4E-5

セキュリティ評価プラットフォームにおける国際標準間の関連情報作成手法の提案と実装

太田 悟† 高橋 雄志† 勅使河原 可海‡ 篠宮 紀彦†
†創価大学工学研究科 ‡東京電機大学未来科学部

1 はじめに

近年，組織はサイバー攻撃の情報資産に対するリスクを適切に管理する必要がある．そのため，政府機関などによりセキュリティ水準を定めたガイドライン（以下，セキュリティ標準）が策定されている [1]．これに伴い，組織の情報資産に対するリスクへの対策状況を，外的機関からの認証を取得することで，利害関係者からの信頼を獲得することが重要視されている [2]．

セキュリティ標準の適切な管理策の実現には，IT システムとセキュリティの専門知識が要求されるが，その両方の専門知識を持つ人材は不足している [3]．そのため，認証取得に必要な要求事項の達成度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 [4]．しかし，組織の規模や製品によってセキュリティ認証の取得範囲や満たすべき要求事項が異なり，単一のセキュリティ評価システムでは評価を行うことが困難である [5]．このような問題を解決するためには，標準の内容や適応範囲に依存しない統合的なセキュリティ評価ツールを実現する必要性があると考えられる．

2 研究目的及び，期待される効果

先行研究では，評価の対象となる標準を整理したデータの入れ替えのみで，評価が可能な統合的なセキュリティ評価プラットフォームを提案してきた [6]．本稿では，セキュリティ評価プラットフォームにおける，異なる標準間でのデータ移行機能に注目する．データ移行機能とは，ある標準 X の対応策の情報を標準 Y の対応策のサンプル情報として提示する機能である．この機能を利用する際には，異なる標準間で同じ項目内容を示す関連情報を必要とするが，必ずしも関連情報が定義されているとは限らないという問題がある．そこで，異なる標準の項目間の相関を取ることで標準間の関連情報を導出する新たな機能を提案し，実装する．

本機能の実装により，異なる標準間において同じ内容の要求事項を判別することが可能となる． 応用例としては以下のことを確認できる．

- 標準が更新された際，旧版と異なる章や新たに作られた章に移った対応策の項目．
- 国際標準などを元に組織内標準などを作成する際，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どうか．
- 既存の組織内標準を用いて認証取得を目指す際，どの程度の要求事項を満たしているのかどうか．

以上が挙げられ，新規の標準を定義する際に，元となる標準との親和性を確かめることが可能となる．

3 相関分析手法

異なる標準の項目間の相関を取る方法は，自然言語処理の手法を用いる．具体的には，文書の言語表現から内容情報を抽出し形式化する処理を行い，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 [7]．

はじめに，関連情報算出の対象となる標準のテキスト情報から，項目ごとに形態素解析を行い，索引語を抽出する．その後，索引語に文書の重要度に応じた重み付けを行う．次に，各項目の重みから項目間の近似度を算出する．最後に，得られた近似度がどちらの標準から見ても最大である項目の組を相関があるとする．

4 関連情報の再現実験

すでに標準間の関連情報が公開されている『ISO/IEC 27001 附属書 A』（以下，標準 A）と『ISMS 認証基準 Ver.2.0 附属書「詳細管理策」』（以下，標準 B）を用いて実験を行う．相関分析手法を用いて標準 A，B の相関を取り，公開されている関連情報（以下，関連情報）をどの程度再現できたか検証，分類する．抽出の分類は，「関連情報の項目を正しく抽出できた組」を OK，再現できなかったもののうち，「関連情報には定義されていないが，相関がある項目の組として抽出された組」を FP（False Positive），「関連情報には定義されているが，相関がある項目として抽出することができなかった組」を FN（False Negative），「本来，相関があるとして抽出すべき項目とは違う項目との相関があるとして抽出された組」を NG（No Good）と定義する．

4.1 実験手順

手順 1： 各標準の索引語の抽出および重み付け

標準 A，B において「章・節・項」（以下それぞれ，大

a Pertinent Information Creation Method Between International Standards in Security Evaluation Platform and Its Implementation
†Satoru OTA †Yuji TAKAHASHI ‡Yoshimi TESHIGAWARA †Norihiko SHINOMIYA
†Graduate School of Engineering, Soka University
‡School of Science and Technology for Future Life, Tokyo Denki University

表 1: 抽出結果の分類と再現率，確からしさ

項目	PI	EI	OK	FP	FN	NG	再現率	確からしさ
大	10	9	9	0	1	0	90.00%	100.00%
中	31	32	30	2	2	0	96.77%	97.55%
小	116	104	103	0	12	1	88.79%	99.04%

PI：関連情報がある項目の組数 EI：抽出した項目の組数

項目・中項目・小項目）の各文書に形態素解析を行い，得られた形態素から不要語を削除し索引語を抽出する．このとき，セキュリティ標準に準拠した複合名詞を定義した辞書を形態素解析に使用する．次に，抽出された索引語に対して一律 1 の重み付けを行う．

手順 2： 近似度の算出

手順 1 によって作成した各標準の項目ごとのデータに対して余弦 [7] を計算し，項目間の近似度を算出する．

手順 3： 相関のある項目の組の抽出

標準 A の各項目から見た標準 B の項目の中で近似度が最大のものを抽出する．標準 B についても同様に抽出し，どちらから見ても項目が一致している組を相関がある項目の組と定義する．

手順 4： 公開されている関連情報との比較

相関がある項目の組を関連情報と比較し分類する．

抽出した組が関連情報をどの程度再現できたかについては再現率（「関連情報の組数」における OK の組数の割合』）で表し，正確度については確からしさ（「抽出した項目の組数」における OK の数の割合）で表す．

4.2 実験結果と考察

相関のある項目の組の抽出を行い，関連情報と比較し分類を行った結果を表 1 に示す．

次に，結果の考察を行う．FP の項目内容については違う対応策について述べられているが，比較している項目と似た表現方法や索引語を用いて記述されているため誤って抽出されたと考えられる．関連情報に示されている正しい項目の内容については，表現方法や索引語が異なっているため，近似度が低くなったと考えられる．そのため，索引語の意味を考慮した関連情報の抽出方法を検討することで再現率を上げられると考える．NG の項目内容は，似たような表現方法や索引語で表されているが，対策を行う時期に違いがあり，公開されている関連情報には存在しない．このため，対策を行う時期や適応する範囲などにも考慮した相関分析の方法を検討することが必要になると考えられる．

4.3 先行研究との比較

先行研究 [8] では索引語の抽出を「専門用語自動抽出システム」[9] を用い，重み付けについては本稿と同様に行ったものである．比較の結果を表 2 に示す．すべての項目で先行研究よりも高い再現率と確からしさを示すことがわかった．このことから，セキュリティ標準に準拠した辞書を使用することで，より正確な関連情報を作成できることがわかった．

表 2: 先行研究との比較

項目	研究	PI	EI	OK	FP	FN	NG	再現率	確からしさ
大	提案	10	9	9	0	1	0	90.00%	100.00%
	先行		8	8	0	2	0	80.00%	100.00%
中	提案	31	32	30	2	2	0	96.77%	93.75%
	先行		28	25	2	5	1	80.65%	89.29%
小	提案	116	104	103	0	12	1	88.79%	99.04%
	先行		97	95	0	19	2	81.90%	97.94%

PI：関連情報がある項目の組数 EI：抽出した項目の組数

5 まとめ

本稿では，セキュリティ評価プラットフォームにおける，異なる標準間での関連情報を導出する新たな機能を提案し，実装した．その後，公開されている標準間の関連情報の再現実験を行い，セキュリティ標準に準拠した辞書を定義することで先行研究よりも高い再現率と確からしさを示すことができた．今後は，2013 年 10 月に『ISO/IEC 27001』が改訂されたので，新旧 ISO/IEC 27001 における関連情報作成実験を行う．また，その他の関連情報が明記されていないセキュリティ標準同士における関連情報作成実験を行い，どの程度関連情報が抽出できるのかについて検証する．

参考文献

[1] 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技術基準（平成 24 年度版），http://www.nisc.go.jp/active/general/pdf/k305-111.pdf

[2] 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

[3] 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/

[4] 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

[5] 日本ネットワークセキュリティ協会：情報セキュリティ対策マップ WG 情報セキュリティ対策マップ検討 WG 活動報告 http://www.jnsa.org/seminar/2013/0607/video_t1.html

[6] 高橋雄志，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, No.2, PP.16-29 2013.9

[7] 徳永健伸:情報検索と言語処理, 東京大学出版会 (1999)

[8] 高橋雄志，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でバイス＆システム 第 3 巻, PP.22-32, 2013.12

[9] 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