金融機関におけるクラウドサービスの利活用とリスク管理等に関するセミナー

総務省「クラウドサービス利用・提供における適切な設定のためのガイドライン」の紹介

（注）以下「本ガイドライン」と略します。

2024年4月3日
日本銀行 金融機構局 金融高度化センター
企画役 有田 帝馬（ありた てつま）

BANK OF JAPAN

1. 本ガイドラインの位置づけ

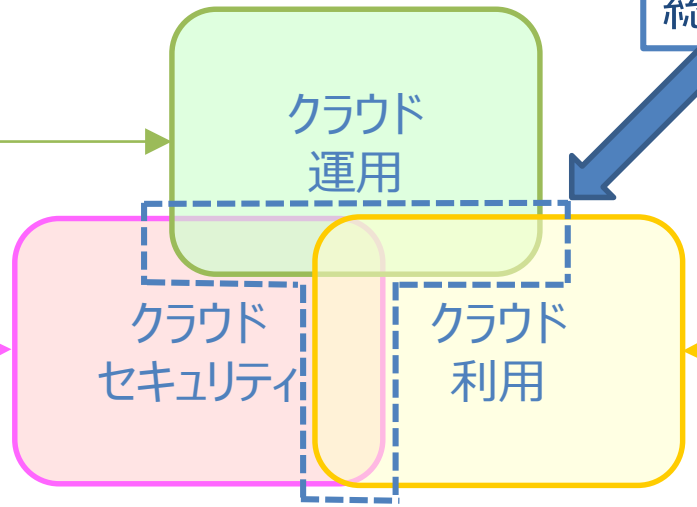
(1) 公的ガイダンス等との関係

・クラウドの運用・セキュリティ・利用については、それぞれに公的ガイダンス等が存在
・本ガイドラインは、公的ガイダンス等をベースとしつつ、運用・セキュリティ・利用に跨る「クラウドの設定」に焦点をあて、設定不備を抑止・防止するための対策を整理したもの

「クラウドサービス利用・提供における適切な設定のためのガイドライン」,2022年10月,総務省

●「クラウドを利用したシステム運用に関するガイダンス（詳細版）」,2021 年 11 月, 内閣官房内閣サイバーセキュリティセンター(NISC)

●「クラウドサービス提供における情報セキュリティ対策ガイドライン（第３版）」,2021年9月, 総務省



●「中小企業のためのクラウドサービス安全利用の手引き」,2019年3月,独立行政法人情報処理推進機構(IPA)
●「テレワークセキュリティガイドライン第5版」の「クラウドサービスの活用の考え方」, 2021年5月,総務省

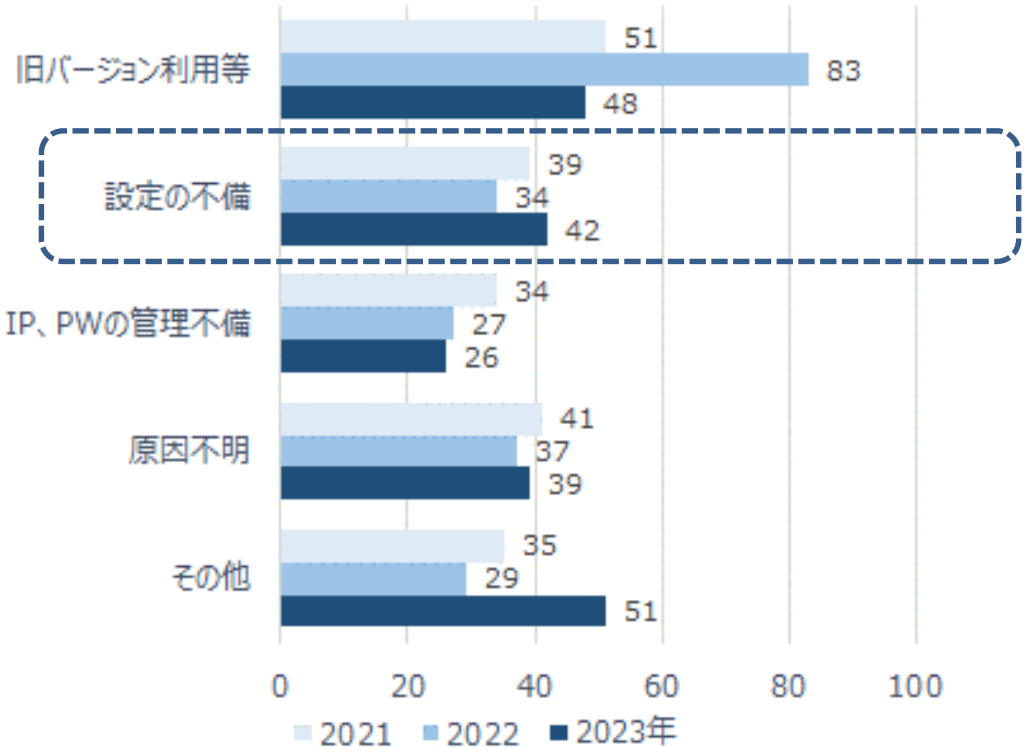
（出所）一般社団法人日本クラウド産業協会（ASPIC）「総務省設定ガイドライン説明会（2024年1月）」資料を元に作成

(2) 本ガイドライン作成の背景

BANK OF JAPAN

・クラウド利用時の設定不備に起因する不正アクセス等の事故が多発
・クラウド事業者、利用者の双方において、設定不備を防ぐ対策の推進が必要

【不正アクセスの原因別件数（IPA届出分）】



（出所）独立行政法人情報処理推進機構「コンピュータウイルス・不正アクセスの届出状況（2023年）」を元に作成

【設定不備によるインシデント事例】

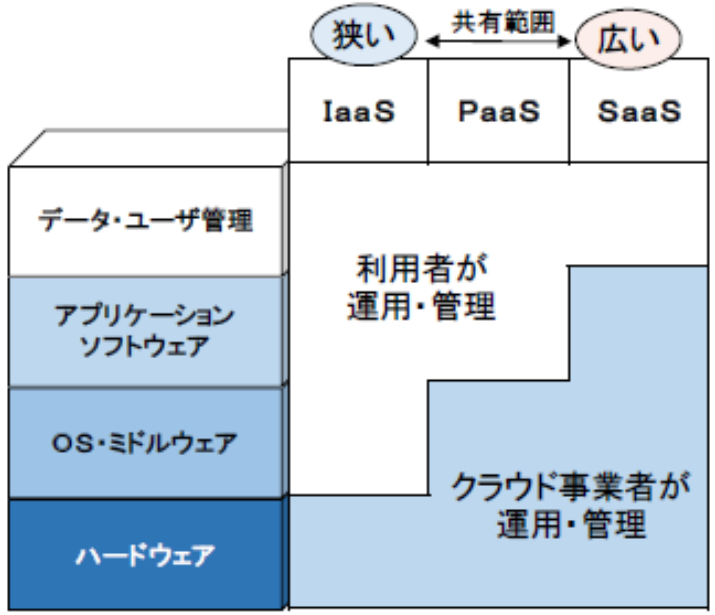
	概要
事例1	クラウド事業者の機能変更により、ユーザーアクセス設定のセキュリティレベルが低下。これに利用企業も気づかず、結果的に機密情報が漏洩
事例2	従業員が個人利用するクラウドに、業務上の機密資料を格納。この資料が公開設定になっていたことが外部からの指摘で判明
事例3	サーバーからクラウドへのデーター移行時に、業務委託先がストレージを公開設定としていた。このため、長期間機密情報が公開された

（出所）総務省「クラウドサービス利用・提供における適切な設定のためのガイドラインの概要（2022年10月）」を元に作成

(3) クラウド事業者と利用者の責任共有

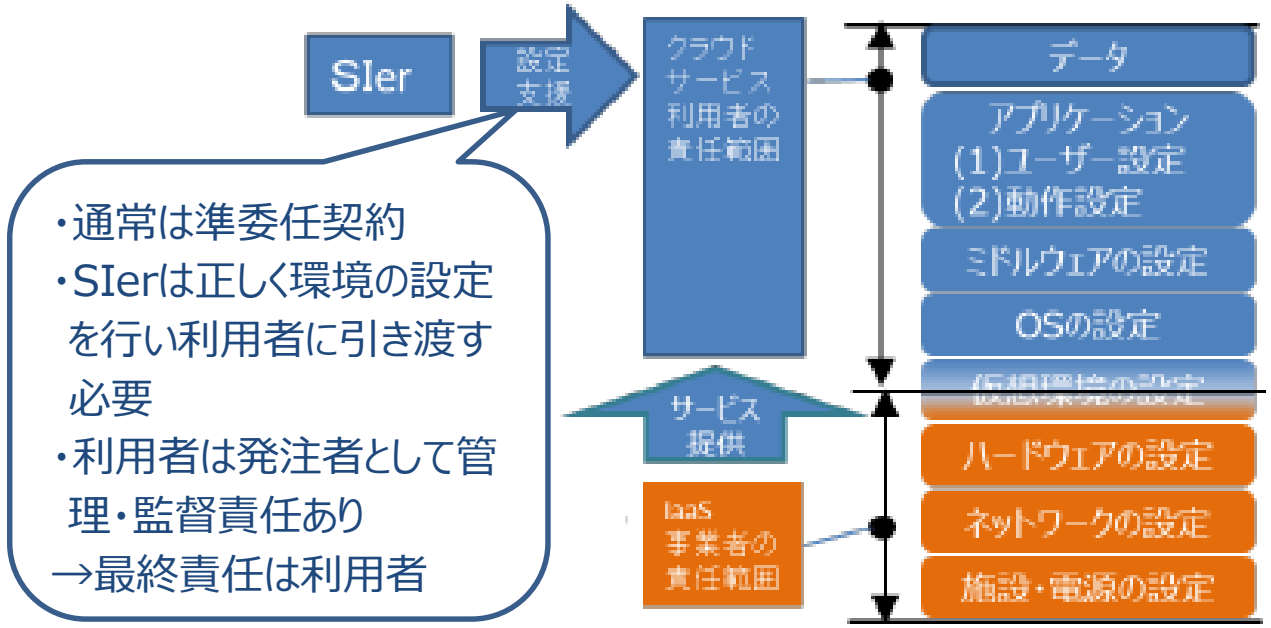
・クラウドの運用・管理は、利用者と事業者で分担（責任共有モデル）。クラウドの適切な設定促進には、両者の協力が重要
・SIerに設定の支援を依頼することも多く、この場合、SIerとの連携も大切になる

【責任共有モデル】



（出所）日本銀行金融機構局「金融機関におけるクラウドサービスの利用状況と利用上の課題について（2024年1月）」より引用

【SIerに設定依頼を行う場合の役割】



（出所）総務省「クラウドサービス利用・提供における適切な設定のためのガイドライン（2022年10月）」を元に作成

(4) 本ガイドラインの構成と想定読者

・本ガイドラインは、設定不備に特化し、利用者、事業者別に、望まれる対策を整理
・想定読者別に整理された構成で、利用方法の解説も付されている

ガイドラインの構成	
Ⅰ.序編	・活用の効果、想定読者 ・ガイドラインの読み方と利用方法 ・用語の定義
Ⅱ.概要編	・クラウドサービスの設定不備のリスク ・クラウドサービスの設定に関する責任共有の考え方
Ⅲ.クラウドサービス利用者編	・利用者側において設定ミスを抑止・防止するための対策 （対策例）クラウド利用における社内ガバナンスの確保、セキュリティにかかる設定項目の確認、支援ツールや外部診断サービス等の活用、設定に関する定期的なチェックや内部監査
Ⅳ.クラウドサービス提供者編	・提供者側において設定ミスを抑止・防止するための対策 （対策例）正しく、十分で、わかりやすくタイムリーな情報の提供、体系的な学習コンテンツの提供、設定項目管理ツールの提供、デフォルト値の見直し

（出所）総務省「クラウドサービス利用・提供における適切な設定のためのガイドラインの概要（2022年10月）」より引用

【想定読者】 想定読者別に利用方法の解説あり

		Ⅰ、Ⅱ	Ⅲ	Ⅳ
利用者	経営層・管理者 狭義利用者	◎	◎	-
	社内向け クラウドサービス開発者	◎	◎	◎
SIer	—	◎	◎	-
事業者	SaaS	◎	-	◎
	IaaS/PaaS	◎	○	◎

（注）狭義利用者：管理者の承認を受け、独自にクラウドを利用する部門
○：IaaS/PaaSを用いてサービスを提供している場合は対象

（出所）総務省「クラウドサービス利用・提供における適切な設定のためのガイドライン（2022年10月）」を元に作成

2. 設定ミスのリスク

(1) 設定とは

・設定は、定義こそシンプルだが、中身は多様
・クラウドの場合、関係者が多い。上は遠い存在と感じ「良きに計らえ」になりがち

定義：システムの動作環境を決定付け、制御するためのパラメータ

中身は多様

「設定」と一言でいっても、システム管理者限定から、一般ユーザーで扱えるものまで幅広い
自由度が高いシステムの場合、一般ユーザーでも高リスクの設定に出来る場合もある

クラウドの場合、関係者が多い

クラウド事業者、利用者側のシステム管理者からエンドユーザーまで、多岐にわたる
しかし、通常は経営層やマネジメント層から遠い存在（「良きに計らえ」になりがち）

(2) クラウドのセキュリティに関する設定項目の類型化

・本ガイドラインでは、CISベンチマーク（注）が示す主要クラウドの設定項目を類型化

		設定内容
1. IDとアクセス管理		誰が、どのリソースに、どのような操作が出来るかの定義
2. ロギングとモニタリング		ログ取得の有効化、フィルタ設定、ログ保存期間の設定等
3. オブジェクトストレージ		アクセス制御、暗号化、ログ取得、一定期間経過後の削除等
4. インフラ管理	仮想マシン	仮想マシンディスク暗号化、エンドポイント保護等
	ネットワーク	外部接続に関するセキュリティ設定、境界防護等の設定等
5. セキュリティ等の集中管理		事業者が提供するセキュリティ集中管理機能、運用管理コンソール、監査ツールの設定等
6. 事業者の提供する、その他のサービスや機能	鍵管理	暗号化のための秘密鍵の設定
	PaaS提供アプリ	アプリ上のアクセス許可の設定等
	データベース	データベースの保護、暗号化等の設定
	コンテナ	コンテナエンジン（Docker等）にかかるセキュリティ設定等
7. その他		IT資産管理、モバイルデバイス管理等の設定

（注）米国国家安全保障局等の政府機関と企業等で構成されるインターネットセキュリティ標準化に取り組む団体（CIS）が公表するガイドライン
（出所）総務省「クラウドサービス利用・提供における適切な設定のためのガイドライン（2022年10月）」を元に作成

(3) 設定に不備があった場合のリスク

・設定に不備があった場合、情報漏洩や不正アクセス等のリスクがある

		設定に不備があった場合のリスク（例）
1. IDとアクセス管理		外部ハッキング、退職者の不正利用、内部情報の外部漏洩等
2. ロギングとモニタリング		インシデントを検知できない、モニタリングの実効性が失われる等
3. オブジェクトストレージ		ライフサイクル設定の誤りによる情報喪失等
4. インフラ管理	仮想マシン	仮想マシンの不適切なバージョン設定によるマルウェア感染
	ネットワーク	ネットワーク設定不備による不正アクセス等
5. セキュリティ等の集中管理		インシデントの影響範囲の拡大を防止できない
6. 事業者の提供する、その他のサービスや機能	鍵管理	攻撃者への鍵の漏洩に伴う、情報漏洩や不正操作
	PaaS提供アプリ	アプリへのアクセス許可等の設定不備による外部からの不正操作
	データベース	データベースの保護や暗号化等の不備による情報漏洩
	コンテナ	コンテナエンジンの設定不備を突いた不正アクセス等
7. その他		インシデントの影響範囲の拡大を防止できない等

（出所）総務省「クラウドサービス利用・提供における適切な設定のためのガイドラインの概要（2022年10月）」を元に作成

3. 設定不備への対策
(1) 設定不備の要因

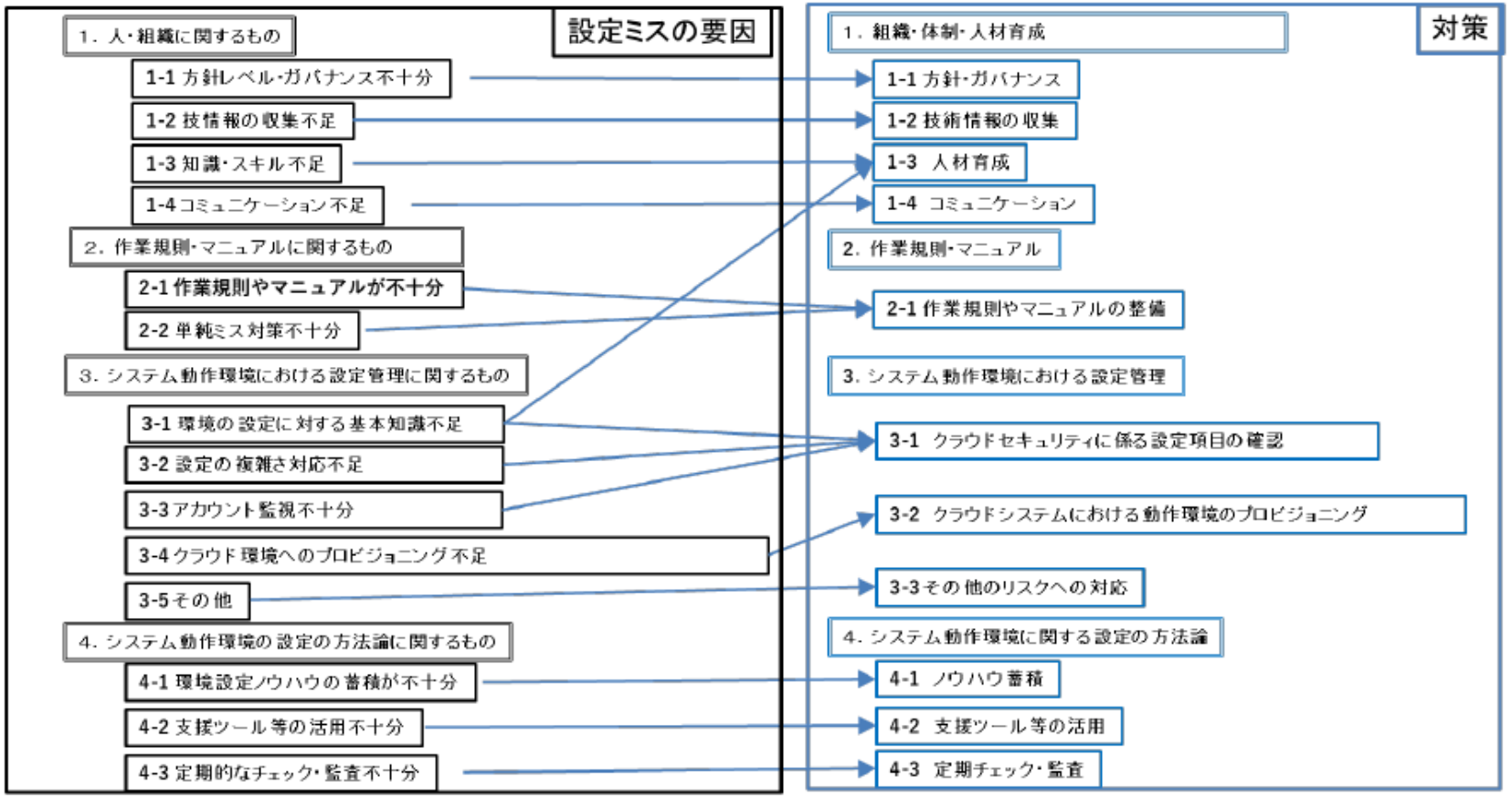
・本ガイドラインでは、利用者と事業者のヒアリング、公開事例調査等を通じ、設定不備の要因を4M（Man, Manual, Machine, Method）フレームワークで分類

4M	設定不備の要因
人・組織に関するもの	方針レベル・ガバナンス不十分、技術情報の収集不足、 知識・スキル不足、コミュニケーション不足
作業規則・マニュアルに 関するもの	作業規則やマニュアルが不十分、単純ミス対策不十分
システム動作環境における 設定管理に関するもの	環境の設定に対する知識不足、環境の複雑さ対応不足、 アカウント監視不十分、クラウド環境へのプロビジョニング不足、その他
システム動作環境の 設定の方法論に関するもの	環境の設定ノウハウの蓄積が不十分、支援ツールなどの活用不十分、 定期的なチェック・監査不十分

（出所）総務省「クラウドサービス利用・提供における適切な設定のためのガイドライン（2022年10月）」を元に作成

(2) 利用者側の対策

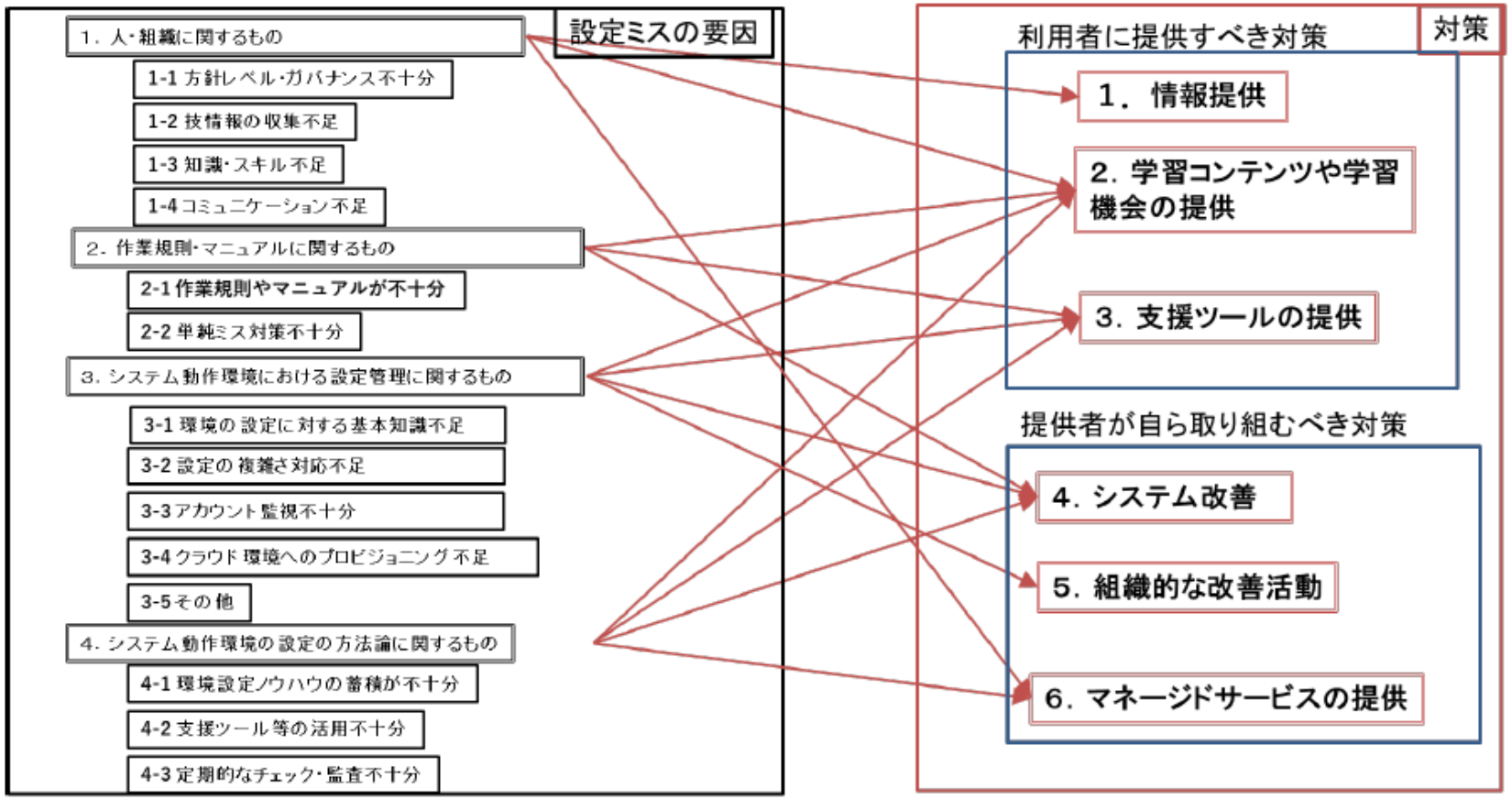
・分類した設定不備の要因に対応する利用者側の対策を導き出し、関連性を基準に整理・体系化。組織体制・人材育成等の4大項目に整理



（出所）総務省「クラウドサービス利用・提供における適切な設定のためのガイドライン（2022年10月）」より引用

(3) 事業者側の対策

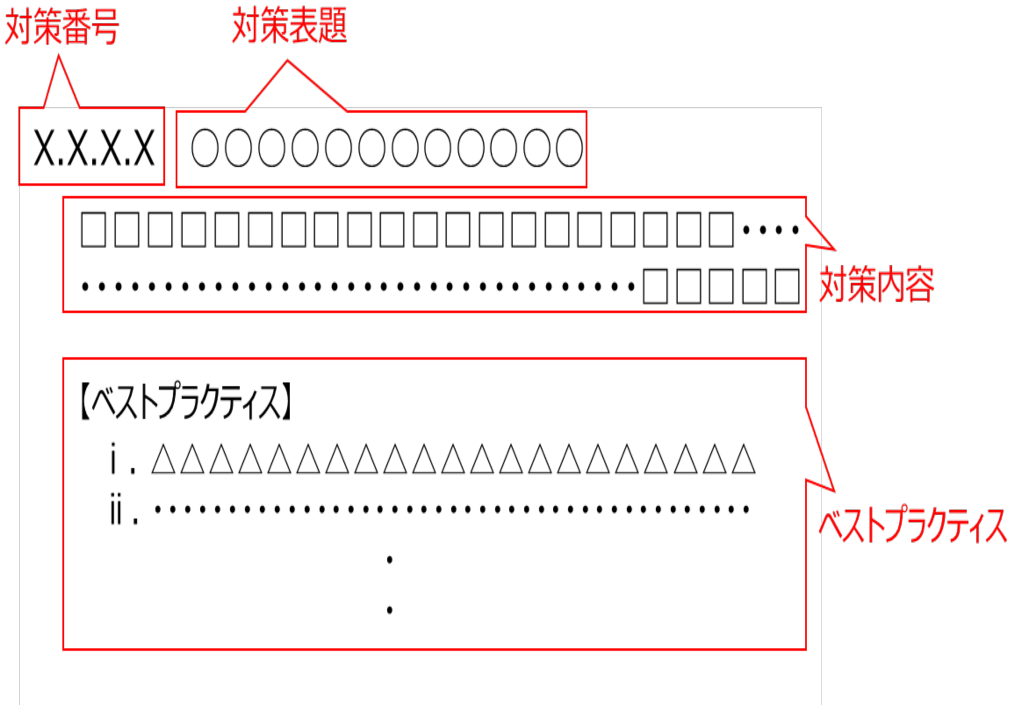
・同様に、設定不備の要因に対応する、①利用者に提供すべき対策と、②事業者が自ら取り組むべき対策を、関連性を基準に整理・体系化



（出所）総務省「クラウドサービス利用・提供における適切な設定のためのガイドライン（2022年10月）」より引用

(4) 個別対策毎に提供される情報

・本ガイドラインでは、個別対策毎に、実施すべき具体的な内容と、参考となるベストプラクティスが纏められている



対策番号
各対策表題に対して一意に割り振られた番号

対策表題
設定不備の抑止・防止のために実施すべき事項として、指標となるもの

「基本」：基本的に実施することが求められる設定不備対策
「推奨」：高い「機密性」「可用性」「完全性」が求められるクラウドで実施することが望ましい対策

対策内容
対策表題で示した事項について、事業者や利用者が実施すべき対策

ベストプラクティス
対策を実施するに当たって、参考となる具体的な実施手法や注意点

（出所）総務省「クラウドサービス利用・提供における適切な設定のためのガイドライン（2022年10月）」を元に作成

(5) 個別対策毎に提供される情報例①（利用者側）

・利用者側の例として「設定項目の管理」をみると、対策として予防的措置と発見的措置を実施できる体制構築、ベストプラクティスとして、ツール・診断サービスの活用や、設定値を監視し自動復元させる仕組みの組み込み等が示されている

Ⅲ．２ 作業規則・マニュアル	
Ⅲ．２．１ 作業規則やマニュアルの整備	
Ⅲ．２．１．１	作業規則の整備
Ⅲ．２．１．２	作業手順書の整備
Ⅲ．２．１．３	ヒューマンエラー対策
Ⅲ．２．１．４	作業手順書に係るマネジメント
Ⅲ．３ クラウドシステム動作環境の設定管理	
Ⅲ．３．１ クラウドセキュリティに係る設定項目の確認	
Ⅲ．３．１．１	設定項目の把握と設定
Ⅲ．３．１．２	設定項目の管理
Ⅲ．３．２ クラウドシステムにおける動作環境のプロビジョニング	
Ⅲ．３．２．１	変化への適応及び体制整備

Ⅲ．３．１．２【基本】設定項目の管理

設定項目の管理の仕組みとして、設定不備のリスクを顕在化させないための措置（予防的措置）と顕在化しても即時に対応できる措置（発見的措置）を実施できる体制を構築すること。

【ベストプラクティス】

i. 管理については、サードパーティやクラウドサービス事業者から提供される設定項目の可視化ツール等を利用する。
ii. 初期の設定だけでなく、設定値の監視の仕組み等を構築する。（予防的措置）
iii. 外部の設定値診断サービス等を活用して定期的に設定値の診断を行う。（予防的措置）
iv. 設定が変更されたことが検知されたら、なるべく早く適正な設定値に戻す、又は自動で復元する仕組みを組み込んでおく。（発見的措置）

IaaS/PaaSを利用している場合

v. 侵害テスト（ペネトレーションテスト）により、リスクのある設定不備を検出する（発見的措置）

（出所）総務省「クラウドサービス利用・提供における適切な設定のためのガイドライン（2022年10月）」を元に作成

(5) 個別対策毎に提供される情報例①（事業者側）

BANK OF JAPAN

・事業者側の例として「十分な情報の提供」をみると、対策として組織的な設定に関する情報提供、ベストプラクティスとして、情報開示認定制度の活用やSOC2レポートの取得を挙げている

Ⅳ．２ 情報提供	
Ⅳ．２．１ 正しい情報の提供	
Ⅳ．２．１．１	正しい情報の提供
Ⅳ．２．２ 十分な情報の提供	
Ⅳ．２．２．１	十分な情報の提供
Ⅳ．２．３ わかりやすい情報の提供	
Ⅳ．２．３．１	わかりやすい情報の提供
Ⅳ．２．４ 利用者別の対応	
Ⅳ．２．４．１	利用者の特性に応じた情報提供
Ⅳ．２．５ タイムリーな情報提供	
Ⅳ．２．５．１	システム動作環境の変更等に伴うタイムリーな情報提供
Ⅳ．２．５．２	公開されたぜい弱性の影響に伴うタイムリーな情報提供

Ⅳ．２．２．１【基本】十分な情報の提供
組織としてシステム動作環境の設定に関する十分な情報を確実に提供すること。

【ベストプラクティス】
i. 情報の開示については、クラウドサービスが十分な情報開示ができているかを審査する、情報開示認定制度があるので、取得を検討する
ii. 第三者評価レポート（SOC2レポート等）を取得しクラウドサービス利用者に開示するのも、自社サービスに関する情報提供のための有効な手段である
iii. 第三者認証や認定の取得に関して、取得状況について自社のWebサイトで発信していくことも情報提供として有効である

（出所）総務省「クラウドサービス利用・提供における適切な設定のためのガイドライン（2022年10月）」を元に作成

４．本ガイドラインの活用案

(1) 金融機関内での活用

・本ガイドラインは設定チェックリストの機能を有することから、金融機関内での活用案として、システム部等におけるリスク管理の枠組み強化や、監査部署の機能向上に繋げることが考えられる

優れた設定のチェックリスト

― 弊行やFISCの関連基準（注）との関係では、設定が中心で焦点が異なることから、相互補完のメリットが期待できる

（注）日本銀行 FSR別冊「クラウドサービス利用におけるリスク管理上の留意点」の別紙「クラウドサービス利用において必要な管理項目と具体的な取組事例」
FISC「金融機関等コンピュータシステムの安全対策基準」「金融機関等におけるクラウド導入・運用に関する解説書（試行版）」

システム部等における、クラウドのリスク管理の枠組み強化

監査部署における、クラウドに関するポイントを押さえた確認

(2)金融機関外での活用

・金融機関外での活用としては、業界によらないガイドラインである特徴を活かし、SIer、業務委託先、クラウド事業者との対話のツールとしての利用が考えられる

業界によらないガイドライン

― 相手の業界によらず、クラウドのリスク管理に関する対話の、共通の土台として利用できる

SIerとの対話

― 例えば、システム運用委託先との、クラウドに関するリスク管理に関する対話

業務委託先との対話

― 例えば、業務のBPO先との、情報管理に関する対話

クラウド事業者との対話

― 例えば、事業者の情報提供体制や、利用者支援ツールに関する対話

(3) ガイドブックの活用

・本ガイドラインのエッセンスを平易に解説したガイドブックが今後公表される予定。「クラウドの設定」の重要性について、経営層やシステム部門以外の部門からの理解を得るうえで、このガイドブックを活用していくことが考えられる

読みやすいガイドブック

― 本ガイドラインの普及と利用促進を目的に、エッセンスを平易に解説

システムに苦手意識のある層への啓蒙

― 例えば、経営層やシステム部門以外の部署に読んでもらい、設定の重要性を理解してもらう（「良きに計らえ」の解消）