今すぐにでも必要なクラウドセキュリティ

～ デジタル変革社会への対応 ～

クラウドバイデフォルト原則への対応（政府自治体）―入札要件への対応
クラウド利用におけるリスクが特定分析され必要な対策が機能していますか？
既存の ISMS ではクラウドサービス利用における対策は実装されていますか？
クラウドセキュリティ対策（管理策）について適用宣言書を見直していますか？
安心して任せられる人材は育成できていますか？

クラウドセキュリティリスクマネジメント
その価値と実践手法をピンポイントで解説

（セミナー内容）

1. **デジタル変革社会への対応**
2. **クラウドセキュリティとは？**
   ISMS でクラウドセキュリティリスク対応の方法
3. **JIS Q 27017 規格発行の経緯と固有のリスク**
   JIS Q 27017 規格の読み解き方
4. **クラウドセキュリティ対策テクニック**
5. **ISMS 適用宣言書の拡張方法**
6. **クラウドセキュリティ認証取得必勝法**

開催日程：**2019 年 10 月 16 日（受講無料）**
14:00～17:00（CPD3 時間実績対応）

開催会場：東京秋葉原
アイ・エヌ・ジーシステムセミナールーム
東京都台東区台東 1-11-10 大木ビル 2 階

受講申請：アイ・エヌ・ジーシステム
担当：柏倉　潤
kashiwakura_j@ingsystem.co.jp
講師：中西 孝治
nakanishi@isms-society.com

クラウドバイデフォルト原則

政府情報システムにおける クラウドサービスの利用に係る基本方針

政府情報システムのシステム方式について、コスト削減や柔軟なリソース の増減等の観点から、クラウドサービスの採用をデフォルト（第一候補）と し、府省ＣＩＯ補佐官の関与の下、事実に基づく客観的な比較を行いその利 用を判断するための考え方等を示した標準ガイドライン附属文書が発行されています。

背景と目的：近年、急速に進化し発展したクラウドサービスは、正しい選択を行えば、コスト削減に加えて、情報システムの迅速な整備、柔軟なリソースの増減、自動化された運用による高度な信頼性、災害対策、テレワーク環境の実現等に寄与する可能性が大きく、政府情報システムにおいても、クラウドサービスを利用することで様々な課題が解決されることが期待されています。しかしながら、これまで政府では、情報セキュリティや移行リスクへの漠然とした不安、不十分な事実認識等から、クラウドサービスの利用に前向きでなかった側面が否定できない。一方、多方面にわたり、クラウドサービスの利用が増加してきている。このような状況において、「世界最先端ＩＴ国家創造宣言・官民データ活用推進基本計画」（平成 29 年 5 月 30 日閣議決定）及び「デジタル・ガバメント推進方針」（平成 29 年 5 月 30 日高度情報通信ネットワーク社会推進戦略本部・官民データ活用推進戦略会議決定）では、クラウド・バイ・デフォルト原則、すなわち、政府情報システムを整備する際に、クラウドサービスの利用を第一候補とすることとされ、「デジタル・ガバメント実行計画」（平成 30 年 1 月 16 日 e ガバメント閣僚会議決定）において、「政府情報システムにおけるクラウド・バイ・デフォルトの基本的な考え方、各種クラウド（パブリッククラウド、プライベートクラウド等）の特徴、クラウド利用における留意点等を整理する」こととされた。このため、本方針では、クラウド・バイ・デフォルト原則を具体化し、各府省が、効果的なクラウドサービスを採用し、かつ、クラウドサービスを効果的に利用するに当たり、クラウドサービス利用検討フェーズに係る基本的な考え方を示すものである。

ISO/IEC 27017:2015（JIS Q 27017:2016）

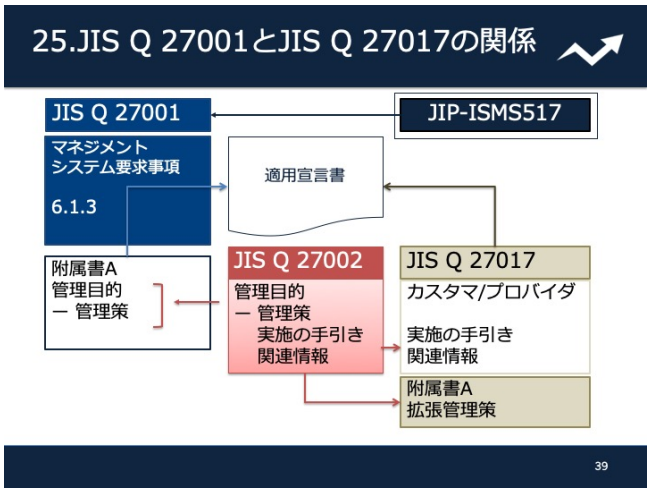
名称：JIS Q 27002 に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範

入札要件への対応や対策実装のために、JIS Q 27017を購入し読み込んでみたが、具体的に何をどのように実施すれば良いのかわからない？というお問い合わせや研修・ワークショップ開催の依頼が急増しています。

本セミナーでは、利用や提供の進むクラウドサービスのメリットを最大限に引き出し（機会を得る）ために、固有のリスクに対応することを目的として、各種ガイドラインやJIS Q 27017/認証要求事項を基にその効率的で効果的な実践方法を解説します。

JIS Q 27002 に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範

この規格は、「クラウドサービスカスタマ及びクラウドサービスプロバイダのための情報セキュリティ管理策の実施を支援する指針を提示する。ある指針は管理策を実施するクラウドサービスカスタマのためのものであり、他の指針はクラウドサービスプロバイダがそれらの管理策の実施を支援するためのものである。」とされており、クラウドサービスを利用する組織・上位のクラウドサービスを利用しサービスを提供する組織（SaaS）・上位サービスを提供する組織（IaaS/PaaS）が、それぞれのリスク対策を実施するための指針として提供されいますので、自組織の状況に合わせて活用することが大切です。



上図は本セミナー資料の一部抜粋です。

JIS Q 27017 は JIS Q 27002 に基づく管理策の実践の規範として発行されており、クラウドセキュリティを実装するためには ISMS が必要です。ISMS（リスクマネジメントプロセス）でクラウド固有のリスクアセスメントの結果、管理策の実装し、漏れがないように JIS Q 27017 拡張管理策と実施の手引きを参照･比較（ギャップ分析/ベースラインアセスメント）して適用することにより『適用宣言書』を追加・拡張します。

本セミナーでは、規格の構造や活用方法を丁寧に解説し、『適用宣言』するまでの手順を説明させていただきます。さらに、サンプルを提供して『適用宣言書』の作成方法（実践手法）を解説します。