Usable Security Management for Network Access Rules of Critical Infrastructure

Jeong-Han Yun[1(✉)], Seungoh Choi[1], Woonyon Kim[1], Hwasun Kang[2], and Sung-Woo Kim[2]

[1] National Security Research Institute, Daejeon, Korea
{dolgam, sochoi, wnkim}@nsr.re.kr
[2] Interaction Design, Graduate School of Techno Design, Kookmin University, Seoul, Korea
kmdesignmediator@gmail.com, caerang@kookmin.ac.kr

Abstract. The security problem of the national critical infrastructure is constantly occurring. In recent years, penetrating into the closure network of the critical infrastructure and attack from the inside frequently occur, so that detecting and managing the internal threat is also a very important security issue. Thus, we developed F.Switch, a network switch that can monitor all traffic without installing a software agent in a controlling system and remotely apply a white-list based access control list (ACL), and we designed F.Manager, which is an integrated management system that can monitor, control and manage multiple F.Switch at the same time, so that the internal security network can be efficiently controlled and managed. In this case, F.Manager, which is an integrated management system, is designed by applying usable security viewpoints and methodologies from the planning period to prevent the decrease of productivity of operator's work due to the manager system which is not user friendly, and we have secured usability that was essential for the control and management of security system by inducing the use of the full function of the program, and discovered the value and role of new usable security in the security area.

Keywords: Integration of security management system · Usable security · Internal network security monitoring · Usability of security management system

1 Introduction

The security problems of the critical infrastructure facility control system that can shake the foundation of the industry such as power, nuclear power, water resource, railroad and traffic system, continuously occur, and the number of occurrences increases every year. To prevent cyber-attacks, most infrastructures consist of closed networks that are disconnected from the outside. But, even in such closed networks, it is difficult to prohibit the entry of external equipment by external personnel for the processing of maintenance or operation of the control system. There are cases of attacks from inside through USB memory penetrating air-gap, so the management of the threat from inside to the control system became a very important security issue.

T. Tryfonas (Ed.): HAS 2017, LNCS 10292, pp. 432–447, 2017.
DOI: 10.1007/978-3-319-58460-7_30

The control system's performance and functionality are optimized for the purpose of security only, so the security agent software might not be available on the system. Due to the stability of systems, the price of tapping equipment and complex cabling reasons, the existing monitoring technique (e.g. mirroring, tapping) on the control system has been reluctant to use (Realistically impossible).

Thus, we developed F.Switch, a network switch, that can monitor all traffics inside the internal network without installing software agent in the control system of the critical infrastructure and apply white list based access control list (network access control list, hereinafter, ACL) remotely.

As described above, F.Switch, was developed to solve various internal security threats, can log all source (IP, MAC, port) - protocol - destination (IP, MAC, port) information of all packets that occurred per the user set unit time, and, unlike sampling based monitoring (e.g. netflow), it monitors all traffics that go through F.Switch to generate log, and can block the traffic that violates ACL and generate alarm, so it solved several problems of the control system security. Also, F.Manager, an integrated management system that can efficiently manage multiple F.Switches installed in the control system network, is designed since there was a problem of the practical security staff having to control and manage multiple F.Switch installed in the control system at once. Figure 1 is the overall concept diagram of F.Manager, the integrated management system.

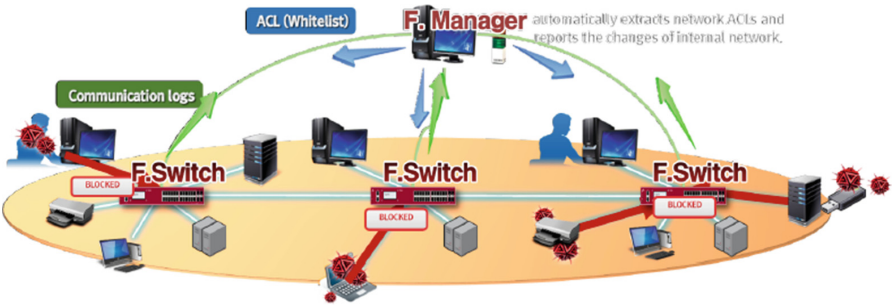

Fig. 1. The overall concept diagram of F.Manager

On this paper shows the contents of the design on the integrated management system, which is F.Manager, through user friendly perspective, that is, the perspective of usable security, during the development of F.Switch, a new concept network security switch that effectively blocks the threat from inside the critical infrastructure control system.

The description of the overall configuration of this paper, which is a development study of the integrated management system F.Manager, in terms of usable security, is as follows.

Section 1 explained the background and purpose of the study on the development of the national key industries control system security integrated management system in terms of usable security, and Sect. 2 introduced the detailed research methods in the

development of F.Manager and explained the secured values through UI screens. Section 3 presented the main functions of the developed F.Manager, Sect. 4 introduced the whole work procedure and integrated information structure diagram designed based on user scenarios, and evaluated the improvement of usability through efficient information design. In Sect. 5, it evaluated the value and role of new usable security in the security area through the system with improved usability and mentioned about the future research.

2 Usable Security Value-Based Security Management System

2.1 Reflection of UX and Usable Security Values to F.Manager

Usable Security is a study that breaks the convention of the security researchers so far that maintaining high security technology and increasing user convenience, that is the security technology and user convenience conflict with each other, Since the interest in the development of user-oriented security technology has been increased by combining human computer interaction (HCI) and user experience (UX) design into information security, it is in 2013 that full-scale research has started in Korea. This study tried to explain that the emphasize on the importance of security shall change from 'Human for System' to 'Human-centered System' and high usability system is not vulnerable to security but is consideration for the users, who are the operators of the security business, and eventually, as a result, this study considered the balance among productivity, user convenience, and security of the security system, which are the goal of usable security, as the most important discovery value, and through the development of F.Manager with the application of UX design methodologies and processes, implemented a human - centered security management system so that users and systems can contribute more to security.

For such purpose, this study looked at the core tasks of the current integrated security management system and the problems in the performance of the core tasks. The key tasks of current critical infrastructure control system's internal network security control is finding the status of the asset at a glance in real time, and verifying what is the communication that is performed by the digital asset used in the standpoint of the security policy to quickly report to the person in charge who can solve the problem when a problem occurs in the verified items, but as in Fig. 2, it is difficult to quickly synchronize hundreds and thousands of assets and security policy to the site situation, and it is very difficult to monitor the changes in the network that continuously occur.

In addition, many changes are occurring continuously but non-regularly during the operation of the control system, such as usage time point, temporary suspension of certain service, starting of new services, introduction of new equipment, and replacement of main-sub system, etc. Security personnel should monitor such status of ACL operations on a daily basis to identify changes in the operating environment as well as identification of assets and services, and continuously analyze these changes to ensure that they are suitable for the security policies and are consistent with actual operation status. On Fig. 2 the graph below, the lower graph shows whether traffic is generated

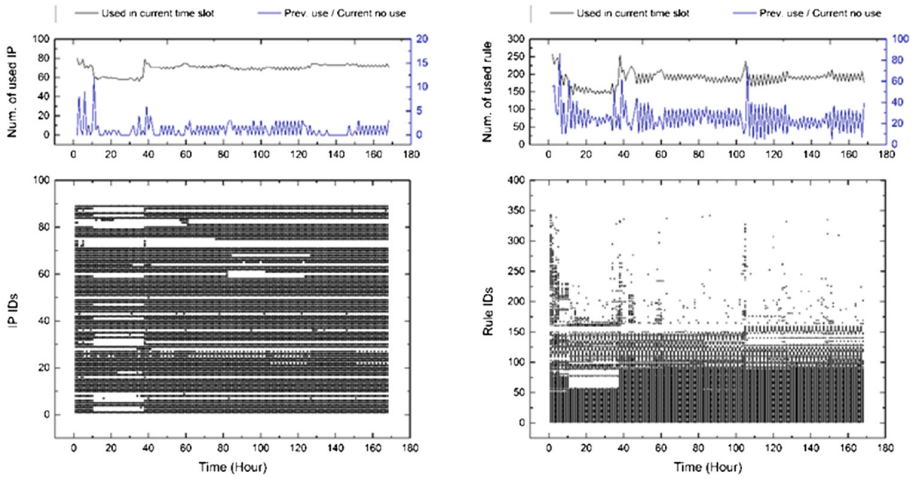

Fig. 2. IP per hour, communication usage (Color figure online)

by IP and ACL per time, and the above graph shows the number of IPs and ACLs currently in use (Black line). It shows the number of unused IPs and ACLs (Blue line). Such work requires continuous analysis of large amounts of data as shown in the above figure, and it cannot be carried out manually, so even if equipment such as F.Switch that can effectively control such status is introduced and F.Manager, integrated management program for integrated management of multiple F.Switch, is developed, if the functions suitable for the work of the security personnel are not provided according to the user's usage frequency or the order of usage, there have to be many limits in the improvement and enhancement of actual work capability at the site, so F.Manager is designed for the users and system to focus more on the value proposition of security from the planning stage.

2.2 Research Method for User Centered Design of F.Manager

For the user-centered design of F.Manager, we developed F.Manager, a new user-centered security management system, through four major research methods as follows. First, we classified the users of the F.Manager, the national key infrastructure control system operators, in terms of UX design and usable security, and analyzed the control system network traffic in real operation and interviewed the related personnel to characterize the security tasks they perform. Secondly, user interface (UI) concept required for UI design of integrated management system was discovered through the derived contents, and integrated information structure (IA) was designed by summarizing all work processes. Third, the work-flow of the functions was summarized through the user scenario based integrated user itinerary map, and the screen design diagram (Wire-Frame) of the entire system functions is developed. Finally, we completed UI/GUI design through wireframes.

Persona Classification and Integrated Needs Analysis. The users who need to perform the works on the system mentioned above vary depending on the level of knowledge related to security and the tasks to be performed. Operational experts (e.g. team leader, system manager, network manager, and security manager) are divided according to information access levels and responsibilities, and simple monitoring personnel also exist. Some users have security knowledge, but in general, there are many personnel who are not the experts in security, and some users are also not familiar with IT technology itself. For these reasons, it is important to classify the main and sub users according to their level of security knowledge and scope of work, and to identify their needs, and it can be said that it is essential to analyze their work processes on the systems, to design efficient work processes through it, and to list up the information during the design of the management system.

UI Concept and Information Architecture. The needs required by the users were derived by analyzing the tasks and paint points in the course of performing the tasks by the users who use the system the most, and system UI concept of F.Manager finally summarized through this is as in Table 1. Once the needs are identified through the UI

Table 1. System UI concept for F.Manager

<table>
<tr><td>UX, usable security oriented strategy</td><td colspan="3">Research & analysis</td><td>Ideation & define
User/system/design UI concept</td></tr>
<tr><td rowspan="5">User goal: easy, fast, and convenient</td><td rowspan="11">System task analysis / System analysis / User needs analysis / User scenario (key task & features finding)</td><td rowspan="5">Minimize risk / Rapid recovery</td><td>Error handing</td><td rowspan="5">Relief: relief, relaxation, reduction, alleviation
Alleviate many worries on the handling and operation of the system to help comfortable system operation by users</td></tr>
<tr><td>Stability</td></tr>
<tr><td>Error-less</td></tr>
<tr><td>Predictability</td></tr>
<tr><td>Secure</td></tr>
<tr><td rowspan="5">System goal: optimized information system</td><td rowspan="6">Simple procedure / Easy to control / Easy to understand / Easy to manage / Customizing-information-classification</td><td>System simple</td><td rowspan="5">Easy: easy, simple, soft, hand-down
Function operation and procedure through system's information system and information is designed to be as simple as possible to help the easiest understanding, handling, and management of the system by users</td></tr>
<tr><td>UI simple</td></tr>
<tr><td>Operation simple</td></tr>
<tr><td>Managing simple</td></tr>
<tr><td>Perception simple</td></tr>
<tr><td rowspan="6">UI design goal: interface design that most effectively shows the optimized information and business design</td><td>Procedure simple</td><td rowspan="6">Convenience: efficiency, convenience, comforts, optimization
It is the same context as the above easy, but, through the display of the situation and information in the system, it minimized the information, process, and operation system compared to the supplied effort and partially permitted personalization to provide the optimized system handling to the users</td></tr>
<tr><td>Information architecture simple</td></tr>
<tr><td rowspan="4">Current state check / Customization</td><td>Efficiency</td></tr>
<tr><td>Economization</td></tr>
<tr><td>Optimization</td></tr>
</table>

concept, it is necessary to integrate the analysis of various tasks and the execution procedures of the tasks, and the information architecture of F.Manager was designed by concentrating on the organization and structure of the contents so that the users are well guided on the structure. As such, it shows that making useful contents structure beyond the complexity of information through the analysis of entire tasks matching the context and the scenarios of the tasks is the most important task of IA. A more advanced and detailed F.Manager IA will be mentioned in Sect. 4.

Workflow, Wireframe of F.Manager. Figure 3 shows Workflow and Wireframe of batch registration of non-registered IP in Whitelist creation wizard page. Which will fix inconvenient tasks of finding non-registered IP list and manually registering one by one were summarized as minimized process through the writing of Workflow, and it was designed to check non-registered IP list in one screen and to complete the batch registration. As such, the functions suitable for the work of the security personnel were designed using experience design methodology to improve the productivity.

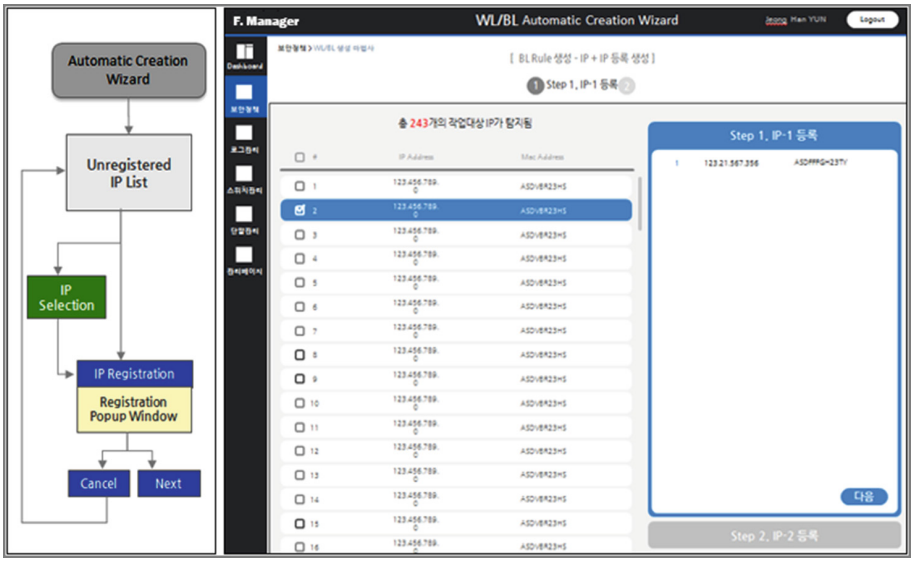

Fig. 3. Workflow, Wireframe of Whitelist/Blindlist automatic creation wizard

3 F.Manager's Main Functions

3.1 F.Manager's Main Functions and UI from the Perspective of UX, Usable Security

One of the most core tasks when a user performs internal network security control is first to understand the status of assets in real time. And secondly, it is to verify the communication performed by the digital assets in use in terms of security policy, and if

problem occurs, quickly reporting to the person in charge who can solve the problem, and this section briefly introduces the main function of F.Manager designed with sufficient considerations of user task characteristics, and tries to explain by presenting the system screen designed with maximum consideration of the user experience.

Dashboard. F.Manager's dashboard is a page that verifies the view of various information in a single page in order to look at system management and control at a glance, and it is designed by analyzing the tasks that shall be performed by the user in the order of the importance of the information and priority of the works.

Figures 4 and 5 are the dashboard information design through the analysis of the importance of the information and work priority and actual UI designed through it.

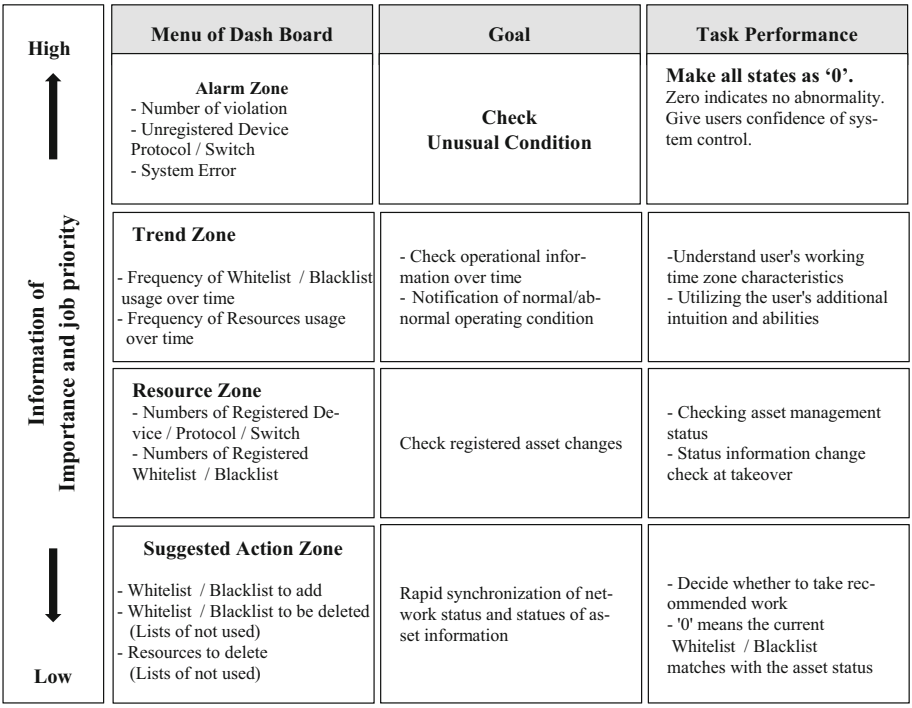

Fig. 4. Information & task priority on dashboard

Client-Sever Relationship Automatic Creation Wizard. There are already many network switches that provide traffic control functions using ACL even if they are not F.Switch. However, as we have seen in the previous section, in order to manage a single control network, it is necessary to create and manage hundreds of IPs and ACLs, and if the user has to manually create all these rules, the user experience has to be bad naturally.

- **NOT easy:** It is difficult to gather information of all devices in SCADA network.
- **NOT convenience:** It is inefficient to manually generate ACL regarding not only service oriented control system but also default service provided by operation system.
- **NOT relief:** It is anxious to make and apply ACL due to the possibility of human error.

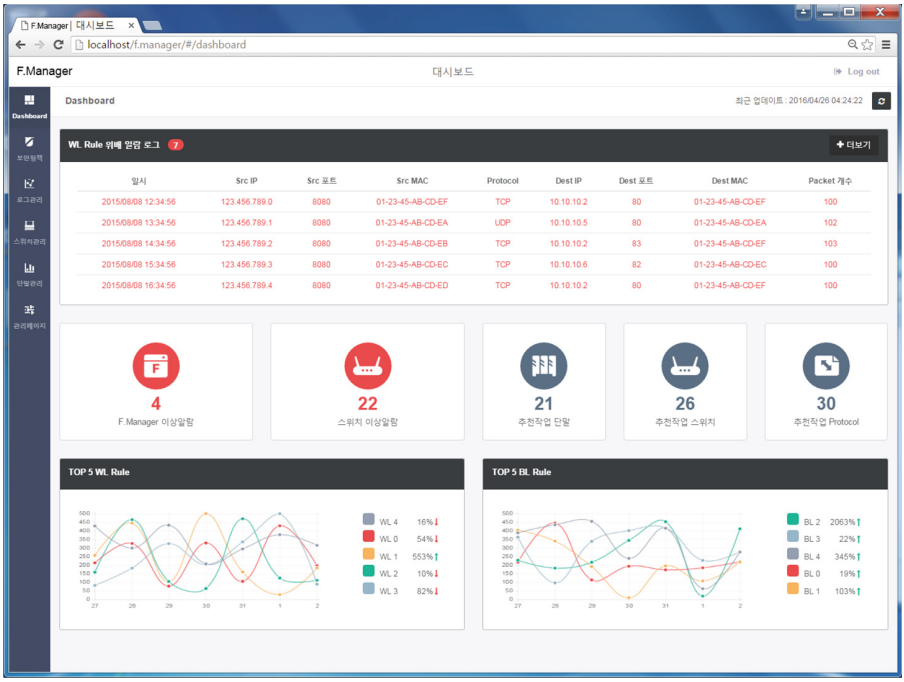

Fig. 5. F.Manager dashboard

F.Switch generates a source-destination type log for all traffic in real time and sends it to F.Manager. F.Manager provides the function to automatically generate server-client type ACL rule using algorithm from collected log information while storing and managing it. This allows users to easily and efficiently extract all communication relationships. The automatically generated result is the server-client relationship that occurred during the user-specified period, and in order to use it as a security policy, the user needs confirmation. Thus, for users to be able to systemically check the generated result and feel safe, and for users to be able to first check the asset information (IP, MAC) and information on the service in use, which can be easily identified at the site, screen providing ACL information is composed as in Fig. 6.

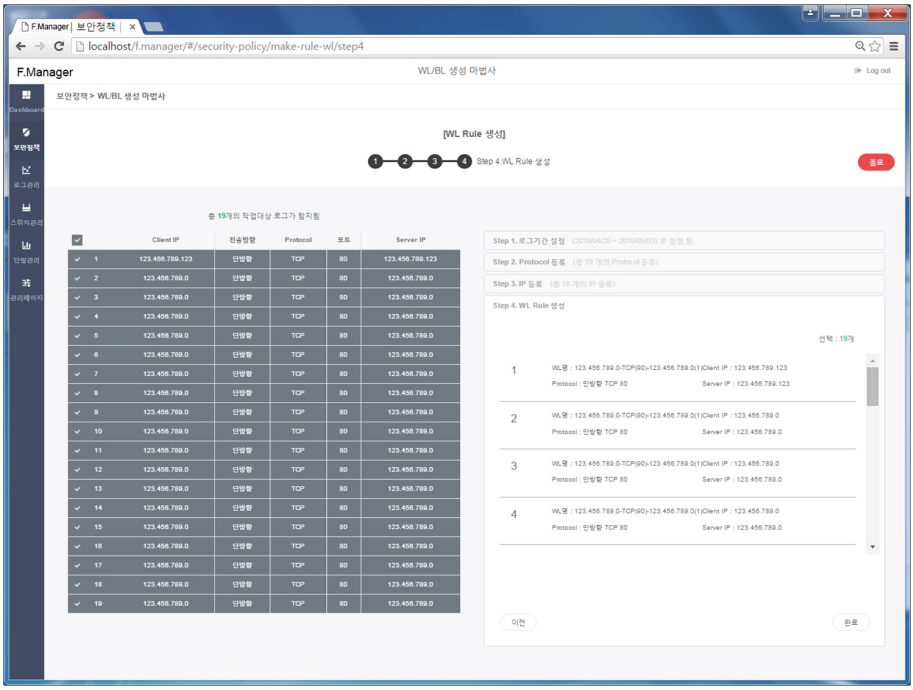

Fig. 6. Automatic generation rule list requiring the decision on whether to apply to the system

Integrated Management Function for Security Rules. Security rules integrated management function. If several F.Switch are introduced and used in one network, the following pain points exist if you need to separate and manage ACLs applied to F.Switch individually.

- **NOT easy:** It is not easy to divide the ACLs required for individual F.Switch exactly based on auto-generated ACL.
- **NOT convenience:** If you need to apply the divided ACL to individual F.Switch, and if you need to change ACL information, such as introducing a new system, the process of finding F.Switch that requires change of ACL at every time is inefficient.
- **NOT relief:** There is an anxiety over whether all ACL corresponding to F.Switch are well divided and correctly applied.

The integrated security rules management function is provided to the user as an integrated form of ACL. Users can manage ACL as if one firewall was introduced in the internal network area where F.Switches was applied. As shown in Fig. 7, the integrated management function automatically distributes the ACL for the monitored traffic for each F.Switch and you can check the application status in real time. Users can feel relieved since they can check that the security policy is well applied to all F.Switches.

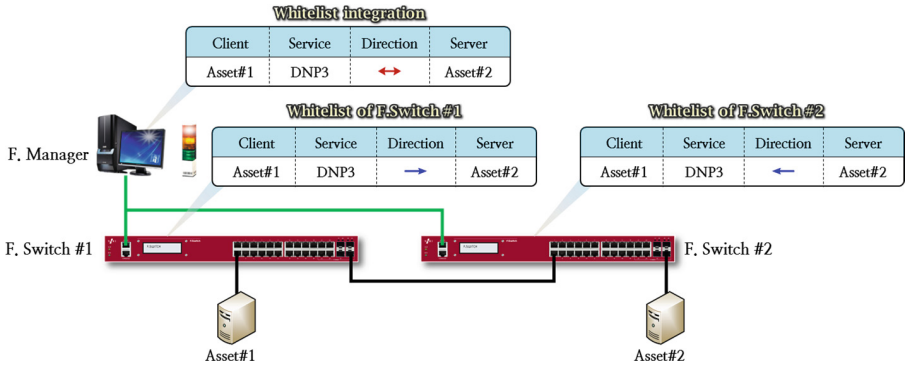

Fig. 7. Whitelist management

Blindlist Feature. It is the main task to help most of the users who check the alarms in real time for prompt response by notifying the information to the relevant person in charge, rather than taking the countermeasures directly. At this time, in order to inform the alarm to the related personnel, firstly, it is necessary to be able to distinguish the type of the alarm, and it is necessary to find the person corresponding to the alarm and quickly transmit the alarm information. That is, it is the first task to identify and distinguish the notifications that have not yet reported, and the second task is to confirm the follow-up of the alarms after the report has been made. The difficulties in performing security tasks with Whitelist based security alarms are as follows.

- **NOT easy:** When an attack or anomaly signal occurs, many alarms related to this occur. It is difficult to distinguish many alarms that occur in real time, so that it is difficult for the user to accurately report to the persons in charge of the alarms.
- **NOT convenience:** Existing systems often show redundant alarms together, but most of the time, the alarms are combined and recognized with the previous input attack pattern. If the user cannot manage the filtering of the alarm suitable for the characteristics of the user according to the relationship by abnormality signal and reporting system, even if the function is excellent, it is inefficient for the user's task.
- **NOT relief:** If alarms are continuously generated, it is difficult to confirm whether the report has been completed to all the related persons, and there is an anxiety that the user cannot be sure of the start and end of the work.

If the persons to whom the information is to be transmitted are determined by the characteristics of the alarm, the user should be able to immediately check the only alarms that he/she should newly report in addition to the alarms that have completed the reporting. For this purpose, Blindlist function was designed and inserted into F.Manager as Fig. 8. Blindlist function does not generate alarms with user defined characteristics in real time alarm window, so that user can easily input characteristics of alarm that need not to be seen at present. This allows you to easily see the alarms that need to be reported by removing alarms from the real-time alarm window as described above.

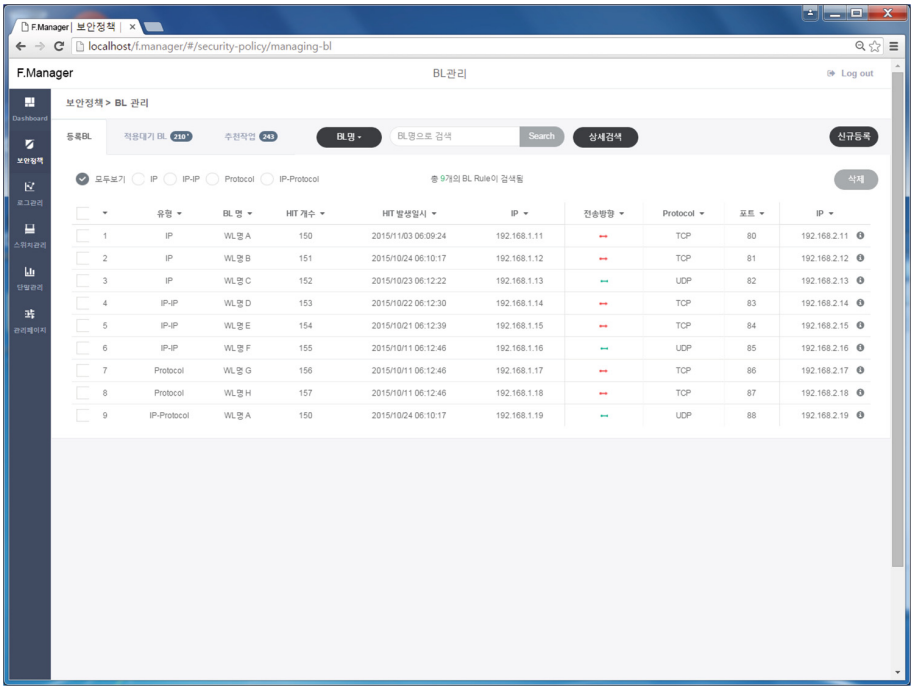

Fig. 8. Blindlist management UI

Alarms of Unused Rules. The user creates the security policy with Whitelist and manages alarms using the Blindlist. The rules written as such are meaningful for the corresponding traffic to occur. The absence of traffic corresponding to the rule may indicate that the rule does not properly reflect the characteristics of the site. If there is remaining security policy for communication and equipment that are not used currently, or if there is remaining blind list rule for alarm that does not occur any more, it is not just favorable for the security, but also, it may cause several adverse effects such as causing confusion for the information recognition by the user (Fig. 9).

In the control system site, there is a separate process for discarding and stopping the equipment, and when the request is received, the related security rules are often manually deleted. Similar things also happen to Blindlist. There are the following problems when rule removal must be performed manually. If the works are carried out as such, there are the following problems.

- **NOT easy:** When an application for deletion due to the disposal of equipment is received, the user should search all relevant rules based on the information and operation status. And the user has the inconvenience of continuously checking the log and operation information in order to determine when Blindlist rules created for temporary use by the user are unnecessary and need to be deleted.

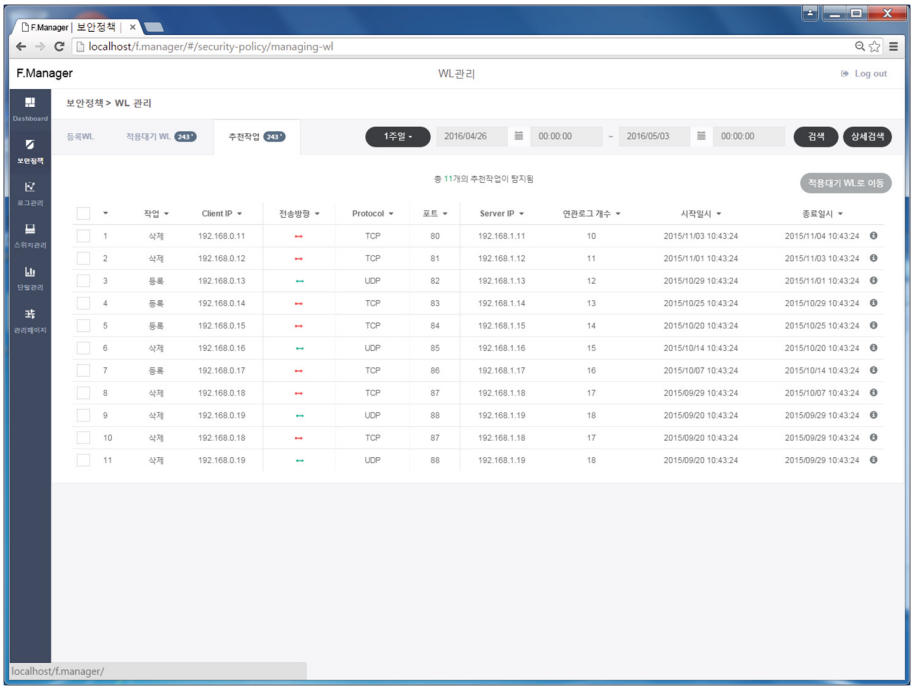

Fig. 9. Suggested actions of unused rules

- **NOT convenience:** The process of manually synchronizing the off-line information such as the report of the relevant personnel and the security rules of the F.Switch monitoring the network in real time, or performing the "automatic generation of the server-client relationship" every time for several information updates are also inefficient.
- **NOT relief:** It is difficult to confirm whether the reporting information of relevant personnel is being performed quickly and accurately and clearly reflected in the security policy, so the security officer may always feel anxiety about the synchronization between the current operation status and the security policy.

We have added the function in F.Manager to tell users if there are rules for Whitelist based ACL and blind list that are have not been used for more than the user specified period. The F.Manager notifies the users of unused rules (no traffic corresponding to the rules) for user specified period of time. This allows the user to more quickly synchronize the status of the site and the security policy. Also, this function can identify and recognize the phenomena that the equipment and service that are to be continuously operated are temporarily stopped.

4 Improved User Experience on F.Manager

4.1 Organize Task Procedures as User Scenarios

IA, user scenario, workflow, and wireframe are designed to preserve the contextual flow of the series of the work processes performed by user with F.Switch and F.Manager during the development of F.Manager applying the usable security perspective and methodologies, and Fig. 10 is an image representatively showing the most core task execution procedure.

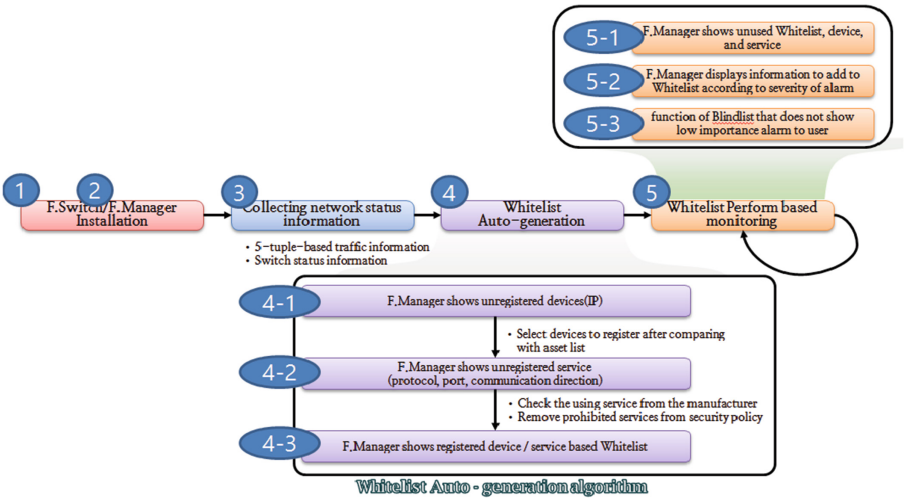

Fig. 10. F.Manager task procedures

It is the process of 1. Installation of F.Switch, 2. Installation of F.Manager, 3. F.-Switch collects network communication log and status information in real time and sends it to F.Manager, 4. Creates and applies Whitelist. 5. Based on this monitoring/observing, 5.1 Recommending of unused rules continuously and repeating the process of checking, deleting unnecessary rules, 5.2 periodically update the Whitelist information using "Whitelist auto generation function [1]" to match asset management status with Whitelist information. 5.3 In case of Whitelist violation alarm, it shows only the alarm that the security officer should perform the corresponding task using the Blindlist.

With this process, it is possible to quickly acquire, control, and manage the program by minimizing the screen switching frequency, touch frequency, and job input frequency naturally on the system.

4.2 Integrated Information Architecture of F.Manager

Figure 11 is the information architecture of newly designed integrated F.Manager through analysis from UX and usable security perspective. Dashboard, terminal

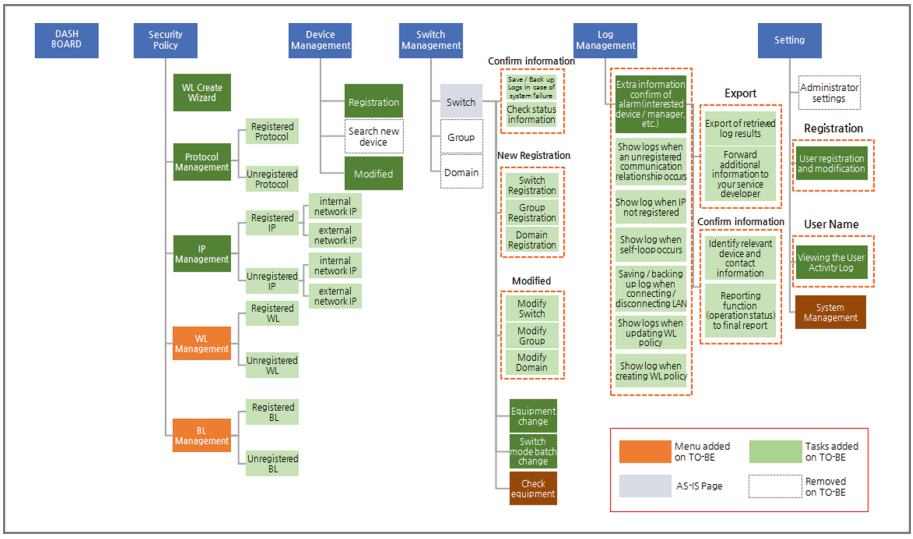

Fig. 11. Integrated F.Manager information architecture

management, switch management, and manager pages, which existed in the past, have been upgraded to reflect the needs of users as much as possible in terms of functions, tasks, and procedure in the tasks. Through personal analysis and entire system analysis, the tasks that improve the manager's business productivity were newly developed, and essential functions are added. They are the functions that are intensively mentioned, including automatic server-client relationship generation wizard security rule integrated management function, Blindlist function, and alarms for unused rules. These functions are intensively applied and designed to the second menu which is security policy and the fifth menu of analysis. In the security policy menu, functions of checking Whitelist security policy information, checking Whitelist security policy violation information, and checking Whitelist security policy change information are added, so that the manager can check asset information easily and quickly. When creating a security policy, the new registration became easier and the task of manual creation became simplified. Furthermore, the automatic generation function added, so after the generation of Whitelist, it can be applied to all F.Switch automatically in batch. Security policy modification and update functions have been also added, and Whitelist update work procedure for F.Switch to add, replace, and remove has become easier and more convenient because of recognition and execution tasks with security policy check and update application. In terms of security management, observing people direct access to network devices or servers is as important as monitoring network traffic. To this end, F.Switch generates an event when the LAN cable is physically connected to/disconnected from the connection point (self-looping), and the security manager can check the alarm and log management function in F.Manager of those events.

4.3 User Productivity Improvement

Prior to evaluating usability through on-site testing at various sites, we tested indirectly the usability improvement using network traffic collected from the key infrastructure control system for F.Switch and F.Manager, and you can check the results in Tables 2 and 3.

Table 2. Usability inspection of system UI through network traffic

Main page	Sub page	Action	Use frequency		Information accessed		Human error		Memorability		Feedback	
			Prev.	Proposed	Prev.	Proposed	Prev.	Proposed	Prev.	Proposed	Prev.	Proposed
Security policy	Whitelist	Add	6	6	1	0	4	0	1	0	0	5
		Modify	6	6	1	0	4	1	1	0	0	0
		Delete	2	2	0	0	0	0	0	0	0	1
		Detail	1	1	0	0	0	0	1	0	0	0
		Confirm	2	3	0	0	0	0	1	0	0	2
	Protocol	Add	11	9	1	0	9	3	1	0	0	3
		Modify	1	10	1	0	0	3	1	0	0	0
		Delete	2	2	0	0	0	0	0	0	0	1
		Detail	1	1	1	0	0	0	1	0	0	0
		Confirm	2	4	0	0	0	0	1	0	0	1
	IP	Detail	2	1	0	0	0	0	1	0	0	0
		Confirm	2	3	0	0	0	0	1	0	0	2
	Whitelist wizard	Protocol	11	1	1	1	9	0	1	0	0	1
		IP	14	1	1	1	5	0	1	0	0	1
Switch	Switch	Add	12	8	1	0	4	3	1	0	0	0
		Modify	12	9	1	0	4	3	1	0	0	0
		Delete	2	2	0	0	0	0	1	0	0	1
		Detail	1	1	1	0	0	0	1	0	0	0
	Switch group	Add	7	7	0	0	5	5	1	0	0	0
		Modify	7	6	0	0	5	3	1	0	0	0
		Detail	1	1	1	0	0	0	1	0	0	0
Device	Device	Add	14	14	1	0	5	5	1	0	0	0
		Modify	14	14	1	0	5	5	1	0	0	0
		Delete	2	2	0	0	0	0	1	0	0	1

Table 3. Summary of usability comparison

Features	Existing F.Manager	New F.Manager
No. of user touch (handling)	135	114
No. of screen conversions	13	2
No. of direct user inputs	59	31
No. of hindrance to information recognition	22	0
No. of providing feedbacks	0	19

First of all, Table 2 shows the results of the frequency of occurrence of representative needs attributes of managers in operation of F.Manager such as accessibility of the information, user error, easiness of remembering, and providing feedback, etc. through the security policy with the highest frequency of usage and menu of switch and

terminal management page, and information accessibility is increased, user error is significantly decreased, and required feedback and guideline are provided at the right time to greatly improve overall productivity [2].

Table 3 is a comparison table of existing F.Manager and the new F.Manager advanced through UX and usable security perspective, it measured the user experience improvement by comparing the number of screen switching times, the number of user manipulations, and the number of direct user input, and the reason that the operation frequency of new F.Manager is remarkably lower is because of the result of achieving process execution through semi-automatic input on the system and minimizing page switching with the consideration of efficiency in UI design. In addition, the number of hindrances of information recognition has been reduced from 22 to 0, and the number of feedbacks has been increased from 0 to 19, so it can be evaluated as that, it maximized productivity and usability together in system management and control as a result of eliminating human errors by the users.

5 Conclusion

We developed F.Switch, a network switch equipped with security function such as a firewall, to prevent cyber accidents by promptly responding to cyber threats while monitoring the entire internal network of the national key infrastructure control system. Internal network monitoring information from F.Switch can be cooperated with various security analysis solutions such as SIEM, etc., so it can be widely used in many ways. However, if the functions appropriate to the user and the characteristics of the user's business are not provided, the user cannot utilize F.Switch effectively and it is judged not as effective to improve the security, so we designed F.Manager, the integrated management system for F.Switch, and we designed the system from usable security perspective so that users could easily and efficiently utilize F.Switch to perform security work. With F.Switch and F.Manager, it can be used not only for rapid asset management, efficient internal network security control, and security policy information management and application, but also for the proper management of service companies, and we expect that it will be a big help for security policy synchronization of individual sites. Since F.Switch and F.Manager are only indirectly tested using network traffic collected from key infrastructure control system, it is difficult to verify 100% improvement of usability of system, but we will test in various sites and continue the study of upgrading of programs that include the needs of the sites.

References

1. Choi, S., Chang, Y., Yun, J.-H., Kim, W.: Traffic-locality-based creation of flow whitelists for SCADA networks. In: Rice, M., Shenoi, S. (eds.) ICCIP 2015. IAICT, vol. 466, pp. 87–102. Springer, Cham (2015). doi:10.1007/978-3-319-26567-4_6
2. Hornbaek, K.: Current practice in measuring usability: challenges to usability studies and research. Int. J. Hum Comput Stud. **64**(2), 79–102 (2006)