Vol.2010-DPS-142 No.45
Vol.2010-CSEC-48 No.45
2010/3/5

情報セキュリティ事件・事故の分析と対策に関する考察

村上　靖[†]　内田　勝也[†]

情報セキュリティ事件・事故は、その規模・内容によっては組織や企業の存続さえ危ぶませるほどの影響がある。発生時の影響の大きさ、事前・事後対応の重要性への理解が進み、セキュリティ対策の導入も進んでいる。しかし、事件・事故は継続して発生している。
類似の情報セキュリティ事件・事故の発生する背景には、原因分析の不十分さが一因にあるのではないかととらえた。情報セキュリティの分野では、原因分析の手法として広く用いられているものは見当たらないが、他の分野においてはさまざまな手法がとられている。
本稿では、この原因分析の手法に着目した。有効な対策につながる事故分析手法を探り、実際に情報セキュリティとは異なる医療分野で使用例のある分析手法を情報セキュリティ事故に適用を試み、その有効性を検証した。また、これらを通じて原因分析の背景となる考え方や、有効な対策を導き出す方法について考察を行った。

A study of information security incident analysis

Yasushi Murakami[†]　and Katsuya Uchida[†]

According to the scale and matter, information security incident has a serious influence upon organizations or companies. At present many countermeasure systems are being introduced. Because many organizations and companies understand its risk and importance to cope with incidents before and after. Although those incidents occur continually.
Imperfect cause analysis is one of the causes. There are no methods of cause analysis that is used generally in the information security field. But there are various methods in the other fields.
In this dissertation, inspect the effective method for the information security field using the method in the medical field. On that basis, study the way of thinking in cause analyzing and how to think out the countermeasure.

1. 研究の背景・目的

1.1 研究の背景

情報セキュリティに関する事件・事故の発生は、直接の被害額、損害賠償の負担のみならず、組織の信用の失墜にもつながる。組織における本来の業務や、資金運用などに問題がなかったとしても、セキュリティ事件・事故を起こしたために、組織の存続が危うくなる場合も少なくない。

しかし、情報セキュリティ事件・事故は継続して発生している。これらの事件・事故はセキュリティ対策を軽視している、あるいは行っていない組織でのみ発生しているのではないと推測する。事件・事故防止策として何らかのセキュリティ対策を行っているにもかかわらず想定外の事件・事故が発生しているのであれば、対策が不十分なものであるか、対策自体が誤っている可能性がある。

また、セキュリティ事件・事故が発生した場合、事件・事故を起こした担当者やその上司の責任が問われ、組織としては「再発防止に努めます」とのコメントは出されても、有効な再発防止策が展開されているのか明確ではない場合もある。

自己あるいは他の組織におけるセキュリティ事件・事故を正しく分析し、自らの組織に当てはめて有効な対策を取り、またこれを見直していくことが事件・事故防止には必要であると考える。このための分析の手法と適用について考察を行う。なお、分析手法については医療や航空、原発など主に情報セキュリティ以外の分野で研究が進んでいるものがあり、適用の可能性について考察していく。

情報セキュリティ事件・事故について、内田研究室では継続的に調査を行っている。これによると発生の件数は減少傾向にはあるが、継続して発生していることがうかがわれる。（表 1　情報セキュリティインシデント）

† 情報セキュリティ大学院大学
Institute of Information Security

Vol.2010-DPS-142 No.45
Vol.2010-CSEC-48 No.45
2010/3/5

表 1　情報セキュリティインシデント
(2009 年国内調査を基準に上位項目のみ記載) [1]

	2008年国内		2009年国内		2008年CSI	
	順位	割合	順位	割合	順位	割合
ウイルス感染	1	60	1	50	1	50
発生していない	2	30	2	42	−	−
ノートPCなどの盗難	3	25	3	15	3	42
内部者のネット・アクセス乱用	4	16	4	10	2	44
DoS攻撃	5	9	5	7	6	21

（回答数：2008年国内調査 714件 2009年国内調査 633件 2008年CSI調査 433件）

また、発生後の対応については、「加害者の特定」、「セキュリティホールをふさぐための暫定措置」などが上位となっており、表面的、属人的なものに留まっている傾向が見られた。（表 2　情報セキュリティインシデント後の対応）

表 2　情報セキュリティインシデント後の対応
(2009 年国内調査を基準に上位項目のみ記載) [1]

	2008J		2009J		2008C	
	順位	割合	順位	割合	順位	割合
加害者を特定しようとした	1	33	1	31	1	60
セキュリティホールをふさぐための暫定措置を施した	4	28	2	29	2	54
セキュリティソフトをインストールした	3	30	3	29	4	37
セキュリティパッチをインストールした	2	31	4	28	3	46
その他	−	22	5	23	−	−
担当部門だけで処理した	5	21	6	23	−	−
組織のセキュリティポリシーを変更した	6	13	7	12	5	33
追加のセキュリティハードウエアを導入した	7	11	8	8	8	23
弁護士に相談した	9	2	9	7	9	18
何もしなかった	8	2	10	6	−	−
外部の法執行機関等に報告した	−	−	−	−	6	27
外部組織に報告しなかった	−	−	−	−	7	24

(回答数:2008 年度国内調査 467 件 2009 年度国内調査 345 件 2008 年度 CSI 調査 295 件)

「組織のセキュリティポリシーを変更した」など、運用を見直す対策をとる割合は低くなっている。これは、事件・事故発生後の原因分析が不十分であるため、結果としての対策が浅いレベルとなってしまい、事件・事故の再発につながっているのではないだろうか。

また、事件・事故の陰には顕在化しない多くの未事故（ヒヤリ･ハット）があるとされている。重大事故を未然に防止する観点からこれらの情報を収集することも必要と考える。

1.2　研究の目的

事件・事故、あるいは未事故の情報を収集した後、これを分析し、原因を洗い出し、再発につなげることが大切である。情報セキュリティの分野では、この分析手法や分析についての考え方が確立しておらず、このため、対策が表面的なものに留まっているのではないかと考えた。安心・安全な社会の構築のため分析手法の研究は不可欠と考え、本考察を行った。

2.　事件・事故の原因分析

2.1　事件・事故と安全

セキュリティ事件・事故とは、守るべき情報資産に対して「保護」が不十分で「コントロール」を失ってしまうことである。たとえば個人情報の漏洩は、暗号化や持ち出し管理などの「保護」が徹底されず、個人情報が本来アクセス権限の無い第三者が手にすることができる状態、つまり「コントロール」が失われた状態を指している。

セキュリティ対策を行っているにもかかわらず、事件・事故が発生するということは、「保護」つまり対策が不十分または誤っているということである。あるいは対策が立案時には適切であったが、環境変化に伴い有効なものではなくなってしまっていることも考えられる。完全に「安全」な状態というものは存在せず、常にリスクは存在している。「安全」とはリスクをその組織が受容可能なレベルまで下げられている状態のことである[2]。この状態を維持するためには、時とともに変化する環境から守るための「保護」の内容の見直しが必要である。

適切な対策を立案・実施し、事件・事故の発生を防止するには、自己及び他の組織で発生している事例の原因分析が欠かせない。原因の区分や分析手法を工夫し、様々な切り口で分析することにより有効な対策をとることが出来、「安全」な状態を目指すことができる。

2.2　分析の必要性

原因分析については、情報セキュリティ以外の分野にも視野を広げて、分析の必要性と、考え方について考察する。

Vol.2010-DPS-142 No.45
Vol.2010-CSEC-48 No.45
2010/3/5

システムが自動化、複雑化し、セキュリティ対策についてもさまざまな防護策がとられる傾向にあるが、このため担当者がすべてを把握することが困難となってしまい、システムが不透明になってしまう場合がある[3]。

旧ソ連のチェルノブイリ原発事故に関して IAEA の事務局長ハンス・ブリック氏は「安全は、潜在的危機を認識している者によって担当されて、はじめてかろうじて保てるのであり、安全だと思い込んでいる者が担当すれば危険が高まる」と述べている[4]。

また、六本木ヒルズの回転ドアによる男児死亡事故は、メーカーの経営破たんなどの中で、「回転ドアは衝突力の低減のため軽量化しなければならない」という知識が技術者間で引き継ぐことが行われず、見栄えや耐風圧のため重量化が進んだ結果起きたとされる[5]。

情報セキュリティの分野においても、システムの複雑化や、複数の人間が介在することによりどこに問題点があるのかがわかりにくくなりがちである。このような状態では原因分析が不十分となり、結果的に表面的な対策をとることしかできなくなってしまう傾向にあるのではないだろうか。これらのことから、事件・事故の再発を防ぐためには、原因分析を十分に行い、原因を突き止めてこれに対する対策を行うことが重要であると考える。

2.3 分析における考え方

事件・事故の分析手法の考察に先立ち、事件・事故を引き起こす最大の要因について理解を深める必要がある。この最大の要因とは「人間」であると考える。先述の個人情報の漏洩においても、暗号化や持ち出し管理などの「保護」が徹底されないのは、何らかの形で人間が介在した結果発生していると考えられるからである。逆に漏洩から守ることについても人間が介在していることは言うまでもない。

つまり、人間の特性を理解することが、原因分析には欠かせない。人間はその特性として、

- 注意は持続できない
- 記憶は永続的でない(忘却する)
- 記憶は変容する
- 外部環境の影響を受ける
- 心理的環境の影響を受ける

など、完璧とはいえないものを持っている[6]。

事件・事故が起きたとき、これを人間が引き起こしたものとして、ヒューマンエラーが原因とされる場合がある。ヒューマンエラーは、人間が本来持っている特性と人間を取り巻く広義の「環境」がうまく合致していないために引き起こされるものである。つまり、ヒューマンエラーは原因ではなく「結果」であり[6]、その「原因」を探ることが再発防止には必要である。ヒューマンエラーを「原因」としている限り、真の原因に対する対策はとることが出来ず、その事件・事故は再発する可能性が高いと考える。つまり、「人の過ち」が原因としている限り「過ちは繰り返される」可能性がある。再発を防止する仕組みを構築することが真の対策といえる。このためには、原因をヒューマンエラーに留めるのではなく、対策につながる原因の究明が必要であると考える。

3. 分析手法

本章では、分析手法についていくつか例を挙げて説明する。また、これらの分析手法についてその特性を考慮して、本稿で適用する手法を決定する。

3.1 分析手法例

原因分析手法の代表的なものとして「4M-4E」、「SHEL」「FTA」等のモデルがある[7][8]。

「4M-4E」モデルにおいて、4M とは「Man(人間)、Machine（機械）、Media（媒体）、Management（管理）」を意味している。4E とは 4M に対する対策をさし、Education（教育）、Engineering（工学）、Enforcement(強化・徹底)、Example(模範・事例)」を指す。「Environment(作業環境)」を加えて 5E とする場合もある。これらをマトリックスとして表に記載していくことにより、さまざまな視点からの分析を行う手法である。[7]

「SHEL」モデルは「Software,Hardware,Environment,Liveware(作業者と他者)」の 5 つの観点から要因分析を行い、評価するものである。これに「Management」を加えたモデルが「m-SHEL」モデルであり、交通やプラント等の事故分析に用いられている。さらに「Patient（患者）」を加えた「Pm-SHELL」モデルが医療分野において用いられている[8]。

「FTA」はフォルトツリー解析の略である。分析対象とする事故等の好ましくない結果を「頂上事象（top event）」として取り上げ、この事象が発生する為の条件と要因を把握する。そして、この頂上事象が発生する条件や要因をツリー状にして下位に展開し、分析する演繹的分析手法である [9] 。条件や要因の発生確率が得られている場合には、単純な理論式を用いて、上位の事象の発生確率を求めることができるが、一般的に発生確率を明確に示すことは困難であり、解析に関する知識がないと算定は難しいとされる。

また、ISMS などで用いられるリスクアセスメントの方法として、以下のものがあげられる [10] 。

・ベースラインアプローチ（Baseline Approach ）
あらかじめ一定の確保すべきセキュリティレベルを設定し、実装するのに必要な対

Vol.2010-DPS-142 No.45
Vol.2010-CSEC-48 No.45
2010/3/5

策を選択し、対象となるシステムに一律に適用することを指す。
・非形式的アプローチ（Informal Approach)
組織や担当者の経験や判断によってリスクを評価することを指す。
・詳細リスク分析（Detail Risk Analysis)
システムについて詳細なリスクアセスメントを行うアプローチで、情報資産に対し、「資産価値」 、「脅威」 、「ぜい弱性」 やセキュリティ要件を識別し、評価することを指す。
・組合せアプローチ（複合アプローチ）(Combined Approach)
複数のアプローチを併用し、それぞれのアブローチの長所短所を相互に補完し、作業の効率化や分析精度の向上を図る。

また、経済産業省「リスク定量化に関する検討資料」というリスク定量化の指針が出されているが、発生確率や対策係数等の想定を行う必要があり、これらが難しいため有効な結果を得ることは困難ではないかと考える。

3.2 分析手法の選択

次に、情報セキュリティ事件・事故の分析にはどのような手法がふさわしいかを考察した。分析にかけることの出来る「人」「時間」などのリソースは一般的に限られており、多数の分析の専門家が長時間かけて実施できるケースはあまり考えられない。現場の担当者が、比較的容易に分析作業を行えるものの方が受け入れられやすいのではないかと考えた。この点「FTA」や「リスク定量化に関する検討資料」による方法は、要素の発生確率の算出が難しいことや、ある程度は分析手法そのものを理解し、使いこなすための専門知識が必要であるため、今回は選択の対象外とした。

また、リスクアセスメントの各アプローチについては、リスクを分析する手法ではあるが、情報資産に対するリスクアセスメントに用いられるものであり、発生した事件・事故の原因分析にそのまま適用することは難しいと考えた。事件・事故の原因分析後、あるいは分析とは別に、本来の利用形態どおり、重要な資産のリスクアセスメントに用いるべき手法ととらえた。

今回分析手法として選択したのは、「Pm-SHELL」モデルの応用例である「Medical SAFER」というツールである。これは、自治医科大学医学部医療安全学教授である河野龍太郎氏が医療向けに開発した分析手法である。「Medical SAFER」においては時系列で事象を整理した後に「Pm-SHELL」の考えを用いて分析を行う。

「Medical SAFER」は現場担当者が自分達の手で事故分析を行えるように、分析に関する専門知識を持たなくとも実行できるように工夫されたものである。筆者は実際に「Medical SAFER」の講習会を医療従事者とともに受講し、その手順や注意点について学んだ[11]。

このことにより、ツールとしての「Medical SAFER」の扱いは容易であり、医療現場だけではなく、情報セキュリティの現場においてもその導入により有効な結果が得られるのではないかとの感触を得ることができた。

また、「Medical SAFER」においては、分析の専門家が現場のヒアリングなどから分析を行うのではなく、現場の関係者が参加して分析作業を行う。このことにより、現場の関係者自身が、何が問題であったのかを深く理解することができ、結果として得られた再発防止としての対応策が、より現場で有効なものとなる期待できる。また、結果としてあがる対応策に対し、自分たちが参加して決めたものという意識が醸成され、上位、あるいは施策の決定組織で決められた対策を行うことに比較して、対応策の実施に現場の協力が期待できると考えた。

4. 分析手法の適用

本章では、情報セキュリティ事件・事故の事例に分析手法を適用した流れについて具体的に述べる。

4.1 手順の確認

本項では、「Medical SAFER」の主な手順についてあげる。
・手順 1： ヒューマンファクターの考え方の理解
注意力が持続しない、類似事項の見間違えを起こす、などは、人間に共通した特性である。まわりの状況がこうした人間の特性に合っていないとヒューマンエラーが引き起こされてしまう。つまり、ヒューマンエラーは原因ではなく、結果であるということを理解する。
・手順 2： 時系列図の作成（事象整理）
何が、どのように起こったのかを時系列に整理、事象の流れ、全体像を把握する。
・手順 3： 問題点の抽出
時系列図を眺め、問題のある行動や通常とは異なる事象を探す。最終的にエラーが発生した点のみだけではなく､途中の過程でも問題であると思われるものを探し出す。
・手順 4： 背後要因図の作成（背後要因を探索）
手順 3 で抽出した問題点がなぜ起こったのか、どのように誘発されたのかを探り図式化する 。
・手順 5： 考えられる対策の列挙
事象の再発防止につなげるため、手順 4 で探った背後要因の連鎖を断ち切るための対策をあげる。対策を多面的に考えるヒントとして、エラー低減のためのガイドライン「GUIDE」を提案している。できるだけ個人の能力に頼らず、周囲環境を変えるような発生防止対策が立てられないかという点から検討をする。また､「エラーの発生を防止する対策」や「エラーの拡大を防止する対策」など多重的に対策をとることも心がける。（図 1　GUIDE[2]）

Vol.2010-DPS-142 No.45
Vol.2010-CSEC-48 No.45
2010/3/5

・手順 6： 対策の優先順位付け
手順 5 で列挙した対策案を評価し、優先順位付けし、実施する対策を決定する。対策を実施することによるエラー防止効果の度合いや、対策をとることによって新たに生じるかもしれないリスクも考慮して検討する。
・手順 7： 対策の実施
誰が、いつまでにどう実施するかを明確にし、対策を実施する。
・手順 8： 実施した対策の評価
対策が的確に実施されたか、再発防止に有効であったかを副作用も含め、評価する。

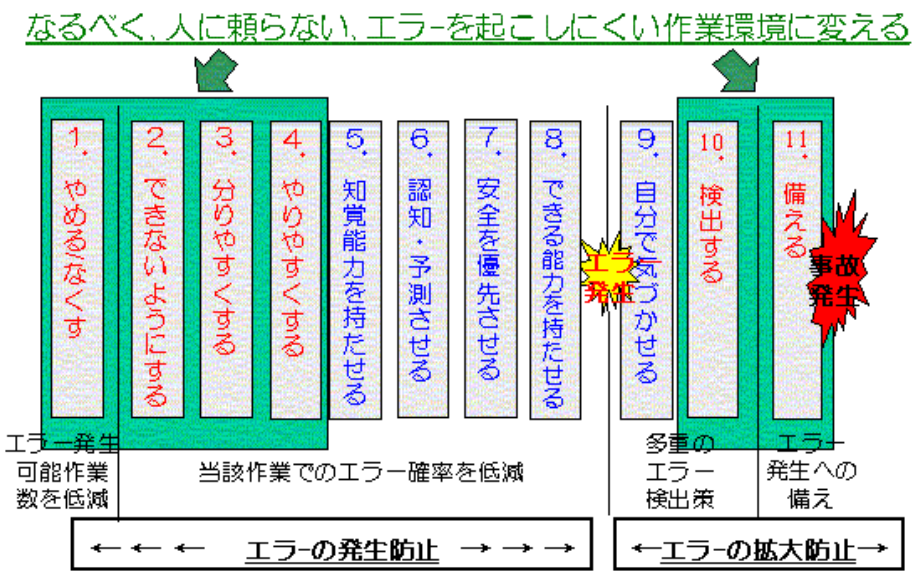

図 1 GUIDE[2]

4.2 実例への適用

本項では分析手順の適用について述べる。先述の「Medical SAFER」について、情報セキュリティ事故への適用を行った。今回は手順 2～7 までを行い、情報セキュリティ事件・事故への適用性を確認した。

対象事例として、2003 年に発生した「大阪府庁内ネットワークのコンピュータウイルスによるネットワーク障害」を取り上げて適用を試みた。本事例は、2003 年 8 月 19 日に大阪府の庁内ネットワークにおいて、コンピュータウイルス（ウェルチア）の感染が広がるとともに、感染した PC より送出される大量のパケットにより、ネットワーク障害が発生したものである。ウイルスの感染/非感染の確認と駆除作業を徹底して行う必要が発生し、約 8,000 台の PC が 2 日間利用できず、3 日目に半数が復旧、完全復旧は障害発生から 5 日後になったとされる。なお、大阪府の平成１５年９月定例会総務常任委員会議事録[12]を参照して分析を行った。

手順 2 の時系列図作成においてはプレイヤーの明確化を行った上で、発生した事象を書き出し時系列に並べた。事象の関連付けについて矢印を用いて表現した。これらの作業により個々の事象から全体の流れを整理することができた。(図 2 時系列図)

手順 3 では手順 2 で作成した時系列図上で事故につながったと思われる事象を、他の事象との関係にも注目して選び出した。 (図 2 時系列図：着色部分)

手順 4 では手順 3 で選んだ問題点の中から特に重要なものを選び出し、これに至る事象や、その背後にある要因を推定し、さらにその要因はといったように洗い出して書き出した。これらを、階層構造を意識しながら関係付け矢印にて図に表した。この際、当事者の立場になって考えることが重要とされている。行動や判断に至る背後要因が当事者の意識により異なる場合があるからである。今回は「職員」の行動に関係する箇所が多くあり、「職員」の立場で考えることが求められた。(図 3 背後要因図)

手順 5 では背後要因図のツリー構造をいずれかの箇所で断ち切り、重要な問題の発生を防止することを主眼に要因の対策案を考えた。この際には対策案が費用面等で現実的かどうかや、具体的・詳細な対策内容まで考慮することはせず、思いつくものを列挙していった。また、流れの中心部分にとらわれることなく、問題に至るいずれかの要素を排除すれば、問題の発生は防ぐことができるとの考えに立ち、対策案をあげた。たとえば職員がパターンファイル更新の不十分な PC を庁内ネットワークに接続したとしても、通信ができない仕組みとなっていれば、「不正パケットをばら撒く」という問題は発生しないことになる。このため、パッチファイル未適用、パターンファイル更新不十分な PC の庁内ネットワーク接続、通信の禁止などをあげた。

手順 6 では手順 5 で挙げた対策案を評価した。背後要因、対策案を表としてまとめた上で、GUIDE（図 1 GUIDE[2]）の観点で分類、効果点を評価し、有効な対策案を洗い出した。ツール内で予め設定されている配点を検討し、結果的にはそのまま採用した。効果の配点は以下（表 3 効果（点）一覧）のとおりである。

Vol.2010-DPS-142 No.45
Vol.2010-CSEC-48 No.45
2010/3/5

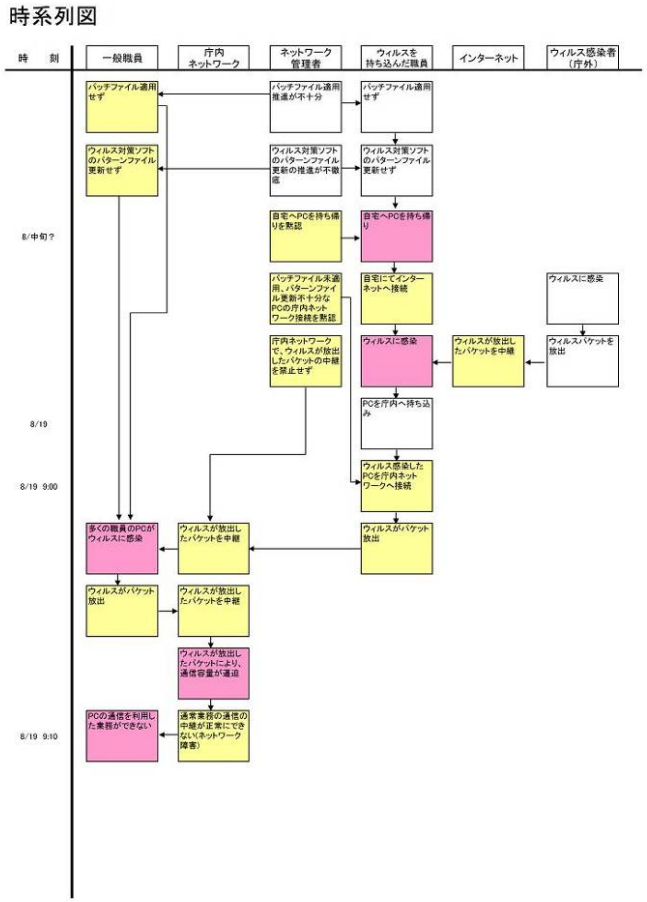

図 2　時系列図

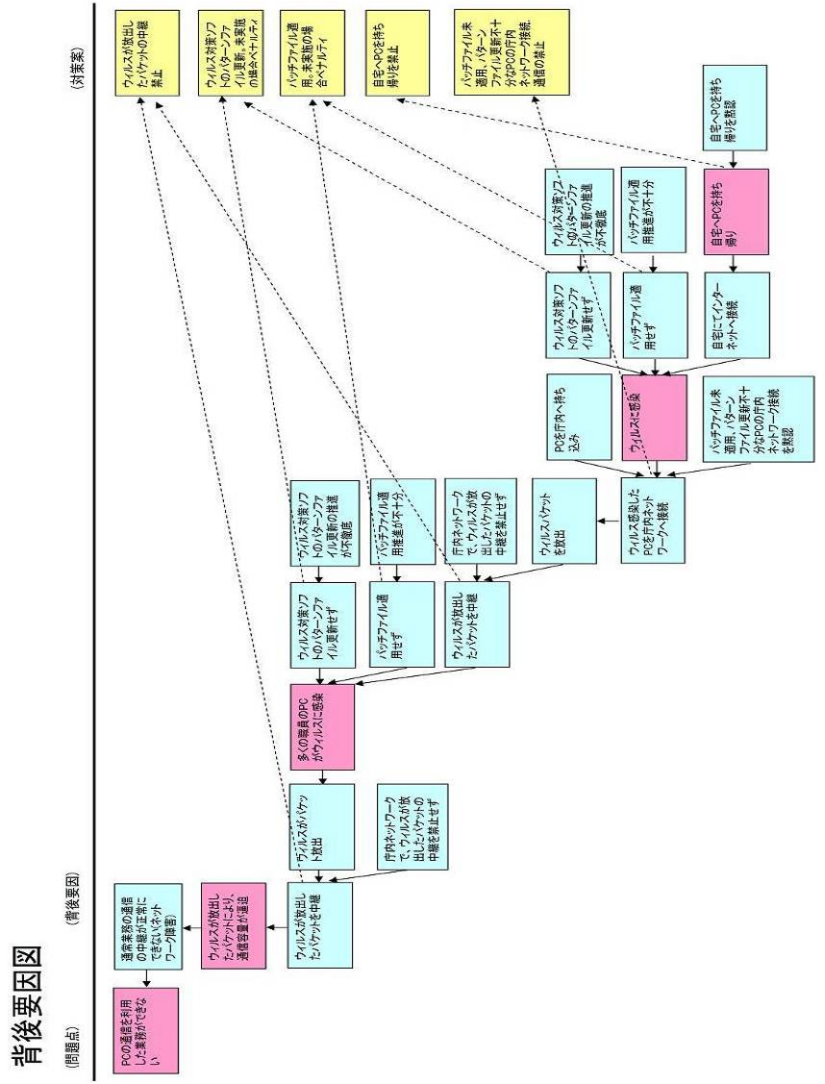

図 3　背後要因図

Vol.2010-DPS-142 No.45
Vol.2010-CSEC-48 No.45
2010/3/5

表 3　効果（点）一覧

効果（点）	GUIDE
10	やめる
	なくす
8	できないようにする
4	わかりやすくする
	やりやすくする
2	検出する
	備える
1	知覚能力を持たせる
	認知・予測させる
	安全を優先させる
	できる能力を持たせる
	自分で気づかせる

また、対策案実施時の「残留リスク」や「その他懸念事項」についても検討し、表に記載した。（表 4　対策決定・効果評価）

手順 7 では、「誰が」「いつまでに実施するか」を明確にし、対策を実行するフェーズである。今回は事例なので、実際に対策を実行することは出来ないが、「誰が」「いつまでに」と「採用／非採用」について想定して表にまとめた。(表 4　対策決定・効果評価)

4.3　適用結果

分析の流れと得られた結果を前項にて述べた。本項では「表 4　対策決定・効果評価」を参照しながら、得られた結果についてまとめる。対策案として挙げたものについて効果点を割り振ったが、これは、GUIDE に沿って人間の特性を考慮し、実施した場合の有効性に応じて配点されるようになっている。表中の No.2～4 は、利用者である各職員の心がけて頼るところが大きく、人間の特性上、もれなく完全に行うことは難しいとして、効果はあまり期待できないとし、点数は低くなっている。No.1 および No.5 についてはネットワーク上にシステム（仕組み）を作って自動的に制御を行い、利用者が禁止行為を行おうとしてもこれが無効となるようにするものであり、仕組みとして「できないようにする」ものであるため、効果が期待でき、したがって点数も高くなっている。点数の高いものから優先して対策を実施していくべきではあるが、実際の対策導入に際しては、システムの構築に時間がかかる場合もあり、導入までのリードタイムや、費用対効果の面についても検討を行う必要がある。

表 4　対策決定・効果評価

NO	背後要因	対策案	効果点 GUIDE	効果点 点数	残留リスク	その他懸念事項	採用	いつまでに	誰が実施する
1	ウィルスが放出したパケットを中継	ウィルスが放出したパケットの中継禁止	②できないようにする	8	中継を禁止するネットワーク機器(システム)の設定更新もれ	システム導入・運用費用	△	次年度	ネットワーク管理者
2	ウィルス対策ソフトのパターンファイル更新せず	ウィルス対策ソフトのパターンファイル更新。未実施の場合ペナルティ	⑨安全を優先させる	1	個人の意識に依存 自動更新設定を行っても解除される可能性あり	ペナルティ内容の検討	○	即時	各職員 (PC利用者)
3	パッチファイル適用せず	パッチファイル適用。未実施の場合ペナルティ	⑨安全を優先させる	1	個人の意識に依存 自動更新設定を行っても解除される可能性あり	ペナルティ内容の検討	○	即時	各職員 (PC利用者)
4	自宅へPCを持ち帰り	自宅へPCを持ち帰りを禁止	⑨安全を優先させる	1	個人の意識に依存	ペナルティ内容の検討 持ち物検査の実施可否検討	○	即時	各職員 (PC利用者)
5	ウィルス感染したPCを庁内ネットワークへ接続	パッチファイル未適用、パターンファイル更新不十分なPCの庁内ネットワーク接続,通信の禁止	②できないようにする	8	パッチファイル、パターンファイル情報の更新もれ 適用時にシステムに影響の出るパッチファイルの検討	システム導入・運用費用	○	次年度	ネットワーク管理者

4.4　実際の対策との比較

分析にて得られた結果と、実際に大阪府内で対策として検討（予定）された内容について比較を行う。（表 5　対策比較）[12]

表 5　対策比較

大阪府	Medical SAFER
・パッチファイルの速やかな適用 ・重要なシステムについて、バックアップ回線の準備 ・ウイルス感染時の復旧マニュアル整備 ・職員遵守事項の作成と周知 ・職員への情報セキュリティ意識の指導啓発 ・情報セキュリティ監査の実施	・ウイルスが放出したパケットの中継禁止 ・ウイルス対策ソフトのパターンファイル　更新。未実施の場合ペナルティ ・パッチファイル適用。未実施の場合ペナルティ ・自宅へ PC の持ち帰りを禁止 ・パッチファイル未適用、パターンファイル更新不十分な PC の庁内ネットワーク接続,通信の禁止

大阪府の対策は、人間の意識改善に負うものが中心で、有効性は低く留まるのではないか考える。「Medical SAFER」を用いた分析結果のほうが、より現場で起きたであろう事象を深く捉えて、有効な対策を挙げることができたと考える。

なお、委員会は事故発生の約 2 ヵ月後に開催されていることから、大阪府としては事故後の対策について既に検討を行った後であったのではないかと推測する。

Vol.2010-DPS-142 No.45
Vol.2010-CSEC-48 No.45
2010/3/5

5. まとめ

5.1 分析手法の評価

前章において、情報セキュリティ事件・事故について、実例を挙げて分析手法を適用した。「Medical SAFER」を適用した感想としては、分析の一連の流れを確認し、原因の分析、対策案の立案やその評価についても無理なく適用できたと思う。また、得られた対応策は、実際に事故発生団体で検討（予定）されたものと比較して劣らず、より深い原因をとらえて、これに対する対策案を挙げることができ、有効性も高いものが得られたと考える。「Medical SAFER」は、医療分野という情報セキュリティとは別分野で利用されているツールではあるが、情報セキュリティ事件・事故にまったく問題なく適用できるばかりか、非常に有効な結果が得られたと考える。

今回取り上げた事故事例は、事故の経緯が比較的公開されているが、それでも感染ルートや庁内ネットワーク環境、職員の意識など、詳細については推測に頼る部分も多かった。分析の材料としてはより多くの情報を得られたほうが、より有効な対策案につながると感じた。また事故の当事者である人間の行動や判断に至る心理的な要因にもう少し切り込むと、より一層有効な対策が得られるのではないかとの手ごたえもあった。これらのことから「Medical SAFER」は分析に関する特殊な知識も不要であるため、現場の事故関係者が利用することにより、より有効な分析が行えるのではないかと考える。また、今後多くの方々の検証により、問題点があれば顕在化させていただければと思う。

5.2 今後の課題

今回は手順 7 の対策案実施の直前までを対象として作業行った。事例への適用なのでこれ以降の作業はできないが、実際に事故の当事者である組織において、該当組織のメンバーが適用を行い、手順 7 の後半（対策の実施）、手順 8（実施した対策の評価）まで実施できれば、ツール適用の有効性がさらに評価できると考える。

本事例においては、ツールによる分析作業を筆者個人で行った。参加した医療関係者向けの講習会では、複数（5～6 名）のメンバーによりブレーンストーミング的に要因の分析を進めることにより、比較的短時間で多くの見解と有効な対応策が挙げられていたと感じた。これらのことから、事象や背後要因の分析、対策案の洗い出しは、複数人で行うほうがより短時間で内容も充実したものが得られると思われる。実際の事故分析においては、関係部門から発生現場の状況に明るいメンバーを集めて分析を行うことが有効と考える。

今回は事例として大阪府の一件だけを取り上げたが、多くの情報セキュリティ事件・事故について分析を行うことも重要ではないかと考える。医療関係者向けの「Medical SAFER」をそのまま利用したが、「Medical SAFER」自体が医療に特化した内容がほとんどないため、問題なく利用できた。しかし、多くの情報セキュリティ事件・事故の事例を分析することにより、事件･事故と原因分析、有効な対応策の関係がパターンとして浮き彫りになるようになれば、さらに分析を効率化することや、対策の横展開することに効果が発揮されるのではないかと期待する。パターンが明らかになるように数多くの事例を扱うことも今後の課題として挙げる。

また、「ヒューマンエラー」の分析手法や対策についての研究は、交通事故や医療事故など、情報セキュリティ以外の分野において研究が進んでいることが書籍等の調査や研修への参加から知ることができた。今回取り上げなかった分析手法や考え方についても、情報セキュリティ事件・事故への適用に有効なものがあるかもしれない。情報セキュリティの事件・事故の再発、未然防止に役立つツールとして、他の手法の応用についても今後の課題としたい。

参考文献

1) 情報セキュリティ大学院大学内田研究室「第 6 回情報セキュリティ調査」 (2009)
2) 河野龍太郎: ヒューマンエラーを防ぐ技術,日本能率マネジメントセンター (2006)
3) James Reason: ヒューマンエラー　ー認知科学的アプローチー,海文堂出版 (1994)
4) 宮城雅子: 大事故の予兆を探る,講談社 (1998)
5) 畑村洋太郎: 失敗学実践講座,講談社 (2006)
6) 河野龍太郎: 医療におけるヒューマンエラー,医学書院 (2004)
7) (財)原子力安全技術センター: IINET システム,http://www.n-iinet.ne.jp/4m5e.htm
8) 小林泰典: Ｐ２Ｐソフトウェアのウイルス感染についてのインシデント分析」情報セキュリティ大学院大学　修士論文 (2008)
9) 中小企業基盤整備機構: 中小企業向け化学物質のリスクアセスメントテキスト,http://www.smrj.go.jp/keiei2/kankyo/h11/book/3rab/html/kagaku1l.htm
10) 日本情報処理会開発協会（JIPDEC）: ISMS ユーザーズガイド,http://www.isms.jipdec.jp/doc/uguide/00top.pdf
11) 河野龍太郎: ヒューマンエラー防止セミナー,株式会社テプコシステムズ
12) 大阪府: 平成１５年９月定例会総務常任委員会お知らせ,http://search.pref.osaka.jp/gikai/discuss/cgi-bin/WWWdispNitteiunit.exe?A=dispNitteiunit&RA=frameNittei&USR=webusr&PWD=&XM=000000000000000&L=1&S=16&Y=%95%BD%90%AC15%94N&B=-1&T=-1&T0=-1&O=-1&P1=&P2=&P3=&P=1&K=380&N=8653&H=1202629&W1=&W2=&W3=&W4=>