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研究

A Study on a Security Evaluation Platform
Based on International Standards

2014 年 3 月

髙橋　雄志

Yuji Takahashi

序文

本論文は，国際標準の特徴的な構造である階層的な文章構造と他の項目への参照指示をもって詳細な条件などを示す記述に着目し，その特徴を活かしたセキュリティ評価を実現するセキュリティ評価プラットフォームの研究について記したものである．

本研究で着目した国際標準とは，ISO/IEC 27000 ファミリーに代表されるセキュリティマネジメントに関する標準である．この標準はセキュリティ認証制度における評価基準となる標準であり，近年企業ではサイバーアタックなどの多くのセキュリティの脅威に対して外部認証機関によりセキュリティが確保されていることを証明することはより重要な要素となってきている．しかし，それらの標準を統合的に扱う環境が整っていない．

本論文では，こうしたセキュリティ認証制度を利用する際に生じる様々な問題点に対して述べ，問題解決のためにセキュリティ評価プラットフォームを構築し，プラットフォームの運用実験により，その有効性を示した．さらに，統合環境を実現するために，重要な課題となる関連情報の作成に関して，標準の各項目間の相関を取り関連情報を作成する手法を提案・検証し，提案するプラットフォームで統合的な環境が構築できることを示した．

第1章 序論

近年，セキュリティ管理の目的の範囲は，組織の資産を守る自己防衛のみから，二次的な加害者になることを防ぐところまで拡大している．これに伴い，組織の安全性の確保及びセキュリティ対策実施状況を対外的に明示するため，外的機関によるセキュリティ評価をすることが重要視されていて，多くのセキュリティ標準が策定されている[1]．しかし，個別のセキュリティ認証の取得に関しても対策の項目に対する網羅性の問題や標準に関する専門知識が要求されるといった問題があり，統合的に扱う環境はまだ整っていない．さらに，一言でセキュリティ認証といっても種類も非常に多く，個々の認証を取得することも容易であるとは言い難い．本研究は，セキュリティ認証の取得における様々な問題を解決するべく，認証取得時に基準となる国際標準などの評価基準の特徴に注目した，セキュリティ評価プラットフォームの構築をし，本論文では，そのプラットフォームに必要な各種機能や仕組みを提案する．

本章では，セキュリティ認証に関する現状，および本研究で取り上げる課題などについて述べ，上記のプラットフォームの必要性を明確にする．

1.1 セキュリティ認証の取得に関する現状

1.1.1 セキュリティ認証制度とは

日本では具体的な評価制度として ISMS 適合性評価制度に基づく情報セキュリティマネジメントシステム（以下，ISMS: Information Security Management System という）認証取得がある．この ISMS 認証は図 1 で示すように認証制度ができて以来取得件数が増加し続けており，2014 年 1 月 31 日現在で 4,443 件と多くの企業・組織が取得している[2]．また，ISMS に関する国際規格としては後述する ISO/IEC 27000 ファミリーがある[3]．

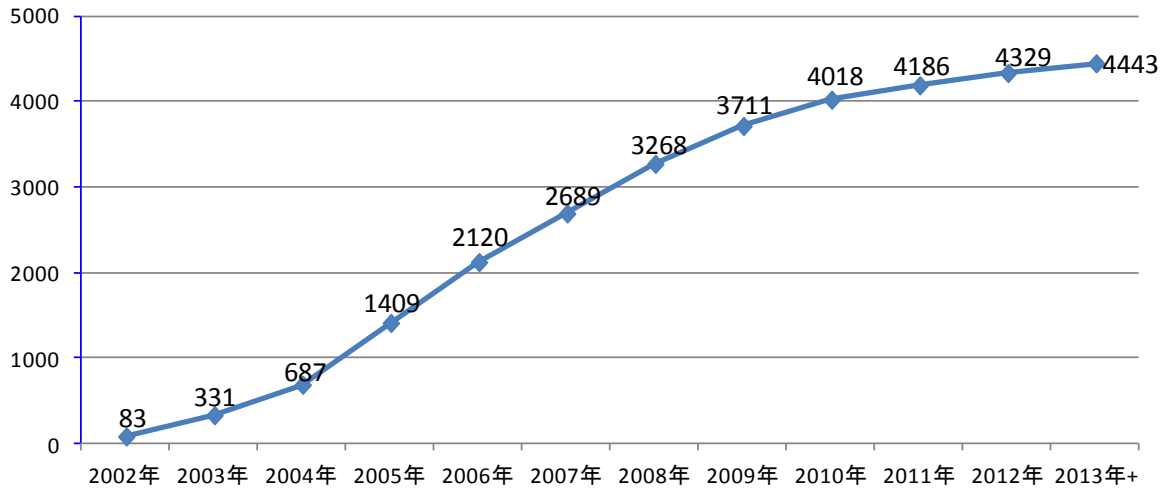


図 1　ISMS 認証取得組織数推移

Figure 1　ISMS certified organizations by year

ISMS などのセキュリティ認証の多くは，ISO/IEC 27001 や ISO/IEC 27002，JIS Q 15001 といった標準を基準として，その標準に記載されている項目を満たすことにより，組織のセキュリティが確保されていることを保証する．また，近年は業界標準の策定が行われるケースもあり，クレジットカード業界団体によって策定された Payment Card Industry Data Security Standard(PCI DSS)[4]というものも存在する．同様にコンシューマ・デバイスの管理に関するセキュリティ技術にも注目されてきている．企業の IT 資産にコンシューマ・デバイスからアクセスすることは，新しい重大なリスクを伴う．そのため，慎重な計画によって十分なセキュリティプロセスおよびセキュリティコントロールを確実に実現し，機密情報と機密性の高いアプリケーションを保護する必要がある．そのため強力なユーザ認証，アイデンティティライフサイクル管理，Web アクセス管理，情報の保護，および暗号化などの領域を含めて，アイデンティティ/アクセス管理の機能の重要性が高まっており，様々な形での標準化も積極的に行われている[5]．

1.1.2 セキュリティ評価システムとその課題

ISMS などのセキュリティ認証の多くは，ISO/IEC 27001 や ISO/IEC 27002，JIS Q 15001 といった標準を基準として，記載されている項目を満たすことにより，組織のセキュ

リティが確保されていることを保証する. こういった認証制度では, 基準となる標準の網羅性, 認証取得担当者の専門知識が不十分なことがあるといった問題がある. これらの問題は, セキュリティ標準から対策を導き出そうとする際に, 標準ごとに使われている用語が違ったり, 細かい表現が違ったり, 粒度(抽象度)が違ったり, 色々な要素が混じっていたりといったことに起因している[6]. また, 組織では認証取得に向け, 基準達成を確認するためのセキュリティ評価システムが活用されている[7]. しかし, 標準は時代の変化に合わせて頻繁に内容が変更される. 中でもセキュリティ関係の標準はまだ充分に試されていないので, ユーザコメントを集め変更が行われる回数が他の標準にくらべて頻繁である. 例えば, 後述する本研究でも使用している ISO/IEC 27001 は 2005 年に発行されて, 2013 年に改定されている. また, 取得を目指す認証が異なったり, 組織規模などに応じて基準とすべき内容が異なったりする. そうした変化は評価対象組織および評価目的が変わると, 認証取得のために, 新たな体制を作ってそれぞれの認証取得にあわせて個別のツールや人員を用いてセキュリティ評価をやり直さなければならないといった状況を作りだす原因となっている. そして, 認証取得のためには多くの時間と労力, 費用が必要となり企業活動における人的, 金銭的な影響が大きいという問題につながっている.

1.2 標準の分析と活用

1.2.1 関連する標準

本研究では, ISMS に代表されるセキュリティ管理の基準で広く用いられている PDCA(Plan-Do-Check-Act cycle)サイクルの概念が適応されている ISO/IEC 27000 ファミリーとしてまとめられたセキュリティ標準に着目をして, セキュリティ評価プラットフォームの構築を目指した.

PDCA サイクルとは図 2 で示すように Plan(計画), Do(実施), Check(点検), Act(処置)の頭文字をとったものである. まず, Plan のステップで ISMS の確立を練り, 次の Do へと移る. ここで確立した ISMS を実際に運用すると共に, 適切な Check を実施する. さらにその中で不具合が発見されれば是正処置, ならびに予防処理 Act を行う. そして, 再び Plan へと戻り, さらに強固な ISMS を確立していく流れとなる.

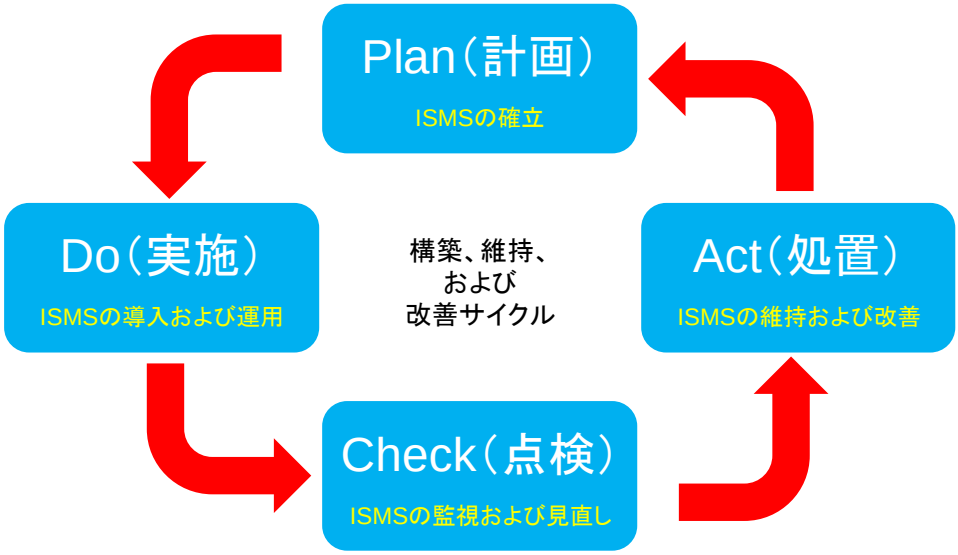


図 2　PDCA サイクルの概念図

Figure 2　Key map pf PDCA cycle

したがって，一度 ISMS が確立できればそれで終わりというわけではなく，ISMS 確立後も PDCA サイクルにのっとって，継続的に改善していくことが重要となる[8].

本研究で構築するセキュリティ評価プラットフォームは，PDCA サイクルの特定の場面でしかつかえないというものではなく，用途に合わせて PDCA サイクルのどの場面でも使えるものを目指している．例えば，Plan の段階で使用する場合は，現状分析の結果を入力し，対策の抜け漏れの確認ができる．Do の段階では，対策を実施していく段階で想定していた項目をカバーできないことがわかった場合に，そのチェックをすることによって全体としての抜け漏れの確認ができる．Check の段階では，対策実施段階で想定されていた通りに各対策が機能しているのかのチェックに利用でき，実際の状況に合わせて対応状況の変更を加えることで抜け漏れの確認ができる．Act の段階では，Plan の段階と同様に再設定した対策の対応状況の抜け漏れが確認できる．といった効果が発揮される．

1.2.2 ISO/IEC によるマネジメントシステム規格の提案

情報セキュリティマネジメントシステムの国際規格を策定している国際標準化機構(以下，ISO)および国際電気標準会議 (以下，IEC) の合同技術委員会(JTC1:Joint Technical Committee 1)よって，汎用的なマネジメントシステム規格(以下，MSS:Management System Standard)が提案されている．このMSSは産業分野別適用を含め，MSS を新たに作成する提案の場合は常に，文献[9]に示されている附属書 SL マネジメントシステム規格の提案の中にある，「妥当性の判断基準となる質問事項」(以下，Appendix 1)に従い，妥当性評価を行わなければならないとある．そして，実際の標準は，同じ附属書 SL の「上位構造，共通の中核となる共通テキスト，共通用語及び中核となる定義」(以下，Appendix 2)に即した形で記述されることとなる．実際に， 1.2.4 節で後述するISO/IEC 27001 の 2013 年版への改定時には，Appendix 2 に即した文章への改定が行われた．この改定時は，Appendix 1 の中で，「場合によっては，これらの質問事項で網羅されていない追加情報も提供することが望ましい．」と書かれているようにAppendix 2 の項目に加えてISO/IEC 27001:2013 独自の項目の追加がなされている[10]．

1.2.3 ISO/IEC 27000 ファミリー

ISO/IEC 27000 ファミリーとは，ISMS に関する国際規格であり， ISO および IEC の設置する合同専門委員会 ISO/IEC JTC1(情報技術)の分科委員会 SC 27(セキュリティ技術)において標準化作業が進められている．この規格群は要求事項であるISO/IEC 27001 をはじめ，ISO/IEC 27000 ファミリーとして様々な規格が検討され，発行されている[3]．また，対象とする範囲が広く，代表的なセキュリティ管理対象である，プライバシー，機密，情報技術におけるセキュリティ課題などをカバーしている．従って，あらゆる規模と形態の組織に適用可能であるといえる．

このファミリーのセキュリティ認証を取得するには，まず組織は情報セキュリティリスクを評価し，必要に応じた適切な情報セキュリティ対策を実装することが求められる．また，情報セキュリティの運用は固定的なものではないので，ISMS には 1.2.1 節で述べたようにPDCA サイクルによる継続的なフィードバックと改善が要求される．ISO/IEC 27000 フ

ファミリーは，現在のところ，2013 年 12 月時点ですでに 13 種類の標準が発行済みであり，他にも多くの標準が作成中となっている[3]. ISO/IEC 27000 ファミリーは多くの分野においての基準となる規格群となり，ISMS に基づく PDCA サイクル運営の重要性を示している.

1.2.4 ISO/IEC 27001

ISO/IEC 27001 は，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ものである[10]. 2013 年 10 月に，第 2 版発行された. 2008 年 10 月に ISO による定期見直しが開始されたが，その一方で，MSS の整合化を図るために，ISO において MSS の上位構造，共通テキスト及び共通用語・定義が開発されたことにより，ISO/IEC 27001 においてもこれらに基づいた改定作業が進められたという経緯がある[11]. 日本の国内規格としては，2006 年 5 月に JIS Q 27001:2006（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）として，第 1 版である ISO/IEC 27001:2005[12]をもとに制定されており，ISO/IEC 27001:2013 発行に伴い，2013 年 12 月現在改定中である. また，ISMS 認証取得時に作成される ISMS 運用マニュアルにおいては，この標準の各項目に示されている内容がセキュリティ要求事項に該当し，適用対象外のものは対象外であることを示すことを含めて，そのすべてを網羅している必要がある. ISMS 認証の審査の際には，このマニュアルに基づき各項目への対応状況が審査の対象となる.

JIS Q 27001:2006 は，項目内容を記述する本文だけで 28 ページになり，解説を含めると 53 ページとなる. また，1.2.9 項で後述する特徴情報となる階層構造と参照関係を示す記述は 200 に及ぶ[13].

1.2.5 ISO/IEC 27002

ISO/IEC 27001 の「附属書 A 管理目的および管理策」と整合がとられている基準に ISO/IEC 27002 がある. こちらは情報セキュリティマネジメントの導入，実施，維持及び改善に関するベストプラクティスをまとめた規格となる. 当初は ISO/IEC 17799 として発行されたが，2007 年 7 月に規格番号が 27002 へ改番され 27000 ファミリーに属するよ

うになった. 2013 年 10 月に, 第 2 版が発行となった. この規格も 2006 年 5 月に JIS Q 27002:2006(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の実践のための規範)として国内規格となっているが, ISO/IEC 27002:2013 発行に伴い, 現在改定中である. このように標準は改訂, 改称されることがあり, この ISO/IEC 27002 はその代表例であると言える.

JIS Q 27002:2006 は, 本文だけで 101 ページになり, 解説を含めると 136 ページとなる. また, 階層構造と参照関係を示す記述は 1,288 に及ぶ[13].

1.2.6 ISMS 適合性評価制度

ISMS 適合性評価制度とは, 第三者機関が組織の情報セキュリティマネジメントシステムを客観的に評価し, 基準をクリアした組織に認証を与えるという制度である[8].

この ISMS 制度には, 制度を支える常用名要素があり, その要素とは以下に示す 3 点となる.

(1) 制度自体を維持運用する組織
(2) ISMS 構築のための基準
(3) ISMS を評価する第三者機関

(1)の制度の維持運用については, JIPDEC(財団法人日本情報処理開発協会)が執り行っており, ISMS の構築基準としては, JIPDEC より「ISMS 認証基準(Ver2.0)」が公表されている. 同文章は, JIOPDEC の Web サイトにて無料で入手可能である. なお, この認証基準は先に述べた ISO/IEC 27001 および ISO/IEC 27002 を JIS 化した JIS Q 27001:2006, JIS Q 27002:2006 といった標準に基づいている.

さらに, ISMS を評価, 認証する第三者機関として, 審査登録機関が設けられている. こうした認証の仕組みは, ISO 9000 シリーズや ISO 14000 シリーズの場合とほとんど同じ仕組みとなっている. この 3 つの要素の関係は図 3 のように示すことができる.

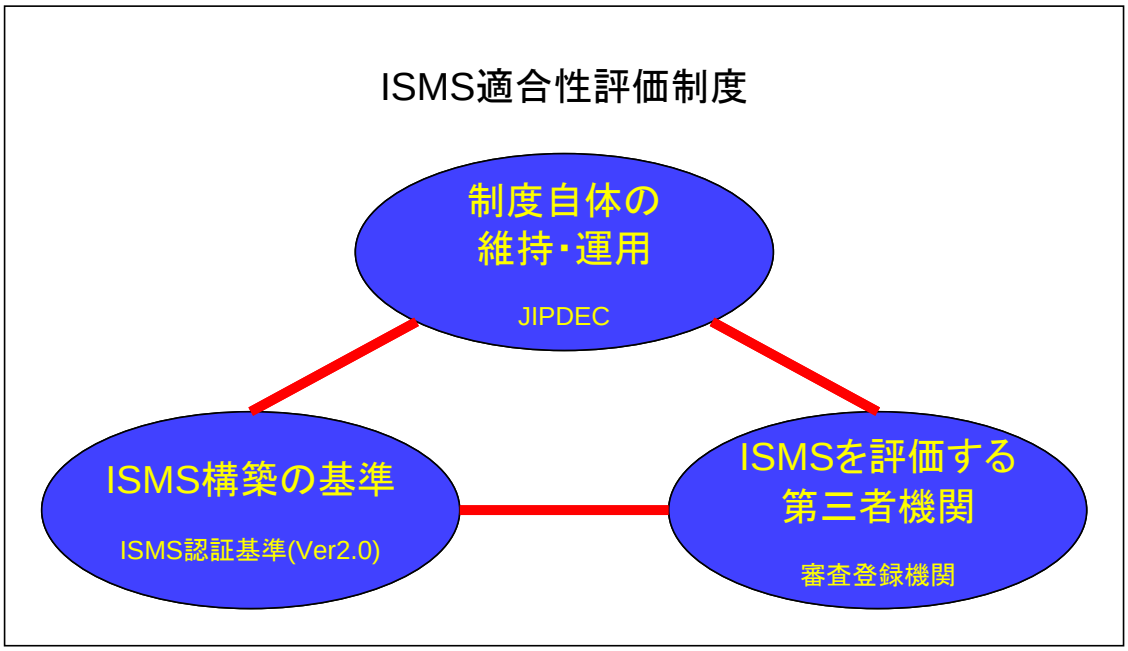


図 3　ISMS 適合性評価制度を支える要素

Figure 3　The elements supporting an ISMS conformity assessment scheme

1.2.7 BS 7799

BS 7799 とは，これまで述べてきた国際標準および日本の国内基準の元となった基準である．この BS 7799 は，BSI（British Standards Institution：英国規格協会）が発行している，情報セキュリティマネジメントに関する基準と仕様を規定したドキュメントである[14]．1995 年に最初の版が発行された後，主にネットワークの発展を考慮に入れた内容の改定が行われ，1999 年に改定版が発行されました．BS 7799 は「BSI/DISC 委員会 BDD/2 情報セキュリティ管理」の下で作成された．

この基準は，特定の製品やシステムが対象ではなく，企業や組織における情報システム全般を対象としている．したがって，セキュリティポリシーから始まり，組織，インフラ，物理的セキュリティ，人員の管理，アクセス制御，システム開発，事業継続など，広範囲にわたる項目が規定されている．つまりこの基準は情報システムの運用管理において，十分なセキュリティを確保することが主な目的となっている．

改訂版では，第一部「情報セキュリティ管理実施基準（以下，BS 7799-1）と第二部

「情報セキュリティ管理システム仕様」(以下, BS 7799-2)と二部構成になった. BS 7799-1 は、2000 年に ISO/IEC 17799 となり, 2007 年には ISO/IEC 27002:2005 と改称された. これに伴って BS 7799-1 は BS ISO/IEC 27002 となった. BS 7799-2 も、2005 年に ISO/IEC 27001 となりそれぞれが国際標準となった. さらに, それらは翻訳されて, 前述したように 2006 年に ISO/IEC 27001 は JIS Q 27001 として, ISO/IEC 27002 は JIS Q 27002 として日本工業規格に策定された.

一般的に BS 7799 として知られていたのは, BS 7799-1 の方であり, あらゆる業種や規模の組織において, 共通して適用可能な情報セキュリティの管理方法がまとめられている. しかし, 当然のことながら, この基準が各組織のあらゆる状態に適合するというわけではなく, あくまでも一般的に推奨される事項が勧告形式で書かれている. したがって, 各組織がセキュリティポリシーや基準を策定する際の参考資料として, あるいは企業間で取引の合意を得るための基準として活用するというのが一般的な活用法となる.

BS 7799-2 は BS 77799-1 の補足的な内容であり, ISMS として BS7799 を実践するための必要事項が仕様書形式で書かれている. したがって, 項目も BS 7799-1 の大項目をそのままなぞった形となっている.

1.2.8 PCI DSS(Payment Card　Industry Data Security Standard)

PCI DSS[5]とは, American Express、Discover Financial Services、JCB International、MasterCard Worldwide、Visa Inc.によって設立された, クレジット会社業界団体である PCI Security Standards Council(PCI SSC)[15]により策定された業界標準である. この PCI SSC は, アカウントデータ保護に関するグローバル規模の開かれた協議会で, 継続中のセキュリティ基準の開発, 強化, 保管, 普及と実施に関する討論の場を提供している. また, PCI SSC のミッションは, PCI セキュリティ基準の教育と啓発を実施して, ペイメントアカウントデータのセキュリティを強化することである.

この標準は, カード会員のデータセキュリティを強化し, 均一なデータセキュリティ評価基準の採用をグローバルに推進するために策定された. これは, カード会員データを保護するために策定された技術面および運用面の要件のベースラインとして利用できるものである.

こうした業界標準の登場により，セキュリティ標準群を統合的に扱う環境の必要性が高まってきている．また，次章の関連研究で紹介する NEC の芦野らの研究では，この PCI DSS を知識ベースとして用いるシステム設定ツールの開発を行っている[16]．

1.2.9 標準の構成

関連する標準では，一般的に図 4 で示すように，本文が論文における「章・節・項」のように 3 段階の階層構造で記述されていることが多い．この構成では，章の部分で評価対象を大別し，節の中で評価対象における詳細を記述し，項の中でさらに詳細な内容を記述している． 例えば，ISO/IEC 27001:2005 では，節に当たる項目ごとにその目的が述べられ，続いて項にわかれて文章の箇条書きを交えて詳細事項が記述されている．

ただし，個々の項目は独立した項目として記述されているものばかりではなく，その項目の条件や附則事項として，他の項目を参照するように記述されているものが数多く存在している．例えば，ISO/IEC 27001:2005 の「7.1 一般」は本文中で 4.3.3 参照との記述があり，本研究で用いる参照ツリーでは図 5 で示すような形で表現する．

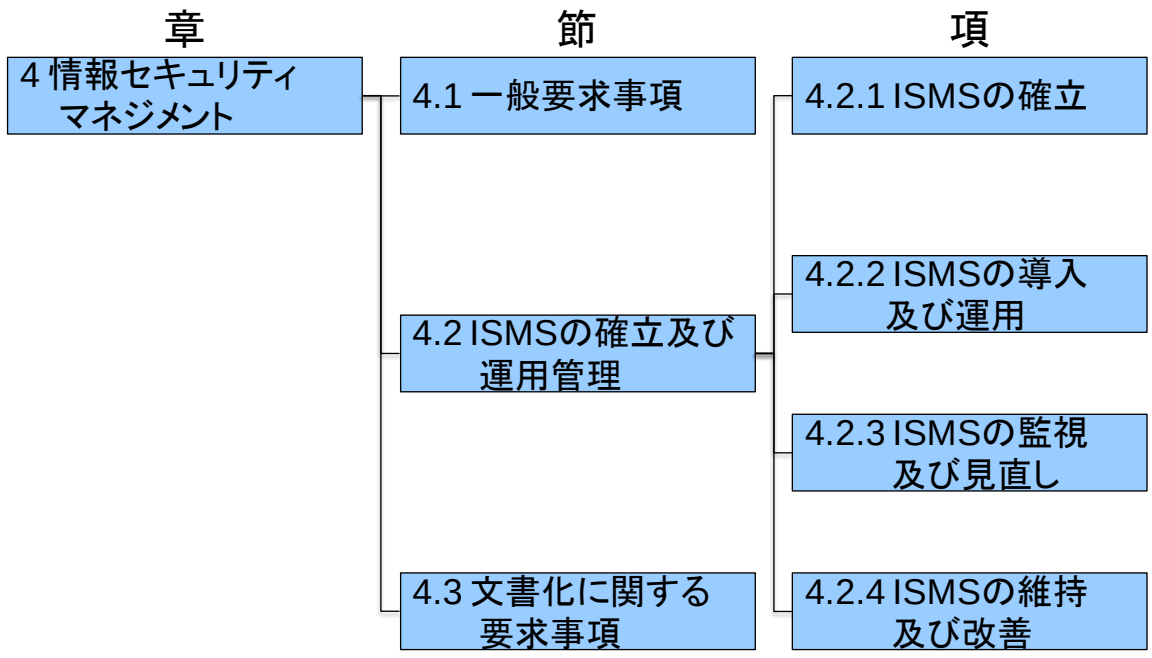


図 4　ISO/IEC 27001 の階層構造の例

Figure 4　Hierarchical structure example of ISO/IEC 27001

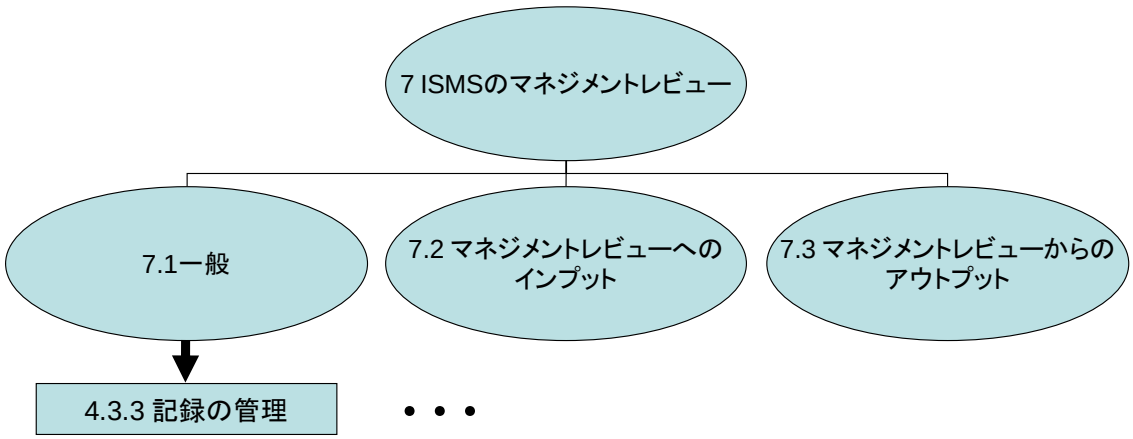


図 5　ISO/IEC 27001 の参照関係の例

Figure 5　Reference-related example of ISO/IEC 27001

1.2.10 対応策による項目の網羅の困難さ

セキュリティ認証の取得においては，基準となる規格の各項目を網羅的にカバーする必要があり，各章ごとの枠組みに応じて対応策の実施やリスクの受諾などの対応方針の決定を行っていく流れとなる．その際に，各章ごとにカバーすべき項目をすべて網羅している必要があるため，章ごとの階層構造と各項目からの参照関係を，的確に把握する必要がある．しかし，ISO/IEC 27001 に限らず，標準では参照を示す記述が多く，標準の各項目がカバーすべき内容（項目）が多岐にわたる．そのため，そのすべてを的確に理解し，網羅的な対応策を選択することが困難であるという問題点がある．

例えば ISO/IEC 27001:2005 では階層構造の項目間の関係も含めた参照関係は 200 存在し，ISO/IEC 27002:2005 に至っては 1288 もの参照関係が存在する．参照先が更に他の項目を参照している場合などを加えると，その数はさらに膨大な数となってしまう．これらの全てが記載されている項目名だけで，内容がわかるような項目であるとは限らない上に，章全体を参照先にしているような場合もある．

1.3 本研究で取り上げる課題

本研究では，セキュリティ評価システムが抱えている，それぞれの基準や認証に合わせた個別のセキュリティ評価ツールが必要となるという問題点，即ちセキュリティ標準群を統

合的に扱う環境がないという問題点を解決するために，個別のセキュリティ評価ツールではなく，基準となる標準の内容に依存せず，評価対象組織および評価目的の変更に対応した評価を実現する仕組みを構築していくものである．

また，基準となる標準の構造が複雑であるため各章で網羅すべきすべて項目を一括管理できることが求められている．

これらの課題をまとめると，以下に示す 3 点の内容となる

(1) セキュリティ認証取得のための共通の枠組みがない
(2) 多くのセキュリティ標準が存在するが、それぞれの関係性を示す情報が不足している
(3) 認証ごと，評価者ごとに，評価方法が異なり共通の評価方式がない

以下，本研究でこれら 3 つの課題をどのように解決していくかを述べる．

1.3.1 セキュリティ評価プラットフォームの構築

本研究では，対象となる標準に依存せず，セキュリティ評価を行うための基盤となるセキュリティ評価プラットフォームを作ることで問題の解決に当たるものである．このセキュリティ評価プラットフォームは基本となる標準を整理した生データ(以下，基本データという)の入れ替えだけで他の標準と同様にセキュリティ評価が行えるプラットフォームとならなくてはならない．本プラットフォームでは，標準の内容ではなく，1.2.6 項で述べた特徴的な構造である階層的な文章構造(以下，階層構造という)と，他の項目への参照指示をもって詳細な条件などを示す記述(以下，参照関係という)に注目した．これらは，標準の変更や異なる標準であっても同様の特徴情報として記述されている．このことに着目し，標準を階層構造に基づいて整理したデータが登録データとなるようにした．そして，階層構造と参照関係を利用した評価値計算をすることによって共通の評価値計算方式を検討した．また，セキュリティ認証に関する知識が深くないユーザに対して，認証取得を意識した対策選定，実施のサポートのための機能を実装することにより，基準となる標準の関係性の複雑さに関する問題の解決も目指している．さらに，基準となる標準が更新さ

れたり，他の認証を取得することになったりといった場合に，過去のデータを活用することによって，よりスムーズに新たな認証を取得できるようサポートを目指す．

1.4 研究の目的とアプローチ

本研究では，セキュリティ評価プラットフォームを構築することにより 1.3 節で掲げた枠組みを構築することを目的としている．また，この目的を達成するために提案するプラットフォームでは，1.3.1 項で示す各種課題について対応した以下に述べる 4 つの機能要件を満たす手法を提案する．

(1) 対象となる基準の種類に依存しない
(2) 基本となる基準を整理した基本データの入れ替えだけで他の基準と同様にセキュリティ評価が行える
(3) 過去のデータを新しい基準に活用できる機能の搭載
(4) セキュリティ評価のための共通の評価値算出方式

1.3 節で述べた課題(1)については，上記の機能要件(1)および(2)を満たす，セキュリティ評価プラットフォーム本体を作ることで解決にあたる．課題(2)については，プラットフォームに機能要件(3)を実現するデータ移行機能を搭載することと，標準の項目間の相関を取り，関連情報を作成することで解決にあたる．課題(3)については，プラットフォームに機能要件(4)を実現する評価値算出方式を搭載することで解決にあたる．

第 2 章では，関連研究について言及し，本研究との違いを示す．

第 3 章では，提案するセキュリティ評価プラットフォームの全体と目的達成のための各種機能の概要を述べる．

第 4 章では，第 3 章で概要を述べた各種機能の有効性検証実験を行いその有効性を示す．また，その中で機能要件の 3 に該当する機能に関する応用実験を行い，提案プラットフォームを有効活用できることを示す．

そして，第 5 章では各種機能を充実させることで目的達成が期待できることを述べる．

また, これらの手法を基盤とした, 今後の研究の展望を述べる.

第2章 関連研究

2.1 セキュリティオントロジーに関する研究

Secure Business Austria の Stefan Fenz らによって Security Ontology[17][18] を用いた ISO/IEC 27001 に対応したセキュリティ対策を行うための研究が行われている[19]. この研究では, ISO/IEC 27001:2005 の項目を「Hard Fact」と「Soft Fact」に分けて Security Ontology と組み合わせることでセキュリティ対策案選定へと導くものである. また, ここで使われている Security Ontology はリスク分析の分野での利用を主眼とした研究となっている[20]. この研究は, Security Ontology の作成, 有効利用を目的とするもので, 我々の研究と違って, 認証取得を主眼に置いた研究ではない. また, 事前にデータ準備が必要となり, Security Ontology の構築や項目の分類などの事前作業などがこれに該当する. 我々の研究では, 基準となる標準のデータのみを使用している. そして, 認証取得時の項目の網羅性に着目しており, 後述の参照ツリーを用いることで, 視覚的なサポートを行っている.

2.2 セキュリティ対策案選択問題に関する研究

静岡大学の加藤らによって ISMS 認証を意識したセキュリティ対策選定手法についての提案が行われている[21]. この研究では, 同大学の中村らによって情報資産, 脅威, セキュリティ対策の関係をモデル化し, セキュリティ対策案選択問題を定式化したモデルを使用している[22]. この研究では, 情報資産, 脅威を網羅する形で結果的に認証に関する項目が網羅できているというものである.

また, このセキュリティ対策案選択問題に関する研究としては, 東京電機大の佐々木らによって研究が続けられている, セキュリティ対策に関する意思決定関与者の合意形成を支援するためのツールとなる, 多重リスクコミュニケータ (Multiple Risk Communicator: MRC) に関する研究がある[23][24]. この研究では, 認証取得の観点でリスク評価を行っているわけではなく, 各関係者同士の合意形成を支援するものである. よって, 認証取得を目的とした際に, 項目の網羅性が保証されていない.

我々の研究では, 提案システムを用いて作られた過去の対策案を提示して, セキュリティ対策案選択問題に対してのサポートを行っている. そのため, 過去の案件できちんと

標準の各項目を網羅している場合は，網羅性を確保することができる．

2.3 セキュリティ標準を意識したセキュリティ評価に関する研究

NECの芦野らによって政府機関統一基準[25]，PCI DSSなどを評価軸に用いたITシステムのシステム設計に関する研究が行われている[16][26]．この研究は，我々の目的とする認証取得を目的としたものではない．また，評価に用いるベースのデータとして，標準の内容をナレッジ化する必要がある．しかし，このナレッジ化には，専門的な知識が必要となり，事前のデータ準備が不可欠となる．

我々の研究では，標準の生データと特徴情報のみを使用するので，システムを動かすために，専門的な知識やその知識を用いた事前の準備が必要とならない．

2.4 複数標準を用いた統合型システムセキュリティ設計に関する研究

日立製作所の諸橋らによってISO/IEC 15408とISO/IEC 27001:2005とを併用した統合型システムセキュリティ設計技法の提案がなされている[27]．この研究では，専門的な知識を有するセキュリティの専門家によって双方のセキュリティ機能要件と管理策のマッピングテーブルが作成される．

我々が提案する，基準の項目間の相関を取り関連情報を作成する手法では，専門的な知識を有するセキュリティの専門家は必要とせずシンプルな手法で，マッピングテーブルに該当するデータを作成することができる．

2.5 日本ネットワークセキュリティ協会の取り組み

NPO 日本ネットワークセキュリティ協会の配下の標準化部会の情報セキュティ対策マップ WG は，2009 年度に発足し，ISO/IEC 27001:2005 をはじめ多くのセキュリティ標準よりセキュリティ対策を収集し，対策の構造化を行いツリー化，モデル化を行っている．この WG での対策収集の過程でそれぞれのセキュリティ標準で記述される用語が違ったり，細かい表現が違ったり，粒度（抽象度）が違ったり，色々なものが混ざっていたりしていることが指摘されている．その後の活動として，対策の正規化，原子化を行っている[6]．これらは，今後作成される標準には有効であるが，現在の標準に適応するのは難し

い.

我々が提案する, 関連情報作成手法は既存の標準同士でも相関を取ることで異なる標準で同じ対策を求める項目を抽出することができる. また, 対策の正規化, 原子化が行われた標準が作られるようになれば, 我々の手法の精度が向上すると推測される.

第3章 セキュリティ評価プラットフォーム

3.1 プラットフォームの構成

提案するセキュリティ評価プラットフォームは，データ入力部，データ管理部，スコア計算部の 3 つの部分にわかれている．本プラットフォームの構成を図 6 に示す．データ入力部で，標準の生データと，構造情報，参照情報，対応策情報および関連情報の入力をする．データ管理部では，入力された標準の生データと構造情報に基づき整理し，参照情報を用いて参照関係の展開を行い，参照ツリーの構成をする．また，入力された対応策情報を用いて,サンプルデータの作成も行う．そして，対応策情報と関連情報を組み合わせることで，データ移行のためのサンプルデータの作成も行う．さらに，スコア計算部で計算された評価値(スコアデータ)の管理もする．そして，データ管理部で作成されたサンプル情報を提示して，データ入力部での対応策情報入力のサポートを行うことができる．スコア計算部では，参照ツリーに基づく参照情報と登録された対応策の施策情報に基づき，評価値計算を行い，データ管理部に計算をしたデータを渡す．なお，それぞれの機能の詳細については後述する．

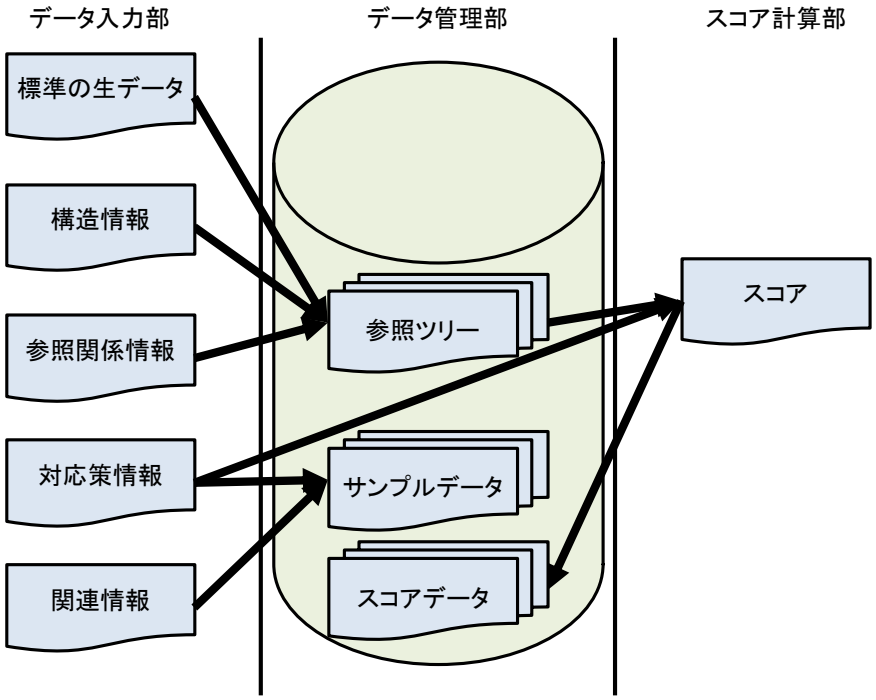


図 6　提案プラットフォームの構成

Figure 6　Structure of proposed platform

3.1.1 プラットフォームのシステム構成

本プラットフォームは，Visual Basic を用いてシステム開発を行った．まずプラットフォーム全体をひとつのプログラムとして構成し，基準のデータとなる項目の基本データ，階層構造と参照関係の情報を用いて参照ツリーを構成するための情報を作る部分，実際に参照ツリーを表示させる部分，対応策の状況を整理する部分，評価値計算を行う部分をそれぞれ独立したプログラムとして構築している．本プラットフォームのプログラム構成図を図 7 に示す．

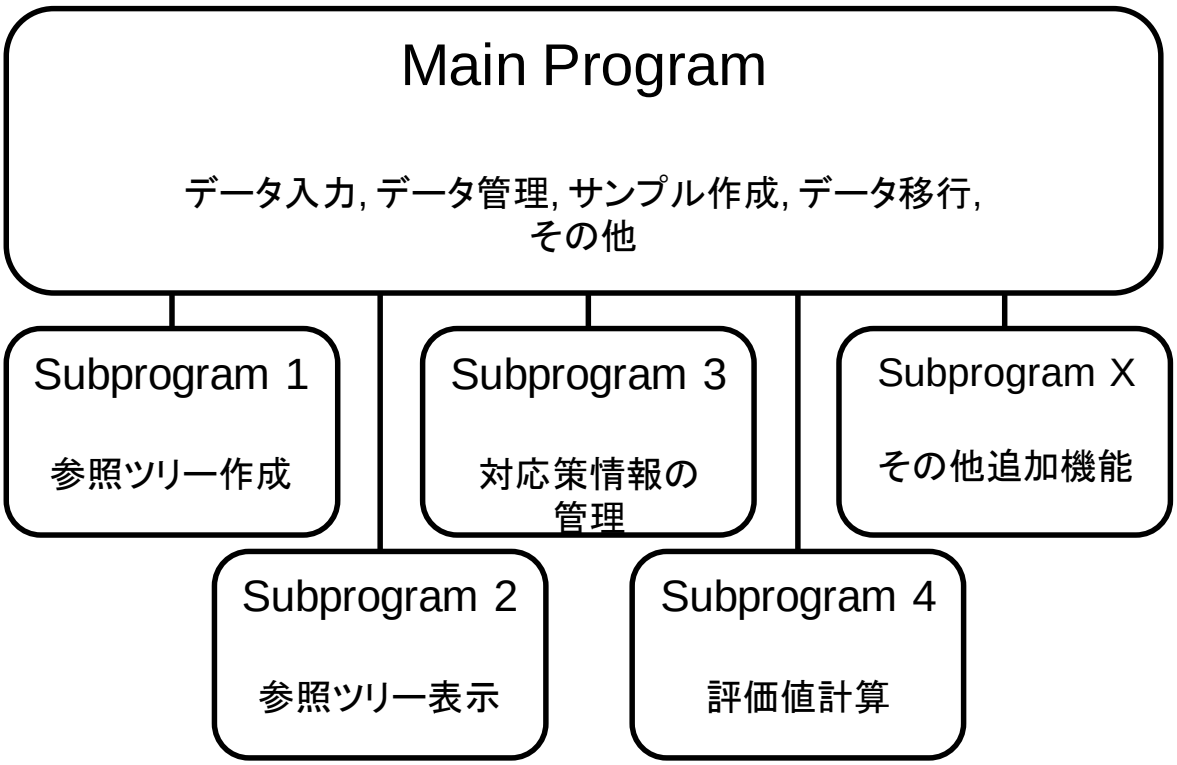


図 7　プログラム構成図

Figure 7　Program configuration diagram

これらの部分は，それぞれ担当する処理をバックグラウンドで行うことによってシステムの稼働を円滑に行えるようになっている．例えば，最初にデータ登録を行った際やデータの変更を行った際に行われる基準全体の参照関係の変更をバックグラウンドで行うことによって，変更中であっても過去のデータの閲覧をすることが可能となる．また，参照ツリ

一の表示，対応策の状況の変更や評価値計算といった処理に時間がかかる部分を独立したプログラムとして稼働させることによって，プラットフォームの本体は常に稼働させることができるようになっている．それとは別に，評価値計算の部分を独立させることにより，複数の評価値計算方法を導入する(または試す)際にその部分のみを入れ替えることによって，スムーズに新しい評価値計算方法に変更することが可能となっている．同様に，参照ツリー表示の部分も，使用者に要望に合わせたプログラムに差し替えてより，使用者の好みに合った表示プログラムを導入することができるようになっている．

3.2 各種機能の動作

データ入力部には，データ入力機能があり，データ管理部ではデータ管理機能，参照ツリー作成機能，参照ツリー表示機能，サンプルデータ作成/提示機能，対応策情報管理機能，データ移行機能があり，スコア計算部には評価地計算機能がある．

3.2.1 データ入力機能

データ入力部の基本機能であるデータ入力機能では以下のデータを入力データとして用いている．

(1) 基準となる標準の生データ
(2) 基準となる標準の構成情報
(3) 基準となる標準の参照情報
(4) 評価対象となる組織の対応策情報
(5) 標準同士の関連を示す関連情報

1 つめの入力データである基準となる標準の生データとは，項目ごとの項目番号，項目名，詳細記述といった基準のドキュメントに書かれている情報そのものとなる．

2 つめの基準となる標準の構成情報とは，項目番号に基づく項目間の関係性を示す情報となる．例えば，先の図 4 で示した ISO/IEC 27001:2005 の例では，「4 情報セキュリティマネジメント」の下には「4.1 一般要求事項」，「4.2 ISMS の確立及び運用管理」，「4.3 文書化に関する要求事項」といった項目が続くといった情報となる．本プラットフォームでは，このような階層をレベルと定義し，最上位の項目をレベル 1 とし，次の階

層をレベル 2 といった形でナンバリングしていく.

3 つめの基準となる標準の参照情報とは, 基準のドキュメント内に直接記述されている参照を示す情報となる. 例えば, 1.2.4 項で説明した「7.1 一般」の項目には(4.3.3 参照)というように参照先が記述されている. 本研究では, このようにドキュメントに直接記述がある参照情報を直接参照と定義する. 構成情報の上位項目が等しいレベル m の項目はレベル m+1 の項目を参照しているとみなす. 本研究では, このような階層構造も参照関係の一部であるように定義することとする. そして, 登録に用いる参照情報は, この直接参照のみを登録し, 参照先に更に参照先がある場合はデータ管理部の処理で自動的に登録データが作成される. また, 複数の基準(標準)が登録されていてその基準同士に関連があり, それぞれの基準のどの項目とどの項目が同じ観点で対策を必要としているかを示している関連情報が提示されている場合はその情報も登録する. ここまでの 3 種類の情報は新しい基準を登録する際に基本となる情報の組となる.

4 つめの評価対象となる組織の対応策情報とは, まず組織で実施している(または実施を予定している)対応策を登録し, その対応策が評価の基準となる標準のどの項目に対する対応策であるのかを示す情報となる. 対応策名, 詳細, 対応状況といったデータからなる情報となり, この情報は様々な情報を作成する元データとなる. 作成される情報とは以下に示す情報となる. まずは, 登録された対応策情報のみで作成される情報としてサンプル情報がある. この情報は, 他の案件でも該当する対応策が, どの項目に対して有効であるのかを示す情報となる. そして, 参照ツリーの構成情報・参照情報と組み合わせてスコア計算部で評価値を出すもとのデータにもなる.

5 つめの標準同士の関連を示す関連情報とは, 基準 X, 基準 Y と二つの基準があった場合にそれぞれの基準の各項目が相手のどの項目と同じ意味(役割)を持つ項目となるのかを示す情報となる. しかし, こういった情報はあまり多く存在しないため未知の基準の組み合わせでも関連情報を導き出す手法を提案している. この情報と 4 つめの対応策情報を組み合わせることで, 異なる基準での対応策をサンプルとして別の基準で提示できるようにしている.

この機能では, これらのデータを入力するためのインターフェースの提供と, データ管理部へ受け渡すためのデータ作成を行う.

3.2.2 データ管理機能

データ管理部のデータ管理機能は，データ入力部からの入力データを各種機能に受け渡す役割を担っている．

データ表示を行う各種機能に対して必要な情報の受け渡しをしたり，入力されたデータから管理用の ID の発行をしたり，データ更新中に様々な処理の受付を一時的に停止したりする．

3.2.3 参照ツリー作成機能

参照ツリー作成機能では，登録された情報に基づき参照ツリーを作成する．直接参照の記述がある項目（以下，参照親という）を根とし，記述されている参照すべき項目（以下，参照先という）を葉とするツリーを構成し，基本ツリーとする．基本ツリーの葉となっている項目が別の基本ツリーの根となっている場合に，図 8 で示すように，前者の葉の部分に後者の根を結合して新たなツリーを構成する．また，構成していく中で，ツリーの根からみて同じ項目を参照先として持つ場合がある．この重複する参照関係は，図 9 で示すような複数箇所で同一項目を参照先として持つ複数参照と，図 10 で示すようなツリーを構成する際にループが発生してしまうループ参照がある．これらの参照が発生した場合には，その重複が確認された部分を葉として確定させ，ツリーの構成を続けるものとする．このようにツリーの結合を繰り返していき，それ以上結合ができなくなるまで結合を繰り返した最大のツリーを参照ツリーとする．

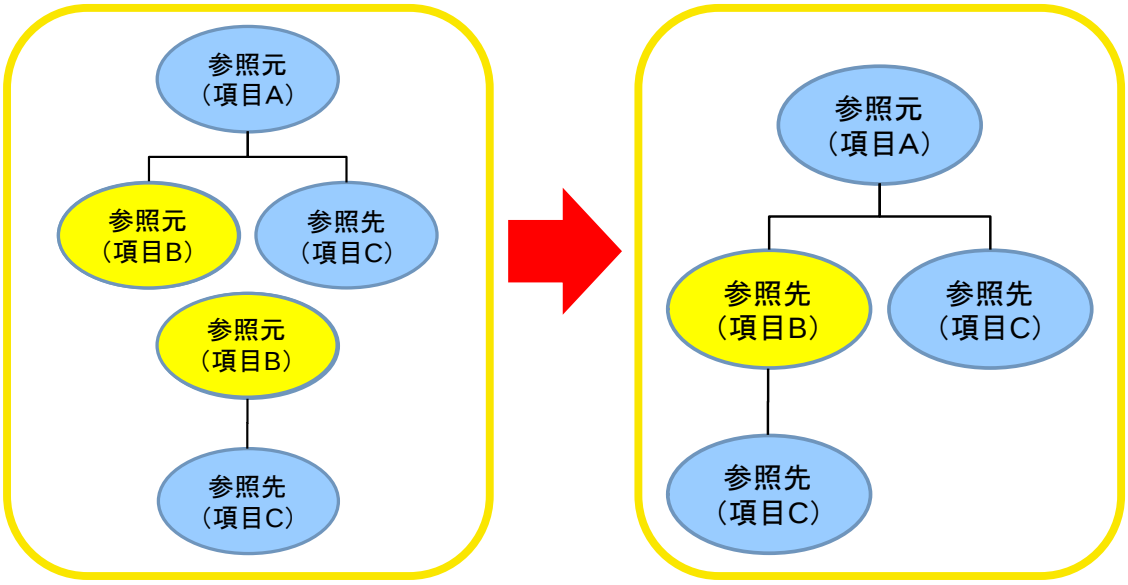


図 8　参照ツリー作成例

Figure 8　Sample of reference tree

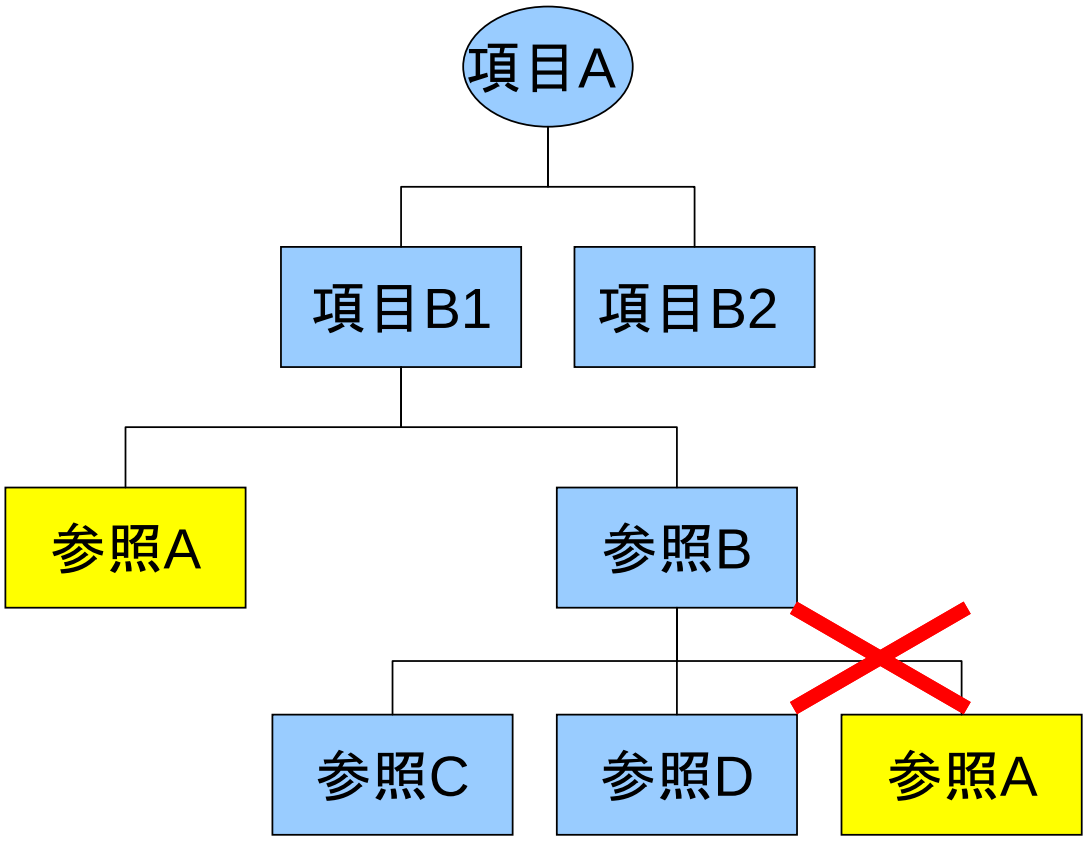


図 9　複数参照の例

Figure 9　Sample of multiple reference

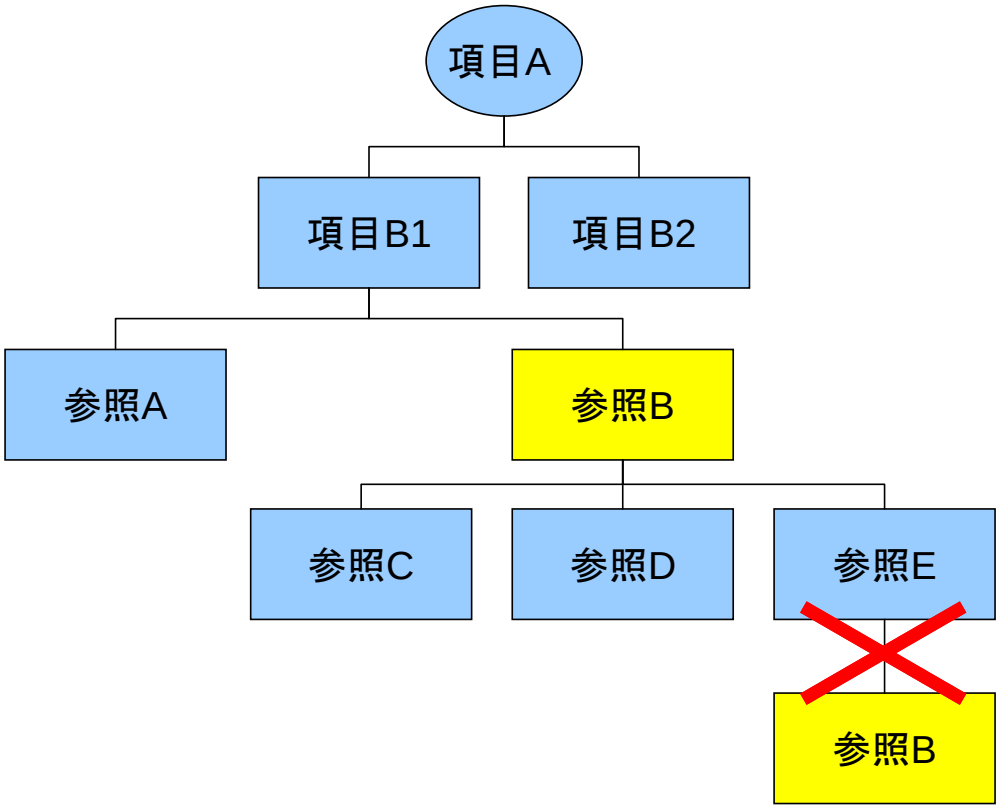


図 10　ループ参照の例

Figure 10　Sample of loop reference

参照ツリーでは項目間の関係を距離として表現し，直接参照されているものを距離 1 とし，以下参照を繰り返すたびに距離を加えていき要素間の距離とする．こうしてすべての項目について参照ツリーを作成し，標準データの管理およびスコア計算部へ評価値算出のための元データを提供する．この機能は 3.1.1 項で示したようにメインプログラムから独立したサブプログラムとして作成されている．なぜなら基準の規模が大きくなったり，参照情報が莫大な量となったりするとその他の動作に支障が出る可能性があるからである．

3.2.4 参照ツリー表示機能

参照ツリー表示機能では，2.2.3 項で作成した参照ツリーの構成情報を用いて実際に参照ツリーをプラットフォームのユーザに提示する．この機能は 2.1.1 項で示したようにメインプログラムから独立したサブプロラムとして作成されている．なぜならば参照ツリー作成機能と同様に規模や情報量が多くなるとその他の作業に支障が出る可能性が合ったり，ユーザが用途や嗜好に合わせてカスタマイズ可能としたりするためである．

3.2.5 サンプルデータ作成/提示機能

サンプルデータ作成/提示機能では，サンプルデータを提供する設定をしている場合に限り対応策と各項目の対応状況の情報のうち対応済となっているデータをサンプルデータとして別途保存する．サンプルデータは，それ以後該当する対応策について他のユーザ（または案件）で対応状況の入力を行う際に提示されるデータとなる．提示されたデータを参考にしながらデータ入力部で入力作業をすることで，ユーザの知識不足に対するサポートが可能となる．対応済として登録されているデータのみをサンプルとする理由としては，以下のような事態を想定しているため対応済みの情報のみをサンプル化することとしている．評価対象としている組織が違った場合に，該当する対応策の効果があったり，なかったりと違ってくる場合もある．また，サンプル数が多くなった場合に，同じ対応策について対応済と未対応といったように，逆の状態のサンプルが提示されてしまう可能性がある．このような場合に，ユーザをうまくサポートすることができず反って混乱させてしまう可能性があると予想される．

3.2.6 対応策情報管理機能

対応策情報管理機能では，データ入力部で入力された対応策情報の管理を行っている．具体的には評価対象組織ごとに基準全体でどこまでカバーできているかといったリストを作成したり，参照ツリーを表示させる時に項目ごとの対応の有無を表示するための情報を作成したり，サンプル提示機能で提示することができるサンプルの設定をしたりする機能となる．

このようにリストを作成することで，組織内のセキュリティ基準がまだ設けられていない場合などには，対応済みリストに基づいて組織内のローカル基準を作成するためのサポート

することができる.

3.2.7 データ移行機能

データ移行機能では, 複数の基準となる標準が登録されていてかつその標準間の関連情報が登録されている場合に, 基準同士の対応策の情報を共有する機能である. サンプル提示機能と連動しており, データ移行機能を用いてデータ移行を行ったデータは, サンプル形式で蓄積保存されるようになっている. 単純にサンプル提示機能を用いて作成されたサンプルとの違いとしては, データ移行機能を用いて作成するデータについては, 対応済のステータス以外のすべてのステータスについてもサンプルとして保存蓄積するというものがある. なぜならば評価対象組織にとってすでに詳細な対応策の情報として登録されている情報なのですべてがサンプルとして有効であると判断することができるからである. このように有効であるとの判断をすることができるが, 標準間の関連が明示されている場合でも, 項目同士が同じ意味合いであるが条件が厳しくなっていたり, 逆にゆるくなっていたりする場合がある. 例えば, 前の基準で効果があると見越して効果が得られなかった場合に, 新しい基準では十分効果があると判別できるケースや, 前の基準で十分な効果を発揮していても新しい基準では十分な効果がない場合などがあるため, データ移行を行った際に, 一度人の目でチェックを行うことが重要となってくる.

このデータ移行機能で使用する標準間の関連情報は, それほど多く公開されているものではない, しかしこのデータ移行機能を使うためには, 関連情報が必要なため, 基準の項目間の相関から関連情報を作成する手法を提案する.

3.2.8 評価値計算機能

スコア計算部の評価値計算機能では, 参照ツリーの構成要素数および 3.2.3 項で述べた距離に着目し各構成要素の参照ツリーの参照親に対する影響度を変更するセキュリティ評価方式を用いて評価値計算を行う. 本論文では以下に示す 4 つの方式を提案してその比較を行った.

（方式 1）構成要素のみに着目した評価方式

対応策有，対応中，未対応といった各状態に対する評価値 $Score$ は，評価をする項目を根とする参照ツリーの構成要素数 n を分母として，i 番目の構成要素 x_i とし，x_i は評価項目に該当する場合は 1 となり，該当しない場合は 0 として総和を分子にとり算出する．以上の計算で，構成要素のうち実際に評価項目に該当している割合を示している．評価値 $Score_1$ を(1)式に示す．

$$Score_1 = \frac{\sum_{i=1}^{n} x_i}{n} \tag{1}$$

（方式 2）最大距離依存型評価方式

評価をする項目を根とする参照ツリーの各構成要素の i 番目の距離を d_i，最大距離 d_{max}，構成要素数を n，i 番目の構成要素 x_i とし，x_i は評価項目に該当している場合は 1 となり，該当しない場合は 0 とする．これらを用いて，距離 1 の項目の影響度を d_{max} とし，以下距離が増加するごとに 1 ずつ影響度を下げていき，その総和を分母として，対応済項目の影響度の総和を分子として評価値を算出する．評価値 $Score_2$ を(2)式に示す．

$$Score_2 = \frac{\sum_{i=1}^{n} \{x_i (d_{\max} - d_i + 1)\}}{\sum_{i=1}^{n} (d_{\max} - d_i + 1)} \tag{2}$$

この方式では参照ツリーの最大距離によって影響度の変化に違いはあるが各構成要素の評価度への影響度が距離に応じて単調減少の形で決定される． 図 11 で示すように参照ツリーの最大距離が大きくなれば距離が近い項目間の影響度の差分が小さくなり，小さくなれば距離が近い項目間の影響度の差が大きくなる．また，この方式では影響度は緩やかに落ちていく．これは，評価値に対する影響度が徐々に落ちていく概念を想定している．

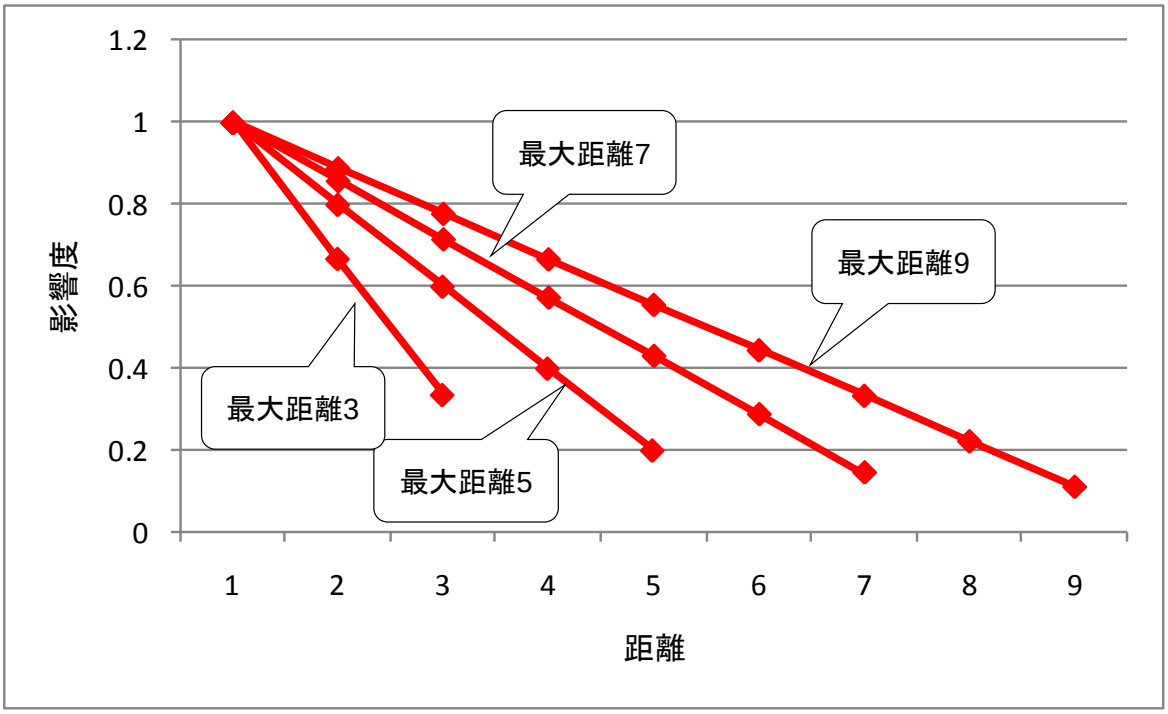


図 11　方式 2 の影響度推移

Figure 11　Degree-of-incidence transition of the type 2

(方式 3)距離の逆数型評価方式

参照ツリーを構成する各構成要素と根との距離を使用する算出方式で，距離の逆数の総和を分母として，対応済構成要素の距離の逆数の総和を分子として評価値を算出する．評値価 $Score_3$を(3)式に示す．

$$Score_3 = \frac{\sum_{i=1}^{n} \frac{x_i}{d_i}}{\sum_{i=1}^{n} \frac{1}{d_i}} \tag{3}$$

この方式では各構成要素の影響度は参照ツリーの最大距離に影響を受けず，純粋に距離によってのみ影響度が決定する．そして，図 4 で示すように，距離が小さいうちに大きく影響度が落ち，距離が大きくなるに従って影響度は緩やかに落ちて行くようになる．しかし，距離が小さいうちに影響度が急激に落ちるのは直接的な要素に対する要素の重要度が下がっているともとることができこの方式のデメリットともなり得るものである．これ

は，評価値に対する影響度が一気に落ち徐々に影響度の差がなくなっていく概念を想定している．

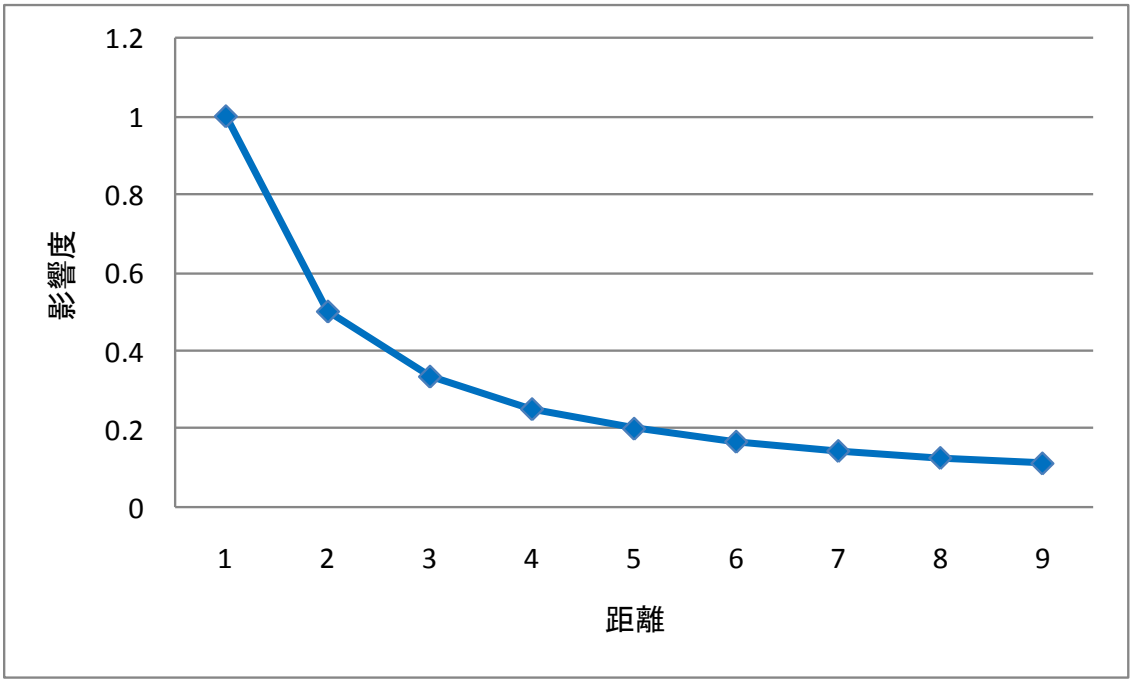


図 12　方式 3 の影響度推移

Figure 12 Degree-of-incidence transition of the type 3

(方式 4)参照ツリーの構成要素の性質によって影響度を変える方式

各構成要素と評価項目の章が異なるという基準で影響度に変化を加えることによって評価値を改善試みるために，評価項目と構成要素の章が同じ場合に方式 2 を，章が異なる場合に方式 3 を採用する方式を方式 4 として提案するものである．その例を図 13 に示す．

この方式 4 では階層構造に代表される評価項目と構成要素の章が同じ場合はゆるやかに影響度が低下していき，参照構造に代表される章が異なる場合は距離に応じて急激に影響度が低下していく様を表現している．また，参照構造でも近しい概念を参照している場合には影響度が比較的高く算出されるという特徴もある．

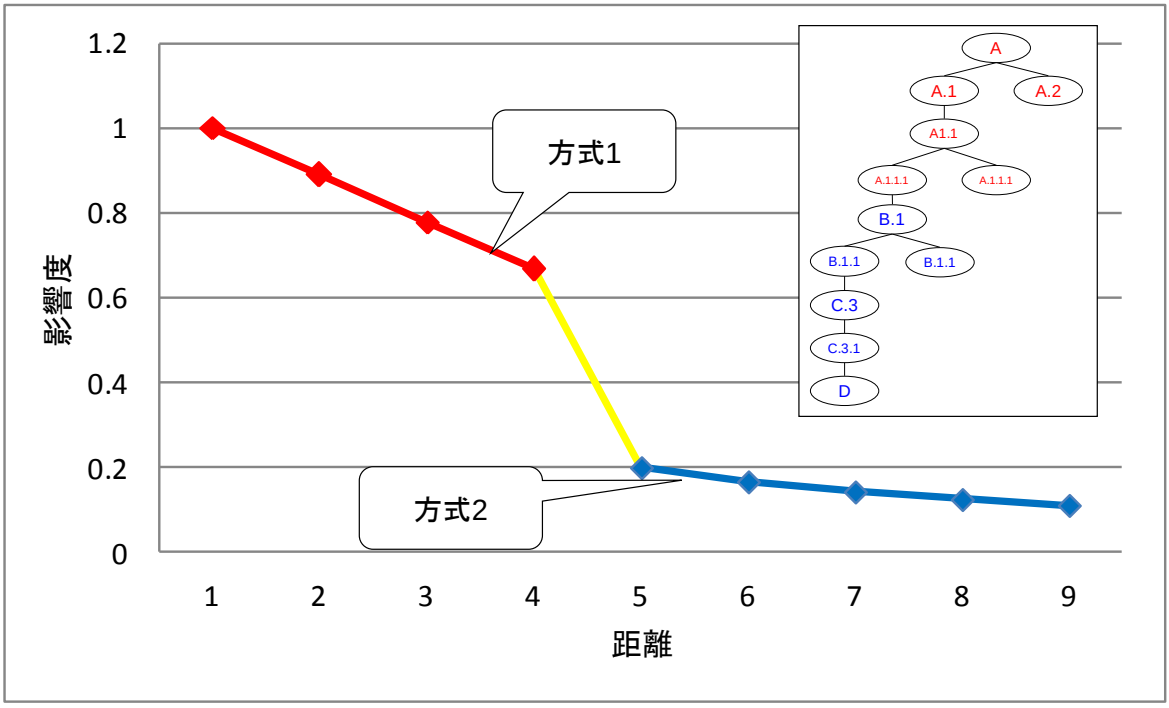


図 13　方式 4 の影響度推移の例

Figure 13 Sample of degree-of-incidence transition of the type 4

3.3 項目間の相関を用いた関連情報作成について

本プラットフォームでは，データ移行機能を使用する際に基準間の関連情報を事前に準備する必要がある．しかし，データ移行を行いたい基準間の関連情報が存在するとは限らない．そういった課題を解決するために本研究では，基準となる標準の項目間の相関を取り，その情報から関連情報を作成する手法を提案している．まずは，その手法のひとつとして，自然言語処理の分野で活用されているテキスト間の近似度算出手法を応用するものを提案した．

3.3.1 項目間の相関を取得

本論文で用いている手法は，文書間の近似をはかり，その近似より双方の基準から見て最も近似が高いものを相関があると定義している．

今回の提案手法では，文書の分類や検索に関する研究において，多数の提案がなされている文書間の近似度を算出する手法を用いている．その手法とは，自然言語処

理と呼ばれる，文書の内容情報を形式化するために，言語表現からその意味を抽出する処理を行い，形式化された内容情報から文書の内容を近似するものである[28].

まず，近似度算出の対象となる文書を確定し，そのテキスト情報を決定する．次に，決定されたテキスト情報を、奈良先端科学技術大学院大学で開発された「茶筌」[29]などを用いて，形態素解析[28]により形態素に分割する．そして，分割した語から，文書の内容を表す形態素や名詞などの単位で，索引語を抽出する．続いて，文書を特徴付ける上で，あまり役に立たない語を，不要語として削除する．さらに，抽出した索引語がその文書の内容にどれだけ密接に関係しているかを，索引語の重要度として付与するために，重み付けを行う．重み付け手法としては，文書中に出現する索引語の頻度を示す，索引語頻度（TF（Term Frequency））や他の文書中の索引語の分布を考慮した，IDF（Inverse Document Frequency），それらを組み合わせた TFIDF がよく用いられる[28]．最後に，重みによりベクトルや行列で表わされた文書間の近似度を算出する．

こうして近似度出した後に，双方の基準から見て最も近似が高いと判断される項目の組が一致した場合に相関があると定義し，相関がある項目の組を見分して関連情報であるか否かを判断するものとなる．後述する実験では，すでに関連情報が定義されている基準の組合せについて，相関から関連情報を作成する実験を行ったため，相関のある項目の組を見分する手法に関することは考察にとどまっている．

3.3.2 応用例

本論文で行った実験は，異なる標準を用いて評価する際に，すでに評価を行った標準の対応策の状況のデータを活用したい，といった要求を想定している．3.3.1 項で述べたテキスト間近似度を算出する手法は，コンピュータを教育に応用する「e ラーニング」のうち，特に Web ブラウザやインターネット上の情報やシステムを利用する WBT（Web Based Training）のコンテンツに関する研究の中で，同一の知識に関する問題を類似問題群としてまとめる技術として，すでに使われている手法を元にしている[30][31]．この文献[31]でいう類似問題群とは，それぞれの問題間のテキスト近似度を用いて同一の専門知識を問う問題の集合を指している．本論文では，それぞれの基準で同一の対応策を求める要件を示す項目を判別する技術として，テキスト間の近似度を用いて相関を

取る手法に応用いる.

したがって, 応用例としては以下のものがあげられる.

- 基準となる標準が更新された場合に, 旧い版と異なる章や新たにまとめられた章に移った項目の抽出.
- 社内基準などのローカルな基準を作成する際に, 国際標準などのグローバルな基準を元にしている場合に, どの程度元となる標準の内容を反映できているのか, 抜け漏れが発生していないかの確認.
- すでに社内基準が設けられていて, セキュリティ認証取得を目指すといった時に, 現状の基準であればどの程度取得を目指す標準に近い基準を満たしているのかの確認.

このような応用をすることによって, これから新たに定義されていく標準にセキュリティに関する項目を加える際には, 元からある標準の項目と照らし合わせて, 要求条件が等しい項目を見つけることができる. そして, 新規の標準を定義する際に, すでに定義されている目的を同じくする標準との親和性を, 確かめることが可能となる.

第4章 各種機能に対する評価実験

提案するプラットフォームにおける各種機能についてそれぞれの機能が目的解決のための要件を満たしているかを評価するための実験を行った. 以下は機能ごとに行った実験付いて述べ, その結果の考察を行ったものである.

4.1 実験 1 : データ入力, 参照ツリーの作成/提示機能に関する実験

実際の標準データの登録および参照ツリーの作成/提示を行ってその動作および効果の確認を行うことを目的とする.

4.1.1 実験概要

まず, 基本データの登録から始まるデータ入力の一連のデータ登録処理を行う. 次に, その登録データを用いて参照ツリーの作成, 提示を行い対応策情報などの追加登録までの処理の確認を行う. また, 対応策情報を登録する際に参照ツリーを見ながら登録ができるのでその効果の検証も行う[32].

4.1.2 実験環境

今回一連の処理を行った基準は国際標準の ISO/IEC 27001:2005, ISO/IEC 27001:2013, ISO/IEC 27002:2005. そして, その附属書の ISO/IEC 27001:2005 附属書 A, ISO/IEC 27001:2013 附属書 A, 国内標準の附属書の ISMS 認証基準 Ver.2.0 附属書「詳細管理策」, PCI DSS v2.0 要件およびテスト手順を選択した.

4.1.3 実験の流れ

最初に基本データの登録を行い, 続いて構成情報, 参照情報の登録を行う. この時点で次の参照ツリーの作成が可能となるため登録処理は一時中断して参照ツリーの作成を開始する. 参照ツリーの作成が完了した後に残りの対応策情報および関連情報の登録を行った. その内, 対応策情報を登録する際には参照ツリーを見ながら入力が行うことができるので参照ツリーを見ながら対応策情報の登録処理を行った.

4.1.4 実験結果

実際に ISO/IEC 27001:2005, ISO/IEC 27001:2013, ISO/IEC 27002:2005, ISO/IEC 27001:2005 附属書 A, ISO/IEC 27001:2013 附属書 A, ISMS 認証基準 Ver.2.0 附属書「詳細管理策」, PCI DSS v2.0 要件およびテスト手順のデータを入力データとして登録を行った. ただし, セキュリティ評価の対象にならない用語の定義などに該当する章についての入力は対象外とした.

項目のデータの登録が終わったら次にそれぞれの項目に関する構成情報と参照情報の登録を行った. この登録の際に構成情報として扱う階層に関する情報は下位の項目は上位の項目から参照をされているという形で登録をした. 同様に直接参照に関する登録を実施した.

中でも複雑な構成をとる国際標準の ISO/IEC 27001:2005 では最大距離は 14, 総参照関係数 4533, ISO/IEC 27002:2005 では最大距離は 32, 総参照関係数 159,169 という数値が参照ツリーの作成によって確認された. このことから標準類のみで参照関係を的確に掌握することが困難であることが数値的にも明らからになった.

それぞれの基準の初期データの登録が完了した後に, 参照ツリーの作成を行った. そして, 実際に参照ツリーを表示させて正しく木構造を作成できているかの確認を行った. その後参照情報の削除, 訂正といった処理を行いその都度正しい木構造が作られているかの確認も行った.

次に, 対応策情報の登録を行った. 登録処理をする時に参照ツリーを表示させながら登録することで項目間の関係性を見ながら登録を行うことができ, 細かい条件などの見落としがないか, 該当する対応策で想定したいた他にカバーできる項目がないかの確認ができることが確認できた.

また, 4 種類の基準(ISO/IEC 27001, ISO/IEC 27002, ISMS Ver.2.0, PCI DSS)で 8 種類(ISO/IEC 27001:2005 の 4 種類と PCI DSS の 2 種類)のデータでの登録実験を行い, いずれも正しく参照ツリーの作成や項目管理を行うことができたことより, 同様の特徴情報を持つ標準類で使用できることを示すことができた.

4.2 実験 2：評価値計算に関する実験

3.2.8 項で述べた方式 1～4 を用いて参照ツリーの構成要素数および距離に着目し各構成要素に重み付けをするセキュリティ評価方式を用いて評価値の比較を行った[33][34][35].

4.2.1 実験概要

最初にセキュリティ認証に関する知識を十分に有している評価者に組織のセキュリティ評価を行ってもらいその達成度を管理分野ごとに表にまとめた. 次に方式 1～3 を用いて同じセキュリティ対策の状況における評価を行い, 被験者の感覚とプラットフォームによる評価値との比較を行った. そして, そこから得られた知見に基づき方式 4 を用いて値の改善ができるかの検証を行った.

4.2.2 実験環境

この実験は, 以下の条件のもと実施した.

- 被験者
  - 情報セキュリティ業務経験有
  - セキュリティ認証に関する知識有
- 対象組織
  - セキュリティ認証取得を目標とした組織
- 情報取得を行ったタイミング
  - ギャップ分析を行う前の段階
- 使用した評価基準
  - ISO/IEC 27001:2005
- 評価する管理分野
  - 4. 情報セキュリティマネジメント
  - 5. 経営陣の責任
  - 6. ISMS の内部監査

- 7. ISMS のマネジメントレビュー
- 8. ISMS の改善

- 対応策の状況選択方法
  - 要求事項に対しての対応策で対応済または未対応の二者択一

具体的な実験の時点は，被験者であるセキュリティ担当者が，資産の洗い出しを終えて現状分析を始めて，セキュリティ認証取得のためのISMSマニュアルに盛り込む内容と実際の組織の状況を照らし合わせて，ギャップ分析を実施している状態となる．ヒアリングを行った組織は，ISO/IEC 27001:2005 のセキュリティ認証（ISMS 認証）を取得することを目的とした組織であり，この組織は過去にセキュリティ認証を取得したことがなく，今回初めてセキュリティ認証の取得を目指している．この実験ではデータ作成の簡素化のために対応中の対応策については，その状況でよりどちらに近いかで対応済か未対応のいずれかを選択してもらった．

4.2.3 実験の流れ

（手順 1）基準値の作成

最初に，評価基準に対して本システムで計算した値と比較する時に基準とすべき評価値を定める．基準値は人の感覚で決めていくため，すべて 10%刻みとした．まず，対象組織に対してセキュリティ対応策の施策状況のヒアリングを行い，そのヒアリングの結果を基に感覚的に判断した現状の達成度を決定する．この達成度を「基準値」とする．

（手順 2）方式 1，2，3，4 を用いた評価値の計算

本システムを用いて，実際に対応策がどの項目の内容についてカバーすることができているのか順次入力をしていく．そして，その入力データを基に，本システム上で評価値を算出する．

（手順 3）評価値の比較 1

最初に基準値と方式 1，2，3 を比較してそれぞれの管理分野の対応策の施工状況と

方式の評価値との関係を調査する.

(手順 4)評価値の比較 2

基準値と方式 2, 3, 4 を比較し方式 3 を採用することによって評価値が改善されていることを確認する.

4.2.4 実験結果

(手順 1) 基準値の作成

現状のヒアリングの後に, 状況を基準(この場合は ISO/IEC 27001:2005)の内容に沿って整理をして, 基準値を決定してもらった. 認証取得に対して, 意欲的に取り組む姿勢を示しているが, 現状ではまだ認証取得のための活動を開始したばかりということもあり, 基準値は表 1 のようになり, 全体的に達成度が低く, 6. 以降の項目については, PDCA サイクルの構築がなされていないため達成度が 0%であるとの判断で値の決定が行われたものである.

表 1 基準値

Table 1 Standard value

管理分野	基準値
4. 情報セキュリティマネジメント	20%
5. 経営陣の責任	50%
6. ISMSの内部監査	0%
7. ISMSのマネジメントレビュー	0%
8. ISMSの改善	0%

(手順 2)方式 1, 2, 3, 4 を用いた評価値の計算

手順 1 で取得したセキュリティ対策の状況を本システムに入力を行い方式 1, 2, 3, 4 のそれぞれの方式で評価値の計算を行った. それぞれの方式によって得られた評価値を評価値 1, 2, 3, 4 とし, その結果は表 2 で示す通りである.

表 2　各方式における評価値

Table 2　Evaluation value in an all directions type

管理分野	基準値	評価値1	評価値2	評価値3	評価値4
4. 情報セキュリティマネジメント	20%	12.75%	12.82%	11.14%	13.98%
5. 経営陣の責任	50%	13.84%	12.94%	14.91%	18.06%
6. ISMSの内部監査	0%	12.77%	9.63%	8.87%	4.91%
7. ISMSのマネジメントレビュー	0%	0.00%	0.00%	0.00%	0.00%
8. ISMSの改善	0%	11.92%	7.27%	6.64%	1.84%

(手順 3)評価値の比較 1

まず, 基準値と評価値 1, 2, 3との比較を行いそれぞれの管理分野でどの方式が最も基準値に近い値を示すのかを基準値から各評価値に差分を取りそれぞれを差分 1, 2, 3 として調べた結果表 3 のような結果となった. 差分の絶対値が低いものほど基準値に近く有効であると言えるので, 方式 1 が最も有効となった管理分野は「4.情報セキュリティマネジメント」となり, その管理分野内の項目の対応が進んでいて, 方式 2 が最も有効となった管理分野は「5.経営陣の責任, 6.ISMS の内部監査, 8.ISMS の改善」となり, その管理分野内の項目ではなく参照先の項目の対応が進んでいるという結果になった. 方式 1, 2, 3 のどれも全ての管理分野で最も有効であるという結果を得ることができなかった.

表 3　方式 1,2,3 の差分

Table 3　Differences of proposed type 1,2,3

管理分野	基準値	方式1	方式2	方式3
4. 情報セキュリティマネジメント	20%	−8.68%	**−8.08%**	−9.55%
5. 経営陣の責任	50%	−36.76%	−39.21%	**−36.64%**
6. ISMSの内部監査	0%	13.24%	10.34%	**10.14%**
7. ISMSのマネジメントレビュー	0%	0.00%	0.00%	0.00%
8. ISMSの改善	0%	13.24%	8.78%	**8.59%**

(手順 4)評価値の比較 2

次に, 手順 3 で方式 2, 3 の単独で評価値を算出する限界が見えたためそれぞれの特徴を活かした形で項目の影響度を算出する方式として方式 4 を採用して手順 3 と同様に基準値との差分を取り差分 4 として差分 2, 3 との比較を行った結果表 4 のような

結果となりすべての管理分野で値の改善がみられた.

表 4　方式 2,3,4 の差分

Table 4　Differences of proposed type 2,3,4

管理分野	基準値	方式2	方式3	方式4
4. 情報セキュリティマネジメント	20%	−8.08%	−9.55%	***−6.02%***
5. 経営陣の責任	50%	−39.21%	−36.64%	***−31.94%***
6. ISMSの内部監査	0%	10.34%	10.14%	***4.91%***
7. ISMSのマネジメントレビュー	0%	0.00%	0.00%	0.00%
8. ISMSの改善	0%	8.78%	8.59%	***1.84%***

4.3 実験 3：サンプル提示機能に関する実験

4.3.1 実験概要

セキュリティ認証に関する知識を十分に有していない管理者に対して，サンプルデータの提示を行うことによって，対応策と標準の各項目を対応付ける作業を行ってもらい．サンプルを提示することで作業のサポートをできるのかを調査した[35].

4.3.2 実験環境

この実験ではロールプレイ実験の形をとり，それぞれの状況は以下に示す通りである.

- サンプルデータ作成者
  - セキュリティ認証に関する知識有
  - 一般セキュリティ業務経験有
- 被験者
  - 本学の大学院生
  - セキュリティ認証に関する知識は不十分
- 対象組織
  - 被験者の所属する研究室
- フェーズ
  - 対応策の抽出が終わった現状分析段階

- 使用した評価基準
  - ISO/IEC 27001:2005
- 評価する管理分野
  - 4. 情報セキュリティマネジメント
  - 5. 経営陣の責任
  - 6. ISMS の内部監査
  - 7. ISMS のマネジメントレビュー
  - 8. ISMS の改善
- 対応策の状況選択方法
  - 要求事項に対しての対応策が対応済または未対応の二者択一

サンプルデータの作成をセキュリティ認証に関する知識があり，一般セキュリティ業務経験がある筆者が行い，セキュリティに関する一般知識はあるが，セキュリティ認証に関する知識は不十分である本学の大学院生に対応策と標準の各項目の対応付け作業を行ってもらった．対象となる組織は被験者が所属する本学の研究室を対象として，対応策の抽出が終わって現状分析を行う段階であると仮定した．評価基準を ISO/IEC 27001:2005とし，4. 情報セキュリティマネジメント以下 8. ISMS の改善までの全項目を対象として対応策の状況選択を行ってもらった．被験者が学生であるため詳細の判断が難しいので，申請中，および現在進行形で対応しているものもすべて対応済という扱いにし，「対応済」「未対応」の二者択一の選択で行った．

また，対応策を選択する段階で認証を意識して対策選定が行われていないため，標準の項目を意識して対応策を立てているわけではない，という前提でデータを作成および取得していることも被験者に伝えている．対応済，未対応とは，標準に明記されている要求事項に対する対応が定まっているか否かで判断している．

4.3.3 実験の流れ

(手順 1)サンプルデータの作成

被験者の所属する研究室のセキュリティを含むシステム全般の管理者に対して現状

のセキュリティ対策全般のヒアリングを実施，文書などについては内容，保管体制を含めて確認を行う．ヒアリング結果を元にシステムにデータ入力を行いサンプルデータの作成を行う．

(手順 2)被験者による対応策の分析 1

手順 1 のヒアリング結果で抽出された対応策についてシステムを用いずに標準の文書のみを用いて対応策と標準の各項目の対応付け作業を行う．

(手順 3)被験者による対応策の分析 2

手順 2 と同じ作業を今度はシステムを用いて行う．ただし，手順 3 の段階ではサンプルの提示は行わず参照ツリーの情報のみを用いて判断をする．ここで作成したデータもサンプルデータとして取得を行う．

(手順 4)被験者による対応策の分析 3

手順 3 と同じ作業を今度はサンプルの提示を追加した形で行う．

(手順 5)被験者へのヒアリング

被験者に対して，手順ごとにどのような判断基準で対応策と標準の各項目の対応付けを行ったのか，またその際に結果に変化があったものの根拠がなんであったのかをヒアリングを行う．

4.3.4 実験結果

(手順 1)サンプルデータの作成

管理者にヒアリングを行って，現在施行されている管理策の中から今回の評価基準に対応しているセキュリティに関するものを選び出し，それぞれの管理策について評価基準に対する対応付けを行い，システムに入力を行ってサンプルデータの作成を行った．

(手順 2)被験者による対応策の分析 1

すでに管理者に対してのヒアリングは終了している状態であるため手順 1 の中で選び出した管理策に対して標準の項目に対する対応付けを手作業で行った. 被験者のセキュリティ認証に関する知識は十分であるとは言えないので, 管理策に対するイメージにあった項目を中心に対応付けする結果となった. そのため, それぞれの管理策がかなり多くの項目に対して有効であるとの回答が作成された.

(手順 3)被験者による対応策の分析 2

手順 2 で行った作業についてシステムを用いることによって参照ツリーによる参照関係の情報を閲覧しつつ同様の作業を行った. 参照ツリーを見ながら作業を行ったことにより, 各管理策について主な項目に対する関連性の低い項目を未対応に見直された回答が作成された.

(手順 4)被験者による対応策の分析 3

手順 3 と同じ作業を, サンプルデータを表示した形でもう一度行ってもらった. この時に表示したサンプルは手順 1 で作成したデータと手順 3 で被験者によって作成されたデータの 2 つを区別できる形で表示して作業にあたった. その結果, さらに管理策に対応していると判断された項目の絞り込みが行われた回答となった.

(手順 5)被験者へのヒアリング

手順 2～4 について被験者について判断基準, 結果の変化の理由についてヒアリングを行った結果, システムを使うことにより項目間の関係性の整理を行うことができたこと, サンプルの提示によって自信をもって項目を選択できたことという解答を得られた. また, サンプルにないデータを残した部分については実際の現場にて感じた感覚を信頼して残しているという解答も得られた.

4.4 実験 4：データ移行機能に関する実験

4.4.1 実験概要

各対応策の状況を『ISO/IEC 27001:2005 附属書 A』と『ISMS 認証基準 Ver.2.0 附属書「詳細管理策」』の二つの視点から対応策の状況と対応付けして実際にデータ移行を行い，それぞれの基準で各対応策の移行されたデータの状況を調べた[36].

4.4.2 情報取得環境

今回の実験では，本学研究室における対応策の状況を各基準に基づき対応付け作業を行った．該当作業は研究室のおける管理責任者を務める学生によって進めたものである．

4.4.3 実験の流れ

はじめに，『ISO/IEC 27001:2005 附属書 A』の内容を確認しながら該当する対応策の洗い出し及び状況の対応付けを実施．次に先の工程で洗い出しを行った対応策について，『ISMS 認証基準 Ver.2.0 附属書「詳細管理策」』を基準として再度状況の対応付けを実施．最後に双方のデータを本プラットフォームのデータ移行機能を使用してデータ変換を行って状況の比較を行うといった流れで実施した．

4.4.4 実験結果

20 件程度の対応策に対して，対応関係がある項目同時で異なる結果を示したものはのべ 120 項目強の項目となった．選択内容が正反対になったもの，片側だけ選択されていたものなどすべてのパターンが発生していた．そして，異なった状況を示した項目の内容を比較し状況の分析を行った結果，以下の 6 種類に分類することができた．

(1) 項目の内容が詳細に明記された．

(2) 項目の内容が曖昧になった．

(3) 項目の上位の項目の内容が異なるため同じ内容でも指し示すものが異なる．

(4)　（指している内容は変わらないが）表現の違いがある.

(5)　同じ内容のことを別の角度から示している.

(6)　双方の基準で同じ管理分野内に配置されていない.

4.5 実験 5：項目間の相関関係に基づく関連情報抽出実験その 1

すでに標準間の関連情報が明示されている『ISO/IEC 27001:2005 附属書 A』(以下, 基準 A という)と『ISMS 認証基準 Ver.2.0 附属書「詳細管理策」』(以下, 基準 B という)の 2 つの評価基準を用いて, 各項目間の近似度を算出する. 算出した近似度は 0～1 の値を取る. 近似度が両方の基準からみて同時に最大値をとるものを相関がある項目の組と定義する. 相関がある項目の組となったものが, 明示されている関係をどの程度再現できているのかを調べる. そして, 再現できたものを OK, 再現できなかったもののうち,「関連付けがあるのに抽出されなかった」ものを FN(False Negative),「関連付けがないのに抽出された」ものを FP(False Positive),「間違った項目を抽出した」ものを NG(No Good)としてそれぞれについて詳細の分析考察を行った[37][38][39].

この 2 つの基準を選んだ理由としては, ISO/IEC 27001:2005 のドキュメントの附録として対比表(以下, 元データという)が公開されていること. そして, 国際的なセキュリティマネジメントの基準である ISO/IEC 27001:2005 とその日本の国内版となる ISMS 認証基準 Ver.2.0 を用いることで, 3.3.2 項の応用例にもあるように, 国際標準と広い意味でのローカル標準としての国内標準の比較が, 実際に可能であるということを示すことも目的としている. また, 具体的な対策に踏み込んだ附属書を使うことで, 定義などの表現がブレ難いものではなく, 表現の幅がある内容同士を比較することができ, より適切に有効性を示すことを目的としている. 以下に続く関連情報抽出実験は, この実験を準備実験と位置付けて追加実験を行ったものとなるので前提を省略する.

4.5.1 実験概要

すでに標準間の関連情報が明示されている二つの基準を用いて, 相関のある項目の組の抽出を行い, 明示されている関連情報がどの程度再現できるのかを検証した.

4.5.2 実験環境

実験では，すでに関連情報が明示されている『ISO/IEC 27001:2005 附属書 A』(以下，基準 A)と『ISMS 認証基準 Ver.2.0 附属書「詳細管理策」』(以下，基準 B)の二つを用いて相関のある項目の組の抽出を行った．実験で相関がある項目の組を検出するために用いる手法としては，テキスト間近似度を求める手法のうち最もシンプルな手法を用いて実験を行った．

4.5.3 実験の流れ

(手順 1)各基準の専門用語の抽出および重みづけ

基準 A, B において，「章・節・項」(以下，大項目・中項目・小項目)に含まれる文書間の近似度を算出するためにまず，専門用語抽出システム[40]により，大項目それぞれに含まれる専門用語を抽出する．次に，抽出されたすべての語に対して重み付けを行う．中項目と小項目についても同様の専門用語抽出と重みづけを行う．

(手順 2)近似度の算出

手順 1 で作成した各基準のデータを余弦[28]により，基準間の近似度を算出する．手順 1 と同様に中項目と小項目についても同様の作業を行う．

(手順 3)相関がある項目の抽出

まず基準 A の各項目から見た基準 B で近似度最大の項目を抽出する．続いて基準 B でも同様に各項目から見た近似度最大の項目を抽出する．抽出された項目がどちらから見ても一致しているもののみを相関がある項目の組としてピックアップする．

(手順 4)元データとの比較

手順 3 で抽出した相関がある項目の組が，明示されている関連情報とどこまで一致しているのかを確認する．再現率は(4)式で示す「正しく抽出された相関がある項目の組数」を「関連情報の組数」で割ったものとして算出する．確からしさは(5)式で示す「正しく抽出された相関がある項目の組数」を「相関がある項目の組数」で割ったものとして算出

する.

$$再現率 = \frac{正しく抽出された相関がある項目の組数}{関連情報の組数} \tag{4}$$

$$確からしさ = \frac{正しく抽出された相関がある項目の組数}{抽出させた相関がある項目の組数} \tag{5}$$

(手順 5)エラー項目の分析

FP, FN, NG となった項目の組すべてにおいてその原因分析を実施する.

4.5.4 実験結果

(手順 1)各基準の専門用語の抽出および重みづけ

今回の実験で用いた基準 A,B は共に大項目以外は項目名と詳細記述となっていたので, 項目名と詳細記述をひとまとめとして専門用語の抽出および重みづけを行った. 重みづけについては, 今回の実験では, 最も単純な手法とするため 2 進重みを適用している. これは, 抽出されたすべての語に対して重み 1 を付与する.

(手順 2)近似度の算出

手順 1 で作成したデータを用いて, 大項目は大項目, 中項目は中項目, 小項目は小項目同士で, 各項目総当たりで近似度の算出を行った.

(手順 3)相関がある項目の抽出

基準 A の項目から見て基準 B で近似度最大となる項目でかつ, 基準 B から見た時も基準 A の元の項目が近似度最大となる項目の抽出を行った結果は表 5 で示すように, 大項目で 8, 中項目で 28, 小項目で 97 件のデータが「相関がある項目の組」となった.

表 5　相関がある項目の組数

Table 5　Number of items with relation

	全項目数		相関がある項目の組数
	基準A	基準B	
大項目	10	10	8
中項目	39	36	28
小項目	133	127	97

(手順 4)元データとの比較

手順 3 で相関がある項目の組を基準 A と B の関連情報と比較を行った結果は

表 6 で示すようになり，大項目，中項目，小項目の全てで 80%を超える再現率を示し，確からしさはいずれも 89%を超える高い値を示す結果となった．

表 6　相関がある項目の組の再現率と確からしさ

Table 6　Recall and probability of an item with relation

	関連がある項目の組数	相関がある項目の組数	OK	FN	FP	NG	再現率	確からしさ
大項目	10	8	8	2	0	0	80.00%	100.00%
中項目	31	28	25	5	2	1	80.65%	89.29%
小項目	116	97	95	19	0	2	81.90%	97.94%

実験の結果，人の作業では見落としが発生しやすい組についても正しく抽出することができた．図 14 は基準 B で基準 A とは別の節に移動した項目の組で実際に抽出した組の例である．

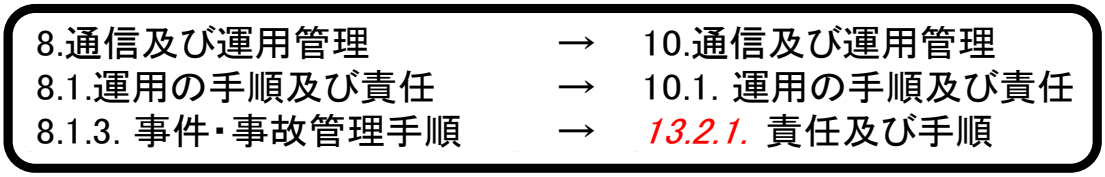


図 14　正しく抽出した組の例

Figure 14　Example of combination extracted correctly

(手順 5)エラー項目の分析

FN 26 件，FP 2 件，NG 3 件それぞれの組合せについてエラー発生の原因を究明するべく基準 A,B の両方から見た各項目への近似度，各項目の文言を詳細に確認した．その結果エラーを出している項目のほとんどが低い近似度を示していることがわかった．

大項目，中項目，小項目のそれぞれを見ると文章量の少ない大項目では手順 1 における専門用語の抽出時点でより適切な判断をすることができれば，FN のうち 1 つが正しい組み合わせで導くことができ，もう一方の FN なった項目の組についても近似語を正しく判別できていれば正しい組み合わせで導くことができたことがわかった．中項目では FP，NG として検出された 3 つの組合せはいずれも近似度が 0.5 を下回る結果となっており低い値を取っている．また，図 15 で示した NG となった項目の組は，項目名だけであれば近似度 1となり完全一致しているが詳細記述の部分を合わせることで近似度が低下しているという結果になった．図 16 で示した FP となった組というのは，文章的には非常によく似ているが上位概念で近似度が低いといったように責任範囲が異なっているものであった．FN となっている組合せについては NG の時のように項目名が一致または高い近似度を示しているケースもあるが，基準 A，B のどちらから見ても最大近似度が低く片側から見たら最大であるがもう一方から見ると次点や次々点の値を取り僅差で検出できなかったケースと全体的に近似度が低くすべての組合せで 0.5 を下回っているといったケースに分類することができた．

項番	項目名	詳細記述		項番	項目名	詳細記述
9.3.	利用者の責任	情報システムへのアクセス権が、適切に認可され、割当てられ、維持されていることを確実にするため。	NG →	11.2.	利用者アクセスの管理	情報システムへの、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。
			OK →	11.3.	利用者の責任	認可されていない利用者のアクセス、並びに情報及び情報処理設備の損傷又は盗難を防止するため。

図 15　NG となった組の例

Figure 15　Example of combination extracted NG

図 16　FP となった組の例

Figure 16　Example of combination extracted FP

小項目については FP となる組合せは現れなかった. が, NG の組合せが 2 つありその両方が片側から見たら最大の近似度を示しもう一方から見るとそれぞれ次点, 次々点の近似度を取っているものであった. FN となる組合せは 19 組と比較的多く検出されたが一部の組合せを除けば中項目の時と同じ 2 つのケースに分類することができた.

以上の分析結果より以下の知見を得ることができた.

(1) 近似度の最大値が 0.5 を下回るような低い値を示す項目は相関がある項目の組がないことが多い
(2) 記述形式が項目名と詳細記述と分かれている場合は項目名の方の近似度がより重要となってくる
(3) 双方からの近似度最大が同じ項目をささず相関がある項目の組がないと判断された場合は近似度上位の項目を含めて検討すると相関がある項目の組を検出できる場合が多くある

4.6 実験 6：項目間の相関関係に基づく関連情報抽出実験その 2

4.6.1 実験概要

4.5 節の実験 5 をベースとして複数の手法を用いて相関がある項目の組の抽出を行い, 再現度が改善できるのか検証を行った. 今回は各専門用語に対する重み付けにつ

いて，各専門用語に重み付けを行いその重み付けの違いによって相関がある項目の組にどのような差異が生まれるかを確認した．また，この実験では，作成したデータを専門的な知識が十分ではないユーザに提示することを目的としているため，NG および FP の抑制を優先的し FN の抑制は考えていない．

4.6.2 実験環境

この実験では，項目名と詳細記述にわかれる基準について，それぞれの専門用語数に着目をした重み付けを行う．これによって相関がある項目の組がどのように変わるのかを確認し，どのような重み付けが有効であるかの検証を行う．

4.6.3 重み付けについて

基準の各項目が「項目名」と「詳細記述」というように記述が分かれている場合に「項目名」の近似度が「詳細記述」の近似度より関連を示す場合に重要である可能性が高いという仮定（以下，仮定 1）と，専門用語が多い方がより重要な内容をしているのではないかという仮定（以下，仮定 2）に基づき専門語抽出を行った後に各専門用語に重み付けを行って精度の向上を図るものである．

この実験では以下の 5 つの方法で重み付けを行いその結果の比較検討を行う．

（方式 1）全ての専門用語に一律の重みをつける

方式 1 では今回の基準となる値とするため実験 5 と同じく全ての専門用語に一律 1 の重みを与える．

（方式 2）標準全体の専門用語数を用いる場合

専門語抽出を行って形態素ごとに分けた際に各項目で「項目名」と「詳細記述」に分けてその専門用語数をカウントする（それぞれ Cnt.name, Cnt.detail とする）．その総合計を「項目名」と「詳細記述」のそれぞれで算出する（それぞれ Sum.cnt.name, Sum.cnt.detail とする）．

ここで，方式 2 をさらに 2 つの方式に分割し，方式 2A と方式 2B を検討した．方式 2A では仮定 1 に基づき，式(6)で示すように各専門用語に対して項目名は項目名の総

計で，詳細記述は詳細記述の総計で割ってそれぞれの専門用語の重みとする．

$$\text{項目名の重み} = \frac{1}{\text{Sum.cnt.name}} \cdot \text{詳細記述の重み} = \frac{1}{\text{Sum.cnt.detail}} \quad (6)$$

そして，仮定 2 に基づいて重み付けを行うために，方式 2B では，式(7)で示すように方式 2A とは逆に，項目名の各専門用語を Sum.cnt.detail で，詳細記述の各専門用語を Sum.cnt.name で割って重み付けをする．

$$\text{項目名の重み} = \frac{1}{\text{Sum.cnt.detail}} \cdot \text{詳細記述の重み} = \frac{1}{\text{Sum.cnt.name}} \quad (7)$$

この方式のメリットは，各項目で専門用語数の偏りが合っても平均して各専門用語に重み付けができることであり，デメリットとしては，各項目の文章量の特徴が反映されないということである．

(方式 3)項目ごとの専門用語数を用いる場合

方式 2 の際に算出した Cnt.name と Cnt.detail を用いて項目ごとに異なる専門用語の重み付けを行い，方式 2 と同様に，方式 3A と方式 3B を検討したものである．

その内，方式 3A は，方式 2A と同様に仮定 1 に基づく重み付けを行うため，式(8)で示すように，各専門用語に対して項目名は Cnt.name で，詳細記述は Cnt.detail で割ってそれぞれの専門用語の重みとする．

$$\text{項目名の重み} = \frac{1}{\text{cnt.name}} \cdot \text{詳細記述の重み} = \frac{1}{\text{cnt.detail}} \quad (8)$$

一方，方式 3B では，方式 2B と同様に仮定 2 に基づく重み付けを行うために式(9)で示すように，方式 3A と逆の要素で割り重み付けを行う．

$$\text{項目名の重み} = \frac{1}{\text{cnt.detail}} \cdot \text{詳細記述の重み} = \frac{1}{\text{cnt.name}} \quad (9)$$

この方式のメリットは，項目ごとの文章量の特徴を反映することができるということであり，デメリットは，専門用語数に偏りがあった場合にその影響を大きく受けてしまうということである．

4.6.4 実験の流れ

(手順 1)各基準の専門用語の抽出

基準 A, B において，大・中・小項目の文書間の近似度を算出するためにまず，専門用語を抽出する．ただし今回実験の対象となるのは提案している手法で重み付けを変えることができる中項目と小項目のみとなる．そのため大項目については今回の実験の対象外とする．また，各項目の専門用語数をカウントしておく．

(手順 2)各専門用語への重み付け

抽出されたすべての語に対して，4.6.3 項で述べた 5 つの方法を用いて重み付けを行う．

(手順 3)近似度の算出

手順 2 で作成した各基準のデータを余弦により異なる基準間における近似度を算出する．作業は手順 1 と同様に中項目と小項目についてのみ行う．

(手順 4)関連がある項目の抽出

まず基準 A の各項目から見た近似度最大の項目を抽出する．続いて基準 B でも同様に各項目から見た近似度最大の項目を抽出する．抽出された項目がどちらから見ても一致しているもののみを相関がある項目の組としてピックアップする．

(手順 5)元データとの比較

手順 4 で抽出した相関がある項目の組が明示されている関連情報とどこまで一致しているのかを確認する. 再現率は 4.5.3 項の式(4), 確からしさは式(5)を用いて算出する.

(手順 6)エラー項目および差分の分析

FP, FN, NG となった項目すべてにおいてその原因分析を実施する.

そして, 重み付けを変えたことによって差が出た組み合わせについてもその原因分析を行う.

4.6.5 実験結果

(手順 1)各基準の専門用語の抽出

今回の実験で用いた基準 A,B は, 共に大項目以外は項目名と詳細記述となっていたので, 項目名と詳細記述をひとまとめとして専門用語の抽出を行った. その際に項目ごとに専門用語数のカウントを行った. その結果, 基準 A では中項目で 2 項目, 小項目で 5 項目, 基準 B では中項目で 2 項目, 小項目で 3 項目が詳細記述の方が専門用語の数が多くなり, また基準 A では中項目で 7 項目, 小項目で 7 項目, 基準 B では中項目で 6 項目, 小項目で 9 項目が項目名と詳細記述で専門用語数が一致した.

(手順 2)各専門用語への重み付け

各項目の専門用語にそれぞれ重み付けを行う. 重み付けを行う際に項目名と詳細記述の両方で同じ専門用語が出現した際はより高い重み付けを行う方の重み付けを優先して専門用語に重み付けを行った. 方式 1 では先の実験と同様に特別な重み付けを行わず全ての専門用語に同じ重みを与えた. 方式 2A, 2B では Sum.cnt.name と Sum.cnt.detail を用いて重み付けを行ったため項目ごとに重みのバラつきはなく基準ごとに同じ重み付けとなった. 方式 3A, 3B では項目ごとの専門用語数にはバラつきがあったため項目ごとの重み付けにもバラつきが生じた.

(手順 3)近似度の算出

手順 2 で 5 つの方式で重み付けを行ったデータを用いて，中項目は中項目，小項目は小項目同士で，各項目総当たりで近似度の算出を行った．

(手順 4)相関がある項目の抽出

基準 A の項目から見て基準 B で近似度最大となる項目でかつ，基準 B から見た時も基準 A の元の項目が近似度最大となる項目の抽出を行った結果を方式ごとにまとめると表 7 で示すようになった．

表 7　相関がある項目の組数

Table 7　Number of items with relation

	中項目		小項目	
	関連がある項目の組数	相関がある項目の組数	関連がある項目の組数	相関がある項目の組数
方式1	31	28	116	97
方式2A	31	30	116	94
方式2B	31	25	116	73
方式3A	31	24	116	93
方式3B	31	27	116	75

(手順 5)元データとの比較

手順 4 で抽出された項目を基準 A と B の関連情報と比較を行った結果は表 8 および表 9 で示すようになった．

中項目では方式 2A で FN，NG が減少して再現率と確からしさの両方が方式 1 に比べ改善され，方式 3A では NG が減少し FN が増加したが確からしさが改善された．方式 2B と 3B ではエラーが増加し再現率，確からしさが共に方式 1 に比べて低い値となった．小項目では方式 2A のみが方式 1 に比べて確からしさが改善された．しかし FN が増加しているため再現率は低下した．その他の方式ではエラーが増加し再現率，確からしさが方式 1 に比べて低い値となった．

表 8　相関がある項目の組の再現率と確からしさ（中項目）

Table 8　Recall ratio and correctness of an item with relation

	関連がある項目の組数	相関がある項目の組数	OK	FN	FP	NG	再現率	確からしさ
方式1	31	28	25	5	2	1	80.65%	89.29%
方式2A	31	30	28	3	2	0	**90.32%**	**93.33%**
方式2B	31	25	20	10	4	1	64.52%	80.00%
方式3A	31	24	22	9	2	0	70.97%	**91.67%**
方式3B	31	27	24	6	2	1	77.42%	88.89%

表 9　相関がある項目の組の再現率と確からしさ（小項目）

Table 9　Recall ratio and correctness of an item with relation

	関連がある項目の組数	相関がある項目の組数	OK	FN	FP	NG	再現率	確からしさ
方式1	116	97	95	19	0	2	**81.90%**	97.94%
方式2A	116	94	93	22	0	1	80.17%	**98.94%**
方式2B	116	73	66	45	2	5	56.90%	90.41%
方式3A	116	93	90	24	1	2	77.59%	96.77%
方式3B	116	75	68	42	1	6	58.62%	90.67%

(手順 6)エラー項目および差分の分析

中項目においては方式 2A, 3A にて NG の数の減少が見られた. これは NG となった項目の組が項目名の方が詳細記述の部分よりもその特徴を示していたと推察できる. また, すべての方式で FP として検出された項目と, 方式 1, 2A, 2B で共通して FP として検出された項目がそれぞれ 1 つずつあり詳細を調べた結果, 該当する項目に対する大項目および小項目が元データで関連が定義されている項目であることがわかった. 概念自体はかなり近いが枠組として別の枠組となっているケースであるとわかった. そして, 方式 2A, 3A の二つの方式だけで FN となった項目の組について調べた結果その組はその他の組と違って項目名だけで判断するのが難しく詳細記述を読んではじめて組が判別できるような内容となっていた. 方式 3A, 2B のみで FP で検出された項目の組では, 正しい組の項目名と詳細記述では項目名の方の専門用語数が多くなるという想定からはずれている項目の組であることがわかった.

小項目においては, 方式 2A･3A にて方式 1 における FN, NG となる項目を多く正し

い組で検出できていたが，方式 1 で検出できていた組で近似度が低かったものについて FN または NG（方式 3A では FP も含む）のエラーが発生しているために再現度が改善されず，方式 3A については確からしさの改善もされなかった．小項目では，中項目以上に専門用語数の差が大きくその影響が大きかったと推察される．重みに直して比較すると最大値は基準 A で 11 倍，基準 B で 16 倍となった．

4.7 実験 7：項目間の相関関係に基づく関連情報抽出実験その 3

4.7.1 実験概要

4.5 節の実験 5 および 4.6 節の実験 6 を準備実験と位置付け，実験 5 の手法を手法 1，実験 6 の方式 2A を手法 2，それに階層構造に関する情報を用いる手法を加えて同じ標準の組合せで相関がある項目の組の抽出を行った．

4.7.2 実験環境

この実験では，標準の特徴情報である階層情報に着目をした相関を求める手法を加えた比較を行った．これによって相関がある項目の組がどのように変わるのか，また，それぞれの手法の利点がどういった場合にあるのかを確認した．

4.7.3 階層情報を用いた相関を求める手法

この手法は，実験 5 で得られた階層構造の情報を反映させた方が有効である，という知見に基づいた手法である．まず，手法 1 と同じ方法で，各項目間の近似度を算出する．そして，算出した近似度を，標準の階層構造に基づき積算し中項目，小項目の近似度を改めて算出する．例えば，基準 A の中項目 1.1 と基準 B の中項目 2.1 の近似度は，手法 1 で算出された基準 A の大項目 1 と基準 B の大項目 2 の近似度と，基準 A の中項目 1.1 と基準 B の中項目 2.1 の近似度を掛け合わせた値になる．このように，近似度を算出した後は，手法 1 と同様に相関がある項目の組の抽出を行う．

4.7.4 実験の流れ

(手順 1)各基準の専門用語の抽出

基準 A, B において, 大, 中, 小項目の文書間の近似度を算出するためにまず, 専門用語を抽出する. ただし今回実験の対象となるのは提案している手法で重み付けを変えることができる中項目と小項目のみとなる. 手法 1, 2 については, 実験 5, 6 の結果を用いる.

(手順 2)各専門用語への重み付け

手法 3 では, 手法 1 と同じくすべての語に一律 1 の重みを与えるものとする.

(手順 3)近似度の算出

手順 2 で作成した各基準のデータを余弦により異なる基準間における近似度を算出する. 作業は手順 1 と同様に中項目と小項目についてのみ行う.

(手順 4)相関がある項目の抽出

これまでの実験と同様にまず, 基準 A の各項目から見た近似度最大の項目を抽出する. 続いて基準 B でも同様に, 各項目から見た近似度最大の項目を抽出する. 抽出された項目がどちらから見ても一致しているもののみを相関がある項目の組としてピックアップする.

(手順 5)元データとの比較

手順 4 で抽出した相関がある項目の組が明示されている関連情報とどこまで一致しているのかを確認する. 再現率は 4.5.3 項の式(4), 確からしさは式(5)を用いて算出する.

(手順 6)エラー項目および差分の分析

FP, FN, NG となった項目すべてにおいてその原因分析を実施する.

そして, 3 つの手法を比較してそれぞれの手法における相関がある項目の組の差分と, それによってわかる手法の最適な利用法について分析を行う.

4.7.5 実験結果

(手順 4)相関がある項目の抽出

手法 3 では，手法 1 で算出した近似度を使って階層的な近似度を算出する．大項目については，階層の最上位となるため，手法 1 および 2 と同じ結果となった．階層的な近似度を算出した後の相関がある項目の組の抽出，組の分類は実験 5 に準ずる．その結果を表 10，表 11 に示す．

表 10　関連がある項目数（手法 3）

Table 10　Number of items with relation

	全項目数		抽出した項目の組数
	基準A	基準B	
大項目	10	10	8
中項目	39	36	25
小項目	133	127	93

表 11　関連がある項目の再現率と確からしさ（手法 3）

Table 11　Recall and probability of an item with relation

	関連がある項目の組数	抽出した項目の組数	OK	FN	FP	NG	再現率	確からしさ
大項目	10	8	8	2	0	0	80.00%	100.00%
中項目	31	25	23	7	1	1	74.19%	92.00%
小項目	116	93	90	23	0	3	77.59%	96.77%

(手順 6)エラー項目および差分の分析

手法 1，2，3 の結果を比較すると，大項目については，項目名と詳細記述に分かれているわけでもなく，更に上位の概念がないことから差が生じない．したがって中小項目のみが比較対象となるため，分類結果を項目レベル毎の表にまとめると表 12，表 13 に示すようになる．

表 12　関連がある項目の再現率と確からしさ（中項目）

Table 12　Recall and probability of an item with relation

	関連がある項目の組数	抽出した項目の組数	OK	FN	FP	NG	再現率	確からしさ
手法1	31	28	25	5	2	1	80.65%	89.29%
手法2	31	30	28	3	2	0	90.32%	93.33%
手法3	31	25	23	7	1	1	74.19%	92.00%

表 13　関連がある項目の再現率と確からしさ（小項目）

Table 13　Recall and probability of an item with relation

	関連がある項目の組数	抽出した項目の組数	OK	FN	FP	NG	再現率	確からしさ
手法1	116	97	95	19	0	2	81.90%	97.94%
手法2	116	94	93	22	0	1	80.17%	98.94%
手法3	116	93	90	23	0	3	77.59%	96.77%

関連情報を作成する際には，FP とNG の二つのエラーが発生し，かつそれを間違った組であると認識できないことが一番の問題となるので，手法 2 が総合的に良い結果を出すことができたといえる．

中項目に関しては，手法 2，3 が手法 1 よりも高い確からしさを示すことができていることから，それぞれの手法を使用する適切な場面があることが伺える．手法 1，2 の FP となる項目の組は，2 つとも同じであるが，手法 3 では発生していない．これは，文言的には大変似ているが関連がない項目で，階層構造を理解していないと判断が難しいケースといえる．また手法 1，3 の NG となる項目の組は同じであるが，手法 2 では正しい項目の組を抽出している．こちらの場合も，文言的に似ているということに変わりは無いが，詳細記述の表記内容によって誤った組を抽出してしまっているものとなる．今回の基準の組合せでは，正しい組で項目名が一致していたため，人の目によるチェックで回避することができるエラーであるといえる．

小項目については，FP となる項目の組は現れなかった．NG となる項目の組については，手法 1，2，3 でどの組み合わせでも共通の項目の組はなかった．手法 2 が数としては1 組と最も少なかったが，近似度は0.470 とNG となった組の中では比較的高く，手法 3 が数としては 3 組と最も多かったが 0.258～0.094 と他の手法に比べて非常に

低い値を示した. それぞれの項目の組を視認すると近似度が低いことからもわかるように関連がないことが, 比較的容易に判別できる組となっていた.

4.8 実験の考察

4.8.1 実験 1 について

この実験では提案プラットフォームの発想の元となった ISO/IEC 27001:2005 だけでなく, ISO/IEC 27002:2005 のような階層構造と参照関係に基づくデータ整理を行うことができる標準については, プラットフォームの基本データとして使用できるということがわかった. 実際に ISMS の附属書, PCI DSS の要件及びテスト手順についても登録および参照ツリーの作成ができたことにより, その他の標準をデータとして使用できる可能性について示すことができた.

4.8.2 実験 2 について

この実験を通してセキュリティ評価を行い際の評価者の思考の方向性として本プラットフォームで整理した参照ツリーの概念でいうところの距離が遠いものや管理分野外の参照先についてその管理分野の達成度における影響度が低くなるということがわかった. また潜在的に影響がある管理分野外の参照先となる項目の影響を見落としてしまうというヒューマンエラーの防止に参照ツリーの概念を用いた評価値の算出方式が有効であるということがわかった.

また, 実験の結果を提示して行ったヒアリングの中で方式を変えることで「5.経営者の責任」についても評価値の改善はみられた. しかし被験者の評価値と差は未だ大きい. この原因については評価基準として将来性を評価に加えたり, 実際の評価項目外の内容を結果に反映させたりする場合があり今回のケースでは認証取得を目指す初期段階であったこともあり将来性に関する追加点が入っていたことがわかった.

4.8.3 実験 3 について

手順 2 の結果より専門的な知識を十分に有していない場合はより多くの項目について対応していると判断する傾向が見て取れた. 手順 2 から 3 に移った際の被験者のヒアリ

ング結果から標準の複雑な関係性について知識を十分に有しているとは言えない担当者が理解をすることが困難であるということが確認することができ，こういった問題に対して参照ツリーを構成し項目間の関係性を視覚的に表現することが有効であると考察できた．手順 3 から 4 に変わった際のヒアリング結果からサンプルデータを表示することによって知識が十分に有しているとは言えない担当者はサンプルデータを参考にしてさらに情報を絞りこんでいって最終的に残った項目と関係性が明確でかつ自分の知識だけでは選択されていなかった項目についての対応を追加していることがわかった．

以上の考察結果から項目間の関係性を明示することでより的確な判断をする手助けとなることがわかった．さらにサンプルを提示することによって自信をもって項目を選びその対応策でどういったことを実現しなければならないのかということも学習させることができることがわかった．

4.8.4 実験 4 について

4.4.4 項に示した(1)(2)(3)については表現の幅によって対応状況に変化が出てくる可能性があるので単純にデータを変換するだけではいけないということが見て取れる．また，(4)(5)(6)については被験者の見落としや知識が不十分な時に対応状況を提示することによってエラーを回避することができることが見て取れる．

4.8.5 実験 5 について

今回は比較的内容の近い基準同士を用いたが，テキスト近似度を用いて関連のある項目を抽出することで高い再現度を得ることができることがわかった．とりわけ抽出された項目の確からしさは非常に高い値を示すことがわかった．また，エラーの原因に文言の解析時に適切な範囲で単語が区切られていないというものがあったり，技術用語を多数使用している故に自動で用語同士が同じ意味を指していると判定できずに近似度が下がってしまい抽出できなかったり，といったものがあった．今回近似度の算出にあたりシンプルな方法を用いて近似度の算出を行ったにも関わらず全体を通して高い再現度，確からしさを示すことができた．このことより自然言語処理の分野で使われているテキスト間の近似度算出手法を用いて基準間の近似度を求めて関連がある項目を抽出する手法が

有効であるとわかった. また, 近似度の算出方法を改善することによってより高い再現度, 確からしさが得られると予想される結果となった.

また, サンプル提示を行うためのデータを作成するという性質上 FP, NG といったエラーについては FN の数がある程度増加しても発生を食い止めることが大事であると思われる. 例えば項目名と詳細記述といったように文言が分かれている場合は今回のような重み付けではなく項目名の方が重要視される重みづけを行ったり, 基準が階層構造を取っているので上位の項目(小項目に対する中項目や中項目に対する大項目)の関連の検出の有無や近似度を考慮したりといったことで結果を改良できるのではないかと予想される.

4.8.6 実験 6 について

実験結果より総合的には方式 2A が高い再現率と確からしさを示しており, 専門用語数によって重み付けを変える方式の中では, この方式 2A が有効であると考えられる. 何故ならこの実験で想定していた専門的な知識が十分ではないユーザに対してより確からしさの高いデータを供給できることになり間違った関連情報を使ってしまう危険性を軽減できたといえる. また, 項目名と詳細記述とに分かれて記述されている基準についてそれぞれの専門用語数に基づいて重み付けを行うことで一部のエラーを回避できることがわかった. 加えて, 各項目の特徴をそのまま反映して近似度算出をするよりも基準全体として平均化して重み付けを行った方がより効果的にデータを抽出できることがわかった. しかし, 一部の例外的な記述となっている項目の組については検出することができなかった.

また, 小項目のように全体の文章量が多い場合は複数の算出手法でそれぞれ検出できたりできなかったりする項目の組が発生することがわかった. このような場合は複数の手法, 例えば方式 1 と 2A のように違う視点で重み付けを行った結果を総合的に判断することにより正しい組を導き出すことも有効であると推察される.

そして, 方式 2B, 3B といった文章量(専門用語数)が多いほど重要な記述であるといった仮定で重み付けを行った方式を試したことによりこのような基準同士の近似度を算出する際には専門用語数によって影響が変わるのではなく意味的な要素を含んで重み

付けを行う方が有効であるということがわかった.

4.8.7 実験 7 について

実験 5, 6, 7 と続く項目間の相関関係から関連情報を導く実験では, 比較的内容の近い基準同士を用いたが, 項目間の相関関係を用いて関連のある項目を抽出することで高い再現率を得ることができることがわかった. とりわけ抽出された項目の確からしさは, 非常に高い値を示すことがわかった. このことより, 自然言語処理の分野で使われているテキスト間の近似度算出手法を用いるなどして, 基準間の相関関係から関連がある項目を抽出する手法が有効であるとわかった. また, 相関を求める方法に意味的な解釈を加えることによって, より高い再現率, 確からしさを得ることができた.

今回検証を行った手法の他にも, 各専門用語の使用頻度などを用いる方法など他にも意味的な解釈をする手法があるので, それらを応用することによって結果が変わってくる可能性もある.

手法 1, 2 では, 小項目について基準 A と基準 B で新たな中項目に属するようになった組を正確に抽出することができた. よって, 対象が大きく異なる基準間や基準のメジャーバージョンアップを行った基準の改版チェックを行う際に, 使用すると有効だと思われる. また, 手法 3 は, 今回の手法の中では最も意味的な判定を重視しているものとなるので, 同じような文言を多く使用する基準を使う場合や, 元の基準の構成があまり変化しないマイナーバージョンアップの改版チェック, 新しい基準が元の基準の特定のカテゴリ(本実験でいうところの大項目)をトレースする形で作られている場合などに, 有効だと思われる.

今回の実験で使用した手法 2, 3 で, 同じ項目の組で関連があると判定された組は, すべて正しい組み合わせであった. そのことから, 目的の違う複数の手法を用いて関連情報を作成した場合には, 各手法で異なる結果が出た項目の組, およびすべての手法で同じ項目の組を示さないものには, エラーが含まれる可能性がある. このような組に, 人の手によるチェックを入れることで, より正確な関連情報の抽出を行うことができると推察される.

4.8.8 実験全体を通しての考察

実験 1, 2, 3, 4 で共通して確認できた内容としてはヒューマンエラーの防止に役立っているということがあげられる. それぞれの実験で防止できるエラーに違いがあるがエラーの根本原因として考えられるものは本研究の課題のひとつである基準となる標準類の複雑な構成に起因しているものが多い. 本アプローチでは参照ツリーを用いることで感覚的, 視覚的な対応をして課題解決に寄与している.

具体的には実験 2, 3 における評価漏れについては参照ツリーを用いることで視覚的なサポートを行いエラーの防止に努め, 実験 3, 4 についてはサンプルの提示という形でこちらも視覚的なサポートをしてエラーの防止に努めている.

そして, 実験 5, 6, 7 ではデータ移行機能を更に活用するために, 項目間の相関を取り, 標準間の関連情報を抽出することが有効であることを示すことができた. 相関を求める際に, 標準の特徴や意味的な要素を加えることで, その後の関連情報抽出の精度を上げることができることもわかった.

第5章 結論

5.1 研究結果のまとめ

本論文では，セキュリティ認証取得時の課題となる，多くの標準が存在し，それらを統合的に扱う環境がないといった問題を解決するために，(1)対象となる基準の種類に依存しない，(2)基本となる基準を整理した基本データの入れ替えだけで他の基準と同様にセキュリティ評価が行える，(3)過去のデータを新しい基準に活用できる機能の搭載，(4)セキュリティ評価のための共通の評価値算出方式，といった機能要件を満たすセキュリティ評価プラットフォームの提案をした．

具体的には，セキュリティマネジメントに関する標準の特徴である階層構造と参照関係に着目し，セキュリティ評価プラットフォームの開発を行った．開発したプラットフォームにISO/IEC 27000 シリーズを中心としたデータの登録を実際に行って，参照ツリーを作成した結果，標準類のドキュメントだけですべての参照関係を掌握することが難しく，参照ツリーを用いて視覚的な表現を行うことが有効であることを示すことができた．

ISO/IEC 27001 だけでなく，ISO/IEC 27002，ISO/IEC 27001 附属書 A，ISMS 認証基準 Ver.2.0 附属書「詳細管理策」，PCI DSS v2.0 の要件およびテスト手順といったいくつかの基準を実際に登録して，同じインターフェースでデータの閲覧，管理が実現できることを確認した．すでに登録，運用実験を行った基準はその文章量，項目数，項目の内容も異なる基準である．このことにより特定の基準だけに適用できる訳ではなく同様の特徴を持つ基準であるならば提案するセキュリティ評価プラットフォームが使用できることを示すことができた．

共通の評価値計算方式を提案，検証する実験では，評価をしたい項目に対してカバーすべき項目を掌握するために評価したい項目を根に持つ参照ツリーの各構成要素について評価する評価値計算方式（方式）の提案を行った．その中で単純に参照ツリーを構成する要素数のうち対応できている項目の割合だけに着目すると，専門家によって評価された値に近い値を出すことができないということがわかった．そこで，参照ツリーの距離に着目し，距離によって評価値計算に与える影響度を変える方式を提案し比較検討を行い評価値計算方式の改善に成功した．しかし，新たに提案した二つの方式（方式 2 および 3）単独ではすべての章での改善をすることができなかった．実験結果から，評価

したい項目と参照ツリーの構成要素となる項目の影響度を変えることでよりよい評価できるのではないかという仮定を立て方式 2 と 3 を組み合わせた方式 4 を提案することですべての章での値の改善に成功した. このことより参照ツリーは距離の概念や参照ツリーを提示することで, 評価したい項目への影響の変化を視覚的に表せることがわかった.

また, 実験後に行ったセキュリティ評価を行ってくれた専門家へのヒアリングで, 評価の時に見落としがちな項目の影響を自動的に反映できていることに対する評価と, 実験では評価値を得るための対応策情報の入力をする際に「対応済」、「未対応」といった二択で回答をしてもらっていたのだが, 認証取得を目指している過程や ISMS の運用中といったプラットフォームの使用環境を考えると二択では表現が難しい状況も評価値計算に反映される可能性の指摘があった. そこで実験データの取得終了後にプラットフォームの改修を行い選択肢に第三の選択肢として「対応中」というステータスの追加を行った. そして, すべての選択肢についての評価値を算出するように評価値計算機能の拡充を行ったことでより詳細な評価を提示することができるようになった.

サンプル提示機能に関する実験では, 参照ツリーとサンプルを一緒に提示することによって対応策が基準のどの項目に対して有効であるかを選択していく作業に際して的確な判断をサポートができることが確認できた. 被験者が思い浮かべる組み合わせとサンプルの組が一致している場合にはより自信をもって項目を選択することができるようになったり, 一致していない場合で思い浮かぶ組がサンプルにない場合は本当に効果があるのか否かを再検証してから選択するなど慎重な選択をするようになったり, 逆に想定していない組がサンプルにあった場合にはその組が見落としではないかという検証を行ったりといったような傾向があった.

データ移行機能に関する実験では, 異なる基準に即して各対応策の基準への対応状況を登録する際に発生する見落としや判断ミスといったそれぞれの基準に対する知識の不備により陥りやすい問題について大きな効果が期待できることがわかった. さらに, データをする際に直接データを移行するのではなくサンプルとしてデータの移行をして提示することで表現が細かくなったり, 大まかになったりしたものについての新しい基準での再検討をスムーズに行うことができることがわかった. このことにより, 異なる基準を用いてセキュリティ評価を行う際の再評価が必要となる問題についてこの機能を使用することでサ

ポートすることができた.

標準間の項目同士の相関関係から標準間の関連情報の作成を行い, データ移行機能をより有効活用する実験を行った. 関連情報が明示されている 2 つの基準を用い基準間の各項目同士のテキスト近似度を算出した結果から項目間の相関を求め関連性を示す情報を抽出した. その結果, 高い再現度で, かつ高い確からしさをもつ関連情報を作成できることがわかった. このように関連情報を作成することができればこれまで基準が変わって再評価をしなければいけなかった際のロールバックを軽減することができることがわかった. 同様に基準が更新された場合も同じように関連情報を作成することによって更新によるセキュリティの再評価に対しても高い効果を得られるのではないかということがわかった. また, シンプルな近似度算出手法で高い再現度, 高い確からしさを示すことができた.

近似度を用いて抽出した関連情報の精度をより高めるために, 各項目の専門用語数に着目して重み付けを行う手法の実験を行った. その結果, 項目ごとにその専門用語数に応じた重み付けを行うより全体として平均化した重み付けを行った方が有効であることがわかった. これは項目ごとの専門用語数にバラつきがありそのバラつきによる影響を平均化した値を用いることで吸収できたものと推察できた. また, 近似度を算出する際には意味的な要素を含んだ重み付けが大事であり単純な文章量では判断できないということがわかった. このことから相関関係を用いた関連情報の抽出の精度をあげることでより有効なデータを作成することができることがわかった.

さらに, 標準の特徴情報である階層情報に着目をして, 意味的解釈を加えた相関を求め前述の二つの手法と比較を行って, それぞれの手法のユースケースの分析を行った. それぞれの手法に利点があり, これらの手法を使い分けることによってより的確な関連情報の作成ができることがわかった.

1.3 節で述べた, 課題(1)「セキュリティ認証取得のための共通の枠組みがない」という問題については, 各種実験を通して, セキュリティ評価プラットフォームを構築することで解決することができることを示した. 課題(2)「多くのセキュリティ標準が存在するが、それぞれの関係性を示す情報が不足している」という問題については, 実験 4, 5, 6, 7 を通して, データ移行機能および関連情報作成手法によって解決できることを示した. 課題

(3)「認証ごと，評価者ごとに，評価方法が異なり共通の評価方式がない」という問題については，実験 2 を通して，標準に依存しない共通の評価値算出方式を示すことで解決できることをしめした．

以上のことから，機能要件を満たす各種機能の開発，評価実験により提案するセキュリティ評価プラットフォームは上記の課題を解決できたものと結論付ける．

5.2 今後の展望

5.2.1 対応策の自動取得機能

これまではすべての対応策について，手入力による情報登録を行ってきた．しかし，ネットワークの設定情報を確認する項目や，フロー制御などについて定められた項目であればテストツールなどを用いることにより，自動で判定を行うことが可能であると考えることができる．そういった項目と実際に自動取得した情報とを照らし合わせて本プラットフォームの入力データや汎用性の高いXMLデータを作成することができれば，これまで手入力で行っていた労力を低減して，かつプラットフォームを用いた入力ミスなどのケアレスミスの低減ができる．

コンピュータやネットワークのセキュリティ上の弱点を発見する手法の一つに，ペネトレーションテストという，システムを実際に攻撃して侵入を試みる手法がある[41]．この手法では特に，ネットワーク接続された情報システムが外部からの攻撃に対して安全かどうか，実際に攻撃手法を試しながら安全性の検証を行うものである．また，不正に侵入できるかどうかだけなく，DoS 攻撃にどれくらい耐えられるかを調べたり，侵入された際にそこを踏み台にしてほかのネットワークを攻撃できるかどうかなどを調べたりすることもある．こういったテストを行うことで，セキュリティソフト導入後の設定不備や，新たなセキュリティホールが発見されたることがある．

標準と情報取得可能な情報との組合せを調査して，一部の項目に対する対応策の有無の自動判定を目指す．

5.2.2 サンプル提示機能

サンプル提示機能については，サンプルの収集方法，信頼性といった根本的な課題が存在する．現在この課題については技術的な側面ではなく運用的な側面での解決方法を検討している．収集方法については，サンプルの使用条件としてサンプルを使用して作成したデータはサンプルデータとして提出するルールを提案している．サンプルの信頼性については，サンプルを収集する中央サーバを構築しサーバ側で機械的に信頼性が高いと判断できる基準として同じ対応策について一定件数以上同じ項目に対応していると登録があるものはそのまま採用し，一定数を下回る項目については人の目による確認を行い，その有効性を認めることができたら採用する方式を提案している．

このような方法を用いてサンプルの信頼性を高めることで機能の充実を目指す．

5.2.3 評価値計算方式

現在は提案プラットフォームで作成した参照ツリーの情報を活用した評価値計算方式を採用している．しかし，この計算方式以外にも多くのセキュリティ評価を行う方式が存在する．提案プラットフォームでは対応策と標準の各項目への対応状況の情報をそれらの方式が元データとして使用できる場合には組み込んで使用することができるような構成をとっている．例えば，参照関係に関する情報を現在のシステムでは，ツリー構造で表現しているが，ツリーではなくグラフで表現することによってグラフ理論を応用し，各項目の重み付けをグラフの重要度に応じて決定する手法などが考えられる．

したがってより有効な評価値計算方式を採用することによりさらに正確な評価値計算をすることを目指す．

5.2.4 運用実験

PDCA サイクルのすべてのフェーズでの適用が可能となるプラットフォームを提案しているが，セキュリティ評価の実際の現場の値を入手することは困難であったために，これまでの実験でギャップ分析および現状分析のフェーズでのみ実データを用いた実験を行ってきた．しかしそれ以外にもセキュリティ評価実施するフェーズは多く存在する．その他には，詳細リスク分析を行っている段階や，すでに認証取得を行って，PDCA サイクルをす

でに運用しているといった段階が，セキュリティ評価をするフェーズに該当する．したがって，その他のフェーズでも組織のセキュリティ評価実験を行い，その時点での有効性の検討をすることでさらに提案するプラットフォームの適応範囲が広げることを目指す．

5.2.5 相関関係を用いた関連情報作成

項目名と詳細記述のそれぞれに属する専門用語に対する重み付けを変えることで一定の効果をあげることができた．同様に，セキュリティ標準の持つ特徴情報である階層情報を用いた手法でも一定の効果をあげることができた．しかし，それぞれにメリットがあるものの，これの手法がすべての場合で有効であるという結論にはいたらなかった．今回実験を行った方法の他にも，重み付けを決定する際に，専門用語の出現頻度に着目するといったものなど他のアプローチ方法も存在している．今後は他のアプローチが基準間の相関を求める際に，有効であるかを検討することで更に精度の高い関連情報が作成することを目指す．

重み付けに関する改良の他には，構文解析の段階で用いる辞書をセキュリティ標準に対応したものに入れ替えることが考えられる．このように辞書を定義する際には，標準の文書内で定義されている言葉を事前に集めて，専用の辞書を作ることが有効であると考え有られる．こうしたセキュリティ用語を定義した辞書を作成することは，JNSA の標準化部会の情報セキュリティ対策マップ検討 WG で検討が行われている，正規化，原子化といった動きにも通じており高い有効性が期待される．

また，本論文内の実験では，想定しているユーザが，専門的な知識を十分に有していないユーザを想定しており，NG および FP のエラーを削減することに主眼を置くものとなっている．もし，想定するユーザを専門的な知識を十分に有しているユーザとする場合は，明らかな NG，FP のデータをユーザ自身が選別できる可能性が高い．したがって FN のエラーを削減することに主眼を置いた抽出方法を検討することで想定ユーザに対してより有効なデータを提供するアプローチの提供を目指す．

5.2.6 適応範囲の拡大

本論文では，ISO/IEC 27000ファミリーを中心としたセキュリティマネジメントの国際標準の特徴的な構成に注目をしてセキュリティ評価プラットフォームの構築を行ってきた．しかし，1.2.6 項で述べたようにセキュリティ認証制度と同様の認証を行う仕組みを持つ標準は，環境マネジメントの国際標準である ISO 14000，品質マネジメントの国際標準である ISO 9000 など多数存在する．これらの標準についても要求事項を提示している ISO 14001，ISO 9001 については 1.2.8 項で述べたような構成をとっているため，本論文で提案したセキュリティ評価プラットフォームを拡張して適応することができると推測される．

したがって，要求事項を提示するドキュメントが同様の特徴を持ち，第三者機関を認証機関としている認証制度についても適応範囲を拡大することによってプラットフォームの実用性，有効性を高めることを目指す．

5.2.7 セキュリティ評価に関する共同研究との連携

筆者らは，2.3 節で述べた NEC の芦野らの研究を共同で進めている．芦野らの研究では標準のナレッジ化が必要となり，ナレッジ化には専門的な知識が必要であることが課題となっている．この問題の解法の一つとして，本研究で提案している，項目間の相関を取り関連情報を作成する手法が適用できるのではないかと考える．この手法を適用することによって，すでに作られたナレッジをもとに関連情報を作成して，新たなナレッジを作成できることが期待される．また，参照ツリーの概念を用いて項目間の関係性を明確化することでナレッジ化する際に必要な階層モデルの作成を補助することが期待される．

また，5.2.1 項で述べた出力結果を芦野らのシステムでも読み込めるようにすることによって，データの共有が期待できる．

5.2.8 マネジメントシステム規格への対応

今後のマネジメント関連の標準の策定および改定については，文献[9]で示される Appendix 1 および Appendix 2 を用いた標準が多く誕生することが予測される．このような統一のフォーマットで記述された標準群は，もととなる Appendix 2 と新たな標準を本

研究で提案している，項目間の相関関係に基づく関連情報抽出手法を使って比較して相関をとることによって以下のことが調査できると期待される．

(1) 新規の基準で Appendix 2 にない項目が検出された場合

Appendix 1 で述べられている「場合によっては，これらの質問事項で網羅されていない追加情報も提供することが望ましい．」に該当する，新規の基準で特に注力して取組もうとしている項目の検出．

(2) 新規の基準で Appendix 2 の項目に該当する項目がない場合

新規の基準では，管理の対象外とみなすことができる項目の検出．または，基準作成時のヒューマンエラーによる記述漏れ．

特に(2)の記述漏れを検出することで，社内基準などを作成した際に，要求事項を正しく反映できていないことを検出できることは，近年問題となっているセキュリティ人材の不足といった問題[42]に対しても人材育成，技術サポートといった効果が期待できる．

参考文献

[1] 財)日本情報処理開発協会:情報セキュリティマネジメントシステム(ISMS)の国際動向と取り組みの実際＜2004 年版＞, 2005.5, http://www.isms.jipdec.jp/doc/ismsintre2004.PDF

[2] 情報マネジメントシステム推進センター:認証取得組織数推移、認証機関別・県別認証取得組織, http://www.isms.jipdec.jp/lst/ind/suii.html

[3] TechTarget ジャパンホワイトペーパー:コンシューマデバイスのセキュリティ戦略計画のために考慮すべきポイント, http://wp.techtarget.itmedia.co.jp/contents/?cid=11501

[4] 情報マネジメントシステム推進センター:国際動向「ISO/IEC 27000 ファミリーについて」, 2013.12, http://www.isms.jipdec.or.jp/27000family_20131212.pdf

[5] Payment Card Industry Security Standards Council: PCI SSC Data Security Standards, https://www.pcisecuritystandards.org/security_standards/

[6] JNSA情報セキュリティ対策マップ検討WG 奥原雅之:情報セキュリティ対策マップ検討WG活動報告 -- セキュリティ対策の構造と戦った 4 年間 --, 2013.6, http://www.jnsa.org/seminar/2013/0607/data/1C-1_map.pdf

[7] 独立行政法人情報処理推進機構:セキュリティ設計評価支援ツール V03, http://www.ipa.go.jp/security/fy13/evalu/cc_system/CCtool_V03/secevtoolv03.htm

[8] 中野明, ㈱コミュニケーションデザインネットワークス:よくわかる最新 ISMS Ver.2 の基本と仕組み, 秀和システム, 2003.6

[9] 統合版 ISO 補足指針−2013 年度版, 2013.6, http://www.jsa.or.jp/itn/pdf/shiryo/iso_supplement_1304.pdf

[10] ISO/IEC 27001 Information technology - Security techniques - Information security management system - Requirements, 2013.10

[11] ISO/IEC 27001:2013 への移行に計画について, 情報マネジメント推進センター, 2013.10, http://www.isms.jipdec.or.jp/ikou/27001_2013/ISO_IEC_27001_2013_transition.pdf

[12] ISO/IEC 27001 Information technology - Security techniques - Information security management system - Requirements, 2005.10

[13] 日本規格協会:JIS ハンドブック 2007(67-1)情報セキュリティ, 日本規格協会, 2007.7

[14] 上原孝之:図解そこが知りたい！ネットワーク危機管理入門, 翔泳社, 2000.7

[15] Official PCI Security Standard Council Site, https://www.pcisecuritystandards.org/index.php

[16] 芦野佑樹, 森田陽一郎, 小泉純, 岡村利彦:セキュリティ標準に基づいたセキュリティレベル評価技術の検討, 情報処理学会 第 154 回 マルチメディア通信と分散処理・第 60 回 コンピュータセキュリティ合同研究発表会, Vol.2013-DPS-154 No.35 Vol.2013-CSEC-60 No.35, 2013.3

[17] Stefan Fenz et al., Ontology based IT-security planning, 12th IEEE International Symposium on Pacific Rim Dependable Computing, 2006

[18] Daniel Feledi et al., Challenges of Web-based Information Security Knowledge Sharing, The 7th ARES(Availability, Reliability and Security) conference (ARES 2012), pp.514-521

[19] Stefan Fenz et al., Information Security Fortification by Ontological Mapping of the ISO/IEC 27001 Standard, 13th IEEE International Symposium on Pacific Rim Dependable Computing, 2007, pp.381−388

[20] Andreas Ekelhart et al., Ontology-based Decision Support for Information Security Risk Management, 2009 International Conference on Information Networking, ICOIN 2009, Proceedings of ICOIN 2009, pp.80−85

[21] 加藤岳久, 山本匠, 西垣正勝, 教育効果を考慮したセキュリティ対策選定手法の検討, 情報処理学会 マルチメディア, 分散, 協調とモバイル(DICOMO2011)シンポジウム論文集, pp.135−140, 2011.7

[22] 中村逸一, 兵藤敏之, 曽我正和, 水野忠則, 西垣正勝, セキュリティ対策選定の実用的な一手法の提案とその評価, 情報処理学会論文誌 Vol.45 No.8, pp.2022-2033, 2004.8

[23] 佐々木良一, 石井真之, 日高悠, 矢島敬士, 吉浦裕, 村山優子, 多重リスクコミュニケータの開発構想と試適用, 情報処理学会論文誌 Vol.46 No.8, 2005

[24] 佐々木良一, 日高悠, 守谷隆史, 谷山充洋, 矢島敬士, 八重樫清美, 川島泰正, 吉浦裕, 多重リスクコミュニケータの開発と適用, 情報処理学会論文誌 Vol.49 No.9, 2008

[25] 内閣官房情報セキュリティセンター:「政府機関の情報セキュリティ対策のための統一基準群(平成 24 年度版)」について, http://www.nisc.go.jp/active/general/kijun24.html

[26] 芦野佑樹, 髙橋雄志, 森田陽一郎, 島成佳, 岡村 利彦, 勅使河原可海, 佐々木良一:セキュリティ標準に基づいたITシステム設計支援ツールの開発, 情報処理学会コンピュータセキュリティシンポジウム 2013(CSS2013)論文集, pp.478−485, 2013.10

[27] 諸橋政幸, 永井康彦, 荒井正人, 手塚悟, ISO15408/ISO27001 統合型システムセキュリティ設計技法の提案, 情報処理学会論文誌 Vol.48 No.11, 2007.11

[28] 徳永健伸: 情報検索と言語処理, 東京大学出版会, 1999

[29] 松本祐治, 北内啓, 山下達雄, 平野善隆, 松田寛, 高岡一馬, 浅原正幸: 形態素解析システム『茶筌』version 2.0 使用説明書 第二版, NAIST Technical Report, NAIST-IS-TR99012, 奈良先端科学技術大学院大学, 1999

[30] 高木輝彦, 高木正則, 勅使河原可海:学生が作成した問題の類似度算出手法の提案と評価, 情報処理学会論文誌, Vol.50, No.10, pp.2426−2439, 2009.10

[31] 池田信一, 高木輝彦, 高木正則, 勅使河原可海:多肢選択式項目の出題パターンと選択肢の類似性に着目した難易度推定方法の提案と評価, 情報処理学会論文誌, Vol.54 No.1, pp.33−44, 2013.1

[32] 髙橋雄志, 勅使河原可海: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検討, 情報処理学会 コンピュータセキュリティシンポジウム 2008(CSS2008)論文集第 2 分冊, pp.815−819, 2008.10

[33] 髙橋雄志, 勅使河原可海: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, 情報処理学会第 46 回コンピュータセキュリティ研究発表会 Vol.2009-CSEC-46, No.13, 2009.7

[34] 髙橋雄志, 勅使河原可海:国際標準の参照関係に基づくセキュリティ評価方式の検討, 情報処理学会 第 142 回 マルチメディア通信と分散処理・第 48 回 コンピュータセキュリティ合同研究発表会, Vol.2010-DPS-142 No.53 Vol.2010-CSEC-48 No.53, 2010.3

[35] 髙橋雄志, 勅使河原可海:国際標準の参照関係に基づくセキュリティ評価方式における非専門家への対応策提示機能の検討, 情報処理学会 マルチメディア, 分散, 協調とモバイル(DICOMO2011)シンポジウム論文集, pp.127 - 134, 2011.7

[36] 髙橋雄志, 勅使河原可海:国際標準の参照関係に基づくセキュリティ評価方式におけるデータ移行機能の検討, 情報処理学会 コンピュータセキュリティシンポジウム 2011(CSS2011)論文集, pp.666 - 671, 2011.10

[37] 髙橋雄志, 池田信一, 勅使河原可海: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へのテキスト類似度の応用, 情報処理学会 第 58 回 CSEC・第 4 回 SPT 合同研究発表会, Vol.2012-CSEC-58 No.36,Vol.2012-SPT-4 No.36, 2012.7

[38] 髙橋雄志, 篠宮紀彦, 勅使河原可海: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改善とその適用, 情報処理学会 マルチメディア・分散・協調とモバイル(DICOMO2013)シンポジウム論文集, pp.846-853, 2013.7

[39] 髙橋雄志, 篠宮紀彦, 勅使河原可海:セキュリティ標準間の関連情報作成手法の検討とその適応, 情報処理学会 第 7 回コンシューマ・デバイス＆システム(CDS)研究発表会, 2013-CDS-7(1), pp.1-8, 2013.05

[40] 東京大学中川研究室・横浜国立大学森研究室: 専門用語自動抽出システム

[41] IT 用語辞典 e-Words, http://e-words.jp/

[42] 情報処理推進機構:「情報セキュリティ人材の育成に関する基礎調査」報告書について, http://www.ipa.go.jp/security/fy23/reports/jinzai/

謝辞

私の研究活動および大学生活は，数多くの方々に支えられてきました．この場をお借りして感謝の言葉を述べさせていただきます．

創立者池田大作先生が創ってくださった創価大学で学ばせて頂き，数多くの素晴らしい方々と出会い博士を目指すきっかけをいただけたことを最初に感謝申し上げます．

創価大学名誉教授の勅使河原可海先生には，学部，博士前期，研究生，博士後期と長きに渡り研究指導を賜り，本当にお世話になりました．特に現在のテーマに切り替えた博士前期の時に，その時点ではまだ未知数であった現在の分野への転向を後押ししてくださった先見性には大きく助けられました．博士後期は社会人学生として戻ってきたこともあり，メールなどを活用し遠隔で時間曜日も問わず議論や論文，プレゼンテーションの推敲にお付き合い頂くなど，献身的かつダイナミックな研究指導をしていただきました．さらに，学外での学会発表や研究会議などに積極的に参加し，時には代理で各所へ御挨拶をさせていただく中で，外へ打って出ることの大切さや，人と人とのネットワークの重要さを，身をもって教えていただきました．また，創価大学を定年退職された後も，創価大学，東京電機大学で幾度も研究指導いただきました．研究活動だけでなく，学生生活や時に私生活の悩みにも，親身になって相談に乗っていただき大きな心の支えとなりました．勅使河原先生と共に，多くの時間を過ごさせていただいたことは大きな財産となっております．心より感謝申し上げます．

指導教員の篠宮紀彦准教授には，勅使河原先生が定年退職されてから研究指導いただきました．学部，博士前期の時代には大学の先輩として，博士後期で大学に戻ってからは教員として，博士後期課程の学生としてのあり方，博士号取得の意味するところ，論文作成上の心構えといった研究指導をいただきました．また，研究指導だけではなく，同じ創価大学の卒業生として，創価大学出身者としての指導も数多く頂きました．旧渡部和研究室の先輩としては，渡部和先生に教わった技術者とはどうあるべきかといった角度でも様々な話を聞かせていただくことができました．特に，情報処理学会の CDS トランザクション論文では，論文の書き方，研究の見せ方をこれまでと違った角度で指摘していただき，大きな躍進をすることができました．多様性のある指導に感謝の思いは尽きません．

また，畝見達夫教授，高見一正教授には，多くの人への研究理解を深めるにはどうすればよいのかという観点を中心に有益なコメントをいただきました．いただきましたコメントをもとに，より多く，広い分野の方に研究を理解いただけるよう，研究の発展に努めてまいります．

東京電機大学の佐々木良一教授，静岡大学の西垣正勝教授には，学外会議や研究会などで，多くの貴重なご意見をいただきました．心より御礼申し上げます．

NEC 芦野佑樹氏とは，共同研究という形で同じ分野での研究活動の活発化に関わることができました．大変にありがとうございました．

ISMS 審査員補の足田氏には，私の研究に対し有益なコメントをいただいたり，様々活発な議論をさせていただいたりしました．このテーマの面白さに気がつけたのは，二人で議論していた時だったことは鮮明に覚えております．篤く御礼申し上げます．

旧勅使河原研究室，旧渡部研究室，篠宮研究室では，多くの仲間と切磋琢磨しあいながら研究活動をすることができました．学部，博士前期の時代では同期の木村博巳氏，野田健治氏，南田元氏，山口勇一氏，ラミレス・ギジェルモ氏をはじめ，先輩後輩たちと金の思い出を作ることができました．博士後期に戻ってからは加藤弘一氏，長野純一氏，佐藤信氏，太田悟氏をはじめ，良き後輩たちと共に研究活動をすることができました．同期のメンバーとは今でも連絡を取り合い，生涯の朋といえる存在となっていることは望外の喜びとなっております．

また，長きに渡った学生生活を陰で支えてくれた家族にも最大級の感謝の言葉を送らせて頂きたいと思っております．父，誠志からは，技術者の先輩としての姿を学び．母，栄子には，研究活動や日々の生活で疲れている時に精神的な部分で多く支えられました．創立者からは博士後期の入学式で親孝行をしなさいと御指導いただきました．このように支えて下さった両親に，報恩感謝の思いは尽きません．弟，達明は，学生時代同じ勅使河原先生のもとでご指導いただきました．勅使河原先生のもとに戻り，博士号に挑戦する私のことを心配しつつも応援してくれました．すでに社会で活躍しているのは，嬉しい限りです．

最後に，これまで共に研究活動に携わってきた全ての方に感謝をいたします．研究活動や多くの方からいただいたご指導を通してブロンズ像の指針「英知を磨くは何のため．君よそれを忘るるな」を胸に，創価大学で学んだことを忘れず，創価大学の卒業生としての誇りも高く，社会で光る人材へと成長して参ります．

【附録 A】業績一覧

論文誌

1) Yuji Takahashi, and Yoshimi Teshigawara: Design and Development of a Security Evaluation Platform Based on International Standards, International Journal of Informatic Society, IJIS Vol.5 No.2, pp.71−81, 2013.8
2) 髙橋雄志, 篠宮紀彦, 勅使河原可海:セキュリティ標準間の関連情報作成手法の検討とその適応, 情報処理学会論文誌 コンシューマ・デバイス&システム 第 3 巻 第 4 号, pp.22−32, 2013.12
3) 髙橋雄志, 篠宮紀彦, 勅使河原可海: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提案, 日本セキュリティマネジメント学会学会誌 Vol.27, pp.16−29, No.2, 2013.9

学会発表

1) 高橋雄志, 勅使河原可海:分散システム環境下におけるリスク分析支援ツールの提案, 情報処理学会 マルチメディア・分散・協調とモバイル(DICOMO2002)シンポジウム論文集, pp.345−348, 2002.7
2) 髙橋雄志, 勅使河原可海:リスク分析ツールにおけるセキュリティ対策目標提示機能の追加の提案, 情報処理学会第 66 回全国大会講演論文集第 3 分冊, pp.603−604, 2004.3
3) 髙橋雄志, 勅使河原可海: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検討, 情報処理学会 コンピュータセキュリティシンポジウム 2008(CSS2008)論文集第 2 分冊, pp.815−819, 2008.10
4) 髙橋雄志, 勅使河原可海: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 第 46 回コンピュータセキュリティ研究発表会 Vol.2009-CSEC-46 No.13, 2009.7
5) 髙橋雄志, 勅使河原可海:国際標準の参照関係に基づくセキュリティ評価方式の検討, 常勝処理学会 第 142 回 マルチメディア通信と分散処理・第 48 回 コンピュータセキュリティ合同研究発表会, Vol.2010-DPS-142 No.53 Vol.2010-CSEC-48 No.53, 2010.3
6) 髙橋雄志, 勅使河原可海, 国際標準の参照関係に基づくセキュリティ評価方式における非専門家への対応策提示機能の検討, 情報処理学会 マルチメディア, 分散, 協調とモバイル(DICOMO2011)シンポジウム論文集, pp.127−134, 2011.7

7) 髙橋雄志, 勅使河原可海:国際標準の参照関係に基づくセキュリティ評価方式におけるデータ移行機能の検討, 情報処理学会 コンピュータセキュリティシンポジウム 2011(CSS2011)論文集, pp.666−671, 2011.10

8) 髙橋雄志, 池田信一, 勅使河原可海: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へのテキスト類似度の応用, 情報処理学会 第 58 回 CSEC・第 4 回 SPT 合同研究発表会, Vol.2012-CSEC-58 No.36,Vol.2012-SPT-4 No.36, 2012.7

9) Yuji Takahashi, and Yoshimi Teshigawara: Design and Development of a Security Evaluation Platform Based on International Standards, Participants Proceedings of International Workshop on Informatics (IWIN) 2012, pp.148−157, Chamonix, France, 2012.9

10) 髙橋雄志, 篠宮紀彦, 勅使河原可海:セキュリティ標準間の関連情報作成手法の検討とその適応, 情報処理学会 第 7 回コンシューマ・デバイス&システム(CDS)研究発表会, 2013-CDS-7(1) pp.1−8, 2013.5

11) 髙橋雄志, 篠宮紀彦, 勅使河原可海: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改善とその適用, 情報処理学会 マルチメディア・分散・協調とモバイル(DICOMO2013)シンポジウム論文集, pp.846−853, 2013.7

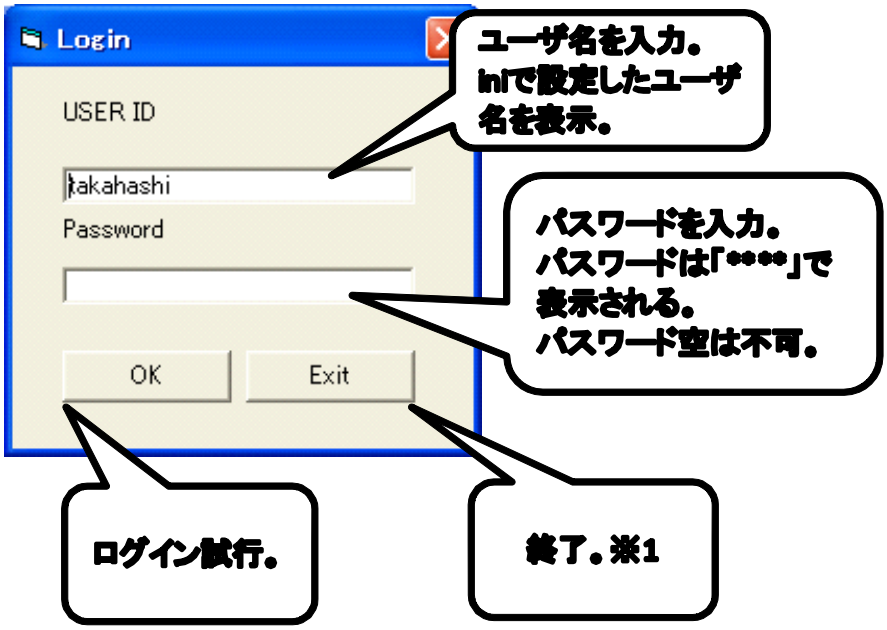
12) 芦野佑樹, 髙橋雄志, 森田陽一郎, 島成佳, 岡村 利彦, 勅使河原可海, 佐々木良一:セキュリティ標準に基づいた IT システム設計支援ツールの開発, 情報処理学会コンピュータセキュリティシンポジウム 2013(CSS2013)論文集, pp.478−485, 2013.10

【附録 B】システム画面解説

1) ログイン画面

ユーザ認証を行う画面，初期ユーザは設定ファイルで設定が可能．

ユーザの種別（Admin ユーザか，一般ユーザか）によってログイン先が分岐する．



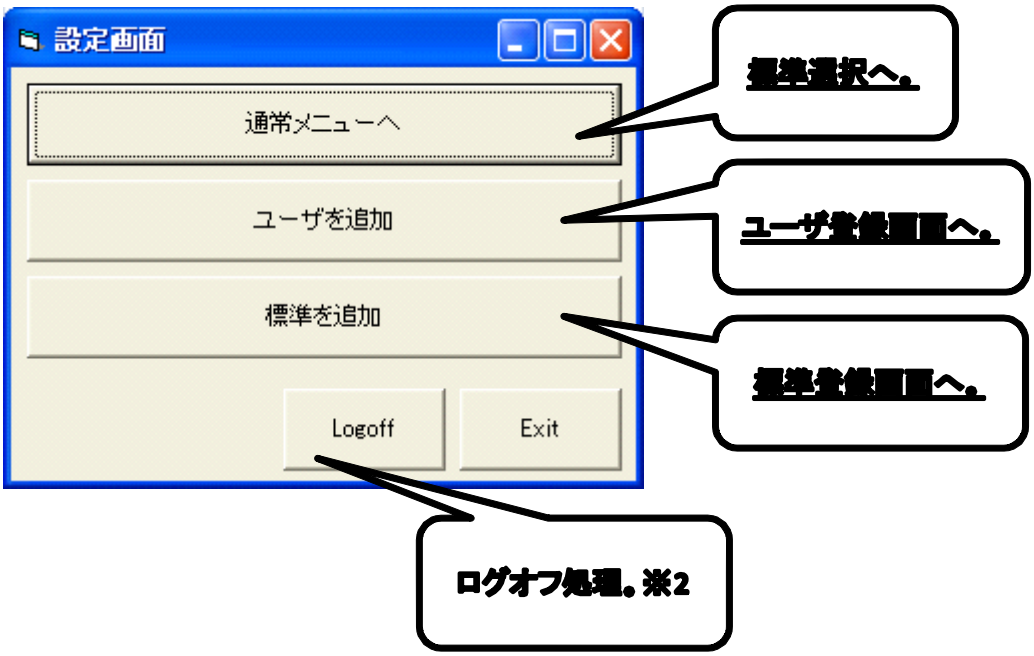
※1：以後「Exit」のボタンは終了処理とする。

認証失敗メッセージ

認証成功メッセージ

2) 設定画面

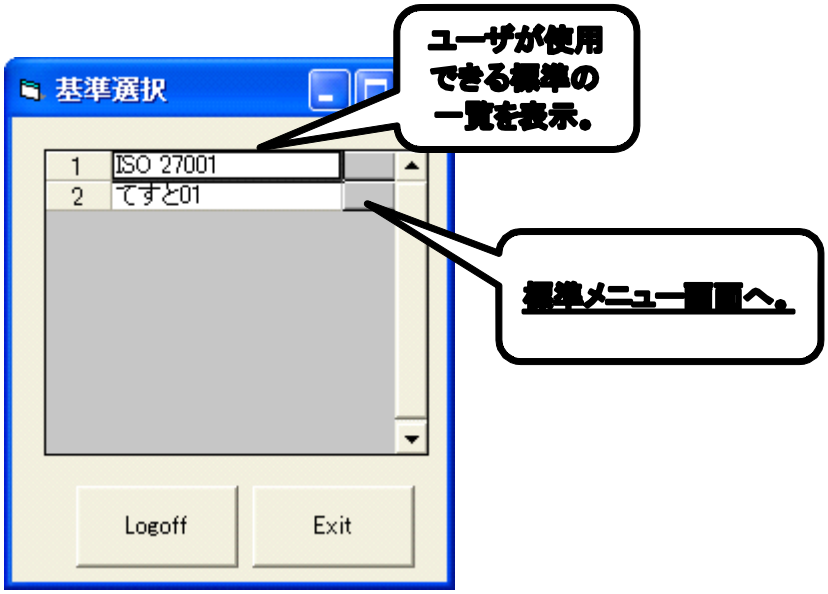
ユーザ種別が Admin ユーザであった場合は，ログイン先がこの画面となる．



※2：以後「Logoff」のボタンはログオフ処理とする。

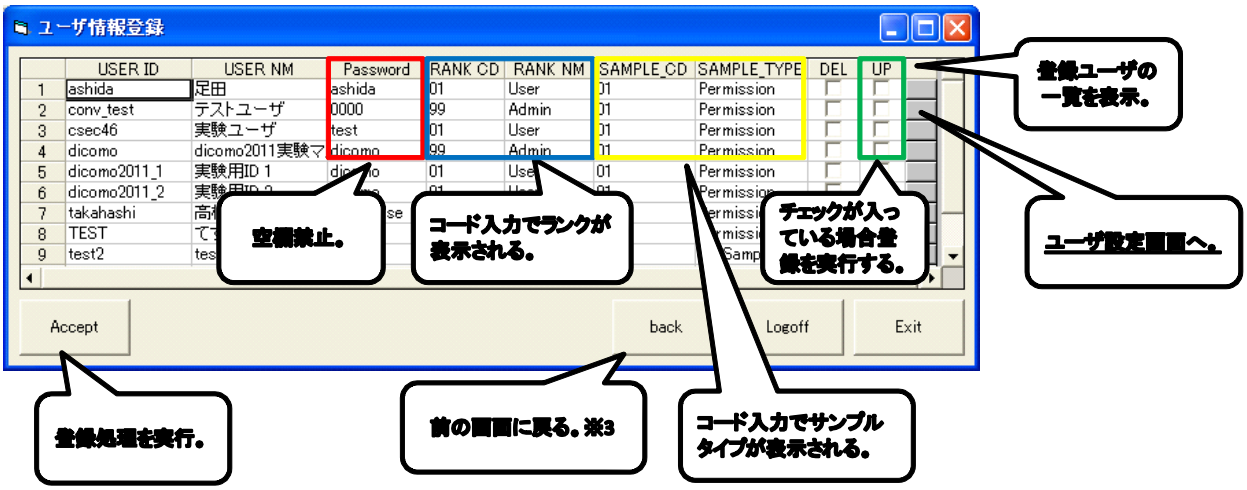
3) 標準選択画面

一般ユーザはログイン後に，設定画面を介さずに標準選択画面に移動する．



4)　ユーザ登録画面

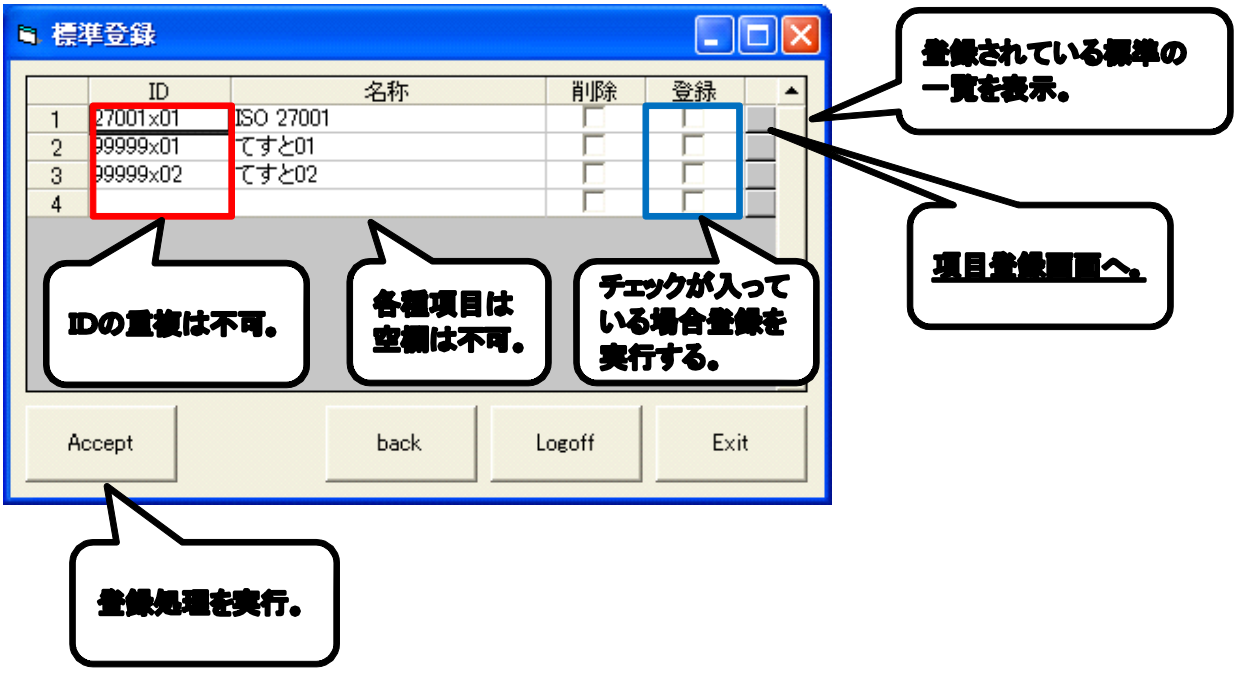
Admin ユーザによって，ユーザの登録，更新，削除を行う画面．



※3：以後「back」のボタンは前の画面に戻る処理とする。

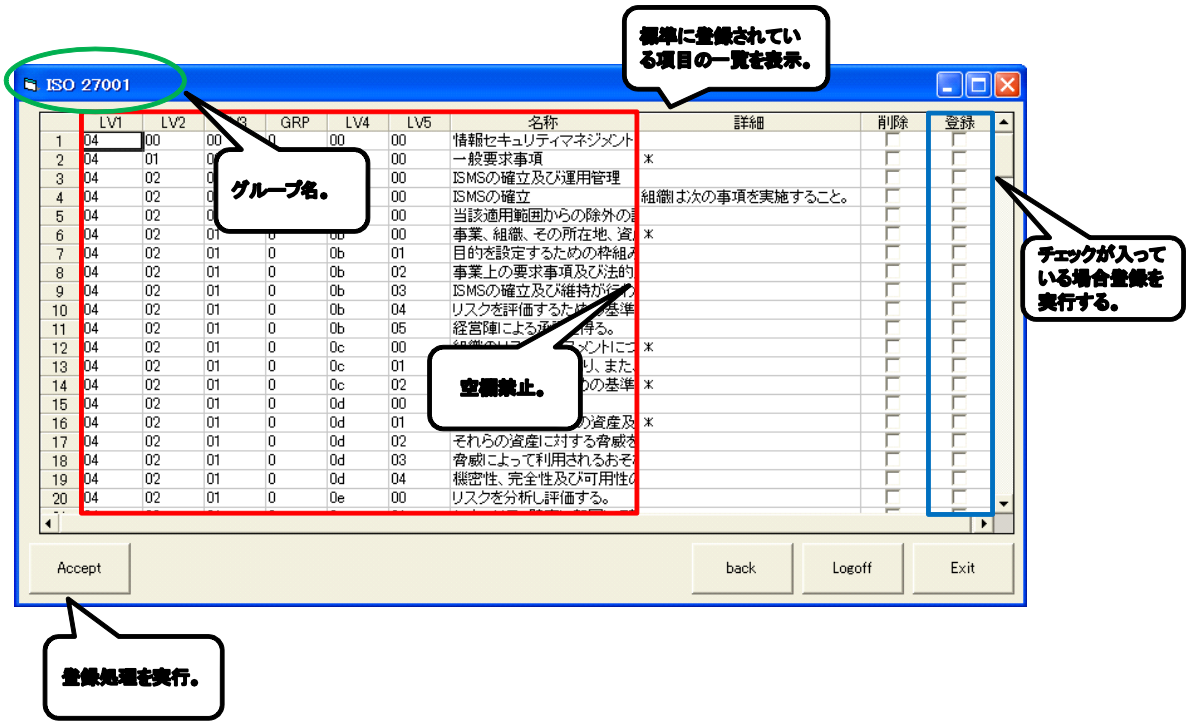
5)　標準登録画面

Admin ユーザによって，評価する標準自体の登録，削除を行う画面．詳細なデータ登録が別画面で行う．



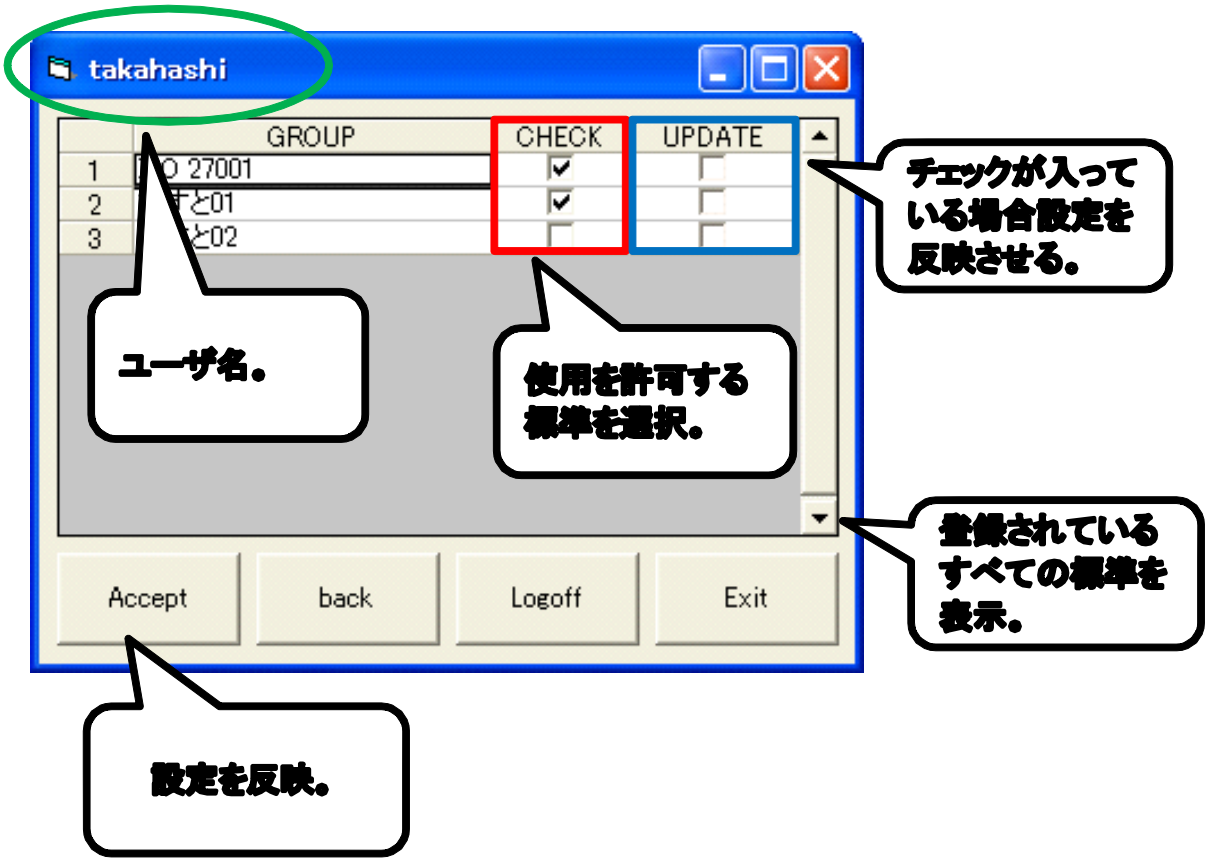
6)　項目登録画面

Admin ユーザによって，標準の項目レベルでのデータ登録を行う画面．本画面で入力されたデータが基本データとなる．



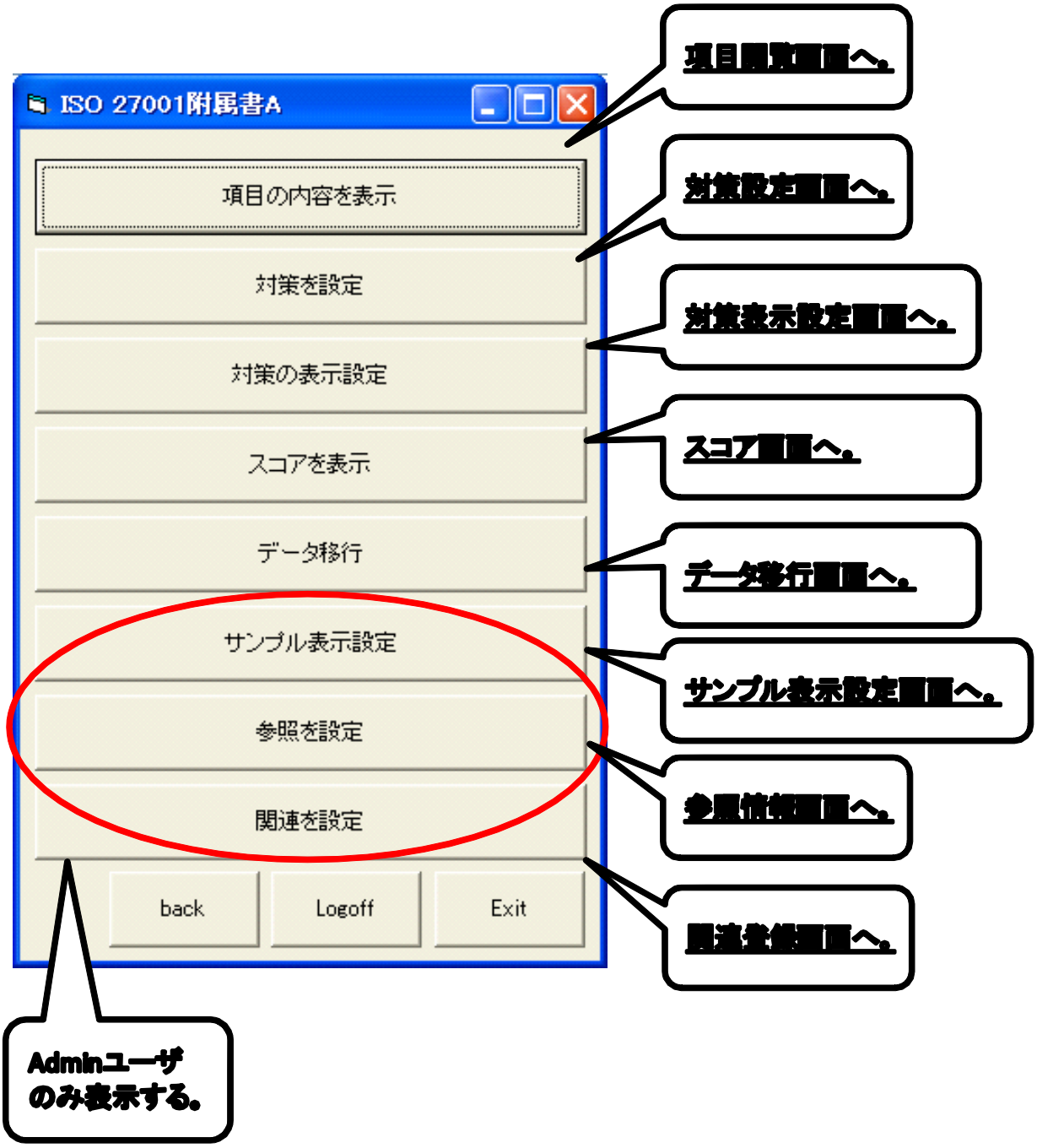
7) ユーザ設定画面

Admin ユーザによって，各ユーザが評価に使用できる標準を設定する画面．



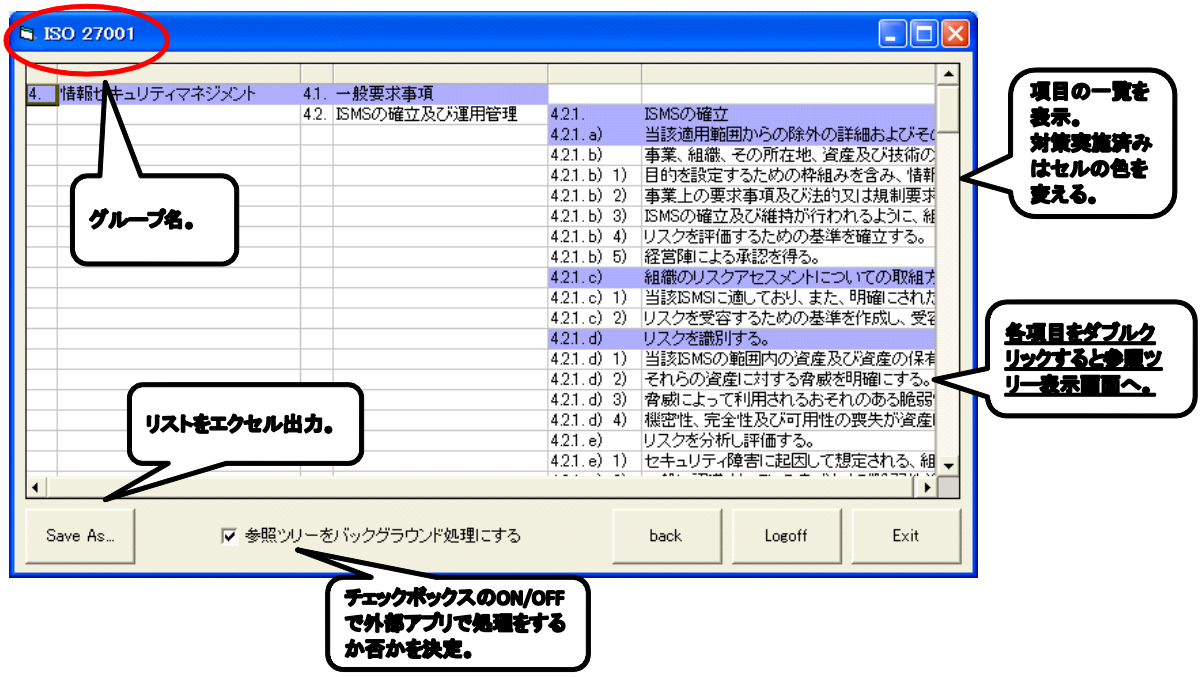
8) 標準メニュー画面

各種機能を使う為の初期メニュー画面. この画面よりプラットフォームの各種機能を使用するための画面に移動する. Admin ユーザと一般ユーザでは使用できる機能に違うがあるため表示が異なる.



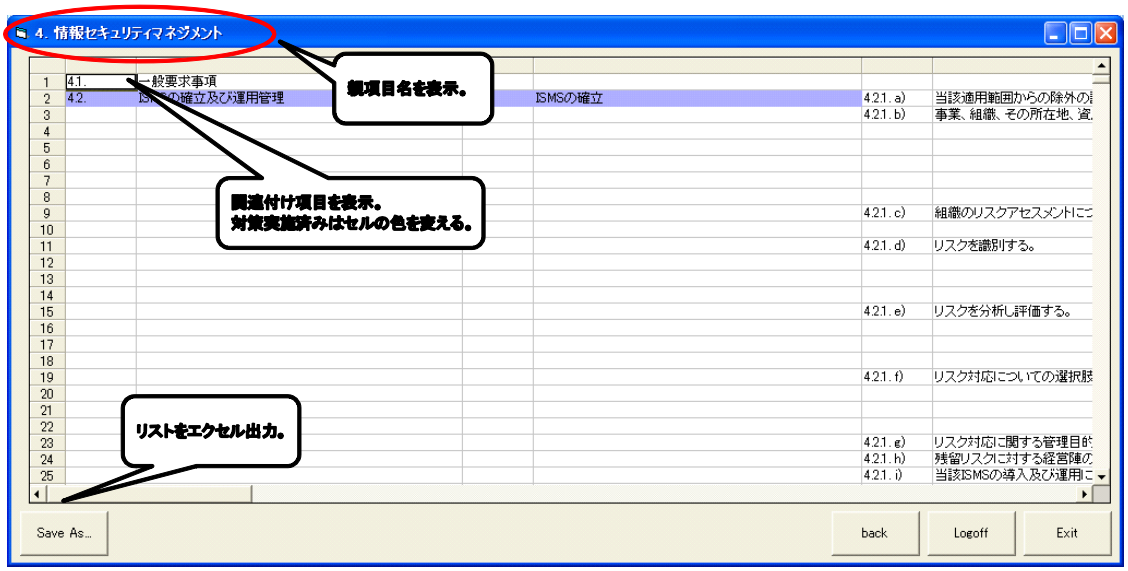
9)　項目閲覧画面

評価対象となる標準を階層構造のみの情報で表示し，対応策の有無で色分けをした画面．



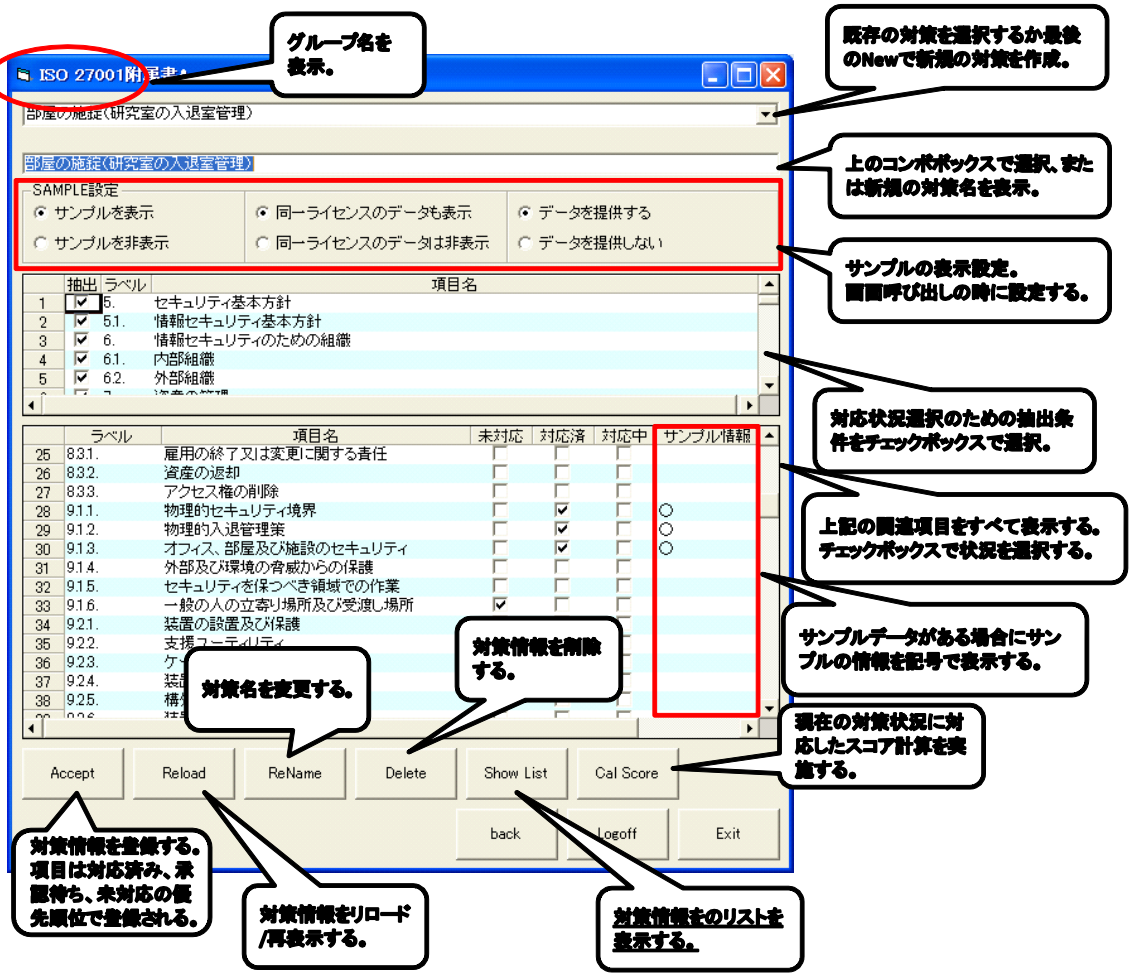
10) 関連表示画面

項目閲覧画面で選択した項目の参照ツリーを表示する画面．

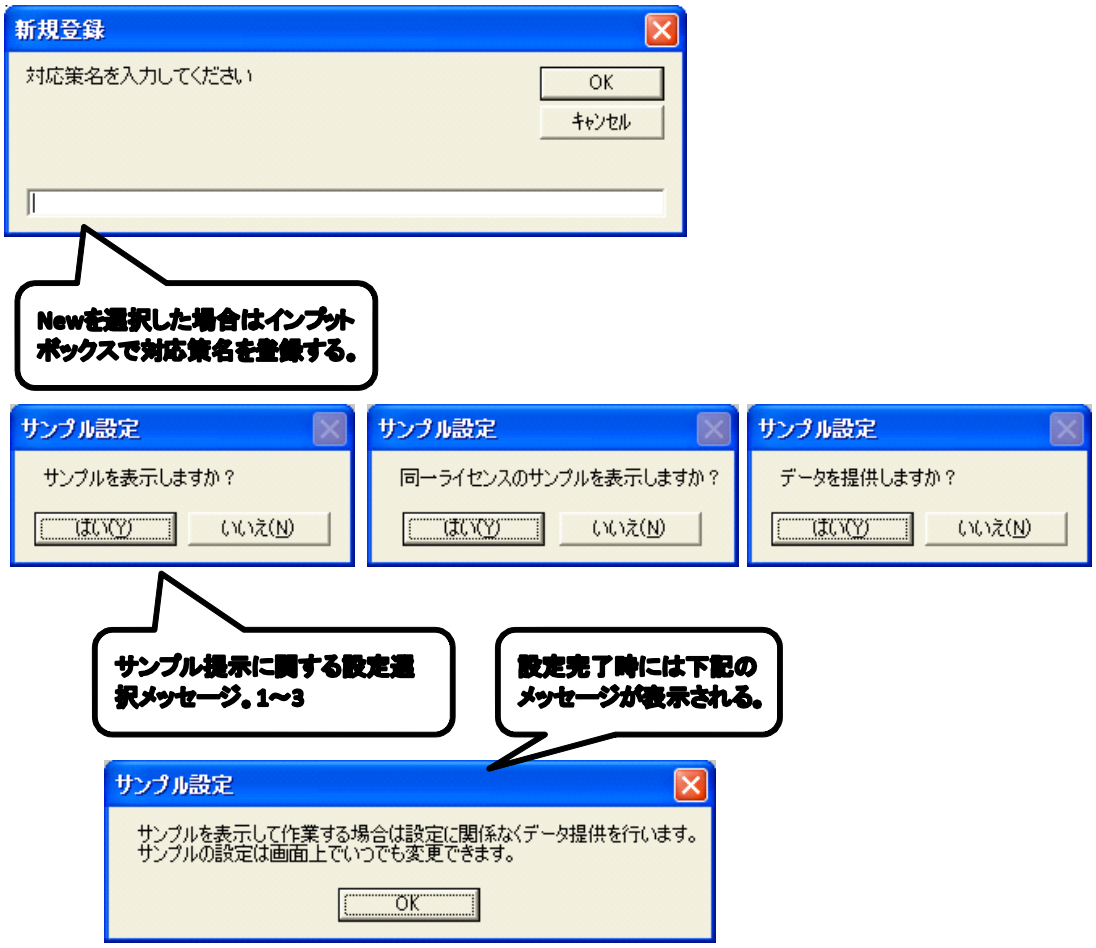


11) 対策設定画面

対策の登録および対策がどの項目に対して対策であるのかを設定する画面.



下記は，対策設定画面で使用しているメッセージ.



12) 対策表示設定画面

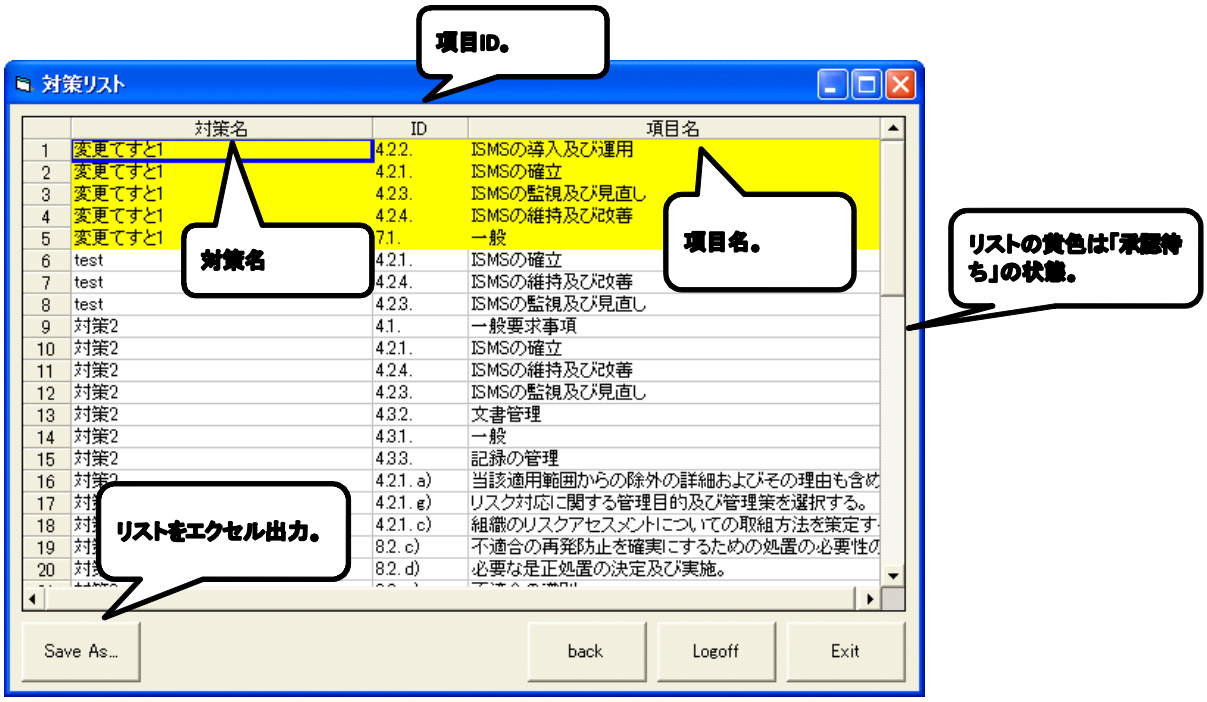
ユーザごとに登録されている対策を使用するか否かを設定する画面.

13) 参照登録画面

管理ユーザによって，標準の参照情報を登録する画面．この情報に基づき参照ツリーを構成する．

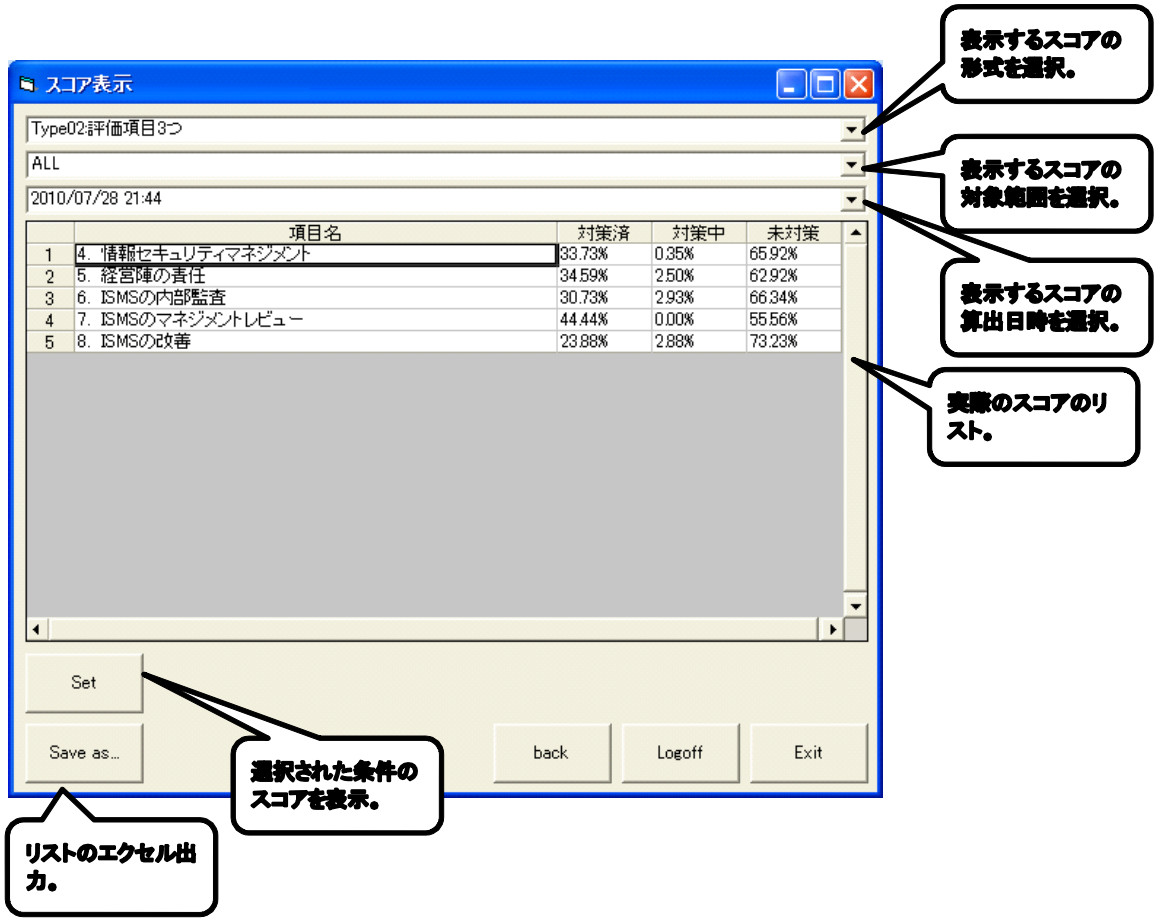
14) 対策リスト画面

登録されている対策と項目の組をリスト表示する画面.



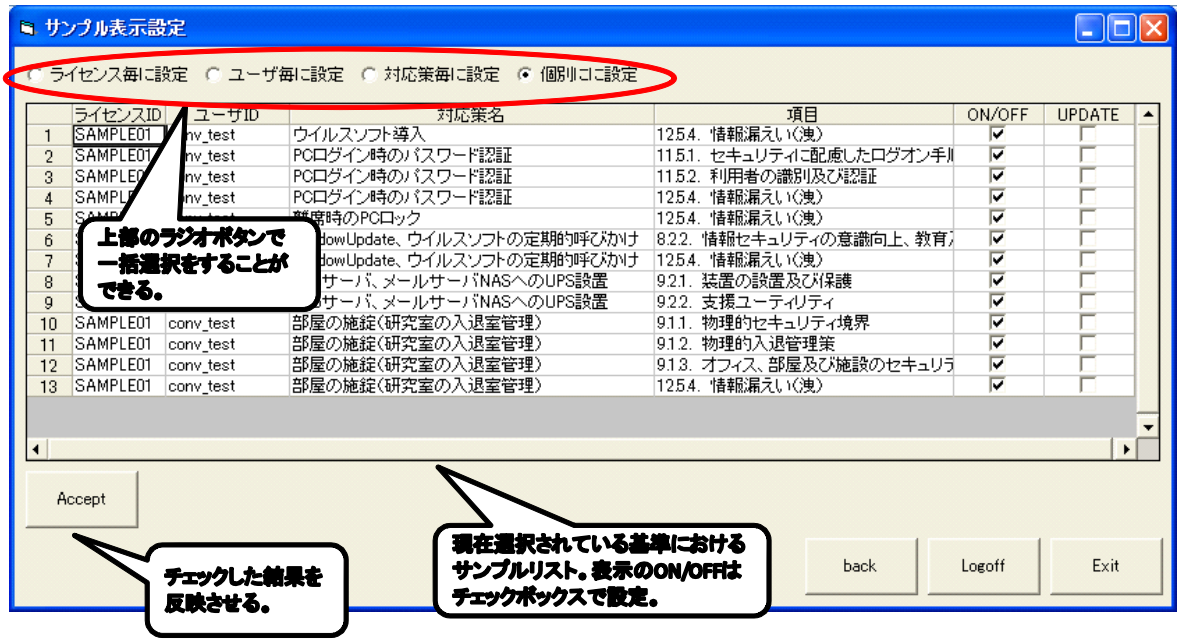
15) スコア画面

対策状況に応じたスコアを表示する画面. 過去に計算したスコアの履歴も参照できる.



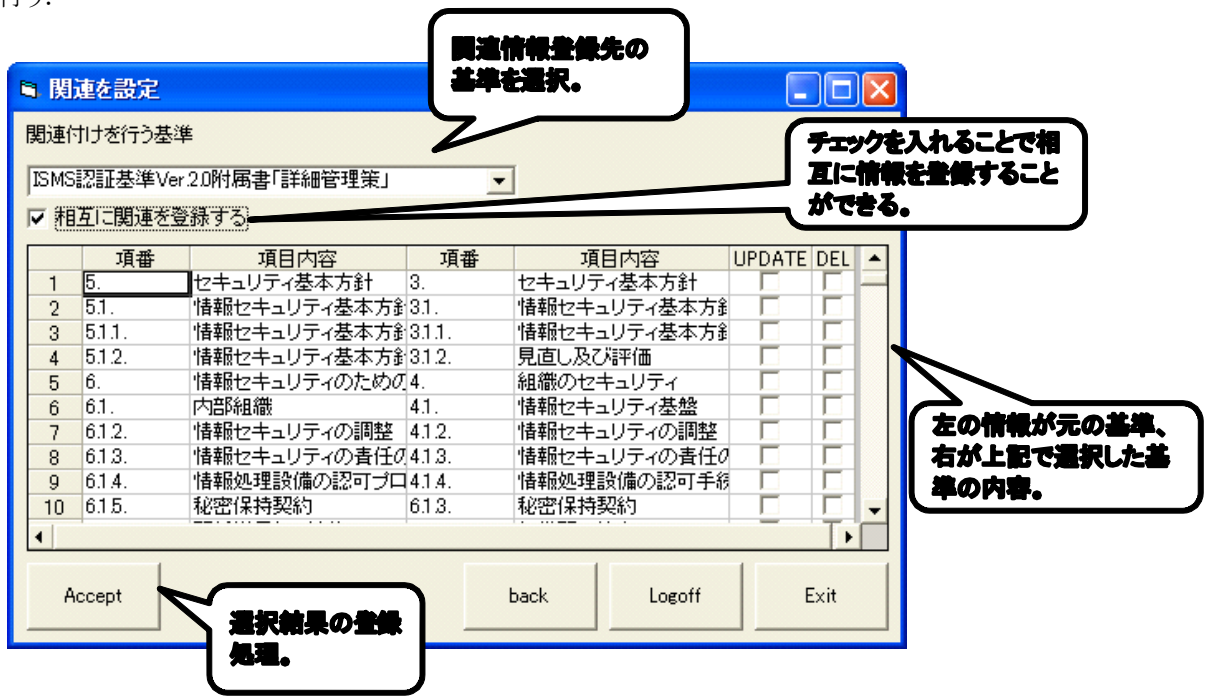
16) サンプル表示設定画面

管理ユーザによって，サンプルの表示設定を行う画面．この画面で設定された表示設定はユーザが設定した表示設定よりも優先される．



17) 関連登録画面

管理ユーザによって，関連情報を登録する画面．ここで登録された情報に基づきデータ移行を行う．



18) データ移行画面

選択した組に対して，関連情報に基づきデータ移行機能を実行する画面

【附録 C】テーブル定義書

システム名	システム1			作成日	2008/4/16 16:19
テーブル名	00_USER			更新日	2008/5/7 18:05
フィールド名	書式	説明			備考
USER_ID	文字列	ユーザ固有のユーザID			重複不可
USER_NM	文字列	ユーザ名			重複不可
PASSWORD	文字列	パスワード			
LAST_LOG_IN	実数型	最後にログインした日時を「YYYYMMDD」の形で記録			
USER_RANK	文字列	ユーザのランク			→04_RANK_M.RANK_ID
SAMPLE_TYPE	文字列	サンプルを使用できるかの区分			→05_U_SAMPLE_M.US_ID
DEL_FLG	文字列	削除フラグ			1:削除データ

システム名	システム1	作成日	2008/4/16　16:22
テーブル名	01_GRP_M	更新日	

フィールド名	書式	説明	備考
GRP_ID	文字列	標準のグループID	重複不可
GRP_NM	文字列	グループ名	
UPDATE_YMD	実数型	更新日を「YYYYMMDD」の形で記録	
DEL_FLG	文字列	削除フラグ	1:削除

システム名	システム1	作成日	2008/4/16　16:38
テーブル名	02_ELEMENT_M	更新日	2009/8/29　12:50

フィールド名	書式	説明	備考
ELEMENT_ID	文字列	各種表示項目のID	重複不可
GRP_ID	文字列	項目の所属する標準グループのID	→01_GRP_M
LEVEL1_ID	文字列	階層1のID	
LEVEL2_ID	文字列	階層2のID	0:LEVEL1の項目
LEVEL3_ID	文字列	階層3のID	0:LEVEL2の項目
LEVEL_GRP_ID	文字列	表示グループ用ID	
LEVEL4_ID	文字列	階層4のID	0:LEVEL3の項目
LEVEL5_ID	文字列	階層5のID	0:LEVEL4の項目
ELEMENT_NM	文字列	項目名	
ELEMENT_INF	文字列	項目の詳細	
UPDATA_YMD	実数型	更新日を「YYYYMMDD」の形で記録	
DEL_FLG	文字列	削除フラグ	1:削除

システム名	システム1	作成日	2008/4/16　16:49
テーブル名	03_MEASURE_M	更新日	

フィールド名	書式	説明	備考
MEASURE_ID	文字列	対策ID	重複不可
MEASURE_NM	文字列	対策名	
GRP_ID	文字列	項目の所属する標準グループのID	→01_GRP_M
SAMPLE_ID	文字列	サンプルの元データを示すID	→40_SAMPLE
DEL_FLG	文字列	削除フラグ	1:削除

システム名	システム1	作成日	2008/5/7　18:06
テーブル名	04_RANK_M	更新日	

フィールド名	書式	説明	備考
RANK_ID	文字列	ランクID	重複不可
RANK_NM	文字列	ランク名	別途仕様有
DEL_FLG	文字列	削除フラグ	1:削除データ

システム名	システム1	作成日	2011/4/27　17:11
テーブル名	05_U_SAMPLE_M	更新日	

フィールド名	書式	説明	備考
US_ID	文字列	ユーザのサンプルタイプを判別するID	重複不可
SAMPLE_TYPE	文字列	サンプルのタイプ	重複不可
DEL_FLG	文字列	削除フラグ	1:削除データ

システム名	システム1	作成日	2008/4/16　16:51
テーブル名	10_USER_GRP	更新日	2008/4/30　16:48

フィールド名	書式	説明	備考
UG_ID	文字列	ユーザと使用できる標準の関係ID	重複不可
USER_ID	文字列	ユーザID	→00_USER
GRP_ID	文字列	使用できる標準のID	→01_GRP_M
LAST_TRY_YMD	実数型	最後に使用した日時を「YYYYMMDD」の形で記録	
DEL_FLG	文字列	削除フラグ	1:削除

システム名	システム1	作成日	2008/4/16　17:01
テーブル名	11_USER_MEASURE	更新日	2009/8/29　13:56

フィールド名	書式	説明	備考
UM_ID	文字列	ユーザが設定した対策に関するID	重複不可
USER_ID	文字列	ユーザID	→00_USER
GRP_ID	文字列	項目の所属する標準グループのID	→01_GRP_M
MEASURE_ID	文字列	対策ID	→03_MEASURE_M
MEASURE_NM	文字列	対策の名称	→03_MEASURE_M
MEASURE_TYPE	文字列	対策の種類	0:通常対策、1:対象外
DEL_FLG	文字列	削除フラグ	1:削除

システム名	システム1	作成日	2008/6/4 16:59
テーブル名	12_ELEMENT_USER	更新日	2009/10/10 20:33

フィールド名	書式	説明	備考
EU_ID	文字列	ユーザが設定した対策に関するID	重複不可
USER_ID	文字列	ユーザID	→00_USER
GRP_ID	文字列	項目の所属する標準グループのID	→01_GRP_M
ELEMENT_ID	文字列	対策実施項目ID	→02_ELEMENT_M
MEASURE_TYPE	文字列	対策の種類	→11_USER_MEASURE
DEL_FLG	文字列	削除フラグ	1:削除

システム名	システム1	作成日	2008/6/11　15:37
テーブル名	13_MEASURE_USER	更新日	

フィールド名	書式	説明	備考
UM_ID	文字列	ユーザが設定した対策に関するID	重複不可
MEASURE_ID	文字列	対策ID	→03_MEASURE_M
USER_ID	文字列	ユーザID	→00_USER
VISIBLE	文字列	非表示フラグ	0:表示、1:非表示
DEL_FLG	文字列	削除フラグ	1:削除

システム名	システム1	作成日	2009/6/3 18:26
テーブル名	14_USER_MEASURE_ELEMENT	更新日	2009/10/10 20:33

フィールド名	書式	説明	備考
UME_ID	文字列	ユーザが設定した対策に関するID	重複不可
USER_ID	文字列	ユーザID	→00_USER
GRP_ID	文字列	項目の所属する標準グループのID	→01_GRP_M
MEASURE_ID	文字列	対策ID	→03_MEASURE_M
TYPE_ELEMENT	文字列	メイン/サブの識別フラグ	0:メイン、1:サブ
ELEMENT_ID	文字列	対策実施項目ID	→02_ELEMENT_M
MEASURE_TYPE	文字列	対応策タイプコード	マスタ参照
SEQ_NUM	整数	シーケンスナンバー	
DEL_FLG	文字列	削除フラグ	1:削除

システム名	システム1	作成日	2008/4/16 17:07
テーブル名	20_ELEMENT_REF	更新日	2009/11/12 16:16

フィールド名	書式	説明	備考
ER_ID	文字列	参照ID	重複不可
GRP_ID	文字列	項目の所属する標準グループのID	→01_GRP_M
LV1_1	文字列	参照元の章ID	→02_ELEMENT_M
ELEMENT_1	文字列	参照元ID	→02_ELEMENT_M
LV1_2	文字列	参照先の章ID	→02_ELEMENT_M
ELEMENT_2	文字列	参照先ID	→02_ELEMENT_M
DEPTH	数値型	参照元よりの距離	自己参照は0
MAX_DEPTH	数値型	参照元の持つ距離の最大値	スコア算出に使用
DEL_FLG	文字列	削除フラグ	1:削除

システム名	システム1	作成日	2009/4/4　17:51
テーブル名	21_REF_TREE	更新日	

フィールド名	書式	説明	備考
REF_ID	文字列	参照ID	重複不可
USER_ID	文字列	ユーザID	→00_USER
GRP_ID	文字列	項目の所属する標準グループのID	→01_GRP_M
ELEMENT_ID	文字列	項目ID	→02_ELEMENT_M
ELEMENT_NM	文字列	項目名	→02_ELEMENT_M
DEL_FLG	文字列	削除フラグ	1:削除

システム名	システム1	作成日	2011/10/26　20:21
テーブル名	22_ELEMENT_CONV	更新日	

フィールド名	書式	説明	備考
CONV_ID	文字列	移行情報ID	重複不可
GRP_ID_1	文字列	移行元グループID	→01_GRP_M
ELEMENT_ID_1	文字列	移行元項目ID	→02_ELEMENT_M
ELEMENT_NM_1	文字列	移行元項目名	→02_ELEMENT_M
GRP_ID_2	文字列	移行先グループID	→01_GRP_M
ELEMENT_ID_2	文字列	移行先項目ID	→02_ELEMENT_M
ELEMENT_NM_2	文字列	移行先項目名	→02_ELEMENT_M
AND_FLG	文字列	0:通常データ、1:N:1、2:1:N	0:通常データ、1:N:1、2:1:N
AND_ID	文字列	CSV	
DEL_FLG	文字列	削除フラグ	1:削除

システム名	システム1	作成日	2008/7/4　16:05
テーブル名	30_SCORE	更新日	2009/10/10　20:34

フィールド名	書式	説明	備考
SCORE_ID	文字列	スコアID	重複不可
USER_ID	文字列	ユーザID	→00_USER
GRP_ID	文字列	使用できる標準のID	→01_GRP_M
ELEMENT_ID	文字列	該当項目ID	→02_ELEMENT_M
SCORE_TYPE	文字列	スコアの計算方式コード	別紙参照
CNT_ALL	実数型	対象項目数	方式によって補正あり
CNT_01	実数型	評価項目1	方式によって補正あり
CNT_02	実数型	評価項目2	方式によって補正あり
CNT_03	実数型	評価項目3	方式によって補正あり
CNT_04	実数型	評価項目4	方式によって補正あり
CNT_05	実数型	評価項目5	方式によって補正あり
CNT_06	実数型	評価項目6	方式によって補正あり
YMD	実数型	登録日を「YYYYMMDDhhmm」の形で記録	
DEL_FLG	文字列	削除フラグ	1:削除

システム名	システム1	作成日	2011/4/27　17:25
テーブル名	40_SAMPLE	更新日	2011/11/2　20:39

フィールド名	書式	説明	備考
SAMPLE_ID	文字列	サンプルデータに振り分けるID	重複不可
License_ID	文字列	サンプル作成元ID	
USER_ID	文字列	ユーザID	→00_USER
GRP_ID	文字列	項目の所属する標準グループのID	→01_GRP_M
MEASURE_ID	文字列	対策ID	→03_MEASURE_M
MEASURE_NM	文字列	対策名	→03_MEASURE_M
TYPE_ELEMENT	文字列	メイン/サブの識別フラグ	0:メイン、1:サブ
ELEMENT_ID	文字列	対策実施項目ID	→02_ELEMENT_M
MEASURE_TYPE	文字列	対応策タイプコード	マスタ参照
SAMPLE_CD	文字列	41番テーブルとリンクしているコード	→41_TMP_SAMPLE
SAMPLE_TYPE	文字列	サンプル区分	別紙参照
VISIBLE	文字列	表示の有無を示すID	0:表示、1:非表示
DEL_FLG	文字列	削除フラグ	1:削除

システム名	システム1	作成日	2011/11/2　20:37
テーブル名	41_TMP_SAMPLE	更新日	

フィールド名	書式	説明	備考
SAMPLE_CD_TMP	文字列	サンプルデータ作成用の元ID（SSではじまるもの）	
SAMPLE_CD	文字列	グローバルなサンプルID（運営から付与されるID）	
USER_ID	文字列	ユーザID	
GRP_ID	文字列	項目の所属する標準グループのID	
MEASURE_ID	文字列	対策ID	
DEL_FLG	文字列	削除フラグ	

システム名	システム1	作成日	2008/6/4　16:51
テーブル名	90_STATE_1	更新日	

フィールド名	書式	説明	備考
STA_ID	文字列		
GRP_ID	文字列	グループ名	→01_GRP_M
STATE	文字列	ステータス	0:UNLOCK、1:LOCK
DEL_FLG	文字列	削除フラグ	1:削除

システム名	システム1	作成日	2008/6/4　14:47
テーブル名	91_STATE_2	更新日	

フィールド名	書式	説明	備考
STA_ID	文字列		
GRP_ID	文字列	グループ名	→01_GRP_M
USER_ID	文字列	ユーザID	→00_USER
STATE	文字列	ステータス	0:UNLOCK、1:LOCK
DEL_FLG	文字列	削除フラグ	1:削除

システム名	システム1	作成日	2008/7/4　16:17
テーブル名	92_STATE_3	更新日	2009/10/14　16:24

フィールド名	書式	説明	備考
STA_ID	文字列		
GRP_ID	文字列	グループ名	→01_GRP_M
USER_ID	文字列	ユーザID	→00_USER
SCORE_TYPE	文字列	スコアの計算方式コードをcsvで記述	※詳細は別紙
STATE	文字列	ステータス	0:NOT READY、1:READY
DEL_FLG	文字列	削除フラグ	1:削除