Vol.2017-IOT-38 No.6
2017/6/24

情報システムのクラウド化とセキュリティガバナンスのあり方に関する考察

晏 康庄[†1]　渡邉 英伸[†2]　相原 玲二[†3]　西村 浩二[†4]

概要：本研究では，学術研究機関のクラウド利用実態調査において，学生数および情報システム機能別による集計・分析の方法を提案し，学術研究機関全体のクラウド普及の度合いをより正確に把握することを目指してきた．一方，学術研究機関がクラウドを利用促進するためのクラウドセキュリティ要件についても検討してきたが，クラウド化に対するセキュリティへの漠然とした不安を明確にするまでには至らなかった．そこで，再分析および見直しを行った結果，クラウド化に対して，組織の情報セキュリティガバナンスを適合することに気づけていない組織が多いことがわかってきた．本論文では，これまでの経緯や考えをもとに情報システムのクラウド化とセキュリティガバナンスのあり方について考察する．

A Study on Cloud Computing of information System and Security Governance

Kangzhuang Yan[†1], Hidenobu Watanabe[†2], Reiji Aibara[†3], Kouji Nishimura[†4]

Abstract: To grasp the status of the Cloud Computing spread in Academic and Research Institutes more accurately, we propose a method of aggregation by recounting the number of students and classify the systems by functions to review the data of the survey report on Science Information Infrastructure Statistics of Colleges and Universities which has been published. On the other hand, even though we have taken the requirement of Cloud Computing Security into consideration, but it did not lead to clarify the anxieties of using Cloud Computing. Therefore, as the result of reanalysis and review it became clear that there are many organizations that are not aware of adapting the organization's information security governance to Cloud Computing. In this paper, we will consider the way of Cloud Computing and Information Security Governance based on the background of past researches.

1. はじめに

大学等の学術機関におけるクラウド化の推進ならびにクラウドサービス利用の在り方を検討する目的で，文部科学省をはじめ，クラウド化に関する実態調査が実施されていた．より正確に学術機関におけるクラウド化推進状況を把握するために，これまで実施された調査の現状を整理し課題について議論してきた[1]．

これまでの学術機関におけるクラウド化の実態調査報告書は，クラウドサービスの利用状況・運用実績・導入計画に関する報告だけとなっている．一方で，一般公開されているこれらの調査報告書では，クラウド化の推進やクラウドサービス利用の在り方に対する具体的な解決策は示されていない．また，実施する調査団体や調査の依頼先の部署がバラバラであるため，類似の質問に対する回答結果が一致しない場合も珍しくない．すなわち，回答した学術機関はこれらの調査結果から有益なフィードバック情報を得ることが難しい状況にある．

本研究では、そうした問題を解決するため，実際にクラウドサービスを利用する側にある学生数をデータとして収集・集計することやシステムを用途別ではなく機能別分類することを提案した．結果としては，学生数で集計した結果は学校数で集計した結果より，クラウド化の実態や影響をより正確に把握することが可能になった．また，平成 26 年度の調査で収集された 1，404 のシステムに対して，それぞれのシステム名称から同様な機能を有するシステム群に分類し，各システム群に対して代表名を付ける処理を行い，国立大学に存在するシステムは大きく 32 の分類になった．また，機能別でクラウド利用の状況を把握することが可能になった．

一方，学術研究機関がクラウドを利用促進するためのクラウドセキュリティ要件についても検討してきたが，クラウド化に対するセキュリティへの漠然とした不安を明確にするまでには至らなかった．

本論文では，クラウド化に対するセキュリティへの漠然とした不安を明確にし，クラウドセキュリティの要件を検討し，情報システムのクラウド化とセキュリティガバナンスのあり方について考察する．

†1 広島大学 大学院総合科学研究科
Graduate School of Integrated Arts and Sciences, Hiroshima University
†2 広島大学情報メディア教育研究センター
Information Media Center, Hiroshima University
†3 2 広島大学情報メディア教育研究センター
Information Media Center, Hiroshima University
†4 2 広島大学情報メディア教育研究センター
Information Media Center, Hiroshima University

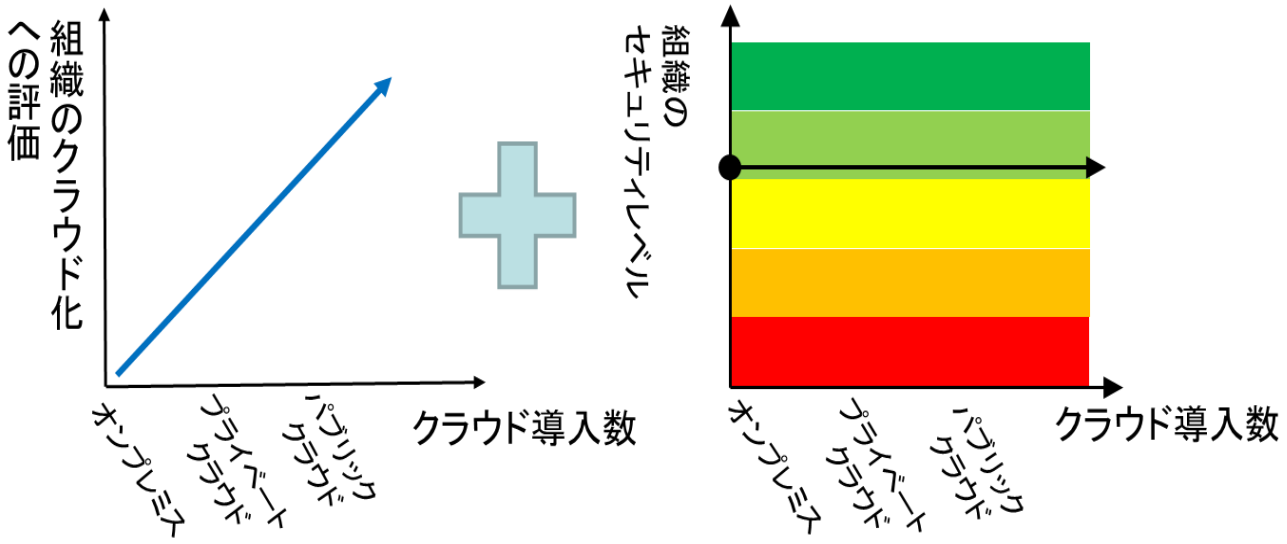

図 1　クラウド化に対する評価の考え方のイメージ

2. セキュリティに対する不安とクラウド化

文部科学省では，国公私立大学の大学図書館やコンピュータ・ネットワーク環境の現状を明らかにし，その改善・充実への基礎資料とするため，平成１７年度から学術情報基盤実態調査を毎年実施している．また，情報システムのクラウド化の実態調査については平成 24 年から実施されており， 平成 28 年度の報告では，627 校の国公立大学に対してクラウドの運用状況，用途，クラウド化の効果，クラウドしない理由について調査結果が示されている．クラウド化していない 1 番の理由はセキュリティ面の不安はトップであり，これは毎年変わっていない．このように，既存の調査ではクラウド化を妨げる理由を把握することができるが，各組織に適応する対策を示すことがなく，クラウド利用に対する不安を解消できず，結局改善には至っていないが現状である．

2.1 実態調査の評価の考え方

我々は，学術機関におけるクラウド化の実態調査結果は，文部科学省が目的としている学術機関全体のクラウドサービスの利用状況・運用実績・導入計画の実態の把握というマクロな視点と個々の組織が自身のクラウド化の進捗状況とクラウドに対するセキュリティの現状を把握するミクロな視点の両方の結果が重要と考える．

図 1 にクラウド化に対する評価の新たな考え方のイメージ図を示す．図 1 の左図は，文部科学省が実施している実態調査の評価イメージである．横軸はオンプレミスで運用している情報システムに対してプライベートクラウドやパブリッククラウドを導入した数であり，縦軸は組織のクラウド化に対する評価である．既存の学術機関におけるクラウド利用の実態調査では大学全体のクラウド利用状況を把握するためのデータを提供するのみである．そのため，報告書からはクラウドをたくさん導入すれば，組織のクラウド化への評価が高いという傾向が見える．一方，図 1 の右図は，個々の組織が自身のクラウド化の進捗状況とクラウドに対するセキュリティの現状を把握するミクロな視点の実態調査の評価イメージである．横軸は左図と同様にクラウドを導入した数であり，縦軸は国際的に組織で望まれる情報セキュリティ水準のレベルである．黄色は最低限満たすべき水準とし，緑色・黄緑は水準を満たしている，赤色・橙色は水準を満たしていないことを表す．パブリッククラウドに移行するほど高い情報セキュリティ水準が求められるが，何もしなければそれを満たせていない組織が多くなる可能性がある．また，自組織の情報セキュリティの適応範囲もクラウド側に拡張しなければならなくなるが，その要求を満たすクラウドを適切に取捨選択ができない組織も多くなる可能性もある．

よって，オンプレミスで満たしていたセキュリティレベルがパブリッククラウドに移行するほど維持することができなくなることが想定される．なお，本論文では，情報システムを組織内に構築して学内の担当者が運用することをオンプレミス，情報システムを組織内にクラウドサービスとして構築して，学内の担当者が運用することをプライベートクラウド，情報システムを組織外にクラウドサービスとして構築して，外部事業者が運用することをパブリッククラウドとする．

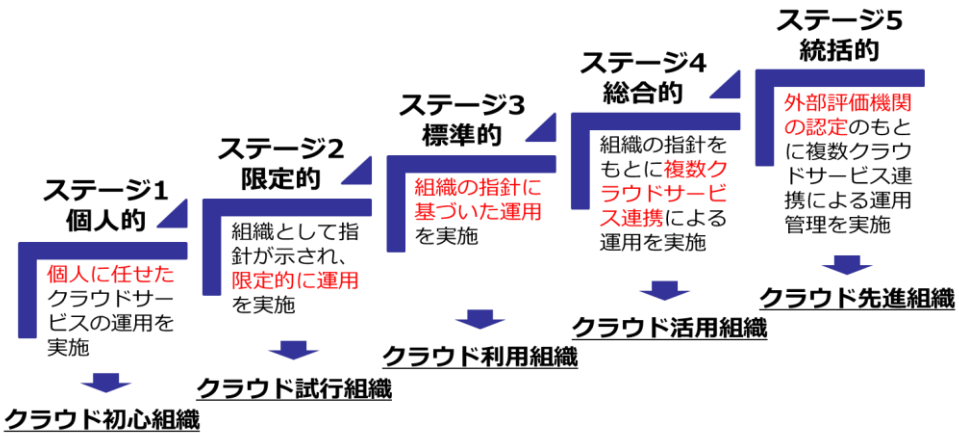

図 2　評価モデル概念図

2.2 セキュリティレベルから見るクラウド化の実態

我々は，クラウド導入運用数と比較できるセキュリティレベルを 5 段階で評価するモデルを考え，セキュリティレベルから見るクラウド化の実態を検証した[3].評価モデルでは，5 段階を判定するために，4 つの大項目要件と 16 個の小項目要件を基準に評価している.

小項目要件については，ISMS[4]および情報セキュリティガバナンス[5]の重要事項を参考に最低限必要と思われる要件を定めており，各評価基準の小項目要件は以下のとおりである.なお,具体的な算出方法などは紙面の都合上,割愛する．詳細は文献[3]を参考にしていただきたい.

評価基準 1：組織的制度・体制の有無
- ✓ 情報セキュリティポリシーの制定
- ✓ 情報セキュリティ委員会や CISO(Chief Information Security Officer)等を中心とする情報セキュリティ管理組織の整備
- ✓ CSIRT(Computer Security Incident Response Team)等の情報セキュリティ対応体制の設置
- ✓ 情報の格付けや外部委託の手続き等の文書化

評価基準 2：組織的導入・運用の有無
- ✓ 外部委託による情報システムの学外運用
- ✓ パブリッククラウドサービスの導入
- ✓ 大規模クラウドサービスの導入
- ✓ 複数クラウドサービス形態の導入

評価基準 3：組織的管理・統制の有無
- ✓ リスクアセスメントやリスク管理の実施
- ✓ 研修・教育・訓練の実施
- ✓ インシデント発生時の対応
- ✓ クラウドサービス利用ガイドラインやセルフチェックリスト等の文書化

評価基準 4：内部監査・外部評価等の有無
- ✓ 内部監査の実施
- ✓ 情報セキュリティガバナンスに対する総合的な評価および継続的な改善
- ✓ クラウド導入前後の評価
- ✓ ISO/IEC27017 ISMS クラウドセキュリティ認証の取得

図 3 に国立大学 86 校におけるオンプレ,プライベート,パブリッククラウド導入運用数とセキュリティレベルの結果を示す．縦軸は各ステージに属する大学の数を示し，横軸は組織で導入したクラウドの数を示している.

ステージ 1 に属する大学は 13 校，ステージ 2 は 58 校，ステージ 3 は 13 校，ステージ 4 は 2 校，ステージ 5 は 0 校であった．この結果が示すようにパブリッククラウドなどクラウド化を進めている組織の多くが，ステージ 1 や 2 であり，セキュリティのレベルが低いままクラウド化を進めている組織が多いも少なくないことが分かる.

2 章のまとめとして，セキュリティ面からみたクラウド化を見たとき，セキュリティレベルが低い組織はクラウド化に対して漠然とした不安を抱えていると思われるが，結果からその傾向はみられなかった．組織がすでに構築している情報セキュリティガバナンスが不十分である場合にもかかわらず，クラウド化を進めている傾向があり，多くの組織がその現状に気付いていないことが考えられる.

3. クラウド化によるセキュリティ面の不安

クラウド化することによって生じる不安とは，クラウド化により情報システムを外部委託するため，自組織の管理範囲外となり，情報セキュリティ上の懸念が増加すると漠然と感じることである．図 4 に学術機関における情報システムのクラウド化のイメージを示す.

一般的に情報システムの運用は，情報システムを導入した上でセキュリティ対策を施し運用管理する．そのため，自営設備による機能に対してセキュリティ対策が十分カバーでき，かつ PDCA を回せていることが前提となる.
その上で，自営設備による実現している機能をクラウド上

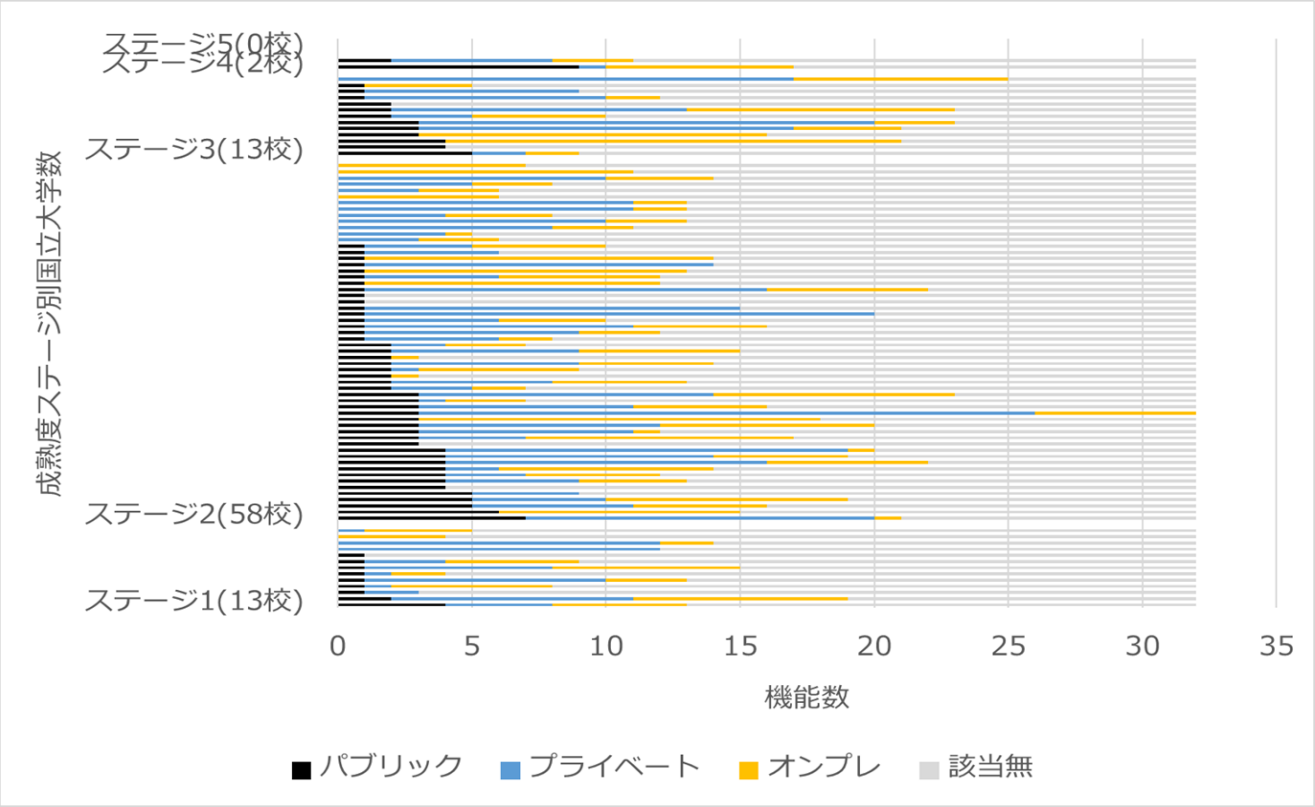

図 3　組織のセキュリティレベルから見るクラウド化の実態の結果

に単純に移行した場合，クラウドサービスによる機能が実現される．一方で，既存のセキュリティ対策がクラウドサービスまで適応できず，クラウドサービスによる機能とセキュリティ対策の間にギャップが生まれることになる．その結果，既存の PDCA を適切に回せなくなる．

このように，クラウド化におけるセキュリティ面の不安とは，ギャップに気づき，既存のセキュリティ対策に対して適切な対策を講じることができていないことで情報セキュリティに対する懸念を漠然と感じることである．

4. クラウド化に対する情報セキュリティガバナンスのあり方

4.1 情報セキュリティガバナンスのあり方

図 5 にクラウドサービスに適合すべきセキュリティガバナンスのイメージを示す．クラウド化によるセキュリティ不安の原因は 2 つと考える．一つは，組織的に情報セキュリティを運用管理する際に既存の情報セキュリティガバナンスと最低限満たすべき情報セキュリティ水準の間にギャップがあるにもかかわらずそのことに気づいていないことである．もう一つは，クラウドの導入によって既存の情報セキュリティガバナンスにギャップが生じることに対して既存のセキュリティガバナンスに適合可能かどうかを確認する枠組みが組織として確立されていないことである．

そこで，本論文ではクラウド化に対する情報セキュリティガバナンスのあり方として，ベースとなる情報ガバナンスの枠組みにクラウド化に合わせた枠組みをアドオンする構造が必要であると考える．すなわち，ベースとなる情報セキュリティガバナンスと最低限満たすべき情報セキュリティ水準との間のギャップを解消する観点とクラウド化によって生じるベースの情報セキュリティガバナンスとのギャップを解消する観点が重要であると考える．

4.2 考察

2 章では実態調査結果から既存の情報セキュリティガバナンスが不十分の可能性があることに気づいていないことで生じるセキュリティの不安を考察した．3 章ではクラウド化によって生じる既存の情報セキュリティガバナンスとギャップに対応可能な枠組みが確立されていないことで生じるセキュリティの不安について述べた．そして 4.1 では，クラウドを導入する前に既存の情報セキュリティガバナンスが最低限望まれる情報セキュリティ水準を満たすこととクラウドと既存のセキュリティガバナンスの適合性を確認可能な枠組みを確立することの 2 つの観点が重要であることを示した．それをもとに，ベースとなる情報ガバナンスの枠組みにクラウド化に合わせた枠組みをアドオンする構造が必要であることを説いた．

この構造の考えは ISMS 認証の考えと同じであることが分かった．

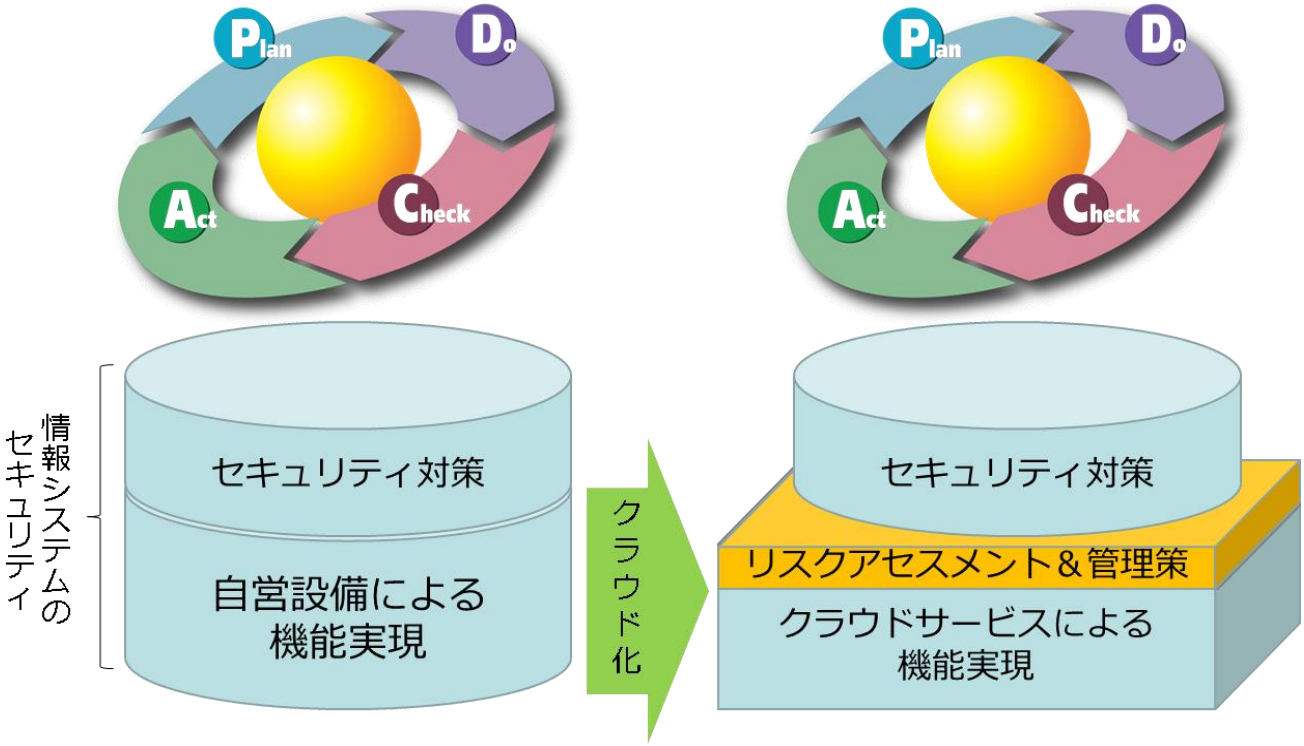

図 4　情報システムのクラウド化のイメージ

ISMS は，情報資産のセキュリティを管理する枠組みを策定するために定められた国際的セキュリティ規格である．ISO/IEC 27001:2013 は情報セキュリティマネージメントにおいて最も基本となる規格である．ISO/IEC 27017:2015 は，ISMS クラウドセキュリティ認証の規格であり，ISO/IEC 27001:2013 のベースの規格にアドオンする構造となっている．ISO/IEC 27017:2015 は，2016 年 9 月 30 日より，認証取得が開始されたばかりの規格である．

本研究では，2016 年 6 月に文献[1]を発表した以降，情報システムのクラウド化に対する情報セキュリティガバナンスのあり方について多くの議論をしてきた．今回，ISMS クラウドセキュリティ認証の規格が開始されたことで，我々の考えは国際的なセキュリティの観点からみても妥当性があるものだと考えられる．

5. おわりに

本論文では，学術機関におけるシステムのクラウド化に対するセキュリティへの漠然とした不安を明確にした．そして，学術機関のクラウド化に対する情報セキュリティガバナンスのあり方として，クラウドを導入する前に既存の情報セキュリティガバナンスが最低限望まれる情報セキュリティ水準を満たすこととクラウドと既存のセキュリティガバナンスの適合性を確認可能な枠組みを確立することの２つの観点が重要であることを説明した．加えて，ベースとなる情報ガバナンスの枠組みにクラウド化に合わせた枠組みをアドオンする構造が必要であることを述べた．

今後の課題としては，アドオン考えを取り入れた情報セキュリティガバナンスの評価モデルおよびアンケートシステムを構築し，学術機関に対して情報セキュリティガバナンスの実態調査を実施することである．

参考文献

[1] 晏康庄，渡邉英伸，西村浩二，近堂徹，相原玲二，合田憲人，岡田義広，学術機関におけるクラウドサービス利用に関する調査結果の分析，情報処理学会研究報告，Vol.2016-IOT-34, No.10，pp.1-7，2016.
[2] 文部科学省，平成 27 年度「学術情報基盤実態調査」概要，2017
[3] 渡邉英伸，晏康庄，西村浩二，相原玲二，合田憲人，吉田浩，岡田義広，学術機関におけるクラウド化成熟度モデルに関する検討，大学 ICT 推進協議会 2016 年度年次大会論文集，2016.
[4] JIPDEC，ISMS ユーザーズガイド -JIS Q 27001:2014(ISO/IEC 27001:2013)対応- リスクマネジメント編，2015.
[5] 経済産業省，情報セキュリティガバナンス導入ガイダンス．http://www.meti.go.jp/policy/netsecurity/secgov-documents.html

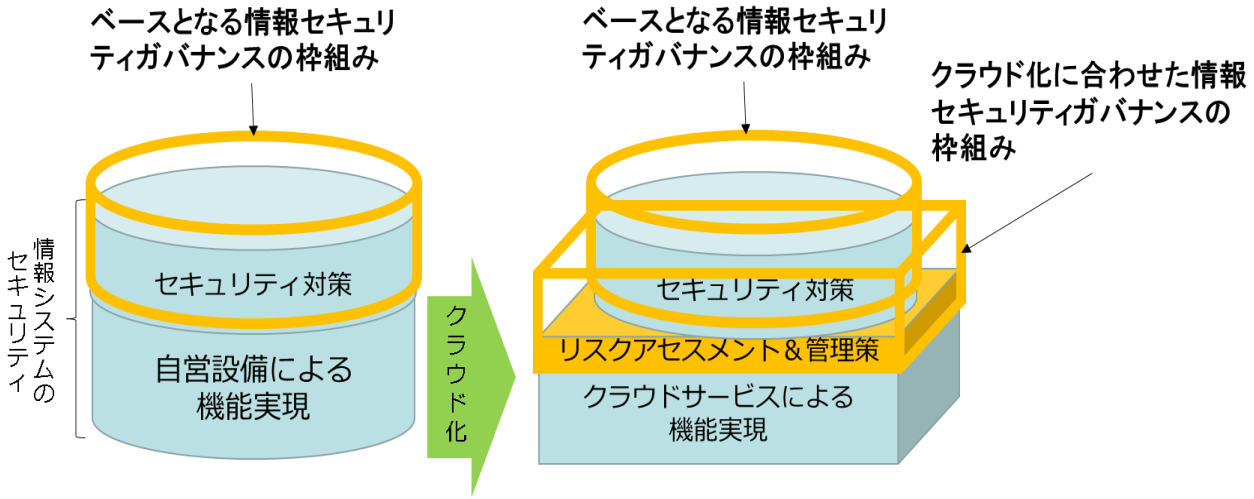

図５　クラウドサービスに適合すべきセキュリティガバナンスのイメージ