情報処理学会論文誌 Vol.63 No.3 899–907 (Mar. 2022)

自治体セキュリティモデルのための リスクアセスメント手法の提案と適用

佐々木 良一[1,a)] 千葉 寛之[2] 甲斐 賢[2] 木下 翔太郎[3]

受付日 2021年6月22日, 採録日 2021年12月3日

概要：情報システムへの社会の依存度の増大により，情報システムに対するリスクアセスメントの重要性が増大してきている．総務省でも地方自治体のマイナンバー利用事務系，LGWAN 接続系，インターネット接続系からなる 3 階層分離モデルに対し，セキュリティリスク，対策コスト，作業の負担度のバランスのとれた対策案の組合せを求める必要があった．著者らは，標的型攻撃のようにシーケンスが深い攻撃に対する定量的リスクアセスメント手法として，イベントツリー分析法とディフェンスツリー分析法を組み合わせた EDC 法（Event tree and Defense tree Combined method）を開発してきた．しかし，EDC 法をそのままこのシステムに適用しようとすると，① 従来の評価指標はコストとリスク低減効果だけに対応するものであり，それ以外に作業負担度も考慮に入れる必要がある，② 侵入先が 2 カ所あり，2 段階の侵入を考慮したリスクアセスメントが必要である，③ 対象システムの構成原案が α モデル，β モデル，β' モデルと複数あり，それぞれをベースにした対策案の最適組合せを求めるとともに，全体としての最適な対策の組合せを求める必要があるなどの問題があった．このような問題を解決するために，拡張 EDC 法とその支援プログラムである PEEDC を開発し，地方自治体セキュリティモデルに適用した．その結果，拡張 EDC 法の有効性を確認するとともに，地方自治体のあるべきセキュリティ対策として種々の具体的知見が得られたので報告する．

キーワード：リスクアセスメント，イベントツリー分析，ディフェンスツリー分析，自治体セキュリティモデル，対策案最適組合せ

Proposal and Application of Risk Assessment Method for Local Government Security Models

Ryoichi Sasaki[1,a)] Hiroyuki Chiba[2] Satoshi Kai[2] Shotarou Kinoshita[3]

Received: June 22, 2021, Accepted: December 3, 2021

Abstract: With the increasing dependence of society on information systems, the importance of risk assessment of information systems is increasing. It is also necessary to request the security model of Japanese local governments in order to determine a combination of countermeasures with a good balance between security risk, countermeasure cost, and work burden. In order to obtain the optimum combination of information system countermeasures for local governments, we have developed an extended event tree and defense tree combined (extended EDC) method, which is an improvement of the previously developed EDC method, and developed a support program for the extended EDC. However, when the EDC method was applied to this system as it was, there were the following three problems. (1) Conventional evaluation indexes correspond only to cost and risk reduction effects, and it is also necessary to take into consideration the degree of work load. (2) There are two intrusion destinations, and a risk assessment that considers two stages of intrusion is required. (3) There are multiple drafts of the configuration of the target system, such as α model, β model, and β' model, and it is necessary to find the optimum combination of countermeasures based on each model and the optimum combination of countermeasures as a whole. In order to solve such problems, we developed the extended EDC method and its support program, PEEDC, and applied them to the local government security model. As a result, we confirmed the effectiveness of the extended EDC method and obtained various useful findings as the ideal security measures for local governments.

Keywords: risk assessment, event tree analysis, defense tree analysis, local government security model, optimal combination of countermeasures

1. はじめに

情報システムへの社会の依存度の増大により，情報システムに対するリスクアセスメントの重要性が増大してきている．

一方，地方自治体の情報システムに対するセキュリティ向上のためセキュリティガイドが 2015 年に総務省によって制定され，内部ネットワークをマイナンバー利用事務系，LGWAN 接続系，インターネット接続系に分離する 3 層分離モデルが推奨されるようになった．ここで，LGWAN というのは地方公共団体を相互に接続する行政専用のネットワークのことである．このモデルの採用により，地方自治体のインシデント数は大幅に低減された．しかし，インターネット接続系から LGWAN 接続系にデータを送る際には，セキュリティの確保のため，メールの無害化やファイルの無害化が必須とされていたが，この手間が大きく，実施していない自治体もあるということが問題になっていた．

そのため，総務省は 2019 年よりモデルの見直しをはかり，ネットワークをマイナンバー利用事務系，LGWAN 接続系，インターネット接続系の 3 つに分離しているもともとのモデルを α モデルというのに対し，自治体職員などによる作業負担を低減し使い勝手を向上するため，LGWAN 接続系の業務の一部と業務端末をインターネット接続系に移す β モデルや β' モデルを示し，これらを採用してもよいという方針を打ち出した．多くの業務をインターネット接続系に移すことにより，インターネット接続系から LGWAN 接続系へのメールやファイルの転送の数を減らすとともに，インターネット接続系に EDR（Endpoint Detection and Response）などを導入することによりそのセキュリティを高めようとするものである．

これらのモデルを提案するにあたっては，総務省としても準定量的リスクアセスメントを実施している．しかし，地方自治体が，具体的対策の組合せを決定するには，攻撃シーケンスが深い攻撃を考慮し，セキュリティリスクと対策コストと作業の負担度の 3 つを組み合わせて最適な構成案を求めるための定量的リスクアセスメント手法が必要になってくると考えた．

著者らは，攻撃のシーケンスが深いシステムに対する定量的リスクアセスメント手法として，EDC 法（Event tree and Defense tree Combined method）[1] を開発してきた．これは Event Tree 分析法と Defense Tree 分析法に最適化手法を組み合わせて用い対策案の最適な組合せを求めるものである．本方式はすでに実システムに適用し，組織のセキュリティ対策を決定するのに実際に利用されている [1]．

しかし，この方式を用いて，自治体のセキュリティ対策の最適な組合せを求めるためには次のような問題があることが分かった．

① 従来の評価指標はコストとリスク値だけに対応するものであった．ここではコストとリスク値以外に対策の実行にあたって自治体の職員などによる作業負担度も考慮に入れる必要がある．

② 侵入先がインターネット接続系と LGWAN 接続系の 2 カ所あり，2 段階の侵入を考慮したリスクアセスメントが必要である．

③ 対象システムの構成原案が α モデル，β モデル，β' モデルと複数あり，それぞれをベースにリスクを最小とする対策案の最適組合せを求めるとともに，それらのうちからリスク値を最も小さくする対策の組合せを求める必要がある．

そこで EDC 法をこれらの問題点に対応できるように改良する方式を確立し，拡張 EDC 法と名付けるとともに，対策案の最適な組合せを求める機能をプログラム PEEDC（Program for Extended EDC）として実装した．

この拡張 EDC 法と PEEDC を，α と β' からなる地方自治体セキュリティモデルに対し，2 段階の侵入を対象とし，リスク，コスト，作業負担度の 3 つの指標を考慮して，最適な組合せを求めるのに適用した．その結果，拡張 EDC 法の有効性を確認するとともに，対策に関する種々の知見が得られたので報告する．

リスクアセスメント手法はいろいろ提案されており（たとえば文献 [2], [3]），著者らもいろいろな手法を提案してきたが（たとえば文献 [4], [5]），定量的方法を，地方自治体のセキュリティモデルに適用し，対策案の最適な組合せを求めた例はない．

以下，本稿では 2 章でリスクアセスメント手法の動向，3 章で自治体セキュリティモデルの概要，4 章で拡張 EDC 法の提案，5 章で自治体セキュリティモデルへの適用結果について報告する．

2. リスクアセスメント手法の動向

セキュリティ対策を実施するために，事前にリスクアセスメントを実施するのがようやく当然になりつつある．リスクマネジメントにおけるリスクアセスメントの位置づけは，**図 1** に示すとおりである．また，リスクアセスメントを構成するリスク分析には次の 4 つのアプローチがある [6]．

(1) ベースラインアプローチ

既存の標準や基準をもとにベースライン（自組織の対策基準）を策定し，チェックしていく方法．簡単にできる方

[1] 東京電機大学
Tokyo Denki University, Adachi, Tokyo 120–8551, Japan
[2] 日立製作所
Hitachi Ltd., Chiyoda, Tokyo 100–8280, Japan
[3] 日立コンサルティング
Hitachi Consulting, Chiyoda, Tokyo 102–0083, Japan
[a)] r.sasaki@mail.dendai.ac.jp

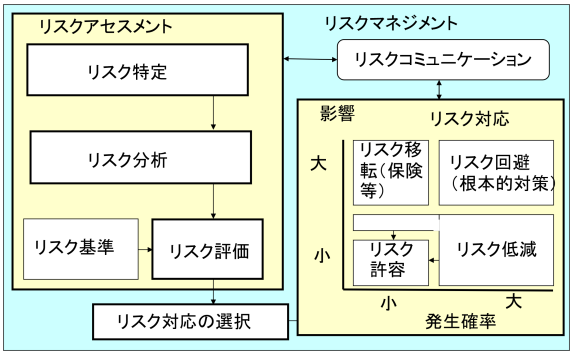


図 1 リスクマネジメントの要素と相互関連
Fig. 1 Risk management elements and interrelationships.

表 1 アセスメントのアプローチ法
Table 1 Assessment approach methods.

アプローチ法	長所	欠点
定量的	費用対効果分析を最も効果的に支援	得られた数値または結果に関する信頼性の説明が必要
準定量的	比較的少ないコストで相互比較が可能に	厳密性が不足
定性的	分析にコストがかからない	経験により結果が異なる場合もある

NIST SP 800-30 Rev.1を参考に作成

法であるが，選択する標準や基準によっては求める対策のレベルが高すぎたり，低すぎたりする場合がある．

(2) 非形式的アプローチ

コンサルタントまたは組織や担当者の経験，判断によりリスクアセスメントを行う．短時間に実施することが可能である属人的な判断に偏る恐れがある．

(3) 詳細リスク分析

詳細なリスクアセスメントを実施．情報資産に対し「資産価値」「脅威」「脆弱性」「セキュリティ要件」を識別し，リスクを評価していく．厳密なリスク評価が行えるものの多大な工数や費用がかかる．

(4) 組合せアプローチ

複数のアプローチの併用．よく用いられるのは，(1) ベースラインアプローチと (3) 詳細リスク分析の組合せ．ベースラインアプローチと詳細リスク分析の両方のメリットが享受できる．

ここでは，厳密なリスクアセスメントが可能な，(3) 詳細リスク分析を採用することとする．詳細リスク分析法としては，**表 1** に示すように，定量的，準定量的，定性的の 3 種のアプローチがあるが，ここでは，費用対効果の推定が可能となる定量的アプローチを採用する．また，リスクマネジメントで扱う範囲は，**図 2** に示すようなものがあり，ここでは範囲 3 を採用し，対策案の最適な組合せまで求められるようにすることにした．

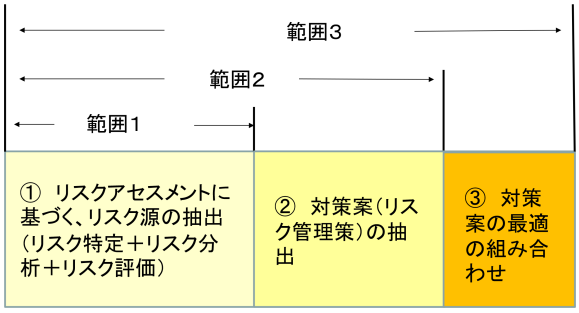


図 2 リスクマネジメントで扱う範囲
Fig. 2 Scope of risk management.

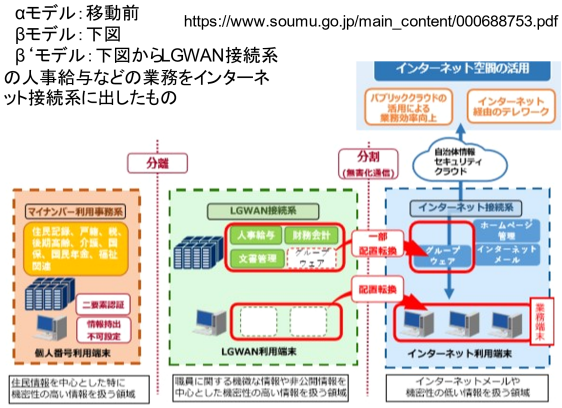


図 3 対象モデル（$\alpha \cdot \beta \cdot \beta'$）の概要
Fig. 3 Outline of the target models (α, β, β').

3. 自治体セキュリティモデルの概要

総務省は，2014 年に自治体情報セキュリティ対策チーム（座長：佐々木良一）を設置し，攻撃リスク低減のための抜本的強化対策として 5 つのセキュリティ対策を提案したが [7]，その中心となるのが，マイナンバー利用事務系，LGWAN 接続系，インターネット接続系に分離しその間のリスク分離を図る対策である（のちに 3 階層分離モデルといわれるようになる）．この対策を用いることにより，地方自治体によるサイバーインシデント件数は大幅に低減されたが，地方自治体から使い勝手の悪さや自治体職員の作業負担度の大きさに関するクレームが多く，総務省は 2019 年 12 月より，「地方公共団体における情報セキュリティポリシーに関するガイドラインの改定等に係る検討会」（座長：佐々木良一）をスタートし，方式の見直しを行った．

その結果，従来のものを**図 3** に示すように α モデルと呼ぶのに対し，負担度の低減を図る β モデルや β' モデルも提案された．ここで，β モデルは，グループウエアを，インターネット接続系に移したもので，β' モデルは人事給与や文書管理や財務会計などもインターネット系に移したものである．いろいろな機能をインターネット接続系に出すことによって，従来行っていた，メールの無害化やファイルの無害化の作業頻度が減り，負担度が低減されるという判断からである．一方，リスクを低減させるためには，

インターネット接続系に EDR（Endpoint Detection and Response）などを導入することを推奨している．これらの方式を提案するにあたって，総務省は準定量的なリスク分析を行っている．

β モデル，β' モデルの導入によって，地方自治体でセキュリティ対策の選択肢が増えた．著者らはそれぞれのセキュリティモデルに対応し，リスク，コスト，作業負担度を考慮してどのような対策を組み合わせるのが最適かや，どのセキュリティモデルに基づくのが最適かを具体的に決定するための手法が必要になると考え，支援手法を検討した．

4. 拡張 EDC 法の提案

4.1 従来の EDC 法の概要

EDC 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法をベースに，対策案の最適な組合せを求める方法であり，著者らが開発したものである．EDC 法は次のような手順で実施される [1]．

ステップ 1：対象の決定

評価対象となる組織を選定し，組織の人数や PC やサーバの数，ネットワークの構成などを明らかにする．

ステップ 2：攻撃法の分析

どのような攻撃を対象とし，どのようなリスクを評価指標とするかを明確化する．たとえば攻撃としては標的型攻撃であったり，内部不正であったりする．評価指標としては，情報の流失や，データの破壊，システムの停止などがある．

ステップ 3：イベントツリー分析

対象とする組織に対する想定した攻撃が想定した評価指標に及ぼす影響を考慮し，イベントツリーを作成する．たとえば，標的型攻撃を対象とし，情報の流出を評価指標とするなら，イベントツリーは図 4 に示すようになる．「ウイルス感染」や「情報の流出」など分岐の条件となるものをヘディング項目と呼んでいる．ここで，シーケンス 1 は，標的型メールが送られてくるが適切な対応をとることによってウイルスに感染することはない事象，シーケンス 2 は，標的型メールが送られてきてウイルス感染してしまうが情報の流出までには至らない事象を表している．また，シーケンス 3 は標的型メールが送られてきてウイルス感染してしまい，情報の流出にまで至ってしまう事象を表している．

これらのシーケンスの発生確率はヘッディング項目であるウイルス感染確率 PH1 や，情報流出確率 PH2 から図 4 に示すようにして計算することができる．また，損害額 M1，M2，M3 は，それぞれのシーケンスごとに類推して与える．たとえば，M1 は，被害がないのでゼロと類推できる．また，M2 は感染した PC の復旧費用，M3 は，情報流出による賠償額や信頼の低下による損失額などが考えられる．シーケンスごとのリスク R1，R2，R3 は通常，各シーケンスの発生確率 $*$ 損害額で定義されており，トータルリスクはそれらの合計となる．このトータルリスクを，評価指標の 1 つとして扱う．

ステップ 4：ディフェンスツリーによるリスク分析

ステップ 3 で用いる PH1 や PH2 を，関連するすべての対策の組合せごとに計算できるようにするものである．PH1 を計算するためのディフェンスツリーは図 5 に示すようになる．攻撃の成功に導く要因を AND 記号と OR 記号を用いアタックツリーとして表現している．

アタックツリーは上位項目 A が下位項目 B と C の AND 条件であらわされるなら，その確率は $PA = PB * PC$ で計算でき，OR 条件であらわされるなら $PA = 1 - ((1 - PB) * (1 - PC)) = PB + PC - PB * PC$ で計算できる．ここで，PA は A の発生確率であり，PB は B の，PC は C のそれぞれ発生確率である．

ここではそのアタックツリーの最下位項目を対策と組み合わせたものを，ディフェンスツリーと呼んでいる．ディフェンスツリーではアタックツリーの最下位項目の対策後の発生確率と，対策後の発生確率と推定コストを与える．

このとき，PH1 の値を計算する式は次式で与えられる．

$$PH1 = PE1 * PE2$$

$$PE1 = 0.1 * X_1 + 0.3 * (1 - X_1)$$

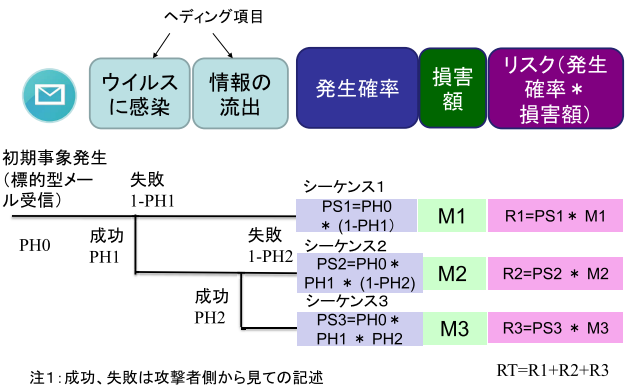


図 4 イベントツリー分析法

Fig. 4 Event tree analysis method.

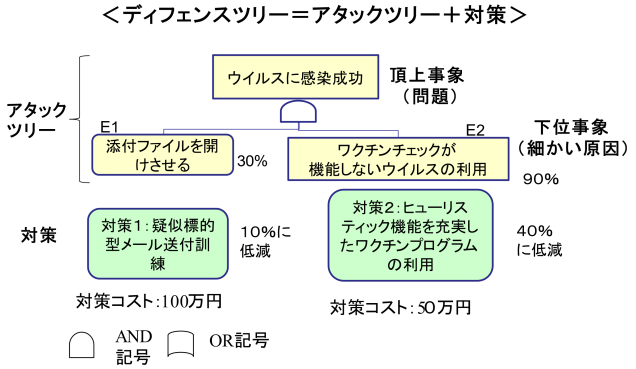


図 5 ディフェンスツリー分析法

Fig. 5 Defense tree analysis method.

$$PE2 = 0.9 * X_2 + 0.4 * (1 - X_2)$$

ここで，対策を i（$i = 1, 2$）とするとき，対策 i を採用するなら $X_i = 1$，しないなら $X_i = 0$ となる．このようにすることによって対策案の採用不採用のすべての組合せについて最上位項目の発生確率 PH1 を表現できるようになっている．PH2 についても同様にして表現が可能である．

ステップ 5：対策案のリストアップとパラメータの推定

標的型攻撃への対策は様々なものが存在するため，ステップ 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，対策案ごとの効果や対策コストの推定を行う．

ステップ 6：目的関数や制約条件の設定と定式化

目的関数を，たとえば，トータルリスクの最小化とし，制約条件をトータルコストとして次のように定式化する．

Minimize:

$$RT \quad (X_i \mid i = 1, 2, \cdots, n) \tag{1}$$

Subject to

$$\sum_{i=1}^{n} C_i * X_i \leqq Ct \tag{2}$$
$$(X_i = 0, 1)$$

ここで RT は，トータルリスクを求めるための関数であり，C_i は i 番目の対策案のコストを表している．X_i は，0-1 変数であり，$X_i = 1$ なら i 番目の対策案を採用し，0 ならば採用しないことを表す．

RT は，イベントツリー分析で説明した式と，ディフェンス分析で説明した式を，「ヘッディング項目の発生確率である PH1 や PH2」を介して組み合わせることで求めることができる．また，対策案 i は，ディフェンスツリー分析により抽出されたものを順序付けしたものである．

ステップ 7：対策案の最適な組合せの計算

ステップ 6 で決定した制約条件を満たす中で目的関数を最小とする対策の組合せを求める．

ステップ 8：リスクコミュニケーションによる関与者の合意形成

分析者と意思決定関与者が集まり，議論し，評価指標や，対策効果，対策コスト，さらには制約条件を変えながら解を求め，合意が形成されるまでこの過程を繰り返す．

4.2 EDC 法の拡張方法

すでに述べたように，自治体システムへの適用にあたっては，次の 3 つの問題の解決が必要である．

問題① 従来の評価指標はコストとリスクだけに対応するものであった．ここではコストとリスク以外に作業負担度も考慮に入れる必要がある．

問題② 侵入先がインターネット接続系，LGWAN 接続系の 2 カ所あり，2 段階の侵入を考慮したリスクアセスメントが必要である．

問題③ 対象システムの構成原案が複数あり，それぞれをベースにした対策案の最適組合せを求めるとともに，それらの中でさらに最適な対策案の組合せを求める必要がある．

そこで，以下の拡張を行った．

問題①を解決するために，定式化において制約条件に，作業負担度を追加する．

問題②を解決するために，攻撃のシーケンスを分析し，イベントツリーの構造に反映させる．

問題③を解決するために，α モデル，β モデル，β' モデルなどの構成原案ごとに対策案の最適な組合せを求めるとともに，同じ制約条件の下でトータルリスクが一番小さいものを全体の最適な対策組合せとして採用する．

5. リスクアセスメント手法の自治体セキュリティモデルへの適用

5.1 対象の決定

ここでは，地方自治体の情報システムを対象とする．モデルケースとしては，人口十万程度の市を対象とし，職員数は約 650 人，PC 数は約 1,000 台とする．これらの PC は図 3 に示すようにインターネット接続系，LGWAN 接続系，マイナンバー利用事務系のどれかに属するものとする．今回の適用ではインターネット接続系，LGWAN 接続系に属する情報システムを対象とする．

また，情報システムの構成原案としては，同じく図 3 に示すように，α モデル，β モデル，β' モデルがある．モデルごとのサーバの所属は，**表 2** に示すとおりである．なお，今回の適用では，まずは，α モデルと β' モデルを対象とする．

5.2 攻撃法の分析

攻撃としては，標的型攻撃や，内部不正攻撃などが考えられるが，ここでは標的型攻撃を対象とする．攻撃の方法は α モデルの場合は**図 6** に示すとおりである．攻撃対象がインターネット接続系の情報だけでなく LGWAN 接続系の情報も含め 2 段階の侵入を考慮しなければならない点

表 2 サーバ機能の所属領域
Table 2 Area to which the server function belongs.

	αモデル	βモデル	β'モデル
インターネットメール	○	○	○
ホームページ管理	○	○	○
LGWANメール	◎	◎	◎
人事給与	◎	◎	○
財務会計	◎	◎	○
文書管理	◎	◎	○
グループウエア	◎	○	○
	2:5	3:4	6:1

注：n:m
n：インタ-ネットにおけるサーバ機能数
m：LGWAN接続系のサーバー機能数

○：インターネット接続系
◎：LGWAN 接続系

7

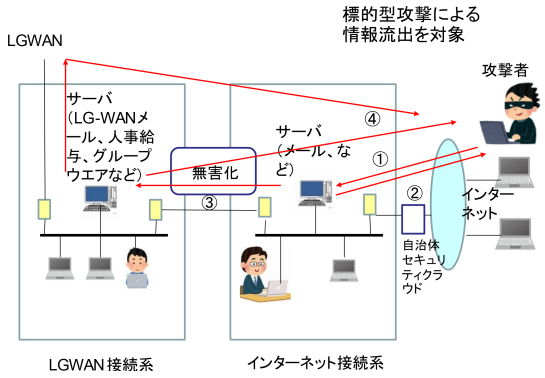
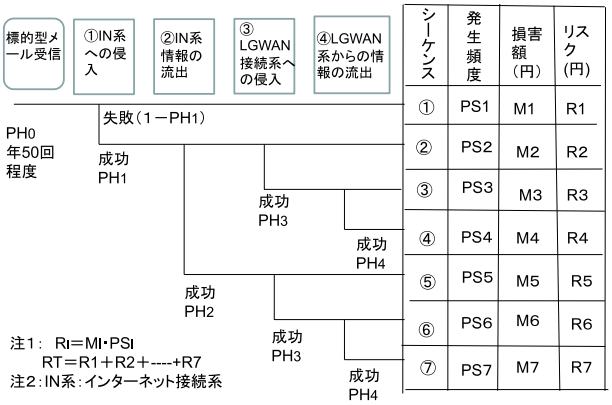


図 6 攻撃方法（α モデルを対象）

Fig. 6 Attack method (for α model).



シーケンス	発生頻度	損害額（円）	リスク（円）
①	PS1	M1	R1
②	PS2	M2	R2
③	PS3	M3	R3
④	PS4	M4	R4
⑤	PS5	M5	R5
⑥	PS6	M6	R6
⑦	PS7	M7	R7

図 7 イベントツリーの構成

Fig. 7 Event tree configuration.

が特徴である．

β' モデルも，インターネット接続系や LGWAN 接続系のサーバの機能数が違うだけで，攻撃の方法は基本的に同じである．

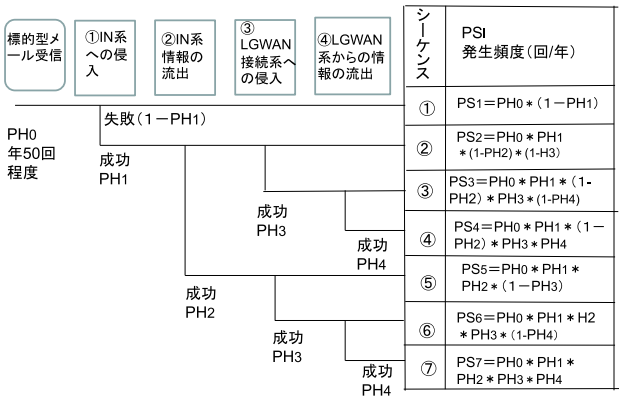
5.3 イベントツリー分析

この攻撃に関するイベントツリーの構成は，**図 7** に示すとおりである．インターネット接続系と LGWAN 接続系という 2 つの領域への侵入をヘディング項目としてそれぞれ用意することにより，4.2 節で述べた問題②に対応できるようになっている．

ここで，シーケンスごとの発生頻度の計算方法は**図 8** に示すとおりであり，損害額（影響の大きさともいう）推定値は**表 3** に示すとおりである．

5.4 ディフェンスツリーによるリスク分析

イベントツリーのヘディング項目別に，ディフェンスツリーを作成する．インターネット接続系への侵入に関するディフェンスツリーは，**図 9** に示すようになる．他のヘディング項目に対するディフェンスツリーも同様にして求めることができる．



シーケンス	PSI 発生頻度（回/年）
①	PS1＝PH0＊(1－PH1)
②	PS2＝PH0＊PH1＊(1-PH2)＊(1-H3)
③	PS3＝PH0＊PH1＊(1-PH2)＊PH3＊(1-PH4)
④	PS4＝PH0＊PH1＊(1－PH2)＊PH3＊PH4
⑤	PS5＝PH0＊PH1＊PH2＊(1－PH3)
⑥	PS6＝PH0＊PH1＊H2＊PH3＊(1-PH4)
⑦	PS7＝PH0＊PH1＊PH2＊PH3＊PH4

図 8 シーケンスごとの発生頻度計算法

Fig. 8 Calculation method of probability for each sequence.

表 3 シーケンスごとの損害額推定値

Table 3 Estimated damage amount for each sequence.

シーケンス		項目	損害額 α	損害額 β	損害額 β′
①	M1	影響はない	0円	0円	0円
②	M2	インターネット接続系PC10台のフォレンジック費用（1台100万円）	1000万円	1000万円	1000万円
③	M3	インターネット接続系PC10台およびLGWAN接続系PC10台のフォレンジック費用（1台100万円）	2000万円	2000万円	2000万円
④	M4	LGWAN系情報漏洩による損害賠償: N種の情報・1000件 ・1万円/件 インシデント対応費・ 2000万円 レビューテーション・1000万円	N=5 8000万円	N=4 7000万円	N=1 4000万円
⑤	M5	インターネット系情報漏洩による損害賠償・N種の情報・件数1000件 ・1万円/件 インシデント対応費 2000万円 レビューテーション 1000万円	N=2 5000万円	N=3 6000万円	N=6 9000万円
⑥	M6	インターネット系情報漏洩による損害賠償・N種の情報1種あたり1000万円 インシデント対応費・2000万円 レビューテーション 1000万円 LGWAN系侵入による災害対策費 2000万円	N=2 7000万円	N=3 8000万円	N=6 1億円
⑦	M7	インターネット系・LGWAN系情報漏洩による損害賠償・賠償額 7000万円 インシデント対応費・4000万円 レビューテーション 2000万円	1億3千円	1億3千円	1億3千円

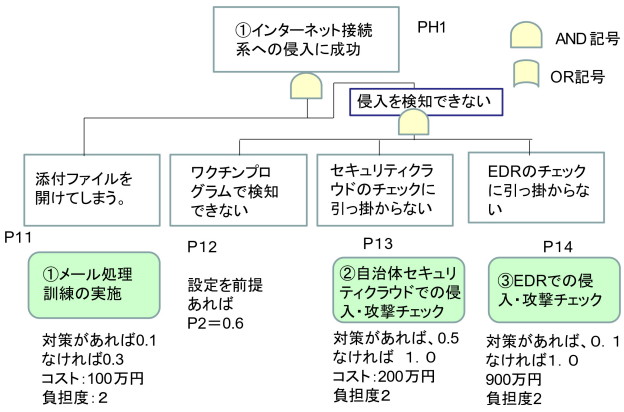


図 9 ディフェンスツリーの一例

Fig. 9 An example of a defense tree.

5.5 対策案のリストアップとパラメータの推定

ディフェンスツリーの下部に示される対策案の数は全体で 7 つであり，その対策コストや対策効果，作業負担度は**表 4** に示すように設定した．

ここでコストは 1 年ごとのものを採用しており，購入するものは，設備コストと運用コストの和とし，設備コストは購入額を 5（年）で割ったものを採用した．また，サービスを利用するものは，1 年ごとの費用を採用した．

作業負担度は，次のように分類し適用した．

表 4 対策案とパラメータ値の推定値
Table 4 Estimated countermeasures and parameter values.

対策案	名称	確率		コスト（円）	作業負担度レベル
		対策なし	対策あり		
①	メール処理訓練の実施	0.3	0.1	100万円	2
②	自治体セキュリティクラウド での侵入・攻撃チェック	1.0	0.5	200万円	2
③	EDRでの侵入・攻撃チェック	1.0	0.1	α:600万円 β′:900万円	2
④	メールの無害化 機能（添付ファイルの取り外し）	0.99	0.1	α:625万円 β′:250万円	α:4 β′:3
⑤	ファイルの無害化機能　DVI利用	0.99	0.1	4800万円	3
⑥	ファイルの無害化機能 仮想ブラウザー利用	0.99	0.3	600万円	3
⑦	LG-WANからの流出 チェック機能	0.3	0.1	500万円	2

$$\text{Min} \quad R\alpha\ (X_i \mid i=1,2,\text{---},n) \qquad \text{---(3)}$$

$$\text{subject to} \quad \sum_{i=1}^{n} C\alpha_i \cdot X_i \leqq Ct \qquad \text{---(4)}$$

$$\sum_{i=1}^{n} B\alpha_i \cdot X_i/n \leqq Bt \qquad \text{---(5)}$$

Rα(): 残存リスクを求める関数
Xi＝1　対策案iを採用
　＝0　対策案iを不採用
Cαi: αモデルで対策案iを実現するコスト（円）
Ct: 対策案に関する制約（円）

Bαi: 対策案iを導入するαモデルにおける負担度
Bt: 作業負担度の平均に関する制約

図 10 α モデルの定式化
Fig. 10 Formulation of α model.

レベル 5　負担が非常に大きい（1 回あたり 1 時間以上）
レベル 4　負担が大きい（1 回あたり 1 時間以内）
レベル 3　負担がかかる（1 回あたり 10 分以内）
レベル 2　負担はやや小さい（1 回あたり 5 分以内）
レベル 1　負担はほとんどない（1 回あたり 1 分以内）

対策効果は，機能がうまく発揮できる確率を推定して用いた．

5.6 目的関数や制約条件の設定と定式化

α モデル向けの対策案の最適組合せ用の定式化結果は**図 10** に示すとおりである．ここでは，制約条件として対策コストだけでなく，対策負担度も導入することによって 4.2 節で述べた問題①に対応している．なお，図 10 の式 (3) の左辺を n で割る定式化を採用したが割らない形で，Bt を調整する定式化も可能である．β′ モデルもパラメータの値は違うが同様にして定式化することが可能である．

両方合わせての最適解は，同じ制約条件下で対策案の最適な組合せを求め，トータルリスクが小さい方が全体の最適解となる．

これらの条件下で最適の対策案の組合せを求めるため，Python[*1]で約 100 ステップからなるプログラム PEEDC（Program for Extended EDC）を開発し，適用した．

[*1] Python は，Python Software Foundation の登録商標である．

表 5 最適化結果 1（α モデル）
Table 5 Optimization result 1 (α model).

	コスト制約	負担度制約	対策案 ①	②	③	④	⑤	⑥	⑦	トータルコスト（円）	トータルリスク（円）	トータルコスト+トータルリスク(円)
①	500万円	5.0	○	○						300万円	1億2598万円	1億2898万円
②	1000万円	5.0	○	○	○					900万円	639万円	1539万円
③	1250万円	5.0	○	○	○					900万円	639万円	1539万円
④	1500万円	5.0	○	○	○				○	1400万円	468万円	1868万円
⑤	2000万円	5.0	○	○	○			○	○	2000万円	466万円	2466万円
⑥	3000万円	5.0	○	○	○	○		○	○	2625万円	286万円	2911万円
⑦	4000万円	5.0	○	○	○	○		○	○	2625万円	286万円	2911万円

表 6 最適化結果 2（α モデル）
Table 6 Optimization result 2 (α model).

	コスト制約	負担度制約	対策案 ①	②	③	④	⑤	⑥	⑦	トータルコスト（円）	トータルリスク（円）	トータルコスト+トータルリスク(円)
①	2000万円	5.0	○	○	○			○	○	2000万円	466万円	2466万円
②	2000万円	2.5	○	○	○			○	○	2000万円	466万円	2466万円
③	2000万円	2.0	○	○	○			○	○	2000万円	466万円	2466万円
④	2000万円	1.5	○	○	○				○	1400万円	468万円	1868万円
⑤	2000万円	1.0	○	○	○					900万円	639万円	1539万円
⑥	2000万円	0.75	○		○					700万円	1416万円	2116万円
⑦	2000万円	0.5			○					600万円	4247万円	4847万円

表 7 最適化結果 3（β′ モデル）
Table 7 Optimization result 3 (β′ model).

	コスト制約	負担度制約	対策案 ①	②	③	④	⑤	⑥	⑦	トータルコスト（円）	トータルリスク（円）	トータルコスト+トータルリスク(円)
①	500万円	5.0	○	○						300万円	1億1437万円	1億2737万円
②	1000万円	5.0	○		○					1000万円	1073万円	2073万円
③	1250万円	5.0	○	○	○					1200万円	463万円	1663万円
④	1500万円	5.0	○	○	○	○				1450万円	458万円	1908万円
⑤	2000万円	5.0	○	○	○	○			○	1950万円	401万円	2351万円
⑦	3000万円	5.0	○	○	○	○		○	○	2550万円	281万円	2831万円
⑧	4000万円	5.0	○	○	○	○		○	○	2550万円	281万円	2831万円

5.7 対策案の最適な組合せの計算

α モデル，β′ モデルについて，コストに関する制約条件や，作業負担度に関する制約条件を種々に変えた場合の対策案の最適な組合せ結果は，**表 5**，**表 6**，**表 7**，**表 8** に示すとおりである．また，主要な部分を整理したものは**図 11**，**図 12** に示すとおりである．

これらの結果から次のようなことがいえる．

（1）表 5〜表 8 に示すように，種々の対策コストや作業負担度の制約のもとにトータルリスクを最小化する対策案の最適な組合せを知ることができる．

（2）また，同じ制約条件で α モデル，β′ モデルの最適解におけるトータルコストを比べることによりその小さい方を全体の最適解として求めることができる．たとえば，コスト制約が 2,000 万円で，作業負担度が 2.0 の場合の最適

表 8　最適化結果 4（β' モデル）
Table 8　Optimization result 4 (β' model).

	コスト制約	負担度制約	対策案 ①	②	③	④	⑤	⑥	⑦	トータルコスト（円）	トータルリスク（円）	トータルコスト+トータルリスク(円)
①	2000万円	5.0	○	○	○	○			○	1950万円	401万円	2351万円
②	2000万円	3.0	○	○	○	○			○	1950万円	401万円	2351万円
③	2000万円	2.0	○	○	○	○			○	1950万円	401万円	2351万円
④	2000万円	1.5	○	○	○				○	1700万円	405万円	2105万円
⑤	2000万円	1.0	○	○	○					1200万円	463万円	1663万円
⑥	2000万円	0.75	○		○					1000万円	1073万円	2073万円
⑦	2000万円	0.5			○					900万円	3219万円	4119万円

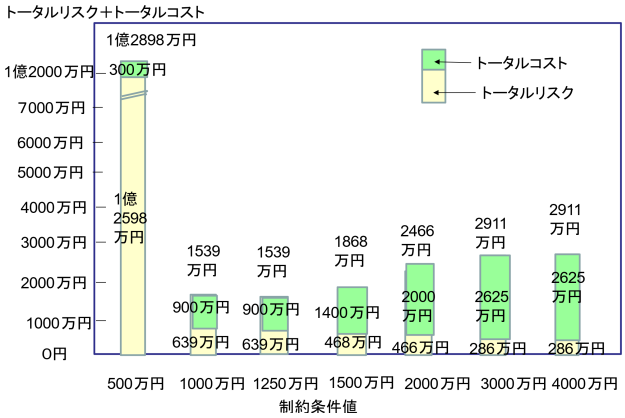


図 11　制約条件別最適値の比較（α モデル）
Fig. 11　Comparison of optimal values by constraint conditions (α model).

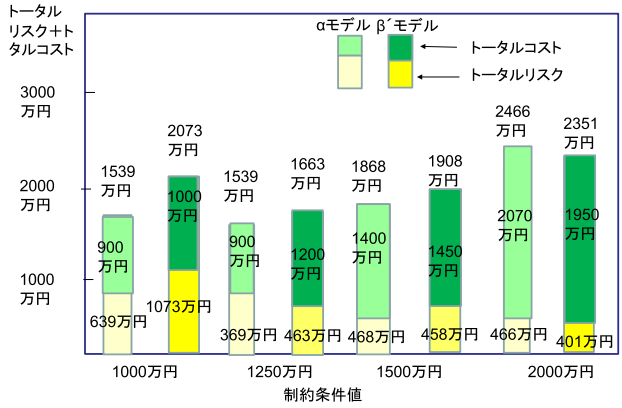


図 12　制約条件別最適値の比較（α モデルと β' モデル）
Fig. 12　Comparison of optimal values by constraint conditions (α model and β' model).

解は，α モデルでトータルリスクが 466 万円で，β' モデルが 401 万円で，トータルリスクが小さい β' モデルの方が全体の最適解になっていることが分かる．この場合の最適な対策案の組合せは，対策案①②③④⑦の組合せである．このようにすることによって，4.2 節で述べた問題③に対応できることが明らかになった．

（3）一方，トータルコスト＋トータルリスクという評価指標に着目すると，図 12 に示すように，トータルコスト＋トータルリスクが最小となるのは α モデルを対象とするものであり，1,000 万円以下をコスト制約とする場合である．その際の最適な対策案の組合せは対策案①②③の組合せであり，トータルコスト＋トータルリスクは 1,539 万円となる．このような分析をすることによって，どのぐらいのコストをかけて対策を実施すべきかの目安が得られる．

（4）表 5，表 7 に示すように，コスト制約の値が変わっても，対策案①のメール処理訓練や，対策案②の自治体セキュリティクラウドでの侵入・攻撃チェック，対策案③の EDR での侵入・攻撃チェックの優先度はいずれの場合も高い．

（5）表 6，表 8 に示すように，負担度制約が厳しくなるにつれて，対策案④のメールの無害化や，対策案⑤，⑥のファイルの無害化対策が排除される傾向にある．

5.8　リスクコミュニケーションによる関与者の合意個形成

分析者と意思決定関与者が集まり，評価指標や，対策効果の値，対策コストの値，さらには制約条件を変えながら解を求め，合意が形成されるまでこの過程を繰り返す．今回は，著者の 1 人の佐々木が分析を行い，千葉，甲斐，木下の 3 人が関与者となって，対策効果やコストの見直しを行い，最終的に合意が得られた解が，5.7 節で述べたものである．

6.　おわりに

地方自治体向けの情報システムのセキュリティに関する対策案の最適な組合せを求められるようにするため，先に開発した EDC 法を改良した拡張 EDC 法を開発し，支援プログラム PEEDC を開発した．これらを地方自治体の情報システムのモデルケースに適用し，採用すべき対策案の組合せについて 5.7 節で示したような種々の知見を得た．

これらの知見は，拡張 EDC 法とプログラム PEEDC を適用することにより得られたものであり，その有用性が確認できたと考えられる．また，EDC 法は要求に沿ったように容易に拡張でき，適用範囲が広いことも明らかになった．

今後，β モデルも含めたうえで，条件を変えていろいろなケースで解を求めていき，地方自治体で対策を決定するのに反映できるようにしていきたいと考えている．

参考文献

[1] 相原　遼，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標的型攻撃に対するリスク分析手法の提案と適用，情報処理学会論文誌，Vol.59, No.3, pp.1082–1094 (2018).
[2] Kavallieratos, G., Katsikas, S. and Gkioulos, V.: Cybersecurity and Safety Co-Engineering of Cyberphysical Systems – A Comprehensive Survey, *Future Internet*, Vol.12, No.4, pp.1–17 (2020).
[3] Ganin, A.A., Quach, P., Panwar, M., Collier, Z.A., Keisler, J.M., Marchese, D. and Linkov, I.: Multicriteria

Decision Framework for Cybersecurity Risk Assessment and Management, *Risk Analysis*, Vol.40, No.1, pp.183–199 (2020).
[4] 佐々木良一：メンテナビリティ・セーフティ・セキュリティを考慮したIoTシステム向けリスク評価手法の開発．情報処理学会論文誌，Vol.61, No.5, pp.1096–1103 (2020).
[5] Hayakawa, T., Sasaki, R., Hayashi, H., Takahashi, Y., Kaneko, T. and Okubo, T.: Proposal and application of Security/Safety Evaluation Method for Medical Device System that Includes IoT, *The 3rd International Conference on Network Security* (*ICNS2018*), Taipei, Taiwan (2018).
[6] IPA：情報セキュリティマネジメントとPDCAサイクルリスクアセスメント，入手先 ⟨https://www.ipa.go.jp/security/manager/protect/pdca/risk_ass.html⟩.
[7] 総務省地域力創造グループ：概要版「新たな自治体情報セキュリティ対策の抜本的強化に向けて」，平成27年11月24日，入手先 ⟨https://www.soumu.go.jp/main_content/000387560.pdf⟩.

佐々木 良一 （正会員）

1971年東京大学卒業．同年日立製作所入社．システム開発研究所でセキュリティ技術，ネットワーク管理システム等の研究開発に従事．2001年より2018年まで東京電機大学教授，現在，同大学顧問・客員教授，工学博士（東京大学）．2002年情報処理学会論文賞受賞．2007年および2017年に総務大臣表彰．2017年電子情報通信学会マイルストーン表彰等．著書に，『インターネットセキュリティ入門』岩波新書，1999年，『ITリスク学　情報セキュリティを超えて』共立出版，2013年，『デジタルフォレンジックの基礎と実践』東京電機大学出版，2017年等．日本セキュリティ・マネジメント学会会長，内閣官房サイバーセキュリティ補佐官等を歴任．

千葉 寛之 （正会員）

1988年北海道大学大学院情報工学専攻修了．同年日立製作所入社．オブジェクト指向によるソフトウェア開発のコンサルティングに従事したのち，1996年にインターネット決済を実現するセキュアプロトコルSET/SECEの開発・標準化に参画して以来，一貫してセキュリティ関連業務に従事．ISMS構築，セキュリティ設計，セキュリティ監査，CSIRT構築等のコンサルティングを担当．2011年10月より2年間，現内閣サイバーセキュリティセンター（NISC）に出向しセキュリティ技術戦略を担当．現在は，トラストを含むセキュリティ事業推進等に従事．日本セキュリティ・マネジメント学会副会長，同ITリスク学研究会幹事．

甲斐 賢 （正会員）

1998年京都大学大学院理学研究科修了．同年（株）日立製作所に入社．以来，システムセキュリティ，サイバーセキュリティの研究に従事．博士（情報学），慶應義塾大学SFC研究所上席所員，東京電機大学サイバーセキュリティ研究所研究員，CISSP．

木下 翔太朗

2016年3月京都大学大学院修了．同年4月日立コンサルティング入社．公共機関向けのコンサルティング部門で，サイバーセキュリティ関連の調査研究やセキュリティポリシの策定等の業務に従事．ISO/IEC JTC 1/SC 27/WG 4エキスパート．