経営経理研究　第 118 号
2020 年 10 月　pp. 43-57

〈論　文〉

# 情報セキュリティ対応組織の経営組織論の視点からの研究

## ── 実践論に基づく CSIRT 研究の可能性 ──

寺　本　直　城

**要　約**

本論文の目的は，情報セキュリティ対応組織を経営組織論の視点から分析することの可能性について論じることである。情報化社会がますます進展し，情報コミュニケーション技術の発展および経営組織への普及が進む現代において，組織をコンピュータセキュリティインシデントから防衛することが重要な経営課題となっている。そのような社会的背景のもと，CSIRT（Computer Security Incident Response Team）を実装する，ないし実装しようと試みる経営組織が増えつつある。しかしながら，CSIRT の構築や運用は多くの場合において困難に直面していると報告されている。本稿では，このような問題意識のもと，主にコンピュータサイエンスの分野から論じられてきたコンピュータセキュリティ対応について，経営組織の視点から展開していくことの可能性について論じた。

本論文は，3 つのセクションにより構成されている。第 1 に，CSIRT の現状について論じた。ここでは，CSIRT とは何か，そして，我が国における CSIRT の置かれた現状について明らかにした。第 2 に，CISRT 研究の現状について議論した。CSIRT 自体は，組織的な議論がそれほど数が多くはないものの行われてきた。組織的な CSIRT 研究・報告・議論がもたらしてきた貢献と，その限界について論じた。第 3 に，実践論的アプローチに基づく CSIRT 研究の可能性について論じた。CSIRT についての組織の分析は今まで規範論に基づいて行われてきた。これらの研究の限界と新しい可能性として実践論に着目した。

**キーワード**：CSIRT，実践論的転回，コンピュータセキュリティインシデント

## 序

本稿の目的は，経営組織の情報セキュリティ対応に対して経営組織論の視点からの分析・研究を展開することの可能性について論じることである。近年，情報コミュニケーション技術（以下，ICT；Information Communication Technology）の進展に伴い，多くの経営組織において情報インフラストラクチャー（以下，情報インフラ）の整備が進んでいる。これらの情報インフラは，企業の業務の合理化・効率化に資するだけでなく，新たなビジネスチャンスを生み出す基盤にもなっている。他方で，近年，企業を含む多くの組織を対象としたサイバー攻撃や大規模な情報漏えい事

故などの，いわゆるコンピュータインシデントの発生例は枚挙に暇がないほど増えつつある。このような事情に鑑みて，近年，組織にとっては，コンピュータインシデントに備えることが非常に重要な経営課題となりつつある。

コンピュータインシデントから組織・企業を防衛するべく，情報セキュリティについての専門的な対応組織としてCSIRT（シーサート；Computer Security Incident Response Team）を構築・実装する組織が増えつつある。この事実が重要なのは，コンピュータインシデントへの対応を個人として行うのではなく，組織的に行おうと考える組織が増えているということである。今や，サイバー攻撃や情報漏えい事故は，悪意をもった個人によるものだけではなく，悪意をもった組織的犯行である場合があることも指摘されている（松原，2017；横浜，2018）。他方で，そのような悪意を持つ個人や組織によるものだけではなく，組織内部の構成員による悪意のない行為（たとえば，単純なミス）などによって引き起こされる場合もある。もはや企業や組織の誰か個人的な構成員が，以上のように多様な原因によって引き起こされるコンピュータセキュリティインシデントから組織を守ることが困難になっている。情報セキュリティに対して組織的対応を行う必要性が増しているということを前提にするならば，情報セキュリティは非常に高度な技術的側面を有しつつも，他方で，組織的な側面が今度さらに重要視されるようになると考えられる。萩原・杉浦（2017）は，CSIRC（シーサーク；Computer Security Incident Response Capability），すなわち「コンピュータセキュリティインシデントへの対応能力」という名称も過去に使われており，本来ならば機能で実施すればよいものであるものの，チームで実施することや協働作業の重要性からCSIRCという言葉は消え，CSIRTが残ったものと考えられると指摘している。

以上の点から，本稿では情報セキュリティ組織の一つであるCSIRTに焦点を当て，CSIRTを組織論的な視点から論じることの重要性や可能性について論じたい。これらを明らかにするために，第1にCSIRTおよびCSIRT研究の現状について明らかにしたい。CSIRTはそのコンピュータセキュリティインシデントへの対応に注目されているという社会的背景があるにも拘らず，その構築や運用については困難に直面している。このセクションでは，CSIRTとは何かといった根源的な問いとともに，CSIRTが置かれている現状そして問題について議論していく。第2にCSIRT研究の動向を経営組織論的に分析するときの視点として実践論的転回について論じていく。第3に，既存のCSIRT研究の動向を組織研究の枠組みに当てはめながら，今後の情報セキュリティ組織研究の方向性を示していく。

## 1. CSIRTの動向

### ⑴ CSIRTの現状

CSIRTとは，コンピュータセキュリティインシデントに対応するための組織・チームを指す言葉である。我が国最初のCSIRTであるJPCERT/CC（ジェイ・ピー・サート・コーディネーション・センター；Japan Computer Emergency Response Team Coordination Center）によれば，コンピュータセキュリティインシデントとは「情報および制御システムの運用におけるセキュリティ上の問題として捉えられる事象」と定義される。組織が有する，あるいは，利用する情報システムや制御システムの運用を阻害するようなセキュリティ上の問題から，組織ないし組織の業務を守る

のがCSIRTの役割である。

コンピュータセキュリティインシデントに初めて関心が集まったのは，1988年のアメリカのMIT（マサチューセッツ工科大学；Massachusetts Institute of Technology）に送り込まれたモリスワームの問題であったとされている。モリスワームはインターネットを通じ，約6,000台のマシンに感染し，それらのマシンに過大な負担を与えることでサービスを停止させるという事態を発生させた。これがコンピュータセキュリティインシデントへの対応ということが注目される契機となった（cf. Eisenberg et al, 1989; Orman, 2003; 寺田 , 2016；萩原・杉浦，2017）。

この事件に対応するために，同年，CMU（カーネギーメロン大学；Carnegie Mellon University）内に，DARPA（アメリカ国防高等研究計画局；Defense Advanced Research Projects Agency）主導で対策チームであるCERT/CC（Computer Emergency Response Team Coordination Center）が設置された。これがCSIRTの源流であるとされている。CERT/CCは，CSIRTの構築や運営を円滑なものにするためのガイドラインとしてWest-Brown et al.（2003）“*Handbook for Computer Security Incident Response Teams*（*CSIRTs*）”を作成している。このハンドブックに書かれたCSIRTの構築・運営方法が一種のスタンダードとみなされており，CERT/CCが置かれているCMUにちなんでCMUモデルと呼ばれている。その意味では，CERT/CCは，いまなおアメリカの中心的な国家CSIRTとして影響力を持っているともいえる。

また，コンピュータセキュリティインシデントはインターネットを介して爆発的に広がる恐れがあるため，世界各国のCSIRTと情報共有などの連携をする必要がある。このような考え方をもとに，CERT/CCが中心となってFIRST（The Forum of Incident Response and Security Teams）が1990年に設立され，今尚，国際的なCSIRT同士の連携を支えている。2020年6月現在，FIRSTには96の国と地域から531のチームが参加しており，我が国からも37チームが参加している（FIRST Members around the world https://www.first.org/members/map（2020年6月1日））。

CSIRTの役割については，一致した見解は見られないもののいくつかのパターンを見ることができる。West-Brown et al.（2003）によれば，CSIRTは通常，事前対応，事後対応，品質管理の3つのサービスの内のどれか，どれかを組み合わせて，あるいは，全ての業務を行うとされている（West-Brown，2003；25）。事前対応とは，セキュリティインシデントについての情報収集・モニタリング，セキュリティ情報の配信や，インシデントの検知などのコンピュータセキュリティインシデントが起こったときの準備である。事後対応は，実際にインシデントが起こった後の対応として，被害を最小化するように，インシデントのハンドリング，さらには解析などを行うサービスを指し示す。品質管理とは，例えば現在多くの製品がインターネットにつながるように設計されているが，そのように設計された製品や技術の評価・管理を行ったり，組織のメンバーたちに教育やトレーニングを実施したり，啓蒙活動を行うことである。West-Brown et al（2003）では，それぞれのCSIRTが設定している目標や課せられた任務に応じて，これらのサービスを選択し，組み合わせたりしながら役割を全うすべきであるとしている。

他方で，寺田（2016）は，CSIRTは消防署をメタファーとして説明可能であるとして，その役割を特徴づけている。消防署は，火事などの災害が起こったときに出動し，それらに対応することだけが任務ではない。消防署は災害が起こらないように見回りをしたり，災害が起こったときに備

えて訓練をしたり，防災設備の点検をしたりしている。CSIRT もそれを同様に，インシデントレディネス（事前対処）とインシデントレスポンス（事後対処）の両方を行う必要があるとしている（寺田，2016；99）。

我が国においては，1996 年に JPCERT/CC が日本情報処理開発協会のセキュリティ対策室の分室として設置されたのがはじめの CSIRT とされている。2007 年には当時 6 チーム存在していた CSIRT が NCA（日本シーサート協議会；Nippon CSIRT Association）を発足した。これは，日本国内の CSIRT 同士の連携を促進することを目的としていた。さらに，2012 年には NISC（内閣サイバーセキュリティセンター：National Center of Incident Readiness and Strategy for Cybersecurity）の情報セキュリティ対策推進会議における「情報セキュリティ対策に関する官民連携のあり方について」の中で，政府の調達契約において情報セキュリティの保全を目的に CSIRT の設置について言及された。これを契機に，それまで情報セキュリティに無頓着であった企業も CSIRT を設置するようになり，我が国における CSIRT の数は急激に増加することとなる。

2007 年に 6 チームからスタートした NCA は，2020 年 6 月 8 日時点で 395 ものチームが加盟するようになっている。

### ⑵ CSIRT の問題点

以上に見てきたように，CSIRT 自体の数は急激に増加しており，より実行力のある情報セキュリティ体制を構築することが重要事項になりつつある。しかし，この現状について様々な問題が提起されている。

IPA（(独)情報処理推進機構：Information-technology Promotion Agency）がまとめた 2020 年現在の最新の報告書において，セイバーセキュリティ体制についてのいくつかの問題点が挙げられている。第 1 に，サイバーセキュリティの予算が，人材ではなく技術投資に集中していることが挙げられている。どうしてもサイバーセキュリティは，技術的な課題であると認識されがちであり，組織の課題と認識されていない。IPA（2020）では，サイバーセキュリティが経営上のリスクとして認識され，短期的に効果を発揮する技術的投資が優先されることは自然な流れではあるものの，中長期的な目線で考えるならば人材の育成・確保が必要であるとしている。

萩原・杉浦（2017）によれば，現在，我が国の CSIRT には 2 つの課題があると指摘している。第 1 に，CSIRT が経営層の真の承認が得られないことを上げている。彼らは，予算に着目し，CSIRT の多くが明確な形で予算が確保されていないことを根拠に，組織として真の承認が得られていないと考察している。また，第 2 に現業との差別化の難しさを課題として挙げている。CSIRT は専門的で技術的な知識の必要性が高いため ICT やセキュリティ知識に富んだ人物や組織，具体的には情報システム管理部門が中心となって構築している傾向が強い。部署横断的な連携が必要であり，且つ，現業との差別化を図るためにも，本来はリスク対策そのものを担う部門や総務部門等のほうが適していると指摘されている（萩原・杉浦，2017；951）。また，彼らの研究の背景には，CSIRT の数が増えてきている反面，「名ばかり CSIRT」と言われる，活動実態のないものや，あっても質の低い CSIRT が登場しているという問題意識も述べられている。

杉原（2018）も，人員や予算といった問題を指摘しているが，さらに，人事異動や査定・考課・報酬についても問題を指摘している。CSIRT は専門性の高い部門であるにも拘らず，多くの企業

で定期ローテーションが行われており，専門的技術の蓄積が阻害されていると述べられている。IPA（2020）でも指摘されているように，コンピュータセキュリティの人材育成が我が国全体で遅れており，専門性の高さから人材育成に時間がかかるという事情のなか，専門的技術の蓄積が遅れるのは問題である。また，CSIRT の活動は，経営層から業務内容が理解されにくく，評価もされにくいといった問題が挙げられている。

以上のように，現在，組織の情報セキュリティに関する話題は，技術的要因は当然のこと，組織的要因にまで拡大している。IPA（2020）の指摘にもあるように，組織の情報セキュリティに関する認識は，一般的には技術的要因と捉えられる傾向にある。あるいは，少なくともその予算配分としては，技術的投資に重きが置かれ，組織への投資がなされていない。しかしながら，IPA（2020）の指摘にもあるように，そして，萩原・杉浦（2017），杉原（2018）が指摘するように，組織のコンピュータセキュリティインシデントは組織的対応が重要になりつつある。その意味では，技術的要因の重要性が一般的に認識されている現状においては，むしろ，コンピュータセキュリティインシデントに関わる組織的要因こそが問題であり，問題となりつつあるということである

## 2. CSIRT 研究の動向

### ⑴ CSIRT 研究の現状

以上に述べてきたように，CSIRT やコンピュータセキュリティインシデント自体がまだ歴史が浅いこともあって，CSIRT や情報セキュリティ組織の研究自体の蓄積はそれほど多くはない。しかしながら，その重要性などから，最近増えつつあるのも事実である。

先にも触れた West-Brown et al.（2003）が，最も古い CSIRT についての研究書である。2003 年版は 2 版であり，初版は 1998 年であるからひときわ古いものであるといえる。これは，CSIRT という存在の解説であり，その要件や運用方法などを解説するものである。さらに，Penedo（2006）は，CSIRT を普及させていくために，CSIRT の必要性や CSIRT の設立に必要な設備やコストなどを示している。また，Globler et al.（2010）は，CSIRT の設立の際に直面する問題について分析をしている。Penedo（2006）や Globler et al.（2010）も，学会報告での予稿集に掲載されたものであり，一連の研究成果として展開されているものは，国際的にも少ないといえる。

我が国においても，日本シーサート協議会編著（2016）は，NCA が主体となって CSIRT の構築から運用までを解説している。また，IPA などが中心となって CSIRT を含めて，組織の情報セキュリティ体制についての現状調査について多く報告されている。他方で，横浜（2018）や松原（2019）が，コンピュータセキュリティインシデントの企業にとっての脅威と，コンピュータセキュリティインシデントに対応することの重要性を説いている。彼らの文献には CSIRT についての言及もされており，組織の情報セキュリティ体制の強化の具体的な方法にも触れられている。

他方で，CSIRT あるいは情報セキュリティ体制について経営組織論の視点から分析・研究をしたものについてもやはり関連学会における予稿集ないし報告書に掲載されたものが中心（e.g. 近藤ら，2013a；近藤ら，2013b；近藤ら，2015；寺本・中西，2014；寺本ら，2015）で，体系だった研究はそれほど多くない。

それは海外においても同様で，たとえば Sawicka et al.（2005）は CSIRT そのものの分析ではな

く，CSIRT が組織に及ぼす影響，とりわけ，組織の変革を促す影響について分析している。もちろん，このような視点は，経営組織研究を進めていくうえでは重要であり，興味深いものでもあるが，やはり報告書としてしか研究成果が蓄積されていない。

我が国においては，CSIRT の現状についての分析を行っている文献がいくつか見られる。例えば，萩原・杉浦（2017）や寺田（2016）は，CSIRT の現状を，CSIRT の運用者の視点から分析している。また杉原（2018）は，CSIRT のメンバーに対してアンケート調査を行い，現状の CSIRT が抱える問題について定量的に実態を明らかにいている。

また，CSIRT の現状調査・分析を業績として残した上記の研究に対して，CSIRT をケースとして積極的に経営組織の理論的拡張を目指した研究も見られる。たとえば，Takagi & Hoshi（2012）は，CSIRT のメンバーたちが組織や技術を継承していくプロセスを，ストーリーテリングの視点から分析している。また，Teramoto（2016）は，CSIRT メンバーの学習について，ゲーミフィケーションと実践論の立場から，そのプロセスを明らかにしようと試みている。近藤ら（2018）は，CSIRT が機能不全に陥っていくプロセスをレジリエンスの観点から明らかにし，「レジリエンスの罠」という概念の提言を行っている。これらの研究は，我が国における CSIRT を組織論的に分析した研究であるといえる。

コンピュータセキュリティインシデントが組織に及ぼす影響についての研究や分析もここ最近になって急進展している。Clearfield and Tilcsik（2018）は，情報インフラや ICT が組織のシステムを複雑かつタイトカップリングな状態にするが故に，大きな失敗・不祥事につながるということを明らかにした。とはいえ，これはどちらかというと，Perrow（1999）のノーマル・アクシデント理論をベースとした組織の失敗・不祥事研究であり，如何に組織が情報セキュリティ体制自体を解明したり，強化したりするかといったことに焦点が当てられているわけではない。しかしながら，Clearfield and Tilcsik（2018）の見解は，コンピュータセキュリティインシデントによる失敗を技術的な問題ではなく，組織的な問題として扱っているという視点は本稿とも一致するものである。

### ⑵ CSIRT 研究の貢献と限界

上述してきた，主に CSIRT の研究は，その原点にある West-Brown et al.（2003）の議論を前提に進められてきているという特徴がある。West-Brown et al.（2003）は，世界で初めて社会的な問題となったコンピュータセキュリティインシデントであったモリスワームへの対応を行ったコンピュータセキュリティインシデントチームに関わる諸団体が，その構築・運用の方法について解説しているものである。そのため，CSIRT の構築・運用の教科書・参考書的な存在であると指摘することができる。 West-Brown et al.（2003）は JPCERT/CC によってを邦訳され，JPCERT/CC はこのハンドブックを我が国における経営組織が CSIRT を導入する際のガイダンス的な資料と位置付けている。West-Brown et al.（2003）は，JPCERT/CC の Web ページからダウンロードできるようになっている。そこには，「この文書は 2003 年に公開されたものであるため，想定している脅威や個別の対応策にはやや古いと捉えられるかもしれないが，背景にある概念は現在でも，またどのような形態の CSIRT 組織でも同じように役立つ（JPCERT/CC Web ページ　https://www.jpcert.or.jp/research/csirt　handbook.html）。」と述べられている。さらに続けて「本ハンドブックが日本国内のインシデント対応組織とこれから作ろうとする組織へのガイダンスとなることを期

待する（JPCERT/CC Web ページ　https://www.jpcert.or.jp/research/csirthandbook.html）.」と述べられている。このことからも，少なくとも我が国における West-Brown et al.（2003）が CSIRT 構築・運用の教科書的存在と位置付けることができる。

さて，我が国における CSIRT 研究は，この West-Brown et al.（2003）の議論を前提として展開されてきた。たしかに West-Brown et al.（2003）の業績はコンピュータセキュリティインシデントの対応事例として最も先進的な見解であったということができ，キャッチアップする立場であった日本企業にとって，また，日本企業全体のコンピュータセキュリティインシデント対策を強化していきたい JPCERT/CC にとっては，有用な資料であったといえる。そのため，West-Brown et al.（2003）の議論を前提としてきた CSIRT 研究は，コンピュータセキュリティインシデント対策のキャッチアップを測る組織や，組織にコンピュータセキュリティインシデント対策について理解させたい立場の研究者たちにとって有用であったといえる。

実際，CSIRT のサービス範囲についての議論や，CSIRT の権限についての議論（萩原・杉浦，2017；寺田，2016）は West-Brown et al.（2003）の議論を原典として利用している。また，杉原（2018）もアンケート項目のうちサービス範囲についての項目や権限についての項目は West-Brown et al.（2003）の議論から抜粋されている。

また，上述したように現状の CSIRT についての研究・調査は，IPA や NCA，JPCERT/CC といった機関の現状調査報告が中心である。

以上に挙げた諸業績は，CSIRT ないし企業の情報セキュリティ体制に対して理念型を提示するとともに，実際の解決策の参照点となり得るであろうという貢献を見出すことができる。

その反面，これらの業績は実務的な記事であり，要件や構築方法の解説にとどまっており，様々な境遇に立たされている CSIRT 自体の分析に踏み込めていないといった限界が共通してみられる。特に本稿がめざす，CSIRT あるいは情報セキュリティ体制の経営組織論的な分析とは視点を異にしている。

既存の CSIRT 研究は，規範論的な側面が重視されてきたということが指摘できる。もともと，コンピュータセキュリティインシデントの対策は，コンピュータサイエンスやコンピュータセキュリティといったか科学の一分野として確立してきたものであるものの，CSIRT の構築や運用といった問題は，コンピュータサイエンスやコンピュータセキュリティの文脈とは切り離されて，一歩遅れて議論されてきた。それは，West-Brown et al.（2003）の「（コンピュータサイエンスが，科学の一分野と認められるようになり，コンピュータセキュリティもコンピュータサイエンスの不可欠な要素として認められてきたのと）同様に，セキュリティ分野において CSIRT の必要性が認められるべきです（West-Brown et al., 2003; XI）。」という主張に表れている。この引用は，初版にむけたものであることから 1997 年時点で書かれた一節であることになる。そこには 1997 年時点での問題を知ることができる。様々な組織のコンピュータセキュリティインシデントの脅威を認識し，これに対応したいメンバーが CSIRT を構築したくても，経営層からコンピュータセキュリティに関する問題に関する支持や理解を得ることが困難であるという問題が現場にはあったと考えられる。さらに，指示や理解を得られ CSIRT の構築が完了し，運用していくことになったとしても，CSIRT とは何かを他の組織のメンバーやステークホルダーに理解させられるような文書情報がないことが問題であったとされている。そのような中から「CSIRT とはかくあるべし」といった規

範が CSIRT 研究の主要な位置を占めてきたと分析することができる。

しかし，このハンドブックが 2003 年に公開され，さらに 2007 年には日本語訳されて，誰でも利用できる形で公開されているにも拘らず，CSIRT を取り巻く問題はいまだ未解決のままである。それどころか問題がさらに多様化し複雑化している。未解決の問題としては，CSIRT の活動が，経営層に理解されず，いまだに真の承認が得られないという課題があるとの萩原・杉浦（2017）の指摘が挙げられよう。West-Brown et al.（2003）の問題意識の出発点は，まさにその経営層に活動の重要性が認識・理解されず，構築に至らない，あるいは，構築が認められても運用が困難であるという CSIRT が多いということであった。にも拘らず，その問題意識がいまだに解決されていない。

また，West-Brown et al.（2003）の時代に比べると，CSIRT の設置が必要とされる業種が増加しつつある。例えば，NCA は当初，HIRT（日立製作所），IIJ-SECT（インターネットイニシアティブ），JPCERT/CC，JSOC（ラック），NTT-CERT（日本電信電話），SBCSIRT（ソフトバンク BB）の 6 チームから発足している（NCA Web ページ，「設立趣意書」http://www.nca.gr.jp/outline/prospectus.html（2020 年 6 月 1 日））。この 6 チームは，我が国における最初期の CSIRT 群ということができるが，これらの企業は全て情報通信産業に位置する企業群であった。当初 CSIRT が必要とされていたのは，このような情報通信産業を営む組織であると考えられていた。しかしながら，特に我が国では上述したように，政府調達にかかる条件として CSIRT の設置を義務つけられたことから，情報通信産業に属せず，インターネットや ICT をユーザーとして利用する企業（＝ユーザー企業）も CSIRT の設置が必要となっている。

ここには少なくとも 2 つの問題点が存在する。第 1 に，萩原・杉浦（2017）の問題意識にあるような「名ばかり CSIRT」の問題である。政府調達という，いわば外部の圧力によって CSIRT というものを作らなければならなくなったという事情から CSIRT が構築された場合，CSIRT があるということを，政府調達の際に政府にアピールできればよいといった事態が起こりうる。そこで，CSIRT という名前のチームのみを作成したものの，運用方法が理解されなかったり，実際に運用することの重要性が理解されなかったりして，活動実態がなくなってしまうという問題が「名ばかり CSIRT」問題である。

第 2 の問題として，CSIRT の重要性・必要性が理解されることの難易度が上がっているということである。当初，CSIRT が必要とされてきたのは，多くが情報通信産業を専ら営む組織であったため，経営層まで比較的コンピュータセキュリティインシデントの脅威が理解されやすい環境であったと考えられる。他方で，ユーザー企業の場合，現場のコンピュータに詳しいメンバーがコンピュータセキュリティインシデントを脅威に感じ，CSIRT の重要性・必要性を認識したとしても，経営層は情報通信産業の企業に比べると，コンピュータセキュリティインシデントに詳しくない，ないし全く理解できない状態であることが考えられる。その場合，ユーザー企業において CSIRT の重要性・必要性を認識させることは，情報通信産業の企業に比べると難しくなることが考えられる。また，この業界の違いは，設立後の運用にも関わってくる。特にユーザー企業の場合，現場のコンピュータに詳しいメンバーに，コンピュータセキュリティインシデントの対応を頼り切ってしまうということが起こりやすい。杉原（2018）の調査からも明らかなように，ジョブローテーションによってコンピュータセキュリティインシデントの対応のノウハウが蓄積されないといった問題

も，現場のコンピュータに詳しいメンバーに，コンピュータセキュリティインシデントの対応を頼り切ってしまうといったことにも起因している。

このように，規範的な研究はCSIRTのあり方を解明し，確かに多くの企業・組織においてCSIRTのあり方について啓蒙してきたといった貢献をしてきた。しかしながら，その反面，特にWest-Brown et al.（2003）を前提とした研究や調査報告は，現状の多くの企業が抱えている問題の解決には至っていない。また，そのような問題を抱えるCSIRTや成功しているCSIRTの構築・運用過程に関する描写について，その枠組みを提供できていないという研究上の限界を有している。

## 3. CSIRT研究の言語論的転回そして実践論的転回へ

以上のような，CSIRTあるいはCSIRT研究の現状の限界を乗り越えるため，本稿ではCSIRT研究の言語論的転回そして実践論的転回の重要性を指摘したい。経営組織論において，実践論的な転回が重要視されるようになって久しい。これは，組織現象を客観的な事物としてみなすという潮流を見直すことに起源をもち，組織現象を言語による産物としてみなそうという第1段階の転回，さらに，組織現象を組織のメンバーによる実践による産物とみなそうという第2段階の転回をさす。

本章では，これらの組織論上の転回がどのようなもので，それがCSIRT研究に展開されることによって得られる示唆について考察する。

### ⑴ 経営組織論における言語論的転回そして実践論的転回へ

伝統的な経営組織研究においては，組織のリアリティは客観的な実在であった。すなわち，組織のリアリティは，組織のメンバーとは独立に存在し，組織のメンバーの行動を決定づける力を持つものであると考えられてきた。このパースペクティブからすると，組織のリアリティは所与であり，疑いようもなく存在するものと捉えられてきた。これは，伝統的な機能主義的な社会科学の伝統によるものでもあった。

それに対し，社会学で起こった言語論的転回が，経営組織研究にも影響を及ぼすようになった。社会学においては，Berger & Luckmann（1966）を中心とした社会構成主義とよばれる潮流が興り，社会現象の見方について根本的な見直しを迫った。社会構成主義のパースペクティブによれば，社会現象は社会と構成する人々によって構成されるものであり，所与の条件とは見なされない。つまり，社会現象は客観的な実在ではない。そして，Burr（1995）によれば，社会現象を構築しているのは言語によってである。

この見方が経営組織研究に影響を及ぼすようになると，組織のリアリティもまた，組織メンバーの言語によって構築されていると考えられるようになった。これが，経営組織研究における言語論的転回である。

たとえば，Orr（1996）は，ゼロックス社のコピー機の修理技術者に対するエスノグラフィー研究を行い，修理技術者たちが言語によって組織のリアリティを構築しているプロセスについて解明した。Orr（1996）は，技術者たちが自らの仕事について話すとき，問題処理や故障修理について

の知識を共有するだけでなく，それによってアイデンティティを確立していることを指摘している。また，これらの技術者たちの語りは，会社が準備したマニュアルや研修以上に，技術者たちの知識の共有に活かされ，彼ら自身の意味世界，つまり組織のリアリティを構成していたのである。

このように，組織を構成する人々の言語に着目し，その言語がどのような意味をもち，どのように組織を構成しているのかを解明していくことを目指したのが，組織の言語論的転回であった。

それに対し，さらに新たな潮流として出てきているのが，実践論的転回であった。これは，言語論的転回が着目した言語の限界に着目している。言語についての限界は，例えば，Polanyi（1966）の人間が持つ暗黙の次元についての議論などに表れてくる。人間は語り得ない次元の知識を持ちうることを考慮すれば，社会のリアリティを言語によって全て説明することは不可能である。ここで，実践への注目が要求されるのである。

Schatzki（2001）によれば，実践とは「共有された実質的な理解の周辺に中心的に組織化された，実体化され物質的に媒介された一連の人間の活動（Schatzki，2001：2）」と定義される。このパースペクティブからは，社会のリアリティは言語ではなく，実践，すなわち人間の活動によって構成されていると考えられる。

また，実践論的転回は，言語の限界を越えようとするだけでなく，伝統的な社会科学と言語論的転回を架橋するものでもある。伝統的な社会科学における社会についての前提に疑義を唱える形で，言語論的転回が出現してきたことは上述の通りである。これらは，伝統的な社会科学が，専ら社会現象から社会の構成員の行動について説明しようと試みていたのに対し，言語論的なアプローチは，社会成員の言語の使用から社会の構成について説明しようと試みてきた。これらの両者の見方は，社会から成員，ないし，成員から社会という一方向的な構成を想定していると，実践論的転回を試みる議論では考えられている。しかしながら，これらは実際は両方向的，相互的に作用している。社会成員の行為は，社会的なコンテクストの中から形成され，また同時に，社会的な行為は社会的なコンテクストを構成するのである。

この実践論的転回は，経営組織研究においては，実践共同体の議論以降注目されてきた。Lave & Wenger（1991）は，多様なコミュニティにおける学習の様態を実践という視点から解明した。彼らは実践共同体とよばれる実践によって構成されているコミュニティへの参加することによってあるコミュニティで一人前と認められる過程を明らかにしている。実践共同体の中で新人は，そのコミュニティでの作法を知らないために，周りの人々の真似をしながら，周辺的な実践を再生産する。この参加様態を正統的周辺参加と呼ぶ。これが，一人前になるにつれて，中心的な実践を生産できるようになり，これを十全参加と呼ぶ。この実践共同体への正統的周辺参加から十全参加への参加形態の変容を通して人間はコミュニティにおけるアイデンティティを確立すると同時に学習していくことを明らかにした。

ここで重視されるのは，知識や技能といったものの客観性への疑義である。学習とは，本来，知識や技能といったものが客観的実在物であるという前提から，それらは記述可能であると考えられ，その効率的・合理的な習得が議論されてきた。しかしながら，Blackler（1995）は①知識は静的なものでなく動的であり，②客観的でなく主観的なものであり，③経験的なだけでなくアプリオリな認識によっても認識される　と伝統的な知識についての前提を批判した。彼は，知識（knowledge）という言葉と使うのをやめ，知識化（knowing）という言葉を使うべきだと主張する。

Blackler（1995）にあっては，この知識化の過程こそが実践そのものであった。

Nicolini et al.（2003）は，すでに実践という概念をベースにした組織における学習・知識化アプローチは一つの確立した研究分野になりつつあると評価している。また，この実践の概念は，Wittington（1996），Wittington（2003）や Johnson et al.（2003），Johnson et al.（2007）によって経営戦略論にまでその影響力が拡大されることになる。

### ⑵ CSIRT 研究の実践論的転回

このように，社会科学あるいは経営組織研究における伝統的な方法，言語論的転回，そして実践論的転回の議論を踏まえて，CSIRT 研究の実践論的転回とその可能性について考えていきたい。

今までの CSIRT 研究は，伝統的な社会科学ないし経営組織研究に則ったものであったといえる。既存の CSIRT 研究の多くは，West-Brown et al.（2003）に代表されるような規範的な CSIRT 像に過度に依存していた。それらは，理想の CSIRT 像という客体があたかも存在するかのように前提とし，その CSIRT 像の中でその組織のメンバーが従事すべき業務やサービスを明らかにしてきた。また，現状についての調査・分析についても，客観的な実在として理想化された CSIRT と，眼前にある問題を抱えた CSIRT，ないし，問題をクリアした CSIRT との差分を求める形で展開されてきた。このような見方は，自然科学的な方法を用いて客観的な法則や真理を追究しようとしてきた伝統的な社会科学の見方と一致する。

他方で，これらの見方は，人間によって組織が構成されているという視点を欠くものであると考えられる。言語論的なアプローチが，組織を構成する要素として，組織成員の言語に注目してきたように，CSIRT は CSIRT を構成する人々の言語によって多元的に存在し得る。そのような見方がいままであまりなされてこなかった。

現状，CSIRT が抱える問題の多くは，CSIRT をめぐる認識の問題であった。コンピュータセキュリティインシデントに脅威を覚える組織メンバーと，それを理解できない経営層の認識の違いや，コンピュータセキュリティインシデントの対応を強化したい政府と，とにかく政府調達さえできればいい企業の認識の違いが，現状の CSIRT の問題として挙げられていた。これらは，伝統的な社会科学における分析によって解決する問題ではない。なぜなら，これらの認識は，全て CSIRT をめぐる多元的なリアリティだからである。伝統的な社会科学的方法論を用いた経営組織研究として CSIRT 研究を進めるということは，このような CSIRT についての多元的な現実を前提に議論することができない。しかし，CSIRT・CSIRT 研究が抱える問題を解明していくためには，この多元的なリアリティの生成過程を解明していく必要がでてくる。このように CSIRT 研究を言語論的アプローチで見ていくことによって，CSIRT・CSIRT 研究が抱える問題について解明することができるということである。

とはいえ，言語論的転回によって可能なのは現象の描写である。言語論的アプローチによる CSIRT 研究では，CSIRT に関わる多元的な現実を描写することが主なミッションになる。また，成功事例や失敗事例の質的研究を通した構築・運用プロセスの解明に留まることになる。実際，CSIRT に関わる人々の活動が，CSIRT の活動を構成するのと同時に，CSIRT に関わる人々は，彼らの立ち位置から活動を規定されている。その側面もまた解明される必要がある。

とくに，長きにわたって JPCERT/CC や NCA では，West-Brown et al.（2003）を前提として，

新出の CSIRT に教育を施してきた。また，IPA や JPCERT/CC は，West-Brown et al.（2003）を前提として，あるべき姿の CSIRT を前提に様々な報告や提言を行ってきた。それが意味するところは，West-Brown et al.（2003）やそれらの報告書・提言は，実際に多くの CSIRT あるいは CSIRT のメンバーの行為を形成しているであろうということである。また他方で，そのように構成された CSIRT あるいは CSIRT のメンバーの行為が CSIRT を構成している。もはや公式の記述や報告書やプランといった産物によるコントロールは限界であり，CSIRT 自体あるいは CSIRT に関わる世界は，実践とその相互作用によって生起される場と認識するのが CSIRT 研究の実践論的転回である。この規範としての CSIRT 論と，言語としての CSIRT 論を架橋していくことによって，CSIRT 活動の実態を解明するとともに，現状多くの CSIRT が抱える問題の多くを解決できるものと考えられるのである。

## 結びに代えて

本稿では，多くの経営組織がコンピュータセキュリティインシデントの対応を強化していかなければならないという現状に鑑みて，コンピュータセキュリティインシデントの対応組織である CSIRT の組織論的な研究の今後の動向について論じてきた。

多くの CSIRT は，その社会的背景とは裏腹に，構築や運用に対して様々な障害に直面している。CSIRT 自体の認知度を上げたり，重要度を理解してもらうことが問題になっているということが，多くの研究や調査によって明らかになってきた。

既存の CSIRT 研究の多くは，伝統的な社会科学の認識論・方法論によってなされてきた。これは，CSIRT の理想の姿について啓蒙するという貢献をしてきた。他方で，既存の CSIRT 研究は必ずしも，上述の CISRT が抱える問題に対して有効な分析がなされていたわけではなかった。

本稿では，経営組織論の言語論的転回および実践論的転回に着目し，CSIRT 研究の言語論的転回，実践論的転回の可能性について論じた。現在，CSIRT が抱える諸問題は，CSIRT についての多元的なリアリティの葛藤状態であると考えることができる。そのようなリアリティが多様に存在することを前提として，それらを記述・解明していくことが CSIRT の言語論的転回を通して可能となる。また，今までの伝統的な CSIRT 研究と，CSIRT の言語論的な研究を架橋し。CSIRT の活動自体の実態を解明し，今ある諸問題を解決していくために，実践論的な見方が必要になってくると考えられる。

最後に本稿の限界あるいは今後の研究の展開について考えていきたい。第 1 に，研究方法についての検討がなされていない。本稿では，社会科学および経営組織研究の潮流から，CSIRT 研究の今後について論じてきたが，それらの研究がどのようになされるかといったことには言及していない。言語論的アプローチにおいても，実践論的アプローチにおいても，質的研究，特に，エスノグラフィックな研究や参与観察，インタビュー法などの，いわゆる解釈的な方法がとられ得る。これは，言語論的アプローチ・実践論的アプローチが志向する社会や組織についての存在論上ないし認識論上の特性から記述的な分析が求められることが明らかであるからである。とはいえ，本稿で言及可能なのはここまでである。実際に，現状の CSIRT が抱える問題を効果的に記述・解明・解決するための，より具体的な研究方法論について今後議論していかなければならない。

第 2 に，本稿では CSIRT の個別で運用される特性しか論じていない。本来，CSIRT は個別で運用されるという側面以外に，企業内で横断的に他部署・他のメンバーと協力しあって運用されるという側面と，他社・他業種の CSIRT 同士で連携しあうという側面が存在する。CSIRT の活動は，自己完結的な業務ではなく，常に企業内外との連携が必要であり，場合によっては，競合他社との連携ですら必要となる場合がある。本稿では，そのような CSIRT の他部門との連携や CSIRT 同志の連携を通した相互作用を前提とした活動形態について言及していない。より CSIRT の活動について明らかにするためには，この連携を前提としているという側面についても焦点を当てて，議論していく必要があるだろう。

**謝　辞**

本稿は，令和元年度拓殖大学経営経理研究所助成による研究成果である。日頃からの拓殖大学経営経理研究所からの多大なる支援に感謝申し上げる。

**参考文献**

Berger, P. L. & T. Luckmann（1966）The Social Construction of Reality: A Treatise in the Sociology of Knowledge, Doubleday & Company（山口節郎訳『現実の社会的構成　知識社会学論考』，新昭社，1997 年）.

Blackler, F.（1995）. Knowledge, Knowledge Work and Organizations: An overview and Interpretation, *Organization Studies*, 16（6）, 1021-1046.

Burr, V.（1995）An Introduction to Social Constructionism, Routledge（田中一彦訳『社会構成主義への招待　言説分析とは何か』，川島書店，1997 年）.

Clearfield, C. and A. Tilcsik（2018）. "*Meltdown: Why Our System Fail and What We Can Do About It.*"（櫻井祐子訳『巨大システム　失敗の本質 ──「組織の破壊的失敗」を防ぐたった一つの方法 ──』東洋経済，2018 年）.

独立行政法人情報処理推進機構（2020）.「企業の CISO 等やセキュリティ対策推進に関する実態調査 ── 調査報告書 ──」，（https://www.ipa.go.jp/files/000081199.pdf（2020 年 6 月 24 日最終アクセス）.

Eisenberg, T., D. Gries, J. Hartmanis, D. Holcomb, M. S. Lynn and T. Santoro（1989）. The Cornell Commission: On Morris and the Worm. *Communications of the ACM*. Vol. 32, No. 6, pp. 706-710.

The Forum in Incident Response and Security Teams（FIRST），Web ページ 'FIRST Members around the World' https://www.first.org/members/map（2020 年 6 月 1 日最終アクセス）

Grobler, M. and H. Bryk（2010）, "Common challenges faced during the establishment of a CSIRT." *Information Security for South Africa*（*ISSA*）, Sandton, Johannesburg, pp. 1-6.

萩原健太・杉浦芳樹（2017）.「CSIRT の最低要件」『コンピュータセキュリティシンポジウム 2017 論文集』，Vol. 2017，No. 2，pp. 950-954.

Johnson, G., L. Melin and R. Whittington（2003）. Micro Strategy and Strategizing: Towards an active based view, *Journal of Management Studies*, 40（1）: 3-22.

Johnson, G., A. Langley, L. Melin and R. Whittington（2007）. *Strategy as Practice*：*Research Directions and Resources,* New York: Cambridge University Press.（高橋正泰監訳。宇田川元一・高井俊次・間嶋崇・歌代豊訳『実践としての戦略 ── 新たなパースペクティブの展開 ──』文眞堂，2012 年）.

JPCERT/ コーディネーション・センター，Web ページ「インシデント対応とは？」https://www.jpcert.or.jp/aboutincident.html（2020 年 6 月 1 日最終アクセス）

JPCERT/ コーディネーション・センター Web ページ 「研究・調査レポート　コンピューターセキュリティインシデント対応チーム（CSIRT）のためのハンドブック」https://www.jpcert.or.jp/research/csirthandbook.html（2020 年 6 月 1 日最終アクセス）

近藤光・寺島健一・寺本直城・杉原大輔・高木俊雄・中西晶（2013）「日本企業における CSIRT 構築の事例 ── カーネギーメロンモデルとの比較 ──」『第 66 回全国大会　日本情報経営学会予稿集（春号）』

pp. 111–114.
近藤光・寺本直城・寺島健一・杉原大輔（2013),「日本企業における CSIRT 構築の事例 ── CSIRT 構築における制度的起業家 ──」『第 67 回全国大会　日本情報経営学会予稿集（秋号)』pp. 85–88.
近藤光・寺本直城・杉原大輔・中西晶（2015)「日本における CSIRT の現状と課題」『第 71 回全国大会日本情報経営学会予稿集（秋号)』pp. 59–62.
Lave, J. and E. Wenger (1991). *Situated Learning*. Cambridge University Press.（佐伯胖訳『状況に埋め込まれた学習 ── 正統的周辺参加 ──』産業図書，1993 年).
松原美穂子（2019).『サイバーセキュリティ ── 組織を脅威から守る戦略・人材・インテリジェンス ──』新潮社.
中西晶・杉浦芳樹・山賀正人・林郁也・杉原大輔・鈴村美代子（2012).「CSIRT とストーリーテリング」『日本情報経営学会第 64 回全国大会予稿集【春号】』，pp. 93–96
Nicolini, D., S. Gherardi & D. Yanow (2003). Introduction: Toward a Practice-Based View of Knowing and Learning in Organizations. In Nicolini, D., Gherardi, S. & Yanow, D. (Eds.) *Knowing in Organization: A Practice-Baced Approach*. M. E. Sharp: pp. 3–31.
日本シーサート協議会編著（2016)『CSIRT 構築から運用まで』NTT 出版.
日本シーサート協議会，Web ページ,「会員一覧」http://www.nca.gr.jp/member/index.html,（2020 年 6 月 8 日).
日本シーサート協議会，Web ページ,「設立趣意書」http://www.nca.gr.jp/outline/prospectus.html（2020 年 6 月 1 日).
Orman, H. (2003). The Morris Worm: A Fifteen-year Perspective. *IEEE Security & Privacy*, Vol. 1, pp. 35–43.
Orr, J. E. (1996). *Talking about Machines: An Ethnography of a Modern Job*. NY: Cornell University Press.
Penedo, D. (2006). Technical Infrastructure of a CSIRT, *International Conference on Internet Surveillance and Protection*, pp. 1–6.
Polanyi, M. (1966). *The Tacit Dimension*, Garden City, NY: Doubleday.（佐藤敬三訳『暗黙知の次元：言語から非言語へ』紀伊國屋書店，1980 年).
寺田真敏（2016).「組織のセキュリティー文化を反映するシーサート活動」『情報管理』，Vol. 59，No. 2, pp. 96–104
Sawicka, A., J. J. Gonzalez and Y. Qian (2005). Managing CSIRT capacity as a renewable resource management challenge: an experimental study. *23rd International Conference of the System Dynamics Society*, pp. 1–32.
Schatzki, T. (2001). Practice mind-ed orders, In T. Schatzki, K. K. Cetina, and E. Savigny (Eds.), *The Practice Turn in Contemporary Theory*, London, UK: Routage.
杉原大輔（2018).「日本における企業内 CSIRT の現状と課題 ── NCA への早期加盟チームの実態から ──」『開智国際大学紀要』，Vol. 17, pp. 5–21.
Takagi, T. and K. Hoshi (2012) Storytelling and Organizational Reality: A Case of the Computer Security Incident. *Okinawa University Journal of Law & Economics*, 18, pp. 1–10.
寺本直城・中西晶（2014)「CSIRT 組織化の契機」『第 69 回全国大会日本情報経営学会予稿集（秋)』pp. 203–206.
寺本直城・杉浦芳樹・林郁也・矢寺顕行・福本俊樹・近藤光・杉原大輔（2015)「我が国における CSIRT の現状と課題」情報経営学会 2015 年度秋季全国発表大会，論文番号 4
Teramoto, N. (2016) "The Game Playing as the Method of Acquiring the Ability of the Cyber Incident Handling", *Asia Pacific Conference on Information Management 2016*, pp. 129–142.
West-Brown, M. J., D. Stikvoort, Kossakowski Klaus-Peter, G. Killcrece, R. Ruefle and M. Zajicek (2003). *Handbook for Computer Security Incident Response Teams (CSIRTs) 2nd ed.*, Carnegie Mellon University.（http://www.sei.cmu.edu/reports/03hb002.pdf：2013 年 3 月 21 日),（有限責任中間法人 JPCERT コーディネーションセンター訳，http://www.jpcert.or.jp/research/2007/CSIRT_Handbook.pdf, 2013 年 3 月 21 日).
Whittington, R. (1996). Strategy as Practice, *Long Range Planning*, 29 (5): 731–735.
Whittington, R. (2003). The Work of Strategizing and Organizing: For a Practice Perspective, *Strategic*

*Organization*, 1 (1): 117-125.
横浜真一（2018）.『経営とサイバーセキュリティ ── デジタルレジリエンス ──』日経 BP 社.

（原稿受付　2020 年 6 月 24 日）