Vol.2019-SPT-32 No.16
2019/3/7

セキュリティフレームワークに基づいた情報セキュリティに関連するガイドラインの内容提示の手法の提案と評価

尾崎敏司[†1]

概要：2012 年に独立法人情報処理推進機構により提示された「情報キュリティ人材の育成に関する基礎調査」と 2014 年のその追加調査によると，約 8.1 万人の情報セキュリティの人材不足が指摘されており，現在もその育成は課題となり続けている．自己学習の起点になると考えられるガイドラインは多く公開されているが，これらのガイドラインがセキュリティ業務のどの部分に該当するのか初学者が把握するのは難しい．尾崎の「情報セキュリティに関連するガイドラインの内容提示の手法の提案とその評価」において，米国国立標準技術研究所の公開している Cybersecurity Framework を基に，Term Frequency-Inverse Document Frequency (tf-idf) による特徴ベクトルを用いて，ガイドラインの文書内容を体系的に可視化する手法の提案がなされている．本研究では，この先行研究の提案手法を，ISO/IEC 27001 の規格と，Council on Cybersecurity の Critical Security Controls を用いて，それぞれ実施し，質的コーディングの結果と比較することでその評価を行った．これにより先行研究がフレームワークに大きく依存せずに適用可能なことを確認した．また，各フレームワークについての関係性と検証の結果を基にどのフレームワークを用いて文書内容を提示するのが適当か検討した．

Proposal to visualize a content of information security guideline based on pre-provided three security frameworks

SATOSHI OZAKI[†1]

1. はじめに

2012 年に独立法人情報処理推進機構（IPA）により提示された「情報セキュリティ人材の育成に関する基礎調査」[1]と 2014 年に行われた追加分析[2]によると，約 8.1 万人の情報セキュリティの人材不足が指摘されており，現在もその育成は課題となり続けている．また，内閣サイバーセキュリティセンターのサイバーセキュリティ人材の育成に関する施策連携ワーキンググループが結成されており，2018 年に「サイバーセキュリティ人材の育成に関する施策間連携ワーキンググループ 報告書」[3] が作成されている．この報告書では，セキュリティの専門家であるスペシャリストと，一般的な社内の IT オペレーションを実施しているゼネラリストの間に，エキスパートと呼ばれる「自社事業とセキュリティ活動をよく知り，現場と経営をつなぐ人材」の必要性を指摘しており，引き続き企業における人材育成が求められていることが伺える．

前述の「情報セキュリティ人材の育成に関する基礎調査」の追加分析によると，約8.1万人の情報セキュリティの人材不足のうち，現在セキュリティ人材を保持していない企業において新たに必要とされる人数は6.1万人と推計されている．同時期に情報セキュリティ大学院大学により行われた「情報セキュリティ事故対応に関わるアンケート調査」[4] の結果においても，無回答層を含めた場合，中小企業における約75%がセキュリティ担当者を保持していない可能性が示唆されており，担当者をおいている場合でも約41%が兼任の担当者1名のみの状態であった．トレンドマイクロ株式会社が2018年9月に発行した「法人組織におけるセキュリティ実態調査2017年版」[5] においては，従業員規模とセキュリティ対策の包括度に相関関係があることが指摘されており，特に，中小企業において引き続き限られた人材・資源の中でセキュリティ対策を実施していくことが必要になると考えられる．

2. 関連技術と本研究の目的

セキュリティ人材育成に関する課題を解決するために，学習を促す手法について様々な提案がなされている．

例えば，2018 年には中矢誠らにより，複数人でプレイする Web ゲームサイトを題材とし，攻防型ハッキング競技

†1 筑波大学
University of Tsukuba

としての体験的な演習が提案されている[6]．また，これに限らず，実際にセキュリティに関連した技術的な問題に挑戦することで，セキュリティに関連した技術を身に着ける CTF (Capture the Flag) によるアプローチに関した研究が多く見られる[7][8]．CTF 形式の学習では，コミュニティの育成を兼ねているためか複数人での学習が前提となっていることが多い．

演習環境に注目したものでは，ネットワークセキュリティ教育に重点を置き，仮想環境で演習環境を構築し実際の攻撃シナリオを演習することのできる環境の提案が行われている[9].

これらの学習手法は，技術的な側面での学習としては有用であると考えられている．しかし，エキスパートつまり「自社事業とセキュリティ活動をよく知り，現場と経営をつなぐ人材」を育成するという観点では，技術に限らない広い視点での学習活動が求められているため，これらの学習だけでは不十分だと考えられる．

技術に限らない幅広い知識が必要なエキスパートを育成するためには，学習者自身の包括的な自己学習を促すアプローチが必要になると考えられる．

また，中小企業においては，限られた人材・資源の中でセキュリティ対策を実施していくことが求められており，業務への適用を前提とした自己学習が重要な位置を占めていると考えられる．

実業務に基づいた自己学習の起点となる対策ガイドラインは多く公開されており，経済産業省で整理されているものに限っても 150 を超える[10]．これらのガイドラインは 30 種程度に分類はされているものの，その項目は体系立てられたものになっておらず，一見してその項目がセキュリティ対策活動のどの部分に該当するかを把握することは難しい．

分野の全体像を把握できる情報が提示されていることは，学習者が自己の学習方策を立てる上で重要になると考えられ，また，利用しているガイドラインと全体像の差分を把握することは次のセキュリティ対策の方策を考える上で重要な情報になると考えられる．

これの問題を解決するために，2019 年 2 月に，尾崎により「情報セキュリティに関連するガイドラインの内容提示の手法の提案とその評価」[11]として，セキュリティ関連のガイドラインについてセキュリティ分野の全体像を把握できるような形で内容を提示する手法が提案されている．この手法では，米国立標準技術研究所（NIST）から発行された Cybersecurity Framework 1.1[12] を基にし， Term Frequency-Inverse Document Frequency (tf-idf) による特徴語ベクトルを用いた文書内容の提示を行う．しかしながら，この研究では，適切な文書集合の作成や新規の分類手法の採用による改善の可能性について述べられているものの，Cybersecurity Framework 1.1 以外の他のフレームワークを用いた場合の評価についてはなされていない．

そこで，本研究では，「情報セキュリティに関連するガイドラインの内容提示の手法の提案とその評価」の文書内容を提示する手法において，Cybersecurity Framework 1.1 の「フレームワークコア」以外のフレームワークを用いて，内容提示とその評価を実施することで，先行研究の手法が採用する「フレームワークコア」のモデルに依存していないことを確認する．

また，各フレームワークの関係性と文書内容の提示という目的との関連性を再確認し，先行研究の提案手法にどのモデルを用いるのが適切か検討を行う．

3. 提案手法

尾崎の先行研究では，全体像を意識した体系的な内容の提示を行うため， Cybersecurity Framework 1.1 の「フレームワークコア」と呼ばれるモデルを基に，文書内容の提示を行うことを検討した．既存のモデルに基づいて内容の提示を行うことにより，文書毎に個別に内容分析を行う場合に比べて，セキュリティ対策活動の全体像の把握や，文書間の内容の比較が容易になると考えられる．

また，この先行研究では，分類精度の量的な評価を可能にするために，事前に解析対象のガイドラインに対して質的コーディングを行っている．

本研究では，国内で Cybersecurity Framework 1.1 と同様にセキュリティ対策の診断指標とし手利用される ISO/IEC 27001[13]，The CIS Critical Security Controls for Effective Cyber Defense version 6.1 (CIS-CSC 6.1) [14] などのフレームワーク（規格，アクションリスト）を用いて内容提示を行う．

この章では，まず本研究で内容提示の枠組みとして用いる ISO/IEC 27001，CIS-CSC 6.1 について概要説明を行い，先行研究で利用されている Cybersecurity Framework 1.1 についても説明を行う．次に，手法の検証のための解析対象である「中小企業の情報セキュリティ対策ガイドライン」について概要の説明を行い，質的コーディングによる評価用データの作成方法について述べる．最後に，提案手法の計算方法について記載する．

3.1 ISO/IEC 27001

ISO/IEC 27001 は，情報資産を守り活用するための情報セキュリティマネジメントシステム（ISMS）に関する国際規格で，「組織の状況」，「リーダーシップ」，「計画」，「支援」，「運用」，「パフォーマンス評価」，「改善」の 7 つの大項目の下に合計 22 の項目が定義されている（表 1）．

本研究では，解析対象が日本語文書であるため，ISO/IEC 27001 を翻訳して作成された JIS Q 27001[15]を用いて提案手法を実施している．

3.2 CIS-CSC 6.1

CIS-CSC 6.1 は，情報セキュリティ対策，特に技術的なセキュリティコントロールに焦点をあてた文書である．文書内では，実行の優先度の高い Basic と発展的な Advanced の 2 つの大項目の下に 20 の項目が定義されている（表 2）．

本研究では，解析対象が日本語文書であるため，NRI セキュアテクノロジーズの翻訳による「The Critical Security Controls for Effective Cyber Defense version 6.1」の翻訳版[16]を利用した．本文書における大項目は，実行優先度に基づいており，モデルの構造を示すものではないため，項目のみを用いて解析を実施した．

表 1 ISO/IEC 27001 の大項目と項目

大項目	項目
組織の状況	組織及びその状況の理解
	利害関係者のニーズ及び期待の理解
	情報セキュリティマネジメントシステムの適用範囲の決定
	情報セキュリティマネジメントシステム
リーダーシップ	リーダーシップ及びコミットメント
	方針
	組織の役割，責任及び権限
計画	リスク及び機会に対処する活動
	情報セキュリティ目的及びそれを達成するための計画策定
支援	資源
	力量
	認識
	コミュニケーション
	文書化した情報
運用	運用の計画及び管理
	情報セキュリティリスクアセスメント
	情報セキュリティリスク対応
パフォーマンス評価	監視，測定，分析及び評価
	内部監査
	マネジメントレビュー
改善	不適合及び是正処置
	継続的改善

表 2CIS-CSC 6.1 の項目

	項目
CSC1:	許可されたデバイスと無許可のデバイスのインベントリ
CSC2:	許可されたソフトウェアと無許可のソフトウェアのインベントリ
CSC3:	モバイルデバイス、ラップトップ、ワークステーションおよびサーバに関するハードウェアお よびソフトウェアのセキュアな設定
CSC4:	継続的な脆弱性診断および修復
CSC5:	管理権限のコントロールされた使用
CSC6:	監査ログの保守、監視および分析
CSC7:	電子メールとWeb ブラウザの保護
CSC8:	マルウェア対策
CSC9:	ネットワークポート、プロトコル、およびサービスの制限およびコントロール
CSC10:	データ復旧能力
CSC11:	ファイアウォール、ルータ、スイッチなどのネットワーク機器のセキュアな設定
CSC12:	境界防御
CSC13:	データ保護
CSC14:	Need - to - Know に基づいたアクセスコントロール
CSC15:	無線アクセスコントロール
CSC16:	アカウントの監視およびコントロール
CSC17:	スキル不足を補うためのセキュリティスキル評価および適切なトレーニング
CSC18:	アプリケーションソフトウェアセキュリティ
CSC19:	インシデントレスポンスと管理
CSC20:	ペネトレーションテストおよびレッドチームの訓練

3.3 Cybersecurity Framework

このフレームワークは，重要インフラストラクチャにおけるセキュリティ対策向けに作成されており，“現在，産業界で効力を発揮している標準，ガイドライン，およびベストプラクティスを集約することで，現在ある多様なサイバーセキュリティアプローチを体系化・構造化し，企業に示している（重要インフラのサイバーセキュリティを向上させるためのフレームワーク 1.0[17]　p2 より引用）”．

先行研究においても，解析の対象とする文書は日本語であるため，IPA が発行している本文書を翻訳した「重要インフラのサイバーセキュリティを向上させるためのフレームワーク 1.0」を用い Cybersecurity Framework 1.1 との差分部分については，英語版からの翻訳を行って解析に利用している．

このフレームワークで提示されている「フレームワークコア」は，機能，カテゴリ，サブカテゴリ，参考情報の四つで構成されており，先行研究の提案手法では主に「フレームワークコア」の機能とカテゴリが利用されている．機能は，基本的なサイバーセキュリティ対策の最も上位の構成要素として「特定」，「防御」，「検知」，「対応」，「復旧」の 5 つが定義されており，カテゴリは各機能をさらに効果毎に分類したものである．

3.4 中小企業の情報セキュリティ対策ガイドライン

このガイドラインは, 中小企業の IT 利用の活用が進む中で中小企業がセキュリティ対策に取り組むための指針として 2009 年に作成され，2017 年に法改正等最新の情報を基に改定されたものである．このガイドラインには，チェックリストなどが同梱されており，学習目的のみだけでなく実際にガイドラインに基づいた運用を行えるよう工夫がされている．特に問題を抱えていると思われる中小企業のセキュリティ担当者が最初にふれるドキュメントであろうと考えられるため，今回の解析・評価の対象とした．

3.5 質的コーディングによる評価用のデータの作成

提案手法の定量的な評価を実施する評価用のデータを得るために，ISO/IEC 27001 と CIS-CSC 6.1 のそれぞれの項目をコード群として,「中小企業の情報セキュリティ対策ガイドライン」に対してテンプレートコーディングを，それぞれ実施した．

コーディングを実施する際には，

a) 原則，1 センテンスごとに評価を行う．「用語の説明＋用語を用いた文」，「説明＋補足事項」などの 2 つ以上のセンテンスで一つの意味を成していると考えられた部分には，そのまとまりでの評価を実施している．
b) 複数の項目に該当すると考えられた場合には，複数のコードを割り振る．

c) 図表など，画像として添付されている項目はコーディングの対象に含めない．
d) コード群（ISO/IEC 27001 もしくは CIS-CSC 6.1 の項目）に適切なコードが存在しない場合には，コードを割り振らない

こととした．

実際のコーディングの結果については，付録として表 5 に記載をした．

コード（各項目）が割り当てらてられた文の数を質的コーディングによる記述数を表すスコア $SQ_i(C_i)$ とし，表 3，表 4 の「質的コーディング」に記載した．

3.6 提案手法

各フレームワークの項目に基づいて，文書中の単語の重要度を評価する方法 tf-idf により特徴語ベクトルを作成し，解析対象の文章の各センテンスとのコサイン類似度で類似度を測定することで，「フレームワークコア」に基づいた内容の推定を行った．

解析対象の文書中のある行 L_j が，IOS/IEC27001 と CIS-CSC 6.1 のある項目 C_i にどの程度関連しているか（つまり内容が類似しているか）は，各項目の記述を基に作成した項目 C_i の特徴語ベクトル $\mathbf{c_i}$ と，ある行 L_j に対して Cybersecurity Framework 1.1 の統計情報を基に作成した特徴語ベクトル $\mathbf{l_j}$ のコサイン類似度で記載することができる．従って，文章全体の中に，項目 C_i に関連する記述がどの程度文章中にあるかを表すスコア $S_i(C_i)$ は，この総和となるので，式 1 で評価することができると考えられる．

$$S_i(C_i) = \sum_j \frac{\vec{l_j} \cdot \vec{c_i}}{|\vec{l_j}||\vec{c_i}|} \quad \cdots\cdots式\ 1$$

具体的には，下記の手順でスコア $S_i(C_i)$ の計算を行った．

1. IOS/IEC27001 と CIS-CSC 6.1 内で各項目 C_i について記述されている部分を確認し，項目ごとに抽出した．また，項目 C_i が属している機能に関する記述も同様に抽出し，項目 C_i の文書の一部として取り扱った．
2. 抽出した全文書集合に対して，分かち書きを実施して，名詞句だけの集合に変換した．
3. 名詞句による文書集合に対して，それぞれの項目 C_i 毎に，tf-idf による特徴語ベクトル $\mathbf{c_i}$ を作成した．
4. 適用対象の文章から 1 行ごと文字列を抜き出し特徴語ベクトル $\mathbf{l_j}$ を計算し，項目の特徴語ベクトル $\mathbf{c_i}$ との間のコサイン類似度を計算した．
5. 項目毎に算出したコサイン類似度の総和を取り，提案手法のスコア $S_i(C_i)$ を計算した．

プログラミング言語は python を用い，分かち書きには，Mecab[18] を，tf-idf とコサイン類似度の計算は scikit-learn[19] のライブラリを利用している．

4. 結果

IOS/IEC27001 と CIS-CSC 6.1 に基づいた提案手法によるスコア $S_i(C_i)$ は，カラーコード表示（緑：低⇔赤：高）とともに，表 3，表 4 の「提案手法による解析」に記載した．IOS/IEC27001 による解析結果については，大項目ごとにスコアの平均値を計算し記載している．

比較のため，先行研究の Cyber Security Framework 1.1 の解析結果も表 5 として引用している．

5. 評価

本研究では，提案手法の評価を行うために事前に質的コーティングを行い各カテゴリの記述数を表す $SQ_i(C_i)$ を計算している．これを用いて提示内容が適切かどうかの評価を行う．

質的コーディングによるスコア $SQ_i(C_i)$ついては，表 3，表 4 の「質的コーディング」の列に記載した．また，IOS/IEC27001 については，大項目ごとの平均値を求めて合わせて記載している．

$S_i(C_i)$ ，$SQ_i(C_i)$について，式 2 で，正規化を行った．正規化後のスコアを表に記載をした．

$$N(X) = \frac{X - x_{min}}{|x_{max} - x_{min}|} \quad \cdots\cdots式\ 2$$

ここで X はデータセット全体を表し，各要素 x の正規化後の値を N (x)と表すこととする．

提案手法のスコアを正規化した値 $N(S_i)$ を要素として持つベクトルを **M** とし，質的コーディングによるスコアを正規化した値 $N(SQ_i)$ を要素として持つベクトルを **Q** とする（式 3）．

$$\vec{M} = (S_1(C_1), \cdots, S_{23}(C_{23}))$$
$$\vec{Q} = (SQ_1(C_1), \cdots, SQ_{23}(C_{23})) \quad \cdots\cdots式\ 3$$

このベクトル **M**, **Q** についてコサイン類似度を計算したところ，ISO/IEC 27001 については，0.843 であった．

また，大項目ごとの平均値についても同様の操作を行い，コサイン類似度を計算したところ 0.884 であった．

一方，CIS-CSC 6.1 を用いた場合では，0.774 であった．

先行研究において，項目に当たるカテゴリレベルでの評価では，0.791，大項目に当たる機能レベルでの評価では，0.966 であった．

以上より，解析のための項目数が 20 程度の場合，利用しているモデルに依存せずに，提案手法を用いることで，8 割前後の精度（人の判断との類似性）で内容を提示することができると考えられる．また，5 項目前後の場合，同様に 9

割前後の精度が期待されることが分かった．先行研究に合わせて，正規化後のスコアの差が 0.5 を超えたものについては，表 3，表 4 中で赤く印をつけている．差が著しく激しい項目については，次の，議論と制限の章で検討を行う

表 3 ISO/IEC 27001 による提案手法によるスコアと質的コーディングによるスコア

	提案手法による解析					質的コーディング		
大項目	大項目毎の平均値	提案手法のスコア	正規化後のスコア	項目	正規化後のスコアの差	質的コーディングによるスコア	正規化後のスコア	機能ごとの平均値
組織の状況	32.186843	15.6127031	0	組織及びその状況の理解	0.027027027	0.027027027	3	5.5
		53.6646565	0.29925945	利害関係者のニーズ及び期待の理解	0.11007026	0.189189189	9	
		38.7667795	0.18209515	情報セキュリティマネジメントシステムの適用範囲の決定	0.019932988	0.162162162	8	
		20.7032348	0.04003447	情報セキュリティマネジメントシステム	0.040034468	0	2	
リーダーシップ	77.419159	73.8532158	0.4580323	リーダーシップ及びコミットメント	0.133707977	0.324324324	14	15
		125.518792	0.86435604	方針	0.48597766	0.378378378	16	
		32.8854687	0.1358416	組織の役割，責任及び権限	0.215509749	0.351351351	15	
計画	130.98087	120.037189	0.82124599	リスク及び機会に対処する活動	0.178754009	1	39	30.5
		141.924559	0.99337913	情報セキュリティ目的及びそれを達成するための計画策定	0.45283859	0.540540541	22	
支援	63.721814	33.7688315	0.14278881	資源	0.061707725	0.081081081	5	6
		52.6182912	0.29103031	力量	0.236976259	0.054054054	4	
		85.1077125	0.54654325	認識	0.465462168	0.081081081	5	
		37.8508224	0.17489161	コミュニケーション	0.068351635	0.243243243	11	
		109.263411	0.73651566	文書化した情報	0.655434575	0.081081081	5	
運用	102.8928	92.2309257	0.60256373	運用の計画及び管理	0.467428599	0.135135135	7	22
		73.6810539	0.45667833	情報セキュリティリスクアセスメント	0.083862206	0.540540541	22	
		142.766427	1	情報セキュリティリスク対応	0.054054054	0.945945946	37	
パフォーマンス評価	70.436268	71.2309825	0.43740976	監視，測定，分析及び評価	0.275247595	0.162162162	8	6.333333
		60.6986611	0.35457835	内部監査	0.246470245	0.108108108	6	
		79.3791593	0.50149106	マネジメントレビュー	0.420409982	0.081081081	5	
改善	53.851064	52.2454734	0.28809829	不適合及び是正処置	0.179990181	0.108108108	6	8
		55.4566544	0.31335261	継続的改善	0.097136394	0.216216216	10	

表 4 CIS-CSC 6.1 に基づいた提案手法によるスコアと質的コーディングによるスコア

提案手法による解析				質的コーディング	
提案手法のスコア	正規化後のスコア	項目	正規化後のスコアの差	正規化後のスコア	質的コーディングによるスコア
34.42109	0.06296	許可されたデバイスと無許可のデバイスのインベントリ	0.13704	0.2	2
39.29959	0.175802	許可されたソフトウェアと無許可のソフトウェアのインベントリ	0.075802	0.1	1
38.23864	0.151262	モバイルデバイス、ラップトップ、ワークステーションおよびサーバに関するハードウェアお よびソフトウェアのセキュアな設定	0.248738	0.4	4
57.08355	0.587151	継続的な脆弱性診断および修復	0.287151	0.3	3
39.37545	0.177557	管理権限のコントロールされた使用	0.077557	0.1	1
34.55492	0.066056	監査ログの保守、監視および分析	0.133944	0.2	2
39.443	0.179119	電子メールとWeb ブラウザの保護	0.179119	0	0
69.95042	0.884766	マルウェア対策	0.584766	0.3	3
31.6991	0	ネットワークポート、プロトコル、およびサービスの制限およびコントロール	0.1	0.1	1
33.3763	0.038794	データ復旧能力	0.061206	0.1	1
51.19634	0.450978	ファイアウォール、ルータ、スイッチなどのネットワーク機器のセキュアな設定	0.350978	0.1	1
40.17882	0.196139	境界防御	0.196139	0	0
62.22556	0.706087	データ保護	0.006087	0.7	7
65.13526	0.773389	Need - to - Know に基づいたアクセスコントロール	0.473389	0.3	3
36.91655	0.120681	無線アクセスコントロール	0.020681	0.1	1
43.83937	0.280808	アカウントの監視およびコントロール	0.080808	0.2	2
74.09094	0.980538	スキル不足を補うためのセキュリティスキル評価および適切なトレーニング	0.019462	1	10
57.25825	0.591192	アプリケーションソフトウェアセキュリティ	0.491192	0.1	1
59.09538	0.633685	インシデントレスポンスと管理	0.133685	0.5	5
74.93237	1	ペネトレーションテストおよびレッドチームの訓練	1	0	0

表 5 フレームワークコアに基づいた提案手法によるスコアと質的コーディングによるスコア
（「情報セキュリティに関連するガイドラインの内容提示の手法の提案とその評価」の表 3 を引用）

	提案手法による解析					質的コーディング		
機能	機能ごとの平均値	提案手法のスコア	正規化後のスコア	カテゴリ	正規化後のスコアの差	質的コーディングによるスコア	正規化後のスコア	機能ごとの平均値
IDENTIFY（特定）	85.10625	83.7107	0.755397	資産管理	0.142494	38	0.61290323	28.33333
		82.49747	0.738171	ビジネス環境	0.609138	8	0.12903226	
		84.70715	0.769546	ガバナンス	0.069164	52	0.83870968	
		90.35975	0.849806	リスクアセスメント	0.188516	41	0.66129032	
		86.25294	0.791494	リスク管理戦略	0.710849	5	0.08064516	
		83.1095	0.746861	サプライチェーンリスク	0.327506	26	0.41935484	
Protection（防御）	87.11211	68.38192	0.537746	アクセス制御	0.408714	8	0.12903226	20.16667
		88.64493	0.825457	意識向上およびトレーニング	0.196425	39	0.62903226	
		100.6844	0.996404	データセキュリティ	0.835113	10	0.16129032	
		100.9377	1	情報を保護するためのプロセスおよび手順	0	62	1	
		80.47797	0.709496	保守	0.709496	0	0	
		83.54582	0.753056	保護技術	0.720798	2	0.03225806	
Detection（検知）	37.21109	31.82964	0.018746	異常とイベント	0.018746	0	0	2.333333
		49.29422	0.266723	セキュリティの継続的なモニタリング	0.15382	7	0.11290323	
		30.5094	0	検知プロセス	0	0	0	
Response（対応）	59.17382	56.82235	0.373614	分析	0.341356	2	0.03225806	6.8
		68.60442	0.540905	伝達	0.266712	17	0.27419355	
		53.80571	0.330781	改善	0.16949	10	0.16129032	
		60.31133	0.423153	低減	0.390895	2	0.03225806	
		56.3253	0.366556	対応計画	0.318169	3	0.0483871	
Recoveriy（復旧）	40.48532	43.0634	0.178252	改善	0.033091	9	0.14516129	3.666667
		37.3109	0.096573	伝達	0.096573	0	0	
		41.08167	0.150114	復旧計画	0.117856	2	0.03225806	

6. 議論と制限

6.1 スコアの差が大きかった項目

表 3，表 4 中で赤く印がつけられている項目のうち，特に差が出ているのは，CIS-CSC 6.1 の「ペネトレーションテストおよびレッドチームの訓練」の項目であった．そこで，この項目の特徴語について具体的に見て確認をしていく．

表 7 に IOS/IEC27001 と CIS-CSC 6.1 の各項目の特徴語上位 10 個を記載している．この表の「ペネトレーションテストおよびレッドチームの訓練」の項目を確認すると，「防御」，「対策」というほかの項目にも当てはまりうると思われる単語が特徴語として抽出されてしまっていることが分かる．

これらの単語を解析対象から削除して再計算を行ったところ，コサイン類似度による評価結果は，0.826 と約 0.05 ポイント向上した．従って，先行研究の Cybersecurity Framework 1.1 を用いた場合と同じく，項目ごとの特徴語の抽出手法の改善を行うことで精度向上が望めると考えられる．

6.2 質的コーディングのスコアの総和の差

質的コーディングによる結果について注目すると，スコアの総和が各モデルで異なる．具体的には，ISO/IEC 27001 の場合，質的コーディングによるスコアの総和は，259 であるのに対して，CIS-CSC 6.1 の場合には，48 であった．これは，今回コード群に適切なコードが存在しない場合には，センテンスにコードを割り振らなかったためである．

適切なコードがコード群に存在しないということは，その文の内容をそのモデルでは表現しきれないということであるため，この数値は，そのモデルが対象の文書の内容をどれだけ包括できているかを表す指標になりうると考えられる．類似度とともに表にすると，表 6 となる（Cybersecurity Framework 1.1 の類似度は，「情報セキュリティに関連するガイドラインの内容提示の手法の提案とその評価」の結果を引用）．

表 6 質的コーディングのスコアの総和とコサイン類似度

	Cybersecurity Framework 1.1	ISO/IEC 27001	CIS-CSC 6.1
質的コーディングのスコアの総和	343	259	48
大項目でのコサイン類似度	0.966	0.884	N/A
項目でのコサイン類似度	0.791	0.843	0.774（0.826）
項目と大項目の関係	効果毎のサブセット	実施フェーズ	実施の優先度

表 7 CIS-CSC 6.1 と ISO/IEC27001 の項目ごとの特徴語

CIS-CSC 6.1		CSC1: 許可されたデバイスと無許可のデバイスのインベントリ	デバイス(0.351)、ネットワーク(0.342)、インベントリ(0.249)、接続(0.224)、資産(0.221)、アドレス(0.196)、システム(0.190)、許可(0.127)、ping(0.121)、ip(0.120)
		CSC2: 許可されたソフトウェアと無許可のソフトウェアのインベントリ	ソフトウェア(0.316)、システム(0.225)、ホワイト(0.224)、リスト(0.220)、実行(0.215)、マシン(0.169)、者(0.169)、許可(0.158)、アプリケーション(0.153)、ファイル(0.138)
		CSC3: モバイルデバイス、ラップトップ、ワークステーションおよびサーバに関するハードウェアおよびソフトウェアのセキュアな設定	イメージ(0.469)、設定(0.286)、変更(0.228)、システム(0.184)、管理(0.183)、セキュア(0.177)、e(0.176)、必要(0.149)、使用(0.131)、新た(0.129)
		CSC4: 継続的な脆弱性診断および修復	脆弱(0.546)、性(0.395)、パッチ(0.273)、スキャン(0.245)、システム(0.141)、リスク(0.135)、者(0.133)、管理(0.123)、適用(0.115)、ツール(0.110)
		CSC5: 管理権限のコントロールされた使用	権限(0.412)、管理(0.394)、者(0.276)、パスワード(0.260)、アカウント(0.245)、使用(0.210)、ユーザ(0.147)、システム(0.133)、攻撃(0.133)、実行(0.126)
		CSC6: 監査ログの保守、監視および分析	ログ(0.614)、ロギング(0.266)、監査(0.191)、分析(0.171)、者(0.170)、攻撃(0.146)、システム(0.134)、形式(0.129)、ツール(0.109)、異常(0.102)
		CSC7: 電子メールとWeb ブラウザの保護	ブラウザ(0.385)、web(0.269)、電子(0.233)、メール(0.229)、url(0.189)、フィルタ(0.182)、メールクライアント(0.143)、サイト(0.135)、パスワード(0.126)、悪意(0.112)
		CSC8: マルウェア対策	ウェア(0.323)、マル(0.291)、対策(0.279)、アンチマルウェアソフト(0.192)、機能(0.166)、防御(0.150)、自動(0.149)、化(0.143)、デバイス(0.134)、更新(0.132)
		CSC9: ネットワークポート、プロトコル、およびサービスの制限およびコントロール	サービス(0.561)、ポート(0.390)、サーバ(0.237)、済み(0.161)、稼働(0.157)、ホストマシン(0.119)、プロトコル(0.112)、デフォルト(0.112)、ネットワーク(0.112)、ライン(0.105)
		CSC10: データ復旧能力	バックアップ(0.784)、データ(0.195)、復旧(0.193)、復元(0.181)、先(0.136)、システム(0.123)、感染(0.113)、必要(0.092)、マシン(0.082)、能力(0.082)
		CSC11: ファイアウォール、ルータ、スイッチなどのネットワーク機器のセキュアな設定	ネットワーク(0.305)、機器(0.301)、設定(0.297)、network(0.240)、変更(0.187)、デフォルト(0.161)、管理(0.161)、ルータ(0.149)、インフラ(0.135)、サービス(0.129)
		CSC12: 境界防御	境界(0.364)、ネットワーク(0.331)、dmz(0.273)、ids(0.176)、network(0.166)、インターネット(0.163)、内部(0.163)、アドレス(0.159)、パケット(0.156)、トラフィック(0.153)
		CSC13: データ保護	データ(0.525)、機密(0.246)、鍵(0.206)、暗号(0.192)、保護(0.178)、network(0.168)、dlp(0.155)、情報(0.149)、不正(0.148)、持ち出し(0.147)
		CSC14: Need - to - Know に基づいたアクセスコントロール	アクセス(0.333)、機密(0.288)、ネットワーク(0.229)、データ(0.222)、情報(0.218)、システム(0.204)、必要(0.189)、レベル(0.188)、通信(0.142)、保管(0.142)
		CSC15: 無線アクセスコントロール	無線(0.757)、アクセス(0.260)、network(0.203)、デバイス(0.156)、ネットワーク(0.143)、wids(0.130)、ポイント(0.115)、接続(0.112)、必要(0.107)、組織(0.087)
		CSC16: アカウントの監視およびコントロール	アカウント(0.682)、ユーザ(0.217)、システム(0.190)、無効(0.180)、アクセス(0.161)、認証(0.132)、時間(0.124)、従業(0.119)、すべて(0.116)、請負(0.112)
		CSC17: スキル不足を補うためのセキュリティスキル評価および適切なトレーニング	従業(0.372)、トレーニング(0.360)、員(0.346)、スキル(0.291)、セキュリティ(0.182)、職務(0.179)、ギャップ(0.179)、実施(0.129)、改善(0.127)、意識(0.102)
		CSC18: アプリケーションソフトウェアセキュリティ	アプリケーション(0.379)、web(0.324)、開発(0.246)、ソフトウェア(0.188)、脆弱(0.144)、アプリケーションファイアウォール(0.143)、攻撃(0.134)、本番(0.129)、入力(0.129)、自社(0.122)
		CSC19: インシデントレスポンスと管理	インシデント(0.658)、レスポンス(0.308)、ハンドリング(0.216)、報告(0.174)、チーム(0.162)、シナリオ(0.129)、者(0.129)、担当(0.127)、手順(0.090)、攻撃(0.090)
		CSC20: ペネトレーションテストおよびレッドチームの訓練	テスト(0.429)、ペネトレーション(0.412)、レッド(0.362)、チーム(0.258)、防御(0.181)、対策(0.161)、攻撃(0.161)、訓練(0.139)、目標(0.112)、実施(0.098)
ISO/IEC	組織の状況	4.1 組織及びその状況の理解	状況(0.352)、課題(0.323)、内部(0.300)、外部(0.280)、組織(0.256)、確定(0.220)、能力(0.220)、記載(0.220)、2010(0.220)、決定(0.201)
		4.2 利害関係者のニーズ及び期待の理解	利害(0.480)、関係(0.441)、者(0.338)、事項(0.290)、要求(0.274)、関連(0.213)、義務(0.200)、規制(0.200)、上(0.200)、法的(0.200)
		4.3 情報セキュリティマネジメントシステムの	適用(0.470)、範囲(0.413)、規定(0.276)、活動(0.253)、組織(0.200)、可能(0.194)、インタフェース(0.172)、依存(0.172)、間(0.172)、境界(0.172)
		4.4 情報セキュリティマネジメントシステム	維持(0.440)、規格(0.409)、改善(0.358)、継続(0.358)、確立(0.338)、要求(0.274)、実施(0.261)、isms(0.217)、事項(0.217)、組織(0.174)
	リーダーシップ	5.1 リーダーシップ及びコミットメント	isms(0.284)、確実(0.278)、リーダーシップ(0.261)、実証(0.261)、支援(0.261)、層(0.231)、マネジメント(0.192)、セキュリティ(0.179)、性(0.179)、事項(0.142)
		5.2 方針	セキュリティ(0.393)、情報(0.374)、目的(0.309)、コミットメント(0.304)、方針(0.253)、可能(0.194)、事項(0.187)、枠組み(0.172)、設定(0.172)、入手(0.152)
		5.3 組織の役割，責任及び権限	トップ(0.456)、マネジメント(0.456)、権限(0.411)、責任(0.342)、報告(0.274)、パフォーマンス(0.211)、isms(0.168)、確実(0.165)、役割(0.137)、内(0.124)
	計画	6.1 リスク及び機会に対処する活動	リスク(0.567)、策(0.379)、管理(0.290)、情報(0.238)、対応(0.189)、セキュリティリスクアセスメント(0.177)、書(0.172)、セキュリティ(0.157)、特定(0.152)、附属(0.143)
		6.2 情報セキュリティ目的及びそれを達成する	セキュリティ(0.389)、情報(0.360)、目的(0.340)、リスク(0.209)、事項(0.206)、達成(0.181)、可能(0.160)、結果(0.151)、階層(0.142)、i(0.142)
	支援	7.1 資源	資源(0.417)、提供(0.417)、維持(0.383)、改善(0.312)、継続(0.312)、確立(0.294)、決定(0.238)、必要(0.238)、実施(0.227)、isms(0.189)
		7.2 力量	力量(0.519)、人々(0.432)、処置(0.259)、雇用(0.236)、訓練(0.236)、教育(0.236)、適切(0.141)、人(0.118)、締結(0.118)、現在(0.118)
		7.3 認識	貢献(0.280)、認識(0.280)、向上(0.280)、自ら(0.280)、便益(0.280)、セキュリティ(0.256)、意味(0.247)、下(0.247)、人々(0.206)、方針(0.206)
		7.4 コミュニケーション	コミュニケーション(0.867)、実施(0.251)、者(0.163)、何(0.144)、内容(0.144)、対象(0.127)、時期(0.127)、伝達(0.098)、内部(0.098)、外部(0.092)
		7.5 文書化した情報	化(0.353)、文書(0.353)、情報(0.293)、管理(0.216)、作成(0.179)、適切(0.161)、必要(0.154)、性(0.154)、次(0.140)、組織(0.137)
	運用	8.1 運用の計画及び管理	計画(0.402)、プロセス(0.302)、実施(0.293)、管理(0.269)、組織(0.245)、必要(0.230)、決定(0.230)、変更(0.229)、情報(0.183)、軽減(0.168)
		8.2 情報セキュリティリスクアセスメント	重大(0.526)、セキュリティリスクアセスメント(0.464)、情報(0.285)、提案(0.263)、変化(0.232)、間隔(0.210)、基準(0.210)、変更(0.179)、考慮(0.167)、場合(0.157)
		8.3 情報セキュリティリスク対応	リスク(0.516)、対応(0.516)、情報(0.381)、セキュリティ(0.321)、計画(0.210)、組織(0.204)、結果(0.187)、保持(0.169)、実施(0.153)、文書(0.153)
	パフォーマンス評価	9.1 監視，測定，分析及び評価	監視(0.572)、測定(0.518)、評価(0.252)、結果(0.247)、分析(0.245)、時期(0.163)、方法(0.136)、妥当(0.126)、実施(0.121)、可能(0.104)
		9.2 内部監査	監査(0.841)、プログラム(0.220)、事項(0.133)、報告(0.129)、実施(0.127)、結果(0.117)、維持(0.108)、性(0.100)、要求(0.100)、計画(0.088)
		9.3 マネジメントレビュー	レビュー(0.422)、マネジメント(0.422)、結果(0.306)、フィードバック(0.230)、機会(0.203)、状況(0.184)、リスク(0.169)、処置(0.169)、isms(0.166)、改善(0.137)
	改善	10.1 不適合及び是正処置	不適合(0.727)、処置(0.385)、発生(0.225)、是正(0.198)、原因(0.150)、場合(0.134)、明確(0.132)、対処(0.132)、レビュー(0.110)、事項(0.108)
		10.2 継続的改善	性(0.695)、妥当(0.346)、改善(0.303)、継続(0.303)、適切(0.303)、有効(0.256)、isms(0.184)、組織(0.148)、化(0.000)、利用(0.000)

表 6 によると，Cybersecurity Framework 1.1 が 343 で最も質的コーディングのスコアの総和が高く，ISO/IEC 27001 の 259，CIS-CSC 6.1 の 48 と続く．そのため，Cybersecurity Framework 1.1 が最も包括的なモデルであると考えられる．Cybersecurity Framework 1.1 が最も包括的なモデルである可能性はこの点以外にも，

- Cybersecurity Framework 1.1 のサブカテゴリの参考文献として ISO/IEC 27001 の付属書 A の項目や CIS-CSC 6.1 の項目があげられていること
- CIS-CSC 6.1 の Appendix C において，CIS-CSC 6.1 の各項目が, Cybersecurity Framework 1.1 のどのカテゴリに対応付けられること

という事実からも推察される．

6.3 制限事項について

先行研究と同じく質的コーディングの結果を評価データとして利用したが，テンプレートコーディングでよく行われる複数人でのコーディングの実施と統計的なすり合わせ処理は，実施していない．しかし，コーディングは提案手法の実験前に行い，コーディングの結果についてもレビューを実施した．

今回解析と評価に用いた「中小企業の情報セキュリティ対策ガイドライン」についても，注意が必要である．

この文書の終盤部分において, ISO/IEC 27001 についての言及がなされており, この活用事例について紹介している．これに関連して

1. この範囲も質的コーディングの対象内に含まれている
2. 製作者が，ISO/IEC 27001 を意識して，ガイドラインを作成している可能性が高い

ため, ISO/IEC 27001 を用いた評価は他のモデルを用いたものよりも高めに出ている可能性があると考えられる．

また，手法の評価に用いた文書も一文書のみであるため, より正確な評価を与えるには解析と評価の対象とする文書数を増やして検証を行う必要がある．

6.4 3 つのうちどのモデルが適切なモデルか

文書内容を体系的に表示するという目的に照らし合わせた場合，適切なモデルは，下記の 2 条件を満たすことが望ましいと考えらえる．

1) 提案手法による内容提示の精度が高いモデル
2) 分野全体を表す包括的なモデル

表 6 にある通り, 項目レベルでの精度では, ISO/IEC 27001

が 0.843 で最も高く，次いで Cybersecurity Framework 1.1 の 0.791，大項目レベルでは，Cybersecurity Framework 1.1 が 0.966 で最も高く，次いで ISO/IEC 27001 が 0.884 となっている．一方で，6.2 の議論から，Cybersecurity Framework 1.1 がセキュリティ分野をより包括的に表したモデルであると考えられる．

そのため，本研究の範囲内では，文書内容を体系的に提示するためのモデルとしては，項目レベルの精度では若干劣るが，Cybersecurity Framework 1.1 の「フレームワークコア」を用いるのが良いと考えられる．

7. 結論

本研究では，「情報セキュリティに関連するガイドラインの内容提示の手法の提案とその評価」の文書内容を提示する手法において，Cybersecurity Framework 1.1 の「フレームワークコア」以外のフレームワークを用いて，内容提示とその評価を実施することで，先行研究の手法が採用する「フレームワークコア」のモデルに依存していないことを確認することを目的として，IOS/IEC27001 と CIS-CSC 6.1 の枠組みを用いて，先行研究と同様の手法を用いて解析と評価を行った．

その結果，解析のための項目数が 20 程度の場合，利用しているモデルに依存せずに，提案手法を用いることで，8 割前後の精度（人の判断との類似性）で内容を提示することができると考えられる．また，5 項目前後の場合，同様に 9 割前後の精度が期待されることが分かった．

また，「中小企業の情報セキュリティ対策ガイドライン」1 文書に対する 3 つのフレームワークでの評価・比較ではあるが，今回の調査結果と各フレームワークの関係性から，文書内容の体系的な提示のためには，Cybersecurity Framework 1.1 を利用すると良いと考えられる．

今後の展望として，セキュリティ分野ではあるが異なるモデルを基に文書内容の提示を実施することができたことにより，他分野でも同一のアプローチによる文書内容の提示が行える可能性があると考えられる．

参考文献

[1] “「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”. https://www.ipa.go.jp/security/fy23/reports/jinzai/, (参照 2019-01-24).
[2] “情報セキュリティ人材不足数等に関する追加分析について（概要）”. https://www.ipa.go.jp/files/000040646.pdf, (参照 2019-01-24).
[3] “サイバーセキュリティ人材の育成に関する施策間連携ワーキンググループ報告書”. https://www.nisc.go.jp/conference/cs/pdf/jinzai-sesaku2018set.pdf, (参照 2019-01-24).
[4] “情報セキュリティ事故に関わるアンケート調査”. http://lab.iisec.ac.jp/~hiromatsu_lab/files/jiko-questionnaire_result.pdf , (参照 2019-01-24).
[5] “法人組織におけるセキュリティ実態調査 2017 年版”. https://appweb.trendmicro.com/doc_dl/select.asp?type=1&cid=236, (参照 2019-01-24)
[6] 中矢 誠, 富永 浩之. Web ゲームサイトを題材とした攻防型ハッキング競技の環境構築と運用実践 - 試行実践に基づいて改善を行った本番実践の結果と分析. 2018,vol 12, 研究報告コンピュータと教育（CE), p1-8
[7] 阿部 隆幸, 中矢 誠, 太田 翔也, 富永 浩之. 学校機関ごとの個別情報を組み込んだ情報セキュリティの導入教育のためのクイズ形式のアドベンチャーゲームの試作. 2017, 第 79 回全国大会講演論文集 p 737 -73
[8] 楠目 幹,阿部 隆幸, 中矢 誠,富永 浩之. 情報セキュリティの導入教育のための大会イベント BeeCon におけるハッキング競技 CTF の問題構築, 2017 第 79 回全国大会講演論文集 p 739 - 740
[9] 湯川 誠人,井口 信和. 仮想マシンを用いた攻防戦型ネットワークセキュリティ学習支援システムにおけるネットワーク型 IDS を用いた不正侵入シナリオの実装, 2018, インターネットと運用技術シンポジウム論文集, 92 - 99
[10] “運用者向けセキュリティ関連コンテンツ一覧”. http://www.meti.go.jp/policy/netsecurity/secdoc/ope_contents.html, (参照 2019-01-24)
[11] 尾崎敏司. 情報セキュリティに関連するガイドラインの内容提示の手法の提案とその評価, 2019 第 148 回 コンピュータと教育研究発表会
[12] ”CYBERSECURITY FRAMEWORK”. https://www.nist.gov/cyberframework, (参照 2019-01-24)
[13] ISO 27001. Information Security Management Systems
[14] Council on CyberSecurity, “The CIS Critical Security Controls for Effective Cyber Defense version 6.1”. https://www.tml.org/p/TheCISCriticalSecurityControlsEffectiveCyberDefense.pdf, (参照 2019-02-04)
[15] JIS Q 27001. 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
[16]「The Critical Security Controls for Effective Cyber Defense version 6.1」の NRI セキュアテクノロジーズの翻訳版 https://sans-japan.jp/resources/CriticalSecurityControls.html, (参照 2019-02-04)
[17] “重要インフラのサイバーセキュリティを向上させるためのフレームワーク”. https://www.ipa.go.jp/files/000038957.pdf, (参照 2019-01-24)
[18] Taku Kudo, Kaoru Yamamoto, Yuji Matsumoto: Applying Conditional Random Fields to Japanese Morphological Analysis, Proceedings of the 2004 Conference on Empirical Methods in Natural Language Processing (EMNLP-2004), pp.230-237
[19] “scikit-learn”. https://scikit-learn.org/stable/, (参照 2019-01-24)