

第 26 回情報通信学会大会個人研究発表

企業情報セキュリティガバナンスに関するグローバル標準の研究

A study of global relevant standard on Corporate Information Security Governance

小倉博行¹、坂本勝²

Hiroyuki OGURA and Masaru SAKAMOTO

概要

情報セキュリティガバナンスの標準化について、ITU-T データネットワーク・テレコミュニケーションソフトウェア研究委員会、経済産業省の研究会等で議論されている。また、情報通信技術に関する標準化活動を担う委員会である情報処理学会情報規格調査会は、ISO/IEC 情報技術合同技術委員会(JTC 1)情報セキュリティ専門委員会や企業 IT 統制作業グループに参加して、情報セキュリティガバナンスと企業 IT 統制の関係や標準化を推進している。本稿では、これら企業情報セキュリティガバナンス標準化動向を踏まえ、グローバル化する IT システム構築のために必要な標準フレームワーク、方法論（プロセスと手法）を 5 層規格カテゴリモデルを用いて考察する。

Abstract

Information Security Governance can be described as an integral element of Corporate Governance by helping to achieve strategic alignment with business objectives, assign responsibility and decision making capability, and comply with laws and regulations.

We consider a global relevant standard framework and methodology on Corporate Governance of IT, by the use of IT, for the system to deliver IT service.

キーワード

情報セキュリティガバナンス、コーポレートガバナンス、
企業 IT 統制、国際標準化、ロバート議事規則

Keywords

Information Security Governance, Corporate Governance,
Corporate Governance of IT, International Standardization, Robert's Rules of Order

¹ 三菱電機株式会社 情報技術総合研究所
Information Technology R&D Center, Mitsubishi Electric Corp.

² 早稲田大学大学院 国際情報通信研究科
Graduate School of Global Information and Telecommunication Studies, Waseda Univ.

1. はじめにーグローバル化する IT 基盤と企業競争力・価値向上を担う情報セキュリティガバナンス

2006 年に実施された ITU-T アンケート調査「一番有益であった国際標準は何であったか」の結果は、第 1 位が MPEG (H. 262/H. 264)映像信号符号化方式 (25%)、第 2 位が No. 7 信号方式 (17.9%) であり、これらの 2 方式の国際標準開発には日本人が多大な貢献を行ってきた。[文献 1, 2]

情報通信サービスは、国内外の多種多様なネットワークや端末が相互に接続することによって、はじめてサービスが実現するものである。このため、情報通信機器をグローバル市場に展開するためには、国際標準に沿って製品を作ることが必須であり、また、国際標準化により相互接続性・相互運用性を確保することによってネットワークのオープン化が進むこととなり、製品やサービスの新規参入が容易になることから、情報通信分野におけるさらなるイノベーションを促進することが期待できる。

また、1995 年に国際標準を国内の基礎とすることを義務づける WTO/TBT 協定 (世界貿易機関/貿易の技術的障害に関する協定) が発効され、情報通信分野の技術革新が進み、情報通信市場が多様化する中で、国際標準が世界市場へ与える影響はますます増大している。わが国でも「オープンな標準」¹に基づく政府調達指針が提示され、国際規格 ISO/IEC 26300 (Office Open XML Format) 等 ISO/IEC JTC 1 や ITU-T による情報通信技術の国際標準化活動が活発化している。²

最近の情報通信サービスの分野では、IT システムのライフサイクルを通して、システム・エンジニアリング・プロセスを適用および実行するための手法や技術、ツールに関する記述を与える国際標準モデルの新提案等が審議されている。[文献 3]

グローバル化する IT システムの安全・信頼性確保のための課題は、物理セキュリティや情報セキュリティの連携に必要な情報を共通プロトコルを用いて相互に通信し、利用者のニーズに応じたセキュリティシステムを構築し、合わせて、セキュリティだけでなく、業務システム、設備管理、情報家電、カーナビ等の IT 機器との連携を国境を越えたマルチベンダ環境でシステム実装することである。この共通プロトコルを、ITU/ISO/IEC 等のオープンな標準技術に準拠させることにより、グローバル市場での SCM (サプライ・チェーン・マネジメント)、物流安全管理等の事業を実現することができる。[文献 4]

一方、昨今の重要インフラ IT システム事業を支える IT (情報技術) は、範囲が広く、進歩が早く、かつ相互の関連が密接であるため、個々の技術を深化するだけでは不十分で、IT システム構築全般に関わる総合的な洞察を行うための標準モデルの開発が必要である。特に、企業情報セキュリティ技術については、従来の暗号アルゴリズムや ID 管理等の技術[文献 5]から、監視～監査～統制というガバナンスの考え方を導入して、セキュリティから企業統治へと統合してゆく必要がある。[文献 6, 7]

本稿では、国際標準に基づく企業情報セキュリティガバナンスの方法論 (プロセスと手法) を開発するための、5 層規格カテゴリモデルについて考察する。

2. 情報セキュリティガバナンスの概念定義

(1) 情報セキュリティガバナンス

わが国において、「情報セキュリティガバナンス」の概念は、次のように定義されている。

「社会的責任にも配慮したコーポレートガバナンス (企業統制) と、それを支えるメカニズムである内

部統制の仕組みを、情報セキュリティの観点から企業内に構築・運用すること」[文献 8]

さらに、企業戦略に整合的な情報セキュリティガバナンスの普及に資するため、情報セキュリティガバナンスの概念について、次のように一層の明確化が図られている。

「様々なリスクの内、情報資産に係るリスクの管理を狙いとして、情報セキュリティに関わる意識、取組及びそれらに基づく業務活動を組織内に徹底させるための仕組み*を構築・運用することを情報セキュリティガバナンスと位置づける。(*経営者が方針を決定し、組織内の状況をモニタリングする仕組み及び利害関係者に対する開示と利害関係者による評価の仕組みを指す)」[文献 9]

(2) 企業 IT 統制

一方「企業 IT 統制」[文献 10]の国際標準化は、ISO/IEC JTC 1 作業グループにて、2008 年に発行された国際規格 ISO/IEC 38500 の維持及びその関連のガイド文書の検討が行われている。[文献 11]

企業 IT 統制の概念については、経済産業省の研究会、ITU-T/SG 17 (データネットワーク・テレコミュニケーションソフトウェア研究委員会)、JTC 1/SC 7 (ソフトウェア・システムエンジニアリング専門委員会) でも同種の議論が行われている。さらに、JTC 1/SC 27 (セキュリティ技術専門委員会) でも情報セキュリティガバナンスの新提案が成立する見込みである。

「企業統制 (コーポレートガバナンス)、ITガバナンス、情報セキュリティガバナンスの関係」の概念については、JTC 1/SC27 が図 1 のように定義している。³[文献 12]

3. 企業 IT 統制フレームワークの設計

(1) 企業統制の責任とドメイン

図 2 に企業統制の責任と 7 つのドメインを示す。[文献 13]

企業統制は、内部と外部の両方の視点で、企業組織の過去、現在、将来の企業活動を対象として、戦略立案、政策作成を行う。そして、CEO (最高経営責任者) と協働して、企業活動の方向付け、モニタと監督を行う。

また企業統制は、情報を含む 7 つのドメインまたは資産群を対象とする。情報と IT とは同一であり、IT は情報を管理し、現在と将来の企業活動を可能にする資源であると考えられる。

つまり、企業統制システムは、管理活動により維持され、統治する企業組織の可視化とコントロールを提供するものと位置づける。

(2) 5 層規格カテゴリモデル

図 3 に、企業 IT 統制フレームワークの 5 層規格カテゴリモデルを示す。⁴[文献 13, 14]

グローバル化する IT システムの企業情報セキュリティガバナンスは、従来の管理者層中心の「“計画→実行→評価→改善” サイクルの企業情報セキュリティ “マネージメント” フレームワーク」から、経営者層も含めた「“方向付け→モニタ→評価→開示・報告” サイクルの企業 “ガバナンス” フレームワーク」へと統合させていく必要がある。

企業 IT 統制層は方向付け (Establishes Context for) を行い、IT 管理コントロール層はその要求目標の達成 (Supports Requirements of) を行う。そして、“テクノロジー (システム実装)” 3 層 (IT システム・アプリケーション、IT システム技術供与、IT コンポーネント・インターフェース) は、QCD (品質、コスト、納期) 管理のための“信頼性→説明責任→追跡可能性→SCM” サイクルの計測可能性

(Measurability) と管理可能性 (Controllability) を保証する。従って、そのための評価指標の設計が必要である。

(3) 法規制適合性の評価指標

情報セキュリティに関する既存の法令・基準・ガイドライン等の分野は、①情報セキュリティ技術、②情報セキュリティ組織運用、③個人情報保護、④内部統制、⑤SLA、⑥IT サービス、⑦事業継続、⑧信頼性の8つのカテゴリに分類できる。[文献 15]

企業 IT 統制は、経営責任者や管理責任者が遵守すべき情報セキュリティに関する組織規定やルール、法令、ガイドライン等の内容と対策内容に矛盾が生じないようにする等の整合性の調整を行う活動である。この企業の情報資産を保護する活動の遵法評価指標として、社内規定・ルール⇒関連・参照可能な基準／ガイドライン⇒ガイドブック⇒実践のための規範(ベストプラクティス) ⇒仕様(認証基準) ⇒法令、の5段階の法規制の遵守レベル(任意法規⇒強制法規)の設定を提案する。この法規制への適合性を評価する指標(計測かつ管理可能なレベル設定項目)は、企業 IT 統制システムの品質特性 (ISO/IEC 9126: 機能性、信頼性、使用性、効率性、保守性、移植性) と対応づけることができる。

4. おわりにーグローバル標準による企業 IT 統制

情報 (&IT) 資産の情報セキュリティを含む企業統制システムのガイドライン・仕様 (認証基準) 等を記述する ITU/ISO/IEC 国際規格文書は、グローバル IT システムのソフト・ロー (強制力のない任意法) であり、その制定審議規則は国際会議のコモン・ローであるロバート議事規則[文献 16]に準ずるものとなっている。

ロバート議事規則は、難しい利害関係者との調整に対処する会議プロセスのベストプラクティス集であり、多様性を尊重して利害関係者を妥協させ決議するための議事法のグローバル標準である。会議の議長は、ロバート議事法に従い、公正無私でなければならない。IT システムの契約書は市場主義による当事者間の自由意志に基づいて作成するものであり、状況に寄って変わるものであるが、一般に、『強制法規 (独禁法、国際条約等) > 契約書 (仕様書等) > 任意法規 (著作権法、グローバル標準等)』という関係がある。[文献 17, 18]

今後、複雑化かつ大規模化する IT システムの持続的成長と革新を行うためには、技術、市場、制度ともにグローバル標準の企業 IT 統制 (企業情報セキュリティガバナンス) システムとして社会実装することが必要であり、市場適合性のある国際標準 (market relevance, global relevant standard) に基づく IT システム構築フレームワークや方法論の開発に貢献してゆきたい。

図 1. 情報セキュリティガバナンスと企業 IT 統制の関係

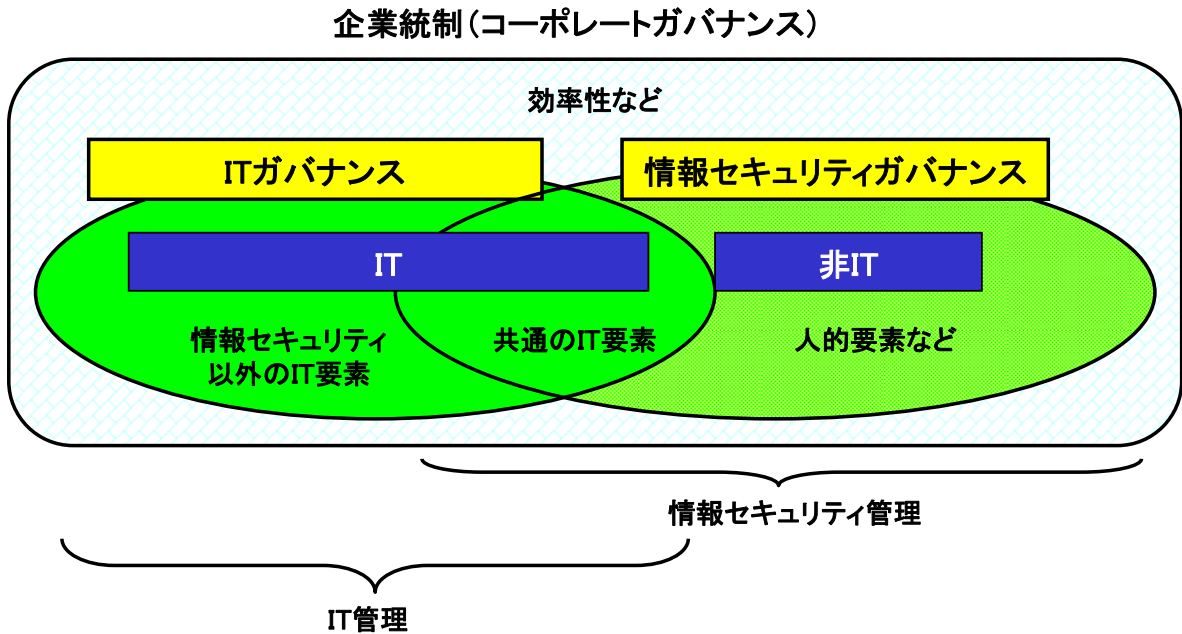


図 2. 企業統制の責任とドメイン

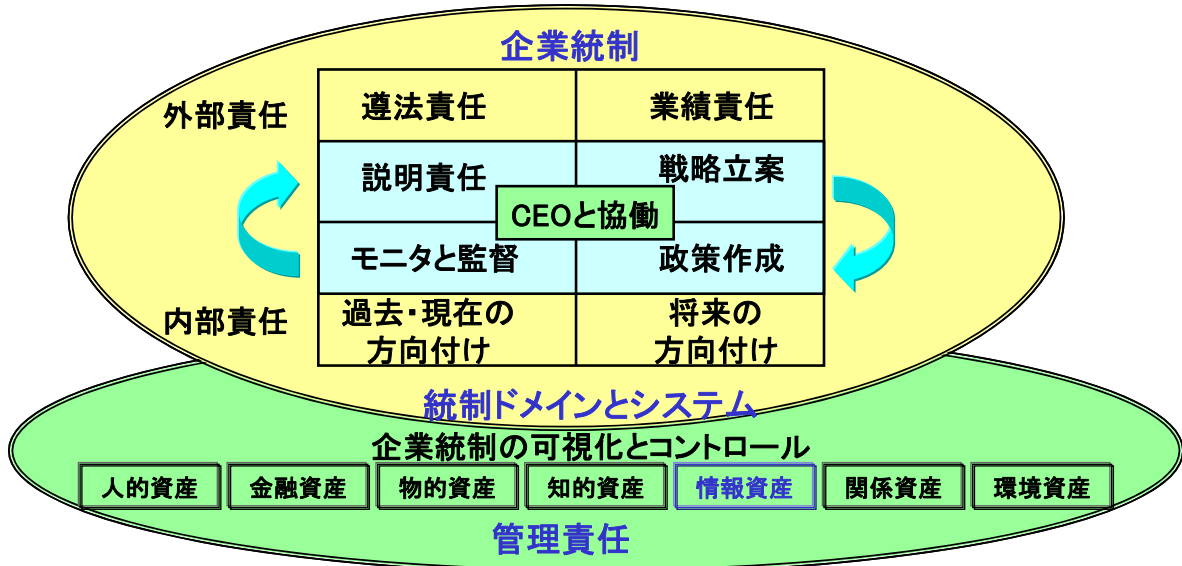
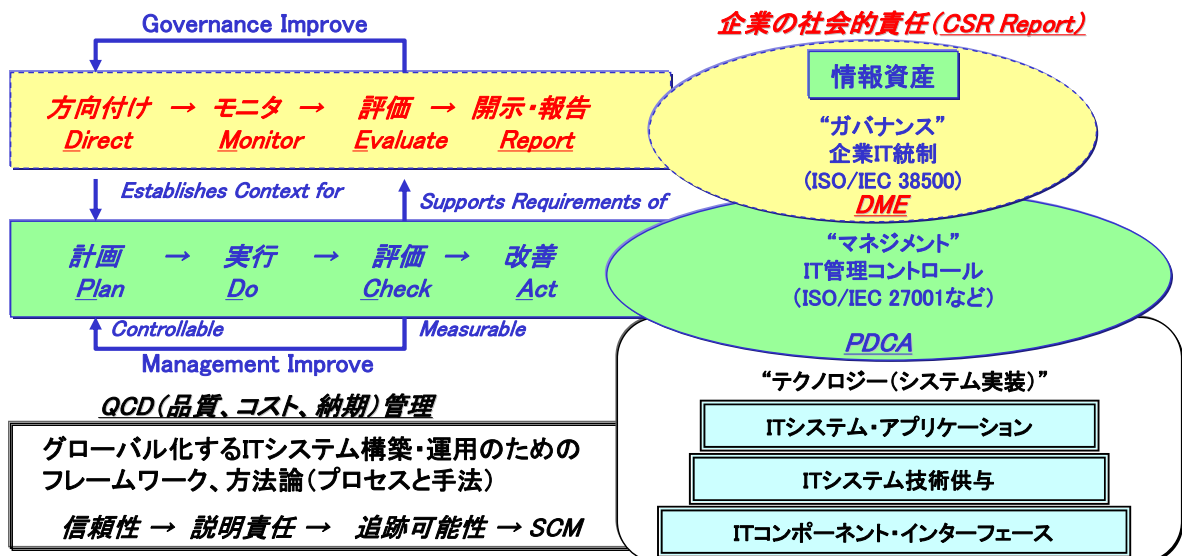


図 3. 企業 IT 統制フレームワークの 5 層規格カテゴリモデル



参考文献（引用順）

- 1 加納貞彦, 「No. 7 信号方式: 電話系通信網の制御インフラ国際標準」, ITU ジャーナル 4 月号特集, 2009. 4.
- 2 安田浩, 「MPEG 標準化活動 20 周年」, IPSJ/ITSCJ 情報技術標準 NEWSLETTER No. 81, 2009. 3.
- 3 ISO/IEC JTC 1/SC7 寄書 N4258, “New Work Item Proposal: Systems Engineering – Systems Engineering Handbook”, 2009. 02. 23.
- 4 (財)流通システム開発センター, 「EPC RFID システム導入における検討事項調査報告書」, 2008.
- 5 小倉博行, 坂本勝, 黒田正博, 「ユビキタスネット社会における情報セキュリティアーキテクチャモデルの研究」, 第 25 回情報通信学会大会個人研究発表, 2008.
- 6 科学技術振興機構/社会技術研究開発センター, 「社会技術シンポジウム/ユビキタス社会のガバナンス」配布資料, 2009. 03. 05.
- 7 経済産業省, 日本経済新聞社, 「情報セキュリティガバナンスシンポジウム 2009」配布資料, 2009. 03. 06.
- 8 経済産業省, 「企業における情報セキュリティガバナンスのあり方に関する研究会」, 2005.
- 9 経済産業省, 「産業構造審議会情報セキュリティ基本問題委員会 中間とりまとめ」, 2008.
- 10 経済産業省企業行動課編, 「コーポレート・ガバナンスと内部統制」, 2007.
- 11 ISO/IEC JTC 1/WG6 寄書 N0011, “WD ISO/IEC 29184 Developmental guide version 1.00”, 2009. 04. 29.
- 12 ISO/IEC JTC 1/SC27/WG1 寄書 N17214, “SC 27 contribution of information security governance in response to JTC1 request”, 2008. 10. 10.
- 13 ISO/IEC JTC 1/IT ガバナンス研究グループ 寄書 SGITG-N0021, “A Framework for Governance of IT”, 2008. 05. 09.
- 14 ISO/IEC JTC 1/John Graham (コンビナー) 寄書 N9318, 「IT ガバナンス研究グループ中間報告」, 2008. 10. 09.
- 15 総務省, 「ASP・SaaSにおける情報セキュリティ対策ガイドライン」参考資料, 2008.
- 16 Henry M. Robert (原著) / 安藤仁介 (訳), 「ロバート議事規則」, ロバート議事規則研究所, 1876/1986.
- 17 矢野直明, 林紘一郎, 「倫理と法/情報社会のリテラシー」, 産業図書, 2008.
- 18 小倉博行, 坂本勝, 「自治体 IT 経費分析に基づく共同利用業務システム経済効果と契約関係モデルの研究」, 第 23 回情報通信学会個人研究発表, 2006.

¹ 2007 年 3 月 1 日 各府省情報化統括責任者 (CIO) 連絡会議 決定「情報システムに係る政府調達の基本指針」別紙 2 P2

² ITU: 国際電気通信連合 (International Telecommunication Union)、1865 年に発足 (国連組織)。ITU-T: 国際電気通信連合 電気通信標準化部門。ISO: 国際標準化機構 (International Organization for Standardization)、1947 年に発足。IEC: 国際電気標準会議 (International Electrotechnical Commission)、1906 年に発足。ISO/IEC JTC 1 (Joint Technology Committee 1): 1987 年に ISO/IEC が設置した情報技術の合同委員会。

³ IT ガバナンスか情報セキュリティガバナンスかに関わりなく、昨今の世界中の法人が必要としている標準化の重要なドメインはガバナンスに関する記述である。SC27 は IT ガバナンス等の他のガバナンス問題の JTC 1 の取扱いにおける他のグループとの共同作業プログラムを情報セキュリティガバナンスのドメインで始めている。IT セキュリティソリューションと技術のみで、企業情報資産保護の問題は解決できない。すなわち、企業情報資産の保護とサポートへの戦略の問題を解決する組織の企業統制は、有効な情報セキュリティガバナンスに依存する。

従って、情報セキュリティガバナンスは、コーポレートガバナンス (企業統制) の統合要素のひとつとして標準化記述することにより、事業目標との戦略的整合を達成し、責任と意思決定能力を与え、法規制への適合に寄与する。

⁴ ISO/IEC JTC1 が開発した各規格における企業情報セキュリティガバナンスの構成要素は、次のとおりである。

規格 ISO/IEC 38500 は企業 IT 統制のみに関連している。規格 ISO/IEC 16085 (ライフサイクルプロセスのリスク管理) は企業 IT 統制に關係する実質的な要素を記述している。一方で 13 の規格は企業 IT 統制に關係する重要な要素を記述している。これら 14 のすべての規格は、企業統制に実質的または重要な関係があり、また IT の管理コントロールのみに関連があると分類できる。企業統制は、管理の監督を含み、管理システムが適切かつ効率的である保証を要求する。その意味において、これらの規格は企業統制に関連すると考えることができる。しかしながら、これらの規格は、統制する経営者自身に対する専門的なガイドラインは提供しておらず、それゆえ、企業統制層 (経営者層) のためには、これらは管理コントロール層 (管理者層) のみに関連した認証基準を与えているだけである。つまり、これらの規格は企業統制の周辺のみを扱っており、管理コントロール関連が大部分である。

同様に、ISO/IEC 27001 (情報セキュリティ管理システムの要件) は、明確に方向付け・コントロールを扱っている一方で、その企業統制関連は、主に管理の取り組みを統制する経営者の管理成果の評価のための基準と組織のセキュリティ計画の効率性を記述している。統制する経営者に対する専門的ガイドラインについてはまったく提供していない。