イベントツリーとディフェンスツリーを併用した リスク分析における共通事象を考慮したリスク計算法の提案

相原遼[1]　　佐々木良一[1]

概要：近年，標的型攻撃による被害が増加傾向にある．標的型攻撃では，対象に応じて攻撃に工夫を加えるという特徴を持ち，この特徴のために標的型攻撃を防ぐことが難しいと言われている．一方で標的型攻撃の研究や調査が進んだことで対策の種類が増加し，それらを施すことでリスクは低下する．しかし，実際にはすべての対策を行うことはコストの面で不可能であり，リスクとコストを考慮した対策の選定が必要となる．そこで標的型攻撃に対して効果的な対策をイベントツリー分析とディフェンスツリー分析を併用した EDC 手法を用いることで分析する．これにより標的型攻撃に対して最も効果的な対策を決定する．しかし，この既存の EDC 手法では 1 つの攻撃が複数事象に影響を与える共通事象と呼ばれる問題を考慮しておらず，正しい計算結果を算出できていない．本稿では，EDC 手法に対して共通事象を考慮したリスク計算法の提案を行うとともに例題でのリスク値計算を行った結果を示す．

Proposal of risk calculation technique for including common mode event in Event Tree and Defense Tree combined method

RYO AIHARA[1]　　RYOICHI SASAKI[1]

1. はじめに

サイバー空間のリスクの増大に伴い,定量的にリスク評価を行い，それに基づき適切な対策案の検討を行うことの必要性が高まっている.このような課題に対処するため従来はフォルトツリー分析法やフォルトツリー分析法を Bruce Schneier が改良したアタックツリー分析法[1]に基づきリスクの評価を行うことが多かった.また, Bistarelli ら[2]は対策の検討を行うためにディフェンスツリーを提案している．その後，アタックツリー分析法やディフェンスツリー分析法に関する種々の改良方式の提案が行われてきた[3][4].

一方,近年,標的型攻撃による被害が増加傾向にある[5].標的型攻撃のような時間経過によって多様な攻撃事象が組み合わされる攻撃に対してはフォルトツリー分析法やアタックツリー分析法，従来のディフェンスツリー法ではリスク評価が困難であった.このため本研究室ではイベントツリー分析法とディフェンスツリー分析法を改良したものを組み合わせることで標的型攻撃に対する対策案の最適な組み合わせ手法を求める方法である EDC(Event tree and Defense tree Combined method)手法を開発した[6]．なお, 同様なリスク分析手法として，原子力プラントの安全評価などに用いられる，フォルトツリー分析法とイベントツリー分析法を組み合わせた手法があるが対策案の組み合わせを求める機能はない.

一つの原因により,複数個所の問題が同時に発生するような共通する事象（以下，共通事象）があるとリスクを大きく過小,あるいは過大評価をすることがあることが知られているが, 従来の EDC 手法ではこの点の配慮が十分なされていなかった．EDC 手法中では、一つの攻撃が複数個所に対して影響を与えるものと、一つの対策が複数の攻撃に影響を与えるものが考えられる．後者については，一つの対策がどの攻撃に対応するものかさえ明確にできれば従来の計算方法で正しくリスク低減効果の推定が可能であるが,前者については，計算方法そのものの改良も必要であることが予想された．本稿は前者の方法に関する検討結果を示すものである．

信頼性工学の分野において，このような問題を共通原因故障と呼ぶ．同分野ではフォルトツリーで表現された問題に対して，MCS(Minimal Cut Set)[7]を導出することで共通原因故障問題の解決を図っている.しかし,イベントツリー分析とディフェンスツリー分析を組み合わせて用いる場合においては, 否定事象を含まざるを得ないという特徴から, MCS では適用できない．そこで，否定事象にも適用できる PIS(Prime Implicant Set) [8]を導出する方式を用いることとした．

セキュリティ評価に共通事象を考慮した研究は従来ない．また，セキュリティ評価以外でも対策案と組み合わせて，評価に PIS を導入した例もない．

本論文では,EDC 手法に対し,PIS を導出することで共通

1 東京電機大学

事象を考慮した計算手法を示すとともに,既存の EDC 手法のままと提案手法を導入した方式の 2 つを用いてリスク評価を行った結果を示すことにより提案方式の有用性を示す.

2. 先行研究

2.1 EDC 手法

EDC 手法とは，イベントツリー分析とディフェンスツリー分析を併用したリスク分析であり，職種や規模，分析の対象とする標的型攻撃を定めてイベントツリー分析とディフェンスツリー分析を行い，分析結果と制約条件から最適な対策を算出することのできる手法である.

① 対象の決定

分析にあたり，まず組織の人数や，PC・サーバ台数等の前提条件を考慮する必要がある．そのため，どのような組織を対象とするのかを決定する.

② 標的型攻撃の分析

標的型攻撃は公開サーバへの不正アクセスや，メールを利用したなりすまし攻撃等の標的を絞った攻撃手法の総称であり，様々な攻撃シーケンスが存在するが，侵入後は共通性が高い．IPA の標的型攻撃のレポート[9]を見ても，攻撃の基本的な流れが同じであることがわかる．そこで，実際に起きた標的型攻撃の事例を基に分析をすることで，攻撃の流れを具体的に把握し，詳細な分析を行う.

③ イベントツリー分析によるリスク分析

②の分析結果にイベントツリー分析(ETA)を適応し，標的型攻撃によって被るリスクと大まかな攻撃の流れを推定する.

④ ディフェンスツリー分析によるリスク分析

③で作成したイベントツリーの各事象にディフェンスツリーを構築し，攻撃が実現する確率とその攻撃への対策を設定する．発生確率等の数値に関しては，すべての人が納得する絶対的な算出根拠は存在しないが，統計データや，関係者が討議し合意した値を用いる．そのうえで，不安が残るものは感度解析でその数値を変えて影響を見たりする.

⑤ 各種対策案の決定

標的型攻撃への対策は様々なものが存在するため，①～④までの分析結果を基に導入する対策案のリストを作成する．また，対策案の効果やコスト，ディフェンスツリーへの適応範囲の値付けを行う.

⑥ 目的関数・制約条件の決定

最適な対策案の組み合わせを求めるのに必要な目的関数と制約条件を決定する

EDC 手法の分析結果から,その対策を施した場合のリスク値とコストに対してリスクコミュニケーションを行い，関与者間で合意形成を図る.全員の合意形成が取れるまで，制約条件などを変更し繰り返すことで対策を決定する.このように EDC 手法を用いてリスク分析を行うことで､攻撃に流れがある標的型攻撃に対して,効果的な対策を分析し，決定する.

2.2 イベントツリー分析

イベントツリー分析とは、発生の好ましくない事象（初期事象）を起点として，その事象がどのようなシーケンスに波及をするかについて確率的に解析する手法である．イベントツリーのそれぞれのシーケンスがたどる各事象の発生確率から，そのシーケンスの発生確率を求める．また求めた発生確率にシーケンスが発生したことによる影響度をかけることで，定量的にリスク値を求めることができる．すべてのシーケンスについてリスク値を求めて合計したものが総合リスク値となり，これらのリスク値を低下させるような状態にすることでリスクの低減を図る指標となる.

EDC 手法上では，図 1 のように攻撃の流れを捉えるために，標的型攻撃メールの送信といったような，攻撃者が引き起こす事象を基にイベントツリーの各事象を設定する．一般的に，影響度は攻撃がより侵攻した場合のシーケンスの方が，攻撃が侵攻しなかった場合に比べて非常に大きくなる.

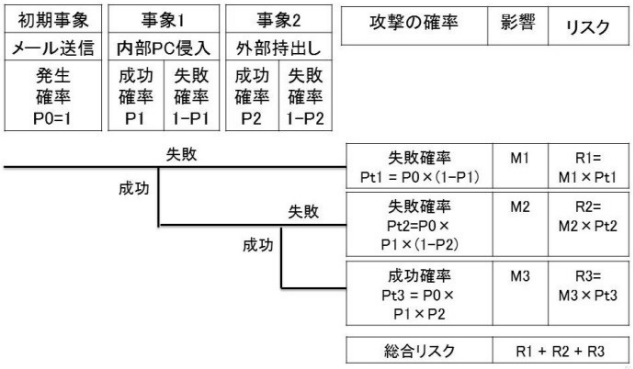

図 1 イベントツリーの例

2.3 ディフェンスツリー分析

ディフェンスツリー分析とは,発生の好ましくないような事象に対して,その要因をトップダウンに分析する手法であるアタックツリー分析に,要因の発生確率を抑えるような対策を加えた分析手法である.イベントツリー分析だけでは困難である各事象の様々な発生パターンとその対策を記述するためにディフェンスツリー分析を用いる.

ディフェンスツリーは大きく分けて事象と対策の二つから構成されている．発生の好ましくない事象を頂上事象とし，より具体的に掘り下げて分析することで、頂上事象を具体的な下位事象に構成して表現する．具体的にするこ

とで下位事象の発生確率を減らすような有効な対策を明確にすることができる．

ディフェンスツリー分析では，図 2 のように下位事象に対策を併記する．図 2 では，下位事象の下に下位事象の発生確率と，さらにその下に対策とその効果を表した数字を表記している．「PC が情報を持っている」事象を a,「プロキシを経由しない通信の成功」事象を b,「C&C サーバブラックリストをすり抜ける」事象を c とすると，頂上事象の発生確率は，xORy を x,y，xANDy を xy と表したとき，ab,ac と表すことができる．ここで Pa=0.7,Pb=0.2,Pc=0.4 を代入することで，頂上事象の発生確率を求めることができる．この場合の発生確率を式(1)に表す． 以降，有効数字は 3 桁とする．

$$
\begin{aligned}
\mathrm{P}(\mathrm{ab},\mathrm{ac}) &= 1-(1-\mathrm{PaPb})\times(1-\mathrm{PaPc}) \\
&= 1-(1-0.7\times0.2)\times(1-0.7\times0.4) \\
&= 0.38 \quad \ldots \quad \text{式(1)}
\end{aligned}
$$

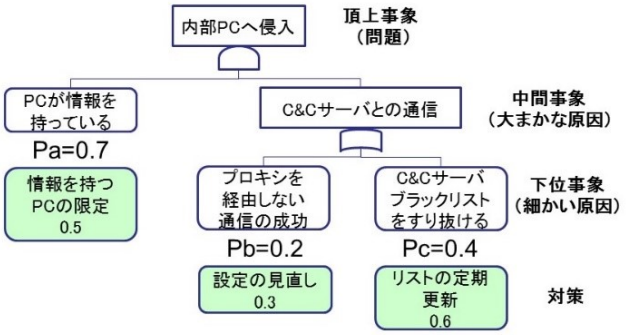

図 2　ディフェンスツリーの例

2.4 対策

ディフェンスツリーにおいて，対策は下位事象の発生確率を低減させるものである．複数の対策のうち，実施した対策の低減率を下位事象の確率にかけていくことで、対策を行った場合の発生確率を求めることができる．したがって，対策の個数が増えるほど，頂上事象の発生確率が減少し，リスク値の低下につながる．

対策を考慮した場合の下位事象の発生確率の一般式は下記の式(2)であらわされる．

$$
Pa' = Pa \times \prod_{i=1}^{n}\{(1-x_i)+P_{di}\times x_i\} \quad \ldots \quad \text{式(2)}
$$

Paは対策を考慮していない場合の発生確率
nはPaに対して対策の総数
iは対策の番号
x_iは対策iの状態を表し，実施した場合に$x_i = 1$，実施しない場合に$x_i = 0$となる
P_{di}は対策iによる低減効果

図 2 で「PC が情報を持っている」事象に対して，「情報を持つ PC の限定」という対策を行った場合について例を示す．対策を考慮した下位事象の発生確率は式(3)のようになる．

$$
\mathrm{Pa} = 0.7, \quad \mathrm{Pa}' = 0.5, \quad \mathrm{n} = 1, \quad \mathrm{i} = 1
$$

$$
\begin{aligned}
\mathrm{Pa}' &= \mathrm{Pa} \times \prod_{i=1}^{n}\{(1-x_i)+P_{di}\times x_i\} \\
&= \mathrm{Pa} \times \prod_{i=1}^{1}\{(1-x_i)+P_{di}\times x_i\} \\
&= Pa \times \{(1-x_1)+P_{d1}\times x_1\} \\
&= 0.7 \times \{(1-1)+0.5\times 1\} \\
&= 0.35 \quad \ldots \quad \text{式(3)}
\end{aligned}
$$

対策を実施したことにより、下位事象の発生確率は Pa から Pa'に変化し，その発生確率は 0.7 から 0.35 と低減している．

このように対策の実施が下位事象の発生確率の低減させる．下位事象の発生確率が低減することで，頂上事象の発生確率の低減，また総合リスクの低減につながる．ディフェンスツリーを用いることで，対策の効果を総合リスクに含めたリスク計算が可能となる．

2.5 対策による効果

対策を実施することで下記の効果がある．

- 対策を実施した下位事象の発生確率の低減
- 下位事象を含むディフェンスツリーの頂上事象の発確率の低下
- ディフェンスツリー分析の対象とした，イベントツリーの事象の発生確率の低下
- イベントツリー中のその事象を含むシーケンスであればその発生確率の増減
- 総合リスク値の減少

EDC 手法による分析が終わった後には，総合リスク値が減少するように対策を選定する．このとき対策を行うことで一般的に総合リスクは低減するが，発生確率が増加し，リスクが増えるシーケンスがある．

前節の図 2 の「PC が情報を持っている」事象に対して，「情報を持つ PC の限定」という対策を行った場合について考える．このとき，前節の通り頂上事象の発生確率は低下する．したがって図 1 の事象 1「内部 PC 侵入」の成功確率 P1 が低下することになる．一方で事象 1 の失敗確率 1-P1 は，成功確率 P1 の否定であるので増加する．これより成功確率 P1 を内包するシーケンスである Pt2 と Pt3 の発生確率は減少する．反対に，失敗確率 1-P1 を含む Pt1 の発生確率は増加することになる．Pt1 の発生確率が増加し，その

リスクが増加することになるが、一般的に，Pt1 の影響度 M1 は攻撃がより進行した場合の Pt2 と Pt3 の影響度 M2 と M3 よりも非常に小さい傾向にある. つまり Pt1 で増加したリスク値よりも，対策によって減少したリスク値が大きいために総合リスク値が低減することなる.

ここでx_i（i=1,2,--,n）の値である 0 か 1 のすべての組み合わせにおけるリスク低減効果とコストなどを求めることにより最適な対策案の組み合わせを求めることが可能となる.

3. 提案手法

3.1 共通事象

共通事象とは,一つの原因に起因して、複数の共通する事象が同時に発生するような事象のことである. 図 3 のフォルトツリーでは「電源断」という共通する事象が一度起きただけで,電球 1 と電球 2 の両方が消えるような故障のことをいう. このような共通事象を考慮しない場合には、確率を重複して計算してしまうことがあり、正確な確率を求めることができない.

共通事象は，信頼性工学の分野では共通原因故障と呼ばれており，このような問題に対して，MCS を導出することで正しい確率を求めることが知られている.

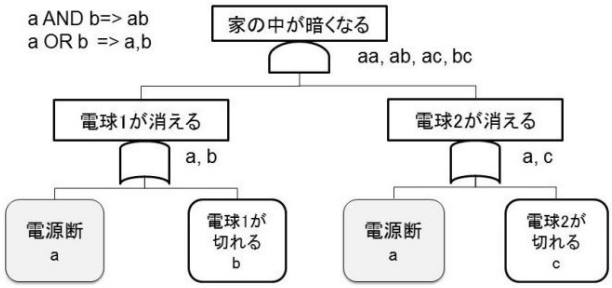

図 3　共通原因故障の例

3.2 MCS

MCS とは,フォルトツリーにおける頂上事象の発生を保証する最小の組み合わせの集合である. ブール演算の吸収則や独立則を用いることで, MCS を導出することができる [10].

図 3 の場合，頂上事象の発生確率は aa,ab,ac,bc と表すことができ，この発生確率に対してブール演算の吸収則や独立則を用いることで，このフォルトツリーである MCS である a,bc を導出することができる. MCS の導出を式(4)に示す.

$$\begin{aligned} aa, ab, ac, bc &= aa, ab, ac, bc \\ &= a, ab, ac, bc \\ &= a, bc \quad \ldots \quad 式(4) \end{aligned}$$

aa はべき等則により a となるが，これは「電源断」が同時に二カ所で起きる事象ではなく，一度発生すれば，両方の電球において「電源断」が発生することを表している. また a,ab や a,ac は吸収則により a となる. これは ab と ac の確率は a に内包されているためである. ここで，MCS を導出する前は aa,ab,ac,bc であるが、これが従来の EDC 手法で使われていた確率の値となる. 仮に a,b,c の各発生確率を 0.2 としたとき MCS を導出していない従来の EDC 手法での場合を式(5)に示す.

$$\begin{aligned} &P(aa, ab, ac, bc) \\ &= 1 - (1 - PaPa) \times (1 - PaPb) \times (1 - PaPc) \times (1 - PbPc) \\ &= 1 - (1 - 0.04) \times (1 - 0.04) \times (1 - 0.04) \times (1 - 0.04) \\ &= 1 - 0.96 \times 0.96 \times 0.96 \times 0.96 \\ &= 0.15 \quad \ldots \quad 式(5) \end{aligned}$$

次に MCS を導出し、確率を求めた場合を式(6)に示す.

$$\begin{aligned} P(a, bc) &= 1 - (1 - Pa) \times (1 - PbPc) \\ &= 1 - (1 - 0.2) \times (1 - 0.04) \\ &= 1 - 0.8 \times 0.96 \\ &= 0.23 \quad \ldots \quad 式(6) \end{aligned}$$

式(5)と式(6)より，MCS を導出していない場合の確率より，MCS を導出した場合の確率がこの場合ではおよそ 1.5 倍大きくなった. これは共通事象を考慮したために，その発生確率の過小評価を防いだためである.

式(4)によって MCS を導出したが，これをフォルトツリーで表すと図 4 のようになる. MCS を導出することで,「電源断」という事象が重複しないような形で表すことができた. このような事象が重複しないようなフォルトツリー分析を最初から行うことができれば MCS の導出は必要ないが，実際にはトップダウンに分析していくというフォルトツリー分析の特徴から，予め共通事象を抜き出すということは難しいため MCS の導出が必要となる.

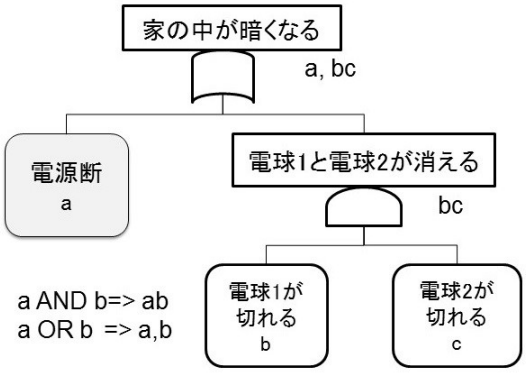

図 4　MCS のフォルトツリー

3.3 PIS

PIS とは, MCS を拡張したものであり，イベントツリー

における各シーケンスの発生を保証する最小の組み合わせの集合である．

ここで、共通事象の扱いにより、評価結果がどの程度異なるかを明確にするため図 1 と図 5 の EDC 手法の例を用いて，分析を行う．事象 1 が成功し，かつ事象 2 が失敗するシーケンスの確率である Pt2 の PIS を導出する．

図 5 の各頂上事象の発生確率は事象 1 を a,b，事象 2 を ac と表すことができる．図 1 の 2 番目のシーケンスの PIS は以下のようになる．

$$\begin{aligned} a,b(\overline{ac}) &= ab(\bar{a},\bar{c}) \\ &= a\bar{a},a\bar{c},b\bar{a},b\bar{c} \\ &= a\bar{c},b\bar{a},b\bar{c} \quad \ldots \quad \text{式(7)} \end{aligned}$$

式(7)は，まず分配則により展開される．このとき，式中の$a\bar{a}$は相補則により 0 となる．これは a が起きた事象と a が起きない事象が同時に発生することがないためである．このようにして PIS を導出することができ，したがって Pt2 の確率は

$$\begin{aligned} Pt2(a\bar{c},b\bar{a},b\bar{c}) &= 1-(1-PaP\bar{c})\times(1-PbP\bar{c})\times(1-PbP\bar{c}) \\ &= 1-(1-0.84)\times(1-0.84)\times(1-0.84) \\ &= 0.41 \end{aligned}$$

となる．

このようにイベントツリーでは，事象の成功と失敗の組み合わせでシーケンスの発生確率を表すため，その発生確率に事象の否定を内包することがある．これにより，本来ならば同時に起きえることがないような場合が存在してしまい、リスク値を大きく過大または過小評価してしまうことがある．その発生が存在しないような場合についても相補則などのブール演算によって排除を行うことで正しい発生確率を求めることができる．

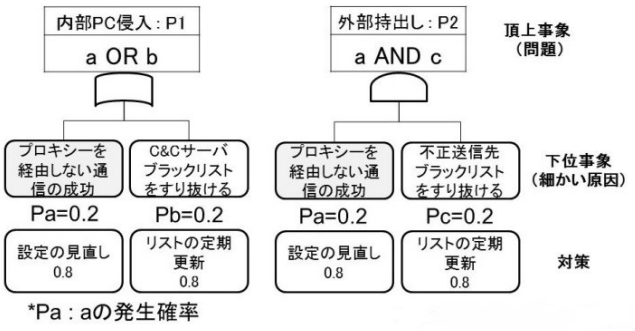

図 5　ディフェンスツリーの例

3.4 適応方法

前節までで述べた手法を EDC 手法に対して適応する．

まず EDC 手法を用いて分析を行う．その後，各シーケンスの発生確率に対して MCS/PIS を導出し，共通事象や起こりえない場合について排除を行う．これにより正しい確率の計算を行う．

4. リスク評価

図 1 と図 5 の EDC 手法の分析例を用いて計算を行い,その結果を示す.イベントツリーの影響度を，ここでは仮に M1 を 10^1, M2 を 10^2, M3 を 10^4 とする.ここで共通事象を考慮したことによる影響度を確認するために，ディフェンスツリーの各下位事象の確率を 0.2,その対策による低減率を 0.8 と同じ値とする．

4.1 リスク評価 1

先行研究との比較を行う.表 1 は,対策を行っていない場合の MCS/PIS を考慮した提案手法と考慮していない先行研究とのそれぞれでリスク値の計算を行った結果である．

表 1　各シーケンスの発生確率とリスク値

	提案手法		先行研究	
	確率	リスク値	確率	リスク値
Pt1	0.64	6.40	0.64	6.40
Pt2	0.41	41.0	0.35	35.0
Pt3	0.04	400	0.01	100
合計		447		141

4.2 リスク評価 2

対策箇所によるリスク値を比較する.表 2 は,提案手法を用いて,ディフェンスツリーの各事象に対策を実施した場合のリスク値の計算を行った結果である．

表 2　対策の違いによる各シーケンスの発生確率

	aに対策		bに対策		cに対策	
	確率	リスク値	確率	リスク値	確率	リスク値
Pt1	0.67	6.7	0.67	6.7	0.64	6.4
Pt2	0.39	39.0	0.36	36.0	0.42	42.0
Pt3	0.03	300	0.04	400	0.03	300
合計		345		442		348

5. 考察

5.1 評価 1 の考察

提案手法と既存の EDC 手法では Pt1 に差異はないが,Pt2,Pt3 は発生確率が増加している.これは既存の EDC 手法において,共通事象を含む場合に確率を過小評価してしまうことがあるためである．

提案手法における Pt3 の確率は既存の EDC 手法に比べ 4 倍に上昇している.これは Pt1,Pt2 に比べ小さく見える

が,Pt3 はすべての攻撃が成功した場合であり,その影響度は他と比べ,より大きくなる傾向にある.したがって Pt3 のリスク値は,既存の EDC 手法と提案手法で大きな差がでることになった.これより，より影響が大きいものが，リスク値において支配的になり，Pt3 の発生確率を低くすることがリスクの低下につながることがわかる．この結果から，分析した標的型攻撃の最悪のシナリオの発生確率を減少させ総合リスク値を下げるために，影響度の大きい出口対策を行うことが有効であることがわかる．

5.2 評価 2 の考察

対策を,共通事象である a とそれ以外の b または c に対して施した場合についてリスク評価を行った結果，a に対して対策を施した場合に最も低い総合リスク値が得られた．このことから各下位事象の発生確率と対策の効果が同じ場合において,共通事象に対して対策をしたほうがより効果的であることがわかる.また，c に対して対策を行った場合には，二番目に低いリスク値を得ることができた．最も低い総合リスク値である a と次に低い b では，影響度が大きい Pt3 のリスク値は同じ値となっている. a と c のそれぞれに対策をした場合の各シーケンスの発生確率を見ると，影響度が 10^1 である Pt1 については c に対策をした場合の発生確率のほうが a にくらべ 0.03 小さく，影響度が 10^2 である Pt2 については a に対策をした場合の発生確率が b にくらべ 0.03 小さくなっている．減少した発生確率は同値であるが、影響度がより大きい Pt2 の発生確率が減少する a に対して対策を実施したほうが、より小さい総合リスク値を得られることがわかる．

評価 2 より，EDC 手法で分析した標的型攻撃の初期事象から最後の事象の間の幅広い部分で有効である対策を行うことで，総合リスク値を減少させることが可能であることがわかった．例えば，SIEM 製品による検知箇所の増加やサンドボックス型製品のような複数個所に効く製品を導入することで，大幅な総合リスク値の減少が望める．

6. おわりに

本稿では,標的型攻撃に対してイベントツリー分析法とディフェンスツリー分析法を併用した EDC 手法において,PIS と MCS を導出することで,共通事象を考慮したリスク値計算を行った.4 章で行ったリスク値計算では，PIS と MCS を導出した確率と従来の EDC 手法での確率の計算を行い比較し, 従来の EDC 手法ではリスクを過小または過大評価してしまうことが分かった．また，同じ発生確率と同じ対策による低減率であるときに，共通事象に対策を行った場合と共通事象でない事象に対策を行った場合では共通事象に対策を行った方がより効果的であることが分かった.

今後の展開として, 対策のコストについての考慮は, EDC 手法での分析後に実施する対策を決定する際に行われるが,対策を決定するための一つの目安として、対策を導入した際の利用者や運営者の負担についての考慮することが挙げられる．また，共通事象に対して同じ対策が有効であることが多いが，すべての共通事象に対策を行うのではなく，共通事象の一部のみに対策を実施したい場合があることが考えられる．さらに，すべての攻撃者の技術レベルには違いがあり、この違いが攻撃事象の成功確率に影響を与える点についての考慮が必要であると考えている．また EDC 手法自体をより円滑に行うために，EDC 手法を行うツールの開発を検討している． EDC 手法を行うツールの要件として，イベントツリー分析，ディフェンスツリー分析が行えること, PIS と MCS を導出し発生確率を求められること，対策の有無によるリスク値の計算ができることが挙げられる．

参考文献

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

[2] Bistarelli,S. Fioravanti.,F. and Peretti,P. :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] Ingols,K. Lippmann,R. Piwowarski,K. :Practical Attack Graph Generation for Network Defense, in Annual Computer Security Applications Conference, ACSAC 2006, pp.121-130(2006).

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

[5] TRENDMICRO : 2015 年、昨年の脅威動向から考える標的型メール攻撃対策,
〈http://www.trendmicro.co.jp/jp/business/solutions/apt/threat2014/index.html〉(参照 2016-2-26)

[6] 石井亮平, 佐々木良一, “イベントツリーとディフェンスツリーを併用したリスク評価手法の提案と標的型攻撃への試適用”, 日本セキュリティ・マネジメント学会第 29 回全国大会 (2015).

[7] 一般財団法人機械振興協会:故障の影響解析(FMEA)と、故障の木解析(FTA)の活用 詳細,
〈http://www.jspmi.or.jp/system/l_cont.php?ctid=130403&rid=836〉(参照 2016-5-4)

[8] Takaragi,K. Sasaki,R. Shingai,S.: 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).

[9] 「高度標的型攻撃」対策に向けたシステム設計ガイド,
〈https://www.ipa.go.jp/files/000046236.pdf〉(参照 2016-2-29)

[10] 油原直弘，氏田博士，“システム安全学―文理融合の新たな専門知”，海文堂出版，407-410 (2015).