Vol.2019-EIP-83 No.7
2019/2/15

組織のセキュリティ文化形成−手法についての一考察−

岡嶋 裕希† 原田 要之助†

概要：近年世界中で繰り返し行われるサイバー攻撃によって情報セキュリティに対する関心が高まっており，企業は脅威への対策を行うことを余儀なくされている．経営層，情報システム部門等，ITリテラシーの高い人々は自組織のセキュリティ対策に関心を持ち，対応策を導入しようという動きがあるが，情報セキュリティ対策の性質上，どうしても利便性とのトレードオフになり業務効率が落ちる等，未だに導入に反対する声もある．その結果今日では情報流出に関する事件のうち，内部不正犯罪が取り上げられてきている．内部不正は職務上与えられた権限を使い行われるため，その対策はもはやシステムだけでは防ぐことは出来ないと言える．
そこで本論文ではこれらを防ぐために，情報セキュリティに関心を持つ組織文化がどのように形成され，またどのように効果的に醸成できるかについて検討する．

キーワード：セキュリティ文化，内部不正，情報セキュリティ教育・意識

A Study of Method -Security Culture Building of Organization-

Yuki Okajima† Yonosuke Harada†

In recent years, companies are forced to take measures against repeated cyber-attacks all over the world due to increased concern with information security. Management, information system department, and IT-literate employee have an interest of security measures and implementation of those. Alternatively, there are even now opposing opinion to introduce those owing to trade-off between security and business efficiency. As a result, nowadays, malicious insider attract rising attention within information leakage incidents. Malicious insider has official authority, and does wrong readily, therefore only measures by system are inadequate.
In this paper, we discuss how to build and foster security culture of organization.

Keywords: Security Culture, Insider criminal, Information Security Education/Awareness Training

1. はじめに

今日世界中で繰り返し行われるサイバー攻撃によってセキュリティに対する関心が高まっており，企業は脅威への対策を行うことを余儀なくされている．経営層，情報システム部門等，ITリテラシーの高い人々は自組織のセキュリティ対策に関心を持ち，対応策を導入しようという動きがあるが，それ以外の人々は自身の業務対応でセキュリティに関心を持つ余裕がなかったり，セキュリティ対策の性質上，どうしても利便性とのトレードオフになり業務効率が落ちる等，未だに導入に反対する声もある．自組織へのセキュリティ意識を定着させるために，教育，研修等のプログラムを導入するが，そもそも意識が低い人々にとっては消極的な作業となってしまい，施策が優れたものであっても，その効果は低くなってしまうと思われる．その結果近年では情報流出に関する事件のうち内部不正犯罪が取り上げられてきている．さらに外部からの攻撃と違い，内部不正は職務上与えられた権限を使い行われる[1]ため，その対策はもはやシステムだけでは防ぐことは出来ないと言える．

そこで本論文ではこれらを防ぐために，セキュリティに関心を持つ組織文化がどのように形成され，また効果的に醸成していくかについて着目する．第2章では内部不正について，第3章では組織文化について，第4章では先行研究について，第5章ではまとめと今後の研究予定について述べる．

2. 内部不正について

2.1 定義

この章では悪のベクトルに文化が形成された結果引き起こされる内部不正について定義する．組織における内部不正防止ガイドライン（日本語版） 第 4 版ガイドライン[2]では「内部者」と「内部不正」について次のように定義している．

(1) **内部者**

役員，従業員(契約社員を含む)及び派遣社員等の従業員に準ずる者(以下，総称して「役職員」という．)又は，役職員であった者のうち，以下の 2 つのどちらかでも満たした者とする．

† 情報セキュリティ大学院大学 情報セキュリティ研究科
Graduate School of Information Security, Institute of Information Security

1. 組織の情報システムや情報(ネットワーク，システム，データ)に対して直接又はネットワークを介したアクセス権限を有する者
2. 物理的にアクセスしうる職務についている者(清掃員や警備員等を除く)

(2) 内部不正

違法行為だけでなく，情報セキュリティに関する内部規程違反等の違法とまではいえない不正行為も内部不正に含める．内部不正の行為としては，重要情報や情報システム等の情報資産の窃取，持ち出し，漏えい，消去・破壊等を対象とする．また，内部者が退職後に在職中に得ていた情報を漏えいする行為等についても，内部不正として取り扱う．

内部規定違反等の違法とまでいえない不正行為も内部不正に繋がる脅威とし，本論文も組織における内部不正防止ガイドライン[2]に沿って内部不正を定義する．

2.2 内部不正の実態

では内部不正は一体どのような性質を持つのか．内部不正による情報セキュリティインシデント実態調査−調査報告書−[3]，2017 Cost of Cyber Crime Study[4]から3のポイントを引用する．

2.3 内部不正の行為理由

情報セキュリティインシデント実態調査−調査報告書−[3]に依ると，民間企業の従業員と内部不正を行った経験を有する者(以下，内部不正経験者とする)に行為の理由を聞いた結果，58.0%は故意が認められない"うっかり"によるものであり，一方42.0%は故意によるものであった．以下それぞれの詳細理由を引用する．

故意が認められない理由

- ルールを知っていたが，うっかり違反した
- ルールを知らずに違反した

故意による理由

- 業務が忙しく，終わらせるために持ち出す必要があった
- 処遇や待遇に不満があった
- ルールはあったが，ルール違反を繰り返している人がいたので，自分もやった
- 持ち出した情報や機材で転職や起業を有利にしたかった
- 企業・組織や上司などに恨みがあった
- 持ち出した情報や機材を換金したかった

故意が認められない理由については，情報セキュリティ教育の徹底によるルール遵守の意識向上，ルールの周知により，ある程度は改善出来ると思われる．

一方故意による理由のうち，「業務が忙しく，終わらせるために持ち出す必要があった」については，持ち出す必要があった理由の一つに近年推奨されている時間外労働時間の削減と，本人の業務量のアンマッチが考えられる．この場合，不正として取り上げられた本人だけでなく，組織的に行われている可能性が高いと考えられる．「ルールはあったが，ルール違反を繰り返している人がいたので，自分もやった」についても同様に組織的に行われている可能性が高いと言える．これらは健全な組織文化の醸成により改善出来る理由ではないかと思われる．

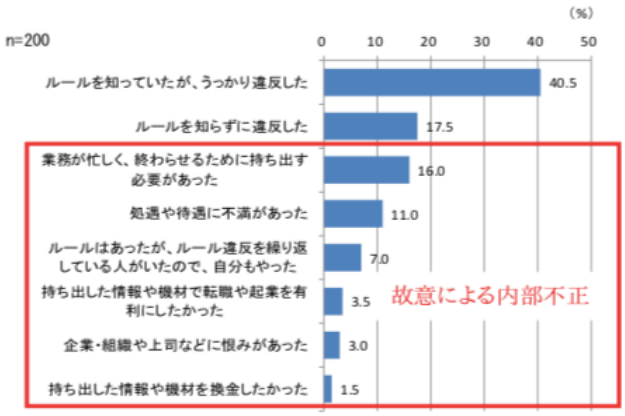

図 1 内部不正を行った理由(内部不正経験者)

2.4 内部不正経験者の属性

情報セキュリティインシデント実態調査−調査報告書−[3]に依ると，内部不正経験者の職務を尋ねた結果，51.0%がシステム管理者(兼務を含む)だった．防止策としては権限の最小化・分散，および作業監視等の対策が有効としている．

半分がシステム管理者という属性上，システム的な対策だけでは不十分であると考えられ，この問題も組織文化の改善により件数を抑えられる可能性がある．

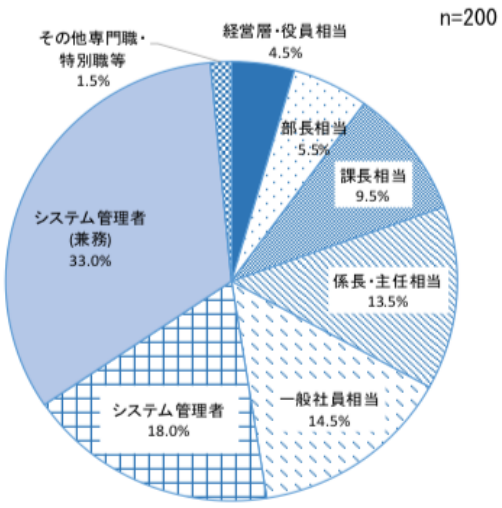

図 2 内部不正経験者の内訳(職務)

2.5 内部不正に依る経済的損失

Ponemon Institute, LLC & Accenture の「2017 Cost of Cyber Crime Study」[4]では，次の 9 つの種類のサイバー犯罪を調査している．

- Web-based attacks
- Denial of services
- Malicious insiders
- Malicious code
- Phishing & social engineering
- Malware
- Viruses, Worms, Trojans
- Stolen devices
- Botnets

その中でも内部不正に当たる Malicious insiders に着目したい．

2016 年は計 465 件のサイバー攻撃を経験した 237 組織に対して調査しており，内部不正の件数は二番目に低い 41%だった．一方年間の平均被害額は，約 16.7 万ドルと最も高かった．

2017 年は計 635 件のサイバー攻撃を経験した 254 組織に対して調査しており，内部不正の件数は二番目に低い 40%だった．一方年間の平均被害額は，約 17.3 万ドルと最も高かった．

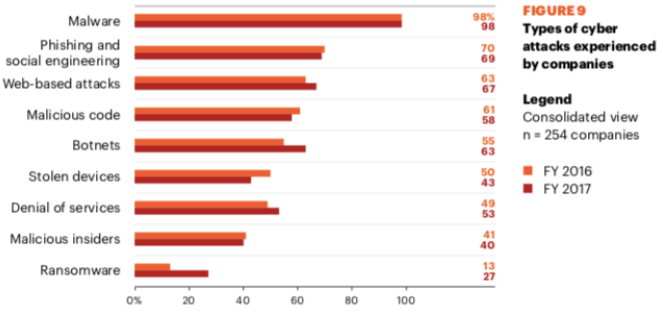

図 3 Types of cyber attacks experienced by companies 2016/2017

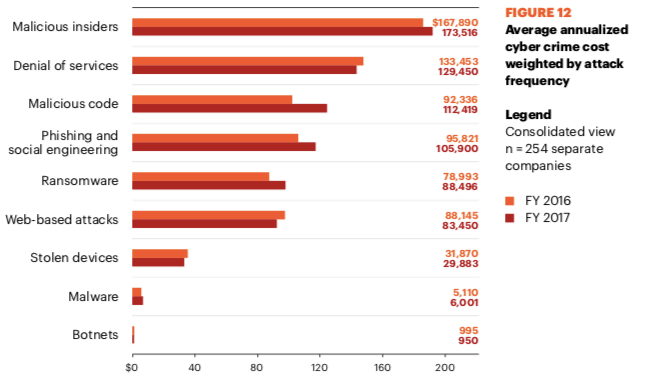

図 4 Average annualized cyber crime cost weighted by attack frequency 2016/2017

これらの結果から，内部犯罪は全体のサイバー攻撃の中で発生する割合は小さいが，発生した場合の経済的損失は大きく，少しでも内部犯罪の件数を減らすことが経済的被害を減らす大きな要因になると考える．不正者が組織内の者なので，外部からの攻撃と比べ，効率よく大量の情報を取得しやすいからだと考えられる．この問題についても健全な組織文化の醸成が役に立つのではないかと考える．

3. 組織文化について

そもそも組織文化とは，その意味が人に依り曖昧であるため，本章にて定義する．

シャインは，「組織文化とリーダーシップ」[5]の中で，組織文化について以下のように述べている．

文化とはグループが外部への適応，さらに内部の統合化の問題に取り組む過程で，グループによって学習された，共有される基本的な前提認識のパターンである．このパターンはそれまで基本的に効果的に機能してきたので適切なものと評価され，その結果新しいメンバーに対し，これらの問題に接して，認識し，思考し，感じ取る際の適切な方法として教えられる．[5]

またシャインは，「組織文化とリーダーシップ」[5]に加え，「企業文化 ダイバーシティと文化の仕組み」[6]の中で3つのレベルに分けて分析することが可能と述べている．

1.人工の産物(Artifact)

最も表層に現れ，容易に観察出来るレベルである．歩き回りながら目にし，耳にし，感じることができるものである．グループが生み出す産物，物理的環境としての建造物，その言語，テクノロジーと製品，その美術的作品，そのスタイル，組織について語り継がれた神話や物語，価値観について書き物として残された文書，目に見える慣習やお祝いの行事，風土，また組織図といった構造的な側面も含まれる．このレベルでは，文化は非常に明確で，直接感情に訴える．[5][6]

2.信奉された信条と価値観(Espoused Belief and Values)

中層のレベルであり，その組織の方針，倫理観，ビジョンなどである．共有される価値観または信条として，最終的には共有される前提認識として定着する．グループの問題の解決に常に貢献した信条と価値観のみが基本的原則に転換される．[5][6]

3.基本的な深いところに保たれている前提認識(Assumption)

深層部分に現れるレベルであり，メンバー全員によって当たり前のものとして受けとめられている．集団で学習した価値観や信念であり，このやり方ならばうまくいくということが，認められ，譲れないものになったものである．組織が成功し続けることで，さらに共有され認められ，それが基本的な前提認識へと昇華する．この過程で創られた信念，価値観は，最終的には「正しい」に違いないと考えられる存在になる．[5][6]

図 5 はこれら 3 つのレベルの考え方を元に，筆者が作図したものである．

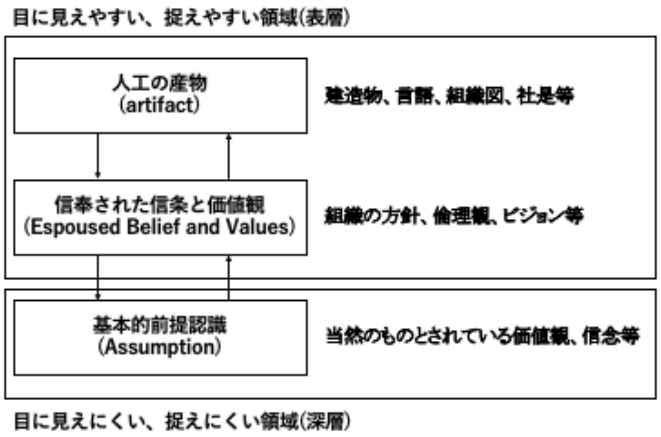

図 5 組織文化三層分解レベル[5]に加筆修正

組織が学習した方法，文化がセキュリティの観点から見て間違ったものとして形成され，共有された基本的な前提認識となる時，不正行為の実行を可能，または容易にする環境[7]もまた形成されてしまう問題が生じる．これは内部不正の発生に繋がる一つの要因になると考えられる．

4. 先行研究

山本[8]は今日の日本における情報セキュリティ事件・事故，及びその対策の状況について，地方自治体における内部監査報告を通じて傾向を把握した結果，技術的側面よりも，その組織に所属する「人」がどのように行動するのか，といった側面が情報セキュリティ対策においては重要であるとした．そして「人」の行動はどのように決定されるのかを探った結果，見える形で計測可能である組織的な取り組みといった側面と組織文化・風土，逸脱行動論，組織性逸脱行為過程に示された側面から検証することが妥当であるとした．

山本は情報セキュリティ逸脱行為を，組織文化・風土との関係についてE.H.Scheinの文化レベルにあてはめて考えている．「情報セキュリティ逸脱行為」は「目に見える組織構造・プロセス（レベル1）」（本論文でいう人工の産物にあたる）に相当し，このレベル1の行動がなぜ発生するのかを調査することで，組織にとって常識となっている事柄であるレベル3に相当する組織風土・文化（本論文でいう基本的前提認識）をWebアンケートにて調査している．

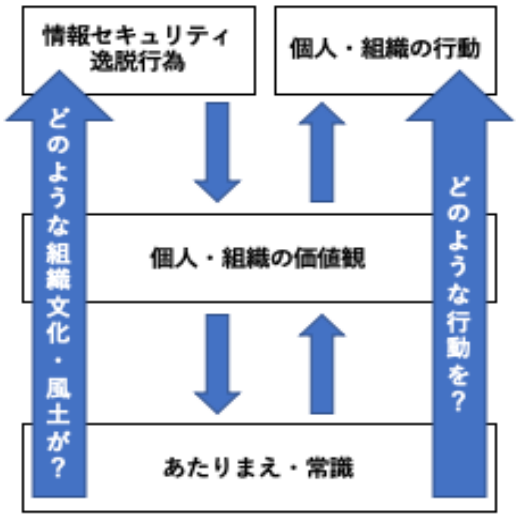

図 6 逸脱行動の仮説イメージ[8]

山本は，アンケート調査結果を，「組織における行動」と「逸脱行動論と組織文化・風土」の 2 つの視点から仮説の検証と相関分析をし，共分散構造分析ソフトにてモデル図を作成している．前者は実際に組織内で行われている組織の行動および個人の行動と情報セキュリティに対する逸脱行動の関係性を分析したものであり，後者は逸脱行動論を中心とした理論と情報セキュリティに対する逸脱行動の関係性を分析したものとしている．

山本は 2 つのモデル図が示唆していることを次のように述べている．

「経営者は情報セキュリティに対する理解を深め，組織的な活動を促進するとともに逸脱行為等につながるネガティブな組織文化・風土を排除すること，現場における責任者が情報セキュリティに対して理解し，業務都合の言葉を言い訳に逸脱行為を許容しないこと，の2点ではないかと考えている．具体的には情報セキュリティに対して目に見える形で行われる組織的な取り組みである「情報セキュリティの教育」，「セキュリティコミュニケーションの活性化」等を行い，促進していくことが，組織全体が「情報セキュリティ」に対して関心を持つ文化を醸成する土台作りとなると考えている．この経営者が出発点となる活動を行うことでその組織内では情報セキュリティに対する価値観が確立していくと考えられ，結果として情報セキュリティを意識した行動となるとともに，情報セキュリティを意識することが常識化していくと考えられる．」[8]

図 7 は山本がこの状態遷移を情報セキュリティ向上にむけてモデル化したものである．

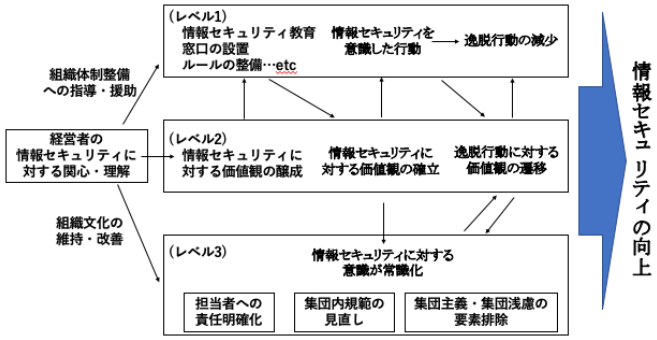

図 7 情報セキュリティ向上に向けたモデル[8]

山本は経営者目線から，情報セキュリティ文化醸成のためには「情報セキュリティ教育」，「セキュリティコミュニケーションの活性化」を挙げているが，現場に取り入れる際の具体的な手法については検討していない．手法について調査することで，セキュリティ文化形成をより現実的なものに出来ると考える．

また，持田[9]は国際原子力機関（IAEA）が提唱する安全文化の概念（INSAG―4）と銀行業界との共有性について，どのように銀行業界に応用していくかを研究している．IAEA 安全文化が提唱する「目に見えない特性を見える化する」ことを，銀行組織の全ての層における組織構成員に浸透させて，共通認識する文化的要素を取り入れる必要があり，そのために，「全ての個人がセキュリティを最優先するという意識を持つ」という安全文化の概念の中にある「個人の尊重」を適用し，スタッフ，管理者，経営層のそれぞれのサブカルチャーを理解し，それぞれの層における個人の目的意識や捉え方に沿って，「セキュリティ文化として組織体の中に持つ」という共通認識を浸透させることが必要である，としている．それぞれのサブカルチャー毎の考え方，それに合わせたセキュリティ文化のモデルを提唱出来れば，更に実用性を帯びたものになると思われる．

原子力機関をはじめ，航空管制，化学プラント，救急医療等の高信頼性組織は，失敗しないように徹底して対策する意識と，常に現状を見直す心構えが一般の組織と比べて高く，組織文化という側面を重視していると考えられる．高信頼性組織での教育，またそれらの業界の規律から，情報セキュリティ教育に活かせるものがあるか調査出来るのではないかと考える．

また近藤[10]は企業の組織変革の方法について研究しており，経営学者である加護野や Kotter らの考え方を元に，組織変革を成功させるための要因として，①新しく定着させたい組織文化を明示すること，②力を持ったチームをつくり新しい文化を組織全体に広めること，③変わりかけた行動さらには考え方を後戻りさせないように変革を徹底すること，の 3 つが必要になると述べている．また組織変革のプロセスを最初に提唱した心理学者である Lewin の考え方である①解凍，②変化，③再凍結を，組織変革の成功要因と組み合わせて図8のように解釈している．

段階	組織変革を成功させる要因
解凍	新しく定着させたい文化を明示する。
	力のあるチームをつくる。
変化	力のあるチームを中心に新しい文化を組織全体に広める。
再凍結	変革を徹底する。

図 8 組織変革の成功要因とプロセス [10]

組織に新しい文化を取り入れるのは容易ではなく，既存の組織文化を守ろうとする組員から抵抗が生まれると考えられる．情報セキュリティの組織文化を形成する際に手法だけを導入しても，実質的な効果が得られず作業になる可能性がある．手法の取り入れ方や，効果が得られる環境についても調査する必要があると考える．

5. まとめと今後の予定

本論文では健全な組織文化の醸成が，内部不正の発生を防ぐ効果があるのではないかという仮説のもと，2章では組織文化について，E.H.Schein の考え方をもとに文化を3層に定義した．3章では内部不正について定義し，実際の調査報告書やレポートから，内部不正の実態，属性，被害影響の大きさについて述べた．4章では先行研究から，組織文化・風土と情報セキュリティ逸脱行為について，サブカルチャー毎に分けて文化を考える必要性について，組織変革の方法について紹介した．

その結果として，内部不正や逸脱行為は，E.H.Schein の組織文化モデルにあてはめて説明することができ，情報セキュリティの向上には，情報セキュリティ教育を通じて情報セキュリティの組織文化を醸成していくことが重要である．経営者は E.H.Schein のモデルにしたがって，3階層の領域を確立することが望ましい．さらに，情報セキュリティを組織文化として根付かせるためにはサブカルチャー毎の考え方，それに合わせたセキュリティ文化に昇華させることが必要である．

ただし，組織文化の導入と構築までは E.H.Schein の考え方でよいが，これを定着させてさらに発展させ，もとに戻らないようにすることが必要となる．Pasquale Gagliardi は，深層にある基本前提レベルで文化が実際に変化するのは新しい価値を漸進的に追加することを通じてのみ可能であり，また革命的変化は既存の文化をどこかへ追いやってしまい，見せかけの変化は実際には起こっていないにも関わらず，起こっているように騙して勘違いさせると警告している [11] ．すなわち，リバウンドしないように継続して組織に変革を進めさせることが必要となる．

今後は高信頼性組織での教育、業界の規律や組織文化から，「情報セキュリティ教育」「セキュリティコミュケーション」に関連する、現場に取り入れる際の具体的な手法について、またその効果が最大限得られるような手法の取り入れ方や，環境について調査していく．これら以外にも様々な組織論を比較検討，特徴を把握し，より多くの視点から情報セキュリティとの関連性を調査していきたい．また内部不正者の心理面について心理

学からアプローチすることによって，逸脱行動をする兆候を見つけ，組織的にそれを事前に防ぐ方法として，セキュリティ教育，危機意識の持たせ方等を調査していく．

参考文献

[1]. IPA:「内部不正による情報セキュリティインシデント実態調査」報告書について，2014 年 https://www.ipa.go.jp/security/fy27/reports/insider/（アクセス, 2018 年 10 月 8 日）
[2]. IPA:組織における内部不正防止ガイドライン（日本語版）第 4 版ガイドライン，2016 年 https://www.ipa.go.jp/files/000057060.pdf（（アクセス, 2018 年 10 月 8 日）
[3]. IPA:内部不正による情報セキュリティインシデント実態調査 -調査報告書-, 2015 年 https://www.ipa.go.jp/files/000051140.pdf（アクセス, 2018 年 10 月 8 日）
[4]. Ponemon Institute, LLC & Accenture :2017 Cost of Cyber Crime Study，2017 https://www.accenture.com/t20171006T095146Z__w__/us-en/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf#zoom=50>（アクセス, 2018 年 10 月 10 日）
[5]. エドガー・H・シャイン:組織文化とリーダーシップ，白桃書房，2012 年
[6]. エドガー・H・シャイン:企業文化 ダイバーシティと文化の仕組み，白桃書房，2016 年
[7]. IPA:組織における内部不正とその対策，2016 年 https://www.ipa.go.jp/files/000059582.pdf（アクセス, 2019 年 10 月 16 日）
[8]. 山本哲寛:日本の組織における組織文化・風土と情報セキュリティ逸脱行為の関係に関する一考察，2010 年
[9]. 持田恭子:安全文化の概念を銀行組織に適用するための考察 -情報セキュリティ管理システムの強化に向けて-2013 年
[10]. 近藤大輔:組織文化を形成するマネジメント・コントロール・システム : 日本航空株式会社に導入されたアメーバ経営の考察
[11]. メアリー・ジョー・ハッチ アン・L・カンリフ:Hatch 組織論，同文舘出版，2017 年
[12]. NIST SP800-50 IT セキュリティの意識向上およびトレーニングプログラムの構築，2013 年
[13]. 諏訪博彦 原賢 関良明:情報セキュリティ行動モデルの構築 – 人はなぜセキュリティ行動をしないのか，情報処理学会論文誌, Vol53, No.9, 2204-2212，2012.
[14]. アメーバ経営学術研究会:アメーバ経営の進化 : 理論と実践， 2017 年
[15]. ジョン P.コッター:第2版 リーダーシップ論 - 人と組織を動かす能力， 2012 年
[16]. 森泉慎吾 白井慎之介:リスクテイキング行動尺度の信頼性・妥当性の再検討，労働科学 87 巻, 6 号 (211) ~ (225) ， 2011 年