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

髙橋雄志† 勅使河原可海†

セキュリティ認証取得に対し，国際標準等を基準として対象を評価する．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．本研究ではこれまで，標準の変化に対応するため，個別の評価ツールではなく，評価基準とする標準の変更のみで標準内容や評価対象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，これまでの実験結果で課題として挙げている評価値計算に関して改善を行い，より専門家の体感値に近い値を算出することができるようになったことが確認できた．また，前述の課題に対して，本プラットフォームの特性を活かし，担当者に適切な情報提示を行う機能の追加を行うことで解決を目指す．過去事例のデータから，セキュリティ認証を意識した対応策と標準の項目の関係性のデータを作成し，セキュリティの知識がそれほど多くない担当者に提示し，的確な対応策の選定をサポートする機能の追加を行った．その有効性の検討の為に，認証に関する知識がそれほど深くない被験者に対してシステムの利用実験を行った．

A Study on Measures Presentation Function for Non-Professional Persons of Security Evaluation Method Based on Reference Relationships among 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 organizations, the security evaluation systems that confirm standards achievement of the platform for the attestation have 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 standards contents and evaluation targets only by changes of the standards used as evaluation criteria. In this paper, an evaluation value calculation that has been enumerated as a problem in a current outcome of an experiment is improved, to calculate values close to the values of specialists. In addition, to the above-mentioned problem, it aims at the solution by adding the function to present the person in charge the relevant information of characteristics of the platform is made the best use of. Related data of countermeasures to consider the security attestation and standard items are made from the data of the case in the past, the function to support the selection of an adequate countermeasure was added to present it to the person in charge who doesn't have enough knowledge of security. The experimental use of the system was executed to the person who have not deep knowledge concerning the attestation for the evaluation of the effectiveness of the proposed system.

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

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する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 認証は認証制度ができて以来取得件数が増加し続けており，2011 年 5 月 20 日現在で 3,797 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．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．

これまでの検討では，セキュリティ認証取得部門の担当者については，認証に関し

て十分な知識を有しているとの前提で検討を進めてきた．しかし，研究の大目的となる標準内容の変化に対応できるという意味では十分な知識を有していない者を対象として，十分な知識を有している者と同様に評価が行えることも重要な課題としてあげることができる．だが，認証に関する知識を十分に有しているとは言えない担当者が，一からすべての標準の項目に対応する対応策を選定することは，標準の項目数や，項目間の複雑な参照構造などを理解していないと適切に選び出すことは大変困難である．

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]．本プラットフォームでは，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した．また，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要件の達成を目指すプラットフォームの検討を行ってきた．そして，プロトタイプシステムの開発を行い，ISO/IEC 27000 シリーズのデータを登録してプラットフォームについて検討を行ってきた[5]．プラットフォームで使用するセキュリティ評価についても同様に，基準とする標準の種類に依存せず，セキュリティ評価が行える必要があり，標準の種類に依存しない評価値算出方式が求められる．これまでの検討でセキュリティ評価について後述する参照ツリーの各構成要素に対して評価に対する影響度を変化させてセキュリティ評価をし，参照ツリーの距離に着目したセキュリティ評価方式について実験を行ってきた結果，距離だけでなく評価項目と各項目の関係により影響度を変えることが有効であるとの知見を得た[6]．本稿では，セキュリティ評価についての改善を行うと共に，新たに本プラットフォームの特性を活かし，担当者に適切な情報提示を行う機能の追加を行うことで前述の知識を十分に有しているとは言えない担当者に関する問題の解決を目指し，実験および検討をする．

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，ISMS 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いる．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）

2.2 ISO/IEC 27001

ISO/IEC 27001 は，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[7]．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．

2.3 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，ISO/IEC 27001 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 1 で示すような形で表現する．

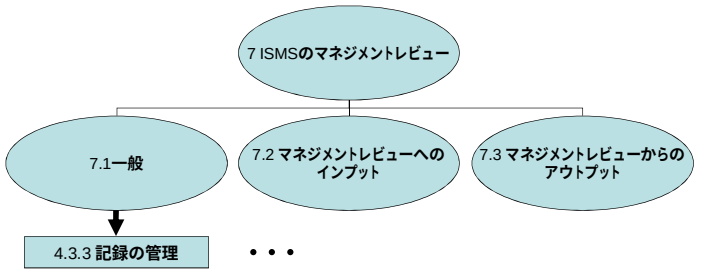

図 1　ISO/IEC 27001 の参照関係の例

2.4 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．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．

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．標準で本文記述されている階層構造と参照関係は，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ため，標準の変更や異なる標準であっても同様に特徴情報として扱うことができる，そこで本研究では，階層構造と参照時関係について着目する．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

3.1 プラットフォームの構成

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構成を図 2 に示す．データ入力部で，標準の生データと，構造情報，および参照情報の入力をする．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. さらにスコア計算部で計算された評価値の管理もする．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．また，今回の機能追加によって新たに対応策情報をデータ提供する設定に限りサンプルデータを作成してデータ管理部にフィードバックするようになった．スコア計算部ではサンプルデータを参照しながら対応策の情報入力を行うこともできるようになった．

3.2 プラットフォームの動作

最初にデータ入力部にてデータの入力作業をする．まず標準の生データを登録する．そして，登録したデータに対して 2.2 節で述べた階層構造に基づく構造情報の登録をする．続いて参照関係情報の登録をする．ここで登録をする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．データの登録がすべて完了したら登録情報をデータ管理部に受渡し次の動作に移行する．

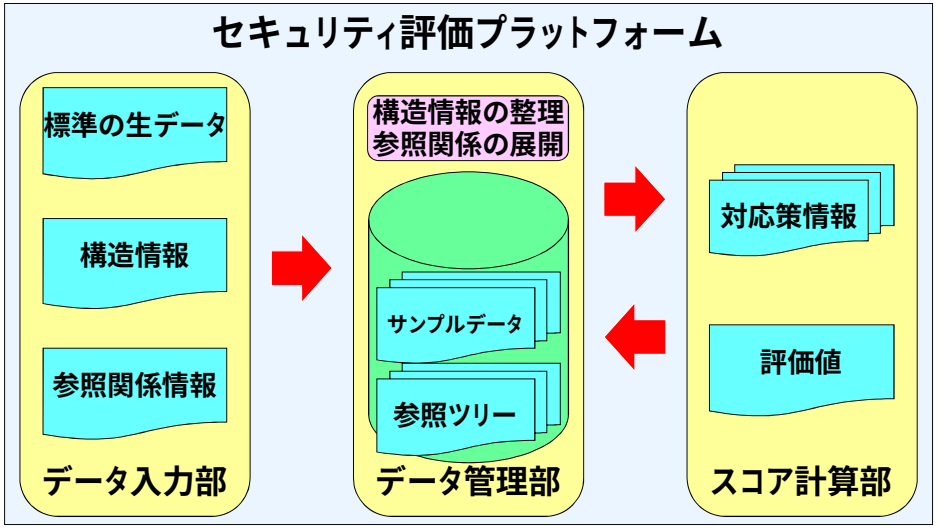

図 2　提案プラットフォームの構成

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 m はレベル m+1 の項目を直接参照しているとみなす．

続いてデータ管理部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，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の展開をする．

スコア計算部ではこの参照ツリーを用いて，セキュリティ評価のための基準の作成をする．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評価値を測るためのものである．実際には参照ツリーの情報を用いた対応策施行情報とサンプルデータによる過去の案件での対応策と標準の各項目のマッピングデータの提示を行い，対応策の施行情報の入力を促す．入力された対応策情報と参照ツリーの情報に基づき評価値計算をするものとなる．また，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マッピング情報のうち対応済みとなっているデータをサンプルデータとして取得し,該当する対応策のサンプルデータとしてデータ管理部に送る．データ管理部に送られたサンプルデータは，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）で標準とのマッピングを行う際に提示されサンプル情報を参考にしながらマッピング作業を行うことができる．本稿では評価値計算について変更を加えた結果の考察と，サンプル提示機能についての検討を行った．

3.3 プラットフォームの特徴

このプラットフォームでは標準に変更があった場合にデータ入力部での情報更新をする．情報更新の後にデータ管理部で自動的に参照ツリーを再構成し，スコア計算部でスコアの再計算をすることによって変更された標準の内容に沿った再評価をすることができるものである．

また，参照ツリーを構成することによって項目間の関係性を視覚化することができる．この参照ツリーを確認しながら対応策の選択をすることで効果的な対応策を設定することの手助けをすることができる．

サンプルデータの表示機能を追加することによって専門知識を十分に有しているとはいえない管理者に知識共有ができるようになった．

4. 参照ツリーの各構成要素の影響度算出方式

これまで，参照ツリーの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てきた．また，参照ツリー内で他の章の項目を参照している場合に，その項目について計算結果における影響度を変更することが有効であるとの結果を得ることができた．本稿では文献[6]で採用した二つの重み付けを参照ツリー内で評価する項目と同じ章の項目と異なる項目でそれぞれ別の方式を採用した評価値計算を行った結果を，個々の評価値計算方式の結果と比較して有効性の検証を行った．

4.1 最大距離依存型評価方式（方式 1）

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 $Score_1$ を(1)式に示す．

$$Score_1 = \frac{\sum_{i=1}^{n}\{x_i(d_{\max} - d_i + 1)\}}{\sum_{i=1}^{n}(d_{\max} - d_i + 1)} \quad (1)$$

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 3 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．

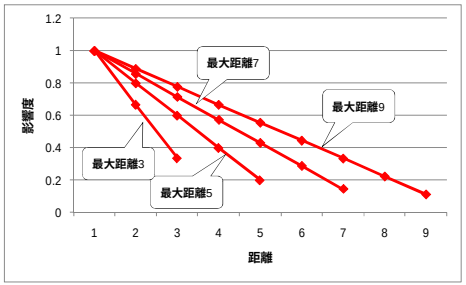

図 3　方式 1 の影響度推移

4.2 距離の逆数型評価方式（方式 2）

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．評価値 $Score_2$ を(2)式に示す．

$$Score_2 = \frac{\sum_{i=1}^{n}\frac{x_i}{d_i}}{\sum_{i=1}^{n}\frac{1}{d_i}} \quad (2)$$

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．

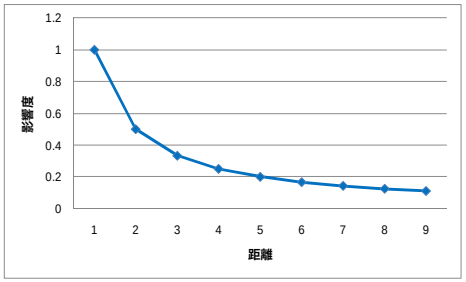

図 4　方式 2 の影響度推移

4.3 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（方式 3）

本稿では文献[6]の実験結果により得た，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できるという知見に着目し，評価項目と構成要素の章が同じ場合に方式 1 を，章が異なる場合に方式 2 を採用する方式 3 を提案するものである．

この方式 3 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．

5. 評価値比較実験

5.1 実験概要

文献[5]で行った実験で取得した，被験者による評価値，回答をしてもらった対応策情報を抽出．対応策情報に基づいて，方式 1，2 と 2 つを組み合わせた方式（以下，方式 3 という）を用いて再度評価値計算を行って被験者の評価値との比較調査をした．

5.2 情報取得環境

文献[5]で行った実験で取得した対応策の情報は，以下の条件のもと実施した実験の結果を使用した．

- 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
  - ギャップ分析をする前の段階
- 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

ギャップ分析とは具体的には，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，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，分析を実施している状態となる．ヒアリングをした組織は，ISO/IEC 27001 のセキュリティ認証を取得することを目的としており，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）基準値の取得

文献[5]で行った実験で被験者によって入力された対応策情報と最終的に決定した評価値を抽出する．そして，比較の基準値はここでの評価値を使用する．

（手順 2）評価値の再計算

手順 1 で抽出をした対応策情報を用いて，方式 1～3 の手法を用いて評価値の再計算をする．

（手順 3）評価値の比較検討 1

基準値と方式 1～3 により算出された評価値との差分 1～3 をとる．得られた数値を比較検討し方式 3 によって評価値の改善ができたのかを検証する．

5.4 実験結果

(1)　手順 1：基準値の取得

文献[5]で行った実験では，5%刻みで値の回答をもらった．その結果を表 1 で示す．

表 1　基準となる評価値

管理分野	被験者の評価
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%

(2)　手順 2：評価値の再計算

再計算によって表 2 で示すような結果を得ることができた，今回の実験でも「7. ISMS のマネジメントレビュー」についてはすべて 0.00%となったため，検討の対象外とした．

表 2　評価値再計算

管理分野	方式1	方式2	方式3
4. 情報セキュリティマネジメント	11.92%	10.45%	13.98%
5. 経営陣の責任	10.79%	13.36%	18.06%
6. ISMSの内部監査	10.34%	10.14%	4.91%
7. ISMSのマネジメントレビュー	0.00%	0.00%	0.00%
8. ISMSの改善	8.78%	8.59%	1.84%

(3)　手順 3：評価値の比較調査 1

被験者の評価値と方式 1～3 との比較結果は，表 3 のようになる．

表 3　基準値と方式 1～3 との比較結果

管理分野	被験者の評価	差分1	差分2	差分3
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%***
8. ISMSの改善	0%	8.78%	8.59%	***1.84%***

上記の結果より方式 1 および 2 を単独で使用した場合に比べて方式 3 では大きく値を改善することができた．

5.5 実験の考察

文献[6]の実験結果から得られた，参照ツリーの根となる要素と各構成要素の章が異なる場合に影響度を変えた場合に評価値の改善ができるのではないかという結論に基づき元々の影響度変更方式のみを採用した場合との比較を行い改善できたことが確認できた．この結果より参照ツリーの根となる要素と各構成要素の章が等しい場合は各構成要素の評価値に与える影響度は距離に応じて低下していくものの極端に低下せずゆるやかに低下していく方が人の感覚値に近いということが考察でき，一方参照ツリーの根となる要素と各構成要素の章が異なる場合は各構成要素の評価値に与える影響度は距離に応じて低下していき極端に低下していく方が人の感覚値に近いということが考察できた．

以上の分析結果より，参照ツリーを用いた評価で経験則に基づく評価に近付けるためには，距離が小さく各要素の章が等しい場合の影響度は高く，距離が大きく各要素の章が異なる場合の影響度は低い評価方式が有効であるといえる．また，その影響度の算出方式を一定ではなく途中で切り替えることでよりよい評価をすることができるようになったと言える．

6. サンプル提示機能に関する実験

6.1 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のマッピングする作業のサポートができるのかを調査した．

6.2 実験環境

今回の実験では以下の環境のもとサンプルデータを作成，実際に対応策と標準の項目のマッピング作業を行った．

- 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

- 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

本実験での評価フェーズでは実際に施行されている対応策を研究室の管理者に対してヒアリングを行い，その内容を標準の各項目に当てはめていく段階となる．

被験者の所属する研究室が，ISO/IEC 27001 のセキュリティ認証を取得すると仮定して各項目へのマッピング作業を行った，そのため，対応策を選択する段階で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特徴がある．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．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みという扱いにした．

6.3 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全体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マッピング作業を行う．

（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基準でマッピングを行ったのか，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．

6.4 実験結果

(1) 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マッピングを行い，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．

(2) 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マッピング処理を手作業で行った．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マッピングする結果となった．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．

(3) 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．

(4) 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．

(5) 手順 5：被験者へのヒアリング

手順 1〜3 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．

6.5 実験の考察

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．

7. 今後の課題

7.1 評価値算出に関する課題

実験結果からわかるように，今回の実験で使用した評価値算出方式で結果の改善をすることはできた．しかし，人の感覚値を表現するにはまだ改良の余地があることがわかった．今後も，様々な評価値計算方式を試し比較検討をし，その有効性の検討を引き続きする．

7.2 サンプル提示機能に関する課題

この機能については，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．

7.3 追加実験に関する課題

本稿では，現状分析のフェーズにおいてセキュリティ評価の実験をした．これまでの実験でギャップ分析のフェーズで実験を行ってきた．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．

8. まとめ

本稿では，人の手によるセキュリティ評価の概念をシステム的に表現することを目的とし，複数の評価方式を用いて，同じ条件下でセキュリティ評価し，その評価値の比較を通して，それぞれの評価方式の有効性の検討をした．

人の手による評価値と参照ツリーの各項目の性質によって評価への影響度を変える方式の比較実験を通して，評価値算出方式が改善されているかの検討をした．実際のデータを用いて評価値算出と比較をした結果，評価値に対する各構成要素の影響度は距離に応じて変化させることによってすべての項目を同じように影響度を変更させた時より改善されるということが分かった．

また，サンプル提示機能の実験で，参照ツリーによる項目間の関係性を視覚的に表現することが有効であること，サンプル提示によって的確な判断をサポートしていけることがわかった．

今後は 7 章で述べた課題に取り組み，評価値算出に対する影響度算出の改善，サンプル提示機能に関する課題に対してのアプローチを検討し，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) 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) 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
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) 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)
6) 高橋雄志，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，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
7) ISO/IEC 27001 Information technology - Security techniques - Information security management system - Requirements, 2005