千葉工業大学
博士学位論文

# オフィス空間における
# 場のセキュリティを考慮した
# センサ活用に基づく
# リスクマネジメントに関する研究

平成 29 年 3 月
米田　翔一

# 論文要旨

1. 研究背景

近年，情報化社会の急速な進展に伴い，ビッグデータやオープンデータなどデータサイエンスに代表されるように，情報が持つ価値は大きくなってきているが，その反面，様々な脅威も顕在化しており，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，企業などでは様々な対策が行われており，例えば，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；情報セキュリティマネジメントシステム）である [1].

しかし，例えば，2015 年におけるサイバー犯罪の検挙件数は 8,096 件という結果を見ると，情報セキュリティは未だ完全とは言い切れず，例えば ISMS においても，その導入により情報セキュリティに関するリスクを軽減することが期待できるが，費用面などの観点から実際に導入することが難しい現状がある [2]．さらに，新たな脅威として，技術の進展に伴い，例えば，ドローンが首相官邸の屋上に不法に着陸するなどの物理的脅威も増えてきており，従来の情報セキュリティだけでなく，物理面の観点からのセキュリティ対策も重要となってきている [3]．これに対し，近年，IoT (Internet of Things)の利用が進んできており，特に，小型化，高精度化でかつ低価格化が進展しているセンサ技術の活用が期待されている [4]．特に，RFID（Radio Frequency IDentification）や監視カメラなどにより，物理的な状況をリアルタイムに把握する活用が注目されており，情報セキュリティマネジメントにおいてもより柔軟性の高いシステムとして期待されている．

2. 研究目的

本論文では，これらの背景の下，企業を対象にミッションクリティカルな情報，即ち，様々な機密情報を取り扱うオフィス空間を対象に，物理面の観点も加味した情報セキュリティマネジメントを新たに提案する．一般に，企業のオフィス空間では，セキュリティに関わる脅威が動的に変化する．即ち，TPO（Time, Place, Occasion）条件によりセキュリティレベルは時々刻々と変化する．これを場のセキュリティと新たに定義し，このように様々な脅威にさらされているオフィス空間におけるリスクアセスメントを行い，さらにその対策案を提案することにより，企業における安心安全な IT ガバナンスに寄与する．

3. 研究結果

3.1 センサ活用による場のセキュリティを考慮したリスクアセスメント

企業を対象に，新たに物理的な観点を加味した，即ち，TPO 条件に基づくオフィス空間における場のセキュリティに対するリスクアセスメントを行った．最初に，リスクマネジメントの代表的手法である RBS（Risk Breakdown Structure）手法により，27 項目のリスク要因を網羅的に抽出した．次に，これら 27 要因に対し，同様に一般的手法であるリスクマトリクス手法に基づき，リスク分析を行った．これにより，ISMS に基づく社員教育の徹底や，導入を容易にする観点からセンサ活用等の対策の重要性を示した [5]．さらに，抽出したリスク要因に対するリスク値を近似計算し，対策前後のリスク値の比較結果から，対策案によるリスク削減効果が 55%であることを示し，定量的観点からも対策案の有効性を明らかにした [6].

3.2 センサ活用による場のセキュリティのリスクマネジメント

ここでは，3.1 で導出した対策案の具現化例により，実用性の観点から対策案の有効性を明らかにする．

(1) TPO 条件に基づく最適クラウド選択

一般に，オフィス空間では，リスクレベルが TPO 条件に応じて動的に変化している．これに対し，近年，企業でも多く活用されている複数クラウドの利用環境を対象に，リスクレベルに応じた最適なクラウドを選択することで対処する手法を提案する．最初に，各クラウドのセキュリティポリシを CSA(Cloud Security Alliance)のガイドラインを基に可視化し，オフィスのリスクレベルを TPO 条件に基づき定量化した．次に，クラウドのセキュリティポリシとオフィスのリスク値を閾値でクラスタリングした結果を機械的に対応させることで，リスク値に応じたクラウドを自動選択可能とした．これにより，TPO 条件による，よりセキュアなクラウド利用が可能となることを示した [7].

(2) センサを活用した ISMS の ROSI(Return on Security Investment)効率化

一般に，ISMS は企業のセキュリティ指針として有効と考えられているが，コストの問題などの観点からその普及は充分ではない．ここでは，コスト削減の観点から，低価格化，高精度化が進んでいるセンサの活用による ISMS の人的稼働の低減化を新たに提案する．最初に，ISMS のコスト構造を「ISMS 実施の手引」を参考に積算法並びに机上シミュレーションにより，そのコスト要因が 140 項目であることを明らかにした．次に，この結果に基づき，これらのコスト要因における人的稼動がコストネックとなることに着目し，このネック要因をセンサで代替可能かを検討した．その結果，現実的な観点を加味し，即ち，運用条件などの現実的な条件を考慮し，詳細に分析を行った．その結果，センサ活用により，人的稼動を約 36%低減することが可能であることを明らかにした [8]-[9].

## 4. 結論

本論文では, IoT など新しい技術が進展するにつれ, その脅威も高度化しているのに対し，企業の安心安全な IT ガバナンスに寄与するために，オフィス空間を対象に情報セキュリティの観点に物理セキュリティの観点を加えた，即ち，オフィス空間における場のセキュリティを考慮したリスクマネジメントを新たに提案した．この結果，オフィス空間において，新たにセンサ活用により，ISMS 導入の普及促進ならびに物理的な脅威に対するリスク低減に寄与しうることを明らかにし，企業におけるさらなる安心安全な IT ガバナンス形成に寄与しうることを示した．

今後，本提案を基にした，センサ活用による TPO 条件に応じた柔軟性の高いセキュリティシステムの具現化により，さらに利便性と機密性の両立を可能とする IT 基盤の構築の一助となることが期待できる．

## 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, http://www.jnsa.org/result/incident/,（参照 2016-06-07）

[3] 坂井俊亮他：画像認証における秘密情報の横流し耐性実験―ランダムアートを中心として―，電子情報通信学会論文誌，Vol.J97-D, No.5, pp.944-952, 2014

[4] 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），http://it.impressbm.co.jp/articles/-/9864?page=4,（参照 2016-06-08）

[5] 米田翔一他：オフィス空間における場のセキュリティを考慮したリスクアセスメント，第 13 回情報科学技術フォーラム（FIT 2014）査読付き論文，RO-006，2014 年 9 月

[6] Shoichi Yoneda, et al.，Risk Assessment in Cyber-physical System in Office Environment, Network-Based Information Systems (NBiS),2015 18th International Conference on, NBiS2015, pp.412-417, Sep.2015

[7] 米田翔一他：TPO 条件に基づく複数クラウドにおける動的クラウド選択手法の提案，電子情報通信学会論文誌，Vol.J99-D, No.10, PP.1045-1049，2016 年 10 月
[8] Shoichi Yoneda, Shigeaki Tanimoto, Michio Shimomura, Hiroyuki Sato, Atsuhi Kanai, Cost Reduction Effect on Running Costs in ISMS Based on Sensors, IEEE 4th Global Conference on Consumer Electronics, GCCE2015, pp.630-631, Oct., 2015
[9] 米田翔一他：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，情報処理学会論文誌，第 57 巻 第 12 号 PP.2743-2756, 2016

## Abstract

1. Introduction of Study

Recently, Cybercrime is becoming a bigger threat because of the rapid progress of the Internet. Therefore, the importance of information security is also increasing. Accordingly, an information security management system (ISMS) is considered to be effective as a security guideline for the organization of companies. Generally, an ISMS performs a risk assessment of the organization of companies and defines the necessary security level. Thus, reducing the risks related to information security in company is possible by introducing such an ISMS. By the way, new threat of physical security, such as drone to land on the roof of the Prime Minister's Office, are increasing. Thus, it is becoming important not only information security but also physical security. For the information security considering physical security, sensor technology is expected to be used. Because, sensor technology is progressing rapidly, miniaturization, high accuracy and price reduction. Furthermore, sensor technology, as typified by a surveillance camera which is the use of a physical state acquisition section, has attracted attention. So, in the information security, sensor technology is expected to be used for more flexible system considering with physical security.

2. Purpose of Study

As mentioned above, we propose a new information security management that considering physical state in office environment, such as using a variety confidential information. Generally, in office environment, threats related to security are changing dynamically by TPO (Time, Place, and Occasion) conditions. Here, we newly defined this environment as a security field. In this way, perform a risk assessment to the security field in office environment. And, we newly propose a countermeasure of information security with physical security to contribute a secure and safety IT governance.

3. Result of Study

3.1. Risk assessment of the security field

Generally, there are various threats in office environment. However, researches of the security field, such as investigation of both the risk of information security and physical security, are not enough. Here, we do a risk assessment against the security field in office environment considering physical security. First, Twenty-seven risk factors were comprehensively extracted by the RBS (Risk Breakdown Structure) method, which is a typical method in the risk management field. Next, the risk analysis is conducted by using the risk matrix method, which is a general method in the risk management field. Thus, the risk matrix method was used to deduce countermeasures. Furthermore, risk values were introduced for use in an ISMS quantitative evaluation for detailed risk assessment. This quantitative evaluation clearly showed that the proposed countermeasures can reduce risks by about 55%.

3.2. Risk management of the security field by sensor utilization

(1) The optimal Cloud selection based on TPO conditions

Generally, in office space, the risk level is changing dynamically according to TPO conditions. By the way, multiple Cloud is used also in the company in recent years. Here, the method of selecting the optimal Cloud according to a risk level is newly proposed for multiple Cloud utilizing environment of such a company. First, each Cloud's security policy was visualized according to the

guideline of CSA (Cloud Security Alliance). Furthermore, about the risk level of an office, it quantified according to TPO conditions of an office. Next, the risk level of each Cloud's security policy and the office risk value (it clusters with a threshold value) were made to match mechanically. Accordingly, auto select of the optimal Cloud according to an office risk value was made available. As mentioned above, by being based on the TPO conditions of an office showed that the optimal Cloud selection was achieved.

(2) Increase in efficiency of the security investment effect of ISMS by sensor utilization

In general, ISMS is considered to be effective as a security guideline for the organization of companies. However, because of such as cost problem of ISMS introduction, generally, ISMS introduction rate of the company are not enough. Here, we newly propose a reduction of human operation with sensor technology to reduce the cost of ISMS introduction. First, clarify the cost structure of ISMS by integration method and a work simulation based on “code of practice for information security controls” of ISMS. So, we investigated substitute items of the human operation based on sensor technology in detail. As this result, we clarify that human operation can about 36% reduced by the sensor technology.

4. Conclusion of Study

In this study, we newly proposed the new risk management to contribute a secure and safety IT governance in companies. Concretely, we proposed risk management of the security field, such as information security with considering of physical security. As a result, by use of sensor technology, we clarified promotion of ISMS and a countermeasure for threat of physical.

In future, by realize a more flexible security system by sensor technology, it can expect to contribute IT infrastructure that have high convenience and high confidentiality.

目次

# 1. 序論

## 1.1 背景

近年，情報化社会の急速な進展につれ，ビッグデータやオープンデータなど，データサイエンスに代表されるように，情報が持つ価値は大きくなってきている．それに伴って，サイバー犯罪などの様々な脅威も顕在化しており，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，企業など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[1-1]. 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（Plan・Do・Check・Action）モデルを採用し情報資産の機密性，可用性，完全性をバランスよく維持し，継続的な改善を行っていくものである．

しかしながら，2015 年には 8,096 件というサイバー犯罪の件数を見ると，情報セキュリティは未だ安全とは言い切れず，例えば ISMS についても，導入することによって，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[1-2]-[1-3]. 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挙げられている[1-4]. 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な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過ぎると回答している [1-5]. 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[1-6]. 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センサ技術の活用による解決が考えられている[1-7]-[1-8].

このセンサ技術に関しては，近年，著しく進展してきている IoT (Internet of Things)が顕在化してきていることが挙げられる．即ち，IoT は，小型化，高精度化，高集積化，低価格化が急速に進展してきており，様々な分野で注目されてきている [1-7]-[1-8]. 特に，センサ技術の活用が期待される．このセンサ技術は，IoT や CPS (Cyber-Physical System)，トリリオン・センサー等 [1-9]に代表されるように，M2M（Machine to Machine）システムにおいて，物理的な状況把握手段への活用が注目されていることから，情報セキュリティにおいても，物理的な状況を考慮した，より柔軟性の高いシステムへの活用が期待できる．

また，ショルダーハッキングなどの人為的なセキュリティの脅威や，ドローンが首相官邸の屋上に不法に着陸するなど，物理的な脅威も増えてきており，情報セキュリティだけでなく，物理面の観点からのセキュリティ対策も重要となってきている．

他方，クラウドの進展に伴い，データセンターが数多く構築されているが，このようなデータセンターでは，厳格な入退室管理が行われている．このように，情報セキュリティに加え物理セキュリティも加味したセキュリティマネジメントが重要になってきている[1-10]-[1-13]. 一般に，守るべき情報資産の価値や脅威は， TPO（時間，場所，機会）条件に応じて常に変化する．このような場合を考慮すると，従来の情報セキュリティに加え，物理セキュリティも加味した総合的なセキュリティの考え方が重要となってくる．しかし，これまでにこのような総合的なセキュリティに言及した研究は十分では無い．

## 1.2　目的

本論文では，これらの背景の下，企業を対象に，ミッションクリティカルな情報，即ち，様々な機密情報を取り扱うオフィス空間を対象とし，TPO 条件によって動的に変化する様々な脅威に対し，従来の情報セキュリティに新たに物理的な観点を加えた情報セキュリティを「場のセキュリティ」と定義する．この場のセキュリティ，即ち，物理的な観点を加えることにより，従来の情報セキュリティの観点からオフィスにおける TPO 条件を加味した動的な観点からより総合的かつ網羅的にリスク要因を抽出し，リスクアセスメントする．即ち，オフィス空間という場に対し，物理セキュリティと情報セキュリティの両面からリスク要因を網羅的に抽出し，定量的に評価する．さらに，具体的なリスク対策を可能とするために，定量的に評価した結果を基にリスク要因を可視化する．

以上により，従来の情報セキュリティによるリスクマネジメントに対し，新たに場のセキュリティとして，物理的な観点，特に TPO 条件を加味することにより，動的な観点からオフィスのセキュリティを総合的かつ網羅的にとらえることにより，１）新たなリスクマネジメントの提案，２）ISMS 普及促進への寄与，を具現化し，オフィス空間の，より安心安全な IT 基盤形成に寄与する．

## 1.3　本論文の構成

本論文は，図 1-1 のように構成する．

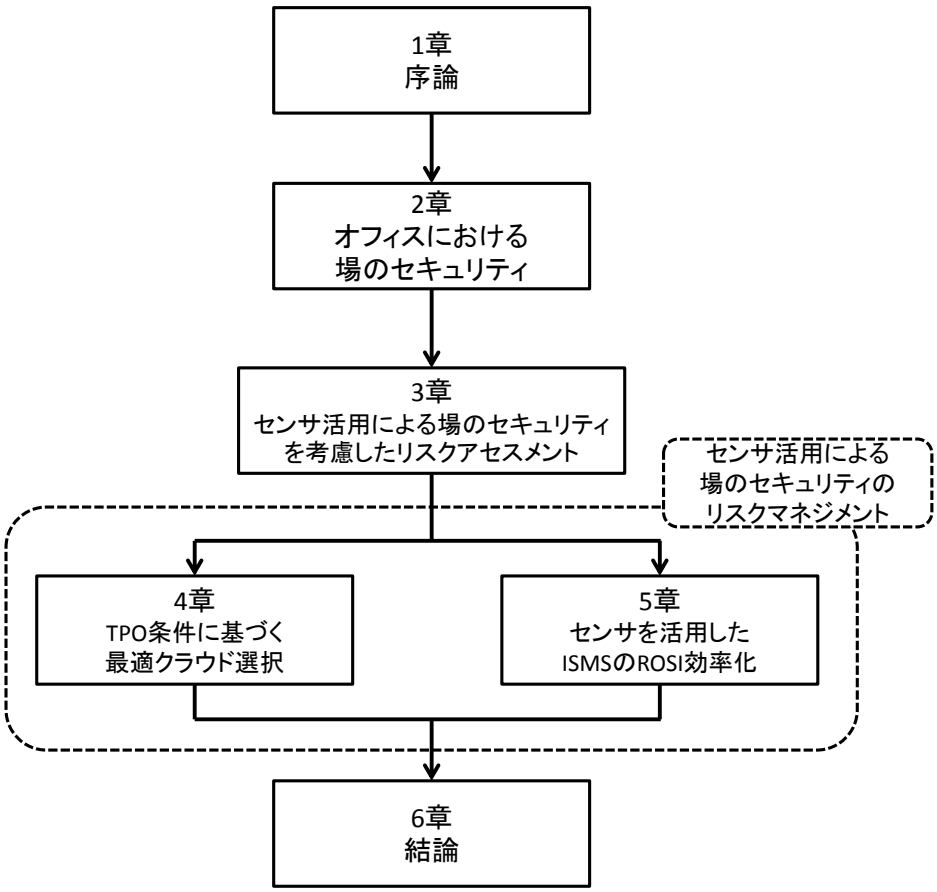



図 1-1　本論文の構成

第 1 章では，本論文の背景及び目的，構成について述べる．

第 2 章では，本論文で新たに提案する場のセキュリティについて，その背景ならびに必要性について具体的に述べる．即ち，オフィス環境を対象に，現状の情報セキュリティ及び物理セキュリティについて述べ，場のセキュリティを定義する．次に，場のセキュリティにおける脅威を基に，現状の課題を明らかにする．

第 3 章では，第 2 章で定義した場のセキュリティに対し，これらのリスク要因を，網羅的に抽出するためにリスクアセスメントを行った結果について示す．具体的には，オフィス空間における場のセキュリティを考慮したリスクアセスメントとして，情報セキュリティの観点に物理セキュリティの観点を加えたリスク分析を行い，リスク要因を抽出し，これらのリスク要因に対し，リスクマトリクス手法に基づきリスク対策案を提案し，情報セキュリティに物理セキュリティを加味した総合的なセキュリティ対策を明らかにする．

次に，第 4 章と第 5 章では，第 3 章のリスクアセスメント結果に対する評価として，新たにセンサの活用をポイントにリスクマネジメントとしての対策案について述べる．

第 4 章では，第 3 章のリスクアセスメント結果を踏まえ，動的な要因として TPO 条件に着目したリスクマネジメントを新たに提案する．具体的には，一般に，企業では，複数クラウドの利用がなされている．この点に着目し，オフィスにおける複数クラウド選択に対し，TPO 条件に応じてセキュアな観点から最適なクラウドを選択する手法を提案し，その有効性について評価した結果について述べる．

第 5 章では，ISMS 普及促進に寄与する観点から，センサ活用によるリスクマネジメント対策による効果について述べる．具体的には，オフィスにおいて，監視カメラなどの，物理セキュリティが用いる各種センサを情報セキュリティマネジメントと組み合わせることによるコストの低減化，特にセンサが人的稼働を軽減出来ることを定量的に検証した結果を中心に，その有効性を評価した結果について述べる

最後に，第 6 章にて，本論文の結論について述べる．

なお，付録として，第 5 章に記した ISMS に関わる費用対効果，特に費用面を導出するに際し，現状の ISMS の規定項目を基に簡潔にとりまとめた結果を示す．

## 参考文献


[1-1]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

[1-2]NPO：情報セキュリティインシデントに関する調査報告書, http://www.jnsa.org/result/incident/,（参照 2016-06-07）

[1-3]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）, http://www.atmarkit.co.jp/fsecurity/special/27spolicy/spolicy01.html,（参照 2016-06-07）

[1-4]警察庁：不正アクセス行為対策等の実態調査, http://www.npa.go.jp/cyber/research/h26/h26countermeasures.pdf,（参照 2016-06-07）

[1-5]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, http://lab.iisec.ac.jp/~harada_lab/survey/2011/2011_questionnaire_result.pdf,（参照 2016-06-08）

[1-6]IPA：情報セキュリティエコノミクスの挑戦，https://www.ipa.go.jp/files/000026120.pdf,（参照 2016-06-08）

[1-7]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）, http://it.impressbm.co.jp/articles/-/9864?page=4,（参照 2016-06-08）

[1-8]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），http://www8.cao.go.jp/cstp/tyousakai/innovation/ict/4kai/siryo3-3.pdf,（参照 2016-06-08）

[1-9]トリリオン・センサー（Trillion Sensors）, IoT {Internet of Things / まとめ}（オンライン）, http://ur0.xyz/sspN,（参照 2016-06-08）

[1-10]　米田翔一，牧野駿，谷本茂明，佐藤周行，金井敦：動的リスク評価に基づくセキュリティ場の提案, プロジェクトマネジメント学会 2013 年度春季研究発表大会, 1501, pp303-307，2013

[1-11]　榎本真也，金井敦，谷本茂明，佐藤周行：ダイナミックに制御する情報漏洩対策システムの検討，FIT2012，L-034, 2012

[1-12]　末次正人，榎本真也，金井敦，谷本茂明，佐藤周行：侵入者の距離によりダイナミックにセキュリティレベルを制御するシステムの検討，情報処理学会研究報告. 2013-CSEC-60(25), 1-6, 2013-03-07

[1-13]　谷本茂明，関良明，木村義政，木内陽介：個人のコンテキスト情報に基づく動的多重帰属グループサービスの提案，情報処理学会論文誌，Vol.51, No.2，575-589，2010

## 2. オフィスにおける場のセキュリティ

ここでは，本論文で新たに提案する「場のセキュリティ」について，その背景ならびに必要性について明らかにする．具体的には，オフィス環境を対象に，現状の情報セキュリティ及び物理セキュリティについて，新たに「場のセキュリティ」について定義する．

次に，場のセキュリティにおける脅威を基に，関連研究を概観するとともに，現状の課題を明らかにする．

### 2.1 情報セキュリティ

一般に，セキュリティとは，情報セキュリティを意味することが多い．ここでは，情報セキュリティに関し，その対象ならびに脅威，さらにこれらの脅威に対する現状の対策に関して概観する．

#### 2.1.1 情報セキュリティとは

企業には，守るべき情報資産がある．情報セキュリティとは，これらの情報資産に対して，正当な権利を持つ個人や組織が，情報や情報システムを意図通りに制御できること，すなわち，情報の機密性，完全性，可用性を維持することである．これらの要素は，情報セキュリティの 3 要素としても知られており，情報セキュリティを検討する上で，これら 3 要素の観点で検討することは網羅性の観点からも重要な要素である．

##### 2.1.1.1 機密性

機密性とは，許可された者だけが情報にアクセスできるようにすることである．この機密性を維持することによって，情報漏えいなどの脅威を予防することが可能となる．

##### 2.1.1.2 完全性

完全性とは，情報や情報の処理方法が，正確で完全であることである．この完全性は，例えば，不正アクセスによって Web ページの情報が改ざんされたり，情報システムが勝手に変更されたりしないよう，適切な保護を行い，決められた取扱い手順を守ることによって確保される．

##### 2.1.1.3 可用性

可用性とは，許可された者が，必要なときに情報や情報資産にアクセスできることを確実にすることである．即ち，情報システムにおいては，常に利用できる状態にしておく必要性があり，これが可用性と呼ばれている．

#### 2.1.2 情報資産

一般に，資産には，不動産や商品など，目に見える資産もあれば，財務情報，人事情報，顧客情報，戦略情報，技術情報などの目に見えない資産も存在する．後者のこのような資産を情報資産と呼び，個人及び組織には多くの情報資産が蓄えられている．近年の情報化社会において，これら情報資産の価値は非常に大きなものとなってきている．

#### 2.1.3 情報資産を取り巻く脅威とその手法

2.1.2 で述べたように，個人や組織における情報資産の価値は大きなものとなってきている．すなわち，その情報資産を狙う悪意ある第三者にとっての価値も大きなものとなってきている．インターネットの進展に伴い，これら情報資産を取り巻く脅威は，いかに示すように，非常に多岐に渡っている．

2.1.3.1　マルウェア

コンピュータウイルスやスパイウェア，ボットなどの使用者や管理者の意図に反して，あるいは気付かぬ内に，コンピュータに入り込み，悪意のある行為を行うプログラムを総称してマルウェアと呼ぶ.

これらマルウェアの内，特にコンピュータウイルスによる被害は，図 2-1 のように，2013 年の第 1 四半期には 1,803 件と依然として多数が報告されている．図 2-1 を見ると，届出件数の推移は減少傾向にあるように見えるが，これは，近年のウイルスが巧妙化・凶悪化し，感染の兆候や脅威が見えにくくなっており，特に，特定の組織や個人を狙う標的型攻撃では，感染を隠ぺいする工夫が巧妙に施され，一般の利用者が感染に気付くことは困難になって来ていることが関係していると考えられている.

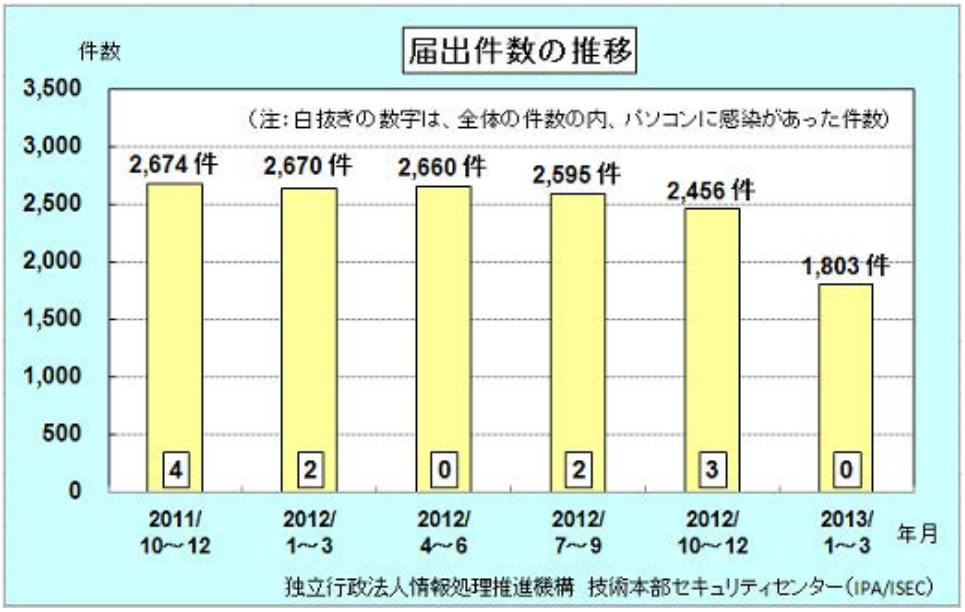



図 2-1　コンピュータウイルスの届出件数の推移[2-1]

一般に，マルウェアに感染すると，以下に示すように，様々な被害を受ける[2-2].

- 情報漏えい

ウイルスの中には，Winny や Share などの P2P ファイル交換ソフトウェアを利用し，使用者の知らぬうちに PC 内のデータなどを公開用フォルダへコピーし P2P ネットワーク上へ流出させたり，感染した PC 内でウェブサーバを立ち上げ，PC 内の全てのファイルを Web ページとしてインターネット上に公開したりするといったものがある．また，ユーザがキーボードから入力した内容を記録するプログラムであるキーロガーなどのスパイウェアによって暗証番号などが盗まれる場合もある.

これらウイルスなどに感染すると，顧客情報などの機密情報が流出してしまうなどの情報漏えいの被害を受けてしまう可能性がある.

- 悪意あるサイトへの誘導やマルウェアのダウンロード

直接不正行為を行うソフトウェアを入れる他に，まずダウンローダを侵入させてから，そのダウンローダを介してネットワーク上に用意したマルウェアをダウンロードさせるマルウェアも存在する.

このタイプのマルウェアは感染した PC からインターネットにアクセスし，別のマルウェ

アを次々とダウンロードし，自らもアップデートしていくため，非常に危険である．
他にもブラウザを乗っ取り，悪意ある Web サイトへ誘導したり，意図しない検索結果を表示したりするマルウェアも存在する．

- DDoS 攻撃(Distributed Denial of Service :分散サービス妨害攻撃)

感染したコンピュータを中継地点として DDoS 攻撃を行うマルウェアも存在する．DDoS 攻撃とは標的のサーバに大量のデータを送ることで過大な負荷をかけ，サーバのパフォーマンスを極端に低下させたり，機能停止に追い込んだりする DoS 攻撃の内，全く関係の無い多数の PC に攻撃プログラムを仕込んでおき，それら分散された PC から一斉に行う DoS 攻撃のことである．
DDoS 攻撃を行うためのマルウェアに感染する PC は数千～数十万に達することもあり，一斉攻撃による負荷は非常に大きなものとなる．実際に企業の Web サイトやサーバに対して DDoS 攻撃を行い，攻撃を停止することと引き換えに金銭を要求する事例もある．

2.1.3.1.1　マルウェア感染の原因

マルウェアは, 何らかのきっかけ, すなわち使用者の操作を利用して PC の中に入り込み, 感染する．主な感染の原因は「USB メモリの接続」,「ファイルのオープン」,「ネットワークへの接続」,「Web ページの閲覧」が挙げられる．

① USB メモリの接続

一例として，Windows XP/Vista には，PC に USB メモリが接続された際，その USB メモリの中に置かれたプログラムを自動的に実行する機能があり，これを利用して感染活動を行うマルウェアがある．このマルウェアは USB メモリに感染する際，通常見ることのできない Autorun.inf というファイルを USB メモリ内に作成することで，マルウェアが自動実行される状態を作る．感染した USB メモリを PC に接続した時や,「コンピューター」に表示される USB メモリドライブを開いた際にマルウェアが起動し, PC が感染してしまう. また, 感染した PC に別の USB メモリを接続した場合，その USB メモリもマルウェアに感染し, 拡散されていく．

② （添付）ファイルのオープン

USB メモリの接続と同様に，メールなどに添付されているファイルを開くことで感染するマルウェアも存在する．マルウェアの仕込まれたファイルの入手先は多岐に渡り，特にメールの添付ファイルや，P2P ファイル交換ソフトウェア，Web サイトからのダウンロードなどが多い.
これらのマルウェアは悪意のあるファイルを開かなければ問題はないが，多くの使用者の気を引くようなファイル名を付けたり，拡張子を偽装する二重拡張子や，表示されるアイコンをフォルダやメモ帳など別のアイコンに偽装したり，さらには偽装に気付かれにくくするために偽装したアイコンと同じプログラムを立ち上げたり，偽のエラー文を表示したりと，使用者がうっかり開いてしまうように仕向ける巧妙な手口が利用されている．

③ ネットワークへの接続

マルウェアがネットワークに接続している PC を調査し，パスワードの設定が甘いなど, 脆弱性のある PC を探し出し, そのセキュリティを破って悪意あるプログラムを侵入させる．

④ Web ページの閲覧

Web ページにアクセスすることによってマルウェアに感染する．攻撃者が予めマルウェ

アを仕込んだ Web サイトを用意し, そこへのアクセスを待つ例があるが, 他にも正規の Web サイトが改ざんされることによってマルウェアを仕込まれ，その Web サイトへアクセスした PC を感染させる例もあり，通常の Web サイトでも，必ずしも安全とは言い切れない.

2.1.3.2　標的型攻撃と誘導型攻撃

主に電子メールなどを用いて特定の組織や個人を狙う攻撃を標的型攻撃と言う．このような攻撃は，限られた対象にのみ検体が送られず，不特定多数を攻撃対象としていないため，ウイルス対策ソフトウェアなどでの対策を行うことが困難である．加えて，攻撃対象の組織や個人に合わせて内容をカスタマイズされているため，怪しいメールとの判断がより難しくなっている.

2005 年 7 月にオンラインショップへの苦情メールに商品の写真と偽ってスパイウェアを忍ばせ，ネット銀行の口座番号や暗証番号を盗み出し，不正に金銭を引き出す例や，2008 年 4 月に IPA の名を騙り，特定の組織にメールの添付ファイルとしてウイルスを送りつける例など，いずれも苦情メールや公的機関を装い，偽装されていることに気付きにくくされている.

また，標的型攻撃に似た攻撃手法として，誘導型攻撃がある．誘導型攻撃は，攻撃者が罠を仕掛けた Web サイトなどを予め用意し，攻撃対象を電子メールなどでその Web サイトへアクセスするよう誘導する．誘導型攻撃は，標的型攻撃などの能動的な攻撃に比べて手間が多いが，外部とのアクセスを極力少なくしているイントラネット内などへの攻撃が容易といった特徴がある.

2.1.4　情報資産を取り巻く脅威への対策

前述したように，インターネットの急激な進展により，情報資産は多くの脅威に晒されている．これら脅威への共通した対策としては Windows Update などの修正プログラムによる脆弱性の解消や，ウイルス対策ソフトウェアのインストールと更新，パーソナルファイアウォールによる監視と検査などがあるが，多くの情報資産を持つ企業が場当たり的にこれらの対策を行うのは効率が悪いだけでなく，コストもかさんでしまう.

限られたコストで最大限の対策を行うためには，特に企業においては，脅威への対策を体系的かつ系統立てて取り組む必要がある．このような対策を行うための国際規格として，ISMS(Information Security Management System: 情報セキュリティマネジメントシステム）がある[2-3],[2-4]．さらに，これら ISMS を組織として遵守するだけでなく，セキュリティインシデントが発生した際に直ちに対策がとれるように，企業では，CSIRT（Computer Security Incident Response Team）を設置することが大企業を中心に実施されてきている．この CSIRT は，コンピュータやネットワーク（特にインターネット）上で何らかの問題（主にセキュリティ上の問題）が起きていないかどうか監視すると共に，問題が発生した場合に，その原因解析や影響範囲の調査を行ったりするものであり，企業内だけでなく，組織間，さらには世界中の組織との間で情報交換を行い，常に最新のセキュリティ対策が行えるように活動している.

2.2　物理セキュリティ

2.1.2 に示したように，情報資産には目に見える形で存在するものも含まれる．これら目に見える形で存在するものには物理的な脅威も発生することが容易に想像されるため，物理セキュリティも重要となる.

物理セキュリティによって守られる情報資産の物理的な脅威は，網羅的な観点から大別すると自然災害，テロ災害，物理的侵入に分けられる．ここでは，これらの観点から，物理セキュリティに関して概観する.

### 2.2.1　自然災害

水害，地震，落雷などの自然災害は，情報資産のセキュリティを脅かす大きな要因となる．自然災害には多くの種類があり，例えば，水害であれば，台風や暴風雨による河川災害やそれに起因する土砂災害などが挙げられる．また，落雷による電源の瞬断は急激な電力変化を引き起こし，作業中のデータを一瞬で消失させてしまうなど，精密にできた情報機器には非常に危険であり脅威となるものである．

同様に，火災による建物の損失も情報資産に大きな影響を与える．火災の発生の原因には，前述した自然災害によるものの他に，煙草や放火などの故意に発生するものがある．こういった火災の原因に対応するには，喫煙ルールを徹底して消火設備を確保する，建物の周囲に燃えやすいものを置かないなどの，一般的な火災予防ならびにその遵守が必要となる．加えて，火災探知機や火災報知機などによって早期発見に努めることも重要である．

### 2.2.2　テロ災害

9.11 事件以降は，テロ対策も注目を浴びている[2-5]-[2-7]．これは，事件の際，他の事業所へバックアップを取っていた企業とそうでない企業とで業務再開までの期間に大きな開きが生じたためである．この業務停止期間の大小によって，市場から撤退を強いられた企業も少なくとも存在している．現在のビジネスはグローバル化が進んでおり，仮に東京が災害に見舞われ，本社が崩壊した場合でも，他国の事業所は問題なく業務を遂行する必要がある．このような状況に備えて，本社崩壊時の事業継続に関する対策なども検討する必要がある．具体的には，図 2-2 に示すように，BCP/DR（Business Continuity Plan/ Disaster Recovery）の導入が大企業を中心に進んでいる．BCP/DR は，同図に示すように，組織の持続的な業務推進に必要なソフトウェアやデータなどの情報資産を物理的に頃なる位置（距離の離れた場所）に二重化して保管することを意味している．


図 2-2　BCP/DR の利用イメージ（参考：http://blog.nedia.ne.jp/2016/03/17/7245.html）

### 2.2.3　物理的侵入

物理的侵入は，セキュリティ侵害の方法としては極めて古典的ではあるが，一度侵入してしまえばその目的を達成しやすいため，危険性が高い．近年は，2.1.2 情報資産の項で述べたように，装置や資産だけでなく，情報自体が持つ価値が大きくなっている．このため，メインフレーム自体を持ち出すことは難しいが，その中のデータや CD,DVD などの記録媒体を持ち出すことは容易であり，それらから大きな損失を被ることがある．

このような脅威に対しては，以下に示す入退室管理や監視，設備管理，警備システムの利用といった対策が必要である

① 入退室管理

データセンタや企業の情報システム部門のサーバルームなど情報資産が集約される場所への出入りについては，厳重な管理が必要である．入退室管理には，高度な制御技術やバイオメトリクス認証を駆使した入退室管理を実施することで，物理的なセキュリティ強化をする必要がある．

② 監視

総合警備会社などの監視カメラシステムを利用することで，不正侵入者の割り出しなどを事後に検査できる．

③ 設備管理

建物の規模が大きくなると日常的な保守作業量が増大し，また法廷有資格者(電気主任技術者，冷凍機械責任者，ボイラー技師など)の配置が必要となる．大型物件などは，建築設計段階で設備要員が常駐し，維持管理することを前提に設計されているため，無駐在方式での運用は不可能であるが，夜間や休日などで建物の利用者がいなくなる時間帯は警備保障会社などの設備異常監視サービスを利用する解もある．

④ 警備システムの利用

警備保障会社などのセキュリティサービスを利用することにより，堅牢な物理的セキュリティ対策を講じることができる．

## 2.3 現状の情報セキュリティならびに物理セキュリティにおける課題

これまで述べたように，一般に，重要な情報資産を扱う組織，特に，高度なセキュリティレベルを確保しなければならない環境においては，情報セキュリティに加え，入退室管理などによって厳格な物理セキュリティを施す必要があることは自明である．

近年，その利用が著しいデータセンターなどにおいては，厳格な物理セキュリティの適用は十分になされており，安心安全な ICT 環境が提供されている．しかし，例えば，一般的なオフィスのように，宅配業者や顧客など来訪者が訪れることのある環境では，その構造上，厳格な物理セキュリティを施すことは困難となる[2-8]．このような環境においては，机の上に置かれた書類やホワイトボード，PC の画面などにある情報を見られてしまう，覗き見といった脅威が発生することが考えられる．すなわち，オフィスでは，機密情報などの重要なデータ，宣伝や広報などの一般的なデータなどが混在しているが，業務遂行上，社員以外の来訪者が訪れることは避けられない状況である．

このようなオフィス環境において，例えば，覗き見のような脅威への対策としては，社員の教育や来訪者の行動範囲をできるだけ少なくする，社員と来訪者を陽に区別できるように社員カードと来訪者カードを色分けするなど，運用面からの対策は提案されているが，システム的な対策は未だ十分に検討されていない．

一般に，このような脅威は，来訪者が訪れた時や，PC 上に機密情報を表示している時など，その TPO 条件に依存する．このため，このような物理的な脅威を検知するためには，情報セキュリティ面の対処，即ち，来訪者が訪れた際は，機密情報を画面上に表示しないなどの考慮が必要となるため，物理セキュリティだけではなく，物理・情報の両セキュリティが必要である．従って，物理セキュリティと情報セキュリティとの連携が必要になると考えられるが，その具体的な手法は未だ明らかにされていない．

## 2.4　関連研究

前述したように，一般には，オフィス空間のようにコスト面等の観点からデータセンターで実現しているような厳格な物理セキュリティを実施することが困難な環境がほとんどである．これに対する対策案では，これまでに具体的な提案は十分ではなく，関連研究としては，以下に示す論文がこれまでに発表されてきている．ここで，本研究は，前述のように，IoT の進展なども加味し，新たに物理面からの脅威について加味した研究について述べるものである．従って，従来より多くの研究がなされている情報セキュリティに関わる研究は，ここでは割愛し，物理セキュリティを加味した関連研究について示す．

具体的には，IoT の進展に伴い，物理面も加味したシステムとして CPS (Cyber Physical System)の検討が進んでいる．以下に，CPS に基づくセキュリティに関する関連研究に関して述べる．

### (1) CPS に関わる研究

これまでに CPS に関する多くのセキュリティ関連の論文が発表されている[2-9]-[2-13]．しかし，これらの論文は，例えば，C´ardenas らの論文 [2-9]で述べられているように，CPS における様々な脅威に対して防御するための技術面に関するもので，主に，システム側の技術について述べられている．このように，従来研究においては，利用者も含めた網羅的で体系的な観点に基づく CPS に関するリスクアセスメントは，十分ではない．

上記に対し，著者らの研究 [2-14]では，プロジェクトマネジメント分野で一般に利用されている RBS(Risk Breakdown Structure)手法 [2-15]ならびにリスクマトリクス手法 [2-16]に基づき，利用者の観点から見た CPS に関わる脅威を網羅的に抽出し，これらの対策案に関するリスクアセスメントの検討を行っている．この論文は，定性的な観点に基づくものであることから，著者らは，さらに，新たにリスク値 [2-17]-[2-18]を導入することにより，定量的な観点からリスクアセスメントを行った結果について述べている [2-19].

### (2) アンビエントネットワークに関する研究

CPS に対する類似形態として，アンビエントサービスがある．アンビエントは，1998 年，米 Palo Alto Ventures の Eli Zelkha と Brian Epstein がフィリップス向けに「2010 年～2020 年ごろの社会」を想定して作成したプレゼンテーション中で使われたのが最初とされている．コンシューマエレクトロニクス，テレコミュニケーション，そしてコンピューティング分野での将来像を「アンビエント社会」と呼び，アンビエント社会 を支え，人の存在に敏感に感応するコンピュータを「アンビエントインテリジェンス」（Ambient Intelligence，AmI）と呼ばれる[2-20]．アンビエントサービスは，図 2-3 に示すように，コンピュータから人間に働きかけることである．「ユビキタス」は「いつでも・どこでも・だれとでも」と人間側からアクションを起こしてコンピュータにアクセスすることを想定しているのに対し，「アンビエント」は，さらに進化し，センサなどで機械側が人間を感知し，機械側から自律的に働きかける，すなわち，従来の「人間から機械へ」の逆方向で「機械から人間へ」働きかけ，個々の人間に適したサービスを提供するものである [2-21].

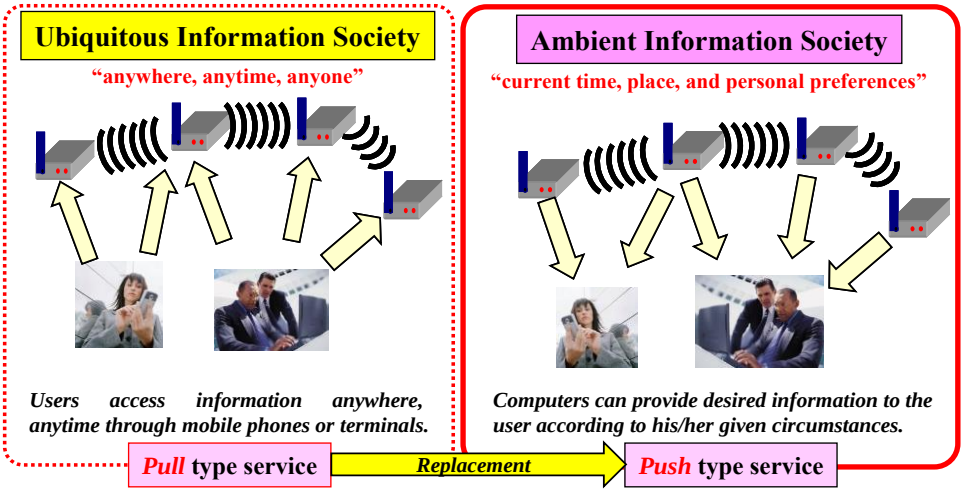



図 2-3　ユビキタスサービスとアンビエントサービス

このアンビエントサービスは，図 2-4 に示すように，CPS とも関わり合いの深いサービスでもある．

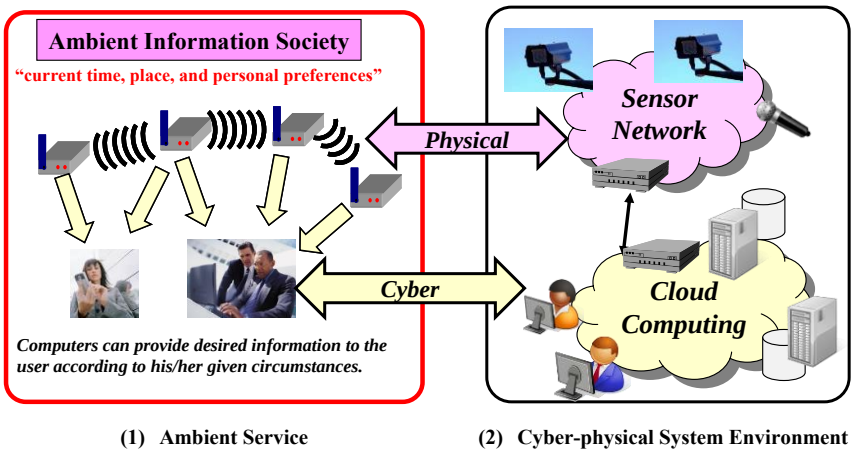



図 2-4　アンビエントサービスと CPS の関係

ところで，アンビエントサービスのセキュリティに関する多くの研究が，これまでに提案されている．しかし，これらの提案は，アンビエントネットワークのアーキテクチャに関する内容である．例えば，ネットワーク・アーキテクチャーの検討の一環として，認証機能などのセキュリティ機能の実装に関する研究がある [2-22]-[2-24]．さらには，セキュリティポリシの実装に関わる研究もなされている [2-25].
これに対し，谷本らの論文 [2-26]-[2-27]では，アンビエントサービスに対し，ユーザ側の観点からのリスクアセスメントの研究が報告されている．本研究では，アンビエントサービスを利用する側から見たリスクアセスメントを行っているが，物理的な環境も含めたいわゆる CPS としての研究まではなされていない．

(3) オフィスの場に着目した研究

オフィスの場に着目した研究としては，榎本らの研究がある [2-28]．この研究では，リアルタイムで変化する脅威に合わせて，セキュリティレベルもダイナミックに制御することで安全性と利便性の両立を考えた手法を提案している．特に，図 2-5 のようなコンセプトとともに，ダイナミックな制御の一例として，図 2-6 のような，Bluetooth 通信の電波受信強度(RSSI: Received Signal Strength Indication)を用いて来客と PC 間の距離を測り，セキュリティレベルをダイナミックに制御するシステムの提案をしている．これにより，ショルダーアタックなどの物理的な脅威に対し，リアルタイムに対応することができる．

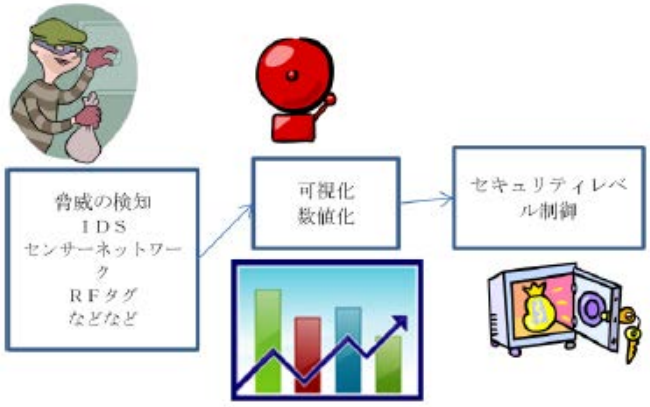



図 2-5　セキュリティダイナミック制御のコンセプト[2-28]

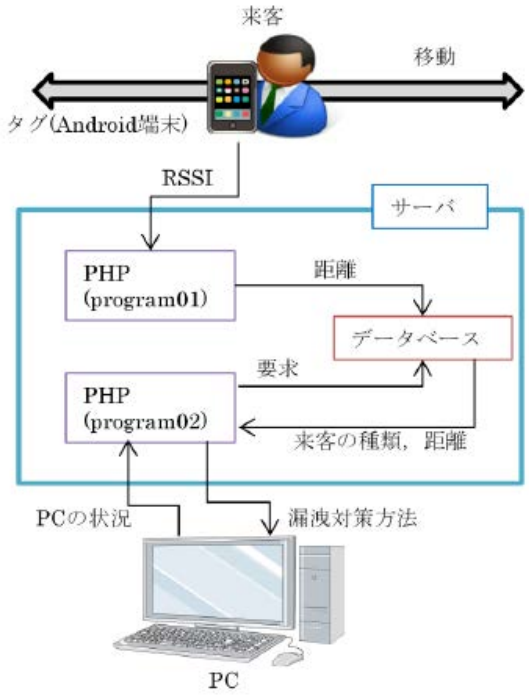



図 2-6　Bluetooth を用いたシステム構成[2-28]

また，末次らは，榎本らのシステムに加え，特に PC 利用者に選択肢を与えることで，より利便性の向上を図っている [2-29].

これに対し，著者らは，従来，独立に対処されてきた情報セキュリティと物理セキュリティを連携させることによる新たな情報セキュリティマネジメントの提案を行った [2-30].

特に，情報セキュリティと物理セキュリティの連携をセキュリティ場と定義し，これに，時間の概念も加える，即ち，リアルタイムに，ある場のセキュリティレベルを検出し，適切なマネジメントに結び付けるためのコンセプトを示した．

しかし，これらの研究においては，センサの利用が単一であったため，いろいろな課題があった．例えば，IC カード（RFID）を用いたリスク検知では，防御ラインとして，ゲスト率を利用していたが，この場合，ゲスト率は低くても，そのゲストが社員の PC の近くにいた場合でも安全とする問題があった．また，測位センサ（Bluetooth）を用いたリスク検知では，複数人の検知が課題であった．これに対し，著者らは，単一センサによるリスク検知の課題を解決するために，センサの複数化を提案する．具体的には，物理セキュリティとして，前述の IC カードと測位センサを組み合わせた，マルチセンサによるリスク検知技術を提案により，従来の単一センサにっ比べて，より精度よく効率的に物理的な脅威検知が可能な情報セキュリティマネジメントシステムを提案している [2-31].

## 2.5 場のセキュリティの定義

ここでは，オフィスにおける場のセキュリティを新たに定義する．一般に，オフィスでは，業務上，そのセキュリティレベルは動的に変化している．具体的には，社員以外の訪問者の有無などにより変化している（O（機会）としての変化）．また，社員は，出張等により業務をオフィス以外で遂行する必要がある（P（場所）としての変化）．さらに，オフィスでは，勤務時間内，勤務時間外で社員の在不在が変化する（T（時間）としての変化）．

このように，オフィスでは，TPO 条件に応じて，その環境が変化することに伴い，情報資産の脅威も併せて動的に変化する．従って，このような脅威に対応するためには，前述のデータセンターなどでは，厳格な入退室管理などによりコストをかけることにより成し得るが，オフィス環境においては，コストの制約に加え，業務の性質上，来訪者等の外的要因は避けがたい．

以上のことから，オフィスにおけるさらなるセキュリティ向上の観点から，従来の情報セキュリティ対策に対し，物理セキュリティを連動させる必要がある．

本論文では，オフィス環境を対象に，新たに物理面を加味した情報セキュリティを，「場のセキュリティ」と定義する．以降，場のセキュリティとは，物理セキュリティを加えた情報セキュリティのことを指し示すこととする．

## 2.6 まとめ

第 2 章では，オフィスを対象に，セキュリティに関わる脅威が動的に変化する，即ち，情報セキュリティ及び物理セキュリティの現状について概観した．

情報セキュリティに関しては，主にマルウェアや標的型攻撃，誘導型攻撃を例に挙げ，さらに，それらの対策を企業として効率的に行うために ISMS や CSIRT があることを示した．

物理セキュリティに関しては，データセンターなどの厳格な物理セキュリティの実施が困難な環境として企業のオフィス空間を対象に，TPO 条件によって時々刻々と変化するリスクに対し，物理セキュリティと情報セキュリティの連携が必要であることを言及した．

これらに対する関連研究に関しては，IoT の進展に伴い，物理面も加味したシステムとして CPS (Cyber Physical System)の検討が進んでいる．しかし，物理的な環境や，利用者も含めた網羅的で体系的なリスクアセスメントの研究まではなされていないことを明らかにした．

最後に，オフィスを対象に， TPO 条件などの動的要因として物理セキュリティを加味した情報セキュリティとして，「場のセキュリティ」を新たに定義した．

参考文献

[2-1]IPA：コンピュータウイルス・不正アクセス届出状況および相談受付状況[2013 年第 1 四半期(1 月～3 月)]，2013
[2-2]IPA：情報セキュリティ読本　四訂版　-IT 時代の危機管理入門-，2013
[2-3]日本規格協会：情報セキュリティマネジメントシステム，JIS Q 27001，2014
[2-4]JIPDEC : ISMS ユーザーズガイド　-JIS Q 27001:2006　(ISO/IEC 27001:2005)対応-，2008
[2-5]外務省：テロ対策関連(米国同時多発テロ事件)，(オンライン) http://www.mofa.go.jp/mofaj/area/usa/terro0109/
[2-6]外務省 : 日本の国際テロ対策協力, (オンライン)http://www.mofa.go.jp/mofaj/gaiko/terro/, 2016
[2-7]東京海上リスクコンサルティング(株)：米国同時多発テロが与えた影響-今後の国際テロ情勢とテロ対策-(第 2 部)，TRC EYE Vol.21(オンライン), http://www.tokiorisk.co.jp/risk_info/up_file/2004020566.pdf，2002
[2-8]牧野：ISMS に基づくセキュリティ場の提案　-動的リスク評価に関する研究-，千葉工業大学卒業論文，2012
[2-9]Alvaro A. C´ardenas, et al., Secure Control: Towards Survivable Cyber-Physical Systems, ICDCS'08, pp. 495-500, 2008
[2-10] Clifford Neuman, Challenges in Security for Cyber-Physical Systems, DHS Workshop on Future Directions in Cyber-Physical Systems Security, Newark, NJ, July 22-24, 2009. http://cimic.rutgers.edu/positionPapers/CPS-Neuman.pdf
[2-11] Radhakisan Baheti, et al., Cyber-Physical Systems, The Impact of Control Technology, T. Samad and A.M. Annaswamy (eds.), 2011. Available at www.ieeecss.org. http://ieeecss.org/sites/ieeecss.org/files/documents/IoCT-Part3-02CyberphysicalSystems.pdf
[2-12] Chris Codella, et al., Continuous Assurance for Cyber Physical System Security, provided by IBM, 2009, http://cimic.rutgers.edu/positionPapers/CPSSW09%20_IBM.pdf
[2-13] Alvaro A. C´ardenas, et al., Challenges for Securing Cyber Physical Systems, http://cimic.rutgers.edu/positionPapers/cps-security-challenges-Cardenas.pdf
[2-14] 米田翔一，谷本茂明，佐藤周行，金井敦：オフィス空間における場のセキュリティを考慮したリスクアセスメント，第 13 回科学技術フォーラム（FIT 2014），RO-006，2014
[2-15] Risk Breakdown Structure, [Online]. Available from: http://www.justgetpmp.com/2011/12/risk-breakdown-structure-rbs.html
[2-16] Cox's risk matrix theorem and its implications for project risk management, [Online]. Available from: http://eight2late.wordpress.com/2009/07/01/cox%E2%80%99s-risk-matrix-theorem-and-its-implications-for-project-risk-management/
[2-17] 佐藤周行，笠松隆幸，田村拓也，小林勇範：情報セキュリティ基盤論，共立出版，2010
[2-18] ISMS Risk Assessment Manual v1.4, [Online]. Available from: https://www.igt.hscic.gov.uk/KnowledgeBaseNew/ISMS%20Risk%20Assessment%20Manual%20v1.4.pdf, 2015.1.4
[2-19] Shoichi Yoneda, Shigeaki Tanimoto, Tsutomu Konosu, Hiroyuki Sato, Atsushi Kanai, Risk Assessment in Cyber-physical System in Office Environment, The International Conference on Network-Based Information Systems, NBiS2015, pp.412-417, 2015
[2-20] 総務省：通信利用動向調査，(オンライン) http://www.soumu.go.jp/johotsusintokei/statistics/statistics05a.html，2009

[2-21] 大阪大学，大学情報科学研究科：アンビエント情報社会基盤創成拠点, http://www.ist.osaka-u.ac.jp/GlobalCOE
[2-22] Mahdi Aiash, et al., “A Survey of Potential Architectures for Communication in Heterogeneous Networks,” The IEEE Wireless Telecommunications Symposium (WTS 2012), April 2012. London, UK.
[2-23] M. Lebre, et al., “Media Independent Transport Service for Ambient Intelligence,” [Online]. Available from: https://ria.ua.pt/bitstream/10773/6601/3/A_Media_Independent_Transport_Service_for_Ambient_Intelligence.pdf, 2015.1.6
[2-24] A. F. Abate, M. D. Marsico, “MUBAI: multiagent biometrics for ambient intelligence,” Journal of Ambient Intelligence and Humanized Computing, Jun. 2011, Vol. 2, Issue 2, pp 81-89, Springer
[2-25] O.Dohndorf, et al., “Adaptive and Reliable Binding in Ambient Service Systems,” IEEE 16th Conference on Date of Conference, pp.1-8, Sept. 2011
[2-26] Shigeaki Tanimoto, Daisuke Sakurai, Yosiaki Seki, Motoi Iwashita, Hiroyuki Sato, and Atsushi Kanai, Risk Management to User Perception of Insecurity in Ambient Service, SNPD 2012: 13th ACIS International Conference on Software Engineering, pp.771-776, 2012
[2-27] Shigeaki Tanimoto, Hiroyuki Sato, Atsushi Kanai, Risk Assessment Quantification of Ambient Service, ICDS 2015 : The Ninth International Conference on Digital Society, pp.70-75, Lisbon, Feb., 2015
[2-28] 榎本真也他:ダイナミックに制御する情報漏洩対策システムの検討, FIT2012, L-034, 2012
[2-29] 末次正人他：侵入者の距離によりダイナミックにセキュリティレベルを制御するシステムの検討, 情報処理学会研究報告. 2013-CSEC-60(25), 1-6, 2013-03-07
[2-30] 米田 翔一，牧野 駿，谷本 茂明，佐藤 周行，金井 敦：動的リスク評価に基づくセキュリティ場の提案，プロジェクトマネジメント学会 2013 年度春季研究発表大会，pp.303-307，2013
[2-31] Shoichi Yoneda, Shun Makino, Shigeaki Tanimoto, Hiroyuki Sato, Atsushi Kanai, Information Security Management System with Physical Security - Improvement of Risk Recognition Function with Multi-sensor –, 7th International Conference on Project Management (ProMAC 2013), Hanoi, Vietnam, November 6-9, 2013

## 3. センサ活用による場のセキュリティを考慮したリスクアセスメント

前述のように，物理と情報を連携させたシステム（CPS: Cyber Physical System，サイバーフィジカルシステム）に関する研究はこれまでにも行われてきているが，それらは主にシステム固有のリスクに関する内容であり，物理及び情報の両面のリスクを連携して総合的にリスク評価したものではなかった．

ここでは，オフィスを対象に，物理面も考慮した総合的なリスクアセスメントを行う．特に，具体的な対策としてリスクマネジメントに寄与するために，リスクの可視化，即ち，定量化に関しても新たに言及する．

### 3.1 オフィスを対象にした場のセキュリティを考慮した定性的なリスクアセスメント

前述したように，TPO 条件に応じて対応可能な情報セキュリティは，オフィスのような，厳格な物理セキュリティを実施することが困難な場所で，特に必要となる．ここでは， 3.1 及び 3.2 において，オフィスを対象にしたリスクアセスメントを行い，その動的変化に対するリスク要因を明らかにするとともに，これらの要因を具体的な対策案に寄与するために可視化する．

#### 3.1.1 オフィス空間における動的要因を加味したリスク要因の抽出

一般に，リスクマネジメントにおいては，リスク要因の特定→分析→評価，の順に検討を進めていく．最初にリスク要因の特定，すなわち，リスク要因の抽出には，一般に，リスクマネジメントの代表的な手法である RBS（Risk Breakdown Structure）手法が用いられている [3-1]．ここでも RBS 手法を用いることとした．具体的には，表 3-1 に示すように，最初に，場のセキュリティの主要因である物理セキュリティと情報セキュリティに分類し，全体で 27 項目のリスク要因を抽出した．

同表では，オフィス空間における場のセキュリティとしてのリスク要因を前述のように，RBS 手法に基づく階層的な観点[3-2] から，最初に，物理セキュリティと情報セキュリティにまず分解した．次の階層では，１．物理セキュリティにおいては，人が関わるか否か，すなわち，人為的な観点から細分化することとした．ここで，人為的な場合は，さらに，意図的か否かとして分解した．

一方，２．情報セキュリティの場合は，インターネットなどが人工物でかつ実体を持たないため，非人為的，すなわち自然現象などといったリスクが存在しないことから，物理的セキュリティにおける人為的か否かの階層は存在しないことが明らかであるため，意図的か否かの階層から細分化していった．

表 3-1(1/2)　RBS 手法に基づく場のセキュリティにおけるリスク要因抽出結果

| 分類 | | | リスク要因 | リスク要因詳細 |
|---|---|---|---|---|
| 1.物理セキュリティ | 1.1 人為的 | 1.1.1 意図的 | 1.1.1.1 侵入 | 許可なしにセキュリティ空間に入られてしまう．一般的に施錠などの抑制システムがある．発生した場合，自由に活動されてしまうため，影響度は高い． |
| | | | 1.1.1.2 盗難 | 書類や機材などの物品を奪われてしまう．法律として禁止され，抑制されている．機材を奪われると，情報漏えいだけでなく業務の続行にも影響がある． |
| | | | 1.1.1.3 聞き出し | 上司などを装って機密情報を聞き出されてしまう．法律として禁止され，抑制されている．情報漏えいの発生など，影響度は大きい． |
| | | | 1.1.1.4 放火 | 社屋に火をつけられてしまう．法律として禁止され，抑制されている．社屋全焼の可能性など影響度は高い． |
| | | | 1.1.1.5 破壊 | 機材を壊したり，回線を切断されてしまう．法律として禁止され，抑制されている．業務続行が難しくなる可能性が高く，影響度は高い． |
| | | | 1.1.1.6 覗き見 | PC の画面などを背後から見られてしまう．一般的に利用されている抑制システムはない．業務続行には影響はなく，見た記憶に頼るため影響はやや低い． |
| | | | 1.1.1.7 聞き耳 | 許可されてない者に会話を聞かれてしまう．一般的に利用されている抑制システムはない．業務続行に影響はなく，聞いた記憶に頼るため影響はやや低い． |
| | | | 1.1.1.8 内部犯行 | 許可された人間に犯行を行われてしまう．一般的に身元の確認などの対策は行っているため，発生頻度は低い．情報漏えいの発生など，影響度は大きい． |
| | | 1.1.2 非意図的 | 1.1.2.1 書置き | メモを書いて机の上などに残してしまう．一般的に利用されている抑制システムはない．置いてあるだけではまだ問題がないため，影響度は低いとする． |
| | | | 1.1.2.2 火の不始末 | 火器を使用したあと，消火し忘れてしまう．一般的に，厳格に管理され抑制されている．火災に繋がる可能性があり，影響度は高い． |
| | | | 1.1.2.3 破壊 | 不注意で機材を落とすなどで壊してしまう．通常使用において機材が壊れることは少ない．業務続行が難しくなるなど，影響度は高い． |
| | | | 1.1.2.4 紛失 | 使用していた機材やデータを失くしてしまう．一般的に利用されている抑制システムはない．情報漏えいなど，影響度は大きい． |
| | | | 1.1.2.5 持ち出し | データや書類などを持って社外に出てしまう．一般的に利用されている抑制システムはない．持ち出しただけではまだ問題がないため，影響度は小さいとする． |
| | | | 1.1.2.6 持ち込み | 許可されていない機材を持ち込んで作業してしまう．一般的に厳格に管理され，抑制されている．ウィルスの感染や情報漏えいの発生など，影響度は高い． |
| | 1.2 非人為的 | | 1.2.1 故障 | 機材などが故障して使えなくなってしまう．一般的に製造時の品質管理などの抑制システムがある．誤動作や業務の停止など，影響度は高い． |
| | | | 1.2.2 災害 | 自然災害に見舞われてしまう．一般的に自然災害の被害に遭う可能性は低い．業務続行が難しくなるなど，影響度は高い． |

表 3-1(2/2)　RBS 手法に基づく場のセキュリティにおけるリスク要因抽出結果

| 分類 | | リスク要因 | リスク要因詳細 |
|---|---|---|---|
| 2.情報セキュリティ | 2.1 意図的 | 2.1.1 ウィルスの感染 | コンピュータウィルスに感染してしまう．一般的にウィルス対策ソフト導入などの抑制システムがある．ウィルスによる被害は多岐に渡り，影響度は高い． |
| | | 2.1.2 不正アクセス | コンピュータに許可なくアクセスされてしまう．一般的にファイアウォール導入などの抑制システムがある．情報漏えいの発生など，影響度は高い． |
| | | 2.1.3 盗聴 | データ通信を傍受されてしまう．一般的に暗号化などの抑制システムがある．情報漏えいの発生など，影響度は高い． |
| | | 2.1.4 なりすまし | ID などを取得して，不正に権限を得られてしまう．法律として禁止され，抑制されている．情報漏えいの発生など，影響度は高い． |
| | | 2.1.5 DoS 攻撃 | コンピュータに大量のデータを送りつけ，停止させられてしまう．一般的にファイアウォール導入などの抑制システムがある．業務が停止するなど，影響度は高い． |
| | | 2.1.6 改ざん | データを許可なく変更されてしまう．一般的にアクセス管理などの抑制システムがある．重要文書のデータ改ざんは業務に混乱を招き，影響度は高い． |
| | | 2.1.7 否認 | 執り行われた契約などを，後からやっていないと否定されてしまう．一般的に，身元のわかる契約で否認することは少ない．業務の混乱など，影響度は高い |
| | | 2.1.8 不正コピー | ソフトなどを許可されてない範囲で複製されてしまう．法律として禁止され，抑制されている．信用の失墜など，影響度は高い． |
| | | 2.1.9 フィッシング | 偽サイトに個人情報などを入力させることによって盗み取られてしまう．法律として禁止され，抑制されている．情報漏えいの発生など，影響度は高い． |
| | 2.2 非意図的 | 2.2.1 誤操作 | システムを誤って操作してしまう．一般的に利用されている抑制システムはない．情報漏えいの発生や重要データの消失など，影響度は大きい． |
| | | 2.2.2 バグ | システムの不具合により意図せぬ動作をしてしまう．一般的に品質管理やテストなどで抑制されている．発生する被害は多岐に渡り，影響度は大きい． |

3.1.2　リスク分析

ここでは，表 3-1 に示す 27 のリスク要因に対するリスク分析を行う．一般に，リスク分析手法には，主に，ディシジョンツリーを用いる方法，リスクマトリクスによる方法が代表的であり，前者が定量的な観点，後者が定性的な観点に基づくものである[3-1].

本論文では，セキュリティ面の課題を取り扱うことから，定性的な観点を基にしたリスクマトリクス手法を用いる．リスクマトリクス手法は，図 3-1 に示すように，リスクの発生頻度，影響度の高低により，回避，低減，保有，転嫁の 4 種類に分類し，その対策を策定するものである．

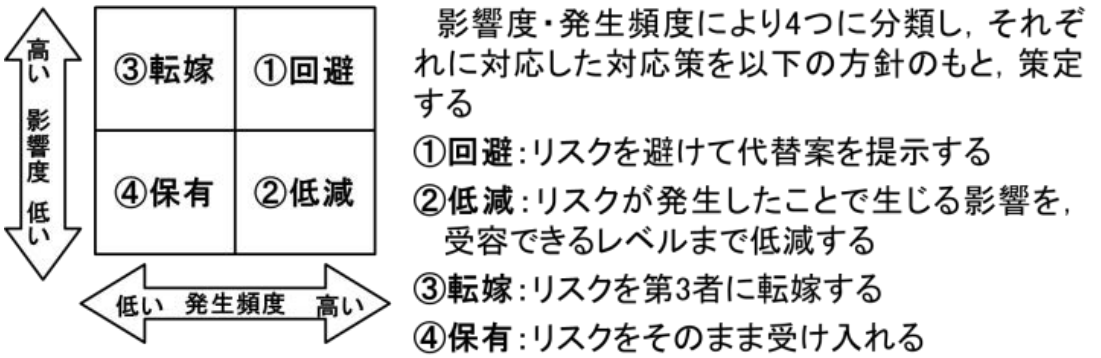



図 3-1 リスクマトリクス手法

3.1.2.1　リスクの分析結果

ここでは，前述の表 3-1 に示す，場のセキュリティにおける 27 のリスク要因に対し，これらリスク要因の個々に対し，図 3-1 に示すリスクマトリクス手法を用いて，詳細に分析を行った．この結果を表 3-2 に示す.

表 3-2　場のセキュリティのリスク要因に対する分析結果

| 分類 | リスク要因 | 発生頻度 | 影響度 | 対応策 |
|---|---|---|---|---|
| 1. 物理セキュリティ | 1.1.1.1 侵入 | 低 | 高 | 転嫁 |
| | 1.1.1.2 盗難 | 低 | 高 | 転嫁 |
| | 1.1.1.3 聞き出し | 低 | 高 | 転嫁 |
| | 1.1.1.4 放火 | 低 | 高 | 転嫁 |
| | 1.1.1.5 破壊 | 低 | 高 | 転嫁 |
| | 1.1.1.6 覗き見 | 高 | 低 | 低減 |
| | 1.1.1.7 聞き耳 | 高 | 低 | 低減 |
| | 1.1.1.8 内部犯行 | 低 | 高 | 転嫁 |
| | 1.1.2.1 書置き | 高 | 低 | 低減 |
| | 1.1.2.2 火の不始末 | 低 | 高 | 転嫁 |
| | 1.1.2.3 破壊 | 低 | 高 | 転嫁 |
| | 1.1.2.4 紛失 | 高 | 高 | 回避 |
| | 1.1.2.5 持ち出し | 高 | 低 | 低減 |
| | 1.1.2.6 持ち込み | 低 | 高 | 転嫁 |
| | 1.2.1 故障 | 低 | 高 | 転嫁 |
| | 1.2.2 災害 | 低 | 高 | 転嫁 |
| 2. 情報セキュリティ | 2.1.1 ウィルスの感染 | 低 | 高 | 転嫁 |
| | 2.1.2 不正アクセス | 低 | 高 | 転嫁 |
| | 2.1.3 盗聴 | 低 | 高 | 転嫁 |
| | 2.1.4 なりすまし | 低 | 高 | 転嫁 |
| | 2.1.5 DoS 攻撃 | 低 | 高 | 転嫁 |
| | 2.1.6 改ざん | 低 | 高 | 転嫁 |
| | 2.1.7 否認 | 低 | 高 | 転嫁 |
| | 2.1.8 不正コピー | 低 | 高 | 転嫁 |
| | 2.1.9 フィッシング | 低 | 高 | 転嫁 |
| | 2.2.1 誤操作 | 高 | 高 | 回避 |
| | 2.2.2 バグ | 低 | 高 | 転嫁 |

表 3-2 より, 場のセキュリティとしてのリスク要因に対する対応策では, 図 3-1 の「転嫁」, すなわち，発生頻度は低いが，影響度が高いものが 27 項目中 21 項目と大半を占めることがわかった．次に,「低減」, すなわち，発生頻度は高いが，影響度が低いものが 4 項目であった．以下，発生頻度が高く，影響度も高い「回避」については 2 項目，発生頻度も 影響度も低い「保有」は 0 項目であった.

### 3.1.3　リスクアセスメント結果

ここでは，表 3-2 の対応策分類の転嫁，低減，回避毎にリスクアセスメントした結果を以下に示す.

#### 3.1.3.1　転嫁に分類されたリスク要因の対策案

転嫁に分類されたリスク要因は，図 3-1 の③転嫁に示すように，リスクを第 3 者に転嫁する方針で対策を検討した．結果を表 3-3 に示す.

表 3-3　転嫁に分類されたリスク要因のアセスメント結果

| リスク要因 | 対策案 | 傾向 |
|---|---|---|
| 1.1.1.1 侵入 | 警備会社に委託するなどより強固な入退室管理システムを導入する | (a)管理強化 |
| 1.1.1.2 盗難 | 盗難保険に入る．外部にバックアップを用意する． | (b)業務停止の防止 |
| 1.1.1.3 聞き出し | クライアント証明書などを利用して確実に本人確認を行う | (a)管理強化 |
| 1.1.1.4 放火 | 火災保険に入る．外部にバックアップを用意する | (b)業務停止の防止 |
| 1.1.1.5 破壊 | 外部にバックアップを用意する | |
| 1.1.1.8 内部犯行 | 雇用契約の内容を調整して法的処罰を与えられるようにする | (c)資産の流出防止 |
| 1.1.2.2 火の不始末 | 火災保険に入る．外部にバックアップを用意する | (b)業務停止の防止 |
| 1.1.2.3 破壊 | 外部にバックアップを用意する | |
| 1.1.2.6 持ち込み | 雇用契約の内容を調整して法的処罰を与えられるようにする | (c)資産の流出防止 |
| 1.2.1 故障 | 修理交換の保障制度を利用する | (b)業務停止の防止 |
| 1.2.2 災害 | 外部にバックアップを用意するなど，事業継続計画を立てる | |
| 2.1.1 ウィルスの感染 | ウィルス定義ファイルを常に更新しておく | (c)資産の流出防止 |
| 2.1.2 不正アクセス | アップデートを常に行い，脆弱性を解消しておく | |
| 2.1.3 盗聴 | アップデートを常に行い，脆弱性を解消しておく | |
| 2.1.4 なりすまし | バイオメトリクスなど，強固な認証システムを導入する | |
| 2.1.5 DoS 攻撃 | アップデートを常に行い，脆弱性を解消しておく | (b)業務停止の防止 |
| 2.1.6 改ざん | アップデートを常に行い，脆弱性を解消しておく | |
| 2.1.7 否認 | 電子公証システムなどを利用する | |
| 2.1.8 不正コピー | 不正コピー確認ツールなどを利用する | (a)管理強化 |
| 2.1.9 フィッシング | 電子公証システムなどを利用する | (c)資産の流出防止 |
| 2.2.2 バグ | 契約内容の調整を行う | (a)管理強化 |

3.1.3.2　低減に分類されたリスク要因の対策案

低減に分類されたリスク要因は，図 3-1 の②低減に示すように，リスクを，受容できるレベルまで低減する方針で対策を検討した．その結果を表 3-4 に示す．

表 3-4　低減に分類されたリスク要因のアセスメント結果

| リスク要因 | 対策 | 傾向 |
|---|---|---|
| 1.1.1.6 覗き見 | 訪問者に画面を見せないようオフィスのポリシーを徹底する | (c)資産の流出防止 |
| 1.1.1.7 聞き耳 | 他者のいる場所での会話に気をつけるようオフィスのポリシーを徹底する | |
| 1.1.2.1 書置き | 機密情報の管理についてオフィスのポリシーを徹底する | |
| 1.1.2.5 持ち出し | 持ち出すデータの管理をオフィスのポリシーを徹底する | |

3.1.3.3　回避に分類されたリスク要因の対策案

回避に分類されたリスク要因は，図 3-1 の①回避に示すように，リスクを避けて代替案を提示する方針で対策を検討した．その結果を表 3-5 に示す．

表 3-5　回避に分類されたリスク要因のアセスメント結果

| リスク要因 | 対策 | 傾向 |
|---|---|---|
| 1.1.2.4 紛失 | 体系的な管理を行い，所定の場所から移動させない | (a)管理強化 |
| 2.2.1 誤操作 | 特に重要なシステムは複数人で操作する，指差し確認などを行う | |

3.1.4　考察

表 3-3～3-5 に示すリスク要因のアセスメント結果を基に考察する．

(1)転嫁

対応策が転嫁に分類されたリスク要因は，表 3-3 に示す結果となった．主に，資産の流出や業務の停止を防止する対策が有効である．具体的には，外部バックアップや証明書等の対策が有効であるが，これらは，一般に新たな費用が発生することになる．

今後，発生確率の低い要因に対して，どこまで対策をすれば良いのか，すなわち，影響度のレベルごとの対応，具体的には，費用対効果に関する定量的な検討が必要になってくると思われる．

(2)低減

対応策が低減に分類されたリスク要因は表 3-4 に示す結果となった．いずれも資産の流出を防止する対策であり，具体的な対策案は，オフィスのポリシーに基づく社員教育によるものであるが，より確実な対策を行うために，システム的な対策案の検討も重要であると考えられる．

(3)回避

対応策が回避に分類されたリスク要因は表 3-5 に示す結果となった. いずれのリスク要因も，非意図的に発生するもので，注意していても完全に避けることが難しいものが挙げられた．対策としては，ISMS などに基づく管理強化が重要である．

(4)保有

対応策が保有に分類されたリスク要因は存在しなかった．セキュリティに関する内容のため，保有可能なリスク要因はなかったと考えられる．

3.2　オフィスを対象にした場のセキュリティを考慮した定量的なリスクアセスメント

前述したように，場のセキュリティを考慮したリスクアセスメントの，定性的な評価は明らかとなった．しかし，より客観性を向上させるためには，定量的な評価が重要となる．

ここでは，オフィス空間における場のセキュリティを考慮した定量的なリスクアセスメントについて示す．

3.2.1　リスク計算式の近似化

ここでは，3.1 で明らかにしたリスクアセスメント結果に対し，定量的な算出を行う．即ち，3.1 で明らかにした場のセキュリティにおける 27 のリスク要因に対し，リスクマトリクス手法による分析により，それぞれのリスク要因に関わる発生頻度と影響度を明らかにした．これらのリスク要因に対する定量化を行う．

一般に，リスク要因に対する定量化手法として，リスク値が挙げられる．このリスク値の計算には，ISMS 等で利用されている以下の式(1)が用いられる [3-3]-[3-5].

$$\text{リスク値} = \text{資産価値} * \text{脅威} * \text{脆弱性} \qquad (1)$$

ここで，一般的には，式(1)の右辺の要素は，その算出が非常に困難である．ここでは，リスク分析と整合性および今回の検討は，初期検討であり，その傾向を知りえることが重要なため，さらなる単純化の観点等から，演繹的にこれらの要素を以下のように近似することとした[3-6]-[3-7].

1)  資産価値の近似

図 3-2 に示すように，式(1)における資産価値は，リスクマトリクスの影響度で近似した．この根拠は，リスクの影響度が大きいということは，その資産価値が大きいことによる．ところで，参考文献[3-3]-[3-5]では，リスク度を 5 段階で定義している．この値をリスクマトリクスの影響度に当てはめる際，リスクマトリクスでは影響度を高低の 2 段階でしか分類していないため，前述のように，今回の検討は，初期検討であり，その傾向を知りえるための単純化の観点から，影響度の高い方をリスク度の最大値である 5 とし，低い方を同じく最低値の 1 とした．

2)  脅威の近似化

脅威に関しては，1)の資産価値と同様に想定した結果，リスクマトリクスの発生頻度で近似した．根拠としては，発生頻度が高いということは，その脅威も大きいといえることから，このように近似した．ここで，参考文献[3-3]-[3-5]では，脅威は 3 段階で定義されているため，1)と同様に，単純化して，発生頻度の高い方を最大値の 3 とし，低い方を最低値の 1 とした．

3) 脆弱性の近似化

脆弱性に関しては，リスクマトリクスの分類に近似した．リスクマトリクスでは，図 3-2 に示すように，影響度と発生頻度のそれぞれ高低により 4 分類されている．ここでは，この 4 分類に対し，以下に示すように，脆弱性を近似した．

- 回避：影響度と発生頻度が共に高いため，最も危険度が高いと考える．即ち，対策を実施しない状況下では，最も脆弱な状況にあるといえる．
- 転嫁及び低減：影響度と発生頻度のどちらかだけが高いため，危険度の高さは中くらいと考える．回避と同様に，対策を実施しない状況下で想定した場合よりも脆弱性は低いといえる．
- 保有：影響度と発生頻度が共に低いため，最も危険度が低いと考える．対策を実施しない状況下では，脆弱性としては最も低い状況にあるといえる．

以上の通り，リスク分析結果が回避となる場合を 3，転嫁及び低減となる場合を 2，保有となる場合を 1 と近似した．

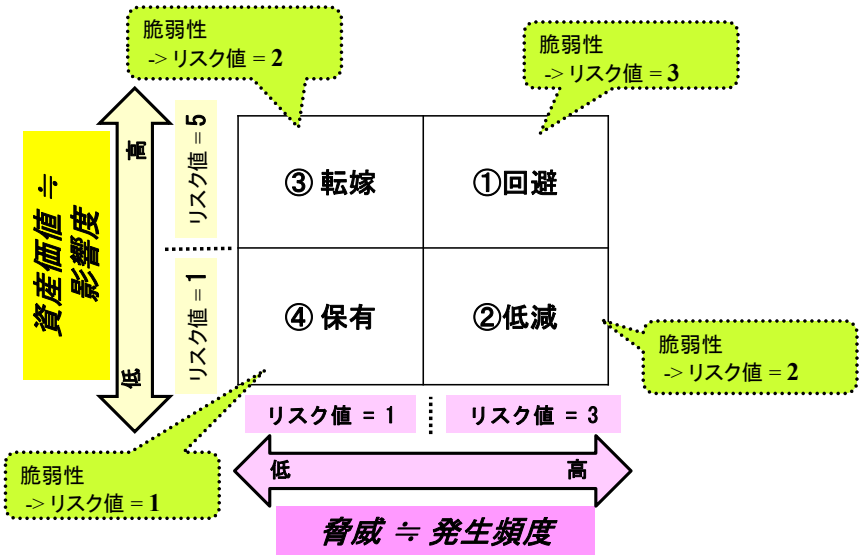



図 3-2　リスク値の近似化 [3-8]

上記の近似化により，式(1)は以下の式(2)に近似される．また，近似された各要素の値を表 3-6 に示す．

リスク値 ≒ 影響度 * 発生頻度 * 分類結果　　(2)

表 3-6　近似された各要素の値詳細

| | 影響度 | 発生頻度 | | 分類結果 |
|---|---|---|---|---|
| 高 | 5 | 3 | 回避 | 3 |
| 低 | 1 | 1 | 転嫁，及び低減 | 2 |
| | | | 保有 | 1 |

3.2.2　リスク値の算出結果

3.1.2.1 で示した場のセキュリティに関するリスク分析結果を，表 3-6 を基に数値化，さらに近似した式(2)によってリスク値を算出した結果を表 3-7 に示す．また，3.1.3 で示した対策を実施することで，リスクが保有可能になると仮定し，この場合，対策後の脆弱性の値は 1 に減じると仮定し，対策後のリスク値の算出結果も表 3-7 に併記した．

表 3-7　対策の実施前及び実施後のリスク値算出結果

| リスク要因 | 資産価値 ≒影響度 | 脅威 ≒ 発生頻度 | 脆弱性 | | リスク値 | |
|---|---|---|---|---|---|---|
| | | | 対策 実施前 | 対策 実施後 | 対策 実施前 | 対策 実施後 |
| 1.1.1.1 侵入 | 5 | 1 | 2 | 1 | 10 | 5 |
| 1.1.1.2 盗難 | 5 | 1 | 2 | 1 | 10 | 5 |
| 1.1.1.3 聞き出し | 5 | 1 | 2 | 1 | 10 | 5 |
| 1.1.1.4 放火 | 5 | 1 | 2 | 1 | 10 | 5 |
| 1.1.1.5 破壊 | 5 | 1 | 2 | 1 | 10 | 5 |
| 1.1.1.6 覗き見 | 1 | 3 | 2 | 1 | 6 | 3 |
| 1.1.1.7 聞き耳 | 1 | 3 | 2 | 1 | 6 | 3 |
| 1.1.1.8 内部犯行 | 5 | 1 | 2 | 1 | 10 | 5 |
| 1.1.2.1 書置き | 1 | 3 | 2 | 1 | 6 | 3 |
| 1.1.2.2 火の不始末 | 5 | 1 | 2 | 1 | 10 | 5 |
| 1.1.2.3 破壊 | 5 | 1 | 2 | 1 | 10 | 5 |
| 1.1.2.4 紛失 | 5 | 3 | 3 | 1 | 45 | 15 |
| 1.1.2.5 持ち出し | 1 | 3 | 2 | 1 | 6 | 3 |
| 1.1.2.6 持ち込み | 5 | 1 | 2 | 1 | 10 | 5 |
| 1.2.1 故障 | 5 | 1 | 2 | 1 | 10 | 5 |
| 1.2.2 災害 | 5 | 1 | 2 | 1 | 10 | 5 |
| 2.1.1 ウィルスの感染 | 5 | 1 | 2 | 1 | 10 | 5 |
| 2.1.2 不正アクセス | 5 | 1 | 2 | 1 | 10 | 5 |
| 2.1.3 盗聴 | 5 | 1 | 2 | 1 | 10 | 5 |
| 2.1.4 なりすまし | 5 | 1 | 2 | 1 | 10 | 5 |
| 2.1.5 DoS 攻撃 | 5 | 1 | 2 | 1 | 10 | 5 |
| 2.1.6 改ざん | 5 | 1 | 2 | 1 | 10 | 5 |
| 2.1.7 否認 | 5 | 1 | 2 | 1 | 10 | 5 |
| 2.1.8 不正コピー | 5 | 1 | 2 | 1 | 10 | 5 |
| 2.1.9 フィッシング | 5 | 1 | 2 | 1 | 10 | 5 |
| 2.2.1 誤操作 | 5 | 3 | 3 | 1 | 45 | 15 |
| 2.2.2 バグ | 5 | 1 | 2 | 1 | 10 | 5 |
| 合計 | | | | | 324 | 147 |

表 3-7 を基にして，対策後のリスク値削減率を表 3-8 に示す．同表に示すように，場のセキュリティにおけるリスク対策前に対し，対策を施した際のリスク値削減率が 55%であることがわかる．このことは，リスク値という相対的な指標ではあるが，具体的に，リスク対策の効果を可視化することが出来，これらの対策を施す際の参考に寄与しうると考えられる．

表 3-8　リスク値の削減率

| | 対策実施前(①) | 対策実施後(②) |
|---|---|---|
| リスク値合計 | 324 | 147 |
| リスク値削減率<br>= (①－②)/ ① | | 0.55 |

3.3　オフィスを対象にした物理セキュリティを考慮したリスクアセスメント結果

オフィス空間における物理セキュリティを考慮したリスクアセスメントとして，情報セキュリティの観点に物理セキュリティの観点を加えたリスク分析を行い，27 項目のリスク要因を抽出した．次に，これらのリスク要因に対し，リスクマトリクス手法に基づき，具体的なリスク対策案を提案し，情報セキュリティに物理セキュリティを加味した総合的なセキュリティ対策について示した．この結果，オフィス空間の場のセキュリティとして，具体的なリスク要因ならびに初歩的な対策案を明らかにした．

さらに，実用性の観点から，より客観性を高めるため，リスク値の算出式による定量化を行った．ここでは，リスク値の算出にあたり，リスクマトリクス手法の各要素に近似する手法を新たに提案し，最終的に，場のセキュリティにおいて抽出したリスク要因を数値化し，さらに，リスク対策前とリスク対策後のリスク値が算出でき，定量化できることを明らかにした．

これらの結果により，場のセキュリティ，即ち，物理及び情報の両面から総合的にリスクアセスメントした結果を新たに導出し，さらにこれらの対策案についても明示し，その効果に関し，実用性の観点からリスク値の導入により可視化し，実際のリスク対策を行う際の参考として提案することが出来た．

3.4　まとめ

第 3 章では，物理面を加味した情報セキュリティとして新たに定義した場のセキュリティのリスクアセスメントについて記した．オフィス空間を想定し，リスクマネジメントの代表的手法である RBS 手法により，27 項目のリスク要因が網羅的に抽出し，これら 27 要因に対し，同様に一般的手法であるリスクマトリクス手法に基づき，リスク分析を行った．

この結果，場のセキュリティのリスク対策案の重要性を明らかにした．さらに，より実用性の高い評価とするため，抽出したリスク要因に対するリスク値を近似計算し，対策前後のリスク値の比較結果から，対策案によるリスク削減効果が 55%であることを示し，定量的観点からも場のセキュリティのリスクアセスメントならびに，リスク対策案の有効性を併せて明らかにした．

参考文献

[3-1]PMI：プロジェクトマネジメント知識体系ガイド第 4 版，2008

[3-2]NTT 情報流通プラットフォーム研究所 : NTT R&D 情報セキュリティシリーズ，事例で学ぶ情報セキュリティマネジメント手法，2006 年

[3-3]M. S. Toosarvandani, N. Modiri, M. Afzali, “The Risk Assessment and Treatment Approach in order to Provide LAN Security based on ISMS Standard,” International Journal in Foundations of Computer Science & Technology (IJFCST), pp. 15-36, Vol. 2, No. 6, Nov., 2012

[3-4]佐藤周行他：情報セキュリティ基盤論，共立出版，2010

[3-5]ISMS Risk Assessment Manual v1.4, [Online]. Available from: https://www.igt.hscic.gov.uk/KnowledgeBaseNew/ISMS%20Risk%20Assessment%20Manual%20v1.4.pdf, 2015.1.4

[3-6]S. Tanimoto, et al., “A Study of Risk Assessment Quantification in Cloud Computing,” 8th International Workshop on Advanced Distributed and Parallel Network Applications (ADPNA-2014), pp. 426-431, Sep., 2014

[3-7]S. Tanimoto, et al., Risk Assessment Quantification of Ambient Service, ICDS 2015 : The Ninth International Conference on Digital Society, pp. 70-75, Lisbon, Feb., 2015

JNSA : 2011 年情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～，http://www.jnsa.org/result/incident/2011.html

[3-8]S.Yoneda, et al., Risk Assessment in Cyber-physical System in Office Environment, Network-Based Information Systems (NBiS), 2015 18th International Conference on, pp.412-417, Sep.2015

[3-9]米田翔一，谷本茂明，佐藤周行，金井敦：オフィス空間における場のセキュリティを考慮したリスクアセスメント, 第 13 回情報科学技術フォーラム(FIT2014)査読付き論文, RO-006，2014 年 9 月

4. センサ活用による場のセキュリティのリスクマネジメント:TPO 条件に基づく最適クラウド選択

ここでは，第 3 章の場のセキュリティのリスクアセスメント結果に対する評価として，ケーススタディとして，センサを活用した TPO 条件に基づいた最適なクラウド選択手法について述べる．具体的には，企業において一般に利用されている複数のクラウドのセキュアな選択手法について述べる．この複数のクラウドは，一般には，各クラウドプロバイダのセキュリティポリシにより運営されている．ここでは，このセキュリティポリシにより運用されているクラウドをここのセキュリティレベルとして定量的に明らかにする．一方，オフィスのセキュリティ環境も前述のように，TPO 条件により動的に変化する．この変化に関してもセキュリティレベルとして定量化する．

これらの結果を基にして，オフィスにおける TPO 条件に基づく動的なセキュリティレベルに応じたクラウド選択が可能な手法について明らかにする．

## 4.1 複数クラウドにおけるデータの価値に基づく静的クラウド選択手法（先行研究 [4-1]）

### 4.1.1 クラウドのセキュリティレベル可視化

表 4-1 に，現状，公開されている代表的なパブリッククラウドのセキュリティポリシに対し [4-2]-[4-7]，そのセキュリティレベルを可視化（数値化）した結果を示す．同表は，CSA のガイドラインに示されているクラウドをセキュアに運用するために必要なフォーカスエリアである 13 項目に基づき可視化した結果である [4-8]．一般に，可視化手法には，各クラウドが CSA 項目に対する充足度（各項目が記されているか否か）による手法，各項目に重みづけして評価する手法が考えられるが，ここでは，初期検討であること，簡易化の観点から，前者の充足度手法を用いた．即ち，CSA 項目との合致度（○の数の合計）で単純評価した．

表 4-1 クラウドセキュリティポリシの数値化結果

| CSAのフォーカスエリア ＼ パブリッククラウド（サービス形態） | | A社 SaaS, PaaS, IaaS | B社 SaaS, Paas | C社 IaaS, PaaS | D社 IaaS | E社 SaaS. PaaS, IaaS | F社 IaaS |
|---|---|---|---|---|---|---|---|
| 1. 物理セキュリティ | 1.1 データセンタ運用 | ○ | ○ | ○ | − | ○ | ○ |
| | 1.2 コンプライアンスと監査マネジメント | ○ | ○ | ○ | ○ | ○ | − |
| 2. サイバーセキュリティ | 2.1 従来のセキュリティ対策等 | ○ | ○ | ○ | − | ○ | ○ |
| | 2.2 アプリケーションセキュリティ | ○ | ○ | ○ | − | − | ○ |
| | 2.3 暗号化と鍵管理 | ○ | ○ | ○ | − | ○ | ○ |
| | 2.4 アイデンティティとアクセス管理 | ○ | ○ | ○ | − | ○ | ○ |
| | 2.5 仮想化 | ○ | − | ○ | − | − | ○ |
| 3. 運用ポリシ | 3.1 ガバナンスとERM | − | − | − | − | − | − |
| | 3.2 法律問題:契約と電子的証拠開示 | − | − | − | − | − | − |
| | 3.3 情報管理とデータセキュリティ | ○ | ○ | ○ | − | ○ | ○ |
| | 3.4 Security as a Service | − | − | − | − | − | − |
| | 3.5 相互運用性と移植性 | − | − | − | − | − | − |
| | 3.6 インシデントレスポンス，通知・復旧 | ○ | − | − | − | − | − |
| CSAの合致度(各項目の○の数の合計値) | | 9 | 7 | 8 | 1 | 6 | 7 |

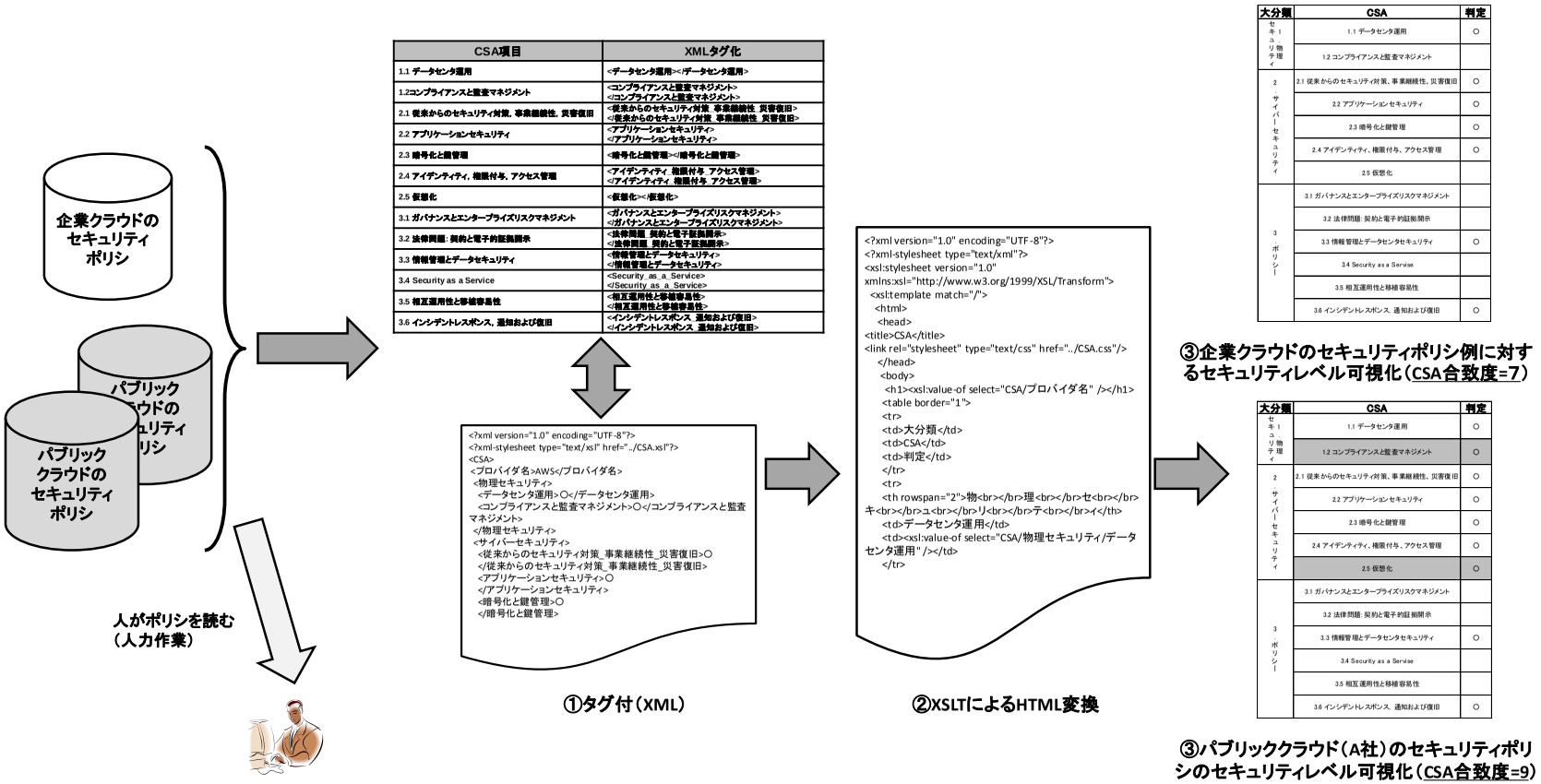
### 4.1.2 データの価値に基づく静的クラウド選択手法

一般に，複数のクラウドを利用する場合，データに求められるセキュリティレベルとクラウドの提供するセキュリティレベル，さらにコストとのマッチングを取って適切なクラウドを選択することが可能である．即ち，機密情報はセキュリティレベルの高いクラウドに置くことが一般に求められるが，このようなクラウドの運用コストは，複数人で運用することが必要になる等，高コスト構造となる．一方，公開情報では，コストを優先条件にしてセキュリティレベルの高くないクラウドを選択することができる．それぞれのデータ

の価値に合わせたセキュリティレベルのクラウドを選択することでコストの合理化が可能になる．しかし，それには，図 4-1 (1)に示すように，人力によりクラウドのセキュリティポリシを理解し，クラウドを選択する必要があった．これには，ポリシを理解するための時間，さらに選択可能か否かを判定するためのスキルが必要であった．

これに対し，先行研究では [4-1]，表 4-1 に示す 13 項目に基づき，各クラウドのセキュリティポリシを XML 手法により自動的に判定可能な可視化手法を提案した．具体的には，図 4-1 (2) ①に示すように, 各クラウドのセキュリティポリシを CSA の 13 項目を基に XML 化（タグ付け）し，さらに XSLT により HTML 化する．この結果, 図 4-1 (2) ③に示すように，各クラウドのセキュリティレベルが HTML により可視化できる（図 4-1 (2) ③の○の数）．即ち，クラウドのセキュリティポリシを予めタグ化しておけば，該当クラウドのセキュリティレベルが短時間でかつ特にスキルも必要とせず容易に判定でき，データの価値に基づくクラウド選択が可能となることを示した．

図 4-1　XMLによるクラウドのセキュリティレベル可視化の自動化




| CSA項目 | XMLタグ化 |
|---|---|
| 1.1 データセンタ運用 | <データセンタ運用></データセンタ運用> |
| 1.2コンプライアンスと監査マネジメント | <コンプライアンスと監査マネジメント><br></コンプライアンスと監査マネジメント> |
| 2.1 従来からのセキュリティ対策，事業継続性，災害復旧 | <従来からのセキュリティ対策_事業継続性_災害復旧><br></従来からのセキュリティ対策_事業継続性_災害復旧> |
| 2.2 アプリケーションセキュリティ | <アプリケーションセキュリティ><br></アプリケーションセキュリティ> |
| 2.3 暗号化と鍵管理 | <暗号化と鍵管理></暗号化と鍵管理> |
| 2.4 アイデンティティ，権限付与，アクセス管理 | <アイデンティティ_権限付与_アクセス管理><br></アイデンティティ_権限付与_アクセス管理> |
| 2.5 仮想化 | <仮想化></仮想化> |
| 3.1 ガバナンスとエンタープライズリスクマネジメント | <ガバナンスとエンタープライズリスクマネジメント><br></ガバナンスとエンタープライズリスクマネジメント> |
| 3.2 法律問題：契約と電子的証拠開示 | <法律問題_契約と電子証拠開示><br></法律問題_契約と電子証拠開示> |
| 3.3 情報管理とデータセキュリティ | <情報管理とデータセキュリティ><br></情報管理とデータセキュリティ> |
| 3.4 Security as a Service | <Security_as_a_Service><br></Security_as_a_Service> |
| 3.5 相互運用性と移植容易性 | <相互運用性と移植容易性><br></相互運用性と移植容易性> |
| 3.6 インシデントレスポンス，通知および復旧 | <インシデントレスポンス_通知および復旧><br></インシデントレスポンス_通知および復旧> |

```
<?xml version="1.0" encoding="UTF-8"?>
<?xml-stylesheet type="text/xsl" href="../CSA.xsl"?>
<CSA>
<プロバイダ名>AWS</プロバイダ名>
 <物理セキュリティ>
  <データセンタ運用>○</データセンタ運用>
  <コンプライアンスと監査マネジメント>○</コンプライアンスと監査
マネジメント>
 </物理セキュリティ>
 <サイバーセキュリティ>
  <従来からのセキュリティ対策_事業継続性_災害復旧>○
  </従来からのセキュリティ対策_事業継続性_災害復旧>
  <アプリケーションセキュリティ>○
  </アプリケーションセキュリティ>
  <暗号化と鍵管理>○
  </暗号化と鍵管理>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<?xml-stylesheet type="text/xml"?>
<xsl:stylesheet version="1.0"
xmlns:xsl="http://www.w3.org/1999/XSL/Transform">
 <xsl:template match="/">
  <html>
   <head>
<title>CSA</title>
<link rel="stylesheet" type="text/css" href="../CSA.css"/>
   </head>
   <body>
    <h1><xsl:value-of select="CSA/プロバイダ名" /></h1>
   <table border="1">
   <tr>
   <td>大分類</td>
   <td>CSA</td>
   <td>判定</td>
   </tr>
   <tr>
   <th rowspan="2">物<br></br>理<br></br>セ<br></br>キ<br></br>ュ<br></br>リ<br></br>テ<br></br>イ</th>
   <td>データセンタ運用</td>
   <td><xsl:value-of select="CSA/物理セキュリティ/データセンタ運用" /></td>
   </tr>
```

| 大分類 | CSA | 判定 |
|---|---|---|
| セキュリティ物理 | 1.1 データセンタ運用 | ○ |
| | 1.2 コンプライアンスと監査マネジメント | |
| 2．サイバーセキュリティ | 2.1 従来からのセキュリティ対策、事業継続性、災害復旧 | ○ |
| | 2.2 アプリケーションセキュリティ | ○ |
| | 2.3 暗号化と鍵管理 | ○ |
| | 2.4 アイデンティティ、権限付与、アクセス管理 | ○ |
| | 2.5 仮想化 | |
| 3．ポリシー | 3.1 ガバナンスとエンタープライズリスクマネジメント | |
| | 3.2 法律問題：契約と電子的証拠開示 | |
| | 3.3 情報管理とデータセンタセキュリティ | ○ |
| | 3.4 Security as a Service | |
| | 3.5 相互運用性と移植容易性 | |
| | 3.6 インシデントレスポンス、通知および復旧 | ○ |

| 大分類 | CSA | 判定 |
|---|---|---|
| セキュリティ物理 | 1.1 データセンタ運用 | ○ |
| | 1.2 コンプライアンスと監査マネジメント | ○ |
| 2．サイバーセキュリティ | 2.1 従来からのセキュリティ対策、事業継続性、災害復旧 | ○ |
| | 2.2 アプリケーションセキュリティ | ○ |
| | 2.3 暗号化と鍵管理 | ○ |
| | 2.4 アイデンティティ、権限付与、アクセス管理 | ○ |
| | 2.5 仮想化 | ○ |
| 3．ポリシー | 3.1 ガバナンスとエンタープライズリスクマネジメント | |
| | 3.2 法律問題：契約と電子的証拠開示 | |
| | 3.3 情報管理とデータセンタセキュリティ | ○ |
| | 3.4 Security as a Service | |
| | 3.5 相互運用性と移植容易性 | |
| | 3.6 インシデントレスポンス、通知および復旧 | ○ |

4.2　TPO 条件に基づく動的クラウド選択手法の提案

4.2.1　オフィスにおける動的セキュリティ環境

一般に, オフィスにおいては, 守るべき情報資産の価値や脅威, 脆弱性は, TPO 条件(Time : 時間，Place : 場所，Occasion : 状況)に応じて常に動的に変化している [4-9]．例えば，オフィスにおいて機密情報を取り扱っている時に，他社の人間が打ち合わせ等で来訪した際，そのリスクは増大する．この場合，機密情報の扱いを取りやめ，公開情報等を扱うようにすることが望ましい. データの価値に基づくクラウド選択においても同様に考えると，4.1.1 で述べた静的選択手法に対し，より実用的な観点からの考慮が重要となる．即ち，機密情報に見合ったセキュリティレベルの高いクラウドの扱いを取りやめ，公開情報に見合ったセキュリティレベルのクラウドを扱うことが望ましい.

このように，オフィスでのクラウド利用を考慮した場合，より実用的な観点から，TPO 条件に応じた適切なクラウド選択が重要となる．このような状況を鑑み，本論文では，オフィスを対象に，TPO 条件に基づく動的なクラウド選択手法を新たに提案する．

最初に，オフィスにおける動的な状況を網羅的に導出し，そのリスクを可視化する．次に，より実用的な観点からクラウドのセキュリティレベルの導出，即ち，重みづけを考慮したレベル付けを行う．最後に，これらを連携させる手法について具体的に提案する．

4.2.2　TPO パターンに対するリスクの定量化

最初に, オフィスにおける TPO 条件の観点からクラウド利用環境を想定する. この場合, 表 4-2 に示すように全部で 8 パターンとなる.

表 4-2　オフィスにおける TPO パターン

| ﾊﾟﾀｰﾝ | T（時間） | P(場所） | O（場合） |
|---|---|---|---|
| ① | 業務時間内 | 社内 | 社員のみ |
| ② | 業務時間内 | 社内 | 社員とゲスト |
| ③ | 業務時間内 | 社外 | 社員のみ |
| ④ | 業務時間内 | 社外 | 社員とゲスト |

| ﾊﾟﾀｰﾝ | T（時間） | P(場所） | O（場合） |
|---|---|---|---|
| ⑤ | 業務時間外 | 社内 | 社員のみ |
| ⑥ | 業務時間外 | 社内 | 社員とゲスト |
| ⑦ | 業務時間外 | 社外 | 社員のみ |
| ⑧ | 業務時間外 | 社外 | 社員とゲスト |

表 4-2 に対し, 式(1)に示すリスク算出式により [4-10], 各パターンのリスク値を求める.

$$\textit{リスク値} = \textit{資産価値（A）} \times \textit{脅威（T）} \times \textit{脆弱性（V）} \qquad (1)$$

ここで，リスク値を求める際には，次の仮定を用いる．資産価値（A）は一定と仮定し，最高値の 5 を用いる．脅威（T），脆弱性（V）については，業務時間内，社内，社員のみの項目を基本（1 とする）とし，表 4-3 に示す仮定で変動させる．これらの仮定の下，表 4-2 の各パターンのリスク値を求めた結果を表 4-4 に示す.

表 4-3　脅威と脆弱性の値の仮定

| 変動要因 | | 評価値の変動 | | 評価値の変動根拠 |
|---|---|---|---|---|
| | | T:脅威 | V:脆弱性 | |
| T | 業務時間内→業務時間外 | －1 | ＋1 | 業務時間外になると社員が減るため，監視の目が少なくなり脆弱性が増すが，脅威は変わらない |
| P | 社内→社外 | ＋1 | ＋1 | 社外に出ることで，社内のセキュリティシステムから外れ脆弱性が増し，盗難などの脅威も増える. |
| O | 社員のみ→社員とゲスト | ＋1 | －1 | ゲストが居ることで，情報を盗み見られるなどの脅威が増えるが，脆弱性は変わらない. |

表 4-4　TPO パターンにおけるリスク値算出結果

| パターン | A（資産価値） | T（脅威） | V（脆弱性） | リスク値＝A × T × V |
|---|---|---|---|---|
| ① | 5 | 1 | 1 | 5 |
| ② | 5 | 2 | 1 | 10 |
| ③ | 5 | 2 | 2 | 20 |
| ④ | 5 | 3 | 2 | 30 |
| ⑤ | 5 | 1 | 2 | 10 |
| ⑥ | 5 | 2 | 2 | 20 |
| ⑦ | 5 | 2 | 3 | 30 |
| ⑧ | 5 | 3 | 3 | 45 |

4.3　重みづけによるクラウドセキュリティレベル

次に，実運用性の観点から，現状のクラウドのセキュリティレベルを評価する．即ち，4.2.1 で述べた重みづけ手法を導入する．この導入に際し，次の仮定を基に相対的な重みづけを行った結果を表 4-5 に示す．

仮定1）　表 4-5 の評価①は，表 4-1 に示す CSA の 13 項目を現状のプロバイダによる採用不採用に関わらず，最低限必要な基準として各 10 点の重みづけとした．

仮定2）　評価②は，現状のプロバイダの CSA 項目の採用状況を現用値として評価した．具体的には，CSA の項目毎に，現状のプロバイダが採用している総数を表 4-1 の全プロバイダ数（=6）で割った値に基準点の 10 を乗じたものである（さらに，小数点 1 位を四捨五入し整数化している）．

最後に①と②を合計したものが実運用性の観点から重みづけしたクラウドのセキュリティレベルとなる．

表 4-5　重みづけによるクラウドセキュリティレベル

| CSAのフォーカスエリア | パブリッククラウド（サービス形態） | 評価① | 評価② | | | | | | | 総合評価（①+②） |
|---|---|---|---|---|---|---|---|---|---|---|
| | | 基準値（10点） | A社 | B社 | C社 | D社 | E社 | F社 | 現用値（○の総和/6） | |
| 1. 物理セキュリティ | 1.1 データセンタ運用 | 10 | ○ | ○ | ○ | − | ○ | ○ | 8 | 18 |
| | 1.2 コンプライアンスと監査マネジメント | 10 | ○ | ○ | ○ | ○ | ○ | − | 8 | 18 |
| 2. サイバーセキュリティ | 2.1 従来のセキュリティ対策等 | 10 | ○ | ○ | ○ | − | ○ | ○ | 8 | 18 |
| | 2.2 アプリケーションセキュリティ | 10 | ○ | ○ | ○ | − | − | ○ | 6 | 16 |
| | 2.3 暗号化と鍵管理 | 10 | ○ | ○ | ○ | − | ○ | ○ | 8 | 18 |
| | 2.4 アイデンティティとアクセス管理 | 10 | ○ | ○ | ○ | − | ○ | ○ | 8 | 18 |
| | 2.5 仮想化 | 10 | ○ | − | ○ | − | − | ○ | 5 | 15 |
| 3. 運用ポリシ | 3.1 ガバナンスとERM | 10 | − | − | − | − | − | − | 0 | 10 |
| | 3.2 法律問題：契約と電子的証拠開示 | 10 | − | − | − | − | − | − | 0 | 10 |
| | 3.3 情報管理とデータセキュリティ | 10 | ○ | ○ | ○ | − | ○ | ○ | 8 | 18 |
| | 3.4 Security as a Service | 10 | − | − | − | − | − | − | 0 | 10 |
| | 3.5 相互運用性と移植性 | 10 | − | − | − | − | − | − | 0 | 10 |
| | 3.6 インシデントレスポンス，通知・復旧 | 10 | ○ | − | − | − | − | − | 1 | 11 |
| 合　計 | | | | | | | | | | 190 |

この表 4-5 を基に, 重みづけを加味した各プロバイダのセキュリティレベル算出結果を表 4-6 に示す.

表 4-6　重みづけを考慮したセキュリティレベル算出結果

| パブリッククラウド | A社 | B社 | C社 | D社 | E社 | F社 |
|---|---|---|---|---|---|---|
| セキュリティレベル | 150 | 124 | 139 | 18 | 108 | 121 |

4.4　TPO パターンに応じた動的クラウド選択手法

ここでは，4.2 に示すオフィスにおける様々なリスクを表 4-4 に示すように数値化した結果と, 表 4-6 に示す現状のクラウドのセキュリティレベルとの動的選択手法について述べる. 即ち，オフィスにおけるリスク値に応じた常に最適なクラウド選択手法について述べる.

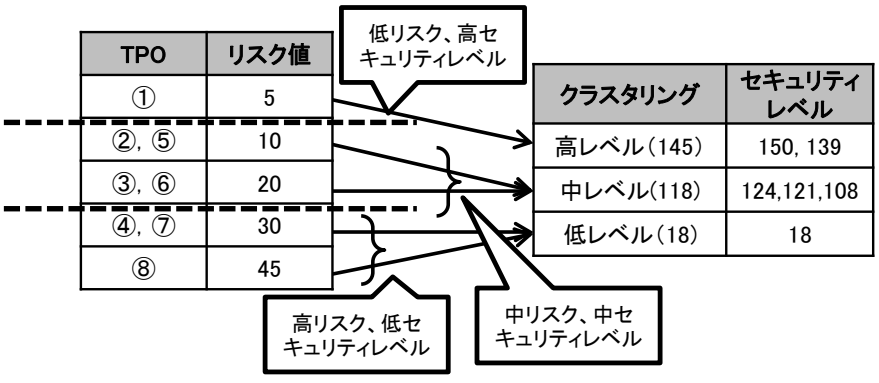
一般に，リスク値に基づくクラウド選択手法には，閾値による機械的な手法が用いられる. 本論文では, さらなる実用的な観点から, オフィスにおける TPO パターンのリスク値, 現状のクラウドのセキュリティレベルを鑑みると，図 4-2(1)のように，リスクは 5 つにクラスタリング，セキュリティレベルは 3 つにクラスタリングできる．これを基に，安全側の観点から，図 4-2(2)に示すような選択手法をとることとする.

| TPOパターン | リスク値 |
|---|---|
| ① | 5 |
| ②, ⑤ | 10 |
| ③, ⑥ | 20 |
| ④, ⑦ | 30 |
| ⑧ | 45 |

| クラスタリング | セキュリティレベル |
|---|---|
| 高レベル（145） | 150, 139 |
| 中レベル(118) | 124,121,108 |
| 低レベル（18） | 18 |

（注）クラスタリングの（ ）内の数字は，平均セキュリテイレベルである

(1 ) リスク値とクラウドのセキュリティレベルのクラスタリング




(2 ) リスク値とクラウドのセキュリティレベルのマッピング

図 4-2　リスク値を基にしたクラウド選択手法

図 4-2(2)を基にして導出した TPO 別のリスクレベルのグラフ，対応するクラウドレベルのグラフを図 4-3 に示す.

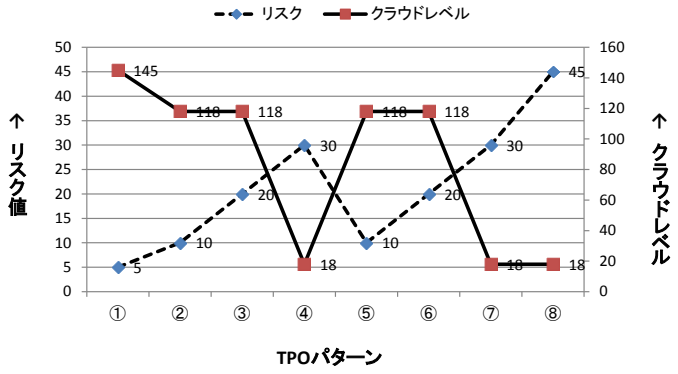



図 4-3　TPO パターンのリスク値とクラウドレベルの関係(1)

図 4-3 に示すように，リスク値が低い場合は，セキュリティレベルの高いクラウドを，リスク値が高くなるとセキュリティレベルの低いクラウドを選択，即ち，リスクレベルに応じた選択ができることがわかる．

次に，図 4-3 に対し，TPO パターンをそれぞれ，(1)勤務時間内／外，(2)社内／外，(3)社員のみ／社員とゲストの 3 パターンに分けてグラフ化すると，図 4-4 のようになる．

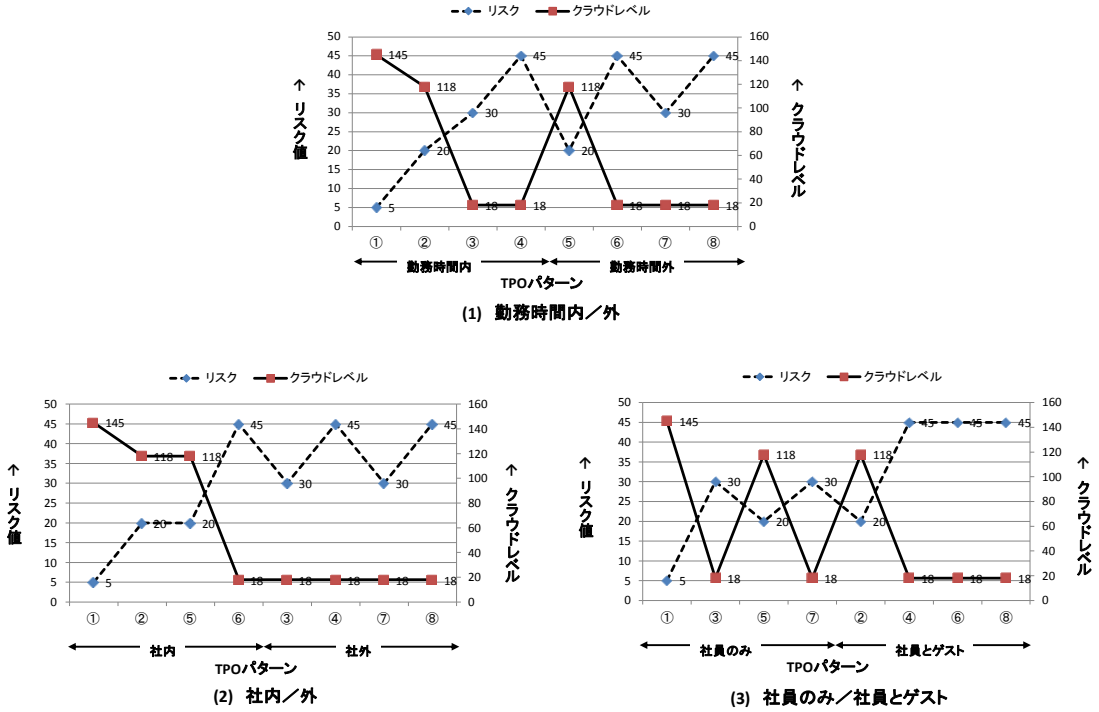



図 4-4　TPO パターンのリスク値とクラウドレベルの関係(2)

図 4-4 (1)~(3)に示すように, 時間外や社外, ゲストがいる場合においては, リスクが高く, その分，クラウド選択も公開情報を扱う，即ち，比較的セキュリティレベルの低いクラウドを選択することが望ましい結果となっていることが分かる．

## 4.5 まとめ

第 4 章では，TPO 条件に基づく最適なクラウドの動的選択手法を新たに提案した．具体的には, CSA の項目に対し, 各クラウドプロバイダのポリシが持つセキュリティレベルを，重みづけを用いることでより実用的な観点で可視化した．さらに，動的に変化するオフィス空間のリスクレベルを TPO 条件に基づき定量化した．これらクラウドのセキュリティポリシとオフィスのリスク値を閾値でクラスタリングし，その結果を機械的に対応させることで，リスク値に応じたクラウドの自動選択を可能とした．これにより，TPO 条件に応じたセキュアなクラウド選択に資することができた．

参考文献

[4-1] 大角地涼介，佐藤亮太，米田翔一，谷本茂明，佐藤周行，金井敦：パブリッククラウドと企業ネットワークのセキュリティポリシー連携マネジメントに関する研究，プロジェクトマネジメント学会春季研究発表大会，pp.205-208, 2015

[4-2]Amazon Web Services：セキュリティプロセスの概要 http://media.amazonwebservices.com/jp/wp/AWS_Security_Whitepaper_JP_201505.pdf，May. 2011

[4-3]Google for Work：Google for Work のセキュリティに関するホワイトペーパー:, http://static.googleusercontent.com/media/www.google.com/ja//a/help/intl/ja/admins/pdf/WP64-1005_Security_Backgrounder_JA.pdf

[4-4]Microsoft Azure のセキュリティ，プライバシー，コンプライアンス, http://go.microsoft.com/fwlink/?linkid=392408&clcid=0x411，Apr. 2015

[4-5]Yahoo！クラウド，http://cloud.yahoo.co.jp/storage/

[4-6]IBM：信頼とセキュリティ，http://www.ibm.com/cloud-computing/social/jp/ja/security/

[4-7]ニフティクラウド：セキュリティホワイトペーパー, http://cloud.nifty.com/pdf/security_whitepaper.pdf，2014

[4-8]日本クラウドセキュリティアライアンス：クラウドコンピューティングのためのセキュリティガイダンス V3.0, http://www.cloudsecurityalliance.jp/j-docs/csaguide.v3.0.1_J.pdf， May. 2013

[4-9]谷本茂明，関良明，木村義政，木内陽介：個人のコンテキスト情報に基づく動的多重帰属グループサービスの提案，情報処理学会論文, Vol. 51, No. 2, 575–589, 2010

[4-10]ISMS Risk Assessment Manual v1.4, https://www.igt.hscic.gov.uk/KnowledgeBaseNew/ISMS%20Risk%20Assessment%20Manual%20v1.4.pdf

[4-11]米田翔一，大角地涼介，谷本茂明，佐藤周行，金井敦：TPO 条件に基づく複数クラウドにおける動的クラウド選択手法の提案，電子情報通信学会論文誌，Vol.J99-D, No.10, pp.1045-1049, 2016 年 10 月

5.　センサ活用による場のセキュリティのリスクマネジメント:センサを活用した ISMS の ROSI 効率化

ここでは，第 4 章と同様に，第 3 章のリスクアセスメント結果に対する評価として，新たにセンサの活用をポイントにリスクマネジメントとしての対策案について述べる．具体的には，ISMS 普及促進に寄与する観点から，センサ活用によるリスクマネジメント対策による効果について述べる．第 2 章でも言及したように，オフィスにおいては，近年の IoT 技術の進展，特にセンサ技術の活用により，例えば，監視カメラなどの物理セキュリティを情報セキュリティマネジメントと組み合わせることによるコストの低減化，特にセンサが人的稼働を軽減出来ることを明らかにする．

5.1　ISMS の現状と課題

企業など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 ISMS は，図 5-1 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 [5-1]．また，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，完全性をバランスよく維持し，継続的な改善を行っていくことを要求している．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，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%)」など，コストに関する要因が挙げられている [5-2]．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挙げられている．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な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過ぎると回答している [5-3].

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わかる．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言われており [5-4]-[5-6]，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．

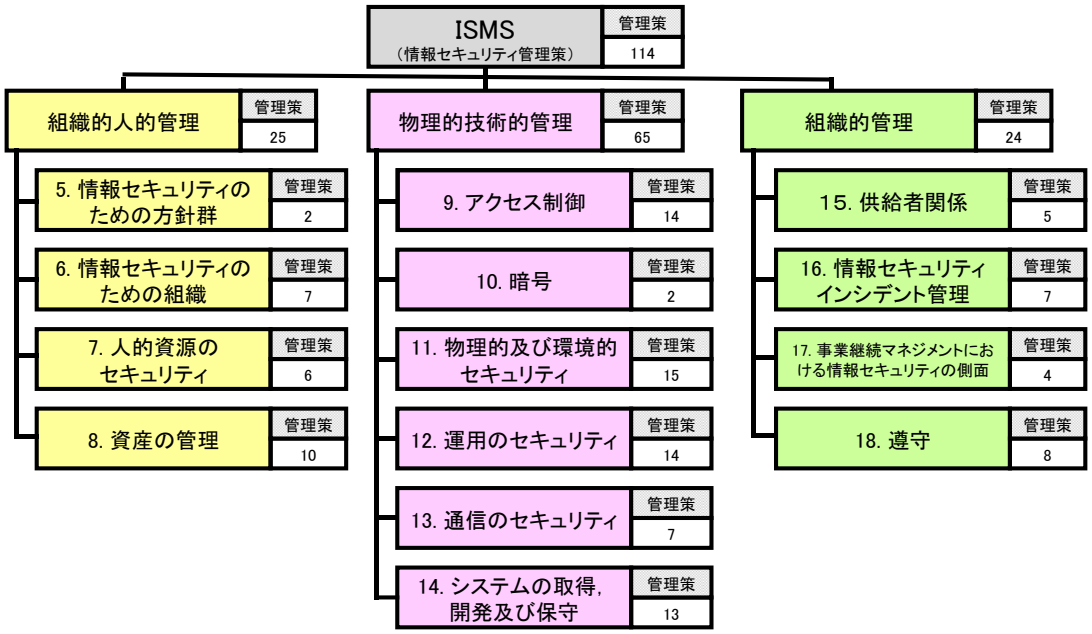



図 5-1　ISMS の管理策（114 項目）の全体構造

## 5.2　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 [5-7]-[5-11], 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 [5-11]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 [5-12]. 関連して, 文献 [5-13]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.

一方, 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 [5-14]-[5-15], これらは費用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, 例えば, 文献 [5-16]では, サイバー攻撃の検知にマルチコプター（ドローン）を利用しているが, これも具体的な費用対効果の導出には至っていない.

## 5.3　ISMS の費用面導出

ここでは, ISMS 費用面の導出について, 机上シミュレーションによる導出を行う. 費用面の導出に際しては, 1）初期コストに着目した静的導出と, 2）運用コストに着目した動的導出に分け, 段階的に導出する.

### 5.3.1　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 [5-17]を参考にした. これらの結果を表 5-1 に示す.

表 5-1　主な分析手法の種類

| 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. | ×<br>・類似事例が無い |
| | **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.** | **○<br>・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. | ×<br>・詳細に評価できるが, 実際のシステムが必要 |

表 5-1 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無いことから類推法を使用することが出来ない．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 5-1 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，推測手法の一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 5-1 に示す ISMS の 114 の管理項目の「実施の手引」を参考にし [5-3]，図 5-2 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．

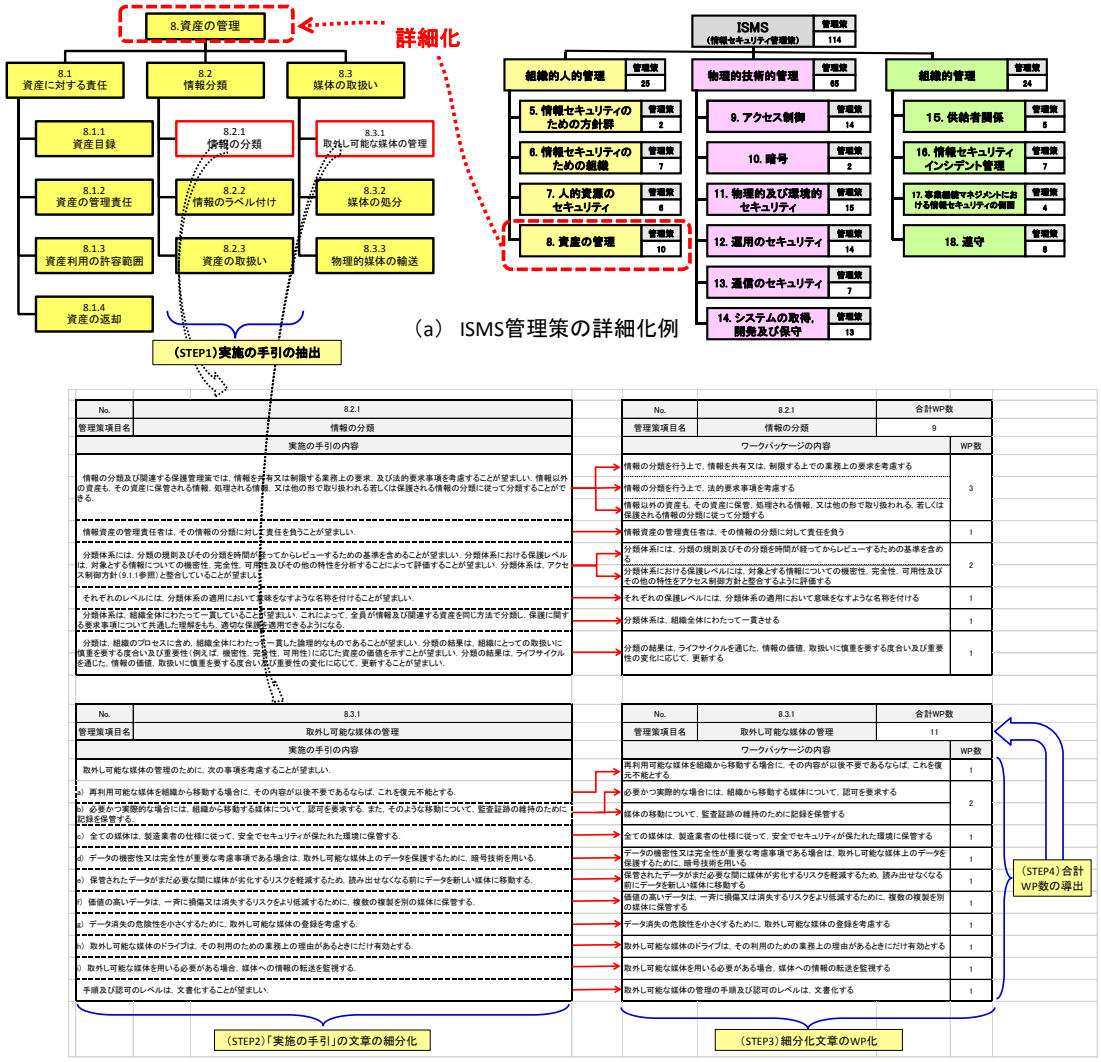



図 5-2　机上シミュレーションによる WP 数の近似算出例

(2-1) ISMS 管理策の詳細化（図 5-2 (a)）

図 5-1 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，これを更に詳細化すると，図 5-2（a）左側のように 10 の管理策に細分化される．文献[5-1]では，この管理策毎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 5-2 (b)）

机上シミュレーションは，図 5-3 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 化し易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．

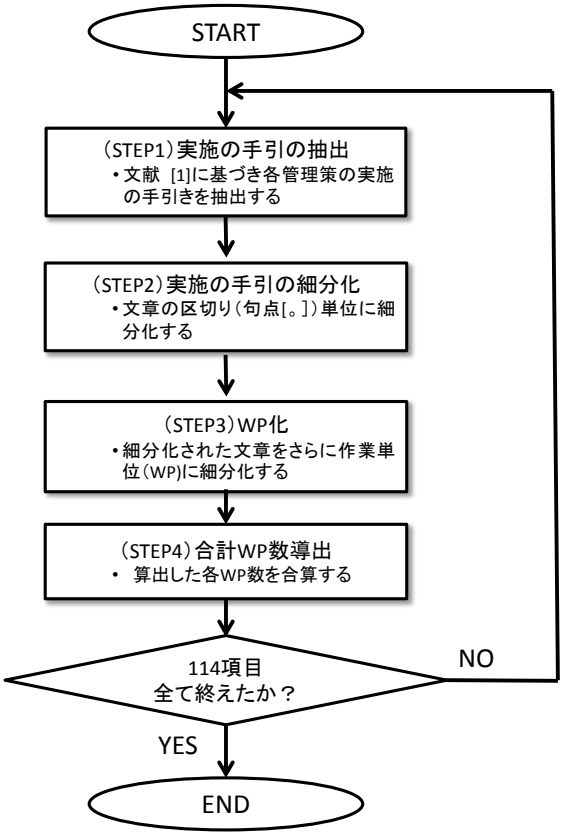



図 5-3　机上シミュレーションによる WP 数算出フロー

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 5-2 (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，即ち，WP 化し易くするために，以下の前提条件に基づき，図 5-2(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 5-2(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．

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 5-2 (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，（作業目的などの）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 5-2(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 で細分化した文章毎に 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 [5-18]．この結果を表 5-2 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，一般には，それぞれ異なっている．従って，それらの工数も当然相違があるが，マクロに見れば，各 WP の工数の大小は，数が多くなるとある程度は相殺され得ることを考慮し，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上でのシミュレーションは今後の検討課題とする．

表 5-2(1/2)　ISMS における費用の近似導出結果（費用≒WP 数）

| 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 |

表 5-2(2/2)　ISMS における費用の近似導出結果（費用≒WP 数）

| No. | ISMSの管理策 | | 費用(≒WP数) |
|---|---|---|---|
| 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 |

5.3.2　ISMS における費用の近似導出（動的導出）

ここでは，表 5-2 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 5-4 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 [5-18].

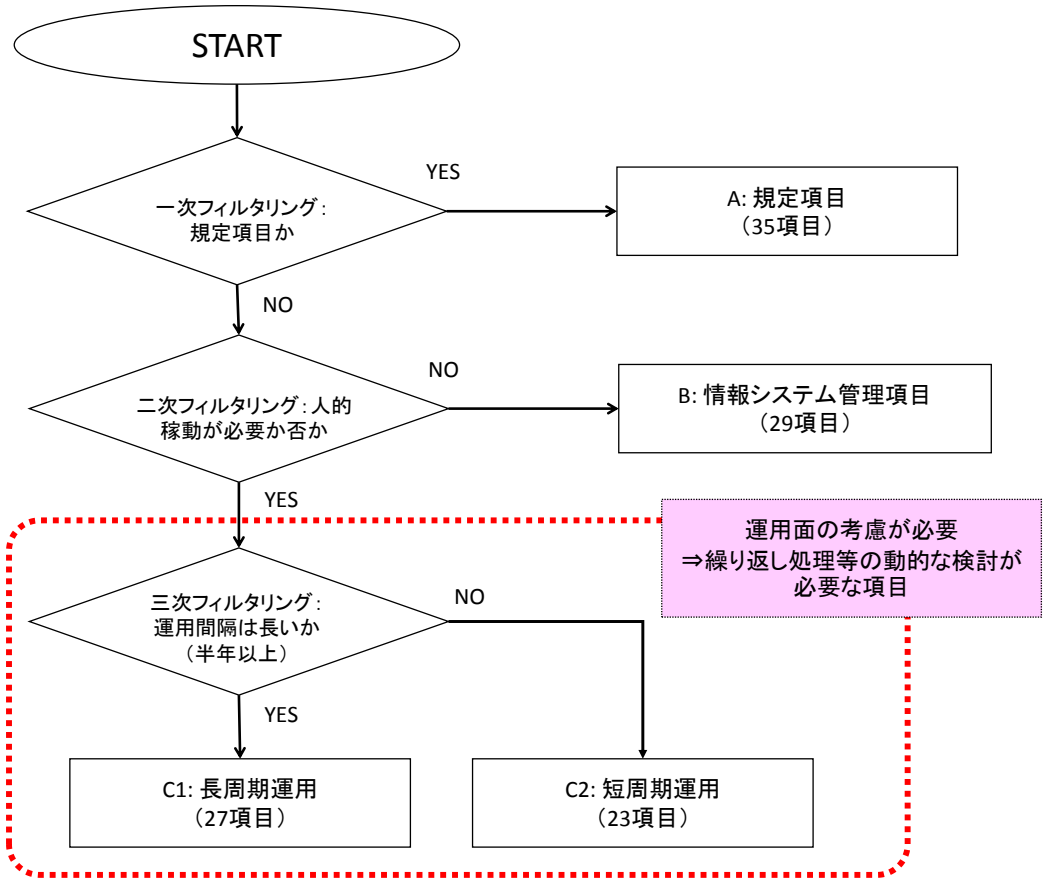



図 5-4　動的費用項目導出フロー

①一次フィルタリング(A: 規定項目を抽出)

表 5-2 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，監査などのように半年もしくは 1 年単位で行うものと(図 5-4 C1: 長周期運用)，入退室管理など時間単位もしくは日毎単位で行うもの(図 5-4 C2:短周期運用)に分類できる．長周期運用は，監査など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．

④運用面を考慮した ISMS 費用の導出結果

次に，図 5-4 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 5-3 に示す観点を用いることとした．

表 5-3　運用面を考慮した動的費用導出の観点

| 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]

表 5-3 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 5-2 を用いた．即ち，表 5-2 の費用に対し，表 5-3 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 5-4 に示す．

表 5-4(1/2)　運用面を考慮した費用導出結果（費用≒WP 数）

| No. | ISMSの管理策 | | 静的費用 | 動的費用 | | |
|---|---|---|---|---|---|---|
| | | | | 図5-4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 |

表 5-4(2/2)　運用面を考慮した費用導出結果（費用≒WP 数）

| No. | ISMSの管理策 | | 静的費用 | 動的費用 | | |
|---|---|---|---|---|---|---|
| | | | | 図5-4の分類 | 3年間回数 | 動的費用 |
| 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 | ｵﾍﾟﾚｰﾃｨﾝｸﾞﾌﾟﾗｯﾄﾌｫｰﾑ変更後のｱﾌﾟﾘｹｰｼｮﾝの技術的ﾚﾋﾞｭｰ | 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 | ICtT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 |

5.4　ISMS の効果の近似導出

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 [5-19]-[5-21]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，（１）式のリスク値により導出する．

**リスク値　＝　資産　×　脅威　×　脆弱性**　　**（１）**

ここで，さらに，図 5-5 に示すように，リスクマトリクスを基にして，（１）式の各パラメータの評価基準を示す [5-19]-[5-21].

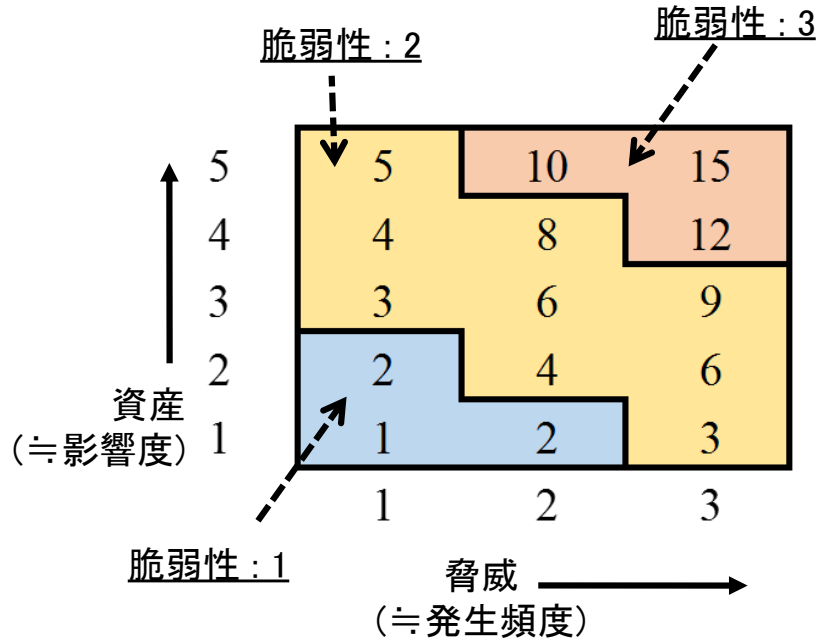



図 5-5　リスク値の各パラメータ評価基準の近似

これらの前提条件を基にして, (1)式により ISMS の 114 の対策に対するリスク値を導出した結果を表 5-5 に示す [5-22].

5.5　ISMS の費用対効果

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

表 5-5(1/2)　ISMS の効果

| 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 |

表 5-5(2/2)　ISMS の効果

| No | ISMSの管理策 | | 効果 | | | |
|---|---|---|---|---|---|---|
| | | | 資産<br>(影響度) | 脆弱性 | 脅威<br>(発生<br>頻度) | リスク値 |
| 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 5-6(1/2)　ISMS における運用を考慮に入れた費用対効果

| No. | ISMSの管理策 | | 効果<br>（≒リスク値） | 費用<br>（≒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 |

表 5-6(2/2)　ISMS における運用を考慮に入れた費用対効果

| No. | ISMSの管理策 | | 効果<br>(≒リスク値) | 費用<br>(≒WP数) |
|---|---|---|---|---|
| 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 | ｵﾍﾟﾚｰﾃｨﾝｸﾞﾌﾟﾗｯﾄﾌｫｰﾑ変更後のｱﾌﾟﾘｹｰｼｮﾝの技術的ﾚﾋﾞｭｰ | 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 |

## 5.6　センサ活用に基づく費用削減効果

ここでは，図 5-4 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 5-4，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．

### 5.6.1　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 5-6 に，また，各センサの概要を表 5-7 に示す．

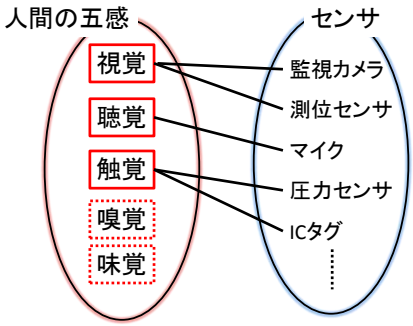



図 5-6　人間の五感とセンサ

表 5-7　各センサの概要

| 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 |

これらのセンサに対し，短周期項目（図 5-4，C2）の業務内容（WP）を対応させた結果を表 5-8 に示す.

表 5-8(1/3)　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 | | ○ | | ○ | | | | | |

# 表 5-8(2/3)　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. | 27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 | | | |
| 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 | | | | | | | | | |
| 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 | | | ○ | ○ | | | | | |

表 5-8(3/3)　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. | 22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 | | | |
| 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，トークン若しくは類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 |

表 5-8 の結果から，短周期項目 23 項目のうち 19 項目が図 5-6 に示す各種センサで代替可能である項目であることが新たにわかった．この結果，図 5-4 のフローは，図 5-7 の破線部分に示すように，さらにセンサ技術の代替可否によって分類できる．

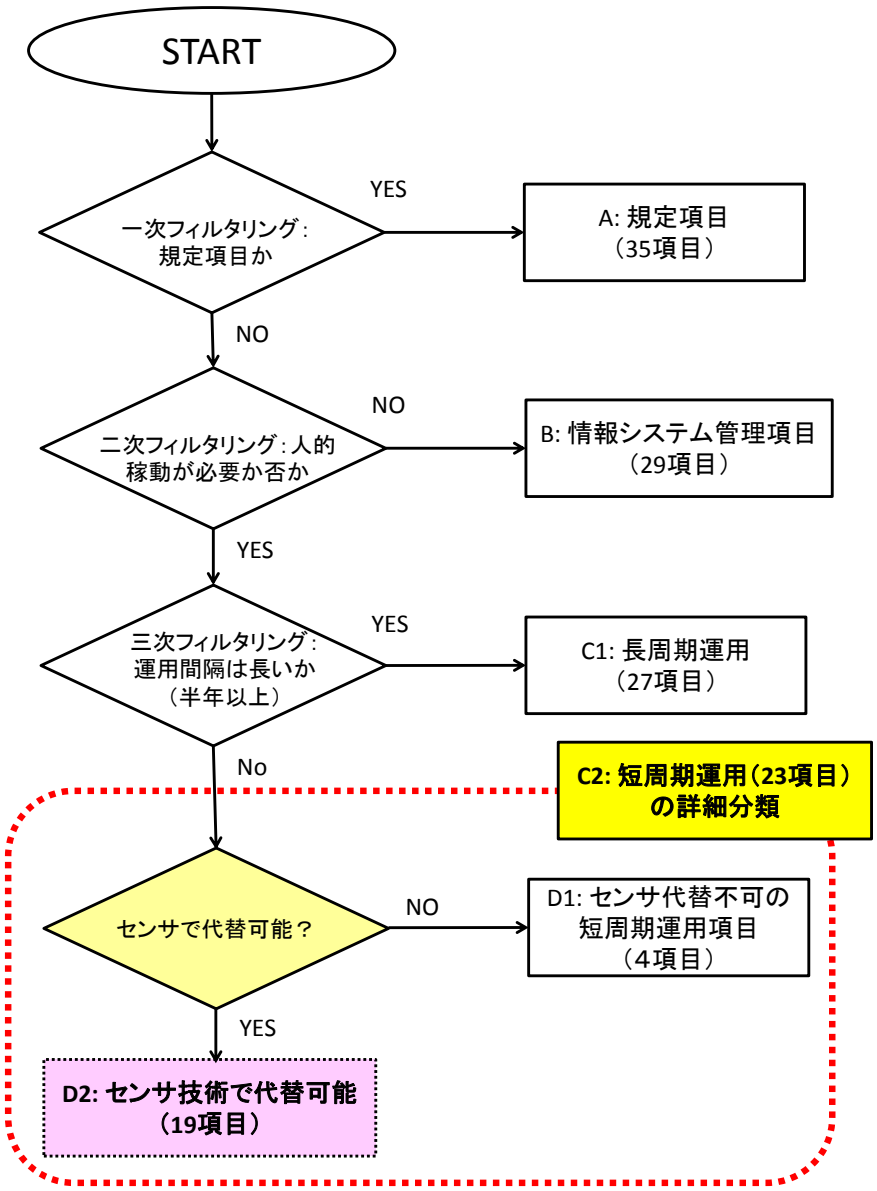



図 5-7　センサ代替可能項目導出フロー

5.7　センサ活用に基づく ISMS 対策に対する費用対効果

5.6 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 5-6 と同様にして導出する．効果は，表 5-6 と同様，表 5-5 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 5-3 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，表 5-8 に示すセンサ活用による削減効果，即ち，全体で 34,290WP 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取りまとめた結果を表 5-9 に示す．

表 5-9(1/2)　センサ活用による費用対効果の導出結果

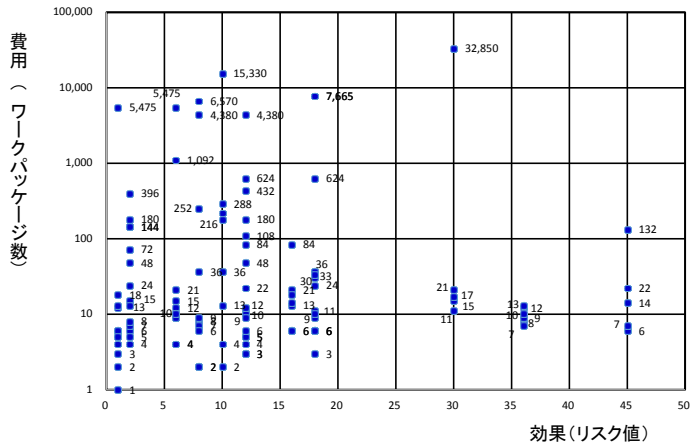
| No. | ISMSの管理策 | | 効果<br>（≒リスク値） | 費用<br>（≒WP数） |
|---|---|---|---|---|
| 1 | 5.1.1 | 情報セキュリティのための方針群 | 45 | 22 |
| 2 | 5.1.2 | 情報セキュリティのための方針群のレビュー | 36 | 12 |
| 3 | 6.1.1 | 情報セキュリティの役割及び責任 | 45 | 6 |
| 4 | 6.1.2 | 職務の分離 | 8 | 2 |
| 5 | 6.1.3 | 関係当局との連絡 | 10 | 2 |
| 6 | 6.1.4 | 専門組織との連絡 | 18 | 36 |
| 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 |

表 5-9(2/2)　センサ活用による費用対効果の導出結果

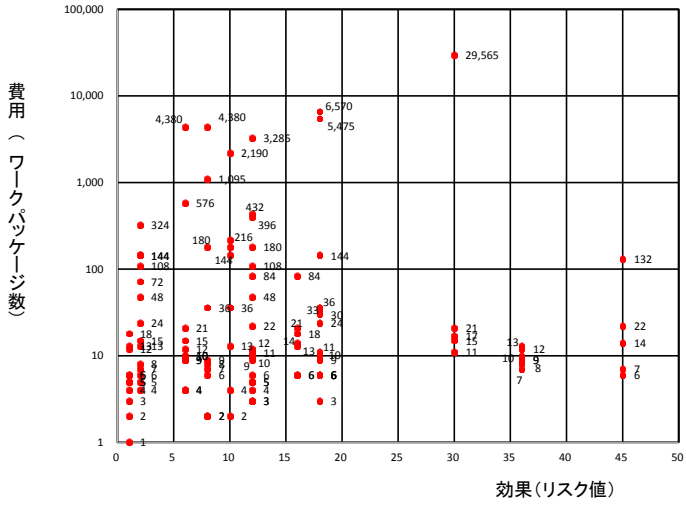
| No. | ISMSの管理策 | | 効果<br>(≒リスク値) | 費用<br>(≒WP数) |
|---|---|---|---|---|
| 57 | 12.1.1 | 操作手順書 | 6 | 10 |
| 58 | 12.1.2 | 変更管理 | 18 | 9 |
| 59 | 12.1.3 | 容量・能力の管理 | 12 | 48 |
| 60 | 12.1.4 | 開発環境，試験環境及び運用環境の分離 | 8 | 8 |
| 61 | 12.2.1 | マルウェアに対する管理策 | 45 | 14 |
| 62 | 12.3.1 | 情報のバックアップ | 16 | 6 |
| 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 | ｵﾍﾟﾚｰﾃｨﾝｸﾞﾌﾟﾗｯﾄﾌｫｰﾑ変更後のｱﾌﾟﾘｹｰｼｮﾝの技術的ﾚﾋﾞｭｰ | 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 |

## 5.8　考察

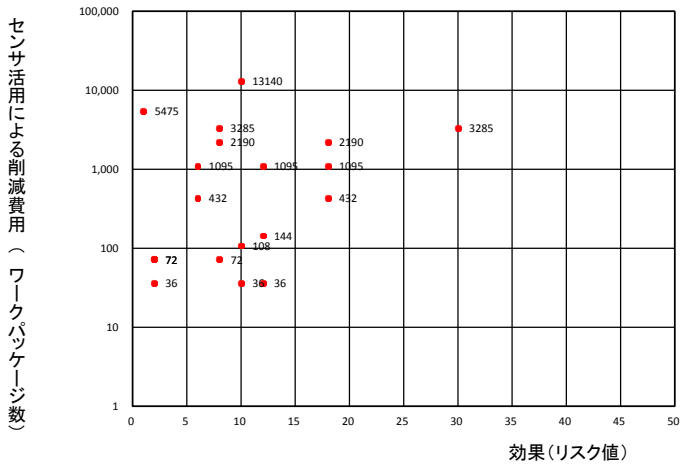
表 5-6 および表 5-9 の結果を二次元化すると，図 5-8 のようになる.




**(a)　センサ活用前の費用対効果**




**(b)　センサ活用後の費用対効果**




**(c)　センサ活用の削減効果　（＝　(a) センサ活用前　－　(b) センサ活用後）**

図 5-8　センサ活用に関わる費用対効果

図 5-8 (a)は，センサ活用が無い場合，図 5-8 (b)は，センサ活用した場合である．図 5-8 (c)は，同図(a)のセンサ活用前費用と同図(b)のセンサ活用後費用を差し引いたものである．すなわち，図 5-7 の D2 項目（19 項目，表 5-8 に示すセンサ代替可能項目（○の項目））の効果を図示している．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 1,000WP 以上のプロット部分）に良く出ていることがわかる．

ここで，ISMS の導入を想定した場合，表 5-8 に示す ISMS 管理策（センサ活用可能な 19 の管理策）に対し，代替可能なセンサ及びその削減効果（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 5-10 に示すように，約 36%の費用削減効果があることがわかった．

表 5-10　センサ活用による費用削減効果

| | センサ活用前 | センサ活用後 |
|---|---|---|
| 費用（WP 数） | 96,069 | 61,779 |

## 5.9　まとめ

第 5 章では，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，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，この削減が出来ると費用削減効果が見込めることがわかった．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代替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%低減することが出来，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．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，センサ活用の有効性を評価し，ISMS 普及促進に寄与した．

参考文献

[5-1]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），
http://www.npa.go.jp/cyber/research/h26/h26countermeasures.pdf（参照 2016-06-07）
[5-2]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），
http://lab.iisec.ac.jp/~harada_lab/survey/2011/2011_questionnaire_result.pdf（参照 2016-06-08）
[5-3]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
[5-4]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.9，1946-1955, 2014
[5-5]内田勝也他：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
[5-6]堀川博史他：デルタ ISMS モデルの提案，情報処理学会研究報告，2015
[5-7]上田哲史他：組織評価と ISMS，情報処理学会研究報告，2012
[5-8]松浦健二他：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
[5-9]高橋雄志他：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
[5-10]長谷川孝博他：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
[5-11]水沼彩子他：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
[5-12]IPA：情報セキュリティエコノミクスの挑戦，IPA（オンライン），
https://www.ipa.go.jp/files/000026120.pdf（参照 2016-06-08）
[5-13]小松文子他：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, 1711-1725, 2010
[5-14]S. Tanimoto, 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
[5-15]S. Tanimoto, 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)
[5-16]岡本薫他：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
[5-17]PMI：プロジェクトマネジメント知識体系ガイド第 4 版，2008
[5-18]JIPDEC：ISMS 認証取得について，JIPDEC（オンライン），
http://www.isms.jipdec.or.jp/ninsyou/（参照 2016-06-09）
[5-19]畑健一郎他： 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
[5-20]佐藤周行他：情報セキュリティ基盤論，共立出版（2010）
[5-21]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，第 86 号，pp.236-246（2005）
[5-22]Ken-ichiro Hata, et al.: A Proposal of Slow Policy Level based on Cost-effectiveness of ISMS's Countermeasure, Proceedings of the 9th International Conference on Project Management (ProMAC2015), pp.B19-124-B19-129(2015)
[5-23]Shoichi Yoneda, Shigeaki Tanimoto, Michio Shimomura, Hiroyuki Sato, Atsushi Kanai: Cost Reduction Effect on Running Costs in ISMS Based on Sensors, IEEE 4th Global Conference on Electronics, GCCE2015, pp.630-631, Oct. 2015

[5-24]米田翔一，畑健一郎，下村道夫，谷本茂明，佐藤周行，金井敦：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，情報処理学会論文誌，第 57 巻第 12 号 pp.2743-2756，2016 年 12 月

## 6. 結論

近年，情報化社会の急速な進展によって，ビッグデータやオープンデータなどデータサイエンスに代表されるように，情報が持つ価値は大きくなってきている．これに対し，様々な脅威も健在化しており，情報セキュリティの重要性もますます重要となっている．さらに，ショルダーハッキングなどの人為的なセキュリティの脅威や，ドローンが首相官邸の屋上に不法に着陸するなど，物理的な脅威も増えてきており，情報セキュリティだけでなく，物理面の観点からのセキュリティ対策も重要となってきている．本論文では，企業を対象に，ミッションクリティカルな情報，即ち，様々な機密情報を取り扱うオフィス空間を対象にし，情報セキュリティの観点に新たに物理セキュリティの観点を加えた，場のセキュリティを考慮したリスクマネジメントについて述べた．物理面の具体的な対象として，最近，注目されているセンサ技術を活用することとした．

具体的には，まず場のセキュリティのリスクアセスメントとして，情報セキュリティの観点に物理セキュリティの観点を加えたリスク分析を行い，27 項目のリスク要因を抽出した．次に，これらのリスク要因に対し，リスクマトリクス手法に基づき，具体的なリスク対策案を提案し，情報セキュリティに物理セキュリティを加味した総合的なセキュリティ対策について示した．さらに，より客観性を高めるため，リスク値の算出式を，リスクマトリクス手法の各要素に近似することで，抽出したリスク要因を数値化し，そのリスク値を算出し，可視化することが出来た．

最後に，センサ活用による場のセキュリティのリスクマネジメントの例として，TPO 条件に基づく最適クラウド選択と ISMS の ROSI 効率化を示した．

TPO 条件に基づく最適クラウド選択では，TPO 条件に応じて，複数のクラウドから適切なセキュリティレベルのものを選択する手法について述べ，情報の価値に合わせた複数のセキュリティレベルのクラウドを利用することにより，コストの合理化とセキュリティレベル維持の両立に資することが出来た．

また，ISMS の ROSI 効率化では，監視カメラなどのセンサを活用することによって，企業など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 ISMS のコストを，机上シミュレーションではあるが，全体の約 36%低減可能であることを示し，連携の有効性を示した．

これらの成果により，様々な機密情報を取り扱うオフィス空間の，さらなる安心安全な IT 基盤の形成に寄与し，TPO 条件に応じた柔軟性の高いセキュリティシステムの実装による，利便性と機密性の両立が可能な情報社会の構築の一助となることが期待される．

今後の課題としては，IoT などの技術の進展に合わせ，継続的にリスクアセスメントの見直しを行っていくことが挙げられる．また，評価等の観点，例えば，費用対効果の観点からは，さらなる精度(粒度)向上や，人の行動にフォーカスした心理面や倫理面などを考慮した検討が重要になってくると思われる．さらに，より実用的は観点からは，企業における情報システム環境の信頼性，安全性，有効性について総合的に監査する「システム監査」などを加味した検討も重要であると考えられる．

謝辞

本論文は，筆者が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博士後期課程在学中に，谷本研究室において行った研究をまとめたものです.

本論文を執筆するにあたって，最後まで多くのご指導ご鞭撻頂いた本学，谷本茂明教授に深く御礼申し上げます.

また，副査として多くの貴重なご意見を下さった本学の堀内俊幸教授，下村道夫教授，遠山正朗教授，岩下基教授，東京都市大学の関良明教授にも厚く御礼申し上げます.

最後に，本論文の各構成論文の共著者として多くのご支援をしていただきました，本学の鴻巣努教授，東京大学の佐藤周行准教授，法政大学の金井敦教授，まいばすけっと株式会社の畑健一郎氏，株式会社ジャステックの大角地涼介氏に深く感謝の意を示し，謝辞にかえさせていただきます.

付録　ISMS (情報セキュリティマネジメントシステム)

ここでは，第 5 章に記した ISMS に関わる費用対効果，特に費用面を導出するに際し，現状の ISMS の規定項目([1]-[2])を基に簡潔にとりまとめた結果について示す.

参考文献

[1] 日本規格協会：JIS Q 27001:2014，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，2014
[2] 日本規格協会：JIS Q 27002:2014，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，2014

ISMS とは，個別の問題ごとの技術対策の他に，組織のマネジメントとして自らのリスクアセスメントにより必要なセキュリティレベルを決め，プランを持ち，資源配分して，システムを運用することによって，体系的かつ系統立てて情報セキュリティに取り組むことである．即ち，組織が保護すべき情報資産について，機密性，完全性，可用性をバランスよく維持し改善することが ISMS の基本コンセプトであり，ISMS を確立，導入，運用，監視，レビュー，維持及び改善するためのモデルを提供するために国際規格 ISO/IEC 27001 が規定されており，2013 年に最新版へ改訂されている．

1.　ISMS（ISO/IEC 27001(JIS Q 27001)）の構成と概要

ISO/IEC 27001 の構成は，「0.序文」，「1.適用範囲」．「2.引用規格」．「3.用語及び定義」．「4.組織の状況」「5.リーダーシップ」，「6.計画」，「7.支援」，「8.運用」，「9.パフォーマンス評価」，「10.改善」及び「附属書 A(規定)　管理目的及び管理策」から構成されている．

ISO/IEC 27001 の概要は以下の通りである．

① 序文

ISO/IEC 27001 は，組織の戦略的決定として，ISMS を確立し，実施し，維持し，継続的に改善するための要求事項を提供するために作成された．ISMS は，リスクマネジメントプロセスを適用することによって，情報の機密性，完全性及び可用性を維持し，かつリスクを適切に管理しているという信頼を利害関係者に与える．

また，この規格は，組織自身の情報セキュリティ要求事項を満たす組織の能力を，組織の内部で評価するためや，外部関係者が評価するために用いることが出来る．

② 適用範囲

ISO/IEC 27001 は，業種，規模，事業の性質を問わずすべての組織に適用可能であり，汎用性がある．この規格への適合を宣言する場合には，箇条 4～10，即ち，「4.組織の状況」「5.リーダーシップ」，「6.計画」，「7.支援」，「8.運用」，「9.パフォーマンス評価」，「10.改善」に規定されているいかなる要求事項も除外できないことが明記されている．

③ 引用規格

ISO/IEC 27001 の規定の一部として，ISO/IEC 27000(JIS Q 27000)が挙げられている．

④ 用語及び定義

この規格で用いる主な用語及び定義について, ISO/IEC 27000(JIS Q 27000)を引用している．

⑤ 組織の状況

組織は, ISMS の適用範囲の決定や, 継続的な改善を行う必要がある. そのためには, ISMS の，意図した成果の達成に影響する内部及び外部の課題の決定，及び利害関係者の決定をするなど，組織の状況の理解が必要となる.

⑥ リーダーシップ

ISMS に関して，その方針の指針及び様々な権限を持つ者が実施すべき内容について記されている．情報セキュリティ方針は，文書化され，組織内に伝達されなければならず，必要に応じて利害関係者もそれを入手可能とする必要がある.

⑦ 計画

ISMS における，リスク及び機会を明らかにし，それらへの対処活動の計画について記されている.

⑧ 支援

ISMS の運用に必要な資源や力量を決定し，それを提供する必要があることについて記されている.

⑨ 運用

ISMS を運用する際の計画やリスクアセスメントなどについて記されている.

⑩ パフォーマンス評価

ISMS を評価するための，監視，測定や内部監査，マネジメントレビューについて記されている.

⑪ 改善

ISMS への不適合に対する処置や，継続的改善に関して記されている.

⑫ 附属書 A(規定)管理目的及び管理策

ISMS の確立の際，組織が選択するべき管理目的及び管理策について記されている．この管理目的及び管理策は ISO/IEC 27002(JIS Q 27002)の箇条 5～18 と整合が取られている.

## 2. プロセスアプローチと PDCA モデル

本項目では ISMS の実装にあたって重要とされている考え方,「プロセスアプローチ」と「PDCA モデル」ついて解説する.

### 2.1 プロセスアプローチ

ISO/IEC 27001 では，組織の情報セキュリティマネジメントを実施するため，多くの活動を明確にしたプロセスアプローチを採用することを推奨している．すなわち，組織の ISMS の確立，導入，運用，監視，レビュー，維持及び改善のためにプロセスアプローチを採用している．このプロセスアプローチという考え方は，品質マネジメントシステム(QMS)の規格である ISO 9001(JIS Q 9001)などで紹介され，日本においても多くの組織で活用されている．プロセスアプローチでは，インプットをアウトプットに変換するために，経営資源を使用して運営管理されるあらゆる活動をプロセスとみなし，組織内に存在するプロセスをシステムとして運用し，運営管理する考え方のことを言う．そのためには，それぞれのプロセスにおいて「インプット」されるものが何で，処理結果として「アウトプット」されるものが何かを多角的に検討し，明確にする必要がある．ここで検討され明確にされた情報セキュリティに関する項目からプロセスに関与する資産のリスクを識別し，適切に情報セキュリティ対策を実施し運用していくことにつながる.

すなわち，ISMS の構築を一連のプロセスとして捉え，各々のプロセスをプロセスアプローチに従って明確化し，その相互関係にあるインプットとアウトプットを把握することで，ISMS の構築に要求される重要な事項を認識することができる．例えば，リスクアセスメントにより明らかになった適用範囲内のリスクに対して情報セキュリティを向上させるためには，適用範囲内のプロセスを取り巻く環境を分析し，影響を及ぼすリスク状態を適切に捉えることが重要である．このリスク及びリスクの変化を的確に認識するためには，管理対象を明確に規定したマネジメントが必要になる．マネジメントを実施することによって組織のプロセス改革の方向性や方針が明確となり，これにより組織全体に情報セキュリティに対する期待やその測定などが徹底される．さらに，測定した結果をフィードバックすることによりマネジメントの改善が行われ，本質的なプロセス改革へとつなげることができる.

ISO/IEC 27001 では，ISMS における管理手法としてプロセスアプローチを採用することを奨励し，それを実現するための考え方として「PDCA モデル」を提示している.

### 2.2 PDCA モデル

ISO/IEC 27001 では，PDCA モデルを採用している．PDCA モデルでは，利害関係者の情報セキュリティの要求事項及び期待をインプットに，これらの要求事項及び期待を満たす情報セキュリティの結果(運営管理された情報セキュリティ)をアウトプットとして導くために必要な活動及びプロセスを ISMS プロセスに適用している.

この ISMS プロセスは，PDCA モデルを採用することで整理され，組織の情報セキュリティ管理体制に継続的な学習と改善の機会を提供する．すなわち，ISO/IEC 27001 では Plan-Do-Check-Act(PDCA: 計画-実行-点検-処置)モデルを採用し，これを ISMS プロセスすべてに適用する．図 1 は，ISMS が利害関係者からの情報セキュリティ要求事項及び期待をインプットとしてどう取り入れ，必要となる活動及びプロセスを経て，その要求事項及び期待を満たした情報セキュリティの成果をどう生み出すかを表している. また, ISO/IEC 27001 では，このモデルに従い，PDCA の各々の項目に対する要求事項を具体的に規定している.

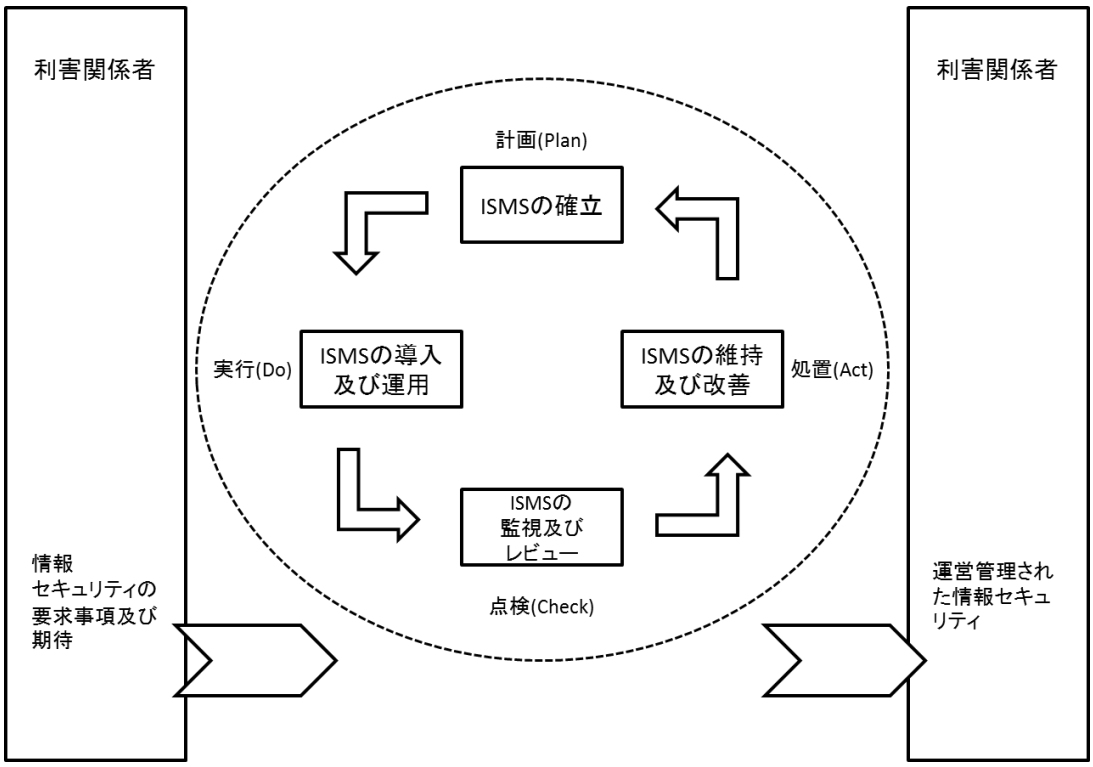



図 1　ISMS プロセスに適用される PDCA モデル

3.　ISMS の確立と運用管理

2.では実装における考え方として「プロセスアプローチ」と「PDCA モデル」の解説をした. 本項目ではそれらの考え方を踏まえた ISMS の確立, 導入及び運用, 監査及びレビュー, 維持及び改善の一連のプロセスをそれぞれのフェーズとステップで解説する.

3.1　ISMS の確立

ISMS を確立するためのステップは，図 2 に示す通りである．

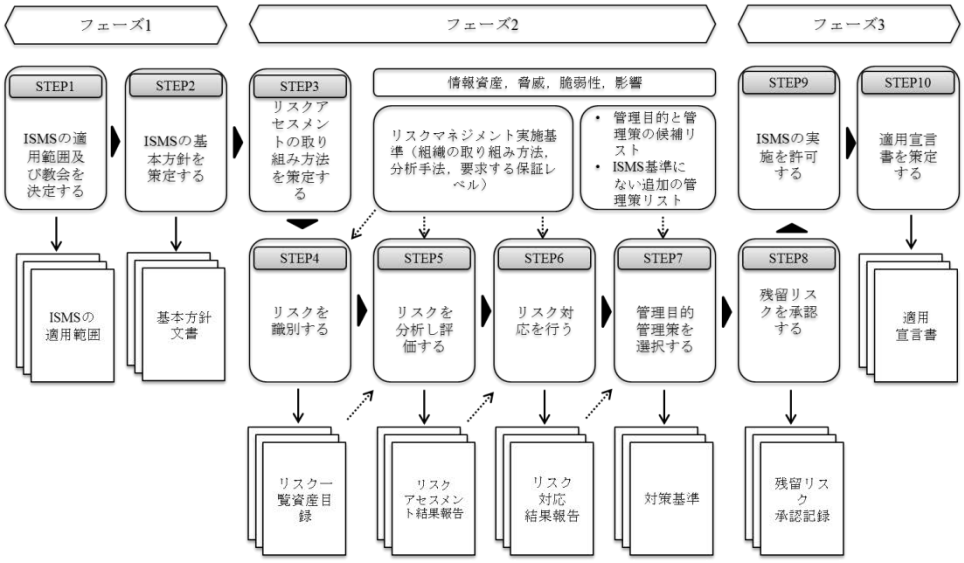



図 2　ISMS の確立のステップ

①　ISMS の適用範囲及び基本方針の確立(STEP1～STEP2)

ISMS の適用範囲は，事業，組織，その所在地，資産及び技術の各特徴の観点から定義する．ISMS の適用範囲及び境界を定義する際には，適用範囲外としたものの詳細とその理由を含める必要がある．ISMS 基本方針は，事業及び法令または規制の要求事項を考慮する．リスクマネジメントの状況と，ISMS を確立し維持する組織環境により，情報セキュリティの全般的な方向性及び行動指針を確立する．なお，ISMS 基本方針は，情報セキュリティ基本方針のさらに上位の方針を示すもので，組織全体のマネジメントシステムの観点から ISMS をどのように位置づけるかを示したものである．

②　リスクアセスメントに基づく管理策の選択(STEP3～STEP7)

上記①で決定した ISMS の適用範囲及び基本方針に基づき，リスクアセスメントの取り組み方法を策定する．選択するリスクアセスメントは，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する．

リスクの特定では，保護すべき情報資産に対して機密性，完全性，可用性を喪失させる脅威，脆弱性及びそれらが事業に及ぼす潜在的な影響の大きさを特定する．すなわち，「リスク」とは現実に脅威を受けた時に想定される「資産が被る影響(資産価値)」と，その資産に対する「脅威の程度」及びその脅威が侵入してくる可能性のある資産の「脆弱性の程度」の組み合わせである．これらの情報資産に対する脅威，脆弱性，発生頻度をベースにリスクアセスメントを実施する．

リスクアセスメントでは，セキュリティ障害による事業上の損害及び発生可能性を評価した結果でリスク水準を算定し，リスク受容するための基準と比較してリスク受容できるか，リスク対応が必要かどうかを決定する．リスク受容ができない場合，リスク対応としてリスク低減(管理策の採用)，リスク保有，リスク回避，及びリスク移転の選択をする．リスクアセスメント(リスクを分析し評価する)の方法として,「ベースラインアプローチ」,「詳細リスク分析」及び「組み合わせアプローチ」などがある．リスクアセスメントの具体的方法については次のとおりである．

I.　ベースラインアプローチ

ベースラインアプローチとは，情報資産ごとにリスクそのものを評価するものではなく，一般の情報セキュリティに関する基準や，業種・業界で採用されている標準やガイドラインなどを参照し，組織全体で共通のセキュリティ対策を実施する．実現可能な水準の管理策を採用し，組織全体でセキュリティ対策に抜け漏れがないように補強していくアプローチである．ベースラインアプローチは，大きく分けると以下の 2 つの手順で実施される．

● ベースラインの決定

ベースラインアプローチでは，組織の達成する情報セキュリティの管理水準について独自の「対策の標準」を作成する．一般に，この対策の標準のことを「ベースライン」と呼ぶ．実際にどのようなコントロールを導入するのか，「できる，できない」の判断をする前に広く管理策についての情報を収集し，組織が要求する情報セキュリティの管理水準が，達成可能なベースラインであるかを検討する必要がある．例えば，他の組織または企業と比較して情報セキュリティの管理水準が必要なレベルであるかを調べるのも効果的である．

● ギャップ分析の実施

ギャップ分析実施の目的は，組織の定める基準への準拠状況の把握にある．

基準で要求される管理のレベルと組織の管理レベルの現状を比較し，「大きな差が認められる個所」，「明らかに管理策の適用を必要としている個所」，「過度に管理策が適用されている個所」などを確認する．

II.　詳細リスク分析

詳細リスク分析では資産ごとの関連するリスクの識別を個別に実施する．リスクが顕在化する頻度は，脅威が発生する(顕在化する)可能性，管理上の弱点に付け込まれる可能性(脆弱性)の他に，資産が攻撃者から見てどれほど魅力的なものかなどにも依存する．

詳細リスク分析では，まずリスク分析の対象範囲の定義づけをしなければならない．これはプロセスが密接に絡み合っているにもかかわらず，安易に範囲を狭め，慎重な定義づけを怠ると，後に不必要な作業の増加や抜けにつながるためである．

III.　組み合わせアプローチ

一般的には，ベースラインアプローチと詳細リスク分析を併用する組み合わせアプローチを採用することが効率的であるとされている．

どのような場合にどのアプローチを採用するかは一概には決定できず，適切なアプローチの採用のための判断材料は，資産に求められるセキュリティ要求事項(事業上の要求事項，法的または規制の要求事項，契約上のセキュリティ義務など)に依存する．組み合わせアプローチには，「ベースラインアプローチ」のみでは，高い水準で管理策が実装されるべきリスクの高いシステムについて対応策が不十分になる可能性があること，また，「詳細リスク分析」をすべてのシステムに適応することは効率的な観点から現実的でないことなどを理由に，それぞれの資産を取り巻くリスク環境を確認し，適切なリスク分析のアプローチを採用し，それぞれのアプローチの弱点を相互に補完しあうことにより，ISMS の適用範囲全体のリスク分析を効率的に実施する目的がある．

リスク対応には，附属書 A「管理目的及び管理策」のリストから適切な管理目的と管理策を選択する．管理策の選択には，リスクの需要基準，法令の要求事項，契約上の義務，及び事業上の要求事項を考慮する．また，附属書 A 「管理目的及び管理策」のリスト選択だけでなく組織の必要に応じて追加の管理目的と管理策を採用することできる．

③　適用宣言書の作成(STEP8～STEP10)

リスク対応後の残留リスクを経営陣が承認し，ISMS の導入及び運用について許可を与える．リスクアセスメントの結果から選択した管理目的及び管理策，並びにこれらを選択した理由と除外の理由を記載した「適用宣言書」を作成する．なお，「適用宣言書」には現在実施されている管理目的及び管理策も含める必要がある．

## 3.2　ISMS の導入及び運用

ISMS を導入及び運用するためのステップは，図 3 に示す通りである．

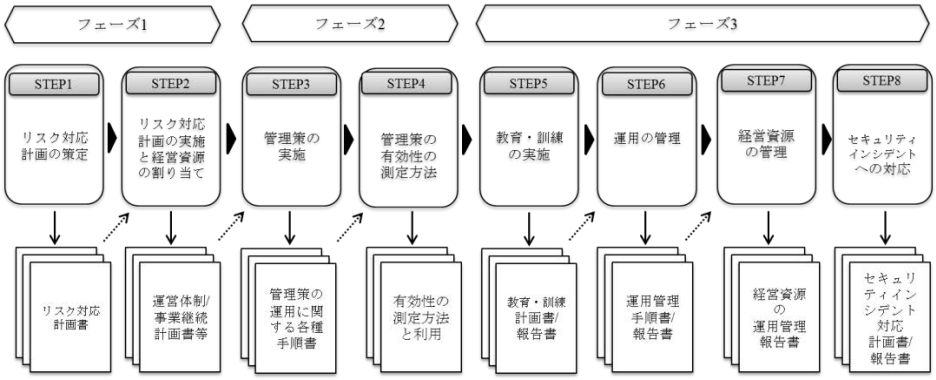



図 3　ISMS の導入及び運用のステップ

①　リスク対応計画の実施(STEP1～STEP2)

リスク対応計画では，受容できないリスクを低減するためにとるべき活動と，選択した管理策の実装に関する計画を明らかにする．このリスク対応計画により，組織が識別したリスクに対する管理策の実施状況と，残留リスクが受容可能なレベル以下に低減されていないリスクへの追加的対策の進捗状況を容易に把握することができる．経営陣は，ISMS の必要性を理解し，リスク対応を確実に実施するために必要な経営資源を割り当てる必要がある．

②　管理策の実施と有効性の測定(STEP3～STEP4)

管理策の運用に関する手順やセキュリティインシデントの発生した際の手順などを文書化し，管理策を実施する．計画された管理目的が選択された管理策によってどの程度達成されているかを判断するために，選択した管理策または一群の管理策の有効性を測定する方法について定義する．また，比較可能で再現可能な結果を出すための管理策の有効性を評価するために，この測定方法をどのように利用すべきかを規定する．管理策が有効であるかどうかは，管理策の導入が，対象とするリスク及びセキュリティ要求事項への適切な対策として機能しているか否かである．

③　運用管理とセキュリティインシデントへの対応(STEP5～STEP8)

役割を割り当てられた要員全てが情報セキュリティに関連する責任を果たし，期待される役割を実行するために必要な力量を持つことを確実にするため，教育・訓練を実施する．

導入した管理策が適切に運用管理されるための手順書を策定するとともに，各手順書の運用管理者，利用者などの関係者の責任を明記する．

セキュリティインシデントに対する被害を最小限に抑えるためには，セキュリティインシデントを適切に検出し，迅速な処置をとることが重要となる．迅速な対応のために手順書を策定し，その内容を定期的に検証していく．

3.3　ISMS の監視及びレビュー

ISMS を監視及びレビューするためのステップは，図 4 に示す通りである．

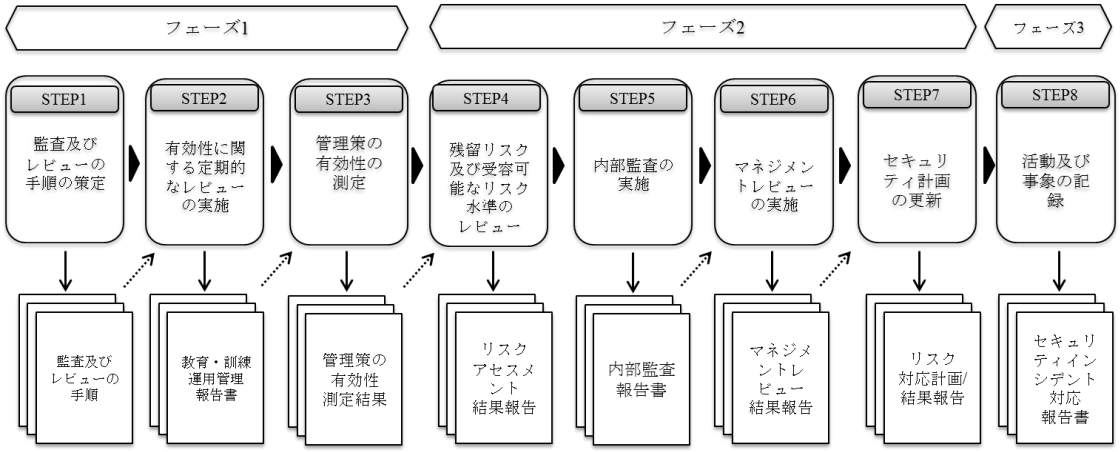



図 4　ISMS の監視及びレビューのステップ

①　管理策の有効性の測定(STEP1～STEP3)

組織は，セキュリティ上の違反行為，セキュリティインシデントの防止，及びセキュリティ違反に対する処置の有効性を判断するため，監視及びレビューの手順を文書化するとともに,監視のための管理策を実施する.ISMS の有効性に関して定期的なレビューをする．有効性の評価は，目標に対する達成度を確認する．セキュリティ要求事項が満たされていることを検証するために，導入した管理策がどの程度有効に機能しているかを測定する必要がある．測定結果は，ISMS の有効性のために活用する．

②　セキュリティ計画の更新(STEP4~STEP7)

ある時点で管理策を実施したとしても，技術の進展や環境の変化に合わせて改善を行う必要がある．そのための活動が内部監査であり，経営陣によるマネジメントレビューである．

組織は，実施された管理策の有効性やリスクアセスメントに生じる変化(組織変更，技術革新，事業の目的及びプロセスの改善，脅威の認識，外部事象)考慮し，残留リスク及び認識された受容可能なリスクレベルをレビューする．ISMS のプロセス及び手順が定められたとおりに実行されているか否かについての内部監査を実施する．

経営陣は，組織の ISMS のプロセスが適切で妥当かつ有効であることを確実にするため，定期的にマネジメントレビューを実施し，ISMS の維持及び継続的な改善を行う．組織が策定したあらゆる情報セキュリティに関するセキュリティ計画(リスク対応計画も含む)を更新する．

③　活動及び事象の記録(STEP8)

ISMS の有効性またはプロセスの実施状況に重大な影響を与える可能性のある活動及び事象を記録する．記録は，要求事項への適合性及び ISMS の有効な運用の証拠を提供するために，作成し維持する．

### 3.4　ISMS の維持及び改善

ISMS を維持及び改善するためのステップは，STEP1 改善策の実施(是正処置・予防措置)と STEP2 講じた処置の伝達となる．

① 改善策の実施(STEP1)

組織は ISMS に改善策を導入しなければならない．この改善策は，ISMS の監視及びレビューを通じて得られたものだけでなく，外部からの改善要求事項なども考慮する．組織は，ISMS 構築にあたり，変化したリスクを特定し，大きく変化したリスクに注意を向けて要求事項を特定する機能がマネジメントプロセスに組み込まれておりマネジメントレビューを通じてリスクアセスメントの結果に基づいた優先順位で予防措置が取られるよう留意することが必要である．

② 講じた処置の伝達(STEP2)

利害関係者すべてに対し，状況に応じた適切な詳しさで処置及び改善策を伝達し，処置及び改善策の進め方について合意を得る．利害関係者は，組織の内部だけでなく外部の利害関係者も含めて配慮する．

## 4.　ISMS の文書化と記録の管理

ISO/IEC 27001 では，その組織の ISMS に関わる方針や記録を文書として作成，保管することが求められている．本項目では ISMS の文書化と記録の管理について解説する．

### 4.1　ISMS の文書化

ISMS の活動では，経営陣が決定した ISMS 基本方針及び目的に基づいて，リスクアセスメント及びリスク対応のプロセスを実施し，その結果によって管理策を選択する．ISO/IEC 27001 では，管理策をリスクアセスメント及びリスク対応のプロセスの結果に基づき選択し，さらに，それらのプロセスが ISMS 基本方針及び目的に基づいて実施されていることを関連付けられるような文書の作成を求めている．

また，リスクアセスメントや有効性の測定方法は，それを実施する人によって異なる方法となってしまっては結果を比較できず，情報セキュリティを効果的に管理することが出来ない．したがって，記録された結果が再現可能なことを確実にするために，文書化は重要になる．また，定めた管理策について管理者及び要因がその通りに実施するように，手順を確立し明文化する必要がある．

ISMS 文書化の程度は，組織の規模及び活動の種類，適用範囲，並びにセキュリティの要求事項及び運営管理するシステムの複雑さによって異なることに留意する必要がある．

### 4.2　文書管理

ISMS 文書は，版管理され適切な文書を必要とする人が必要なときに使用可能な状態で管理されている必要がある．ISMS 文書の管理について，文章体系を考慮した管理手順を確立し，文書管理する必要がある

4.3　記録の管理

記録は, 組織の ISMS が要求事項へ適合していること及び運用の効果を示す証拠として作成，維持，管理する必要がある．PDCA プロセス全般における活動の記録，管理策の実施状況の記録, 及び ISMS に関連する全てのセキュリティインシデントの発生に関する記録を維持することが要求される．

また, ISO/IEC 27001 の附属書 A「A.18 順守」の中の A.18.1.3(記録の保護)では,「記録は，法令，規制，契約及び事業上の要求事項に従って，消失，破壊，改ざん，認可されていないアクセス及び不正な流出から保護しなければならない」となっている．法的要求事項に関係する文書は，記録として管理する必要がある．

記録の管理として，次の事項の実施などが効果的である．

- 識別，保管，保護，検索，保管期間及び廃棄に関して必要な管理を文書化すること
- 運営管理プロセスで記録の必要性及び記録の範囲を定めること
- 会社法など保管期間が定められている場合には，法的要求事項に適合した保存期間を決定すること

5.　経営陣の責任とマネジメントレビュー

ISMS には全社的な活動が必要である．そのため経営者は ISMS をよく理解しておく必要がある．本項目では経営者の責任とマネジメントレビューを解説する．

5.1　経営陣の責任

①　経営陣のコミットメント

ISMS の活動のあらゆる段階において，様々な活動が実施されることを確実にするためには，経営陣のコミットメント(約束・関与)が必要である．

コミットメントは，経営陣の果たすべき重要な役割であり，ISMS に関連する活動(確立，導入，運用，監視，レビュー，維持及び改善)すべてを含む内容である．

コミットメントの証拠を示すことが要求されており，ISMS 企保運方針等の確立，役割及び責任経営資源の提供, リスクの受容基準及び受容可能なレベルの決定, ISMS の内部監査，マネジメントレビューの実施などがある．

②　経営資源の運用管理

組織は，ISMS の必要性を理解し，そのために必要な経営資源を決定し，提供することが要求されている．また，組織における ISMS に定義された責任を割り当てた要員すべてが，要求された職務を実施する力量を持つことを確実にするために，教育・訓練を実施させるか，適格な要員を雇用する責任がある．実施した教育・訓練については，その有効性を評価し，力量を持った要員の確保に役立てることが重要である．必要とされる力量は，それぞれの業務により異なっている．

さらに組織は，全ての要因が自らの情報セキュリティについての活動が持つ意味と重要性とを認識し，ISMS の目的の達成に向けてどのように貢献できるかを認識することを確実にする必要がある．

5.2　ISMS 内部監査

組織は ISMS の管理目的，管理策，プロセス及び手順が次の事項を満たしているか否かを判断するため，ISMS 内部監査を定期的に実施することが要求されている．

- この規格及び関連する法令(個人情報法，著作権法，不正競争防止法など)または規制の要求事故への適合
- 特定された情報セキュリティ要求事項への適合
- 有効な実施，維持
- 期待された実施

ISMS 内部監査は計画的に実施される必要がある．監査員は，監査の対象となる管理目的，管理策，プロセス及び手順の状況と重要性，並びにこれまでの監査結果を考慮して監査プログラムを策定する．監査の実施にあたり，監査のための評価基準，対象範囲，頻度及び方法を定義する．監査員の選定においては，監査に関連する一連のプロセスを実施する力量のほかに監査プロセスの客観性及び公平性を確実にする必要がある．なお，客観性を確保するためにも，自らの業務を監査することはできない．

組織は，監査員に関連する責任並びに監査に関連する一連のプロセスを文書化された手順の中で規定する必要がある．監査を受けたプロセスなどに責任を持つ管理者は，発見された不適合及びその原因を除去するための処置を遅滞なく確実に講じるとともに，実施した改善活動は，講じた処置の検証及び検証結果の報告を含める必要がある．

5.3　ISMS のマネジメントレビュー

マネジメントレビューは，経営陣が ISMS の効果を把握し，改善するための意思決定をする一連のプロセスである．マネジメントシステムの有効性を確保するために，経営陣の責任を明確化し，あらかじめ定められた間隔(少なくとも年 1 回)で実施することが要求されている．

経営陣は，組織の ISMS が引き続き適切で妥当かつ有効であることを確実にするために，情報セキュリティ基本方針及び目的を含む ISMS の変更の必要性を評価する．また，マネジメントレビューの結果は，記録として維持される必要がある．マネジメントレビューへのインプット情報としては，次のようなものが挙げられる．

- 内部監査や外部監査の結果
- 顧客，取引先，従業員といった利害関係者からのフィードバック
- 新たに利用可能となった技術，新製品・新サービスに関する情報
- 実施した予防処置及び是正処置の実施状況及びその結果
- 過去において，取扱われなかった脆弱性または脅威などに対するリスクアセスメントの必要性の判断
- 管理策または一群の管理策に対して，有効性を測定したことによって把握できた内容(有効性測定の結果)
- 過去のマネジメントレビューの結果に適切に対応したかどうかのフォローアップの状況などの報告
- 経営環境の変化，組織の変化などを含む ISMS に影響を及ぼす可能性のあるすべての組織内外の変化

経営陣は，インプットされた情報に基づいて経営の意思決定を行う必要がある．マネジメントレビューからのアウトプット(改善すべき事項の決定及び処置)として，ISMS の有効性の改善，リスクアセスメント及びリスク対応計画の更新，契約上の義務，管理策の有効性を測定する方法の改善などがある．特に，ISMS に影響を与える可能性のある内外の事象に対応するために，情報セキュリティを実現する手順及び管理策を修正する必要がある．

5.4　ISMS の改善

①　継続的改善

情報セキュリティの継続的な改善に経営陣が責任を持つことにより，情報セキュリティ対策が確実に実施され，組織のセキュリティ水準も継続して向上することが期待できる．情報セキュリティ基本方針及び目的，監査結果，監視した事象の分析，是正処置，予防処置並びにマネジメントレビューのアウトプットを通じて，ISMS の有効性を継続的に改善することが重要である. また, ISMS の要求事項への不適合が発生することを防止するために，その原因を除去すること，及び不適合発生の予防処置の必要性を評価することが要求されている．

②　是正処置

監査やマネジメントレビューの結果などにより，ISMS の導入及び運用に関連する不適合が発見された場合，不適合の原因を除去するための処置及び再発防止のための処置を講じる必要がある．この是正処置のためには，不適合の特定，不適合の原因の決定，不適合の再発防止を確実にするための処置の必要性の評価，必要な是正処置の決定及び実施，取った処置の結果の記録，取った是正処置のレビューを含んで文書化された手順を必要とする．

③　予防処置

起こりうる不適合を早期に発見し，処置を講じる必要がある．組織は，リスクの変化に着目して予防処置についての仕組みがマネジメントプロセスに組み込まれており，マネジメントレビューを通じてリスクアセスメントの結果に基づいた優先順位で予防処置がとられるように留意する．この予防処置のためには，起こり得る不適合及びその原因の特定，不適合の発生を予防するための処置の必要性の評価，必要な予防処置の決定及び実施，取った処置の結果の記録，取った予防処置のレビューを含んで文書化された手順を必要とする．

6.　附属書 A(規定)管理目的及び管理策の概要

ISO/IEC 27001 における「管理目的及び管理策」は，附属書 A(規定)として明記されている．この規定は，ISMS の確立プロセスにおけるリスク対応として適切な管理目的及び管理策を選択するためのものである．また，全てを網羅してはいないため，組織は必要に応じて追加の管理目的及び管理策を選択することもできる．

附属書 A(規定)に記載する管理目的及び管理策のリストは，ISO/IEC 27002(JIS Q 27002：2014)の箇条 5 から箇条 18 の管理目的及び管理策を抜き出したものである．すなわち，「管理策及び管理目的」は，ISO/IEC 27002(情報セキュリティ管理策の実践のための規範)との整合性が図られており，完全に一致する規定となっている．附属書 A(規定)における 14 の管理領域と 35 の管理目的及び 114 の管理策は，表 1 に示す通りである．

表 1　管理領域別の管理目的及び管理策

| 対策 | 附属書A(規定)の管理領域 | 管理目的数 | 管理策数 |
|---|---|---|---|
| 組織的人的管理 | A.5 情報セキュリティのための方針群 | 1 | 2 |
| | A.6 情報セキュリティのための組織 | 2 | 7 |
| | A.7 人的資源のセキュリティ | 3 | 6 |
| | A.8 資産の管理 | 3 | 10 |
| 物理的技術的管理 | A.9 アクセス制御 | 4 | 14 |
| | A.10 暗号 | 1 | 2 |
| | A.11 物理的及び環境的セキュリティ | 2 | 15 |
| | A.12 運用のセキュリティ | 7 | 14 |
| | A.13 通信のセキュリティ | 2 | 7 |
| | A.14 システムの取得，開発及び保守 | 3 | 13 |
| 組織的管理 | A.15 供給者関係 | 2 | 5 |
| | A.16 情報セキュリティインシデント管理 | 1 | 7 |
| | A.17 事業継続マネジメントにおける情報セキュリティの側面 | 2 | 4 |
| | A.18 順守 | 2 | 8 |
| 合計 | | 35 | 114 |

表 1 の附属書 A(規定)の 14 の管理領域に規定されている管理目的及び管理策の概要は，次の通りである．

7.　情報セキュリティのための方針群

情報セキュリティのための方針群は，事業上の要求事項や目的，関連する法令及び規制に対する取組みなどを示したものであり，情報セキュリティに対する経営陣の方針及び支持を提示するものである．また，あらかじめ定められた間隔あるいは重大な変化が生じたときには，情報セキュリティのための方針群が妥当でかつ有効であることを確実にするためのレビューをする必要がある．

表 2　A.5.1 情報セキュリティのための経営陣の方向性

| 管理目的名 | 管理目的 | 管理策番号 | 管理策名 | 管理策概要 |
|---|---|---|---|---|
| A.5.1 情報セキュリティのための経営陣の方向性 | 情報セキュリティのための経営陣の方向性及び支持を，事業上の要求事項並びに関連する法令及び規制に従って提示するため． | A.5.1.1 | 情報セキュリティのための方針群 | 情報セキュリティのための方針群は，これを定義し，管理層が承認し，発行し，従業員及び関連する外部関係者に通知しなければならない． |
| | | A.5.1.2 | 情報セキュリティのための方針群のレビュー | 情報セキュリティのための方針群は，あらかじめ定めた間隔で，又は重大な変化が発生した場合に，それが引き続き適切，妥当かつ有効であることを確実にするためにレビューしなければならない． |

8. 情報セキュリティのための組織

情報セキュリティのための組織は，内部組織とモバイル機器及びテレワーキングの 2 つの管理目的に分類される．

8.1 内部組織

組織内において情報セキュリティを確立するために，経営陣は，組織の資産を不注意または故意によって不正使用されないように，役割及び責任を適切に割り当てる必要がある．また，情報セキュリティインシデントに適切に対処するために，関係当局(監督官庁など)や専門家による団体などとの連絡体制を維持する必要がある．

表 3 A.6.1 内部組織

| 管理目的名 | 管理目的 | 管理策番号 | 管理策名 | 管理策概要 |
|---|---|---|---|---|
| A.6.1 内部組織 | 組織内で情報セキュリティの実施及び運用に着手し，これを統制するための管理上の枠組みを確立するため． | A.6.1.1 | 情報セキュリティの役割及び責任 | 全ての情報セキュリティの責任を定め，割り当てなければならない． |
| | | A.6.1.2 | 職務の分離 | 相反する職務及び責任範囲は，組織の資産に対する，認可されていない若しくは意図しない変更又は不正使用の危険性を低減するために，分離しなければならない． |
| | | A.6.1.3 | 関係当局との連絡 | 関係当局との適切な連絡体制を維持しなければならない． |
| | | A.6.1.4 | 専門組織との連絡 | 情報セキュリティに関する研究会又は会議，及び情報セキュリティの専門家による協会・団体との適切な連絡体制を維持しなければならない． |
| | | A.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 | プロジェクトの種類にかかわらず，プロジェクトマネジメントにおいては，情報セキュリティに取り組まなければならない． |

8.2　モバイル機器及びテレワーキング

モバイル機器及びテレワーキングを用いることによるリスクを管理するために，その条件及び制限を定めた，方針及びその方針を支援するセキュリティ対策を実施する必要がある．テレワーキングとは，オフィス以外で行うあらゆる作業形態を指し，コンピュータ端末を用いた在宅勤務や遠隔作業及び仮想的な作業などの従来とは異なる作業環境も含まれている．

表 4　A.6.2 モバイル機器及びテレワーキング

| 管理目的名 | 管理目的 | 管理策番号 | 管理策名 | 管理策概要 |
|---|---|---|---|---|
| A.6.2 モバイル機器及びテレワーキング | モバイル機器の利用及びテレワーキングに関するセキュリティを確実にするため. | A.6.2.1 | モバイル機器の方針 | モバイル機器を用いることによって生じるリスクを管理するために，方針及びその方針を支援するセキュリティ対策を採用しなければならない. |
| | | A.6.2.2 | テレワーキング | テレワーキングの場所でアクセス，処理及び保存される情報を保護するために，方針及びその方針を支援するセキュリティ対策を実施しなければならない. |

9. 人的資源のセキュリティ

人的資源に関するセキュリティとして，雇用前(組織が関係を開始する前)，雇用期間中(組織との関係が継続している期間)，雇用の終了または変更(組織との関係が終了または変更すること)の 3 つの管理目的に分類される．

9.1 雇用前

雇用をする場合，従業員及び契約相手がその責任を理解し，求められている役割にふさわしいことを確実にする必要がある．全ての従業員候補者の経歴の確認については，関連する法令，規制及び倫理に従って行う必要がある．また，その雇用条件は，情報セキュリティのための方針群を反映し，その責任及び義務を明確にする必要がある．特に，情報セキュリティに関する特定の役割のために雇用する場合は，候補者が充分な力量を持つこと及び組織から見て信頼できることが重要となる．

表 5 A.7.1 雇用前

| 管理目的名 | 管理目的 | 管理策番号 | 管理策名 | 管理策概要 |
|---|---|---|---|---|
| A.7.1 雇用前 | 従業員及び契約相手がその責任を理解し，求められている役割にふさわしいことを確実にするため． | A.7.1.1 | 選考 | 全ての従業員候補者についての経歴などの確認は，関連する法令，規制及び倫理に従って行わなければならない．また，この確認は，事業上の要求事項，アクセスされる情報の分類及び認識されたリスクに応じて行わなければならない． |
| | | A.7.1.2 | 雇用条件 | 従業員及び契約相手との雇用契約書には，情報セキュリティに関する各自の責任及び組織の責任を記載しなければならない． |

9.2　雇用期間中

雇用期間中では，組織内の構成員全体にセキュリティの適用を確実にする必要がある．そのために，定期的な意識向上プログラムの実施や，正確かつ公平な取扱いができる，周知された懲戒手続きを用意する必要がある．また，これらを確実に実施するための，経営陣の責任を明確にする必要がある．

表 6　A.7.2 雇用期間中

| 管理目的名 | 管理目的 | 管理策番号 | 管理策名 | 管理策概要 |
|---|---|---|---|---|
| A.7.2　雇用期間中 | 従業員及び契約相手が，情報セキュリティの責任を認識し，かつ，その責任を遂行することを確実にするため． | A.7.2.1 | 経営陣の責任 | 経営陣は，組織の確立された方針及び手順に従った情報セキュリティの適用を，全ての従業員及び契約相手に要求しなければならない． |
| | | A.7.2.2 | 情報セキュリティの意識向上，教育及び訓練 | 組織の全ての従業員，及び関係する場合には契約相手は，職務に関連する組織の方針及び手順についての，適切な，意識向上のための教育及び訓練を受けなければならず，また，定めに従ってその更新を受けなければならない． |
| | | A.7.2.3 | 懲戒手続 | 情報セキュリティ違反を犯した従業員に対して処置をとるための，正式かつ周知された懲戒手続を備えなければならない． |

9.3　雇用の終了及び変更

雇用終了及び変更では，従業員及び契約相手の，雇用の終了または変更後も有効な責任について伝達し，その遂行を確実にする必要がある．また，雇用の変更に関しては，現在の雇用の終了と，新しい雇用の開始との組み合わせとして管理することが望ましい．

表 7　A.7.3 雇用の終了及び変更

| 管理目的名 | 管理目的 | 管理策番号 | 管理策名 | 管理策概要 |
|---|---|---|---|---|
| A.7.3　雇用の終了及び変更 | 雇用の終了又は変更のプロセスの一部として，組織の利益を保護するため． | A.7.3.1 | 雇用の終了又は変更に関する責任 | 雇用の終了又は変更の後もなお有効な情報セキュリティに関する責任及び義務を定め，その従業員又は契約相手に伝達し，かつ，遂行させなければならない。 |

10.　資産の管理

資産の管理は，資産に対する責任，情報分類，媒体の取扱いの 3 つの管理目的に分類される．

10.1　資産に対する責任

資産を管理するために，組織の資産を特定し，適切な保護を行う責任を定める必要がある．組織の資産を明らかにし，その管理責任及び利用規則を定める必要がある．また，雇用が終了する際には，組織の資産を全て返却することを確実にする必要がある．

表 8　A.8.1 資産に対する責任

| 管理目的名 | 管理目的 | 管理策番号 | 管理策名 | 管理策概要 |
|---|---|---|---|---|
| A.8.1　資産に対する責任 | 組織の資産を特定し，適切な保護の責任を定めるため． | A.8.1.1 | 資産目録 | 情報及び情報処理施設に関連する資産を特定しなければならない．また，これらの資産の目録を，作成し，維持しなければならない． |
| | | A.8.1.2 | 資産の管理責任 | 目録の中で維持される資産は，管理されなければならない． |
| | | A.8.1.3 | 資産利用の許容範囲 | 情報の利用の許容範囲，並びに情報及び情報処理施設と関連する資産の利用の許容範囲に関する規則は，明確にし，文書化し，実施しなければならない． |
| | | A.8.1.4 | 資産の返却 | 全ての従業員及び外部の利用者は，雇用，契約又は合意の終了時に，自らが所持する組織の資産の全てを返却しなければならない． |

10.2　情報分類

情報の適切なレベルでの保護を確実にするため，情報の必要性，優先順位及びその情報を取り扱う場合に期待する保護の程度を示すために情報を分類する必要がある．また，分類体系に応じて情報のラベル付けを行い，取扱いに関する手順を策定し実施する必要がある．

表 9　A.8.2 情報の分類

| 管理目的名 | 管理目的 | 管理策番号 | 管理策名 | 管理策概要 |
|---|---|---|---|---|
| A.8.2　情報分類 | 組織に対する情報の重要性に応じて，情報の適切なレベルでの保護を確実にするため． | A.8.2.1 | 情報の分類 | 情報は，法的要求事項，価値，重要性，及び認可されていない開示又は変更に対して取扱いに慎重を要する度合いの観点から，分類しなければならない． |
| | | A.8.2.2 | 情報のラベル付け | 情報のラベル付けに関する適切な一連の手順は，組織が採用した情報分類体系に従って策定し，実施しなければならない． |
| | | A.8.2.3 | 資産の取扱い | 資産の取扱いに関する手順は，組織が採用した情報分類体系に従って策定し，実施しなければならない． |

10.3　媒体の取扱い

媒体に保存された情報を保護し，認可されていない開示や変更，破壊を防止する必要がある．これを確実にするために，媒体の管理や処分及び輸送の手順を定める必要がある．

表 10　A.8.3 媒体の取扱い

| 管理目的名 | 管理目的 | 管理策番号 | 管理策名 | 管理策概要 |
|---|---|---|---|---|
| A.8.3　媒体の取扱い | 媒体に保存された情報の認可されていない開示，変更，除去又は破壊を防止するため． | A.8.3.1 | 取外し可能な媒体の管理 | 組織が採用した分類体系に従って，取外し可能な媒体の管理のための手順を実施しなければならない． |
| | | A.8.3.2 | 媒体の処分 | 媒体が不要になった場合は，正式な手順を用いて，セキュリティを保って処分しなければならない． |
| | | A.8.3.3 | 物理的媒体の輸送 | 情報を格納した媒体は，輸送の途中における，認可されていないアクセス，不正使用又は破損から保護しなければならない． |

11. アクセス制御

アクセス制御は，アクセス制御に対する業務上の要求事項，利用者アクセスの管理，利用者の責任，システム及びアプリケーションのアクセス制御の 4 つの管理目的に分類される．

11.1 アクセス制御に対する業務上の要求事項

アクセスの制御に対する業務上の要求事項として，適切なアクセス制御規則，アクセス権及び制限を決定し，文書化及び定期的なレビューを行う必要がある．特に，ネットワークへのアクセスに関しては，その利用の方針を設定する必要がある．

表 11 A.9.1 アクセス制御に対する業務上の要求事項

| 管理目的名 | 管理目的 | 管理策番号 | 管理策名 | 管理策概要 |
|---|---|---|---|---|
| A.9.1 アクセス制御に対する業務上の要求事項 | 情報及び情報処理施設へのアクセスを制限するため. | A.9.1.1 | アクセス制御方針 | アクセス制御方針は，業務及び情報セキュリティの要求事項に基づいて確立し，文書化し，レビューしなければならない. |
| | | A.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 | 利用することを特別に認可したネットワーク及びネットワークサービスへのアクセスだけを，利用者に提供しなければならない. |

11.2 利用者アクセスの管理

利用者のアクセスを管理し，認可されたアクセスを確実にし，認可されていないアクセスを防止する必要がある．アクセス権の割当てのために，利用者の登録及び削除について正式なプロセスを実施する必要がある．また，その必要性に応じて，適切なアクセス権を提供する必要がある．特に，特権的アクセス権及び秘密認証情報(パスワードなど)は，アクセス制御方針に従って，正式なプロセスによって管理される必要がある．提供されたアクセス権は，定期的にレビューし，雇用の終了や変更に応じて，適宜削除及び修正する必要がある．

表 12　A.9.2 利用者アクセスの管理

| 管理目的名 | 管理目的 | 管理策番号 | 管理策名 | 管理策概要 |
|---|---|---|---|---|
| A.9.2　利用者アクセスの管理 | システム及びサービスへの，認可された利用者のアクセスを確実にし，認可されていないアクセスを防止するため． | A.9.2.1 | 利用者登録及び登録削除 | アクセス権の割当てを可能にするために，利用者の登録及び登録削除についての正式なプロセスを実施しなければならない． |
| | | A.9.2.2 | 利用者アクセスの提供 | 全ての種類の利用者について，全てのシステム及びサービスへのアクセス権を割り当てる又は無効化するために，利用者アクセスの提供についての正式なプロセスを実施しなければならない． |
| | | A.9.2.3 | 特権的アクセス権の管理 | 特権的アクセス権の割当て及び利用は，制限し，管理しなければならない． |
| | | A.9.2.4 | 利用者の秘密認証情報の管理 | 秘密認証情報の割当ては，正式な管理プロセスによって管理しなければならない． |
| | | A.9.2.5 | 利用者アクセス権のレビュー | 資産の管理責任者は，利用者のアクセス権を定められた間隔でレビューしなければならない． |
| | | A.9.2.6 | アクセス権の削除又は修正 | 全ての従業員及び外部の利用者の情報及び情報処理施設に対するアクセス権は，雇用，契約又は合意の終了時に削除しなければならず，また，変更に合わせて修正しなければならない． |

11.3　利用者の責任

秘密認証情報(パスワードなど)の保護を確実にする必要がある．利用者は，自らの責任で秘密認証情報を保護する必要があり，組織は，そのためのルールを示す必要がある．

表 13　A.9.3　利用者の責任

| 管理目的名 | 管理目的 | 管理策番号 | 管理策名 | 管理策概要 |
|---|---|---|---|---|
| A.9.3　利用者の責任 | 利用者に対して，自らの秘密認証情報を保護する責任をもたせるため． | A.9.3.1 | 秘密認証情報の利用 | 秘密認証情報の利用時に，組織の慣行に従うことを，利用者に要求しなければならない． |

11.4　システム及びアプリケーションのアクセス制御

情報へのアクセスは，アクセス制御方針に従って，セキュリティに配慮した適切なログオン手順によって制御する必要がある．特に，システム及びアプリケーションによる制御を無効にできるようなユーティリティプログラムの使用や，プログラムのソースコード及び関連書類へのアクセスは厳重に管理する必要がある．また，パスワードを管理するシステムは，利用者のパスワードを良質なものにすることを確実にするよう，構築する必要がある．

表 14　A.9.4 システム及びアプリケーションのアクセス制御

| 管理目的名 | 管理目的 | 管理策番号 | 管理策名 | 管理策概要 |
|---|---|---|---|---|
| A.9.4 システム及びアプリケーションのアクセス制御 | システム及びアプリケーションへの，認可されていないアクセスを防止するため． | A.9.4.1 | 情報へのアクセス制限 | 情報及びアプリケーションシステム機能へのアクセスは，アクセス制御方針に従って，制限しなければならない． |
| | | A.9.4.2 | セキュリティに配慮したログオン手順 | アクセス制御方針で求められている場合には，システム及びアプリケーションへのアクセスは，セキュリティに配慮したログオン手順によって制御しなければならない． |
| | | A.9.4.3 | パスワード管理システム | パスワード管理システムは，対話式でなければならず，また，良質なパスワードを確実とするものでなければならない． |
| | | A.9.4.4 | 特権的なユーティリティプログラムの使用 | システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用は，制限し，厳しく管理しなければならない． |
| | | A.9.4.5 | プログラムソースコードへのアクセス制御 | プログラムソースコードへのアクセスは，制限しなければならない． |

12. 暗号

暗号は，暗号による管理策のみの管理目的が分類されている．

12.1 暗号による管理策

情報を保護するため，暗号は適切かつ有効に利用する必要がある．暗号の利用に関する方針定め，暗号鍵の生成，保管，保存，読出し，配布，使用停止及び破壊を含むライフサイクル全体にわたるプロセスが必要となる．

表 15 A.10.1 暗号による管理策

| 管理目的名 | 管理目的 | 管理策番号 | 管理策名 | 管理策概要 |
|---|---|---|---|---|
| A.10.1 暗号による管理策 | 情報の機密性，真正性及び／又は完全性を保護するために，暗号の適切かつ有効な利用を確実にするため． | A.10.1.1 | 暗号による管理策の利用方針 | 情報を保護するための暗号による管理策の利用に関する方針は，策定し，実施しなければならない． |
| | | A.10.1.2 | 鍵管理 | 暗号鍵の利用，保護及び有効期間（lifetime）に関する方針を策定し，そのライフサイクル全体にわたって実施しなければならない． |

13. 物理的及び環境的セキュリティ

物理的及び環境的セキュリティは，セキュリティを保つべき領域と装置の 2 つの管理目的が分類されている．

13.1 セキュリティを保つべき領域

組織の情報及び情報処理施設のある領域を保護するため，物理的セキュリティ境界を設ける必要がある．セキュリティを保つべき領域では，認可された者だけにアクセスを許可するために，適切な入退室管理や，オフィス，部屋及び施設に対する物理的セキュリティを規定する必要がある．また，外部及び環境(自然災害や人的災害など)の脅威から保護，セキュリティを保つべき領域での作業，受渡し場所の隔離などについても検討する必要がある．

表 16　A.11.1 セキュリティを保つべき領域

| 管理目的名 | 管理目的 | 管理策番号 | 管理策名 | 管理策概要 |
|---|---|---|---|---|
| A.11.1　セキュリティを保つべき領域 | 組織の情報及び情報処理施設に対する認可されていない物理的アクセス，損傷及び妨害を防止するため. | A.11.1.1 | 物理的セキュリティ境界 | 取扱いに慎重を要する又は重要な情報及び情報処理施設のある領域を保護するために，物理的セキュリティ境界を定め，かつ，用いなければならない. |
| | | A.11.1.2 | 物理的入退管理策 | セキュリティを保つべき領域は，認可された者だけにアクセスを許すことを確実にするために，適切な入退管理策によって保護しなければならない. |
| | | A.11.1.3 | オフィス，部屋及び施設のセキュリティ | オフィス，部屋及び施設に対する物理的セキュリティを設計し，適用しなければならない. |
| | | A.11.1.4 | 外部及び環境の脅威からの保護 | 自然災害，悪意のある攻撃又は事故に対する物理的な保護を設計し，適用しなければならない. |
| | | A.11.1.5 | セキュリティを保つべき領域での作業 | セキュリティを保つべき領域での作業に関する手順を設計し，適用しなければならない. |
| | | A.11.1.6 | 受渡場所 | 荷物の受渡場所などの立寄り場所，及び認可されていない者が施設に立ち入ることもあるその他の場所は，管理しなければならない．また，可能な場合には，認可されていないアクセスを避けるために，それらの場所を情報処理施設から離さなければならない. |

13.2　装置

装置(構外で用いるもの及び移動するものを含む)の保護については，環境上の脅威及び災害からのリスク，並びに情報への認可されていないアクセスのリスクを低減し，損失又は損傷から情報を保護する必要がある．サポートユーティリティ(電気，通信サービス，空調など)やケーブル配線もまた，故障から保護する必要がある．これらには装置の保守作業も含まれる．特に，構外にあったり無人状態となったりしている装置のセキュリティは，その特性を考慮して適用する必要がある．また，机上に書類を放置しないことや情報をスクリーンに残したまま離席しないこと，事前の認可なしで装置などを構外に持ち出さないといった点も考慮する必要がある．

表 17(1/2)　A.11.2 装置

| 管理目的名 | 管理目的 | 管理策番号 | 管理策名 | 管理策概要 |
|---|---|---|---|---|
| A.11.2　装置 | 資産の損失，損傷，盗難又は劣化，及び組織の業務に対する妨害を防止するため． | A.11.2.1 | 装置の設置及び保護 | 装置は，環境上の脅威及び災害からのリスク並びに認可されていないアクセスの機会を低減するように設置し，保護しなければならない． |
| | | A.11.2.2 | サポートユーティリティ | 装置は，サポートユーティリティの不具合による，停電，その他の故障から保護しなければならない． |
| | | A.11.2.3 | ケーブル配線のセキュリティ | データを伝送する又は情報サービスをサポートする通信ケーブル及び電源ケーブルの配線は，傍受，妨害又は損傷から保護しなければならない． |
| | | A.11.2.4 | 装置の保守 | 装置は，可用性及び完全性を継続的に維持することを確実にするために，正しく保守しなければならない． |
| | | A.11.2.5 | 資産の移動 | 装置，情報又はソフトウェアは，事前の認可なしでは，構外に持ち出してはならない． |

表 17(2/2)　A.11.2 装置

| 管理目的名 | 管理目的 | 管理策番号 | 管理策名 | 管理策概要 |
|---|---|---|---|---|
| A.11.2　装置 | 資産の損失，損傷，盗難又は劣化，及び組織の業務に対する妨害を防止するため． | A.11.2.6 | 構外にある装置及び資産のセキュリティ | 構外にある資産に対しては，構外での作業に伴った，構内での作業とは異なるリスクを考慮に入れて，セキュリティを適用しなければならない． |
| | | A.11.2.7 | 装置のセキュリティを保った処分又は再利用 | 記憶媒体を内蔵した全ての装置は，処分又は再利用する前に，全ての取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを消去していること，又はセキュリティを保って上書きしていることを確実にするために，検証しなければならない． |
| | | A.11.2.8 | 無人状態にある利用者装置 | 利用者は，無人状態にある装置が適切な保護対策を備えていることを確実にしなければならない． |
| | | A.11.2.9 | クリアデスク・クリアスクリーン方針 | 書類及び取外し可能な記憶媒体に対するクリアデスク方針，並びに情報処理設備に対するクリアスクリーン方針を適用しなければならない． |

14. 運用のセキュリティ

運用のセキュリティは，運用の手順及び責任，マルウェアからの保護，バックアップ，ログ取得及び監視，運用ソフトウェアの管理，技術的ぜい弱性管理，情報システムの監査に対する考慮事項の 7 つの管理目的に分類されている．

14.1 運用の手順及び責任

情報処理設備の正確かつセキュリティを保った運用を確実にするため，すべての情報処理設備の管理及び運用のための責任体制及び手順を確立し，適切な操作手順は，文書化し維持する必要がある．

表 18 A.12.1 運用の手順及び責任

| 管理目的名 | 管理目的 | 管理策番号 | 管理策名 | 管理策概要 |
|---|---|---|---|---|
| A.12.1 運用の手順及び責任 | 情報処理設備の正確かつセキュリティを保った運用を確実にするため. | A.12.1.1 | 操作手順書 | 操作手順は，文書化し，必要とする全ての利用者に対して利用可能にしなければならない. |
| | | A.12.1.2 | 変更管理 | 情報セキュリティに影響を与える，組織，業務プロセス，情報処理設備及びシステムの変更は，管理しなければならない. |
| | | A.12.1.3 | 容量・能力の管理 | 要求されたシステム性能を満たすことを確実にするために，資源の利用を監視・調整しなければならず，また，将来必要とする容量・能力を予測しなければならない. |
| | | A.12.1.4 | 開発環境，試験環境及び運用環境の分離 | 開発環境，試験環境及び運用環境は，運用環境への認可されていないアクセス又は変更によるリスクを低減するために，分離しなければならない. |

14.2　マルウェアからの保護

情報及び情報処理施設を，マルウェアから保護する必要がある．これには，マルウェアに対する検出・修復ソフトウェア，情報セキュリティに対する認識，及びシステムへの適切なアクセス・変更管理についての管理策に基づく必要がある．

表 19　A.12.2 マルウェアからの保護

| 管理目的名 | 管理目的 | 管理策番号 | 管理策名 | 管理策概要 |
|---|---|---|---|---|
| A.12.2 マルウェアからの保護 | 情報及び情報処理 施設がマルウェアから保護されることを確実にするため. | A.12.2.1 | マルウェアに対する管理策 | マルウェアから保護するために，利用者に適切に認識させることと併せて，検出，予防及び回復のための管理策を実施しなければならない. |

14.3　バックアップ

データの消失から保護するため，バックアップの方針を定める必要がある．運用手順において，このバックアップ方針に従っていることを確実にする必要がある．

表 19　A.12.3 バックアップ

| 管理目的名 | 管理目的 | 管理策番号 | 管理策名 | 管理策概要 |
|---|---|---|---|---|
| A.12.3 バックアップ | データの消失から保護するため. | A.12.3.1 | 情報のバックアップ | 情報，ソフトウェア及びシステムイメージのバックアップは，合意されたバックアップ方針に従って定期的に取得し，検査しなければならない. |

14.4　ログ取得及び監視

利用者の活動，例外処理，過失及び情報セキュリティ事象を記録したイベントログを取得し，保持し，定期的にレビューする必要がある．特に，ログを操作できるなどの特権を与えられた利用者の作業は注意する必要がある．また，これらのログは改ざん及び認可されていないアクセスから保護し，その時刻表示は統一されていることを確実にする必要がある．

表 20　A.12.4 ログ取得及び監視

| 管理目的名 | 管理目的 | 管理策番号 | 管理策名 | 管理策概要 |
|---|---|---|---|---|
| A.12.4 ログ取得及び監視 | イベントを記録し，証拠を作成するため. | A.12.4.1 | イベントログ取得 | 利用者の活動，例外処理，過失及び情報セキュリティ事象を記録したイベントログを取得し，保持し，定期的にレビューしなければならない. |
| | | A.12.4.2 | ログ情報の保護 | ログ機能及びログ情報は，改ざん及び認可されていないアクセスから保護しなければならない. |
| | | A.12.4.3 | 実務管理者及び運用担当者の作業ログ | システムの実務管理者及び運用担当者の作業は，記録し，そのログを保護し，定期的にレビューしなければならない. |
| | | A.12.4.4 | クロックの同期 | 組織又はセキュリティ領域内の関連する全ての情報処理システムのクロックは，単一の参照時刻源と同期させなければならない. |

14.5　運用ソフトウェアの管理

運用システムの完全性を確実にするため，運用システムに関わるソフトウェアの導入は管理する必要がある.

表 21　A.12.5 運用ソフトウェアの管理

| 管理目的名 | 管理目的 | 管理策番号 | 管理策名 | 管理策概要 |
|---|---|---|---|---|
| A.12.5 運用ソフトウェアの管理 | 運用システムの完全性を確実にするため. | A.12.5.1 | 運用システムに関わるソフトウェアの導入 | 運用システムに関わるソフトウェアの導入を管理するための手順を実施しなければならない. |

14.6　技術的ぜい弱性管理

技術的ぜい弱性に対し，適切かつ時機を失しない処置をするために，管理プロセスを確立する必要がある．また，インストールしてもよいソフトウェアの種類についての方針も定める必要がある．

表 22　A.12.6 技術的ぜい弱性管理

| 管理目的名 | 管理目的 | 管理策番号 | 管理策名 | 管理策概要 |
|---|---|---|---|---|
| A.12.6 技術的ぜい弱性管理 | 技術的ぜい弱性の悪用を防止するため. | A.12.6.1 | 技術的ぜい弱性の管理 | 利用中の情報システムの技術的ぜい弱性に関する情報は，時機を失せずに獲得しなければならない．また，そのようなぜい弱性に組織がさらされている状況を評価しなければならない．さらに，それらと関連するリスクに対処するために，適切な手段をとらなければならない. |
| | | A.12.6.2 | ソフトウェアのインストールの制限 | 利用者によるソフトウェアのインストールを管理する規則を確立し，実施しなければならない. |

14.7　情報システムの監査に対する考慮事項

運用システムの監査活動による，業務プロセスの中断などの影響を最小限に抑える必要がある．隔離された複製に対するアクセスや，営業時間外などで監査を実施するなど，慎重に計画し，合意を得る必要がある．

表 23　A.12.7 情報システムの監査に対する考慮事項

| 管理目的名 | 管理目的 | 管理策番号 | 管理策名 | 管理策概要 |
|---|---|---|---|---|
| A.12.7 情報システムの監査に対する考慮事項 | 運用システムに対する監査活動の影響を最小限にするため. | A.12.7.1 | 情報システムの監査に対する管理策 | 運用システムの検証を伴う監査要求事項及び監査活動は，業務プロセスの中断を最小限に抑えるために，慎重に計画し，合意しなければならない. |

15.　通信のセキュリティ

　通信のセキュリティは，ネットワークセキュリティ管理と情報の転送の 2 つの管理目的が分類されている．

15.1　ネットワークセキュリティ管理

　全てのネットワークは，それぞれに必要なセキュリティ要求事項を特定し，管理する必要がある．また，大規模なネットワークの場合は，グループごとにネットワークを分離させ，アクセスを管理する必要がある．

表 24　A.13.1 ネットワークセキュリティ管理

| 管理目的名 | 管理目的 | 管理策番号 | 管理策名 | 管理策概要 |
|---|---|---|---|---|
| A.13.1　ネットワークセキュリティ管理 | ネットワークにおける情報の保護，及びネットワークを支える情報処理施設の保護を確実にするため． | A.13.1.1 | ネットワーク管理策 | システム及びアプリケーション内の情報を保護するために，ネットワークを管理し，制御しなければならない． |
| | | A.13.1.2 | ネットワークサービスのセキュリティ | 組織が自ら提供するか外部委託しているかを問わず，全てのネットワークサービスについて，セキュリティ機能，サービスレベル及び管理上の要求事項を特定しなければならず，また，ネットワークサービス合意書にもこれらを盛り込まなければならない． |
| | | A.13.1.3 | ネットワークの分離 | 情報サービス，利用者及び情報システムは，ネットワーク上で，グループごとに分離しなければならない． |

15.2　情報の転送

通信設備を利用した情報転送の方針及び手順を定め，外部関係者とも合意を得る必要がある．特に，電子的メッセージ通信に含まれる情報は，適切に保護する必要がある．また，法的に強制できる表現を用いて，秘密保持契約や守秘義務契約の要求事項を文書化しておく必要がある．

表 25　A.13.2 情報の転送

| 管理目的名 | 管理目的 | 管理策番号 | 管理策名 | 管理策概要 |
|---|---|---|---|---|
| A.13.2　情報の転送 | 組織の内部及び外部に転送した情報のセキュリティを維持するため. | A.13.2.1 | 情報転送の方針及び手順 | あらゆる形式の通信設備を利用した情報転送を保護するために，正式な転送方針，手順及び管理策を備えなければならない. |
| | | A.13.2.2 | 情報転送に関する合意 | 合意では，組織と外部関係者との間の業務情報のセキュリティを保った転送について，取り扱わなければならない. |
| | | A.13.2.3 | 電子的メッセージ通信 | 電子的メッセージ通信に含まれた情報は，適切に保護しなければならない. |
| | | A.13.2.4 | 秘密保持契約又は守秘義務契約 | 情報保護に対する組織の要件を反映する秘密保持契約又は守秘義務契約のための要求事項は，特定し，定めに従ってレビューし，文書化しなければならない. |

16.　システムの取得，開発及び保守

システムの取得，開発及び保守は，情報システムのセキュリティ要求事項，開発及びサポートプロセスにおけるセキュリティ，試験データの 3 つの管理目的が分類されている．

16.1　情報システムのセキュリティ要求事項

情報システムのセキュリティ要求事項は，情報システムの設計，開発及び実装する前に特定し合意した上で文書化する必要がある．特に，アプリケーションサービスのトランザクションや，公衆ネットワーク上でのセキュリティは，法的要求事項を考慮し，適切に保護する必要がある．

表 26　A.14.1 情報システムのセキュリティ要求事項

| 管理目的名 | 管理目的 | 管理策番号 | 管理策名 | 管理策概要 |
|---|---|---|---|---|
| A.14.1　情報システムのセキュリティ要求事項 | ライフサイクル全体にわたって，情報セキュリティが情報システムに欠くことのできない部分であることを確実にするため．これには，公衆ネットワークを介してサービスを提供する情報システムのための要求事項も含む． | A.14.1.1 | 情報セキュリティ要求事項の分析及び仕様化 | 情報セキュリティに関連する要求事項は，新しい情報システム又は既存の情報システムの改善に関する要求事項に含めなければならない． |
| | | A.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 | 公衆ネットワークを経由するアプリケーションサービスに含まれる情報は，不正行為，契約紛争，並びに認可されていない開示及び変更から保護しなければならない． |
| | | A.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 | アプリケーションサービスのトランザクションに含まれる情報は，次の事項を未然に防止するために，保護しなければならない．<br>― 不完全な通信<br>― 誤った通信経路設定<br>― 認可されていないメッセージの変更<br>― 認可されていない開示<br>― 認可されていないメッセージの複製又は再生 |

16.2　開発及びサポートプロセスにおけるセキュリティ

セキュリティに配慮した開発のための方針及び原則を定め，開発環境を確立する必要がある．特に，システムの変更管理における手順は文書化し，パッケージソフトウェアの不必要な変更は抑止する必要がある．また，新規，あるいは更新したシステムは，開発期間中にセキュリティの試験を行い，受入れ試験も行う必要がある．特に，オペレーティングシステムを変更した場合は，悪影響がないように，重要なアプリケーションのレビューを行う必要がある．加えて，外部委託でシステム開発を行う場合，その開発活動を監督し，監視する必要がある．

表 27(1/2)　A.14.2 開発及びサポートプロセスにおけるセキュリティ

| 管理目的名 | 管理目的 | 管理策番号 | 管理策名 | 管理策概要 |
|---|---|---|---|---|
| A.14.2　開発及びサポートプロセスにおけるセキュリティ | 情報システムの開発サイクルの中で情報セキュリティを設計し，実施することを確実にするため． | A.14.2.1 | セキュリティに配慮した開発のための方針 | ソフトウェア及びシステムの開発のための規則は，組織内において確立し，開発に対して適用しなければならない． |
| | | A.14.2.2 | システムの変更管理手順 | 開発のライフサイクルにおけるシステムの変更は，正式な変更管理手順を用いて管理しなければならない． |
| | | A.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 | オペレーティングプラットフォームを変更するときは，組織の運用又はセキュリティに悪影響がないことを確実にするために，重要なアプリケーションをレビューし，試験しなければならない． |
| | | A.14.2.4 | パッケージソフトウェアの変更に対する制限 | パッケージソフトウェアの変更は，抑止しなければならず，必要な変更だけに限らなければならない．また，全ての変更は，厳重に管理しなければならない． |

表 27(2/2)　A.14.2 開発及びサポートプロセスにおけるセキュリティ

| 管理目的名 | 管理目的 | 管理策番号 | 管理策名 | 管理策概要 |
|---|---|---|---|---|
| A.14.2　開発及びサポートプロセスにおけるセキュリティ | 情報システムの開発サイクルの中で情報セキュリティを設計し，実施することを確実にするため． | A.14.2.5 | セキュリティに配慮したシステム構築の原則 | セキュリティに配慮したシステムを構築するための原則を確立し，文書化し，維持し，全ての情報システムの実装に対して適用しなければならない． |
| | | A.14.2.6 | セキュリティに配慮した開発環境 | 組織は，全てのシステム開発ライフサイクルを含む，システムの開発及び統合の取組みのためのセキュリティに配慮した開発環境を確立し，適切に保護しなければならない． |
| | | A.14.2.7 | 外部委託による開発 | 組織は，外部委託したシステム開発活動を監督し，監視しなければならない． |
| | | A.14.2.8 | システムセキュリティの試験 | セキュリティ機能（functionality）の試験は，開発期間中に実施しなければならない． |
| | | A.14.2.9 | システムの受入れ試験 | 新しい情報システム，及びその改訂版・更新版のために，受入れ試験のプログラム及び関連する基準を確立しなければならない． |

16.3　試験データ

試験に用いるデータは，個人情報などの秘密情報を含まないよう，慎重に選定する必要がある．秘密情報を含むデータを利用する場合は，取扱いに慎重を要する部分を消去または変更することによって保護する必要がある．

表 28　A.14.3 試験データ

| 管理目的名 | 管理目的 | 管理策番号 | 管理策名 | 管理策概要 |
|---|---|---|---|---|
| A.14.3　試験データ | 試験に用いるデータの保護を確実にするため. | A.14.3.1 | 試験データの保護 | 試験データは，注意深く選定し，保護し，管理しなければならない. |

17.　供給者関係

供給者関係は，供給者関係における情報セキュリティと供給者のサービス提供の管理の 2 つの管理目的が分類されている．

17.1　供給者関係における情報セキュリティ

供給者による情報へのアクセス及びセキュリティに関する方針を定め，合意を得る必要がある．特に，情報通信技術サービス及び製品のサプライチェーンに関連する情報セキュリティの要求事項を定め，合意を得る必要がある．

表 29　A.15.1 供給者関係における情報セキュリティ

| 管理目的名 | 管理目的 | 管理策番号 | 管理策名 | 管理策概要 |
|---|---|---|---|---|
| A.15.1　供給者関係における情報セキュリティ | 供給者がアクセスできる組織の資産の保護を確実にするため. | A.15.1.1 | 供給者関係のための情報セキュリティの方針 | 組織の資産に対する供給者のアクセスに関連するリスクを軽減するための情報セキュリティ要求事項について，供給者と合意し，文書化しなければならない. |
| | | A.15.1.2 | 供給者との合意におけるセキュリティの取扱い | 関連する全ての情報セキュリティ要求事項を確立しなければならず，また，組織の情報に対して，アクセス，処理，保存若しくは通信を行う，又は組織の情報のための IT 基盤を提供する可能性のあるそれぞれの供給者と，この要求事項について合意しなければならない. |
| | | A.15.1.3 | ICTサプライチェーン | 供給者との合意には，情報通信技術(ICT)サービス及び製品のサプライチェーンに関連する情報セキュリティリスクに対処するための要求事項を含めなければならない. |

17.2　供給者のサービス提供の管理

供給者のサービスは監視及びレビューし，合意における情報セキュリティの条件を確実にしていることを確認する必要がある．また，供給者のサービスの変更は管理し，そのリスクを考慮する必要がある．

表 30　A.15.2 供給者のサービス提供の管理

| 管理目的名 | 管理目的 | 管理策番号 | 管理策名 | 管理策概要 |
|---|---|---|---|---|
| A.15.2　供給者のサービス提供の管理 | 供給者との合意に沿って，情報セキュリティ及びサービス提供について合意したレベルを維持するため． | A.15.2.1 | 供給者のサービス提供の監視及びレビュー | 組織は，供給者のサービス提供を定常的に監視し，レビューし，監査しなければならない． |
| | | A.15.2.2 | 供給者のサービス提供の変更に対する管理 | 関連する業務情報，業務システム及び業務プロセスの重要性，並びにリスクの再評価を考慮して，供給者によるサービス提供の変更（現行の情報セキュリティの方針群，手順及び管理策の保守及び改善を含む．）を管理しなければならない． |

18.　情報セキュリティインシデント管理

情報セキュリティインシデント管理は，情報セキュリティインシデントの管理及びその改善のみの管理目的が分類されている．

18.1　情報セキュリティインシデントの管理及びその改善

情報セキュリティインシデント管理に関する管理層の責任及び手順を確立する必要がある．情報セキュリティ事象や弱点は適切な責任者へ，迅速に報告することを確実にする必要がある．情報セキュリティ事象は，評価し，その対応の手順を文書化する必要がある．特に，懲戒処置及び法的処置のために必要となる証拠の特定，収集，保存の手順を定める必要がある．また，これらインシデントへの対応内容は，再発防止などに利用していく必要がある．

表 31　A.16.1 情報セキュリティインシデントの管理及びその改善

| 管理目的名 | 管理目的 | 管理策番号 | 管理策名 | 管理策概要 |
|---|---|---|---|---|
| A.16.1　情報セキュリティインシデントの管理及びその改善 | セキュリティ事象及びセキュリティ弱点に関する伝達を含む，情報セキュリティインシデントの管理のための，一貫性のある効果的な取組みを確実にするため. | A.16.1.1 | 責任及び手順 | 情報セキュリティインシデントに対する迅速，効果的かつ順序だった対応を確実にするために，管理層の責任及び手順を確立しなければならない. |
| | | A.16.1.2 | 情報セキュリティ事象の報告 | 情報セキュリティ事象は，適切な管理者への連絡経路を通して，できるだけ速やかに報告しなければならない. |
| | | A.16.1.3 | 情報セキュリティ弱点の報告 | 組織の情報システム及びサービスを利用する従業員及び契約相手に，システム又はサービスの中で発見した又は疑いをもった情報セキュリティ弱点は，どのようなものでも記録し，報告するように要求しなければならない. |
| | | A.16.1.4 | 情報セキュリティ事象の評価及び決定 | 情報セキュリティ事象は，これを評価し，情報セキュリティインシデントに分類するか否かを決定しなければならない. |
| | | A.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は，文書化した手順に従って対応しなければならない. |
| | | A.16.1.6 | 情報セキュリティインシデントからの学習 | 情報セキュリティインシデントの分析及び解決から得られた知識は，インシデントが将来起こる可能性又はその影響を低減するために用いなければならない. |
| | | A.16.1.7 | 証拠の収集 | 組織は，証拠となり得る情報の特定，収集，取得及び保存のための手順を定め，適用しなければならない. |

19.　事業継続マネジメントにおける情報セキュリティの側面

事業継続マネジメントにおける情報セキュリティの側面は，情報セキュリティ継続と冗長性の 2 つの管理目的が分類されている．

19.1　情報セキュリティ継続

組織は，事業継続マネジメントプロセスまたは災害復旧管理プロセスに，情報セキュリティの継続を織り込み，それを確実にする必要がある．また，情報セキュリティの継続のためのプロセスをレビューし，それが妥当かつ有効であることを確実にする必要がある．

表 32　A.17.1 情報セキュリティ継続

| 管理目的名 | 管理目的 | 管理策番号 | 管理策名 | 管理策概要 |
|---|---|---|---|---|
| A.17.1 情報セキュリティ継続 | 情報セキュリティ継続を組織の事業継続マネジメントシステムに組み込まなければならない. | A.17.1.1 | 情報セキュリティ継続の計画 | 組織は，困難な状況（adverse situation）（例えば，危機又は災害）における，情報セキュリティ及び情報セキュリティマネジメントの継続のための要求事項を決定しなければならない. |
| | | A.17.1.2 | 情報セキュリティ継続の実施 | 組織は，困難な状況の下で情報セキュリティ継続に対する要求レベルを確実にするための，プロセス，手順及び管理策を確立し，文書化し，実施し，維持しなければならない. |
| | | A.17.1.3 | 情報セキュリティ継続の検証，レビュー及び評価 | 確立及び実施した情報セキュリティ継続のための管理策が，困難な状況の下で妥当かつ有効であることを確実にするために，組織は，定められた間隔でこれらの管理策を検証しなければならない. |

19.2　冗長性

情報システムの可用性に関する業務上の要求事項を特定し，必要に応じて，冗長性のある構成要素またはアーキテクチャを考慮する必要がある．

表 33　A.17.2 冗長性

| 管理目的名 | 管理目的 | 管理策番号 | 管理策名 | 管理策概要 |
|---|---|---|---|---|
| A.17.2 冗長性 | 情報処理施設の可用性を確実にするため. | A.17.2.1 | 情報処理施設の可用性 | 情報処理施設は，可用性の要求事項を満たすのに十分な冗長性をもって，導入しなければならない. |

## 20. 順守

順守は，法的及び契約上の要求事項の順守と情報セキュリティのレビューの 2 つの管理目的が分類されている．

### 20.1 法的及び契約上の要求事項の順守

関連する法令，規制及び契約上の要求事項を特定し，文書化する必要がある．特に，知的財産権及び権利関係のあるソフトウェア製品の利用に関する要求事項を確実にするための手順を考慮する必要がある．また，記録及び個人情報は各要求事項に従って保護することを確実にする必要がある．加えて，暗号化機能についても，関連する協定，法令及び規制を順守するよう，考慮する必要がある．

表 34　A.18.1 法的及び契約上の要求事項の順守

| 管理目的名 | 管理目的 | 管理策番号 | 管理策名 | 管理策概要 |
|---|---|---|---|---|
| A.18.1 法的及び契約上の要求事項の順守 | 情報セキュリティに関連する法的，規制又は契約上の義務に対する違反，及びセキュリティ上のあらゆる要求事項に対する違反を避けるため． | A.18.1.1 | 適用法令及び契約上の要求事項の特定 | 各情報システム及び組織について，全ての関連する法令，規制及び契約上の要求事項，並びにこれらの要求事項を満たすための組織の取組みを，明確に特定し，文書化し，また，最新に保たなければならない． |
| | | A.18.1.2 | 知的財産権 | 知的財産権及び権利関係のあるソフトウェア製品の利用に関連する，法令，規制及び契約上の要求事項の順守を確実にするための適切な手順を実施しなければならない． |
| | | A.18.1.3 | 記録の保護 | 記録は，法令，規制，契約及び事業上の要求事項に従って，消失，破壊，改ざん，認可されていないアクセス及び不正な流出から保護しなければならない． |
| | | A.18.1.4 | プライバシー及び個人を特定できる情報(PII)の保護 | プライバシー及び PII の保護は，関連する法令及び規制が適用される場合には，その要求に従って確実にしなければならない． |
| | | A.18.1.5 | 暗号化機能に対する規制 | 暗号化機能は，関連する全ての協定，法令及び規制を順守して用いなければならない． |

20.2　情報セキュリティのレビュー

情報セキュリティをマネジメントする組織の取組みが，引き続き適切，妥当及び有効であることを確実にするために，定期的または重大な変化が生じた場合にレビューする必要がある．また，管理者は，方針，標準類及びその他適用される規制で定められた情報セキュリティの要求事項が満たされていることをレビューする必要がある．特に，情報システム(ハードウェアやソフトウェア)の制御が正しく実施されていることを確実にするためのレビューを行う必要がある．

表 35　A.18.2 情報セキュリティのレビュー

| 管理目的名 | 管理目的 | 管理策番号 | 管理策名 | 管理策概要 |
|---|---|---|---|---|
| A.18.2 情報セキュリティのレビュー | 組織の方針及び手順に従って情報セキュリティが実施され，運用されることを確実にするため. | A.18.2.1 | 情報セキュリティの独立したレビュー | 情報セキュリティ及びその実施の管理（例えば，情報セキュリティのための管理目的，管理策，方針，プロセス，手順）に対する組織の取組みについて，あらかじめ定めた間隔で，又は重大な変化が生じた場合に，独立したレビューを実施しなければならない. |
| | | A.18.2.2 | 情報セキュリティのための方針群及び標準の順守 | 管理者は，自分の責任の範囲内における情報処理及び手順が，適切な情報セキュリティのための方針群，標準類，及び他の全てのセキュリティ要求事項を順守していることを定期的にレビューしなければならない. |
| | | A.18.2.3 | 技術的順守のレビュー | 情報システムを，組織の情報セキュリティのための方針群及び標準の順守に関して，定めに従ってレビューしなければならない. |