ISMS 導入のための情報セキュリティインシデントコスト定量化について

For quantification information security incident cost in the introduction of ISMS

永井好和† 市川哲彦† 長谷川孝博※ 小河原加久治‡ 多田村克己‡

Yoshikazu NAGAI† Yoshihiko ICHIKAWA† Takahiro HASEGAWA※

Kakuji OGAWARA‡ Katsumi TADAMURA‡

ynagai@yamaguchi-u.ac.jp†, ichikay@yamaguchi-u.ac.jp†, cithase@ipc.shizuoka.ac.jp※,

ogawara@yamaguchi-u.ac.jp‡, tadamura@yamaguchi-u.ac.jp‡

†山口大学 大学情報機構メディア基盤センター ※静岡大学 情報基盤センター

‡山口大学大学院 理工学研究科

†Media and Information Technology Center, Organization for Academic Information, Yamaguchi Univ.

※Center for Information Infrastructure, Shizuoka Univ.

‡Graduate School of Science and Engineering, Yamaguchi Univ.

（要旨）

本論文では，情報セキュリティマネジメントシステム（ISMS;Information Security Management System）導入に際して，人件費を含めた情報セキュリティインシデントコストを定量的に把握する方法を提案する．情報セキュリティインシデントやそれに対する複数の是正・予防措置を，限られた予算枠内で実施するために，各施策の緊急度や重要度の比較に利用可能な指標が必要となる．インシデントにより発生する損失額は重要な指標の 1 つである．損失額としては，インシデントによる逸失利益や壊れた機器などの直接的に発生した損失と，原状回復費用などを合わせて算出すべきである．活動基準原価管理などの作業時間管理を含む個別原価管理を採用している組織では，人件費を含めてイベント毎のコストは原価として把握可能であるが，そうではない国立大学法人においては，個々のインシデントのコスト算出は極めて困難である．しかしながら，このような組織内でも一定の基準単価を定めて作業項目別の所要金額を算出する事は可能である．これらの所要金額の合計値をインシデントコストとみなす事により，インシデント間の大きさの比較が可能となる．ここで算出されるコストは，国立大学法人の会計基準に則った経費を算出するものではなく，インシデント相互の比較の為の定量的数値として意味をもつものである．山口大学では，提案方式を ISMS 構築において適用し，その効果を確認した．

キーワード:インシデントコスト，定量化，ISMS，情報セキュリティ

（Abstract）
We propose a method to quantitatively grasp the cost of the information security incident including the labor cost when the information security management system (ISMS) is introduced. In order to execute several corrective and preventive actions within a limited budget, we need some indicators to compare the level of urgency or importance on each action. The amount of a loss generated by the incident is one of the key indicators. The total amount of loss shall consist of not only the loss directly caused by the incident such as broken equipments and lost profits, but also the indirect cost to recover to the original state. In the organization that adopts the individual cost management including the working hours management like the activity-based management etc., the cost of each event can be understood as a cost including the labor cost. But if the organization does not adopt such accounting, calculating the cost of individual incidents is extremely difficult. However, to calculate the amount required, such values for certain criteria in the organization is possible. By calculating the total value of the amount required by these factors as a incident cost, we can compare the magnitude of the multiple incident in the organization. We applied the proposed method to constructing ISMS in Yamaguchi University, and confirmed the effectiveness.

Key words : incident cost, quantifying, ISMS, information security

1. はじめに

インターネットの普及が進み，情報システムが様々な脅威にさらされている中で，企業において情報セキュリティマネジメントシステム(ISMS；Information Security Management System)の導入が盛んである．国立大学においても，これを導入する動きがある．情報セキュリティマネジメントに関しては，国際規格（ISO/IEC27001）[4]が定められ，これに呼応して JIS 規格（JIS Q 27001）[8]が定められている．この規格への適合性を第 3 者機関が評価・認証する制度も，（財）日本情報経済社会推進協会（JIPDEC；Japan Institute for Promotion of Digital Economy and Community）により運用されている[12]．2012 年 5 月現在，全国で 4,000 を超える組織体がこの認証を獲得している[13]．国立大学法人情報系センター協議会の中に，先行して ISMS 適合性評価制度下での認証を受けた大学を中心として ISMS 研究会が立ち上げられたのも ISMS 導入機運の高まりを表している[5]．JIS Q 27001 の付属書 A.13.2.2 には「情報セキュリティインシデントの形態，規模及び費用を定量化し監視できるようにする仕組みを備えなければならない」という管理策が記載されており，情報セキュリティインシデントの費用を定量化して監視するように求められている．

製造業などの企業において個別原価計算[3]を採用している場合，個々のインシデントコストは原価として把握される．情報処理産業などにおいても，情報システムの開発原価を把握するため個別原価計算制度を採用する企業があり，そこでは，人件費も個別の案件ごとに把握して製造原価に組み入れている．また，活動基準原価計算（ABC;Activity-Based Costing）を採用して，業務毎の原価を把握している企業や自治体では，業務ごと(あるいは，作業項目ごと)の人件費についても把握されている[7]．以下，このような法人を「作業別人件費算出法人」と称する．作業別人件費算出法人においては，従業員の作業項目別の所要時間を集計し，人件費が原価計算に組み入れる仕組みが確立されている．このような法人の中でも，インシデント対策が作業の 1 つとして取り扱われる場合とそうでない場合とがある．後者においてはインシデントを発生させた業務のコストの中に含めて集計され，インシデントコストとして認識されないこともある．ISMS 適合性認証を受け ABC を採用している市川市などの自治体においては，業務別人

件費は把握しつつもインシデント対応に要したコストのみを抽出して把握することはなされていない[1]. 一方, 国立大学においては, 国立大学法人化の際に企業会計が導入されたとはいえ, 人件費を作業別に捉える仕組みにはなっていない[15]. 個別の業務ごとのコストを把握する仕組みはなく, インシデント対策作業毎に人件費などのインシデントコストを定量的に把握する習慣や仕組みもない. したがって, JIS 規格に適合した ISMS を構築するには, コスト定量化(算出)の仕組みを新たにつくる必要がある. すなわち, インシデントコストの要素を明確にして計算方法を確立する事が求められる. 本論文では, インシデントコスト算出の仕組みがないという ISMS 構築時の課題を解決する為に, 先行事例[9]などを踏まえて算出モデルを構成したうえで, インシデントコスト算出の仕組みを提案する. 提案に際して, モデル組織を想定して説明する. 提案する方式は, 個別インシデントに費やした人件費を含めてそのコストを算出し, 売上や利益という概念を必要としない国立大学における逸失利益を推計している点, さらには, インシデントの規模を 1 つの指標(金額)で比較可能としている点, 等の特徴がある.

2. 一般的なインシデントコスト算出方法と国立大学法人への適用上の課題

2.1 インシデント管理の範囲

ISO/IEC27001[4](JIS Q 27001)[8]の補助資料でもある ISO/IEC TR 18044:2004 (Information security incident management)によると「インシデントとは, 望まない又は予期しない単独又は一連の情報セキュリティ事象であって, 事業運営を危うくする確率, 及び情報セキュリティを脅かす確率が高いもの」と定義されている[11]. また, ITIL(Information Technology Infrastructure Library)[2]においては, インシデント管理と問題管理を別のプロセスとして捉えている. 前者の目的は, 可能な限り迅速に異常状態(あるいは非定常状態)を脱して平常状態(あるいは定常状態)に戻す点にある. 従って原因追求よりも早く平常状態に戻すことが優先される. これに対して後者の目的は, インシデントの原因を明確にしたうえで再発や類似事故発生を防止し, 業務への悪影響を最小限に抑える事にある. このため, 問題管理においては, 時間をかけてでも根本原因を追及して是正処置を講ずる事が大切になる. ITIL にいう問題管理の対象となる「問題」の中には, インシデント発生前のリスク対策としての改善要求対応なども含む. インシデントの内容によっては, その対応により平常状態(あるいは定常状態)に回復した後も根本原因追究やその解決策さらには再発予防策の検討・実施・検証の作業が残り, 長期間にわたる対応作業となる場合もある.

本論文では, ISMS 運用下の組織におけるインシデントのコストの算出を目的としており, インシデント発生による異常状態が解消されて管理者への報告が完了するまでの作業をインシデント管理の対象としている. 図 2 は対象範囲内の作業を示すものである. さらに, ISMS 適用範囲内の情報資産(JIS27001 附属書 A.7.1.1 の項で要求される資産目録に掲載される)に係るインシデントを対象とし, これにより発生する損害を算出するべきインシデントコストとする. 本論文では, 前述の図 2 に示されるインシデント管理範囲内の作業に必要なコストの算出方法を提案する.

2.2 一般的なコスト算出モデルにおけるインシデントコスト

ISMS に関する規格(ISO/IEC27001[4]もしくは JIS27001[8])においては, 情報セキュリティの 3 要素(機密性(Confidentiality), 完全性(Integrity), 可用性(Availability))を維持することを要求している. 管理対象の情報資産全てにおいて, 障害によってこれら情報セキュリティが阻害される可能性がある. 情報処理推進機構(IPA;Information-technology Promotion Agency, Japan:旧情報処理振興事業協会)の

「被害額算出モデル」報告書[9]によれば，組織体にとって被害額の把握が重要である．生じる損失額には，「情報セキュリティインシデントに関わる調査　調査報告書 Ver1.0」[10]によれば，表 1 のような項目があり，インシデントコストは各被害額の合計額である．同報告書に被害額項目の算出式が明記されているものについては，表 1 の備考欄に記載している．ここでいう「被害額」の合計が本論文の「インシデントコスト」にあたる．「被害額算出モデル」報告書[9]では，算出モデルと推計値として算出する範囲が提示されており，2 次的被害額は対象外としている．前記 2 つの報告書いずれにおいても，「インシデントコストの把握が重要であるにもかかわらず，我が国の企業や組織において充分把握できていない」と書いている．実際，著者らが調査した限り，インシデントの対応事例や対策技術等に関する文献はあるが，インシデントコストに関する他の文献の存在は確認されていない．前記文献[9,10]におけるコスト算出方式は，一般企業を想定しており，売上，原価，利益が明確な場合に適用可能な方法である．国立大学法人への適用にあたっては，幾つかの解決すべき課題（次節参照）があり，そのまま適用することは出来ない．本論文では，これらの課題を解決したうえで，国立大学法人におけるインシデントコストの算出方式を設定し提案する．なお，本論文では可用性を阻害するインシデントに限定してそのコスト算出について述べる．

2.3 国立大学法人への適用上の課題

前節で述べたコスト算出方法の国立大学法人への適用に際して表 2 の 3 つの課題がある．提案するコスト算出方式が必要とするデータを収集する仕組みが必要な事は言うまでもない．以下，表 2 記載の課題について順に説明する．

ここで，図 1 のサーバ側ネットワークスイッチ（以下，スイッチ）が故障し，これを予備の機器に交換して 1 時間後に回復した事例を考えてみる．この場合，消費したコストは取り替えたスイッチの費用だけではない．原因究明や障害部位の特定や機器入れ替え後の動作確認など，対応には人件費が必要である．国立大学法人においては，故障し交換した機器（スイッチ）の費用（価格）はコストとして扱うが，原因究明や障害部位の特定，あるいは機器の動作確認などに要した人件費は，従来インシデントコストには参入しない．結果として当該インシデントコストに含まれる人件費を 0 円と見なすこととなる．国立大学法人においては，個別イベント毎に要した人件費を捉える仕組みが制度化されておらず，これら個別案件対応の人件費を算出する習慣もない．表 1 の項番 2「復旧に要したコスト」の中の人件費など，インシデントコストに占める人件費を算出するために，個別のインシデント対応作業時間を記録し，人件費を算出する方法を確立する必要がある．これが第 1 の課題である．

もちろんコスト計算作業そのものにもコスト（人件費）が必要である．注意を要するのは，業務運営への影響の小さいインシデントに対してもコスト計算作業は必要であるということである．対策の為の作業量が小さいインシデントに対して過大な手間や時間をかけてコスト計算を実施することは本末転倒と言わざるを得ず，コスト算出の対象とすべきインシデントの範囲を適切に決定するべきである．これが第 2 の課題である．

さらに，表 1 の中の「売上」や「利益」は国立大学法人においては意味をなさないため，一般的なコスト算出法を国立大学法人に適用するに当たっては，逸失利益の定義及びその定量化が必要である．また，表 1 記載の多くの被害額の項目は，個別のインシデントに対して確定するのが困難な情報である．とりわけ表 1 の「潜在化被害額」（項番 7～項番 9）は，企業を含むほとんどの組織においても算出することが極めて困難である．前出の文献[9]においても「2 次的被害額」（表 1 の項番 3～6 及び項番 8～9）については推計することを断念している．これらの項目については，国立大学法人においての評価方法や定量化方法を決定する必要がある．これが第 3 の課題である．

3. インシデントコスト算出モデル

この章では，国立大学法人のモデル（本章では単にモデルという）として大学のキャンパスネットワークを例として，これを維持管理する情報系センター（以下，センター）におけるコスト算出対象範囲を設定し，インシデント別の人件費の考え方を説明する．

3.1 国立大学法人のモデル

キャンパスが複数(m)あるとし，各キャンパス A_i(i=1,2,…,m)では，n_i 棟の建物がキャンパスネットワークで結ばれていて，各建物（図 3 では A_{ij}(i=1,2,…,m；j=1,2,…,n_i)棟と表示）間はスイッチ同士で接続されており，センターは各建物の入り口であるスイッチ迄を管理していると設定する．当モデル（図 3）では，1 台の端末には，センターが管理する IP アドレスが 1 つ割り当てられている．各建物のスイッチの先には，スイッチが接続され，さらにその先にユーザの PC やサーバが q_{ij} 台接続されている．場所によってはサブネットが接続されるケースもある．本論文では議論を簡単にするため，各キャンパス A_i 内の建物の数（n_i）や各建物 A_{ij} 内の端末数（q_{ij}）が同数であるものとし，それぞれ n，q とする．さらに，ネットワークに接続される機器には IP アドレスが割り当てられ，全てセンターに届け出てセンターが管理する DNS (Domain Name System)に登録されているものと設定する（ここでは，IP アドレスの数は端末数と等しい）．大学内には，自らサブネットを構成し，サブネット内のローカルアドレスを各機器に IP アドレスとして割り当てて，中心となるサーバのアドレスのみをセンターに届けている場合がある．この場合はサブネット全体を 1 台の機器と扱う．

3.2 センターサービスとコスト計算対象インシデント

モデルにおいてセンターは，サーバを設置して学内に各種 IT サービスを提供している．図 4 は，モデルのキャンパスの1つ（A_i）においてセンターが提供するサービスの利用範囲とセンターの保守範囲を示している．サービスの利用範囲（図 4 の淡く網掛けしている点線内の範囲）とは，インシデント発生時に影響を受ける範囲であり，業務効率低下を伴う範囲でもある．各建物内のスイッチより先のネットワークについては，各部局のネットワーク管理者が設置されており，センターの管理外としている．センターはこの範囲内に影響を与えるインシデントについて対策を行い，国立大学法人としてのインシデントコストを算出する．ただし，後述のように軽微なインシデントについてはコストの算出を省略する．この範囲は，サービスの種類（たとえば，メールサービスやデータストレージ提供サービス，等）によって，学内全体の場合もあれば特定の範囲に限定される場合もある．保守範囲（図 4 の濃く網掛けしている範囲）とは，センターがその範囲内の機器を維持管理する範囲であり，センターが対策するべきインシデント発生時には，修復のための保守部品などをセンターの予算にて調達する．保守範囲以外のサービス利用範囲内で発生するインシデントに対しては，センターは対応作業を実施するが，修復のための保守部品などの調達にセンターの予算を使わない．保守範囲には，学内ネットワーク機器を含めて，サーバ室等のセンターが管理する施設に設置されている機器全てが保守範囲に含まれる．

4. 課題への対応

4.1 作業別人件費算出方法の確立（第 1 の課題）

4.1 1 人件費の考え方

人件費については，時間単価（円／人時）に所要時間を乗じた金額を算出すれば良いが，時間単価の設定が極めて困難である．厳密には，実際に対策に当たった要員毎の時間単価（教職員の給与等を元に個人別に算定される金額）を基に算出すべきであるが，プライバシーの問題と個人毎に単価を設定することによる計算の煩雑さを避けることも必要である．そのため本

論文では，公開されている情報[6,14]から，全学の常勤教職員の平均年間給与を所定年間勤務時間で除した金額を時間単価と設定し，インシデントコスト中人件費合計 C_0 は，4.1.2～4.1.4 に記載するような計算方法により算出される．本論文では年度内異動の少ない常勤職員に関する公開情報をもとに算定し，全学共通の数値を設定することとしている．これにより，インシデント毎の作業時間が判れば，対策に要した人件費が算出できる事となり，第 1 の課題に対応できたこととなる．最近では，常勤教職員以外にも非常勤教職員が障害対応するケースもある．しかし，時間単価設定方式については本提案の本質的な部分では無いことから，年間の就業期間や就業時間の把握が困難な非常勤職員を除外し，大学全体で一定の指標でインシデントの規模を比較することとしている．

4.1.2 作業工程と人件費

(1) 組織 A における教職員の時間単価は，全員共通かつ全工程で共通とし年度毎に算出して設定するものとする．一般的には，当該作業に従事する教職員の資格や年齢により時間単価は異なるが，ここでは説明と集計作業を単純にするため，組織 A 全体に亘って均一な時間単価を設定する．

(2) 国立大学法人（本章では以下，組織 A）は，N 人の教職員から構成される．それぞれの教職員を E_i (i=1,2,…,N)と表示する．

(3) 組織 A が各教職員 E_i のために負担する年間人件費は固定金額とし，C_i (i=1,2,…,N)と表示する．

(4) 組織 A のすべての業務がプロジェクト体制で推進され，各プロジェクトには番号が振られて，それぞれを P_j (j=1,2,…,M)と表示する．M は，本論文で対象とするインシデント発生年度（以下，当年度）の組織 A のプロジェクトの総数である．

(5) 組織 A では，組織内業務（各プロジェクト）を遂行する上での作業項目を分類しており，それぞれを工程と呼んで W_k (k=1,2,…,L)と表示する．

(6) 全ての教職員は，並行して複数のプロジェクトメンバーとなり，作業を進める．

(7) 教職員 E_i がプロジェクト P_j において工程 W_k のために $t_{(i,j,k)}$ の時間を費やしたと想定する．

4.1.3 時間単価の設定と人件費算出式

(1) 当年度の組織 A における総作業時間 T は，$T=\sum_k \sum_j \sum_i t_{(i,j,k)}$ となる．

(2) 組織 A の当年度の人件費合計は，$C=\Sigma C_i$

(3) 組織 A における当年度の作業時間単価は，$C_u=C／T$ と設定される．

4.1.4 インシデント対応作業と人件費

(1) あるインシデントへの対策を，n 人の教職員 E_h (h=1,2,…,n)[{E_h | h=1,2,…,n} ⊂ {E_i | i=1,2,…,N}]からなるプロジェクト P_0 として実施するものと設定する．

(2) 各教職員 E_h が，当該インシデント対策のため（現状復帰のため）それぞれ工程 W_k の作業を $t_{(h,0,k)}$ 時間実施するものと設定する．

(3) 当該インシデント対応のための作業時間の合計 t_0 と人件費 C_0 は，次式で計算される．

a. $t_0 = \sum_k \sum_h t_{(h,0,k)}$

…インシデント対応作業時間合計

b. $C_0 = C_u \times t_0$

…インシデントコスト中の人件費合計

4.2 インシデントコスト算出範囲の限定（第 2 の課題）

インシデントコスト算出作業のためのコストがインシデントコストの大半を占めるほど（逆に言えば，小さなインシデント）であれば，損失額を大きくしない意味でも，当該インシデントのコスト算出を省略すべきである．また，従来コストを定量的に把握する仕組みや習慣がない組織の場合，ISMS 導入当初においては，より重要なインシデントのコスト算出作業に限定するとともに，個々の計算精度を追求するよりも，個別インシデントのコスト評価を着実に実施していくことが大切で

あり，コスト算出作業による本来の業務時間の減少を極力抑えるべきである．ISMS におけるPDCA 実施過程（Plan，Do，Check，Actionをサイクリックに実施していくことをいう）の中で，順次仕組みを充実していくことを前提とし，本論文では，可用性喪失時間が一定時間以上の場合や，影響を受けた範囲が一定の範囲以上の場合等の重要なインシデントにコスト算出範囲を限定する．すなわち，定量化の範囲を現実的に可能な範囲 [1]に限定することにより第 2 の課題を解決する．閾値など具体的な条件は，ISMS に組織 A の経営陣に認められた ISMS 実施手順の中で規定する．

本論文では，教育用計算機を含む学内ネットワークの停止を重要視し，前述の ISMS 実施手順で規定された条件に該当する場合にインシデントコスト算出の対象とすることで議論を進める．

4.3 逸失利益の定義と算出方法の決定（第 3 の課題）

可用性に関わるインシデント（学内ネットワークや機器の停止）では，表面化する 1 次的被害の1つに逸失利益がある．本来稼働していれば実施された業務により生産されたはずの付加価値が得られないからである．企業の場合と異なって売上額等の評価指標がないため，本論文では，本来生み出されるべき付加価値を生み出すための費用を評価指標として設定する．表 3 は，表 1 を国立大学のインシデントに当てはめたものである．このインシデントにおけるコストを，

表 3 の項番 1 から項番 4 の各被害額の合計金額

と設定する．

ネットワークや機器の停止に関する逸失利益の算出では，全学の端末台数に応じた損失額を算出するが，複数キャンパスあるいは複数の建物の中にある端末台数（3.1 節の q_{ij}）を同数（3.1 節の q）とみなすことにより，コスト算出を簡便にする．影響を受けた機器の台数を正確に把握すれば，より正確なコスト算出が可能である．しかし，4.2 節で述べたように，正確さを追及するあまり作業を困難にすることを避けて着実にコスト算出を可能とするため，簡略化している．表 4 は学内ネットワーク停止に関する逸失利益算出方法を表している．機器の停止に関しても同様の考え方で逸失利益算出表を用意する．表 4 で算出される金額は端末が全く使えなくなった場合であり，業務効率低下による被害額算出式に記載のある「サービスへの業務依存度（重み）」は 1.0 である．端末は稼働しているものの一部のサービスのみが停止する場合，この数値は 1 以下になる．また，サービスを受ける個人によって，個々のサービスへの依存度は異なり，その値を決定する際にはその人の主観も入ると考えられる．この数値を客観的に決定する方式については，のちに述べるように今後の課題でもあるが，本論文では実用性を重視して，センター所属員へのアンケートにより，コスト計算上考慮するサービス項目とそれによる業務依存度（重み）を表 5 の通り設定する．もちろん，ISMS の PDCA 実行過程において定期的に見直されることにより，逐次精度を高める事を前提としているのは言うまでもない．一部のサービスが停止した場合，表 5 に示す各種サービスへの業務依存度（重み）を乗じた数値により業務効率低下による被害額を算出する．複数のサービスが停止する場合には，それらそれぞれの重みを加算する．ただし，合計が1を超える場合には，1.0 を合計値とする．大学によっては，表 5 に掲載されていないサービスを提供する場合もあるが，本論文では主要な（インシデントによる影響が比較的大きい）サービス項目を挙げている．

4.4 インシデントコスト計算に必要な情報

情報セキュリティ事象の処置が終了し平常状態に戻った時には，図 2 記載のとおり，コスト計算ワークシート（対応報告書）を作成し管理者に報告すると同時に，コスト計算のための情報を ISMS 事務局 [2]宛送付して当該インシデントについてのコスト計算を実施する．本論文では，コスト算出に必要なデータを説明するため，図 5 にコスト計算ワークシートの例を示し，コスト計算

に必要なデータ項目を明確にする. 図 5 の中で薄く網掛けした項目がコスト計算に必要なデータ項目である. 図 6 は, 図 5 の逸失利益に関する影響範囲(①～⑤)と障害の重み(①～⑥)の種類を凡例として示す図表である.

図 5 のワークシートにおいては, 原状復帰迄の時間(t 時間), 影響範囲(G ¥/時), 障害の重み(B), 対応者別作業時間(C1 人時～C4 人時), 旅費(D k¥), 物品購入費用(E k¥), その他(F k¥), 影響を受けた端末台数(r 台), 影響を受けてサービスが低下した時間(K 時間), 人件費単価(Uk¥/人時)の 10 項目である. ( )内は図 5 の中の対応するデータ項目につけた記号とその単位である. 影響範囲については, 図 6 凡例 A の①～⑤のいずれかに対応する算出式で計算される時間当たりの被害額(G)を決める. 障害の重みについても, 図 6 凡例 B の①～⑥のいずれかを選択して, 同凡例に従い重みを決定する. 決定の方法は 4.3 節の表 5 についての説明のとおりである. 図 5 の逸失利益欄の 5 定数のうち r 以外の数値は国立大学法人毎の定数であり, r はインシデント毎に決定される数値である. 可用性に関するインシデント(M k¥)は, これらのデータに基づき次式で計算される.

$$M = G \times t \times B/1000 + (C1+C2+C3+C4) \times U + D+E+F+ r \times B \times K \times U$$

ここで, 人件費単価 U は, 4.1 節で説明した考え方に基づき設定されており, 国立大学法人毎に異なる値が設定されるべきである. また,「影響を受けた端末台数」については, センターが管理するネットワークにおける DNS サーバ(Dmain Name Server)に登録される IP アドレスの数を使用する. センターが提供するネットワークサービス範囲と一致することがその理由である.

5. 提案方式の試行と検証

5.1 定量化方式(提案方式)適用事例

ここ迄の計算方法を, 2.3 節に記載した具体例に適用してみる. まず, 人件費の単価に関しては, 筆者所属大学の場合, 平成 20 年度一人当たり年間給与額が 6, 642 千円, 年間勤務時間数 1,944 時間であるため, 時間単価は約 3,417 円となる. そこで, 通常千円単位でインシデントコストの算出を行うことから, 百円単位迄で丸めて時間単価を 3,400 円と設定した.

2.3 節に記載した具体例では, 1 つの校舎(建物)全体において 1 時間のサービス停止に遭遇し, 6 名の教職員が延べ 5 時間をかけて対処している. アクセスできなくなったサーバは共用データベースを提供するものであるとともに, メールサーバを兼ねていたものである. 壊れたスイッチの簿価が1万円, 新たに購入して交換したスイッチの価格が 10 万円であった. また, この障害の間, 当該校舎(建物)内の全ての端末がネットワークに接続できなくなった. キャンパス内の建物の数が 4 棟, また, 当該キャンパスにおけるネットワーク維持コストは月額 480 万円, 端末台数は 500 台であった. (人件費の時間単価は前述の通り 3,400 円である.)この場合, コストは次のように計算され, a～c の合計で 98 万 2 千円となる. これを表 4 の各変数に代入すると, Y=4,800/240=20, m=1, q=4 である. (設定値は図 5 記載の値と異なる.)

a. 逸失利益 : Y/m/n = 20/1/4/＝5(k¥)
b. 復旧に要した費用 : 10(壊れた機器の価格)＋100(代替品購入価格)＋3.4×5(復旧作業人件費) ＝ 127(k¥)
c. 業務低下による被害額 : 3.4(人件費時間単価)×500(端末台数)×(0.2(ﾒｰﾙ機能の重み)＋0.3(共有ﾌｫﾙﾀﾞの重み))×1(停止時間)＝850(k¥)

従来このケースにおいては, 機器の価格(10 万円)のみをコストと捉えていた. 人件費を算入しない場合は 10 万円, 算入した場合は約 98 万円, この金額の差(88 万円)を見ても人件費が無視できない大きさであり, 算出することの必要性と提案方式の有用性が判る.

5.2 実務への適用(試行)

山口大学では, 平成 21 年度から実際の ISMS 構築において提案方式を適用し, 平成 22 年 9

月の ISMS マネジメントレビューにおける経営陣への報告に使用した. その報告によれば, その間のインシデントは全てが可用性に関するインシデントであった. その中でコスト計算を実施した 2 件と, 他大学のインシデントコスト計算事例 2 件ついて, その結果を一覧表にしたのが表 6 である [3]. いずれの事例においても, 入れ替えた機器の費用のみをコストとする従来の金額に比べて大きなコストがかかっている事が判る. 表 6 の事例番号 3 においてはサーバ(機器)の交換が必要であったが, 他の 3 件は機器の入替えを必要としない事例である. 表 6 の「差異(B-A)」の欄の様に, 機器の入替えの無い場合, 従来はコスト 0(ゼロ)と評価されていた事例が, 決してそうではないことが判る. 表 6 記載の各案件ごとに作成したインシデントコスト計算ワークシート [4] を見れば, 人件費がほとんどを占めている事が判り, インシデントコストに人件費を算入して, インシデントの大きさを比較することの重要性も浮かび上がってくる. 特に事例番号 1 及び 2 では, 学内ネットワークが全学的に停止したことによる影響として業務効率低下による損失が大きな金額となっている. マネジメントレビューでは, 人件費の一部が障害対応に使用されている事実を目に見える形で報告がなされた. 経営陣にもインシデント発生の状況とその対応にかなりの人件費が必要であることに対する理解を得て, 是正のための作業実施とそれによるコスト消費について承認を得ることができた.

6. おわりに

本論文では, インシデントごとの人件費の算出が可能な, 国立大学法人向けのインシデントコストの定量化方式を提案し, 筆者所属大学での適用事例を示した. 提案したコスト算出方式により, 従来インシデントを定量的に把握することなく是正・予防措置を実施してきた組織において, 個々のインシデントの大きさを定量的に把握し, 相互に比較することが可能になった.

さらに, 作業毎の所要時間を記録する習慣がない国立大学法人において, インシデント対応という一部の作業のみとはいえ, 本来(インシデントが発生しなければ)不要であるはずの作業時間の存在を数値で実感させる仕組といえる. これは、表 6 を見れば明らかであり, 少々のコストや要員を投入してでもインシデントを減らそうとするモチベーションに結びつく. 筆者が所属するセンターの ISMS のマネジメントレビューにおいて, CIO(最高情報責任者;Chief Information Officer)がインシデントの大きさを把握し, 対応方法の選択や状況判断するための情報として役立つことも確認できている.

さらに, 本論文でインシデントコストの計算や報告の流れや手順を示した. コスト計算自体にも人件費が必要となるが, コンピュータシステム化して, データ入力を含むコスト計算作業の省力化は可能である. 今後, 個別原価計算制度や活動基準原価計算の採用状況や, ISMS における PDCA 実践状況に応じてコスト計算要素の見直しを行い, さらにはインシデントコストの計算精度を向上させることは課題の1つである.

本論文では, インシデント対応に必要な人件費に着目しているが, 教職員の作業量を作業項目別に把握する仕組みを確立すれば, センターに必要な作業量が可視化され, 要員数と作業量の関係を説明する為の資料としても役立つと考えられる. 作業項目ごとの時間を記録する仕組みを, 教育・研究に従事する教職員の活動全般に広げるべきかどうかは, 今後の検討課題として残る. しかし, 一部とはいえ, インシデントコストを定量的に把握できる提案方式は, 優先順位をつけてリスク対応できる仕組みへの可能性を大きくし, 国立大学法人におけるリスクマネジメントに役立つ成果であり, 広く活用が期待される.

注)

1) ここで言う「現実的に可能な範囲」とは, ISMS を運用する組織体にとって, コスト算出作業その

ものによる作業量増が本来の業務に支障を与えない範囲で，構成員が極端な負担を感じることなく，無理なくコスト計算が実施出来る範囲を意味する．組織体としてその範囲について合意するべきである．

2) 図 2 中の「ISMS 事務局」は，ISMS 運営組織内にあって当該組織における情報セキュリティ責任者を補佐し，ISMS に係る管理事務を担うグループである．インシデント管理に関してはこれを記録しその対策の進捗などをフォローアップする役割を担うグループである．図 2 の中では，インシデントを記録し管理台帳を更新するタスクに関する部分を掲載している．

3) 本論文で提案するコスト算出方式の適用事例として，共著者の一人が所属する静岡大学情報基盤センターの協力を得て，静岡大学のインシデントについてコストを算出したものである．しかしながら表 6 に掲載している 4 件それぞれの大学名は伏せさせて頂いている．

4)「インシデントコスト計算ワークシート」は図 5 を参照されたい．図 5 における「人件費」の欄の金額とインシデントコスト（図 5 の「M」）における割合をみれば本文に記載した事を理解できる．また，表 6 掲載の個別事例の「インシデントコスト計算ワークシート」の掲載は控えさせていただいている．

参考文献

[1] 市川市「ABC(Activity-Based-Costing)について ～活動基準原価計算～」，http://www.city.ichikawa.lg.jp/pla02/1211000002.html （Jun.26.2012）

[2] 英国 OGC（Office of Government Commerce），サービスサポート(2003 年出版)，itSMF Japan,2003

[3] 岡本清，『原価計算六訂版』，国元書房，2000

[4] 国際標準化機構（International Organization for Standardization），*Information technology – Security techniques – Information security management systems - Requirements, International Standard ISO/IEC27001*, ISO/IEC ,2005.

[5] 国立大学法人情報系センター協議会 ISMS 研究会「ISMS 研究会」，http://sigisms-nipc.cc.yamaguchi-u.ac.jp/ （Jun.26.2012）

[6] 国立大学法人山口大学，役職員の給与水準の公表，http://ds.cc.yamaguchi-u.ac.jp/~jinjika/kyuuyo/housyu_kyuuyo.html （Jun.26.2012）

[7] 櫻井通晴ほか，『ABC の基礎とケーススタディ ABC からバランスト・スコアカードへの展開』，東洋経済新報社，2004

[8] 島弘志，『JIS Q 27001(ISO/IEC27001)情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項』，JIS 規格 ，2006.

[9] 情報処理振興事業協会（現，情報処理推進機構）セキュリティセンター，『「被害額算出モデル」報告書』，p1&pp7-10，情報処理振興事業協会，2003

[10] 情報処理振興事業協会セキュリティセンター：情報セキュリティインシデントに関わる調査調査報告書 Ver.1.0，pp.17-20，情報処理振興事業協会，2002

[11] 中野康二・中野初美・平野芳行・吉田健一郎，『ISO/IEC 17799:2005 詳解情報セキュリティマネジメントの実践のための規範』，pp292-304，日本規格協会，2007

[12] 日本情報経済社会推進協会（JIPDEC），ISMS 適合性評価制度，http://www.isms.jipdec.jp/isms.html （Jun.26.2012）

[13] 日本情報処理開発協会（JIPDEC），ISMS 認証取得組織数推移(2010 年 5 月)，http://www.isms.jipdec.jp/lst/ind/suii.html （Jun.26.2012）

[14] 文部科学省，国立大学法人等の役職員の給与等の水準（平成 20 年度），http://www.mext.go.jp/b_menu/houdou/21/07/attach/1282400.htm （Jun.26.2012）

[15] 文部科学省,「国立大学法人会計基準」及び「国立大学法人会計基準注解」に関する実務指針(平成 15 年 7 月 10 日, 平成 23 年 2 月 15 日改訂版), http://www.mext.go.jp/component/a_menu/education/detail/__icsFiles/afieldfile/2012/04/09/1289344_06.pdf （August.1.2012）

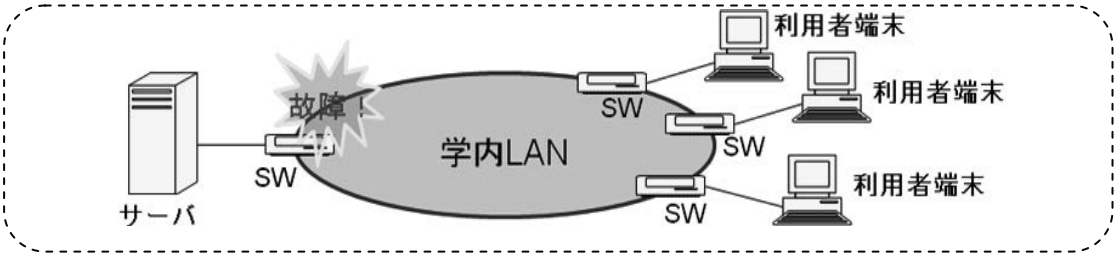

図 1　ネットワークスイッチ故障イメージ図

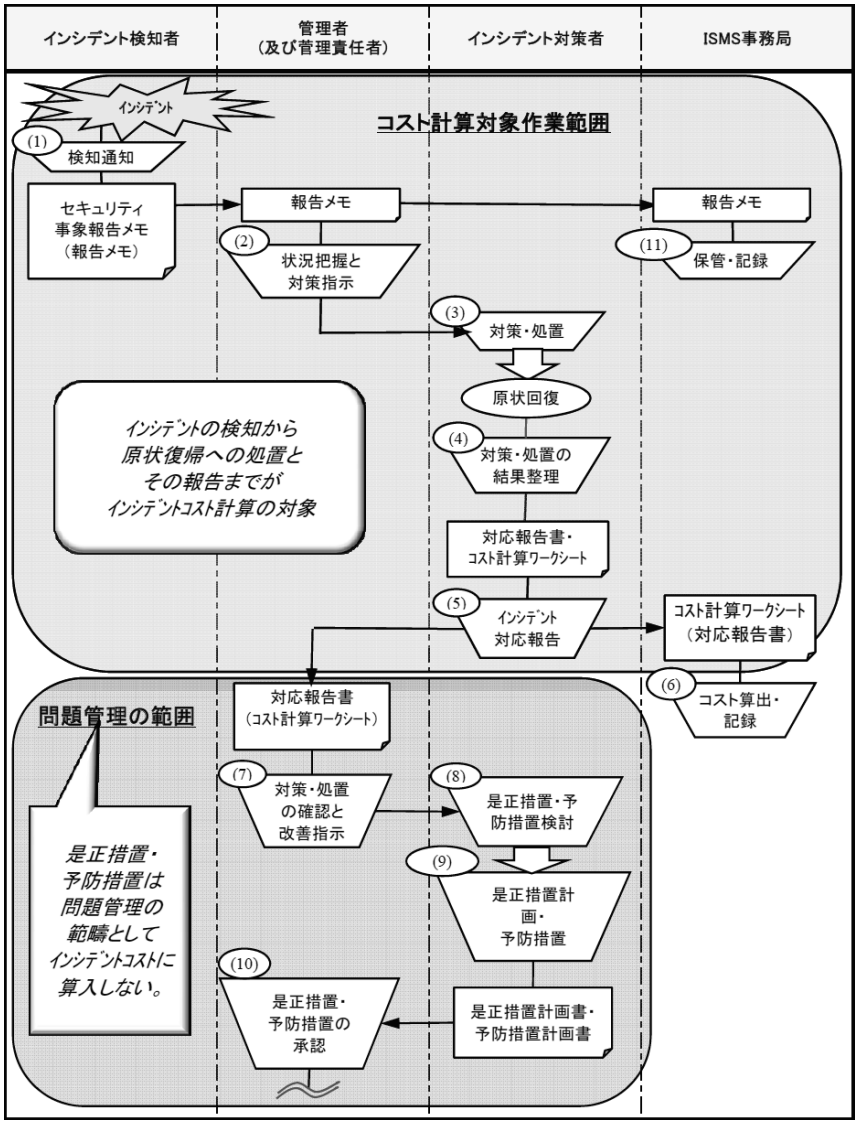

図 2 インシデント報告の流れ

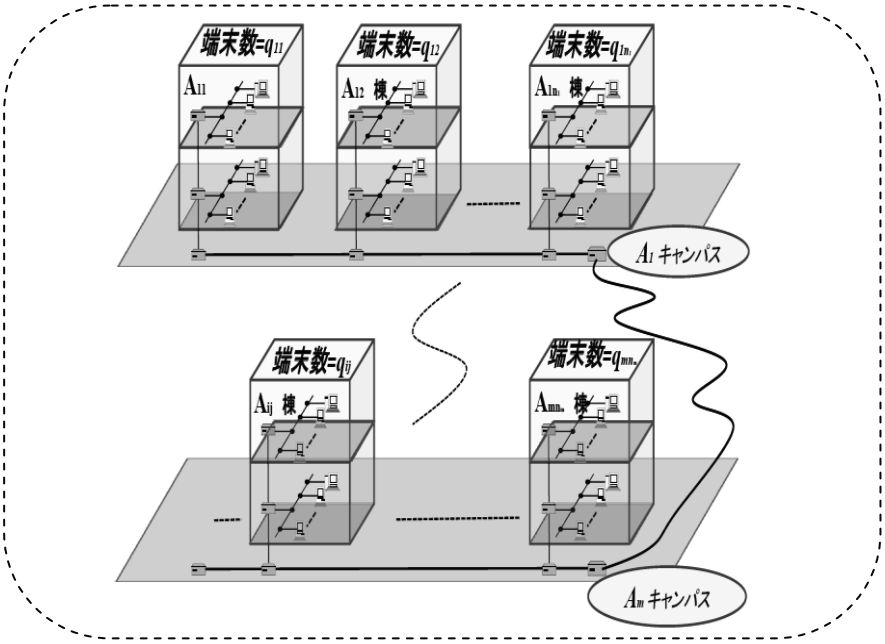

図 3　モデルキャンパスのネットワークイメージ

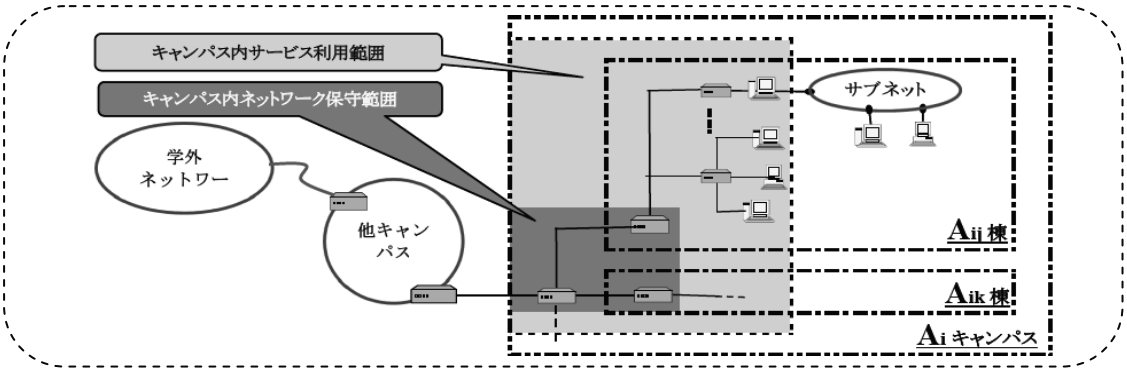

図 4　ネットワーク監視と保守の責任範囲イメージ図

障害NO. :

障害名称 :		インシデントコスト : (k¥)	M
発生日時			
原状(正常状態)復帰時刻			
対応完了日時			

(1)	逸失利益 (影響範囲)×(障害の重み)×(現状復帰迄の時間) ……			(補足)
	原状(正常状態)復帰までの時間(時間)		t	(補足)
	影響範囲 (凡例Aの①~⑤を選択)	① ② ③ ④ ⑤	G	(影響の状況)
	凡例A	図6　参照		
	定数 a	4,000,000	月次のネットワーク維持費用	
	定数 m	3	キャンパス数	
	定数 q	200	建物内の端末台数	
	定数 n	10	キャンパス内の建物数	
	定数 r	r	影響を受けた端末の台数	
	障害の重み (凡例Bの①~⑥を選択)	① ② ③ ④ ⑤ ⑥	B	(障害の重み設定根拠)
	凡例B	図6　参照		

(2)	復旧に要した費用(復旧費用)……			(補足)
	人件費	(作業概要)		
	単価: U 3.4 k¥/人時	対応者名	作業時間(人時)	対応作業内容
	①		C1	
	②		C2	
	③		C3	
	④		C4	
	旅費 (k¥)	D	(内訳)	
	物品購入費用 (k¥)	E	(内訳)	
	その他 (k¥)	F	(内訳)	
(3)	業務効率低下による被害額 (a×b×c×3400)……			(補足)
	a. 影響を受けた端末台数		r	
	b. サービスへの業務依存度 (凡例Bの「障害の重み」と同じ)		B	
	c. 影響を受けてサービスが低下した時間		K	

図 5　可用性に関するインシデントコスト計算ワークシート例

	項番	インシデント規模	算出式	説明
逸失利益凡例A	①	全学停止	Y=a/(30*8)　円/時	・月次のネットワーク維持費用をa円，1日8時間とする．月間の日数については，30日とみなす．
	②	キャンパス全体	Y/m　円/時	・キャンパス内の端末台数が各キャンパスで同数であるとみなし，キャンパス数をmとする．
	③	建物全体	Y/m/n　円/時	・建物内の端末台数(q)を建物間で同数であるとみなし，キャンパス内の建物数をnとする．
	④	建物の一部	(Y/m/n)×(r/q)　円/時	・停止により使用不能となった端末の台数をr台とする．
	⑤	計算機個別	Y/m/n/q　円/時	・評価しない
	項番	障害の種類・レベル	重み	説明
逸失利益凡例B	①	全サービスの停止（学内ネットワークの停止）	1.0	・学内ネットワークを利用する全てのサービス（機能）の利用ができない．
	②	認証機能の停止	0.7	・教育用端末・情報コンセント・メールが全て利用不可
	③	拠点間の分断	0.7	・認証機能が停止する．
	④	メール機能の停止	0.3	・学内外の業務上の情報交換機能が停止する．（WEBを参照することは可能な場合）
	⑤	WEBサービスの停止	0.3	・WEBサービスの依存度は限られているため．
	⑥	共有フォルダの停止	0.2	・多くの教職員・学生が利用しているが，共有フォルダを使用しない業務が続行できる．

図 6　可用性に関する逸失利益の凡例

表 1　企業等一般的組織におけるインシデントに係る被害額分類表

項番	大分類	中分類	小分類	備考
1	表面化被害額	1 次的な被害額	逸失利益	「時間当たりの売り上げに対する利益」×「システムないしサービスの停止していた時間」
2			復旧に要したコスト	
3		2 次的な被害額	各種の補償・補填	
4			損害賠償	
5			謝罪広告費用	
6			その他	
7	潜在化被害額	業務に関わる潜在化被害額	業務効率低下による被害額	「固定費（人件費）」×「インシデントによる影響を受けた人数」×「IT 感応度（業務依存度）」×「停止時間」
8		業務外の潜在化被害額	風評被害	
9			企業のイメージダウン	

表 2 国立大学法人への適用のための 4 つの課題

項番	課題	補足説明（必要となる取り組み）
1	作業別人件費算出方法の確立	インシデント毎の作業時間を記録し，インシデント別人件費を算出する仕組みを確立する．
2	インシデントコスト算出範囲の決定	インシデントコストよりもコスト計算作業そのもののコストが大きい場合，コスト計算作業を省略できるように，コスト計算対象範囲を限定する．
3	逸失利益の定義と算出方法の決定	売上や利益のない国立大学法人における逸失利益の金額算出方法を決める．また，一般的にも極めて困難な 2 次的被害額の，国立大学法人における取扱い方法を決める．

表 3　ネットワーク停止による被害額表

項番	大分類	中分類	小分類	備考
1	表面化被害額	1 次的な被害額	逸失利益	・全学停止，キャンパス全体停止，建物全体停止，建物の一部停止，計算機別停止，に分類して表 4 のとおり設定 ・ネットワーク上で，一部サービスのみの停止の場合，表 4 の「サービスへの業務依存度（重み）」を乗ずる．
2			復旧に要したコスト	・「壊れた機器の価格」＋「代替品購入価格」＋「工事費用」＋「復旧作業人件費」
3		2 次的な被害額	各種の補償・補填，賠償費用，謝罪広告費用	・発生しない（謝罪広告費用すなわち Web ページ作成作業費は項番 2 の「復旧作業人件費」に含む）
4	潜在化被害額	業務に関わる潜在化被害額	業務効率低下による被害額	「一人時あたり人件費）」×「影響を受けた端末台数」×「サービスへの業務依存度（重み）」(*1)×「停止時間」(*2)
5		業務外の潜在化被害額	風評被害，イメージダウン	・評価しない

*1:表 5 参照，*2:障害検知時刻から正常状態への復帰時刻迄の時間

表 4　ネットワーク停止による逸失利益算出表

項番	インシデント規模	算出式（円/時）	説明
1	全学停止	Y=a/(30*8)	・月次のネットワーク維持費用をa円，1 日 8 時間とする．月間の日数については，30 日とみなす．
2	キャンパス全体	Y/m	・キャンパス内の端末台数が各キャンパスで同数であるとみなし，キャンパス数をmとする．（3.1 節参照）
3	建物全体	Y/m/n	・建物内の端末台数(q)を建物間で同数であるとみなし，キャンパス内の建物数を n とする．（3.1 節参照）
4	建物の一部	(Y/m/n)×(r/q)	・停止により使用不能となった端末の台数を r 台とする．
5	計算機個別	Y/m/n/q	・評価しない

表 5　サービスへの業務依存度（重み）一覧表

項番	影響を受けるサービス	重み	説明
1	認証機能の停止	0.7	・教育用端末・情報コンセント・メールが全て利用不可
2	拠点間の分断	0.7	・認証機能が停止する．
3	メール機能の停止	0.3	・学内外の業務上の情報交換機能が停止する． （Web を参照することは可能な場合）
4	Web サービスの停止	0.3	・Web サービスの依存度は限られている．
5	共有フォルダの停止	0.2	・多くの教職員・学生が利用しているが，共有フォルダを使用しない業務が続行できる．

表 6 インシデントコスト算出事例 （単位;円）

事例番号	件名	差異(B-A)	A.従来方式によるコスト	B.提案方式によるコスト(C欄内訳の合計)	C. 提案方式によるコスト内訳		
					逸失利益	復旧費用	業務効率低下による被害額
1	ループ配線によるFW上流からストーム	41,945,070	0	41,945,070	36,670	20,400	41,888,000
2	GIP用L3スイッチハングアップ	18,352,243	0	18,352,243	16,043	10,200	18,326,000
3	Webサーバ故障	115,467	200,000	315,467	6,667	227,200	81,600
4	演習室PC接続不可	6,089	0	6,089	139	5,100	850
5	Aキャンパス停電	1,700	0	1,700	0	1,700	0
5 件合計		*60,420,569*	*200,000*	*60,620,569*	*59,519*	*264,600*	*60,296,450*