Vol.2015-EIP-67 No.3
2015/2/28

複数企業にまたがったITサービスのサプライチェーンにおけるITガバナンスの課題について

原田要之助[†1]　久保知裕[†2]

単独の企業に対するITガバナンスのフレームワークについてはさまざまな研究がなされ，成果はISO/IEC38500となり企業経営等に生かされてきた．一方，複数の企業や自治体等の組織で構成されるスマートシティなどのプロジェクトではITがサービス提供の中核となるものの，ITガバナンスやリスクについては複数の組織間で相反する利害関係を伴うため十分な研究がなされていない．本研究では、複数の企業等が連携する組織形態において，組織毎に異なるITガバナンスを統合するものが必要になることを明らかにする．

IT governance issues on IT Services supply chain by multiple enterprises

YONOSUKE HARADA[†1]　TOMOHIRO KUBO[†2]

Supply Chain is a common business model of IT services provider collaboration, which aims to achieve superiority in operational efficiency by optimizing individual competences of enterprises. IT governance has been studied focusing on a single enterprise and its redulted in ISO/IEC38500 standardization which is widely utilized all over the world. On the other hand, IT governance on the Supply Chain based on IT services such as Smar City prokject which is comppoosed of enterprises, local governments and NPOs has not been studied. This is because there are potential conflicts of interest among those organization on IT supply and return. which are not one However, one of important elements to determine efficiency of supply chain is an IT Governance and Infromation security. This paper present current problems to be solved and propose counter soluteon as the new IT Governance among multiple enterprise and its architectuture.

1. 背景と研究の目的

1.1 背景

単独の企業に対するITのマネジメントやガバナンスのフレームワークについてはさまざまな研究がなされ，成果が企業経営に生かされてきた．しかし，複数の企業間で構成されるコンソーシアム（例えば，スマートシティなど）やサプライチェーンで繋がった企業間のITに関わるガバナンスについては，十分な研究がなされていない．

近年，企業などの組織が行う事業活動は，単独の組織で完遂することは難しい．サプライチェーンのように複数の組織にまたがって業務活動が行われ，最終消費者に商品やサービスといった価値を届けることが一般的になっている．企業間の連携活動においては，プロセスの連携，情報伝達や共有が重要であり，ITはその基盤となる．2010年以降は企業が所有する情報システムのみならず，IoT（Internet of Things）等，様々な機器がインターネットを介して結びつけられ，クラウド上におかれた情報システムで制御される環境も生まれつつある．一方で，情報システムやネットワークの障害や，内部不正やサイバー攻撃等による情報流出や改ざん等の問題などが新しいリスクとして顕在化している．これは，ITが一つの企業に関係津できず，様々な他の企業や組織に依存していることによると考えられる[1]．すなわち，例えば，サプライチェーンを構成する企業間を接続するITサービスの障害が，連携するプロセスを阻害してサプライチェーン自体に影響を与える．また，利用しているクラウド上のサービスプロセスが誤動作したり，誤ったデータが投入されたり，途中のデータが改ざんされたりすることでサプライチェーン全体のプロセスが正常に動作しなくなることが考えられる．さらに，サプライチェーンのプロセスの一番弱いところを攻撃するなり，セキュリティ管理の弱い企業を狙って攻撃することで，その企業のみならずサプライチェーン上の全ての企業のサービスを停止させたり，品質低下を起こすことが可能である．これが，サプライチェーン企業全体の株価に影響を与えるシナリオも成り立つ．

単独の企業が独立したシステムを構築・運用・利用していた時代に比べると，複数の企業が連携して事業活動を行う場合の情報セキュリティなどのリスクは，問題の発生可能性，影響の大きさともに高まっている．

2. ITのサプライチェーンのガバナンスや情報セキュリティに関する課題について

ITサービスのサプライチェーンの問題点については，近年

†1 情報セキュリティ大学院大学
Institute of Information Security
†2 情報セキュリティ大学院大学
Institute of Information Security

研究が進み始めた．以下では，既存研究のまとめと課題について述べる．

2.1 既存研究のまとめ

(1) IT アウトソーシングとプロセスアプローチ
IT サービスの外部委託の管理については，再委託など多重委託されることが多い．河野ら[2]は，IT サービスの多重委託における内部犯罪を分析して，「IT アウトソーシングを活用する場合，情報セキュリティの観点から，委託先に対する適切な管理が重要となる．委託元は，情報システムを取り巻く技術や環境の目まぐるしい変化に対応し， IT 外部委託先管理の実効性の維持・向上に努めなければならない」ことから，IT サービスのサプライチェーンの構成企業がそれぞれ独立にマネジメントシステムを構築するだけでは十分でないことを指摘している．これを解決するために，複数の企業間にまたがる IT サービスを一体的なものと見なして，全体の外部委託先管理を複数企業間にまたがったマネジメントシステムとして構築し，プロセスアプローチによって有効性を維持・向上していく仕組みについて考察している．

(2) 金融機関の IT サービスのサプライチェーン
嶋作ら[3]は，具体的な金融機関と IT ベンダや IT プロバイダで構成される IT サービスのサプライチェーンに着目して検討している．その結果,「委託元が直接コントロール出来ない困難さもあり，適切な管理体制の確立が求められる．また，多重委託での外部委託は，さらに困難さが増すため，外部委託においては，リスクオーナーの所在を明確にし，委託元による確実な監督が求められる」ことを明らかにしている．とくに，「金融機関とシステムベンダとでは，内部統制の体制面においては，業種間に大きな差異は見受けられなかった．しかし，（略）企業間のリスク認識に大きな差があり，外部委託を行う場合，共通のリスク認識を持つ事が重要であると思われる．共通のリスク認識を持つためには，リスクコミュニケーションを密にし，意見の摺合せが重要となる」としている．すなわち，IT サービスのサプライチェーンにおいては，チェーンを構成する企業間の管理体制そのものではなく，リスク認識などが異なるため，結果的に，ガバナンスやマネジメントが異なることを指摘した．すなわち，IT サービスのサプライチェーンでは企業間の契約に基づく委託関係が形成されるだけではサプライチェーン全体としてのガバナンスや情報セキュリティの観点から十分ではないことを明らかにした．

(3) 複数企業にまたがる IT サプライチェーンのリスク
久保らは[1][4][5]，複数企業にまたがる IT サービスのサプライチェーンのガバナンスモデルや情報セキュリティリスクについて，他の分野を事例として述べている．例えば，化学物質や紛争鉱物の取引，児童労働についてはサプライチェーン全体を対象にした法的，もしくは準ずる形態（国際基準など）によって拘束もしくは義務が科せられていることから，「IT のサプライチェーンについては，全体を見渡した視点が欠けていたり，国際標準の普及が妨げられたりしている．」と述べている．また，アンケート調査や文献調査から，「日本企業における 5 つの課題をまとめている．(表 1 参照)

表 1 日本企業のサプライチェーンの課題（出所：[1]）

(1)	サプライチェーン全体の可視化ができていない
(2)	サプライチェーンを構成するサプライヤとの協力関係の構築が難しい
(3)	サプライチェーンのセキュリティリスクの認識が機密性に偏っている
(4)	サプライチェーンにおけるリスク管理において国際標準の利用が進んでいない
(5)	サプライチェーンのセキュリティリスク認識の啓発や対処方法の普及施策が不十分である

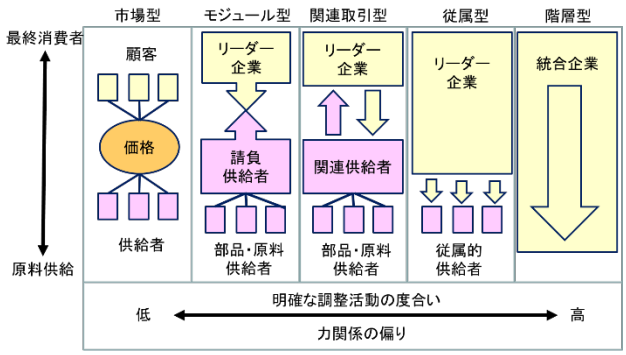
また，久保らは「日本企業が IT のサプライチェーンを取り巻くリスクを俯瞰して分析すること，業界や個々の企業における協力会のような活動を通して知恵を絞ることで，海外にも通用する管理手法が確立できる」と述べている．

(4) 価値連鎖でつながった企業間における IT ガバナンス
原田・小倉は[6]，価値連鎖には，ものやサービスの提供，調達，購買などの経済行為のみならず，所属する業界や団体，CSR 活動，コミュニティ活動などあらゆる活動によって生成されるものが含まれる．しかし，これらの価値連鎖においては，例えば，連携した企業の一部に不正行為などがある場合，関連している企業全体が，さまざまな形で不利益を被ることにもなる．すなわち，企業は企業間の取引のみならず，さまざまな場面で，活動に対してガバナンスすることが求められることを明らかにしている．

2.2 サプライチェーンモデルの適用について

Gereffi らによるサプライチェーンの研究[7]では，主に製品の流通について，最終消費者と原料供給者（企業）間に存在する企業のサプライチェーンをいくつかのモデルに整理している．これを図 1 に示す．この研究では，主に製品やサービスのサプライチェーンにおけるモデルであるが，IT サービスにおけるサプライチェーンについても適用が可能である[1]． Gereffi らは，サプライチェーン市場が，階層型から市場型へと発展していくと述べている．しかし，最終消費者への製品やサービスに比べると，IT サービスの場合については，例えば，携帯電話のネットワークサービス提供に見られるように，選択肢は多くない．そのため，

市場型モデルが製品の場合のように，階層型から市場型に向けて進化するかについては今後の市場の成長を見なければ分からない．ただし，多数の企業が関係するこれらのモデルは当てはまると考えられる．



- 市場型：スポット市場で，供給側，調達者の切り替えコストは低い．
- モジュール型：多少とも供給者は調達者のニーズに合わせてカスタマイズする．請負納入の場合は，供給者が設備や原料手配などの便宜をはかる．
- 関連取引型：供給者と調達側は特別な設備への投資など依存関係を持つ．地縁や評判，親族などの関係で結びついた取引である．
- 従属型：大規模な調達者に小規模な供給者が従属した関係である．調達者による，統制やモニタリングが頻繁に行われる．
- 階層型：垂直統合の進んだ形態で，本社と子会社の関係が代表的である．

図 1　グローバルバリューチェーンガバナンス（Gereffi ら[7]）

図 1 の企業間における調整活動は，企業間の情報提供と統制の関係とみることもできる[1]．統合企業のように取引内容の外部開示ができない場合，企業間での内部の調整活動がこれに変わる．スポットで調達する市場型では調整活動における企業間の情報提供と統制活動の重要性は相対的に低い．一方，階層型や従属型では，リーダー企業が調整活動を実施することとなる．モジュール型の場合は，リーダー企業と請負供給者が対等の立場となるので，市場型と同様，調整活動は少ない．これらのことから，企業間における IT ガバナンスのモデルを考える場合にも，企業間の統制活動や情報の共有や開示の程度に違いがあることが分かる．また，業界の特性でもモデルが決まること，事業環境の変化によってもモデルが変化することが考えられる．

IT サービスの場合，事業者の競争も激しく需要変動が激しいので，サプライチェーンを構成する企業間では正確で迅速な情報交換が重要である．例えば，サプライチェーンに問題が発生すると IT サービスの提供ができなくなるので，情報セキュリティリスクは高い．

2.3　サプライチェーンの全体の価値について

Christopher らは，サプライチェーン全体の情報の可視化と統制が必要であり，以下の三つの要素を挙げている [8]．

- 情報の正確性,可視化とアクセス
- 統制が効かない状況の警告
- 修正するための対応

これらの要素を構築・運用することでサプライチェーン全体の効率性や統制を維持することができる．この考え方は，ガバナンスや情報セキュリティを考える上で参考になる．また，IT のアーキテクチャは自組織のみを守る対策だけでなくチェーン全体を対象とすることが重要である．同様に，長内らは IT サプライチェーンに参加する企業共通のセキュリティ基盤の構築を提案している[9].

2.4　共通価値の創造について

Porter と Kramer らは，2011 年に CSR（企業の社会的責任）を発展させた新しい概念として CSV（Creating Shared Value：共通価値の創造）を提唱している[10]．CSR は社会的な利益を優先する概念であり利潤追求と本来は相反すると考える．これに対して，CSV は，企業が様々なニーズや課題に取り組むことで社会に役立つ価値を創造し，その結果，自企業にも経済的価値がもたらされるという考え方である．すなわち，企業の本来の活動と CSR やフィランソロピーを包む広い概念となっている．また，市場についても，経済的なニーズではなく，社会全体としてのニーズと考えることで，経済的価値と社会的価値を同時に高めることができるとしている [10]. また，次の 3 点を特徴としている．

- 社会的課題を解決するプロダクトの開発・販売
- バリューチェーンの競争力強化と社会貢献の統合
- 事業活動地域での事業基盤強化と地域貢献の統合

なお，この CSV の概念は，バリューチェーンで繋がった多数の企業で構成されるサプライチェーン全体の価値創造に応用できると考えられる．ただし，Porter らはサプライチェーンで繋がった企業間の CSV について明示的に述べてはいない．

一方，赤池・水上は，「CSV 経営―社会的課題の解決と事業」[11]の中で，トヨタのサプライチェーンと CSR を統合した活動を分析して,「公益と事業駅を両立させる開発投資活動」を CSV として位置づけている．すなわち，CSV の概念は複数の企業によるバリューチェーンの共通の利益や社会的責任を追求するモデルの指標として利用することができる．

3.　IT ガバナンスのモデル

3.1　　単独企業の IT ガバナンス

(1)　ISO/IEC 38500:2014

ISO/IEC 38500［1］は，企業の IT についてのガバナンスを扱う規格である．2014 年には JIS 化が予定されている．IT

ガバナンスの概念は，ISACA が 1990 年代に提唱したもので，CobiT3 から用いられている．コーポレートガバナンスは OECD が策定したもので，概念から構成されている．ISO/IEC38500 のモデルは，経営陣（Governing Body）が実施するべき 6 つの原則(図 2 参照)とプロセスとしての EDM（Evaluate-Direct-Monitor）（図 3 参照）で構成される．

- Principle 1: Responsibility
- Principle 2: Strategy
- Principle 3: Acquisition
- Principle 4: Performance
- Principle 5: Conformance
- Principle 6: Human Behaviour

図 2　IT ガバナンスの 6 つの原則(出典:ISO/IEC38500:2015)

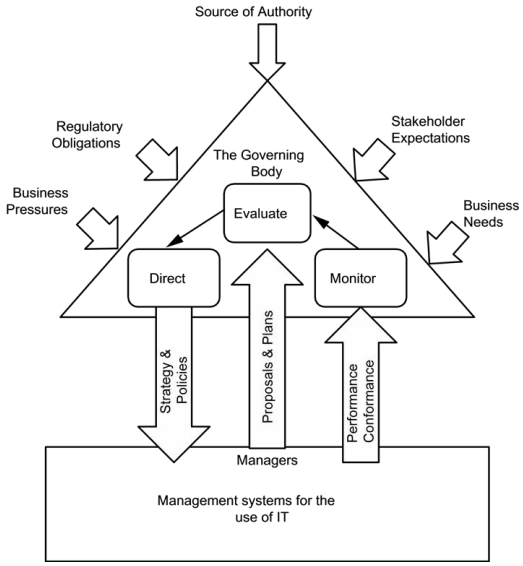


図 3. IT ガバナンスの参照モデル(出典:ISO/IEC38500:2015)

3.2　サプライチェーンのガバナンスについて

一方，加護野は，日本企業について，「企業間協働の取引相手が企業統治に重要な役割を演じている．取引ネットワークによる企業統治こそ，株主による企業ガバナンスがほとんど行われているにもかかわらず，日本の企業がよい経営を行ってきた理由である．」と述べている[12]．すなわち，日本企業では，サプライチェーンで連携した企業グループのガバナンスが株主のよるガバナンスよりも機能していることを述べている．日本企業では，大企業の多くが図 1 の階層型や従属型であり，統合企業やリーダ企業がサプライチェーン全体をガバナンスしていることを指摘している．さらに，加護野は，「取引相手は，企業ガバナンスに関して深い関心を持っている．共同企業の経営がうまく行われなくなると，ビジネス・システムが崩壊して自社の存在が危うくなるからである．協働企業は株主よりもより効果のあるガバナンスを行うことができる．日々の取引を通じて経営のよしあしをより早く，よりよく知ることができるからである．これは，取引パートナーは，(日本的な株式の持ち合いなどで）長期的な取引利益を期待して投資を行っている．その投資への見返りを確保するためには，取引相手の経営を安定化される必要がある．そのために利益の再分配が行われることすらある.」と述べており，サプライチェーンの構成企業を含んだ全体のガバナンスが存在していることを指摘している．[12]

加護野は，サプライチェーンにおける企業グループのガバナンスが存在していること，全体をまとめるのは，必ずしも，図 1 の統合企業やリーダ企業による者ではないことをしめしている．サプライチェーン全体のガバナンスが存在することからは，サプライチェーン全体を対象にした IT ガバナンスが存在して，構成企業全体を対象にした IT の最適化が図られると考えられる．

3.3　契約面からのサプライチェーンの IT ガバナンス

サプライチェーン全体の IT ガバナンスについて，サプライチェーンにまたがる IT の契約について見ていく．日本セキュリティ監査協会では，サプライチェーンの企業間の委託関係をモデル化している．これを図 4 に示す．図 4 では，経済的な合理性から，サプライチェーン全体に関わる価値連鎖を企業間の契約行為によって，局所化・単純化することができることとしている．また，このようにすることで，図 1 の階層型，従属型，関連取引型の統合企業やリーダ企業にとって，企業の責任を局所化できる都合のよいモデルになっている．一方，従属する企業にとっても局所的に責任をとることで，調達が保証されるなどの関係を維持できるなどのメリットがあった．したがって，企業活動のフレキシブルを担保するもの考えられてきた．

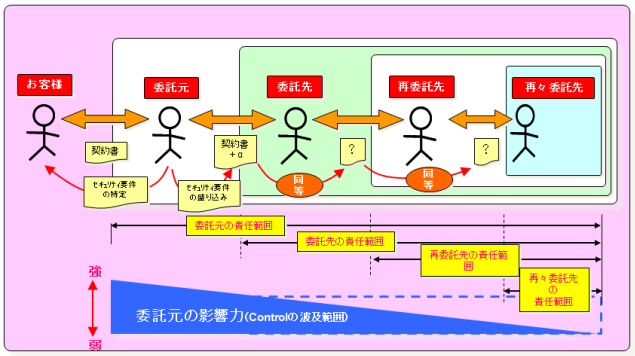


図 4. サプライチェーンにおける契約の影響力の低下（出所:日本セキュリティ監査協会[13]）

しかし，現在は，契約で企業間の関係を単純化したために，サプライチェーンの一部の問題が全体に影響を与えることになったり，サプライチェーンで情報が共有さくなるなどの問題が指摘されてきた．久保らは，化学物質や紛争鉱物の取引，児童労働について，元請け企業が自社の責任をサプライチェーンの他国にある末端企業に転嫁して，自社の

責任を逃れることが多発したこと．その対策として，国際的に元請けを含めてサプライチェーン全体で責任をとらせることが進んでいることを指摘している[1]．化学物質や紛争鉱物の取引，児童労働については，元請け企業が全体の責任を遂行できるような仕組みを国際基準をベースに義務づけている．この流れは，現在，IT サービスのサプライチェーンには適用されていない．久保は，サプライチェーンの不祥事が元請け企業やサプライチェーン全体に影響を与える事実をあげて，考慮すべきとしている[1]．

IT サービスのサプライチェーンにおいて，元請けがチェーン全体の責任を持つようにするためには，図 4 の局所的な契約や取引では，元請けが末端に対して影響力をもてないため，サプライチェーンを管理できない．そこで，元請けの外部委託する要求条件の影響力が委託先で低下しない新しいモデルを提唱している[13]．これを図 5 に示す．

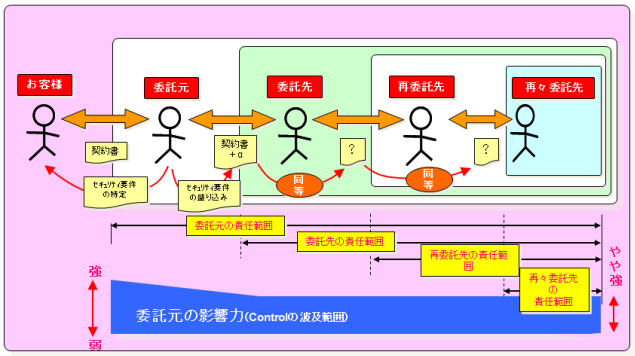


図 5. サプライチェーンにおける契約の影響力の維持（出所：日本セキュリティ監査協会[13]）

日本セキュリティ監査協会の図 5 のモデルでは，IT サービスのサプライチェーン全体を対象とする共通の契約行為を契約の際に追加することを提唱している．すなわち，IT サービスについては，サプライチェーン全体を対象とした共通の仕組みを追加する．これは，化学物質などの共通の規制を追加してすることと等価なモデルである．

3.4 サプライチェーンの IT リスクについて

(1) NISR の SCRM について

NIST の IR7622「連邦情報システムのための試験的な SCRM（Supply Chain Risk Management）プラクティス」 ではサプライチェーン全体に対するサイバー攻撃のリスクを指摘したうえで，情報システムのライフサイクルを通したリスクの定義と管理策を提唱している．「情報システムセキュリティ」，「調達」，「法律」，「情報システムのオーナーとサービス提供者」の 4 つの柱がサプライチェーンリスクをコントロールする能力を決めるとしている[15]．NIST が提供する SCRM のベストプラクティスを表 2 に示す．

表 2 SCRM のベストプラクティス（出所[16]）

①	インテグレータとサプライヤの活動を調達者から見て最大可視化する．
②	使用している構成要素の機密性を守る．
③	サプライチェーンの保証を要求に組み込む．
④	信頼性の高い構成要素を選定する．
⑤	多様性を取り入れる．
⑥	重要なプロセスと構成要素を防護する．
⑦	防護性の高い設計にする．
⑧	サプライチェーン環境を防護する．
⑨	構成要素へのアクセスや公開を制限するシステム構成にする．
⑩	外部サービスの利用やメンテナンスを正規の活動として扱う
⑪	システム開発のライフサイクルを通じて試験を実施する．
⑫	システム構成を管理する．
⑬	人をサプライチェーンの一部と考える．
⑭	サプライチェーンに関する意識啓発，教育・訓練を行う．
⑮	サプライチェーンの配送メカニズムを強化する．
⑯	運用システムを防護し，モニターし，監査する．
⑰	要求の変更について交渉する．
⑱	サプライチェーンの脆弱性を管理する．
⑲	ソフトウェア更新時やパッチ適用時のサプライチェーン・リスクを低減する．
⑳	プライチェーン・インシデントに対応する．
21	廃棄時のサプライチェーン・リスクを低減する．

(2) ENISA のサプライチェーン管理

ENISA はサプライチェーン管理の複雑性，サプライチェーン全体に渡る IT ガバナンスの欠如，それによって共通した取り組みが実施できていないこと，セキュリティ管理のための製品やテクニックの欠如などの問題を指摘している．これらの課題に対応するための施策として，信頼性や整合性を評価するためのフレームワークの必要性を提唱している[16]．

(3) リスク対策としてのサプライチェーンのガバナンス

嶋作らは， IT サービスのサプライチェーンにおいて，個々の企業において IT ガバナンスが実施されていても，リスクが異なることから，サプライチェーン全体として，共通したリスク認識を持てないことが不正などの問題の根本原因となっていると指摘している[3]．

また，河野らは，IT サービスのサプライチェーンにおいて，個々の企業の IT がバンスでは，サプライチェーンの問題を解決できないことを指摘し，サプライチェーン全体を一体的なものと見なしてプロセスアプローチを適用することが必要であり，さらには，サプライチェーンを監査できるようにすることを提案している．以上のアプローチからは，単独企業における IT ガバナンスでは，複数企業から構成されるサプライチェーンのガバナンスには十分でないことが分かる．

4. 複数企業に関わる IT ガバナンスや情報セ

キュリティの統合アーキテクチャの必要性

3 章で述べたように，IT サービスのサプライチェーン全体を対象とした IT ガバナンスが必要である．これには，全体を一体的に扱う「アーキテクチャ」が必要と考えられる．原田・小倉[6]は，スマートシティプロジェクトにおける複数企業に適用するアーキテクチャを提案している．構造については，図 6 のようなサプライチェーン全体に対してアーキテクチャモデルを提案している．このアーキテクチャは複数企業を一体的に見なして統合的な機能を持つことになる．図 6 では，全体としてのビジョンやミッションを定義してサプライチェーン全体の組織戦略や目標を明らかにすることが必要となることを示している．以下では，このアーキテクチャについて考察する．

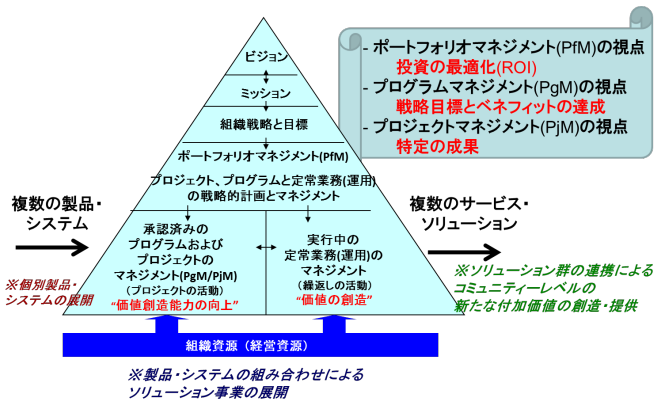


図 6. 複数企業における IT ガバナンスのアーキテクチャ（出所：原田・小倉 [6]）

(1)アーキテクチャの構成

複数の企業を一つにまとめた図 6 のモデルでは個々の企業の IT ガバナンスとサプライチェーン全体との対応をとる必要がある．これは，個々の企業が実践している IT ガバナンスを否定するものではなく，個々の企業の IT ガバナンスと全体の IT ガバナンスとの Performance 及び Acquisision のコーディネーションが必要となる．この案を図 7 に示す．

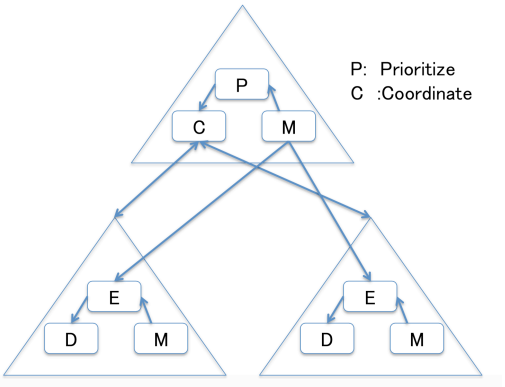


図 7　サプライチェーンのガバナンスモデル案

図 7 では，上位の三角形が全体の IT ガバナンスの機能を示し，下位の三角形は個々の企業の IT ガバナンスを指す．上位の全体の P は個々の企業のパフォーマンスをモニタして，企業間のアクティビティを測定してポートフォリオマネジメントの基礎データとする．一方，C は個々の企業の IT ガバナンスと全体の IT ガバナンスとの相互作用としての調整機能（Coordination）である．すなわち，P と C が全体の IT ガバナンスとして，サプライチェーン全体のポートフォリオマネジメントやプログラムマネジメントをリードする．次に，このような機能を前提とした場合の原則についての案を図 8 に示す．

- Principle 1: サプライチェーンの Responsibility
- Principle 2: サプライチェーンの Strategy
- Principle 3: 企業間の Acquisition
- Principle 4: 企業の Performance
- Principle 5: サプライチェーンの Conformance
- Principle 6: サプライチェーンの Human Behaviour

図 8　サプライチェーンの全体の IT ガバナンスの原則案

(2) アーキテクチャの実装

図 7 と図 8 に対して複数の企業がどのようにこのモデルに組み入れられるか．サプライチェーンを構成する企業間の IT ガバナンス間のマッピングを行う．また，企業間でコンフリクトする場合には，ポートフォリオマネジメントで企業間の連携や利害関係の調整が必要となる．以下にアーキテクチャに要請される点について述べる．

(a) アーキテクチャについて

原田・小倉[6] では，複数企業の例として英国のスマートシティプロジェクトを例にアーキテクチャの必要性を述べている．ここでは，統合アーキテクチャとして，企業間の相互運用性，IT サービスのインフラストラクチャーおよびデータの利用及び IT 利用者に向けた技術仕様が作成されていることを示し，スマートシティとしての都市政策立案者が，戦略を策定し，都市全体を管理し，新たな製品やサービスを開発するために必要な知識を，コード化（codify＝「アーキテクチャ」化）するべきとしている．これをベースにするためには，IT サービスについてもスマートシティ全体を対象にした IT ガバナンスが必要であり，そのための IT サービスに関するアーキテクチャが必要になるとしている．

(b) アーキテクチャの適用可能性

米国のスマートシティでは，民間にまかせた「市場」的な思考が強い．しかし，公共性を担保するために自治体のオンブズマンによる監視などの関与も見られる．米国やドイツなどのスマートシティプロジェクトなどと共通する点があり，アーキテクチャが適用できるかについて調査する必要がある[6]．

(c) アーキテクチャの構成要素・レイヤ構成

原田・小倉[6]は，アーキテクチャとしては，図 9 に示すような構造を提案している．これは，5 つのレイヤから構成される．具体的には技術の 3 つのレイヤと IT ガバナンスと IT マネジメントの 2 つの非技術レイヤで構成される．

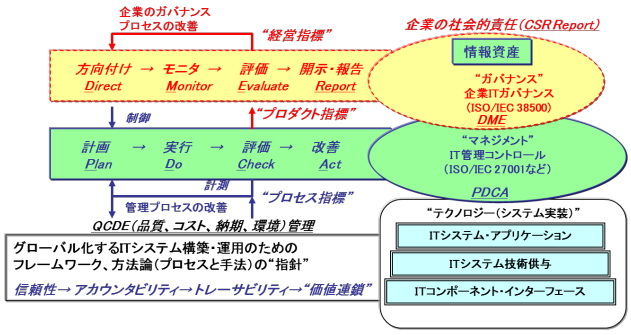


図 9. 複数企業における IT ガバナンスのアーキテクチャ（出所：原田・小倉 [6]）

図 9 では，IT ガバナンスと IT マネジメントについては，内部構造として EDM 及び PDCA が述べられている．しかし，EDM の主体が何か，また，各企業がどのように関わるかについては今後の研究としている．

(d) アーキテクチャと既存の標準類とのマッピング

(C) に述べたレイヤ構成が明らかになると，次は各レイヤでの技術のインタフェースや標準類，規格類について適用可能性を検討する必要がある．ここでは，既存の多くの規格をベースにプロトコルやインタフェースを利用することが必要となる．これは，IT サービスのサプライチェーンでは，既存の規格やデファクト標準を使って構築されており，これを全て置き換えるのはコスト面から現実的ではない．できる限り，利用できるものを活用すべきである． この例の一案を図 10 に示す．今後，ISO，IEC，ITU，IETF，IEEE などの既存の規格やデファクトを調査して図 10 を完成させる必要がある．

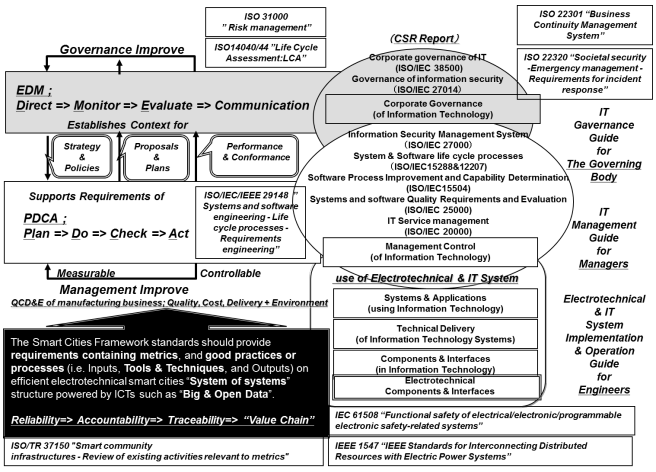


図 10 アーキテクチャに対応した既存の国際規格類のマッピングの一案（出所：原田・小倉[6]）

5. 課題

以上の考察からは，IT サービスのサプライチェーンのガバナンスについて，モデルとアーキテクチャの必要性について述べた．以下に今後の課題について述べる．

(1) サプライチェーン全体の可視化ができていない

久保らは，サプライチェーンの多層化，グローバル化によってサプライチェーン自体の可視化が難しくなっていることを指摘している[1]．これは，IT ガバナンスにおいても同様である．すなわち，企業間における透明性が担保されないと，図 7 に示す全体の Coodination やポートフォリオマネジメントが可能にならないからである．これは，企業にとっては有利・不利が交錯することになるので，チェーン全体の利益や規制などの情報を参加する企業全てに開示して同意を得る必要があるからである．

(2) アーキテクチャの適用において，構成企業間の協力関係の構築が難しい

関係するサプライヤの数が増加している．グローバル化に伴って国や地域，文化の多様性を考慮しなければならなくなっている．また，チェーン全体のコスト削減を求める中で，参加企業のリスク対応は全体で考えていく必要がある．例えば，サプライチェーンの一部の企業のリスクが高いと，その部分を攻撃される可能性があるからである．

(3) 国際規格の重要性

チェーンのグローバル化が進む一方で，企業によってはローカルは規格を利用しているケースが考えられる．今後，サプライチェーンが多数の企業で構成され，さらに，新しい IT 技術が駆使されていくと考えられる．このような中では，個社の要件を契約などで縛ると，将来的にサプライチェーンの進歩を阻害することになる．グローバルな広く利用されている国際規格が重要な要素となる

(4) ガバナンスの認識の啓発

IT ガバナンスには法的な拘束力がなく，企業間のコンセンサスをベースに決まる．そのため，サプライチェーン全体での課題への認識が低い場合，サプライチェーン全体に迷惑をかけてしまうことがある．例えば，サプライチェーン上の化学物質や紛争鉱物の取引などでは法的，もしくは準ずる形態の拘束もしくは義務がある．これを知らずに違反した場合，全体への影響，例えば，ブランドの毀損や法的な罰則などで全体に損害を与えることが想定される．サプライヤの協力会などを通した啓発，教育，改善支援活動が重要となる．

6. まとめ

サプライチェーンにおけるガバナンスは，多くの場合，階層型や従属型などでリーダ企業が全体を統率する形態が中

心であり，リーダ企業のガバナンスが全体のガバナンスでもあった．加護野の指摘するように，日本企業では，このようにサプライチェーンに参加することが目的化していて，運命共同体的な立場から結果的にガバナンスが機能していた．しかし，企業の多くがグローバル化しているため，サプライチェーンの対象が広がり，関連取引型やモジュール型など多数のモデルの形態も広がっている．この中では，従来のようなリーダ企業が強権的にリードすることも難しく，また，参加企業も運命共同体的な意識を持たなくなってきている．すなわち，新しいモデルを前提としたサプライチェーンのガバナンスが必要となっている．また，サプライチェーンにおける IT ガバナンスや情報セキュリティの在り方についての研究は，海外でも試行錯誤の段階である．

本稿では，このような問題点や課題を俯瞰して，IT ガバナンスを調整するモデルを提案している．また，このモデルを実現するためには新しいアーキテクチャが必要となる．このアーキテクチャについても考察して，新しいアーキテクチャを構築する際の考え方を提案している． なお，これらの提案が実現できるかについては，今後の課題である．

謝辞

本研究に関して，様々な指導や助言を頂いた原田研究室の先輩，同僚の皆様に感謝します．また，この研究を国際規格として検討いただいている ISO/IEC JTC1 SC40WG1 のメンバ（国際，国内）の皆さまに謹んで感謝の意を表します．

参考文献

1）久保知裕，原田要之助，サプライチェーンにおける情報セキュリティの研究，情報処理学会研究報告（EIP），2014-EIP-65(3)，pp.1-8，（2014 年 9 月）
2）河野翔太・原田要之助，プロセスアプローチを用いた IT 外部委託先管理の研究，情報処理学会研究報告（EIP），2014-EIP-64(3)，pp.1-8，（2014 年 5 月）
3）嶋作泰洋・原田要之助，有価証券報告書にみるリスク認識のあり方について－金融機関とシステムベンダの認識の差異－，情報処理学会研究報告（EIP），2014-EIP-64(1)，pp.1-8，（2014 年 5 月）
4）久保知裕，原田要之助，日本企業のサプライチェーンにおける情報セキュリティガバナンスに関する研究，情報処理学会研究報告（EIP），2014-EIP-63(12)，pp.1-7
5）久保知裕，原田要之助，サプライチェーンにおける日本企業の情報セキュリティガバナンスに関する研究，第 28 回研究大会，システム監査学会，2014 年 6 月 6 日
6）原田・小倉，価値連鎖でつながった企業間における IT ガバナンスの一考察，2014 年春期研究発表大会，経営情報学会 2014 年 6 月 1 日
7）Gary Gereffi，John Humphrey，Timothy Sturgeon，The governance of global value chains，Review of International
8）Martin Christopher，Hau Lee，Mitigating Supply Chain Risk Through Improved Confidence：International Journal of Physical Distribution & Logistics Management，vol.34，No.5，2004，pp.388-396
9）長内仁，後藤厚宏，企業間における情報セキュリティ連携アーキテクチャの検討，電子情報通信学会技術研究報告，巻：112 号：463，pp.699-704
10）Michael Porter，Mark R. Kramer，Creating Shared Value，Harvard Business Review，2011 年 6 月
11）赤池・水上，CSV 経営―社会的課題の解決と事業，NTT 出版，2013 年 7 月
12）日本セキュリティ監査協会，サプライチェーン情報セキュリティ管理について，2012 年，http://www.jasa.jp/information/result/pdf2011/2011_supplychain_doc01.pdf，アクセス 2014 年 1 月
13）加護野忠男，日本のビジネス・システム，国民経済雑誌，199(6)，PP.1-10
14）Dan Palmer，BSI，IEC スマートシティ白書ワークショップ，2014 年 3 月
15） NIST，NISTIR7622，Notional Supply Chain Risk Management Practices for Federal Information Systems，2012 年 6 月，pp.1-15
16）横山恭三，米国のサプライチェーンセキュリティ対策(3)，https://www.bsk-z.or.jp/kakusyu/pdf/26.12sapuraiche-nnhp.pdf，アクセス 2014 年 1 月
17）ENISA，An overview of the ICT supply chain risks and challenges，and vision for the way forward，pp.19-28