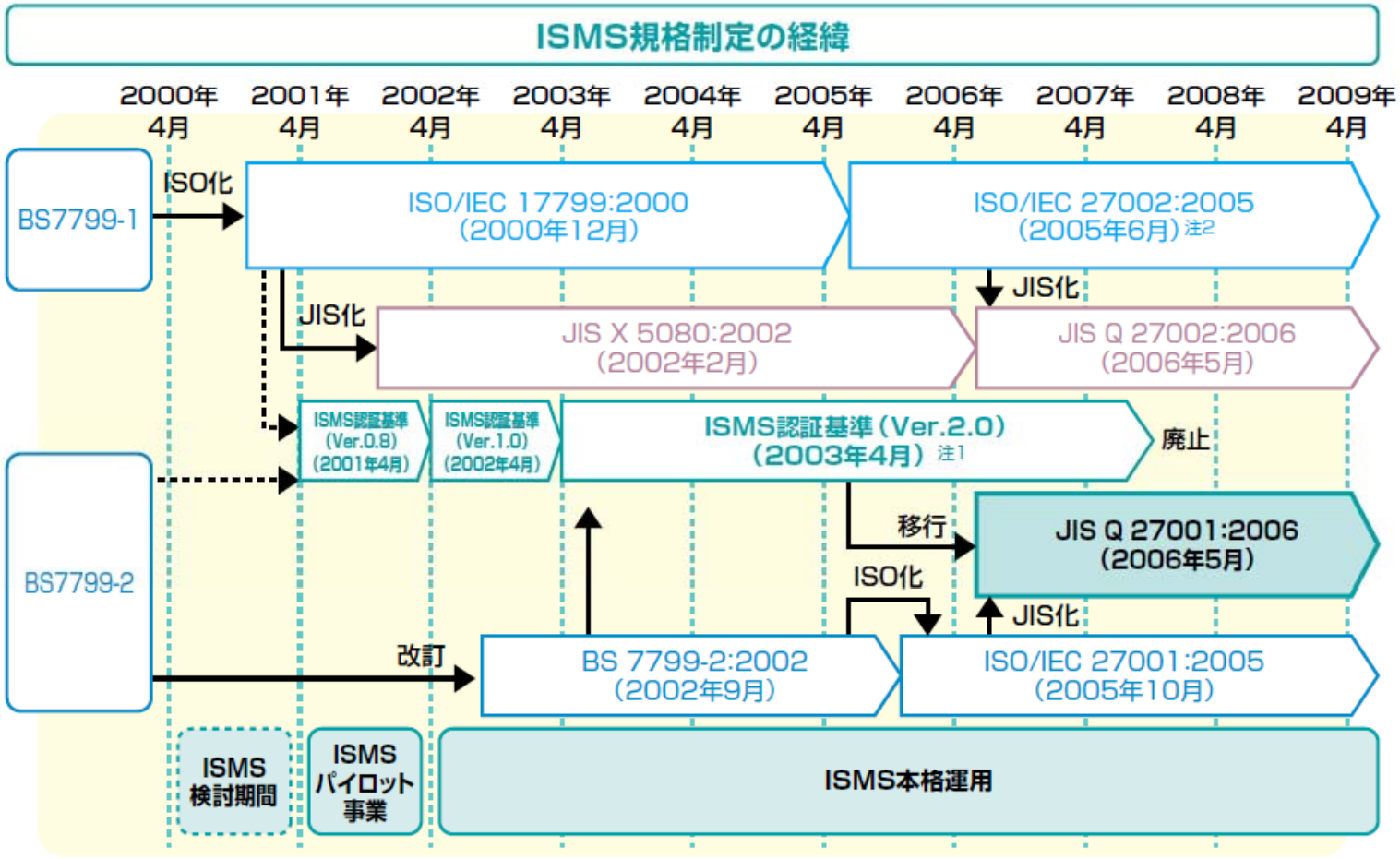
日本(経産省):
情報セキュリティガバナンス制度

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- 情報セキュリティベンチマーク制度(2005)
- 情報セキュリティ報告書制度(2005)
- ISMS 認証制度(2000)
- 情報セキュリティ監査制度(2003)
  - 利用者合意方式(2008)
  - 社会的合意方式(2008)
- 情報セキュリティ格付け制度(2009)
- その他　BCP
  - 事業継続計画(2005、2012年改訂)
  - ITサービス継続計画(2008制定、2011年改訂)

ISMSの歴史

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

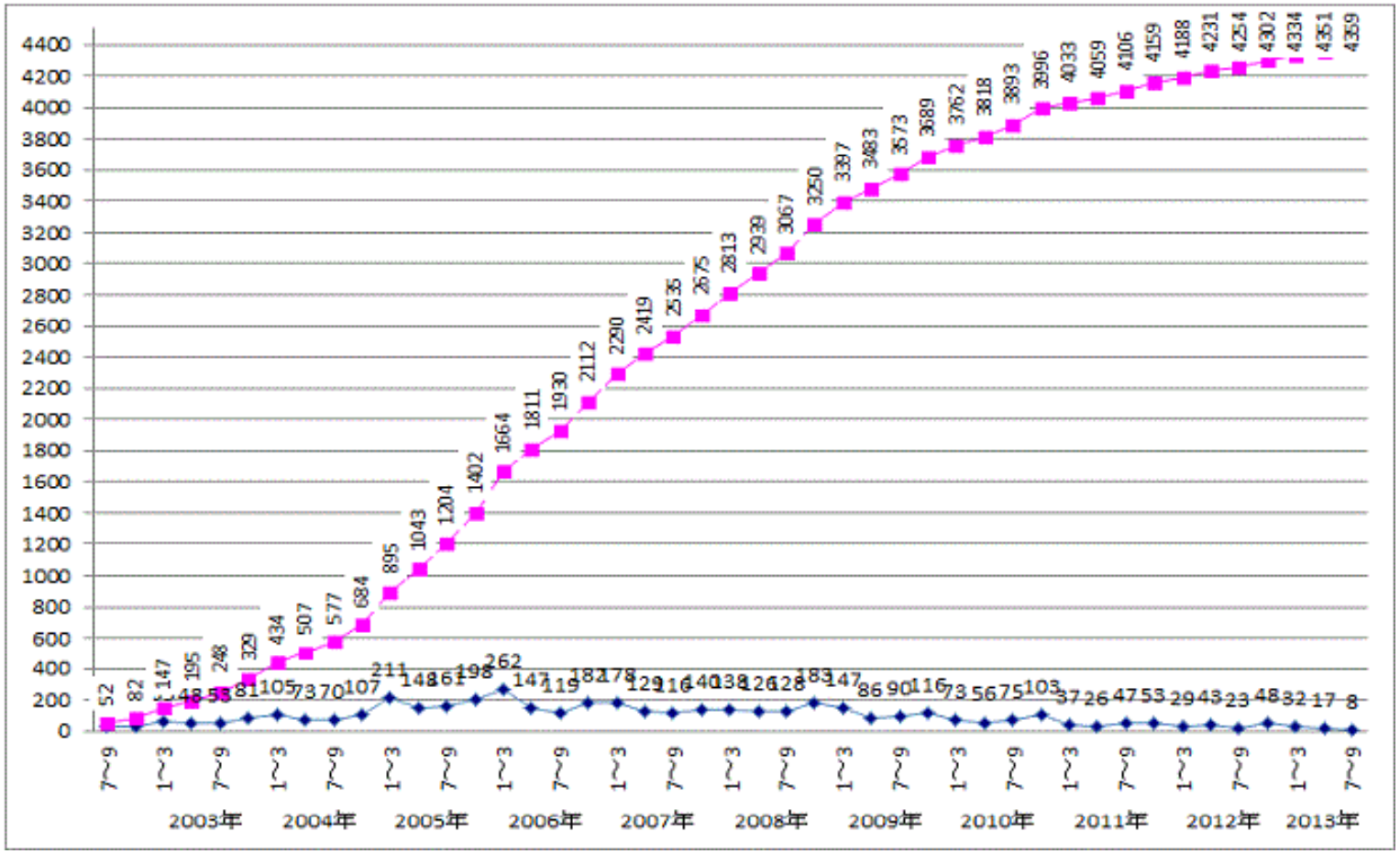


備考：BSは英国規格、ISO/IECは国際規格、JISは国内規格、ISMS認証基準（Ver.n）はJIPDEC規格。
注１：ISMS認証基準（Ver.2.0）は、BS 7799-2:2002をベースとし、用語、表現についてはJIS X 5080:2002との互換性を確保。
注２：ISO/IEC 27002:2005（2007年7月に変更）の旧規格番号は、ISO/IEC 17799。

ISMS登録事業者数の推移

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- 13年8月末時点で、4359事業所（11年8月3901）

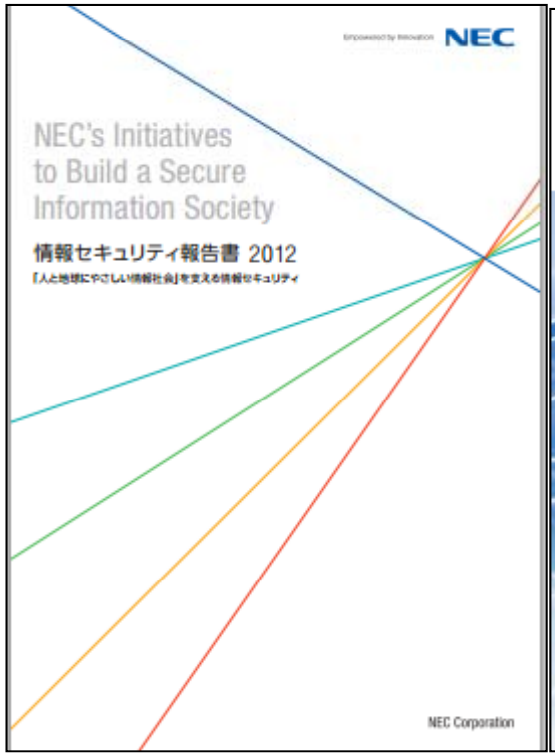


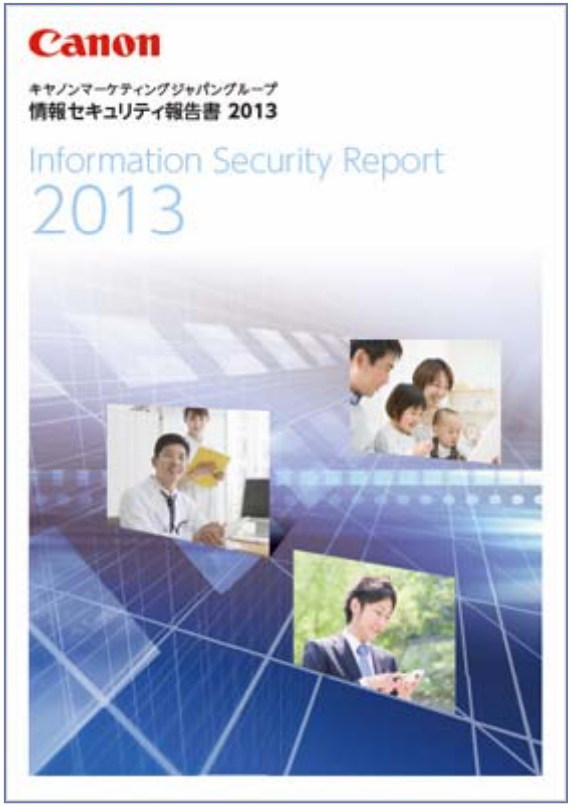
出所：http://www.isms.jipdec.jp/lst/ind/suii.html

情報セキュリティ報告書

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- 各社が自社の情報セキュリティについてステークホルダに報告する（CSR報告書のアナロジー）





「監査(audit)」とは?

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

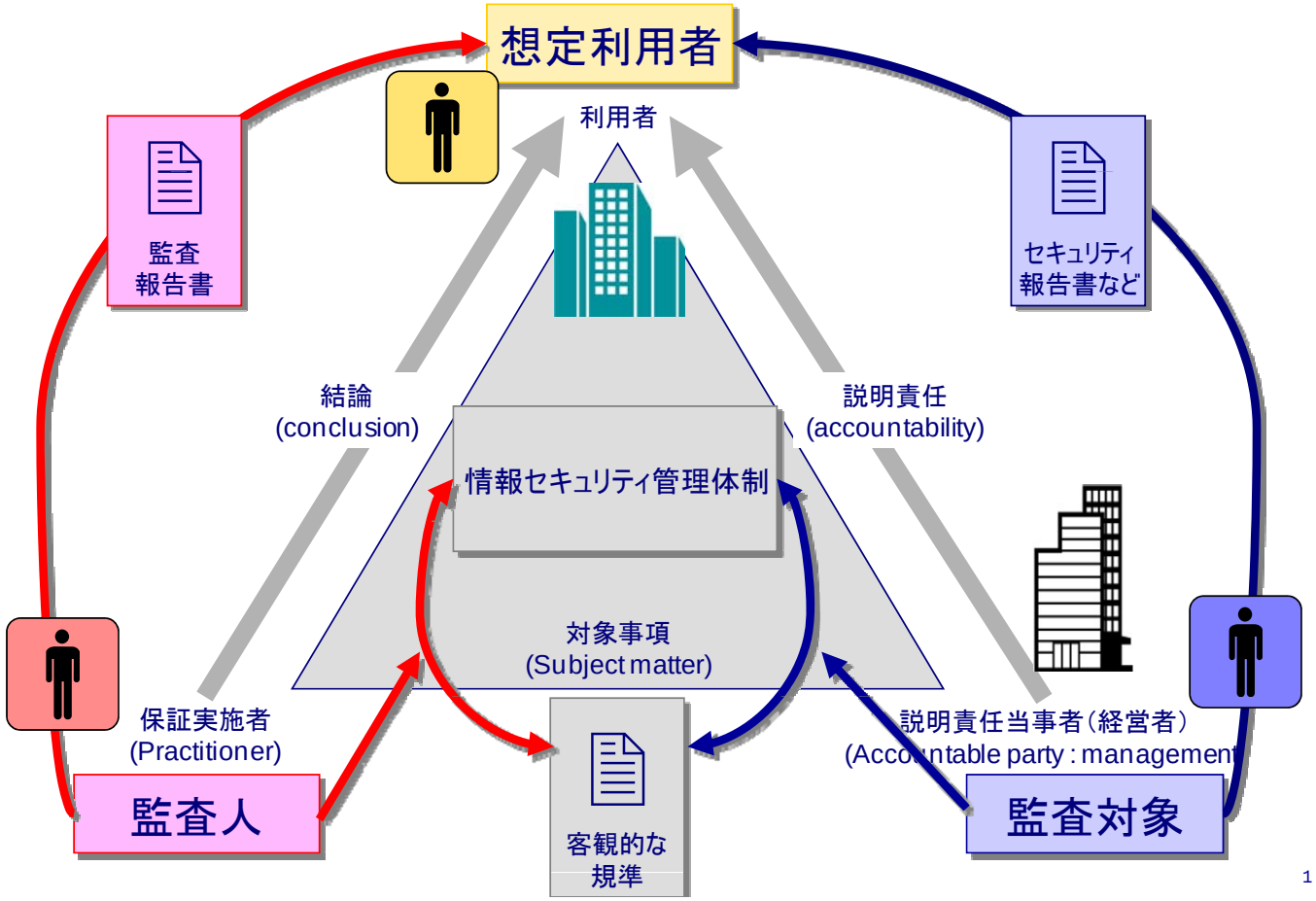
- 「監査(audit)」とは、
- **ある目的のために**組織体の行為を、独立の立場にある第三者が検証・評価することで、その**真実性や妥当性などを確認し、その結果を関係者に報告**すること。これにより、なんらかの説明責任を果たし、一定の信頼を付与する機能や行為。

- 何らかの責任追跡(accountability)を果たす機能や行為
- 「自己証明は監査にあらず」
- 認証は、要求条件全てについて条件を満足することが必要となるので、監査とは異なる

出所:JASA平成17年度保証型監査促進プロジェクト　中間報告書

監査における三者関係

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



出所：JASA公認情報セキュリティ監査人研修教科書

「保証」の概念

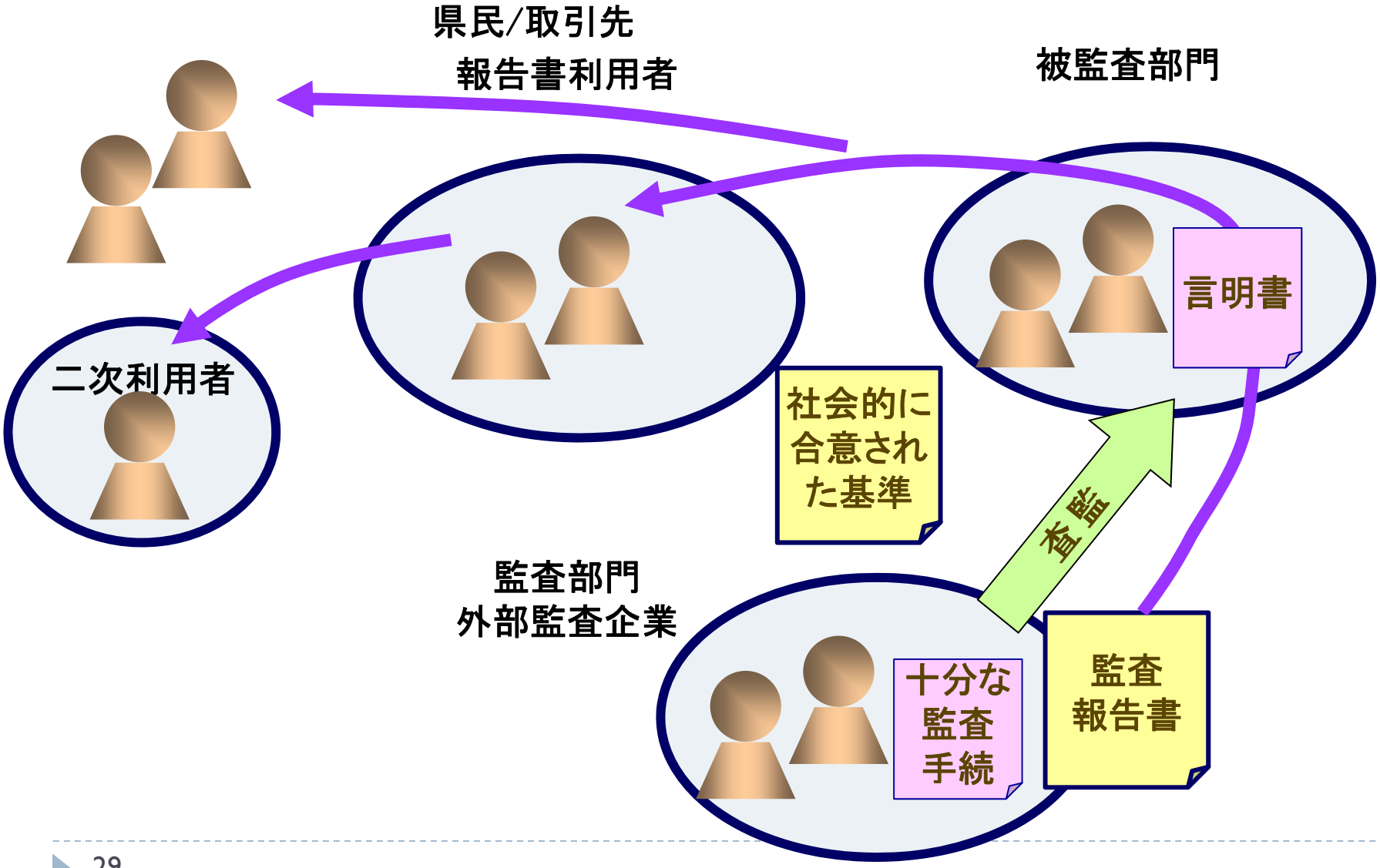
- 「合理的保証(reasonable assurance)」とは
  - 「保証型監査の監査人が情報セキュリティ監査基準に従って監査を実施した結果、言明と監査人が把握した事実との間に相違がないことについて、相当程度の心証を得たとの専門家としての判断を結論として述べること」

- 保証型監査における保証業務の定義
  - 「監査対象の経営者が発した言明に対し、監査人が合理的な方法と証拠に基づき、監査の対象となる組織体の情報セキュリティに関するマネジメントとコントロールが監査手続きを実施した限りにおいて適切である旨（または不適切である旨）の意見を述べること」

- 保証型監査における保証程度の度合い
  - 保証型監査においては、「合理的保証」のみが存在しうると考える。ここでいう合理的とは、経済的合理性、技術的合理性、社会的合理性などを意味する。

出典：JASA平成17年度保証型監査促進プロジェクト　中間報告書

保証型監査の例（JASAの保証型監査モデル）



出所：JASA公認情報セキュリティ監査人研修教科書

保証型監査の方式

	社会的合意方式	利用者合意方式	被監査主体合意方式
監査手続の十分性の担保	社会的に合意された基準に照らして十分な監査手続であるとの監査人の判断	監査目的に照らした監査手続の十分性について利用者の合意が存在	監査目的に応じた手続として監査主体と被監査主体が合意し1次利用者の確認がある
実施する監査手続	監査人が必要と考える手続	1次利用者と合意した、期待に応えられる監査手続	被監査主体と合意し利用者の確認を得た監査手続
保証の内容	設計監査または実装監査	設計監査または実装監査	実装監査
保証の方法	意見表明方式	意見表明方式	結果報告方式
保証の対象	言明方式	言明方式	非言明方式
保証の対象とする期間	時点監査（期間監査も条件を満たせば可能）	時点監査（期間監査も条件を満たせば可能）	時点監査または期間監査
監査の対象範囲	監査の主題にかかわる重要部分を欠いていないこと	監査の主題にかかわる重要部分を欠いていないこと	被監査主体と合意し利用者の確認を得た部分
監査報告書の利用者	不特定	特定された1次利用者に限定	特定された1次利用者に限定
報告書記載	信じるに足る	期待する水準にある	結果を報告する
適用可能な具体例	委託先の監査結果を広く利害関係者に公表したい場合	報告書利用者である委託者が委託先に期待する水準が明確な場合で、委託先がその期待に応えていることについて保証を得たい場合	受託者として求められる事項の遵守について保証を得たい場合

出所：JASA公認情報セキュリティ監査人研修教科書

監査法人による保証サービス（統制、セキュリティ）目的により3形態

	SOC1	SOC2	SOC3
適用する基準	SSAE16 （AT801）	AT101	AT101
対象となる業務	委託会社の財務報告に関連すると考えられる受託会社の内部統制	セキュリティ、可用性、処理のインテグリティ、機密保持、プライバシーに関する受託会社の内部統制	セキュリティ、可用性、処理のインテグリティ、機密保持、プライバシーに関する受託会社の内部統制
レポートの利用者	委託会社の財務諸表監査を実施する監査人 受託会社の経営者 委託会社の経営者	受託会社の経営者 委託会社の経営者	配布制限なし

（AICPA “Service Organizations: New Reporting Options” より抜粋したものに基づく）

セキュリティ、可用性、完全性、機密保持、プライバシに関する内部統制の保証を追加できる

出所：吉川・市川、受託会社の内部統制に関する保証報告制度、あずさ監査法人(KPMG)
AZ Insight, Vol. 47, 2011年9月号

SOCのロゴの利用

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

Service Organization Control (SOC) Reports

Service Organization Control (SOC) reports are internal control reports on the services provided by a service organization providing valuable information that users need to assess and address the risks associated with an outsourced service.

CPAs

Provides information to user auditors and service auditors on understanding and performing SOC engagements.

Users

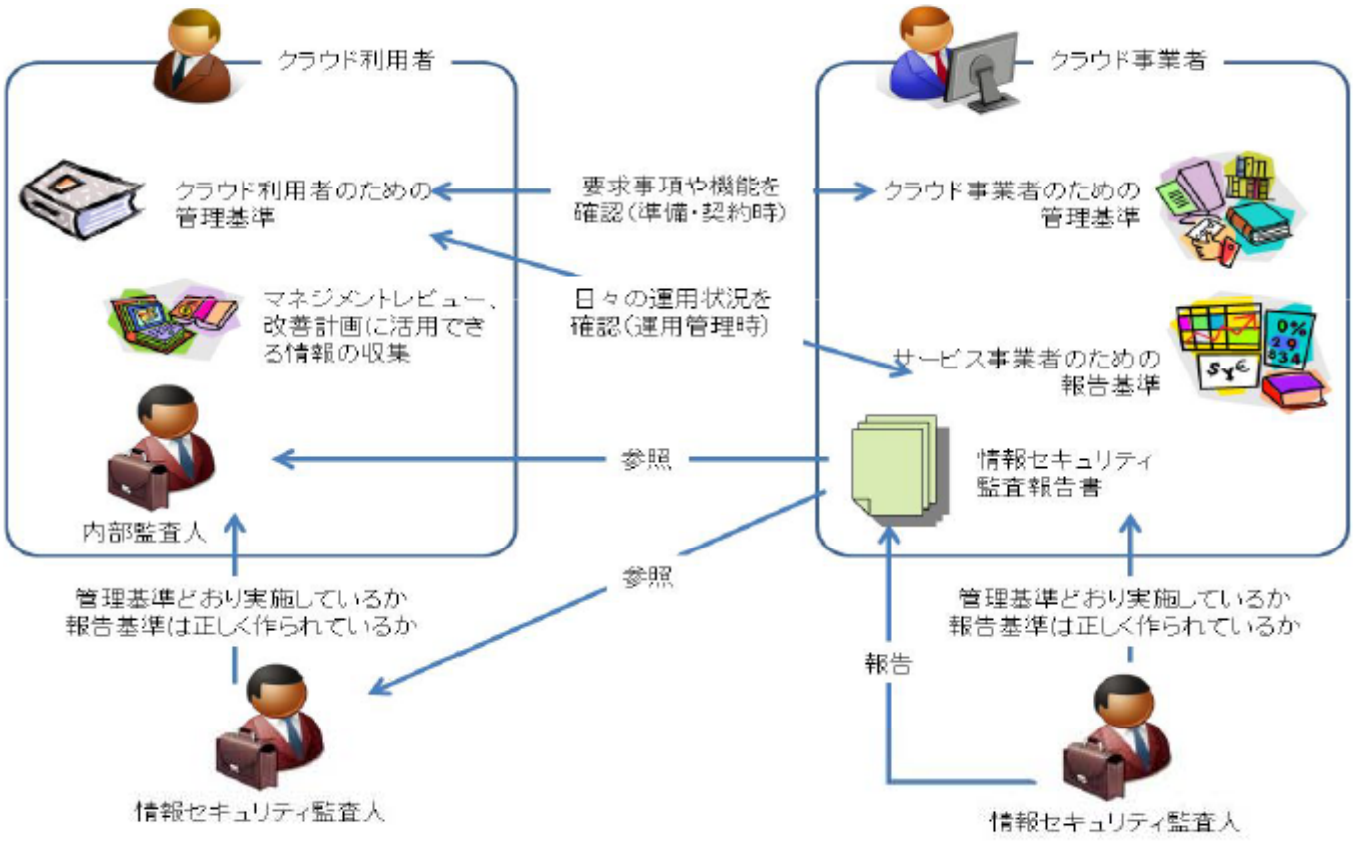
Provides information to user entities on how to mitigate the risks associated with outsourcing services.

Service Organizations

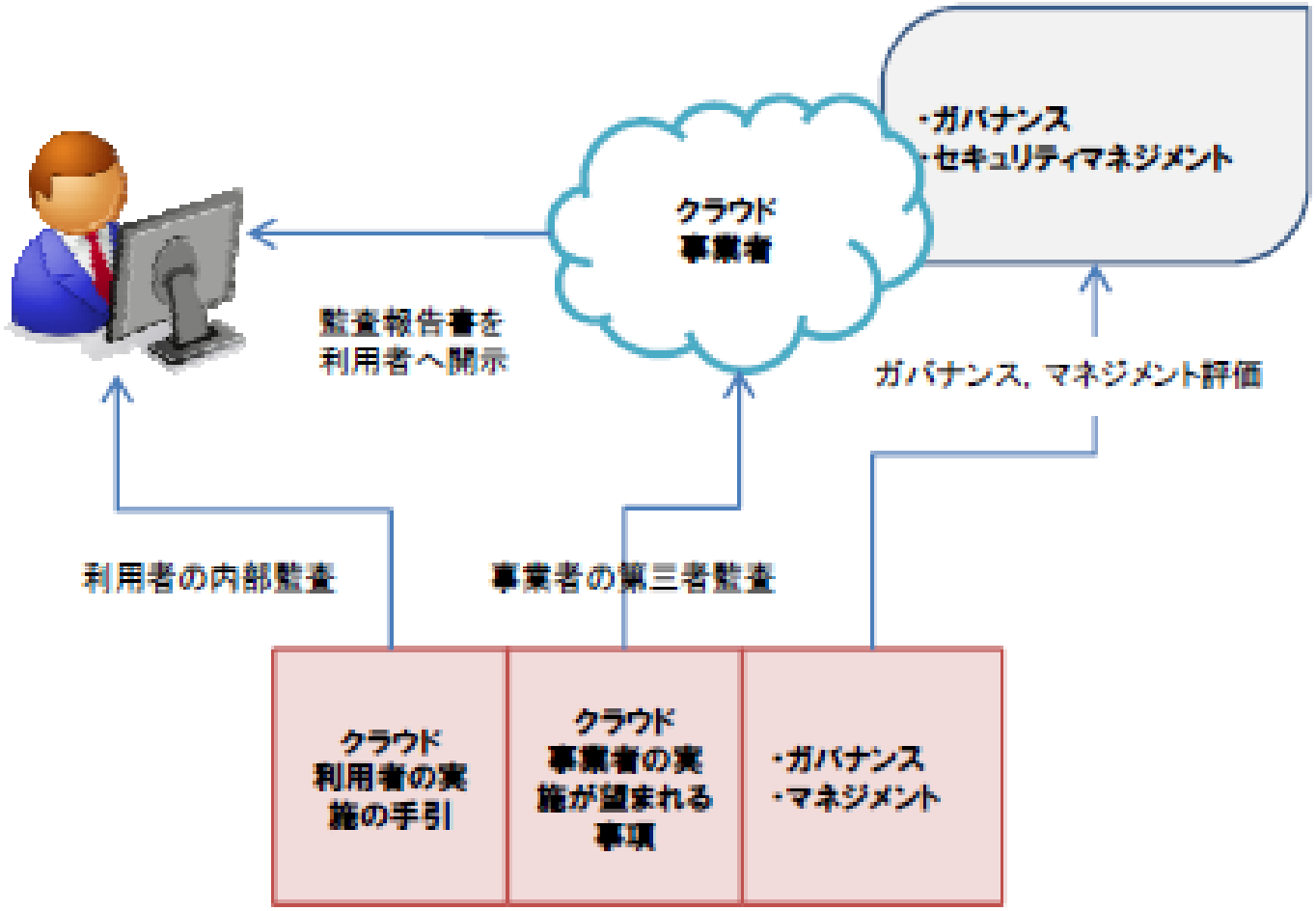
Provides information to service organizations on building trust and confidence in their systems.

クラウドサービス事業者の認証・保証制度

情報セキュリティ監査の適用



出所：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



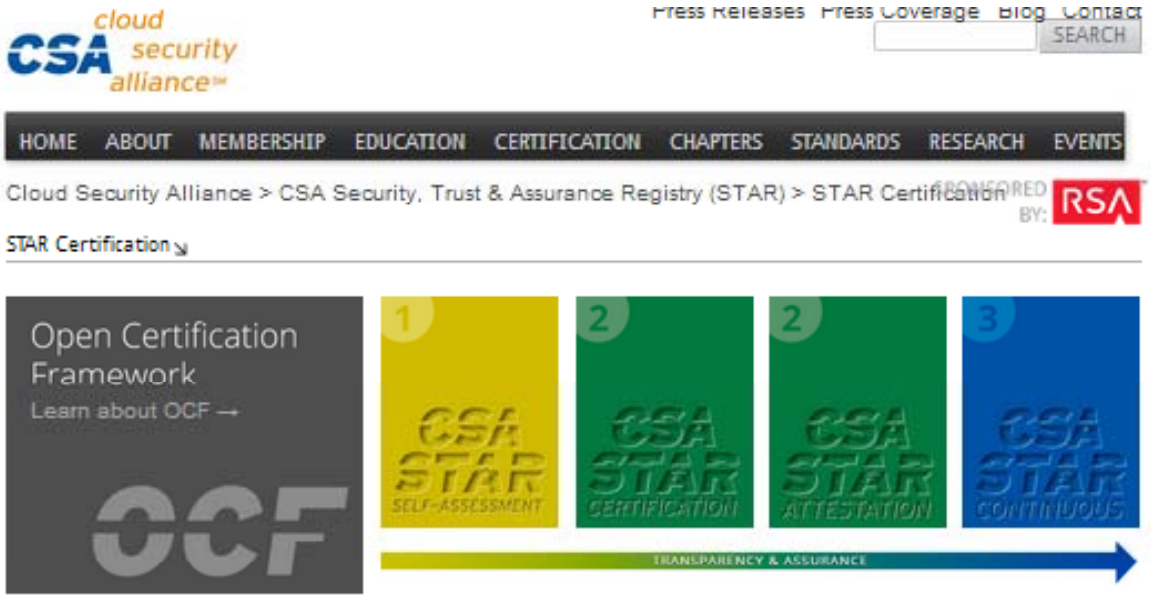
出所：クラウドサービス利用のための情報セキュリティマネジメントガイドライン

CSA

- クラウド･プロバイダーの認証スキーム
  - CSAのセキュリティガイダンスとコントロール目標を利用
  - 認証機関や公認会計士による、独立した第三者評価・保証を組み合わせている
- 4レベルで構成
  - 1. Self Assessment（自己評価）
    - CSA STAR RegistryにCSAのガイドラインへの準拠状況を表明
  - 2.. Third-party independent assessment（第三者評価）
    - ISO/IEC 27001:2005 評価基準をCSA Cloud Controls Matrix (CCM)と組み合わせ、認証機関による評価
  - 3.. Attestation（保証）
    - 監査法人による保証を組み合わせた
  - 4. Continuous monitoring-based certification（継続評価）

CSAのSTAR

- STAR Self-Assessment（自己評価）
- STAR Certification（認証機関による認証）
- STAR Attestation（保証機関による保証）
- STAR Continuous（継続性の保証）



Example Certificate

bsi.

By Royal Charter

Certificate of Registration

CLOUD SECURITY MANAGEMENT SYSTEM - STAR CERTIFICATION 2013

This is to certify that:

[redacted]

Holds Certificate Number: **STAR 12345**

and operates an Information Security Management System which complies with the requirements of STAR Certification and has achived Gold Certification for the following scope:

Information Security Management System
[redacted] **This in accordance with the Statement of**
Applicability revision [redacted]

For and on behalf of BSI:

Gary Fenton, Global Assurance Director

Originally Registered: 13/06/2011 Latest Revision Date: 18/10/2012 Expiry Date: 13/06/2014

Page: 1 of 2

CSA STAR CERTIFICATION

...making excellence a habit.

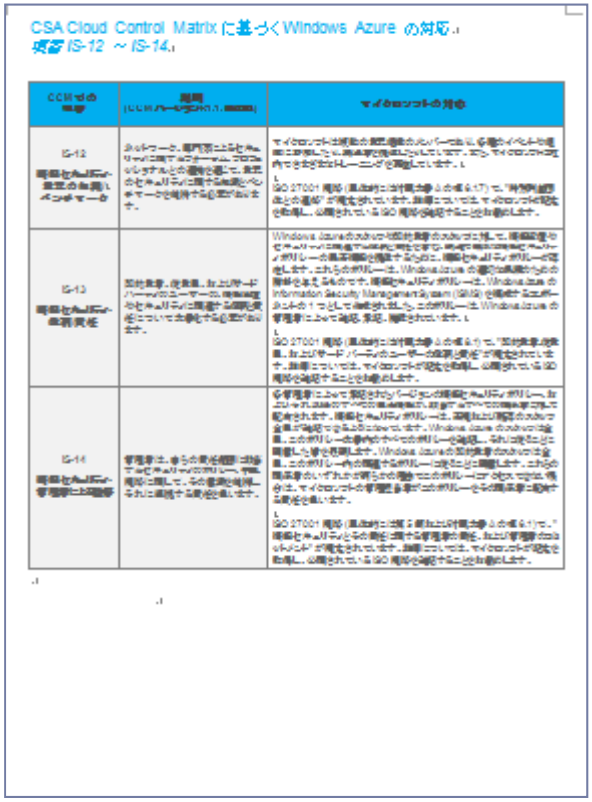
出所：https://cloudsecurityalliance.org/star/certification/

STAR の自己評価の仕組み

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- クラウド･プロバイダがセキュリティの最小限の透明性を確保
  - CSAがクラウドの情報セキュリティのガイドラインを提示（CCM）
  - プロバイダは、情報セキュリティマネジメントに合わせてCCMによる情報セキュリティマネジメントシステムを構築し、そのエビデンスを公開する
  - エンドユーザーは、公開情報をもとにプロバイダを比較評価できる
- The Consensus Assessments Initiative Questionnaire（CAIQ）
  - CAIQは、クラウドサービスで実施しているセキュリティコントロールを文書化するための業界標準。140の監査人や利用者が行うコンセンサスアセスメントイニシアティブアンケートから構成

MicrosoftのSTAR対応の情報公開


CSA Cloud Control Matrix に基づく Windows Azure の対応

MSは、CSAのCCM（自主点検）
ISO/IEC27001:2005（認証）

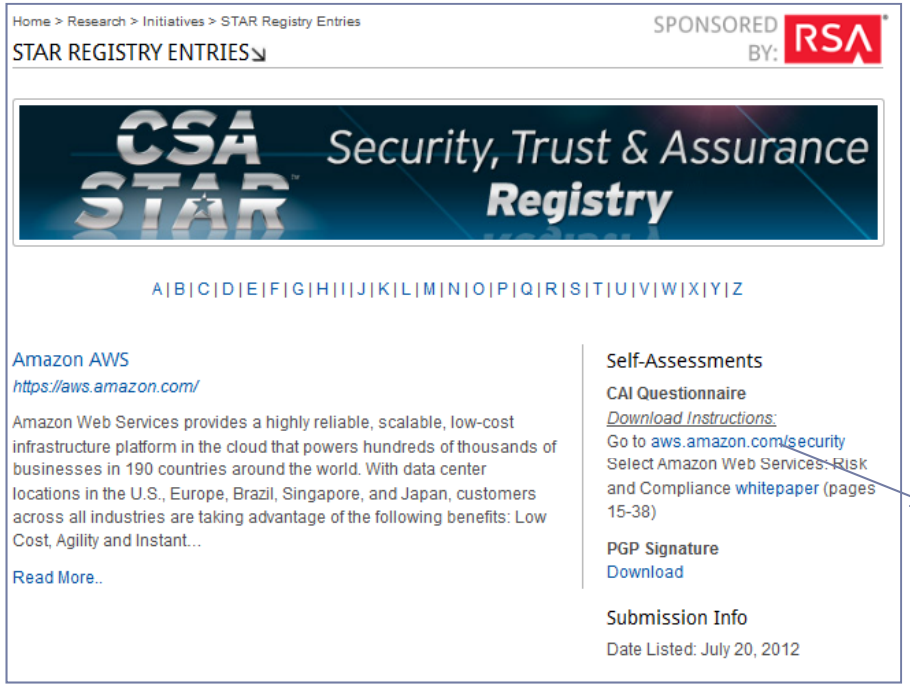
CCMとISMSの付属書Aの管理策を並べて準拠性を説明

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

CCM での項番	説明 (CCM バージョン R1.1. 最終版)	マイクロソフトの対応
IS-12 情報セキュリティ - 業界の知識/ベンチマーク	ネットワーク、専門家によるセキュリティに関するフォーラム、プロフェッショナルとの連携を通じて、業界のセキュリティに関する知識とベンチマークを維持する必要があります。	マイクロソフトは複数の業界組織のメンバーであり、各種のイベントや組織に参加したり、講演者を提供したりしています。また、マイクロソフトは社内でさまざまなトレーニングを実施しています。 ISO 27001 規格 (具体的には付属文書 A の項 6.1.7) で、"特別利益団体との連絡" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。
IS-13 情報セキュリティ - 役割/責任	契約業者、従業員、およびサードパーティのユーザーの、情報資産やセキュリティに関連する役割と責任について文書化する必要があります。	Windows Azure のスタッフや契約業者のスタッフに対して、情報資産やセキュリティに関連する役割と責任を含む、明確で簡潔な情報セキュリティ ポリシーの最新情報を提供するために、情報セキュリティ ポリシーが存在します。これらのポリシーは、Windows Azure の適切な保護のための指針を与えるものです。情報セキュリティ ポリシーは、Windows Azure の Information Security Management System (ISMS) を構成するコンポーネントの 1 つとして作成されました。このポリシーは、Windows Azure の管理者によって確認、承認、推奨されています。 ISO 27001 規格 (具体的には付属文書 A の項 8.1) で、"契約業者、従業員、およびサード パーティのユーザーの役割と責任" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。
IS-14 情報セキュリティ - 管理者による監督	管理者は、自らの責任範囲に該当するセキュリティのポリシー、手順、規格に関して、その意識を維持し、それに準拠する責任を負います。	各管理者によって承認されたバージョンの情報セキュリティ ポリシー、およびそれ以降のすべての更新情報が、該当するすべての関係者に対して配布されます。情報セキュリティ ポリシーは、新規および既存のスタッフ全員が確認できるようになっています。Windows Azure のスタッフは全員、このポリシー文書内のすべてのポリシーを確認し、それに従うことに同意した旨を表明します。Windows Azure の契約業者のスタッフは全員、このポリシー内の関連するポリシーに従うことに同意します。これらの関係者のいずれかが何らかの理由でこのポリシーにアクセスできない場合は、マイクロソフトの管理担当者がこのポリシーをその関係者に配布する責任を負います。 ISO 27001 規格 (具体的には第 5 節および付属文書 A の項 6.1) で、"情報セキュリティとその責任に関する管理者の責任、および管理者のコミットメント" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。

STARのセルフアセスメント（自己評価）

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



Amazonのセルフアセスメントをクリックすると
Amazonのページに移動

CSAのSTARのページに掲示されているAmazonの状況（セルフアセスメント）にリンクする

STAR認証取得のメリット

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- 国際規格（ISO/IEC 27001）とクラウドセキュリティに関するマネジメントシステム（CSAによるCCM)を構築できる
  - 外部の認証機関から評価によって、クラウドサービスの成熟度のレベルやパフォーマンスをチェックできる
  - 4つの段階となっているので、目標を定めやすい
- 認証機関が、マネジメントススステムの有効性について評価する（BSIがISMSとCCMを組み合わせて認証）
  - サービスプロバイダがクラウドサービスを提供する上で、何を実践すべきかについて知る
  - 利用者も自社の情報セキュリティマネジメントの状況（ISMSなど）に遭わせることができる
- **認証と保証を組み合わせた点が新しい**

情報セキュリティの透明性と説明責任、利用者と提供者の認識ギャップ

説明責任

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- 経営陣の関与、情報セキュリティ対策、利用している基準、および自社の情報セキュリティの達成レベルを
- 経営陣の関与では、責任の明確化がポイント
  - 外部基準か、公開された基準でない限り、説明責任は果たせない。なお、外部基準を利用している場合は、どの基準の項目の具体的な開示が必要である。
- 第三者による客観性が求められる
  - 自社の情報セキュリティについて、客観的に説明できるようにすることが求められ、そのためには評価がなされていることが必要。これを担保するものとして、保証が求められる。
  - 情報セキュリティの監査などがある。

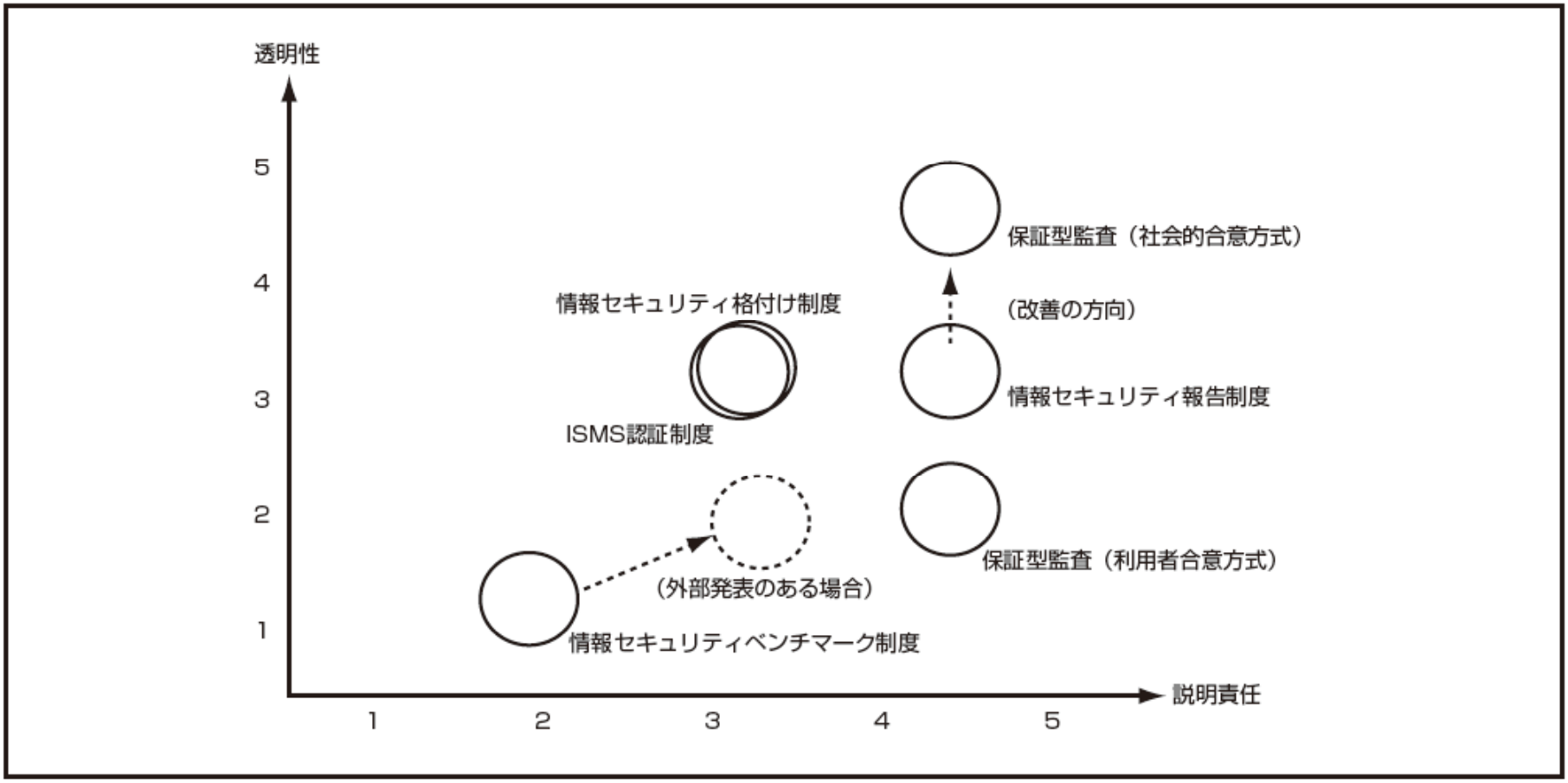
 出所：佐藤・原田、クラウドサービスにおける第三者認証制度の考察、情報処理学会研究報告 Vol.2013-EIP-59 No.1 Feb. 2013

透明性

- 企業が公表する情報セキュリティの内容について、透明性を持つことが重要である
  - 情報セキュリティ対策が、適切性、網羅性、完全性を持つこと
- 透明性には、公表した情報セキュリティ対策について、以下が求められる
  - 客観的であること
  - 検証可能性があること（評価できること）
  - 他と比較できること

日本の情報セキュリティガバナンスの制度比較

図表 11　情報セキュリティガバナンスの比較

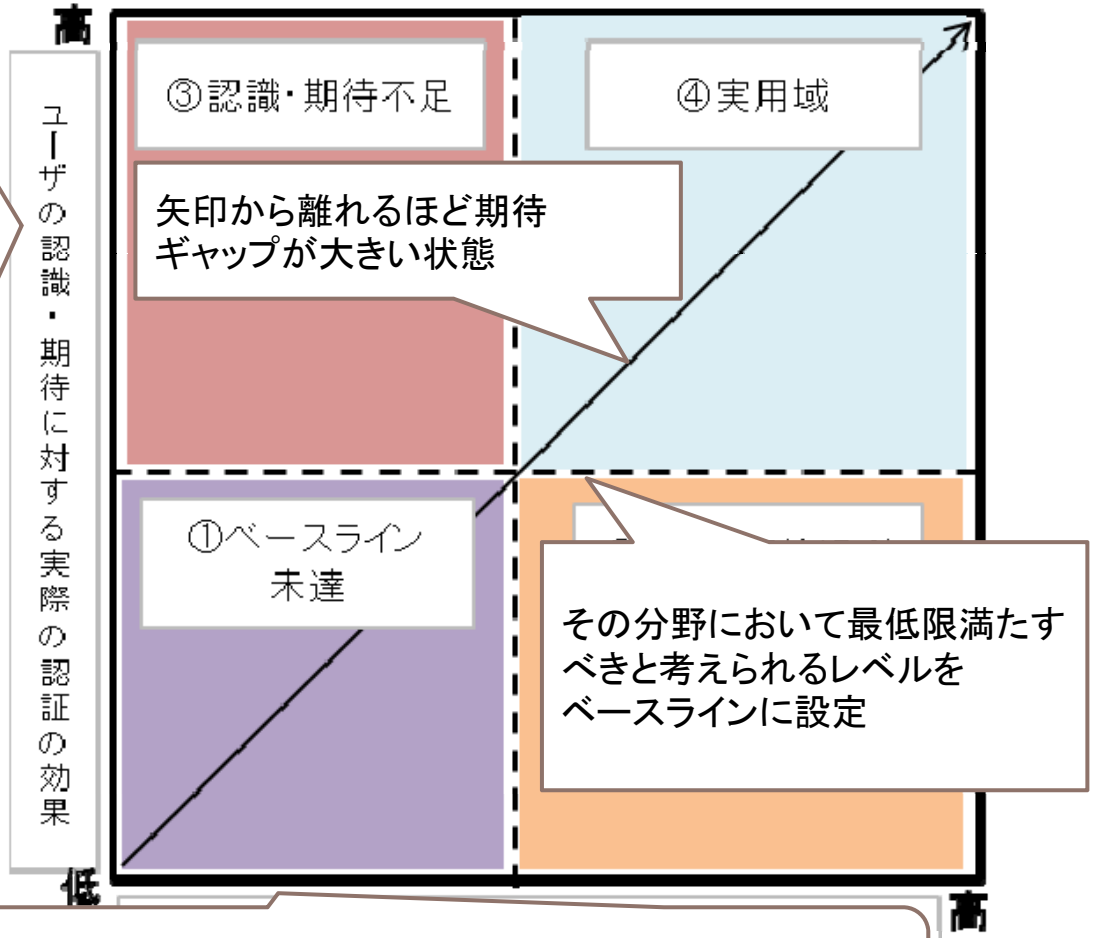


出典：情報セキュリティガバナンスと説明責任,InfoCom Review Vol.49 (2009)より

期待ギャップを考慮した認証制度の評価
評価モデル

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

・制度の認知や普及度
・何を対象として、どの程度の水準か
・事故発生時に説明責任を果たすか
ユーザ側の責任は
・事業者選定理由の説明として使えるか
…etc.



認証制度は、
ユーザの認識・期待に対し、それをどの程度満たすものか？（説明可能か）

48出所：佐藤・原田、クラウドサービスにおける第三者認証制度の考察、情報処理学会研究報告 Vol.2013-EIP-59 No.1 Feb. 2013

期待ギャップを考慮した認証制度の評価

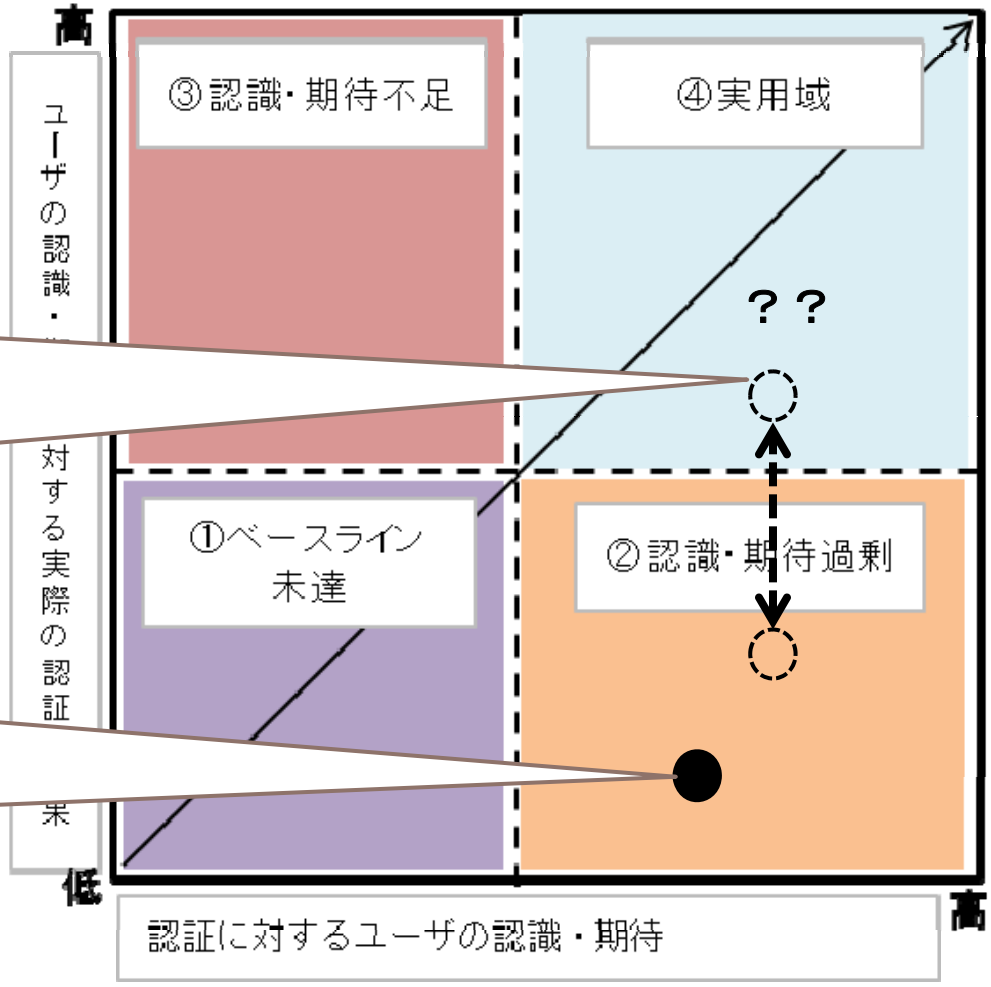
評価モデルの適用と考察

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

②認識・期待過剰

・ISMS等
「適用宣言書」等が公開されていないので、どのレベルにあるのかがわからない状態
⇒情報公開制度などにより補う必要がある

・Pマーク
保証の範囲となる「事業の用に供する個人情報」についてユーザの認識が違っている



49出所：佐藤・原田、クラウドサービスにおける第三者認証制度の考察、情報処理学会研究報告 Vol.2013-EIP-59 No.1 Feb. 2013

期待ギャップを考慮した認証制度の評価

評価モデルの適用と考察

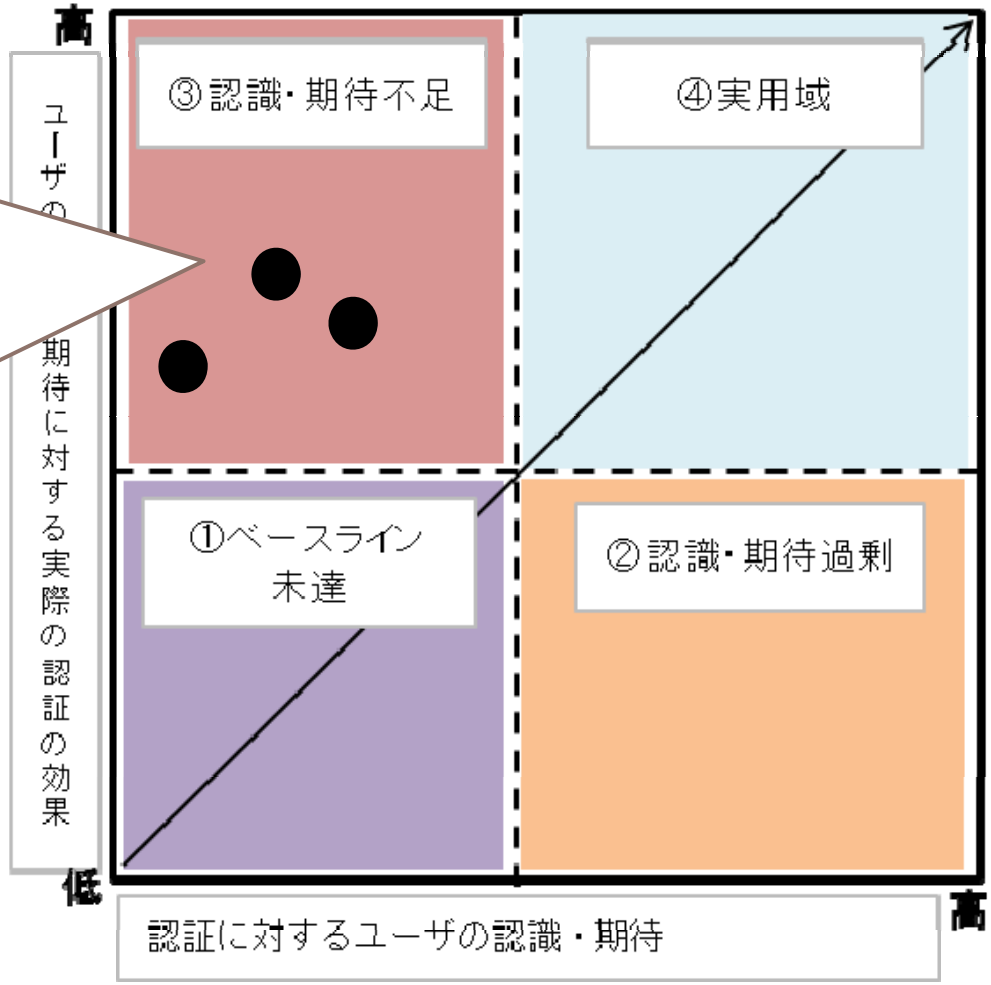
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

③認識・期待不足

・認証取得にかかるコストに見合ったインセンティブが得られない

⇒政府主導によりインセンティブを与える

⇒範囲を限定することによりコストを下げる
・PCI DSS：分野を限定
・ITSMS：サービスレベルを明確に定義　等



50出所：佐藤・原田、クラウドサービスにおける第三者認証制度の考察、情報処理学会研究報告 Vol.2013-EIP-59 No.1 Feb. 2013

まとめ

- クラウドのリスクはまだまだ十分でないと考えられ、そのためには、プロバイダのガバナンスが重要となる。
  - プロバイダには、情報セキュリティ対策面でのより説明責任が要請され、高い透明性が必要
  - 透明性としては、プロバイダと利用者との認識ギャップを埋める工夫が必要
- STARの4つの段階は参考になる
  - 自己点検と情報公開
  - 認証
  - 監査、保証
  - 継続させる工夫
- ガバナンスや監査は重要

ご清聴ありがとうございました