Proposal of an Improved Event Tree and Defense Tree Combined Method for Risk Evaluation with Common Events

Ryo Aihara, Ryohei Ishii and Ryoichi Sasaki
Tokyo Denki University
Senjuasahi-cho 5, Adachi-ku, Tokyo-to, 120-8551 JAPAN
aihara@isl.im.dendai.ac.jp, sasaki@isl.im.dendai.ac.jp

ABSTRACT

Damage caused by targeted attacks has increased in recent years. In order to cope with the issue, we previously developed the event tree and defense tree combined (EDC) method for obtaining the optimal combination of countermeasures against targeted attacks based on security analyses. However, the original EDC method cannot deal with common events, i.e., events that are the common cause of more than one type of problem", here and in the main text. In order to deal with common events, instead of minimal cut set (MCS) operation, we introduce the prime implicant set (PIS) operation, which can obtain cut sets, including negative events, for the sequence of the event tree. The results of a numerical experiment confirm that the occurrence probability can be calculated correctly by introducing the PIS. Moreover, if PIS operation is not implemented, the overall risk may be underestimated by a factor of three.

KEYWORDS

APT, Targeted attack, Risk assessment, Defense tree, Attack tree.

1 Introduction

Proper quantitative risk analysis is essential in order to employ proper countermeasures against ever-increasing cyber-attacks. A number of revised methods based on attack tree analysis [1], developed by Bruce Schneier, have been proposed. Bistarelli et al. [2] proposed a defense tree in order to determine possible countermeasures.

However, it is difficult to apply these methods to attacks, such as targeted attacks, that are composed of a variety of attack events that occur over time.

In recent years, the damage caused by targeted attacks has been on the rise [3]. Therefore, we developed the event tree and defense tree combined (EDC) method [4]. The EDC method, which consists of an event tree analysis method and the defense tree analysis method, can also obtain the optimal combination of countermeasures against targeted attacks based on a security analysis.

Although there already exists a similar risk analysis method which incorporates event tree analysis and fault tree analysis and is used for the safety assessment of nuclear power plants,[5] this method cannot determine appropriate countermeasures.

By applying the EDC method to a targeted attack on a small company, we confirm that the EDC method is useful for obtaining the optimal combination of countermeasures against targeted attacks. However, the original EDC method did not consider common events, which are events that cause more than one problem at the same time. In general, if a common event is not taken into consideration, the risk will be underestimated or overestimated.

In the original EDC method, the following two common events can be considered:

(1) The impact of a countermeasure on multiple attacks.

(2) Events that are the common cause of more than one type of problem.

For common event (1), if the correct countermeasure is applied to the attacks, it is possible to correctly estimate the risk reduction effect by the conventional method of calculation. For common event (2), improved calculation methods are expected to be required.

In the present paper, we investigate a method of addressing the problems related to common event (2). In the field of reliability engineering, this type of common event is referred to as a common mode failure. In this field, after expressing the relationship of vents by a fault tree, the common mode failure in the fault tree problem is usually solved using a minimal cut set (MCS) calculation [6].

However, for the case of using a combination of event tree analysis and defense tree analysis, because of the requirement to include a negative event, it is impossible to solve a common event problem using an MCS, as described in detail in Section 3.2. Therefore, we decided to use the method of deriving the prime implicant set (PIS) that can be applied to negative events [7].

Although the number of studies dealing with the security evaluation is increasing [8][9], there are no studies that take into account a common event in the security evaluation. There are also no studies that have used the PIS for assessment in conjunction with the proposed countermeasures, in the field of security evaluation or any other field.

In the present paper, we present a calculation method that takes into account a common event by deriving the PIS for the EDC method. After we propose this method, which enables common event operation using the EDC method, the effect of considering a common event used in the EDC method is demonstrated through a numerical experiment.

2 Original EDC method

2.1 Overview of the original EDC method

The original EDC method includes a function to obtain the optimal combination of countermeasures. The combination of event tree analysis and defense tree analysis is used in the original EDC method, which is suitable for analyzing targeted attacks consisting of a variety of attack events that occur over time.

The original EDC method is implemented as follows.

Step 1 Determine the target for evaluation

The target for evaluation is determined. As an example, a small WEB service company is considered as a target.

Step 2 Analyze the target

The target is analyzed for formulation. For example, the number of servers and PCs of the company are estimated for use in the evaluation. Moreover, a targeted attack similar to the attack on the Japan Pension Service was assumed in this case.

Step 3 Decide the objective function and the constraints function.

In the sample case, the total cost, which is the overall risk and the cost to implement the countermeasures, was selected as the objective function. The cost to implement the countermeasures was selected as the constraint.

Step 4 Propose alternative countermeasures

The countermeasures, for example, education on how to handle suspicious emails or the introduction of a sandbox, are proposed in order to determine the overall risk.

Step 5 Formulate a combinatorial optimization problem

The objective function and constraint function can be expressed by the following numerical formula, which includes zero-one variables:

$$Min\ f\ (x_1, x_2, x_3, \cdots, x_n) + \sum_{i=1}^{n} c_i \cdot x_i \qquad (1)$$

$$\text{subject to} \sum_{i=1}^{n} c_i \cdot x_i \leq c_t \qquad (2)$$

where x_i represents the zero-one variable. If the i-th countermeasure is adopted, $x_i = 1$, otherwise $x_i = 0$. Here, c_i represents the cost of the i-th countermeasure, c_t is the constraint on the total cost, and f is the function to calculate the overall risk using event tree analysis and defense tree analysis, as described in some detail in Sections 2.2 and 2.3.

Step 6 Obtain the optimal combination of the proposed countermeasures

By using a combinatorial optimization program, the optimal combination of the proposed countermeasures is obtained.

2.2 Event tree analysis

Event tree analysis is a probabilistic risk analysis technique. In event tree analysis, after an undesirable event, which is referred to as the initiating event, has occurred, the sequence of events that follows is expressed as a tree, as illustrated in Fig. 1.

In this case, Events 1 and 2 are the heading items. For each heading item, the tree is branched into success and failure branches from the viewpoint of the attackers. Here, sequence 1 indicates that, even though a targeted mail containing malware was sent to the institute, no PCs at the institute were infected. Sequence 2 indicates that, even though a PC was infected, the attacker failed to obtain information from the institute. In contrast, sequence 3 indicates that, after a PC was infected, the attacker obtained information from the institute.

Next, in the event tree analysis, the success probability P_j for heading item j is calculated using defense tree analysis. The failure probability for heading item i can then be obtained as $(1 - P_j)$.

The probability of the sequence can be obtained by multiplying the probability of the initiating event and the occurrence probability of the heading items. For example, in the case of Fig. 1, the probability of sequence 1, 2, and 3, which are represented as $P_1{}'$, $P_2{}'$, and $P_3{}'$ can be obtained as follows:

$$\begin{aligned} P_1{}' &= (P_0 \cdot (1 - P_1)) \\ P_2{}' &= (P_0 \cdot P_1 \cdot (1 - P_2)) \\ P_3{}' &= (P_0 \cdot P_1 \cdot P_2) \end{aligned} \tag{3}$$

The risk value of sequence k can be calculated by multiplying the probability of sequence k and the magnitude of the impact due to the occurrence the sequence k, as follows:

$$R_k = P{'}_{k} \cdot M_k \tag{4}$$

The overall risk is defined as the summation of the risks of all sequences, as below:

$$\mathrm{R}_t = \sum_{k=1}^{K} R_k \tag{5}$$

The overall risk R_t is used as an index to reduce the risk.

Here, the success probability P_j for heading item j is estimated using defense tree analysis of the present situation and the situation after countermeasure i was implemented.

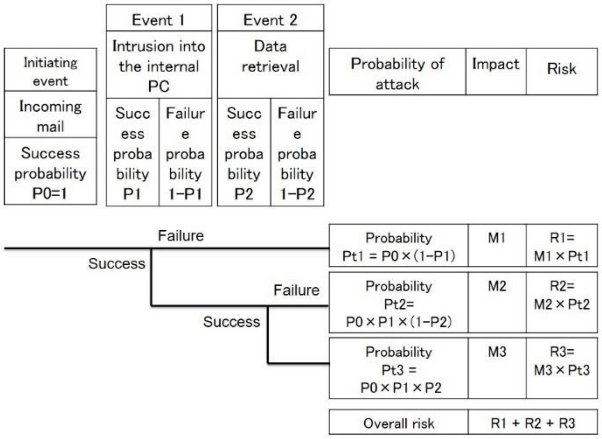

Figure 1. Example of an event tree

2.3 Defense tree analysis

In the present paper, the defense tree consists of an attack component and a defense component, as illustrated in Fig. 2. The attack component is expressed by the upper part of the defense tree. The top event of the defense tree represents the success of the attack related to each heading item of the event tree. Therefore, the probability of the top event of the defense tree is equal to P_j, which represents the success probability of the j-th heading item. The causes of the success are represented using AND/OR gates as shown in Fig. 2. The expansion to the lower direction using AND/OR gates is continued until reaching the level at which the countermeasure is prepared.

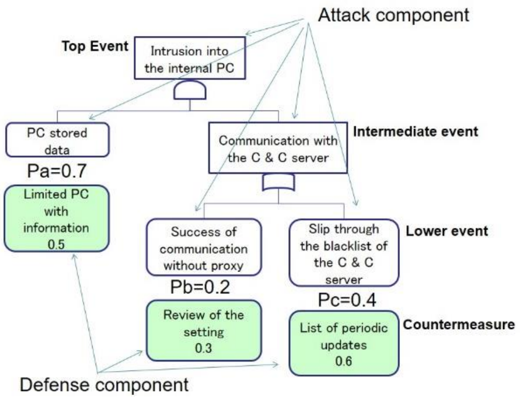
Attack component
Top Event
Intrusion into the internal PC
PC stored data
Communication with the C & C server
Intermediate event
Pa=0.7
Limited PC with information 0.5
Success of communication without proxy
Slip through the blacklist of the C & C server
Lower event
Pb=0.2
Pc=0.4
Review of the setting 0.3
List of periodic updates 0.6
Countermeasure
Defense component

Figure 2. Example of a defense tree

The defense component of the defense tree is represented by box indicating a considerable countermeasure under the lowest event of the attack component, as shown in Fig. 2. Multiple countermeasures can be prepared for one of the lowest events on the attack tree.

The probability of the top event of the defense tree before carrying out countermeasures is calculated as follows.

Here, we define a as the event "Data retrieval", as shown in Fig. 2.

We also define b as the event "Success of communication that does not pass through a proxy", and c as the event "Slip the C & C server's blacklist".

In the present paper, "xORy" is represented as the "x, y", and "xANDy" is represented as "xy". Then, the top event can be represented as "ab, ac" from the structure of the defense tree. If P_a, which indicates that the probability of a, is 0.7, $P_b = 0.2$, and $P_c = 0.4$, then the probability of the top event can be calculated as follows:

$$\begin{aligned} P_i &= P(ab, ac)\\ &= 1-(1-P_a \cdot P_b) * (1-P_a \cdot P_c)\\ &= 1-(1-0.7\times 0.2)\times(1-0.7\times 0.4)\\ &= 0.38 \end{aligned} \tag{6}$$

Next, we explain the method used to calculate the top event probability after carrying out measure i to the lowest event for example a. First, the probability of event a when the i-th countermeasure was carried out can be calculated as follows:

$$Pa' = Pa \times \prod_{i=1}^{n} \{(1-x_{ai}) + P_{ai} \times x_{ai}\} \tag{7}$$

where x_{ai} are zero-one variables. If the i-th countermeasure for event a is adopted, x_{ai} = 1, else $x_{ai} = 0$. Moreover, n is the number of countermeasures, and P_{ai} represents the decrease effect when the i-th countermeasure for event a was adopted.

In the case of Fig. 2, $n = 1$ and $P_{a1} = 0.5$. Then, if the countermeasure is adopted, the value of Pa' is equal to 0.35. Therefore, the probability of the top event is

$$\begin{aligned} P_j &= P(a'b, a'c)\\ &= 1-(1-{P_a}' \cdot P_b) * (1-{P_a}' \cdot P_c)\\ &= 1-(1-0.35\times 0.2)\times(1-0.35\times 0.4)\\ &= 0.20 \end{aligned} \tag{8}$$

As a result, Step 5 can be described as follow.

Step 5-1 Obtain the cut set of the attack component of each defense tree. In the case of Fig. 4, the cut set is a,b and ac.

Step 5-2 Obtain the formulation to obtain the success probability considering countermeasures for each sequence (See Equations (7) and (8)).

Step 5-3 Obtain a formulation to calculate the probability considering alternative countermeasures for each sequence (see Equation (3)).

Step 5-4 Obtain a formulation, such as Equation (4), to calculate the risk for each sequence.

Step 5-5 Obtain a formulation to calculate the overall risk (See Equation (5)).

2.4 Application of the original EDC

The original EDC was applied to a small WEB service company [4]. In this case, the number of heading items of the event tree was eight. The number of alternative countermeasures was 12. When the value of $c_t = 2M$yen or $3M$ yen, the optimal combination of countermeasures was obtained.

The application confirmed that the EDC method is useful for obtaining the optimal combination of countermeasures against targeted attacks.

3 Proposed method

3.1 Common events

When multiple events occur at the same time due to a single causal event, the causal event is referred to as the common event.

First, we explain the common event using a fault tree.

In Fig. 3, the common event is expressed as “Power outage”. If a power outage occurs, the event “Room darkens” immediately, although the event “Power outage” is described in two parts in Fig. 3.

If such common events are not considered, it will be impossible to obtain an accurate probability.

A common event is referred to as a common mode failure in the field of reliability engineering.

We can obtain the correct probability in deriving the MCS for this problem.

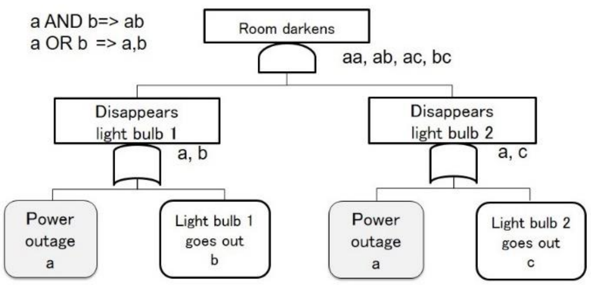

Figure 3. Examples of common mode failure in a fault tree

3.2 MCS operation

The MCS is a set of minimum combinations that guarantee the occurrence of the top event in the fault tree. The MCS can be derived using the absorption rule and the idempotent rule in Boolean operation [10].

In Fig 3, the cut set of the top event represented as aa, ab, ac, bc for the case in which no common events are considered. Using the absorption rule and the idempotent rule of Boolean operations, it is possible to derive the MCS for the top event of this fault tree as follows:

aa, ab, ac, b
$= a, ab, ac, bc$ (because aa is transformed into a according to the idempotent rule)
$= a, bc$ (because a, ab, and $ac$are transformed into a according to the absorption rule) (9)

The probability of the top event without considering the common event is calculated as follows:

$$\begin{aligned} &P(aa, ab, ac, bc) \\ &= 1 - (1 - Pa \cdot Pa) \times (1 - Pa \cdot Pb) \\ &\qquad \times (1 - Pa \cdot Pc) \times (1 - Pb \cdot Pc) \\ &= 1 - (1 - 0.04) \times (1 - 0.04) \times (1 - 0.04) \\ &\qquad \times (1 - 0.04) \\ &= 1 - 0.96 \times 0.96 \times 0.96 \times 0.96 \\ &= 0.38 \qquad (10) \end{aligned}$$

When we consider a common event and MCS operation is used, the probability of the top event is calculated as follows:

$$\begin{aligned} P(a, bc) &= 1 - (1 - Pa) \times (1 - Pa \cdot Pb) \\ &= 1 - (1 - 0.2) \times (1 - 0.04) \\ &= 1 - 0.8 \times 0.96 \\ &= 0.23 \end{aligned} \qquad (11)$$

From Equations (10) and (11), we can determine that the probability in the case of deriving the MCS becomes approximately 1.5 times larger than that without MCS operation.

As shown here, if we do not consider the common event, the risk can be easily underestimated. It is easy to also use MCS operation in the defense tree. However, in the EDC method, event tree analysis and the defense tree are used in combination.

The event tree illustrated in Fig. 1 has two heading items. Let defense trees related to heading items 1 and 2 be expressed as shown in Fig. 4. Here, the extended defense tree, which represents sequence 3, is shown in Fig. 5. This extended defense tree is similar to the original defense tree, and it is possible to use MCS operation.

On the other hand, the extended defense tree, which represents sequences 1 and 2, is shown in Fig. 5. This extended defense tree includes a negative event. It is impossible to apply MCS operation to this type of tree. Therefore, instead of MCS operation, we use PIS operation, which is an extension of MCS operation, and was studied in Boolean operations (See Table 1).

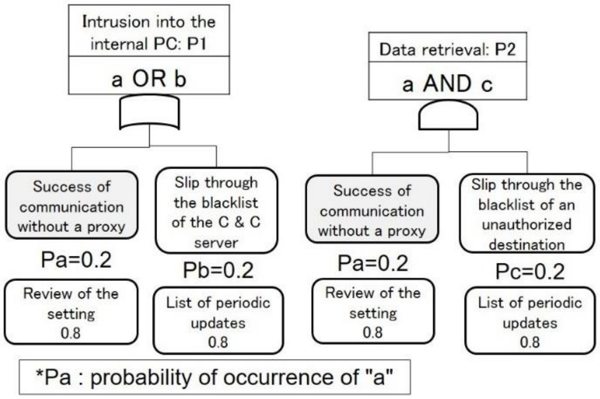
Intrusion into the internal PC: P1
a OR b
Success of communication without a proxy
Slip through the blacklist of the C & C server
Pa=0.2
Pb=0.2
Review of the setting 0.8
List of periodic updates 0.8
Data retrieval: P2
a AND c
Success of communication without a proxy
Slip through the blacklist of an unauthorized destination
Pa=0.2
Pc=0.2
Review of the setting 0.8
List of periodic updates 0.8
*Pa : probability of occurrence of "a"

Figure 4. Example of a defense tree

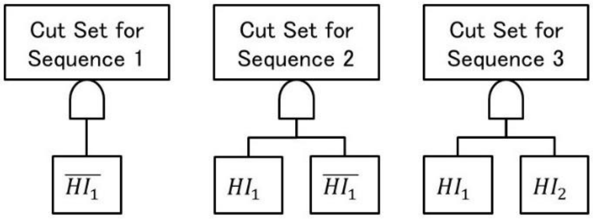

Figure 5. Sequences 1 through 3 expressed by the extended defense tree

3.3 PIS operation

The PIS for the extended defense tree for sequence 2 can be obtained as follows.

Here, the cut set of event 1 is a, b, and that of event 2 is ac:

$(HI1)(\overline{HI2}) = a, b(\overline{ac}) = ab(\bar{a}, \bar{c})$
$= a\bar{a}, a\bar{c}, b\bar{a}, b\bar{c}$ ($a\bar{a}$ in the formula is made null according to the complementation rule of PIS operation)
$= a\bar{c}, b\bar{a}, b\bar{c}$ (12)

The complementation rule means that it is impossible for the event to both exist and not exist at the same time.

The complementation rule is included in PIS operation but is not included in the MCS.

The absorption rule and the idempotent rule are also included in PIS operation.

Here, the probability of the top event of the extended defense tree shown in Fig. 5 can be calculated as follows.

$$\begin{aligned} &P(a\bar{c}, b\bar{a}, b\bar{c}) \\ &= 1 - (1 - P_a \cdot P_{\bar{c}}) \times (1 - P_b \cdot P_{\bar{c}}) \\ &\qquad \times (1 - P_b \cdot P_{\bar{c}}) \\ &= 1 - (1 - 0.84) \times (1 - 0.84) \times (1 - 0.84) \\ &= 0.23 \end{aligned} \qquad (13)$$

3.4 Method of applying the improved EDC method

The flow for applying original EDC method was described in Section 2.1. The EDC is improved in Step 5 “Formulate a combinatorial optimization problem”. The improvement is to add a function for dealing with a common event. The procedure for calculating the overall risk is as follows:

Step 5-1 Obtain the cut set of the attack component of each defense tree. (See Fig. 4.)

Step 5-2 Obtain the PIS for each sequence.

For sequence 1

$$\overline{HI1} = (\overline{a,b}) = \bar{a}\bar{b} \qquad (14)$$

For sequence 2

$$\begin{aligned}(HI1)(\overline{HI2}) &= (a,b)(\overline{ac})\\ &= (a,b)(\bar{a},\bar{c}) \qquad (15)\end{aligned}$$

For sequence 3

$$\begin{aligned}(HI1)(HI2) &= (a,b)(ac)\\ &= (aac, abc)\\ &= (ac) \qquad (16)\end{aligned}$$

Step 5-3 Obtain a formulation to calculate the probability considering alternative countermeasures using the PIS and zero-one variables for each sequence.

$$P_1' = P_0 \cdot \overline{P_1} = P_0 \cdot \overline{P_a} \cdot \overline{P_b} \fallingdotseq P_0 \qquad (17)$$

$$\begin{aligned}P_2' &= P_0 \cdot P_1 \cdot \overline{P_2}\\ &= P_0\big(1-(1-P_a)(1-P_b)\big)(\overline{P_a}\,\overline{P_c})\\ &\fallingdotseq P_0\big(1-(1-P_a)(1-P_b)\big)\end{aligned}$$

(by introducing a countermeasure as zero-one variables, when one countermeasure is applied to events a and b, respectively.)

$$\begin{aligned}&= P_0 \cdot (1-\\ &\quad (1-(P_a \cdot ((1-x_{a1}) + P_{a1} \cdot x_{a1})))\\ &\quad (1-(P_b \cdot ((1-x_{b1}) + P_{b1} \cdot x_{b1})))) \qquad (18)\end{aligned}$$

where x_{a1} represents zero-one variables. If the first countermeasure for event a is adopted, then $x_{a1} = 1$, otherwise $x_{a1} = 0$.

Here, x_{b1} represents zero-one variables. If the first countermeasure for event b is adopted, then $x_{b1} = 1$, otherwise $x_{b1} = 0$.

Here, P_{a1} represents the reduction rate when countermeasure first for event a, and P_{b1} represents the reduction rate when countermeasure first for event b.

$$P_3' = P_0 \cdot P_1 \cdot P_2 = P_0 \cdot P_a \cdot P_c$$

(by introducing a countermeasure as zero-one variables when one countermeasure is adopted for events a and c, respectively)

$$\begin{aligned}&= P_0 \cdot P_a((1-x_{a1}) + P_{a1} \cdot x_{a1})\\ &\quad \cdot P_c((1-x_{c1}) + P_{c1} \cdot x_{c1}) \qquad (19)\end{aligned}$$

where x_{c1} represents zero-one variables. If the first countermeasure for event c is adopted, then $x_{c1} = 1$, otherwise $x_{c1} = 0$.

Here, P_{c1} represents the reduction rate when the first countermeasure is adopted for event c.

In Fig. 4, $P_a = 0.2$, $P_b = 0.2$, $P_b = 0.2$ $P_{a1} = 0.8$, $P_{b1} = 0.8$, and $P_{c1} = 0.8$.

Step 5-4 Obtain a formulation such as Equation (4) to calculate the risk for each sequence.

Step 5-5 Obtain a formulation such as Equation (5) to calculate the overall risk.

Table 1. Rules used in PIS operation

Rule	Example
Idempotent rule	aa => a
Absorption rule	(a, ab) => a
Complementation rule	(a, ā) => Null

4 Experimental risk evaluation

Table 2 shows the results of the calculated overall risk considering a common event using PIS operation and without considering a common event. Here, M1, which represents the impact of sequence 1 of the event tree illustrated in Fig. 1 is set to 10^1. In the same manner, M2 is set to 10^2, and M3 is set to 10^3. In addition, the probability of each lowest event of the defense tree is set to 0.2, and the reduction rate due to the countermeasures is set to 0.8 in order to clarify the effect of taking a common event into account.

The results indicate that the overall risk may be underestimated by a factor of three if we did not use PIS operation.

Table 2. Probability and risk for each sequence

	Proposed method		Previous study	
	probability	risk	probability	risk
P_1'	0.64	6.40	0.64	6.40
P_2'	0.41	41.0	0.35	35.0
P_3'	0.04	400	0.01	100
total		447		141

Table 3 shows the overall risk when the same countermeasure is applied to each of the lowest events in the defense tree. Here, a is a common event, and b and c are not common events. From Table 3, we can determine that the overall risk can be reduced to the greatest degree when the countermeasure was applied to the common event.

Table 3. Probability of the occurrence of each sequence due to the use of a different countermeasure

	Countermeasure applied to event a		Countermeasure applied to event b		Countermeasure applied to event c	
	probability	risk	probability	risk	probability	risk
P_1'	0.67	6.7	0.67	6.7	0.64	6.4
P_2'	0.39	39.0	0.36	36.0	0.42	42.0
P_3'	0.03	300	0.04	400	0.03	300
total		345		442		348

5 Conclusion

In the present paper, we proposed a method that enables common event operation with the original EDC method. Here, the EDC method, which incorporates event tree analysis and defense tree analysis, is used to obtain the optimal combination of countermeasures against targeted attacks.

In order to enable common mode operation, instead of MCS operation, we introduce PIS operation, which can obtain a cut set including negative events for the sequence of the event tree.

The results of the numerical experiment confirmed that we can calculate occurrence probability correctly by introducing the PIS. Moreover, if we did not use PIS operation, the overall risk may be underestimated by a factor of three. Furthermore, if two countermeasures have the same reduction rate and occurrence probability, applying a countermeasure to a common event is more effective than applying it to a non-common event.

In order to use the EDC method more effectively, we intend to develop a support program for the revised EDC method. Moreover, the EDC method and the support program will be applied to a number of targets.

REFERENCES

[1] B. Schneier, ”Attack trees,” Dr. Dobb’s journal, vol.24, pp. 21-29 (1999).

[2] S. Bistarelli, F. Fioravanti, and P. Peretti, ”Defense trees for economic evaluation of security investments,” in Availability, Reliability and Security. ARES 2006. The First International Conference on, p. 8 pp(2006).

[3] Symantec : 2013 ISTR Shows Changing Cybercriminal Tactics , 〈 http://www.symantec.com/connect/blogs/2013-istr-shows-changing-cybercriminal-tactics 〉 (references 2016-7-27)

[4] R. Ishii, R. Sasaki “Proposal of Risk Evaluation Method using Event Tree and Defense Tree and Its Trial Application to Targeted Attack, in Japan Society of Security Management,” p.8 pp(2015) (in Japanese).

[5] N. Yuhara and H. Ujita, System Safety Studies. kaibundo publishing, (2015) (in Jpanese)

[6] D. Kececioglu，“Reliability Engineering Handbook,” vol.2，Prentice Hall，222-231 (1991)

[7] K. Takaragi, R. Sasaki, and S. Shingai “An Algorithm for Obtaining Simplified Prime Implicant Sets in Fault-Tree and Event-Tree Analysis,” IEEE Transactions on Reliability, vol.R-32, pp.386-390(1983).

[8] K. Ingols, R. Lippmann, and K. Piwowarski, “Practical Attack Graph Generation for Network Defense,” in Annual Computer Security Applications Conference, ACSAC 2006, pp.121-130(2006).

[9] A. Roy, D. S. Kim and K. S. Trivedi, “Attack countermeasure trees (ACT): towards unifying the constructs of attack and defense trees,” in Security and Communication Networks, vol.5, pp. 929-943(2012).

[10] Fault Tree Handbook with Aerospace Applications 〈 https://www.hq.nasa.gov/office/codeq/doctree/fthb.pdf 〉