

令和 6 年 6 月 16 日現在

機関番号：32638

研究種目：若手研究

研究期間：2020～2023

課題番号：20K13594

研究課題名（和文）日本企業における情報セキュリティ組織の継承プロセスに関する実践論的研究

研究課題名（英文）The Process Taking Over the Information Security Teams in Japanese Companies: An Organizational and Practical Approach

研究代表者

寺本 直城（TERAMOTO, Naoki）

拓殖大学・商学部・准教授

研究者番号：10755953

交付決定額（研究期間全体）：（直接経費） 1,400,000円

研究成果の概要（和文）：本研究課題では、企業を含む多くの経営組織において近年課題となっている情報セキュリティの向上を目的に、その業務を行う組織やチームを対象として、それらの組織やチームの継承プロセスを、その組織やチームの人々が実際になにをしているかという実践論的な視点から解明を試みた。情報セキュリティの対応チームの多くはなんらかのインシデントが発生したり、世間の注目を浴びた際には、そのチーム自体も注目され、それゆえに設立されたり、強化されたりする。他方で、インシデントが減少したり、世間の注目を浴びなくなってしまうと予算や人員が減らされ、その存続が危うくなる。本研究ではそのような問題を乗り越える方法を検討した。

研究成果の学術的意義や社会的意義

現在、企業は悪意ある主体からのサイバー上での攻撃にさらされたり、組織の内部者の無意識や悪意のない行動からサイバー上で危機的な状況に陥ることもある。そのような状況に対応するために情報セキュリティ体制を強化したり、それを担当する部署やチームを構築する企業も増えている。本研究はそのような情報セキュリティ体制の維持や継続的な強化をすすめる組織に対して貢献するという社会的意義を有していた。また、本研究は実践論的な視点を取り入れている。経営学や経営組織論における実践論的な知見は未だ発展途上の分野でもあり、本研究は経営学・経営組織論における実践論的に知見を積み重ねるといった学術的意義を有している。

研究成果の概要（英文）：This research project aimed to improve the capability for information security handling, which has become a issue for many organizations including companies in Japan. This project attempted to clarify the succession process of these organizations and teams from a practical perspective, focusing on what the people in these organizations and teams actually do. When an incident occurs or when a team dealing with information security attract attention, the team itself also comes under the spotlight, and as a result, it is established or strengthened. On the other hand, when incidents decrease or the team ceases to receive public attention, its budget and personnel are reduced, and its continued existence becomes threatened. In this project, I examined ways to overcome such problems.

研究分野：経営組織論

キーワード：経営組織論 情報セキュリティ CSIRT 実践 高信頼性組織化

様式 C - 19、F - 19 - 1 (共通)

1. 研究開始当初の背景

本研究を開始した当時から現在に至るまで、様々な経営組織において情報セキュリティに関連する事故や不祥事、いわゆるサイバーインシデントが多発している。このようなサイバー上の事故や不祥事に対応する組織の設立もここ数年相次いでいる。他方で、一旦設立されたサイバーインシデントの対応組織の継続的な運営は困難で、数年で存続が厳しくなってしまう組織も存在する。特に営利を目的とする企業にとって、サイバーインシデントへの対応は実際に何らかのインシデントに見舞われたり、世間でそれが注目されている間は重要な経営上の問題として捉えられるが、その後サイバーインシデントが減少したり、世間からそれほど注目されなくなると、経営上の問題としての意識も失われてしまい、予算や人員が削られてしまう傾向にある。その意味でサイバーインシデントに対応するための組織は、自己の目的を削減する方向で動く組織であると言える。しかしながら、実際に当該組織がなくなってしまうと、また情報セキュリティ上の問題に見舞われる可能性もあり、継続的な運営が必要となる。そのため、情報セキュリティ対応組織は、常に自己の存在目的を達成しながら、同時に自己の存在意義を創造し続けなければならない。つまり、継続的な情報セキュリティ対応組織の維持と強化をするために、当該組織の構成員がすべきことを明らかにすることが、今後の経営組織を考えるうえで非常に重要な問題となりうるということである。

2. 研究の目的

以上の背景に鑑み、本研究課題では日本企業における CSIRT (Computer Security Incident Response Team: 企業内に設置されるサイバーインシデントに対応するチーム) の継承はどのようなプロセスを経て行われるかと明らかにすることを目的とした。さらにこの問いに基づき、経営組織の継承プロセスについての実践論からの理論的研究 CSIRT の構築メンバーや運営メンバーの実践と、CSIRT の構築・運営の相互作用・個別の CSIRT とそれを取り巻く組織 (所属組織や NCA) との相互作用はどのようなものか 日本企業における情報セキュリティ組織の継続的な運営のあり方とはどのようなものか の 3 点を明らかにすることを目的とした。

3. 研究の方法

本研究課題は以下の方法を用いて実施された。

(1) 既存研究のレビューと理論研究

はじめに本研究課題に関連する既存研究のレビューを行った。この目的は第 1 にサイバーインシデントの現状や情報セキュリティ対応組織の設立・運営状況の確認を行うことであった。これについては具体的には毎年、独立行政法人情報処理推進機構が刊行している『情報セキュリティ白書』を中心にレビューを行った。第 2 の目的は、本研究の研究方法でもある実践論に基づく組織研究の動向を把握することであった。これについては、実際に実践論の視点からの研究を試みた組織研究や社会研究を行った英語論文と日本語論文を中心にレビューを行った。

(2) データ収集

本研究課題の遂行に必要なデータを収集した。前述した、独立行政法人情報処理推進機構が刊行している『情報セキュリティ白書』によって、現在発生しているサイバーインシデントの種類やその状況のデータを収集した。また、実際に、CSIRT の構築メンバーや運営メンバーにインタビューをとったり、彼らの会合への参与観察を通してケースの構築を行った。

同時に、情報セキュリティ組織以外の組織における継承プロセスを理解するために、特に職人芸と呼ばれる技能を必要とする企業に対してもインタビュー調査や業務への参与観察を通してデータを収集し、こちらについてもケースの構築を行った。

(3) 定性的分析の実施

上述の収集されたデータに基づき、研究対象としたケースを定性的に分析した。特に、研究対象とした組織が、どのような背景に基づき設立され、その際に構築メンバーや運営メンバーは何を考え、どのように行動したのか、ケースを経時的に見たときに組織の構成員たちは、何をターニングポイントとして認識しているのかといった視点を中心に分析を行った。

4. 研究成果

本研究課題においては、いかなのような研究成果が得られた。

(1) 情報セキュリティ組織の実践論的転回の可能性

情報セキュリティ組織やその体制については、多くはコンピューターサイエンスの分野から議論されてきた。それは、そもそも情報セキュリティが注目されるようになった最初期において重要だったのは、サイバーインシデントの技術的な側面であったからである。そのため、現在で

も、情報セキュリティに関連する議論の多くは技術的な側面からの議論が大半をしめている。また、情報セキュリティ組織の構築や運営についても、情報セキュリティの技術的な側面から、規範論的な成果が多くみられる。例えば、CSIRT の構築や運営を円滑なものとするためのガイドラインは、カーネギーメロン大学内に設置されたアメリカ国防高等研究計画局主導で設置された対策チームが作成したガイドラインが利用されている。

他方で、情報セキュリティ体制の考え方は各組織や各組織が置かれる国や地域によって異なる。例えばユーザー企業と情報関連企業とでは、そもそも情報セキュリティの考え方やその重要性も異なるはずである。そのようにまった異なるはずの背景を持ちながら、利用されるガイドラインは共通のものとなっているのである。

このような情報セキュリティ組織の考え方は、ガイドラインに則った CSIRT を過度に理想化し、それぞれの CSIRT が実際にすべきこと、あるいは実際に日本企業の情報セキュリティ対応組織やその人々が行っていることを分析するという視点が欠如していた。実際には、ガイドラインと情報セキュリティ対応組織の行為は相互作用しており、人々がガイドラインをどのように認識しているのか、また実際に何を行っているのかという視点からの研究によって、情報セキュリティ組織に対してより重要な示唆を得ることができると考えられることが解明された。

(2) 組織の継承プロセスについて

組織の継承、とくにマニュアル化しにくい技能を扱う組織や事業はいかに継承されるかといった問題は、情報セキュリティ特有の問題ではなく、多くの企業や組織に関連する問題であるといえる。もし、その技能がある世代の個人から次の世代へ引き継がれない、あるいは引き継ぐことが困難である場合、組織や事業も継承できないということになりかねない。そのような中で、どのようにそれが継承されるのか、そのプロセスを明らかにした。

本研究成果は、(1) の実践論的な転回に基づき、技能を受け継ぎたいと考える個人がどのように技能を授けたいと考える個人とともに実践しているのか、ケースをもとに明らかにした。たとえば、ケースにおいては「よくわからないながら、何回も同じ行動を繰り返す」といったことが述べられ、技能が身につくまで、再起的に自分(達)がしていることについてわかる(意味付けされる)といったプロセスが明らかになった。もともと、実践に基づく学習は、Lave & Wenger (1991) や Wenger et al. (1998) などに代表される「実践を通じた学習」や「実践コミュニティ」といった概念から議論されてきた。この研究成果でも、それらの既存研究にあった現象と同等の事象が見られることが明らかになった。他方で、これらの研究成果に付け加えて、これらの人々が自分たちの持っている技能をどのように認識しているか、そしてその認識に至ったプロセスが明らかになった。

(3) 本研究成果の公表

これらの本研究成果は、国内の学術雑誌における論文投稿および、国内外の学会において報告された。

本研究成果は日本企業における CSIRT (Computer Security Incident Response Team: 企業内に設置されるサイバーインシデントに対応するチーム) の継承はどのようなプロセスを経て行われるかと明らかにすることを目的として定性的な実証研究に取り組んだ結果である。しかし、本研究課題がスタートした 2020 年度は、本研究課題の申請を行った 2019 年度の社会的状況とは全く異なるものであった。それは新型コロナウイルスの蔓延に伴い、多くの国内の経営組織で業務のオンライン化が急速に進展したということであり、それは 2019 年度の本研究課題の申請の時には全く想定できなかったものでもある。同時に、情報セキュリティの問題はより重要な経営課題となり、本研究の意義はさらに増し、本研究課題をさらに拡張する必要があることが社会的背景から要請されている。

また同時に情報セキュリティ体制を強固にすることばかりに執着することによって、通常業務の非効率になることも指摘され始めている。組織の人々をサイバーインシデントから守るための訓練が、むしろ組織の人々の日々の業務を圧迫している などの問題である。

本研究課題が遂行されている間、組織のイノベーションなどを促進する要素として心理的安全性といった概念が注目されるようにもなった。この概念は、組織をサイバーインシデントから守る概念としても重要である。今後は、さらに経営組織をサイバーインシデントから守りつつ、組織の効率性を両立し、社会および学術的な要請にこたえられるよう研究をすすめることを予定している。

5. 主な発表論文等

〔雑誌論文〕 計1件（うち査読付論文 1件 / うち国際共著 0件 / うちオープンアクセス 1件）

1. 著者名 寺本直城	4. 巻 118
2. 論文標題 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	5. 発行年 2020年
3. 雑誌名 経営経理研究	6. 最初と最後の頁 43-57
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 -

〔学会発表〕 計1件（うち招待講演 0件 / うち国際学会 0件）

1. 発表者名 深見嘉明・中村暁子・福田大年・寺本直城
2. 発表標題 珈琲焙煎プロファイルデータによる製品開発と組織形成
3. 学会等名 2022年度経営情報学会九州・沖縄支部 & 組織ディスコース研究部会合同研究発表会
4. 発表年 2023年

〔図書〕 計3件

1. 著者名 高橋 正泰	4. 発行年 2022年
2. 出版社 文真堂	5. 総ページ数 260
3. 書名 経営組織論のフロンティア	

1. 著者名 高橋 正泰、木全 晃	4. 発行年 2022年
2. 出版社 文真堂	5. 総ページ数 272
3. 書名 組織のメタファー	

1. 著者名 経営学史学会、風間 信隆	4. 発行年 2022年
2. 出版社 文真堂	5. 総ページ数 247
3. 書名 合理性から読み解く経営学	

〔産業財産権〕

〔その他〕

-

6. 研究組織

氏名 (ローマ字氏名) (研究者番号)	所属研究機関・部局・職 (機関番号)	備考

7. 科研費を使用して開催した国際研究集会

〔国際研究集会〕 計0件

8. 本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関