	アオヤマ　トモミ
氏　　名	**青山　友美**
学位の種類	博士（工学）
学位記番号	論博第304号
学位授与の日付	2019年12月18日
学位授与の条件	学位規則第４条第２項該当　論文博士
学位論文題目	Control Systems Security and Communication- Achieving Organizational Resilience through Exercise （制御システムセキュリティとコミュニケーション- 演習で実現する組織レジリエンス）
論文審査委員	主査　教授　渡辺　研司 教授　荒川　雅裕 教授　齋藤　彰一 教授　大林　厚臣 （慶應義塾大学）

論文内容の要旨

This thesis aims to propose the model for cyber security exercise design proportional to the maturity of the organization. This thesis is composed of six chapters, each of them dealing with the different aspects of cyber security design and execution.

Chapter 1: Chapter 1 is introductory and describes how cybersecurity risk becomes more and more relevant to industrial systems and critical infrastructures and its potential impacts.

Chapter 2: In this chapter, we examine the available resources to understand the trends and definition of the field. The chapter consists of 3 sections. Section 1 reviews the literature in the related field to define exercises. Section 2 investigates current ICS security exercises available in the field. We discuss the limitation of the conventional approach. Section 3 illustrates the trends specific to the Japanese market and what makes it peculiar.

Chapter 3: The interaction between two parties makes cyber incident response unique in comparison with natural hazards. We discuss the uniqueness of the filed from three p

perspectives; 1) the time-lag of the adversarial interaction, 2) the shift of focused activities, and 3) the management challenges. In this chapter, we investigate the nature of incident management by observation studies at a large scale adversarial exercise.

Chapter 4: ICS security exercise should be designed and applied proportional to the organization's preparedness. This chapter introduces the model to be applied to design the exercise from three axes: exercise participant, exercise style, and the goal of the exercise. The chapter illustrates how exercises can play the role of a driving power to improve an organization and community's cyber security preparedness. We discuss the details for how the model should be applied to understand the existing exercises. It highlights the limitation of current cyber security exercise landscape.

Chapter 5: Achievement of a secure and resilient society requires a shared protocol among stakeholders. Even within the organization, cyber incident communication is a challenge because of the conflicting value of safety and security. We designed the training program specifically to address this problem in align with the maturity-based exercise model presented in chapter 4. This chapter shows the illustrative example of the exercise design and implementation. With one set of the testbed, we illustrated that exercises can be tailored to specific preparedness. The details of conducted training program elements were provided.

Chapter 6: Conclusion
This interdisciplinary study was based on an investigation of both organizational behavior and exercise management. Discussion-based exercise tailored to the organizations' maturity cultivates a shared mental model among participants. We conclude that exercises can play the role of a driving power to improve an organization and community's cyber security preparedness. In this chapter, we conclude the study by discussing the exercise management implications, the research implications, and the implications for the organization behavior.

論文審査結果の要旨

申請者青山氏は政府、セキュリティ専門組織、重要インフラ事業者などからの依頼に基づく、政策立案支援、演習実施・評価、海外調査などを通じ得られた幅広い経験と専門性の高い知見に基づき、社会経済を支える重要インフラ事業における制御システムのセキュリティの取り組みを分析し、その限界を明らかにし官民全体のインシデント対応における問題点を示すと同時に、訓練と演習の組み合わせによる設計と実施を通じた、制御システムのセキュリティと組織内コミュニケーション体制の強化、そしてその結果として組織のレジリエンス向上を実現する枠組みを提案した。また、その枠組みに基づき開発したトレーニングプログラムを実証結果と共に示し実効性を明らかにした。

本論文は、組織の成熟度に応じたサイバーセキュリティ演習を設計する枠組み提案することを目的としている。また、７つの章で構成されており、サイバーセキュリティ演習の設計と実行について結論を導くために必要な各要素の考察が各章で展開されている。

第１章は序章として、産業システムおよび重要インフラにおけるサイバーセキュリティリスクの台頭と影響の可能性について、幅広い現状分析を通じその課題について論じている。

第２章では、セキュリティ演習の定義と現状の調査・分析に基づく「あるべき姿」の考察を展開している。本章は3つの節で構成され、まず最初に関連分野の先行研究・文献他のレビューを通じて演習を定義している。次に現在、制御システム分野で用いられている主要なセキュリティ演習の調査・分析に基づき、従来のアプローチの限界について論じている。そして、最後に日本における実装に求められる特有な要素を明確にとりまとめている。

続く第３章では、サイバー事案対応は、自然災害対応とは異なり攻撃側と防護側との相互作用が影響することが特徴であることを述べた上で、以下３つの分析を通じて、技術面のみならず組織のマネジメント能力が重要であること、更にはコミュニケーションとタスク管理がレジリエンス向上のボトルネックになっていることを明らかにした。1）タイムラインの不均等性、２）対応体制の動的変化、３）マネジメントにおける問題抽出。

そして第４章では、制御システムセキュリティ演習の内容と組織の成熟度の関係が明らかになっていない課題に対し、事業者が成熟度に合わせて演習を俯瞰的に選択できるモデルを提案した。さらに、成熟度向上のために異なるタイプの演習を組み合わせて段階的に実施するプログラムを提案している。

更に、第５章では第４章で提案された成熟度に合わせた演習設計の枠組みを用いて、演習プログラムを計画・実行する方法について、同じ組織内であっても、安全性とセキュリティの価値が相反するような状況をコミュニケーションにより解消しながら対応する事例を、実際に開発・実施された演習を用いて検証・考察している。

そして最後の第６章では、１）制御システムのセキュリティ確保において、IT部門・制御システム部門と経営層のコミュニケーションが課題である、２）演習・トレーニングは単体で行うのではなく組織の成熟度に合わせた複合プログラムとして計画すべきである、３）レジリエンスの獲得・向上にはAwareness（啓蒙）、Preparedness（特定シナリオへの準備）が地盤として必要である、と結論づけた。

本論文は制御システムのサイバーセキュリティ演習が体系だって行われていない状況は、サイバー攻撃リスクが台頭する状況においては喫緊の社会的課題であると位置づけ、課題の要素分解とその解決に必要な枠組みとツールを開発・統合して提案することで、今後のあるべき姿を実効性の高いモデルとして示したものであり、本分野の更なる発展に寄与するところが大きい。よって、本論文は博士（工学）の学位論文として十分に値するものと認める。