DDoS Correspondence Index for Evaluating Performance Management

Hyung-Won Kim, Nam-Yong Lee and Jong-Bae Kim, *Member, KIMICS*

***Abstract*— The damages from DDoS attacks are increasing as DDoS attacks are taking various forms. This has resulted not only in decreased reliability of organizations and corporations but also in the threat of national security. Organizations and corporations are making significant efforts in developing a system through which they can appropriately correspond to DDoS attacks. However, the studies on objective index for evaluating the performance of DDoS correspondence are lacking. The majority of the existing studies have been on the information protection & management system on a large scale.**

Accordingly, the scope of this thesis will be limited to DDoS correspondence to propose correspondence index for quantitatively measuring and managing them. The statistical techniques such as SMART technique and factor analysis will be utilized accordingly.

***Index Terms*— DDoS, Correspondence index, performance of DDoS**

I. INTRODUCTION

IN recent, DoS (Denial of Service) attack or DDoS (Distributed Denial of Service) attack is increasing. What is more serious is that such DDoS attack techniques are evolving and becoming more advanced [1].

After July 7, 2009, the government has been implementing the government-wide DDoS correspondence system development project for each ministry and office under the major theme of "Hacking Virus Response Advancement" through its significant increase in the budget, and seeking to introduce necessary equipment and software for the information protection task. In addition, private companies such as ISPs (Internet Service Providers) have been also inspecting their response system and reinforcing equipment, solutions and staff under the general command of Korea Internet & Security Agency (KISA).

However, they are being passive in making continuous investments due to the absence of detailed and objective measurement standard for the effects and efficiency according to the characteristics of information protection system.

Although the evaluation or certification task on information protection and management system is underway in recent, it only presents general guidelines or standards on information protection and management system. Accordingly, the current circumstance is that it is difficult to utilize them as the index for understanding the level of development of DDoS correspondence system or the effectiveness of response system or quantitatively measuring the performance.

Accordingly, DDoS correspondence index that allows objective measurement will be set in this study and the metric through which the index can be measured and managed will be proposed.

II. RELATED WORKS

In the aspect of information protection evaluation, the existing studies are mainly divided into two approaches. The first approach is a system of evaluation that centers on the security function and performance aspect of product/system such as TCSEC (Trusted Computer System Evaluation Criteria) and ITSEC (Information Technology Security Criteria). Such existing evaluation standard is limited in its flexibility from mainly using evaluation standard per product as it cannot evaluate various products required in the private sector [2][3].

The second approach is a system of evaluation that centered on the managerial aspect such as ISO 27001[4] and ISO 27002[5]. Especially, ISO 27001 and 27002 are based on BS7799 developed for the purpose of being used as common document that can be referred by the managers responsible for organization information security and maintenance, and they have been designed to be the foundation of organization security standard. Accordingly, there is an issue with ISO 27001 and ISO27002 standard in that it is difficult for the organization that is being evaluated to achieve improvement in the information protection and management system even though they could be suitable for the information protection and management guideline since they are evaluation system with the guideline and advisory characteristic and that centers on the managerial aspect.

Manuscript received October 26, 2010; revised November 1, 2010; accepted November 10, 2010.

Hyung-Won Kim is with the Department of IT Policy and Management , Soongsil University, Seoul, 156-743, Korea (Email: hwkim@edsk.co.kr)

III. DDOS CORRESPONDENCE INDEX

In this chapter, the process of deducing DDoS correspondence index and the metric for measuring the response index deduced will be presented.

A. DDoS Correspondence Index Deduction Process

Based on ISO 27004, a study on information protection and manage system measurement, mapping is performed for the index in its relation with DDoS correspondence strategy. Based on the DDoS correspondence strategy currently being mentioned, four types of response strategies of DDoS correspondence system development, base facility expansion, continuous evolvement and enhancement of personal security awareness are deduced. Through SMART Analysis [6], 7 indexes that are considered to be related to DDoS correspondence strategy are deduced as the standard index for the mapping. As for the measurement (evaluation) items for measuring the deduced standard index, the measurement items considered to be required for measuring the standard index are identified based on the national information protection level evaluation index model, individual information protection level diagnosis index by Ministry of Public Administration & Security and ISO 27004. Figure 1 shows the standard index and measurement item deduction process.

As for the 28 measurement items identified, factor analysis [7] is conducted to analyze the result and deduce 6 sub-indexes that are named by reflecting the characteristics of DDoS. In addition, a metric is proposed to allow quantitative measurement of the measurement items for measuring the six sub-indexes. Figure 2 shows the process of deducing DDoS index based on the factor analysis result on the identified measurement items upon the consideration that there is a connection with the standard index.

In the proposed DDoS index, the level index and performance index are categorized according to the availability of identifying the response situation of the current organization and the effect on the process result after the occurrence of issue. As for the proposed sub-index, Cronbach's alpha [8] was applied to verify the reliability of 7 groups being grouped according to the factor analysis result and identified 6 groups with Alpha > 0.500 and 90% of reliability level to deduce them as DDoS sub-index. As for the DDoS sub-index and measurement item, they are changed appropriately to the purpose of sub-index and measurement item exclusively for DDoS instead of general information protection system by reflecting the characteristics of DDoS.

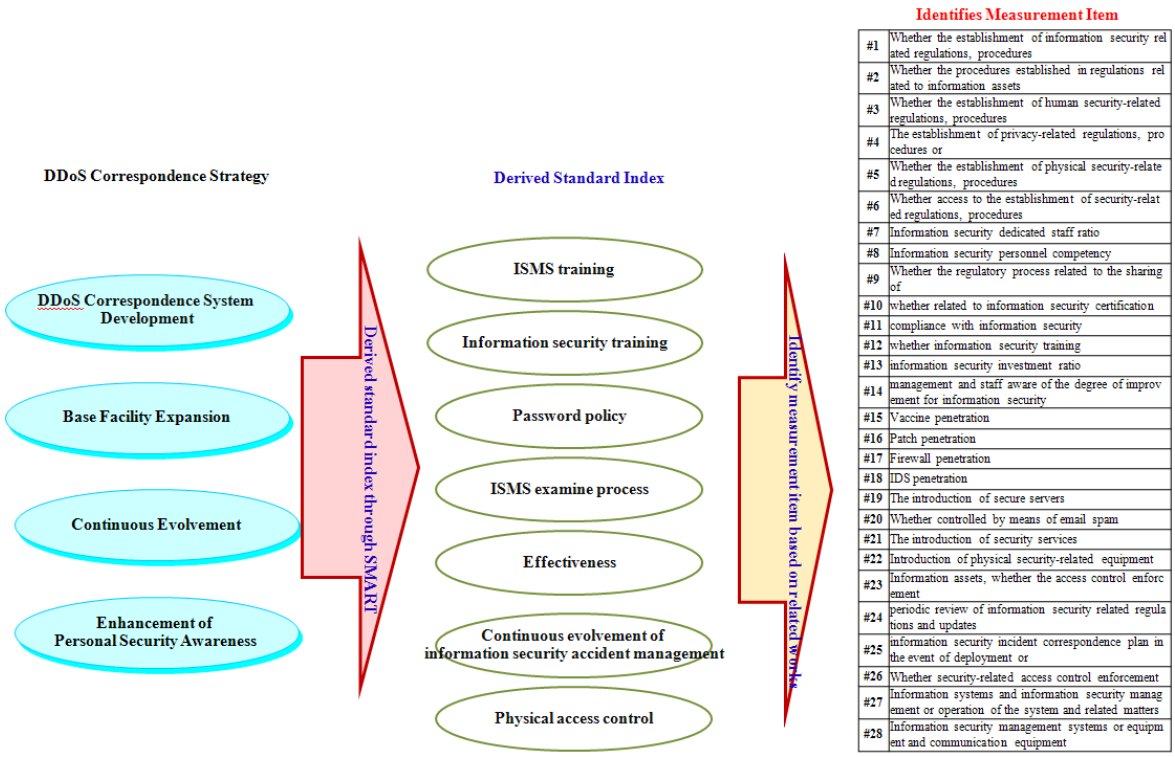

Fig. 1. Standard index and measurement item deduction process

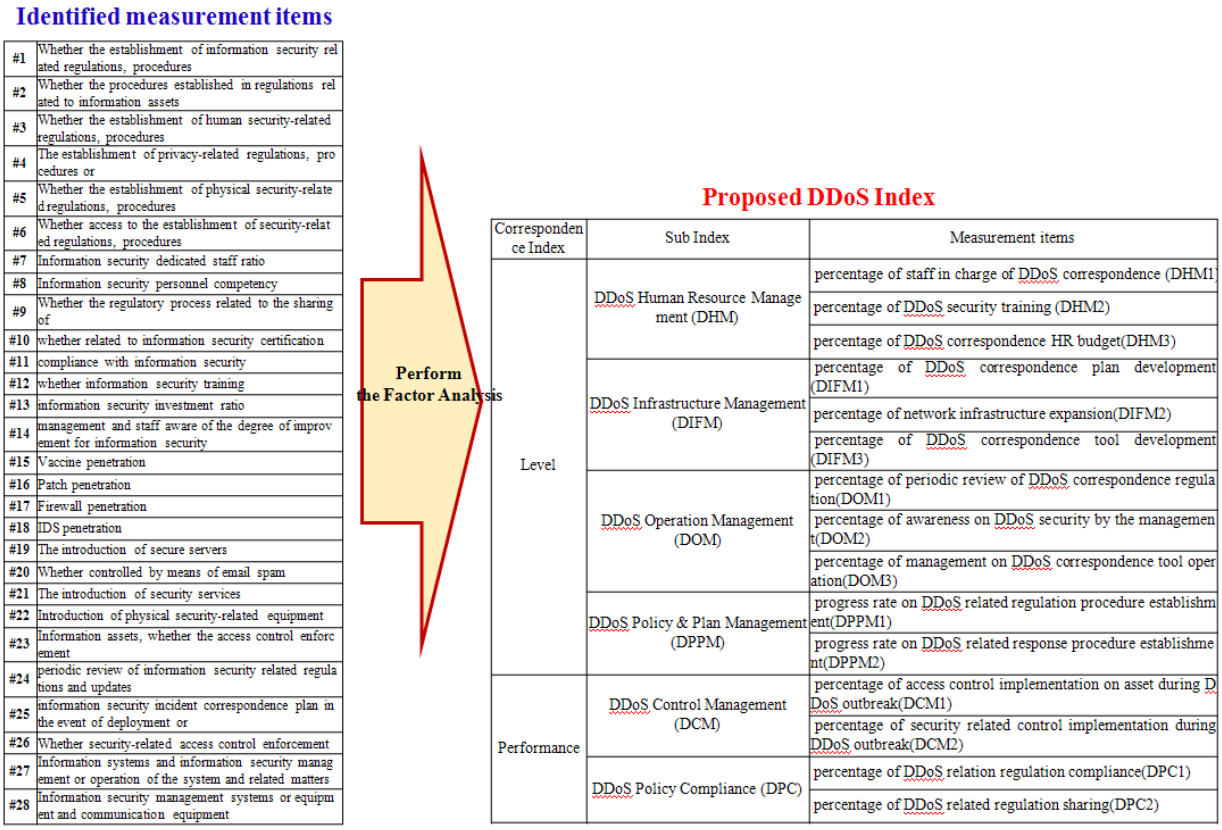

Fig. 2. Process of deducing DDoS index based on the factor analysis result

In the proposed DDoS index, the level index and performance index are categorized according to the availability of identifying the response situation of the current organization and the effect on the process result after the occurrence of issue. As for the proposed sub-index, Cronbach's alpha [8] was applied to verify the reliability of 7 groups being grouped according to the factor analysis result and identified 6 groups with Alpha > 0.500 and 90% of reliability level to deduce them as DDoS sub-index. As for the DDoS sub-index and measurement item, they are changed appropriately to the purpose of sub-index and measurement item exclusively for DDoS instead of general information protection system by reflecting the characteristics of DDoS.

B. Measurement Metric for Response Index

The identified sub-index is categorized into level index and performance index. The definition of each sub-index is as follows.

DDoS Human Resource Management (DHM): check the effective management of DDoS staff. Accordingly, check the percentage of staff in charge, provision of training and response budget.

$$DHM = (DHM1 + DHM2 + DHM3)/3$$

DDoS Infrastructure Management (DIFM): check the effective management of infrastructure for responding to DDoS attack. Accordingly, check the percentage of response plan development, network infrastructure, response tool development, etc.

$$DIFM = (DIFM1 + DIFM2 + DIFM3)/3$$

DDoS Operation Management (DOM): check the effective regulation on DDoS attack, high awareness of DDoS security by the management and operation management items of DDoS correspondence tool to check the effective management of DDoS correspondence operation.

$$DOM = (DOM1 + DOM2 + DOM3)/3$$

DDoS Policy & Plan Management (DPPM): check the effective management of DDoS related procedure or response procedure

$$DPPM = (DPPM1 + DPPM2)/2$$

DDoS Control Management (DCM): check the effective control of asset and implementation of security related control during DDoS attack

DCM = (DCM1 +DCM2)/2

DDoS Policy Compliance (DPC): check the appropriate response according to DDoS related regulation (procedure or response procedure) during DDoS attack and proper sharing of related regulation

DPC = (DPC1 + DPC2)/2

C. DDoS Correspondence Index Adaptation

Level response index is determined through the mean value of its sub-indexes of DDoS HR Management (DHM), DDoS Infrastructure Management (DIFM), DDoS Operation Management (DOM) and DDoS Policy & Plan Management (DPPM). Less than 20% shows insignificant level of DDoS correspondence and 20% ~ 50% shows the planned DDoS correspondence and 50~80% shows effective DDoS correspondence and 80~100% shows the operation and management of DDoS correspondence.

Performance response index is determined through the mean value of its sub-indexes of DDoS Control Management (DCM) and DDoS Policy Compliance (DPC). Less than 20% shows insignificant level of performance, and 20%~50% shows performance and 80~100% shows the management of performance. The proposed indexes must be continuously managed and the comparative data for the result values must be obtained.

The calculation of the level index of DDoS correspondence index using the proposed measurement indexes is as follows.

Li indicates the sub-index that constitutes the level response index, and L1 indicates DDoS HR Management, and L2 indicates DDoS Infrastructure Management, and L3 indicates DDoS Operation Management, and L4 indicates DDoS Policy & Plan Management. In the formula, n indicates the number of measurement items in i domain.

Different weights can be allocated to the measurement items in order to calculate the value of each index according to the DDoS correspondence goal and business goal. In the case of Wi, it indicates the weight of the sub-index in the order of i and such weight can be adjusted according to the response goal and organization. The scope of the value of Q, which is the total sum of the entire correspondence index is 0～V. Here, V becomes the total sum of Wi. Higher value of QL indicates more effective the level of DDoS correspondence.

$$QL = \sum_{i=1}^{4} Li \times Wi$$

Accordingly, comprehensive conclusion can be made on the performance index.

$$QP = \sum_{i=1}^{2} Pi \times Wi$$

IV. VALIDATION

Based on the measurement items in the existing studies [9][10][11], 28 measurement items related to the standard index were deduced. A group survey research was conducted for the same group for which SMART Analysis was conducted in order to verify the connection between the deduced measurement items and the actual DDoS, namely, the identification with the connection to the standard index.

The survey asked the connection between each measurement item and DDoS. The question of “Do you think the following measurement item is needed in measuring DDoS?” was asked for 28 items, and the answer was in multiple choice form of selecting only one of the five answers (1. Not needed at all / 2. Not needed / 3. Normal / 4. Needed / 5. Very needed), and the scale from 1 to 5 was used.

Using the survey result, factor analysis was conducted to determine the significance of the measurement items identified and if they belong to similar groups. In addition, Cronbach's Alpha [8] was conducted to verify the reliability of the groups identified based on the factor analysis result. The result is as shown in Figure 3.

The result of factor analysis conducted on the survey of 28 measurement indexes revealed that 7 significant groups among 11 components were identified. The group that contained only 1 element and the group that was not included in the reliable level were excluded. The reliability of the 7 identified groups was verified through Cronbach's Alpha to deduce 6 groups.

	Component Matrix(a)							
		Component					Cronbach's Alpha	Alpha > 0.500, 90%)
		1	2	3	4	5		
1	#7	0.744	-0.077	0.244	0.047	-0.079	0.697	O
	#13	0.616	0.301	0.019	-0.022	-0.050		
	#12	0.533	-0.042	0.441	-0.129	0.196		
	#8	0.532	-0.107	0.160	0.329	-0.005		
2	#25	-0.582	-0.134	0.302	0.157	-0.003	0.582	O
	#28	-0.523	0.117	0.510	0.426	-0.198		
	#22	-0.485	-0.158	0.468	-0.226	0.026		
3	#24	-0.136	0.685	-0.016	0.366	-0.046	0.557	O
	#5	0.124	0.579	-0.026	0.163	-0.262		
	#14	0.075	0.555	-0.013	-0.051	-0.396		
	#27	0.082	0.448	0.079	-0.388	-0.371		
4	#11	0.515	-0.649	-0.027	0.216	0.009	0.522	O
	#9	0.019	-0.582	0.393	-0.040	-0.226		
5	#3	-0.086	0.189	0.630	-0.107	0.093	0.561	O
	#1	-0.211	0.111	0.626	-0.256	-0.037		
	#6	0.110	0.316	0.523	0.187	-0.098		
	#2	-0.298	-0.160	0.505	-0.169	-0.023		
6	#23	-0.170	-0.124	0.092	0.491	0.136	0.533	O
	#26	0.390	0.031	0.212	0.488	-0.035		
7	#10	-0.361	0.376	-0.073	0.136	0.548	-0.022	X
	#19	0.327	0.322	0.406	-0.129	0.485		

Fig. 3. Execute result Of Cronbach's alpha

Cronbach's Alpha indicates the reliability of group composition. The reliability value is in the range of 0～1 and the similarity of group is higher when the value is closer to 1. In the case of higher than 0.9, it is considered as being in a very similar level ($p < 0.01$) and, in the case of higher than 0.7, it is considered as having achieved the statistically reliable level ($p < 0.05$). In the case of higher than 0.5 for the reliability value, it is considered as having achieved generally reliable level ($p < 0.10$). Based on the factor analysis, grouping the measurement indexes with the correlation value of higher than 0.5 indicates the reliability level of 95%, which has the same meaning as the Cronbach's Alpha value of higher than 0.7.

In this study, 6 groups with Cronbach's Alpha value of higher than 0.5, namely, the groups with 90% of reliability level were finally deduced. The six groups deduced were considered as the sub-indexes proposed in this thesis and the names of the sub-indexes were given by reflecting the characteristics of DDoS.

IV. CONCLUSIONS

The information security task also needs to be evaluated for its performance through objective index. Accordingly, 7 standard indexes were deduced through the indexes of ISO 27004 and a survey research on the relation with DDoS correspondence strategy. A survey research was conducted by identifying 28 measurement items through which the deduced standard indexes can be measured and the relation as the DDoS index item, and factor analysis and Cronbach's Alpha were conducted for the survey result to deduce sub-indexes by identifying 6 significant groups among the total of 11 groups. As the grouping results are the measure items for general information security task, the measurement items were changed to measure DDoS for which metric was proposed.

The level and performance on DDoS attack response can be examined by proposing response indexes through which the DDoS correspondence system can be measured. The indexes proposed do not entirely cover every DDoS situation. Therefore, there is a need for the indexes to be applied to organizations that are actually performing DDoS correspondences based on the proposed framework through which the deduced indexes need to be continuously supplemented.

REFERENCES

[1] Simon Liu, “Surviving Distributed Denial-of-Service Attacks”, IEEE Computer, pp51-53, 2009.
[2] Christos Douligeris and Aikaterini Mitrokotsa, “DDOS ATTACKS AND DEFENSE MECHANISMS: A CLASSIFICATION”, Computer Networks: The International Journal of Computer and Telecommunications Networking, vol.44 , Issue.5, pp.643-666, 2004.04.
[3] Ruiliang Chen, Jung-Min Park, and Randolph Marchany, “A Divide-and-Conquer Strategy for Thwarting Distributed Denial-of-Service Attacks”, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, vol.18, no.5, pp.577-588, 2007. 05.
[4] ISO/IEC 27001, Information technology - Security techniques - Information security management systems - Requirements, ISO, 2005.
[5] ISO/IEC 27002, Information Technology - Code of Practice for Information Security Management, ISO, 2007.
[6] McShane, S.L., Von Glinow, M.A., Organizational behavior: emerging realities for the workplace revolution(3rd), McGraw-Hill. 2005.
[7] Gorsuch R. L., Factor Analysis, Hillsdale, 1983.
[8] Cronbach L.J., “Coefficient alpha and internal structure of tests”, Psycometrika, Vol.16, No.3, pp.297-334, 1951.
[9] KISA, National Infoamtion Security Evaluation Index Model, KISA, 2006.
[10] MINISTRY OF Public Administration and Security, Evaluation Index of Personal Information Protection Level, MOPAS, 2007.
[11] ISO/IEC 27004, Information technology - Security techniques - Information security management - Measurement, ISO, 2009.

Hyung-Won Kim regular member
2010. 8 : Graduate School of the Soongsil University (go through Doctor course of Engineering)
<Interest> : Information Security, Digital forensics etc.

Nam-Yong Lee
1979 : Soongsil University (Computer Science)
1983 : Korea University (MIS)
1993 : Mississippi State University (MIS)
<Interest> : ITSM, Software Test, System Engineering etc.

Jong-Bae Kim regular member
1996. 2 : University Of Seoul(Management)
2002. 8 : Graduate School of the Soongsil University (Master of Engineering)
2004. 8 : Graduate School of the Soongsil University (Doctor of Engineering)
<Interest> : Methodology, Open-Source, Mobile-Agent etc.