

組織の事業継続性向上に資する情報セキュリティリスク分析手法の提案

頼永 忍†

原田 要之助‡

†株式会社インターリスク総研
101-0062 東京都千代田区神田駿河台 4-2-5
shinobu.yorinaga@ms-ad-hd.com

‡情報セキュリティ大学院大学
221-0835 神奈川県横浜市神奈川区鶴屋町 2-14-1
yo-harada@iisec.ac.jp

あらまし ISMS適合性評価制度が日本で開始して10年が経過し、「情報セキュリティマネジメントシステム」という言葉も広く一般に浸透してきた。その一方で、本来情報セキュリティマネジメントはCIA(機密性・完全性・可用性)を対象としているが、現実には機密性が偏重(可用性を軽視)されたマネジメントが推進されてきている。2011年3月11日に発生した東日本大震災では、津波などにより情報資産の可用性が喪失し、組織の事業継続性を脅かす事態が多数発生した。情報セキュリティの取り組みは事業が継続してこそ成立するものであり、可用性の確保は今後情報セキュリティマネジメントでも重要視されるべきである。本稿ではそのためのリスク分析手法を提案する。

Proposal for Information Security Risk Analysis Method

Submission for Improving Organization Business Continuity

Shinobu Yorinaga†

Yonosuke Harada‡

†Consulting Department 2, InterRisk Research Institute & Consulting, Inc.
4-2-5, Kanda Surugadai, Chiyoda-ku, Tokyo 101-0062, JAPAN
Shinobu.yorinaga@ms-ad-hd.com

‡Institute of Information Security
2-14-1 Tsuruya-Cho Kanagawa-ku, Yokohama-City, Kanagawa, 221-0835 JAPAN
yo-harada@iisec.ac.jp

Abstract Ten years has passed since the ISMS certification initiated in Japan. A term "Information Security" has widely spread and used. However, the "confidentiality" of Information Security has been more focused than "availability" in Japan, due to Privacy Protection Law. In Tohoku Region Pacific Coast Earthquake in 2011, most of the IT in that region has stopped and swept away by tsunami. IT availability as well as business continuity has all lost. For ISMS, most organization has implemented less attention on "availability" which we should revisit its importance again. In this thesis, we propose new risk analysis methodology combined BIA and MTPD to ensure both confidentiality and availability for protecting information asset and its business process.

1 はじめに・研究の背景

日本におけるISMS(情報セキュリティマネジメントシステム)認証評価制度が立ち上がって10年が経過したところである。

その間、2005年10月にISMSの認証基準ISO/IEC 27001:2005が国際標準となったこともあり認証組織数の増加は加速し、その認証組織数は2011年8月現在3862事業所で世界トップである。(全世界では7279事業所)

ISMSは情報資産のCIA(機密性・可用性・完全性)を管理するマネジメントシステムである[1]が、2011年に発生した東日本大震災では情報資産の「可用性」を直撃し、多くの情報が失われた。情報の喪失は、その情報を利用している業務の継続性の喪失と直結する。多くの組織で重要な業務の情報が失われ、事業継続に多大なダメージを受けた。

ISMSに限らず、組織のいかなる取り組みも事業継続が前提であり、事業継続が脅かされるリスクは確実に管理しなければならない。

情報セキュリティマネジメントは、これまでの取り組みが機密性に偏りすぎたことで組織が最優先に考えなければならない「事業継続」に関するリスクを見過ごしていた、あるいは逆に増加させていたのではないかと、言う疑問を持つに至った。

これを解決する為、ISMSのフレームワークの問題点を指摘、その改善を提案すると共に、情報資産の可用性リスクを適切に評価し、情報セキュリティマネジメントの組織の事業継続性を高めるアプローチを提案する。

2 日本における情報セキュリティマネジメントの現状

2.1 機密性の重視

ISO/IEC 27001:2005[2]では、「セキュリティ障害に起因すると予想される、組織における事業的影響のアセスメントを行う。このアセスメントでは、その資産の機密性、完全性又は可用性

の喪失の結果を考慮する。」と述べられている。

しかしながら、日本における情報セキュリティマネジメントの取り組みは、機密性を重視して運用されてきた。その理由として、2007年の個人情報保護法完全施行後、多発する個人情報漏洩、Winnyを媒介としたワームなどによる情報流出事故などが発生し、機密性の確保とその管理が社会的コンセンサスとなったことが挙げられる。

各種調査においても、機密性毀損リスクの顕在化(主として情報漏洩)に特化したものが多く、公的機関によるガイドライン、研修資料等においても、機密性低減に向けた対策がほとんどであり、完全性、可用性の観点の対策例にはあまり触れられていない。[3]

これらの理由により、事実上日本の情報セキュリティマネジメントでは「セキュリティリスク対応 = 機密性確保」の構造になっている。

2.2 可用性の軽視

2.2.1 リスク定量化の必要性和提供された基準

ISO/IEC 27001:2005には「選択するリスクアセスメントの方法は、それを用いたリスクアセスメントが、比較可能で、かつ、再現可能な結果を生み出すことを確実にしなければならない。」とある。リスクを比較可能にするために必要な取り組みは何より定量化であり、ISMSを実施するトップマネジメントが求める定量化とは多くの場合「金銭的価値への換算」である。

すなわち、リスクが顕在化したときに想定される被害がどの程度なのかは、リスクへの対応コストをどこまでかけるべきかというコストパフォーマンスの問題として理解されていると言えよう。

例えば、「金銭的価値への換算」の例として2004年のISPからの個人情報漏洩事件での見舞金「500円」が挙げられる。

この事件以後、同様の漏洩事件ではここで用いられた「1件あたり500円」という慣例が定着

している[4]。

個人情報保護(機密性毀損リスクの過剰反応[5])と、そのリスクの金銭的価値への容易な可換性により、機密性のリスクが優先的に評価、対応され、逆に毀損時のリスク定量化が困難な完全性や可用性のリスクは重要視されなくなったと考えられる。

2.2.2 評価基準の不在

可用性のリスクアセスメントが重要視されないもう一つの理由に、評価基準の不在があると考えられる。具体的には、ISMSを導入している多くの企業が参考になっている JIPDEC 発行の ISMS ユーザーズガイド[6]には、機密性の評価基準は詳述されているものの、完全性及び可用性の評価基準が記載されていない。

それだけでなく、情報資産における「完全性が十分に確保された状態」「可用性が十分に確保された状態」を例示したセキュリティ関連の資料や解説書がほとんど存在しないため、そもそも情報資産が完全性及び可用性を十分に担保できている状態、あるいはそれが毀損された際の影響の理解が一般に浸透していない。そのため誤った理解(機密性の評価基準を他の要素に当てはめただけ)で完全性や可用性が評価される、あるいは世間の風潮を「反映」し、機密性に偏った対策のみが行われるなどの問題が起きている。

3 東日本大震災により顕在化した問題

3.1 情報の滅失による事業基盤の喪失(可用性毀損リスクの顕在化)

東日本大震災(以下「本震災」という)は、宮城県名取市付近で 5km 以上内陸まで津波が押し寄せるなど、太平洋沿岸地域を中心として大きな被害をもたらした。本震災における被害の特徴は、広域にわたる津波被害であり、これは 1995 年の阪神淡路大震災、2004 年の中越地震、2007 年の中越沖地震でも見られず、津波によ

る顕著な被害については 1993 年の北海道南西沖地震まで遡るが、本震災ほどの広域に渡った津波被害は近年例がない。

本大震災において大きく報道された問題の一つが、「宮城県南三陸町における戸籍情報の部分滅失」である。庁舎に電子保存していた戸籍データが津波で流失したものの、同県気仙沼市の仙台法務局気仙沼支局で保存していた複本を元にロールバック、4 月 25 日に復元が完了した事象である。[7]

戸籍データは、戸籍法施行規則第十五条により、月次で法務局へ複本を保存することになっており、そのため、1 月下旬から 3 月 11 日までの戸籍申請情報が滅失し、再申請の呼びかけが行われ、現在も継続中である。

本事象は戸籍法から検討する必要があるため、ここでは深く考察することは避ける。ただし可用性の重要性を示す事象として有用である。

3.2 可用性リスクと事業継続性への影響

東日本大震災で発生した津波による情報滅失は、無権限者に閲覧可能な状態をもたらす事象とはならず、機密性リスクが問題となったわけではなかった。本事象では、「情報が使えなくなる、情報にアクセスできなくなる」という可用性リスクが顕在化した。業務は必要なリソースが欠けるとその遂行が出来なくなる。リソースには当然情報資産も含むが、仮に情報資産の機密性が保たれていたとしても、その可用性が失われれば、その情報を利用している業務の継続、業務の重要度によっては企業の存続が行えなくなり、結果情報セキュリティに限らないあらゆるマネジメントが無力化する。激甚被災地ではそのようなケースが数多くあったと考えられる。

情報セキュリティにおいてスコープに入れるべき可用性要素がなおざりになっていたことによって、組織に大きな「セキュリティ事象」が発生し、その一部は事業継続上大きな影響が出たことは、本震災からの教訓として確実に認識をする必要がある。

4 震災を経た新しい情報セキュリティの形

4.1 機密性評価と可用性評価の違い

ISMS のリスクアセスメントは、一般的に「リスクの特定」「リスクの分析・評価」「リスク対応」「リスク受容」の順に行われていく。この過程で、リスク対応を決定する際に、組織は目指すべきセキュリティのレベルを設定する。[2]ここで機密性と可用性ではアプローチが異なっている。

4.1.1 機密性

機密性を担保する場合、まず特定した情報資産の情報の識別を決定する(「公開」、「社外秘」、「極秘」などにレベル分けする)。次にその情報資産が現在管理されている状況と情報の識別に対応した望ましい管理レベルとのギャップを分析し、差がある場合はギャップを埋めるべく対策(アクセスコントロール)を行うことが一般的である。

4.1.2 可用性

一方、可用性については、機密性と同様なアプローチを取ることが難しい。

可用性についても機密性と同様に、「組織として確保すべき可用性」のレベルを定義し、そのベースラインに向けてリスク対応を行うことになる。では、その「組織として確保すべき可用性」をどのように決定するか、が重要となる。

「可用性」とは、「利用が許されたエンティティが使いたいときに使えること」であり、その評価基準は「どの程度の時間、利用できなくても経営に影響しないか」である。すなわち、「情報利用の許容中断時間」はその情報が用いられている業務の中断時間に関係してくる。機密性が、その情報自体が持つ価値、特性に関係するのに対し、可用性はその情報を用いる「業務」の重要度が評価に密接に関係してくるのである。

4.1.2.1 情報資産管理時の問題

ISMS などでも多く用いられてきた情報資産台帳は、情報資産とそれを用いる業務とが関連づけられていない(例を表 1 に示す)。「業務との関連付け」については ISO/IEC 27001:2005 にも明確に要求されておらず(4.2.1 d)、情報資産の可用性評価に対する規格要求事項が不足しており、何らかの形で補完する必要がある。

表 1 情報資産管理台帳例

情報資産管理台帳									
部門名								作成日	
								作成者	
番号	書名・データ名	管理責任者	保管責任者	形式・保管場所			保管期間		個人情報を含む
				紙	電子データ				
				サーバー/クライアント	媒体	紙	電子データ		

4.1.2.2 リスク評価基準の問題

ISMS ユーザーズガイドでは、情報セキュリティにおけるリスク値を

「資産価値 × 脅威(起こりやすさ) × 脆弱性(起こった際のインパクト)」

により算出し、リスクの大きさの判定、及びリスク対応の優先度を決定する。しかし、この算出方法では今般発生した本震災のような、いわゆる未曾有の大災害に対しては、「起こりやすさ」が極小となり、算出されるリスク値が過小評価される。そのため、可用性リスクの評価については、既存のリスク評価方法を当てはめることが妥当ではなく、新しい評価手法を導入する必要がある。

5 事業継続性を高めるリスク評価手法の提案

5.1 可用性評価手法の改善

情報セキュリティの事業継続性を高めるためには可用性評価手法の改善が不可欠である。

情報セキュリティマネジメントに事業継続マネジメントの概念を導入し、ISMS のリスク評価手法を拡張することが必要である。

5.2 リスク評価への時間の概念の導入

可用性リスクの評価で最も重要な要素は「時間」である。

英国の BCM 専門家グループ、BCI が作成した Good Practice Guideline 2008[8]ではリスクマネジメントと事業継続マネジメントの違いの一つに「Key Parameters」を挙げている。(表 2 参照)

表 2 RM と BCM の違い(GPG2008 抜粋)

	Risk Management	Business Continuity Management
Key Method	Risk Analysis	Business Impact Analysis
Key Parameters	Impact & Probability	Impact & Time
Type of incident	All types of events – though usually segmented	Events causing significant business disruption

この中で、リスクマネジメントではインパクトと発生頻度で評価するのに対し、事業継続マネジメントではインパクトと中断時間で評価としている。そこで事業継続性を確保するために管理すべき時間的要素として「最大許容停止時間¹ (MTPD: Maximum Tolerable Period of Disruption)」と目標復旧時間² (RTO: Recovery Time Objective)の 2 点をリスク評価に導入することを提案する。

5.3 ビジネスインパクト分析実施の提案

可用性は情報資産単体を評価しても決定されず、情報資産を利用している業務の重要度により決定されると前記した。業務の重要度を分析する際に用いられる手法の一つがビジネスインパクト分析(BIA)である。情報セキュリティのリスク評価の前段階として BIA を導入することを提案する。BIA では、企業にとっての重要な業務(主要な業務／事業継続に不可欠な業務)

¹ 組織が最大限許容できる業務中断の最長時間。これを超えて業務停止が継続していると、該当業務あるいは組織事業の継続に著しい影響を及ぼす可能性が高まる。

² 組織が目指す該当業務の復旧時間。一般的には MTPD より短くなる。該当業務のステークホルダー、競合他社等との関係などを勘案して決定する。

とそれを構成する業務リソース、最大許容停止時間、目標復旧時間の分析、決定を行い、業務重要性評価(優先度付け)を行う。この順序は主に「非常時にどの業務を優先するかを示す。BIA のサンプルを表 3 に示す。

表 3 BIA アウトプット例

部門	業務	関連部署	経営資源				影響評価				業務重要性評価	復旧時間	
			人	施設・設備	情報	インフラ	財務的影響	顧客への影響	社会的影響	合計		最大許容停止時間	目標復旧時間
〇〇部	〇〇業務	〇〇部	4名 A主任	Aサーバ	DB-A DB-C	電気	3	3	3	7	高	6hr	3hr
〇〇部	〇〇業務	なし	10名 H課長	Aサーバ	DB-B	電気	1	2	2	5	中	48hr	24hr
〇〇部	〇〇業務	〇〇部	7名 Mさん	Bサーバ	DB-D	電気	2	1	1	4	低	24hr	12hr
〇〇部	〇〇業務	なし	2名 C課長	Zサーバ 機械B	DB-B DB-Z	電気 水	1	3	3	7	高	12hr	6hr
***	***	***	***	***	***	***	***	***	***	***	***	***	***

5.4 情報資産管理台帳の拡張

BIA で特定した業務重要性評価を用いて情報資産の可用性を評価する。情報資産の可用性はそれと紐付いた業務の業務重要性評価に準じた値となる。

下表 4 の例では、「高 = 3」「中 = 2」「低 = 1」とした。

表 4 情報資産管理台帳改善例

情報資産分類	情報資産名	業務名	業務重要性評価(※)	情報管理責任者	保管場所	情報媒体	保管期間	C	A
データ	顧客情報データベース	リテール営業業務	高	営業部長	キャビネット	CD-D VD-B D	2013年度末	2	3
データ	〇〇	〇〇業務	中	〇〇部長	キャビネット	Aサーバ	2013年度末	1	2
データ	クレジットカード情報	支払業務	低	〇〇部長	キャビネット	Bサーバ	2013年度末	2	1

例えば、支払業務は、A は重視されないが C は高い。上記の分析からは C × A で考えると、顧客情報データベースが最重要となる。

5.5 脆弱性レベル基準の変更

リスク評価での変更点は、可用性評価における脆弱性レベルの基準を「災害などからの想定復旧時間の MTPD、RTO 達成度合い」にすることである。これにより、可用性リスクを定量的に把握することが出来、この結果、あとどの程

度復旧時間を短縮すれば良いのか(MTPD を満たすには後何時間、RTO を満たすには後何時間、というように)を個々の情報資産の重要度から具体的に判断し、対策に繋げることが可能となる。

可用性における脆弱性レベルは以下表 5 のようにすべきである。

表 5 可用性の脆弱性レベル改善例

脆弱性レベル	説明
5	現状の想定復旧時間が最大許容停止時間を満たしていない
2	現状の想定復旧時間が最大許容停止時間を満たすが、目標復旧時間を満たしていない
1	現状の想定復旧時間が目標復旧時間を満たす

想定復旧時間が MTPD を超過している状態は、災害などの際に組織の存続に多大な影響を及ぼす可能性がある状態であり、原則的に組織として許容してはならない。(表 6)。ここで示した脆弱性レベルの「5」は、「許容しない」ことを示す値である。一般的なリスクアセスメントでは、4.1.2.2 で示した計算式によるリスク値を元に、一定の値以下のリスクは自動的に受容(保有)するアプローチが採用されるが、情報資産の可用性が MTPD を満たさない状態が自動的に受容(保有)されないような値にするべきである。

表 6 リスクアセスメントシート例(抜粋)

資産名	資産価値	脅威シナリオ	脅威レベル	実施している対策(現状の状態)	脆弱性影響度	脆弱性レベル	リスク値	リスク対応
AAA	2	2	3	盗難	...	...	2	...
				地震	1	→	5	3 15
BBB	2	2	1	盗難	...	...	2	...
				地震	1	→	5	3 15

6 おわりに

本稿では、既存の情報セキュリティマネジメント(ISMS)の特徴と、それらがもたした脆弱性、2011 年の東日本大震災により露呈した問題点、課題を踏まえ、今後進んでいくべき情報セキュリティの方向性として、可用性を重視したアプローチが必要となることそのためのリスク評価方法とを提案した。本稿では、リスク分析、リスク評価の進め方とそれにより得られる効用について論じ、提案したが、今後、具体的なリスク対応

の内容、リスク対応の中での機密性と可用性とのバランスの取り方、機密性喪失がもたらす事業継続リスクの分析及び本アプローチとの統合など、さらに具体的なアプローチを検討し、提案して行きたいと考えている。

7 謝辞

本研究の実施にあたり、直接多くのご支援、ご助言を戴いた情報セキュリティ大学院大学情報セキュリティ研究科教授小柳和子先生に、深謝の意を表す。リスク評価に関する検討において多くのご助言を戴いた株式会社インターリスク総研研究開発部上席テクニカルアドバイザー飛嶋順子氏、並びに同社コンサルティング第一部上席テクニカルアドバイザー長井健人氏に感謝の意を表す。

参考文献

- [1] ISO, IEC, ISO/IEC 27002:2005, 2005
- [2] ISO, IEC, ISO/IEC 27001:2005, 2005
- [3] 情報処理推進機構, 5分でできる! 情報セキュリティポイント学習, 2009,
http://www.ipa.go.jp/security/vuln/5mins_point/105_themes.html
- [4] 日本ネットワークセキュリティ協会, 2010 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~, 2011
- [5] 田淵 義朗, 「場当たり個人情報」から「攻めの情報活用」へ / SAFETY JAPAN コラム, 2006 年 3 月 30 日,
<http://www.nikkeibp.co.jp/sj/2/column/c/12/>
- [6] 日本情報経済社会推進協会,
ISMS ユーザーズガイド-JIS Q
27001:2006(ISO/IEC27001:2005)対応—リスクマネジメント編—, 2008
- [7] 法務省, 東日本大震災により滅失した戸籍の再製データの作成完了について, 平成 23 年 4 月 26 日,
http://www.moj.go.jp/MINJI/minji04_00024.html
- [8] BCI, Good Practice Guideline 2008, 2008