IEIE Transactions on Smart Processing and Computing, vol. 3, no. 2, April 2014
http://dx.doi.org/10.5573/IEIESPC.2014.3.2.65

Design and Load Map of the Next Generation Convergence Security Framework for Advanced Persistent Threat Attacks

Moongoo Lee

Department of Smart IT, Kimpo College / Seoul, South Korea yeon0330@kimpo.ac.kr

***** Corresponding Author: Moongoo Lee

Received November 20, 2013; Revised December 27, 2013; Accepted February 12, 2014; Published April 30, 2014

** Regular Paper*

***Abstract*:** An overall responding security-centered framework is necessary required for infringement accidents, failures, and cyber threats. On the other hand, the correspondence structures of existing administrative, technical, physical security have weakness in a system responding to complex attacks because each step is performed independently. This study will recognize all internal and external users as a potentially threatening element. To perform connectivity analysis regarding an action, an intelligent convergence security framework and road map is suggested. A suggested convergence security framework was constructed to be independent of an automatic framework, such as the conventional single solution for the priority defense system of APT of the latest attack type, which makes continuous reputational attacks to achieve its goals. This study suggested the next generation convergence security framework to have preemptive responses, possibly against an APT attack, consisting of the following five hierarchical layers: domain security, domain connection, action visibility, action control, and convergence correspondence. In the domain, the connection layer suggests a security instruction and direction in the domains of administrative, physical and technical security. The domain security layer has consistency of status information among the security domain. A visibility layer of an intelligent attack action consists of data gathering, comparison and decision cycle. The action control layer is a layer that controls the visibility action. Finally, the convergence corresponding layer suggests a corresponding system of before and after an APT attack. The administrative security domain had a security design based on organization, rule, process, and paper information. The physical security domain is designed to separate into a control layer and facility according to the threats of the control impossible and control possible. Each domain action executes visible and control steps, and is designed to have flexibility regarding security environmental changes. In this study, the framework to address an APT attack and load map will be used as an infrastructure corresponding to the next generation security.

***Keywords*:** Infringement, Failure, Cyber threat, Administrative, Technical, Physical, Convergence security

1. Introduction

Understanding an Advanced Persistent Threat (APT) attack, which is a new type of cyber-attack that considers the security of the converged correspondence of administrative, physical and technological factors, is extremely important. Without depending on automatic tools and a unitary solution, this study defines the subject data to be protected, and suggests the overall corresponding structures as follows: strengthening access control, reinforcing end point security, cyber security, the encryption of important information, analyzing the strategy of abnormal activities, security education, and the necessity of exclusive organization taking force. This study established a security strategy for each domain based on the factors that need to be reinforced for security. Each domain separates the security strategy and methods into defense, analysis, and control. A subdivided strategy

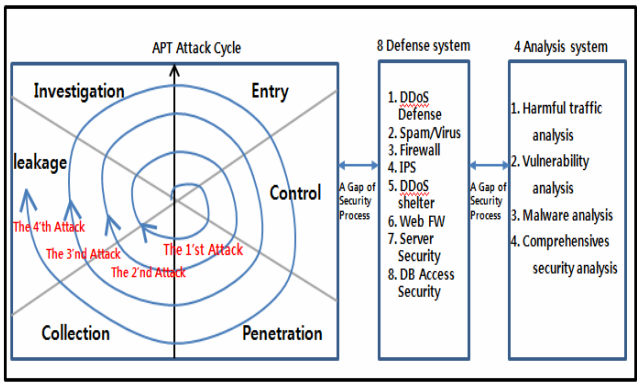

Fig. 1. Corresponding Method Gap of Integrated Security for the APT Attacks Cycle.

designs a convergence security framework based on the connectivity and efficiency, and suggests a road map for this.

2. Features of APT Attack and Necessity to Improve the Defense Strategy

2.1 Features of an APT Attack

In the process of investigation, entry and control, the attacker defines the target and plans the attacking strategy. In the penetration step, it connects to an individual and a group, and plants malignant codes. In the collection step, inside information is collected by operating a remote control bot. In the leakage step, inside information is leaked with a command and control server. An APT attack is a new type of cyber- attack that repeats continuously until it achieves an objective using a range of intelligent attacking methods. The detection of an APT threat is difficult even before a large scale of losses and damage occur or after an accident, and an even a systemized organization can be damaged. This shows that only fragmentary detection cannot penetrate the final attacking objective. The previous 8 level defense (DDoS defense, spam or virus, invasion prevention, invasion blocking, DDoS shelter, web firewall, server security, DB access security) and 4 level analysis (analyzing harmful traffic, vulnerability, malignant code and integrated security) process lacks connectivity and there is a gap. Therefore, it needs to penetrate the attacking characteristics and technological defects and considers the converged correspondence of administrative, physical and security factors [1, 2].

Advanced Threat

The entire APT attacking scenario is “intelligent” in that it is organized through considerable time and effort. Therefore, it cannot penetrate the final objective with penetration detection.

Persistent Threat

To achieve an objective at a great distance of time, six step cycles repeat with the spiral life cycle silently and

Table 1. Comparison of a Mass Market Attack And an APT AttackOF MA.

Division	APT Attack	Parison
Target	Particular Target	Many and unspecified persons
Purpose	Definite purpose	Indefinite purpose
Malicious code malformation	Presence	Presence
Zero-day Exploit	General use	Nonuse
Investigation	Continuous penetration	Minimize
Penetration method	Primarily attack client PC and approach to final target system	Mostly access to vulnerable system directly
Method of purpose achievement	After attaining an authority, systematically and confidentially act	Immediately after attaining authority, act

confidentially, inside or outside of the target organization. As the life cycle repeats for 6 months to 1 year, the attacking skills become elaborate and the scale of damage expands.

2.2 APT vs. Mass-market Attack Comparison

An APT attack does not depend on an automatic attacking tool, it is not standardized and is processed for a long time. Most damage is not recognized before the damage is visualized. In some cases, it cannot recognize the damage even after it has occurred [3, 4].

This requires an improvement in availability because the current converged log analysis system for an APT attack only performs a simple collection other than connectivity analysis between the security USB and the server security. To design the converged security framework against an APT attack, the following requirements need to be met [5, 6].

2.3 Correspondence Strategy for the Next Generation Convergence Security Framework of APT Attacks

A conventional multi security layer for the latest attacks has an independent executing process and performs simple collection except for a server security and connectivity analysis of security USB. Hence, it is a process of simple collection, as shown in Fig. 2. Therefore, although various controls and monitoring of the server security in management infrastructure are consistent, the efficiency of jobs decreases and it becomes unsuitable for an intelligent attack response, such as APT, which can be an persistent attack because it performs an integration analysis processing system according to an integrated log analysis. Therefore, to design a convergence security framework regarding an APT attack, the following requirements should be satisfied.

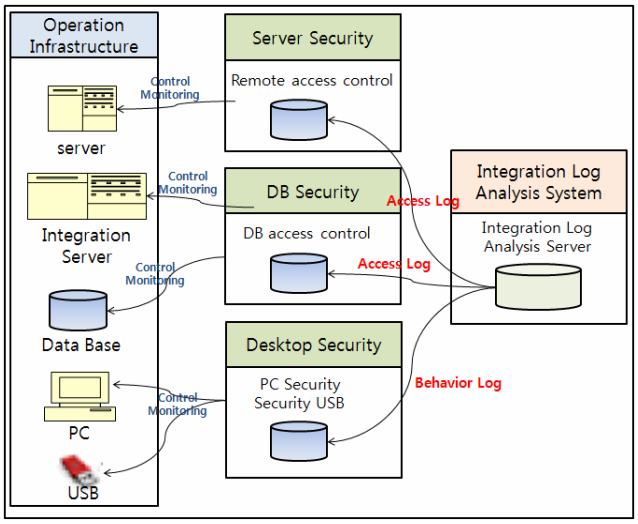

Fig. 2. A simple Log Analysis Process Conventional Multi Security Layer.

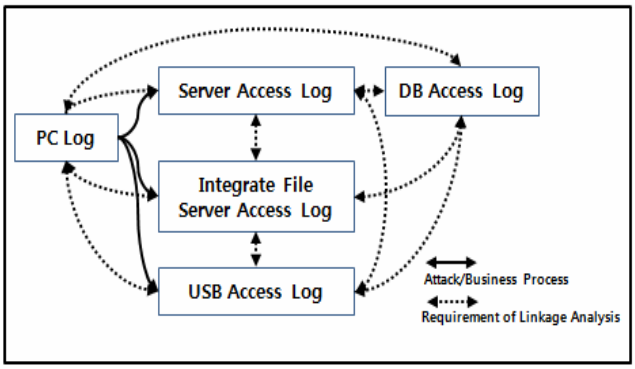

Fig. 3. Example of Process Linkage.

1. Appropriate domain composition

To defend against an APT attack effectively, it should not depend on a unitary solution and automatic tools, and should prepare a corresponding strategy, which is information and human oriented. This should include all 3 domains, which are administrative, physical and technological domains, and the convergence security should be added against a composite threat [7].

2. Connectivity of domains

The connectivity of domains should be constructed so the 3 independent domains are mutually correlated as a convergence aspect. To reinforce correlation analysis, it should analyze the mutual correlation of the connected logs occurring simultaneously and distinguish the normal activities. The system should set an application plan of integrated log analyzed results, and suggest targets, relations, exploration, results and possible intrusion types by standardizing the integrated log analysis result templates.

3. Possibility of preemptive defense

This should convert to a preemptive attack to defend against an APT attack, which can overcome the passive controls of external attacks and consequence management levels.

A preemptive attack is needed to make all defenses possible against an API attack, which is becoming the most intelligent over consequence management levels, passive control of external attacks

4. Flexibility of environment change

Security threat changes continuously and develops. The framework should be changed and developed flexibly corresponding to the changes in the security environment.

3. Design of Convergence Security Frameworks for APT Attack Correspondence

To defend against an APT attack effectively, it should not depend on a unitary solution and automatic tools. In addition, it should prepare a counterstrategy that is oriented to information and humans [8].

3.1 Design of an Administrative, Physical, Technical Security Domain

1. The design of Administrative Security

Administrative Security is a composite of extension that is based on governance, and includes physical and technological security to protect intelligence assets. This also suggests that the guidelines and direction corresponding to compliance and international standards. Administrative security is designed to have 4 criteria (rules, organizations, processes and information), as well as a management cycle, which is an action - plan - check - do. Rule is composed based on the Standard Compliance, ISMS, ISO-20000 and BS-25999 certification, and organization is composed of an Information Security Officer, Security Manager, Security Screening Committee and Related Organization Coordination Scheme.

Process includes personal security, emergency countermeasures, backup and recovery, information system introduction, information security education, and

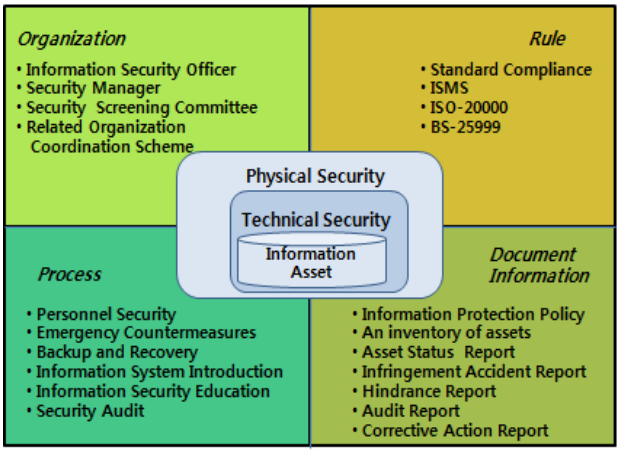

Fig. 4. Design of Administrative Security.

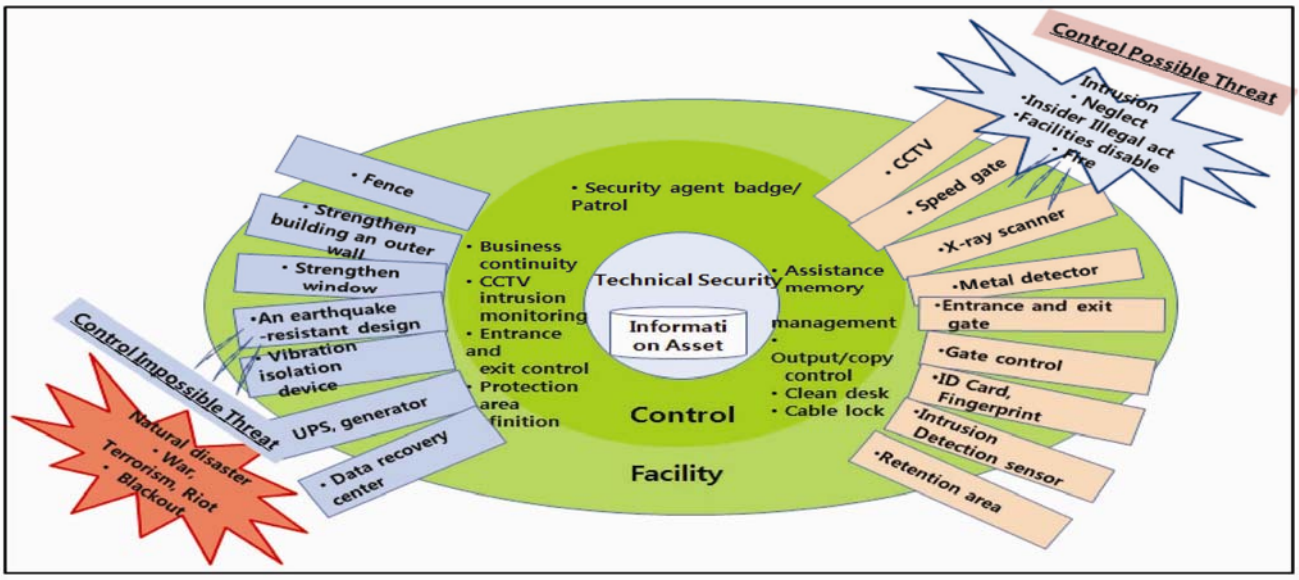

Fig. 5. Design of Physical Security.

security audit. Information has an Information Protection Policy, inventory of assets, Asset Status Report, Infringement Accident Report, Hindrance Report, and Audit Report, Corrective Action Report.

Considering that an insider acts as a medium intentionally or unintentionally, the administrative security corresponding method should be reinforced in terms of social technological attacks. Personal security (insider or outsider) of a process from the 4 criteria should monitor or perform corrective actions periodically to address the social technological attack types.

2. The design of Physical Security

A physical security should be designed to 2 criteria which are a facility and a control, as shown in Fig. 4, to protect information assets. The control criterion is based on security equipment installation, such as a security agent badge, patrol, business continuity, CCTV intrusion, monitoring entrance and exit control, protection area definition, assistance memory management, output and copy control, and clean desk and cable lock. The facility criterion is designed to control both impossible and possible threats.

To respond to control impossible threats, fence, strengthen building an outer wall, strengthen window, earthquake resistant design, vibration isolation device, UPS, generator, and disaster recovery construction, are generalized. The control possible action suggests plans for a reaction against an intrusion, insider's illegal acts, facility disabilities and fires. This can be the entrance and exit control of the data center and computer room against a person without permission. Another control is that even if a person is permitted, he or she cannot be given access to a specific protective area using a metal detector, X-ray scanner and detecting devices. In addition, it is composed of CCTV, speed gate, metal detector, gate control, ID card, fingerprint, intrusion detection sensor, and retention area.

3. Design of Technical Security

Technical security is planned to protect from DDoS(Distributed Denial of Services) attacks throughout the logical approach to information assets, Hacking attempts, insiders' trial to attack, which makes the total directional safeguard possible against external and internal attacks by 8 factors of defense, 10 levels of analysis, and 17 elements of control at technical security systems. Therefore, the strategies of technical security can protect against inter and outside attacks.

The defense criterion starts from attacks of an external internet and it is in charge of the defense of each section, i.e. the network, server, and database. The criterion operates the DDoS response equipment, spam/virus filtering device, firewall, intrusion prevention system DDoS cyber shelter, web firewall, server security solution, DB access security solution, and internal and external net separation. At the analysis level, it performs secondary analysis and correspondence that occur at the defense level. Harmful traffic analysis, integrated security analysis, packet analysis, malignant code analysis, and vulnerability analysis, invasion attempt traces. Honey net, emergency responses are examples of analysis level responses.

The control domain only allows authorized access to information assets. To disconnect illegal acts, such as information spills, with technological methods, it mostly concentrates on preventing intentional or unintentional attacks by users working in computer rooms, developers, system operators, and managers. For this, harmful websites blocking, radio blocking, remote access control, integrated authentication: single sign on, integrated approach console, account management, security USB, PC security, PC data encryption, integrated file server, information leakage prevention are used. Recently, as cloud computing spreads, security under a cloud environment becomes significant. Even in a cloud computing environment, security solutions that are suggested in a control domain are similar.

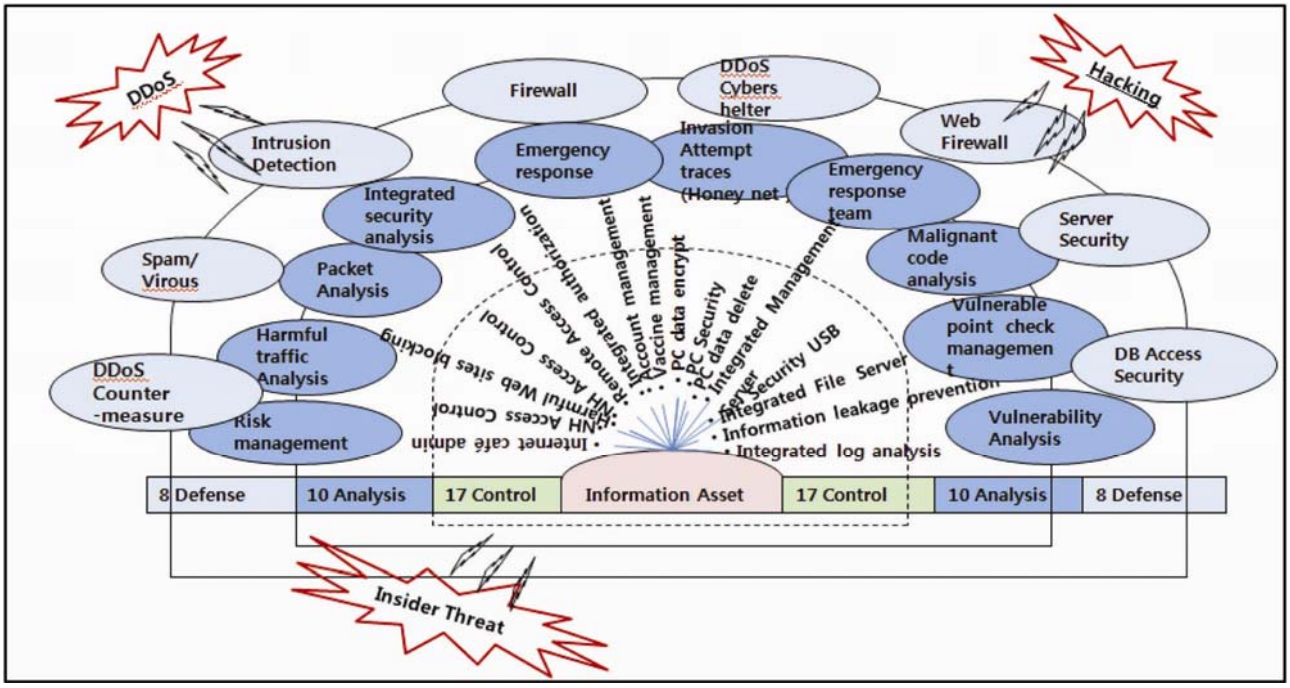

Fig. 6. The Design of Technical Security.

3.2 A Design of Domain Connection Layer

The linkage layers of each domain of the next generation convergence security frame work represents the intersect connections of administrative, physical, and technological security domains, as shown in Fig. 7.

This designs the security in 4 intersections. One is the intersection of administrative, physical and technical securities as a convergence aspect. An intersection between administrative security and technological security, an intersection between administrative and physical securities, and an intersection between technological security and physical security are the other intersecting connections. Historic information of each security domain should be stored as a database and the system should be realized to perform a security task using this information.

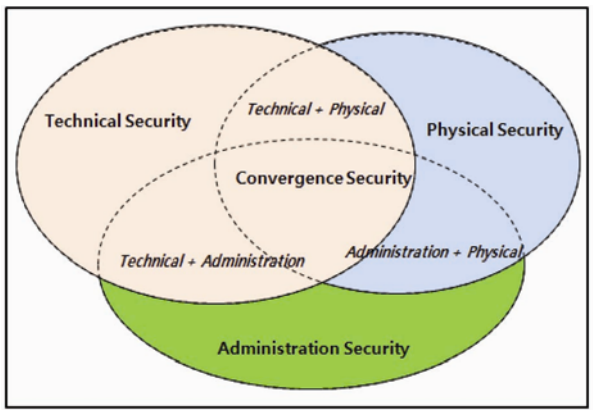

Fig. 7. Diagram of Domain Connection Layer.

3.3 Diagram of an Action Visibility Layer

A feature of an APT attack makes tracking impossible by deleting the traces throughout long term elaborate advance preparation, a phased approach toward an objective, and an attempt to destroy the information assets after achieving an objective. For this, approximately each section, i.e. administrative, physical, and technical security response, processes like 'Business Process Management', 'Entrance & Exit Traceability Management', 'Information Asset Traceability Management', 'Control Terminal(Zero-Client)', 'Cloud Security', should be visualized by repeating the collection, comparison, decision, and notification.

Therefore, a diagram of the action visibility layer, as shown in Fig. 8, should analyze the accumulated data of

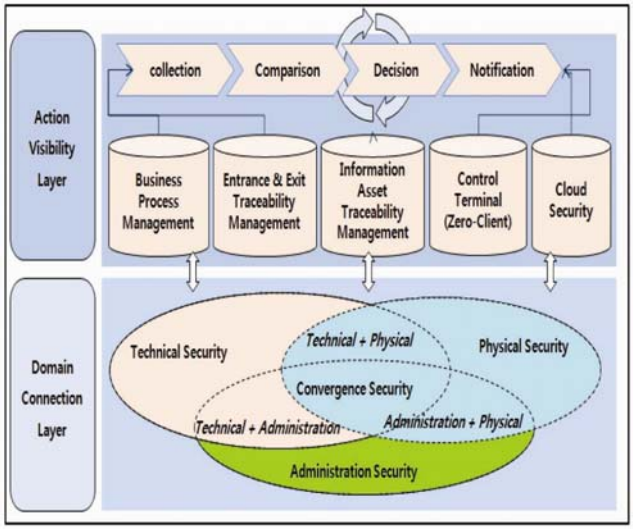

Fig. 8. Block Diagram of the Action Visibility Layer.

the connection layer and provide transparency. The target data of action visibility are classified as follows.

Data based on business process management

BPM provides visibility for all task processes that are performed in data centers or computer rooms. Important task processes represent 4 domains, which are an IT plan and systemization, information system introduction and construction, service operation and supports, monitoring and evaluation, and 34 substructure control processes (defined in COBIT 5.0).

Data of access history management

This maintains and manages all the information that enters and exits the data center or computer center, and these records range from residing workers, transient workers, and visitors.

Data of Zero-Client

In order to direct controls for the user performance, such as the desk top, PC, laptop, tablet PC, and in place of a data center, computer room or access of various terminal units outside of company with VPN, institutes a Virtual Desktop Infra structure (VDI) in an organization, standardizes terminal environment of users and simplifies the access routes.

Data of cloud security

Because of the efficient resource management, the user convenience cloud computing infrastructure introduction is increasing. On the other hand, a conventional computing environment faces risks from the structural features of the cloud environment, such as the operating system, network, process, hypervisors and managers. The system visualizes the administrative activity records, such as cloud computing environment construction based on the encryption skills of TPM (Trusted Platform Module), access control throughout cloud visors, authorized booting, and safe storage set up.

3.4 A Diagram of Action Control Layer

The diagram of action control layer shown in Fig. 8 defines the abnormal activities using the Business Rule Engine (BRE) to control the visualized activities, and it performs performance monitoring by business activity monitoring.

The action control layer consistently detects abnormal actions and makes a judgment. As a process that separates the control terminal from the access routes of a virtual desktop infra-environment by performing a control process by blocking the abnormal activities.

The action control layer performs processes, such as ‘unusual, aberration action definition’, ‘monitoring action definition’, ‘abnormal action decision’, ‘abnormal action disconnection’, and ‘reporting and statistics’.

3.5 Diagram of the Convergence Correspondence Layer

To address intelligent and convergence APT attacks, the system constitutes the visualized layers and forms

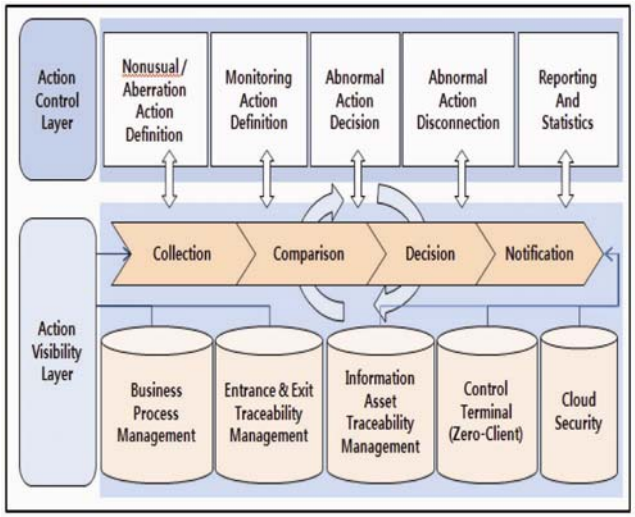

Fig. 9. Block Diagram of Action Control Layer.

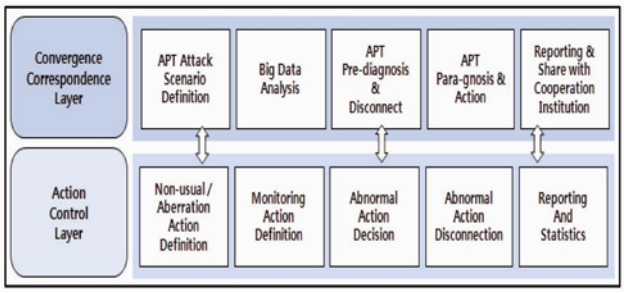

Fig. 10. Block Diagram of Convergence Correspondence Layer.

activity control, ultimately convergence security layers that can block before or after APT attacks about the abnormal activities. The convergence correspondence layer, as shown in Fig. 9, defines the scenario of an APT attack that is known as an APT intrusion attack case.

Throughout the simulation processes according to the characteristics of the information assets, it extracts the attack specialized scenarios. A range of attack scenarios are possible and it defines the scenario for the detection of whole steps of the scenario and middle stages as well. For large data analysis, it introduces high-capacity distributed file systems and composes a SDW(security data warehouse). Based on this, it performs typical or atypical data analysis. In addition, based on SDW, it performs data mining, as well as periodic extraction of an APT attack scenario, and performs the management of changes in the convergence security by instituting convergence corresponding layers.

3.6 Final Design of Convergence Security Framework

Against an APT attack, administrative, physical and technical security realization occurs through the connectivity between administrative and technical security, connection of the administrative and physical security, and technical and physical security connection, which are inter-

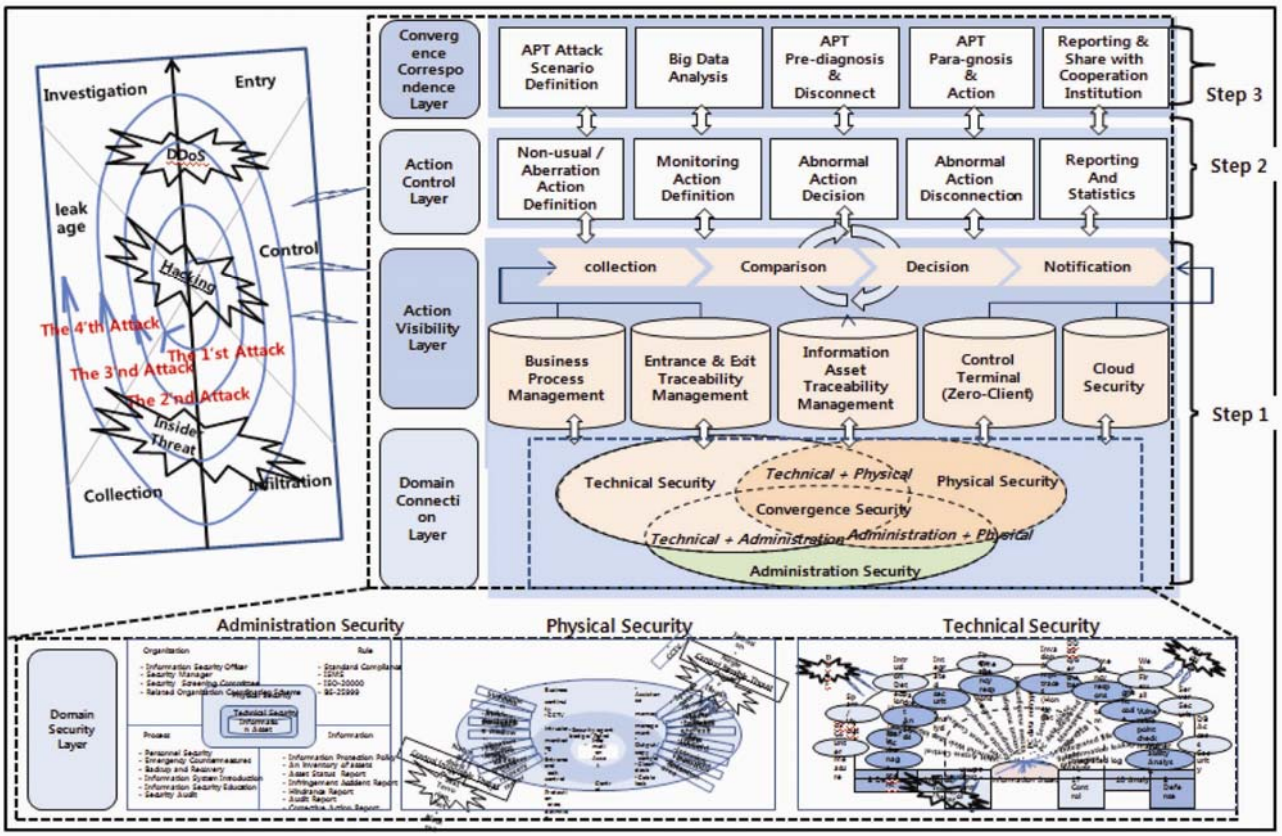

Fig. 11. Convergence Security Framework for an APT Security Strategy.

connecting each security process of each section, and the visualizing layer is the first step of the process. The second process blocks the abnormal actions by controlling visualized actions based on first step.

Finally, the correspondence layer is designed to perform an APT attack scenario definition, 'big data analysis', 'APT pre-diagnosis and disconnect,' 'APT paragnosis and action', 'reporting and share with cooperation institution', as shown in Fig. 11.

4. Load Map of Convergence Security Framework for the APT Attack Security Correspondence

Against an APT attack, the load map of the convergence security framework was performed, as shown Fig. 12.

The first step of the implementation load map is 'connectivity and visualization'. For the first security area connectivity, the administrative, technical and physical security performance should be connected, and the history information connectivity for the events, log data connection should be continued. Secondly, for 'activity visualization configuration', business process management, exit and entrance information management, information asset access history and event management should be performed, and for visualized monitor composition, collection, comparison, decision and reporting process are performed. Thirdly, for 'activity configuration standardization' control terminals, such as zero-client, cloud security, desktop virtualization, VDI(virtualization desktop infrastructure), SBC(server based computing), SaaS, PaaS, IaaS, etc. are applied.

The second step is 'action control activity'. First of all, the abnormal and normal activities are defined. Normal activities perform the business procedures of business process management that are authorized by the users. The abnormal activities are the unauthorized activity that reached critical amounts. Secondly, it constructs action monitoring. At this point, it monitors the performance processes and the event occurrence based on BRE. Thirdly, when the access activity is abnormal or deviated action, the confirmation process should be performed. Fourthly, abnormal performance blocking should be carried out by separating the abnormal activity from the control terminal, VDI route.

On third step of the load map, the 'convergence security step,' APT attack scenarios should be defined by collecting the known scenarios and the detection of specialized attack scenarios. Secondly, in a high capacity distributed file system composition and SDW composition, typical or atypical data analysis, large data analysis by data mining should be executed. Thirdly, by a SBI (Security Business Intelligence) set up, processed APT detection and blocking function, APT pre diagnosis or blocking is composed. Fourthly, the detection of an APT attack that has completely invaded, an APT paragnosis and measures are continued. Finally, a reporting or sharing system with cooperation is realized.

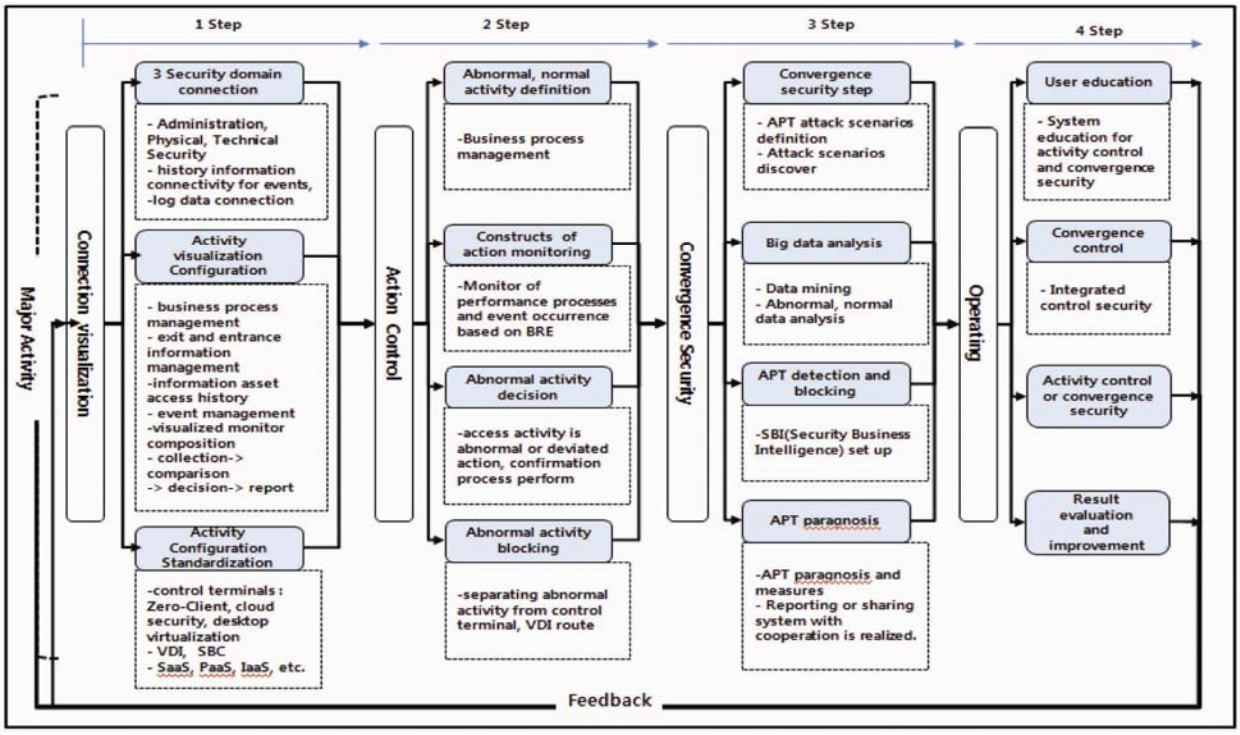

Fig. 12. Load Map of the Convergence Security Framework.

The fourth step is the 'operating' step. Firstly, system education for activity control and convergence security and user education training is performed. Secondly, convergence control is performed from integrated control security to the convergence security. Thirdly, activity control or convergence security performance are performed and the result evaluation and improvement are carried out.

5. Conclusion

This paper proposed correspondence to the next generation convergence security framework and load map against APT attacks. The system is designed to have several layers, such as the connectivity of each domain and each security layer, action visualization layers, action control layer and convergence correspondence and suggested load map of each step. The introduced convergence security framework is designed to manage the changes to convert from an integrated security framework to the convergence security framework by considering the connectivity, sections, and steps. For the suggested APT attack correspondence, the framework and load map are used for the infrastructure of a convergence security correspondence strategy for the next generation security response system.

Acknowledgement

This study was supported by KIMPO College's Research Fund.

References

[1] Command Five Pty Ltd. "Advanced Persistent Threat: A Decade in Review" 2011. Article (CrossRef Link)
[2] AhnLab "A Whole New Approach in combating Advanced Persistent Threats", 2012 Article (CrossRef Link)
[3] Binde, Beth E., McRee, Russ., and O'Conner, Terrence J. (2011). "Assessing Outbound Traffic to Uncover Advanced Persistent Threat". Article (CrossRef Link)
[4] Blue Coat Labs Report: Advanced Persistent Threats, BlueCoat, BlueCoat, 2011. Article (CrossRef Link)
[5] Woo Bong Cheon, Won Hyung Park, Tai Myoung Chung, "Design and Implementation of ATP(Advanced Persistent Threat) Attack Tool Using HTTP Get Flooding Technology", The Journal of Korean association of computer education / v.14 no.6, 2011, pp.65-73 Article (CrossRef Link)
[6] Segyun Park, "(A)Study on Effective APT Attack Defense of Endpoint Level", The korea Institute of Information Scientists and Engineers 2013 Conference. 2013. 6, pp.732-734 Article (CrossRef Link)
[7] Frankie Li, ran2, "A Detailed Analysis of an Advanced Persistent Threat Malware", SANS Institute Infosec Reading Room, Oct 2011. Article (CrossRef Link)
[8] Moongoo Lee, Chunsock Bae, "Next Generation Convergence Security Framework for Advanced Persistent Threat", Journal of the Institute of Electronics Engineers of Korea, Vol. 50, No. 9 September 2013 pp. 92-99. Article (CrossRef Link)

Moongoo Lee is Professor of the Dept. of Smart IT at Kimpo College, Seoul, KOREA. She is the director of the Computer Society at the IEIE. She received B.S. in Computer Science at Soongsil University in 1984, M.S. in Computer Education at Ewha Womans University in 1993, and Ph.D. in Computer Science at Soongsil University in 2000. Her research interests include Information Security, Algorithm Design, and other fields of Computer Science.