別紙2

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の改定の概要

改定のポイント１

クラウド事業者がIoTサービスに参入しようとする際に注意すべきリスク、そのリスクに対する具体的な情報セキュリティ対策等を記載した実務的なガイドラインが求められる（※１）。

【改定】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に、**「IoTサービスを提供する際のリスクに対する対応方針」を追記**

（※1）関連するガイドラインとして「IoTセキュリティガイドラインVer1.0」（IoT推進コンソーシアム・総務省・経済産業省、2016年7月策定）があるが、これはIoT機器のライフサイクルに焦点を当ててリスクと対策を体系的に示したものである。

改定のポイント２

クラウド事業者が参照する情報セキュリティ対策ガイドラインとして、総務省では二つのガイドラインを公表しており、どちらを参照して良いか分かりにくい状況にある。

① ASP・SaaSにおける情報セキュリティ対策ガイドライン（2008年１月）
② 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（2014年４月）（※２）

【改定】**二つのガイドラインを統合**することとし、「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２版）」として**クラウド事業者が参照するガイドラインを一元化**

（※2）関連するガイドラインとして「クラウドサービスの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」（経済産業省、2011年4月策定・2014年3月改定）があるが、これは主にクラウドサービスの利用者を対象としたものである。

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２版）の構成

第２版の構成（５部構成）

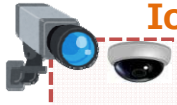
Ⅰ．序編
Ⅰ．1．はじめに
Ⅰ．2．ガイドラインの位置付け
Ⅰ．3．ガイドラインの活用の効果
Ⅰ．4．ガイドラインの全体構成
Ⅰ．5．ガイドラインの利用方法
Ⅰ．6．用語の定義
Ⅰ．7．参考文書

経営者等の組織管理者向け（第Ⅱ部）

Ⅱ．組織・運用編（注）
Ⅱ．1．情報セキュリティへの組織的取組の基本方針
Ⅱ．2．情報セキュリティのための組織
Ⅱ．3．連携クラウド事業者に関する管理
Ⅱ．4．情報資産の管理
Ⅱ．5．従業員に係る情報セキュリティ
Ⅱ．6．情報セキュリティインシデントの管理
Ⅱ．7．コンプライアンス
Ⅱ．8．ユーザサポートの責任

現場の技術担当者向け（第Ⅲ部）

Ⅲ．物理的・技術的対策編（注）
Ⅲ．1．アプリケーション、プラットフォーム、サーバ・ストレージ、ネットワークに共通する情報セキュリティ対策
Ⅲ．2．アプリケーション、プラットフォーム、サーバ・ストレージ
Ⅲ．3．ネットワーク
Ⅲ．4．建物、電源（空調等）
Ⅲ．5．その他



IoTサービス関連（第Ⅳ部）

改定のポイント１

Ⅳ．IoTサービスリスクへの対応方針編
Ⅳ．1．概要
Ⅳ．2．IoTサービスのリスク
Ⅳ．3．対応策を割り当てるIoTサービスリスクの抽出
Ⅳ．4．IoTサービスを提供するクラウド事業者が取るべき対応策の導出
Ⅳ．5．リスク対応策

改定のポイント２

Ⅴ．参考資料
Annex１　組織・運用編　対策項目一覧表
Annex２　物理的・技術的対策編　対策項目一覧表
Annex３　典型的なクラウドサービスのパターン化とクラウドサービスの典型的な構成要素の図式化
Annex４　利用者接点とICTサプライチェーンに着目したクラウドサービスの特徴
Annex５　利用者接点とICTサプライチェーンに着目した要求事項
Annex６　利用者接点とICTサプライチェーンに着目した情報セキュリティ対策
Annex７　クラウド事業者が過度の責任を負わないための注意点
Annex８　【事例集】調査テンプレートの記入例

追記

IoTサービスを提供する際のリスクに対する対応方針

第Ⅳ部並びに第Ⅴ部Annex７及びAnnex８に

統合

ASP・SaaSにおける情報セキュリティ対策ガイドライン

（2008年1月）

第Ⅱ部及び第Ⅲ部並びに第Ⅴ部Annex１～Annex３に

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

（2014年4月）

第Ⅴ部Annex４～Annex６に

（注）「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」の一部の内容は、第Ⅱ部・第Ⅲ部にも掲載。

第Ⅱ部(組織・運用編)・第Ⅲ部(物理的・技術的対策編)の概要

○ 第Ⅱ部は、**情報セキュリティを確保するために求められる運用管理体制等**をとりまとめたもの。
○ 第Ⅲ部は、**クラウドの典型的なシステム構成に対する情報セキュリティ対策**をとりまとめたもの。

第2版第Ⅱ部のイメージ（Ⅱ．2．節の例）

Ⅱ．２．情報セキュリティのための組織

Ⅱ．２．１．内部組織

Ⅱ．２．１．１．【基本】

経営陣は、情報セキュリティに関する取組についての責任と関与を明示し、人員・資産・予算の面での積極的な支援・支持を行うこと。

【ベストプラクティス】
i. 情報セキュリティに関する取組にあたっては、必要となる調整（各種判断や連絡・指示、協力等）が適切に行われるよう、関連する役割及び職務機能を持つ代表者（CIO 、CISO 等）を定めることが望ましい。

（中略）

ISO/IEC27002との紐付け、利用者接点とICTサプライチェーンに着目した情報セキュリティ対策

6.1内部組織
【目的】組織内で情報セキュリティの実施及び運用に着手し、これを統制するための管理上の枠組みを確立するため。

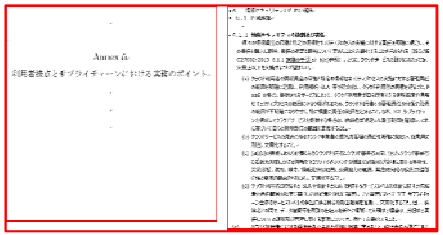
6.1.1情報セキュリティの役割及び責任
【管理策】全ての情報セキュリティの責任を定め、割り当てることが望ましい。

6.1.2職務の分離
【管理策】相反する職務及び責任範囲は、組織の資産に対する、認可されていない若しくは意図しない変更又は不正使用の危険性を低減するために、分離することが望ましい。

【利用者接点とICTサプライチェーンに着目した要求事項】
Annex５ 198ページを参照

【利用者接点とICTサプライチェーンに着目した情報セキュリティ対策】
Annex６ 226～227ページを参照

詳細な内容を確認する場合は第Ⅴ部（Annex）へ



ASP・SaaSにおける情報セキュリティ対策ガイドラインを基に構成

どのクラウド事業者にも実践的で取り組みやすい構成としたもの

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の内容を紐付け

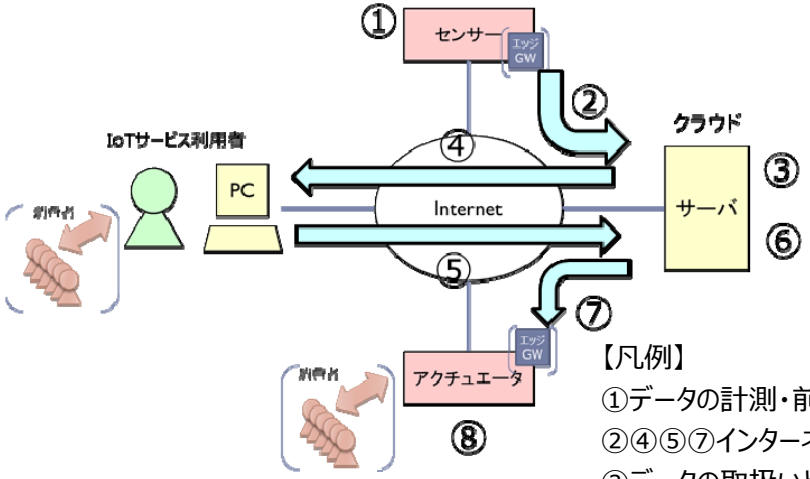
ISO/IEC27002と紐付けされた利用者接点とICTサプライチェーンに着目した要求事項や情報セキュリティ対策等を記載したもの

第Ⅳ部（IoTサービスリスクへの対応方針編）の概要

○　クラウド事業者が**IoTサービスを提供する際のリスクを整理**し、**そのリスクに対する情報セキュリティ対策を導出する方法**をとりまとめたもの。

Step1　リスクの整理

三つの観点（A.多様な事業者間連携、B.ロール（※1）を実行するコンポーネント（※2）と運用・保守の多様な提供形態、C.多様なデータ取扱形態）**を踏まえ、クラウド事業者がIoTサービスを提供する際のリスクを整理**。その際、以下のIoTサービスの類型図を活用することができる。



【凡例】
①データの計測・前処理等、
②④⑤⑦インターネット接続、
③データの取扱いと表示等の提供、
⑥制御コマンドの提供、
⑧駆動前処理・駆動等

（※1）　ロールとは、IoTサービスの提供にあたり必要となる役割のこと。具体的には、「IoTサービスの提供環境を整備・維持する」役割（利用者契約、機器等提供、機器等推奨等）や「IoTサービスを実行する」役割（計測、処理・分析等）が挙げられる。

（※2）　コンポーネントとは、IoTサービスの構成要素のこと。IoT機器、組込みアプリケーション等がある。

Step2　情報セキュリティ対策の導出

整理したリスクに対応する情報セキュリティ対策を導出し、対策を実行する。

ロール	対応策を割り当てるIoTサービスリスク	リスク対応策項番
利用者契約	IoTサービス利用者が想定外のIoT機器等を接続するリスク	A-1：【利用者機器の接続】
	IoTサービス利用者が問題のあるアプリケーションやデータを使用するリスク（違法である等）	A-1：【利用者機器の接続】
	IoTサービス利用者が調達するIoT機器／アプリケーション／事業者等をクラウド事業者が十分に統制できないリスク	A-1：【利用者機器の接続】 A-2：【持ち出しIoT機器等の事故時の責任分担】 A-3：【利用者が設置したエッジコンピュータ】

リスク対応策	具体的なアクション
A-1 【利用者機器の接続】 IoTサービス利用者が自分で接続するIoT機器、組込むアプリケーションやデータについても構成管理の対象に含めるよう、IoTサービス利用者との契約にあたり折衝すること	・IoTサービス利用者が自分でIoT機器を接続する前に、当該機器の情報を取得し、それがIoTサービス設計時に設定した共通基準に適合しているかを確認できるよう、IoTサービス利用者との契約条件に明記している ・上記の契約条件に基づき、IoTサービス利用者が自分のIoT機器を実際に接続する前に、IoT機器の情報を取得し、確認している

第Ⅴ部（参考資料）の概要

		内容
第Ⅱ部・第Ⅲ部関連	Annex 1 Annex 2	**組織・運用編　対策項目一覧表** **物理的・技術的対策編　対策項目一覧表** （それぞれの対策を一覧にしたチェックリスト）
	Annex 3	**典型的なクラウドサービスのパターン化とクラウドサービスの典型的な構成要素の図式化** （クラウドサービス種別のパターン化に関する解説、典型的な構成要素を図式化し例示）
	Annex 4	**利用者接点とICTサプライチェーンに着目したクラウドサービスの特徴** （クラウドサービス提供における供給者モデルや利用者接点等における五つの観点について詳述）
	Annex 5	**利用者接点とICTサプライチェーンに着目した要求事項** （利用者接点とICTサプライチェーンにおける要求事項を解説）
	Annex 6	**利用者接点とICTサプライチェーンに着目した情報セキュリティ対策** （利用者接点とICTサプライチェーンに着目した実務のポイントを解説）
第Ⅳ部関連	Annex7	**クラウド事業者が過度の責任を負わないための注意点** （IoT機器を自ら提供する場合と提供しない場合の具体的なユースケースを例示）
	Annex8	**【事例集】 調査テンプレートの記入例** （クラウド事業者がIoTサービスリスクを整理するためのテンプレートを具体的に例示）