Graduate School of Science and Technology Doctoral Thesis Abstract

Laboratory Name (Supervisior)	**Cyber Resilience (Youki Kadobayashi (Professor))**		
Student ID	**2121429**	**Submission Date**	**2025/6/24**
Name	**MOHAMMAD HAFIZ HERSYAH**		
Thesis Title	**Towards a Risk-Secured Container Ecosystems in Cloud Environment: A Study on System, Human Insider and Human Capital Perspectives** クラウド環境におけるリスク保護されたコンテナ・エコシステムの構築に向けて：システム、内部関係者、人的資本に関する研究 視点		

Abstract

In today's evolving cloud computing landscape, ensuring robust security involves more than just managing software tools like Docker containers and Kubernetes. While foundational to cloud infrastructure, these technologies must work in harmony with the human element, often called "humanware." This convergence of software, hardware, and human behavior forms the backbone of modern cybersecurity defense, especially in containerized environments where insider actions can significantly shape security outcomes, whether intentional or accidental.

This dissertation's core is a comprehensive exploration of risks inherent in container-based systems, beginning with Docker environments. While containers are widely praised for their scalability and efficiency, they also introduce unique vulnerabilities stemming from dynamic threat vectors. This study undertakes a methodical risk assessment of Docker deployments by applying established standards and frameworks such as ISO/IEC 27000, ISO 31000, NIST 800-30, and the MITRE ATT&CK matrix. The aim is to understand the security posture from both technical and procedural standpoints and to derive practical mitigation strategies that are actionable in real-world implementations.

As orchestration shifts toward Kubernetes, new challenges emerge. The initial risk assessment reveals critical gaps, especially concerning adversarial tactics such as privilege escalation, lateral movement, and persistent access. These threats often exploit the complex nature of Kubernetes, highlighting the limitations of traditional risk management approaches in fully capturing the intricacies of orchestrated container environments.

Recognizing that cybersecurity extends beyond technical infrastructure, the study next delves into insider threats: one of the most underestimated aspects. It specifically examines how behavioral science intersects with security by analyzing personality traits associated with the Dark Triad—Machiavellianism, narcissism, and psychopathy. Utilizing machine learning techniques such as Random Forest, XGBoost, and Support Vector Machines, the study identifies behavioral patterns that may indicate elevated internal risk. This analysis helps shape a predictive framework capable of identifying potential insider threats before they escalate into incidents.

The dissertation proposes a multi-attribute risk assessment model to address the layered complexity of modern container environments. This model integrates Fuzzy Analytic Hierarchy Process (Fuzzy AHP), the Domain Mapping Matrix, and Fuzzy Logic to provide a nuanced evaluation of risk levels. It supports more accurate prioritization of mitigation efforts, particularly for threats associated with Kubernetes environments. The framework is designed to reflect real-world adversarial behavior, including tactics like data destruction, endpoint and network denial of service, system recovery inhibition, and resource hijacking, all mapped from MITRE ATT&CK.

Beyond technical solutions, the research emphasizes the critical role of human-centric cybersecurity training. A tailored program based on the KEMP instructional design, ARCS motivational model, and revised Bloom's taxonomy was developed to bridge the gap between theoretical knowledge and practical application. Delivered through both local servers and public cloud platforms, the program aims to build essential skills in risk analysis, decision-making, and cybersecurity investment evaluation. Its effectiveness is measured through participant feedback and statistical analysis, revealing significant improvements in technical capability and security awareness.

In summary, this dissertation advocates for a holistic security approach that combines technological sophistication with a deep understanding of human behavior. By addressing the interdependencies between software, hardware, and humanware, the research lays out a strategic roadmap for securing containerized infrastructures. The findings reinforce the importance of aligning human capital development with technological innovation, offering practical guidance to organizations navigating the increasingly complex terrain of cyber threats.