Vol.2015-SPT-16 No.14
Vol.2015-EIP-70 No.14
2015/11/20

情報セキュリティマネジメントシステムの ボトムアップ手法に関する考察

曽我充哉[†1]　原田要之助[†1]

概要：ISMS をベースとする情報セキュリティマネジメントは，国際標準である ISO/IEC 27001 で規定されるようにトップダウンによるマネジメントで進められる．一方で，日本企業の経営はボトムアップの文化を持っており，企業運営もボトムアップで行われている．現在，日本企業の情報セキュリティマネジメントは，ボトムアップ型である環境下で，トップダウンによるマネジメントを導入している問題がある．しかしながら，同じトップダウンによって進められる品質マネジメントの分野では，日本型経営の特徴でもある TQC 等のボトムアップによるマネジメントで成功をしており，情報セキュリティマネジメントにおいてもボトムアップ手法が応用できるのではないかと考えられる．本論文では，情報セキュリティマネジメントシステムにおけるボトムアップ手法について考察を行う．

キーワード：ISMS, PDCA，日本型経営, TQC，ボトムアップアプローチ，トップダウンアプローチ

A study on the bottom-up approach for information security management System.

MITSUYA SOGA[†1]　YOUNOSUKE HARADA[†1]

Abstract: The information security management based on ISMS is pushed forward by the management of the top-down approach so that it is prescribed in ISO/IEC 27001 which is an international standard. On the other hand, the Japanese company has own corporate culture of the bottom up management style, and the management is carried out with a bottom up approach.
The problem is that the information security management of the Japanese company introduces the top-down approach management under the environment that is a bottom up style management. However, in the field of quality management pushed forward with a same top-down approach, the bottom-up approach achieves success in many Japanese companies by the TQC approach which is a Japanese management feature. Therefore, bottom-up approach may be applied to the management of information security.
The purpose of this paper is a study of the bottom-up approach for information security management.

Keywords: ISMS, PDCA, Japanese-style business management, TQC, bottom-up approach, top-down approach

1. はじめに

現在，情報システムは，社会において欠くことのできない重要な基盤となっている．情報システムを使用しない経済活動は不可能であり，安定的なシステム運用が求められている．

一方で，情報システムを対象としたセキュリティインシデントは増加を続けている．独立行政法人情報処理推進機構(以下，IPA という)の情報セキュリティ白書 2015[1]によれば，日本における 2014 年度のセキュリティインシデントとしてはインターネットバンキングやクレジットカード情報の不正利用の被害件数が過去最悪を更新したことや，内部不正による情報漏洩によって国内史上最悪の顧客情報の流出事件等があり，企業活動にとって重大な影響を及ぼす事件が発生していると述べられている．すなわち，被害規模の増大とともに，企業における情報セキュリティマネジメントの重要性が年々高まっている．

1.1 日本における情報セキュリティマネジメントの規格・ガイドライン

現在，日本の多くの企業で取り入れられている情報セキュリティマネジメントの規格としては，ISO/IEC 27001:2013（以下，ISO/IEC 27001 という）を JIS 化した JIS Q 27001:2014[2]（以下，JIS Q 27001 という）が挙げられる．この規格の策定は，元々英国規格協会が 1995 年に策定した BS7799-1 から始まり，1997 年に情報セキュリティマネジメントの要求条件をまとめた BS7799-2 が作られ，2000 年には BS7799-2 をベースに ISO/IEC17799:2000 が策定された[3]．その後，図 1 に示すとおり ISO/IEC17799:2000 は 2005 年に内容を見直されたのち ISO/IEC27002:2005 に改称され，同じ年に BS7799-1 を基にして ISO/IEC27001:2005 が作成された．2013 年に他の

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

Vol.2015-SPT-16 No.14
Vol.2015-EIP-70 No.14
2015/11/20

規格との整合性をとられた ISO/IEC27001:2013 及び ISO/IEC27002:2013 が策定されている[4]．以下では，規格のあとの年号を省略した場合には 2013 年版を指す．

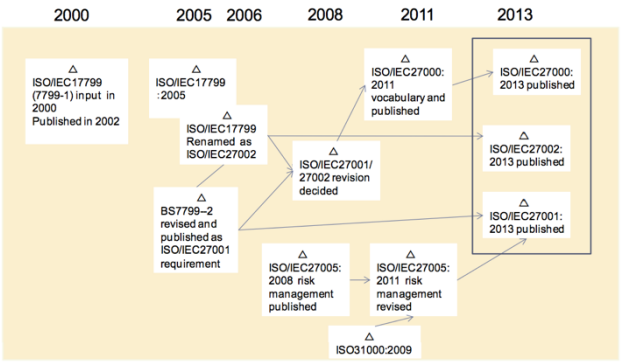

図 1　情報セキュリティマネジメント規格の変遷[4]

これまでに，規格の改定が行われているが，基本的な考え方であるトップマネジメントを中心としたプロセスアプローチや PDCA サイクル，継続的改善といった今日では一般的な情報セキュリティマネジメントの考え方は変わっていない．

JIS Q 27001 は，一般財団法人日本情報経済社会推進協会（以下，JIPDEC）が推進する ISMS 適合性評価制度における ISMS 認証基準のベースとなっている．JIPDEC によると，認証企業数は増加しており，図 2 に示すとおり 2015 年 8 月 27 日時点で 4691 社が導入・維持している．

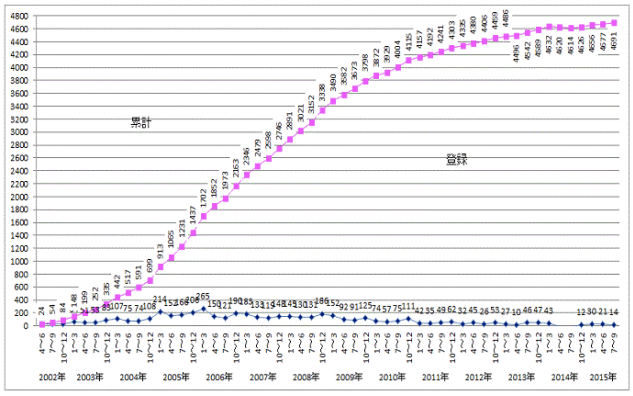

図 2　ISMS 認証取得組織数推移[5]

また，情報セキュリティマネジメントに関係するガイドラインとしては経済産業省が経営者，管理者を対象としたものが策定されている．経営者向けのものとしては「情報セキュリティガバナンス導入ガイダンス」があり，管理者向けとしては「情報セキュリティマネジメントシステムの国際標準（ISMS）（自社の情報セキュリティ対策の適正な改善メカニズム（PDCA サイクル）の構築)」がある．また，JIPDEC が公開するする ISMS のガイドラインもあり，いずれも ISO/IEC 27001 を補完する目的で作成されたものとなっている．

日本において，官民双方ともに情報セキュリティマネジメントとしては，ISO 等の国際規格に則ったトップダウンマネジメントの考え方で進められてきたことがわかる．

1.2 ボトムアップ手法の重要性

ISO/IEC 27001 では，情報セキュリティマネジメントを組織的に継続させる手法として，品質改善等でも使用されている PDCA サイクルを用いたトップダウンマネジメントが規定されている．一方，経済産業省のガイダンスでは，ボトムアップの重要性について以下のように述べられている．[6]

“全体としての統一感をもったセキュリティ対策のデザインを描くことは重要であるが，ボトムアップの対策レベルの改善もまた重要である．日本の企業では，現場における品質管理サークルを通じてさまざまな経営改善を行っている企業が多い．情報セキュリティ対策を現場での品質管理サークルを通じて改善していくという手法も考えられる．”

すなわち，日本の企業では日本的経営の特徴でもあるボトムアップ手法による情報セキュリティマネジメントが実践されてきており，このアプローチも重要であると考えられる．さらに，今後，現場で利用するあらゆる機器などがインターネットに繋がるようになる（IoT 対応）で現場の情報をリアルタイムで収集できるようになる．さらに，企業の製造・サービス提供等の元への情報機器の増加やクラウドの利用がますます進むと考えられる．すなわち，現場からの情報の収集や活用がより重要となり，ボトムアップ手法との親和性がよくなると考えられる．その結果，いままでのようなトップダウンによる一極集中で均質的なマネジメントだけではカバーしきれない．そこで，これらの部分を，現場の自主性に任せる形でボトムアップ的に補う必要が出てくると考えられる．

しかしながら，情報セキュリティマネジメントにおけるボトムアップ手法については，ISO/IEC 27001 の考え方として含まれていないものである．トップダウンマネジメントで作られた規程類を持つ会社において，情報セキュリティをボトムアップで実施すると，現場での裁量に委ねる部分が大きくなり，本来の規程類から外れた行為となる可能性が高くなると考えられる．

本論文では，日本の強みであるボトムアップによる改善を情報セキュリティの向上に応用するために，まず，ボトムアップを可能とする日本型経営の特徴的な要素を分析し，日本におけるマネジメントの特異性を観察した上で，情報セキュリティマネジメントにおけるボトムアップ手法の可能性について考察を行う．

Vol.2015-SPT-16 No.14
Vol.2015-EIP-70 No.14
2015/11/20

2. 先行研究調査

2.1 日本型経営と人本主義

日本型経営の特徴的な点については，伊丹による「日本型コーポレートガバナンス 」で分析がなされている．そのなかで，日本の経営と英米の経営を比較して，各々の特徴をまとめて「人本主義と資本主義」と定義されており，表 1 の特徴があげられている．

表 1　人本主義と資本主義[7]

	人本主義	資本主義
企業の概念	従業員主権	株主主権
シェアリングの概念	分散シェアリング	一元的シェアリング
市場の概念	組織的市場	自由市場

企業の概念として，英米では株主が会社の主権を持つとされるが，日本では従業員の会社への帰属意識が高く，時として敵対的買収などでは経営層と従業員が協力して反対運動を行ったりする特徴がある．

また，情報や決定権，責任等のシェアリングの概念としては，英米は一元的に集中させるが，日本は部門単位や部署単位での権限移譲が多く経営層や管理層は調整役の位置づけになっている．

市場の考え方としては，英米は純粋な自由市場であるが，日本は自由市場であるものの，時として関連企業と優先的に契約をすることがある．すなわち，長期的な信頼や関係を大切にする傾向があり，自由市場に共同体の原理が入ったものとして考察されている．

人本主義の持つメリットとしては，長期的な雇用が確保されることから，技術の蓄積やコミュニケーションによる情報効率の良さなどが挙げられている．

2.2 社長セキュリティと係長セキュリティ

人本主義の考え方を基に，日本における情報セキュリティの考え方を示した先行研究として，IPA の研究会報告書である「日本型経営と情報セキュリティ研究会」[8]が挙げられる．報告書では，人本主義によるボトムアップ型の日本的経営のなかで，トップダウンが不可欠である情報セキュリティ施策を，不適合を起こさずに埋め込む必要性について述べられている．

報告書には，ボトムアップとトップダウンの融合の重要さについて述べられており，そのための方策として「社長セキュリティと係長セキュリティ」[9]が提唱されている．現在の，日本企業における情報セキュリティ対策は，情報システム部門の現場に任せておけばよい（係長セキュリティ）というボトムアップの段階に留まっている．しかし，大規模な情報漏洩等のケースでは経営者が記者会見を行い謝罪することが増えてきている．そのため，情報セキュリティが経営上のリスクであることを経営者が強く認識するようになってきている．すなわち，情報セキュリティについてもトップダウンによる意思決定が重要になってきている．報告書にはボトムアップ型の企業文化を踏まえて，経営者が情報セキュリティに対してトップダウン型の対策を組み合わせてゆくこと（社長セキュリティ）が重要であると述べられている．

PDCA の観点で社長セキュリティと係長セキュリティを組み合わせる観点からは図 3 のようになる．情報セキュリティを担当する情報システム部門で行っていた仕事を，会社全体の仕事とするために経営層を巻き込んだ全社的な仕事に改める．さらには，社長を巻き込んで経営と情報セキュリティが密接に連携することを踏まえて，計画から改善までの一連のサイクルを回すことを示唆している．

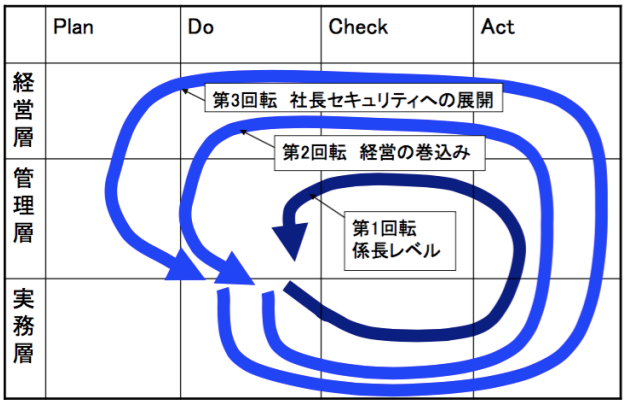

図 3　社長セキュリティと係長セキュリティ[9]

3. 日本において情報セキュリティマネジメントが機能しにくい原因の仮説

3.1 日本の PDCA の特徴

ここまで述べた日本の特異性は情報セキュリティマネジメントの手法である PDCA サイクルにおいても存在すると想定して，ISO/IEC 27001 で用いられているものをトップダウン型，日本企業が得意とする改善活動の PDCA をボトムアップ型と考えて，両者の違いを比較した．

トップダウン型 PDCA は，経営者の計画(P)を従業員に実行(D)させ，成果を監査(C)し，不備があれば改善(A)させるものである．これを図 4 に示す．一貫して，PDCA サイクルを回す主体である経営層は仕事を行わずに，管理することに徹しているものである．このトップダウン型 PDCA は本来の定義通りのマネジメント手法であると言える．

Vol.2015-SPT-16 No.14
Vol.2015-EIP-70 No.14
2015/11/20

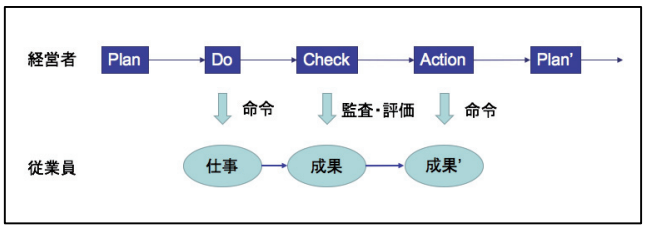

図 4　トップダウン型 PDCA

一方，日本の多くの企業の現場では，マネジメント自体を中間管理職や従業員に権限委譲している．これを筆者らは，ボトムアップ型 PDCA と呼ぶ．これを図 5 に示す．図 5 では経営者の方針を受けた中間管理職や従業員が，自身で計画(P)を立て，実行(D)してみて成果を確認(C)し，不備があれば自発的に改善(A)を行うもので，経営者は定期的に進捗の報告を受け，良い取り組みがあれば他部署に水平展開を行う手法である．ボトムアップ型 PDCA では，PDCA サイクルを回す主体と，仕事の主体が一体となっており，マネジメント手法というよりもワークフローとしての意味合いが強いものである．

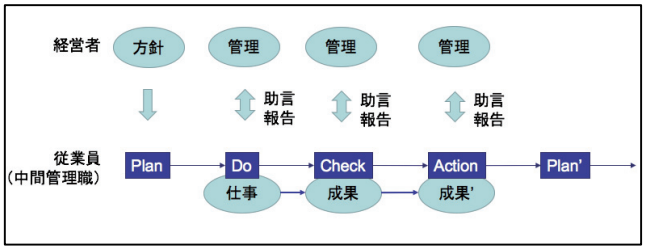

図 5　ボトムアップ型 PDCA

日本における実例を考えてみると，トップダウン型 PDCA は ISO/IEC のマネジメント手法で使われるだけでなく，官公庁が行う施策のマネジメント等でも見ることができる．一方で，ボトムアップ型 PDCA は，QC サークルの七つ道具として運用に用いられている．また，web 検索で「新入社員研修等 PDCA」といったキーワードで検索すると，社員が仕事を進めるための研修やセミナー等を多く見ることができ，多くの企業や組織において，仕事を効率的にマネジメントするための手法として使われていることが分かる．

トップダウン型 PDCA とボトムアップ型 PDCA の特徴をまとめると表 2 のように比較することができると考えられる．

表 2　2 つの PDCA の特徴

	トップダウン型 PDCA	ボトムアップ型 PDCA
主体	経営者・管理者	中間管理職・従業員
対象	従業員	自分自身
条件	経営者が業務全般を細かく管理していること	従業員が全体のプロセスを見渡せること
目的	経営者が品質のマネジメントをするためのもの	従業員が自分自身の仕事をマネジメントするためのもの
特徴	C は，計画通りに実行されたかを監査する A は，足りない部分を補う意味が強い	C は，セルフチェック A は，TQC 的な改善活動を意味する

3.2 PDCA の発展経緯

PDCA について，まず，トップダウン型，ボトムアップ型の由来について検討した．まず，PDCA についての歴史的な経緯を分析した Moen による調査結果 を図 6 に示す．図 6 より分かることは，科学的手法（科学的検証）から始まった仮説検証型のプロセスは，プラグマティズムという実際の経験から真理を導く実用主義に発展し，工業的な応用として計画・生産・検査のサイクルでシェハートサイクルや，今日の PDCA の原型であるデミングサイクルに発展していった．また，1960 年代に日本にデミングサイクルが取り入れられた後に，日本においては QC サークルとしての PDCA サイクルに発展していったことが述べられている．

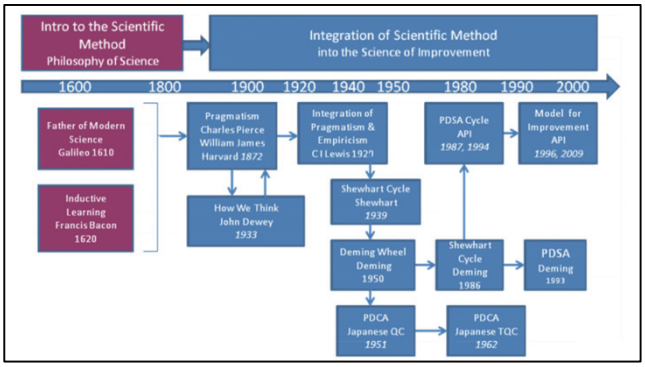

図 6　Evolution of the PDCA cycle[10]

以上により，同じ経営の管理手法として生まれた PDCA サイクルの概念ではあるが，人本主義と資本主義と呼ばれる労働環境の違いがその後の発展に影響し，仮定としておいたトップダウン型 PDCA と日本型（QC による）PDCA に分離していったことが分かる．この日本型 PDCA の本質は，提案しているボトムアップ型 PDCA と同じである．

3.3 情報セキュリティマネジメントが日本で機能しにくい理由

これまで見てきた PDCA サイクルの特徴を基に，日本において情報セキュリティマネジメントが上手くいかない会社の特徴を考察すると，会社の社風が日本型経営でボトム

Vol.2015-SPT-16 No.14
Vol.2015-EIP-70 No.14
2015/11/20

アップ型であるのにも関わらず，情報セキュリティマネジメントのみトップダウン型 PDCA でマネジメントしようとしていることで歪みが生じ，結果として規程類はあるものの，現場の裁量に委ねられた部分が多いことが原因ではないかと推測される．

また，他の理由として，ボトムアップ手法で取り組もうとしたが現場での人材不足により実施出来なかったとも考えられる．図 7 は 2 章で取り上げた「社長セキュリティと係長セキュリティ」を企業の組織体制に合わせて図示したものである．当初，セキュリティ技術に長けた担当者が在籍する情報システム部門内だけでセキュリティを取り扱う係長セキュリティに留まる状況であったが，近年の重大なセキュリティ事件により経営者を含めて情報セキュリティの重要性が社会的に認知されるようになり，「社長セキュリティと係長セキュリティ」が提唱された 2010 年と比べて，社長セキュリティに近づいている状況であると考えられる．しかしながら，実際に情報システムを利用するユーザ部門については，情報システム部門が支援を行うのみで，ボトムアップ的にユーザ部門が情報セキュリティ対策に取り組むことは無いものと推測される．

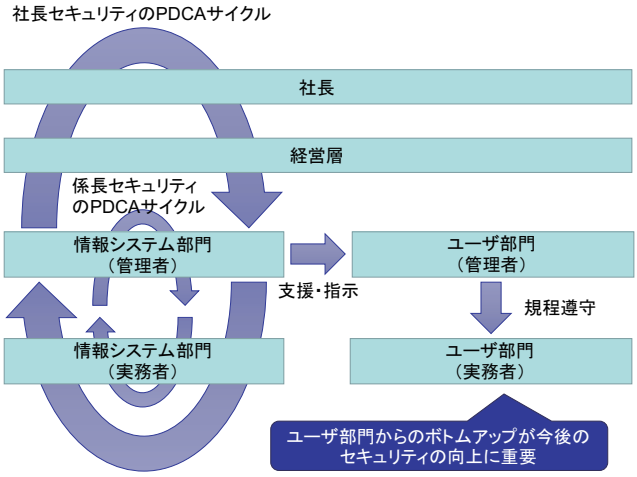

図 7　企業における情報セキュリティ体制

上記で述べたユーザ部門が主体的にセキュリティに取り組めないことの理由は，社会的には人材不足という形で現れている．図 8 に示す経済産業省が検討した「セキュリティ人材の確保に関する研究会」報告書［11］によると，ユーザ企業において事業部門（ユーザ部門）と情報システム部門の間で調整を行う矢印 B と C の人材が不足しており，試験制度の新設により，まず B ができる人材を拡大してゆく方針が打ち出されている．

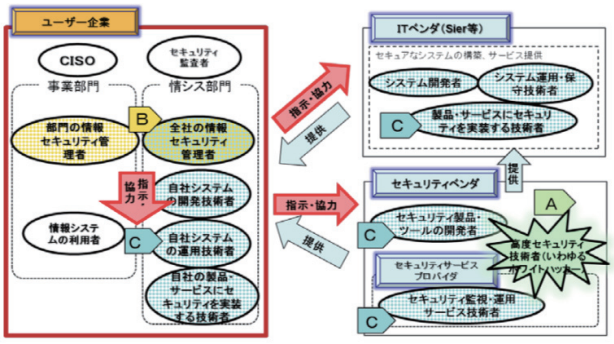

図 8　必要となる情報セキュリティ人材像[11]

ボトムアップ型 PDCA においては，表 2 の条件で示した通り従業員が全体のプロセスを見渡すことが必要となるため，実務において情報セキュリティ全般を見渡せる人材が不足している状況ではボトムアップ型 PDCA で進めることが困難であると考えられる．

4. ボトムアップによるマネジメントの事例

4.1 他規格でのボトムアップによるマネジメント

3 章までで述べたように，情報セキュリティマネジメントについて，ISO/IEC 27001 はトップダウンで進める必要があるが，日本型経営においてはボトムアップ型 PDCA で業務が進められることから，上手く機能しないと考えられる．

一方で，ISO 規格の多くはトップダウン型 PDCA サイクルを取り入れたトップダウンマネジメントで構成されており，ISO9001 の品質マネジメントにおいても同様にトップダウンでのマネジメントが記述されている．日本においては図 6 で示した日本型 QC（品質管理）に代表されるボトムアップ型 PDCA による改善活動で成果が得られている状況である．

同じ日本型経営の環境において，品質マネジメントでボトムアップ手法が成果を上げることができるにも関わらず，情報セキュリティマネジメントでボトムアップ手法が十分に取り入れられていないのには何らかの要因があると考えられる．

4.1.1 医療業界での海外への TQM 導入事例

具体的な要因の調査として，医療業界における品質向上の施策の一環で独立行政法人 国際協力機構 国際協力総合研修所により報告された医療分野における海外への TQM（総合的品質管理）の導入事例について取り上げる[12]．

病院のマネジメントスタイルは，日本においても欧米型企業に近い構造になっている．病院の経営層と従業員である医師は完全に職務が分離されていることや，医師個人の能力主義の傾向が強くあることにより，マネジメントのスタイルとしてはトップダウンによるマネジメントが取られ

ていることが多い．ところが，1990 年代に入り，重大な医療事故等により医療の質の向上が求められるようになり，日本の産業界で成功を収めていた TQM を活用して医療品質の向上が求められるようになった．国内で TMQ により一定の成功が得られたことから，その後，海外へも医療分野における TQM が展開され，国際協力機構の元で支援等が行われてきた．

4.1.2 医療分野での TQM の成功要因

こうした医療分野での成功要因を分析することで，同じくトップダウンによるマネジメントが求められる情報セキュリティ分野においてボトムアップによるマネジメントを導入するために必要となる要因について考察した．

報告書では，日本と海外における医療分野での TQM を導入した事例について現地の環境状況や要因分析がなされている．表 3 に各国での成功事例について抜粋してまとめた．

表 3　海外展開時の成功要因（抜粋）[12]

	成功要因
日本	リーダーシップ 臨床目標と経営目標の融合
タイ	リーダーシップ プロセス・マネジメント ピアレビュー 失敗からの学び
スリランカ	リーダーシップ システム・アプローチ 自己完結型
フィリピン	リーダーシップ 海外からの支援 品質管理の受容性
バングラディッシュ	（未発現）
ザンビア	トップのコミットメント みじかな問題への取り組み

各国とも労働環境や仕事に対する考え方，社会の成熟度など様々であるが，共通的な成功要因として以下の 4 点がまとめられている．

- リーダーシップ
- プロセス・マネジメント
- システム・アプローチ
- ピアレビュー

4.1.3 情報セキュリティにおけるボトムアップによるマネジメントに必要な要因

ここで，日本における情報セキュリティについて考察すると，既に TQM を実施した経験のある企業においては，ボトムアップ型 PDCA を導くことができる組織作りができていると考えられる．ボトムアップ型 PDCA を進める上で，目標の管理ではなくプロセス・マネジメントの考え方に基づいてすすめることや，能力主義でなくシステム・アプローチの戦略をとり相互に検証し合うピアレビューで改善してゆくことは理解されている．

唯一，不足している要因は，強いリーダーシップを発揮することができる人材である．これは，第 3 章で述べた不足している情報セキュリティ人材のマネージャー層のことを指す人材である．情報セキュリティについての知識を持ちながら，実務としての課題を解決してゆくことができる現場でのリーダーが必要な要因であると考えられる．

4.2 ボトムアップによるマネジメントの必要性

4.2.1 ファーストサーバ事件

日本においてボトムアップ型 PDCA による情報セキュリティ対策が有効であると述べてきたが，一方で，情報システムに関連した業務では，現場のノウハウや創意工夫に強く依存した運用がなされている状況もある．ボトムアップ型 PDCA の観点でみれば有意義な従業員の行動であっても，正しくマネジメントされなければ逆に問題となるケースも考えられる．

2012 年に発生したファーストサーバ株式会社におけるデータ消失障害[13]は，システム変更の際に担当者が独自方式の更新プログラムを実行したことにより顧客のデータを誤って削除してしまった事件である．作業マニュアルはあるにもかかわらず、10 年以上にわたって担当者の独自方式で運用されており上長もその運用を容認している状況であった．

情報システムに限らず情報セキュリティにおいても，優秀な技術者であればあるほど使いやすいツールや手法を独自に生み出す傾向があり，ボトムアップ的な改善として独自な行動をよかれと考えてとることが多い．しかしながら，正しいマネジメントがなければ，システム・アプローチや水平展開に繋がらず，局所的なものとなり，事故などの場合には，逆に問題を起こしてしまう危険性がある．このような事例に対応するには，トップダウンによる画一的な運用では限界があり，ボトムアップによる改善を受け止めて，個別事象に対応できる優秀なマネージャー層の人材が必要になると考えられる．

このような人材は，野中らが提唱した「ミドル・アップダウン・マネジメント」[14]におけるミドル・マネジャーに相当する人材である．トップの方針や考え方を適切に解釈しつつ、ボトムアップで得られた情報セキュリティに対する暗黙知を，組織全体の知識として蓄積してゆくことができる人材が必要であると言える．

5. おわりに

近年のセキュリティインシデントの増加により，企業に

おける情報セキュリティ対策についても，セキュリティ専門組織の構築や ISMS 導入，インシデントレスポンスチームの導入等の組織的な動きが多く見られるようになってきている．しかしながら，現場目線でのボトムアップによる情報セキュリティ対策のあり方については，まだ各企業において手探り状態であり，具体的にどうすれば良いかについて分かっていない．

本論文では，日本的経営の考え方を基に，ISMS 等のトップダウンによる情報セキュリティ対策だけでなく，ボトムアップ型 PDCA も重要であると述べた．そして，既に QC サークル等の改善活動等で培われた組織体制を活用してより良い情報セキュリティ対策を行うためには、情報セキュリティに対して適切にリーダーシップを発揮できるマネージャー層の拡大が重要であると結論付けた．

既に日本企業の中には，従業員自身が情報セキュリティ対策を積極的に取り組むことができるように教育等を開始している企業もある．より具体的なボトムアップ事例の調査については今後の研究課題としたい．

日本企業が得意とする組織の運営方法を生かして，より質の高い情報セキュリティ対策を各企業がおこなえるようになることを期待するものである．

謝辞

本論文の執筆にあたり，ご指導頂いた情報セキュリティ大学院大学の教授陣，また多くの助言を頂いた原田研究室の客員研究員及びメンバーに対して感謝の意を表します．

参考文献

1) 独立行政法人 情報処理推進機構, 2014 年度の情報セキュリティの概況，情報セキュリティ白書 2015 電子書籍版，序章-1.1 章 (2015)
2) 中尾康二・山﨑哲・山下真・日本情報経済社会推進協会, ISO/IEC 27001:2013(JIS Q 27001:2014）情報セキュリティマネジメントシステム要求事項の解説，日本規格協会（2014）
3) 独立行政法人情報処理推進機構，情報セキュリティマネジメントの規格や標準，情報セキュリティマネジメントと PDCA サイクル (https://www.ipa.go.jp/security/manager/protect/pdca/standard.html), 2015 年 9 月 22 日参照
4) 原田要之助，情報セキュリティマネジメント規格の改訂と問題点について，情報処理学会研究報告 IPSJ EIP Technical Report, pp.2-3 (2013)
5) 一般財団法人 日本情報経済社会推進協会, ISMS 認証取得組織数推移， http://www.isms.jipdec.or.jp/lst/ind/suii.html (2015 年 9 月 22 日参照)
6) 経済産業省情報セキュリティ政策室，情報セキュリティガバナンス導入ガイダンス, ,情報セキュリティガバナンス –情報化社会を勝ち抜く企業の経営戦略-, p.26 (2009)
7) 伊丹敬之，日本企業の人本主義システム，日本型コーポレートガバナンス, pp.59-80 (2000)
8) 独立行政法人 情報処理推進機構，日本型経営と情報セキュリティ, http://www.ipa.go.jp/files/000027858.pdf (2013)
9) 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)
10) Moen, Ronald, and Clifford Norman. "Evolution of the PDCA cycle.", www.westga.edu/~dturner/PDCA.pdf, pp.2-7 (2006)
11) 経済産業省，セキュリティ人材の確保に関する研究会 中間報告，産業構造審議会 商務流通情報分科会 情報経済小委員会（第 6 回）配布資料 , pp.11-12 (2015)
12) 長谷川敏彦，保健医療セクターにおける「総合的品質管理（TQM）手法」による組織強化の研究，独立行政法人 国際協力機構 国際協力総合研修所, pp.80-81 (2006)
13) ファーストサーバ株式会社 第三者調査委員会，調査報告書<最終報告書>要約版，ファーストサーバ株式会社, pp.4-8 (2012)
14) 野中郁次郎，第５章 知識創造のためのマネジメント・プロセス，知的創造企業<電子書籍版>，第 5 章 1-2 (1996)