INFORMATION
Volume 19, Number 5, pp.1549-1555

ISSN 1343-4500

Construction of Port Logistics Security System based on the Information Security Management System

Jae-Hoon Sim* and Gyusung Cho*

**Department of Port Logistics System, TongMyong University, Busan 608-711,Korea*
E-mail: gscho@tu.ac.kr

Abstract

The port logistics industry has been seeing rapid growth due to development of IT technology. However, it also has come with new problems of security threats. Even though information crime like hacking and cyber terror is getting serious, port management plan for the threats is still not enough. Existing security system is only focusing on physical field, but also various side effects can occur, because it has designed without consideration for the distinct characteristics of port logistics. Therefore, we need a new port security system that specialized in port. In this paper, we consider the Port Logistics Security System (PLSS) based on the Information Security Management System (ISMS) and we apply the PLSS to Automated Container Terminal System.

Keywords: Port Logistics Security System, Automated container terminal, Physical Security Systems, Technical security system, Information Security Management System.

1. Introduction

Port logistics industry began to form an unprecedented remarkable development. Various state-of-the-art equipment is beginning to be applied to the logistics field, In particular, the Port of Rotterdam in the Netherlands appeared to start is automated container terminal cost savings, improved stability, improved processing speed, etc.[1-2]. There are considerable advantages over the existing container terminal. However, port, along with advances in technology, now has a new problem that security threats. Automation, only the proportion of unmanned technology has increased a substantial portion, damage caused by security threats will increase significantly.From the aircraft terrorism that happened, not only the United States is a direct affected countries, other countries also began to introduce some of the system related to the logistics of security. Requests for logistics security, is greatly enhanced with individual countries and international organizations, logistics security, has been fixed to now the trend.Of course, in the domestic logistics security it is actively going on. However, Contrast the developed IT skills, Education and awareness of the port for security threats is still a state that is not enough. Dealing with security incidents not even a manual and systematic. In addition, national security plan, because it is designed to be able to apply to all occupations, it may not be suitable for looking at the specificity of the port[3-4]. Therefore, to solve this problem, there is a need to rebuild the port logistics security. This paper shows the

framework of Port Logistics Security System based on the concept of Information Security Management System (ISMS) and a construction plan of Port information security.

2. Definition of Port Logistics System

2.1 Automated Container Terminal

Definition of Automated container terminal is "Ship of the core processes of container terminal operators unloading operations, transfer operations, automates some or all of the yard work terminal device" andsimply, it is an unmanned operation facility without any human interference and access.At a rate of existing labor costs in an automated container terminal operating costs 25%, lower nearly half than the 45% of the existing container terminal. Investment expenses were 116%, higher and operating costs compared to conventional container terminal is cheaper than 16% to from three to four years later after the terminal doors open can to recover the investment, it is very economical [5].

2.2 Port Logistics Security Systems

Generally security means to protect the state from causing crime, danger and loss. Port logistics combined with port and logistics mean distribution activities in port such as carrying trade. Therefore, port logistics security systems are to protect distribution activities from danger and loss during operating, and when occurred serious situations, it is to secure as quick perform subsequent recovery restoration [6].

3. Construction of the Port Logistics Security Systems

In this study, it was classified separately in the physical security and technical security two of port logistics security system. Security of the port, there is a tendency to focus on only the physical security, such as installation of the fence and lock so that we intend to deal with hacking, also technical security to protect against security threats such as DDos attack [7].

3.1 Physical Security Systems

Physical Security Systems means that to secure property, information and facilities against various hazards such as fence, personnel expenses, CCTV and even defense manpower [8]. To establish this system, IT equipment is essential. Recently, rising in the logistics industry assignment is balanced with the logistics of security and logistics efficiency, it is also excellent work with equipment utilization in security aspect, and can be achieved by efficient logistics solutions to simplify, as well. The equipment is mainly used in harbors, RFID and E-seal; there is a CSD (Container Security Device). The tag identification technology is to

identify the tags attached to goods and containers that are stacked in the port by radio, you can check the information of the product, for example, by detecting the ambient conditions and processes the necessary data it is a technique. Since the container can know visible different movements invalid or has been opened and closed in a manner, or predetermined routes, but it has significant advantages in terms of security. It requires integration with information and communication systems, besides and there must be security system be build associated with. Security equipment.

(1) Facility Security

The Facility Security part includes access control, Information Security Area, In and out of external equipment, and Public security work environment.Most core facilities of the security are a security. The automated container terminal, of course, there is a monitoring device, such as a closed circuit television, both machines may not be able to complement all the parts. By various laws and regulations, but the demand for security personnel have continued to increase, personnel in charge of this are the reality is missing. It is necessary to budgeting associated with the port security personnel recruitment, at night; monitoring and recording by CCTV should be conducted.

(2) Cargo Security

The Cargo Security part includes Establishment of cargo transportation procedures, Establishment of transportation security, Cargo inspection and tracking, Inspection of container, Seal and security of container. RFID-based tag identification techniques, by attaching a tag to the cargo and the container is intended to be detected automatically recognize information of an object by wireless communication using at reader a certain frequency band. Attached tag information can be used to recognize the information of the surrounding environment; it is possible to check the abnormal opening and closing of the container. Collect these tag information, and can establish a cargo security system without like to be processed.

(3) Equipment Security

Equipment security is the first-priority project to utilize IT equipment. Especially, RFID can be exposed to malevolent threatening element during mutual authorizing process, because it has to use wireless channel. Like weakness of RFID skill can cause serious problem related to security information of group and protecting personal privacy safety.Therefore, we should use mutual authorizing system to be able to guarantee security in back-end database saved and managed information of reader.

3.2 Technical Security System

Technical security means technical methods to protect damage, falsification and outflow of information from external threats such as hacking, virus, DDoS attacks and cyber terror. Establishment of technical security system is an urgent issue in port at the moment, as container terminal has changed from existing to automated skill based on IT [9]. The most important part of the technical security system is a configuration of a crisis procedures can be applied when a situation of the violation takes place. It constitutes procedures for crisis response that can be applied to the port by utilizing each step of response procedures for the management system of information protection. Setting of specific crisis response procedures, framework of the security system, will be able to respond proactively than when security breach accident.

(1) Port Emergency Response Procedures

The Port-DRP has configured in the crisis response procedures suitable for crisis response procedures of each stage of the existing information management system in port. Establishment of specific crisis response procedures, framework of the security system, will be able to respond proactively than when security breaches accident. Crisis response procedures of existing information protection management system, there are some differences in the configuration Steps and name as necessary and characteristics of each organization. but, In general, prevention → detection / analysis → response → recovery, such as 4 stages you are running by easily configure. In Port-DRP, detection reception, analysis / response, is divided into three stages of the processing / reporting, it was further subdivided in the analysis / response phasesuch as fig 1.When the first infringement accident reported or detected infringement accident was has been received, immediately analyzes the type of infringement accident and determine the priority. Beforehand to be defined the type of infringement accidents through the IT systems, such as Rule-base and expert system. When analysis process is processed via a computer system, it is possible to significantly save the time to understand the problems when the accident occurrence. Since the past problems after the occurrence, the record is stored in a database, reliable. After infringement accident analysis finished and then proceeds immediately, attack type response procedures selection stage. Malware, DDOS attacks, unauthorized access attacks, such as a composite structure attacks, and to understand the type of the corresponding security attacks, and a security measures associated with it can be established quickly. At this point, you need to be able to use the features of Automatic shut-off through the artificial intelligence technology of the IT system. When the malware code attack is detected, immediately, disconnect the connection of the

Internet and to start tracking by searching the entry pathway.

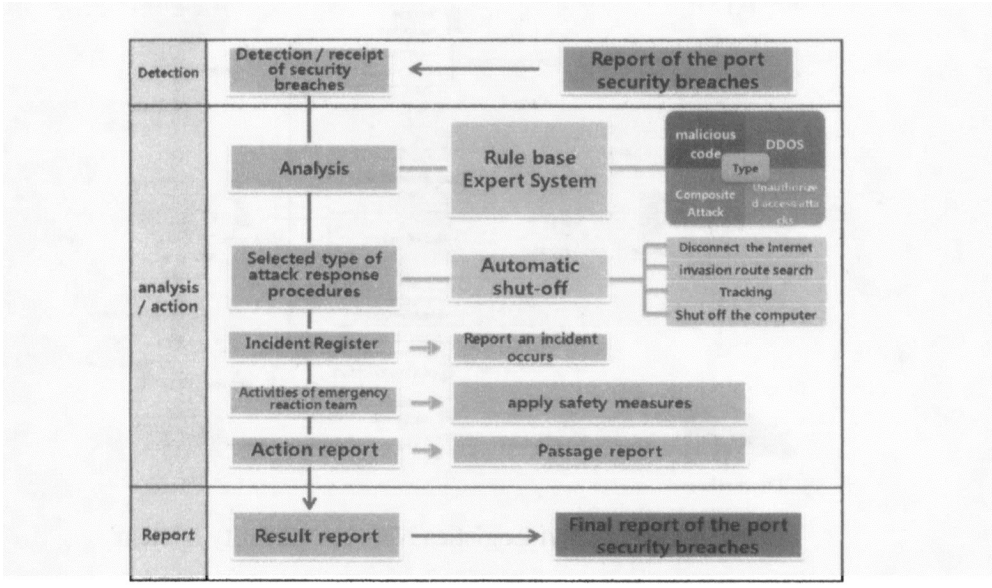

Fig 1. Emergency Response Procedures of Port Logistics Security System

(2) Port Logistics Network Security System

Port logistics network security system is a security infra available to be security mandatory of terminal device approached at port network. According to expansion of wireless network infra and development of smart device, lots of employees in port are utilizing business use or application of cellphone at work. However, such terminal devices are always exposed to security threats. Port logistics network security system is an automatic control system to assure and hold back for terminal device security that connected or continuous monitoring according to security policy. In Fig 2, the work of the port terminal can be divided largely into two dropping work and Unloading work, more detailed instructions, ship docked -> Unloading work -> yard move -> yard work -> is a work completion report.In this case, the worker, via a terminal that holds for each major work is to report to the control center, in the center, assign a work order and location of the information to the worker in the control system. In this case, data received from the outside must undergo beforehand check procedures comply with the security policy.

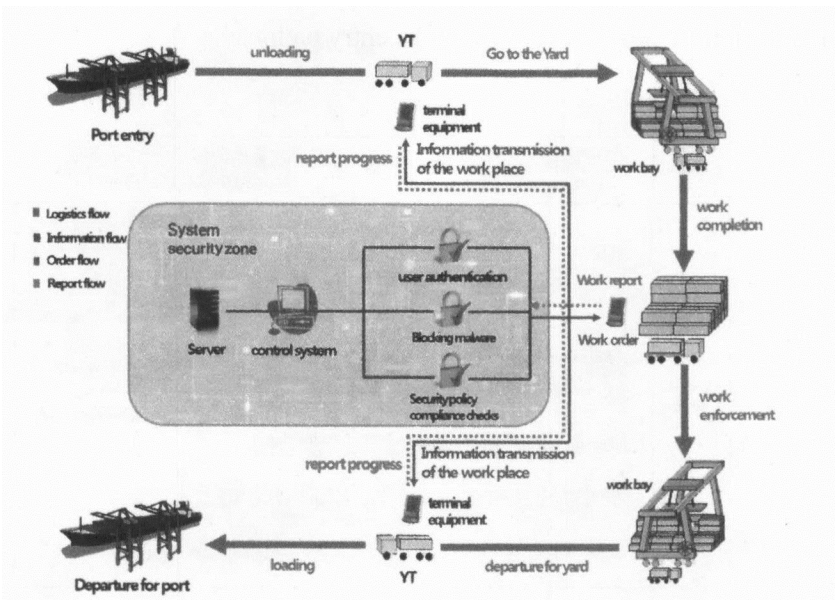

Fig 2. Concept of Port Logistics Network Security System.

4. Conclusions

In this study, we have tried to re-format from traditional information security management system to specific port logistics information security system. There are merits that not only handling focused on physical security from the past, but also considering about technical security to protect threats such as DIDOs attack and hacking. Recently in logistics industry, security system is balanced with protection and efficiency and to ensure customer reliability through the visibility of accuracy and can be achieved by efficient logistics solutions to simplify. We hope security of port is look forward improving better than now through considered security system not only physical, also technical, and as re-think about domestic port security.

5. Acknowledgments

This work was supported by the ICT-PL Convergence Grants of Tongmyong University based on the National Research Foundation of Korea(NRF) grant and the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIP) (No. 2015R1D1A1A01061115).

References

[1] Ko, H.J., A Study on the Implications and Trends of Logistics Security Assurance Programs for International Trade Facilitation, *Journal of Korea Port Economic Association*, 27(2011), 333-354.

[2] Kwon, K.H. and Kang, J.Y., Thoughts on Security System to Ensure Safety of Port

Logistics, *Soongsil Law Review*, 29(2012), 301-322.

[3] You, J.M. and Park, I.K. Android Storage Access Control for Personal Information Security, *The Journal of the Institute of Internet, Broadcasting and Communication*, 13(2013), 123-128.

[4] Sim, J.H., Ha, K.H., Choi, Y.H., Kim, H.Y., Bakker, J.S. and Cho, G.S., A Study on Construction Plan of Port Logistics Security System for Automated Container Terminal, *Advanced and Applied Convergence Letters* (2015).

[5] Kim, S.E., Choi, J.H. and Kim, C.H., A Study on Measures to Develop the Port Logistics Security Industry,*Research project report of Korean Maritime Institute,* (2009).

[6] Lan, H.P., Toan, L.B., Nguyen, H.T., Khuong, N.A. and Minh Man, N.V., An Approach for Scheduling Problem in Port Container Terminals: Moving and Stacking, *International Journal of Internet, Broadcasting and Communication*, 7(2015), 1-5.

[7] Kim, S., Compatibility Analysis between Security Tactics and Broker Architecture Pattern, *The Journal of the Institute of Internet, Broadcasting and Communication*, 15(2015), 19-24.

[8] Kumpanya,D. and Thaiparnat,S., Real Time Electrical Energy Computing Tool, *International Journal of Advanced Culture Technology*, 3(2015), 113-119.

[9] Lee, K.C., Moon, S. J., Lee, J. Y. and Jung, K.D., Design of Integrated Medical Information System Based on The Cloud, *International Journal of Advanced Smart Convergence*, 4(2015), 88-92.

*Corresponding author: Gyusung Cho, Ph.D.

Department of Port Logistics System, Tongmyong University, 428, Sinseon-ro, Nam-gu, Busan, 608-711, Republic of Korea.

E-mail: gscho@tu.ac.kr