審査結果報告をうけて

論文「サイバーセキュリティにおけるインシデント対応コミュニティの発展 ―目的、機能、文化から見る CSIRT―」(受付番号 31-7)についての 2019 年 5 月 22 日付けのメールありがとうございました。論文の価値を認めていただいたことを大変嬉しく思います。また、論文を良くするための貴重なコメントをありがとうございました。ご指摘に基づいて、論文を以下のように改定いたしました。

本文書は査読者から頂いたコメントを引用し、その下に返答を書いております。

査読者 A

> 先行研究に比して筆者が互恵主義を CSIRT 文化の中心と捉えなおすためには事例（実証研究）についてさらに具体的な根拠を示した論述が必要であると考えられる。具体的には 12 頁 5.2 の「互恵主義の発露」の部分の論述であり、歴史的事実等の論拠、出展を示すことでより論理が明確になると考えられる。

ご指摘ありがとうございます。先行研究が 4 つの文化を見出した中、そのうちの 1 つである互恵主義のみを取り出した点については脚注に補足説明を加えました。(修正ポイント脚注番号 11 を参照)

また互恵主義が現在も国際的な CSIRT コミュニティに「みられる」だけでなく、「明文化され半ば義務として期待されている」ことがより明らかに伝わるよう、p12 に運営理念にも「メンバー間の助け合い、集合知の活用をミッション・ステートメントにかかげている」ことを追記しました。

> また、細かな点であるが、7 頁 6 行目～7 行目、「この中で本研究が着目するのは、サイバー空間における被害者の救済と復旧を目的としたグループである。インシデント対応というグループに分けることができる。」の部分は記述ミスと思われるが、論理がつながらなかった部分である。

ご指摘ありがとうございます。「インシデント対応というグループに分けることができる。」の文を削除しました(p7 修正ポイント B 参照)

査読者 B

> ① 多くの読者，特にインターネット技術者などにも理解が可能なように，組織の概念の規定することの意義を述べてください．

ご指摘ありがとうございます。CSIRT の持つ科学的知識を政策に取り入れていく必要は

繰り返し主張されていますが、その際に CSIRT とは何であるかの自己紹介ができる必要があるという趣旨で修正を行いました。(p6 修正ポイント A 参照)

② 目的，機能，文化というレンズを通すことの必然性を明らかにしてください.

ご指摘ありがとうございます。目的、機能、文化のレンズの妥当性に関するご指摘ととらえました。このレンズを通せば図表 3 に列挙した各種グループと CSIRT の違いを明らかにできました。5 章 3 節に記した ISAC など類似のレジームとの境界の不明瞭さの問題を除けば妥当と考えています。

③ 本論文であげる CSIRT は，国家 CSIRT のことと読めますが，組織（企業内）CSIRT ではないことを明示してください．企業内 CSIRT も互恵主義を特長とします.

ご指摘ありがとうございます。本論文では単に CSIRT と言った場合、組織内 CSIRT も含みます。明確にわかるように p16 脚注 2 に本論文で単に CSIRT と言った場合はそれらすべてを含むことを追記しました。

④ 目的における被害者の救済と復旧は，論文にもありますが，30 年前の目的と想定されます．これを現代の CSIRT への目的に当てはめる必然性を明らかにしてください．組織は，環境の変化により変化していくものであるため，現代の CSIRT の目的をもって概念化する必要があるのではないでしょうか.

ご指摘ありがとうございます。目的の経年変化への着目という大変重要な指摘と捉えました。筆者自身が FIRST 年次会合(2013-2018)に参加し参与観察を行った経験からは、目的に変化は見られませんでした。加えて、2014 年の IGF、2014 年の Bradshaw の研究なども、「CSIRT とは被害者の救済やインシデントからの復旧を目指す組織」と定義しており、本論文では現代の CSIRT も目的は被害者の救済と復旧であり、それを使って概念化を行っていると考えます。

⑤ リスク社会において，サイバーセキュリティに関するインシデント対応能力として，CSIRT を設置することは，リスクの共有化を図ることが重要な論点になります．リスクを発見し制御するには，リスクの共有化が重要です．本論文における組織概念を規定する際に，リスクの共有化が含まれていないことに違和感を感じます．この点の著者の考えを述べてください.

ご指摘ありがとうございます。リスク共有は極めて重要な課題と認識しています。とりわけ CSIRT は 3 章 2 節に書いたとおり、その発足の動機自体がリスクの共有にありました。このことがより明確に伝わるよう修正を行いました。(p8 修正ポイント C)

本研究の文脈におけるリスク共有とは、インシデント対応なりサイバー攻撃者の検挙・訴追なり、技術の標準化を適切に行うための手段と捉えます。政府も、情報機関も、警察も、市民活動家も、それぞれの目的を達するための独自のリスク共有を既に行っていると捉えると、リスク共有は CSIRT に固有のものとは言い難く、概念化の条件に入れるのは難しい

と考えました。

また上記変更によって増えた字数を削るため、脚注４と６を削除しました。