情報処理学会論文誌 Vol.57 No.12 2743–2756 (Dec. 2016)

センサ活用に基づく情報セキュリティエコノミクス：ISMSにおける費用対効果の効率化に関する検討

米田 翔一[1,a)] 畑 健一郎[1] 下村 道夫[1] 谷本 茂明[1] 佐藤 周行[2] 金井 敦[3]

受付日 2016年3月8日, 採録日 2016年9月6日

概要：近年，インターネットが社会基盤として重要な位置づけとなるにつれ，サイバー犯罪の脅威もより大きなものとなってきている．それにともない，情報セキュリティの重要性もますます高まっている．これに対し，企業等の組織のセキュリティ指針として有効と考えられているのがISMS（Information Security Management System）である．ISMSでは，情報セキュリティに対する要求事項を達成するために，PDCAモデルを採用し，情報資産の機密性，可用性，完全性をバランス良く維持し，継続的な改善を行っていくものであるがその普及は十分でない．主な原因として，ISMSを導入したことによる効果が予測しにくい点，ISMSにおける管理項目数や作成するドキュメントが多すぎる点等があげられている．前者の課題に対し，情報処理推進機構（IPA）等では，情報セキュリティエコノミクスが提唱されており，セキュリティ対策に対する投資効果の構造解明の重要性が指摘されている．後者の課題に対しては，IoT（Internet of Things）に代表されるように，センサ技術は高精度化や小型化に加え，低価格化も進んできており，その活用が期待できる．本論文では，これらの背景の下，現状のISMS普及を妨げている主な要因であるコスト構造を費用対効果として明らかにする．さらに，ISMSにおける人的稼働要因をセンサの活用により，低減化を試みた結果について明らかにする．これらにより，ISMSの普及促進に寄与し，より安心安全なネットワーク運用に寄与する．

キーワード：情報セキュリティマネジメントシステム，センサ，情報セキュリティエコノミクス，費用対効果

Information Security Economics Based on Sensor Utilization: A Study of Cost Effectiveness Improvement by Sensor Utilization in Information Security Management System

Shoichi Yoneda[1,a)] Kenichirou Hata[1] Michio Shimomura[1]
Shigeaki Tanimoto[1] Hiroyuki Sato[2] Atsushi Kanai[3]

Received: March 8, 2016, Accepted: September 6, 2016

Abstract: In recent years, the Internet occupies the important position as infrastructure. On the other hand, it is thought ISMS (Information Security Management System) that it is effective as a security guideline of the organization of a company etc. In ISMS, in order to attain the requirements over an information security, the PDCA model is adopted. Thus, the confidentiality, availability, and integrity in information property are maintained with sufficient balance, and the continuous improvement is made. However, the spread of ISMS(s) in the present condition is not sufficient. As this main cause, the point that the ISMS introduction effect is indefinite, and the point with many ISMS control items are mentioned. Information Security economics is advocated for the former subject in Information-technology Promotion Agency (IPA). Thus, the importance about the structure probe of the investing effects of security countermeasures is pointed out. For the latter subject, utilization of sensor technology is expectable that it is represented by IoT (Internet of Things). In this paper, the cost structure probe of ISMS is clarified as cost effectiveness under these backgrounds. Furthermore, it clarifies about the cost reduction result of ISMS by sensor utilization. By the above-mentioned, it contributes to spreading and promotion of ISMS, and contributes to securer and safer network operation.

Keywords: information security management system, sensor, information security economics, cost effectiveness

1. はじめに

近年，インターネットの急激な進展につれ，サイバー犯罪の脅威もより大きなものとなってきている．それにともない，情報セキュリティの重要性もますます高まっている．これに対し，企業等の組織のセキュリティ指針として有効と考えられるのがISMS（Information Security Management System，情報セキュリティマネジメントシステム）である．ISMSとは，個別のセキュリティ対策に加え，組織のマネジメントとしてリスク評価を行い，必要なセキュリティレベルを定めてシステムを運用することである [1]．ISMSでは情報セキュリティに対する要求事項を達成するために，PDCAモデルを採用し情報資産の機密性，可用性，完全性をバランス良く維持し，継続的な改善を行っていくものである．ISMSを導入することで，情報セキュリティに関するリスクを軽減することが可能となるが，日本では，実際に導入することが難しい企業は少なくない [2], [3]．

ISMSの普及を妨げている主な原因は，警視庁が企業に対して行ったアンケートによると，情報セキュリティ対策実施上の問題点として，コストに関する要因があげられている [4]．また，ISMSを導入している企業に対し，情報セキュリティ大学院大学が行ったアンケート結果からは，ISMSにおける管理項目数や作成するドキュメントが多すぎると回答している [5]．

ここで，前者のコストに対する課題に対し，IPA等では，情報セキュリティエコノミクスが提唱されており，セキュリティ対策の投資効果の構造解明の重要性が指摘されている [6]．また，後者のISMSの管理稼働が多すぎる課題に対しては，IoT（Internet of Things）での利用，小型化，高精度化，高集積化が近年著しく進展している [7], [8]，センサ技術の活用による解決が考えられる．すなわち，センサ技術は，IoTやトリリオン・センサ等 [9] に代表されるように，M2Mシステムでの活用が注目されていることから，ISMSにおいても人的稼働の代替案としての活用が期待できる．

本論文では，これらの背景の下，現状のISMS普及を妨げている主な要因であるコスト構造解明の観点から，セキュリティエコノミクスに着目し，ISMSの費用対効果を机上シミュレーションにより導出する．さらに，ISMSの課題である管理面の多さに対し，その人的稼働要因をセンサの活用により，低減化を試みた結果について明らかにする．これらにより，ISMSの普及促進に寄与し，より安心安全なネットワーク運用に寄与する．

[1] 千葉工業大学大学
Chiba Institute of Technology, Narashino, Chiba 275–0016, Japan
[2] 東京大学
The University of Tokyo, Bunkyo, Tokyo 113–8658, Japan
[3] 法政大学
Hosei University, Koganei, Tokyo 184–8584, Japan
[a)] s1291015lb@s.chibakoudai.jp

2. ISMSの現状と課題

2.1 ISMSの現状

ISMSは，**図 1** に示すように，組織的人的管理，物理的技術的管理，組織的管理の3つの管理面から階層的に構成され，合計114の管理項目が規定されている [1]．

2.2 ISMSの課題

ISMSでは情報セキュリティに対する要求事項を達成するために，PDCAモデルを採用し，情報資産の機密性，可用性，完全性をバランス良く維持し，継続的な改善を行っていくものである．しかし，企業において，その普及は十分でない．この原因として，前述のように，警視庁が企業に対して行ったアンケートによると，情報セキュリティ対策実施上の問題点として，「費用対効果が見えない（59.6%）」，「コストがかかりすぎる（49.8%）」等，コストに関する要因があげられている [4]．このように，ISMSを導入したことによる効果が予測しにくい点があげられている．また，ISMSを導入している企業に対し，情報セキュリティ大学院大学が行ったアンケート結果では，4割強の企業がISMSにおける管理項目数や作成するドキュメントが多すぎると回答している [5]．

このように，企業がISMSを導入するためには，まだ不明確な点が多いことが分かる．また，情報セキュリティマネジメントシステムとして運用するには多くのコストと手間が発生するといわれており [10], [11], [12]，前述のセキュリティエコノミクスの観点からISMSにおける費用対効果を明らかにすることは，喫緊の課題である．

2.3 関連研究

(1) ISMSに関する研究

ISMSに関する研究としては，主にISMS導入に関する研究がほとんどである [13], [14], [15], [16], [17]，いずれもISMS認証を取得し，その継続に関わる課題とその解決策

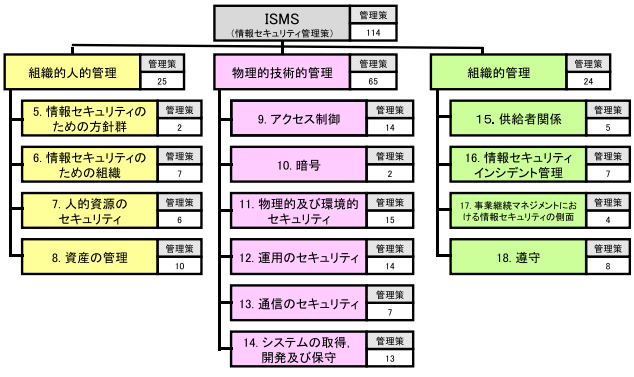

図 1 ISMSの全体構造
Fig. 1 Structure of ISMS.

としてのポリシ策定方法やマネジメントの在り方について述べられている．これらは，これからISMS認証を取得し，運用するために有効となるものであるが，いずれも費用面，効果面に関わる検討は，十分にはなされていない．特に，文献[17]では，ISMS認証取得組織に対するアンケート結果に関し，インタビューも交えて，認証取得のための体制から監査や教育に至るきめ細かい検討が行われているが，具体的な費用対効果面に関する検討はなされていない．

(2) 情報セキュリティエコノミクスに関する研究

情報セキュリティエコノミクスに関する研究は，前述のように，IPAによって提案されている[6]．関連して，文献[18]では，個人の利得と認知構造に言及した興味深い研究もなされているが，ISMS自体に言及した研究は，まだ十分ではない．著者らの先行研究では，PKIやディジタルフォレンジクスに関する費用面の検討として，積算法を用いた研究があるが[19], [20]，効果面に関する定量的な導出のみであり，費用対効果としての研究はなされていない．

(3) セキュリティに対するセンサ活用に関する研究

セキュリティに対するセンサ活用の研究では，たとえば，文献[21]では，サイバー攻撃の検知にマルチコプタ（ドローン）を利用している．著者らの先行研究[22]では，センサを用いたISMSのコスト低減効果の検討がある．この論文では，ISMSの管理項目を規定項目（初回のみ規定）と運用項目（ランニングコストが必要）に分け，さらに，運用項目を監査的なもの（長周期型）と入退室等の短期間に繰り返し運用が必要なもの（短周期型）に分類し，この短周期型にセンサが活用できる点を示したが，具体的な費用対効果の導出には至っていない．

3. ISMSにおける費用面の導出

ここでは，ISMS費用面の導出について，著者らの先行研究[22]を基に，机上シミュレーションによる導出を行う．この際，初期コストに着目した静的導出と運用コストに着目した動的導出の2つの対象に分けて導出する．

3.1 ISMSにおける費用の近似導出（静的導出）

(1) 費用の分析手法

ここでは，ISMSにおける費用を定量的に導出するために，プロジェクトマネジメントやソフトウェア開発等において，一般的に用いられている定量化手法[23]を参考にした．これらの結果を**表1**に示す．

表1 主な分析手法の種類
Table 1 Type of main analytical methods.

分析手法		内容	評価
推測法	類推法	経験値による見積もりであり，過去の類似の開発事例から開発規模を類推する手法.	× 類似事例が無い
推測法	**積算法**	**WBS(Work Breakdown System) 手法[23]によって細分化されたワークパッケージ毎に工数を求め， それらの推定した工数を積上げることにより，見積もりを行う.**	**○ WBS化により 容易に見積りが可能**
実測法		ISMSを運用させて，実際にかかった工数やコストを導出する.	× 詳細に評価できるが， 実際のシステムが必要

表1において，推測手法では，これまでにISMSのコスト構造に関しての定量的な導出例が十分でないことから類推法を使用することができない．これに対し，積算法では，ISMSの費用構造をWBS手法により細分化した結果を用いることにより，容易に導出が可能である．実測法に関しては，表1の中で最も詳細な結果が見込めるが，本格的なシステムを構築し，さらに詳細な実測が必要となり，実測のための費用がかかるため，現実的ではない．

以上より，本論文では，推測手法の1つである積算法を用いた．具体的には，積算法に基づく机上シミュレーションにより，ISMSの費用面を導出した．

(2) ISMSの費用導出（机上シミュレーション）

ここでは，(1)に示す積算法を用いて，ISMSの費用を導出する．具体的には，図1に示すISMSの114の管理項目の「実施の手引」を参考にし[1]，**図2**に示すように，机上（作業）シミュレーションを行うことで，これらを作業単位（ワークパッケージ（Work Package，以降WP））として細分化し，この細分化単位を工数として近似する．

(2-1) ISMS管理策の詳細化（図2(a)）

図1に示すISMS管理策に対し，「8. 資産の管理」を例に示す．ISMS管理策は，階層構造をとっているため，これをさらに詳細化すると，図2(a)左側のように10の管理策に細分化される．文献[1]では，この管理策ごとに実施の手引きが詳細に記されていることから，机上シミュレーションでは，この実施の手引きをベースとする．

(2-2) 机上シミュレーション（図2(b)）

机上シミュレーションは，**図3**に示すように，以下の4段階の手順をとっている．

- STEP1：ISMS管理策の実施の手引を抽出する．
- STEP2：抽出した実施の手引の文章をWP化しやすいように細分化する．
- STEP3：細分化された文章をWP化する．
- STEP4：WP数の合計を求める．

具体的な机上シミュレーションとして，「8.2.1 情報の分類」，「8.3.1 取外し可能な媒体の管理」を例にとり詳細に説明する．

- STEP1：ISMS管理策の実施の手引きから「8.2.1 情報の分類」を抽出する．
- STEP2：抽出した「8.2.1 情報の分類」の実施の手引は，図2(b)の左側上部に示すように，一連の文章として記されている．この文章に記されている内容を費用化，すなわち，WP化しやすくするために，以下の前提条件に基づき，図2(b)の左側のように，最初に文章の細分化を行う．
  1) 文章の区切り（句点[。]）単位に細分化することを基本とする．文章によっては，WP化の容易性の観点から関連する作業（例：図2(b)「8.2.1 情報の分類」の左側の1番目）を一括りにして細分化する．

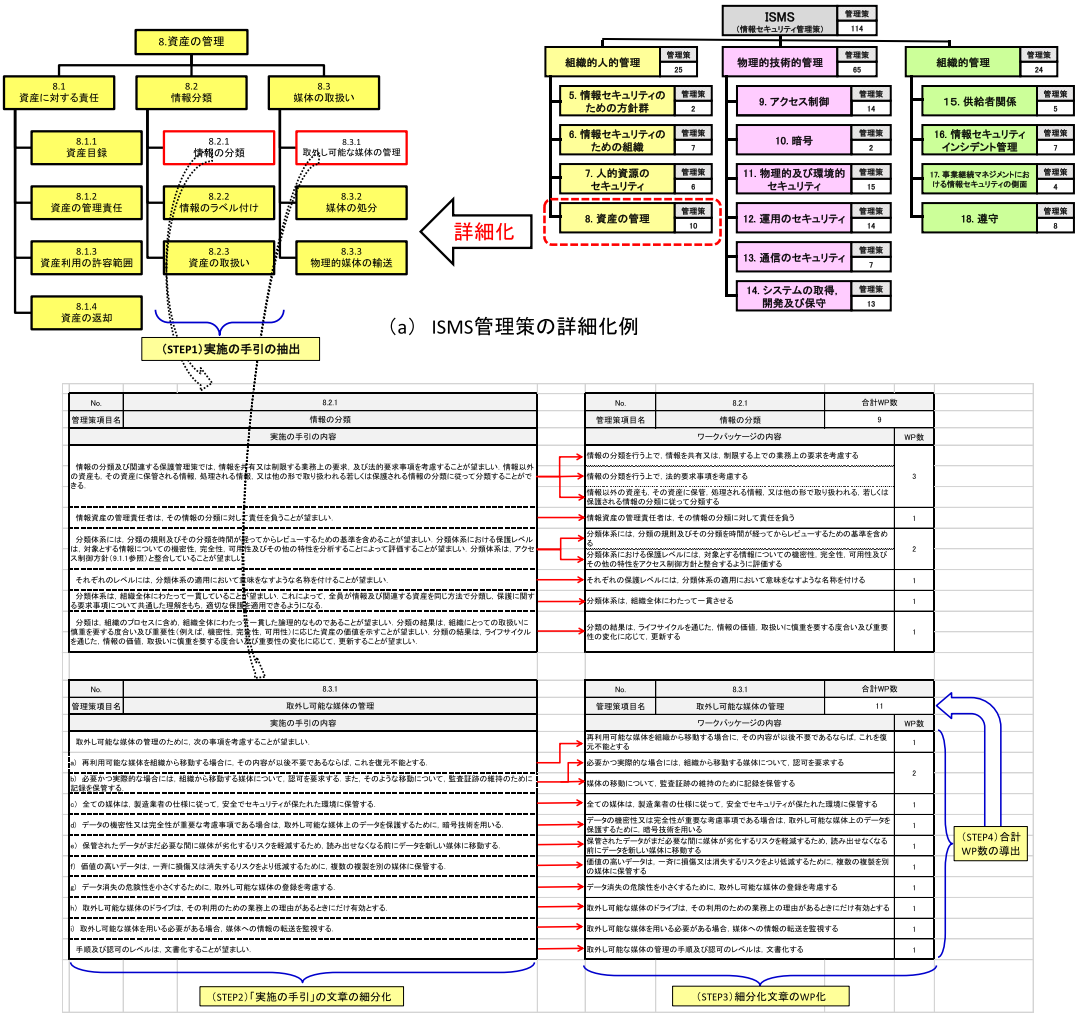

図 2　机上シミュレーションによる WP 数の近似算出例

Fig. 2　Approximation calculation example of the number of WPs based on theoretical simulation.

2)　管理策によっては，「8.3.1 取外し可能な媒体の管理」の実施の手引（図 2 (b) の左側下部）のように要素を列挙する形で記されているものもある．このようなパターンに関しても，先の例と同様に，各内容を文章の区切り（句点 [。]）単位を基本として分割し，これを基に WP 化した．

3)　管理策の文章中にある，「また」に関しては，作業を併記する「また」については 2 つの WP に細分化し，（作業目的等の）作業ではないことを併記する「また」については 1 つの WP とする．
「および」に関しても同様のルールとした．

4)　図 2 (b) の「8.3.1 取外し可能な媒体の管理」の 1 行目にあるように，作業に関係なく単に解説のみの文章は省く．すなわち，WP 化しない．

- STEP3：STEP2 で細分化した文章ごとに WP 化（例；……を考慮する，……を分類する等）を行う．
- STEP4：STEP3 で算出された WP 数を合算することで，ISMS の各管理策の WP 数を算出する．

以上に示す机上シミュレーションにより ISMS の各管理策に対し，WP（≒工数）を近似的な費用として導出した [24]．この結果を**表 2** に示す．

(2-3) 考察

机上シミュレーションにより算出した各 WP の作業内容は，それぞれ異なっている．したがって，それらの工数も当然相違があるが，マクロ的な観点からは，各 WP の工数の大小はある程度は相殺されうることを考慮し，今回の机上シミュレーションでは，前述のように，「WP ≒ 工数」であると単純化して考えることとした．

よりミクロな検討，すなわち，各 WP の工数をより詳細に見積もったうえでのシミュレーションは今後の検討課題とする．

3.2　ISMS における費用の近似導出（動的導出）

ここでは，表 2 で導出した結果に対し，運用面を考慮した動的な費用を含めた費用導出を行う．具体的には，**図 4** に示すフローに基づき，動的費用の検討が必要な管理項目

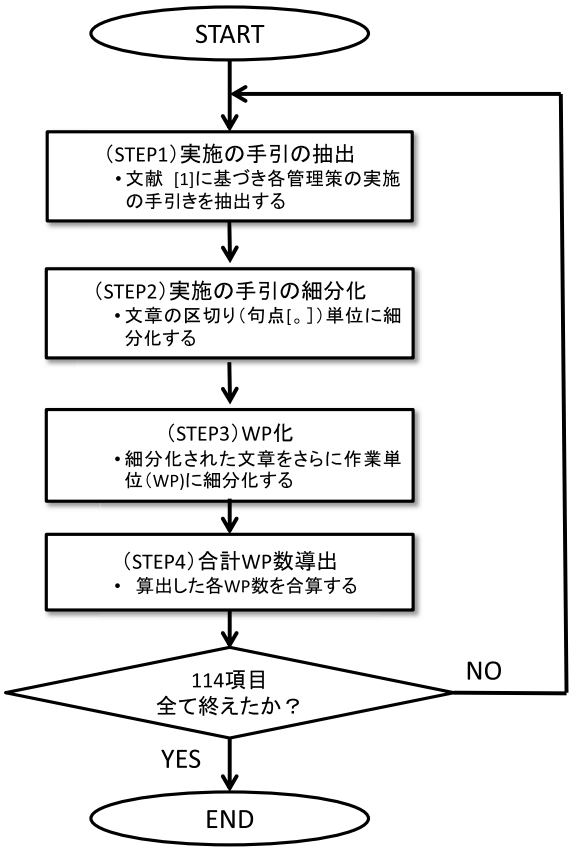

図 3 机上シミュレーションによる WP 数算出フロー
Fig. 3 Calculation flow of the number of WPs by theoretical simulation.

を絞り込んだ後に，絞り込んだ項目個々の費用を見積もることで全体の動的費用を導出する．なお，導出に際し，ISMS 認証取得から再認証審査の期間（3 年）を基準とした [25].

(1) 一次フィルタリング（A：規定項目を抽出）

表 2 に示す ISMS の管理項目の中には最初に規定するだけで，以降は特段の運用稼働が発生しない規定に関する管理項目がある．最初にこの規定に関する管理項目を抽出し，114 項目中，35 項目が該当した．

(2) 二次フィルタリング（B：情報システム管理項目を抽出）

二次フィルタリングでは，人的稼働が必要か否かに関して分類し，不要なものを情報システム管理項目と定義した．

(3) 三次フィルタリング（C：運用項目を抽出）

ここでは，ISMS 管理項目の運用面の特徴に着目した．ISMS 管理項目の運用面では，監査等のように半年もしくは 1 年単位で行うものと（図 4 C1：長周期運用），入退室管理等時間単位もしくは日毎単位で行うもの（図 4 C2：短周期運用）に分類できる．長周期運用は，監査等人による高度な知識やスキル，総合的な判断が必要となる作業が主となるため，後述するセンサ技術で代替するのは得策ではないものである．

表 2 ISMS における費用の近似導出結果（費用 ≒ WP 数）
Table 2 Computed results of costs in ISMS (Cost ≒ WPs).

No.	ISMSの管理策		費用（≒WP数）
1	5.1.1	情報セキュリティのための方針群	22
2	5.1.2	情報セキュリティのための方針群のレビュー	4
3	6.1.1	情報セキュリティの役割及び責任	6
4	6.1.2	職務の分離	2
5	6.1.3	関係当局との連絡	2
6	6.1.4	専門組織との連絡	6
7	6.1.5	プロジェクトマネジメントにおける情報セキュリティ	3
8	6.2.1	モバイル機器の方針	11
9	6.2.2	テレワーキング	22
10	7.1.1	選考	7
11	7.1.2	雇用条件	5
12	7.2.1	経営陣の責任	7
13	7.2.2	情報セキュリティの意識向上，教育及び訓練	5
14	7.2.3	懲戒手続き	6
15	7.3.1	雇用の終了又は変更に関する責任	2
16	8.1.1	資産目録	5
17	8.1.2	資産の管理責任	4
18	8.1.3	資産利用の許容範囲	2
19	8.1.4	資産の返却	4
20	8.2.1	情報の分類	9
21	8.2.2	情報の分類ラベル付け	5
22	8.2.3	資産の取り扱い	7
23	8.3.1	取り外し可能な媒体の管理	11
24	8.3.2	媒体の処分	8
25	8.3.3	物理的媒体の輸送	5
26	9.1.1	アクセス制御方針	11
27	9.1.2	ネットワーク及びネットワークサービスへのアクセス	6
28	9.2.1	利用者登録及び登録削除	4
29	9.2.2	利用者アクセスの提供	5
30	9.2.3	特権的アクセス権の管理	10
31	9.2.4	利用者の秘密認証情報の管理	7
32	9.2.5	利用者アクセス権のレビュー	5
33	9.2.6	アクセス権の削除又は修正	6
34	9.3.1	秘密認証情報の利用	8
35	9.4.1	情報へのアクセス制限	6
36	9.4.2	セキュリティに配慮したログオン手順	15
37	9.4.3	パスワード管理システム	9
38	9.4.4	特権的なユーティリティプログラムの使用	9
39	9.4.5	プログラムソースコードへのアクセス制御	7
40	10.1.1	暗号による管理策の利用方針	7
41	10.1.2	鍵管理	11
42	11.1.1	物理的セキュリティ境界	8
43	11.1.2	物理的入退管理策	7
44	11.1.3	オフィス，部屋及び施設のセキュリティ	4
45	11.1.4	外部及び環境の脅威からの保護	6
46	11.1.5	セキュリティを保つべき領域での作業	4
47	11.1.6	受渡場所	7
48	11.2.1	装置の設置及び保護	10
49	11.2.2	サポートユーティリティ	5
50	11.2.3	ケーブル配線のセキュリティ	6
51	11.2.4	装置の保守	7
52	11.2.5	資産の移動	4
53	11.2.6	構外にある装置及び資産のセキュリティ	4
54	11.2.7	装置のセキュリティを保った処分又は再利用	3
55	11.2.8	無人状態にある利用者の装置	4
56	11.2.9	クリアデスク・クリアスクリーン方針	5
57	12.1.1	操作手順書	10
58	12.1.2	変更管理	9
59	12.1.3	容量・能力の管理	4
60	12.1.4	開発環境，試験環境及び運用環境の分離	8
61	12.2.1	マルウェアに対する管理策	14
62	12.3.1	情報のバックアップ	6
63	12.4.1	イベントログ取得	13
64	12.4.2	ログ情報の保護	3
65	12.4.3	実務管理者及び運用担当者の作業ログ	1
66	12.4.4	クロックの同期	2
67	12.5.1	運用システムに関わるソフトウェアの導入	9
68	12.6.1	技術的ぜい弱性の管理	17
69	12.6.2	ソフトウェアのインストールの制限	4
70	12.7.1	情報システムの監査に対する制限	9
71	13.1.1	ネットワーク管理策	7
72	13.1.2	ネットワークサービスのセキュリティ	4
73	13.1.3	ネットワークの分離	5
74	13.2.1	情報転送の方針及び手順	13
75	13.2.2	情報転送に関する合意	11
76	13.2.3	電子的メッセージ通信	6
77	13.2.4	秘密保持契約又は守秘義務契約	10
78	14.1.1	情報セキュリティ要求事項の分析及び仕様化	6
79	14.1.2	公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮	13
80	14.1.3	アプリケーションサービスのトランザクションの保護	10
81	14.2.1	セキュリティに配慮した開発のための方針	10
82	14.2.2	システムの変更管理手順	13
83	14.2.3	オペレーティングプラットフォーム変更後のアプリケーションの技術的レビュー	3
84	14.2.4	パッケージソフトウェアの変更に対する制限	5
85	14.2.5	セキュリティに配慮したシステム構築の原則	7
86	14.2.6	セキュリティに配慮した開発環境	10
87	14.2.7	外部委託による開発	11
88	14.2.8	システムセキュリティの試験	3
89	14.2.9	システムの変更管理手順受入れ試験	4
90	14.3.1	試験データの保護	4
91	15.1.1	供給者関係のための情報セキュリティの方針	14
92	15.1.2	供給者との合意におけるセキュリティの取扱い	21
93	15.1.3	ICTサプライチェーン	10
94	15.2.1	供給者のサービス提供の監視及びレビュー	8
95	15.2.2	供給者のサービス提供の変更に対する管理	12
96	16.1.1	責任及び手順	13
97	16.1.2	情報セキュリティ事象の報告	8
98	16.1.3	情報セキュリティ弱点の報告	2
99	16.1.4	情報セキュリティ事象の評価及び決定	5
100	16.1.5	情報セキュリティインシデントへの対応	7
101	16.1.6	情報セキュリティインシデントからの学習	2
102	16.1.7	証拠の収集	7
103	17.1.1	情報セキュリティ継続の計画	4
104	17.1.2	情報セキュリティ継続の実施	6
105	17.1.3	情報セキュリティ継続の検証，レビュー及び評価	3
106	17.2.1	情報処理施設の可用性	3
107	18.1.1	適用法令及び契約上の要求事項の特定	3
108	18.1.2	知的財産権	12
109	18.1.3	記録の保護	3
110	18.1.4	プライバシー及び個人を特定できる情報の保護	6
111	18.1.5	暗号化機能に対する規制	4
112	18.2.1	情報セキュリティの独立したレビュー	6
113	18.2.2	情報セキュリティのための方針群及び標準の準拠	4
114	18.2.3	技術的遵守のレビュー	6
合計			813

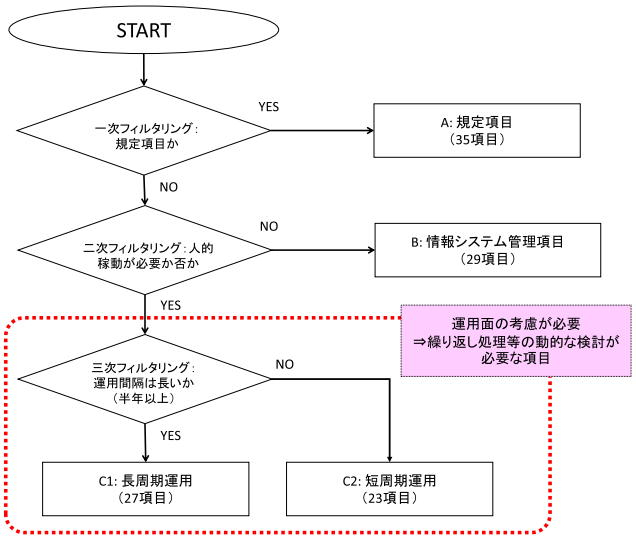

図 4 動的費用項目導出フロー
Fig. 4 Deducing flow of dynamic cost items.

表 3 運用面を考慮した動的費用導出の観点
Table 3 Viewpoint of dynamic cost derivation with operation.

ISMS 管理項目	動的な費用 導出の観点	繰返回数 (3 年間)
A: 規定項目	初期検討時のみ	1 回
B: 情報システム 管理項目	初期検討時のみ，以降は人的稼働が不要	1 回
C1: 長周期運用	監査系，レビューなどの項目が該当するため，一般には，四半期から 1 年周期となる	3 回〜12 回
C2: 短周期運用	短周期運用系では，主に保守系の項目が該当する，このため，時間単位（朝昼夜の 3 回/日）から月 1 回の点検までが該当する	36 回〜 3, 285 回※

※：3,285 [回] = 3 [回/日] * 365 [日/年] * 3 [年]

(4) 運用面を考慮した ISMS 費用の導出結果

次に，図 4 の結果を基に，ISMS における運用面を考慮した費用の導出を行う．その際，前述のように，運用サイクルを ISMS 認証取得から再認証審査の期間（3 年）を基準とした．最初に，運用面を考慮した費用の導出として，**表 3** に示す観点を用いることとした．

表 3 に示す観点の下，114 の管理項目に対し，運用面の費用を導出した．導出のベースとなる費用は，表 2 を用いた．すなわち，表 2 の費用に対し，表 3 の観点で求めた 3 年間の繰返回数を乗じて算出した．結果を**表 4** に示す．

3.3 ISMS における効果の近似導出

ここでは，ISMS における効果の導出を行う．効果の導出に際し，ISMS の管理項目を適用することによりリスクをどれだけ低減できるかと仮定して近似的に導出した．具体的には，文献 [26], [27] を参考に，各管理項目が保有するリスク値を，資産（≒ 影響度）と脅威（≒ 発生頻度），脆弱性に対し，式 (1) のリスク値により導出する．

$$\text{リスク値} = \text{資産} \times \text{脅威} \times \text{脆弱性} \quad (1)$$

表 4 運用面を考慮した費用導出結果（費用 ≒ WP 数）
Table 4 Cost computed result with operation (cost ≒ WPs).

No.	ISMSの管理策	静的費用	動的費用		
			図4の分類	3年間回数	動的費用
1	5.1.1 情報セキュリティのための方針群	22	A	1	22
2	5.1.2 情報セキュリティのための方針群のレビュー	4	C1	3	12
3	6.1.1 情報セキュリティの役割及び責任	6	A	1	6
4	6.1.2 職務の分離	2	A	1	2
5	6.1.3 関係当局との連絡	2	A	1	2
6	6.1.4 専門組織との連絡	6	C1	6	36
7	6.1.5 プロジェクトマネジメントにおける情報セキュリティ	3	C1	12	36
8	6.2.1 モバイル機器の方針	11	A	1	11
9	6.2.2 テレワーキング	22	A	1	22
10	7.1.1 選考	7	C1	3	21
11	7.1.2 雇用条件	5	A	1	5
12	7.2.1 経営陣の責任	7	C1	12	84
13	7.2.2 情報セキュリティの意識向上，教育及び訓練	5	C1	3	15
14	7.2.3 懲戒手続き	6	A	1	6
15	7.3.1 雇用の終了又は変更に関する責任	2	C1	3	6
16	8.1.1 資産目録	5	C2	36	180
17	8.1.2 資産の管理責任	4	C2	36	144
18	8.1.3 資産利用の許容範囲	2	C1	3	6
19	8.1.4 資産の返却	4	C1	3	12
20	8.2.1 情報の分類	9	A	1	9
21	8.2.2 情報の分類ラベル付け	5	A	1	5
22	8.2.3 資産の取り扱い	7	A	1	7
23	8.3.1 取り外し可能な媒体の管理	11	C2	36	396
24	8.3.2 媒体の処分	8	A	1	8
25	8.3.3 物理的媒体の輸送	5	C2	36	180
26	9.1.1 アクセス制御方針	11	A	1	11
27	9.1.2 ネットワーク及びネットワークサービスへのアクセス	6	A	1	6
28	9.2.1 利用者登録及び登録削除	4	C1	3	12
29	9.2.2 利用者アクセスの提供	5	B	1	5
30	9.2.3 特権的アクセス権の管理	10	C1	3	30
31	9.2.4 利用者の秘密認証情報の管理	7	C1	3	21
32	9.2.5 利用者アクセス権のレビュー	5	C1	3	15
33	9.2.6 アクセス権の削除又は修正	6	C1	3	18
34	9.3.1 秘密認証情報の利用	8	B	1	8
35	9.4.1 情報へのアクセス制限	6	B	1	6
36	9.4.2 セキュリティに配慮したログオン手順	15	B	1	15
37	9.4.3 パスワード管理システム	9	B	1	9
38	9.4.4 特権的なユーティリティプログラムの使用	9	A	1	9
39	9.4.5 プログラムソースコードへのアクセス制御	7	C1	12	84
40	10.1.1 暗号による管理策の利用方針	7	A	1	7
41	10.1.2 鍵管理	11	C1	12	132
42	11.1.1 物理的セキュリティ境界	8	C2	36	288
43	11.1.2 物理的入退管理策	7	C2	2,190	15,330
44	11.1.3 オフィス，部屋及び施設のセキュリティ	4	A	1	4
45	11.1.4 外部及び環境の脅威からの保護	6	C2	36	216
46	11.1.5 セキュリティを保つべき領域での作業	4	C2	1,095	4,380
47	11.1.6 受渡場所	7	C2	156	1,092
48	11.2.1 装置の設置及び保護	10	C2	3,285	32,850
49	11.2.2 サポートユーティリティ	5	C2	36	180
50	11.2.3 ケーブル配線のセキュリティ	6	C2	1,095	6,570
51	11.2.4 装置の保守	7	C2	36	252
52	11.2.5 資産の移動	4	C2	156	624
53	11.2.6 構外にある装置及び資産のセキュリティ	4	C2	156	624
54	11.2.7 装置のセキュリティを保った処分又は再利用	3	C1	12	36
55	11.2.8 無人状態にある利用者の装置	4	C2	1,095	4,380
56	11.2.9 クリアデスク・クリアスクリーン方針	5	C2	1,095	5,475
57	12.1.1 操作手順書	10	A	1	10
58	12.1.2 変更管理	9	A	1	9
59	12.1.3 容量・能力の管理	4	C1	12	48
60	12.1.4 開発環境，試験環境及び運用環境の分離	8	B	1	8
61	12.2.1 マルウェアに対する管理策	14	B	1	14
62	12.3.1 情報のバックアップ	6	B	1	6
63	12.4.1 イベントログ取得	13	B	1	13
64	12.4.2 ログ情報の保護	3	B	1	3
65	12.4.3 実務管理者及び運用担当者の作業ログ	1	B	1	1
66	12.4.4 クロックの同期	2	B	1	2
67	12.5.1 運用システムに関わるソフトウェアの導入	9	B	1	9
68	12.6.1 技術的ぜい弱性の管理	17	B	1	17
69	12.6.2 ソフトウェアのインストールの制限	4	B	1	4
70	12.7.1 情報システムの監査に対する制限	9	A	1	9
71	13.1.1 ネットワーク管理策	7	B	1	7
72	13.1.2 ネットワークサービスのセキュリティ	4	A	1	4
73	13.1.3 ネットワークの分離	5	A	1	5
74	13.2.1 情報転送の方針及び手順	13	A	1	13
75	13.2.2 情報転送に関する合意	11	A	1	11
76	13.2.3 電子的メッセージ通信	6	B	1	6
77	13.2.4 秘密保持契約又は守秘義務契約	10	B	1	10
78	14.1.1 情報セキュリティ要求事項の分析及び仕様化	6	A	1	6
79	14.1.2 公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮	13	B	1	13
80	14.1.3 アプリケーションサービスのトランザクションの保護	10	B	1	10
81	14.2.1 セキュリティに配慮した開発のための方針	10	A	1	10
82	14.2.2 システムの変更管理手順	13	B	1	13
83	14.2.3 オペレーティングプラットフォーム変更後のアプリケーションの技術的レビュー	3	B	1	3
84	14.2.4 パッケージソフトウェアの変更に対する制限	5	B	1	5
85	14.2.5 セキュリティに配慮したシステム構築の原則	7	B	1	7
86	14.2.6 セキュリティに配慮した開発環境	10	A	1	10
87	14.2.7 外部委託による開発	11	C1	3	33
88	14.2.8 システムセキュリティの試験	3	C1	12	36
89	14.2.9 システムの変更管理手順受入れ試験	4	C1	12	48
90	14.3.1 試験データの保護	4	B	1	4
91	15.1.1 供給者関係のための情報セキュリティの方針	14	A	1	14
92	15.1.2 供給者との合意におけるセキュリティの取扱い	21	A	1	21
93	15.1.3 ICTサプライチェーン	10	A	1	10
94	15.2.1 供給者のサービス提供の監視及びレビュー	8	C1	3	24
95	15.2.2 供給者のサービス提供の変更に対する管理	12	B	1	12
96	16.1.1 責任及び手順	13	A	1	13
97	16.1.2 情報セキュリティ事象の報告	8	C1	3	24
98	16.1.3 情報セキュリティ弱点の報告	2	C1	3	6
99	16.1.4 情報セキュリティ事象の評価及び決定	5	C2	1,095	5,475
100	16.1.5 情報セキュリティインシデントへの対応	7	C2	1,095	7,665
101	16.1.6 情報セキュリティインシデントからの学習	2	B	1	2
102	16.1.7 証拠の収集	7	C2	1,095	7,665
103	17.1.1 情報セキュリティ継続の計画	4	A	1	4
104	17.1.2 情報セキュリティ継続の実施	6	A	1	6
105	17.1.3 情報セキュリティ継続の検証，レビュー及び評価	3	C1	3	9
106	17.2.1 情報処理施設の可用性	3	A	1	3
107	18.1.1 適用法令及び契約上の要求事項の特定	3	A	1	3
108	18.1.2 知的財産権	12	C2	36	432
109	18.1.3 記録の保護	3	C2	36	108
110	18.1.4 プライバシー及び個人を特定できる情報の保護	6	B	1	6
111	18.1.5 暗号化機能に対する規制	4	B	1	4
112	18.2.1 情報セキュリティの独立したレビュー	6	C1	3	18
113	18.2.2 情報セキュリティのための方針群及び標準の準拠	4	C2	36	144
114	18.2.3 技術的順守のレビュー	6	C1	12	72
合計		813	合計		96,069

表 5 ISMS の効果
Table 5 Effect of ISMS.

No	ISMSの管理策	効果			
		資産 (影響度)	脆弱性	脅威 (発生頻度)	リスク値
1	5.1.1 情報セキュリティのための方針群	5	3	3	45
2	5.1.2 情報セキュリティのための方針群のレビュー	4	3	3	36
3	6.1.1 情報セキュリティの役割及び責任	5	3	3	45
4	6.1.2 職務の分離	4	2	1	8
5	6.1.3 関係当局との連絡	5	2	1	10
6	6.1.4 専門組織との連絡	3	2	3	18
7	6.1.5 プロジェクトマネジメントにおける情報セキュリティ	3	2	3	18
8	6.2.1 モバイル機器の方針	2	2	3	12
9	6.2.2 テレワーキング	2	2	3	12
10	7.1.1 選考	3	2	1	6
11	7.1.2 雇用条件	1	1	1	1
12	7.2.1 経営陣の責任	4	2	2	16
13	7.2.2 情報セキュリティの意識向上，教育及び訓練	5	3	2	30
14	7.2.3 懲戒手続き	1	1	1	1
15	7.3.1 雇用の終了又は変更に関する責任	1	1	1	1
16	8.1.1 資産目録	3	2	2	12
17	8.1.2 資産の管理責任	2	1	1	2
18	8.1.3 資産利用の許容範囲	2	1	1	2
19	8.1.4 資産の返却	1	1	1	1
20	8.2.1 情報の分類	1	2	3	6
21	8.2.2 情報の分類ラベル付け	2	1	1	2
22	8.2.3 資産の取り扱い	2	1	1	2
23	8.3.1 取り外し可能な媒体の管理	2	1	1	2
24	8.3.2 媒体の処分	1	1	2	2
25	8.3.3 物理的媒体の輸送	2	1	1	2
26	9.1.1 アクセス制御方針	3	2	3	18
27	9.1.2 ネットワーク及びネットワークサービスへのアクセス	3	2	3	18
28	9.2.1 利用者登録及び登録削除	3	2	1	6
29	9.2.2 利用者アクセスの提供	3	2	2	12
30	9.2.3 特権的アクセス権の管理	3	2	3	18
31	9.2.4 利用者の秘密認証情報の管理	4	2	2	16
32	9.2.5 利用者アクセス権のレビュー	2	1	1	2
33	9.2.6 アクセス権の削除又は修正	4	2	2	16
34	9.3.1 秘密認証情報の利用	4	3	3	36
35	9.4.1 情報へのアクセス制限	3	2	3	18
36	9.4.2 セキュリティに配慮したログオン手順	3	2	1	6
37	9.4.3 パスワード管理システム	4	3	3	36
38	9.4.4 特権的なユーティリティプログラムの使用	4	3	3	36
39	9.4.5 プログラムソースコードへのアクセス制御	3	2	2	12
40	10.1.1 暗号による管理策の利用方針	5	3	3	45
41	10.1.2 鍵管理	5	3	3	45
42	11.1.1 物理的セキュリティ境界	5	2	1	10
43	11.1.2 物理的入退管理策	5	2	1	10
44	11.1.3 オフィス，部屋及び施設のセキュリティ	3	2	1	6
45	11.1.4 外部及び環境の脅威からの保護	5	2	1	10
46	11.1.5 セキュリティを保つべき領域での作業	4	2	1	8
47	11.1.6 受渡場所	3	2	1	6
48	11.2.1 装置の設置及び保護	5	3	2	30
49	11.2.2 サポートユーティリティ	5	2	1	10
50	11.2.3 ケーブル配線のセキュリティ	4	2	1	8
51	11.2.4 装置の保守	4	2	1	8
52	11.2.5 資産の移動	3	2	3	18
53	11.2.6 構外にある装置及び資産のセキュリティ	3	2	2	12
54	11.2.7 装置のセキュリティを保った処分又は再利用	5	2	1	10
55	11.2.8 無人状態にある利用者の装置	3	2	2	12
56	11.2.9 クリアデスク・クリアスクリーン方針	1	1	1	1
57	12.1.1 操作手順書	1	2	3	6
58	12.1.2 変更管理	3	2	3	18
59	12.1.3 容量・能力の管理	3	2	2	12
60	12.1.4 開発環境，試験環境及び運用環境の分離	2	2	2	8
61	12.2.1 マルウェアに対する管理策	5	3	3	45
62	12.3.1 情報のバックアップ	4	2	2	16
63	12.4.1 イベントログ取得	1	1	2	2
64	12.4.2 ログ情報の保護	1	1	1	1
65	12.4.3 実務管理者及び運用担当者の作業ログ	1	1	1	1
66	12.4.4 クロックの同期	1	1	1	1
67	12.5.1 運用システムに関わるソフトウェアの導入	2	2	2	8
68	12.6.1 技術的ぜい弱性の管理	5	3	2	30
69	12.6.2 ソフトウェアのインストールの制限	3	2	1	6
70	12.7.1 情報システムの監査に対する制限	3	2	1	6
71	13.1.1 ネットワーク管理策	4	3	3	36
72	13.1.2 ネットワークサービスのセキュリティ	3	2	2	12
73	13.1.3 ネットワークの分離	3	2	2	12
74	13.2.1 情報転送の方針及び手順	5	2	1	10
75	13.2.2 情報転送に関する合意	5	3	2	30
76	13.2.3 電子的メッセージ通信	3	2	3	18
77	13.2.4 秘密保持契約又は守秘義務契約	4	3	3	36
78	14.1.1 情報セキュリティ要求事項の分析及び仕様化	3	2	2	12
79	14.1.2 公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮	4	2	2	16
80	14.1.3 アプリケーションサービスのトランザクションの保護	3	2	3	18
81	14.2.1 セキュリティに配慮した開発のための方針	3	2	2	12
82	14.2.2 システムの変更管理手順	4	3	3	36
83	14.2.3 オペレーティングプラットフォーム変更後のアプリケーションの技術的レビュー	2	2	3	12
84	14.2.4 パッケージソフトウェアの変更に対する制限	1	1	1	1
85	14.2.5 セキュリティに配慮したシステム構築の原則	2	2	2	8
86	14.2.6 セキュリティに配慮した開発環境	2	2	3	12
87	14.2.7 外部委託による開発	3	2	3	18
88	14.2.8 システムセキュリティの試験	2	2	2	8
89	14.2.9 システムの変更管理手順受入れ試験	1	1	2	2
90	14.3.1 試験データの保護	1	1	1	1
91	15.1.1 供給者関係のための情報セキュリティの方針	4	2	2	16
92	15.1.2 供給者との合意におけるセキュリティの取扱い	5	3	2	30
93	15.1.3 ICTサプライチェーン	3	2	1	6
94	15.2.1 供給者のサービス提供の監視及びレビュー	2	1	1	2
95	15.2.2 供給者のサービス提供の変更に対する管理	2	2	3	12
96	16.1.1 責任及び手順	1	1	1	1
97	16.1.2 情報セキュリティ事象の報告	3	2	3	18
98	16.1.3 情報セキュリティ弱点の報告	2	2	2	8
99	16.1.4 情報セキュリティ事象の評価及び決定	3	2	1	6
100	16.1.5 情報セキュリティインシデントへの対応	3	2	3	18
101	16.1.6 情報セキュリティインシデントからの学習	2	2	2	8
102	16.1.7 証拠の収集	3	2	3	18
103	17.1.1 情報セキュリティ継続の計画	5	2	1	10
104	17.1.2 情報セキュリティ継続の実施	4	2	2	16
105	17.1.3 情報セキュリティ継続の検証，レビュー及び評価	3	2	2	12
106	17.2.1 情報処理施設の可用性	3	2	2	12
107	18.1.1 適用法令及び契約上の要求事項の特定	3	2	3	18
108	18.1.2 知的財産権	2	2	3	12
109	18.1.3 記録の保護	2	2	3	12
110	18.1.4 プライバシー及び個人を特定できる情報の保護	3	2	3	18
111	18.1.5 暗号化機能に対する規制	1	1	2	2
112	18.2.1 情報セキュリティの独立したレビュー	1	1	1	1
113	18.2.2 情報セキュリティのための方針群及び標準の準拠	2	1	1	2
114	18.2.3 技術的遵守のレビュー	2	1	1	2
合 計					1,521

表 6 ISMS における運用を考慮に入れた費用対効果
Table 6 Cost effectiveness with operation in ISMS.

No.	ISMSの管理策	効果 (≒リスク値)	費用 (≒WP数)
1	5.1.1 情報セキュリティのための方針群	45	22
2	5.1.2 情報セキュリティのための方針群のレビュー	36	12
3	6.1.1 情報セキュリティの役割及び責任	45	6
4	6.1.2 職務の分離	8	2
5	6.1.3 関係当局との連絡	10	2
6	6.1.4 専門組織との連絡	18	36
7	6.1.5 プロジェクトマネジメントにおける情報セキュリティ	18	36
8	6.2.1 モバイル機器の方針	12	11
9	6.2.2 テレワーキング	12	22
10	7.1.1 選考	6	21
11	7.1.2 雇用条件	1	5
12	7.2.1 経営陣の責任	16	84
13	7.2.2 情報セキュリティの意識向上，教育及び訓練	30	15
14	7.2.3 懲戒手続き	1	6
15	7.3.1 雇用の終了又は変更に関する責任	1	6
16	8.1.1 資産目録	12	180
17	8.1.2 資産の管理責任	2	144
18	8.1.3 資産利用の許容範囲	2	6
19	8.1.4 資産の返却	1	12
20	8.2.1 情報の分類	6	9
21	8.2.2 情報の分類ラベル付け	2	5
22	8.2.3 資産の取り扱い	2	7
23	8.3.1 取り外し可能な媒体の管理	2	396
24	8.3.2 媒体の処分	2	8
25	8.3.3 物理的媒体の輸送	2	180
26	9.1.1 アクセス制御方針	18	11
27	9.1.2 ネットワーク及びネットワークサービスへのアクセス	18	6
28	9.2.1 利用者登録及び登録削除	6	12
29	9.2.2 利用者アクセスの提供	12	5
30	9.2.3 特権的アクセス権の管理	18	30
31	9.2.4 利用者の秘密認証情報の管理	16	21
32	9.2.5 利用者アクセス権のレビュー	2	15
33	9.2.6 アクセス権の削除又は修正	16	18
34	9.3.1 秘密認証情報の利用	36	8
35	9.4.1 情報へのアクセス制限	18	6
36	9.4.2 セキュリティに配慮したログオン手順	6	15
37	9.4.3 パスワード管理システム	36	9
38	9.4.4 特権的なユーティリティプログラムの使用	36	9
39	9.4.5 プログラムソースコードへのアクセス制御	12	84
40	10.1.1 暗号による管理策の利用方針	45	7
41	10.1.2 鍵管理	45	132
42	11.1.1 物理的セキュリティ境界	10	288
43	11.1.2 物理的入退管理策	10	15,330
44	11.1.3 オフィス，部屋及び施設のセキュリティ	6	4
45	11.1.4 外部及び環境の脅威からの保護	10	216
46	11.1.5 セキュリティを保つべき領域での作業	8	4,380
47	11.1.6 受渡場所	6	1,092
48	11.2.1 装置の設置及び保護	30	32,850
49	11.2.2 サポートユーティリティ	10	180
50	11.2.3 ケーブル配線のセキュリティ	8	6,570
51	11.2.4 装置の保守	8	252
52	11.2.5 資産の移動	18	624
53	11.2.6 構外にある装置及び資産のセキュリティ	12	624
54	11.2.7 装置のセキュリティを保った処分又は再利用	10	36
55	11.2.8 無人状態にある利用者の装置	12	4,380
56	11.2.9 クリアデスク・クリアスクリーン方針	1	5,475
57	12.1.1 操作手順書	6	10
58	12.1.2 変更管理	18	9
59	12.1.3 容量・能力の管理	12	48
60	12.1.4 開発環境，試験環境及び運用環境の分離	8	8
61	12.2.1 マルウェアに対する管理策	45	14
62	12.3.1 情報のバックアップ	16	6
63	12.4.1 イベントログ取得	2	13
64	12.4.2 ログ情報の保護	1	3
65	12.4.3 実務管理者及び運用担当者の作業ログ	1	1
66	12.4.4 クロックの同期	1	2
67	12.5.1 運用システムに関わるソフトウェアの導入	8	9
68	12.6.1 技術的ぜい弱性の管理	30	17
69	12.6.2 ソフトウェアのインストールの制限	6	4
70	12.7.1 情報システムの監査に対する制限	6	9
71	13.1.1 ネットワーク管理策	36	7
72	13.1.2 ネットワークサービスのセキュリティ	12	4
73	13.1.3 ネットワークの分離	12	5
74	13.2.1 情報転送の方針及び手順	10	13
75	13.2.2 情報転送に関する合意	30	11
76	13.2.3 電子的メッセージ通信	18	6
77	13.2.4 秘密保持契約又は守秘義務契約	36	10
78	14.1.1 情報セキュリティ要求事項の分析及び仕様化	12	6
79	14.1.2 公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮	16	13
80	14.1.3 アプリケーションサービスのトランザクションの保護	18	10
81	14.2.1 セキュリティに配慮した開発のための方針	12	10
82	14.2.2 システムの変更管理手順	36	13
83	14.2.3 オペレーティングプラットフォーム変更後のアプリケーションの技術的レビュー	12	3
84	14.2.4 パッケージソフトウェアの変更に対する制限	1	5
85	14.2.5 セキュリティに配慮したシステム構築の原則	8	7
86	14.2.6 セキュリティに配慮した開発環境	12	10
87	14.2.7 外部委託による開発	18	33
88	14.2.8 システムセキュリティの試験	8	36
89	14.2.9 システムの変更管理手順受入れ試験	2	48
90	14.3.1 試験データの保護	1	4
91	15.1.1 供給者関係のための情報セキュリティの方針	16	14
92	15.1.2 供給者との合意におけるセキュリティの取扱い	30	21
93	15.1.3 ICTサプライチェーン	6	10
94	15.2.1 供給者のサービス提供の監視及びレビュー	2	24
95	15.2.2 供給者のサービス提供の変更に対する管理	12	12
96	16.1.1 責任及び手順	1	13
97	16.1.2 情報セキュリティ事象の報告	18	24
98	16.1.3 情報セキュリティ弱点の報告	8	6
99	16.1.4 情報セキュリティ事象の評価及び決定	6	5,475
100	16.1.5 情報セキュリティインシデントへの対応	18	7,665
101	16.1.6 情報セキュリティインシデントからの学習	8	2
102	16.1.7 証拠の収集	18	7,665
103	17.1.1 情報セキュリティ継続の計画	10	4
104	17.1.2 情報セキュリティ継続の実施	16	6
105	17.1.3 情報セキュリティ継続の検証，レビュー及び評価	12	9
106	17.2.1 情報処理施設の可用性	12	3
107	18.1.1 適用法令及び契約上の要求事項の特定	18	3
108	18.1.2 知的財産権	12	432
109	18.1.3 記録の保護	12	108
110	18.1.4 プライバシー及び個人を特定できる情報の保護	18	6
111	18.1.5 暗号化機能に対する規制	2	4
112	18.2.1 情報セキュリティの独立したレビュー	1	18
113	18.2.2 情報セキュリティのための方針群及び標準の準拠	2	144
114	18.2.3 技術的遵守のレビュー	2	72
合計		1,521	96,069

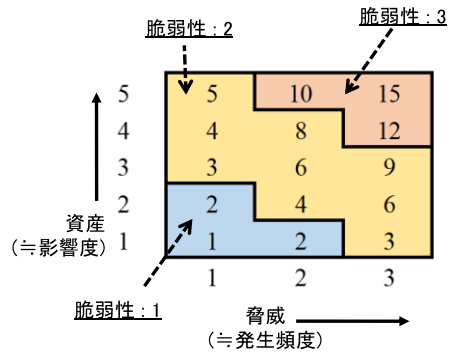

図 5 リスク値の各パラメータ評価基準の近似

Fig. 5 Approximation of each parametric evaluation standard.

ここで，**図 5** に示すように，リスクマトリクスを基にして，式 (1) の各パラメータの評価基準を示す [26], [27].

これらの前提条件を基にして，式 (1) により ISMS の 114 の対策に対するリスク値を導出した結果を**表 5** に示す [28].

3.4 ISMS 対策に対する費用対効果

表 4 の運用面を考慮した費用導出結果（WP 数で近似）と表 5 の効果導出結果（リスク値で近似）を費用対効果としてとりまとめた結果を**表 6** に示す.

4. センサ活用に基づく費用削減効果

ここでは，図 4 のフローにおける ISMS 管理項目で，運用面の考慮が必要となる短周期項目（図 4，C2）の 23 項目について，現状のセンサ活用が可能な項目について検討した結果を示す.

4.1 短周期項目におけるセンサ活用の可否について

ISMS における短周期項目の管理項目をセンサで活用する際に着目すべき点は，人的稼働の削減である．この場合，人の活動として，人間の五感にポイントを置いた．人間の五感の視覚，聴覚，嗅覚，味覚，触覚のうち，特に，ISMS 運用に大きく関わると思われる，視覚，聴覚，触覚の 3 つにフォーカスし，これに関わるセンサを抽出した．その結果を**図 6** に，また，各センサの概要を**表 7** に示す.

これらのセンサに対し，短周期項目（図 4，C2）の業務内容（WP）を対応させた結果を付録 A.1 に示す.

付録 A.1 の結果から，短周期項目 23 項目のうち 19 項目が図 6 に示すセンサで代替可能である項目であることが新たに分かった.

この結果，図 4 のフローは，**図 7** のように，さらにセンサ技術の代替可否によって分類できる.

4.2 センサ活用に基づく ISMS 対策に対する費用対効果

4.1 節での検討結果を基に，ここでは，センサ活用による ISMS 対策の費用対効果の改善効果を明らかにする.

具体的には，表 6 と同様にして導出する．効果は，表 6 と同様，表 5 の効果導出結果（リスク値で近似）を用いる．費用に関しては，表 3 に示す運用面を考慮した費用導出結果（WP 数で近似）に対し，付録 A.1 に示すセンサ活用による削減効果，すなわち，全体で 34,290 WP の削減が見込める．これらの結果をセンサ活用に基づく ISMS 対策に対する費用対効果としてとりまとめた結果を**表 8** に示す.

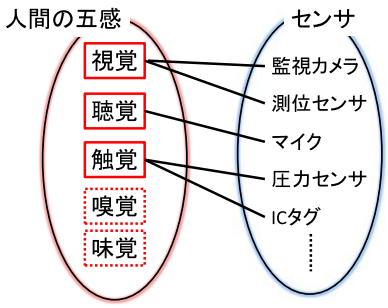

図 6 人間の五感とセンサ

Fig. 6 Man's senses and sensor.

表 7 各センサの概要

Table 7 Summary of each sensor.

センサ	センサの活動概要	コスト削減効果	センサで代替可能な主な管理項目の詳細	
			管理項目番号	管理項目詳細
監視カメラ	実際の活動状況を監視する．偽装や虚偽の活動が無いよう，映像として証拠を得る．	相互監視などの複数の目が必要な場合にその代替となる	11.1.2 物理的入退管理策	セキュリティを保つべき領域への，外部のサポートサービス要員によるアクセスは許可を必要とし，監視する
			11.1.5 セキュリティを保つべき領域での作業	安全面の理由の為及び悪意ある活動の機会を防止するための両面から，セキュリティを保つべき領域での監督されていない作業は，回避する
測位センサ	距離を測ることによって，対象が所定の位置にいることを監視する．	主にPC前から離れたことを検知し，ロック操作を確実にすると共に，教育の負担を軽減する	11.2.8 無人状態にある利用者装置	コンピュータ又はモバイル機器は，利用していない場合，キーロック又は同等の管理策によって，認可されていない利用から保護する
			11.2.9 クリアデスク・クリアスクリーン方針	コンピュータ及び端末は，離席時には，ログオフ状態にしておくか，又はパスワード，トークン若しくは類似の利用者認証機能で管理されたスクリーン及びキーボードのロック機能によって保護する
マイク	対応時の判断など，映像だけでは難しい作業状況を監視する．	詳細なログを音声データとして取得し，ログデータ作成作業の負担を軽減する	16.1.4 情報セキュリティ事象の評価及び決定	評価及び決定の結果は，以後の参照及び検証のため詳細に記録する
			16.1.5 情報セキュリティインシデントへの対応	後で行う分析のために，関連するすべての対応活動を適正に記録することを確実にする
圧力センサ	主に接触状態を監視する．扉などの開閉を監視することが出来る．	セキュリティを保った扉の開閉作業を代替する	11.1.6 受渡場所	受渡場所の外部扉は，内部の扉が開いているときにはセキュリティを保つ
				入荷物は，輸送中に開封された痕跡がないかを検査し，開封の痕跡が見つかった場合には，直ちにセキュリティ要員に報告する
ICタグ	人あるいは物を個別に識別し，誰（どれ）が作業を行ったのか監視する．	認証作業や作業者の特定を代替する	8.3.1 取外し可能な媒体の管理	媒体の移動について，監査証跡の維持のために記録を保管する
			11.1.1 物理的セキュリティ境界	敷地及び建物へのアクセスは，認可された要員にだけ制限する

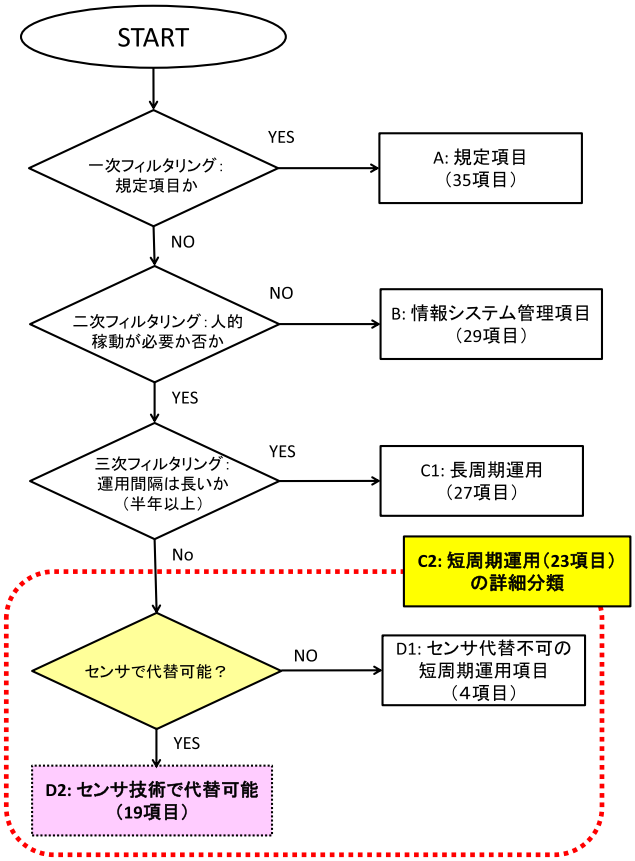

図 7 センサ代替可能項目導出フロー
Fig. 7 Deducing flow of sensor substitution items.

いる．この図に示すように，センサ活用の効果は，運用稼働が大きい箇所（同図で費用が 1,000 WP 以上のプロット部分）によく出ていることが分かる．

ここで，ISMS の導入を想定した場合，付録 A.1 に示す ISMS 管理策（センサ活用可能な 19 の管理策）に対し，代替可能なセンサおよびその削減効果（センサ活用による WP 削減数）を明示した．これにより，相対的な値ではあるが，ISMS 導入の際の費用削減効果が明らかになり，ISMS 導入促進に寄与しうると考えられる．

今回の提案における総合的な評価としては，**表 9** に示すように，約 36%の費用削減効果があることが分かった．

5. おわりに

本論文では，ISMS の普及促進の観点から，現状の ISMS 対策の費用構造を運用面にフォーカスし，動的な費用を明らかにした．さらに，効果面に関しても言及し，先行研究の結果を基に，リスク値として表した．動的な費用算出においては，人的稼働がかなりの割合を占めることから，この削減ができると費用削減効果が見込めることが分かった．これに対し，近年のセンサ技術の進展から，人的稼働がどの程度センサにより可能かに関して詳細に検討した結果，最終的には，全体の費用を約 36%低減させることができ，これにより費用対効果の効率化も見込めることを示した．

表 8 センサ活用による費用対効果の導出結果
Table 8 Result of cost effectiveness by sensor utilization.

No.	ISMSの管理策		効果（≒リスク値）	費用（≒WP数）
1	5.1.1	情報セキュリティのための方針群	45	22
2	5.1.2	情報セキュリティのための方針群のレビュー	36	12
3	6.1.1	情報セキュリティの役割及び責任	45	6
4	6.1.2	職務の分離	8	2
5	6.1.3	関係当局との連絡	10	2
6	6.1.4	専門組織との連絡	18	36
7	6.1.5	プロジェクトマネジメントにおける情報セキュリティ	18	36
8	6.2.1	モバイル機器の方針	12	11
9	6.2.2	テレワーキング	12	22
10	7.1.1	選考	6	21
11	7.1.2	雇用条件	1	5
12	7.2.1	経営陣の責任	16	84
13	7.2.2	情報セキュリティの意識向上，教育及び訓練	30	15
14	7.2.3	懲戒手続き	1	6
15	7.3.1	雇用の終了又は変更に関する責任	1	6
16	8.1.1	資産目録	12	180
17	8.1.2	資産の管理責任	2	108
18	8.1.3	資産利用の許容範囲	2	6
19	8.1.4	資産の返却	1	12
20	8.2.1	情報の分類	6	9
21	8.2.2	情報の分類ラベル付け	2	5
22	8.2.3	資産の取り扱い	2	7
23	8.3.1	取り外し可能な媒体の管理	2	324
24	8.3.2	媒体の処分	2	8
25	8.3.3	物理的媒体の輸送	2	108
26	9.1.1	アクセス制御方針	18	11
27	9.1.2	ネットワーク及びネットワークサービスへのアクセス	18	6
28	9.2.1	利用者登録及び登録削除	6	12
29	9.2.2	利用者アクセスの提供	12	5
30	9.2.3	特権的アクセス権の管理	18	30
31	9.2.4	利用者の秘密認証情報の管理	16	21
32	9.2.5	利用者アクセス権のレビュー	2	15
33	9.2.6	アクセス権の削除又は修正	16	18
34	9.3.1	秘密認証情報の利用	36	8
35	9.4.1	情報へのアクセス制限	18	6
36	9.4.2	セキュリティに配慮したログオン手順	6	15
37	9.4.3	パスワード管理システム	36	9
38	9.4.4	特権的なユーティリティプログラムの使用	36	9
39	9.4.5	プログラムソースコードへのアクセス制御	12	84
40	10.1.1	暗号による管理策の利用方針	45	7
41	10.1.2	鍵管理	45	132
42	11.1.1	物理的セキュリティ境界	10	180
43	11.1.2	物理的入退管理策	10	2,190
44	11.1.3	オフィス，部屋及び施設のセキュリティ	6	4
45	11.1.4	外部及び環境の脅威からの保護	10	216
46	11.1.5	セキュリティを保つべき領域での作業	8	1,095
47	11.1.6	受渡場所	6	660
48	11.2.1	装置の設置及び保護	30	29,565
49	11.2.2	サポートユーティリティ	10	144
50	11.2.3	ケーブル配線のセキュリティ	8	4,380
51	11.2.4	装置の保守	8	180
52	11.2.5	資産の移動	18	192
53	11.2.6	構外にある装置及び資産のセキュリティ	12	480
54	11.2.7	装置のセキュリティを保った処分又は再利用	10	36
55	11.2.8	無人状態にある利用者の装置	12	3,285
56	11.2.9	クリアデスク・クリアスクリーン方針	1	0
57	12.1.1	操作手順書	6	10
58	12.1.2	変更管理	18	9
59	12.1.3	容量・能力の管理	12	48
60	12.1.4	開発環境，試験環境及び運用環境の分離	8	8
61	12.2.1	マルウェアに対する管理策	45	14
62	12.3.1	情報のバックアップ	16	6
63	12.4.1	イベントログ取得	2	13
64	12.4.2	ログ情報の保護	1	3
65	12.4.3	実務管理者及び運用担当者の作業ログ	1	1
66	12.4.4	クロックの同期	1	2
67	12.5.1	運用システムに関わるソフトウェアの導入	8	9
68	12.6.1	技術的ぜい弱性の管理	30	17
69	12.6.2	ソフトウェアのインストールの制限	6	4
70	12.7.1	情報システムの監査に対する制限	6	9
71	13.1.1	ネットワーク管理策	36	7
72	13.1.2	ネットワークサービスのセキュリティ	12	4
73	13.1.3	ネットワークの分離	12	5
74	13.2.1	情報転送の方針及び手順	10	13
75	13.2.2	情報転送に関する合意	30	11
76	13.2.3	電子的メッセージ通信	18	6
77	13.2.4	秘密保持契約又は守秘義務契約	36	10
78	14.1.1	情報セキュリティ要求事項の分析及び仕様化	12	6
79	14.1.2	公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮	16	13
80	14.1.3	アプリケーションサービスのトランザクションの保護	18	10
81	14.2.1	セキュリティに配慮した開発のための方針	12	10
82	14.2.2	システムの変更管理手順	36	13
83	14.2.3	オペレーティングプラットフォーム変更後のアプリケーションの技術的レビュー	12	3
84	14.2.4	パッケージソフトウェアの変更に対する制限	1	5
85	14.2.5	セキュリティに配慮したシステム構築の原則	8	7
86	14.2.6	セキュリティに配慮した開発環境	12	10
87	14.2.7	外部委託による開発	18	33
88	14.2.8	システムセキュリティの試験	8	36
89	14.2.9	システムの変更管理手順受入れ試験	2	48
90	14.3.1	試験データの保護	1	4
91	15.1.1	供給者関係のための情報セキュリティの方針	16	14
92	15.1.2	供給者との合意におけるセキュリティの取扱い	30	21
93	15.1.3	ICTサプライチェーン	6	10
94	15.2.1	供給者のサービス提供の監視及びレビュー	2	24
95	15.2.2	供給者のサービス提供の変更に対する管理	12	12
96	16.1.1	責任及び手順	1	13
97	16.1.2	情報セキュリティ事象の報告	18	24
98	16.1.3	情報セキュリティ弱点の報告	8	6
99	16.1.4	情報セキュリティ事象の評価及び決定	6	4,380
100	16.1.5	情報セキュリティインシデントへの対応	18	5,475
101	16.1.6	情報セキュリティインシデントからの学習	8	2
102	16.1.7	証拠の収集	18	6,570
103	17.1.1	情報セキュリティ継続の計画	10	4
104	17.1.2	情報セキュリティ継続の実施	16	6
105	17.1.3	情報セキュリティ継続の検証，レビュー及び評価	12	9
106	17.2.1	情報処理施設の可用性	12	3
107	18.1.1	適用法令及び契約上の要求事項の特定	18	3
108	18.1.2	知的財産権	12	396
109	18.1.3	記録の保護	12	108
110	18.1.4	プライバシー及び個人を特定できる情報の保護	18	6
111	18.1.5	暗号化機能に対する規制	2	4
112	18.2.1	情報セキュリティの独立したレビュー	1	18
113	18.2.2	情報セキュリティのための方針群及び標準の準拠	2	144
114	18.2.3	技術的遵守のレビュー	2	72
合計			1,521	61,779

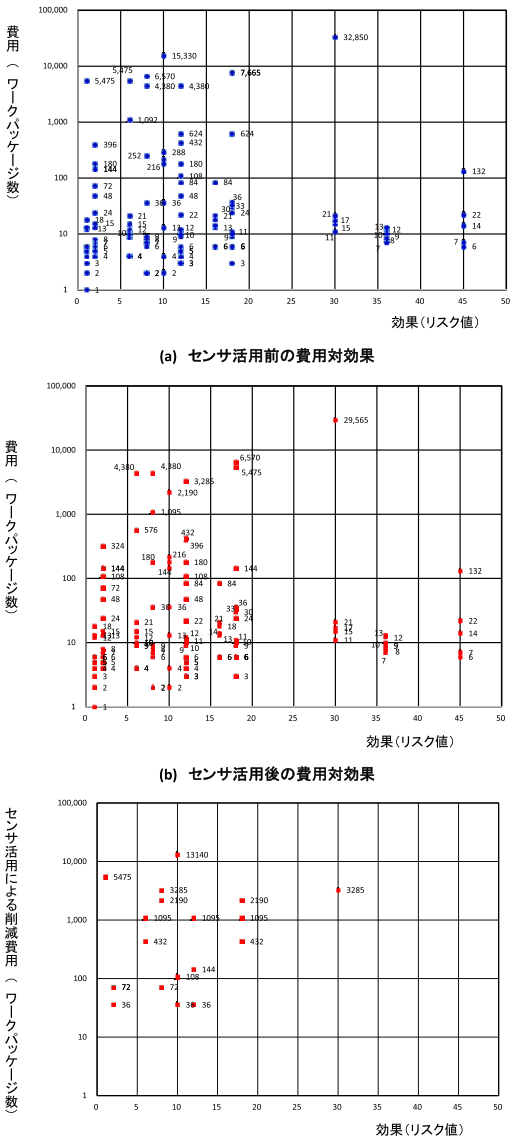

図 8 センサ活用に関わる費用対効果

Fig. 8 Cost effectiveness with sensor utilization.

表 9 センサ活用による費用削減効果

Table 9 Cost reduction effect with sensor utilization.

	センサ活用前	センサ活用後
費用（WP 数）	96,069	61,779

これらにより，机上シミュレーションではあるが，ISMS に関する費用対効果を明らかにすることで，情報セキュリティエコノミクスの課題解決の一助とした．

今後の課題は，実際の ISMS 運用状況を調査することにより，費用算出の粒度向上を図ることである．また，ISMS においてセンサ等の IoT 技術を活用する際には，IoT 技術自体のセキュリティにも留意する必要があり，検討すべき重要な課題である．今後，CSA ジャパン（日本クラウドセキュリティアライアンス）における IoT セキュリティガイダンス [29] 等も参考にして検討を進めていく予定である．

謝辞 本研究は，JSPS 科研費 15H02783 の助成を受けたものです．

参考文献

[1] 日本規格協会：情報技術—セキュリティ技術—情報セキュリティ管理策の実践のための規範，JIS Q 27002(ISO/IEC 27002)（2014 年 3 月 20 日改正）．
[2] NPO：情報セキュリティインシデントに関する調査報告書，NPO（オンライン），入手先 ⟨http://www.jnsa.org/result/incident/⟩（参照 2016-06-07）．
[3] 宇崎駿介：情報セキュリティポリシーの現状，@IT（オンライン），入手先 ⟨http://www.atmarkit.co.jp/fsecurity/special/27spolicy/spolicy01.html⟩（参照 2016-06-07）．
[4] 警察庁：不正アクセス行為対策等の実態調査，警察庁（オンライン），入手先 ⟨http://www.npa.go.jp/cyber/research/h26/h26countermeasures.pdf⟩（参照 2016-06-07）．
[5] 情報セキュリティ大学院大学：セキュリティマネジメントの運用状況アンケート，情報セキュリティ大学院大学（オンライン），入手先 ⟨http://lab.iisec.ac.jp/˜harada_lab/survey/2011/2011_questionnaire_result.pdf⟩（参照 2016-06-08）．
[6] IPA：情報セキュリティエコノミクスの挑戦，IPA（オンライン），入手先 ⟨https://www.ipa.go.jp/files/000026120.pdf⟩（参照 2016-06-08）．
[7] 通信とセンサーに見る最新技術動向 PART 3：IT Leaders（オンライン），入手先 ⟨http://it.impressbm.co.jp/articles/-/9864?page=4⟩（参照 2016-06-08）．
[8] 総務省：センサーの進展，第 4 回 ICT 共通基盤技術検討ワーキンググループ（オンライン），入手先 ⟨http://www8.cao.go.jp/cstp/tyousakai/innovation/ict/4kai/siryo3-3.pdf⟩（参照 2016-06-08）．
[9] トリリオン・センサー（Trillion Sensors），IoT{Internet of Things / まとめ}（オンライン），入手先 ⟨http://ur0.xyz/sspN⟩（参照 2016-06-08）．
[10] 佐々木良一：IT リスク学の提案と最近の動向，情報処理学会論文誌，Vol.55, No.9, pp.1946–1955 (2014).
[11] 内田勝也ほか：ISMS 認証事業所調査からみたセキュリティマネジメントの課題，情報処理学会研究報告 (2012).
[12] 堀川博史ほか：デルタ ISMS モデルの提案，情報処理学会研究報告 (2015).
[13] 上田哲史ほか：組織評価と ISMS，情報処理学会研究報告 (2012).
[14] 松浦健二：大学における ISMS 準拠のセキュリティポリシ策定に関する一考察，情報処理学会研究報告 (2004).
[15] 高橋雄志ほか：国際標準に基づいたセキュリティ評価プラットフォームの有効性の検討，情報処理学会研究報告 (2009).
[16] 長谷川孝博ほか：ISMS から ITSMS への取り組みについて，情報処理学会研究報告 (2012).
[17] 水沼彩子ほか：ISMS 認証取得及びその継続における課題と解決策について，情報処理学会研究報告 (2009).
[18] 小松文子ほか：情報セキュリティ対策における個人の利得と認知構造に関する実証研究，情報処理学会論文誌，Vol.51, No.9, pp.1711–1725 (2010).
[19] Tanimoto, S. et al.: Quantifying Cost Structure of Campus PKI Based on Estimation and Actual Measurement, *Journal of Information Processing*, IPSJ, Vol.20, pp.640–648 (2012).
[20] Tanimoto, S. et al.: A Study of Cost Structure Visualization for Digital Forensics Deployment, *2nd ACIS International Conference on Computational Science and Intelligence 2015*, pp.167–170 (2015).
[21] 岡本 薫ほか：マルチコプターを用いたサイバー攻撃に対する一検討，*DICOMO2014* (2014).
[22] Yoneda, S. et al.: Cost Reduction Effect on Running

Costs in ISMS Based on Sensors, *2015 IEEE 4th Global Conference on Consumer Electronics* (*GCCE 2015*), pp.630–31 (2015).
[23] PMI：プロジェクトマネジメント知識体系ガイド第 4 版 (2008).
[24] 畑健一郎ほか：情報セキュリティマネジメントシステムにおけるスローポリシー導入に関する検討，電子情報通信学会技術研究報告：信学技報 LOIS2014-55, pp.91–96 (2015).
[25] JIPDEC：ISMS 認証取得について，JIPDEC（オンライン），入手先 ⟨http://www.isms.jipdec.or.jp/ninsyou/⟩（参照 2016-06-09）.
[26] 佐藤周行他：情報セキュリティ基盤論，共立出版 (2010).
[27] 岡本卓馬：情報セキュリティにおけるリスクの定量化手法，*UNISYS TECHNOLOGY REVIEW*, No.86, pp.236–246 (2005).
[28] Hata, K. et al.: A Proposal of Slow Policy Level based on Cost-effectiveness of ISMS's Countermeasure, *Proc. 9th International Conference on Project Management* (*ProMAC2015*), pp.B19-124–B19-129 (2015).
[29] CSA ジャパン：IoT 早期導入者のためのセキュリティガイダンス, CSA ジャパン（オンライン），入手先 ⟨https://www.cloudsecurityalliance.jp/newsite/?p=1703⟩（参照 2016-06-24）.

付　　録

A.1 センサ代替可能チェックリストならびに WP 削減効果の算出

No.	C2項目（23項目）に分類されるISMS管理項目	ワークパッケージ		代替センサ可否チェック（○：代替可能）					センサ代替可能なWP数	3年間の繰返回数	センサ活用によるWP削減数
		ワークパッケージの内容	WP数	ICタグ	測位センサ	監視カメラ	マイク	圧力センサ			
1	8.1.1 資産目録	情報のライフサイクルに関連した資産を特定する	5						0	36	0
		情報のライフサイクルの重要度を文書化する									
		文書を，専用の目録又は既存の目録として維持する									
		資産目録は，正確かつ最新に保ち一貫性を持ち他の目録と整合させる									
		特定された資産は管理責任者を割り当て分類する									
2	8.1.2 資産の管理責任	資産の目録を確実に作成する	4	○					1	36	36
		資産を適切に分類及び保護をする									
		適用されるアクセス制御方針を考慮に入れ，重要な資産に対するアクセスの制限及び分類を定め，定期的にレビューする									
		資産を消去又は破壊する場合に，適切に取り扱うことを確実にする									
3	8.3.1 取外し可能な媒体の管理	再利用可能な媒体を組織から移動する場合に，その内容が以後不要であるならば，これを復元不能とする	11						2	36	72
		必要かつ実際的な場合には，組織から移動する媒体について，認可を要求する									
		媒体の移動について，監査証跡の維持のために記録を保管する		○		○					
		全ての媒体は，製造業者の仕様に従って，安全でセキュリティが保たれた環境に保管する									
		データの機密性又は完全性が重要な考慮事項である場合は，取外し可能な媒体上のデータを保護するために，暗号技術を用いる									
		保管されたデータがまだ必要な間に媒体が劣化するリスクを軽減するため，読みだせなくなる前にデータを新しい媒体に移動する									
		価値の高いデータは，一斉に損傷又は消失するリスクをより低減するために，複数の複製を別の媒体に保管する									
		データ消失の危険性を小さくするために，取外し可能な媒体の登録を考慮する		○							
		取外し可能な媒体のドライブは，その利用のための業務上の理由があるときにだけ有効とする									
		取外し可能な媒体を用いる必要がある場合，媒体への情報の転送を監視する									
		取外し可能な媒体の管理の手順及び認可のレベルは，文書化する									
4	8.3.3 物理的媒体の輸送	信頼できる輸送機関又は運送業者を用いる	5						2	36	72
		認可された運送業者の一覧について，管理者の合意を得る									
		運送業者を確認する手順を導入する									
		輸送途中に生じるかもしれない物理的損傷から内容を保護，するため梱包を十分な強度とし，また，製造業者の仕様にも従う		○							
		媒体の内容，適用された保護，並びに輸送の責任窓口への受渡時刻及び目的地での受け取り時刻の記録を特定するログを保持する		○		○					
5	11.1.1 物理的セキュリティ境界	それぞれの境界の位置及び強度は，境界内に設置している資産のセキュリティ要求事項及びリスクアセスメントの結果に基づき，物理的境界を定める	8						3	36	108
		情報処理施設を収容した建物又敷地の境界は，境界には隙間がなく，又は容易に侵入できる箇所がないように物理的に頑丈にする									
		敷地又は建物への物理的アクセスを管理するための有人の受付又はその他の手段を備える		○		○					
		敷居及び建物へのアクセスは，認可された要員にだけ制限する		○							
		認可されていない物理的アクセス及び周囲への悪影響を防止するため，適用できる場合は，物理的な障壁を設置する									
		セキュリティ境界上にある全ての防火扉は，該当する地域標準，国内標準及び国際標準が要求するレベルの抵抗力を確立するため，壁と併せて，警報機能を備え，監視し，試験する									
		全ての外部に接する扉及びアクセス可能な窓を保護するため，侵入者を検知する適切なシステムを，地域標準，国内標準に沿って導入し，予めしたがって試験する			○	○	○	○			
		組織が自ら管理する情報処理施設は，外部関係者が管理する施設から物理的に分離する									
6	11.1.2 物理的入退管理策	訪問者の入退の日付及び時刻を記録する	7	○		○			6	2,190	13,140
		アクセスが事前に承認されている場合を除き，全ての訪問者を監督する		○		○					
		適切なアクセス制御の実施によって，秘密情報を処理又は補完する領域へのアクセスを認可された者だけに制限する		○		○					
		全てのアクセスについて，物理的な記録日誌又は電子形式の監査証跡を，セキュリティを保って維持及び監視する		○		○					
		セキュリティを保つべき領域では，目に見える証明書の着用を要求し，関係者が付き添っていない訪問者及び目に見える証明書を着用していない者を見かけた場合は，直ちにセキュリティ要員に知らせる体制を作る		○		○					
		セキュリティを保つべき領域又は秘密情報処理施設への，外部のサポートサービス要員によるアクセスは，限定的かつ必要なときにだけ許可し，このアクセスは許可を必要とし，監視する		○		○					
		セキュリティを保つべき領域へのアクセス権は，定期的にレビューし，更新し，必要な時には無効にする									
7	11.1.4 外部及び環境の脅威からの保護	火災からの損害を回避する方法について，専門家の助言を得る	6						0	36	0
		洪水からの損害を回避する方法について，専門家の助言を得る									
		地震からの損害を回避する方法について，専門家の助言を得る									
		爆発からの損害を回避する方法について，専門家の助言を得る									
		暴力行為からの損害を回避する方法について，専門家の助言を得る									
		その他の考えうる自然災害又は，人的災害からの損害を回避する方法について，専門家の助言を得る									
8	11.1.5 セキュリティを保つべき領域での作業	要員は，セキュリティを保つべき領域の存在又はその領域内での活動を，知る必要性の原則に基づく範囲でだけ認識していることを考慮する	4						3	1,095	3,285
		安全面の理由の為及び悪意ある活動の機会を防止するための両面から，セキュリティを保つべき領域での監督されていない作業は，回避する		○		○					
		セキュリティを保つべき領域が無人のときは，物理的に施錠し，定期的に点検する		○		○					
		画像，映像，音声又はその他の記録装置は，認可されたもの以外は許可しない		○		○					
9	11.1.6受渡場所	建物外部からの受渡場所へのアクセスは，識別及び認可された要員に制限する	7	○		○			3	144	432
		受渡場所は，配達要員が建物の他の場所にアクセスすることなく荷積み及び荷降ろしができるように設計する									
		受渡場所はの外部扉は，内部の扉が開いているときにはセキュリティを保つ				○		○			
		入荷物は，受け渡し場所から移動する前に，爆発物，化学物質又はその他の危険物がないかを検査する									
		入荷物は，事業者へ持ち込むときに資産の管理手順に従って登録する									
		可能な場合には，入荷と出荷とは，物理的に分離した場所で行う									
		入荷物は，輸送中に開封された痕跡がないかを検査し，開封の痕跡が見つかった場合には，直ちにセキュリティ要員に報告する		○				○			
10	11.2.1 装置の設置及び保護	装置は，作業領域への不必要なアクセスが最小限になるように設置する	10						1	3,285	3,285
		取扱いに慎重を要するデータを扱う情報処理施設は，施設の使用中に認可されていない者が情報を覗き見るリスクを低減するため，その位置を慎重に定める									
		許可されていないアクセスを回避するために，保管設備のセキュリティを保つ				○					
		特別な保護を必要とする装置は，それ以外の装置と一緒にすると，共通に必要となる保護のレベルを増加させてしまうため，その保護のレベルを軽減するため，他と区別して保護する									
		潜在的な物理的及び環境的脅威のリスクを最小限に抑えるための管理策を採用する									
		情報処理施設の周辺での飲食及び喫煙に関する指針を確立する									
		情報処理施設の運用に悪影響を与えることがある環境条件を監視する									
		全ての建物に，落雷からの保護を適用し，全ての電力及び通信の引込線に避雷器を装着する									
		作業現場などの環境にある装置には，特別な保護方法の使用を考慮する									
		電磁波の放射による情報漏えいのリスクを最小限にするため，秘密情報を処理する装置を保護する									
11	11.2.2 サポートユーティリティ	装置の製造業者の仕様及び地域の法的要求事項に適合している	5						1	36	36
		事業の成長及び他のサポートユーティリティとの相互作用に適応する能力を，定期的に評価する									
		適切に機能することを確実にするため，定期的に検査及び試験をする									
		必要であれば，不具合を検知するための警報装置を取り付ける				○					
		必要であれば，物理的な経路が異なる複数の提供元を確保する									

No.	C2項目（23項目）に分類されるISMS管理項目	ワークパッケージ		代替センサ可否チェック（○：代替可能）					センサ代替可能なWP数	3年間の繰返回数	センサ活用によるWP削減数
		ワークパッケージの内容	WP数	ICタグ	測位センサ	監視カメラ	マイク	圧力センサ			
12	11.2.3 ケーブル配線のセキュリティ	情報処理施設に接続する電源ケーブル及び通信回線は，可能な場合には，地下に埋設するか，又はこれに代わる十分な保護手段を施す	6						2	1,095	2,190
		干渉を防止するために，電源ケーブルは，通信ケーブルから隔離する									
		取扱いに慎重を要するシステム又は重要なシステムのため，外部電線管の導入，点検個所・終端個所の施錠可能な部屋又は箱への設置を行う									
		ケーブルを保護するための電磁遮断の利用を行う									
		ケーブルに取り付けられた認可されていない装置の技術的探索及び物理的検査を行う				○					
		配線板，端子盤及びケーブル室へのアクセスを管理する		○		○					
13	11.2.4 装置の保守	装置は，供給者の推奨する間隔及び仕様に従って保守する	7						2	36	72
		認可された保守要員のみが，装置の修理及び手入れを実施する		○		○					
		故障と見られるもの及び実際の故障の全て，並びに予防及び是正のため保守の全てについての記録を保持する				○	○				
		装置の保守を計画する場合には，この保守を，要員が構内で行うのか，又は組織の外で行うのかを考慮し，適切な管理策を実施する									
		必要な場合には，装置から秘密情報を消去するか，又は保守要員が十分に信頼できる者であることを確かめる									
		保守約定で定められた，保守に関する全ての要求事項を順守する									
		保守の後，装置を作動させる前に，その装置が改竄されていないことを及び不具合を起こさないことを確実にするために検査する									
14	11.2.5 資産の移動	資産を構外に持ち出すことを許す権限をもつ従業員及び外部の利用者を特定する	4						3	144	432
		資産の持出し期限を設定し，また，返却がそのとおりであったかを検証する		○		○					
		必要かつ適切な場合は，資産が構外に持ち出されていることを記録し，また，返却時に記録する		○		○					
		資産を扱う又は利用する者について，その識別情報，役割及び所属を文書化し，この文書は，その装置，情報又はソフトウェアと共に返却させる		○		○					
15	11.2.6 構外にある装置及び資産のセキュリティ	構外に持ち出した装置及び媒体は，公共の場所に無人状態で放置しない	4						1	144	144
		装置の保護に関する製造業者の指示を常に守る									
		在宅勤務，テレワーキング及び一時的サイトのような構外の場所についての管理策を，リスクアセスメントに基づいて決定し，状況に応じた管理策を適切に適用する									
		構外にある装置を，複数の個人または外部関係者の間で移動する場合には，その装置の受渡記録を明記した記録を維持する		○			○				
16	11.2.8 無人状態にある利用者装置	実行していた処理が終わった時点で，接続を切る	4						1	1,095	1,095
		適切なロック機能によって保護する									
		利用の必要がなくなった場合，アプリケーション又はネットワークサービスからログオフを行う									
		コンピュータ又はモバイル機器は，利用していない場合，キーロック又は同等の管理策によって，認可されていない利用から保護する			○	○					
17	11.2.9 クリアデスク・クリアスクリーン方針	取扱いに慎重を要する業務情報又は重要な業務情報は，必要のない場合，特にオフィスに誰もいない際には施錠し保管する	5	○		○			5	1,095	5,475
		コンピュータ及び端末は，離籍時には，ログオフ状態にしておくか，又はパスワード，トークン若しくは同次の利用者認証機能で管理されたスクリーン及びキーボードのロック機能によって保護する．			○	○					
		コンピュータ及び端末を利用しないときは，施錠，パスワード又は他の管理策によって保護する			○	○					
		コピー機及びその他の再生技術の認可されていない利用は防止する		○		○					
		取扱いに慎重を要する情報又は機密扱い情報を含む媒体は，プリンタから直ちに取り出しておく		○	○						
18	16.1.4 情報セキュリティ事象の評価及び決定	連絡先の者は，合意された情報セキュリティ事象・情報セキュリティインシデントの分類基準を用いて各情報セキュリティ事象を評価する	5						1	1,095	1,095
		評価した各情報セキュリティ事象を情報セキュリティインシデントに分類するかを決定する									
		インシデントの分類及び優先順位付けは，インシデントの影響及び程度の特定に役立てる									
		情報セキュリティインシデント対応チームが存在する場合は，確認又は，再評価のため，評価及び決定の結果をこのチームに転送する									
		評価及び決定の結果は，以後の参照及び検証のため詳細に記録する				○	○				
19	16.1.5 情報セキュリティインシデントへの対応	情報セキュリティインシデントの発生後，できるだけ速やかに証拠を収集する	7						2	1,095	2,190
		必要に応じて，情報セキュリティの法的分析を実施する									
		必要に応じて，段階的取り扱いを行う									
		後で行う分析のために，関連するすべての対応活動を適正に記録することを確実にする				○	○				
		知る必要性を認められている内部・外部の他の要員又は組織に対し，情報セキュリティインシデントの存在または関連するその詳細を伝達する									
		インシデントの原因又はインシデントの一因であることが判明した情報セキュリティ弱点に対処する									
		インシデントへの対応が滞りなく済んだ後，正式にそれを終了し，記録する				○	○				
20	16.1.7 証拠の収集	管理状態の一連の履歴を考慮する	7			○	○		1	1,095	1,095
		証拠の保全を考慮する									
		要員の安全を考慮する									
		関与する要員の役割及び責任を考慮する									
		要員の力量を考慮する									
		文書化を考慮する									
		要点説明を考慮する									
21	18.1.2 知的財産権	ソフトウェア製品及び情報製品の合法利用を明確に定めた知的財産権遵守方針を公表する	12						1	36	36
		著作権を侵害しないことを確実にするために，ソフトウェアは，知名度の高い，かつ，定評のある提供元だけを通じて取得する									
		知的財産権を保護するための方針に対する認識を持続させ，それらの方針に違反した要員に対して懲罰処置をとる意思を通知する									
		適切な資産登録簿を維持・管理し，知的財産権の保護が求められている全ての資産を特定する									
		使用許諾を得ていることの証明及び証拠，マスタディスク，手引きなどを維持・管理する		○		○					
		使用許諾で許可された最大利用者数を超過しないことを確実するための管理策を実施する									
		認可されているソフトウェア及び仕様許諾されている製品だけが導入されていることのレビューを行う									
		適切な使用許諾条件を維持・管理するための方針を定める									
		ソフトウェアの処分又は他人への譲渡についての方針を定める									
		公衆ネットワークから入手するソフトウェア及び情報の使用条件に従う									
		著作権法が認めている場合を除いて，商用記録を複製，他形式に変換，又は抜粋しないことを徹底する									
		著作権法が認めている場合を除いて，書籍，生地，報告書又はその他文書の全部または一部を複写しない									
22	18.1.3 記録の保護	記録及び情報の保持，保存，取り扱い処分に関する指針を発行する	3						0	36	0
		記録及びそれらの記録の保持することが望ましい期間を明確にした保持計画を作成する									
		主要な情報の出典一覧を維持・管理する									
23	18.2.2 情報セキュリティのための方針群及び標準の遵守	不順守の原因を特定する	4						0	36	0
		遵守を達成するための処置の必要性を評価する									
		適切な是正処置を実施する									
		是正処置の有効性を検証し，又不備は弱点を特定するために，とった是正処置をレビューする									
合　計			140						41		34,290

米田 翔一

2014 年千葉工業大学大学院社会システム科学研究科マネジメント工学専攻修士課程修了．現在，同博士後期課程在籍．情報セキュリティマネジメントに関する研究に従事．プロジェクトマネジメント学会会員．

畑 健一郎

2016 年千葉工業大学大学院社会システム科学研究科マネジメント工学専攻修士課程修了．在学中情報セキュリティマネジメントに関する研究に従事．現在，まいばすけっと株式会社社員．

下村 道夫

1988 年早稲田大学理工学部電子通信学科卒業，1993 年同大学院電気工学専攻博士後期課程修了．同年日本電信電話株式会社入社．以来，高度インテリジェントネットワーク，SIP 対応ファイアウォール，DNS，シングルサインオン等のサーバソフトウェアの研究開発，ネットワーク活用新サービス創出の研究に従事．2012 年津田塾大学非常勤講師．2012 年法政大学兼任講師，2014 年より千葉工業大学社会システム科学部プロジェクトマネジメント学科教授，現在に至る．博士（工学）．電子情報通信学会，プロジェクトマネジメント学会各会員．

谷本 茂明 （正会員）

1982 年徳島大学工学部電気工学科卒業．1984 年同大学大学院工学研究科電気工学専攻修了．同年日本電信電話公社入社．主にプライベートネットワークシステムにおける研究開発に従事．2009 年千葉工業大学社会システム科学部准教授．2012 年より教授．現在，情報セキュリティマネジメント，特に PKI 応用，クラウドセキュリティ等の研究に従事．博士（工学）．電子情報通信学会シニア会員，プロジェクトマネジメント学会，日本経営工学会，IEEE 各会員．本会シニア会員．

佐藤 周行 （正会員）

1985 年東京大学卒業，1990 年同大学大学院修了．理学博士．現在，東京大学情報基盤センター准教授，2005 年より国立情報学研究所客員准教授．専門は，コンピュータサイエンス，情報セキュリティ．日本ソフトウェア科学会，ACM，IEEE 各会員．

金井 敦 （正会員）

1980 年東北大学工学部通信工学科卒業．1982 年同大学大学院工学研究科情報工学科博士前期課程修了．同年日本電信電話公社電気通信研究所入社．ソフトウェア開発プロセス，ソフトウェア分散開発環境，Web サービス開発技術，ネットワークコミュニティ，情報セキュリティ，ネットワークセキュリティの研究開発に従事．2008 年から現在，法政大学理工学部応用情報工学科教授．博士（情報科学）．著書に『攻めと守りのシステムセキュリティ』等．電子情報通信学会シニア会員，IEEE 会員．本会シニア会員．