Vol.2015-DPS-162 No.5
Vol.2015-CSEC-68 No.5
2015/3/5

インシデント情報を使用した最適なセキュリティ対策の選定

佐藤智裕[†1]　　田中英彦[†2]

今日，企業や行政機関などの多くの組織が情報システムを利用している．これらの情報システムには対策が施されているものの，多様化するリスクによりセキュリティ事故が発生している現状がある．その背景には，セキュリティ対策の選定が管理者の勘や経験で行われていることや，ベンダー任せであることが，結果的に最適な対策の選定に至っていないという状況が考えられる．
そこで，本論文はコンピュータセキュリティインシデントが組織や情報システムの特徴を反映して発生していることに着目し，それらのインシデント情報に実際の損害額を設定し，原因・対策まで展開することで，最適なセキュリティ対策の選定を可能にするモデルを確立した．通常，インシデント情報は機密事項として取り扱われることが多いが，本手法ではその点についても問題がないよう配慮している．
さらに，本手法を用いて実際の事故事例を検証し，利用について考察を述べる．

Optimum selection of security measure using computer security incident data

TOMOHIRO SATO[†1]　HIDEHIKO TANAKA[†2]

Nowadays many organizations such as companies and administrations use information system. Though measures are taken in these information system, a large number of security accidents are taking place by diversifying the risks. The reasons behind this include the fact that a security measures selection is now greatly dependent on the knowledge/experience of a system designer,and handing it over to a vendor.
Then the present study has established a model which can select the optimum security measures. According to setting an amount of damage in the incident information,thoroughly developed to the problem and its causes, by focusing on that computer security incident has occurred as a result of reflecting the features of organization and information system. Moreover this method takes the respect, an incident information is usually treated as a classified ones, into consideration.
Furthermore, I would like to verify actual security accidents having occurred by using my method, and describe consideration of its utilization.

1. はじめに

1.1 背景

現在，企業や行政機関などの多くの組織がコンピューターやサーバー，通信機器，モバイル端末，専用装置等，数多くの情報デバイスをネットワークで接続した，情報システムを使用しており，主な目的は，組織運営やサービス提供や社会基盤の整備，維持などである．

組織運営を目的としたものには，Ｅメールによる組織内外のコミュニケーションや，Web を使用した情報発信，情報収集，専用ソフトでの従業員管理，生産管理，業務管理などがあり，サービス提供や社会基盤の整備，維持などを目的としたものには，自治体による行政システムや，金融機関による金融システム,鉄道,航空などの運行システム，電気，ガス，水道などのインフラなど制御システムの他，医療やスマートシティ，軍事目的などがある．

このような状況おいて，情報システムのセキュリティ事故による組織への影響は，業務停止にとどまらない．事故対応の調査，復旧，対策費用，顧客対応などでの損害賠償など，多くの時間やコストがかかり，逸失売上の発生も加わることで企業収益にも大きく影響する．結果として，組織に対する信頼が失墜し，組織自体の存続が危ぶまれる事態の発生も考えられる．

もちろんこれらの組織では，進化する内外からのサイバー攻撃やセキュリティ事故，近年のモバイル化やクラウド化,仮想化などの事業環境の変化,雇用の多様化等により，日々増している情報セキュリティリスクに備えるために，多くの分野にまたがった情報セキュリティ対策を実施している．

しかし，情報システムは，組織ごとに個別に設計されており，それぞれに特徴がある．これらの情報システムごとの特徴を個別に把握し，それぞれに最適な情報セキュリティを選定できればよいが，それは極めて困難である．その結果，セキュリティ対策を実施するベンダーに言われるがままの対策を導入したり，コストのみにとらわれてセキュリティ対策を選定することで，各組織の情報システムに最適な情報セキュリティ対策が選定されていないことが多い．

このような問題に対し，組織に特有な情報を使用することで，組織の情報システムに最適な情報セキュリティ対策を選定する方法について本論文で提案する．

†1 情報セキュリティ大学院大学、NEC フィールディング株式会社
INSTITUTE of INFORMATION SECURITY , NEC Fielding,Ltd.
†2 情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

Vol.2015-DPS-162 No.5
Vol.2015-CSEC-68 No.5
2015/3/5

1.2 目的

本研究の目的は，組織によって異なる情報システムにおいて，組織に特有な情報を使用することで，それぞれの情報システムに最適なセキュリティ対策を選定することが出来るようにすることである．

本研究では，組織に特有な情報として，その組織で過去に発生したコンピュータセキュリティインシデントの情報（以下,「インシデント」という）を使用することを特徴としている．

ただし，通常，組織で発生したインシデント情報は組織内で秘密事項として取り扱うことが多く，このインシデント情報をセキュリティ対策の選定に使用する本提案では，インシデント情報を外部のセキュリティ対策を実施するベンダーに公開する必要がないように考慮した．

これにより，組織に特有かつ機密情報であるインシデント情報を，外部へ提供することなくセキュリティ対策の選定に使用し，組織の情報システムに最適なセキュリティ対策を選定することが出来るようになる．

2. 情報システムとセキュリティ対策

2.1 情報システムとは

「情報システム」という言葉の定義については，情報システム学会[1]でも述べられているように多くの見解があるが，本論文では「コンピューターやサーバー，通信機器，モバイル端末，専用装置等，数多くの情報デバイスをネットワークで接続し，それらを使用して組織の運営や意思決定に必要な情報の収集や蓄積，編集，解析などを行うシステム」を言う．

2.2 セキュリティ対策の現状

情報システムでは，多くの情報資産を取り扱っており，これらはセキュリティ上の脅威から守る必要がある．

経済産業省の調査[2]によると，これらの情報システムにおける情報セキュリティ対策の実施率（いずれかの情報セキュリティ対策で「既に実施している」と回答した企業数の割合）は 86.4%であり，今日，多くの企業で何かしらの情報セキュリティ対策が実施されている．

しかし，これだけ多くの企業が情報セキュリティ対策を実施しているにもかかわらず，1 年間で 24.4%の企業が情報セキュリティトラブルを起こしている．

2.3 セキュリティ対策の問題点

組織では，進化する内外からのサイバー攻撃やセキュリティ事故，近年のモバイル化やクラウド化，仮想化などの事業環境の変化，雇用の多様化等により，日々増している情報セキュリティリスクに備えるために，多くの分野にまたがった，情報セキュリティ対策を実施している．

本来，情報セキュリティ対策の導入分野や製品の選定の際に，組織で起こりうるセキュリティ事故や，組織の情報システムに適した情報セキュリティ対策を選定するべきであるが，これまでは,「この情報セキュリティ対策をセキュリティベンダーに勧められた」「同業他社と同じ対策を実施したい，すればよい」「この情報セキュリティ対策のスキルしかない」「情報セキュリティ対策製品を 1 つのベンダーで統一したい」「十分な予算がない」などの理由から，実際には組織に最適な情報セキュリティ対策が選定されていないという問題が発生していた．

2.4 セキュリティ対策の選定方法に関する先行研究

中村ら[3]の研究では，資産 A，脅威 T，対策 CM を『資産と脅威の関係』と『脅威と対策の関係』でモデル化した．

『資産と脅威の関係』では，資産の資産価値を V とし，脅威の発生確率を P とし，その脅威が発生した時のそれぞれの資産への影響を E としたマトリックス表を作成する．これにより，一つの資産への影響は脅威ごとに存在し，1 つの脅威は複数の資産への影響があることが分かる．なお，脅威が資産へ影響を与えない場合，影響 E は 0 となる．

次に,『脅威と対策の関係』では，対策のコストを C とし，その対策により，低下する脅威の発生確率を効果 R (0 ≦R≦1)とする．これにより，一つの対策の効果が脅威ごとに異なることが分かる．

ここで，各対策の実施の有無を S とし，対策を実施した場合は S が 1 となり，対策を実施しなかった場合は，S が 0 となる．

	資産A_1 価値V_1	資産A_2 価値V_2	…
脅威T_1 確率P_1	影響 E_{11}	影響 E_{12}	…
脅威T_2 確率P_2	影響 E_{21}	影響 E_{22}	…
・ ・	・ ・	・ ・	・ ・

表 1　資産と脅威の関係

	対策CM_1 コストC_1	対策CM_2 コストC_2	…
脅威T_1 確率P_1	効果 R_{11}	効果 R_{12}	…
脅威T_2 確率P_2	効果 R_{21}	効果 R_{22}	…
・ ・	・ ・	・ ・	・ ・

表 2　脅威と対策の関係

その結果，以下の式より全対策の実施の有無を計算し，残存している総資産から対策コストを減じた値を最大にする対策の組み合せが最適だとしている．

$$\sum_k \left\{ V_k \prod_j \left[1 - E_{jk} P_j \prod_i \left(1 - R_{ji} S_i \right) \right] \right\} - \sum_i C_i S_i$$

ただし，上記の手法では脅威の発生確率など，実際の環境で実現するには，導出困難な数値が多いことが課題の 1 つである．

3. コンピュータセキュリティインシデント

3.1 コンピュータセキュリティインシデントとは

JPCERT/CC では，コンピュータセキュリティインシデン

Vol.2015-DPS-162 No.5
Vol.2015-CSEC-68 No.5
2015/3/5

トを「情報システムの運用におけるセキュリティ上の問題として捉えられる事象」[4]としている．
JPCERT/CC が四半期ごとに発行している「インシデント報告対応レポート」[5]によると，2011 年から 2014 年のインシデント調整件数は，以下のグラフに示す通り，増加傾向にあることがわかる．

図 1　インシデント調整件数の推移（2011 年～2014 年）

3.2 CSIRT の現状

組織ではこのようなインシデントに対応（検知，分析，把握，解決，再発防止，情報蓄積等の実施）するためのチームが必要であるが，従来は情報システム部門や総務部門，法律の知識が必要な場合は法務部門などが，その都度適任者を集めて対応していたのに対し，現在ではインシデント対応を実施する専門部隊を常設し，事前に策定した手順に沿って一元的に対応する組織が増えてきている．

このような，組織内で起こるインシデントへの対応を専門的に実施するチームを「CSIRT（Computer Security Incident Response Team）」といい，現在では企業のみならず各府省庁などの組織にも設置されている．

日本シーサート協議会の加盟チーム数は年々増加しており，2015 年 2 月 6 日現在 71 チームが加盟している[6]．また，世界的な組織である FIRST(Forum of Incident Response and Security Teams)では，日本の 23 チームを含む 316 チームが加盟している[7]．

これは，近年の増加するインシデントへの対応や，インシデントの発生が組織へ与える影響の大きさが認識されている結果である．

3.3 インシデント情報の取り扱い

一般的にインシデントの情報は「組織や情報システムの機密情報が含まれるものが多い」というセキュリティ上の課題や，「発生したインシデントにより組織への信頼や評価に悪影響を及ぼす」などの理由から，組織内で発生したインシデントを公表，報告することや，情報提供すること対して消極的な姿勢をとる組織が多い．

情報セキュリティトラブルの情報処理推進機構への届出状況をみても，「全て届け出ている」と回答した企業の割合は 13.1%，また，「一部届け出ている」と回答した企業の割合は 25.4%であり，両者を合わせても 38.5%と低い数値であることがわかる[2]．

3.4 インシデントの特性

組織に蓄積されているインシデント情報は，組織それぞれに特色がある．

そこで，2011 年から 2013 年を対象に日本ネットワークセキュリティ協会が実施した調査[8][9][10]を使用して，組織におけるインシデント情報の特性を検証した．

調査では，各年の業種別のインシデント公表件数やインシデントの原因比率を公表している．その中でも，検証で使用した業種は，「公務(他に分類されるものを除く)」「金融業，保険業」「教育，学習支援業」「情報通信業」「医療，福祉」の５つである．その理由として，これらの５つの業種は 2011 年から 2013 年までの業種ごとのインシデント公表件数で，いずれの年においても上位５業種となっており発生件数も全ての年で 50 件を超えており，まとまった件数のインシデントが確保できたからである．

	2013 年	2012 年	2011 年
公務	587（1 位）	486（2 位）	516（1 位）
金融業，保険業	294（2 位）	1,094（1 位）	332（2 位）
教育，学習支援業	158（3 位）	302（3 位）	216（3 位）
医療，福祉	76（4 位）	106（4 位）	109（4 位）
情報通信業	75（5 位）	83（5 位）	95（5 位）

表 3　業種別インシデント公表件数（上位 5 業種）

ここで，組織によってインシデントに特徴があるかを確認するため，今回の調査対象となった個人情報漏えいインシデントの原因について，業種別の特徴を確認してみた．

企業や自治体等の単一の組織におけるインシデントの特徴ではなく，1 業種を 1 組織と見立てインシデントの特徴を確認した理由として，公表されている情報が 1 年単位のもので，ある単一の組織におけるインシデントの特徴を確認してもまとまった件数を得ることが出来ないためである．

まず，初めの検証として，単年における業種ごとに発生した個人情報漏えいインシデントの原因割合を確認する．

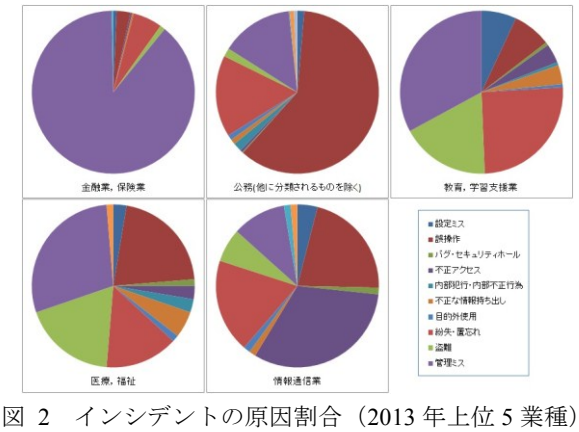

図 2　インシデントの原因割合（2013 年上位 5 業種）

上記の結果，各業種では同じ個人情報漏えいというインシデントでありながら，その原因割合が大きく異なることが確認できた．これは，2011 年から 2013 年までのすべての調査で同様であった．

次に，各業種において各年の原因割合を同様に調査した．その中でも下記の3業種に注目する．

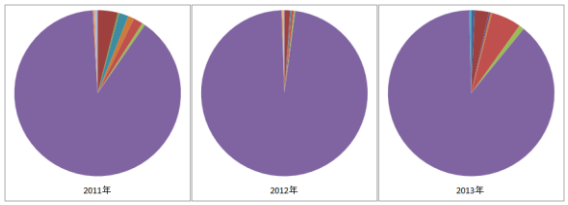

図 3　金融業，保険業におけるインシデントの原因割合

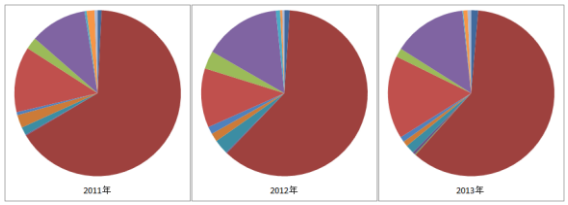

図 4　公務におけるインシデントの原因割合

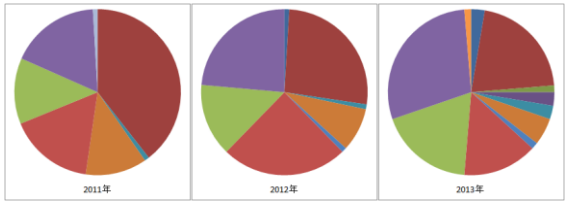

図 5　医療，福祉におけるインシデントの原因割合

上記の結果，同じ業種の場合，各年のインシデントの原因割合が類似していることが分かった．
この２つの結果から，個人情報漏えいという単一のインシデントの原因を調査しただけでも，業種ごとに違いがあり，同じ業種では同様のインシデントが発生しているという特徴が分かった．

4. インシデント情報を使用した最適なセキュリティ対策の選定について

4.1 提案手法概要

本提案手法では，組織がセキュリティ対策を選定する際に，その組織や組織の情報システムに特有な情報である「組織で発生したインシデント情報」を使用して，組織に最適なセキュリティ対策を選定する．

組織で発生するインシデントは，組織の社会的立場や業務内容，組織の情報システムなどの特徴に左右されるものであるため，組織のセキュリティ対策の選定にその組織のインシデント情報を使用することは，組織にとって最適なセキュリティ対策の選定が実施できることになる．

ただし，通常，セキュリティ対策製品やサービスを選定するのは外部のセキュリティベンダーであるが，組織のインシデント情報は外部に提供することは困難であるため，外部組織へインシデント情報を提供することなくこれを実現する．

また，本提案手法では複数存在するセキュリティ対策から最適な組み合わせを導出するプロセスとして，インシデント対応時にかかった費用（損失額）と組織の予算，対策費用の導出可能な数値を用いることとしている．

提案手法を実現する方法としては，全体の作業を３つに分けて実施する．

まず第 1 段階で，各組織は自組織で発生したインシデント情報を記録，蓄積し，そのインシデント情報を基に，インシデントの分類，インシデント毎の損失額の算出，原因の分析を実施し，その原因に対するセキュリティ対策項目を導き出す．このとき，インシデント毎の損失額を各セキュリティ対策項目まで展開する．

次に，第 2 段階では第 1 段階で導き出した組織に必要なセキュリティ対策項目に対してセキュリティ対策技術である製品やサービスを紐づける

最後に，第 3 段階では第 2 段階で導き出したセキュリティ対策技術の組み合わせから最適なものを選定する．

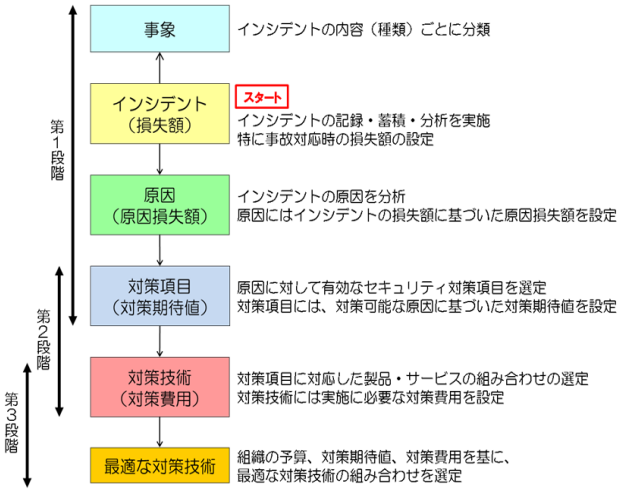

図 6　提案手法の展開イメージ

4.2 組織で発生したインシデントの記録

組織でインシデントが発生した場合は，インシデントごとに詳細な情報を記録する必要がある．通常，インシデントの対応記録には，組織内の事故受付表や報告書，チェックシートなどに基づいて記録が残される．これらに記録すべき事項としては，セキュリティベンダーやセキュリティ専門機関などが発行しているインシデント発生時の対応ガイドを参考 にすることが多く，たとえば，NIST(National Institute of Standard and Technology)の「Computer Security Incident Handling Guide(SP800-61)」 [11] や NTT-CERT Security Tips[12]，情報セキュリティ大学院大学の「情報セキュリティ事故対応ガイドブック」[13]などで，記録の重要性や記録するべき事項などが述べられている．

なお，本提案手法では，通常のインシデント対応時に記録される情報を使用する．そのため，本提案手法のために特別に記録するべき情報はなく，本提案手法の実現のため

の特別な負担が発生することはない．提案手法の実施に必要な記録は以下のとおりである．

- 事故内容
- 発生日時
- 対象資産
- インシデントの種類
- 原因
- インシデント対応時にかかった費用（損失額）

インシデントの発生日時を明確にすることで，情報セキュリティ対策選定の際に，どの期間のインシデント情報を対象として使用するかを絞ることが可能である．

また，対象資産やインシデントの種類が明確になっていれば，対象資産ごとやインシデントの種類ごとの情報セキュリティ対策の選定をすることも可能となる．

原因に関しては，インシデント発生の引き金となった原因を記録する．複数の原因が重なってインシデントが発生した場合は複数の原因を記録する．

損失額は，インシデント対応のために使用した費用を算出し記録する．なお，この損失額にはインシデントに対する今後の対策費用（対策製品の導入や再発防止のための教育費用など）は含まず，インシデントの検知からそのインシデントの収束までに使用した費用を記録する．主な費用は対応時の人件費になるが，そのインシデントの対応に必要となった特有の機材や調査費，外部への委託費，見舞金や裁判費用，相談窓口用の電話回線の契約などの通信費，謝罪広告の費用など発生したものはすべて含める．

4.3 インシデントの分析

記録したインシデントの種類の分類と原因の分析を行い，インシデントの損失額をもとに原因損失額を設定する．

インシデントは内容ごとにインシデントの種類で分類する．インシデントの種類はあくまでも発生したインシデントの最終的な状況（結果）である．例えば，Web サーバに不正アクセスがあった場合でも，Web サーバが停止した場合はサービス停止となり，Web ページが改ざんされた場合は情報改ざんとなる．

次にインシデントの原因を分析し，インシデントの損失額から原因損失額を割り当てる．インシデントの損失額はインシデント発生時の対応費用であったが，対象の原因がなければインシデントも発生しなかったため，インシデントの原因に対して損失額を割り当て，これを原因損失額という．この時，１つのインシデントに対して原因が複数存在する場合は，原因の数でインシデントの損失額を均等割りし，それぞれの原因に原因損失額として割り当てる．

インシデントの種類	事故内容	損失額	原因	原因損失額
種類 A	事故内容 1	a	不正アクセス	a/2
			設定ミス	a/2
	事故内容 2	b	物品管理ミス	b
	事故内容 3	c	ウイルス感染	c
種類 B	事故内容 4	d	設定ミス	d
種類 C	事故内容 5	e	ウイルス感染	e
種類 D	事故内容 6	f	DoS 攻撃	f

表 4　インシデントと原因損失額の設定例

その後，同じ原因に対してはセキュリティ対策項目が同一となるため，原因損失額を合算する．これにより，それぞれの原因に対して最終的な原因損失額が設定される．

原因	最終的な原因損失額
不正アクセス	a/2
設定ミス	a/2+d
物品管理ミス	b
ウイルス感染	c+e
DoS 攻撃	f

表 5　最終的な原因損失額の設定例

これによって，対象の原因を対策した場合，その原因に設定されている原因損失額に相当する損失を減少させることが出来ることとする

4.4 セキュリティ対策項目への紐づけ

原因損失額が設定された原因に対し，セキュリティ対策項目の紐付けを実施する．この際，原因に対し，対象の対策項目を実施すれば，原因を取り除くことが出来るものをセキュリティ対策項目として設定する．原因に対して有効な対策項目が複数あってもよいが，いづれか１つでも対策項目を実施した場合，紐付いている原因がなくならなければならない．もし，複数の対策項目を同時に実施しないと，対象の原因がなくならない場合は，原因を分割し，１つでも対策項目を実施すれば原因をなくすことが出来るように原因を細分化する

これにより，各セキュリティ対策項目にはそのセキュリティ対策項目によって取り除くことができる原因に設定されている原因損失額が対策期待値として反映される．

4.5 セキュリティ対策技術（製品・サービス）の選定

セキュリティ対策項目を実現できる製品・サービスであるセキュリティ対策技術を選定する．１つのセキュリティ対策技術では，１つまたは複数のセキュリティ対策項目を実施できる．これは，通常，製品やサービスは単一のセキュリティ対策項目に対応するものもあれば，複数のセキュリティ対策項目に対応しているものもあるためである．

セキュリティ対策技術	セキュリティ対策項目		
	ウイルス対策	不正アクセス対策	DoS 攻撃対策
ウイルス対策製品 A	○	×	×
ウイルス対策製品 B	○	○	×
GW 対策製品 A	×	○	○
GW 対策製品 B	○	○	×

○…対応可能　×…対応不可能

表 6　セキュリティ対策項目と対策技術の対応例

また，あるセキュリティ対策項目に対応するするセキュリティ対策技術が複数ある場合は，すべてリストアップする．ただし，複数のセキュリティ対策技術で同一のセキュリティ対策項目に対応している場合はもっとも安価なセキュリティ対策技術を選定する．

セキュリティ対策技術を選定する際は，セキュリティ対策技術である製品・サービスを導入，使用するための費用（対策費用という）も算出しておく．

4.6 最適なセキュリティ対策技術（製品・サービス）の選定

最後に，ここまででリストアップされたセキュリティ対策技術から最適な組み合わせの選定を行う．

セキュリティ対策技術の組み合わせパターンが複数存在する場合は，その中から組織に最適なセキュリティ対策技術の組み合わせを選定する必要がある．

ここで，最適なセキュリティ対策技術の組み合わせを選定する際に以下の３つの数値を使用する．

- 組織の予算
- セキュリティ対策技術の対策費用
- セキュリティ対策項目の対策期待値

はじめに，組織のセキュリティ対策の実施には費用が必要であるが，これは無限に使用できるものではない，組織には使用可能な予算が決められているため，本提案では，組織の予算内で最適なセキュリティ対策を実施することとする．

どのセキュリティ対策技術の組み合わせパターンが最適かを導き出す条件として，以下の条件を順番に適用する．

1) セキュリティ対策技術を組み合わせた場合の対策費用が組織の予算内に収まること
2) その場合に対策可能な対策項目における対策期待値の和が最大になること
3) 対策期待値の和が同一のパターンが複数存在する場合は，対策費用の和が最小になるもの

上記の条件をもとに選出された組み合わせを最適とする．

これにより，組織のインシデントで発生した損失額を予算内で最大限減少させることが出来，組織にとって最適なセキュリティ対策が選定されていると言える．

なお，対策技術によって対応可能な複数の対策項目が同一の原因に属する場合，対策期待値は重複して加算しない．

5. ケーススタディ

5.1 ケーススタディに使用したインシデントデータ

ケーススタディに使用したインシデントデータは，JNSA の調査結果[9]の中から，昨今の状況を踏まえ個人情報漏えいインシデントで注目されている「教育，学習支援業」とした．また，組織の抽出として単一の組織を抽出してもまとまった件数が確保できないため，組織の構成や社会的立場，活動内容が近い「大学」で発生したインシデントを抽出し，それを一組織で発生したと想定して提案手法を実施することとした．

- 対象とするインシデントデータ：58 件

5.2 ケーススタディの実施

まず，組織で発生したインシデントの情報を記録する．JNSA の調査結果には，組織名（大学名）やインシデントの詳細は記載されていない．そこで，情報を詳しく記録するために JNSA より詳細データを提供して頂くとともに，ケーススタディの対象となっているインシデントについて，公開されている以下の項目を確認した．

- 発生日時
- 対象資産（すべて個人情報である）
- インシデントの種類（すべて情報漏えいである）
- 原因（本論文用にインシデントを調査し，JNSA の原因より詳細に分析）
- 損失額（ケーススタディでは JNSA の損害賠償額を使用）

次に，インシデントの種類の分類と原因の分析および原因損失額の設定を実施する．JNSA の調査は個人情報漏えいインシデントに関して行われているため，インシデントの種類はすべて情報漏えいである．次にインシデントの原因分析を，JNSA およびケーススタディの対象とした組織から公開されている資料を基に実施した．

項番	発生日時	原因区分（JNSAによる）	インシデントの概要	原因1	原因2	損失額	原因損失額
1	2012/4/21	不正な情報持ち出し	・学生の情報を保存したUSBメモリの紛失 ・無断で持ち出していた	USB紛失	情報の無断持ち出し（USB）	120.45	60.23
2	2012/10/10	不正アクセス	・第三者からの不正アクセスがあり学生情報が流出	不正アクセス		534.60	534.60

表 7　ケーススタディの対象データ（一部）

この結果，原因ごとにインシデントの損害額が原因損失額として展開され，以下のようになる．この段階で，既にどの原因を対策することが組織にとって重要であるかがわかる．

原因	原因損失額
USB 紛失	1,461.53
PC 紛失	3,962.85
バックの盗難	3,802.43
車からの盗難	2,264.25
研究室からの盗難	24.90
メール誤送信	248.70
FAX 誤送信	30.90
手紙誤送付	111.15
情報の無断持ち出し(USB)	2,671.20
情報の無断持ち出し(紙)	164.18
不正アクセス	107,056.15
バグ・セキュリティホール	356.05
サーバの設定ミス	4,528.50
紙媒体の管理ミス	717.98
リテラシーの欠如	1.65
外部委託管理の不備	5.70
バック紛失	1.80

表 8　原因と設定した原因損失額一覧

なお，今回は損失額が不明なインシデントについては取り扱わないものとする．これは，JNSA の調査において，漏えい人数や漏えい内容が不明で損害賠償額が計算できなかったものである．しかし，実際の組織では損失額に実績値を使用するため，このようなことはない．

ここまでで導き出した原因に対して，対策項目を紐づける．各対策項目には前項で導き出した原因損失額が対策期待値として反映される．

原因	対策項目1	対策項目2	対策項目3
USB紛失	USB紛失防止	USB暗号化	
PC紛失	PC紛失防止	PC暗号化	シンクライアント
バックの盗難	鞄用盗難防止		
車からの盗難	車用警報装置		
研究室からの盗難	入退室管理	防犯カメラ	
メール誤送信	メール誤送信防止		
FAX誤送信	FAX誤送信防止	FAXペーパーレス化	
手紙誤送付	手紙誤送信防止	手紙ペーパーレス化	
情報の無断持ち出し（USB）	情報持ち出し制御	アクセス管理	
情報の無断持ち出し（紙）	印刷制御		
不正アクセス	不正アクセス対策		
バグ・セキュリティホール	脆弱性管理対策		
サーバの設定ミス	設定に対する監査		
紙媒体の管理ミス	紙媒体管理		
リテラシーの欠如	教育		
外部委託管理の不備	外部委託規程構築		
バック紛失	バック紛失防止		

表 9　原因に対するセキュリティ対策項目

次に，セキュリティ対策項目を実現できる製品・サービスであるセキュリティ対策技術を選定していく．対策技術には対策費用を設定する．通常，これは製品やサービスを導入，運用するための価格である．

なお，ケーススタディでは実際の製品・サービスをもとに，架空のセキュリティ対策技術およびその費用を当てはめる．ここで，対策期待値および対策費用の単位は円などの通貨である．ただし，いずれも単位が同一であれば，数値を比較するだけなので単位自体はそんなに重要ではない．

そのため，ケーススタディでは特に単位を定めない．

対策項目	対策期待値	対策技術（対策費用）																
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
		500	400	600	300	200	150	250	200	100	80	200	150	1,200	100	300	400	150	100
USB紛失防止	1,461.53	○																	
USB暗号化			○																
PC紛失防止	3,962.85	○																	
PC暗号化			○																
シンクライアント				○															
鞄用盗難防止	3,802.43	○																	
車用警報装置	2,264.25					○													
入退室管理	24.90						○	○											
防犯カメラ								○											
メール誤送信防止	248.70								○										
FAX誤送信防止	30.90									○	○								
FAXペーパーレス化										○									
手紙誤送信防止	111.15											○							
手紙ペーパーレス化										○									
情報持ち出し制御	2,671.20				○								○						
アクセス管理				○									○						
印刷制御	164.18			○	○						○								
不正アクセス対策	107,056.15													○					
脆弱性管理対策	356.05				○										○		○		
設定に対する監査	4,529.50															○	○		
紙媒体管理	717.98									○	○								
教育	1.65																	○	
外部委託規程構築	5.70																		○
バック紛失防止	1.80	○																	
架空の製品・サービス		物理対策（ワイヤー等）	暗号化ソフト・ツール	シンクライアント環境の構築	資産管理ソフト	車用警報装置	入退室管理システム（カード）	入退室管理システム（顔認証）	メール誤送信防止システム	紙媒体電子化システム	複合機	手紙自動送付システム	ファイルアクセス制御	IPS・IDS等GW製品	脆弱性・パッチ管理システム	監査サービス	侵入テスト	教育	コンサルティング

表 10　セキュリティ対策項目と対策技術のマトリックス

最後に，組織の予算，対策可能な項目の対策期待値，選定する対策の費用を基に最適なセキュリティ対策の選定を実施する．

本ケーススタディにおける組織の予算を 1,000 とした場合，予算内で最大の対策期待値を導き出すのは以下の場合となる．

S1,S12,S15=1 500+150+300=950（対策技術 1,12,15 を実施）

この場合，対象となる対策項目は以下である．

- USB 紛失防止
- PC 紛失防止
- 鞄用盗難防止
- 情報持ち出し制御
- アクセス管理
- 設定に対する監査
- バック紛失防止

上記の対策期待値の合計は 16428.3 と予算内での組み合わせで最大となるため，組織にとって最適なセキュリティ対策の選定が実施できたといえる．

6. 実際の組織での利用における考察

6.1 実施段階における提案手法の利用者について

提案手法は手順を３つに分けて実施している．それぞれの手順をどの組織が実施するかによって，それぞれでメリットやデメリットなどの違いや特徴がある．以下は各段階で想定する利用者とその理由である．

	想定する利用者	理由
第１段階	（セキュリティ対策を実施する） **組織**	・組織の機密情報であるインシデント情報を取り扱うため ・特別な専門知識が必要ないため
第２段階	**セキュリティ専門家** （外部のセキュリティベンダーなど）	・セキュリティ対策項目に対し製品やサービスを紐づける際に，情報セキュリティに関するトレンドや製品・サービスに関する知識が必要であるため
第３段階	（セキュリティ対策を実施する） **組織**	・最適なセキュリティ対策技術の組み合わせ選定の判断材料として組織の予算情報を使用するため ・特別な専門知識が必要ないため

表 11　各段階で想定する利用者

6.2 組織の意見や情報セキュリティのトレンドの反映

提案手法では，最終的に最適なセキュリティ対策技術の組み合わせを選定する際に，組織の予算，対策期待値，対策費用のみを判断材料として使用するため，セキュリティ対策を実施する組織の意見や情報セキュリティのトレンドが反映されないことがある．

組織の意見の取り込みについては，組織が特定のセキュリティ対策項目に重点を置きたい場合はその対策項目を必須にすることや対策期待値を高く設定することで対応可能である．

また，組織が特定のセキュリティ対策技術を選定したい場合は，セキュリティ対策技術のリストアップの際に選定対象とし，最適な組み合わせ選定の際に対象の対策技術の選定を必須に設定することで対応可能である．

また，インシデントには攻撃手法や攻撃対象などその時々の情報セキュリティのトレンドが反映されるものであ

るが，提案手法では組織で過去に起こったインシデントのみを取り扱うため，最新のインシデントや流行しているインシデントでもそれらが組織で発生していない限り提案手法に取り込めない．

このような場合は，組織で起こる可能性があるインシデントを発生したとみなして，みなしインシデントとして提案手法に取り込んで実施することで，セキュリティ対策の選定材料に反映させることが可能である．

ただし，この場合は，インシデントの損失額が不明であるため，他組織との CSIRT 連携での情報収集や同様のインシデントを基に損失額の値を導き出す必要がある．また，この場合も，自組織と同様の他組織などの情報を基にすることで，インシデントの特徴を有効的に利用することが出来る．

6.3 利用シーンによる特徴

組織のセキュリティ対策の選定に提案手法を使用するシーンについては以下の３点を想定している．

(1) **組織のセキュリティ対策を刷新する場合**

組織の情報システムに対するセキュリティ対策の刷新（システムのリプレース等）を実施するタイミングで，提案手法を使用して過去のインシデント情報を基に最適な対策の選定を実施する

(2) **組織のセキュリティ対策の一部を変更する場合**

既存の対策技術の利用を前提に提案手法を使用する

(3) **既存のセキュリティ対策の最適性を確認する場合**

今後起こりうるインシデントをみなしインシデントとして提案手法に取り込み，既存の対策技術の利用を前提に提案手法を使用する

7. まとめ

7.1 研究の成果

(1) **組織のインシデント情報を使用したセキュリティ対策の選定**

組織で発生するインシデントは，組織に特有であるため，組織の情報セキュリティ対策の選定材料に使用することは有効である．

(2) **導出可能な数値を使用した最適な組み合わせの選定**

これまでのようなセキュリティ事故の発生頻度や攻撃の成功率など導出が困難な数値とは異なり，実績値である損失額（インシデント対応にかかった費用）をインシデント情報に設定し，最適なセキュリティ対策の選定材料として使用した．

(3) **機密情報であるインシデント情報の取り扱いに考慮**

提案手法を３段階に分け，利用者を明確にすることで，機密情報であるインシデント情報の取り扱いを考慮した手法を実現した．

7.2 今後の課題

(1) **みなしインシデントの損失額の精度**

組織で発生する可能性があるインシデントをみなしインシデントとして含める場合，設定する損失額の精度が高くなければ提案手法自体の精度が下がる．

(2) **インシデント情報の確保が困難な組織への対応**

本提案手法ではインシデント情報を使用するが，中小企業などの組織においてはまとまった数のインシデント情報が存在せず，本提案手法の利用が困難である．そのため，業種・業界内や組織間でのインシデント情報の共有による対応が必要となる場合がある．

(3) **時間経過によるインシデントの変化に対する対応**

本提案手法では，過去のインシデント情報を利用するが，その中には今後発生しないインシデントも含まれる可能性がある．また，未知のインシデントをいかにみなしインシデントとして新たに取り込むことが出来るかなど，組織によってはインシデントの選択が必要となる．

(4) **実際の組織による検証**

提案手法を実際の環境で実施し検証を重ねる必要がある．

謝辞　本研究のためにデータを提供していただいた JNSA の関係者の皆様に，謹んで感謝の意を表します．

参考文献

1) 情報システムの定義 > 情報システム – 情報システム学会 ISSJ， http://www.issj.net/is/02/index.html,(2015/2/6).
2) 経済産業省：平成 25 年度我が国情報経済社会における基盤整備（情報処理実態調査の分析及び調査設計等事業）調査報告書, (2014).
3) 中村 逸一，兵藤 敏之，曽我 正和，水野 忠則，西垣 正勝：セキュリティ対策選定の実用的な一手法の提案とその評価，情報処理学会論文誌，Vol.45,No.8,pp. 2022-2033,(2004).
4) JPCERT コーディネーションセンター インシデント対応とは？，https://www.jpcert.or.jp/ir/,(2015/2/6).
5) JPCERT コーディネーションセンター インシデント報告対応四半期レポート，http://www.jpcert.or.jp/ir/report.html,(2015/1/14).
6) 会員一覧｜CSIRT - 日本シーサート協議会, http://www.nca.gr.jp/member/,(2015/2/6).
7) FIRST.org / FIRST Members, https://www.first.org/members, (2015/2/6).
8) 日本ネットワークセキュリティ協会 : 2011 年情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～，(2012).
9) 日本ネットワークセキュリティ協会 : 2012 年情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～，(2014).
10) 日本ネットワークセキュリティ協会 : 2013 年情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～, (2014).
11) NIST:Computer Security Incident Handling Guide(SP800-61), (2012).
12) 日本電信電話株式会社：NTT 技術ジャーナル“NTT-CERT Security Tips―第 6 回 インシデントへの対応”，Vol.18,No.4,(2006).
13) 情報セキュリティ大学院大学：情報セキュリティ事故対応ガイドブック，(2011).