別紙3

くらしの中に
総務省
MIC Ministry of Internal Affairs and Communications

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

令和４年10月

総務省 サイバーセキュリティ統括官室

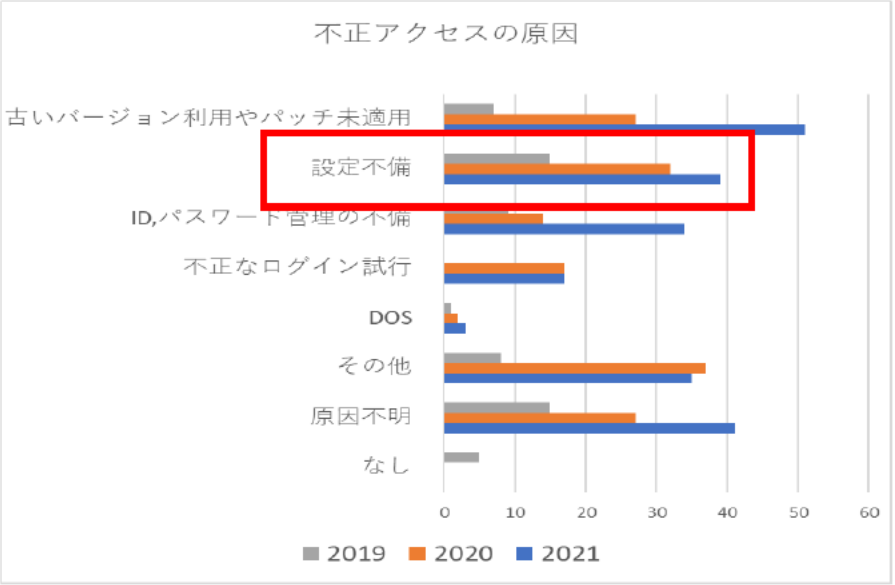
ガイドライン作成の背景

■ クラウドサービスを利用する際の設定ミスに起因する障害や情報漏えいといった事故が多発している。
■ 不正アクセスの原因として、設定不備が多い状況にある中で、クラウドサービスの適切な設定の促進を図り、安心安全なクラウドサービスの利活用を推進していくため、推奨されるセキュリティ対策を指針として示している。

事例１	クラウドサービス提供事業者が、提供しているSaaSの機能変更を行った。これに伴い、当該SaaSのユーザーアクセスに関する設定について、結果的にデフォルトでセキュリティレベルが下がってしまった。利用企業側はこれに気づかず、低いセキュリティレベルのまま利用し続けた結果、機密情報が大量に流出した。
事例２	企業従業員が個人的にクラウドサービスを利用し、自社の業務で利用する機密情報を格納していた。後にこれらのファイルが公開設定であったことが外部からの指摘で判明した。
事例３	ある企業の業務委託先が、サーバからクラウドサービスへのデータ移行を行う際に、ストレージの設定を公開設定としていた。これにより長期間機密情報が公開されている状態になった。

上記の事例の要因としては以下のような点が挙げられる。

・利用企業におけるクラウドサービス設定値に関する理解の不足と使用しているクラウドサービスに関する情報の不足
・委託先管理やシャドーITへの対応策などの体制面の不備
・設定不備を抑止するための体系的な対策の不備



出典：「コンピュータウイルス・不正アクセスの届出状況」，2018~2021年，独立行政法人 情報処理推進機

ガイドラインの位置づけ

■ 「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）をベースに、「クラウドサービスの設定」に特化し、クラウドサービス利用側、提供側それぞれを対象に、実施することが望ましい対策を記載。

■ 利用側としては、クラウドサービスの適切な設定を促進する趣旨から、個人として利用し設定等を行わないエンドユーザではなく、企業内においてサービス全体の動作に関わる設定を行う者を主たる対象としている。

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
-セキュリティに係る設定項目の確認
-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

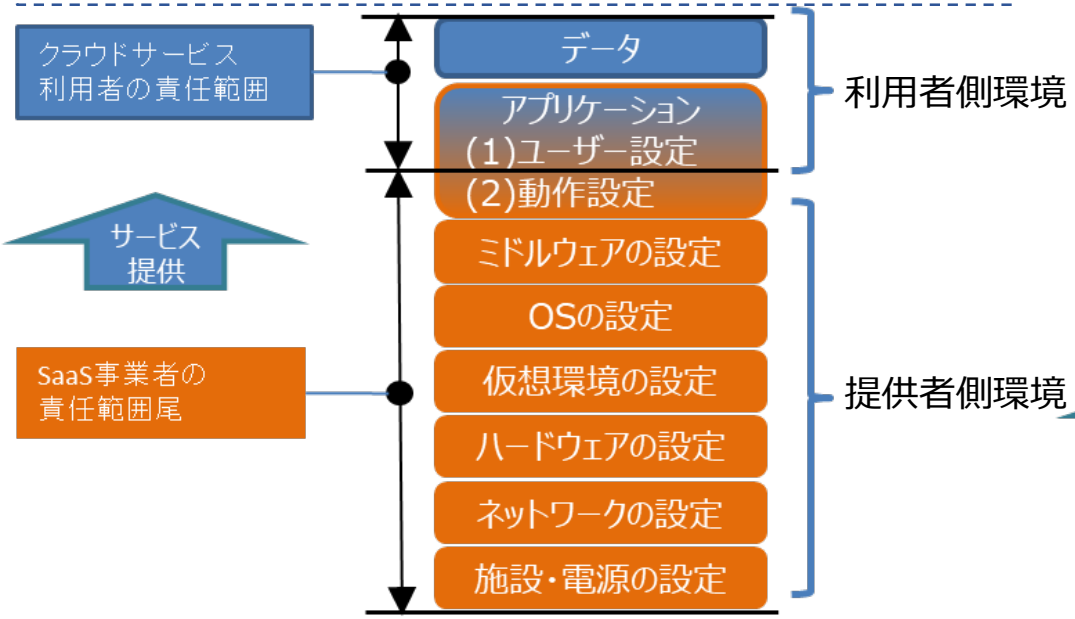
想定読者		主に読んでいただきたい部分		
分類	小分類	Ⅱ.前提および概要	Ⅲ.クラウドサービス利用側に求められる対策	Ⅳ.クラウドサービス提供側に求められる対策
①クラウドサービス利用者	経営層・セキュリティ管理者	◎	◎	-
	クラウドサービス管理者	◎	◎	-
	（狭義の）クラウドサービス利用者	◎	◎	-
	社内向けクラウドサービス開発者	◎	◎	◎
②SIer	-	◎	◎	-
③SaaS事業者	-	◎	○	◎
④IaaS/PaaS事業者	-	◎	-	◎

クラウドサービス事業者とクラウドサービス利用者の責任と役割

- クラウドサービスの情報セキュリティを高めるためには、クラウドサービス事業者とクラウドサービス利用者が協力して、クラウドサービスに対する責任を共有することが必要（責任共有モデル）。
- クラウドサービスの適切な設定を促進するためには、クラウドサービス事業者が適切な設定のための対策を施したサービス提供やわかりやすい情報提供を行うとともに、クラウドサービス利用者がそれを受けて適切な設定を行うという両者の協力が重要。

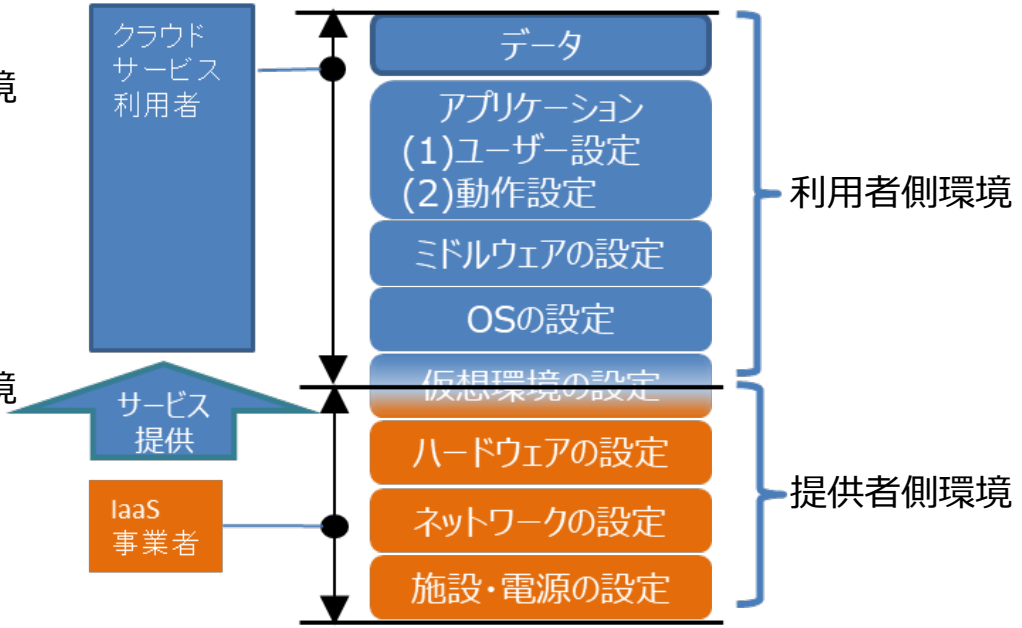
＜SaaSの場合＞

クラウドサービス利用者の責任：
データとアプリケーションの範囲の一部（利用者アカウントや業務データの設定）
SaaS事業者の責任：
アプリケーションの動作に係る設定等提供するアプリケーション以下の提供側環境の設定



＜IaaSの場合＞

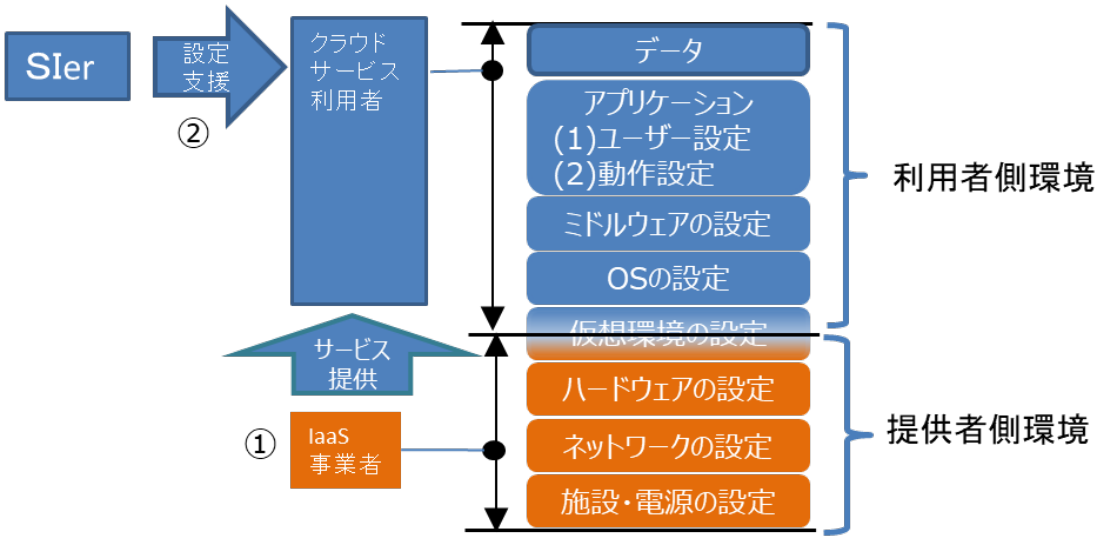
クラウドサービス利用者の責任：
仮想環境上で動作しているOSを含むすべてのソフトウェアの管理
IaaS事業者の責任：
ゲストOS等が動作するための仮想環境の構築と管理等提供する仮想環境以下の提供側環境の設定



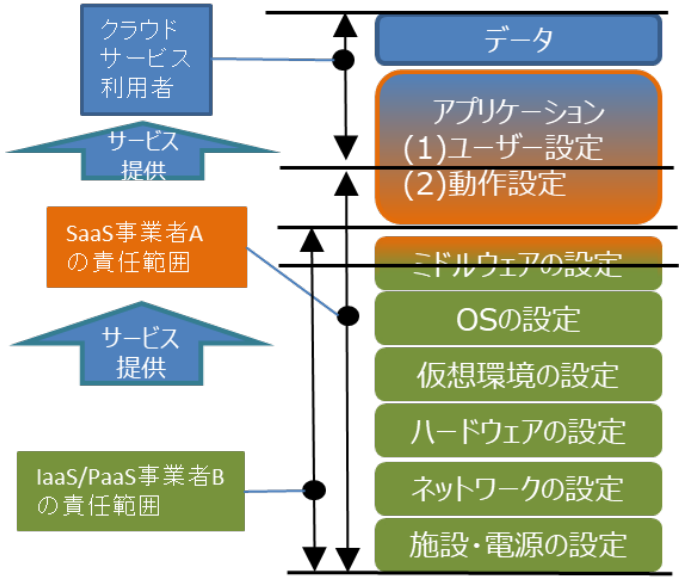
留意すべき責任共有モデル

- 日本のクラウドサービス利用の特徴として、運用保守をSIer等に外注していることがあげられる。
- 留意すべき責任共有モデルのパターンとして、以下のようなものがある。
  ①SIerが設定作業を行う場合は、通常、準委任契約となり、作業についてはSIerが責任を負うが、最終責任はクラウドサービス利用者となる。
  ②他社のPaaSを利用してSaaSを提供する場合、SaaS事業者がクラウドサービス利用者との契約者であることから、提供するクラウドサービス全体の管理責任を負う

＜ SIerが関与する場合＞



＜SaaS事業者が他社のIaaS/PaaSを利用する場合＞



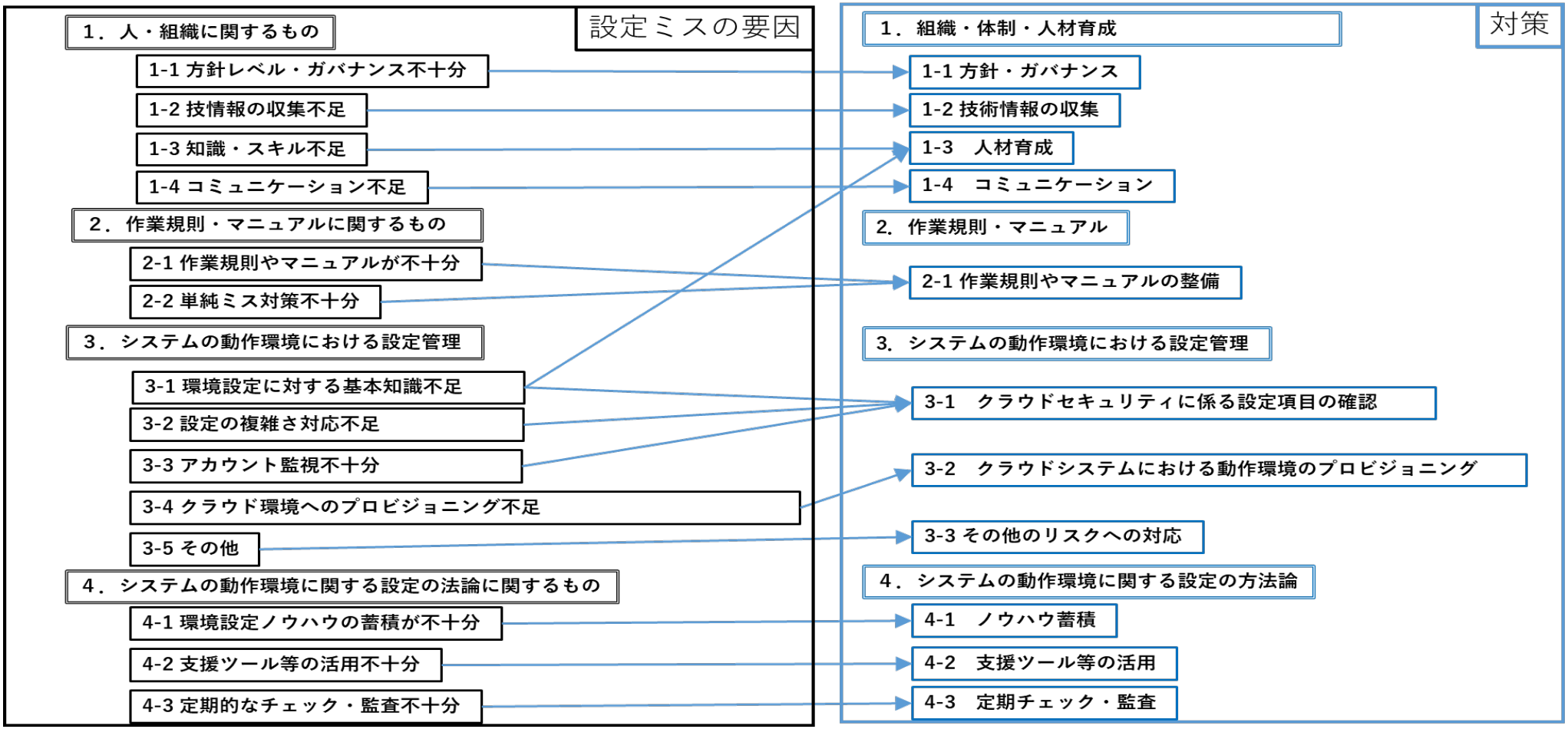
クラウドの設定項目の類型と設定不備の場合のリスク

■ 米国CIS(Center for Internet Security)が発行するCIS Benchmarks®で示されている主要なクラウド基盤の各製品におけるセキュリティ設定項目を比較し、設定項目を類型化して分類。
■ 各設定項目の類型について、設定不備があった場合のリスクは下表のとおり。

No.	セキュリティ設定項目の類型	考えられるリスク
1	IDとアクセス管理（IAM）	・一般利用者と管理者を明確に分離して認証の設定・管理を行わないことで、管理者権限の設定が甘いものとなり、外部からハッキングされるリスク ・アクセス管理を厳密に設定しないことで、アクセス管理に不慣れな一般利用者が不注意で個人情報を公開してしまうリスク ・退職者のユーザIDやパスワードの失効させずに放置することにより、不正に利用されるリスク ・ゲストユーザーの権限を適切に設定しないことによりゲストユーザに想定外の情報が漏えいしてしまうリスク ・サービスアカウントにおいて、APIのアクセスキー及びシークレットキー（クレデンシャル情報）の設定管理が不十分でシステム全体の乗っ取りが発生するリスク
2	ロギングとモニタリング	・デフォルトのロギングオフ設定の解除を忘れて、モニタリングが機能しない、異常が起きても気が付かないなどのリスク ・OSS（Open Source Software）のログ監視ソフトのぜい弱性をつかれて情報漏えいするリスク
3	オブジェクトストレージ	・オブジェクトストレージのアクセス権設定を厳密に行わずに情報漏えいを起こすリスク ・ライフサイクル設定を適切に行わずに、データ喪失を引き起こすリスク
4	インフラ管理	
4.1	仮想マシン（VM,VPS）	・仮想マシンのセキュリティパッチを怠り、不正アクセスを受けたり、マルウェアに感染するリスク
4.2	ネットワーク	・基本的なネットワークセキュリティの設定を確実に行わずに利用することで、不正アクセスやマルウェア感染のリスク
5	セキュリティ等の集中管理	・IaaS/PaaSが提供する各種の集中管理機能は、デフォルトで起動していないことが多く、起動しないままでは広範囲に及ぶインシデント等が発生するリスク
6	IaaS／PaaSが提供する、その他のサービスや機能	
6.1	鍵管理	・秘密鍵をKMS（鍵管理システム）や暗号化を用いずにオブジェクトストレージ等に保管すると、サーバが不正アクセスを受けたり、マルウェアに感染した場合に、攻撃者に鍵が漏えいし、情報漏えいや不正操作につながるリスク
6.2	PaaSが提供するアプリケーション	・クラウドでアプリケーションを提供する事業者から提示されるアクセス許可などの設定やデフォルトの公開範囲等の設定を確実に行わないことで、不正アクセスなどが起こるリスク
6.3	データベース	・クラウドで使用するデータベースの保護、監査、暗号化などの設定及びデフォルト設定値の確認を確実に行わないことで、不正アクセスを受け、情報漏えい等を引き起こすリスク
6.4	コンテナ	・クラウドサービスのアプリケーション構築で広く利用されているコンテナそのものとコンテナ管理システムに対するセキュリティ設定を確実に行わないことで、不正アクセスやコンテナを標的にしたマルウェアの感染リスク
7	その他の設定項目	上記以外のクラウドサービス事業者が提供する統合資産管理、モバイルデバイス管理、バックアップ等のサービスについてはIaaS/PaaS事業者から提示されるセキュリティ設定を適切に設定しないと広範囲に及ぶインシデント等が発生するリスクがある。

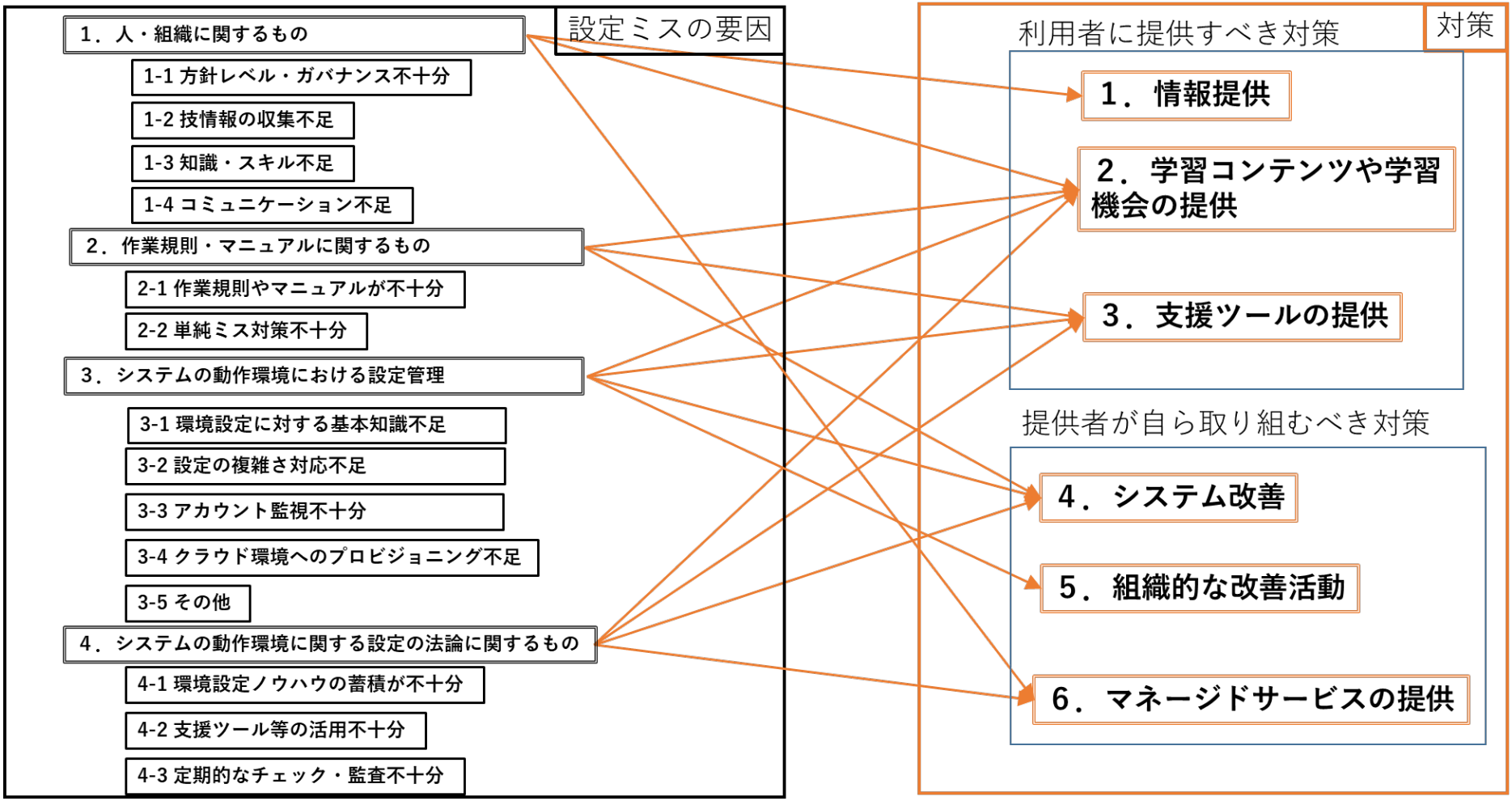
設定不備の要因と対策（クラウドサービス利用側）

- クラウドサービス利用者及びクラウドサービス事業者に対するヒアリング調査の結果と公開事例の調査結果から得られた個々の原因を、４Ｍのフレームワーク（Man,Manual,Machine,Method）で分類。＜設定ミスの要因＞
- さらに、それぞれの要因に対する対策を導き出し、親和性の高いものについてグループの整理を実施。＜対策＞



設定不備の要因と対策（クラウドサービス提供側）

■ クラウドサービス提供側についても同様に、設定ミスの要因の導出と、対応する対策の分類を行った。



クラウドサービス利用側に求められる対策

■ P.6で整理したクラウドサービス利用側に求められる対策項目の内容は以下のとおり。

Ⅲ　クラウドサービス利用側に求められる対策	
Ⅲ．１　組織体制・人材育成	
Ⅲ．１．１　クラウドサービス設定不備の抑止・防止に係る方針的事項	クラウドサービス利用において、ガバナンスの確保やルール形成、人材育成への取組などの組織的方針を明確にする。
Ⅲ．１．２　技術情報の収集	各種設定値の変更等の技術情報を日頃から収集し、リスク分析対策立案のサイクルを組織的に確立する。
Ⅲ．１．３　人材育成	クラウドサービスの設定におけるリテラシーの向上や動作環境設定における技術力の向上を確実にする。
Ⅲ．１．４　コミュニケーション	組織として利害関係者との窓口の明確化、定期的な情報交換を行うと共に、コミュニケーションのルートと方法を確立する。
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	クラウドシステムの設定について作業規則及び作業手順を整備し、定期的に見直す。併せてヒューマンエラー対策を組み込む。
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	自社で利用するクラウドサービスの設定項目を理解し、予防的措置と発見的措置を実施できる体制を構築する。
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	クラウドシステムの仕様変更や機能追加等により、デフォルトの設定値が変更されるなどの変化に準備し対応する。
Ⅲ．３．３　その他のリスクへの対応	課金管理や日本国以外の法律が適用されるリスクなど様々なリスク対応について明確にし、対応方針を文書化する。
Ⅲ．４　クラウドシステム動作環境に関する設定の方法論	
Ⅲ．４．１　ノウハウの蓄積	設定方法について組織のノウハウとして蓄積するため、マニュアル化、ツール導入などを行う。
Ⅲ．４．２　支援ツール等の活用	複雑化する設定項目の管理について設定不備の検出ツールや監視ツールなどの支援ツールを活用する。
Ⅲ．４．３　定期的な設定値のチェックと対応	設定項目について定期的なチェックを行うとともに、内部監査や外部診断などを行う。

（参考）クラウドサービス利用側のベストプラクティスの例

■ 各対策内容については、どのようなクラウドサービスでも実施すべき【基本】と、高い「機密性」「可用性」「完全性」を求められるサービスにおいて実施することが望ましい【推奨】に分類した上で、参考となる具体的な実施手法等をベストプラクティスとしてまとめている。
■ 設定項目の確認時、社内でのチェックやSier等との調整に活用できるよう設定項目の類型と対策のリストをベストプラクティスとして提示。

■対策内容

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**	典型的なクラウドの設定項目について知り、自社で利用するIaaS/PaaSの設定項目を把握し設定すること。（クラウドサービスの設定についてSIerが支援する場合は、双方において良く確認を行うこと）	基本
Ⅲ．３．１．２	**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（予防的措置と呼ぶ）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。	基本

■ベストプラクティス

No.	セキュリティ設定項目の類型	類型項目における推奨設定の概要
1	**ＩＤとアクセス管理（IAM）**	IDとアクセス管理とは、「誰が」「どのリソースに対し」「どのような操作ができるか」を定義し、アクセス制御を実現するために提供されているサービスである。管理者はクラウド全体のセキュリティに関与するため、管理者アカウントとユーザアカウントを分離し、管理者アカウントには多要素認証を必須にする等の設定を確実に行うほか、組織の要件に応じてユーザアカウントのIPアドレス制限など各種設定を確実に行う必要がある。特にゲストユーザーについては、不要な情報公開を避けるため、必要最小限の権限とする。また、暗号化キーは統合管理サービスで集中管理することを推奨する。なお、管理者がIDとアカウントを網羅的に把握する仕組み（申請ベースで中央での払い出し、CASBによる新規アカウントの個別発行不可等）を設ける必要がある。
2	**ロギングとモニタリング**	ロギングは、クラウドにおける挙動やアラート発報の基本となるものである。デフォルトでは、アクティブになっていないサービスもあるので、適切にロギング設定を行い、アラートや監査を行えるようにしておく必要がある
3	**オブジェクトストレージ**	クラウド利用におけるオブジェクトストレージのセキュリティでは、データの外部漏えいに備えて暗号化等が基本となるが、暗号化キーの管理方法なども重要となる。また、オブジェクトストレージの公開設定などデフォルト値も確認しておく必要がある
4	**インフラ管理**	
4.1	**仮想マシン（VM,VPS）**	物理サーバを論理的に分離する仮想マシンを利用する際、仮想マシン のディスク暗号化、エンドポイント保護などの設定を確実に行う必要がある。また、ホスト OS、ゲストOS 等の最新パッチ、ウイルス対策（AV、EDR等）の設定及びその監視・運用（MDR、SOC等）についても留意する必要がある。
4.2	**ネットワーク**	クラウド利用は、インターネット経由となるため、外部ネットワークとのアクセスに関する基本的なセキュリティ設定、仮想プライベートクラウドのセキュリティ設定、Firewall/IPS/IDSやWAFなどによる境界防護および境界内防護等に関する設定を確実に行う必要がある。加えて、重要情報を扱うシステムでは、信頼できるVPNによる通信の暗号化などのネットワークセキュリティ対策を検討する。
5	**セキュリティ等の集中管理管理**	IaaS/PaaSが提供するセキュリティ集中管理機能、キーマネジメントサービス、運用管理コンソール、監査ツール、コスト管理サービスなど、構成管理を横断的に集中管理可能なツールやサービスを積極的に利用することを推奨する。これらはデフォルトでは有効化されていない場合があるため、有効化のための設定確認を推奨する。
6	**IaaS／PaaSが提供する、その他のサービスや機能**	※これらは、短期間で新しく追加される。下記の項目以外にも追加された時点で、設定値についても確認を行う必要がある。
6.1	**鍵管理**	鍵管理は安全に秘密鍵を管理・作成・制御する方法を提供する。暗号化鍵の管理に係る設定については、IDとアクセス管理、ロギングとモニタリング等とも関連し、集中管理するサービスを提供するクラウドもある。使用するクラウドに応じた適切な設定を行う必要がある。
6.2	**PaaSが提供するアプリケーション**	クラウドで提供されるアプリケーションには様々なものがあるが、個々の事業者から提示されるアクセス許可などの設定やデフォルトの公開範囲等の設定を確実に行う必要がある
6.3	**データベース**	クラウドで使用するデータベースの保護、監査、暗号化などの設定及びデフォルト設定値の確認を確実に行う必要がある。
6.4	**コンテナ**	コンテナとは、ホストOS 上で「コンテナエンジン」と呼ばれるシステムを動作させ、「コンテナ」と呼ばれる実行環境を複数構築する技術である。コンテナを利用する際は、コンテナエンジンに係るセキュリティ関連の設定を確実に行う必要がある。
7	**その他の考慮事項**	上記以外のクラウドサービス事業者が提供する統合資産管理、モバイルデバイス管理等のサービス等については、個々の事業者から提示されるセキュリティ設定を確実に行う必要がある。また、これらはデフォルトでは起動していないことが多いので、起動のための設定値を確認することを推奨する。

クラウドサービス提供側に求められる対策①

■ P. 7 で整理したクラウドサービス提供側に求められる対策項目の内容は以下のとおり。

Ⅳ　クラウドサービス提供側に求められる対策	
Ⅳ．１　組織体制・人材育成	
Ⅳ．１．１　クラウドサービス設定不備の抑止・防止に係る方針的事項	クラウドサービス提供において、ガバナンスの確保やツール提供、人材育成への取組などの組織的方針を明確にする。
Ⅳ．２　情報提供	
Ⅳ．２．１　正しい情報の提供	設定マニュアル等については、複数人のチェックを行うなど、ドキュメントの品質管理の問題として組織で対応を行う。
Ⅳ．２．２　十分な情報の提供	クラウドサービス事業者には自社サービスの説明責任があることから、責任分担も含めた設定に関する十分な情報を提供する。
Ⅳ．２．３　わかりやすい情報の提供	ITに詳しくない利用者にも配慮し、各設定の背景や選択した場合の影響を説明する。マニュアルは、読みやすく適切な分量とする。
Ⅳ．２．４　利用者別の対応	利用者の業務環境ごとに必要な設定が異なる場合に配慮して、利用者ごとの特性に応じた情報を提供する。
Ⅳ．２．５　タイムリーな情報提供	機能変更やぜい弱性対応など、すぐに対応すべき設定変更があることに配慮し、タイムリーな情報提供を行う。
Ⅳ．３　学習コンテンツや学習機会の提供	
Ⅳ．３．１　学習コンテンツの提供	利用者の知識不足や理解不足による設定ミスを減らすため、体系的、網羅的なわかりやすい学習コンテンツを提供する。
Ⅳ．３．２　学習機会の提供　－　環境の設定に関する説明	利用者の設定に関する学習のため、セミナーや研修を開催する他、情報共有のためのユーザー同士のコミュニティ形成を行う。
Ⅳ．４　利用者支援ツールの提供	
Ⅳ．４．１　設定項目管理ツールの提供	設定項目管理ツールを提供することにより、利用者の管理作業を軽減し、設定ミスを削減する。
Ⅳ．４．２　設定項目診断ツールの提供	もし設定ミスが発生しても、問題化する前に発見し修正するためのツールとして設定項目診断ツールを提供する。

クラウドサービス提供側に求められる対策②

Ⅳ．５　システムの改善　－　ミスが発生しにくいシステムの提供	
Ⅳ．５．１　設定方法の見直し	設定値をリストから選択する方式や、ヘルプウィンドウを表示する機能などにより、設定ミスが発生しにくいシステムを開発する。
Ⅳ．５．２　デフォルト値の見直し	デフォルト値がそのまま変更されなかったため情報漏えいに至ったケースが多発している。デフォルト値は可能な限りセキュリティの高い設定とする。
Ⅳ．５．３　セルフチェック機能の追加	クラウドサービス利用者が設定作業を行う際に、作業完了前にチェックできる機能を設ける。
Ⅳ．５．４　利用者における設定機会の削減	人為的なミスを削減するため、利用者が自身で設定する項目を削減するよう努める。
Ⅳ．５．５　暗号化機能の提供	万が一設定不備により情報が漏えいした場合の対策として、重要な情報に対する暗号化機能を提供する。
Ⅳ．６　継続的な改善　－　ＰＤＣＡを回す	
Ⅳ．６．１　情報収集	利用者からのフィードバック、公的機関からの情報、ベンダーから提供される情報などは確実に収集する。
Ⅳ．６．２　サービスの改善	収集した情報を社内の改善計画に反映し、システム改善、マニュアルの改訂等のサービス改善を行う。
Ⅳ．７　マネージドサービスの提供	
Ⅳ．７．１　マネージドサービスの提供	管理、運用まで含めて請け負う「マネージドサービス」を提供することにより、利用者の設定作業の負担を軽減する。

（参考）クラウドサービス提供側のベストプラクティスの例

■ 提供側によるわかりやすい情報の提供について、注意すべき点についてもベストプラクティスとして示したことに加え、関連性の高い日本語化の問題をコラムとして提示。

■対策内容

Ⅳ．２　情報提供			
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**	組織としてシステム動作環境の設定に関するわかりやすい情報を確実に提供すること。	基本

■ベストプラクティス

i. 各設定値の意味や背景となるセキュリティポリシーを解説するとともに、その設定値を選択した場合の影響等についても説明する必要がある。例えば暗号化設定の選択肢では、ぜい弱なものはその旨を明示する必要がある。
ii. 具体的な環境の設定に関する例を示すことも有効である。
iii. セキュリティ上のリスクがある設定など、特に注意が必要な箇所は必ず読まれるように工夫することが必要である。
iv. 分厚いマニュアルは読む気がしなかったり、読んでも理解できなかったりすることが多い。適切な分量のマニュアルを作成するとともに、要約版や検索ツールも同時に提供することが望ましい。
v. 利用者が行う環境の設定を動画で提供する企業が増えている。文字の情報だけでなく、画像や映像による情報提供はクラウドサービス利用者の理解を助ける。

＜コラム＞　日本語（化）の問題

海外で開発されたサービスを日本で提供する場合、翻訳（日本語化）の際に十分注意する必要がある。翻訳された日本語がわかりにくかったために、設定ミスが起きた事例がある。設定メニューや設定マニュアル等の翻訳の際には、日本語がネイティブな担当者が最終チェックをすることが望ましい。

なお、国内企業の日本語母語話者が作成したマニュアルでも意味がわかりにくいものがあるので、組織としてのレビューが必要なのは同様である。