Vol.2009-CSEC-46 No.13
2009/7/2

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

髙橋雄志† 勅使河原可海†

セキュリティ認証取得においては，国際標準等を基準として対象組織を評価する．組織では，認証取得に向け，基準達成を確認するセキュリティ評価システムが活用されている．これまで，標準の変化に対応するため，評価基準とする標準の変更のみで標準内容や評価対象組織，評価する目的の変化に対応した評価ツールを実現するプラットフォームの検討を行ってきた．本稿では，プラットフォームのプロトタイプシステムを作成し，複数の標準のデータの登録，およびセキュリティ認証取得を前提とした組織の対策データの登録実験を行い，プラットフォームの有効性の検討を行った．

A Study on Validity of Security Evaluation Platform Based on International Standards

Yuji TAKAHASHI† and Yoshimi TESHIGAWARA†

To obtain acquisition of security attestation, the target organization is evaluated based on the international standards. In the organization, the security evaluation system that confirms standards achievement of platform for the attention has been used. In order to correspond to changes of the standards, we have been studying a platform that realizes the evaluation tool corresponding to changes of the standard contents and evaluation targets only by changes of the standards used as evaluation criteria. In this paper, we develop a prototype platform system, and used it on an experimental bases by registrating multiple standard data and counter measures for to platform, and the registration experiment of the measures for the organization to which the security attention was required. In addition, we evaluated its validity of the platform.

1. 研究の背景と目的

近年，セキュリティの目的は，組織の資産を守る自己防衛のためのセキュリティから，セキュリティ被害が原因となる二次的な加害者にならないためのセキュリティまで範囲が拡大している．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行うことが重要視されている[1]．具体的な評価として ISMS 適合性評価制度に基づく ISMS 認証取得がある．この ISMS 認証は認証制度ができて以来取得件数が増加し続けており，2009 年 5 月 22 日現在で 3,182 件と多くの企業・組織が取得している[2].

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, 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[3]．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．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が発生することとなり，多くの時間と労力，費用を必要として企業活動における影響が大きいという問題がある．

このような問題を解決するために，個別のセキュリティ評価ツールではなく，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ツールを実現する仕組みの必要性が高まってきている．

本研究では，対象となる標準に依存せず，プラットフォームの基本となる標準を整理した基本データ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について検討を行ってきた[4]．また，セキュリティ評価についても同様に基準とする標準の内容に依存せず，セキュリティ評価が行える必要があり，プラットフォーム内で標準の内容に依存しないセキュリティ評価のためのスコア算出方式が求められる．

そこで，標準の内容ではなく，その特徴的な構造である階層構造と参照関係に着目し，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たした．また，階層構造と参照関係を利用したスコア計算をすることによって要件の達成を目指

† 創価大学大学院工学研究科
Graduate School of Engineering, Soka University

すプラットフォームの検討を行ってきた．また，ISO/IEC 27001 のデータをそのプロトタイプシステムに登録を行ってプラットフォームについて検討を行ってきた[4].

しかし，これまでの検討では ISO/IEC 27001 のみでプラットフォームについて検討を行ってきたので，その他の標準についても同様に本プラットフォームの仕組みが適応できるのか検討ができていなかった．本稿では，新たに ISO/IEC 27002 のデータの登録を行い，ISO/IEC 27001 以外でもプロトタイプシステムによるデータ使用が可能であるか検討を行う．そして，現場のセキュリティ担当者の視点で，対応策データの登録を行う実験を実施し，その実験により得られたデータに基づき被験者の主観によるセキュリティ評価とプラットフォームに基づくセキュリティ評価の差分調査実験を通して，その評価値から標準の構造に着目したカバー率によるセキュリティ評価の有効性の検討を行う．

2. 標準の分析と活用

2.1 ISO/IEC 27000 シリーズ

ISO/IEC 27000 シリーズとは，国際標準化機構 (ISO) と国際電気標準会議 (IEC) が共同で策定する情報セキュリティ規格群である．このシリーズは対象とする範囲が広く，代表的なセキュリティ問題である，プライバシー，機密，情報技術におけるセキュリティ問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．

このシリーズ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制御を実装することが求められる．また情報セキュリティは固定的なものではないので，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）には PDCA サイクル（Plan-Do-Check-Act cycle）による継続的なフィードバックと改善が要求される．多くの標準の策定が予定されており，現在のところ，以下の 4 つが策定済みであり，他にも多くの標準が準備中となっており，ISO/IEC 27000 シリーズは多くの分野においての基準となる標準群となり ISMS に基づく PDCA サイクル運営の重要性を示している．

(1) ISO/IEC 27001 - 組織の ISMS を認証するための要求事項（2005 年発行）
(2) ISO/IEC 27002 - ISMS 実践のための規範（2005 年発行）
(3) ISO/IEC 27005 - 情報セキュリティのリスクマネジメント (2008 年発行)
(4) ISO/IEC 27006 - 認証/登録プロセスの要求仕様（2007 年発行）

- ISO/IEC 27001

ISO/IEC 27001 とは，規格の名称を「Information technology – Security techniques - Information security management system」といい，ISMS を確立，導入，運用，監視，見直し，維持及び改善するためのモデルを提供することを目的として作成されている[5]. 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，そのすべてを網羅している必要がある．ただし，すべての内容についての対策を必要とする訳ではなく，適用対象外のものは対象外であることが明記されていればよい．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．

- ISO/IEC 27002

ISO/IEC 27002 とは，規格の名称を「Information technology - Security techniques - Code of practice for information security management」といい，日本語訳は JIS Q 27002「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」となる[6]. ISMS を立ち上げ，実装し，運用するための情報セキュリティ管理に関するベストプラクティスを提供する．

元来は 1999 年に発行された英国規格 BS 7799-1:1999 であり，それがそのまま初版の ISO/IEC 17799:2000 となったものであり，2005 年に改訂され，2007 年に現在の ISO/IEC 27002:2005 と改称され，ISO/IEC 27000 シリーズの一部となったものである．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．

本稿では ISO/IEC 27002 を追加データとして分析および登録をする．

2.2 標準の構成

標準では一般的に本文が「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．

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，図 1 で示すように ISO/IEC 27001 の「7.1 一般」は本文中で 4.3.3 参照との記述がある．

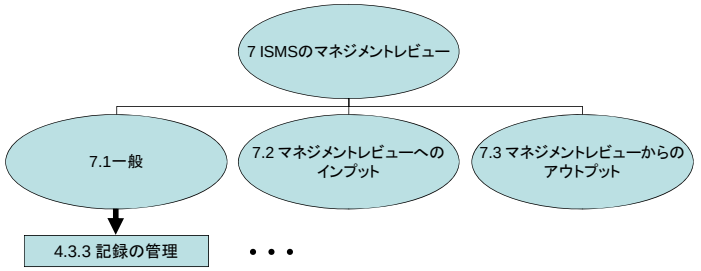

図 1　ISO/IEC 27001 の参照関係の例

2.3 対応策による項目の網羅の困難さと解決策

セキュリティ認証においては，基準を網羅的にカバーする必要があり，構成の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決定を行っていく流れとなる．その際に，各章（管理分野）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，標準ではこういった参照関係が多く，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．

そのため，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．そこで本研究では，階層構造と参照関係は標準が変わっても同様に扱われるため，標準が変わっても同様に標準を扱うことができるという点に着目する．そして，階層構造と参照関係を利用することによって，基準が変わっても章ごとに網羅すべき項目を一括管理できるようなプラットフォームの実現によって問題の解決を図る．

3. プラットフォームの概要

本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 つの部位にわかれている．本プラットフォームの概念図を図 2 に示す．データ入力部で，標準の生データと，2.2 節で述べた階層構造に基づく構造情報，および参照情報の入力を行う．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行う．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，参照ツリーのカバーリングのスコア計算を行う．

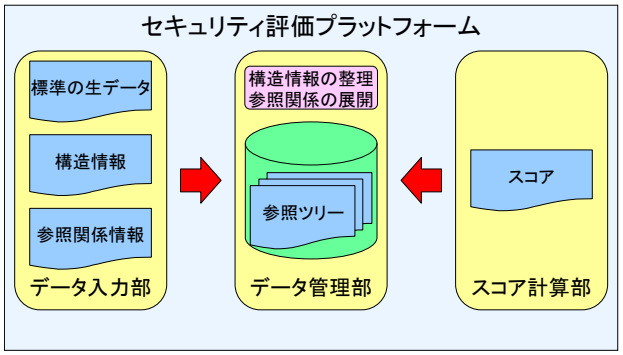

図 2　提案プラットフォームの概念図

構造情報と参照情報は，階層に基づく情報と標準本文に記述されている直接的な参照（以下，直接参照という）情報のみが登録される．本プラットフォームでは階層をレベルと定義し，章をレベル 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き，レベル n はレベル n+1 の項目を直接参照しているとみなす．登録された情報に基づき，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ような場合に，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，複数箇所で同一項目を参照先として持つ複数参照と，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．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 とする．

この参照ツリーを用いて，標準データの管理およびセキュリティ評価のための基準の作成を行う．基準とは，標準の章・節・項を参照親に持つ参照ツリー全体のカバーリングの度合いを測るためのものであり，ツリーの構成要素数を基にスコア計算をするものとなる．本稿で使用しているプロトタイプシステムでは単純に構成要素数を分母とし，対応済項目数の割合を計算する形を採っている [4].

4. 標準データ追加実験

これまでに，実際に ISO/IEC 27001 のデータを登録して，単純なスコア計算をするプロトタイプ開発を行った[4].

今回，ISO/IEC 27001 について管理分野が他の管理分野全体を参照し，更にその管理分野が元の管理分野を参照しているループ参照について，追加で参照情報を登録した．

また，違う標準を同様の構造情報に基づいたデータ登録により複数の標準が取り扱えるということを確認するため，新たに ISO/IEC 27002 のデータを基本データとして登録を行って分析を行った．

4.1 章全体を含むループ情報の追加

これまでの検討では，章ごとにわけてセキュリティ評価を行うことを意識していたため，章全体を参照先として持つような参照については，登録を行っていなかった．

今回のセキュリティ評価実験を通して，章全体を参照とする場合の経験則に基づくセキュリティ評価とプロトタイプシステムが算出する達成度の差分を調査するにあた

り，このようなループ参照の影響を確認するため，参照情報の追加を行った．

4.2 階層構造の解析及びデータ登録

ISO/IEC 27002 の構成としては 1～4 章まではセキュリティ評価の対象ではないので，今回の入力対象データとして 5 章の「セキュリティ基本方針」以下の項目を入力対象とした．

階層としては一番浅い部分で 3 階層，最も深い部分では 5 階層であった．

上記の作業で ISO/IEC 27002 の 5 章から 15 章までで 1,050 件のデータを基本データとして登録を行った．データ数は前回の ISO/IEC 27001 の 160 件に比べて約 6.5 倍のデータ件数であった．

4.3 参照関係の登録

4.2 節のデータに参照関係の設定を実施する．最初に階層構造による参照関係の登録を行い，次に，直接参照の参照情報について登録を行った．続いて，直接参照以外の参照関係を設定する．ここでは複数参照とループ参照の関係があった場合に，距離の短い方を参照親との距離として登録をする．

ISO/IEC 27002 では最大距離は 32，総参照関係数 159,169 という数値が参照データ作成によって確認された．この数値は ISO/IEC 27001 と比べて最大距離が約 2 倍，総参照数は 35 倍という大きな数値となった．しかし，参照ツリーの作成に当たっては，項目数が多い分，時間はかかるものの，ISO/IEC 27001 の時と変わりなく参照ツリーを作成することができた．

今回用いた ISO/IEC 27002 では，ループ参照が多く存在していることが明らかになった．ループ構造の中でも，章が他の章全体を参照し，かつ参照されている管理分野が元の管理分野を参照しているケースは，参照されている管理分野同士が密接な関係にあり，かつ相互の影響が大きいと推察される．

なお，プロトタイプシステムにおけるスコア算出方式では，このような相互参照の関係となるようなケースでは同一スコアが算出されることとなる．具体的な達成度の算出への影響については，5 章の実験にて体感値によるセキュリティ評価と，プロトタイプシステムの算出した達成度の比較を行うことで影響度について考察を行う．

5. セキュリティ評価実験

5.1 実験概要

プラットフォームのプロトタイプシステムを用いて，セキュリティ認証取得を意識した組織のセキュリティ評価を行い，管理分野ごとに被験者の体感による評価値とプロトタイプシステムが算出する評価値の差分調査を行った．また，評価値の差分が生じる管理分野については，範囲を絞り調査を実施し，差分が生じる原因について考察を行った．

5.2 実験環境

今回の実験は，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
- フェーズ
  - ギャップ分析を行う前の段階
- 使用した評価基準
  - ISO/IEC 27001
- 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
- プロトタイプシステムにおける組織評価方法
  - 要求事項に対しての対応策有または対応策無の二者択一

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 のセキュリティ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．対応策の有無とは，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を示している．

5.3 実験の流れ

（手順 1）事前準備

最初に，評価基準に対して目標とすべき評価値を定める．なお，目標値および達成度を決める際には，プロトタイプシステムでは小数第 2 位まで表示されるが，それ以外の目標値と達成度は，人の感覚で決めていくため，すべて 10%刻みとする．次に，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「達成度 1」とする．そして，対応策を管理分野ごとに分けて考える今回の実験に合わせて，頭の中で対応策の情報を整理してもらった段階で，再度達成度を決定する．ここで決定した達成度を「達成度 2」とする．達成度 2 が最初に設定した目標値を下回った場合は

指摘有りとし，「指摘 1」とする．

（手順 2）プロトタイプシステムを用いた対応策登録および情報修正

事前の情報収集および目標設定，達成度の判断が終わった後に，プロトタイプシステムを用いて，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，入力終了後に，システムを使って対応策の内容を整理したことによって達成度を修正した方がよいと思った管理分野については，達成度を修正する．ここで決定した達成度を「達成度 3」とする．ここでも，指摘 1 と同様に指摘の有無を判別し，指摘有となったものは「指摘 2」とする．

本来のギャップ分析では，対応がなされていない項目についてピックアップしていく方式を採ることが多いのだが，今回の実験では PDCA サイクルを意識しており，今後，対応できなくなったり，予想通りの効果を得られなかったりした対応策の情報を容易に修正できるように，あえて対応済み項目の情報を作成する手法を採ることとした．

（手順 3）プロトタイプシステムによるスコア算出

入力されたすべてのデータ登録を基に，プロトタイプシステム上でスコアを算出する．プロトタイプシステムでは，管理分野ごとに参照ツリーを構成し，参照ツリーの頂点の根となる部分の達成度について，根を除くすべてのノードを対象としてカバー率を算出している．ここで算出したスコアを「達成度 4」とする．ここでも，指摘 1 および 2 と同様に指摘の有無を判別し指摘有となったものは「指摘 3」とする．

（手順 4）達成度の差分調査

達成度 2 から達成度 3 の値を引き差分を計算し，達成度 4 から達成度 3 を引き差分を計算して達成度の差分調査を行う．前者を「差分 1」，後者は「差分 2」とする．差分調査では，差分があったものについては，被験者に差分が生じた理由についてヒアリングを行い，その理由を確認する．差分 2 で差分大となったものについては，管理分野の参照ツリーを確認して，参照ツリーがどのような構造になっているのかを確認する．

（手順 5）指摘の原因分析

指摘 1～3 の管理分野について，詳細分析として管理分野よりひとつ下の階層の項目についての評価を確認する．具体的には，指摘 1 および 2 では，指摘内容としてどの管理項目が指摘の要因となっているのかを被験者が手動で選択していき，指摘 3 ではプロトタイプシステムが算出したスコアが低い項目を指摘の要因であると判断する．

なお，実験で使用したプロトタイプシステムでは，標準の各項目に対して，対応策の有無のみを入力する形式となっており，各項目について適用対象外と設定する機能を有していない．そのため，実験を行ったギャップ分析のフェーズよりも前のフェーズで，対象組織の状況に応じて適用対象外とする項目が発生していた場合があったとしても，スコア計算および参照ツリーの構成の際に適応対象外とした項目が含まれてしまう可能性がある．

5.4 実験結果

● 手順 1：事前準備

認証取得に対して，意欲的に取り組む姿勢を示しており，目標はすべての管理分野に対して表 1 で示すように，100%を目標としていることがわかった．しかし，現状ではまだ認証取得に対して動き始めたばかりということもあり，達成度 1 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%であるとの認識である．現状のヒアリングの後に，状況を基準（この場合は ISO/IEC 27001）の内容に沿って整理をして，被験者には改めて達成度 2 を決定してもらった．その結果は表 1 のように下方修正された．下方修正の原因は，要求事項レベルで管理分野ごとの達成度の再検討を行ったことにより，より認証取得を意識した状況を把握することができ，ヒアリング結果よりも慎重な数値を取るという理由による．以上の結果から，この組織は現状ではすべての管理分野が指摘 1 に該当すると判断した．

表 1　事前情報

管理分野	事前情報			
	目標値	達成度1	達成度2	指摘1
4. 情報セキュリティマネジメント	100%	30%	20%	有
5. 経営陣の責任	100%	70%	50%	有
6. ISMSの内部監査	100%	0%	0%	有
7. ISMSのマネジメントレビュー	100%	0%	0%	有
8. ISMSの改善	100%	0%	0%	有

● 手順 2：プロトタイプシステムを用いた対策登録および情報修正

セキュリティ認証の取得に初めて望みかつ，ギャップ分析の段階ということで，現状，対応がすでにできている項目は少なく，網羅性も低いデータとなった．続いてプロトタイプシステムの入力を通して，基準の構成全体を意識しながら情報の整理を行った結果として達成度を決定する．この結果，表 2 で示すように，達成度 3 は達成度 2 から変化はなかった．達成度の変化がなかったため，すべての管理分野が指摘 2 に該当するという結果になった．

表 2　事前情報とプロトタイプシステム使用後の比較

管理分野	事前情報		対策登録終了時		
	目標値	達成度2	達成度3	指摘2	差分1
4. 情報セキュリティマネジメント	100%	20%	20%	有	0%
5. 経営陣の責任	100%	50%	50%	有	0%
6. ISMSの内部監査	100%	0%	0%	有	0%
7. ISMSのマネジメントレビュー	100%	0%	0%	有	0%
8. ISMSの改善	100%	0%	0%	有	0%

● 手順 3：プロトタイプシステムによるスコア算出

プロトタイプシステムによるスコア算出の結果は，表 3 のようになり，5，7，8 の管理分野で同じ達成度が算出された．これは，これらの管理分野がお互いの管理分野全体を参照しているループ構造をとっていることが原因である．

表 3　プロトタイプシステムとの比較結果

管理分野	対策登録終了時		プロトタイプシステム		
	達成度3	差分1	達成度4	指摘3	差分2
4. 情報セキュリティマネジメント	20%	0%	11.32%	有	-8.68%
5. 経営陣の責任	50%	0%	13.24%	有	-36.76%
6. ISMSの内部監査	0%	0%	13.24%	有	13.24%
7. ISMSのマネジメントレビュー	0%	0%	0.00%	有	0.00%
8. ISMSの改善	0%	0%	13.24%	有	13.24%

● 手順 4：達成度の差分調査

表 1 表 2 から，差分 1 については差分がないとの結果になった．これは，事前段階で情報を整理する際に，すでに標準の内容を確認して達成度を出していたため，変化がなかったと推察される．ヒアリング結果でも同様内容と，今回の達成度の粒度が 10%刻みということもあり，体感値での大きな変化がなかったことも理由のひとつとしてあげることができるとの回答を得ることができた．

次に，差分 2 については，表 3 で示すような差分が発生した．4 と 5 の管理分野ではプロトタイプシステム側の評価が低く，6 と 8 の管理分野では逆にプロトタイプシステム側の評価が高く，7 の管理分野では差分無しというで 3 通りの結果となった．それぞれの達成度 4 がこのような結果となった要因を分析し，結果について被験者にヒアリングを行いつつ差分発生の原因について考察を行う．

被験者に実際の参照ツリー全体構成を確認してもらいつつ，プロトタイプシステムの算出方式を説明し，被験者の達成度を決める指標とのギャップを確認する作業を行う．

● 手順 5：指摘の原因分析

今回の実験では目標値がすべて 100%でかつ，ギャップ分析のフェーズですべての対応が浣腸していないということもあり，指摘 1～3 ですべての管理分野で指摘有りとの結果になった．今回の分析では，管理分野における各管理対策方針のついての達成度を詳細に決定するのではく，原因となる項目を選択する形式とし，ヒアリングを実施して，プロトタイプシステムとの達成度の比較を行う．この中で，管理分野 6，7，8 では達成度 2，3 で 0%との結果であるので，原因を抽出する対象とするのは難しいと判断した．そのために，管理分野 4，5 についてのみ原因分析を行う．

まず，管理分野 4 に関しては，表 4 で示すように，ヒアリングでは 2 つの項目が原因であると判断されたが，プロトタイプシステムでは 4.1 の項目のみが 4.の項目の達成度を下回るスコアを算出する結果となった．

表 4　情報セキュリティマネジメントに関する指摘原因分析

管理分野	指摘の有無	管理対策方針	原因の有無	スコア
4. 情報セキュリティマネジメント	有	4.1. 一般要求事項	有	0.00%
		4.2. ISMSの確立及び運用管理	無	13.24%
		4.3. 文書化に関する要求事項	有	11.46%

管理分野 5 に関しては，表 5 に示すように，ヒアリングの結果は，項目 5.2 の方に原因があるのではないかとの回答を得られた．一方，プロトタイプシステムが算出した達成度は共に 13.24%となりここでも参照ツリーのループ構造によって同じ要素で構成されている参照ツリーとなっていることの影響が出ている結果となった（図 7 参照）．しかし，5.1 と 5.2 の参照ツリーの構成要素のうち，対応策有となる項目は，参照ツリーの根に近い部分にあることがわかった．このことから体感による，達成度を決定する際には，距離の短い項目の影響が大きいと推察される．

表 5　経営陣の責任の指摘原因分析

管理分野	指摘の有無	管理対策方針	原因の有無	スコア
5. 経営陣の責任	有	5.1. 経営陣のコミットメント	無	13.24%
		5.2. 経営資源の運用管理	有	13.24%

また，管理分野 4，5 問わず適応対象外の項目が含まれていることによって達成度に微妙な差異が生じている可能性も多いのではないかとの指摘もあった．

5.5 実験の考察

● ケース 1：差分調査においてプロトタイプシステム側の評価が低い場合

このケースは，管理分野 4 と 5 の差分の数値に大きな開きがあるので，5 の管理分野にはより大きな特徴があるのではないかと推察できる．最初に，管理分野 4 の結果について参照ツリーを確認しつつ差分の原因を考察した結果，参照ツリーでは根から距離がある項目なると，ひとつの要求事項について細かい条件を示している部分となってきているので，根からの距離が離れるほど体感値による達成度に影響する度合いが下がっているのではないかとの指摘があった．

続いて，管理分野 5 の参照ツリーを確認しつつ，大きな差分が出ている結果につい

ての考察を行う．この参照ツリーでは，管理分野 7 と 8 の全体を相互に参照しているループ構造をとっていることが明らかになった．今回の実験では，管理分野 6 以降の項目については，PDCA サイクルがまだ回っていないので，未対応であるとの入力が行われている．被験者からは，管理分野の意味合いからも，関係性は非常に深いことは正しいと思われるが，達成度に関する影響度が大きすぎるのではないかとの指摘があった．このことより基準とする管理分野が異なる参照項目のスコア計算への影響度を下げられるような仕組みが必要であるとの指摘があった．

- ケース 2：差分調査においてプロトタイプシステム側の評価が高い場合

このケースには，管理分野 6，8 が該当する．今回のケースでは，管理分野 5，6，8 の達成度 4 が一致している．これは，ツリーの構造に差があるもののノードについてはまったく同じ構成要素となっていることが理由である．従って，3 つ管理分野の達成度に差がなく，直接的に対応ができていない管理分野についても達成度が提示されることになった．ただし，達成度が提示されていること自体には被験者の同意を得ることができた．その理由としては，例え管理分野そのもので問われている内容が，すべてできていなくとも他の影響を受け達成度が上がる，という観点は同意でき，このようなケースも正しいと言えるとのことであった．しかし，先の管理分野 5 での考察結果からもわかるように管理分野をまたいだ参照では，達成度への影響度が同じであるべきではないという考えから差分としての数値が大きすぎるとの指摘があった．管理分野 5，6，8 に基づく考察結果としては，参照に基づき他の管理分野の項目によって達成度が高くなるケースがあるが，管理分野をまたいだ場合の達成度への影響は低くあるべきであるとの指摘を得ることができた．

- ケース 3：同じレベルの項目で達成度 4 が同じ場合

今回の実験では，管理分野 5，6，8 と管理対策方針 5.1，5.2 がそれぞれ該当する．このような結果となる原因は，達成度の算出方式が，構成要素数のみを用いてからである．指摘の原因分析で，参照ツリーにおける対応策有となる項目を確認した際に，それぞれのツリーで対応策有の項目の距離が異なり，体感に基づく達成度では，距離が長い項目について対策ありとなっているケースの方が原因であると挙げられている．このように達成度を算出する際には，距離により影響度を変えるべきであると推察される．

以上の分析結果より，スコア計算については，距離を考慮して達成度を計算する必要性が高いのではないかと推察される．また，管理分野をまたぐ参照を持つ場合には，管理分野が異なる参照項目のスコア計算結果への影響度が下げる仕組みが必要であると推察される．実際に実験結果として，階層構造のみを意識して達成度を決めた場合には 0%となるケースであっても，参照ツリーを構成して他の管理分野の影響を反映されるようになった場合に，例えその管理分野としての対応をしていない場合であっても全体の達成度があがるという結果を得ることができ，その概念に被験者の同意を得ることができた．しかし，その同意には影響度を考慮すべきであるとの条件があり，そのことは原因分析の際にも同じような結果が出ることとなった．

そして，参照ツリーを構成することによって，評価項目が網羅すべき項目の関係を視覚的に表現することができているのではないかということである．参照ツリーにおける距離の概念を的確に利用することにより，この関係性をより明確に示していると推察される．また，この距離の概念は達成度にも大きく影響を及ぼすであろうことが実験を通して推察することができた．

プロトタイプシステムについても，ユーザインタフェースの課題を多く発見することができた．プロトタイプシステムでは，対応策について対応済と未対応という二者択一の状態でデータの登録を行った．その結果，適応対象外となる項目の対応状況が，未対応扱いとなったり，承認段階でまだコミットメントが取れていない，現在対応が進行中の対応も，また未対応という形で登録をせざるを得なかったりしたとのコメントを得た．また対応策の最終判断は対応済または未対応となる部分になる部分については問題ないのだがセキュリティ評価を行う段階がどのフェーズに該当するのかによって選択できる内容を増やしたほうがより効果的なインタフェースであるというコメントも得た．

6. 今後の課題

- 登録データに関する課題

今回は ISO/IEC 27002 ベースのデータ追加を行ったが，この他の標準についても同様にセキュリティ評価のためのデータとして使用できるか検討する．具体的には，ISO/IEC 27000 シリーズの他の標準を中心に，引き続きデータの登録を検討している．

また，対応策登録については，現在の対応済と未対応といった形だけでなく，適応対象外，コミットメント申請中といった選択肢を加えてより肌理細やかな対応策設定および柔軟な選択ができるようなプロトタイプシステムの開発を行う．本プラットフォームでは複数の標準で類似する内容のものを相互に参照できるようにすることを考えている．将来的には基準となる標準をひとつと限定せずに複数の標準についても同時に対策設定を行えるものを目指す．標準のバージョンアップ時には下位バージョンの設定を活用できるものを目指す．また基準となる標準が項目内容の更新ではなく，変更が行われた場合，元の標準で設定を行った対策の情報を新しい標準向けに自動で変換できるものを目指す．

- スコア算出に関する課題

実験結果として参照関係の距離によって参照ツリーの根に当たる部分から距離がある項目については，影響度が異なる方が体感値に近いとの回答が得られている．この回答に基づき，距離を考慮した達成度の計算方法を検討する．

更に実験結果として管理分野が異なる参照を持つ参照ツリーについては他の管理分野の項目の影響度を下げて達成度を計算する方が体感値に近いとの回答が得られた．この回答に基づき，管理分野が異なる参照についての影響度についての検討をする．

- 追加実験に関する課題

本稿ではギャップ分析のフェーズにおいてセキュリティ評価の実験を行った．今回のフェーズ以外でも詳細リスク分析を行っているフェーズであったり，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フェーズであったりといった複数の組織の状態における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行う．

7. まとめ

本稿では，対象となる標準に依存せず，プラットフォームの基本となる標準を整理したデータ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について述べ，その有効性についての検討を，データ追加実験とセキュリティ評価実験を通して行った．

データ追加実験により，ISO/IEC 27001 や ISO/IEC 27002 のように，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データとして使用できるのではないかということについて検討を行った．実際に ISO/IEC 27002 の登録に問題はなく ISO/IEC 27001 だけがデータとして登録できるものではなく,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．

また，実際にセキュリティ認証の取得を意識した組織のセキュリティ評価をプロトタイプシステム上で行うことで，本プラットフォームのスコア算出方式の有効性の検討と，課題の洗い出しを行った．参照ツリー構成と達成度算出について，実際のデータに基づく分析を行い，参照ツリーが項目間の効果的な情報を提供できるのではないかとの意見を得た．このことは，参照ツリーを構成し，提示することが，正確なセキュリティ評価を行う上で有益であるということを示している．

また，達成度については各項目についての影響度を参照ツリーの項目間の距離および参照先が標準の章をまたがった際の影響度について考察を行った．参照ツリーを構成する要素数だけに着目するスコア算出方式では，体感値との間の差分が大きく，算出される達成度に違和感があるとの問題が明確になった．また，参照先に章をまたぐような項目が含まれる場合も，算出される達成度に違和感があるとの問題が明確になった．これら 2 つの問題点を解決するために，項目間の距離と，章をまたぐ参照先に関する達成度への影響度を考慮した,達成度算出方式を検討することが課題となった．

そして，プロトタイプシステムのユーザインタフェースについては，対応策登録について，対応策有と対応策無といった二者択一では，状況を的確に登録できないとの問題が明確になった．この問題を解決するために，各項目について設定できる対応策の状況の追加が課題となった．

今後は 6 章で述べた課題に取り組み，多くの標準で適用できること，算出されるスコアの改善，様々なフェーズでの適応を確認し，プラットフォームの有効性を高めていく．

謝辞　本稿の実験にご協力頂いた ISMS 審査員補の足田様に，この場をお借りして謹んで感謝の意を表する．

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＞，平成 17 年 5 月
2) 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) 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
4) 高橋雄志, 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)
5) ISO/IEC 27001 Information technology - Security techniques - Information security management system - Requirements, 2005
6) ISO/IEC 27002:2005 Information technology - Security techniques - Code of practice for information security management