社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2007－DPS－130 (76)
2007－CSEC－ 36 (76)
2007／3／2

ISO/IEC 17799の管理項目の関連性を考慮したセキュリティ対策の選択基準の検討

高橋 達明 ラミレス・カセレス・ギジェルモ・オラシオ 勅使河原 可海
創価大学大学院工学研究科 東京都八王子市丹木町1-236
E-mail: {ttakaha, guillerm, teshiga} @soka.ac.jp

概要：近年，企業の抱える情報資産を守るために多くの企業がセキュリティポリシー策定などの情報セキュリティ対策がとられている．セキュリティポリシーを策定するのに手助けとなるのが情報セキュリティマネジメントの実践のための国際標準ISO/IEC 17799である．これまで，企業にとって必要な管理策を選択するために，ISO/IEC 17799の管理項目を「参照」という記述に着目した分類，リスクの発生前・発生時・発生後に取るべき対策に分けた分類を行なってきた．そして本研究では，この二つの分類手法を組み合わせることにより企業にとって必要となる管理策の選択基準となる可能性を示した．この選択基準を用いることにより，ISMSを確立する際にもっとも時間をかける作業である「リスク対応に関する管理目的および管理策を選択する」の手間が軽減される．

キーワード：ISO/IEC 17799，情報セキュリティ対策，情報セキュリティマネジメントシステム（ISMS），情報セキュリティインシデント，リスク管理，セキュリティ対策選択基準

A Study on Selection Criteria of Security Countermeasures considering to relationship of the Security controls on ISO/IEC 17799

Tatsuaki TAKAHASHI Guillermo Horacio RAMIREZ CACERES
Yoshimi TESHIGAWARA
Graduate School of Engineering, Soka University
1-236 Tangi-cho, Hachioji, Tokyo 192-8577, Japan
E-mail: {ttakaha, guillerm, teshiga} @soka.ac.jp

ABSTRACT: Recently, in order to protect the information property, many enterprises are using information security policies including security policy making. An international standard for information security management, ISO/IEC 17799"Code of practice for information security management" is helpful for those who make security policies. At first, in order to select a necessary management policy for business organizations we classify the ISO/IEC 17799 controls, paying attention to the descriptions "See". Next, we should classify countermeasures into three categories; before, the exact time and after the risk is emerged. In this research, by combining these classification techniques, we could show the possible selection criteria of security countermeasures needed for business organizations. This selection criteria facilitates the most time-consuming work "Select control objectives and controls for the treatment of risks" when the ISMS is build.

Keywords: ISO/IEC 17799, Information Security Countermeasures, Information Security Management Systems (ISMS), Information Security Incident, Risk Management, Selection Criteria of Security Countermeasures

1. はじめに

近年，企業の抱える情報資産を守るために，多くの企業が情報セキュリティ対策をとっている．ファイアウォールや侵入検知システムなどのシステム・技術面での情報セキュリティ対策だけでなく，情報セキュリティ教育の実施やセキュリティポリシー策定などの運用・体制面の情報セキュリティ対策も多くの企業でとられている．その中でも多くの企業が情報セキュリティマネジメントシステム(ISMS: Information Security Management Systems)適合性評価制度[1]という国際的に整合性のとれた情報セキュリティマネジメントに対する第三者適合性評価制度を取得し，社内に情報セキュリティマネジメントの仕組みを作り，運用面から情報セキュリティの強化を行なっている． ISMS 適合性評価制度の認証取得事業者数は 2005 年 8 月に 1000 社を超え，世界第 1 位の認証取得数となる[2]．図 1 に現在までの ISMS 評価制度認証取得事業者数を示す．

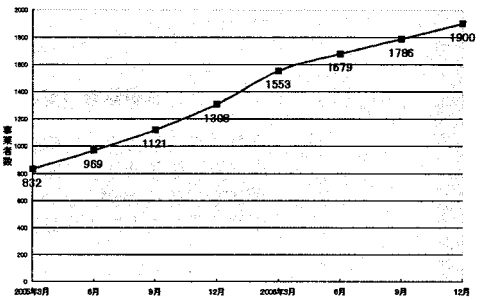


図 1　ISMS 評価制度認証取得事業者数[3]

現在までの ISMS 評価制度認証取得事業者数の増加し，今後入札条件や電子商取引への参加の条件に ISMS 適合性評価制度の取得の有無が問われることが予想される[4]．このことから，企業にとって ISMS を構築し，情報資産を運用面からも保護していく重要性がさらに高まってくることがわかる．

組織が ISMS を構築するための要求事項をまとめた国際標準として ISO/IEC 27001:2005[5]がある．その中で，リスク対応の管理項目として使われているものに組織の情報セキュリティに責任を持つ人々に向けた効果的な ISMS を実施するための規範（ベストプラクティス－最良の慣行）をまとめた国際標準として ISO/IEC 17799[6]がある．ISO/IEC 27001 に基づきリスクアセスメントを行い，リスク対応の管理項目を ISO/IEC 17799 より選択することが ISMS を構築する際にもっとも時間をかける作業であることが多くの事例からわかる[7]．この原因として， ISO/IEC 17799 自体の分類が不適切であり複雑な構造になっていること，実際の企業の環境に適合させることは困難であることが挙げられる．さらに，ISO/IEC 17799 から必要となる管理項目を選択することは，多くの時間や費用がかかり，情報セキュリティに関する専門的な知識が必要であるとされている．そのため，必要となる ISO/IEC 17799 の管理項目を選択するために外部の情報セキュリティの専門家が提供しているセキュリティコンサルティングサービスなどを利用し専門家の経験則によって選択される現状がある[7].

2. 研究の目的

本研究では，ISO/IEC 17799 の管理項目を選択するための指標作りを目的とし，ISO/IEC 17799 に記述されている管理項目の新しい分類基準の検討を行った．これまで「参照」という記述に着目した分類手法[8]，リスクを基点とした分類手法[9]を提案してきた．

しかし，それぞれの分類手法で網羅される管理項目は 7 割程度で必要な管理項目の選択基準を考えるにあたっては十分に満たしているとはいえない．そこで，本研究では 2 つの分類手法を組み合わせて構造化に関することにより，必要な管理項目をするための指標となる選択手順を作成した．そして本研究の選択手順とこれまでの管理項目の選択手法との比較・検討を行なった．

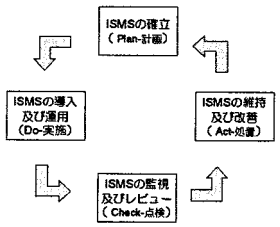
2.1 期待される効果

ISMS を構築するための指標を作成する，特に管理項目の選択に関する基準を作成することにより，ISMS を構築する人々が自分たちの企業にとって必要な管理項目だけを選ぶことができるのではないかと考える．その結果，これまでのように必要以上の管理項目の選択に対して時間やコストをかける必要がなくなると考えられる．そして，新しい分類基準を作成することにより，ISMS を構築する人々は，分類基準に則り管理項目を順に選択すればよいこととなる．そのため，ISMS の構築に関する必要な専門的な知識がなくとも ISMS を構築できると考える．さらに，外部に ISMS の構築を委託する必要もなくなるため，時間とコストの削減が可能であると考える．

3. ISMS

ISMS とは「マネジメントシステム全体の中で，事業リスクに対する取組み方に基づいて，情報セキュリティの確立，導入，運用，監視，レビュー，維持及び改善を担う部分」と ISO/IEC 27001 の中で定義されている．ここでいうマネジメントシステムには，組織の構造，方針，計画作成活動，責任，実践，手順，プロセス及び経営資源が含まれる．つまり，ISMS とは企業などの組織が情報を適切に管理し，機密を守るための包括的な枠組みのことである．コンピュータシステムのセキュリティ対策だけでなく，セキュリティポリシーや，それに基づいた具体的な計画，計画の実施・運用，一定期間ごとの方針・計画の見直しまで含めた，トータルなリスクマネジメント体系のことを指す．

このように“Plan-Do-Check-Act(計画－実行－点検－処置)”のプロセスを順に実施し，最後の改善を次の計画に結び付け，らせん状に継続的な業務改善活動などを推進するマネジメント手法を PDCA サイクルという．ISMS プロセスの構築に PDCA モデルが適用されている． 図 2 に，ISO/IEC 27001 で定義されているプロセスに適用される PDCA モデルを示す．



ISMSの確立（計画-Plan）	リスクマネジメント及び情報セキュリティの改善に関連した，ISMS 基本方針，目的，プロセス及び手順の確立
ISMSの導入及び運用（実行-Do）	ISMS 基本方針，管理策，プロセス及び手順の導入及び運用
ビュー（点検-Check）	スのパフォーマンスのアセスメント，適用可能ならば測定及びアセスメント結果のレビューのための経営陣への報
ISMSの維持及び改善（処置-Act）	置及びマネジメントレビューの結果又はその他の関連情報に基づいた，是正処置及び予防処置の実施

図２　ISMS プロセスに適用される PDCA モデル[6]

4. ISO/IEC 17799

ISO/IEC 17799 は，2000 年 12 月に組織として情報セキュリティに取り組みための管理項目を定めた国際標準である．この標準には，人的・物理的・環境的なセキュリティ，通信及び運用管理，法的適合性など，技術，管理，利用，運用などの様々な側面から情報セキュリティを守るための実践のための規範となっている．日本では，2002 年に JIS X 5080 として国内規格化されている．

ISO/IEC JTC 1/SC 27 の会合において改定作業が行われ 2005 年 6 月には新しい ISO/IEC 17799:2005 が発行された．2000 年版のセキュリティ管理項目は，管理項目そのものの記述のほかに，その実施に伴うガイドラインなどの情報が一体となっており，理解しにくいものであった．2005 年版では，管理項目の部分，実施の手引の部分，関連情報の部分と明確に分割され，理解し易い内容となった．そして，個々の管理項目の実施の手引の記述においては，最新技術（脆弱性管理等）の取り込み，記載の明確化，規格を通じた記述内容の整合性確保などの編集作業がなされ，2000 年版には 127 個の管理項目が，2005 年版では 133 個の管理項目に整理された．

ISO/IEC 17799 の構造は階層構造をとっており，以下に示す 11 の管理分野の下に 39 の管理目的，さらにその下に 133 の管理項目という形で図 3 のような 3 層構造をとっている．

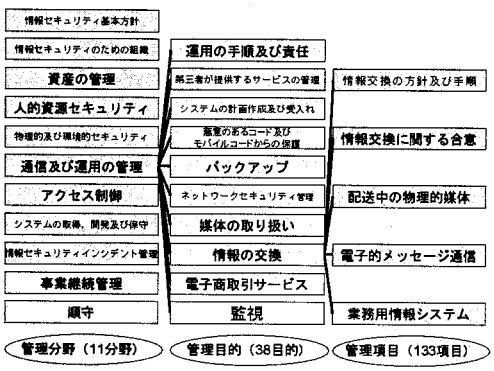


図３　ISO/IEC 17799 の構造

5. 提案手法

5.1 「参照」とは

一つの管理項目を満足するために，いくつかの要件がある．その要件の記述の中に図 4 のような「参照」という記述がある．なお，管理項目を表す数値（6.1.7 など）に関しては，ISO/IEC 17799 の記述に従った．

> **6.1.7 専門組織との連絡**
> **管理項目**
> 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することが望ましい。
>
> **実施の手引**
> 情報セキュリティに関する研究会又は会議への参加は，次のことを達成する手段として，考慮することが望ましい。
> a. 最適な慣行に関する認識を改善し，関係するセキュリティ情報を最新に保つ。
> b. 情報セキュリティ環境の理解が最新で完全であることを確実にする。
> c. 攻撃及びぜい弱性に関連する早期警戒警報，勧告及びパッチを受理する。
> d. 専門家から情報セキュリティ助言を得る。
> e. 新しい技術，製品，脅威又はぜい弱性に関する情報を共用し，交換する。
> f. 情報セキュリティインシデントを扱う場合の，適切な連絡窓口を提供する（*13.2.1 参照*）。
>
> **関連情報**
> セキュリティ問題に関する協力及び調整を得られやすくするために，情報共有に関して合意を確立することができる。このような合意では，取扱いに慎重を要する情報の保護に対する要求事項を明確にすることが望ましい。

図４　「参照」の例

この「参照」とは，要件を満足するために関連のある管理項目を指す．そこで，参照先として記述されている管理項目は，参照が記述されている管理項目を満足するために必要であると定義する．ここで定義した関係性を「直接参照」と定義する．直接参照した管理項目にもさらに直接参照する管理項目が存在する場合があり，これらも元の管理項目にとって必要な管理項目となる．このような関係性を「間接参照」と定義する．そして，直接参照と間接参照を合わせたものを「参照」と定義する．本分類手法では，管理項目の中に記述されている「管理策」という項目に記述されている「参照」についてのみを用いて参照構造を作成した．

5.2 「参照」の構造化

これまで検討してきた「参照」という関係性は，階層関係にある．そこで，この関係性を分岐数に制約のない根付き木に置き換えることとした．各管理項目を「節点」として，「親」である管理項目が参照先として記述されている管理項目を「子」とした．「子」とされた管理項目に対しても，その「子」となる管理項目があるかを辿り，木を作成する．なお，「子」となる管理項目が生成している木内に存在する場合は省くものとした．

分岐数に制約のない根付き木を作成するためのアルゴリズムを検討し，C 言語をもちいて各管理項目における分岐数に制約のない根付き木を作成した．図 5 に管理項目における分岐数に制約のない根付き木の例を示す．「参照」という関係性から生成されたデータを用いて，管理項目の選択基準の検討を行なった．

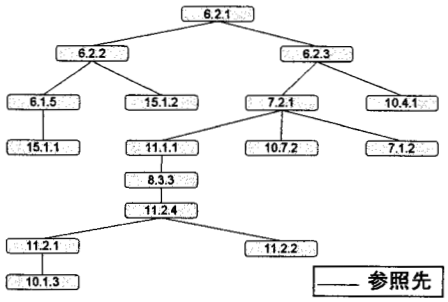


図5　管理項目の分岐数に制約のない根付き木

5.3 リスクを基点した分類手法

ISO/IEC 17799に記述されている管理項目をリスクの発生を基点とした場合，以下の3つに分類した．

1) リスクの発生を予防するために取るリスク発生前の管理項目
2) リスクの発生を検出するためにとるリスク発生時の管理項目
3) リスクが発生した後に状態を回復のために取るリスク発生後の管理項目

その中でもリスクの発生を予防するために取るリスク発生前の管理項目を以下の3つに分類した．

1) 現在の状態を維持するための管理項目
2) リスクの発生を検出するために事前に取るべき管理項目
3) リスクの発生後に状態を回復するための管理項目

このように，リスクの発生を基点とした場合，管理策の選択基準は図6のようになると定義する．

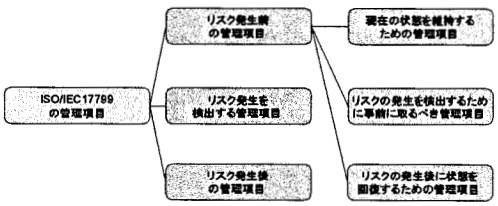


図6　リスクの発生を基点とした管理項目選択基準

先にあげた分類に関して実際にISO/IEC 17799の133個管理項目に記述されている「管理策」「実施の手引き」という項目から，それぞれの管理策がどの分類に属するかを選択した．

なお，一つの管理項目が，記述内容からリスク発生前の管理項目でもリスク発生後の管理項目でもあるような管理項目があった．それは，一つの管理策に対して，「実施の手引き」の内容が多いものでは数十個の項目が記述されていることがわかったからである．そのため，今回の分類わけでは一つの管理項目を一つだけの分類項目に属することは困難であると判断し，いくつかの分類に属してもよいと定義した．

この分類によってリスク発生時の管理項目に分類された管理項目を表1に示す．

表1　リスク発生時の管理項目

9.1.1	物理的セキュリティ境界
9.1.2	物理的入退管理策
10.4.1	悪意のあるコードに対する管理策
10.10.1	監査ログ取得
10.10.2	システム使用状況の監視
10.10.3	ログ情報の保護
10.10.4	実務管理者及び運用担当者の作業ログ
10.10.5	障害のログ取得
13.1.1	情報セキュリティ事象の報告
13.2.1	責任及び手順

この10個の管理項目は，リスクが発生したことを検出するものであり，この「検出」という動作を実現するために必要な管理項目を他の管理項目の中から選択し，その管理項目をこれらの管理項目を実現するために必要な管理項目であると定義することとした．表1にある管理項目に記述されている「管理策」という部分からリスクの検出にかかわる文章を選択し，その文章を実現すべき管理項目をISO/IEC 17799の記述の中から手動で選択した．

例えば，図7のような発生時に必要な管理項目の「管理策」という記述がある．その中から発生を検出することに関する語句を抽出する．ここでは，「報告」，「警告」という語句が検出に関する語句であるとした．

- 13.2.1 責任及び手順

<管理策>

－情報セキュリティの事象及び弱点の報告に加えて，情報セキュリティインシデントを検知するために，システム，警告及びぜい弱性の監視を利用すること

図7　発生時に必要な管理項目

これらの語句に関する管理項目から必要と思われる管理項目を選択した．必要であるとした管理項目を表2に示す．同様に，そのほかの発生時に必要な管理項目，発生後に必要な管理項目に対しても同様の分類を行なった．

表2　必要な管理項目

報告	5.1.1	情報セキュリティ基本方針文書
	6.1.5	秘密保持契約
	6.1.6	関係当局との連絡
	6.2.3	第三者との契約におけるセキュリティ
	10.2.2	第三者が提供するサービスの監視及びレビュー
	10.4.1	悪意のあるコードに対する管理策
	10.10.5	障害のログ取得
	13.1.1	情報セキュリティ事象の報告
警告	10.4.1	悪意のあるコードに対する管理策
	10.10.2	システム使用状況の監視
	11.5.1	セキュリティに配慮したログオン手順
	15.1.5	情報処理施設の不正使用防止

5.4 必要な管理項目の選択手順

これまで検討を行なってきた分類手法を組み合わせるにあたって，5.3節にある「リスク発生を検出する管理項目」「リスク発生後の管理項目」に必要な管理項

目は，「参照」の関係性と同様であると考える．そこで，2つの分類手法を組み合わせてISO/IEC 17799に記述されている管理項目の中から重要とされる管理項目を選択できる指標を作成するために，管理項目の構造化に関する検討を行なった．

この2つの分類手法を組み合わせたときの「参照」を用いることに新たな分岐数に制約のない根付き木を作成し検討を行なった．図8に2つの分類手法を組み合わせたときの管理項目の参照の例を示す．

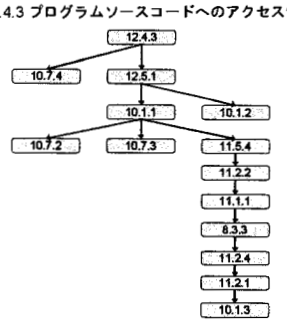


図8　組み合わせたときの管理項目の参照の例

この2つの分類手法を用いることにより，133の管理項目のうち121の管理項目が「参照」の関係性にあることがわかった．そして，14の管理項目が「根」となることがわかった．その内，「11.5.3 パスワード管理システム」，「12.3.1 暗号による管理策の利用方針」は，119の管理項目を子として持つ木となることがわかった．さらに，この2項目の子となる管理項目の中で同じ管理項目が「参照」関係にあるもの管理項目が32項目あり，表3にその管理項目を示す．

表3　同じ管理項目が参照関係にあるもの管理項目

6.1.7	専門組織との連絡
6.2.1	外部組織に関係したリスクの識別
6.2.3	第三者との契約におけるセキュリティ
8.1.2	選考
8.1.3	雇用条件
8.2.1	経営陣の責任
8.2.2	情報セキュリティの意識向上，教育及び訓練
8.2.3	懲戒手続
8.3.1	雇用の終了又は変更に関する責任
9.1.2	物理的入退管理策
10.2.2	第三者が提供するサービスの監視及びレビュー
10.4.1	悪意のあるコードに対する管理策
10.5.1	情報のバックアップ
10.8.1	情報交換の方針及び手順
10.8.5	業務用情報システム
10.10.1	監査ログ取得
10.10.2	システム使用状況の監視
10.10.3	ログ情報の保護
10.10.4	実務管理者及び運用担当者の作業ログ
10.10.5	障害のログ取得
11.2.3	利用者パスワードの管理
12.2.1	入力データの妥当性確認
12.2.2	内部処理の管理
12.3.2	かぎ(鍵)管理
12.4.1	運用ソフトウェアの管理
12.6.1	技術的ぜい弱性の管理
13.1.1	情報セキュリティ事象の報告
13.2.1	責任及び手順
13.2.3	証拠の収集
14.1.1	事業継続管理手続への情報セキュリティの組込み
14.1.4	事業継続計画策定の枠組み
14.1.5	事業継続計画の試験，維持及び再評価

そして，先にあげた14の管理項目のうち表4に示す12の管理項目は参照する管理項目が存在せず，独立した管理項目として考えることになる．このことから，必要な管理策を考える際にこれらの管理策は内容を確認し必要であるかを検討することになる．

表4　独立した管理項目

9.1.3	オフィス，部屋及び施設のセキュリティ
9.1.6	一般の人の立寄り場所及び受渡場所
9.2.6	装置の安全な処分又は再利用
9.2.7	資産の移動
10.6.2	ネットワークサービスのセキュリティ
11.4.1	ネットワークサービスの利用についての方針
11.4.3	ネットワークにおける装置の識別
11.5.5	セッションのタイムアウト
11.5.6	接続時間の制限
12.2.3	メッセージの完全性
12.2.4	出力データの妥当性確認
15.3.2	情報システムの監査ツールの保護

本研究の分類手法に基づいた関係性を用いることにより，参照している管理項目が多い重要となる管理項目から必要であるかを検討していけば少ない検討回数で必要となる管理項目がわかると考えた．

まず根となる管理項目の中から「11.5.3 パスワード管理システム」，「12.3.1 暗号による管理策の利用方針」の管理項目が必要かを検討し，必要であるとなったならば参照とされている119の管理項目を選択する．もし，必要でないと判断したならば，表3にあげた管理項目が必要であるかを検討し，必要であるとなったならば参照とされている118の管理項目を選択する．これらの34の管理項目の中でも必要な管理策がなければ参照数の多い管理項目から順に必要であるかを検討していくことになる．最後に，独立した管理項目である表4にある12の管理項目が必要であるかを検討し，選択するかを決定すればよいことになる．このような順番で必要であるかを検討することによって，すべての管理項目に対して検討したこととなる．

そこで，「11.5.3 パスワード管理システム」，「12.3.1 暗号による管理策の利用方針」の2つの管理項目に対して必要であるかの検討を行い，どちらかの管理項目を必要な管理項目とし，表4にある12の管理項目を検討することが14回という最も少ない検討回数ですべての管理項目に対して検討をおこなったこととなる．これは，一つ一つの管理項目に対して必要かを検討するのに比べて約10%の検討回数で必要な管理項目の選択が可能となる．

これによって，管理項目に対して必要な管理項目が決まっているので情報セキュリティポリシーを策定する企業にとって必要な管理項目が簡単に短時間に選択することが可能である．さらに，あらかじめ選択すべき管理項目の順序が決まっているので，情報セキュリティポリシー策定するためのISO/IEC 17799の管理項目を選択するのに必要な知識の軽減が見込まれる．加えて，多くの管理項目から参照されている管理項目は情報セキュリティポリシーを策定する企業にとって選択すべき指標となる管理項目としても考えることができる．

5.5 有効性の評価

本手法の有効性を検討するために，5.4 節で述べた最も少ない検討回数となる環境の検討を行なった．5.4 節の結果から検討回数が少なくなるときは参照が多いものを必要であると選択したときである．したがって，参照が多い「11.5.3 パスワード管理システム」，「12.3.1 暗号による管理策の利用方針」の２つの管理項目に対して必要である判断されるような環境ならば管理項目の検討回数を減らすことができると考えた．

「11.5.3 パスワード管理システム」とは，「パスワードを管理するシステムは，対話式とすることが望ましく，また，良質なパスワードを確実とすることが望ましい」とある．この管理項目の目的は「11.5 オペレーティングシステムのアクセス制御」であり，オペレーティングシステムへの，認可されていないアクセスを防止するためのものである．企業において，従業員が自ら使用する端末に対してパスワードを作り管理することによって，不正なアクセスを防止することになる．このことはもはや常識的になっているため，この管理策はどの企業においても必要ではないかと考えた．

次に，「12.3.1 暗号による管理策の利用方針」とは，「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，実施することが望ましい」とある．この管理項目の目的は，「12.3 暗号による管理策」であり，暗号手段によって，情報の機密性，真正性又は完全性を保護するためのものである．この管理項目は，機密性の高い情報の機密性を確保するために行なう管理項目であると考えられる．この機密性の高い情報とは，従業員，取引先の個人情報や社内秘などとされた漏洩することによりその企業の業務に支障をきたす情報であると考える．これらのことから，大企業であれば多くの機密性の高い情報を有していると想像されるためこの管理項目は必要であると思われる．そして，いわゆる中小企業においては，リスクアセスメントの結果により，機密性の高い情報が多く保護すべきだと判断された場合に必要となる．

このようなパスワード管理を行い，機密性の高い情報を有する企業は最も少ない検討回数で管理項目の選択ができると考えた．

6. 今後の発展と課題

今回の検討では管理項目の参照の関係を分析しやすくするために分岐数に制約のない根付き木であるとした．しかし，「参照」という関係性を考えたとき関係性の表現として有向グラフとすることが最も適していると考えられる．この分類手法による有向グラフを作成し分析することによって，各管理項目の関連性の強度や互いに参照し合っているなどさらなる関係性を導き出し，これらが選択の手法としてどのように活用できるかを検討する必要がある．

さらに今後本研究を進めていくにあたって必要な検討事項は以下のようなものが挙げられる．

1) ISO/IEC 17799 の管理項目の選択基準の定量的な評価手法の検討
2) 検討を行なった分類手法を用いたシステムを構築し，実際の環境での適用した場合の有効性の評価
3) ISO/IEC 15408 などの情報セキュリティに関する国際標準との関連性を導き出し，より広範囲な情報セキュリティを考慮したセキュリティ対策の選択基準の作成
4) 検討を行なった分類手法から実際の情報セキュリティポリシーを策定するための方法を検討

7. 参考文献

[1] 情報セキュリティマネジメントシステム(ISMS)適合性評価制度：http://www.isms.jipdec.jp/

[2] 報道資料：ISMS 認証取得事業者数が 1,000 件を超える：http://www.isms.jipdec.jp/doc/press20050826.pdf

[3] 認証取得事業者数推移，審査登録機関別・県別認証取得事業者数(2006 年 9 月 1 日現在)：http://www.isms.jipdec.jp/lst/ind/suii.html

[4] 情報セキュリティマネジメントシステム(ISMS)適合性評価制度 お問い合わせ&FAQ: http://www.isms.jipdec.jp/faq/faq1.html

[5] ISO/IEC 27001:2005 Information technology - Security techniques - Information security management systems – Requirements

[6] ISO/IEC 17799:2005 Information technology -- Security techniques -- Code of practice for information security management

[7] ISMS 構築事例集～情報セキュリティへの取り組み事例～：http://www.isms.jipdec.jp/doc/const/constall.PDF

[8] XML を用いた ISO/IEC 17799 の構造化に関する検討，第 31 回コンピュータセキュリティ研究会，情報処理学会研究報告 2005-CSEC-31，pp43-48，2005-12

[9] ISO/IEC 17799 に基づくリスクの発生を基点としたセキュリティ対策の選択基準の検討，第 9 回コンピュータセキュリティシンポジウム 2006，コンピュータセキュリティシンポジウム CSS2006 論文集，pp399-404，2006-10