Vol.2020-EIP-88 No.11
2020/6/5

情報セキュリティマネジメントに対する経営層の関与

神橋基博 [1]

概要：情報セキュリティの向上は経営課題の一つであり，情報セキュリティマネジメントには経営層の積極的な関与が期待される．一方，類似の概念としてシステム管理があり，そちらにも経営層の関与が期待される．本研究では IT ガバナンスの概念モデルに基づき，経済産業省「システム管理基準」「情報セキュリティ管理基準」における経営層の関与を定量化し，比較することで，両者の重複と差異を明確化する．両者ともに経営層の関与は見られるものの，「システム管理基準」では「メカニズム」概念への関与が強いのに対して，「情報セキュリティ管理基準」では「責任」概念への関与が強い傾向が示される．この結果は，情報セキュリティの確保は社会システムの一員としての組織体にとって重要であることを示している．

キーワード：情報セキュリティ，情報セキュリティマネジメント，情報システム管理，IT ガバナンス

Management Involvement in Information Security Management

MOTHIRO KAMBASHI[†1]

Abstract: Improving information security is one of the management issues, and it is expected that management will be actively involved in information security management. On the other hand, there is system management as a similar concept, and the involvement of management is also expected there. In this research, based on the conceptual model of IT governance, quantification and comparison of the involvement of management in "System Management Standards" and "Information Security Management Standards" of the Ministry of Economy, Trade and Industry will clarify the duplication and difference between the two. Although both sides have management involvement, the "system management standard" has a strong involvement in the "mechanism" concept, while the "information security management standard" has a strong involvement in the "responsibility" concept. This result shows that ensuring information security is important for organizations as members of social systems.

Keywords: Information Security, Information Security Management, Information System Management, IT Governance

1. はじめに

近年におけるインターネットの普及と技術の進歩によって，情報セキュリティをめぐる環境は大きく変化してきた．IPA によると，インターネットが日本に普及し始めた 1990 年代において，情報セキュリティは，不正アクセス対策のためのファイアウォールや IDS の導入，ウイルス対策などの技術的対策が主流となっていた．しかし，2000 年 1 月における省庁ホームページの改ざん事件，4 月における郵政省のサーバがスパムメールの中継に利用される事件などを契機として，同年 7 月に政府は「情報セキュリティポリシーに関するガイドライン」を策定した．この一連の流れにより，情報セキュリティマネジメントが浸透し始め，情報セキュリティは，情報システム部門だけに任せるのではなく，組織全体で取り組むものであり，経営者の関与が重要であることが認識されはじめた．[1]

2010 年代には，ビジネスにおいて，情報システムが企業の収益性向上に不可欠なものとなった．一方で，企業が保有する顧客の個人情報や重要な技術情報を狙うサイバー攻撃が増加し，手口は巧妙化するようになった．これらの攻撃に従来の対策では対応できなくなり，情報システムおよびセキュリティに対する投資は，経営者による判断が必要となった．[2]

企業において，どのように情報セキュリティを管理するか，すなわち情報セキュリティマネジメントは，その重要性が増すにつれて，経営者の関与が求められるようになってきた．企業が情報セキュリティマネジメントを向上する際に，2 つの質問が考えられる．第一の質問は，経営者はどのように情報セキュリティに関与すべきなのだろうか，というものであり，第二の質問は，情報セキュリティマネジメントと近縁の概念である情報システム管理とどのように異なるのかという質問である．第一の質問に答えるために，公的あるいはデファクトなガイドラインとして，複数の団体が情報セキュリティに関するガイドラインを公開している．ガイドラインが改訂される際には，時代の要請を反映すると考えられる．従って，経営者の関与の重要性が増しているのであれば，改訂前後の差異を分析することで，どのような関与が求められていたのかを明らかにすることが可能となる．第二の質問に答えるためには，情報セキュリティマネジメントに関するガイドラインと情報システム

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

管理に関するガイドラインを同じ尺度で比較することで，その重複と差異を明らかにすることが可能となる．

本研究では，情報セキュリティマネジメントおよび情報システム管理に関するガイドラインを分析対象として，経営者の関与について，改訂前後の差異，およびガイドライン間の差異を明確にすることを目的とする．

分析にあたっては，計量テキスト分析と呼ばれる手法を用いて，経営者とその関与の関連性を定量化することでガイドラインの比較を試みる．同一ガイドラインの改訂前後を比較することで，経営者の関与がどのように変化したかを明らかにする．また，同一の尺度を用いて異なるガイドラインを比較することで，情報セキュリティマネジメントと情報システム管理における経営者の関与について，重複と差異を明らかにする．

2. 従来の研究

情報セキュリティマネジメントに対する経営者の関与について原田(2008)は，「情報セキュリティガバナンス」という用語を用いて説明している．情報セキュリティガバナンスは，取締役会と上級役員の責務であり，コーポレート・ガバナンスにとって不可欠な存在であるとしている．また図 1 に示す通り，情報セキュリティは，IT ガバナンスと整合してコーポレート・ガバナンスを支え，上級役員のコミットメント，セキュリティを意識した文化，良好なセキュリティのプラクティス，さらに方針へのコンプライアンスが必要であることを指摘している．[3]

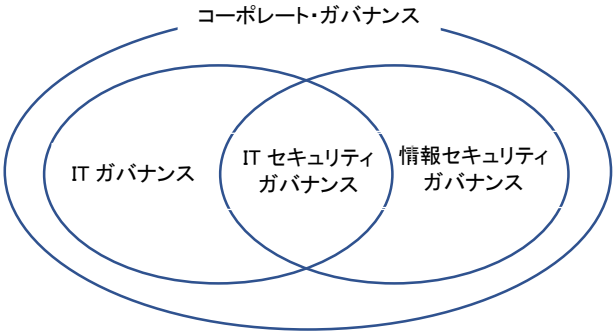

図 1 IT ガバナンスと情報セキュリティガバナンスの関係
(原田(2008), p27)

また，林(2010)では企業における情報セキュリティの状況を係長クラスが情報セキュリティ対策を一生懸命やっているが，その意図がトップには届いていない「係長セキュリティ」とし，「社長セキュリティ」が必要であるとして，5 つの「Awareness 提言」を行った．[4]

3. 分析対象と手法

3.1 分析の対象

本研究では，情報セキュリティマネジメントと情報システム管理における経営者の関与を分析するために，ガイドラインを分析対象とする．その理由は，現実における経営者の関与は組織体によって差異があるものの，ガイドラインはその時代におけるコンセンサスとしてまとめられたものであり，経営者がどうあるべきかを表したものであるためである．従って，経営者の関与が時間とともに重視されるようになったことを示すためには，分析対象とするガイドラインは改訂を重ねていることが望ましい．また，情報セキュリティマネジメントと情報システム管理を比較するためには，それぞれのガイドラインが同一の機関・組織体によって発行されていることが望ましい．

このような条件を満たすガイドラインとして，本研究では情報セキュリティマネジメントに関するガイドラインとして経済産業省の「情報セキュリティ管理基準」を，情報システム管理に関するガイドラインとして同省の「システム管理基準」を分析対象とする．

「情報セキュリティ管理基準」は 2003 年に組織体が効果的な情報セキュリティマネジメント体制を構築し，適切なコントロールを整備・運用するための実践的な規範として国際標準である ISO/IEC 17799:2000 を基にして策定されたものである．その後，2005 年に実践規範である ISO/IEC 27001:2005 および ISO/IEC 27002:2005 が策定されたことから，2008 年に「情報セキュリティ管理基準」の改訂（以下，2008 年度版）が行われた．また，2013 年には国際標準が ISO/IEC 27001:2013 および ISO/IEC 27002:2013 に改訂され，大幅な変更が加えられたことから，2016 年に再度改訂(以下，2016 年度版)が行われた．[5]

「システム管理基準」はもともと 1985 年に当時の通商産業省が「システム監査基準」として公開された内の実施項目として記載されていたものが，2004 年の改訂に際して分離されたもの(以下，2004 年度版)である．その後，システム管理基準に含まれる IT ガバナンスや事業継続管理が国際標準化されるとともに，クラウドやアジャイルなど新たな技術や手法といった変化に対応するために，2018 年に改訂（以下，2018 年度版）が行われた．[6]

本研究では情報セキュリティ管理基準の 2008 年度版，2016 年度版，システム管理基準の 2004 年度版，2018 年度版を分析対象とすることで，改訂前後における経営の関与の差異，情報セキュリティマネジメントと情報システム管理の差異を比較する．

3.2 分析の手法

2 つのガイドラインおよびその改訂前後を比較するため，本稿ではテキストマイニング等で用いられる計量テキスト分析を用いる．樋口(2014)によって，「計量的分析手法を用いてテキスト型データを整理または分析し，内容分析(content analysis)を行う方法」と定義される計量テキスト分析は，分析者の主観による影響を極小化するため，二段階で分析を進める．第一段階では，多変量解析を適用するために，あらかじめ形態素解析を用いて，文章中の用語の出現回数を一覧表にリストアップする．

第二段階では，同義語を考慮した分析を行うためにコーディングルールを用いる．コーディングルールとは，用語の分類を抽出するため，ルールを設定して用語を分類する．本稿では，経営者およびその関与を表す用語について，コーディングルールを用いて分類する．

第三段階では，分類されたグループ間の関連性を定量化する．計量テキスト分析においては，2 つの用語が，同一文中に出現する場合に，2 つの用語の間には共起性があるとする．この共起性を用いることで概念の関連性を定量化することが可能となる．なお，本稿では，共起性を表す指標として，ガイドラインの特徴を考慮し，Jaccard 係数[a]を使用する．

3.2.1 経営者を表す用語

経営者を表す用語について，情報セキュリティ管理基準の 2008 年度版は「経営陣」が用いられている一方，2016 年度版では，「経営陣」に加えて「トップマネジメント」，「管理層」も用いられている．「トップマネジメント」と「経営陣」は同じ意味とされており，本文では「トップマネジメント」，附属書では「経営陣」と使い分けがされている．また，「管理層」は，管理責任のある者の意味であり，「トップマネジメント（経営陣）」とその他の管理者の総称とされている．[7]

同様に，システム管理基準の 2004 年度版では，経営者を表す用語として「組織体の長」が用いられている．加えて「情報システム化委員会」は，情報システムに関する活動全般について，モニタリングを実施し，必要に応じて是正措置を講じ，組織体の長に報告する[8]とされていることから，「委員会」および「委員」は経営者の機能を一部委譲されていると考えられる．2018 年度版では，「組織体の長」という表現は見られない代わりに「経営陣」が用いられる．また「情報システム戦略委員会」，「プロジェクト運営委員会」などの委員会が経営者の機能を一部委譲されている点は 2004 年度版と同様である．

3.2.2 経営者の関与

上記のように異なるガイドラインでは異なる用語が同じ意味を指すために用いられる．従って，ガイドラインを比較するためには，あらかじめ用語をグルーピングする必要がある．経営者の関与についても，経営者が何に関与するのかという観点で用語を整理する必要がある．本研究では神橋(2020)における「IT ガバナンスの概念モデル」を用語の分類に使用する．[9]

IT ガバナンスの概念モデルでは，IT ガバナンスの定義が研究者によって異なるのは，IT ガバナンスが単一の概念ではないことの反映であり，表 1 に示す複数にグループ化された概念の組み合わせによって表現されることを示した．

表 1 IT ガバナンスの概念モデルにおける概念グループ
(神橋(2020) p.46 表 19 より抜粋)

グループ	基本的な概念
メカニズム	構造(Structure)，戦略(Strategy)，意思決定(Decision Making)，メカニズム(Mechanism)
能力	能力(Capability，Competence)，成熟度(Maturity)，有効性(Effectiveness)
規律	規則(Rule)，監査(Audit，Oversight)，説明責任(Accountability)
行動	評価(Evaluate)，指示(Direct)，モニタ(Monitor)，リーダーシップ(Leadership)，人間行動(Human Behavior)
責任	社会的責任(Responsibility)，利害関係者(Stakeholder)，法令遵守(Compliance)

3.2.3 コーディングルールの検討

各ガイドラインにおける用語の使い方を踏まえ，本稿で使用するコーディングルールを表 2 で示す．

表 2 本稿で用いるコーディングルール

グループ	用語
メカニズム	計画，方針，戦略，経営戦略，指針，権限，情報戦略，プロセス，指揮命令系統，目標
能力	知識，能力，人材，人的資源，経験
規律	ルール，手順，手続き，使命，規程，規定，基準
行動	評価，識別，分析，指示，把握，モニタリング，是正，人間行動，任命，モニタ，マネジメントレビュー
責任	コンプライアンス，遵守，責任，利害関係者，関係者
経営者	組織体の長，経営陣，委員，委員会，トップマネジメント，管理層

a Jaccard 係数とは，文章中の 2 つの用語間の共起性を表現するために使用される指標の一つである．用語 A と用語 B について，n(A∩B)を用語 A と用語 B の両方が出現する文の数，n(A∪B)を用語 A または用語 B が出現する文の数としたときに n(A∩B)/n(A∪B)によって算出される．0 から 1 までの値を取り，共起性が強いほど 1 に近づく，この係数にはどちらの条件もあてはまらない文の影響を無視するという特徴があり，一文の中に登場する語の数が少ない文書の分析に適している．

4. 分析結果と考察

4.1 システム管理基準における改訂前後の比較

4.1.1 各グループの出現率

2004 年度版および 2018 年度版のシステム管理基準における各グループの出現率は図 2 の通りである．改訂前後で各グループの出現率はほぼ同じ傾向を示すが，2018 年度版では，「行動」，「経営者」のグループの出現率が増加している点に特徴がある．

2018 年度度のシステム管理基準において，ISO/IEC 38500:2015 を参照し，IT ガバナンスを重視している．この ISO における IT ガバナンスの概念は表 2 における「行動」グループに属している．これが，「行動」および「経営者」のグループの出現率が増加した要因と考えられる．

図 2 システム管理基準における
概念グループと経営者の出現率

4.1.2 各グループと経営者の関連性

2004 年度版および 2018 年度版のシステム管理基準における「経営者」と他のグループの関連性は図 3 の通りである．5 グループ全てにおいて「経営者」との関連性が増加している点に特徴がある．

ISO/IEC 38500:2015 における IT ガバナンスは「行動」グループに属するが，「行動」グループだけでなく，他の 4 グループについても関連性が増加していることは，IT ガバナンスだけでなく，システム管理においても経営者の関与の重要性が反映されている．

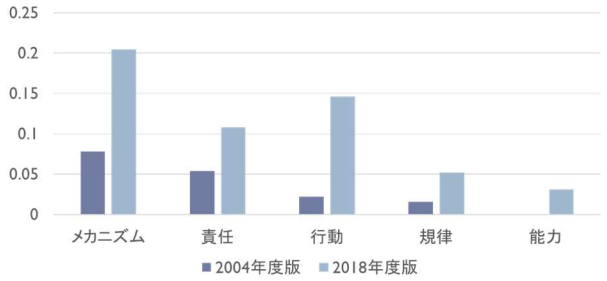

図 3 システム管理基準における
概念グループと経営者の関連性

4.2 情報セキュリティ管理基準における改訂前後の比較

4.2.1 各グループの出現率

2008 年度版および 2016 年度版の情報セキュリティ管理基準における各グループの出現率は図 4 の通りである．改訂前後で各グループの出現率はほぼ同じ傾向を示すものの，全グループの出現率が低下している点に特徴がある．

2016 年度版の情報セキュリティ管理基準では，管理策が大幅に追加されており，ガイドライン全体における各グループの出現率低下となっていると考えられる．

図 4 情報セキュリティ管理基準における
概念グループと経営者の出現率

4.2.2 各グループと経営者の関連性

2008 年度版および 206 年度版の情報セキュリティ管理基準における「経営者」と他のグループの関連性は図 5 の通りである．「能力」を除いた 4 グループにおいて「経営者」との関連性が増加している点に特徴がある．

特に，2016 年度版では「マネジメントレビュー」を介して経営者が情報セキュリティマネジメントに関与しているために「行動」グループの増加に繋がっている．

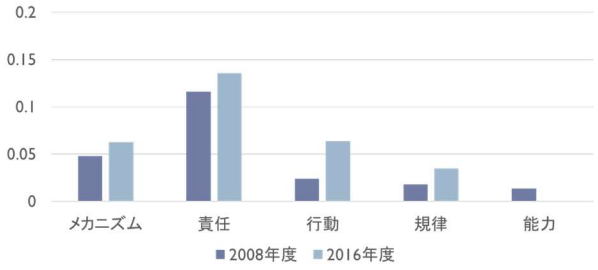

図 5 情報セキュリティ管理基準における
概念グループと経営者の関連性

4.3 考察

「情報セキュリティ管理基準」と「システム管理基準」は異なるガイドラインであるために，各図の数値を直接比較することはできない．しかしながら，図 2 および図 4 において，各グループの出現率が類似の傾向を示すから，情報セキュリティマネジメントと情報システム管理において，管理の対象は異なっていても，管理の枠組みにおいては共通項を持つことを示唆すると考えられる．

一方, 図 3 および図 5 において, 各グループと「経営者」との関連性が異なる傾向を示すことは，情報システム管理と情報セキュリティマネジメントが同じ管理の枠組みを持っていても，経営者が重点的に関与するポイントが異なっていると考えられる．システム管理基準において「メカニズム」と「行動」が「経営者」と高い関連性を示すことは，情報システム管理の重点が組織内に置かれていることを示唆する. また, 情報セキュリティ管理基準において,「責任」が「経営者」と高い関連性を示すことは，情報セキュリティマネジメントにおいて，組織外に重点が置かれていることが示唆される．

これらは，情報システム管理に属する，プロジェクト管理，運用・保守，災害対策などは，あくまでも社内の問題であり，それらの管理が不十分であっても組織外に及ぼす影響が限定的と見なされていると考えられるのに対して，情報セキュリティマネジメントに属するセキュリティポリシー，アクセスコントロールなどは，一旦，問題が発生するとその影響は組織外に波及する可能性が高いとみなされていると考えられる．

5. まとめ

本研究では，計量テキスト分析を用いてガイドラインである「情報セキュリティ管理基準」および「システム管理基準」を分析することで，情報セキュリティマネジメントおよび情報システム管理における経営者の関与を比較した.

情報セキュリティマネジメントと情報システム管理の共通点として，2 点が明らかにされた．まず，両ガイドラインにおける改訂において，経営者との関連性は増加しており，それぞれにおいて経営者の関与の必要性が増加していることが反映されている．また，両ガイドラインにおいて, 各概念グループの出現率の傾向は類似していることは，情報セキュリティマネジメントと情報システム管理は，管理の対象が異なっていても，管理の枠組みにおいて共通項を持つことを示唆している．

一方，情報セキュリティマネジメントと情報システム管理の相違点として，経営者が関与する領域の差異が認められた. 情報システム管理において,「メカニズム」と「行動」が高い関連性を示し, 組織内に重点が置かれている. また, 情報セキュリティ管理基準において,「責任」が高い関連性を示し，組織外に重点が置かれている．

これらの結果は，情報セキュリティの専門家にとっては感覚的には認識されていたかもしれないが，本研究によって定量的に示すことが可能になった．

なお，今回用いた分析手法は他のガイドラインにおいても適用が可能である．

例えば，経済産業省が公開するガイドラインの内，情報セキュリティに関連するものとして,「サイバーセキュリティ経営ガイドライン」,「デジタルトランスフォーメーションを推進するためのガイドライン」などがある．[10][11]

これらにおける概念グループの出現率，経営者との関連性に関する, 情報セキュリティ管理基準と比較することで, サイバーセキュリティ，デジタルトランスフォーメーションにおける経営者の関与を比較することが可能となると考えられる．

また，本研究では「IT ガバナンスの概念モデル」を用いて概念グループを分類したが, IT ガバナンスと異なり情報セキュリティマネジメント，サイバーセキュリティ，デジタルトランスフォーメーションでは，経営者と関連する異なる概念グループが存在する可能性がある．

これらの点については, 今後の課題として取り組みたい.

参考文献

[1] IPA, 情報セキュリティガバナンス https://www.ipa.go.jp/security/manager/know/meaning/governance.html (2020.04.19 アクセス)
[2] 経済産業省, サイバーセキュリティ経営ガイドライン, https://www.meti.go.jp/policy/netsecurity/mng_guide.html (2020.04.19 アクセス)
[3] 原田要之助，IT ガバナンスと情報セキュリティガバナ ンスの構築に向けて，2008 https://expo.nikkeibp.co.jp/erm/2008/pdf/H4.pdf (2020.04.19 アクセス)
[4] 林紘一郎，係長セキュリティから社長セキュリティへ: 日本的経営と情報セキュリティ，情報セキュリティ総合科学 第 2 号，2010，p1-42.
[5] 経済産業省，情報セキュリティ管理基準（平成２８年改正版），2016，p1
[6] 経済産業省,「システム監査基準」及び「システム管理基準」の改訂について https://www.meti.go.jp/policy/netsecurity/sys-kansa/h30kaitei.html (2020.04.19 アクセス)
[7] 経済産業省，情報セキュリティ管理基準（平成２８年改正版），2016，p5 脚注
[8] 経済産業省，システム管理基準，2004，p2
[9] 神橋基博，IT ガバナンスモデルの研究 －金融機関の事例を中心とした分析－，情報セキュリティ大学院大学博士論文，2020，p45-46
[10] 経済産業省，サイバーセキュリティ経営ガイドライ Ver 2.0，2017 https://www.meti.go.jp/policy/netsecurity/mng_guide.html (2020.04.19 アクセス)
[11] 経済産業省，DX レポート ～IT システム「2025 年の崖」克服と DX の本格的な展開～，2018 https://www.meti.go.jp/shingikai/mono_info_service/digital_transformation/20180907_report.html (2020.04.19 アクセス)