経済産業省委託事業
平成２３年度企業・個人の情報セキュリティ対策促進事業
（グローバルなクラウドセキュリティ監査の利用促進）

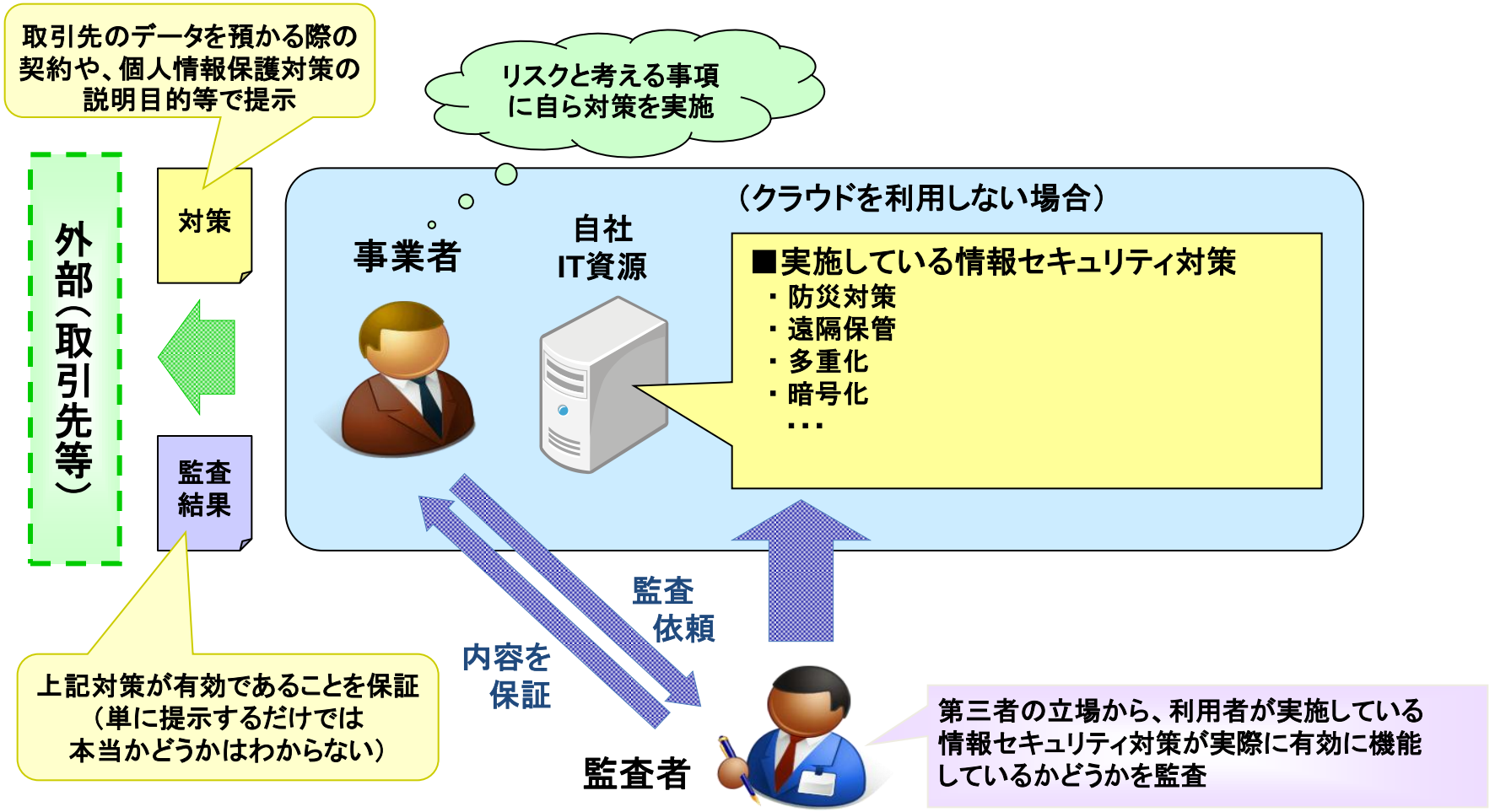
クラウドサービスを安全に活用するための情報セキュリティ監査の利用促進に向けた取り組みについて

2012年9月14日

特定非営利活動法人
日本セキュリティ監査協会

情報セキュリティ監査の枠組み（保証型監査）

情報資源に対して適切な保護策が実施されていることの客観的な保証の手段として、情報セキュリティ監査の実施が有効であり、取引場面等で利用されている



クラウドサービスへの情報セキュリティ監査の適用における課題

クラウドでは標準的サービスの提供を前提としているにもかかわらず、現行の情報セキュリティ監査を適用しようとすると個別に詳細な言明をする必要があり、現実には対応困難

自社運用と同等以上の対策になっているか？

事業者は、言明に個々の管理策を記載する必要がある

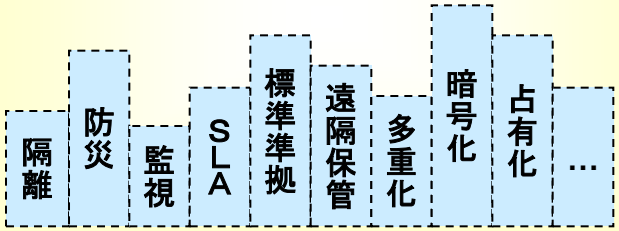
どこまで詳細な管理策を提示しなければいけないのか？

利用者

■言明の内容

事業者が利用者と約束した情報セキュリティ管理策を、約束通りに行うことを宣言

言明：事業者が利用者に安全であることを宣言すること



クラウドサービス事業者

監査結果

言明内容を保証

監査依頼

監査者

第三者の立場から、クラウドサービス事業者の開示内容をもとに、言明内容が実際に有効に機能しているかどうかを監査

【課題①】
詳細な管理策を明示することは、ぜい弱性の開示につながり、リスクが増大する。対象を絞り、個別にしたいが費用がかさむ。

【課題②】
詳細な管理策が開示されないとリスクがわかりにくい
費用負担は安さが売り物のクラウドになじまない

クラウドの利用目的に応じた2種類の言明

- 個別に言明を定義する手間を省くため、一般的な利用において管理すべきリスクと、特に慎重な取り扱いが必要な用途で管理すべきリスクを定義した。前者に対応した言明を「基本言明」、後者を「特約言明」と呼ぶ。
- 基本言明は簡略に対策を講じているとの表現で公開可能とし、言明ができる要件を詳細に定める。特約言明では特約の内容が要件となる
- 言明した事業者が要件を満たしているかを監査し、保証を与えることで言明の信頼性を確保する
- 基本言明と特約言明をクラウドの利用目的に応じて活用することで、事業者は利用者ごとに対応する負荷が減り、利用者は簡単に事業者の安全性を判断できるようになる。

クラウド情報セキュリティ管理基準

基本言明の要件を定義

【利用者のメリット】
一般的なリスク対策の有無を手間をかけずに判断可能

利用者

■ **基本言明**

基本的なセキュリティ要件を満たしている旨の言明なので、詳細な管理策を提示しなくてよい。

隔離	防災	監視	SLA	標準準拠	遠隔保管	多重化	暗号化	占有化	…

■ **特約言明**

事業者は、基本言明に加えて、利用者から特に要望された事項に対応していることを、特約言明で宣言する。

クラウドサービス事業者

【事業者のメリット】
利用者ごとの対応負荷が削減されることによる効率化

基本言明書（例）

20XX年MM月DD日

○○クラウドサービス提供業務の情報セキュリティに関する言明

○○○○○○○○株式会社
代表取締役社長　○○　○○

当社は，○○クラウドサービス提供業務を実施するにあたり，クラウド基本言明要件に準拠して，○○クラウドサービスに供するシステム環境における顧客が保有するシステム及びその管理のために当社が取り扱う情報に対する情報セキュリティ対策を，以下の通り整備し，実装し，運用しています。

・利用者が使用する論理的領域は，その利用者以外のアクセスから保護されていること
・利用者が使用する論理的領域は，その利用者の合理的な要求に従って漏れなく正確に処理又は保存されていること
・利用者が使用する論理的領域は，その利用者が要求した時に約定した範囲で使用が可能であること

・利用者が扱う情報は，その利用者以外のアクセスから保護されていること
・利用者が扱う情報は，その利用者の合理的な要求に従って漏れなく正確に処理又は保存されていること
・利用者が扱う情報は，その利用者が要求した時に約定した範囲で使用が可能であること

・当社が扱う利用者に関する情報は，未承認又は不正なアクセスから保護されていること
・当社が扱う利用者に関する情報は，業務上の合理的な必要に応じて漏れなく正確に処理又は保存されていること
・当社が扱う利用者に関する情報は，業務の必要に応じて要求した時に約定した範囲で使用が可能であること

・以上の事項に関して，その利用者に対し必要な説明が可能であること

以上

クラウドサービスに適した情報セキュリティ監査の枠組み

「基本言明」でクラウドの基本的なセキュリティ要件を規定し、利用者ごとの個別の要望事項には「特約言明」で対応することで、クラウドの特性にあった情報セキュリティ監査を実現

基本言明への対応状況を全利用者共通で開示
特約言明には個別対応

基本言明(＋特約言明)に準拠している旨を提示

利用者

基本言明
一般的な利用において管理すべきリスクに対応

または

特約言明
特に慎重な取り扱いが必要な用途で管理すべきリスクに対応

クラウドサービス事業者

監査結果

監査依頼

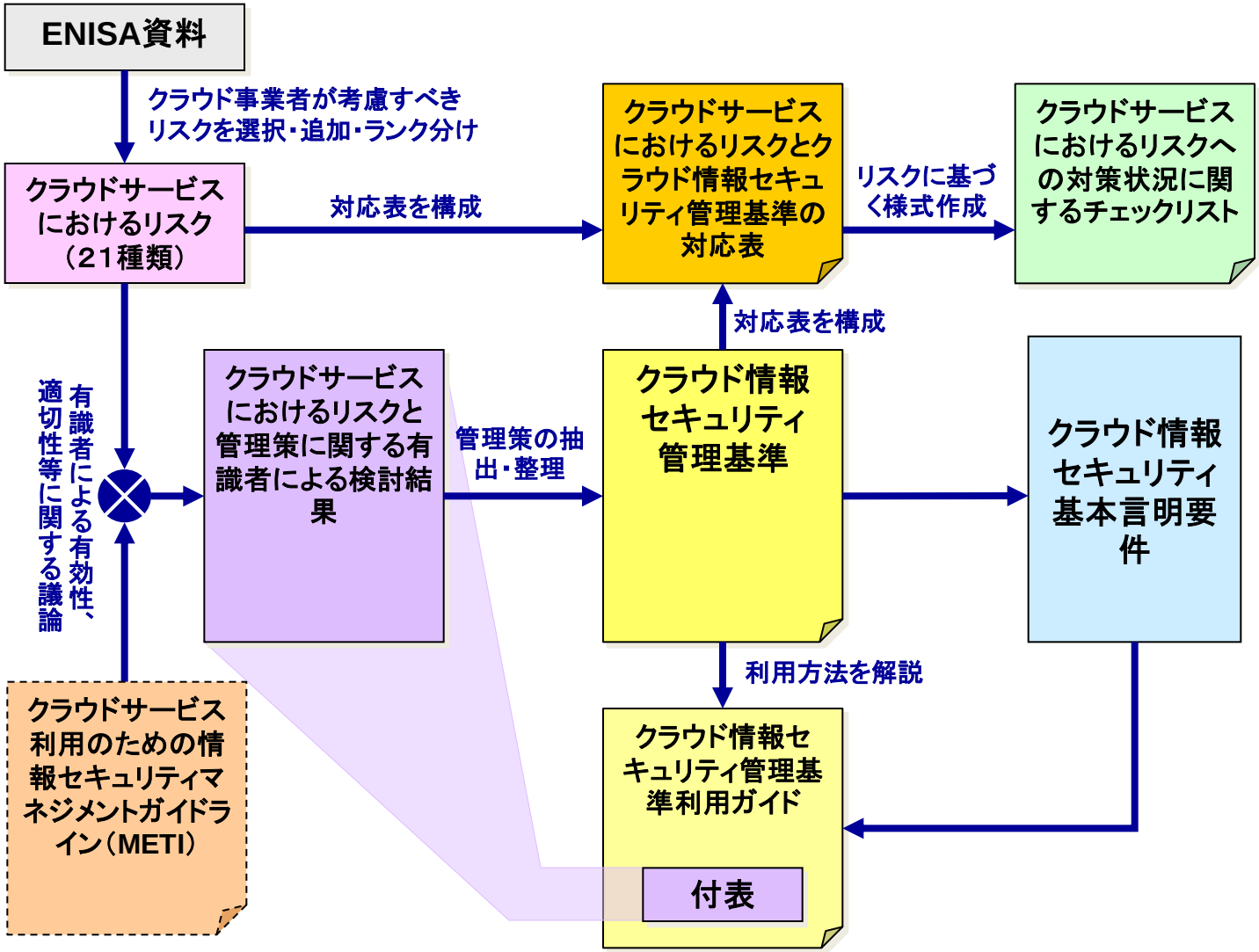
言明内容を保証

【監査者のメリット】
基本言明の共通化を通じた監査実施の効率化

監査者

第三者の立場から、クラウドサービス事業者の開示内容をもとに、言明内容が実際に有効に機能しているかどうかを監査
- 基本言明の監査: サービス単位で実施
- 特約言明の監査: 利用者単位で実施

公表される各文書の関係



言明要件は、情報セキュリティ管理基準に準拠したクラウドセキュリティ管理基準に依拠する。

ENISA資料：“Cloud Computing - Benefits, risks and recommendations for information security”, European Network and Information Security Agency, November 2009.（日本語訳：『クラウドコンピューティング：情報セキュリティに関わる利点、リスクおよび推奨事項』, 独立行政法人情報処理推進機構, 2010）

クラウドサービスにおけるリスク（２１種類）

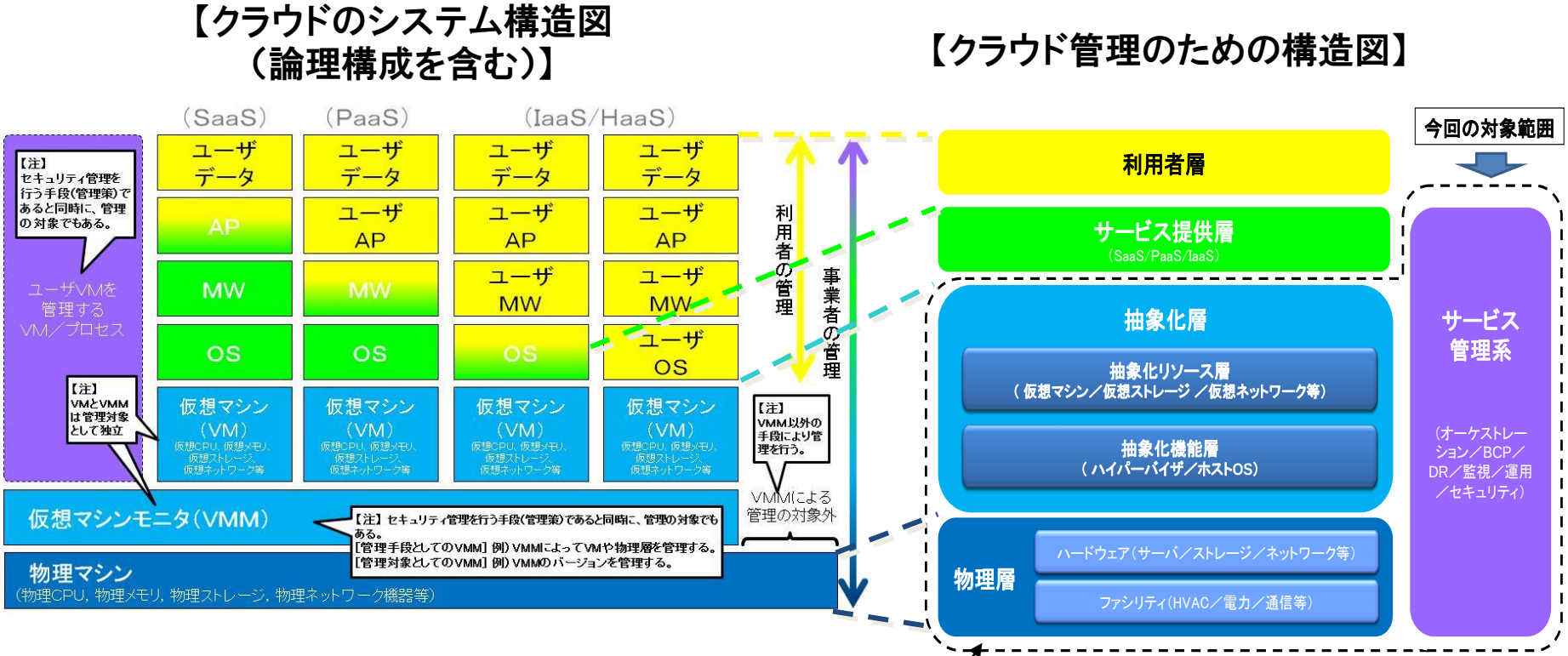
	番号	リスクの識別名	リスクの具体的内容	対応関係
リスク高	H01	リソース・インフラの高集約によるインシデントの影響の拡大	・仮想化技術はリソースの利用効率を高める一方、障害発生時の影響も拡大させる。また、効率化のためのデータセンタの大規模利用も、データセンタ内のネットワークの設定ミスのような障害が発生した場合の影響を拡大させる。	（新たに追加）
	H02	仮想／物理の設計・運用の不整合	・仮想化技術を用いたシステムには従来の設計・運用管理のノウハウが通用しないことが多く、仮想/物理にまたがるコンピュータとネットワークの大規模化・複雑化が、予期せぬ不具合、大規模障害を発生させる可能性がある。	（新たに追加）
	H03	他の共同利用者の行為による信頼の喪失	・他のユーザの活動により、同じクラウドサービスを利用するユーザのIPアドレスが外部サービスによりブロックされる。 ・他のユーザの活動により、利用していたストレージが押収されてサービスの継続が困難になる。	ENISA No.4
	H04	リソースの枯渇（リソース割当の過不足）	・予想を超えるユーザの需要増により、インフラやリソースが需要を満たせずサービスに支障が生ずることで、ユーザの減少や評判の低下を招く。これを回避するためのリソース増強が過剰投資として収益性を低下させる。	ENISA No.8
	H05	隔離の失敗	・クラウドサービスを構成するメカニズムの不備・欠陥や脆弱性への攻撃により、異なるユーザやサービス間の隔離が失われることで、ユーザの機密情報の漏えいなどが生じ、事業者の評判が失墜する。	ENISA No.9
	H06	サービスエンジンの侵害	・脆弱性等を通じてサービスエンジンの制御を奪われることで、クラウドサービスに特化した攻撃（サービスエンジン経由の情報漏えい、リソースの逼迫化によるサービスのマヒ等）が行われる可能性がある。	ENISA No.19
リスク中	M07	クラウドプロバイダでの内部不正－特権の悪用	・クラウド事業者における従業員の悪意の行動が、あらゆるクラウドサービスに影響を及ぼす。 ・従業員が犯罪組織の標的とされ、上記の行動を行う。	ENISA No.10
	M08	管理用インターフェースの悪用（操作、インフラストラクチャアクセス）	・クラウドサービスのユーザ向けのリソース制御インタフェースが悪用され、サービス全体に影響を及ぼす。 ・クラウド事業者の管理者の制御用インタフェースも同様に悪用されることで、さらなる影響を及ぼす。	ENISA No.11
	M09	データ転送途上における攻撃、データ漏えい（アップ/ダウンロード時、クラウド間転送時）	・ユーザ環境とクラウドサービス、もしくは分散されたクラウドサービス相互間でのデータ転送機会が生ずることで、その転送中のデータの漏えいのリスクが生じる。	ENISA No.12, ENISA No.13
	M10	セキュリティが確保されていない、または不完全なデータ削除	・ストレージやバックアップテープ等の物理媒体を他のユーザと共用する場合、媒体には常時複数ユーザのデータが記録されるため、特定ユーザのデータだけを消去する目的で、その媒体を物理的に破壊することはできない。	ENISA No.14
	M11	クラウド内DDoS/DoS攻撃	・同じクラウドサービス内からDDoS/DoS攻撃が行われることで、インターネット経由よりも大きな被害が発生する。	ENISA No.15
リスク低	L12	ロックインによるユーザの忌避	・外部リソースを利用してデータを保護する必要性が生じても、相互接続性がないために、データ移行ができない。	ENISA No.1
	L13	ガバナンスの喪失	・ユーザが下位層を対象としたガバナンスを失うことのリスクを憂慮し、クラウド利用を躊躇する。	ENISA No.2
	L14	サプライチェーンにおける障害	・認証等のサービスを外部委託することで、その委託先に脆弱性が存在するとクラウドサービスにも影響が及ぶ。 ・どの部分を外部委託しているかを明示しないことで、ユーザによるクラウドサービスへの信頼度が低下する。	ENISA No.7
	L15	EDoS攻撃（経済的な損失を狙ったDoS攻撃）	・悪意のユーザによるアカウントの乗っ取り、従量制リソースの浪費等を通じて、ユーザに経済的損失をもたらす。	ENISA No.16
	L16	事業者が管理すべき暗号鍵の喪失	・悪意の関係者により暗号鍵が不正利用されることで、ユーザの機密データの漏えいが生ずる。 ・クラウド事業者が暗号鍵を喪失することでデータの復号が困難となり、ユーザのデータにおける完全性が損なわれる。	ENISA No.17
	L17	不正な探査・スキャンの実施	・攻撃のためのデータ収集が、クラウドサービスの環境を通じて、より容易に行われる可能性がある。	ENISA No.18
	L18	証拠提出命令と電子的証拠開示	・クラウドサービス上にデータが集中することで、司法当局によるデータの押収が行われた場合に、開示したくないデータまで開示されるリスクが増大するため、ユーザによるクラウドサービス利用を躊躇させる要因となる可能性がある。	ENISA No.21
	L19	司法権の違い	・クラウドサービスの物理的インフラが設置される地域（国、州など）によっては、異なる司法上の解釈や独裁的な警察権力、国際的取り決めが遵守されないなどの影響がユーザに及ぶ可能性がある。	ENISA No.22
	L20	データ保護	・ユーザが許可していないデータの処理が勝手に行われることで、ユーザがクラウド利用を躊躇する可能性がある。 ・ユーザが合法的でない方法で収集したデータが、クラウドサービス上に蓄積される可能性がある。	ENISA No.23
	L21	ライセンス	・クラウド利用者のライセンス費用は仮想マシンの数に応じて飛躍的に増大することがある。 ・PaaSやIaaSの場合、クラウド内部で発生した独自の成果物がユーザの知的財産として保護されない可能性がある。	ENISA No.24

注：「対応関係」欄のNo.は前ページ「ENISA資料」において挙げられているクラウドサービスにおけるリスクの整理番号に対応。

クラウド固有の管理策を検討するために用いた クラウドサービスのレイヤーモデル

レイヤーに分けることで、技術的管理策を明確にした

【参考資料】クラウドサービスのレイヤーモデル説明



＜対象を当該レイヤに限定する理由＞

- 上位層はサービス毎にリスクや条件が異なり、**共通の管理策を検討することが困難**
- クラウド固有のリスクは、物理層から抽象化層およびサービス管理系で発生する**技術的リスクが主体**
- 対策の有効性は下層の状況に依存する場合が多いため、**最下位層（物理層）からの検討が必要**

レイヤー別管理策

同じリスクに対しても、レイヤーにより詳細管理策が異なる。クラウドセキュリティガイドラインの内容を管理基準に置き換えたうえで、レイヤーごとに提示することで、何をすべきか事業者が分かるようにしている。

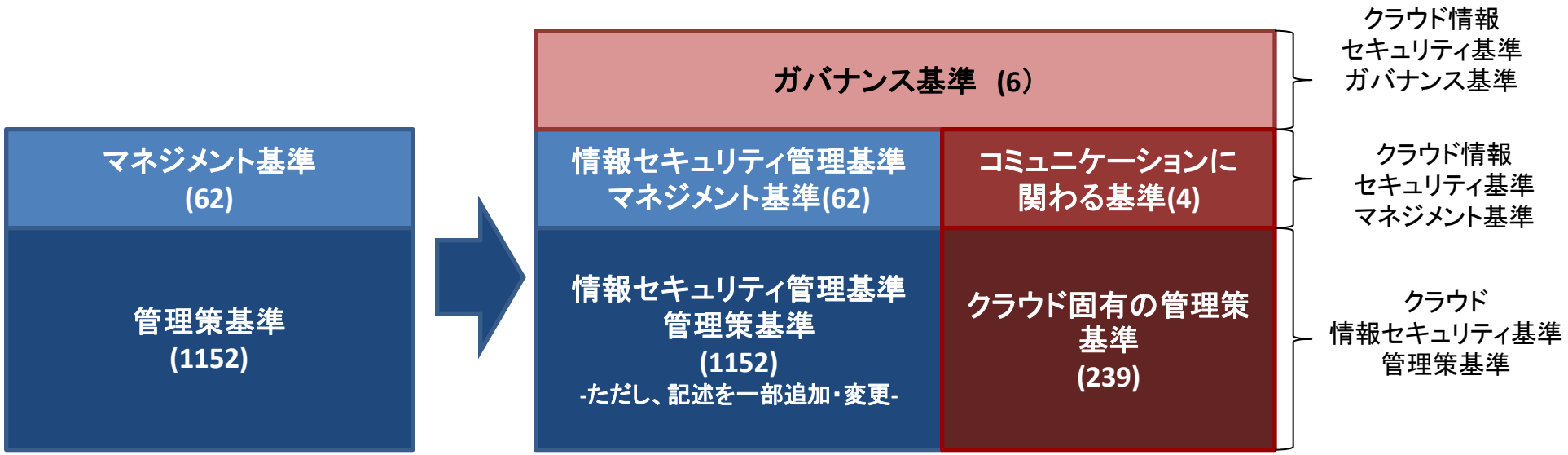
H01:リソース・インフラの高集約によるインシデントの影響の拡大

レイヤ		目指すべき水準	想定されるリスク		クラウド事業者における対策の視点	対応するクラウド管理基準	残留リスク
			脅威	脆弱性			
抽象化層	リソース層	一部の障害、一地域の災害が大規模なサービス停止を招かないこと	バグ・・・・	複雑なサーバ設計・運用・・・	・・・わかりやすいシステムにする	6.3.2.2 新しいシステムを受け入れる仕組みの整備・・・	不注意によるミス
	機能層			事業が連載し・・・	障害の大規模化を防ぐため、・・・	C.2.1.1一部の仮想化機能・・・冗長化	想定できない異常の出現
物理層			故障・・・・	単一障害点（その箇所が停止すると・・・）	クラウドサービスの全面的な停止を・・・	6.6.1.16停止が許容できない・・ネットワークの冗長化 C.1.1.1一部の情報処理施設・・・冗長化	冗長部の同時障害
サービス管理系		一部の障害、一地域の災害が・・・			クラウドサービスを停止させないため・・・	C.2.1.1一部の仮想化機能・・・冗長化	多数同時障害

クラウドサービスにおけるリスクと管理策に関する有識者による検討結果

クラウドセキュリティ管理基準と情報セキュリティ管理基準

クラウドコンピューティングを利用すると、利用者が管理できない環境（ガバナンスが及ばない環境）にコンピュータ資源を置き、情報処理を行う。このため、利用者は、事業者の情報セキュリティガバナンスが確立し、適切な情報セキュリティマネジメントが行われており、かつ、事故等のためのリスクコミュニケーションが確立されていることを確認することで、自らコンピュータ資源や情報を管理できないことによるリスクを抑制する。
情報セキュリティ管理基準に、情報セキュリティガバナンスとリスクコミュニケーションの基準を追加した、クラウド固有のコントロールを加えたものが、クラウドセキュリティ管理基準である。



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

クラウド情報セキュリティ管理基準とは

情報セキュリティ監査制度を活用して、クラウド事業者のセキュリティレベルに一定の保証を与えることにより、クラウドコンピューティングの普及・発展を促進するための主体別・業種別管理基準※の１つである（主体＝サービス提供者、業種＝クラウドサービス業）。下記の３種類の基準より構成（合計**1463**項目）。

※ 詳細は本資料**22**ページを参照

分類		記載内容
クラウド情報セキュリティ管理基準	ガバナンス基準 (6項目)	・情報セキュリティガバナンスのフレームワークの方向付け（Direct）、モニタリング（Monitor）、評価（Evaluate）、監督（Oversee）、報告（Report）に必要な実施事項を定める。 ・それぞれの事項は「情報セキュリティガバナンス導入ガイダンス」（経済産業省 平成21年6月）を基にして策定。
	マネジメント基準 (66項目)	・情報セキュリティマネジメントの計画、実行、点検、処置に必要な実施事項に、リスクコミュニケーションを加えて定めたもの。 ・それぞれの事項は、JIS Q 27001:2006（情報技術—セキュリティ技術—情報セキュリティマネジメントシステム—要求事項）及びISO/IEC 27005:2008（情報技術—セキュリティ技術—情報セキュリティリスクマネジメント）を基にして策定。 ・項目の抽出に際しては、ISMS認証取得を目指している組織、独自に情報セキュリティマネジメントの確立を検討している組織、情報セキュリティ監査を実施する組織、情報セキュリティ監査を受ける組織など幅広い利用者を想定。
	管理策基準 (1391項目)	・組織に情報セキュリティマネジメントの確立段階において、リスク対応方針に従って管理策を選択する際の選択肢を与えるもの。 ・それぞれの事項は、JIS Q 27001:2006附属書A「管理目的及び管理策」、JIS Q 27002:2006、「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」及びクラウドサービスにかかわるリスク分析を基に専門家の知見を加えて作成。 ・「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」の「クラウド事業者の実施が望まれる事項」及び既存のISMS認証などとの整合性にも配慮。 ・「情報セキュリティ管理基準（平成20年改正版）」にない管理策で、クラウドサービスにおいて特に考慮すべきものを、管理策基準の最後に追加。

クラウド利用者における3つの選択肢

クラウドサービスを選定する際、事業者の監査利用の有無、利用者の知識に応じて、下記の３つの方法を使い分けることができる。
従来の方式の改善形である特約言明方式が高度な知識を有する利用者向けであるのに対し、今回新たに提供される２方式は、いずれも一般の利用者がより簡単にクラウド事業者を選ぶための仕組みである。
利用者は、それぞれの方式の特徴を比較して、自組織に適した方法を選ぶことができる。

利用者

監査が及ぶ事業者

基本的なセキュリティ対策の実施が保証されているサービスを使いたい

→ **基本言明方式**
監査済みの基本言明を開示している事業者のサービスを選定

より高度なセキュリティ機能の提供が保証されるサービスを使いたい

→ **特約言明方式**
特約言明を要求した上で、その内容を監査

監査を受け入れない事業者を評価する場合

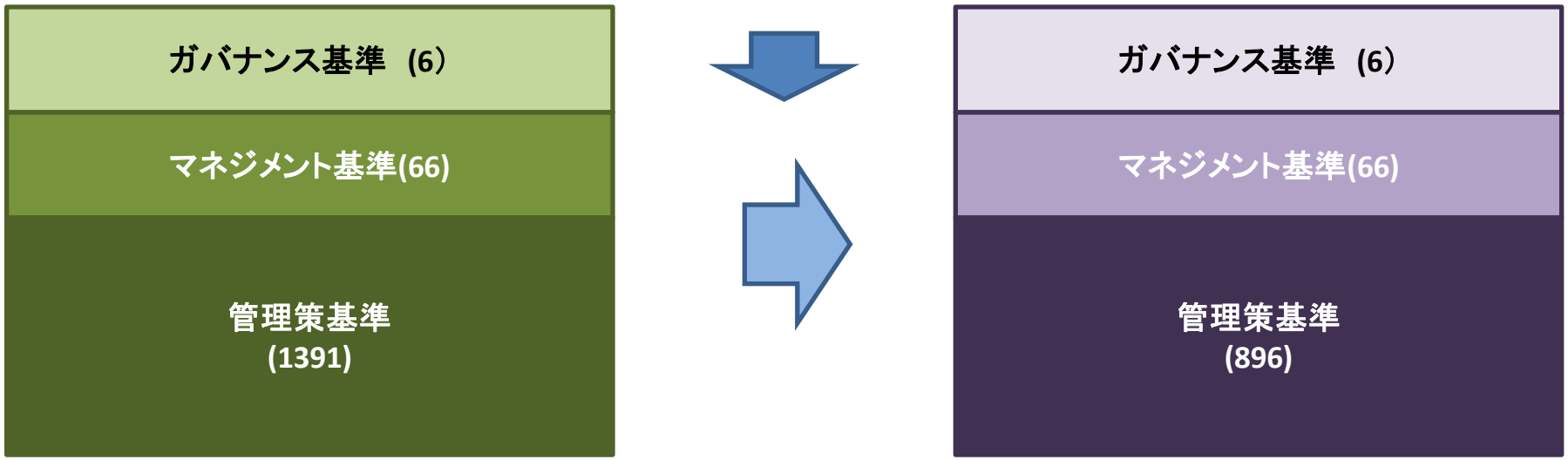
自社で必要なセキュリティ対策が実施されていることを確認して使いたい

→ **チェックリスト方式**
事業者の開示情報について、チェックリストで基本言明要件が満たされているかを確認し、サービスを選定（※）

（※）チェックリストは、監査を受け入れない事業者（例えば外のクラウドサービス等）を対象として評価する場合に用いることを想定する。

基本言明要件

情報セキュリティ対策の基本的事項と
リスク高・中に対応する項目を抽出



クラウドセキュリティ管理基準

基本言明要件

情報セキュリティ対策の基本的事項;「セキュリティポリシーを作る」、「従業員を教育するなど」のどのような組織・業務でも行うべき事項

基本言明に基づき確保する安全性

- 「クラウド情報セキュリティ管理基準」では、基本言明の担保に必要な項目を「基本言明要件」として抽出・整理している。基本言明は、経営者が想定されるリスクへの対策が確実に行っていることを宣言する。
- 監査は、経営者が宣言通りにリスク対策を行っていることを保証する。
- 利用者は、基本言明を行い、監査でそれが保証された事業者を選択することで、基本的な情報セキュリティ対策に関する確認の手間を省くことができる。

クラウドサービスにおけるリスクと管理策に関する有識者による検討結果

H01:リソース・インフラの高集約によるインシデントの影響の拡大

レイヤ		目指すべき水準	想定されるリスク		クラウド事業者における対策の視点	対応するクラウド管理基準	残留リスク
			脅威	脆弱性			
抽象化層	リソース層	－	－	－	－	6.3.2.2 新しいシステムを・・・ 6.3.2.3新しいシステムを・・・	－
抽象化層	機能層	一部の障害、一地域の災害が大規模なサービス停止を招かないこと	バグ・・・・	事業が連載し・・・	障害の大規模化を防ぐため、・・・	C.2.1.1一部の仮想化機能・・・	想定できない異常の出現
物理層			故障・・・・	単一障害点（その箇所が停止すると・・・）	クラウドサービスの全面的な停止を・・・	6.6.1.16停止が許容できない・・・ C.1.1.1一部の情報処理施設・・・	冗長部の同時障害
サービス管理系		一部の障害、一地域の災害が・・・			クラウドサービスを停止させないため・・・	C.2.1.1一部の情報処理設備・・・	多数同時障害

言明の担保に必要な管理基準項目の抽出・整理
（21種類のリスクのうち、高と中の11種類から抽出）

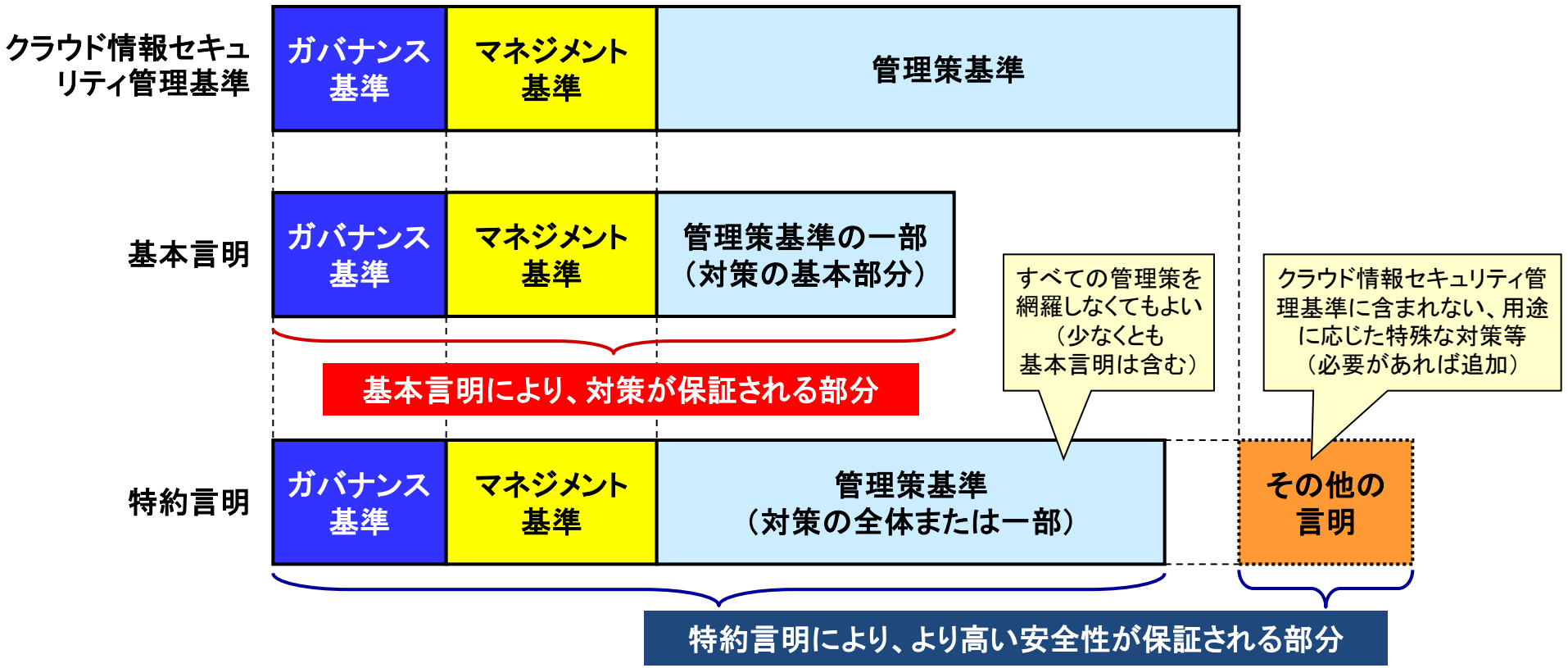
赤枠がクラウド情報セキュリティ基本言明要件

	番号	リスクの識別名
リスク高	H01	リソース・インフラの高集約によるインシデントの影響の拡大
リスク高	H02	仮想／物理の設計・運用の不整合
リスク高	H03	他の共同利用者の行為による信頼の喪失
リスク高	H04	リソースの枯渇（リソース割当の過不足）
リスク高	H05	隔離の失敗
リスク高	H06	サービスエンジンの侵害
リスク中	M07	クラウドプロバイダでの内部不正－特権の悪用
リスク中	M08	管理用インターフェースの悪用（操作、インフラストラクチャアクセス）
リスク中	M09	データ転送途上における攻撃、データ漏えい（アップ/ダウンロード時、クラウド間転送時）
リスク中	M10	セキュリティが確保されていない、または不完全なデータ削除
リスク中	M11	クラウド内DDoS/DoS攻撃

基本言明の表明は、中レベル以上のリスクへの対策を約束するものである

特約言明とは

- 特約言明とは、基本言明に加えて追加の管理策が必要と判断する場合に、事業者と合意して追加した管理策を事業者が講じていることの表明をいう。
- 特約言明の内容は利用者毎に異なることが想定され、利用者が個別に特約言明について情報セキュリティ監査を依頼することによって、その内容が保証される。



利用者に求められるリスク対処

クラウド情報セキュリティ管理基準の全ての項目を実施しても、リスクがゼロになるわけではない。技術的な限界など「不可抗力の事故のリスク」がある。基本言明は、これに加えて低廉なサービスの特性を踏まえた標準サービスとして低リスクへの対応がなくても表明できる。利用者はこれらを自覚し、必要な対処を行うことが求められる。

クラウドサービスのリスクと言明との関係

	クラウドサービスにおけるリスク全体		
管理策の適用範囲	「クラウド情報セキュリティ管理基準」の遵守事項をすべて実施した場合に対策が講じられるリスク		不可抗力の事故リスク（「クラウド情報セキュリティ管理基準」をすべて遵守しても防げないリスク）
	基本言明において対策が講じられるリスク	基本言明の残留リスク（基本言明をもとに対策を講じても防ぐことができないリスク）	
リスクの例	・高集約化がもたらす影響（リスク＝高） ・隔離の失敗（リスク＝高） ・内部不正による特権の悪用（リスク＝中）	・司法権の相違がもたらす影響 ・事業者が管理すべき暗号鍵の喪失 ・特定仕様へのロックイン	・ゼロデイ攻撃 ・検知前の被害

チェックリストとは

チェックリストとは、クラウドサービスの21の個別のリスクについて、事業者による対策状況を利用者が評価できるようにしたものである。

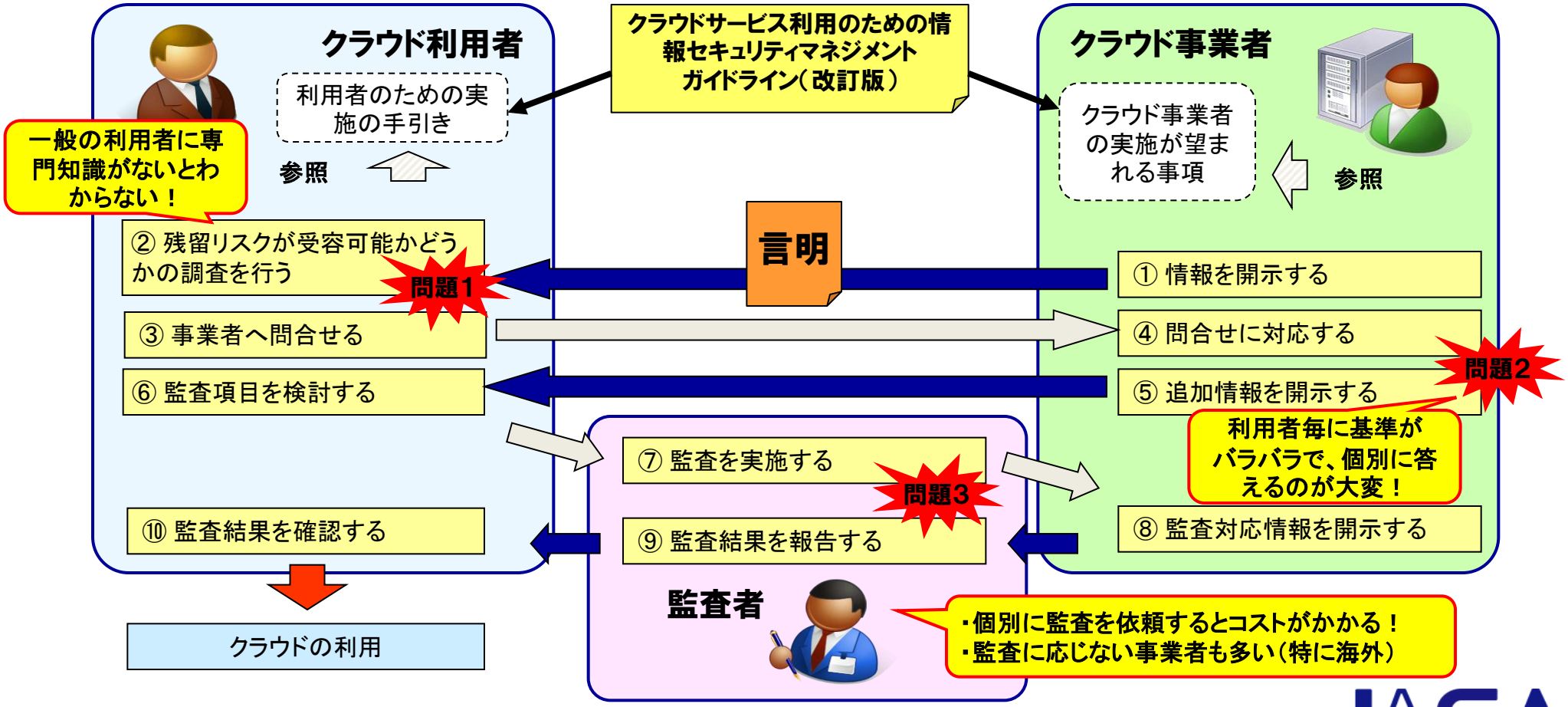
クラウドサービスにおける情報セキュリティ対策に関するチェックリスト（記入済み例）

対象：Aサービス（X株式会社）

番号	リスクの種類	事業者による説明（実施している対策の概要）	利用者記入欄	
			判断	判断の根拠
H01	クラウドサービスにおける高集約化がもたらす悪影響	何らかの異常や大災害が生じた場合でも、サービスの全面停止を防ぐため、地理的に離れた3箇所以上の拠点でサービスを提供しています。いずれかの拠点が稼働していればサービスの継続が可能です。	○	対策として適切と判断。
H02	クラウドサービスを構成する仮想システムで障害が発生することによる被害	機器の障害や操作ミスがサービスに影響を及ぼさないようにするため、自動監視システムを常時稼働し、異常の早期検知を図るとともに、仮想システムで異常が生じにくくなるような設計を行い、厳格なテストを通じてその効果を検証済みです。	○	自社運用よりも障害可能性は低いと見込まれることから、適切と判断。
H03	クラウドサービス内の他利用者の活動による悪影響	パブリッククラウドサービスの性質上、他のお客様の活動による影響を完全に排除することは困難です。他利用者の影響が気になるお客様にはプライベートクラウドサービスをお勧めしております。	×	他利用者の影響を受けることは避けたいが、コスト的にプライベートクラウドの利用は困難。
H04	クラウドサービスの提供に必要な資源の枯渇による被害	通常の利用ではお客様が必要とされる資源が不足する心配はございませんが、万一不足となった場合はサービス約款に基づく対応をさせていただいております。	○	これまでのX社の運用実績から障害可能性は低いと判断。
H05	クラウドサービスにおいて他利用者が自分のデータにアクセスすることによる被害	お客様毎にデータは完全に隔離されています。この隔離が失われることのないよう、弊社の情報セキュリティポリシーのもとにシステムの脆弱性対策を実施するとともに、不正アクセスの早期検知のための監視システムを常時稼働させております。	○	これまでのX社の運用実績から障害可能性は低いと判断。
H06	クラウドサービスの基盤インフラへの攻撃がもたらす被害	Aサービスの基盤インフラは、お客様用の通信回線とは別の回線を通じて管理しており、外部からの攻撃を困難にしております。さらに、弊社の情報セキュリティポリシーのもとにシステムの脆弱性対策を実施しております。	○	これまでのX社の運用実績から障害可能性は低いと判断。

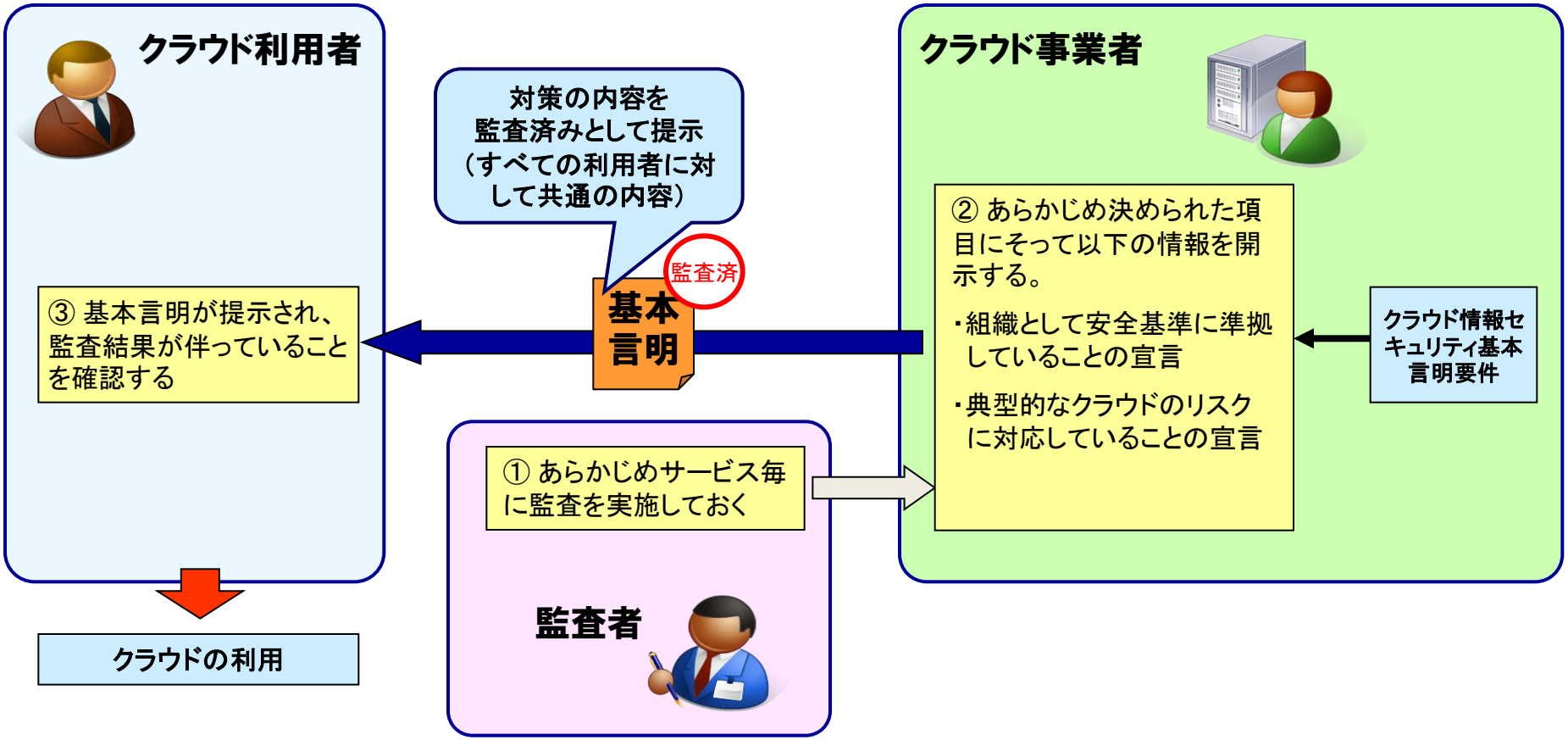
これまでのクラウドサービスで安全な利用を求めるには

安全な事業者を選ぶためには、利用者が自ら手引き等を参照して、個別に事業者に問い合わせ、監査にて確認する必要があった。事業者とのやり取りには、専門知識が必要とされるため、一般の利用者にはハードルが高かった。また事業者が個別の対応に手間がかかる等の問題があった。



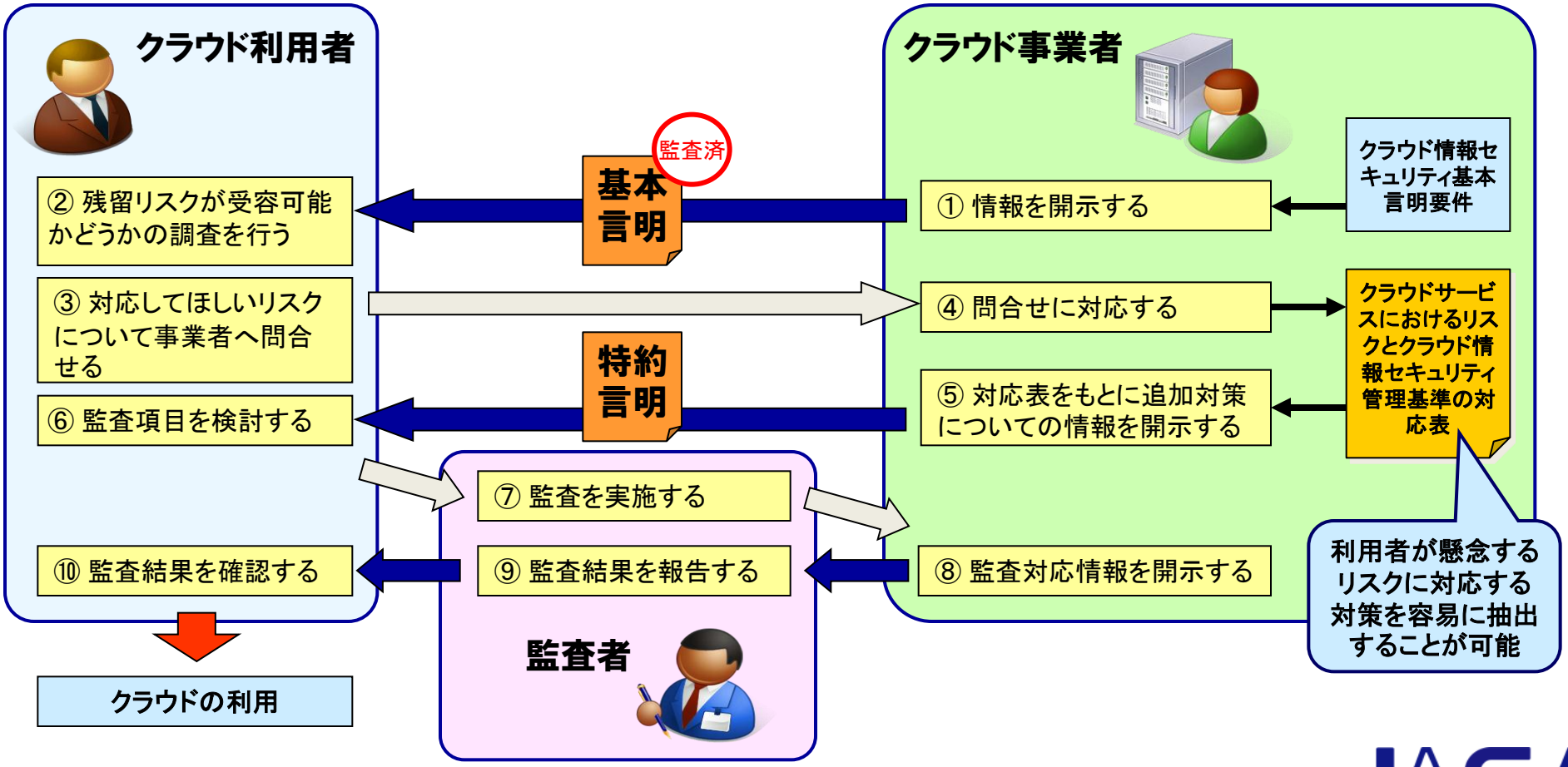
基本言明方式によるクラウドサービスの利用

基本言明方式の場合、チェックリスト方式と比較して監査のプロセスが加わるため、言明内容の信頼度が高い。利用者は基本言明に監査結果が伴っていることを確認するだけでよいため、情報セキュリティ対策に要する負荷が著しく小さい。



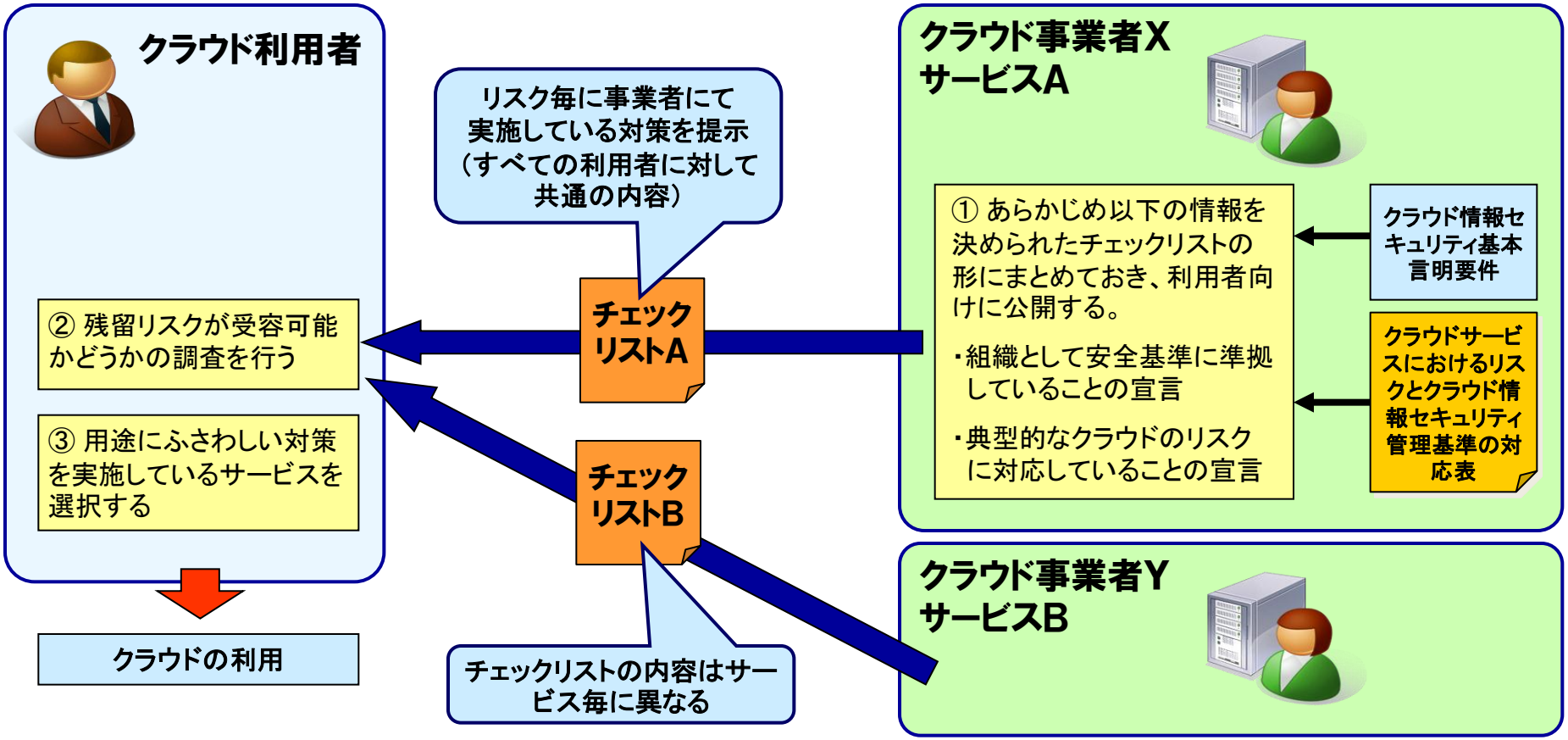
特約言明方式によるクラウドサービスの利用

特約言明方式の場合、利用者とクラウド事業者の間のやりとりの総数は以前と変わらないが、基本言明要件の活用により利用者自ら行う作業の負荷を大幅に削減することが可能となる。事業者においても、リスクとクラウド情報セキュリティ管理基準の対応表を活用することで、利用者の要望に効率的に対応することができる。



チェックリスト方式によるクラウドサービスの利用

クラウド事業者が開示している情報に基づき、利用者がクラウドのセキュリティを判断するためのチェックリストはリスク毎に整理されているため、利用者はサービスがどのリスクに対応しているかを容易に判断することができる。ただしチェックリストの内容は監査による保証を伴わないため、後述の基本言明方式に比べると信頼度は劣る。

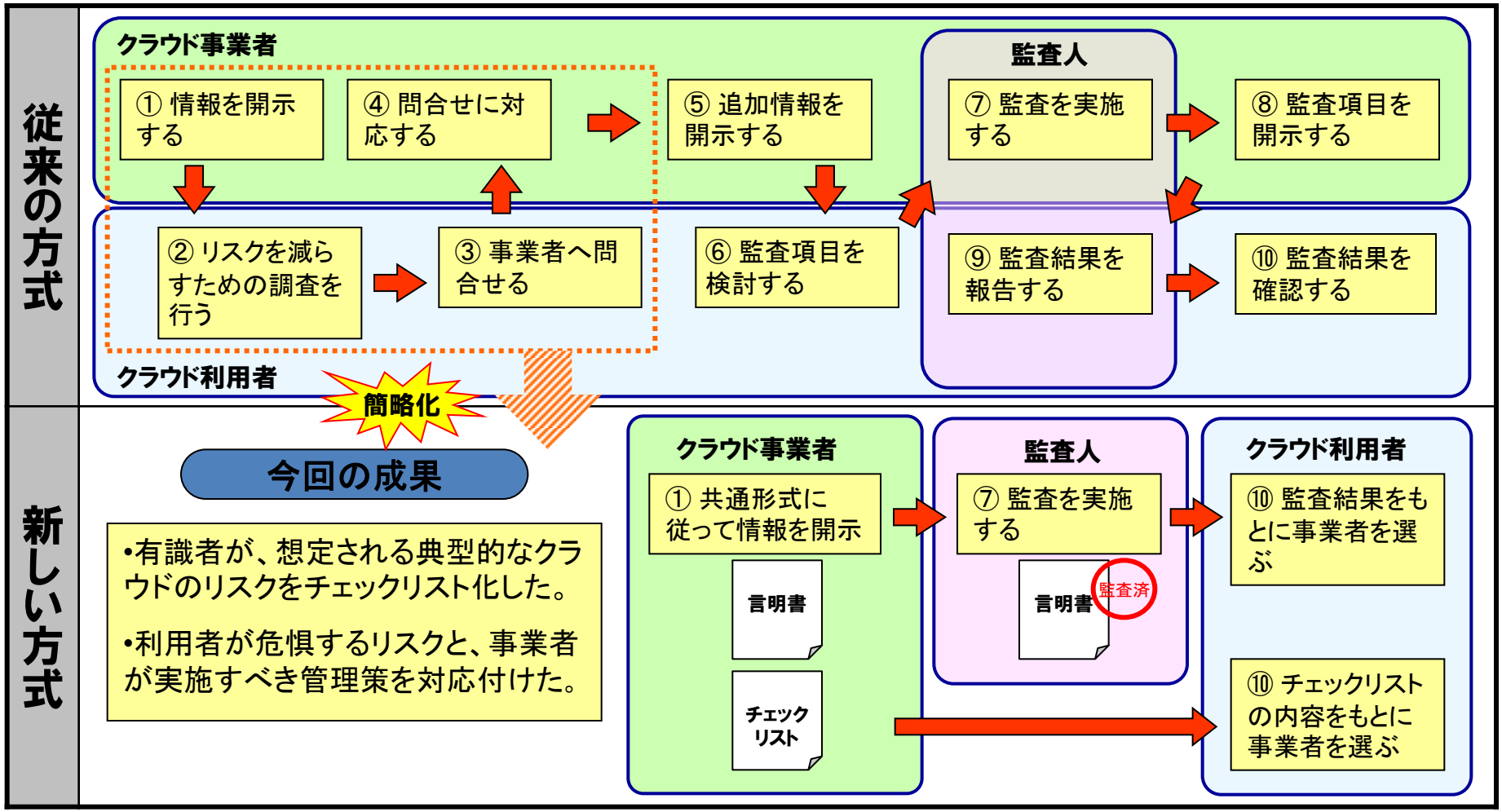


各方式の比較

	基本言明方式	特約言明方式	チェックリスト方式
想定利用者	基本的なセキュリティを確保したい組織。 おもに中小企業～大企業	自社に合わせた、高いセキュリティを要求する組織。金融機関など。	一般的なセキュリティを要求する組織。 中小企業～大企業。
取組み易さ	**易しい**	**難しい**	**普通**
	基本言明を行っているかどうかのみを基準として判断すればよい。	各種資料を理解し、判断する力が求められる。事業者とのやり取りに、専門知識が必要である。	各事業から提示されたチェックリストを比較し、最も自社のニーズに適した事業者を選ぶ。
監査の必要に基づくコスト	**安い**	**高い**	**安い**
	事業者はあらかじめ監査を受けているため、利用者が監査を行う必要はない。	各事業者に対して、個別に監査を行う必要がある。	監査を前提とせず、事業者が関連情報を開示するのみであるため、コストはかからない
カスタマイズ性	**無し**	**有り**	**無し**
	基本言明の要件は業界全体で1種類しかない。	自社のセキュリティ要件に従って、事業者が安全であるかどうかを判断できる。	チェックリストはサービス毎に提供されるが、全利用者に共通の内容。
信頼性	**高い**	**高い**	**低い**
	独立した監査人が確認するので、対策が実装され、運用されている事が保証される。	独立した監査人が確認するので、対策が実装され、運用されている事が保証される。	事業者の信頼に依存しており、情報が確かであるかは保証されない。

新たな方式がもたらす効果

「言明」と「チェックリスト」を用いることで、従来の方式において利用者が個別に問い合わせをしていたプロセスを簡略化することができる。



まとめ

これまでは、クラウド利用者が安全な事業者を選ぶためには、事業者が実施すべき専門的な安全対策の基準を理解し、事業者を監査するための費用負担がかかる方法しかなかった。

多くの企業にとってハードルが高く、「クラウド利用に不安があるから使わない」もしくは「サービス内容を理解しないまま使う」という問題が起きていた。

本取り組みでは、利用者が「簡単に安全に」事業者を選べるように、利用者と事業者のコミュニケーションを円滑にする仕組みを作った。事業者が対策をすべき典型的なクラウドのリスクが整理された。

今回作った仕組みにより、クラウドの利用に躊躇していた中小企業などが簡易方式でクラウド利用を決断できるようになる。また、事業者が共通の基準に従うことでサービス品質向上が期待される。

安全なクラウド利用が世の中に広まる

有識者会議（WGメンバーリスト）

【有識者】

有賀　貞一	経済産業省産業構造審議会情報経済分科会情報サービス・ソフトウェア小委員会人材育成WG委員長
石原　潤二	日本電気株式会社 経営システム本部 セキュリティ技術センター 主任
内田　仁史	株式会社セールスフォース・ドットコム　シニアプリンシパルアーキテクト
（主査）大木　榮二郎	工学院大学 情報学部 情報デザイン学科　教授
織茂　昌之	日立製作所情報・通信グループセキュリティ・トレーサビリティ事業部　HIRTセンタ長
加藤　雅彦	株式会社インターネットイニシアティブセキュリティ情報統括室　シニアエンジニア
岸原　孝昌	一般社団法人モバイル・コンテンツ・フォーラム　常務理事
久保田　朋秀	ニフティ株式会社営業本部サービスソリューション営業部アライアンスチーム　シニアテクニカルディレクター
佐藤　元彦	伊藤忠テクノソリューションズ株式会社ITサービスコンサルティング部 セキュリティアシュアランス課　課長
塩崎　哲夫	富士通株式会社　セキュリティソリューション本部　クラウドセキュリティセンター長
清水　友晴	株式会社三菱総合研究所情報技術研究センタークラウドセキュリティグループ　主任研究員
柄　登志彦	大成建設株式会社　社長室　情報企画部長
中尾　康二	KDDI株式会社 運用統括本部　情報セキュリティフェロー
間形　文彦	日本電信電話株式会社 NTT情報流通プラットフォーム研究所セキュリティマネジメント推進プロジェクト 主任研究員
三原　渉	SGシステム株式会社　取締役　事業戦略担当
米澤　一樹	株式会社シマンテックシステムエンジニアリング本部　シニアマネージャー

【関係団体】

内山　友弘	独立行政法人情報処理推進機構 セキュリティセンター普及グループ
下村　正洋	特定非営利活動法人日本ネットワークセキュリティ協会　事務局長
永宮　直史	特定非営利活動法人日本セキュリティ監査協会　事務局長