A Method of Selecting Optimal Measures for Security and Usability with Fault Tree Analysis and State Transition Diagram

Koichi Kato* and Yoshimi Teshigawara**

*, **Graduate School of Engineering, Soka University, Japan
*kokatou@soka.ac.jp, **teshiga@t.soka.ac.jp

Abstract -A network must have enough usability to achieve its constructional purpose and enough security to protect information assets. Security and usability, however, are in a trade-off relation. To select appropriate measures is difficult because of following reasons: (i) chain relations exist in risks, in services use and between them, and (ii) risks, usability and measures have complex relations. This paper proposes a method of analyzing risk/usability in consideration of chain relations and selecting measures for security and usability, using fault tree analysis (FTA) and state transition diagram (STD). Furthermore, by using probability of state transition, the STD can be converted to a Bayesian network and thereby our method can infer causes of incidents. As a result, the method can also select effecting measures to manage and monitor the network.

Keywords: Risk Management, Usability, Fault Tree Analysis, State Transition Diagram, Bayesian Network.

1 INTRODUCTION

Recently, a variety of network environments are being constructed, such as home networks, enterprise or university networks and high-speed public wireless networks. These networks are established for various purposes of accessing to the Internet as well as resource sharing, business efficiency, etc.

On the other hand, information systems on a network have many risks such as hacking and information leakage. The occurrence of a risk event may cause not only direct damages by business suspension or system recovery works but also loss of organizational credibility. Therefore, today a variety of measures to reduce risks are taken in a network.

In order to achieve original purposes of a network, striking a good balance between security for protecting information assets and usability of services is important. However, security and usability are generally in a trade-off relation. For example, security measures can disturb comfortable use of information systems by increasing steps of the using process for users or slowing down the execution speed of the systems. Excessive security measures decrease usability level. In contrast, excessive usability decreases security level. Consequently, to balance security with usability is difficult.

In addition, to manage and monitor the points related to risks and usability are important measures to check whether security issues happen and services are properly provided [1]. However, to decide appropriate monitoring points is difficult in a network locating with many devices.

As the related work, in order to decide the priority of risks to deal with, Zuccato [2] described the decision matrix and Guan et al. [3] evaluated security with Analytic Hierarchy Process (AHP) and the risk level matrix. They analyzed risks from a certain viewpoint such as an expert and did not consider existence of multiple stakeholders. Yajima et al. [4] suggested the multiplex risk communicator to decide measures based on the agreement among stakeholders. However, they did not analyze usability in detail. Kotenko and Stepashikin [5] as well as Wang [6] described each security evaluation method using the attack graph. They could analyze events of incidents and decide measures visually in consideration of the network configuration. However, they cannot express effects on usability caused by the selected measures.

Our research has approached the matter in two ways: (i) a method of selecting optimal measures at changing implemented measures [7] and (ii) expression model of risks, usability and measures [8]. This paper proposes a method of selecting optimal measures to construct a network that has enough usability to operate businesses and enough security to protect information assets by combining above-mentioned method and model. This method analyzes phases of risks and services use with FTA and STD. As a result, we can quantify risks and usability and select optimal measures intuitively by visualizing risks, usability and measures.

2 RESEARCH ISSUE

2.1 Risk and Usability Analysis with Chain Relations

There exist relations of risk chains that the occurrence of a single risk event causes other multiple risks. In addition, in the risk chains, an elemental event in the process of an occurrence of a risk event may diverge to other risks. Similarly, there exist relations of usability chains that deterioration of a usability level causes a decrease in other usability levels. Therefore, analyzing relations among risks and usability with chain relations is needed to maintain usability levels and to reduce risk levels.

2.2 Relations among Risk, Usability and Measures

Relations among measures and risks/usability are complex. Several measures can be taken against a single risk. On the contrary, a measure also can be effective to some risks. Moreover, measures for risks may affect some

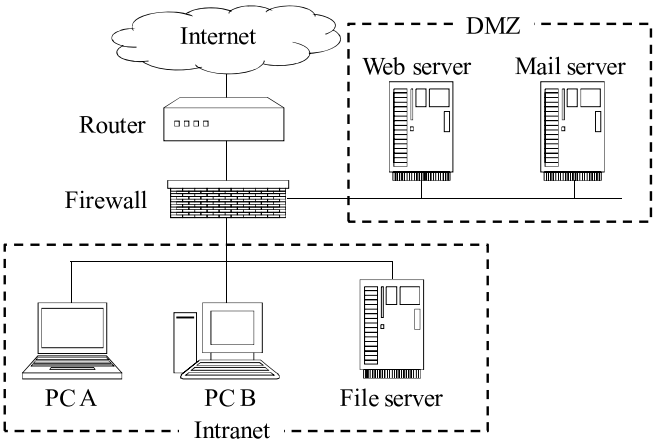

Figure 1: Example of network configuration.

usability. Therefore, analyzing these relations properly and effectively is needed.

2.3 Optimal Measures Selection

We define the meaning of "optimal measures" as a combination of measures that system administrators and users accept with satisfaction about security and usability at the time. Our research targets both phases of implementing measures and changing ones. The requirements for security and usability can vary depending on the situation such as that administrators and/or users require higher level of security or usability.

Objective evaluation of security and usability level earned by candidate measures are needed to select appropriate measures. Our method quantifies probability and the value of risks, which are general metric, and usability. The value of usability in our method is the rate of comfortable service use based on a completely free use of the service with no affects by measures.

We may select excessive or insufficient measures which cause unexpected security and usability decrease only with calculating theoretical optimal measures. Therefore, a scheme to decide appropriate measures intuitively for system administrators and users is needed.

In addition, the validity of monitoring points for security/usability cannot be evaluated because the points are often decided by experimental rules. Moreover, there exist no objective metrics to infer causes of incidents at the occurrence of a risk event. Then objects of analysis to identify the causes may spread unnecessarily. Therefore, a scheme to select monitoring points and specify the causes of incidents is needed.

3 RISK AND USABILITY ANALYSIS WITH FTA

Our method adopts FTA as a quantification method. FTA has following features: (i) it can analyze preventive factors against an achievement of a specific goal, (ii) it can organize measures to control each factor and (iii) it can decide appropriate measures to exact points. FTA makes Fault Tree (FT) that the top is an event as the result of an occurrence of other causal events and these events are joined by logical AND/OR gates [9].

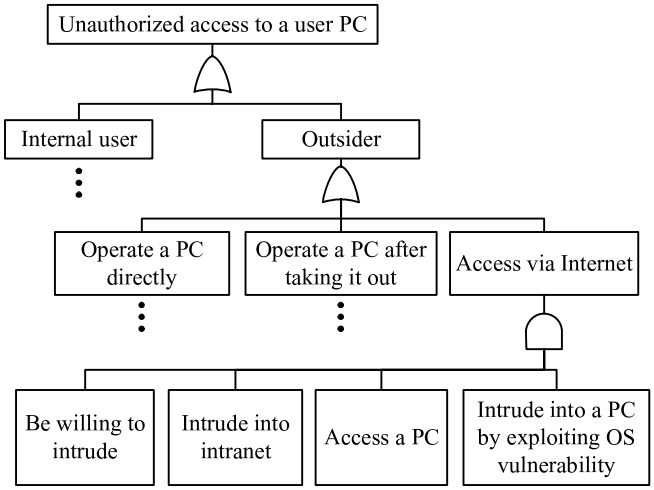

Figure 2: Fault tree for unauthorized access to a user PC.

Table 1: Analysis of risks and measures.

basic event	probability	measure	risk decrease	state
Be willing to intrude	0.7	-	-	-
Intrude into intranet	0.7	Authentication for network access	0.9	0
		FW access control	0.7	1
Access a PC	0.7	At a PC: PFW access control	0.5	1
Intrude into a PC by exploiting OS vulnerability	0.4	At a PC: OS update	0.7	1

3.1 Network Example

To describe our method with some tangible examples, we assume a simple network example as shown in Figure 1. The network is separated into DMZ and intranet. A web server and a mail server are located on the DMZ. General users work using each user PC. The users can use files on a file server, browse web sites and send and receive e-mails.

3.2 Risk Analysis

Generally, some phases exist in the process of an occurrence of a risk event. A risk can be inhibited by measures preventing from occurring each phase based on the concept of defense in depth [10].

In order to quantify risk probabilities, our method makes FTs of risks. First, an unexpected risk event is placed at the top of the FT. Second, attack phases are developed at the bottom as shown in Figure 2. Third, measures related to each basic event, which is a leaf of the tree, are clarified. Finally, the probability of a basic event, the rate of risk decrease in an object basic event by a measure and the implementation state of a measure, which has yes or no selectively, are assigned as shown in Table 1. Note that the acronyms means firewall (FW) and personal firewall (PFW)

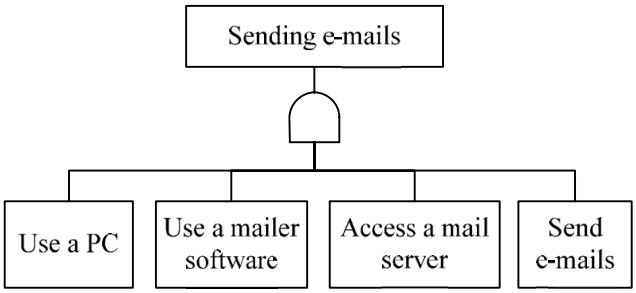

Figure 3: Fault tree for the usability of rending e-mails.

Table 2: Analysis of a service usage and measures.

basic event	usability	measure	usability decrease	state
Use a PC	1	-	-	-
Use a mailer software	1	At a PC: password for a mailer software	0.3	1
Access a mail server	1	At a PC: PFW access control	0.1	1
Send e-mails	1	At a mail server: Authentication for sending e-mails	0.1	1

and the value of the implement state (described as *state* in Table 1) has 0 as "not implement" or 1 as "implement".

Risk probability is formulated as follows. The probability of the top event is calculated based on minimal cut sets, which are minimum collections of basic events such that if they all occur the top event also occur.

The P_{top} , which is the probability of the top event, gives

$$P_{top} = 1 - \prod_{c \in C} \left\{ 1 - \prod_{e \in Ec} P_e \prod_i \left(1 - X_i \Delta P_{e,i} \right) \right\} \quad (1)$$

where c is a minimal cut set, C is a set of c, e is a basic event in a cut set, E_c is a set of e in c, P_e is the probability of e, $X_i \in \{0, 1\}$ is the implementation state of measure i and $\Delta P_{e,i}$ is the rate of risk decrease in e by i.

3.3 Usability Analysis

Some phases exist in the process of using a service as risks. However, service use may become insufficient because security measures may prevent from realizing some phases.

In order to quantify usability of services, our method makes FTs of services use. First, an object service is placed at the top of the FT. Second, using phases are developed at the bottom as Figure 3. Third, measures related to each basic event are clarified. Finally, usability of a basic event, the rate of usability decrease in an object basic event by a measure and the implementation state of a measure are assigned as Table 2. Note that the value of usability of each basic event is 1 as a standard according to the definition in section 2.3.

The analysis based on the concept of phases in our method can calculate effective measures preferentially because a measure to recover usability of the violated phase

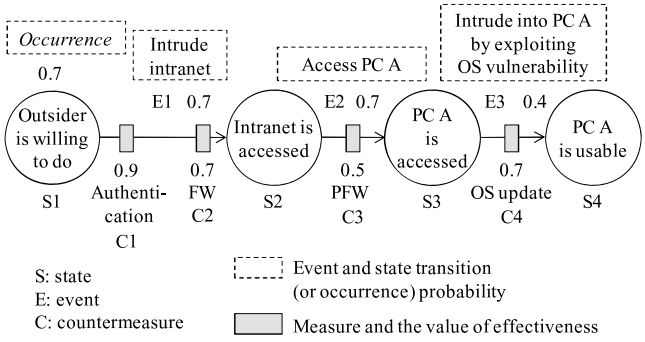

Figure 4: STD of unauthorized access to a user PC.

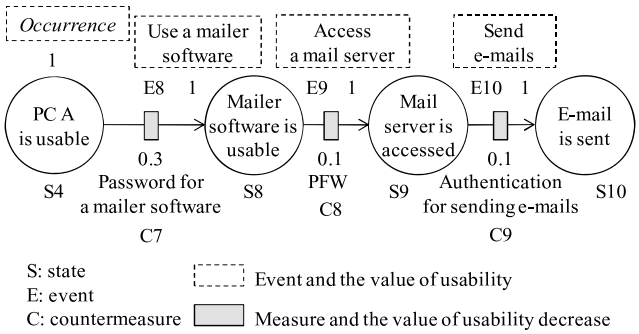

Figure 5: STD of sending e-mails.

increases usability largely as compared with another one related to other phases. Therefore, our method can select appropriate measures consisting with actual service use.

The U_{top} , which is usability of the top event, gives

$$U_{top} = 1 - \prod_{c \in C} \left\{ 1 - \prod_{e \in Ec} U_e \prod_i \left(1 - X_i \Delta U_{e,i} \right) \right\} \quad (2)$$

where U_e is the usability of a basic event e and $\Delta U_{e,i}$ is the rate of usability decrease in e by measure i.

4 RELATIONAL ANALYSIS WITH STATE TRANSITION DIAGRAM

We analyze relations among risks, usability and their chain relations with STD. FTA can also analyze these relations by combining FTs. However, the combining may make analysis complex and proper recognition of the relations difficult because FTs may become enormous and we may not identify where each event in FTs happens in an object network. In contrast, the method to make STD and incorporate with a network model can analyze risk, usability and these relations visually and intuitively.

4.1 Creating and Combining the STD of Risk and Usability

The STD of a risk as shown in Figure 4 is created by assuming a basic event in the FT at Figure 2 as an event in the STD and a result of the event of the FT as a state in the STD. Similarly, the STD of usability as Figure 5 is created from Figure 3.

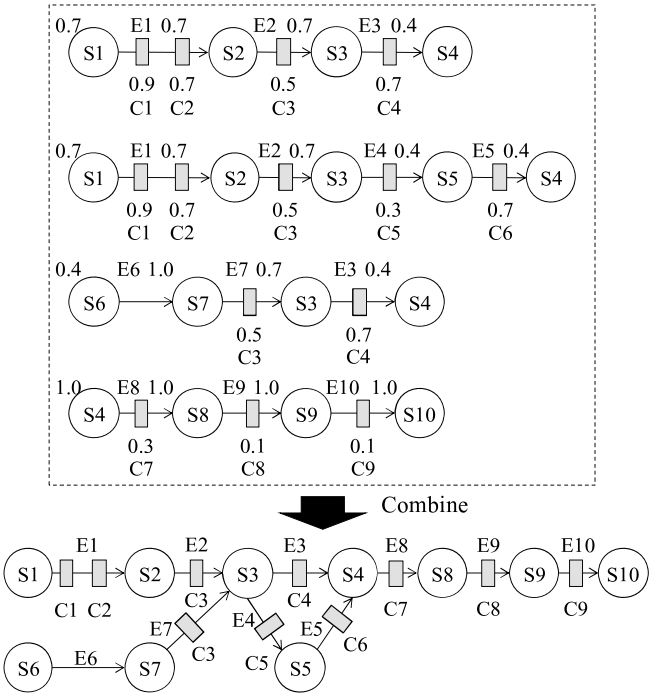

Figure 6: Combining of STDs.

Each arrow from one state to another has state transition probability, which is equal to probability/usability of a basic event as shown in Table 1 and Table 2, owing to the correspondence relation between FT and STD. In addition, measures to prevent from realizing a phase are placed on the arrow. Some measures can be placed on a single arrow.

The risk/usability decrease by a measure in Figure 4 and Figure 5 are also equal to the one in Table 1 and Table 2. The value is treated as the rate of blocking the state transition. Additionally, a state occurring independently such as motivation, "be willing to *do something*", has the occurrence probability.

The STDs can be combined by merger of the same state as shown in Figure 6. In order to combine the STDs, idempotent and distributive laws are applied because the STDs correlates with the FTs and states and events in the STD can be treated as constituent factors of risks and usability [9]. Note that commutative law cannot be applied because state transition has direction.

The STDs of both risks and usability are also combined by merger of the same states such as "PC A is usable" in both Figure 4 and Figure 5. In the case of, for example, leaking data from PC A by an e-mail, the value of 1 which is the standard of usability changes directly into success probability of the attack. Therefore, the STD of usability changes to that of risk.

The STDs are deployed on a network model. An organization has some network segments such as DMZ and intranet which may be divided into proper areas based on business departments. Based on the existing defense in depth model [11], our method creates a network model that has network segments and machines in each segment. The machines are also developed into some layers.

For example, a simple network configuration in Figure 1 changes into the model as shown in Figure 7 by separating

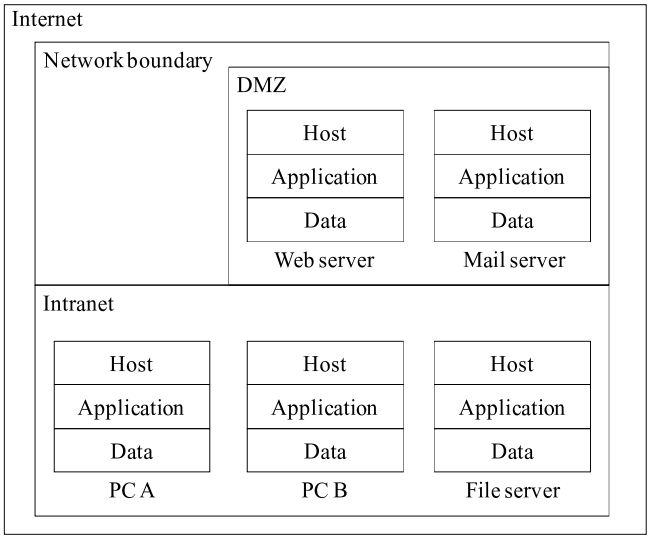

Figure 7: Model of the network as shown in Figure 1.

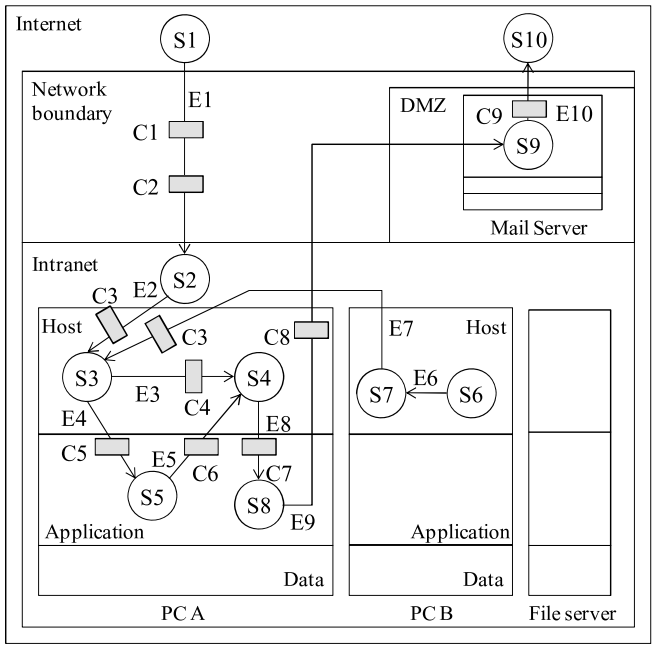

Figure 8: Deployment of risks, usability and measures on the network model.

the network into DMZ and intranet and developing each machine into the layers of host, application and data. The STDs are deployed on this network model as shown in Figure 8. Each state is on a layer to occur. Each arrow passes through some related layers. Each measure is set on a layer to implement.

In addition, STDs can be copied from one machine to others where machines in a common segment have same risks. Differences such as implementation states of measures among machines can also be customized as needed.

Details of the model should be decided depending on objects and accuracy of risk analysis that the organization requires. In the case of Figure 7, the firewall is excepted because we regard it as one of measures. The router is also omitted because we think it does not face threats. The

network model, for example, may treat several segments as a single area and add layers related to hardware such as memory devices like hard disks and I/O devices like LAN cards.

4.2 Risks and Usability Quantification

With Formula (1) and (2) by FTA, we quantify each risk and usability. On the other hand, STD expressing chain relations can also quantify them.

A risk probability, the value of a risk and usability can be quantified using a created model such as Figure 8. First, we decide an object risk and select states as starting points and ending point in order to quantify risk probability. At this time, several starting points can be selected. Next, we extract paths going from each starting point to the ending point. Then, the risk probability P_n in path n gives

$$P_n = \prod_{e \in E_n} P_e \prod_i \left(1 - \Delta P_{e,i} X_i\right) \quad (3)$$

where e is an event included in n (e include the occurrence of a starting point), E_n is a set of e, P_e is a state transition probability or the occurrence probability of e, $X_i \in \{0, 1\}$ is the implementation state of measure i and $\Delta P_{e,i}$ is the rate of probability decrease in e by i.

Finally, a total probability P_{total}, which means that at least one of the selected starting points arrive to the ending point, gives

$$P_{total} = 1 - \prod_{n \in N} \left(1 - P_n\right) \quad (4)$$

where N is a set of all paths.

In addition, Formula (3) and (4) equate to Formula (1) because STD has a correspondence relation to FT. Therefore, we must not exponentiate same state transition probability and the rate of risk/usability decrease by same measure in a case that several paths include a common event. We must replace exponent as follow [9]:

$$\left\{P_e \prod_i \left(1 - \Delta P_{e,i} X_i\right)\right\}^2 \rightarrow \left\{P_e \prod_i \left(1 - \Delta P_{e,i} X_i\right)\right\}$$

Furthermore, we can calculate the value of a risk in consideration of the value of assets. This paper define the value of risk as

Value of a risk = Value of assets × Risk probability.

For example, when a state on the data layer is selected as an ending point, state transitions arriving to the state are the risks about data. The value of risk is calculated using the value of data and risk probability calculated by Formula (3) and (4). When object assets are several data, we must calculate the value of the risk on a data-by-data basis because of differences of the value of data. In addition, when the implementation state and/or the rate of probability decrease by a measure are (or should be) different from each data, we copy and customize STDs and calculate the risk probability and the value of the risk on an asset-by-asset.

Table 3: Transforming state transition probability to conditional probability.

P(S1)
P_{S1}

P(S6)
P_{S6}

S1	P(S2)
T	P_{E1}
F	0

S6	P(S7)
T	P_{E6}
F	0

S2	S7	P(S3)
T	T	1-(1-P_{E2}) (1-P_{E7})
T	F	P_{E2}
F	T	P_{E7}
F	F	0

S3	P(S5)
T	P_{E4}
F	0

S3	S5	P(S4)
T	T	1-(1-P_{E3}) (1-P_{E5})
T	F	P_{E3}
F	T	P_{E5}
F	F	0

* P(S2), P(S3), P(S4), P(S5) and P(S7) are the conditional probability.
T means that the transition to the state is done.
F means that the one is not done.

Similarly, usability can be calculated by Formula (3) and (4) based on paths from starting points and an ending point. Note that $\Delta P_{e,i}$ is the rate of usability decrease in e by measure i.

4.3 Causal Inference of Incidents

We can regard STDs such as Figure 8 as a model expressing cause-and-effect relations in a probabilistic viewpoint. Therefore, we can treat STDs as a Bayesian network with changing the state transition probability into the conditional probability when each state transition probability is independent of previous and following phases. As a result, we can infer the probability of causes of the occurrence of a risk event.

For example, in Figure 8, we suppose that the state S4 occurred and all measures had not been implemented. Table 3 shows the conditional probability of sates existing in the path to S4. The probability that S1 had occurred gives as follow:

$$P(\mathrm{S1}|\mathrm{S4}) = P(\mathrm{S1} \cap \mathrm{S4}) / P(\mathrm{S4})$$

For another example, when we analyze closed object states such as {S2, S3, S4, S5}, there is no occurrence probability. In this case, we calculate the arrival probability of S2 as the occurrence probability with Formula (3) and (4).

In this way, our method can infer the probability of causes which are states existing on the turned paths from the target state.

5 EXPERIMENT

We experiment to apply our method at the stages of implementing and changing measures in a simple network example. We then confirm that our method can analyze phases of risks and usability and select optimal measures in consideration of their implementation place.

5.1 Assumption

In order to avoid complex analysis, we assume a simple network as shown in Figure 1. As mentioned at section 3.1, general network users browse web sites, send and receive e-mails and use files on a file server.

We analyze risks selectively because real results of risk analysis in actual organization networks are unavailable due to their confidentiality about security. Target risks are following: (i) unauthorized access to a PC via networks, (ii) data leakage of a confidential file via networks and (iii) virus infection on a PC. Target services relating to usability are following: (i) browsing web sites, (ii) sending e-mails, (iii) reading e-mails and (iv) using files in the file server.

In this experiment, each value is quantified in some levels. Regarding risks, the state transition probability of a phase has four levels (0.1, 0.4, 0.7, 1.0). The rate of risk decrease by a measure has five levels (0.1, 0.3, 0.5, 0.7, 0.9). Regarding usability, the state transition probability of a phase has the value of 1 as a standard. The rate of usability decrease by a measure has five levels (0.1, 0.3, 0.5, 0.7, 0.9). In addition, the implementation state of a measure has two levels (0, 1).

5.2 Risk Analysis and Measures Selection

(1) The Model Creation

First, we model the network. In this experiment, the network was modeled as shown in Figure 7.

Second, we analyze assets, threats, vulnerabilities and phases about target risks and usability like Figure 2 and Figure 3. Then, we clarify measures to basic evens based on [12] and assign the probability of a basic event, the rate of risk/usability decrease by a measure and the implementation state of a measure like Table 1 and Table 2. Finally, we express risks and usability as STDs and deploy them on the network model with measures. As a result, the model was created as shown in Figure 9.

In this case, all of the event name, the state transition probability and the risk/usability decrease by measures are eliminated from Figure 9 in order to avoid the complication of the model. Most parts of the STDs about the PC B are also eliminated because they were copied from the PC A.

(2) Utilization of the Model for Risk Analysis and Measures Selection

Some results of risk analysis and implement states of measures with FTA were reconsidered at the STD model creation.

First, several phases were modified to expand them in more detail because the model could not express several measures on an appropriate layer. The reason is that the phases of risks and the place to implement measures become clear. Specifically, we added the state named “inappropriate application use” and redeployed the measure named “application update” from the host layer to the application layer. In addition, we added the candidate of a measure named “limitation of usable applications” on the transition from “PC access” (on PC A) to “inappropriate application use”. This measure, however, is not drawn in Figure 9 because we decided not to implement it.

Next, some of state transition probabilities were modified. Common phases in some risks had different probabilities each other even though the probability should be equal regardless of previous or following phases. The reason of these modifications is, similarly as above mentioned, that we can discover inconsistency of results of risk analysis by combining STDs.

Similarly, some of the rates of risk decrease by measures were modified. These values had been different from each measure even though the measures were clarified in common at analyzing risks. The reason of these modifications is that we can discover inconsistency of the rate of risk decrease by combining STDs.

Furthermore, some of the rates of risk decrease and implementation states of measures were added to insufficiently analyzed phases. We found that a measure effects to a specific target phase as well as to other phases. The reason of this work is that we can recognize whether a measure effects to other events passing through the same layer because the model can clarify phases of risks and the layer of a measure implementation. For example, we found that the measure named “access rights” for the risk of data leakage relates to control of a virus infection and sending/receiving attached files in an e-mail, and then added the measure on appropriate places of the data layer.

Finally, measures to effect some phases of risks in common are added as follows: “web filtering”, “PFW preventing inbound access”, “PFW preventing outbound access” and “limitation of attached files in e-mails”. The reason of these additions is that we can consider whether there are measures effecting on some events. For example, the above “web filtering” effects on three phases efficiently.

(3) Quantitative Assessment of Risks and Usability

Table 4 shows the probability of risks and the value of usability at the initial analysis with only FTA and at the second analysis with both FTA and STD. We assessed the value of assets simply as shown in Table 5 and calculated the value of risks as shown in Table 6 from the probabilities and the values of the assets, which are amount of damage at the occurrence of risk events. Note that though these results include some probabilities/values of risks increase and usability decrease, they do not mean selected measures were inappropriate but our method could analyze risks and usability more accurately.

As a result, our method can assess risks and usability quantitatively and select measures to reduce risks and improve usability.

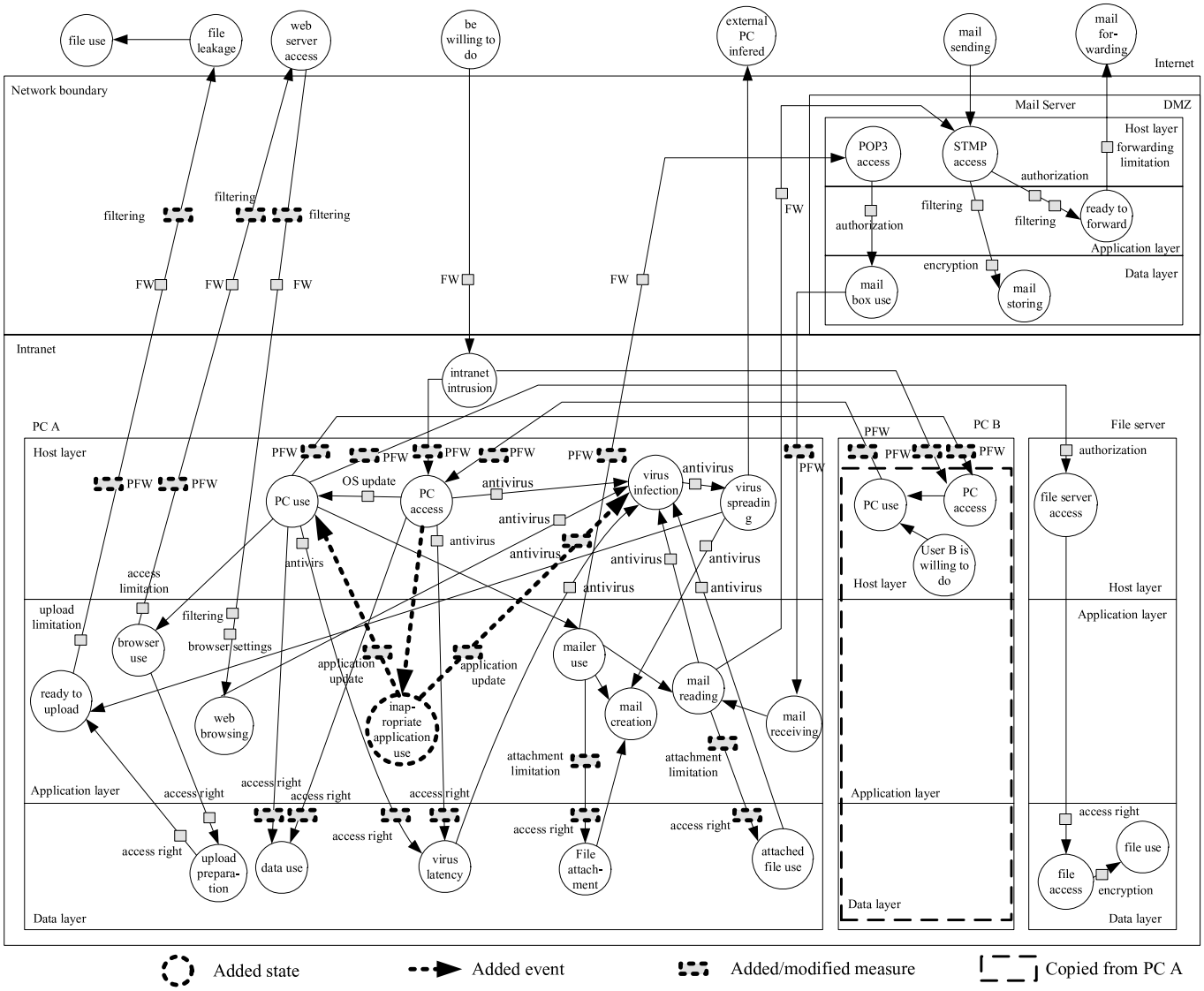

Figure 9: Modeling of risks, usability, and measures in the assumed network.

5.3 Analysis to Change Measures

For reviewing or changing measures, to identify shift of security and usability levels is important. In this situation, alternative measures may be needed.

Our method with FTA can calculate optimal measures to change measures by solving a discrete optimization problem with an objective functions to minimize risk increase or usability decrease and constraint functions to maintain levels of risks and usability. We can recognize the impact of changing measures visually by combining the above method with STD.

We suppose that, for example, a user of PC A requires opening a certain port of the firewall temporarily. The network becomes being intruded more easily by attackers via Internet if the firewall port is opened. At the same time, this change causes increasing probabilities to arrive all of the states continuing from the state named "intranet intrusion".

The additional measures selected with FTA in [7], although the results are not exact because of the difference of an environment assumption, were as follows: (a) account lockout after login failure, (b) logging of PC access, (c) password protection on a screen saver and (d) prohibition of using HTML e-mail. Table 7 shows the risk probability, the value of risks and the usability at usual network operation, at firewall port opened and at above four measures added.

We can clarify that all of the selected additional measures are implemented on PC A using Figure 9. The port opening of firewall can be configured to effect only to PC A. Contrarily, a measure to the transition before or immediately following "intranet intrusion" should affect other users. On the other hand, the selected measures do not affect other users. Therefore, our method can select measures in consideration of their effects and the implementation layer.

In addition, another effective measure is "authentication for network access" (which is not drawn in Figure 9 because we decided not to implement it) deployed on the same transition as the firewall. The measure prevents intranet from being intruded. The other measure is "PFW" on the transition continuing directly from "intranet intrusion". The measure prevents the state from transiting to other states.

Table 4: Probability and usability at the first analysis with only FTA and reanalysis with both FTA and STD.

Target of analysis		FTA	FTA and STD
(R1)	Unauthorized access	0.0285	0.0494
(R2)	Information leakage	0.0430	0.0198
(R3)	Virus infection	0.0181	0.0158
(U1)	Browsing web sites	0.810	0.590
(U2)	Sending e-mails	0.590	0.372
(U3)	Reading e-mails	0.590	0.413
(U4)	Using files in the file server	0.729	0.510

Table 5: Assumption of the value of assets.

(unit: yen)

Use PC	1,000,000
Confidential files	
about product development	50,000,000
about customers	10,000,000
Not confidential files	100,000

Table 6: The value of risks calculated from the value of assets and the probability.

(unit: yen)

	Object	FTA	FTA and STD
(V1)	About user PC	46,551	65,245
(V2)	About all files	2,581,968	1,188,176
	total	2,628,519	1,253,421

From a viewpoint of analysis, our method can identify potential states, which may occur by chain relations, by following STDs from a base state, which is directly caused by the transition that the changed measure had inhibited. Similarly, the method can also identify causes to raise the base state by tracing STDs back. At the same time, we can identify influences on usability.

From a viewpoint of selecting measures, in order to maintain (or reduce) risks, the method can narrow down the candidates of measures, depending on the concept of preventing chains or resolving causes of the risks. On the other hand, in order to maintain (or increase) usability, the method can also narrow them down, depending on the concept to improve usability of chain phases or resolve causes of usability decrease.

5.4 Probabilistic Causal Inference

We focus on the state named "PC A is usable", which means unauthorized use of PC A, as an example. First, paths reversed from the state are extracted from the STDs in Figure 9. The result is shown in Figure 10. Note that Figure 10 includes measures which are not implemented and limits the states on the PC B to S6, S7 and related events. In addition, we connect an event directly from S2 to S7 in order to make the STD simpler though we should analyze

Table 7: Shift of risks and usability caused by changing measures.

probability and usability

	At usual operation	At the FW port opened	At other measures added
(R1)	0.0494	0.0796	0.0518
(R2)	0.0198	0.0375	0.0269
(R3)	0.0158	0.0215	0.0195
(U1)	0.590	0.590	0.590
(U2)	0.372	0.372	0.335
(U3)	0.413	0.413	0.372
(U4)	0.510	0.510	0.510

value of risk

(V1)	65,245	101,094	71,298
(V2)	1,188,176	2,251,166	1,619,260
total	1,253,421	2,352,261	1,690,558

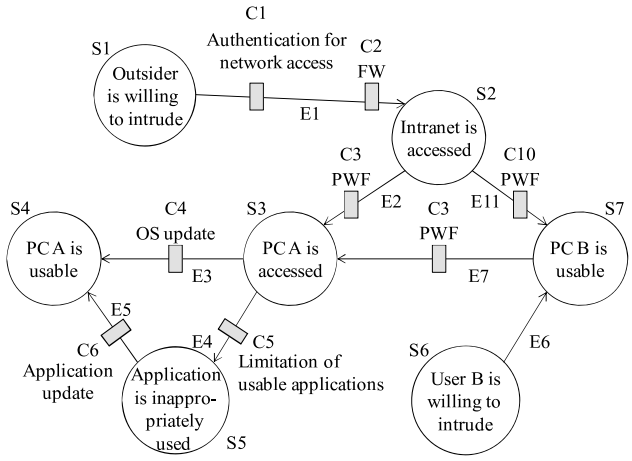

Figure 10: Candidates of the causes in unauthorized use of PC A.

events of accessing to and intruding into the PC B via Internet.

Next, we change state transition probability to conditional probability and infer causes of the incident. The state transition/occurrence probabilities, the rate of risk decrease and the implementation states of measures were analyzed at section 5.2 as shown in Table 8.

Then, we infer causes of S4. Table 9 shows the probability of each state which had occurred before S4 occurred at usual network operation, at a certain port of firewall (C2) opened and at "authentication for network access" (C1) added respectively.

At usual network operation, because the firewall protects from inappropriate access via Internet, outsiders might be willing to intrude into intranet (S1) but the probability of successful intrusion was inhibited (S2). On the other hand, the probability that the PC B was used (S7) and the user B was willing to intrude (S6) were high. These probabilities mean that an internal user is more suspicious.

Table 8: Assigned values of states, events and measures at the analysis.

state or event	state transition /occurrence probability	measure	risk decrease	state
S1	0.7	-	-	-
S6	0.4	-	-	-
E1	0.7	C1	0.9	0
		C2	0.7	1
E2	0.7	C3	0.5	1
E3	0.4	C4	0.7	1
E4	0.4	C5	0.3	0
E5	0.4	C6	0.7	0
E6	1.0	nothing	-	-
E7	0.7	C3	0.5	1
E11	0.7	C10	0.5	1

At a certain port of the firewall opened, outsiders can access intranet more easily via Internet. The probability of intrusion by outsiders (S2) became higher drastically. This result means that an outsider is more suspicious.

At "authentication for network access" added, the probability of intrusion by outsiders (S2) decreased significantly. The probability that the PC B was used (S7) and the user B was willing to intrude (S6) became extremely higher. These probabilities mean that an internal user is highly suspicious.

Note that the attacker had surely accessed to the PC A (S3) before he/she operated it without authorization (S4). On the other hand, intruding into the PC A (S5) is absolutely not related to whether vulnerabilities of the operating system or of an application is exploited, which means whether the transition from S3 to S4 goes through S5 or not. Therefore, the following conditional probabilities are constant.

$$P(\mathrm{S3}|\mathrm{S4}) = 1, \quad P(\mathrm{S5}|\mathrm{S4}) = 0.72$$

As a result, our method can infer probabilistic causes of risks. Therefore, we can use the probabilities as one of information to select network monitoring points for proactive measures and to analyze causes of incidents for reactive ones.

6 EVALUATIONS

We evaluate our method for resolution of research issue described in chapter 2.

6.1 Analysis of Risk and Usability with Chain Relations

In the experiment, we analyzed phases of risks and services use with FTA and converted to STD. we clarified the chain relations among risks by combining the STDs. We also analyzed the phases of services use and clarified relations among usability.

Table 9: Probability of causation of unauthorized use of PC A.

	At usual operation	At the FW port opened	At authentication added
$P(\mathrm{S1}\|\mathrm{S4})$	0.78	0.86	0.73
$P(\mathrm{S2}\|\mathrm{S4})$	0.38	0.77	0.15
$P(\mathrm{S3}\|\mathrm{S4})$	1.00	1.00	1.00
$P(\mathrm{S5}\|\mathrm{S4})$	0.72	0.72	0.72
$P(\mathrm{S6}\|\mathrm{S4})$	0.8	0.59	0.92
$P(\mathrm{S7}\|\mathrm{S4})$	0.9	0.78	0.96

In addition, the STDs of risks and usability were combined. The combined STDs clarify the relation among risks and usability. Moreover, the inconsistencies among risk analysis results are discovered and modified with combined STDs.

As a result, we confirm that our method can analyze risks and usability with their phases in consideration of chain relations. Furthermore, our method can assess risks and usability by calculating the risk probability, the value of risks and the usability as the result of section 5.2.

6.2 Analysis of Relations among Risks, Usability and Measures

In the experiment, the combined STDs were deployed on the network configuration model based on defense in depth. The incorporated model could express correspondence relations among phases of risks and usability.

In addition, measures clarified with FTA are developed on the appropriate layer in the incorporated model. We can recognize clearly the implementation place of measures.

On the other hand, our method can analyze relations among risks, usability and measures because influence on risks and usability at changing measures became clear in section 5.3.

6.3 Selecting Optimal Measures and Causal Inference

At first measures selection in the experiment, we could seek efficient measures preventing some of objective risks by analyzing the risks based on phases. We also visually found inconsistencies among the results of analysis and lack of requisite measures. As a result, the method can analyze effectiveness and the implementation place of measures exactly and select optimal measures.

At changing measures, we recognized the influence on risks and usability visually and quantitatively. We can select measures based on the concept of preventing causes or chains, which mean prior or latter phases. Consequently, our model can select optimal measures to inhibit risks increase and/or usability decrease.

On the other hand, we inferred probabilistic causes of a risk. We can detect incidents by monitoring events with high probability of causes and/or machines including some of the

events. In addition, we can identify causes of incidents efficiently by investigating such events mainly.

7 CONCLUSION AND FUTURE WORKS

We have proposed the method to analyze risks and usability in consideration of chain relations and select optimal measures. The method analyzes each risk and usability with FTA, converts the results to STDs and deploys the STDs on the network model based on defense in depth. The method can be converted to a Bayesian network and thereby it can infer causes of incidents.

Through the experiment, we confirm that our method can quantitatively and intuitively (i) analyze risks and usability, (ii) select optimal measures and monitoring points and (iii) be available to trace causes of incidents.

The occurrence probability of a state, the state transition probability and the rate of risk/usability decrease by measures must be exact to assess risks and usability correctly. However, to assign proper value is difficult because these values may be different from each environment or each user. One of the solutions to solve this problem is to cycle risk analysis, assessment and review through network operation. The other solution is that stakeholders decide the values through negotiations, generally called risk communication such as [4].

Moreover, Figure 9 is too complicated even though we treat only three risks and four services. In the case of analyzing more risk and usability, the number of states and transitions may become huge. In contrast, the increase of the number of states may converge at certain number because risks/usability related to the same layer often have a common transition. Additionally, each state transition must be independent of the previous and next transitions in order to infer probabilistic causes. One way to achieve this state independency is to involve some parameters in each state and each event, such as time of transition and a person who transits the states. However, excessive number of parameters may increase the number of states and transitions. We will study more about this problem.

REFERENCES

[1] ISO/IEC 27002. http://www.iso.org/iso/home.htm

[2] A. Zuccato, A Decision Matrix Approach –to Prioritize Holistic Security Requirements in E-commerce, Security and Privacy in the Age of Ubiquitous Computing: IFIP TC11 20th International Information Security Conference, pp.35-49, Springer (2005).

[3] B.-C. Guan et al., Evaluation of Information Security Related Risks of an Organization –the Application of the Multi-criteria Decision-making Method, Proceedings of IEEE 37th Annual International Carnahan Conference on Security Technology, pp.168-175 (2003).

[4] H. Yajima et al., Evaluation of the Participant-Support Method for Information Acquisition in the "Multiplex Risk Communicator", LNCS, Vol.4558, pp.195-203 (2007).

[5] I. Kotenko and M. Stepashkin, Attack Graph Based Evaluation of Network Security, LNCS, Vol.4332, pp.216-227 (2006).

[6] L. Wang et al., Measuring the Overall Security of Network Configurations Using Attack Graphs, LNCS, Vol.4602, pp.98-112 (2007).

[7] K. Kato and Y. Teshigawara, A Proposal of Selecting Optimal Countermeasures with Security and Usability in a Special Network Use, IPSJ Journal, Vol.49, No.9, pp.3209-3222 (2008) (in Japanese).

[8] K. Kato and Y. Teshigawara, A Study on a Model of Risks and Countermeasures Based on the Concept of Defense in Depth, Multimedia, Distributed, Cooperative, and Mobile (DICOMO) Symposium 2008, pp.1531-1540 (2008) (in Japanese).

[9] J. D. Andrews and T. R. Moss, Reliability and Risk Assessment -Second Edition, Professional Engineering Publishing (2002).

[10] Microsoft TechNet, Security Content Overview. http://technet.microsoft.com/en-us/library/cc767969.aspx

[11] Microsoft TechNet, Chapter 3: Antivirus Defense-in-Depth. http://technet.microsoft.com/en-us/library/cc162798.aspx

[12] ISO/IEC 13335. http://www.iso.org/iso/home.htm