クラウドを利用したシステム運用に関するガイダンス（概要）

クラウドサービスを利用する重要インフラ事業者において、適切なシステム運用をしていただけるよう、「クラウドを利用したシステム運用に関するガイダンス」を2021年11月に策定しました。

- クラウドサービスは便利ですが**リスク**もあります
- **誰がどの範囲まで責任を持つ**のかステークホルダー間で認識を共有しましょう
- システム構築・運用時の**注意点**
- 普段からステークホルダー間で**コミュニケーション**を実施しましょう
- **インシデント発生時に対応できる体制**を整え、対応しましょう

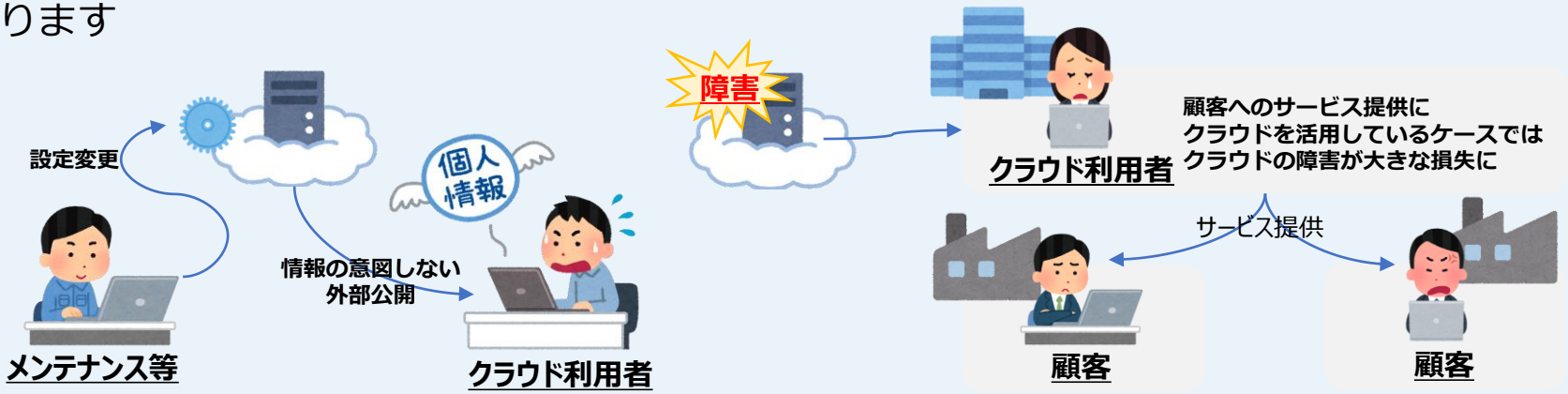
資料はこちら：
https://www.nisc.go.jp/policy/group/infra/cloud_guidance.html
御意見などはこちら：
重要インフラ基準等受付
nisc-infra-kijyun@cyber.go.jp

内閣官房内閣サイバーセキュリティセンター
重要インフラ第1グループ

クラウドサービスは便利ですがリスクもあります

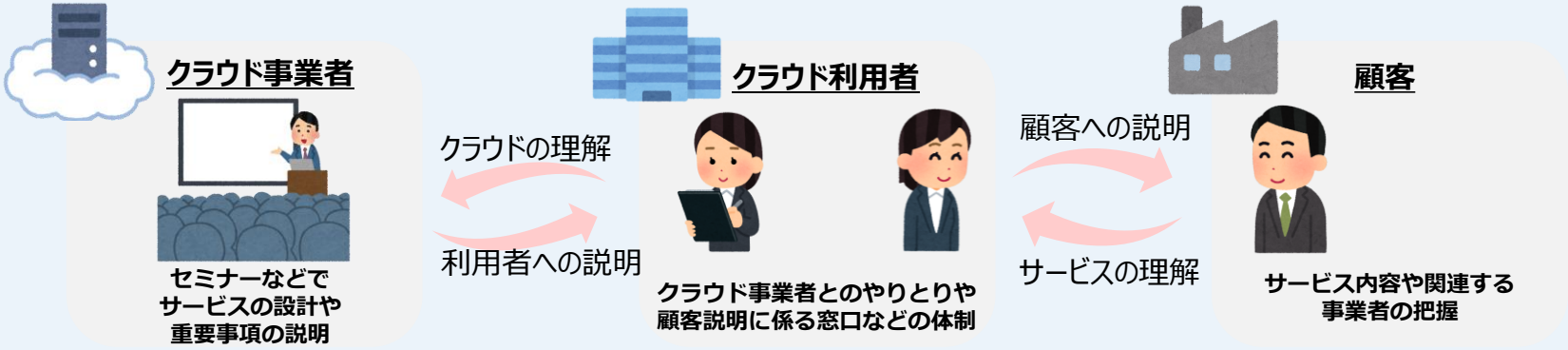
● クラウドサービス利用におけるリスク

設定不備による**情報漏えい**、クラウドサービス**障害の影響の波及**といったリスクがあります



● クラウドサービスのリスク管理

このようなリスクを正しくマネジメントするためには、**ステークホルダーとの連携**が欠かせません。



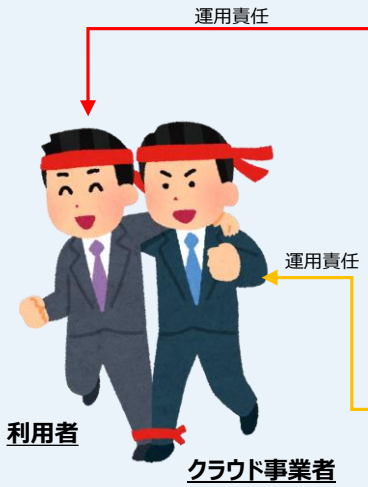
誰がどの範囲まで責任を持つのかステークホルダー間で認識を共有しましょう

● 責任共有モデル

クラウドサービスは、
- クラウド事業者
- 利用者

それぞれで**運用責任を共有**しており
二人三脚で成り立っているサービスです。

管理するデータや設定情報などについては利用者側の責任であることを
意識する必要があります。



区分	IaaS	PaaS	SaaS
設定	ポリシー	ポリシー	ポリシー
	設定	設定	設定
	端末	端末	端末
アプリ	データ	データ	データ
	アプリケーション	アプリケーション	アプリケーション
環境	ランタイム	ランタイム	ランタイム
	ミドルウェア	ミドルウェア	ミドルウェア
	コンテナ管理機能	コンテナ管理機能	コンテナ管理機能
OS	オペレーティングシステム	オペレーティングシステム	オペレーティングシステム
仮想化	仮想化ソフトウェア	仮想化ソフトウェア	仮想化ソフトウェア
	ハードウェア	ハードウェア	ハードウェア

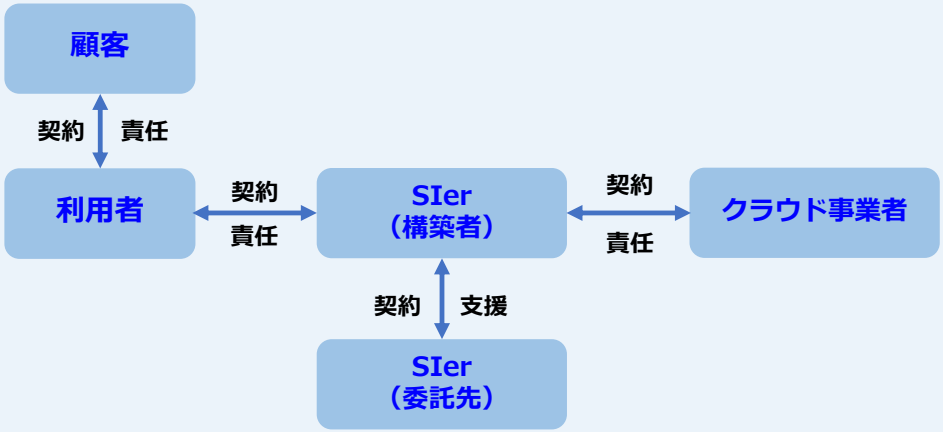
利用組織が管理　クラウド事業者が管理

基本的なクラウドサービスの責任共有モデルの考え方

● ステークホルダー

とりわけ日本においては、
システムインテグレーター（SIer）が
利用者から業務を請け負い、
クラウド事業者に代わりクラウドサービスを
提供するケースが少なくありません。

サービス利用に係る**それぞれのステークホルダーがどのような契約関係**にあるのか、
留意するようにしましょう。



クラウドサービスに係るステークホルダーの例

システム構築・運用時の注意点

● クラウド利用時（選定～運用）の注意点

クラウドサービスには、提供される機能や責任範囲毎に複数の選択肢が存在します。またサービス選定後も、いくつかの注意点が各工程毎に存在します。
利用にあたっては、クラウドサービスを利用する目的、目標を明確にした上で、**自組織に適したサービスを選定しましょう。**

SLA
(Service Level Agreement)

サポート内容等を参考に、様々な種類（IaaS/PaaS/SaaS）から自組織に適したサービスを選定する

利用するクラウドサービスの理解を深め、ステークホルダー間の役割分担を確認する

通常時/インシデント発生時の各ステークホルダーの責任範囲を明確にする

選定 → **設計** → **実装** → **検証** → **運用**

自組織の現状を把握し、インシデント発生時の運用も想定した設計を行う

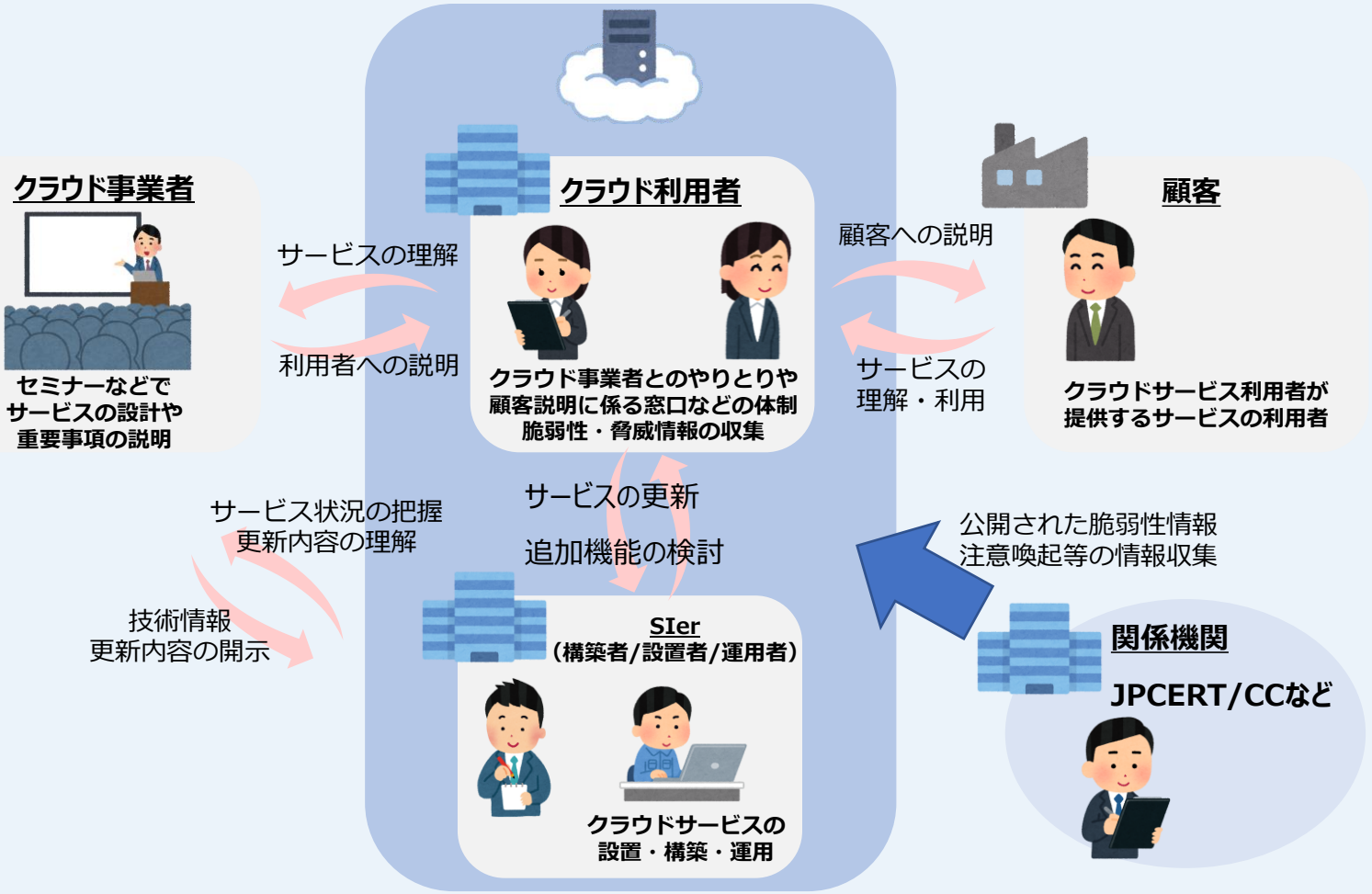
オンプレミス環境と同様、サービスのポリシーや設定が適切であることを、確認する

データ保護の措置について
クラウドサービスは物理サーバーを自組織内で所持しないため、サーバーの設置場所が国外である場合があります。サーバーおよび保管されるデータは設置された国の法規制の影響を受ける場合があり、その国の法制度や実施体制が十分でない場合はその国の法執行機関の命令により、データが強制的に開示されるリスクがあります。
データの開示が懸念される場合は「設計」の段階で、暗号化等によるデータ保護の措置について検討するようにしましょう。

普段からステークホルダー間でコミュニケーションを実施しましょう

● ステークホルダー間のコミュニケーション例

多くの場合、クラウドサービスを構築・運用する際にはステークホルダーが複数存在します。
ステークホルダー間で定期的にコミュニケーションをとり、**連絡体制の把握や相互の信頼関係の構築につとめる必要があります。**



インシデント発生時に対応できる体制を整え、対応しましょう

● インシデント発生時の対応

システムの停止判断、ログの分析、ステークホルダーへの情報共有などを実施しましょう。

インシデント発生時には、原因究明に努める必要があります。
インシデント対応が行えるように、あらかじめ**クラウド事業者が提供可能な情報について確認**しておくことや、
組織内でも**広報や法務に関係する窓口**について対応し、いつでも連携できる体制を構築しておきましょう。

また、インシデント発生時にどこの組織に調査や解析などをお願いするのか、事前に見当をつけておくことも大切です。
一組織だけで対応が難しい場合には、**コミュニティ団体等に参画し、協力してインシデントの解決**に取り組むようにしましょう。