2016/12/08

クラウドサービスにおけるISO/IEC27017を適用した情報セキュリティマネジメントシステムの実践

工学院大学情報学部

ISO/IEC JTC1/SC27/WG1国内主査

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

山﨑　哲

ご説明内容

1. クラウドサービスにおける情報セキュリティマネジメントシステムを推進する動力

2. クラウドサービスにおける２つの組織の情報セキュリティマネジメントシステムを動かす５つの動力

(1) 動力１：クラウドサービスカスタマ/プロバイダの情報セキュリティの役割と責任の明確化

(2) 動力２：クラウドサービスカスタマ/プロバイダの情報セキュリティ目的の設定

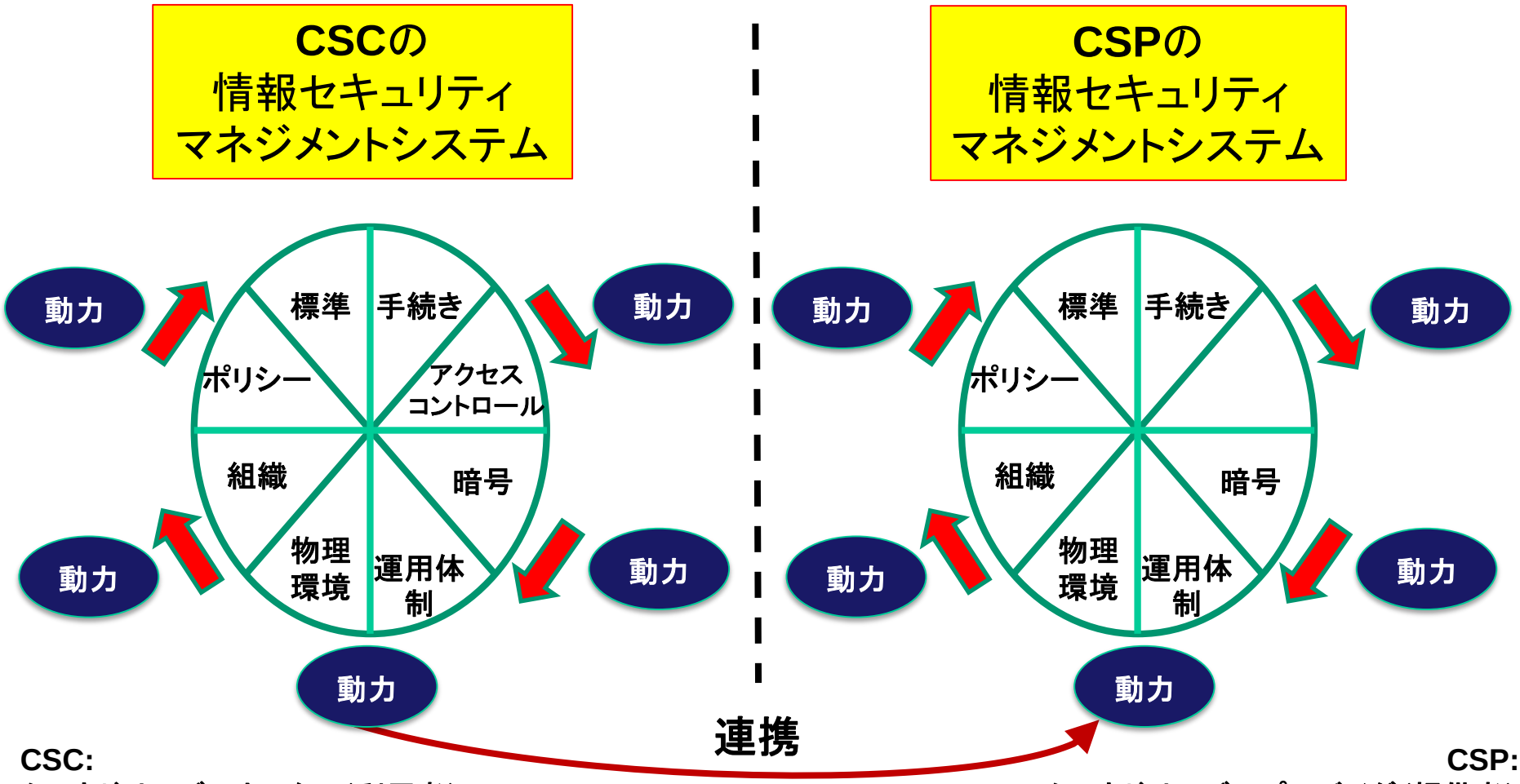
(3) 動力３：クラウドサービス利用/提供におけるリスクアセスメントとリスク対応の実施

(4) 動力４：クラウドサービス利用/提供における監視・測定・分析・評価の実施

(5) 動力５：クラウドサービスカスタマ/プロバイダの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。
CSCとCSPの「情報セキュリティマネジメントシステムの動力」はお互いに連携して働きます。

車＝情報セキュリティマネジメントシステムの要素

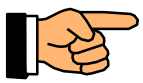


CSC:
クラウドサービスカスタマ（利用者）

CSP:
クラウドサービスプロバイダ（提供者）

ご説明内容

1. クラウドサービスにおける情報セキュリティマネジメントシステムを推進する動力



2. クラウドサービスにおける２つの組織の情報セキュリティマネジメントシステムを動かす5つの動力

(1) 動力１:クラウドサービスカスタマ/プロバイダの情報セキュリティの役割と責任の明確化

(2) 動力２:クラウドサービスカスタマ/プロバイダの情報セキュリティ目的の設定

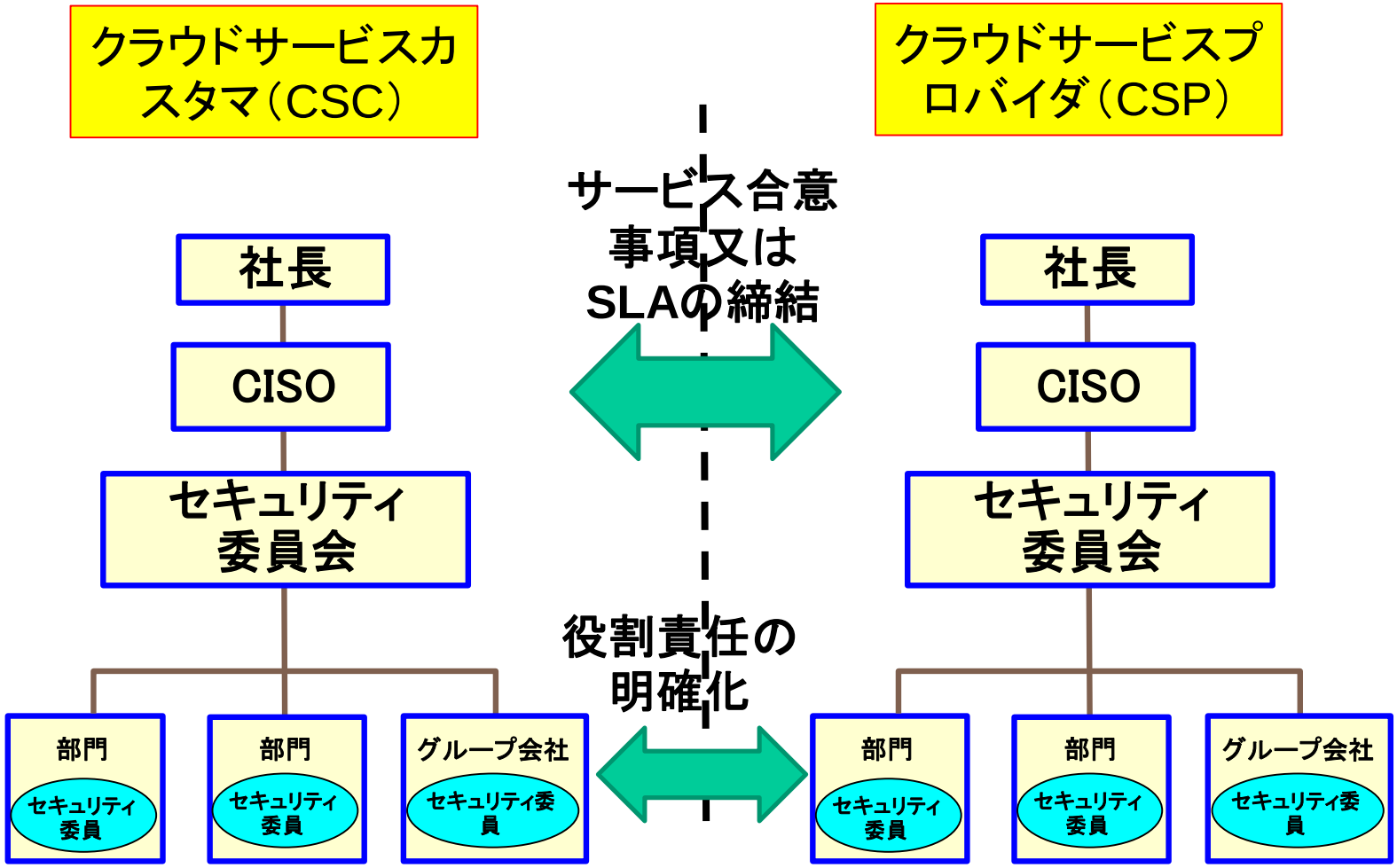
(3) 動力３:クラウドサービス利用/提供におけるリスクアセスメントとリスク対応の実施

(4) 動力４:クラウドサービス利用/提供における監視・測定・分析・評価の実施

(5) 動力５:クラウドサービスカスタマ/プロバイダの情報セキュリティガバナンス

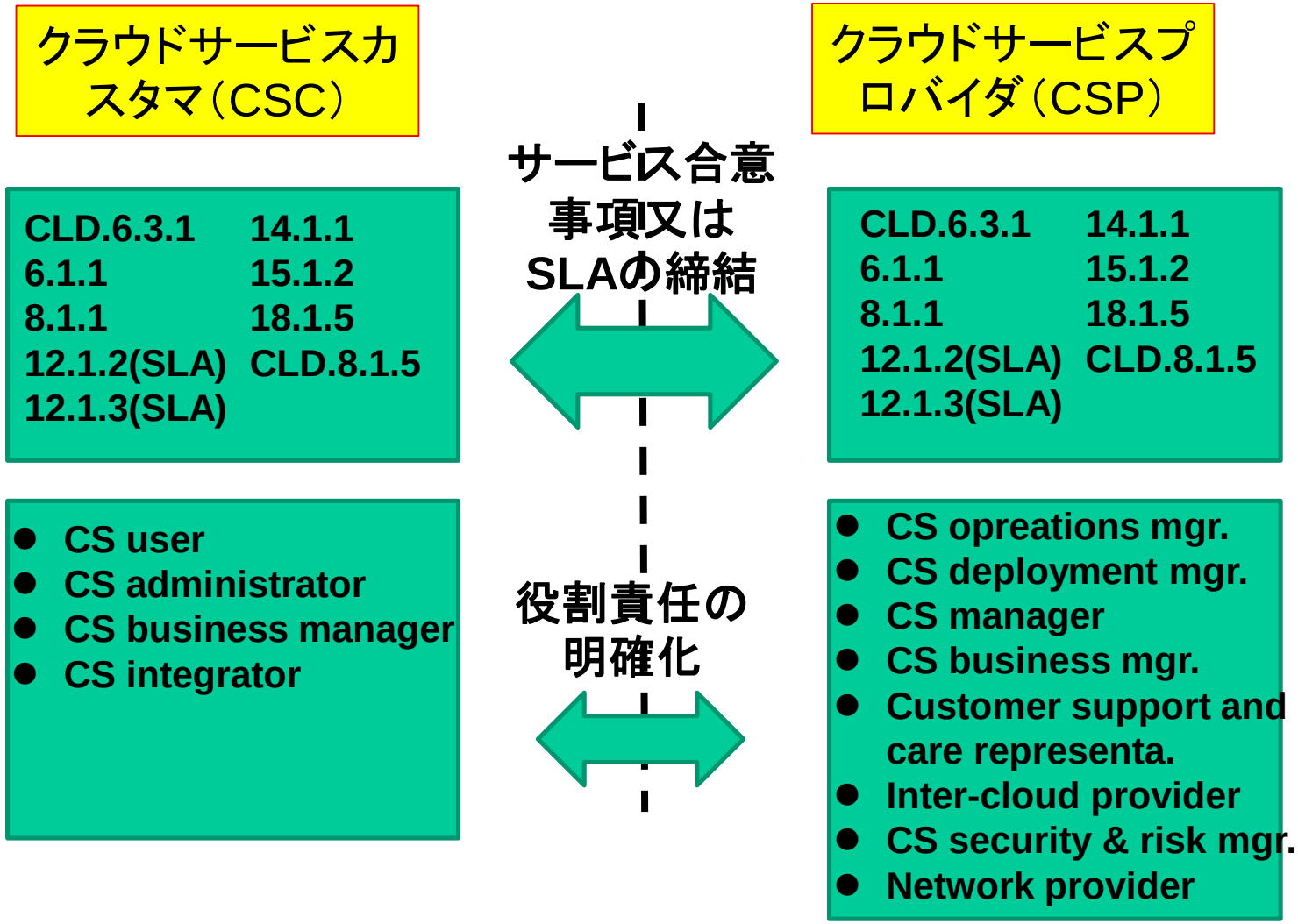
(1) 動力1：クラウドサービスカスタマ/プロバイダの情報セキュリティの役割と責任の明確化

- 情報セキュリティの取り組み体制 -



(1) 動力1：クラウドサービスカスタマ/プロバイダの情報セキュリティの役割と責任の明確化

- Agreements and Roles & Responsibilities -



事例：ISO/IEC27017の箇条（本文 CLD.6.3.1）

- クラウドサービスカスタマ向け実施の手引の例
  - CLD.6.3.1 クラウドコンピューティング環境における役割及び責任の分担

    管理策

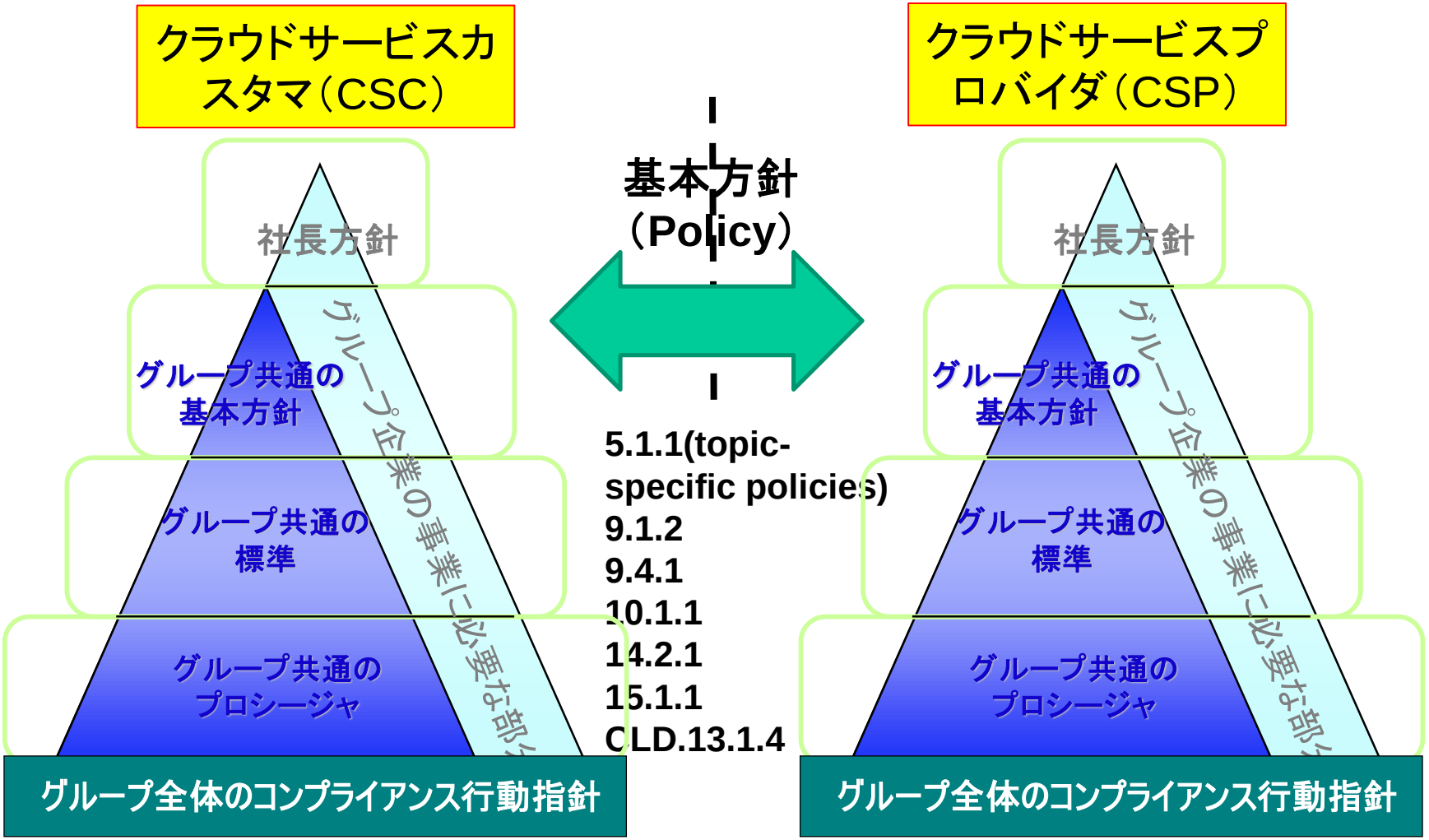
    クラウドサービスの利用において共有する情報セキュリティの役割を遂行する責任は、クラウドサービスカスタマ及びクラウドサービスプロバイダのそれぞれにおいて*特定の関係者に割り当て、文書化し、伝達し、実施する*ことが望ましい。

    クラウドサービスのための実施の手引

クラウドサービカスタマ	クラウドサービスプロバイダ
クラウドサービスカスタマは，*クラウドサービスの利用にあわせて方針及び手順を定義又は追加*し，クラウドサービスユーザにクラウドサービスの利用における*自らの役割及び責任を意識*させることが望ましい。	クラウドサービスプロバイダは，自らの*情報セキュリティの能力，役割及び責任を文書化し伝達する*ことが望ましい。併せて，クラウドサービスプロバイダは，*クラウドサービスの利用の一部としてクラウドサービスカスタマが実施及び管理することが必要となる情報セキュリティの役割及び責任を，文書化し伝達*することが望ましい。

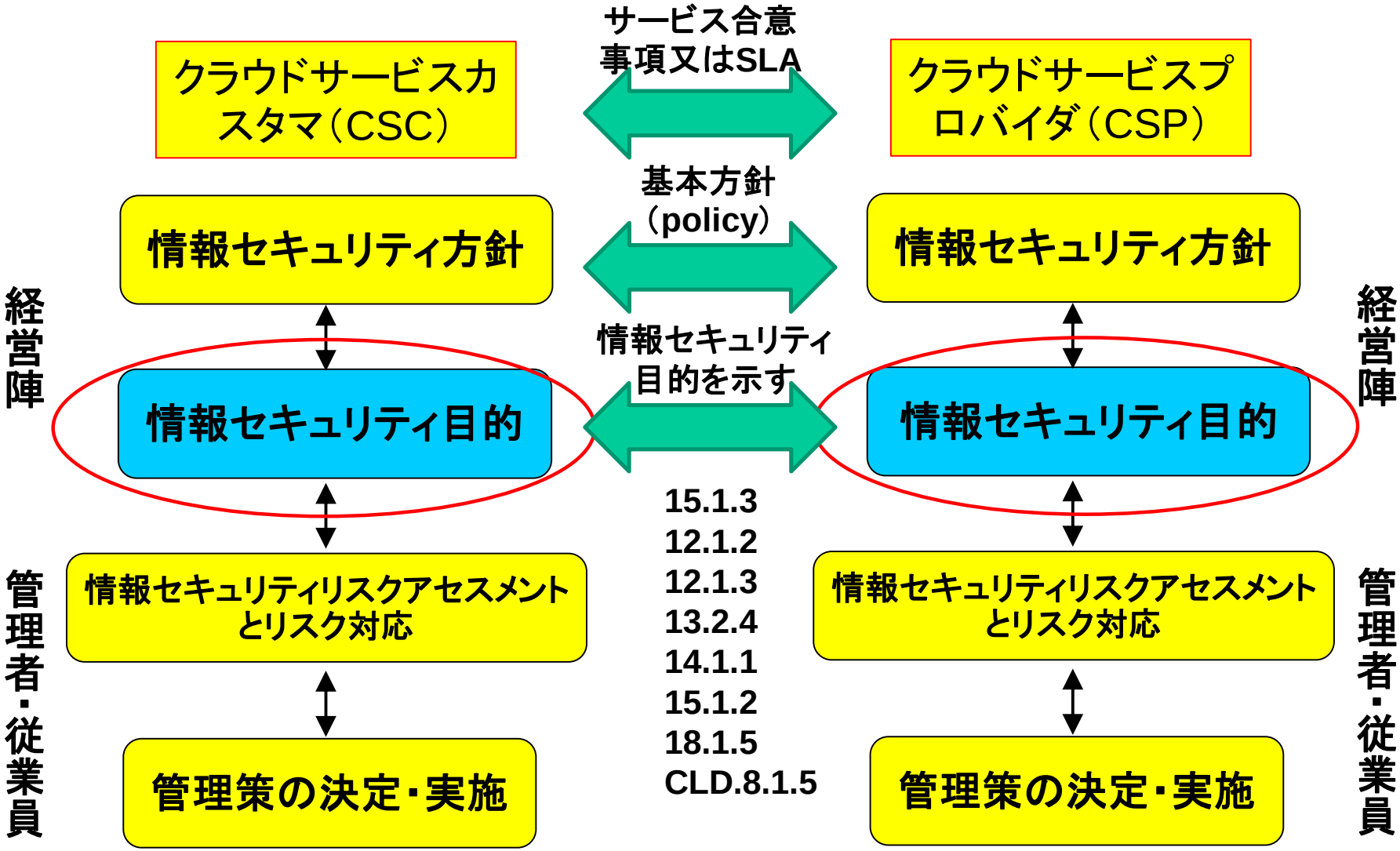
(1) 動力1：クラウドサービスカスタマ/プロバイダの情報セキュリティの役割と責任の明確化

- 組織の規定体系 -



(2)動力2:クラウドサービスカスタマ/プロバイダの情報セキュリティ目的の設定

- 情報セキュリティ目的はセキュリティ対策の原点です -



(2)動力2:クラウドサービスカスタマ/プロバイダの情報セキュリティ目的用者の設定

- 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）

クラウドサービスプロバイダの事例

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%*）

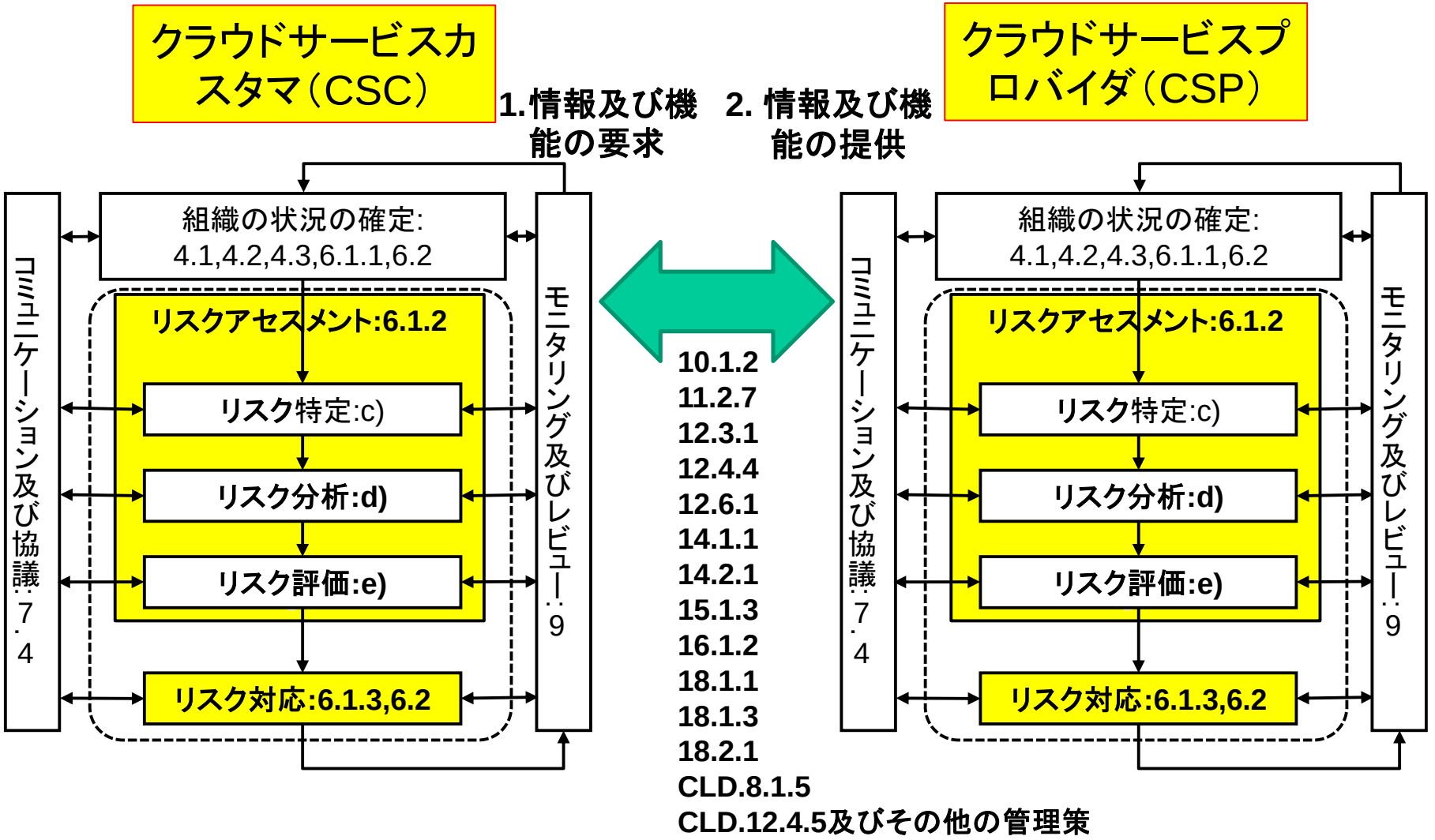
クラウドサービスプロバイダのデータセンターの事例

15.1.3 ICT supply chain

情報セキュリティ目的(営業部門)	情報セキュリティ目的(データセンター)	情報セキュリティ目的(クラウドサービス)
● 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％）*	● 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％）*	● 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. 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. 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

(3) 動力3：クラウドサービス利用/提供におけるリスクアセスメントとリスク対応の実施

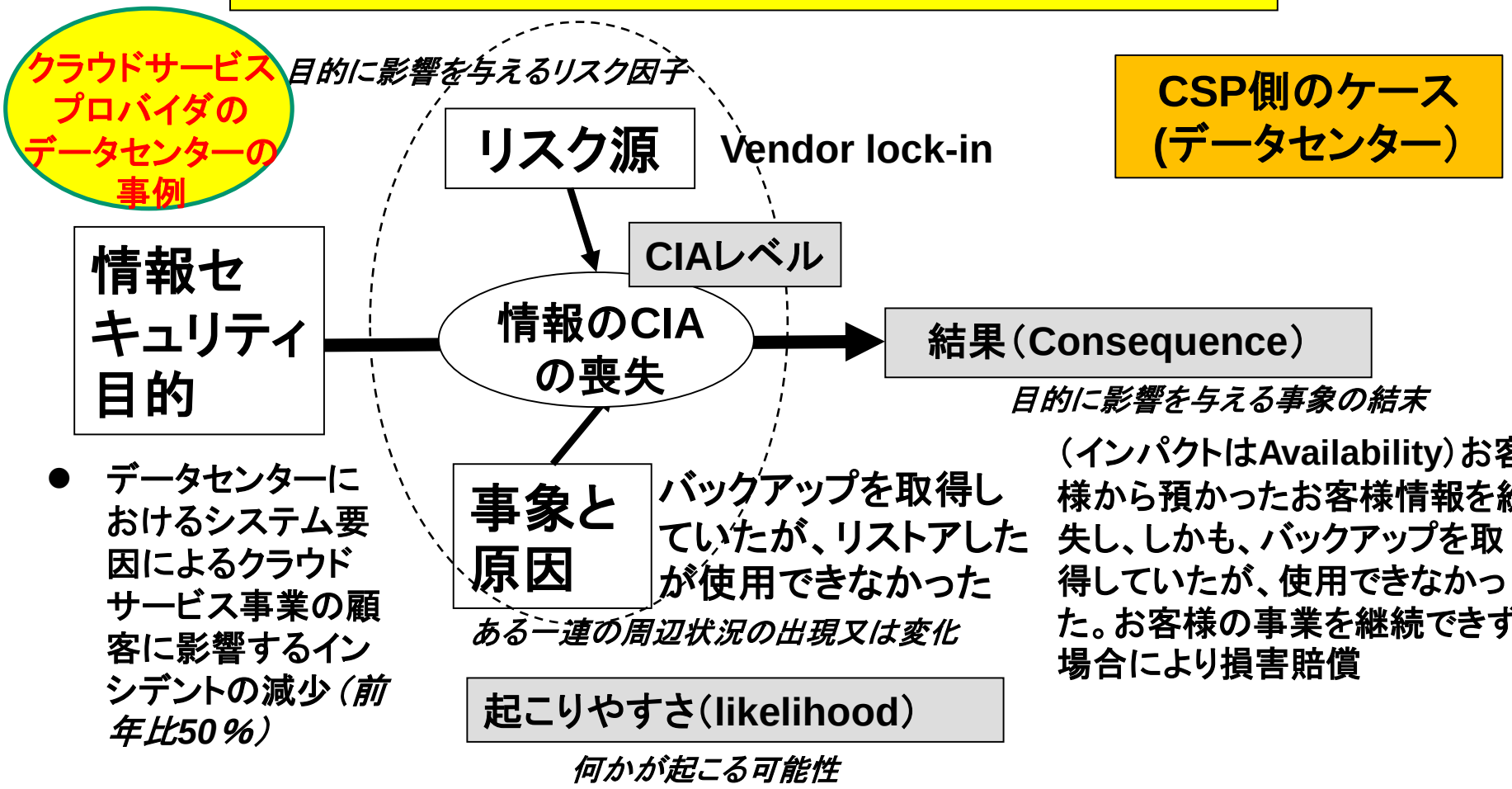
- リスク特定、リスク分析、リスク評価-



(3) 動力3：クラウドサービス利用/提供におけるリスクアセスメントとリスク対応の実施

- クラウドサービスプロバイダ（データセンター）の事例-

リスクの定義＝目的に対する不確かさの影響



- データセンターにおけるシステム要因によるクラウドサービス事業の顧客に影響するインシデントの減少（*前年比50％*）

（インパクトはAvailability）お客様から預かったお客様情報を紛失し、しかも、バックアップを取得していたが、使用できなかった。お客様の事業を継続できず、場合により損害賠償

(3) 動力3:クラウドサービス利用/提供におけるリスクアセスメントとリスク対応の実施

- リスクアセスメント及びリスク対応のCSCからCSPの連携の事例-

CSC/CSP	クラウドサービスカスタマ（CSC）	提携	クラウドサービスプロバイダ(データセンター)(CSP)
情報セキュリティ目的	サービスの使用可能性(Availability)を基準(Criteria)以上とする		システム要因によるクラウドサービス事業の顧客に影響するインシデントの減少
リスクアセスメント対象	異なるサービス間の整合性（データ破壊したクラウドの使用を中止して別システムに移行。取っていたバックアップデータを使用して、システムの継続を実施）		
事象	①データ破壊に依るシステム停止。③バックアップデータを使用を試みたが使用できなかった	⇔	②CSCにバックアップデータを提供した。④（CSCよりの連絡）CSCのシステムで、利用できない
リスク源	アクセス制御不備、バックアップテストの未テスト	⇔	バックアップデータに、特定の開発業者のソフトウェアを含んでいる(Vendor lock-in)
結果	CSCがシステムの使用ができず、結果的にサービスの利用停止となった。		CSPが提供するシステムにおいてシステム停止が発生し、再開ができない。

クラウドサービス固有（specific）のリスクアセスメントの対象に潜むリスク源

	クラウドサービスカスタマ（CSC）	クラウドサービスプロバイダ（CSP）
リスク源	● Loss of governance ● Responsibility ambiguity ● Isolation failure ● ***Vendor lock-in*** ***（事例4）*** ● Compliance and legal risks ● Handling of security incidents ● Management interface vulnerability ● Data protection ● Malicious behaviour of insiders ● Business failure of the provider ● ***Service unavailability*** ***（事例2）*** ● Migration and integration failures ● Evolutionary risks ● Cross-border issues ● Insecure or incomplete data deletion	● Responsibility ambiguity ● Inconsistency and conflict of protection mechanisms ● ***Isolation failure*** ***（事例1）*** ● Unauthorized access to the provider's systems. ● ***Jurisdictional conflict*** ***（事例3）*** ● Insider Threats ● ***Supply Chain vulnerability*** ***（事例5）***

事例：ISO/IEC27002の箇条（本文 12.3.1）

- クラウドサービスカスタマ/プロバイダ向け実施の手引の例
  - 27002: 12.3.1 情報のバックアップ
    - 管理策

      情報，ソフトウェア及びシステムイメージのバックアップは，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。

      ➔ 27017には、記述されませんが、この内容が、適用の対象となります
    - 実施の手引

      バックアップ方針を確立し，情報，ソフトウェア及びシステムイメージのバックアップに関する組織の 要求事項を定めることが望ましい。バックアップ方針では，保管及び保護に関する要求事項を定めることが望ましい。災害又は媒体故障の発生の後に，全ての重要な情報及びソフトウェアの回復を確実にするために，適切 なバックアップ設備を備えることが望ましい。バックアップ計画を策定するときは，次の事項を考慮に入れることが望ましい。

      a) バックアップ情報の正確かつ完全な記録及び文書化したデータ復旧手順を作成する。

      b) ・・・・・・

事例：ISO/IEC27017の箇条（本文 12.3.1）

- クラウドサービスカスタマ向け実施の手引の例
  - 27017: 12.3.1 情報のバックアップ

JIS Q 27002の12.3.1に定める管理策並びに付随する実施の手引及び関連情報を適用する。次のクラウドサービス固有の実施の手引も適用する。

クラウドサービスのための実施の手引

クラウドサービス固有の導入の手引き

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がクラウドサービスの一部としてバックアップ機能を提供する場合は，クラウドサービスカスタマは，***クラウドサービスプロバイダにバックアップ機能の仕様を要求***することが望ましい。また，クラウドサービスカスタマは，***その仕様がバックアップに関する要求事項を満たすことを検証***することが望ましい。 クラウドサービスプロバイダがバックアップ機能を提供しない場合は，***クラウドサービスカスタマがバックアップ機能の導入に責任***を負う。

リスクアセスメントの対象に関するヒント

事例：ISO/IEC27017の箇条（本文 12.3.1）

- クラウドサービスプロバイダ向けImplementation guidanceの例
  - 27017: 12.3.1 Information backup

クラウドサービスのための実施の手引

クラウドサービス固有の導入の手引き

クラウドサービスプロバイダ

クラウドサービスプロバイダは，クラウドサービスカスタマに，***バックアップ機能の仕様を提供***することが望ましい。その仕様には，必要に応じ，次の情報を含めることが望ましい。

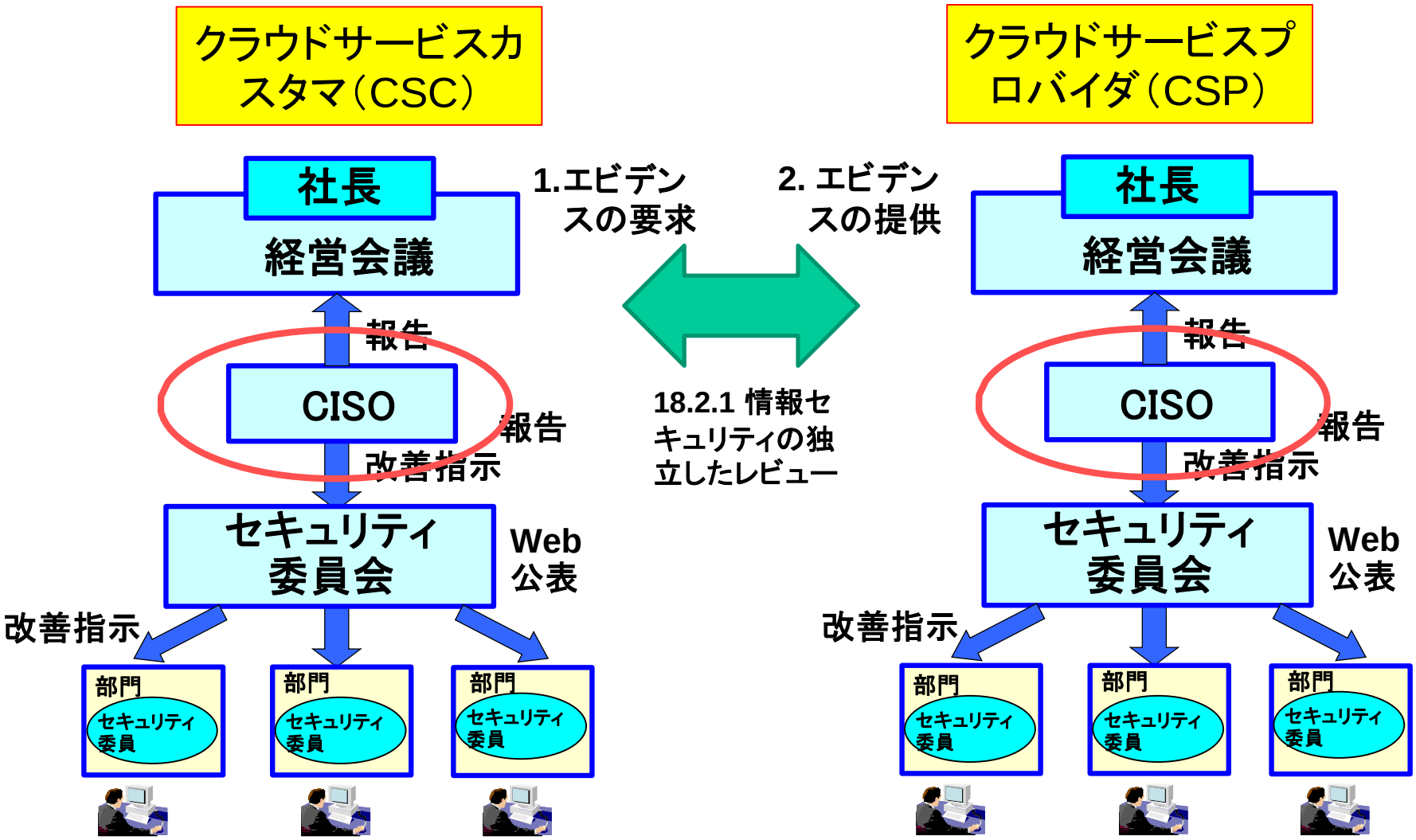
- バックアップ範囲及びスケジュール
- 該当する場合には暗号を含む，バックアップ手法及びデータ形式
- バックアップデータ保持期間
- バックアップデータの完全性を検証するための手順
- バックアップからのデータ復旧手順及び所要時間
- バックアップ機能の試験手順
- バックアップの保存場所

クラウドサービスプロバイダは，クラウドサービスカスタマに***バックアップにアクセスさせるサービスを提供***する場合には，***仮想スナップショットなどの，セキュリティを保った，他のクラウドサービスカスタマから分離したアクセスを提供***することが望ましい。

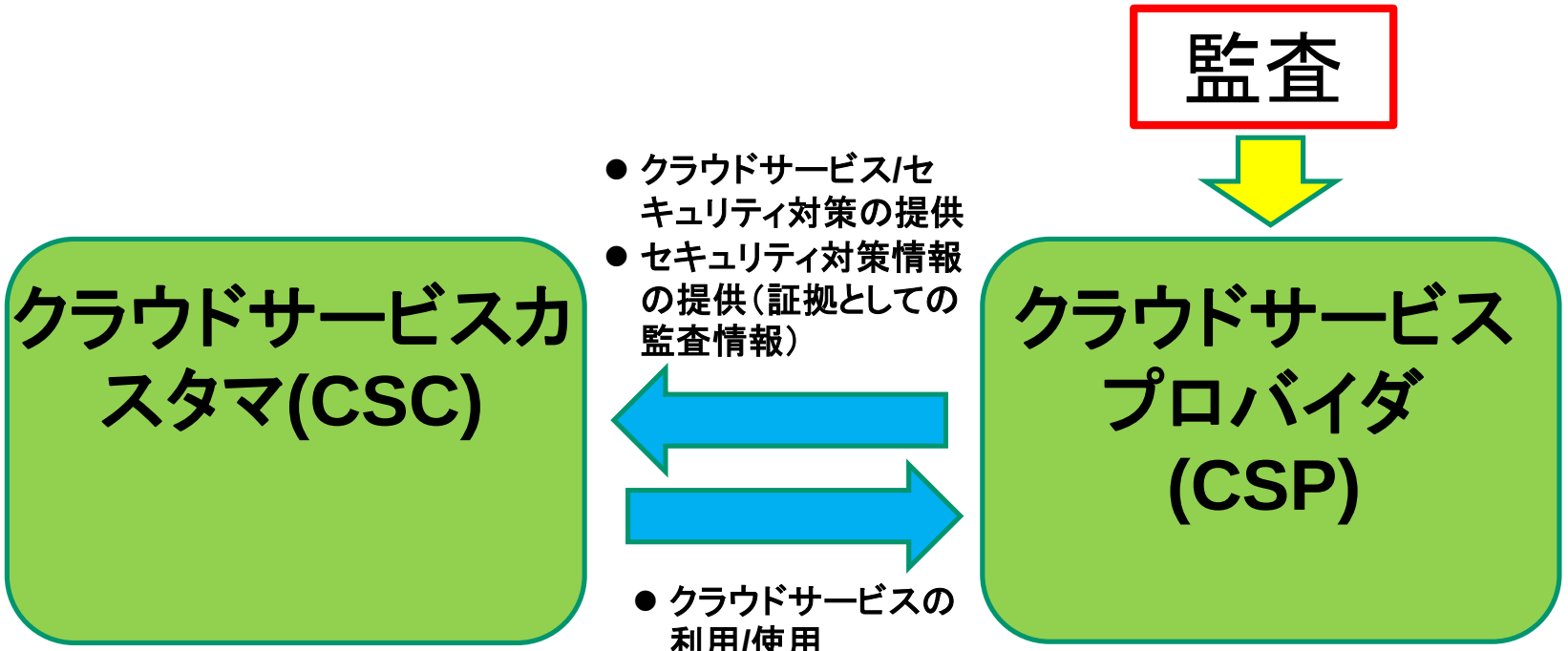
リスクアセスメントの対象に関するヒント

(4)動力４:クラウドサービス利用/提供における監視・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 -



CSCは、信頼できるCSPの監査情報を把握できないとセキュリティ対策はできない



① CSCは、システム及びセキュリティ対策の主要な部分をCSPに委ねている

② CSCは、CSPの提供する情報及びセキュリティ対策に応じて、セキュリティ対策を実施（言い換えると信頼できるCSPの監査情報を把握できないとセキュリティ対策はできない）

③ CSPは、CSCのセキュリティ対策を支援するセキュリティ対策及び情報を提供（信頼できるセキュリティ対策と監査情報の提供）

④ CSPは、複数のCSCのセキュリティレベルを考慮したセキュリティ対策を提供

事例：ISO/IEC27017の箇条（本文 18.2.1）

- クラウドサービスカスタマ/プロバイダ向け実施の手引の例
  - 27002: 18.2.1 情報セキュリティの独立したレビュー
    - 管理策

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することが望ましい。

➔ 27017には、記述されませんが、この内容が、適用の対象となります

    - 実施の手引

経営陣は，独立したレビューを発議することが望ましい。このような独立したレビューは，情報セキュリティをマネジメントする組織の取組みが，引き続き適切，妥当及び有効であることを確実にするために 必要である。このようなレビューは，改善の機会のアセスメントを含むことが望ましい。また，方針及び 管理目的を含むセキュリティの取組みの変更について，その必要性の評価を含むことが望ましい。このようなレビューは，レビューが行われる領域から独立した個人・組織（例えば，内部監査の担当部 署，独立した管理者，このようなレビューを専門に行う外部・・・・

➔ 27017には、記述されませんが、この内容が、適用の対象となります

事例：ISO/IEC27017の箇条（本文 18.2.1）

- **クラウドサービスカスタマ向け実施の手引の例**
  - **27017: 18.2.1 情報セキュリティの独立したレビュー**

JIS Q 27002の**18.2.1**に定める管理策並びに付随する実施の手引及び関連情報を適用する。次のクラウドサービス固有の実施の手引も適用する。

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
クラウドサービスカスタマは，***クラウドサービスのための情報セキュリティ管理策及び指針の実施状況がクラウドサービスプロバイダの提示どおり***であることについて，***文書化した証拠を要求する***ことが望ましい。その証拠は，***関係する標準への適合の証明書である場合***もある。

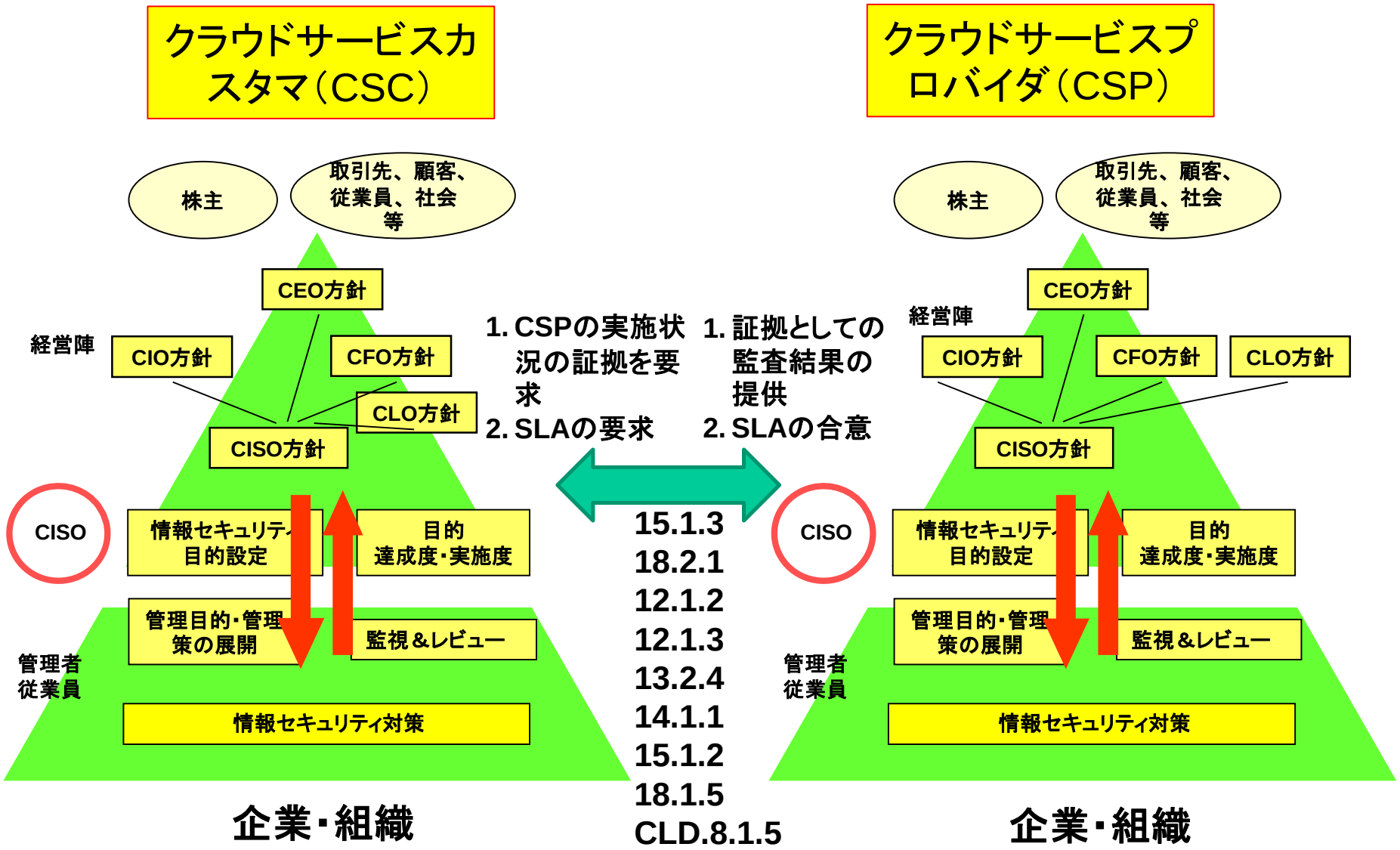
事例：ISO/IEC27017の箇条（本文 18.2.1）

- **クラウドサービスプロバイダ向け実施の手引の例**
  - **27017: 18.2.1 情報セキュリティの独立したレビュー**

クラウドサービスプロバイダ
クラウドサービスプロバイダは，***クラウドサービスプロバイダが主張する情報セキュリティ管理策の実施を立証***するために，クラウドサービスカスタマに***文書化した証拠を提供する***ことが望ましい。 個別のクラウドサービスカスタマの監査が現実的でない又は情報セキュリティへのリスクを増加させ得る場合，クラウドサービスプロバイダは，***情報セキュリティがクラウドサービスプロバイダの方針及び手順に従って実施され，運用されていることの独立した証拠を提供する***ことが望ましい。この証拠は，契約の前に，クラウドサービスの利用が見込まれる者に利用できるようにしておくことが望ましい。クラウドサービス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確保されていることを条件***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レビューへの関心を満たすために受け入れられる方法であることが一般に望ましい。独立した監査が現実的でないとき，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。

(5)動力5：クラウドサービスカスタマ/プロバイダの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 -



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	クラウドコンピューティング環境における役割及び責任の共有及び分担	Compliance and legal risks Malicious behavior of insiders
CLD.8.1.5	1	1	クラウドサービスカスタマの資産の除去	Responsibility of ambiguity Data protection
CLD.9.5.1	1	1	仮想コンピューティング環境における分離	Isolation failure
CLD.9.5.2	1		仮想マシンの要塞化	Inconsistency and conflict of protection mechanism Isolation failure
CLD.12.1.5	1	1	実務管理者の運用のセキュリティ	Evolutionary risks Insecure or incomplete data deletion
CLD.12.4.5	1	1	クラウドサービスの監視	Data protection
CLD.13.1.4	0	1	仮想及び物理ネットワークのセキュリティ管理の整合	Inconsistency and conflict of protection mechanism

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
クラウドセキュリティコントロール専門委員会委員長

山﨑　哲