	オオタ　ユイタカ
氏　　名	**太田　結隆**
学位の種類	博士（工学）
学位記番号	博第1252号
学位授与の日付	2022年3月31日
学位授与の条件	学位規則第４条第１項該当　課程博士
学位論文題目	Human Resource Development to Improve Organizational Resilience to Cyber Incidents （サイバーインシデントに対する組織的レジリエンス向上のための人材開発）
論文審査委員	主査　教授　橋本　芳宏 教授　渡辺　研司 教授　荒川　雅裕 教授　山下　善之 （東京農工大学）

論文内容の要旨

Chapter 1:

In this chapter, based on the cyber incidents that have targeted ICS so far, we will explain the reality that cyber-attacks threaten the safety of ICS..

Chapter 2:

In chapter 2, based on the research background described in Chapter1, I will propose that organizational structure and ICS- BCP required to respond to cyber incidents be developed.

I will also present the elements required for companies to respond to cyber incidents and describe the issues involved in achieving them.

Chapter 3:
In this chapter, I categorize exercises for experiencing cyber incidents in ICS and explain why I developed two types of exercises.
The exercise we developed can be categorized into two types.
The first is an exercise focusing on simulated experience, in which we use a testbed owned by our laboratory to deepen exercise participants' understanding of the impact of cyber-attacks on ICS and the actual possible field-side action of the operators in the field.
The second is a simulation-type exercise in which participants simulate a response to a cyber incident as a member of a virtual company and discuss how to look at things to respond to a cyber incident.
The purpose and implementation of each exercise, as well as the framework developed to design the exercise, will be explained.

Chapter 4:
In this chapter, I will explain the method of human resource development using the exercises described in Chapter 3, and the human resources needed to manage and develop the exercises. It also explains the mechanism for improving the exercises.

Chapter 5:
This chapter describes the exercises we conducted based on the exercises and exercise implementation methods presented in Chapters 3 and 4. It also shows the new findings obtained by analyzing the exercise results and the feedback from exercise participants.

Chapter 6:
This chapter will summarize what has been discussed in this paper to solve the problem set in chapter 2.

Chapter 7:
n the final chapter, I will conclude this study and discuss the remaining works to be studied in the future.

論文審査結果の要旨

本論文は、現在、サイバーリスクに晒されているプラント、ICSを対象に挙げており、今後、ますますサイバーリスクが強まりつつある環境の中で企業のビジネス継続とプラントの安全、国民の生活に関して、サイバーインシデントを起こさない環境づくりだけではなく、サイバーインシデントが発生してしまったとしても被害を最小限にするための組織および人材開発という観点で重要な視点を提供するものと考える。

この分野は、従来から安全への意識が高く、長い間安全について様々な研究が行われているという特徴がある。しかし、その安全を脅かすリスクとして近年サイバーリスクが強まってきている。サイバーリスクはICSよりも、情報漏洩・暗号化などのIT分野での研究が進んでおり、ICSにおけるサイバーリスクを題材としている研究は少ない。また、いくつかの研究ではサイバーリスクつまりサイバー攻撃を受けないための環境づくりに焦点を当てている。今までの安全への意識としては、不安全な状態にしないようにする、つまり、インシデント発生前に焦点を当てた考え方となっている。全てのサイバー攻撃を防ぐことができないという大きな課題を抱えているにもかかわらず、ICSセキュリティの分野でサイバーインシデント発生後の対応を取り扱う研究は少ない。また、ICSへのサイバーリスクが強まってきたのが近年であるため、殆どの人にとってサイバーリスクがICSへ与える影響を理解できていない。

そのため、研究室で保有しているテストベットを題材としサイバー攻撃を自身の手で行うことでサイバー攻撃がICSへ与える影響を整理し、ICSでサイバーインシデントが発生した場合の被害を最小限にするためのアプローチとして「サイバーインシデントへ強い組織づくり」と「人材開発」の二つの観点で必要なアプローチを整理した。

これら「組織づくり」と「人材開発」の重要性を理解してもらうためには、まずはICSにおけるサイバーリスクがどのような影響を与えるのかを理解してもらう必要があり、また「組織づくり」と「人材開発」はそれぞれの企業の特色が強く反映されるものである。従って、ICSのサイバーリスクを認識してもらうとともに、まずは理想の組織・人材を議論できるように演習というアプローチを行った。

この演習では、ICSでのサイバーリスクを自分事と捉え、主体性を持って物事に取り組んでもらうために、自分の目で見て、自分で考え、自分の手を動かすことに焦点を当てている。この演習では、俯瞰的にこの問題について議論ができるようにシンプルなシナリオで構築することによって、ICSでのサイバーリスクのイメージがしやすく、そのリスクに対応するために必要となりえる組織およい人材育成について、議論・検討できるような知見を得るものとなっている。

申請者は、プラントを建設するエンジニアリング会社に勤務しており、この研究成果を基に、サイバーインシデントに強いプラントづくりにも活用する機会があり、この研究は、新規性が高いだけではなく、実用性も高いものと考えられ、今後の展開が期待される。

審査委員会は、この研究を、博士(工学)に充分値するものとして評価した。