A Exploratory Study on R&D Strategies in Industrial Technology Security

Hangbae Chang[1], Jonggu Kang[1] Hyukjun Kwon[2], and Ilsun You[3]

[1] Daejin University, San 11-1, Sundan-Dong, Gyeonggi-Do, 487-711, Korea
hbchang@daejin.ac.kr and Jaikang7@gmail.com
[2] Yonsei University, New Millenium Hall, 262 Seongsanno, Seodaemun-Gu, Seoul, 120-749, Korea
junkwon@yonsei.ac.kr
[3] Korean Bible University, 205, Sanggye-Dong, Nowon-Gu, Seoul, 139-791, Korea
isyou@bible.ac.kr
⋆

Abstract. To enhance international competitiveness through the protection of cutting-edge industrial technology, it is essential to establish the policy for strengthening ability to develop industrial security technology and raising international competitiveness. In this study we investigated and analyzed not only the ecumenic trend but also the present condition, then we executed the deduction of the industrial security technology development program in a aspect of government and analyzed the current status of the technical security technology for developing security technology and increasing leaks of the advanced industrial technology.

1 Present Status of Industrial Technology Leakage

According to the survey conducted by National Intelligence Service in 2008, the number of disclosure of domestic industrial technology leakage is 125 from 2000 to December of 2007. If these cases were not detected, it could have caused approximately 95 trillion won of property loss. If we have a look at the status of annual industrial technology leakage disclosure, the number of attempts to thieve technology which were less than 10, but it has recorded 26 in 2004, 29 in 2005, 31 in 2006, 32 in 2007. It indicates a constant increase and is urgent to prepare a strategy to prevent the technology leakage.

The main subject of industrial technology leakage is primarily divided into internal and external stakeholders[9]. The industrial technology leakage by insider which targets important information or electronic documents occurs via personal computer, web based e-mail, and internet messenger[1][2]. And in case of offline documents, it was reported as they are flowed out through Web, trespass by outsider committing system hacking with virus or warm, larceny by outsider flowing

⋆ D. Chadwick, I. You and H. Chang (Eds.): Proceedings of the 1st International Workshop on Managing Insider Security Threats (MIST2009), Purdue University, West Lafayette, USA, June 16, 2009. *Copyright is held by the author(s)*

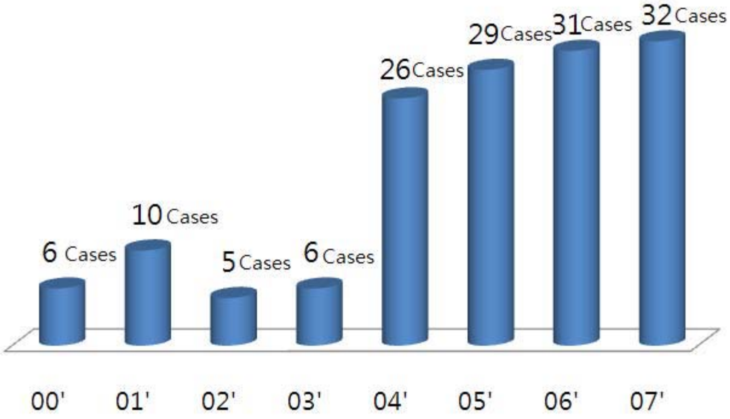


Fig. 1. Status of Industrial Information Leakage

out offline documents produced by printer or photocopier. There exists an actual case that outsider for maintenance accessed database of business process system and flowed the large amount of information and offline documents out.

Likewise, to prevent an industrial technology leakage, domestic authority concerned put Technology Leak Prevention and Industrial Technology Protection and Support Act in operation to improve the competitiveness of domestic industrial and contribute to development of national economy by preventing illegal leakage of the industrial technology. Yet for a concrete application of this Act, it is essential that the current status of industrial technology security and further study of this field is needed. Thus in this study, we analyzed the current level of domestic industrial security technology and technical competitiveness. We expect to utilize analysis data as basic information for improving international competitiveness and ability to develop industrial security technology[6].

To execute this plan, we analyzed the needs for industrial technology protection and designed the technical framework to fulfill those needs which were deduced. Following designed framework, we analyzed a current level of technology and limitation then deduced further development subject[8][10].

2 Investigation of Needs for Industrial Security Technology

In this study, to investigate actual needs for industrial security technology, we visited 15 providers of technology and 15 demander of technology then conducted in-depth interviews. The primary needs for industrial security technology are as followings[4][5]:

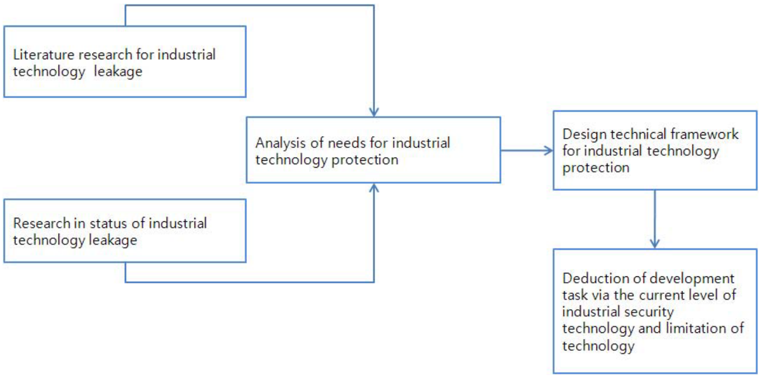

Literature research for industrial technology leakage
Research in status of industrial technology leakage
Analysis of needs for industrial technology protection
Design technical framework for industrial technology protection
Deduction of development task via the current level of industrial security technology and limitation of technology

Fig. 2. Research Methodology

- As a result of the investigation, it appeared to be essential to develop counter measures for emergence of various portable storage devices(secure digital card, compact flash card, memory stick) and communication methods(infrared data communications, wireless internet, blue tooth, etc)
- Some security technologies for ordinary business documents(word, excel, power point files) have reached secure level, but security technologies for blueprints or program source documents have yet to be well developed
- The access control method is mainly used for database security technology rather than encryption due to a performance problem and there exist needs for some technology enabling illegal SQL questions to be standardized.
- Measure model for security level of remote computer is still on the way of development. And further researches about control method and resource utilization authority management for computers which reached some extent of security level.
- Currently, there occurs some security vulnerable spot in the linked section because there isnt the integration between physical and technical security.

3 Technical Industrial Security Technology Framework Design

In this study, according to disadvantage analysis result derived from risk analysis process, we applied industrial security technology design methodology based on risk analysis for solving vulnerability[3]. Information security technology development methodology based on risk analysis listed vulnerability and threats for information asset through information asset identification and analysis. Then we designed technical industrial security technology framework by reflecting assessment result about influence and risk caused by certain attack to needs for security technology development.

Before anything else, the patterns of the security vulnerability of the personal computer are classified as the damage of internal information in personal computers caused by malicious external access(outflow of document file by hacking tool considering the vulnerability of operation system, virus, worm), unreliability(external penetration according to the absence of window password during booting, outflow of document file caused by the absence of screen saver) of personal computer(access control) management, and intentional internal documentation leakage by personal computer user(via e-mail, portable storage device).

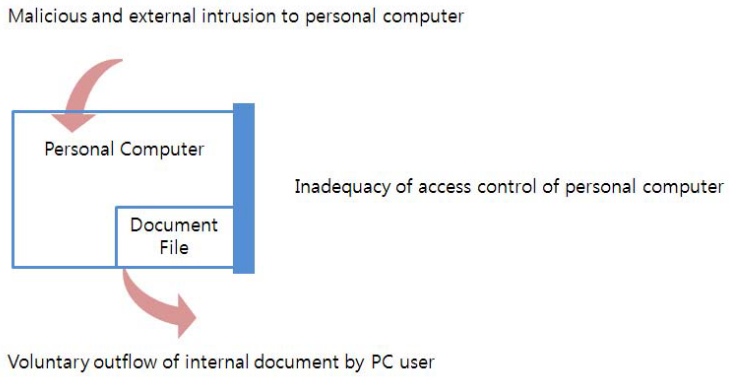

Malicious and external intrusion to personal computer
Personal Computer
Document File
Inadequacy of access control of personal computer
Voluntary outflow of internal document by PC user

Fig. 3. Patterns of security vulnerability of PC

The patterns of the vulnerability of electronic document are classified as unencryption(circulation of the unclassified confidential document) and ungraduation, inadequacy of access control in a way of reading, editing, conveyance, and printing of the documents(abuse of users' authority, illegal outflow via e-mail and portable storage devices, theft and loss), and illegal use of destructed document(undestruction after using document, illegal outflow of document by restoring deleted document)

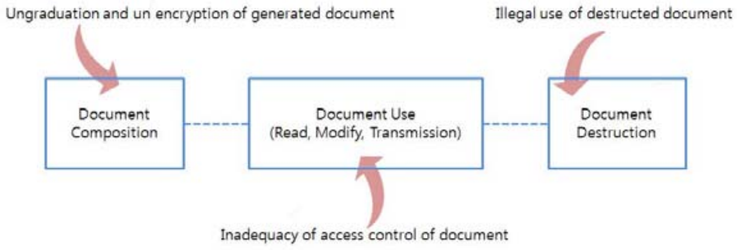

Ungraduation and un encryption of generated document
Illegal use of destructed document
Document Composition
Document Use (Read, Modify, Transmission)
Document Destruction
Inadequacy of access control of document

Fig. 4. Patterns of inadequacy of access control for document

The patterns of the vulnerability of database are classified as indiscreet access to database(read or outflow unrelated data file, abusing access authority) of server administrator(or usual user), outflow of data file peculating access authority), outflow of data file by peculating access authority of database(outflow of data file by peculating id and password of user or administrator), and information damage caused by the malicious penetration from outside of the organization to server or database.

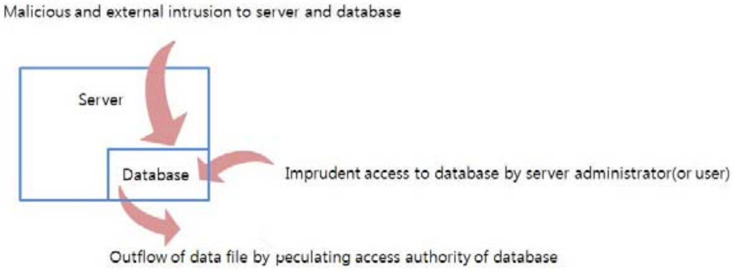

Malicious and external intrusion to server and database
Server
Database
Imprudent access to database by server administrator(or user)
Outflow of data file by peculating access authority of database

Fig. 5. Patterns of vulnerability of database

Lastly, the patterns of the vulnerability of network are classified as packet sniffing, penetration utilizing the vulnerability of network equipment, and network pulse sniffing.

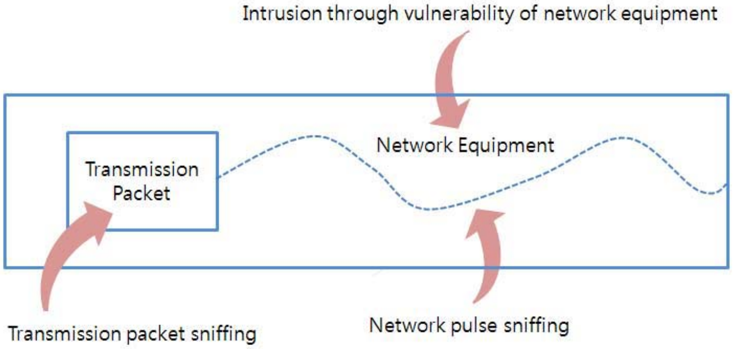
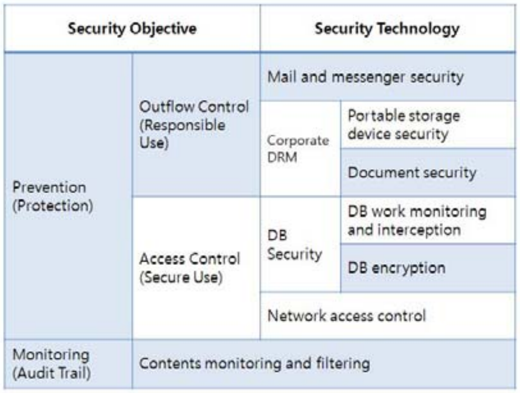

Intrusion through vulnerability of network equipment
Transmission Packet
Network Equipment
Transmission packet sniffing
Network pulse sniffing

Fig. 6. Patterns of vulnerability of network

Generally, there exist the technical measures for preventing outflow of information which are classified as cut off or restriction of access to information, encryption of data or files blocking the access made by unauthorized users, blocking file transmission or restriction to the channel of outflow, destruction of device where data or file is stored, and monitoring log in which the outflow of the data or file leaves traces. Based on vulnerability analysis about identified information asset, we executed Delphi method with professional group related to literature review and relevant field workers(3 university professor, 3 professionals working for security corporation), then we distinguished security objective from security technology and designed them as table 1. The Delphi method is that we collected opinions of professional group via survey and surveyed statistical analysis result from professional group again then repeat the collection of opinion and aggregate. This method provides a chance to modify each professionals opinion and it is positive of a chance to utilize others opinion. Currently more than 90% of technology foresight field use Delphi method and it is settled down as universal method. It has another advantage that it help get reliable assessment result via professional groups participation.

A mail and messenger securities that are to prevent a industrial technology leakage encrypt contents of e-mail and messenger via internet also filter them in observance of rules. A portable storage device security is that it implements authority control on portable storage devices(USB, mobile phone, memory card, etc) which can be connected with personal computer.



Security Objective		Security Technology	
Prevention (Protection)	Outflow Control (Responsible Use)	Mail and messenger security	
		Corporate DRM	Portable storage device security
			Document security
	Access Control (Secure Use)	DB Security	DB work monitoring and interception
			DB encryption
		Network access control	
Monitoring (Audit Trail)	Contents monitoring and filtering		

Table 1. Industrial Security Framework

A document security aiming at controlling an approach to industrial technology block an attempt to access made by unauthorized or illegal person based on encryption of the existing file. The document security also applies security regulation to the all procedures which are made from a generation of the document to disposal of the document including distribution of them. And it makes it possible to grasp a channel of the important documents outflow so that it can prevent unauthorized outflow or thief of confidential documents and product blueprint. Database security technology consists of database activity monitoring and blocking technology. Both of technologies function as a means of protection which guards stored data in the database from unauthorized access, intentional modification and elimination of data, and contingency obstructing datas consistency. Database encryption technology not only encrypts data but also stores them. And when it is necessary, it restore the encrypted data and reads or modifies them then encrypts them again. Network access control technology protects internal network and user terminal through certain procedures that execute an isolation, cure, and permitting an access regarding terminal unmatched with security policy after inspecting a status of terminal from a stage of network access.

Consequently, contents monitoring and filtering technologies observe the distribution of industrial technology founded on a business regulation related to certain application programs. This technology also detects an inappropriate transfer of the sensible information in network.

4 Analysis of the Current Status and Limitation of Industrial Security Technology

As a result of in-depth interview research, a technology of portable storage device security is developed when various portable storage devices (secure digital card, compact flash card, memory stick, etc.) appear and new means of communication are developed. Yet there appear a problem caused by collision with controlling existing devices in interoperability.

Document security technology has restriction on program source file and a blueprint due to the big size of file, interoperability between various kinds of form of file and applications, and the needs for multi-level collaboration. And there is lack of steady state of security technology development (currently it is not possible to collect and integrate the usage history of files or the usage history of read and write. It is also impossible to control downloads and authority to use after download).

Database activity monitoring and blocking technology cannot control an access made by each user unit but can control an access made by application unit because database security technology cannot recognize which client access the database in case of access conducted through application server. When database encryption technology encrypts database, it encrypts index at the same time so that the speed of data search become slower. Also it takes long time to encrypt or decrypt large amount of data table. Unfortunately, this disadvantage may cause service halt.

Network access control technology blocks an ill-intentioned program or attempt that both of them are executed by computer users qualified for proper security level according to organizations regulation. It has emerged to develop an integrated security technology which can manage change in security policy or health condition of computer.

Currently, contents monitoring and filtering technology for ordinary corporation and public office occupy 1GB of server for 1 hour-long log of operation history and after 1 month the operation history would produce approximately 300 500GB of log. That makes it difficult to trace log after all.

5 Establishing a Strategy for Industrial Security Technology Development

As previously explained, many security technologies are being developed with various perspectives to protect industrial technology. But there is much work related to managing technologies aimed at controlling outflow and those technologies only provide protection to arranged file format. Also technologies for monitoring have a potential to commit a detection error and cannot provide real-time interception. Inconsequence, future industrial security technology is needed to be developed as policy-oriented based on organizations business process. Accordingly in this study, we deduced further technology development task as followings with professional group by Delphi method.

First, control system for different types of portable storage device conduct access control regardless of producer or operational environment and when doing data transferring to external, it still maintains access control on data from a remote computer. In detail, this control system consists of advancement of portable storage device and channel control technology, external transmission security file which supports confidentiality, integrity, and tenacity. The external transmission security file conducts encryption of document and convey decryption key to external authorized user so that user who receives security file can read relevant document without installing a certain program into terminal. The mere execution of security file let user read document under permissible range.

Industrial technology document integrated security system fulfills security and compatibility among technologies which process security related to electronic document. And it guards program source file and blueprint that possess unique feature for business process. Considering relevant work environment, security technology of program source file and blueprint should solve following security needs.

Particularly, collaboration possible industrial technology electronic document security technology should conduct an access control for user and application program at the same time. It also needs to develop integrated electronic security technology, being linked with the existing office document security technology. The current compatibility and expansion possible document security integrated technology cannot provide interoperability, when a document transmission occurs between two different organizations. So this technology prevents a document transmission in which security technology is not applied. Accordingly, API(Application Program Interface) which can control information leakage made from document distribution in the organizations should be developed.

The high-performance database security system solves vulnerability that a detour of database access through web application has and minimizes user pro-

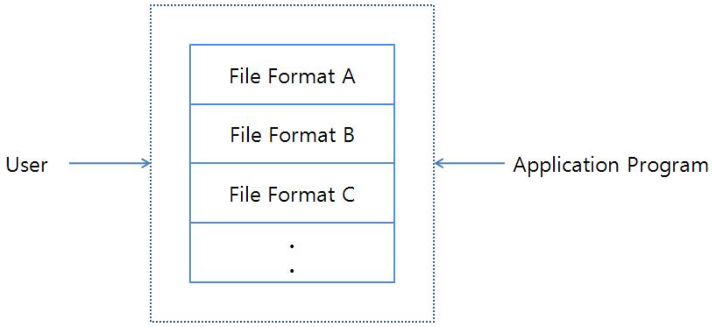


Fig. 7. Improved e Document Security

cess delay which occurs during encryption of database field. In detail, access detection and prevention technology controls non standard SQL inquiry form web application. When the trouble appears in the database security server providing connection -oriented network service, this technology guarantees accessibility allowing the application sever to access database directly.

The fast encryption(decryption) of database and search technology use encrypted index and safe key management which supports the encryption(decryption) of database field. It also provides an index search via index at the same time.

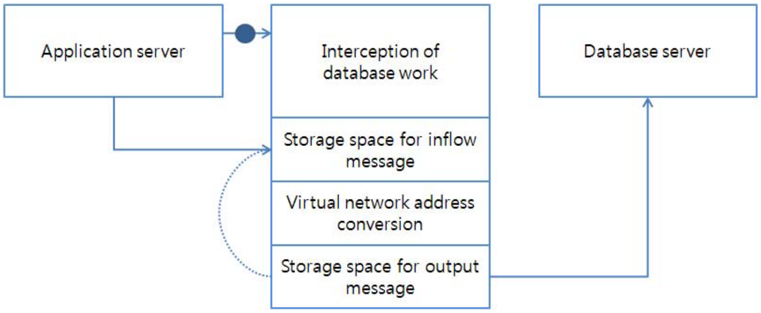

Application server
Interception of database work
Database server
Storage space for inflow message
Virtual network address conversion
Storage space for output message

Fig. 8. Improved Database Security

Eventually, role-oriented network end point security system solves an incompatibility with remote access computer and guarantees interoperability among network access control technologies. It also supports network access control which embodies flexible industry standard infra protection and include user group and environment.

6 Exploratory Study Result regarding Industrial Security Technology

To enhance the international competitiveness by protecting up-to-date industrial technology, we have to analyze the current level of domestic industrial security technology and technical competitiveness[7]. Furthermore it is vital to establish the policy for improving the competitiveness of domestic industrial by devise a policy to support development task. In this study, we analyzed the all-pervading trend and present status of industrial security technology. Then, we conducted the deduction of national development task and analyzed current level of domestic industrial security technology for prevention of industrial technology leakage and improvement of technology.

In detail, we analyzed the status of industrial technology leakage, and grasped the main subject of leakage, channel, and method. We then designed industrial security framework with identification of industrial technology asset, research of literature, and visiting provider and demander of industrial security technology

On the next stage, we applied Delphi Method to the professional group and deduced the segmented development task. As a result, we designed the control system for different types of portable storage devices, integrated security system for industrial technology documents, high-performance database security system, and role-oriented network end point access control system.

The result of this study may be utilized to enhance an international competitive power and devise the policy for industrial security technology development ability as basic contents. Industrial security framework based on researches and practitioners is also anticipated to provide an approach method regarding industrial technology leakage prevention, detection and countermeasure. Hereafter, it is needed to develop information security management system for industrial security specialized in industrial technology protection which can carry out integrated management. There also exists necessity for further research concerning physical and managerial security system for industrial technology protection.

References

1. ISO/IEC: ISO/IEC TR 13335-4: 2000(E).: Information Technology - Guidelines for the Management of IT Security Part 4. (2000)
2. XiSEC/AEXIS Consultants.: BS7799 Information Security SME Guide. XiSEC/AEXIS Consultants. (2002)
3. Forte, Dario.: Information Security Assessment: Procedures and Methodology. Computer Fraud & Security. (2000)
4. Gartner.: Hype Cycle for Governance, Risk and Compliance Technologies. (2008)
5. Gartner.: Understanding Data Leakage. (2007)
6. Hone, Karin and Eloff, JHP.: What makes an effective information security policy?. Network security. (2002)
7. Jan Eloff, Mariki Eloff.: Information Security Management - A New Paradigm. Proceedings of SAICSIT, (2003)

8. M.M.Eloff, S.H. von Solms.: Information Security Management: An Approach to combine Process Certification And Product Evaluation. Computers & Security. (2000)
9. Dodson Rob.: Information Incident Management. Information Security Technical Report. (2001)
10. Weill, P. and M.: What IT Infrastructure Capabilities are needed to Implement e-Business Models?. Vitale MIS Quarterly Executive. (2002)