A Framework Development for Correspondence Criteria of DDoS

Bum-jae Kim, Yong-tae Shin, Jong-bae Kim *Regular Members*

Abstract

the government and companies build a ddos correspondence system hastily to protect assets from cyber threats. it is become more and more intelligent and advanced such as ddos attack. however, when outbreaks of the social incidents such as 7.7 ddos attack or cases of the direct damage occurred, information security systems(iis) only become the issue in the short term. as usual, sustained investment about iss is a negative recognition.

since the characteristic of iss is hard to recognize the effectiveness of them before incidents occurs. also, results of incidents occurred classify attack and detection. detailed and objective measurement criterion to measure effectiveness and efficiency of iss is not existed. recently, it is progress that evaluation and certification about for the information security management system(isms). since these works propose only a general guideline, it is difficult to utilize as a result of isms improvement for organization.

therefore, this paper proposes a framework to develop main criteria by a correspondence strategy and process. it is able to detailed and objective measurements.

Key Words : ddos, information security system, correspondence strategy, framework

Ⅰ. Introduction

Recently, Denial of Service(DoS) or Distributed Denial of Service(DDoS) attacks increase more and more. Last July 7, forty-five sites such as Korea and an American government office, financial institutions, internet service companies suffered the vast damage by DDoS attacks. This attack was a chance to realize importance of the Internet Security again. It is a problem that such as DDoS attacks does evolve more and more[2].

The government and the companies came to have necessity of the infrastructure expansion by the DDoS damage once again this time by an opportunity. Therefore, the government revises a related policy for qualitative development than the quantitative development and preparation or ruins a multidirectional effort such as supports for IT service companies.

The government was largely increase on a budget after 7.7 attacks for "Enhancement of Hacking Virus Correspondence". Each departments of the government places an order for a business of DDoS Correspondence System and promotes it. Also, they do the equipment and efforts such as the software introduction for information Security Equipment.

The system of Information Security occurs from social event. However, when related organizations are damaged, there is a common notion that the system of Information Security is issued in the short term, and that it passively makes a continuous investment. Because its effect is difficultly recognized before events occur, it only exist decision about results that are invasions or defense when events occur, and there doesn't exist detailed and objective criteria of effectiveness and efficiency.

Evaluation for the Information Security Management System and the certification are going in these days, This only proposes a general indicator and standard for the Information Security Management

* Department of computer, soongsil university(bjkim111@naver.com),
** Department of computer, soongsil university(shin@ssu.ac.kr), *** e-enterprise co., ltd.(kjb123@empas.com),
논문번호 : 10011-0201, 접수일자 : 2010년 2월 1일

System.

How much is the administration building is absolutely level, through which government agencies and businesses have some level of DDoS countermeasure system is built and managed. Also the constructions of the countermeasure system how many applying with the index will be able to qualitatively measure an effect and the result is the difficult actual condition in infringement confrontation.

Therefore, in spite of specific and objectively measurable indicator for the DDoS confrontation system, these indicators are required overall confrontation system in addition to DDos counter measuring strategy and procedure, and it should be selected through the overall analysis of each organization. Also, indicator is not a object toward measurement of current statement, making a general analysis through various cases should be preceded since it ultimately has to act as a guideline for improvement of information protection management system of object organization according to the result.

This paper presents the DDoS confrontation system and a project model which can be used for constructing DDoS confrontation of each organization as the first exercise(assignment) for these trials. Furthermore, framework laying stress on guides and procedures of the indicator development for the result measurement and the level of constructed confrontation system will be presented.

Ⅱ. Related works

2.1 DDoS'attack and obstruction technology

Attack of Distributed Denial of Service is defined as the attack on infected PC or server by a hacker to exhaust the resource of a particular system and make normal service of the system no more available.[3,10]. To counter this DDoS attack, development of individual security technology is important, but ultimately, we cannot obstruct the attack of DDoS effectively until the whole moves in unity to perform an organic counteraction[2].

From this perspective, with a division of attack process pre-attack/attack/post-attack (3 stages), requirements for countering DDoS and for counteractive technology against DDoS considering the entire environment of IT network can be summarized by stage as the following[1,9].

Table 1. Requrements for counter technology by stage of ddos attack

Step	Division	Requirements
Prior to attack	Counter for attack agent development stage	Endeavor to prevent attack agent development /distribution through revision of law
	Counter for attack agent spreading stage (Screening for possible attack agents via detecting/reconstructing/analyzing execution files sent and received on the network)	- Developing analytic technology for dynamic malignant program - Constructing early-warning system on a national level via sharing collected information on malignant programs sent and received - Developing technology of Object Authentication for analyzing reliability of execution files - Developing technology of detecting, reporting and removing execution files installed regardless of the user's intention - Collecting attack agents by positioning weak websites within Honey.net
	Counter for controlling attack agents	- Analyzing various forms of approaches to C&C server and then developing technology for their detection - Analyzing on the access standard by which attack agent approaches C&C server to induct it on the counter system with specified request for connecting approach to C&C server and developing related technology capable of ordering a removal of attack agent itself according to the relevant access standard

Occurrence ofattack	Backbone network-level countermeasure	- Monitoring on the backbone network and developing DDoS equipment that can collect and analyze all the network traffic sent and received on the backbone network to detect the indication of attack
	Edge network-level countermeasure	- Detection technology for applied class of DDoS attack via analyzing traffic characteristics of applied programs - Measure for separating zombie PC from network on the level of Edge network
	Attack target server-level countermeasure	- Developing technology for obstructing attack incurring no decrease in server's efficiency by materializing in H/W within the network interface card to perform detection and obstruction of attack using its own CPU
	Integrated analysis-level countermeasure(At the time of attack occurrence, collecting various security events occurring across the network for integrated analysis and use)	- Country-level integrated control system to be managed and operated by government agency under a legal and institutional support that can collect DDoS attack-related information, promptly detect an attack and deliver information by its integrated analysis in automated method, and tracking down zombie PC, attack agent distribution system, C&C server and attacker's position
Posterior to attack occurrence	-	- Extracting systems used for attack to remove an attack agent from the relevant system as well as a possibly existing weakness - Identifying the C&C server and place of diffusing attacking agents by detailed analysis of collected attack agents and applying techniques of Blackhole Routing, Sinkhole Routing, etc. on the network traffic attempting to approach to relevant server and diffusion place to control access and delete attack agents automatically - Extracting the core characteristics of an attempted attack, and generating and distributing a signature that can promptly detect and obstruct a future possible same attack

Needless to say, materializing such a counteractive system requires a resolution of legal and institutional problems as well as technological ones[5]. This system needs various data in a number of different management networks to be collected under the integrated DDoS attack counteractive control system for simultaneous analysis, and for this purpose, the many management networks should be able to provide information using the same interface or protocol. So the integrated counteraction doesn't become possible until prescriptions on the form, content, etc. of the offered information and legal/institutional actions needed for actual delivery of information, including standardization of protocol, to make relevant information offered[7].

2.2 Measuring and evaluating methods for information security management system (ISMS)

As regards information security, content of existing studies is largely divided by two approaches.

First is, like TCSEC (Trusted Computer System Evaluation Criteria), ITSEC (Information Technology Security Criteria), etc., the evaluation system focused on the aspect of security functions and efficiency of the product or system. These existing evaluation criteria, chiefly using assessment standards by product, cannot evaluate on various

goods as demanded by the civilian sector, setting limitations in flexibility[6].

Second is, like BS7799[13,14], the evaluation system focused on the aspect of management. Especially, BS7799 was developed for the use as a general document to be referenced by managers responsible for materializing and maintaining information security of an organization with an intended basis for its security standard. Accordingly, BS7799 criteria, characteristic of a guideline and recommendation and an evaluation system focused on a managerial side, can be suited to a guideline for information security management, but it has a problem of uneasy improvement or enhancement itself on the information security management system of a target organization for evaluation[4].

Whereas, ISO/IEC TR 13335 GMITS (Guidelines for the Management of IT Security)[15-18], the current international standard for information security management, proposes 14 procedures focused on the process of information security management[6].

Information security management necessitates not only constructing an organization's system for it but also accurate, continued measurement and evaluation of the information security management system currently in operation. Through this measurement and evaluation work, an organization can grasp the levels of its current information security management system and needed requirements, and based on it, continued improvements on its ISMS is possible.

In addition, as an ISMS methodology for securing important information assets, ISO 27001[12] has been established for the international standard and now most widely in use. Similar concepts include SP 800-53 [11], COBIT4x[19], etc. and each country and organization is using diverse models in application.

Existing criteria and models investigated above are universal and for general purpose in character, providing no specific methodology or analytic methods for applying criteria.

Table 2. Process for information security management

Area	Process
IT-security purpose strategy and policy	IT security purposes and strategies
	IT security policies of an organization
Risk analysis	Upper-level Risk analysis
	Detailed Risk analysis plan setup and approval
	Asset identification and value assessment
	Threat assessment
	Weakness assessment
	Risk assessment
Materialization of IT security	Materialization of security measures
	Education and Training for security awareness improvement
	IT system approval
Follow-up	Security criteria verification
	Monitoring
	Accident handling
	Change control

Ⅲ. DDoS correspondence process and critera framework

3.1 DDoS correspondence system model

Since DDoS offense technology has been incessantly in progress, it is difficult to propose a technologically perfect defense method on it. What is needed is equipment of the system and process capable of counteracting to diverse threats of attack promptly and effectively and an effort to develop oneself through continued learning about varying patterns of attack. To this end, correspondence system should be built in two perspectives.

First, only after a detailed analysis on attacker's offense strategy, technique, damage influence and responsive technique by site, should the current problems be derived to construct an effective correspondence system to secure the availability of the site.

Second, freed from one-dimensional counter-measure focused on equipment, lasting correspondence system should be built through setting up omni-directional DDoS defense architecture with harmony between policy, correspondence technology and enlarged volume installation.

Processes and items summarized for establishing this aspect of DDoS correspondence strategy are shown in Table 3 below.

Also, for effective counteraction on DDoS, correspondence system and process from detection of attack to counteraction on accident should be prepared in advance, as shown in Table 4.

Besides, since one DDoS equipment cannot block all DDoS attack, we should respond synthetically through an organic management of security equipments existing within the system. Integrated management through communication between security equipments in the company includes IP/Port

Table 3. Process for information security management

Step	Detailed process and item
Review on business requirements	- Analysis of requirements in terms of business continuity
Defining scope for correspondence system	- Analysis of business objective, industry characteristics, etc. - Defining chief defense targets by reflecting requirements
Identifying offense pattern	Identifying the level of threatening damage by form of DDoS attack
Infrastructure and volume analysis	- Grasping the composition of infrastructure and present status of equipment operation - Criteria estimation and measurement of current volume from the aspect of availability for defense target
Managerial operation form analysis	Analysis of operational form from a managerial aspect (process, policy, etc.)
Establishing plan for volume	Establishing a volume buildup plan for defense of attack in order to enable defense above a certain level of threat from attack
Establishing infrastructure buildup system	Building up network and security equipment and server according to forms of attack, establishing infrastructure buildup plans for separated counteraction within a region and for between regions
Establishing correspondence system by threat level	Establishing policy, process and R&R for counteraction on attack by threat level
Follow-up	Continued management and counteraction

Table 4. DDoS correspondence system and process

Step	System and process
Detection of DDoS attack	Detection by sensor equipment and collection of outside warnings - Sensor: DDoS solution, PW, WAF, IDS, etc. - Outside warnings: KISA, ISAC, CERT, ISP, etc.
Defining and analyzing Risk level	Defining Risk levels for target Risk equipment Risk level analysis: level of traffic load and access to session Defining normal level : selection of mean for average 1~3 months
Situation dissemination	Disseminating situation to persons in charge and concerned according to Risk level - Disseminating situation to persons in charge and concerned in accordance with network of emergency contacts - Method : SMS, e-mail, fixed-line and mobile phone - Persons concerned : KISA, CERT, ISP, IDC, etc.
Counteraction to invasion accidents	Progress of correspondence process according to attack level - Grasping damage situation (access difficulty, system error, etc.) - Analyzing attack pattern (TCP, HITP, network) - Attacking place analysis and obstruction process

interception, detection of the latest pattern from IDS/IPS, traffic distribution from switch apparatus, malignant code/weakness detection from server security tool, virus/worm cure from client vaccine, etc. One example of setting up a responding policy by attack pattern from this perspective, applying it to each system and constituting and managing a map dealing with DDoS attack would be Table 5.

3.2 Framework for developing DDoS correspondence criteria

Criteria available for measuring correspondence system built in consideration of DDoS correspondence system and process model proposed in the previous section includes performance criteria, Risk criteria and level criteria, designed from three different viewpoints. In this perspective, this thesis

Table 5. A map dealing with ddos attack

DDoSAttack			A	B	C	D	E	F	G	H
Logical	HOST	Tear Drop		√			√			
		Bonk		√			√			
		Land Attack		√			√			
		Win Nuke		√			√			
		Pingof Death		√			√			
Bandwidth	ICMP	DirectFlooding	√							
		BroadcastFlooding	√							
	UDP	DNSUDPFlooding	√							
		DNSQueryFlooding	√							
		DNSReplyFlooding	√							
		FraggieAttack	√							
	TCP	SYNFlooding			√					
		ACKFlooding					√			
		MalformedFlagFlooding					√			
Resource	APPLICATION	GETFlooding			√	√			√	√
		CCAttack			√	√			√	√
		CircleCCAttack			√	√			√	√
		SlowrisAttack			√				√	√
	HOST	SYNFlooding				√			√	√
Invasion	HOST	InjectionAttack						√		√
		XSSAttack						√		√

Explanatory note : A: Router (ISP), B: Router (Border), C: DDoS Obstruction equipment, D: DoS, E: Finewall, F: IPS, G: Reverse Proxy, H: Web Server

proposes the framework of correspondence criteria, which is mapped out on the side of DDoS correspondence system model and process, as shown in Fig.1.

Actually, to make criteria for measurement, it is needed to make as many criteria pools as possible, which must be refined and improved through continued measurement and feedback.

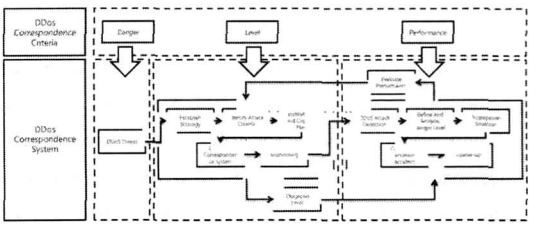


Fig 1. Framework of DDoS Correspondence riteria

Candidates for criteria can be selected through information security policy with specified responsibilities, periods of time, results, etc. for execution items, or be made by dissecting an organization's information security duties into detailed levels of process defined in input-disposal-output forms through handling time, cost, quantity and quality of outputs, ratio, etc. for each process.

Criteria framework proposed in this study composes the frame of developing criteria in three terms of Risk criteria, level criteria and performance criteria, on the standard of DDoS correspondence process model. Definitions of framework for developing criteria from each viewpoint are as follows:

First, Risk criteria are the concept proposed by risk management technique such as ERM (Enterprise Risk Management), an element to represent the current situation, and an criteria by the outside factor. Examples include occurrence rate of infringement accidents and weekly occurrence count of network attacks, which is outside threat level impossible to control on the basis of individual organization, warning against Risk in the near future, etc. Therefore, an individual organization should have a view from the point of collection and analysis, rather than measurement and control. In case of directly making a Risk criteria from within an organization, it needs to use the Risk list derived from existing analytic result of information security Risk, effect assessment on personal information, etc.

Next, level criteria means the level seen from the angle of criteria, which includes ISO 27001, GAP analysis score of ISMS, maturity score like SSE-CMM, etc.

Objective performance management on information security duty like DDoS counteraction is more difficult and demanding than any other commitment. In considering the aspect of performance management or efficiency, how to set up an accurate criteria of measurement and implement it is important.

Performance criteria are the field developed through traditional management theory and technique such as BSC (Balanced Score Card), 6

Sigma, etc. Security patch ratio, correspondence handling time, ratio of finishing information security class, etc. may come under this element of accounting for the efficiency and level of realizing the relevant duty performed.

Ⅳ. Process of developing DDOS correspondence criteria

The first step for developing correspondence criteria is composition of measurement criteria. Composition of a measurement criteria pool is possible by brining criteria made public or by directly drawing them out from duty. Data to be consulted as an open criteria are such as NIST SP 800-55[20], ISO 27004 (WD)[21] or related standard documents or books. However, these methods are hardly applicable to one's own company and likely to make little effect if attempted, so a better one is to directly draw out criteria from one's work and an organization's environment.

Identifying concerns of the interested parties: This is to identify the interested parties and their concerns from the criteria. All people belonging to an organization can be interested parties as to security, but the extent is different according to their positions. The representative of an organization, CIO, manager of information system/network, information security engineer, etc. can be seen as the chief persons concerned. Also, CFO, education/training organ, HR management, personnel field, etc. can be auxiliary persons concerned with their business related to information security, though security is not their main duty. These persons concerned have different interests and main points by their role, position, etc.

Defining the goal and objective: It is to identify and document the efficiency objective and goal of information security system that can guide an information security measure on particular information system.

Review on the policy, guideline and process of information security: As a baseline for an organization's policy and process, it describes security measures, requirements and how to realize technologies for attaining the goal and objective of information security.

Review on materializing an information security program: It reviews the existing criteria and related data used for inducting the criteria. After review, applicable information should be extracted and proper proof of materialization that supports criteria development and data collection should be identified. Criteria referable to here are system security plan/follow-up information on information security-related activities (Infringement accident report, test, network management, audit format, etc.) /Risk evaluation and invasion test results/certification documents/Result of continued monitoring/contingency plans/configuration management plan/training result and statistics, etc.

Next step is the course of deriving core criteria from the criteria pool chosen above and it is to make up a portfolio of criteria officially recognized for the result of and reward for DDoS correspondence duty.

Criteria development and selection: An organization should document criteria in a standardized form so that they may guarantee the repetition for the time of developing criteria. It should be provided with details needed for collecting, analyzing and reporting criteria, e.g. on the standard of Table 6.

Also, in selecting from deciding on the priority of criteria, work in compliance with the existing policy and process gives massive derivable criteria, so it is important to opt for two or three criteria with high priority for each participant.

Also important is to set an efficiency goal for criteria and according to the trait of each, efficiency of applicable criteria should be set through quantitative or qualitative analysis.

Once an criteria is selected, it should be used not only for measuring efficiency, investigating the reason for failure or improvement, but also for promoting the realization of consistent policy, efficient policy change for information security and continued improvement along with redefinition of a goal or objective. Therefore, the process of developing and selecting criteria is an activity

Table 6. EXAMPLE OF CRITERIA TEMPLATE

Field	Data
Identifier	The only identifier that is used for tracking down and arranging an criteria
Objective	Strategic object
Criteria	Description for measurement, such as 'percent', 'number of pieces', 'frequency', 'mean', etc.
Pattern	Division on perception materialized by criteria, such as effectiveness/efficiency, effect, etc.
Formula	Calculation on mathematical values expressed by an criteria
Goal	Goal of a satisfaction grading for criteria
Content of materialization	Criteria calculation, validity of performed activity, reason for dissatisfaction, etc. on a particular criteria
Frequency	Describes how often data is collected, analyzed and reported
Dept in charge	Indicates chief participants: owner, collector, user, etc. of information
Source of data	Location of data used for calculating an criteria
Report format	Report format on an criteria: pie chart, line chart, bar graph, other formats, etc.

requiring a continued feedback from inside.

After finishing deriving core criteria, it is the step for materializing actual criteria and for building a system to perform measurement. Considerations for successful performance include reviews on subject and cycle of measurement, location of data for measurement, method of collection, examination, etc. and these items should be reflected in the process of measuring criteria or document for defining criteria. Detailed content of each process is as follows:

Preparation for data collection: This means setting up a plan for materializing criteria program. The plan comprises the subject of plan / role and responsibility of measurement including responsibility for collecting, analyzing and reporting data/process of collecting, analyzing and reporting criteria adjusted to the structure, process, policy and process of a particular organization/detailed matters of cooperation for the interested parties/development or selection of tools for collecting or tracking down data/report form for criteria summary/rules for continued monitoring, etc.

Data collection and analysis of result: This step collects and integrates the criteria data according to the procedures defined in the plan for materializing criteria and stores in a form suited for analysis and report (e.g. database or spreadsheet). On the collected criteria data, gap analysis is conducted through comparison with the goal and causes for low efficiency and parts in need for improvement are defined by identifying the gap between actual and wanted efficiencies.

Identifying activities for improvement: It is the step for developing plans that can be a road map for resolving the gap analyzed in the previous step. For these plans, one should determine the scope of improvement activities based on causative elements or results (Composition or fluctuation of the system, education or training on the staff, purchase of security equipment, change in security policy, etc.) as well as the priority among betterment activities on the basis of the goal for a general relief of Risk. Though reform activity usually affects a singular efficiency, there are cases where resolution costs are too high for a problem. Therefore, a whole cost-benefit analysis should be performed through the method of sorting costs of reform activity in ascending order and impact of activity in descending order to choose the highest-ranking practical activity for improvement from the list of priority.

Case development and acquisition of resources: Resources for decisions through the process so far should be reflected on the budget and acquired. Analysis reports through the former process can be the proof for budgeting.

Application to reform activity: Application includes reform activity regarding security program, security policy on the parts of technology, management, etc. By controlling and documenting reform activity, a better impact can be expected on revised activities and reformed items.

Activities for developing and applying criteria, which have been defined so far, can be secured of the result only when maintaining the continuity of execution and management in collecting, analyzing and reporting data. Monitoring on the progress and continuing with revision activities affect the normal

materialization and management of protection policies on the information system. In addition, many criteria for frequency and quantity help avoid problems by modifying the course quickly based on the system in the event of taking unplanned action or not acting as demanded.

V. Conclusions

'No measurement, no management.' has now become an inescapable maxim for the business of IT field, too. Duty of information security, too, can no longer be an exception for the subject with its performance results appraised via objective criteria.

In this thesis, a correspondence model especially focused on the correspondence strategy and process for DDoS attack, among the spheres of information security, which has been an issue until now, was proposed to be consulted for establishing a general DDoS correspondence system. Besides, by measuring DDoS correspondence system quantitatively, system of criteria for priority and a thorough management for effect and framework for development process were proposed.

The framework proposed in this study was ultimately intended to offer the common process and guidelines for developing the level criteria, Risk criteria and performance criteria in DDoS correspondence system, so in actual development of criteria, content of criteria can become different according to the traits of each area. That is, for level criteria, idea of maturity should be additionally considered and Risk criteria should be considered on the national level rather than individual organizations. Also, Performance criteria should be approached from the viewpoint of return on investment (ROI). However, as to the strategy and methodology for developing each of criteria, it is efficient to refer to the framework proposed in this study as a model.

In the years to come, it is expected to develop more detailed criteria through individual researches on the sphere of each criterion.

References

[1] Yang-Seo Choi, Jin-Tae Oh, Jong-Soo Jang, and Jae-Cheol Rhew, "A Study on Integration Correspondence System of DDoS Attack" KIISC, Vol.19, no.5, 2009.10.

[2] KISC(Korea Internet Security Center), "Analysis Report about A domestic main site object DDoS attack", KISA, 2009. 7.

[3] KISC, "Classification and Analysis of Denial of Service attacks", 2000.12.

[4] Hee-Myung Lee, Jong-In Lim, "A Study on the Development of Corporate Information Security Level Assessment Models", KIISC, Vol.18, No. 5, October 2008.

[5] KISC, "All about DDoS(Technical Seminar)", KISA, 2008.

[6] Yun Ji Na, "A Study on the Evaluation Indices for Evaluation of the Information Security Level on the Enterprise Organization", JIS(Journal of Information and Security), Vol.6, No.3, September 2006.

[7] KISC, "A Study about Risk Analysis and Countermeasure of DoS", KISA, 2000. 12.

[8] KISA, http://www.kisa.or.kr

[9] Peng, T., Leckie, C., and Ramamohanarao, K., "Survey of Network-based Defense Mechanisms Countering the DoS and DDoS Problems", ACM Comput. Surv. 39, 1, Article 3, April 2007.

[10] Jelena Mirkovic, Peter Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms", ACM SIGCOMM Computer Communication Review, Vol.34, Issue2, pp. 39-53, April 2004.

[11] SP800-53(Rev.2) : Recommended Security controls for Information Security, 2007. 10, NIST

[12] ISO/IEC27001 : 2005(FDIS) Information Security Management System Requirements

[13] BS7799 Part 1 "Information Security Management - Code of practice for information security management", BSI, 1999

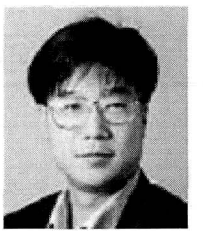
[14] BS7799 Part 2 "Information Security Management - Specification for information security

management", BSI, 1999
〔15〕 ISO/IEC JTC1/SC7/WG1 "Guidelines for the Management of IT Security(GMITS) : Part 1 - Concepts and Model", 1997
〔16〕 ISO/IEC JTC1/SC7/WG1 "Guidelines for the Management of IT Security(GMITS) : Part 2 - Managing and Planning IT Security", 1998
〔17〕 ISO/IEC JTC1/SC7/WG1 "Guidelines for the Management of IT Security(GMITS) : Part 3 - Techniques for the Management of IT Security", 1998
〔18〕 ISO/IEC JTC1/SC7/WG1 "Guidelines for the Management of IT Security(GMITS) : Part 4 - Selection for Safeguard", 1999
〔19〕 Information Systems Audit and Control Association, "COBIT, Management Guideline, 3rd Edition", 2000
〔20〕 SP800-55(Rev.1) : Performance Measurement Guide for Information Security, 2008. 7, NIST
〔21〕 ISO/IEC27004(WD) : 2008(FDIS) Information security management measurements

Bum-Jae Kim Regular Member

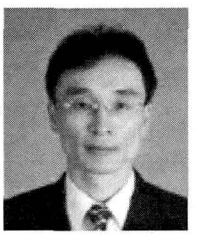
B.S. in German language and literature, Seoul National Univ., 1988.
M.S. in Computer Engineering, Yonsei Univ., 2000.
Ph.D. Program in Computer Science, Soongsil Univ., current.
CEO of L&Ksys Co,ltd, current
<Interest> Multicast, Group Communication, Internet Security, Mobile Internet Communication. etc.

Yong-Tae Shin Regular Member



B.S. in Industrial Engineering, Hanyang Univ., 1985.
M.S. in Computer Science, Univ. of Iowa, 1990.
Ph.D. in Computer Science, Univ. of Iowa, 1994
Guest Professor in Michigan State Univ., 1994
Associate Professor in Computer Science, Soongsil Univ., current.
<Interest> Multicast, Group Communication, Internet Security, Mobile Internet Communication. 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.