

2015/9/17



クラウド時代におけるセキュリティ統制の在り方

- ISO/IEC 27001およびISO/IEC 27017のころ(狙い) -

工学院大学情報学部

ISO/IEC JTC1/SC27/WG1国内主査

ISO/IEC 27017 Project Editor

クラウドセキュリティコントロール専門委員会委員長

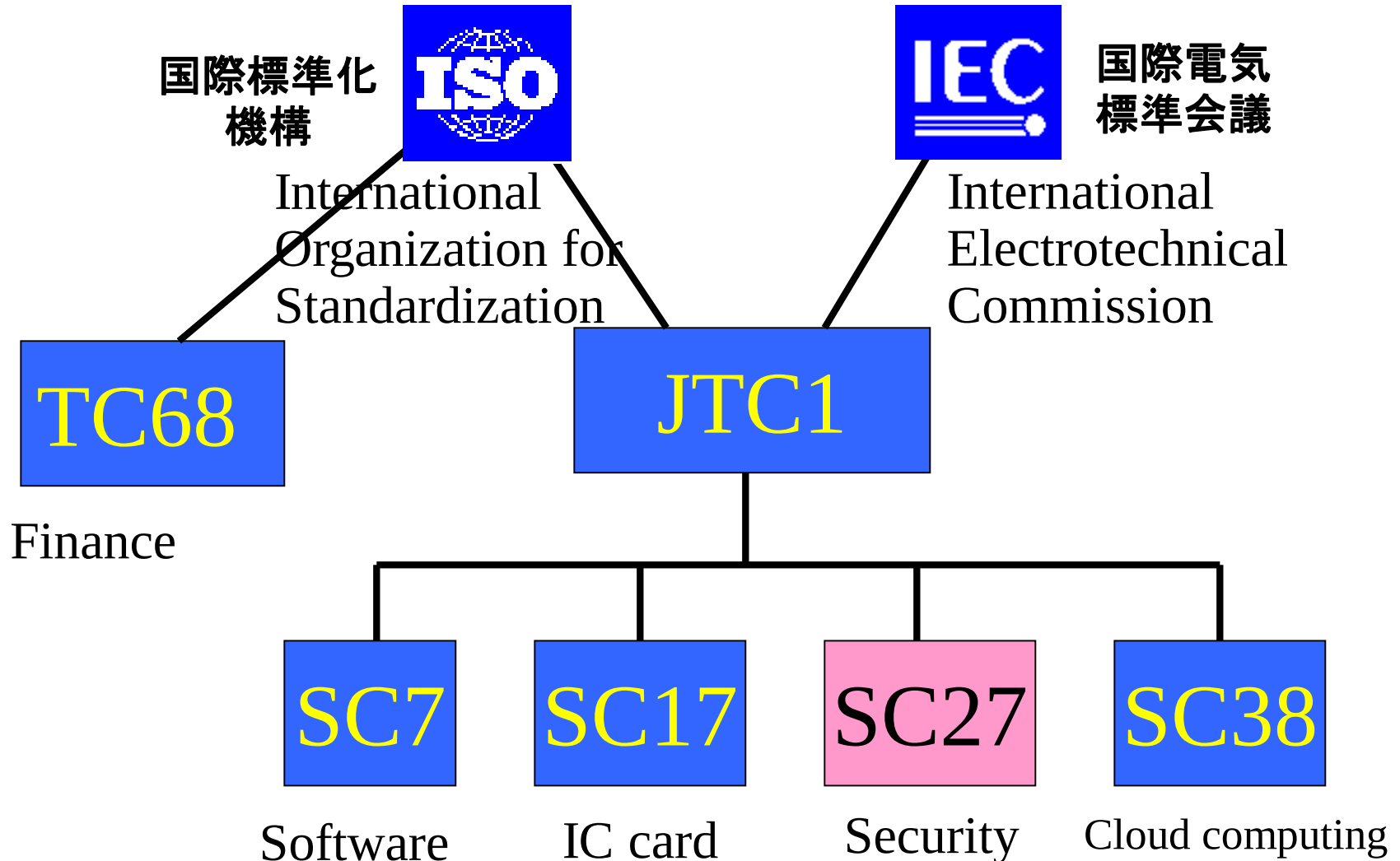
やまさき さとる

山崎 哲

Copyright SC27/WG1 Japan, 2015

国際標準の組織

(セキュリティはISO/IEC SC27 in JTC1)





WG formation in SC27

WG1:ISO/IEC 27000 ISMS family of standards

WG2: Security technology, mechanism

WG3: Security evaluation criteria

WG4:

- Network security
- Application security
- BCP services, others

WG5:

- Privacy
- Identity management
- Biometrics



ご説明内容 – 全体

Part 1. ISMS要求事項：ISO/IEC27001のころころ(狙い)
(Slide 5 ～ Slide 19)

Part 2. クラウドISMS規格：ISO/IEC27017のころころ(狙い)
(Slide 20 ～ Slide 40)

ご説明内容 – Part1 (ISO/IEC27001のころ)

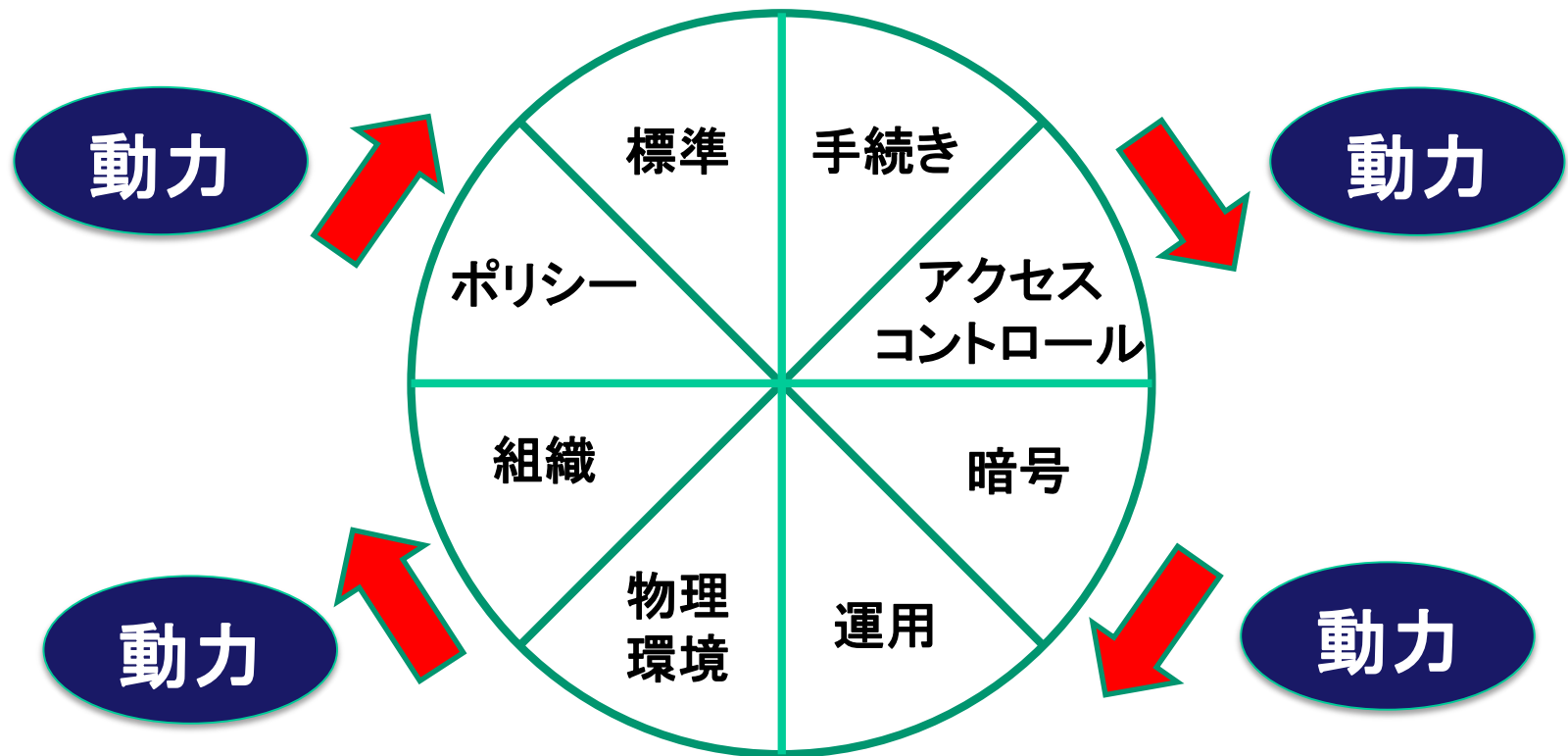


1. 情報セキュリティを推進する動力

- (1) 情報セキュリティ目的の導入
- (2) リスクアセスメントとリスク対応の実施
- (3) 情報セキュリティの役割と責任の明確化
- (4) 監視・測定・分析・評価の実施
- (5) 情報セキュリティガバナンス

車は動力がないと動きません。
セキュリティの動力は何でしょうか。

車＝セキュリティの仕組み



ご説明内容 – Part1 (ISO/IEC27001のころ)

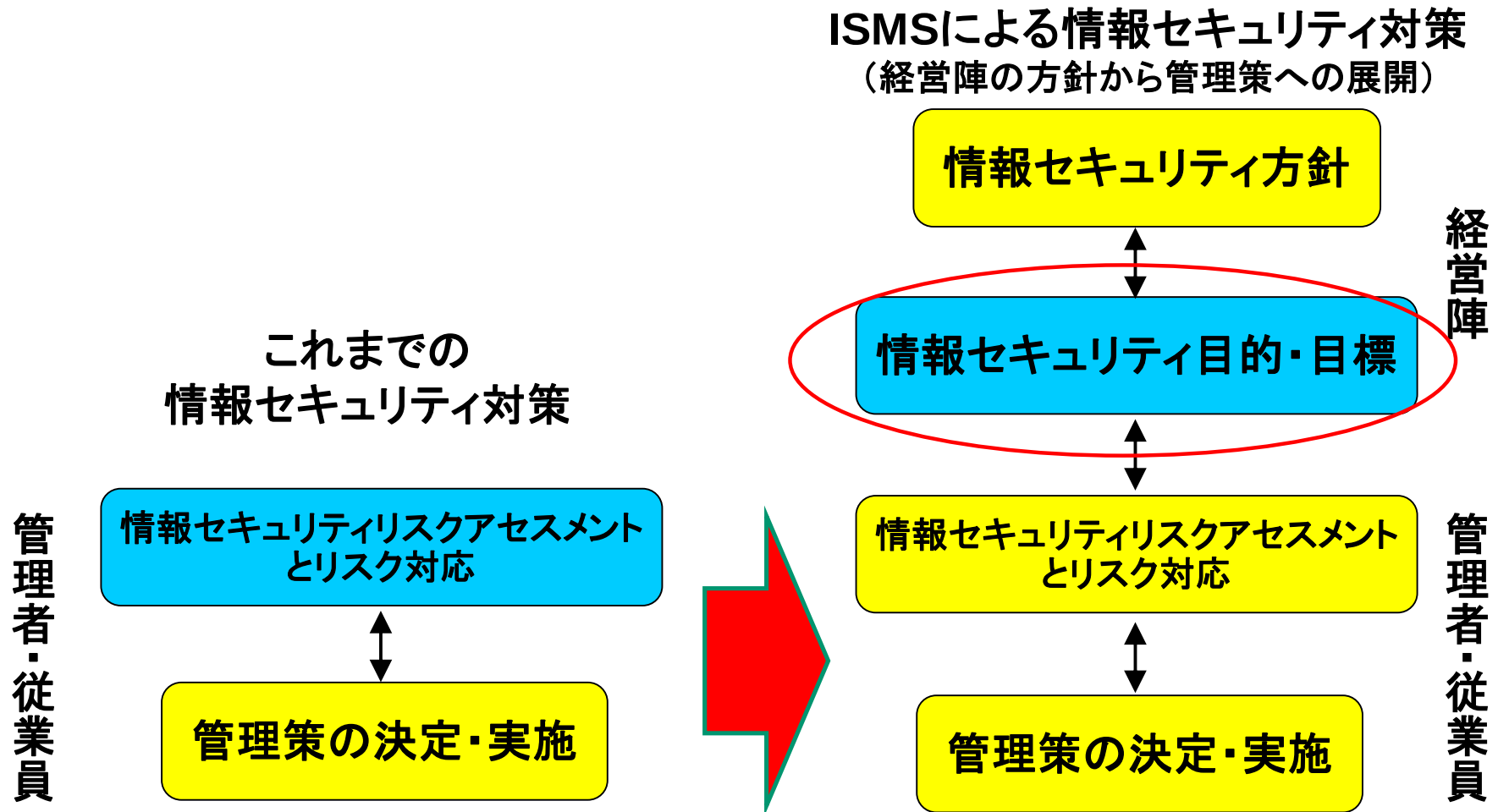
1. 情報セキュリティを推進する動力



- (1) 情報セキュリティ目的の導入
- (2) リスクアセスメントとリスク対応の実施
- (3) 情報セキュリティの役割と責任の明確化
- (4) 監視・測定・分析・評価の実施
- (5) 情報セキュリティガバナンス

(1) 情報セキュリティ目的の導入

- 情報セキュリティ目的・目標はセキュリティ対策の原点です -



(1) 情報セキュリティ目的の導入

- 情報セキュリティ目的の設定の事例(組織構成上) -

- 企業活動に貢献するための情報セキュリティ目的の確立
(事例)

クラウドサービス 提供者の事例

クラウドサービス提供者 (営業部門)の事例

情報セキュリティ目的 (組織の最高位)

- お客様に影響するインシデントを減らしクラウドサービス事業の信頼性を確保する(インシデント=前年比50%)

情報セキュリティ目的 (営業部門)

- お客様情報を含む営業社員のパソコンの紛失インシデントの減少(前年比50%)

1. 実施事項
2. 必要な資源
3. 責任者
4. 達成期限
5. 結果の評価方法

情報セキュリティ目的 (データセンター)

- システム要因によるクラウドサービス事業顧客に影響するインシデントの減少(前年比50%)

1. 実施事項
2. 必要な資源
3. 責任者
4. 達成期限
5. 結果の評価方法

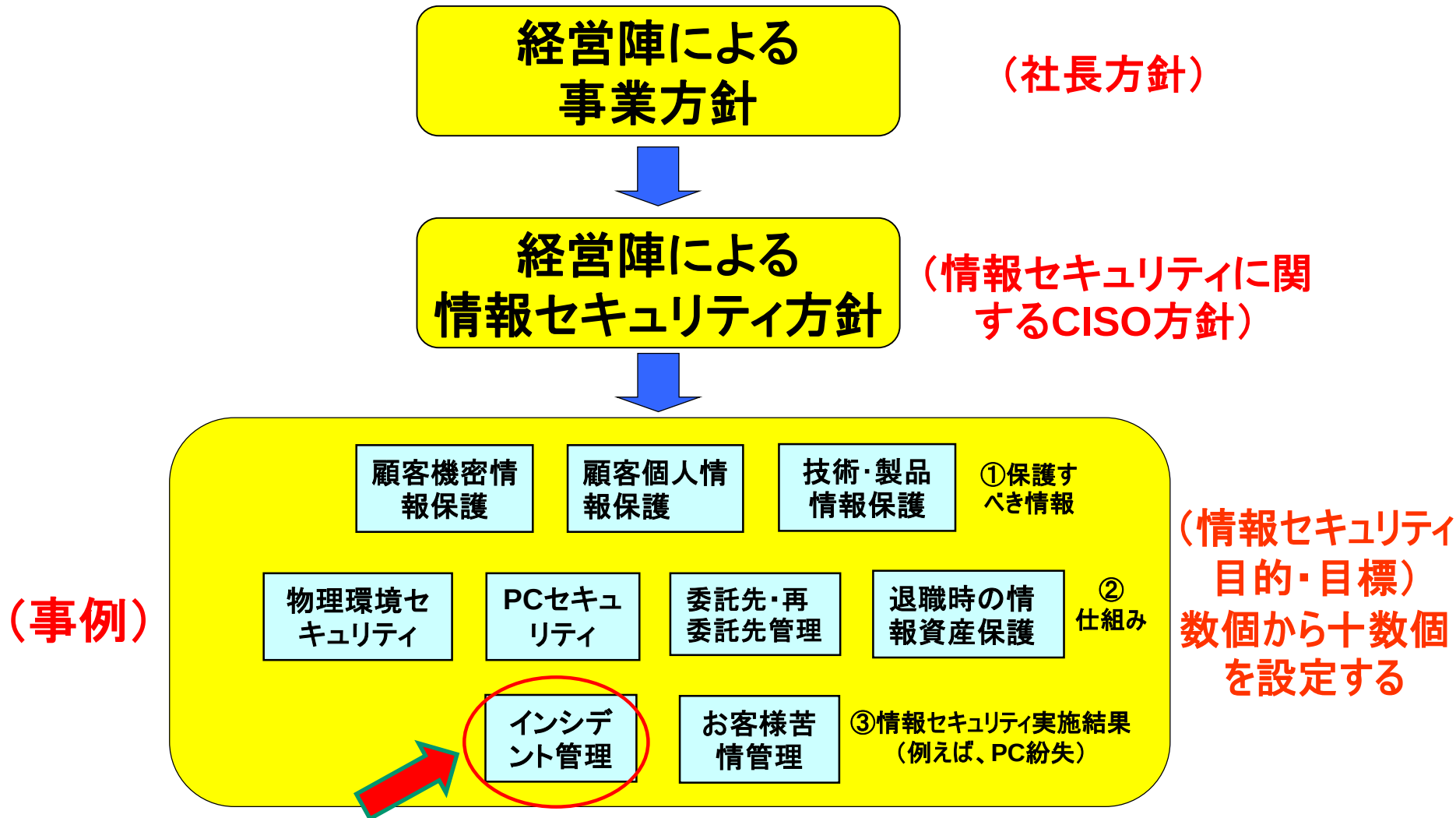
情報セキュリティ目的 (クラウドサービス)

- お客様サービス提供前に必ずSLAを締結(サービス毎に100%)

1. 実施事項
2. 必要な資源
3. 責任者
4. 達成期限
5. 結果の評価方法

(1) 情報セキュリティ目的の導入

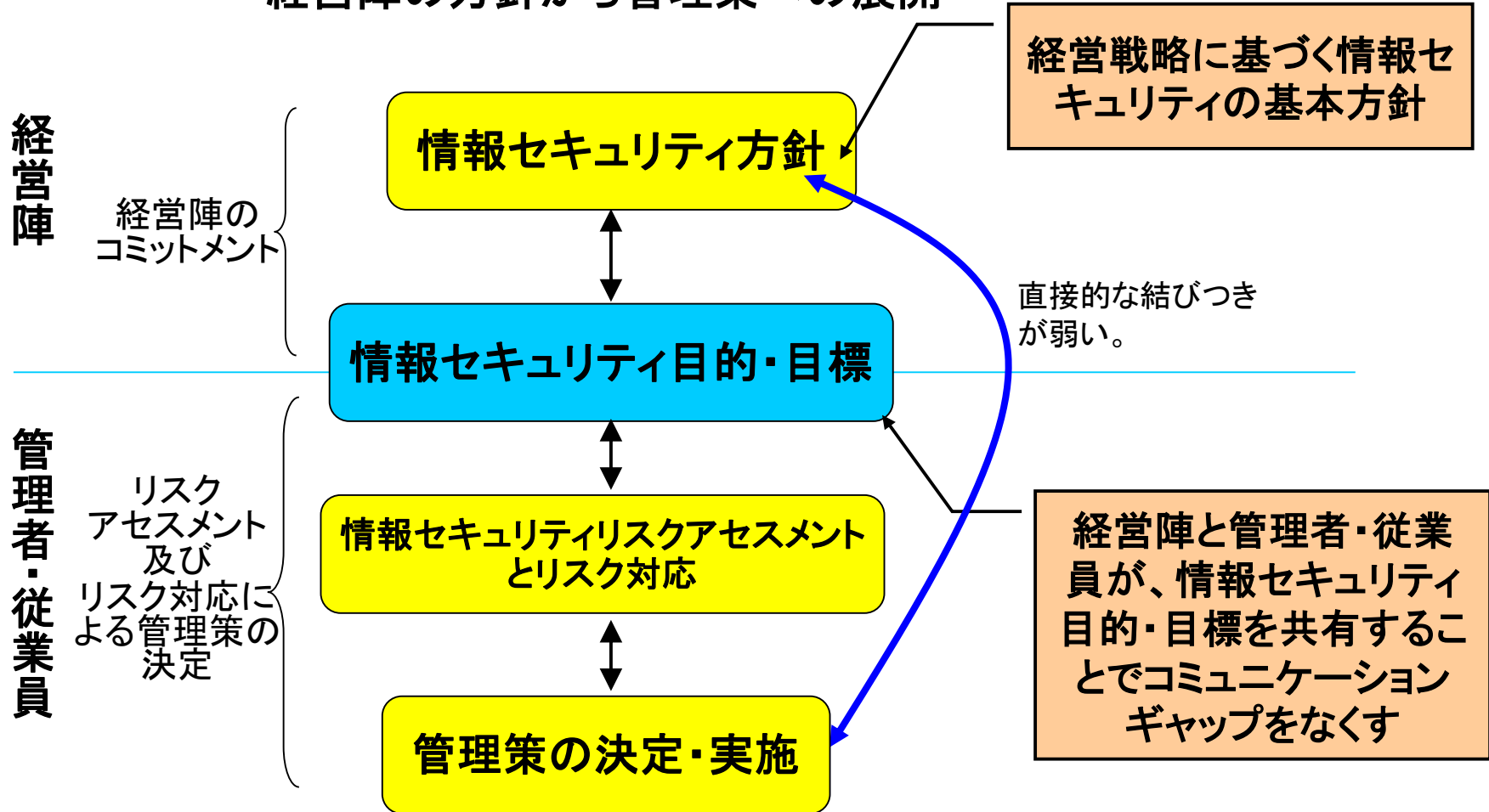
- 情報セキュリティ目的の設定の事例(目的設定の展開) -



(1) 情報セキュリティ目的の導入

- 経営陣と管理者・従業員とのパイプ役となる情報セキュリティ目的・目標の設定 -

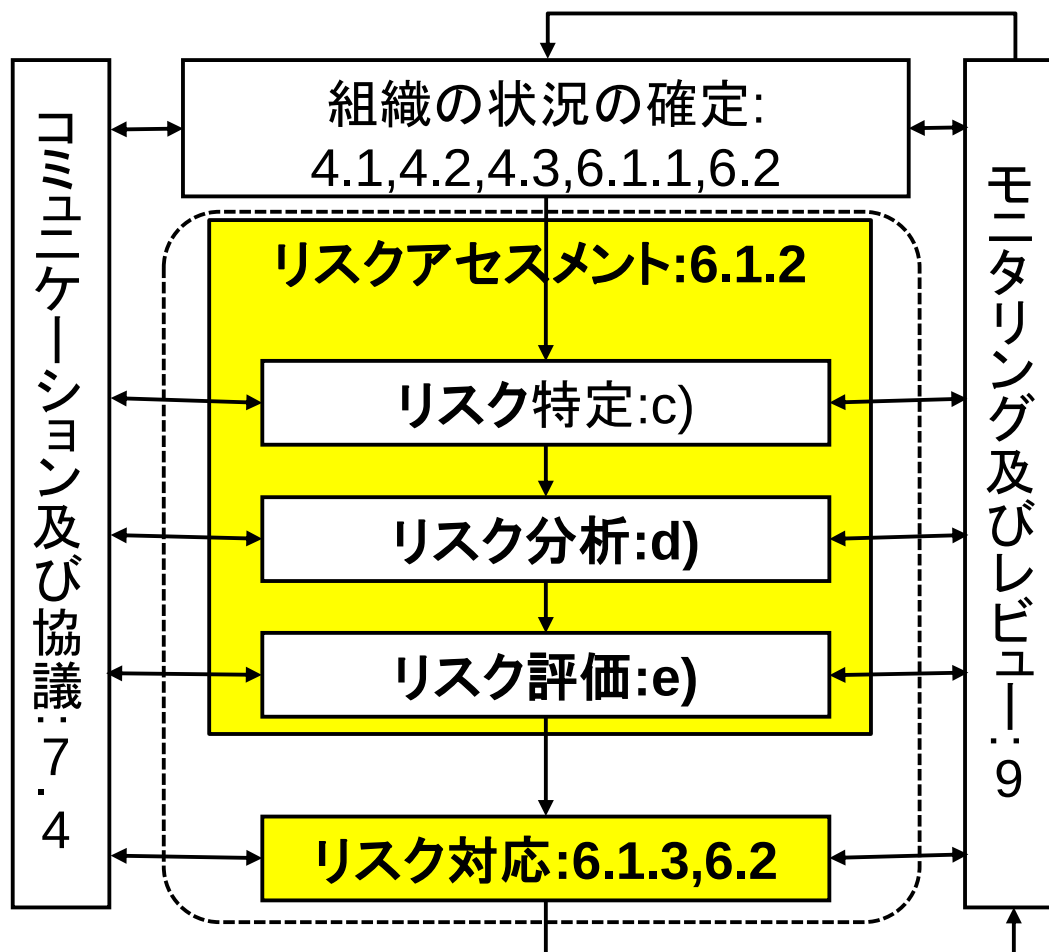
経営陣の方針から管理策への展開



(2) リスクアセスメントとリスク対応の実施

- リスク特定、リスク分析、リスク評価 -

リスクの定義＝目的に対する不確かさの影響

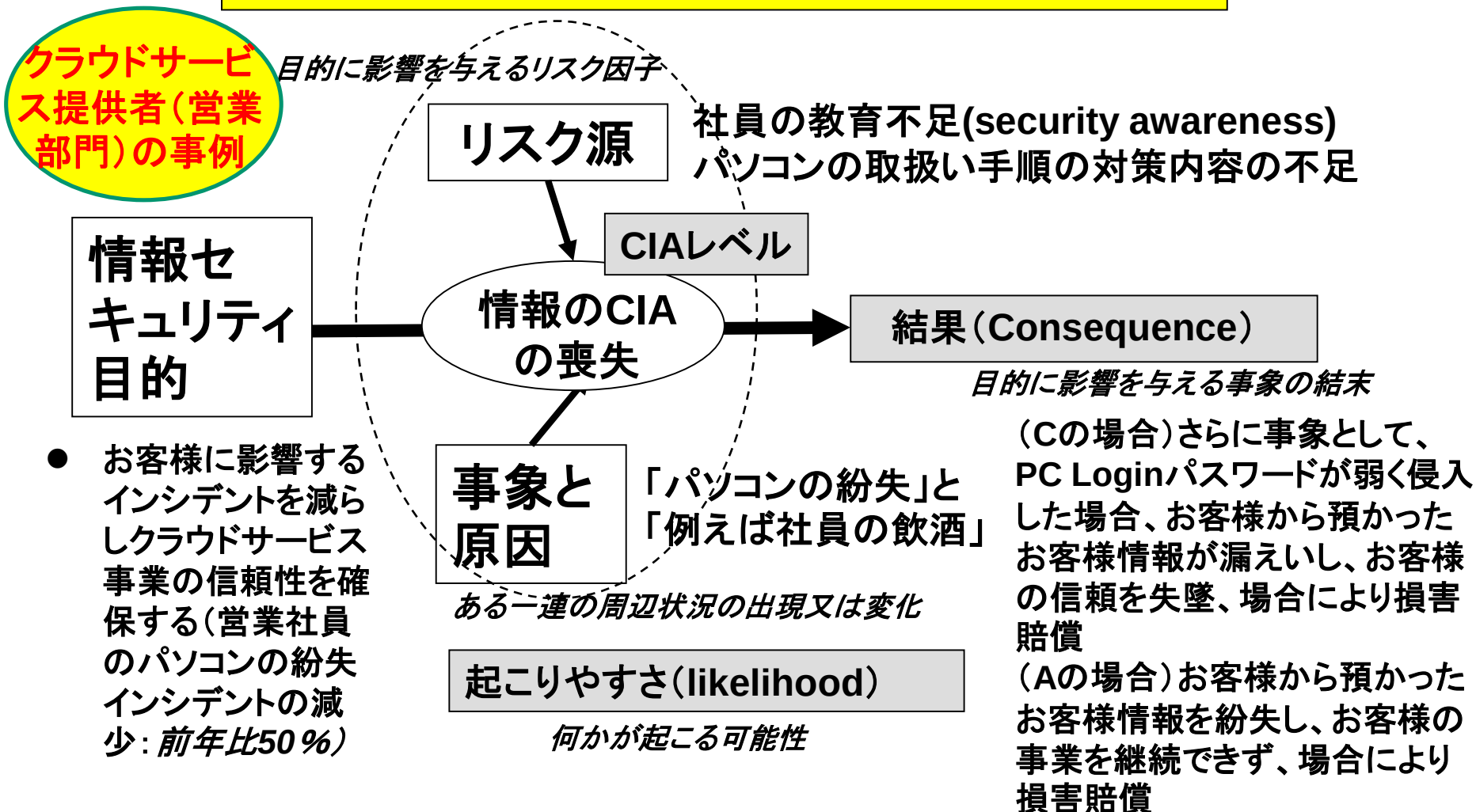


(注)
リスクマネジメント
プロセス図
(ISO/IEC31000
から引用)

(2) リスクアセスメントとリスク対応の実施

- クラウドサービス提供者(営業部門)の事例-

リスクの定義＝目的に対する不確かさの影響

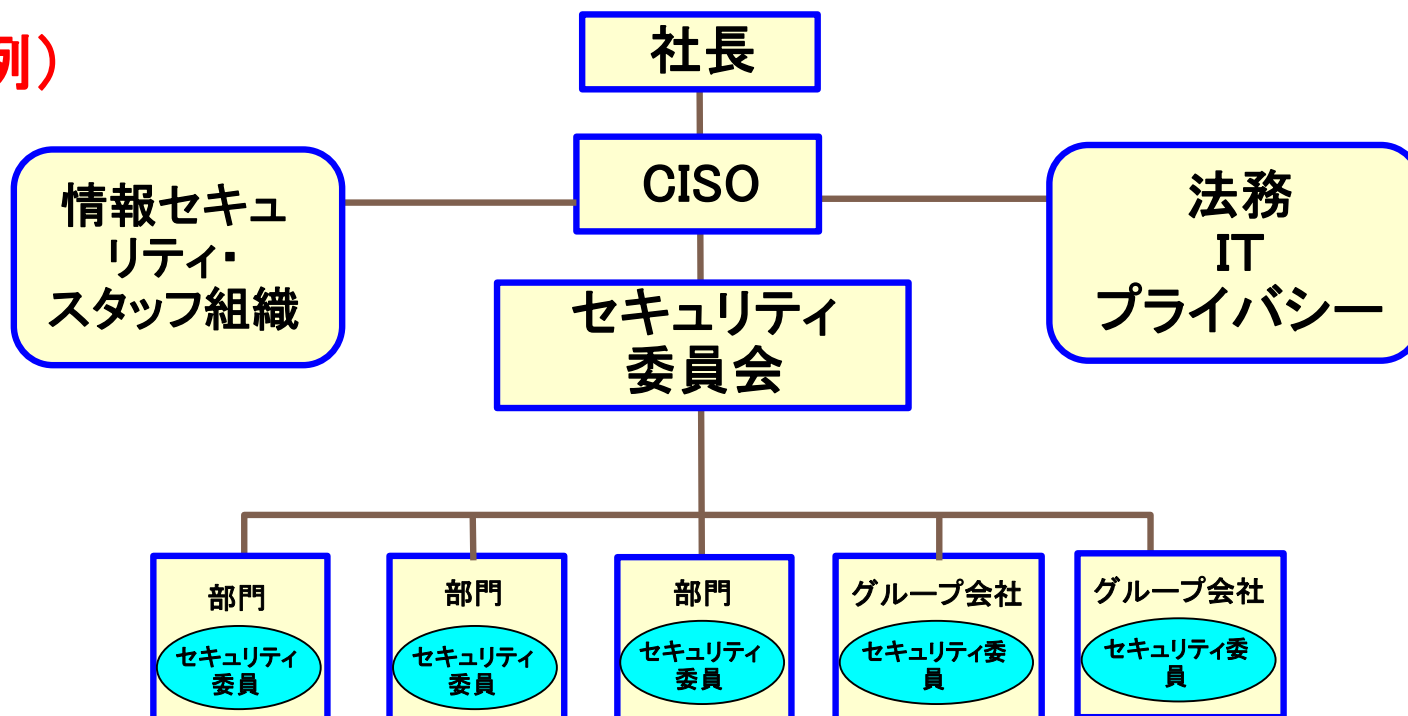


(3) 情報セキュリティの役割と責任の明確化

- 情報セキュリティの取り組み体制 -

- ① 情報セキュリティを統括するトップマネジメント(CISO)の設置
- ② 関連する物理セキュリティ・ITセキュリティ・プライバシーを統括
- ③ セキュリティ委員会は各部門及び各グループ会社から代表者(委員)を選出

(事例)



(3) 情報セキュリティの役割と責任の明確化

- グループ企業としての規定体系 -

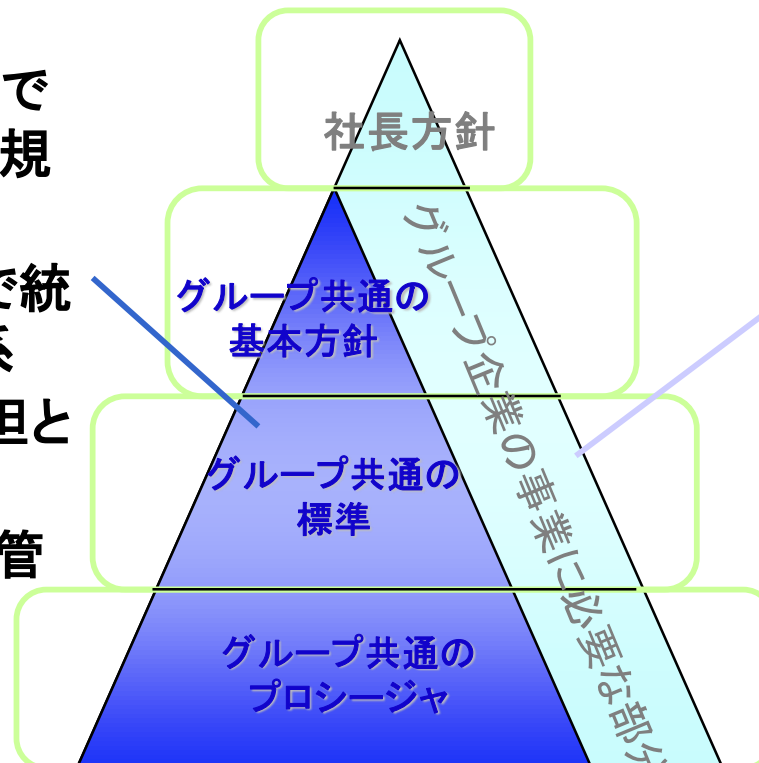
グループ企業としての規定体系を明確にする必要があります。例えば、グループ企業共通に遵守すべき規程類とグループ企業特有の規程類を、全体で整合性を取って実施します。

グループ企業全体で
共通に遵守すべき規
程類

- グループ全体で統一した管理体系
- 明確な責任分担と内部統制
- ITセキュリティ管理体系

(事例)

グループ全体のコンプライアンス行動指針



(例えば)グループにおける
一企業は、グループ企業全
体で共通に遵守すべき規程
類と整合性を取って、グルー
プ企業特有の規程を追加

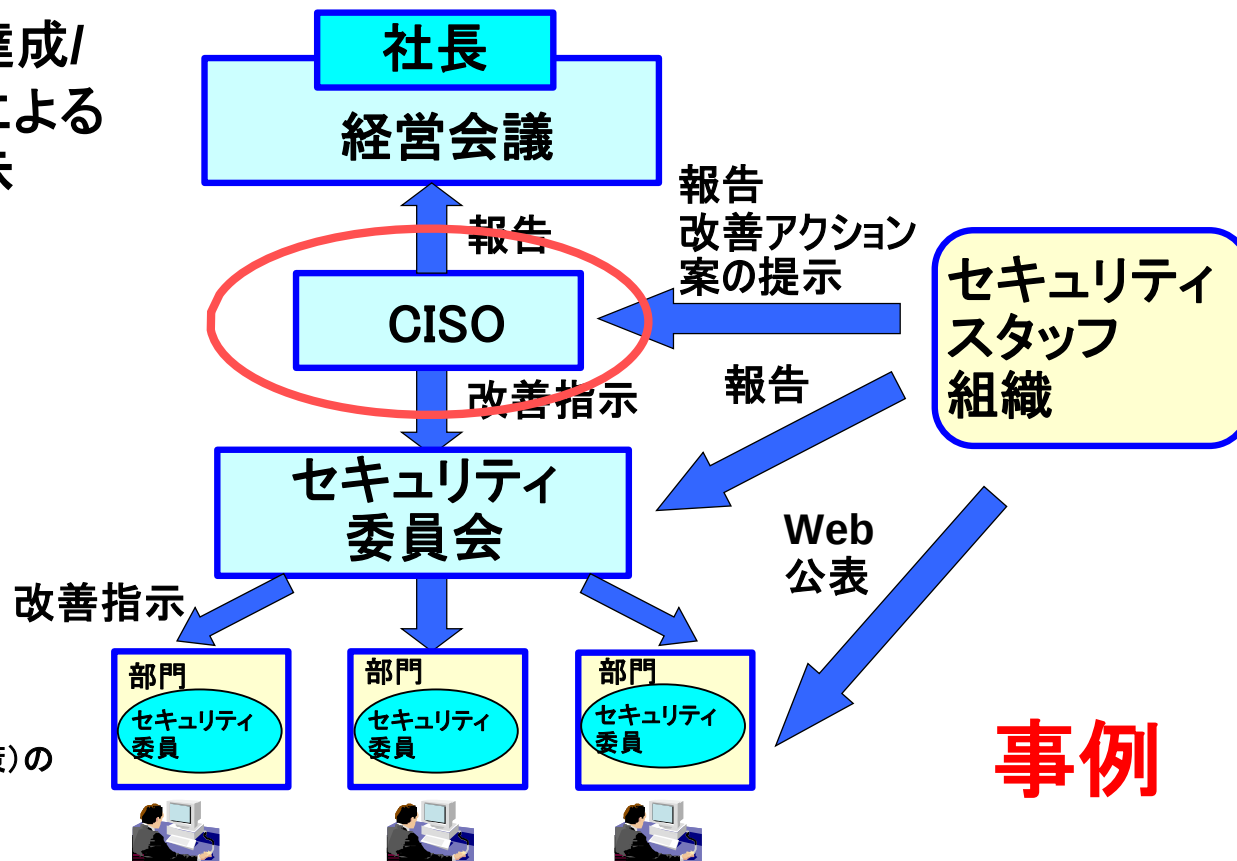
- お客様情報の保護
- 先進的なワークスタイル
- ISMSフレームワークに
基づくマネジメント

(4) 監視・測定・分析・評価の実施

- 情報セキュリティパフォーマンスとISMS有効性の評価の体制 -

経営陣から従業員まで含めた“監視、測定、分析、評価”を可能とする体制を構築することにより、セキュリティの見える化を指向した的確にセキュリティの改善アクションが取れる運用管理を実施することが要求されている。

目的の達成/
管理値による
改善指示



- 監視
- 測定
- 収集
- 計算
- 分析
- 評価
- 報告
- 改善アクションの指示
- 改善アクションの実施
- 実施しないとペナルティ

(4) 監視・測定・分析・評価の実施

- 情報セキュリティパフォーマンスとISMS有効性の評価 -

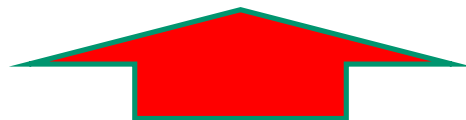
監視・測定・分析により評価する項目

1) 情報セキュリティパフォーマンス

- 不適合及び是正処置
- 監視及び測定結果
- 監査結果
- 情報セキュリティ目的の達成

2) ISMSの有効性

- 情報セキュリティ目的の達成するために計画し実施した管理策の実施状況と、情報セキュリティ目的の達成状況との比較



監視、測定、分析、評価

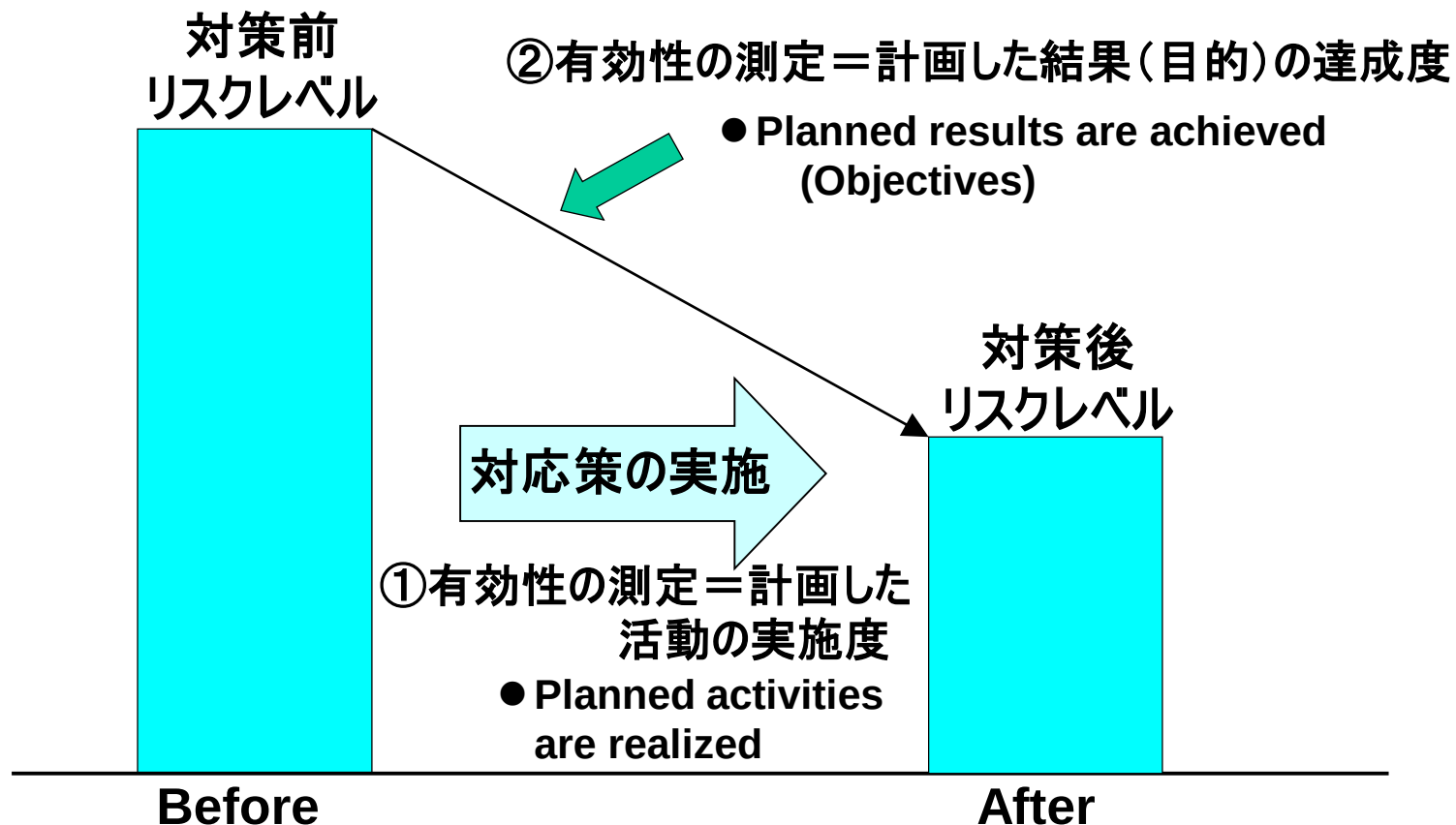
(4) 監視・測定・分析・評価の実施

- 有効性の定義、ISMSにおける有効性の評価 -

ISO/IEC27000:2014

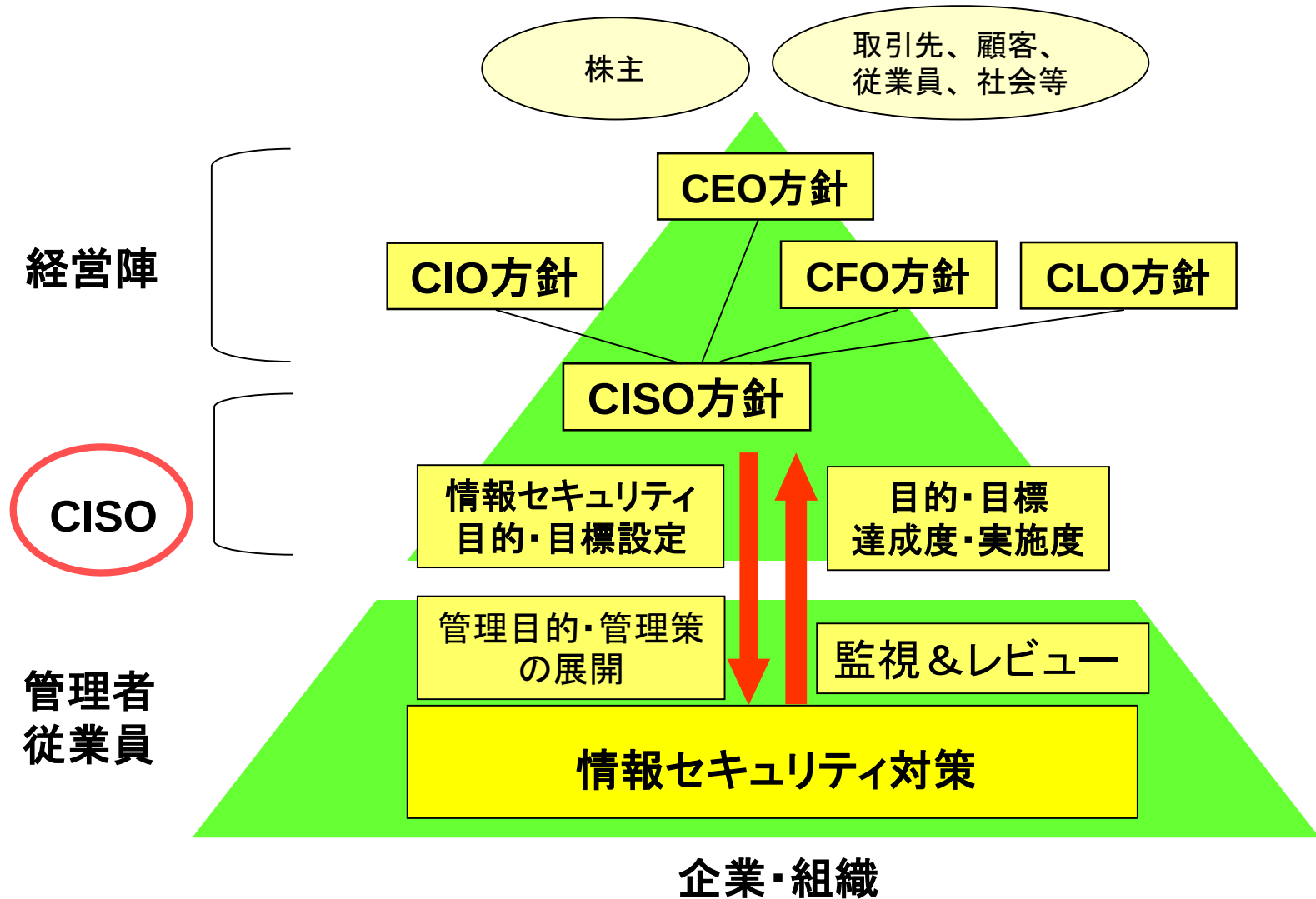
有効性の定義

計画した活動を実行し、計画した結果を達成した程度



(5) 情報セキュリティガバナンス

-組織 (Organization) を指揮 (Direct) し、統制 (Control) するCISO -



ご説明内容 – Part2 (ISO/IEC27017のころ)

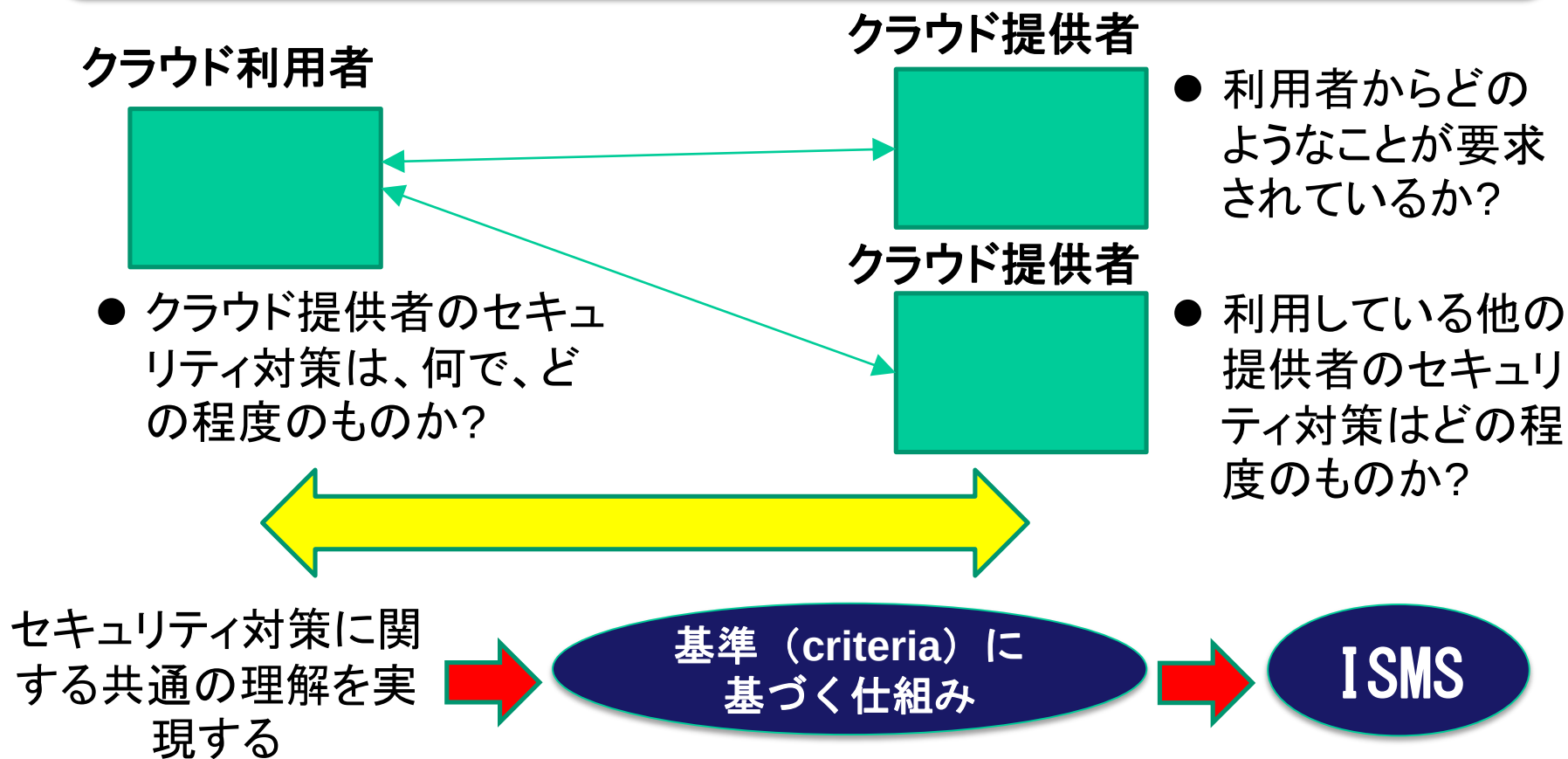


1. クラウドサービスはCSCとCSPの間で対応して実施
 - (1) 日本からの国際標準化の提案
 - (2) クラウドサービス分野別ISMS認証
 - (3) クラウドサービスのアーキテクチャ
 - (4) ISO/IEC 27017の構成
2. クラウドサービス固有は実施の手引きに記述
 - (1) クラウドサービス固有とは
 - (2) クラウドサービス固有の環境におけるリスク源
 - (3) ISO/IEC 27017の適用事例

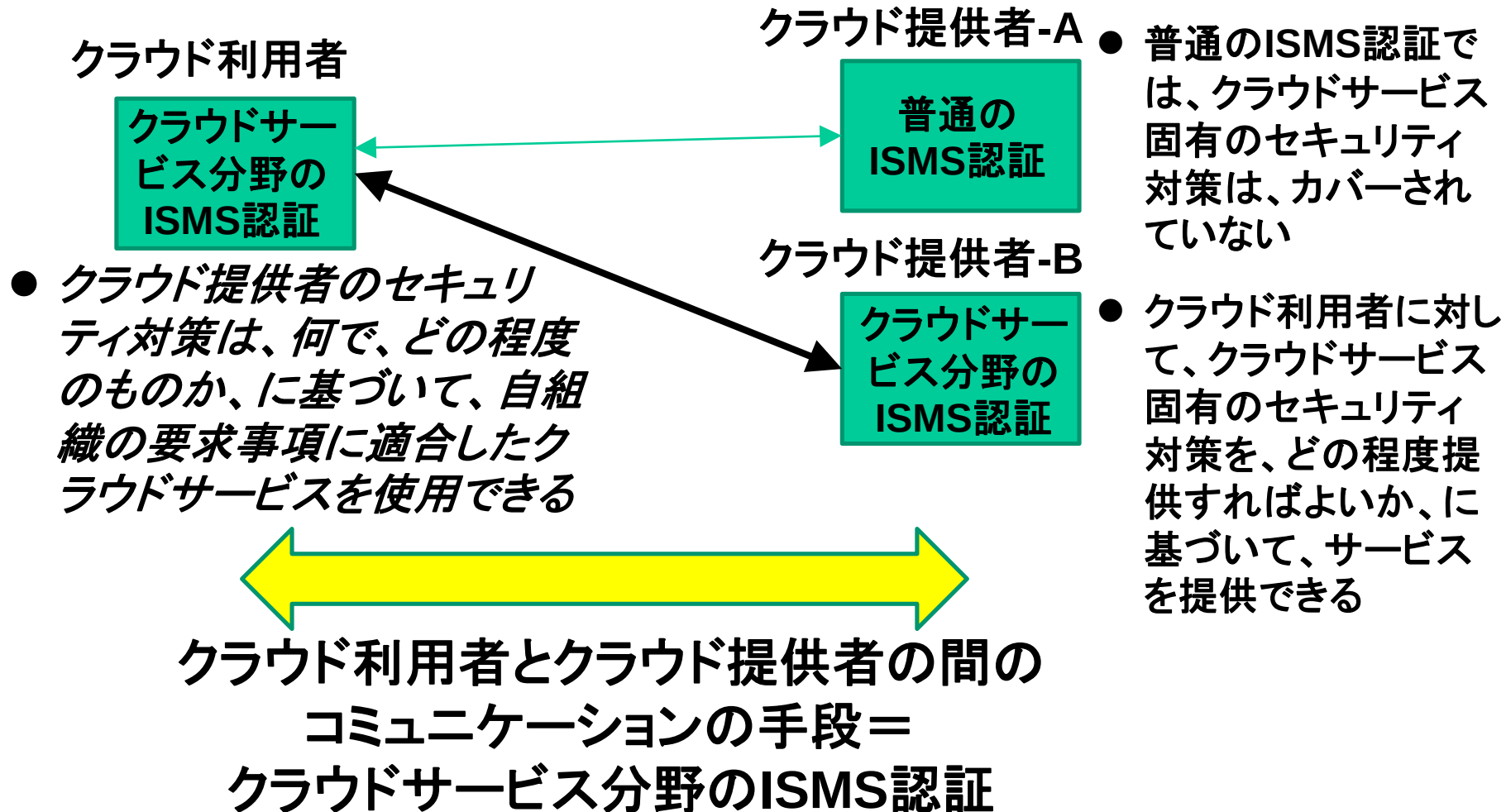
(1) 日本からの国際標準化の提案

- 基準に基づく共通の理解を得る仕組みの提案 -

クラウド利用者の課題を解決するためには、基準(Criteria)に基づいて、クラウドの利用者と提供者の間で、(国際環境において) 共通の理解を実現するための仕組みの確立が必要である



(2)クラウドサービス分野別ISMS認証



(2)クラウドサービス分野別ISMS認証

- ISMS要求事項とクラウドサービス分野の管理策 -

ISMS要求事項

ISO/IEC 27001

- ISMS要求事項 (本文)
- Annex A (based on 27002)

分野別管理策 (Sector specific controls)

27017クラウドサービス分野
別管理策および実施の手引
き (CSC+CSP)

その他の分野別管理策およ
び実施の手引き (27011
等)

➔ クラウドサービス
固有の対策

- 27017 Cloud Security Control setは、情報セキュリティリスクアセスメント、情報セキュリティリスク対応の結果、27001 Annex Aとともに、必要な管理策を決定するために参照される
- 27017は、同時に他の分野別管理策(例えば、27011)とともに、組み合わせて、使用することができる

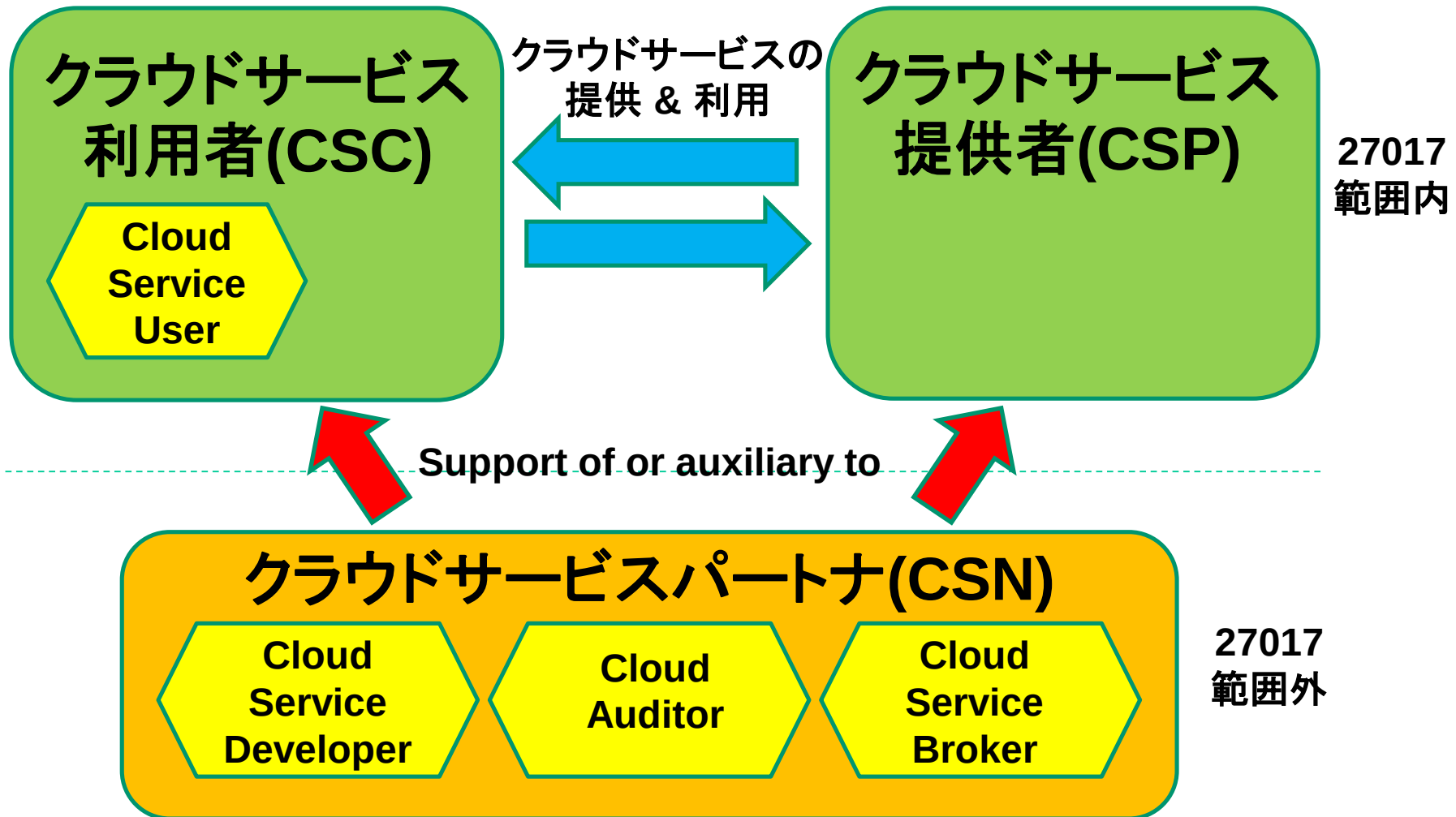


(2)クラウドサービス分野別ISMS認証

- この新規プロジェクトにより Sector specific control set standard を用いたISMS認証の制度が整備されると、次のような分野対応のISMS認証が成立することになる。
 - ISMS認証(General) : ISO/IEC 27001
 - **ISMS認証(for CSC) : ISO/IEC 27001 + 27017 (CSC)**
 - **ISMS認証(for CSP) : ISO/IEC 27001 + 27017 (CSP)**
 - ISMS認証(for Telecom): ISO/IEC 27001 + 27011
 - ISMS認証(for Telecom+CSP): ISO/IEC 27001 + 27011 + 27017(CSP)

(3) クラウドサービスのアーキテクチャ

- ISO/IEC17789:Reference architecture -





(4) ISO/IEC 27017の構成

- ISO/IEC27017とISO/IEC27002の関係 -

(1) タイトル

ISO/IEC 27002

Code of practice for information security controls

ISO/IEC 27017

Code of practice for information security controls
based on ISO/IEC 27002 for cloud services

箇条(Clauses)の関係

27002及び27017の箇条(Clauses)は、同じ

5 Information security polices

6 Organization of information security

7 Human resource security

8 Asset management

9 Access control

10 Cryptography

11 Physical and environmental security

12 Operations security (事例2. 12.3.1)

13 Communications security

14 System acquisition, development and maintenance

15 Supplier relationships

16 Information security incident management

17 Information security aspects of business continuity management

18 Compliance (事例3. 18.1.1)

Annex A (27017) Cloud Service Extended Control Set(事例1 CLD9.5.1)

(4) ISO/IEC 27017の構成

- ISO/IEC27017の構造 -

ISO/IEC 27017の構造は、Control（管理策）毎に、Implementation guidance（実施の手引き）を、テーブル形式で記述する。

a. 各Control（管理策）の様式

- Each subclause

Control X.X.X and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific implementation guidance also applies.

- Subclause header

Implementation guidance for cloud services

Other information for cloud services.

b. Implementation guidance（実施の手引き）はテーブル形式

- **Type1**

Cloud service customer	Cloud service provider
Implementation guidance	Implementation guidance

→ CSCとCSPは
対応して実施

- **Type2**

Cloud service customer	Cloud service provider
Implementation guidance	

→ CSCとCSPの実
施内容が同一

c. Annex A (Cloud Service Extended Control Set)

- 27017 uses 'CLD. X.X.X'

ご説明内容 – Part2 (ISO/IEC27017のころ)

1. クラウドサービスはCSCとCSPの間で対応して実施
 - (1) 日本からの国際標準化の提案
 - (2) クラウドサービス分野別ISMS認証
 - (3) クラウドサービスのアーキテクチャ
 - (4) ISO/IEC 27017の構成



2. クラウドサービス固有は実施の手引きに記述
 - (1) クラウドサービス固有とは
 - (2) クラウドサービス固有の環境におけるリスク源
 - (3) ISO/IEC 27017の適用事例

(1) クラウドサービス固有（specific）とは

ISO/IEC 27017審議過程で、管理策および実施の手引きがクラウドサービス固有（Specific）と判断できる環境として、以下の環境を考慮することとした。同様の内容が、他のNBからも提案された。

1. コンピューティング資源の一部を共有し、その上に個々の利用者が管理するシステムが構築されるなど、提供者と利用者関係が緊密かつ複雑である。（事例2）
2. クラウドコンピューティングサービスは、その提供の仕組みの詳細を利用者が知ることがなくても手軽に利用できる半面、利用者にブラックボックスとなっている。
3. オンプレミスとクラウドコンピューティングサービス、あるいはクラウドコンピューティングサービスと他のクラウドコンピューティングサービスの併用など、多様な利用があり、それらの間の整合性が取りにくい。（事例1）
4. 膨大な利用者が一つの資源を共有している。
5. 仮想化技術を幅広く取り入れており、その結果として、一瞬にして環境が変わる（数千台のサーバが一瞬に消えるなど）。
6. 論理環境と物理環境が多様に入り組んだ複雑で巨大なコンピュータシステムである。
7. 資源がグローバルに分散配置されている。
8. クラウドコンピューティングサービス上に他のクラウドコンピューティングサービスが行われるなど、クラウドを組み合わせたサービスが存在する。

(2) クラウドサービス固有（specific）の環境におけるリスク源（事例：Annex B参照）

	クラウド利用者	クラウド提供者
リスク源	● Loss of governance ● Responsibility ambiguity ● Isolation failure ● <u>Vendor lock-in（事例1）</u> ● Compliance and legal risks ● Handling of security incidents ● Management interface vulnerability ● Data protection ● Malicious behaviour of insiders ● Business failure of the provider ● Service unavailability ● Migration and integration failures ● Evolutionary risks ● Cross-border issues ● Insecure or incomplete data deletion	● Responsibility ambiguity ● Inconsistency and conflict of protection mechanisms ● <u>Isolation failure（事例2）</u> ● Unauthorized access to the provider's systems. ● Jurisdictional conflict ● Insider Threats ● Supply Chain vulnerability

(3) 事例1：リスクの特定の手順

- 事例1（事象及びその原因：CSCデータ破壊によるシステム停止, リスク源：開発業者ロックイン（lock-in）、結果：システム停止後、再開できない）

考え方
(事例)

リスクアセス
メント対象

事象 及び
その原因

リスク源

結果

- 事例：異なるサービス間の整合性

(注)

リスクの特定は、
各組織の情報セ
キュリティ目的の
下で実施される

- 事例：データ破壊(CSC)及びシステム停止（CSC）。データ破壊がシステム停止に直結。

- 事例：開発業者の lock-in

- 取得していたバックアップが使用できず、システム停止後、再開できない



データ破壊が発生

当該クラウドの使用を中止して別システム（例えば別クラウド、又は自社システム）に移行。取っていたバックアップデータを使用しようとしたが、lock-inのため、使用できない（システム停止による運用の継続ができない）

開発
業者

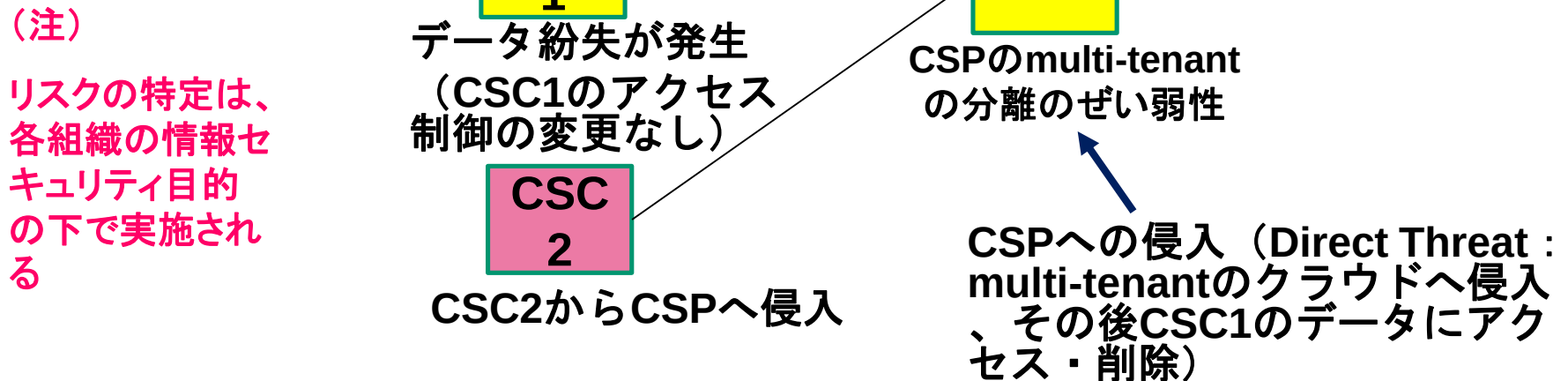
直接クラウドに属さないソフト開発業者がlock-inの場合

事例2：リスクの特定の手順

参照：事例1.（クラウドコンピューティング）

- 事例2（事象及びその原因: Loginを通過してCSPへの侵入、リスク源: CSPのmulti-tenantの分離のぜい弱性、結果：CSC1のデータ紛失）

考え方 (事例)	リスクアセス メント対象	事象 及び その原因	リスク源	結果
	● 事例：コンピューティング資源の一部共有	● 事例：CSC2からCSPへの侵入、及びCSC2から悪意の運用管理によりCSC1へのデータアクセス・紛失	● 事例：CSP multi-tenantの分離のぜい弱性（不完全さ）	● 事例：CSC1のデータにアクセスされデータが削除、その結果、信頼性喪失



補足（１） ISO/IEC27017の実施の手引き一覧表

箇条（Clause）	CSC	CSC/CSP	CSP	Subclause計
5	1		1	2
6	2		2	7
7	1		1	6
8	2		2	10
9	5		6	14
10	2		1	2
11	1		1	15
12	7		6	14
13	1		1	7
14	2		2	13
15	2		2	5
16	2	1	2	7
17				4
18	5		5	8
Total	33	1	32	114

補足（2）ISO/IEC27017の追加管理策一覧表

管理策番号	CSC	CSP	管理策の内容	リスク源
CLD.6.3.1	1	1	Shared responsibility	Compliance and legal risks Malicious behavior of insiders
CLD.8.1.5	1	1	Removal of assets	Responsibility of ambiguity Data protection
CLD.9.5.1	1	1	Segregation in virtual computing environments	Isolation failure
CLD.9.5.2	1		Virtual machine hardening	Inconsistency and conflict of protection mechanism Isolation failure
CLD.12.1.5	1	1	Critical operations	Evolutionary risks Insecure or incomplete data deletion
CLD.12.4.5	1	1	Monitoring cloud services	Data protection
CLD.13.1.4	0	1	Consistent virtual and physical networks	Inconsistency and conflict of protection mechanism



今後の発行に向けたプロセス

ITU-T X.1631 | ISO/IEC 27017

- 05/12/2015 Approved going to FDIS (SC27)
- 06/16-07/13/2015 Approved (ITU-T)
- 07/31-10/01/2015 FDIS balloting (JTC1)
- 10 or 11/2015 ISO/IEC 27017 to be Published
- 04/2015- Working for JISQ27017



おわりに

ご清聴有難うございました。

工学院大学情報学部

ISO/IEC JTC1/SC27/WG1国内主査

ISO/IEC 27017 Project Editor

クラウドセキュリティコントロール専門委員会委員長

山崎 哲