

政府情報システムにおける クラウドサービス利用の現状と課題

政府CIO補佐官

阿部 政夫

アジェンダ

自己紹介（政府CIO補佐官について）

背景

クラウド活用に向けて

「霞が関クラウド構想」はどうなった

課題と今後の方向性

マルチクラウドの考え方

クラウドサービスの利用検討プロセス

情報セキュリティ上の制約

米国（連邦政府）におけるクラウド利用

まとめ



自己紹介（政府CIO補佐官について）

平成25年度から内閣官房において「CIO補佐官プール制」を導入し、内閣官房において政府CIO補佐官を一元的に採用・管理することにより、「臨機応変かつ機動的な支援」「政府全体としてのナレッジの共有・蓄積」を行うことを可能とし、政府全体としてのITガバナンスの強化及び府省横断的な取組みの強化に取り組んでいます。

政府全体又は各府省における電子行政の高度化・効率化・合理化等に関する

- 電子行政戦略の検討
- 政府情報システムの整備、管理などに関する政府共通ルールの推進・改善
- 府省共通システムの改善、更改に関する検討
- 各府省における情報システムに関する予算要求・調達・運用の各段階における高度化・効率化・合理化
- 各府省における重要プロジェクト・システムのレビュー

私は2015年4月に政府CIO補佐官に就任し、文部科学省のCIO補佐官を併任していますので、文部科学省関係のシステムを中心に担当しています。

背景

これまでは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るが、**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。**

「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)

「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)

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)
「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」こととされたところである。

クラウド活用に向けて

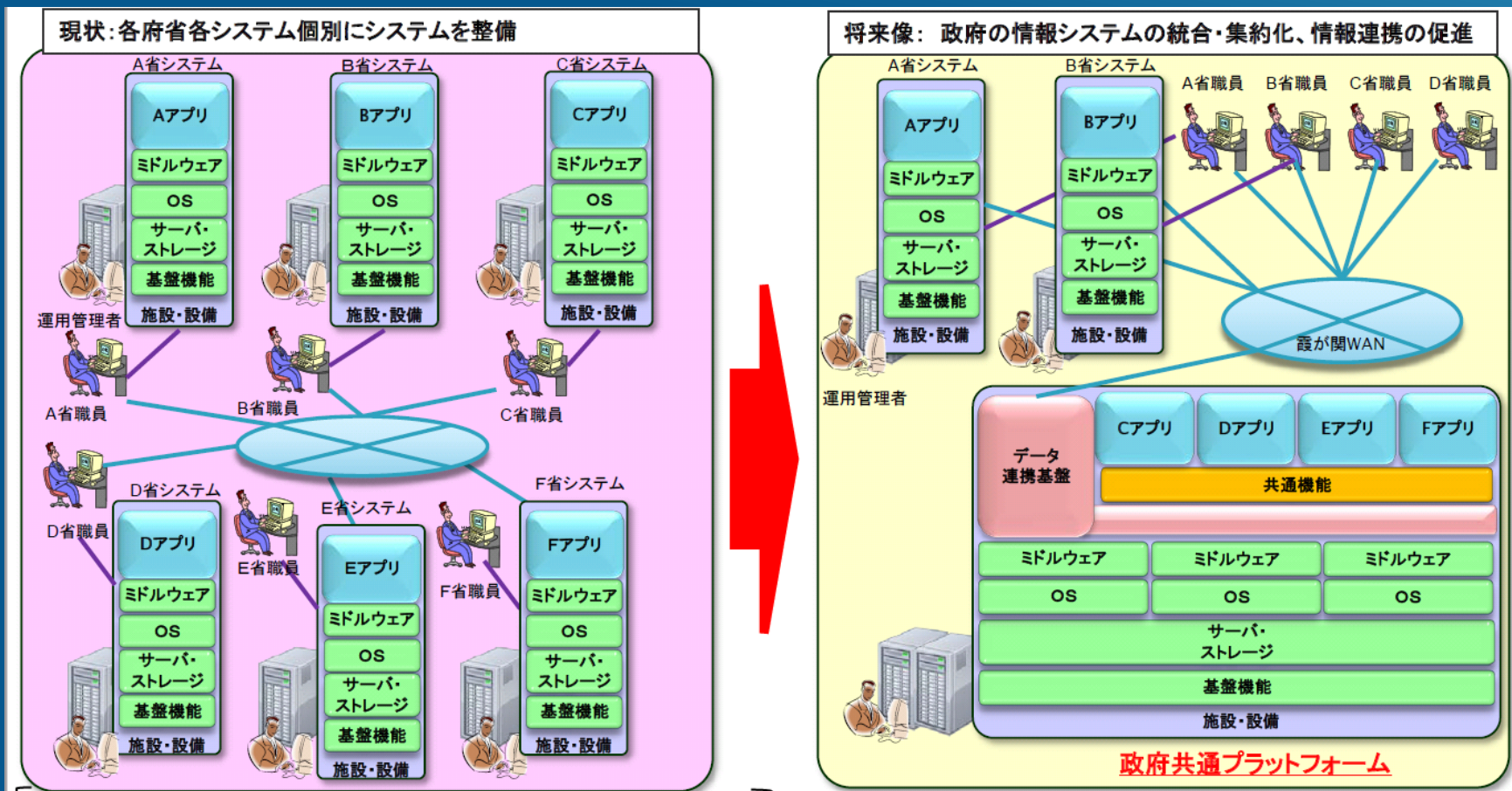
クラウド・バイ・デフォルト原則

クラウドサービスの利用を**第一候補**として、その検討を行うものとする。

政府情報システムは、クラウド・バイ・デフォルト原則、すなわち、**クラウドサービスの利用を第一候補として、その検討を行うものとする**。その際、「3.1 クラウドサービスの利用検討プロセス」に基づき、情報システム化の対象となるサービス・業務、取扱う情報等を明確化した上で、メリット、開発の規模及び経費等を基に、検討するものとする。
なお、本プロセスは、技術の進展や選択肢となる新たなクラウドサービスの出現に応じて、各利用検討の内容や順序は、適宜見直しを行うものとする。

「霞が関クラウド構想」は怎么样了

政府のIT戦略本部は2009年7月、新たなIT政策として「i-Japan戦略2015」を公表
「デジタル特区等による三大重点プロジェクト（電子政府・電子自治体、医療・健康、教育・人財）の推進」「産業・地域の活性化及び新産業の育成」「あらゆる分野の発展を支えるデジタル基盤の整備推進」→ 霞が関クラウド（政府共通プラットフォーム）



課題と今後の方向性

■ 政府の調達方式とのなじみの悪さ

- ・ほとんどのシステム調達は「請負契約」方式（定額での契約）
- ・単年度予算（前年度要求）
- ・リソースに見合った課金が難しい

■ 手続きの複雑さ（お役所的）

- ・仮想マシンを1つ立てるにも複雑な書類のやりとりが必要
- ・何か変更するにも手続きと時間が必要
- ・リソースの追加には数年前からの「予約」が必要

■ 高止まりするコスト

- ・構築・運用事業者が固定化することにより競争が働きにくくなる
- ・移行することにより「コスト増」となるケースが多く発生

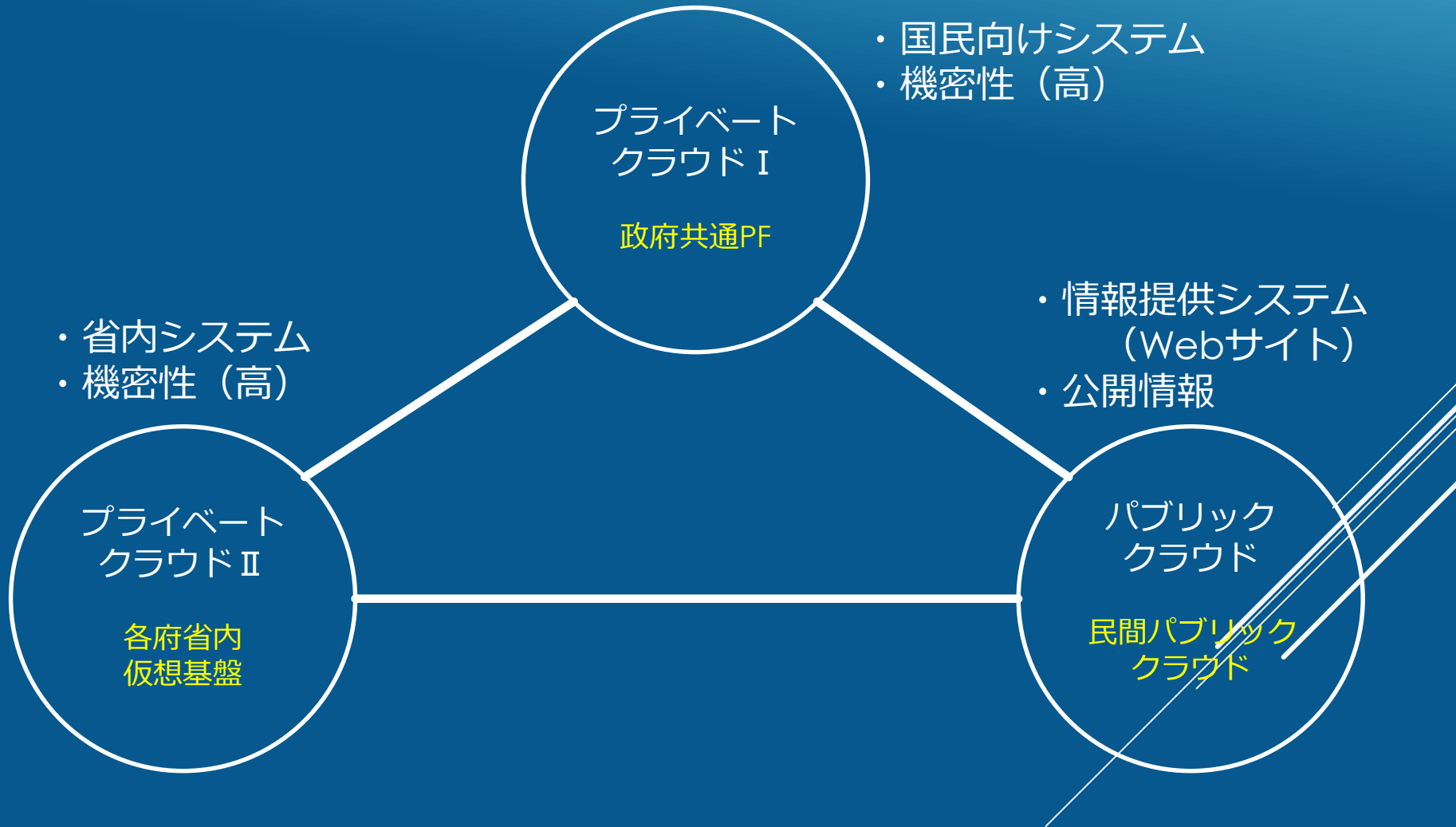
利便性やコストは「クラウド利用」とは言いがたく、政府情報システムの「データセンタ統合」程度の効果に留まっている。

第二期政府共通プラットフォーム計画

民間クラウドサービスを全面的に活用し、2020年第三四半期より供用開始の予定

マルチクラウドの考え方

政府情報システムにおけるマルチクラウドの考え方はそれほど明確にはなっていないが、おおむね以下の構造



クラウドサービスの利用検討プロセス

「クラウド・バイ・デフォルト」における検討プロセスは以下のようになっているが、現状とはまだかなりの乖離がある。

SaaSの利用検討

Step1 : SaaS (パブリック・クラウド)



Step2 : SaaS (プライベート・クラウド)



IaaS/PaaSの利用検討

Step1 : IaaS/PaaS (パブリック・クラウド)



Step2 : IaaS/PaaS (プライベート・クラウド)



いずれのクラウドサービスもその利用が著しく困難である場合、又はいずれのクラウドサービスの利用メリットがなく、かつ、クラウドサービスによる経費面の優位性も認められない場合のみ**オンプレミス**とする。

情報セキュリティ上の制約

「クラウド・バイ・デフォルト」を標榜するものの、政府情報システムにおいては情報セキュリティ上の制約が厳しく、**使って良いのか悪いのか、現場で判断するのは難しい。**

(1) 特定秘密（特定秘密の保護に関する法律（平成25年法律第108号）第3条第1項に規定する特定秘密をいう。）及び行政文書の管理に関するガイドライン（内閣総理大臣決定。初版平成23年4月1日。）に掲げる**秘密文書中極秘文書に該当する情報をパブリック・クラウド上で扱わないものとする。**

(2) クラウドセキュリティ認証等の認証基準、監査フレームワークの監査報告書の活用や個別の調査等により、クラウドサービス提供者から提供されているサービスが**統一基準を満たしていることを確認**するものとする。

(3) クラウドサービス利用時の伝送路は暗号化するものとする。格納されるデータやデータベースについても、**機微な情報については暗号化**を行うものとする。データの暗号化に使用する鍵については、クラウドサービス提供者側よりも利用者側で管理することが望ましく、選択可能な場合は利用者側で鍵管理が可能な暗号機能を選ぶものとする。

米国（連邦政府）におけるクラウド利用

米国には、「FedRAMP」（Federal Risk and Authorization Management Program）という連邦政府共通のクラウドサービス調達のためのセキュリティ基準がある。



クラウドサービスプロバイダーが、このプログラムの認証を受けて登録されると、省庁ごとに新たな調達評価の手続きを経ることなく、提供／調達することが可能な仕組み。



連邦政府全体でクラウドへの移行が進んでいる。
より高いセキュリティレベルが要求される国防・軍事分野では、クラウドサービス事業者およびそのユーザーに対して、国防総省がFedRAMPに独自の要求事項を加味した認証制度を構築。

まとめ

- 政府全体で「クラウド・バイ・デフォルト」の掛け声はかかったが、調達方式や課金方式にこれまでの政府情報システム（オンプレ）とは異なる課題が多く、民間企業のようには進んでいない
- 大手のパブリッククラウド事業者はグローバルに事業展開を行っており、サプライチェーンリスクや契約面での明確な基準や認証制度がないことも影響
- 官民でのビッグデータ活用やA Iなど、クラウド利用が前提となるなか、「クラウド・バイ・デフォルト」を強かに推進していく必要があると認識