メンタルモデルに着目した情報セキュリティ対策の教材のユーザーインタフェース改善とその効果に関する研究

２０２２年　３月

尾崎　敏司

メンタルモデルに着目した情報セキュリティ対策の教材のユーザーインタフェース改善とその効果に関する研究

尾崎　敏司

システム情報工学研究科

筑波大学

２０２２年　３月

目次

図目次

表目次

１．序論

この部では，まず情報セキュリティ対策の現状と課題について検討を行い，その後本論文の目的と構成について述べる．

1.1. 情報セキュリティ対策の現状と課題

本章ではまず，情報セキュリティ対策についての定義を行い，その後情報セキュリティ対策の現状について確認し課題を検討する．

1.1.1.　情報セキュリティ対策とは

この節では，情報セキュリティ対策とサイバーセキュリティ対策という用語について定義を行う．

まず，情報セキュリティ対策について定義するために，情報セキュリティの定義について確認する．情報セキュリティは，ISO/IEC 27000 [1]や，それを翻訳した JIS Q 27000 [2]においては，以下のように定義されている．

> *情報セキュリティ（information security）情報の機密性，完全性, 及び可用性を維持すること. 注記 さらに，真正性，責任追跡性，否認止，信頼性などの特性を維持することを含めることもある.*
>
> *機密性（confidentiality）認可されていない個人，エンティティ又はプロセスに対して，情報を使用させず，また，開示しない特性*
>
> *完全性（integrity）正確さ及び完全さの特性.*
>
> *可用性（availability）認可されたエンティティが要求したときに，アクセス及び使用が可能である特性.*
>
> *真正性（authenticity）エンティティは，それが主張するとおりのものであるという特性*
>
> *否認防止（non-repudiation）主張された事象又は処置の発生，及びそれらを引き起こしたエンティティを証明する能力.*
>
> *信頼性（reliability）意図する行動と結果とが一貫しているという特性.*
>
> *—ISO/IEC 27000:2013*

ここでの「エンティティ」とは，個人，集団，団体，法人を包括した一つの存在を示す概念であり，「プロセス」とは，相互に関連作用する一連の活動を意味している．責任追跡

性については，JIS Q 27000 上では明示的に定義がなされていないが，1989 年に発行された IS0 7498-2 [3]や，それを基に作成された JIS X 5003 [4]では，以下のように定義されている．

> *責任追跡 (accountability) あるエンティティの動作が，そのエンティティに対して一意に追跡できることを保証する特性.*
>
> *—JIS X 5003*

従って，情報セキュリティ対策とは，「あるエンティティ（個人，集団，団体，法人）において，情報の機密性，完全性，可用性，真正性，責任追跡性，否認防止，信頼性を維持するための一連の対策」を指すと定義できる．

また，情報セキュリティに似た用語として，サイバーセキュリティという用語が用いられることがある．サイバーセキュリティという用語は，ISO/IEC 27032:2012 [5] で以下のように定義されている．

> *preservation of confidentiality, integrity and availability of information in the Cyberspace*
>
> *—ISO/IEC 27032:2012*

従って，サイバーセキュリティとは，Cyberspace－サイバー空間における情報セキュリティであると考えられる．サイバー空間は，同様に ISO/IEC 27032:2012 の中で以下の様に定義されている．

> *the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form*
>
> *—ISO/IEC 27032:2012*

これを日本語に訳すと「人，ソフトウェア，インターネット上のサービスが，それに接続された技術装置やネットワークを介して相互に作用することで生じる複雑な環境で，物理的な形では存在しないもの」となる．そのため，サイバーセキュリティとは，特定のエンティティに限らずその周辺の要素（人，ソフトウェア，サービス）の相互の関係性まで含んだ環境に対しての情報セキュリティであると考えられる．

一方で， サイバーセキュリティ基本法の第二条 [6]においては，サイバーセキュリティは，以下のように定義されている．

> *「サイバーセキュリティ」とは、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式（以下この条において「電磁*

的方式」という）により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体（以下「電磁的記録媒体」という）を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む）が講じられ、その状態が適切に維持管理されていることをいう。

―“サイバーセキュリティ基本法 平成二十八年四月二十二日公布（平成二十八年法律第三十一号）改正

この法令では，前半の「電子的方式、～安全管理のために必要な措置」と後半の「情報システム及び情報通信ネットワークの安全性及び信頼性確保のために必要な措置」の 2 種類の措置が定義に含まれているが，どちらも前述のサイバー空間の定義に含まれていると考えられる．

以上より，サイバーセキュリティ対策とは，情報セキュリティ対策の対象を拡張した概念であり，「特定のエンティティに限らずその周辺の要素（人，ソフトウェア，サービス）の相互の関係性まで含んだ環境に対して，情報の機密性，完全性，可用性，（真正性，責任追跡性，否認防止，信頼性，）を維持するための一連の対策」と定義できる．

しかしながら，ISO/IEC 27032:2012 で定義されているサイバー空間の定義については，2017 年に改定には至らなかったが改定に向けた議論がなされるなど，多様な理解・解釈が存在しており未だ議論の最中にあると考えられる．

そこで，本論文においては，多様な理解・解釈が含まれる可能性があるサイバーという用語の使用を避ける目的で，サイバーセキュリティではなく情報セキュリティという用語を用いている．ただし，本研究における情報セキュリティ対策は，サプライチェーンなどの一つのエンティティに限らない周辺の要素（人，ソフトウェア，サービス）の関係性に含まれるため，実際には，上述で定義したサイバーセキュリティ対策と同じ意味で用いている．

1.1.2. 情報セキュリティに関わる人材不足

特定の企業や組織を標的とした標的型攻撃の被害の深刻化や，情報セキュリティに関する脅威の多様化や高度化に伴い，情報セキュリティに関わる人材の不足が 10 年ほど前から問題になっている．例えば，IPA が Web サイト [7]上に公表している 2012 年に発表した「情報セキュリティ人材の育成に関する基礎調査」 [8] および 2014 年に発表した継続研究 [9] によると，必要な情報セキュリティ人材数は約 8 万人と推定されており，2014 年の時点では，約 6 万人の人材が不足していると考えられてる．

また，廣松らが「情報セキュリティ事故対応ガイドブック」 [10]を作成する際に用いた情報セキュリティ大学院大学と神奈川県の共同調査「情報セキュリティ事故に関するアンケート調査報告書」 [11] の中では，日本の中小企業の約 25%が情報セキュリティの担当者を有しておらず，約 41%が他の業務との兼務者 1 名のみしか有していないと述べられている．しかしながら，この質問項目については無回答のものが 54%を占めており，これらの企業は 0 名である可能性が高いと述べられている．そのため，実態としてはより多くの中小企業において，情報セキュリティの担当者を準備できていないと考えられる．

1.1.3. サプライチェーン攻撃

中小企業などの小中規模の団体を対象とした攻撃の被害は軽微に捉えがちだが，情報セキュリティ対策は中小企業などの小中規模の団体を含む多くの組織で求められてきている．

最終的な攻撃対象にたどり着くための初段の攻撃として，安全性の低い関連企業や取引先の企業を攻撃する，サプライチェーン攻撃と呼ばれる攻撃手法がある．例えば， 2011 年に IPA により Web ページ上 [12]で公開された事例 [13]では，攻撃の初期段階として，最終攻撃対象の企業が所属する業界団体の職員の PC への侵入が行われている．また，標的型攻撃に限らず，2017 年に経済産業省により公開された「産業分野におけるサイバーセキュリティ政策」 [14]では，2017 年に流行したワーム型のランサムウェアである WannaCry の事例で，サプライチェーン経由で欧州企業から国内企業に感染した事例があると報告されている．このような事例以外でも，IPA により調査・公開されている「情報セキュリティ 10 大脅威 2021」 [15]の組織編において「サプライチェーン攻撃」は 4 位となっており，初めてサプライチェーン攻撃が順位に現れた 2019 年から高い順位を維持し続けている．

そのため，社会全体のセキュリティを向上させるためには，直接の攻撃の対象となる企業・政府組織のみでなく，中小企業など小中規模の団体における情報セキュリティを向上させることも重要となると考えられる．

法令面からもサプライチェーン全体に対して，情報セキュリティ対策が求められている．例えば，個人情報保護法（個人情報の保護に関する法律） [16] の 22 条では，以下のように取扱事業者に対して，委託先に対する安全管理義務を定めている．

> *個人情報取扱事業者は，個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。*
>
> *—改正個人情報保護法（個人情報の保護に関する法律）22 条*

これは，2017 年 5 月の公布により個人情報を取り扱うすべての事業者が対象となるように

改正が行われており，中小企業などの小さな団体もその対象に含まれる．

また， EU 加盟国（及び欧州経済領域の一部であるアイスランド，ノルウェー，リヒテンシュタイン）の個人データ保護を規定する法として 2018 年 5 月 25 日に策定された一般データ保護規則（GDPR: General Data Protection Regulation）においても，同様の条例が 28 条の 1 項で定められている．

> *Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject*
>
> *—General Data Protection Regulation, Article 28 Processor - 1*

ここでの controller とはデータの管理者を指し，この条項ではデータの管理者以外がデータを処理する場合において，処理を行う者が適切な技術的，組織的な対策を行うことを求めている．一般データ保護規則は，EU 加盟国と取引する全ての企業に適用されるため，中小企業のような小さな団体もその対象に含まれる可能性がある．

以上より，法令の観点からも中小企業における情報セキュリティ対策は求められていると考えられる．

1.1.4. 情報セキュリティ人材の育成について

セキュリティ人材の不足を受けて，日本の内閣サイバーセキュリティセンターにおいて，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 [17]が組織され，そのワーキンググループから 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」 [18]が発表されている．この報告書では， サイバーセキュリティに関わる人材を戦略マネジメント層と実務者・技術者層に分類している．このうち戦略マネジメント層については，報告書内で『「戦略マネジメント層」に相当する人材層に期待される知識・スキルは、技術系にとどまらず、ビジネス系、社会系、人間系など幅広い知識が必要である』（p14）とされている． また，実務者・技術者層においても戦略マネジメント層の指揮の元，「システムの企画や管理、システム構築を担う立場としてサイバーセキュリティのリスクマネジメントを実践する役割」（p10）を果たし，「リスクやセキュリティ対策など、サイバーセキュリティの実践に関わる内容について、説明を行うことが必要である」（p11）とされ，緊急時には，「関係者との連絡、調整や技術的な対処」（p11）を行うことが期待されている．そのため，実務者・技術者層についても，広く情報セキュリティについて知識や企業活動についての理解が求められると考えられる．

また，産業横断サイバーセキュリティ人材育成検討会 [19]が Web ページ [20]上で公開

している第二期最終報告書 [21] では，サイバーセキュリティの専門家や，一般的な IT 運用の専門家以外に，その両専門分野を繋げるようなセキュリティと企業活動の両方を理解しているエキスパートの必要性について述べられている．このエキスパートは，企業内のセキュリティ活動を統括していると述べられており，「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」における戦略マネジメント層や実務者・技術者層を包括する概念に相当すると考えられる．

1.1.5. 情報セキュリティ人材の獲得・育成における課題

1.1.2.節から 1.1.4 節で見てきたように，特に中小企業において情報セキュリティ人材の不足が指摘される一方で，あらゆる団体において 1.1.5 節で述べたようなエキスパートが存在することが望まれている．しかしながら，中小企業のような小さな団体においては新たにそのような人材を採用するのはリソースの問題から難しいと考えられる．そのため，エキスパート人材を確保するためには，既にいる情報システム担当者などの人材を情報セキュリティ担当者としても育成し，双方の知識を持ち合わせたエキスパート人材を作り上げることが必要となると考えられる．エキスパート人材へとなるためには，情報セキュリティ専門家としての個々の対応技術や分析そのものへの深い理解よりも，それらについての広い理解と自社のシステムとの関わりについて学ぶことが必要である．「産業横断サイバーセキュリティ人材育成検討会」 第二期最終報告書の中では，情報セキュリティ専門家とエキスパートである情報セキュリティ担当者の関係が会計士と（経営層に繋がるような）経理人材の関係性で例えられている．経理人材は，会計士としての詳細な知識は必要とされないがそれを理解するに足る知識と会社の経営に対する知見の両方が求められるのと同様に，情報セキュリティ担当者は，広くセキュリティについて学び自社組織に関わる部分について適用し続ける必要がある．これを実現するためには，情報セキュリティ対策に関する効果的な自己学習方法についての検討が重要である．

情報セキュリティの学習に役立つようなガイドラインやドキュメントなどの教材は現在多く発行されており，かつては経済産業省の Web サイト上にまとめられていた（現在では公開を終了してアーカイブ化されている [22]）．それらは，経営者向け，運用者向け，開発者向けに大別されており，情報セキュリティ担当者にとっては，特に，経営者向け，運用者向けが関係すると考えられる．経営者向けのものでは，ガバナンスや個人情報保護法に言及した解説書が多く，運用者向けのものでは，ガイドラインやガイドブックに限らず，セキュリティポリシーのサンプルやインデントレポートを含む多種の文書が整理されていた．公開当時，運用者向けのコンテンツのみでも 150 以上のコンテンツが登録されており，学習のための文書は十分に存在していると考えられる．経済産業省の Web サイトでの一覧化は行われなくなったが，これらの情報セキュリティの学習に役立つガイドラインやドキュメントは現在でも存在はしており，また，経済産業省のサイバーセキュリティ政策のサイト [23]上では，サイバーセキュリティ経営ガイドライン [24]などの経営者向け

のいくつかのガイドラインに絞って公開を行っている．

以上より，効果的な自己学習の方法を検討していく上では，新たに文書のコンテンツを作成するのではなく，既にあるコンテンツを活かすために，それらの学習教材のユーザーインタフェースや文書整理の方法を改善することが重要になってくると考えられる．特に本研究においては，インタフェースで重要視されるメンタルモデルの観点から，教材のユーザーインタフェースの議論を行う．

1.1.6. 本研究における用語定義

前節の課題において重要な用語である「教材」,「ユーザーインタフェース」,「メンタルモデル」は，定義や用法が分野や研究者により異なることがある．そこで，この項ではこれらの用語の一般的な定義について確認し，本研究で想定する適用範囲について述べる．

1.1.6.1. 教材

教材とは，一般には授業や学習に用いる教科書，副読本，標本などを指し，鈴木は教材を「ある人が何かを教えようと考えて，そのための材料として用意するもの」(鈴木 2002 p.2) [25]として定義している．そのため，厳密には教科書などの文書教材以外にもスライドなどのプレゼンテーション資料，映像教材，Web ページ，テストさらには学習管理のためのツールなども教材に含まれる．

本研究においては，このうち特に教科書や副読本などで特に文章による解説を主な内容とするものを対象としている．これは，本研究が独学を意図しており独学においては教科書などの文章による解説を利用することが多いと考えるからである．近年では，映像教材による教授も盛んにおこなわれているが，本研究ではこれを対象とはしない．プレゼンテーション資料についても，文書量が多いものについては本研究のアプローチの対象となりうるが，画像や映像が主体のものは対象としない．

しかしながら，本研究で得られる学習者のメンタルモデルについての示唆は，文書によらない教材においても参考になりうると考える．

1.1.6.2. ユーザーインタフェース

一般にユーザーインタフェースとは，ヒューマンマシンインタフェースのことを指し，コンピュータとその利用者の間で情報のやり取りを行う際の情報伝達の方法について意味することが多い．しかし，本研究ではこれを一般化して,「利用者が何かデバイスを用いる際に情報のやり取りを行う際の情報伝達の方法」をユーザーインタフェースとして定義して，特に，文書教材にもインタフェースがあると捉える．

従って，本研究における「教材のインタフェース」とは，文書に記載された内容（学習項目や本文，図表）そのものではなく，内容の並び順や表示方法や構成のことを指す．

本研究は文書の内容の改善ではなく，このユーザーインタフェースの観点から改善を試

みるものである．

1.1.6.3. メンタルモデル

メンタルモデルは，1943 年に Kenneth Craik によって初めて使用された用語であり，彼は，人間の心は現実の「小規模なモデル」を構築し，それを使って出来事を予測したり，説明を下敷きにしたりすると主張した [26]．この際，Craik は人間の推論は言語的なルールに基づいて行われると考えたが，現在では，ヒューマンマシンインタフェースやユーザビリティの分野でも研究が進み，スケッチや図なども含んだ概念として取り扱われる．例えば，Mental Models Global Laboratory [27]では，メンタルモデルを心理的スケッチ，建築家の設計図，図形，コミックストリップのようなものであると解説している．その正確な定義については研究毎に異なり，例えば，タッチパネル GUI に関する土井らの研究[28]では，「ユーザが操作対象インタフェースの操作を理解・想起しやすくするために構築する心理的モデル」として定義している．

そこで，本研究においては，メンタルモデルを「業務遂行者が対象業務を体系的・網羅的に実施するために対象業務の内容に対して構築する心理的モデル」として定義とする（ここでのモデルとは，言語的な説明に限らず図示やスケッチなども含む）．より具体的には，本研究では情報セキュリティ対策を対象業務とするため，「情報セキュリティ担当者が情報セキュリティ対策を体系的・網羅的に実施するために構築された情報セキュリティ対策の内容についての心理的モデル」を情報セキュリティ対策に対するメンタルモデルとして定義し調査対象とする．

1.2. 目的

本研究ではセキュリティ対策の学習者のメンタルモデルに着目し，以下の 3 点を目的として研究を行った．

1) 学習者が既存のガイドラインなどを教材として体系的に学習できるよう，情報セキュリティに関する教材の内容を，体系的な枠組みに基づいて提示すること
2) 教材のユーザーインタフェースを実際に改善するアプローチについて提案すること
3) 教材の改善の効果の確認として，以下の 2 点を明らかにすること
   3-1) 教材（のインタフェース）が学習者のメンタルモデルにどのように影響を及ぼすか
   3-2) メンタルモデルが学習効果とどのように関係するのか

まず，1)の目的に対して，既存の情報セキュリティに関する文書の内容をベクトルとして表現する手法の提案を行った．次に，2）の目的に向けて，その表現手法を援用して既存の教材の改良を行った．最後に，3）の目的に向けて，既存の教材と改良後の教材の 2 種類の教材を用いて比較実験を行い，それらが学習者のメンタルモデルに与える影響や学習の

効果に与える影響について測定，検証した．

また，メンタルモデルの調査においては，特定のセキュリティ技術についての調査が行われることが多く，本研究のように包括的な情報セキュリティ対策についてのメンタルモデルの調査が行われたものはない．また，情報セキュリティ教育分野の観点でも，実務者の自己学習を想定して教材の効果やメンタルモデルへの影響の調査を行ったものは存在しない．従って，目的の 3 を達成することにより，本研究はこれらの観点から貢献を行うことができると考える．

1.3. 本論文の構成と研究の流れ

本論文の構成について述べる．

第 2 部では，近年の関連研究について説明し，本研究の位置づけの確認を，情報セキュリティ分野におけるメンタルモデル研究と，情報セキュリティ分野での教育の観点から行う．

第 3 部では，本研究で基盤となる Ecological Interface Design（EID）の Abstraction hierarchy（AH）と Cybersecurity Framework(CSF) [29]とそれらの関係性について説明を行う．

第 4 部では，教材の作成の前段階として，既存の情報セキュリティに関する文書内容を C に基づいて評価する手法を提案する．これは，1.2 章に記載の 1)の目的を達成とともに，フレームワークと既存の教材を結びつけるための手段として利用することができる．

第 5 部では，5.1 章においてその手法を応用した教材の改良を行い，5.2 章においてその教材を用いて行った予備実験について述べる．ここで提示している教材の作成手順が，1.2 章に記載の 2)の目的に対応しており，予備実験の分析結果が，1.2 章に記載の 3-1)の目的に対応する．

第 6 部では，本実験の内容とその分析結果について述べる．予備実験とここでの分析結果が，1.2 章に記載の 3-1)と 3-2)の目的に該当する．

最後に，第 7 部において本研究の総括を行う．

本研究は，下記のような流れに従って実施された．

1) 教材のインタフェースが提供すべき適切なメンタルモデルについて検討をして，それに近い形式のセキュリティフレームワークについて調査する．
2) そのフレームワークに基づいて体系的に文書内容を表示する手法の提案を行う．この手法は既存の教材の内容とフレームワークを関連付けることにも用いられるため，教材のインタフェース改善のための手法の提案という側面を持つ．
3) この手法を用いて教材の改良を行う．
4) 改良された教材を用いた実験について設計して予備実験を通して調整を行う．
5) 本実験を行いその結果について分析をする．

それぞれの段階に対応する部・章と 1.2 章で記載した目的との関係を表 1 に記載する.

表 1　研究の流れ

Table 1　Research Process

研究の段階	対応する部・章	対応する目的
1)	3.　関連要素	
2)	4. セキュリティ対策文書の内容の表現手法の提案とその評価	1)学習者が既存のガイドラインなどを教材として，体系的に学習できるよう情報セキュリティに関する教材の内容を，体系的な枠組みに基づいて提示するこ
3)	5.1. Cybersecurity Framework に基づいた教材改良	2)教材のユーザーインタフェースを実際に改善するアプローチについて提案すること
4)	5.2. 作成した教材を用いた予備実験	3-1）教材（のインタフェース）が学習者のメンタルモデルにどのように影響を及ぼすかについて，確認する（副次的）
5)	6. 改良後の教材の効果とメンタルモデルの学習効果への影響	3-1）教材（のインタフェース）が学習者のメンタルモデルにどのように影響を及ぼすかについて，確認する. 3-2）メンタルモデルが学習効果とどのように関係するのかについて，確認する

２．研究の位置づけ

第 2 部では，近年の情報セキュリティにおけるメンタルモデルに関わる研究と情報セキュリティ教育の研究についてまとめ，本研究の位置づけについて確認する．

2.1. 情報セキュリティ分野のメンタルモデル研究

ユーザブルセキュリティの分野では，メンタルモデルは，重要な要素の一つである．そのため，情報セキュリティ分野におけるメンタルモデルに関する研究は多く存在する．

例えば，管理者とユーザーの間の HTTPS に対するメンタルモデルの違いを示した Krombholz らの研究 [30]や，暗号化に関するユーザーの 4 つの種類のメンタルモデルを指摘した Wu らの研究が挙げられる [31]．これらの研究では，実験参加者に図示作業を含む半構造化インタビューを行いメンタルモデルについて明らかにしている．また，Fulton らは，メディアがメンタルモデルに与える影響を明らかにし，誤ったメンタルモデルを植え付けないための推奨事項を述べている [32]． Mai らは，暗号通貨システムのユーザーが持っているメンタルモデルについて調査を行い，多くのユーザーは不正確または不十分なメンタルモデルを保持していることを確認し，メンタルモデルがツールのインタフェースによる影響を受けている可能性を示唆した [33]．この研究においても，実験参加者に図示作業を含む半構造化インタビューを行いメンタルモデルについて明らかにしている．しかしながら，いずれも特定のセキュリティ技術についてのメンタルモデルの調査に限定されたものであり，包括的な情報セキュリティ対策に対するメンタルモデルについての研究は行われていない．本研究はこの観点から貢献するものである．

2.2. 情報セキュリティ分野での教育研究

情報セキュリティ分野で用いられる教育・訓練についても研究されているが，その主な研究対象は，従業員の教育・訓練と情報セキュリティ対策の技術についての教育である．例えば，Capture The Flag (CTF) のようなライブ競技やゲーミフィケーションの手法，訓練方式の教育は，セキュリティの専門家の育成のために広く研究されてきた [34] [35] [36]．従業員向けの研究で精神面に着目したものでは，Chul による精神的なフロー状態に着目したものが知られている [37].

本研究で問題としている企業内での経営者とセキュリティの専門家をつなぐ包括的なエキスパートの育成に関する研究としては，専門家教育のための大学・大学院のカリキュラムを調査した，孫らの研究 [38]が挙げられる．孫らは，アメリカ国立標準技術研究所（NIST） [39]の下に設置されている NICE（The National Initiative For Cybersecurity Education）が定義した Cybersecurity Workforce Framework [40]に基づいて大学と大学院におけるセキュリティ教育課程カリキュラムの分析を行った(ただし，Cybersecurity Workforce Framework は 2020 年に Workforce Framework for Cybersecurity に改定されて

いる [41]). この研究では，Cybersecurity Workforce Framework の 783 個の技術能力項目を 62 種類の項目に集約している．この 62 の項目について，a） Cybersecurity Workforce Framework 内の単語出現数でつけた 62 項目の順位と，b）大学・大学院カリキュラムと 62 項目の対応付けを行い科目の数でつけた順位の二つの順位を作成し a）と b）の間の Spearman 順位相関係数を用いて，大学・大学院カリキュラムの妥当性を検証している．

この研究は，大学・大学院教育を対象に，カリキュラム開発の要求分析を目的として，Cybersecurity Workforce Framework に基づいた項目を単語の出現数や科目数で順位づけて比較を行い，教育課程全体の妥当性を評価している．

これは大学，大学院におけるカリキュラムについてその妥当性を評価する研究であり，実務者の自己学習を想定し，教材の方略的な利用の補助や個々の教材の効果とメンタルモデルへの影響の調査を行う本研究とは対象が異なる．

３．関連要素

第 3 部では，今回の教材のユーザーインタフェースの改良に利用した Ecological Interface Design の Abstraction Hierarchy (AH)と，情報セキュリティ対策を体系化・構造化した枠組みである Cybersecurity Framework(CSF) [29]，さらに， CSF と AH の関係性ついて説明する．その後，その他のセキュリティの枠組みについても同様に AH との関係性を検討する．これらについて論じることで，1.3 章の研究の流れの 1)で述べた通り，教材のインタフェースが提供すべき適切なメンタルモデルについて検討をして，それに近い形式のセキュリティフレームワークについて調査する．

また，自習についての一般的な学習理論である自己調整学習についてもここで述べる．

3.1. Ecological Interface Design

Ecological Interface Design(EID) は，1980 年代後半から 1990 年代前半にかけてデンマークのリソ国立研究所でヒューマンシステムの信頼性に関する広範な研究を行った Rasmussen と Vicente らによってインタフェース設計の枠組みとして提案され [42] [43]，複雑な社会システム，例えばプロセス制御（原子力発電所，石油化学プラントなど），航空，医療などの様々な領域に対して適用されてきた [44]．

EID では，周辺の環境と人間の知覚，認知，行動を理解することに重きを置いており，Abstraction Hierarchy(AH)や Skills, Rules, Knowledge (SRK) framework などの分析手法を用いて業務や周辺環境の分析を行いインタフェースの作成を実施する．

EID は主にヒューマンマシンインターフェースの設計に利用されるが，この EID に基づくインタフェースにより，ユーザーは正しいメンタルモデルを獲得することができ，ユーザーの認知的負荷を最適化することが知られている．例えば，古川らは，複雑なシステム（本研究では携帯電話）の適切なメンタルモデルをユーザーが持てるように支援するために，AH に基づいた自己学習法を提案しその効果を評価している [45]． AH は，EID において作業領域を分析し表現するために用いられる手法で，分析対象とする作業分野について，階層的に表現した図を作成する．典型的な物理的な装置では，AH は，Functional Purpose(FP), Abstract Function(AF), Generalized Function(GF), Physical Function(PF), Physical Form(PFo)の 5 つの階層で構成される．各層の説明を車の例と共に，表 2 に示し，具体的な車の AH の例を図 1 に示した．AH では図上の各構成要素の関係性が重要視され，下位の階層にある要素が必ず上位の階層にある要素の手段となるような「目的-手段」の関係で結ばれる（最上位にはシステム全体の目的が置かれる）．

本研究では，教材の改善において，この AH に基づいたインタフェースを提供する．

表 2　物理装置における Abstraction Hierarchy の典型的な層構造

Table 2　Typical structure of Abstraction Hierarchy in a physical device

層	設定されるもの	車の例
Functional Purpose	システムの目標と目的	・人や物を素早く輸送する ・人や物を安全に輸送する
Abstract Function	システムの目標を制御する基本的な法則や原則	・質量保存の法則 ・エネルギー保存の法則
Generalized Function	法則や原則を制御するための仕組み	・燃料の貯蔵，・発火，・燃焼， ・機械の動作，・排気　など
Physical Function	仕組みを達成するための物理的な構成要素	・ガソリン，・タンク　など
Physical From	構成要素の具体的な形状や位置や素材など	・タンクの位置，・材質　など

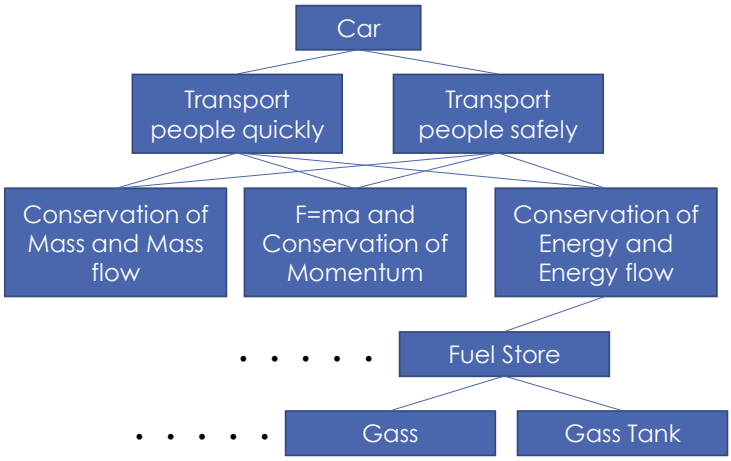


図 1　Catherine M.Burns, John R.Hajdukiewicz “Ecological interface Design” [44] の Figure 2.3 と 2.8 の 改変

Figure 1 Adapted from “Table 2 Cybersecurity Framework Core” in “Framework for Improving Critical Infrastructure Cybersecurity”

3.2. Cybersecurity Framework

CSF は，米国国立標準技術研究所（National Institute of Standards and Technology : NIST）から発行されているセキュリティフレームワークである．

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，現在ある多様なセキュリティ対策を体系化・構造化して，示している．CSF では，フレームワークコアと呼ばれるモデルが提示されており，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いる（図 2, 表 3）．

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「識別」，「防御」，「検知」，「対応」，「復旧」の 5 つが定義されている．

カテゴリは，機能をさらにセキュリティの効果によって 23 個に分類したものであり，サブカテゴリは，さらに具体的な対策に分類したものである．参考情報は，各サブカテゴリについて期待される成果を達成するための，既存の標準・ガイドライン・ベストプラク

ティスについてまとめたものである．

本研究では日本語文書を対象とするため，IPA により Web サイト上 [46]で公開されている CSF の 1.1 版の翻訳版である「重要インフラのサイバーセキュリティを改善するためのフレームワーク　1.1 版」 [47]を基に研究を行っており，用語やテキストマイニング時に用いる文章は，翻訳版に基づいて行われている．以降，本論文中で Cybersecurity Framework もしくは，その略称としての CSF が出てきた場合，この 1.1 版を指している．

表 2:フレームワークコア

機能	カテゴリー	サブカテゴリー	参考情報
識別 (ID)	**資産管理 (ID.AM):** 自組織が事業目的を達成することを可能にするデータ、人員、デバイス、システム、施設が、識別され、組織の目的と自組織のリスク戦略における相対的な重要性に応じて管理されている。	**ID.AM-1:** 自組織内の物理デバイスとシステムが、目録作成されている。	**CIS CSC** 1 **COBIT 5** BAI09.01, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: 自組織内のソフトウェアプラットフォームとアプリケーションが、目録作成さ	**CIS CSC** 2 **COBIT 5** BAI09.01, BAI09.02, BAI09.05

図 2　重要インフラのサイバーセキュリティを改善するためのフレームワーク　1.1 版の「表 2 フレームワークコア」より部分的に引用

Figure 2 Adapted from “Table 2 Cybersecurity Framework Core” in “Framework for Improving Critical Infrastructure Cybersecurity”

表 3　重要インフラのサイバーセキュリティを改善するためのフレームワーク　1.1 版の「表 1 機能とカテゴリーの識別子」にサブカテゴリ数を追記して引用

Table 3　Adapted from “Table 1 Function and Category Unique Identifiers” in “Framework for Improving Critical Infrastructure Cybersecurity”

機能 ID	機能	カテゴリ ID	カテゴリ(サブカテゴリ数)
ID	識別	ID.AM	資産管理 (6)
		ID.BE	ビジネス環境 (5)
		ID.GV	ガバナンス (4)
		ID.RA	リスクアセスメント (6)
		ID.RM	リスクマネジメント戦略 (3)
		ID.SC	サプライチェーンリスクマネジメント(5)
PR	防御	PR.AC	アイデンティティ管理とアクセス制御(7)
		PR.AT	意識向上およびトレーニング(5)
		PR.DS	データセキュリティ(8)
		PR.IP	情報を保護するためのプロセス及び手順 (12)
		PR.MA	保守 (3)
		PR.PT	保護技術 (5)
DE	検知	DE.AE	異常とイベント(5)
		DE.CM	セキュリティの継続的なモニタリング (8)
		DE.DP	検知プロセス(5)
RS	対応	RS.RP	対応計画の作成 (1)

		RS.CO	コミュニケーション(5)
		RS.AN	分析 (5)
		RS.MI	低減 (3)
		RS.IM	改善 (2)
RC	復旧	RC.RP	復旧計画の作成 (1)
		RC.IM	改善 (2)
		RC.CO	コミュニケーション (3)

3.3. Cybersecurity Framework と AH の関係性

CSF のフレームワークコアの機能，カテゴリ，参考情報の関係は目的と手段の関係性を持っているため，　情報セキュリティ対策における先に説明した AH の一種として捉えることができると考える．

フレームワークコアの表 3 の上では明示的に記載されていないが，CSF 最終的な目的は名前からも，サイバーセキュリティ（情報セキュリティ）の実行と改善にあると考えられる．これが AH における FP に当たると考えられる．

この目的を達成するためには，社内の状況を「識別」し，「防御」し，何か発生した場合に「検知」し，「対応」し，「復旧」する必要がある．これは，CSF の機能にあたり，AH では AF にあたると考えられる．この機能を達成するため，それぞれの「カテゴリ」を実行する必要がある．これは AH における GF にあたる．例えば，「識別」は，「資産管理」や「ガバナンス」などのカテゴリを実行することによって達成される．さらにこのカテゴリを達成するためには，サブカテゴリ―の項目を達成する必要がある．これは AH における PF にあたる．例えば，「資産管理」のカテゴリを達成するためには，自組織内の物理デバイスとシステムの目録や，ソフトフェアプラットフォームやアプリケーションの目録，データフロー図の作成などが実行される必要がある．CSF 上では，AH の PFo に当たるものは規定されていないが，実際に作成・運用されているセキュリティポリシーやプロセス，導入されたシステムが，これに該当すると考えられる．以上の関係性を，表 4 としてまとめる．

表 4　AH と Cybersecurity Framework のフレームワークコアの関係

Table 4　Relationship between AH and Cybersecurity Framework Core

AH 層	フレームワークコア	具体的な例
Functional Purpose	記述なし	情報セキュリティ対策の実行と改善
Abstract Function	機能	識別，防御，検知，対応，復旧
Generalized Function	カテゴリ	資産管理，ビジネス環境，ガバナンス　など
Physical Function	サブカテゴリ	自組織内の物理デバイスとシステムの目録作成　など
Physical Form	記述なし	実際のポリシー，プロセス，システム

3.4. その他の枠組みについて

ここでは，3.3 章の議論の補足として，CSF 以外の一般的な情報セキュリティに関連する枠組みについて確認して，それらが AH になりうるかの検討を行う．

3.4.1. ISO/IEC 27001

ISO/IEC 27001:2013 [48]（および，JIS Q 27001:2014 [49]）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）に関して，国際標準化機構（ISO）と国際電気標準会議（IEC）が共同で策定した国際規格である．その目的は，リスクマネジメント情報の機密性，完全性及び可用性を維持し，かつ，リスクを適切に管理しているという信頼を利害関係者に与えることにあるとされている．したがって，情報セキュリティ全般を対象にしているものではなく，リスクマネジメントに注力した規格であると考えられる．

また，規格の構成としては，「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 5）． しかし，これは ISO マネジメントシステムの枠組みを定義する附属書 SL の Appendix3 によって定義された上位構造であり，情報セキュリティ分野に基づいて作成されたものではない．

以上より，ISO/IEC 27001:2013 は，情報セキュリティ対策おいて重要な規格ではあるが，特定範囲に限定された規格であり，構成も一般に定義されたものであるため，情報セキュリティ対策全体に対しての AH として利用することは難しいと考えられる．

表 5　ISO/IES 27001 の大項目と項目

Table 5　Items of ISO/IES 27001

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

3.4.2. Center for Internet Security(CIS) Control

CIS Control（または，CIS Critical Security Controls）は，米国のセキュリティ専門団体である SANS Institute が取りまとめるセキュリティ対策フレームワークである．システムやネットワークに対する一般的なサイバー攻撃を軽減するために，一連の防護策を整理，優先度付けしたもので，既存の法律，規制，およびポリシーなどの枠組みにマッピングされている．2021 年 5 月に公開された CIS Critical Security Controls Version 8 [50]では，Control と呼ばれる 18 の項目が定義されており，さらに各項目の中の個別の保護手段を IG 1 から IG 3 までの実装グループ(Implementation Group)に分類している（表 6）．実装グループは,実装の優先度を表すグループで，IG 1 が最も優先的に実装を行うべき項目であると考えられている．

各 Control と各保護手段の関係は目的と手段の関係性と捉えることが可能だが，段階的な階層構造を構築しているわけではないため，AH として利用することは難しいと考えられる．

表 6　CIS- Critical Security Controls 8 の項目

Table 6　Items of CIS- Critical Security Controls 8

	項目
CONTROL1:	組織の資産のインベントリと管理
CONTROL2:	ソフトウェア資産のインベントリと管理
CONTROL3:	データ保護
CONTROL4:	組織の資産とソフトウェアの安全な構成
CONTROL5:	アカウント管理
CONTROL6:	アクセス制御管理
CONTROL7:	継続的な脆弱性管理
CONTROL8:	監査ログ管理
CONTROL9:	電子メールと Web ブラウザの保護
CONTROL10:	マルウェアの防御
CONTROL11:	データ復旧
CONTROL12:	ネットワークインフラストラクチャ管理
CONTROL13:	ネットワークの監視と防御
CONTROL14:	セキュリティ意識向上とスキルのトレーニング
CONTROL15:	サービスプロバイダーの管理
CONTROL16:	アプリケーションソフトウェアセキュリティ
CONTROL17:	インシデントレスポンスと管理
CONTROL18:	ペネトレーションテスト

3.4.3. Cyber Kill Chain

Kill Chain はもともと軍事で使用される言葉で，標的の特定，標的への部隊派遣，標的への攻撃の決定と命令，そして最終的な標的の破壊という，軍事的な攻撃の構造について述べたモデルである．各段階は鎖のようにつながっており，一部の行為を妨害することで，攻撃そのものを失敗させることができると考えられている． Lockheed Martin 社の Eric M. Hutchins らの研究 [51]において，この概念を情報セキュリティの標的型攻撃に適用した

ものが，Cyber Kill Chain [52] である．Cyber Kill Chain は Reconnaissance，Weaponization，Delivery，Exploitation，Installation，Command & Control，Actions On Objectives の 7 つのステップで構成されている．

Reconnaissance は，日本語では偵察と訳されることが多く，攻撃対象となる企業の情報を収集する行為である．例えば，e-mail アドレスや組織構造や取引先の情報を入手する行為が該当する．

Weaponization は，日本語では武器化と訳されることが多く，攻撃に必要なエクスプロイトコードや，マルウェアを準備する段階を表す．

Delivery は，日本語ではそのままデリバリーとされるか，配送と訳され，攻撃対象の組織の人間にエクスプロイトコードやマルウェアを実行させる行為である．例えば，関係者を装った標的型の e-mail や水飲み場型の攻撃が該当する．

Exploitation は，日本語ではそのままエクスプロイトとされて，脆弱性へのコードの実行を指す．

Installation は，日本語ではそのままインストールとされ，Exploitation の結果として発生するマルウェアのインストールを意味している．

Command & Control（C2 ないし C&C）は，日本語では遠隔操作と訳される場合もあり，インストールしたマルウェアを用いて対象の端末操作を行う．この段階では，必要に応じて権限昇格などを行いながら他の端末への再感染などを繰り返して対象組織内の探索を行う．

Actions On Objectives は，日本語では目的の実行と訳され，目的の情報を探し出した後持ち出すことを意味する．

本来の Kill Chain と同じく，この一連の鎖のうち一部分を妨害することで攻撃者の攻撃目的を失敗させることが Cyber Kill Chain のアプローチである．しかしながら，モデルそのものは，攻撃について枠組みを与えたものであり，情報セキュリティ対策そのものについての情報は含まれていない．そのため，情報セキュリティ対策の枠組みとして利用することは難しいと考えられる．また，単層構造のハイレベルな概念であり，AH にみられるような複層構造を持っているわけではないため，この点からも AH としては不適切であると考えられる．

3.4.4. MITRE ATT&CK

MITRE ATT&CK [53] は，米国の連邦政府が資金を提供する非営利組織である MITRE が発表しているセキュリティフレームワークで，ATT&CK は Adversarial Tactics, Techniques, and Common Knowledge の略で，敵対的戦術，テクニック，共通知識を意味している． MITRE ATT&CK: Design and Philosophy [54]によると，このフレームワークは Cyber Kill Chain などのハイレベルなモデルよりも具体的な技術・技法について整理している．

その構成としては，Pre- ATT&CK マトリクス，エンタープライズ向けのマトリクス，モバイル向けのマトリクスと 3 つのマトリクスが定義されている．Pre- ATT&CK マトリクスは，Cyber Kill Chain の Reconnaissance から Delivery の段階についてまとめており，エンタープライズ向け，およびモバイル向けのマトリクスは Exploitation 以降の段階について，攻撃対象とするデバイスごとにまとめている．

各マトリクスは，Tactics（戦術），Techniques/Sub-Techniques（技術・手法），Adversary Group（サイバー攻撃者グループ）, Software（攻撃ツール）, Mitigations（緩和策）の情報を保持しており，これらは 図 3 に示すような関係性がある．

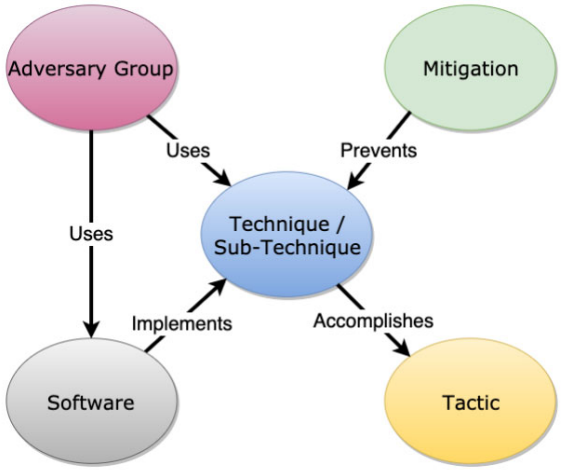


図 3 MITRE ATT&CK: Design and Philosophy [54]の Figure 3. ATT&CK Model Relationships から引用

Figure 3 Quoted from “Figure 3. ATT&CK Model Relationships” in “MITRE ATT&CK: Design and Philosophy”

本研究で注目すべきなのは，Tactic と Technique の関係性で，Technique は Tactic を達成するための手段として整理されている．これは AH の満たすべき目的手段関係と一致しており，MITRE ATT&CK は，この観点で AH の候補となりうる．しかしながら，MITRE ATT&CK は，Cyber Kill Chain と同じく攻撃手法について枠組みをあたえたものであるため，情報セキュリティ対策の枠組みとして利用することは難しいと考えられる（その一方で，攻撃者の AH を検討する場合では，MITRE ATT&CK は AH の候補として有力である）．

3.4.5. Cybersecurity Workforce Framework

Cybersecurity Workforce Framework は，サイバーセキュリティにおける様々な業務やそれに求められる能力などを共通化するために NIST が策定したフレームワークで，サイバーセキュリティ人材に求められる役割や業務の遂行に必要とされる具体的な知識，技術，能力が定義されている．具体的には，一番上位の概念として 7 つの Category（業務分野）

が定義されており，その下に 33 個の Specialty Area（専門分野）さらにその下に 52 個の Role（役割），さらにその下に 1007 個の Task（業務)が定義され，その下に Knowledge（知識）・Skill（技術）・Ability（能力)が紐づく．セキュリティ対策について注目したものではなく，役割とその遂行能力について着目した枠組みで，情報セキュリティ対策そのものについては着目していない．そのため，この枠組みを情報セキュリティ対策の AH として利用するのは難しいと考えられる．

3.5. 自己調整学習に関する研究

自己調整学習とは，1990 年代からアメリカの教育心理者 Barry Zimmerman らが中心となって提案している教育心理学の理論体系で，学習者の主体的な学習方略を重要視している [55] [56]．学習方略とは，学習に取り組む戦略のことで，自己調整学習では，学習方略を大きく，認知的方略（例：関連付けて覚える），メタ認知的方略（例：勉強時間と学習範囲を記録する），動機付け方略（例：学習の目的を書き出す）に分けている．

このうち認知的方略に含まれる体制化方略と図示化方略は，国内では，松沼 [57]により英語の現在完了形の学習において，実験的に学習効果の向上が確認されている．体制化方略とは，「何らかの理論や枠組みによって学習要素を相互に関連付けて整理する方法」であり，図示化方略とは，文字通り「図示により整理」を行う方法である．

本研究で試みている体系的な文書内容の提示やインタフェースの改善は，CSF に基づいており，これは自己調整学習の文脈では，体制化方略に当たると考えられる．

４．セキュリティ対策文書の内容の表現手法の提案とその評価

第 4 部では， 3.2 章で解説した Cybersecurity Framework(CSF)のフレームワークコアに関連付けて，情報セキュリティに関連する文書の内容を表現する方法についての提案と評価を行った．この部の内容は，「Cybersecurity Framework に基づく情報セキュリティガイドラインの内容可視化の提案」 [58]に基づいている． 1.3 章の研究の流れの 2)で述べた通り，フレームワークに基づいて体系的に文書内容を表示する手法の提案を行う．また，この手法は既存の教材の内容とフレームワークを関連付けることにも用いられるため，教材のインタフェース改善のための手法の提案という側面を持つ．

4.1. 概要

この部では CSF のフレームワークコアと文書の関係性を明らかにする手法について提案を行い，その手法についてその結果の妥当性の検証を行った．4 部の研究の概要図を図 4 に示す．4.2 章で目的について改めて述べ，4.3 章で CSF に基づいた表現手法の提案を行い，4.4 章においてその結果についての検証を行う．

この提案手法[1] には，2 つの目的が存在する．

1) セキュリティ関連のガイドラインに関して CSF に基づいて整理を行うことで，学習者の体制化方略を補助する．
2) EID に基づいた教材の改善の事前準備として，教材の内容と CSF のフレームワークコアの関係性を明らかにする．

本研究では，実際に複数の文書に対して提案手法に基づいた分析しベクトル的に表現することを試みた．その後，質的コーディングの結果との比較を行い，CSF に基づいたテキストマイニングの結果の妥当性を検証した．

CSF のフレームワークコアの「機能」と「カテゴリ」に基づいて，質的コーディングを実施して得た結果と提案手法の結果の類似性を，コサイン類似度とピアソン積率相関係数を用いて確認した．コサイン類似度を「機能」で比較した場合は平均 0.907,「カテゴリ」で比較した場合は平均 0.761 となり，相関係数も「機能」による比較では強い正の相関を示し，「カテゴリ」による比較でも正の相関を示した．これにより提案手法の分析結果の妥当性について確認できた．

1 この後現れる「提案手法」という用語は，全てこの部で説明をする「tf-idf とコサイン類似度を用いて CSF の枠組みで文書の内容をベクトル的に表現する手法」を指している．数理的に新規性のある提案が行われいるわけではない．

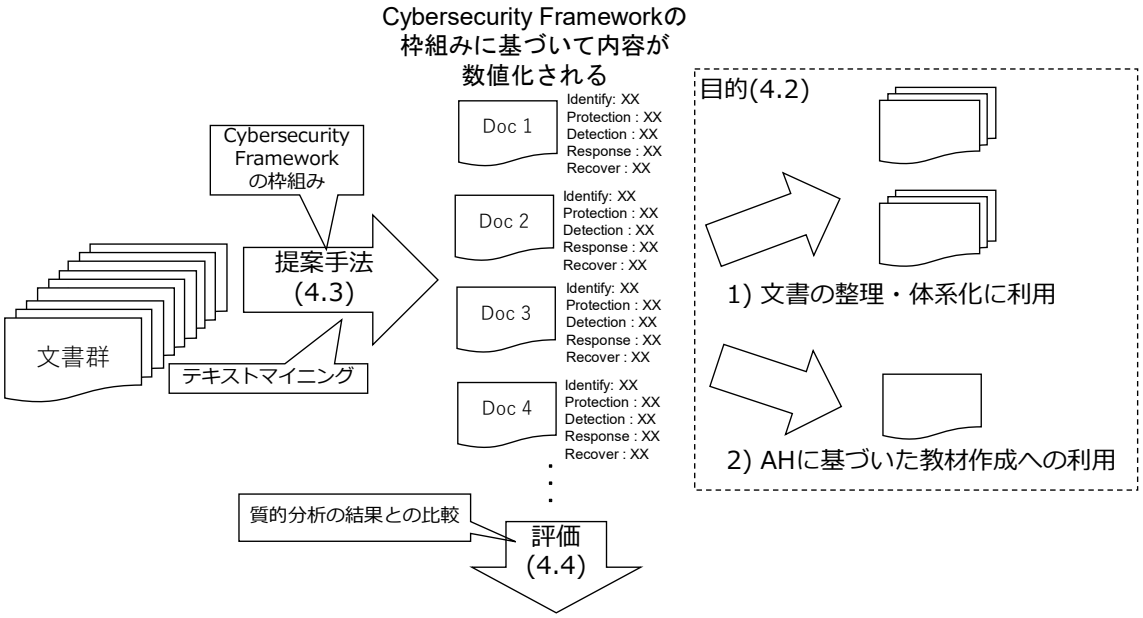


図 4　第 4 部の提案の概要図

Figure 4 Schematic diagram of Part 4

4.2. 目的

この第 4 部では，主に以下の 2 つを目的として研究を進めた．

1．多数ある情報セキュリティ関連の教材を上手く整理して学習させることを目的に，体制化方略の補助となるような文書内容を分析し表示する方法の提案

2．EID に基づいた教材の作成の前段階として，既存の情報セキュリティに関する文書を CSF のフレームワークコアの内容と結びつける手法の提案

上記の目的を満たすような手法について提案を行い，その手法の妥当性の評価を行った．提案手法では，CSF のフレームワークコアに基づいて，解析対象とした情報セキュリティに関連したガイドラインや文書の中に，情報セキュリティ対策のどの機能とカテゴリがどの程度含まれているかを表現した．

4.3. 提案手法—Cybersecurity Framework のフレームワークコアに基づく文書内容の提示

CSF のフレームワークコアのカテゴリに基づいて，単語の重要度を評価する手法である TF-IDF [59]により，解析対象とした情報セキュリティに関連したガイドラインの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重要とみなされる単語の類似性を評価することで，フレームワークコアに基づいた内容の情報の提示を行う．

文書の内容表現や可視化や要約の取り組みでは，文書の内容・構造などを仮定せずに対象の文書を目的に合致する形式で再構成し可視化を行う方針と，文書の内容・構造を事前に仮定して，それに従って解析・再構成を行う方針が存在すると考えられる．前者の方針

は多く研究がなされており，近年でも，Park らによる対話的に語彙を入力させて文書の内容を可視化する手法が研究されている [60].

一方，後者の方針による研究事例は少なく，例えば，2006 年の赤石による物語構造に基づき動的に連想される情報を提示するフレームワークの研究を挙げることができる [61]. しかしながら，特に情報セキュリティ関連の文書について，フレームワークに基づいて文書内容の表現や可視化を試みたものは存在していない.

情報セキュリティ分野では， 体制化された情報である既存のフレームワークが既にいくつか存在しているため、情報セキュリティ対策の文書の内容の表現や要約において，事前に内容や構造を仮定して解析することにより，体制化方略につながる情報提示を容易に行うことができると考えられる．特に，本研究で利用した CSF の枠組みは第 3 部で検討した通り AH に類似した構造を持っており，AH に基づいたユーザーインタフェースは効果的な学習を提供する可能性が示唆されている.

また，枠組みを用いない内容表示方法では，解析対象の文書の内容のみでその文書内容を表現するため，その文書にある特定の内容が書かれていないという情報を表現することは難しい．しかし，既存のフレームワークを用いることで，文書上に記述がない分野がある場合でも，その分野について記載がないことを表現することができると考えられる．これにより，学習者が教材を選択する際にすでに学習済みの内容を多く含む教材を避けることができると考えられる.

補足として，一般的によく使われることの多い「枠組みを用いないテキストマイニング手法」を本研究の対象としている文書に適用した場合の結果についての検討を行っているが，それは付録 1 に記載する.

4.3.1. TF-IDF

TF-IDF とは，Term frequency-Inverse document frequency の略であり，単語がどれだけ重要かを反映することを目的とした数値統計量である．情報検索，テキストマイニング，ユーザーモデリングなどの検索において，単語の重み付け要素としてよく用いられる.

単語の文書内の出現頻度である Term Frequency(TF)と，ある単語がでてくる文書頻度の逆数の対数である Inverse Document Frequency(IDF)の積で表現される.

TF，IDF 共に様々な定義が存在するが，一般的には下式のように定義される.

$$tfidf_{ij} = tf_{ij} \cdot idf_i \quad \cdots\cdots\text{式 1}$$

$$tf_{ij} = \frac{n_{ij}}{\sum_k n_{kj}} \quad \cdots\cdots\text{式 2}$$

ここで，分子 n_{ij}は，ある単語t_iの文書d_j内での出現回数を表し， 分母 $\sum_k n_{kj}$は文書d_j内のすべての単語の出現回数の和を表している.

$$idf_{ij} = \log \frac{|D|}{|\{d:d \ni t_i\}|} \quad \cdots\cdots\text{式 3}$$

ここで，分子$|D|$は，解析対象とするすべての文書の数を表し，分母$|\{d: d \ni t_i\}|$は，単語t_iが含まれる文書の数を表す．

文書内で頻繁に出現する単語はその文書中で重要な単語であると考えられる一方で，あらゆる文書で一般に高い頻度で出現してしまう単語も存在すると考えられる．この問題に対して，IDF は共通して現れる一般的な語を低く評価することでフィルタのように働く．これにより TF-IDF では，特定の文書にしか出現しない単語がより高く評価されることになる．

TF-IDF の分析を行うことで，対象の文書群の単語の全てに対して，ある文書における重要度を定めることができる．本論文では，ある文書に現れる単語すべての重要度をベクトルで表記したものを特徴語ベクトルと呼称する．

本研究で用いている TF-IDF について説明する．本研究で TF-IDF の計算に用いている scikit-learn [62]のライブラリ上では，上記の一般的な定義と異なる実装が行われている．

具体的には，TF の定義は変わらないが，IDF の計算で異なる定義が用いられている．scikit-learn のライブラリ上の定義 idf_{ij}' を以下に示す．

$$idf_{ij}' = \log \frac{1+|D|}{1+|\{d:d \ni t_i\}|} + 1 \quad \cdots\cdots\cdots \text{式 } 4$$

ここでは，log 中に分母と分子に 1 を足す平滑化処理が行われている．

また，デフォルトでは TF-IDF は L2 正規化された状態で出力される．つまり，scikit-learn のデフォルトでは TF-IDF を以下のように定義している．

$$tfidf_{ij} = \left\| tf_{ij} \cdot idf_{ij}' \right\|_2 \cdots\cdots\cdots \text{式 } 5$$

本実験では，scikit-learn の定義によって計算を進めているが，TF-IDF の基本的な考え方や効果は変わらないと考えられる．

4.3.2. 提案手法

解析対象の文書中のある行 L_j が，フレームワークコアのあるカテゴリ 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，CSF の記述を基に作成したカテゴリ C_i に対して TF-IDF を用いて作成した特徴語ベクトル $\mathbf{c_i}$ と，ある行 L_j に対して CSF 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．

文章全体の中にカテゴリ C_i に関連する記述がどの程度あるかを表すスコア $S_i(C_i)$ は，$\mathbf{l_j}$ と $\mathbf{c_i}$ のコサイン類似度の総和となるので，下式で評価することができると考えられる．

$$S_i(C_i) = \sum_j \frac{\vec{l}_j \cdot \vec{c}_i}{|\vec{l}_j||\vec{c}_i|} \cdots\cdots\cdots \text{式 } 6$$

具体的には，下記の手順 1 から 5 でスコア $S_i(C_i)$ の計算を行った．手順を図示したものを図 5，図 6，図 7 として示す．本研究では，プログラミング言語は python を用い，TF-IDF とコサイン類似度の計算は scikit-learn を利用している．

1. CSF の翻訳版である「重要インフラのサイバーセキュリティを改善するためのフレームワーク　1.1 版」内で各カテゴリ C_i について記述されている部分を実際に読んで確認し，カテゴリごとに抽出した．また，カテゴリ C_i が属している機能に関する記述も同様に実際に読み抽出し，あるカテゴリ C_i の文書の一部として取り扱った（図 5 の 1. を参照）．具体的には，「重要インフラのサイバーセキュリティを改善するためのフレームワーク　1.1 版」の本文 2.1 や付録 A などの各機能，カテゴリについての説明を用いている．
2. 抽出した各カテゴリと機能の文書集合に対して，Mecab [63]を用いて標準のシステム辞書で分かち書きと形態素解析を実施して名詞を取り出し，名詞だけの集合に変換した（図 5 の 2.を参照）．
3. 名詞句による文書集合に対して，それぞれのカテゴリ C_i 毎に，正規化した TF-IDF による特徴語ベクトル $\mathbf{c_i}$ を作成した（図 5 の 3.を参照）．また，同時に「重要インフラのサイバーセキュリティを改善するためのフレームワーク　1.1 版」の語彙と文書頻度を得た．作成された特徴語ベクトルの次元は 361 次元で，各カテゴリの上位 10 の単語については，「表 7　カテゴリ毎に抽出された特徴語上位 10 個」として記載した．

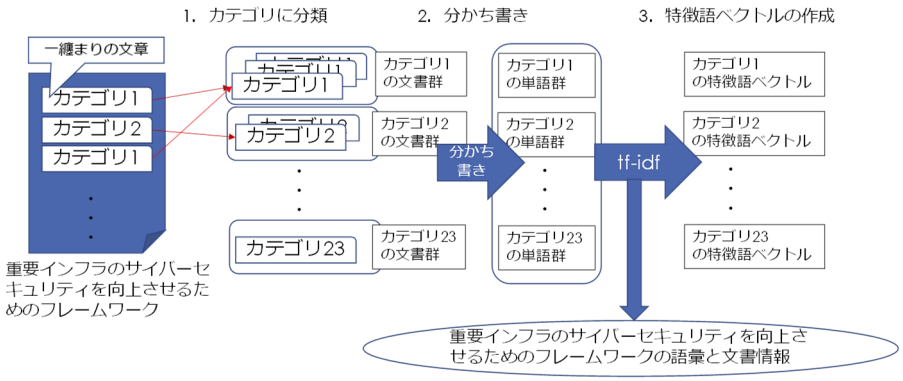


図 5　手順：フレームワークコアの機能とカテゴリの特徴語ベクトルの作成

Figure 5 Schematic diagram of the proposal: Creating feature word vector of Cybersecurity Framework's categories and functions

表 7　カテゴリ毎に抽出された特徴語上位 10 個

Table 7　Top 10 words extracted for each category by TF-IDF

機能	カテゴリ	特徴語上位 10 個　() は TF-IDF の値
識別	資産管理	管理(0.367)，リスク(0.298)，ビジネス(0.281)，事業(0.250)，特定(0.236)，戦略(0.223)，組織(0.193)，資産(0.183)，サイバーセキュリティリスク(0.177)，理解(0.157)
	ビジネス環境	ビジネス(0.351)，管理(0.302)，リスク(0.295)，上(0.264)，理解(0.233)，順位(0.193)，優先(0.193)，サイバーセキュリティリスク(0.175)，付け(0.175)，組織(0.157)
	ガバナンス	管理(0.398)，リスク(0.317)，サイバーセキュリティリスク(0.289)，ビジネス(0.267)，理解(0.256)，上(0.209)，ガバナンス(0.200)，組織(0.199)，特定(0.158)，環境(0.149)

	リスクアセスメント	リスク(0.351)，ビジネス(0.305)，サイバーセキュリティリスク(0.289)，管理(0.266)，特定(0.214)，資産(0.210)，組織(0.199)，企業(0.193)，アセスメント(0.181)，機能(0.173)
	リスク管理戦略	リスク(0.523)，管理(0.276)，ビジネス(0.267)，戦略(0.224)，順位(0.178)，サイバーセキュリティリスク(0.178)，優先(0.178)，組織(0.169)，許容(0.167)，度(0.167)
	サプライチェーンリスク	リスク(0.368)，管理(0.302)，サプライチェーンリスク(0.263)，ビジネス(0.253)，評価(0.237)，組織(0.198)，順位(0.185)，優先(0.185)，サイバーセキュリティリスク(0.169)，特定(0.150)
防御	ID 管理とアクセス制御	アクセス(0.532)，認可(0.306)，保護(0.211)，認証(0.197)，防御(0.196)，制御(0.196)，トランザクション(0.175)，管理(0.174)，ユーザ(0.158)，デバイス(0.158)
	意識向上およびトレーニング	トレーニング(0.344)，向上(0.322)，意識(0.322)，保護(0.303)，防御(0.215)，セキュリティ(0.212)，責任(0.193)，関連(0.181)，手順(0.171)，教育(0.168)
	データセキュリティ	保護(0.494)，データ(0.280)，性(0.265)，完全(0.249)，防御(0.240)，情報(0.226)，可用性(0.211)，機密(0.188)，セキュリティ(0.182)，記録(0.150)
	情報を保護するためのプロセスおよび手順	保護(0.524)，手順(0.267)，防御(0.242)，情報(0.218)，プロセス(0.213)，セキュリティ(0.176)，範囲(0.174)，コミットメント(0.174)，経営(0.154)，目的(0.139)
	保守	保守(0.449)，保護(0.317)，修理(0.263)，制御(0.225)，防御(0.225)，実施(0.194)，手順(0.179)，アクセス(0.168)，用(0.155)，コンポーネント(0.155)
	保護技術	保護(0.501)，技術(0.363)，防御(0.242)，手順(0.193)，セキュリティソリューション(0.189)，セキュリティ(0.184)，ポリシー(0.181)，制御(0.170)，確保(0.167)，レジリエンス(0.155)
検知	異常とイベント	検知(0.569)，異常(0.462)，イベント(0.417)，タイムリー(0.232)，把握(0.154)，発見(0.154)，サイバーセキュリティイベント(0.142)，継続(0.142)，モニタリング(0.142)，可能(0.125)
	セキュリティの継続的なモニタリング	モニタリング(0.523)，検知(0.501)，継続(0.289)，サイバーセキュリティイベント(0.253)，セキュリティ(0.190)，有効(0.173)，検証(0.173)，異常(0.157)，発見(0.157)，識別(0.144)
	検知プロセス	検知(0.776)，異常(0.273)，イベント(0.226)，プロセス(0.224)，タイムリー(0.205)，継続(0.151)，テスト(0.140)，発見(0.137)，サイバーセキュリティイベント(0.126)，モニタリング(0.126)
対応	分析	対応(0.571)，分析(0.439)，実施(0.196)，支援(0.186)，適切(0.178)，サイバーセキュリティイベント(0.178)，低減(0.165)，対処(0.165)，検知(0.165)，計画(0.148)
	コミュニケーション	対応(0.535)，機関(0.216)，執行(0.216)，法(0.216)，コミュニケーション(0.216)，調整(0.191)，間(0.191)，利害(0.182)，内外(0.173)，関係(0.172)
	改善	対応(0.655)，改善(0.311)，教訓(0.269)，過去(0.203)，現在(0.203)，活動(0.197)，意思(0.163)，計画(0.155)，サイバーセキュリティイベント(0.150)，低減(0.139)
	低減	緩和(0.393)，対応(0.381)，低減(0.323)，インシデント(0.269)，根絶(0.236)，拡大(0.236)，影響(0.182)，サイバーセキュリティイベント(0.174)，実施(0.174)，対処(0.162)
	対応計画	対応(0.726)，計画(0.295)，発生(0.223)，検知(0.219)，実施(0.214)，サイバーセキュリティイベント(0.214)，対処(0.132)，低減(0.132)，維持(0.123)，タイムリー(0.116)
復旧	コミュニケーション	復旧(0.628)，者(0.187)，計画(0.168)，ベンダ(0.165)，被害(0.165)，コミュニケーションコーディネーティングセンター(0.165)，オーナー(0.165)，インターネットサービスプロバイダ(0.165)，csirt(0.165)，機能(0.142)
	改善	復旧(0.712)，計画(0.302)，改善(0.259)，教訓(0.224)，将来(0.169)，機能(0.145)，軽減(0.135)，実現(0.135)，状態(0.135)，阻害(0.135)
	復旧計画	復旧(0.779)，計画(0.294)，維持(0.184)，タイムリー(0.173)，サイバーセキュリティイベント(0.159)，実施(0.159)，機能(0.124)，阻害(0.115)，状態(0.115)，軽減(0.115)

4. 適用対象の文章から 1 行ごと文字列を抜き出して，「重要インフラのサイバーセキュリティを改善するためのフレームワーク　1.1 版」の語彙と文書頻度を用いて，特徴語ベクトル $\mathbf{l}_j$ を計算した（図 6）.

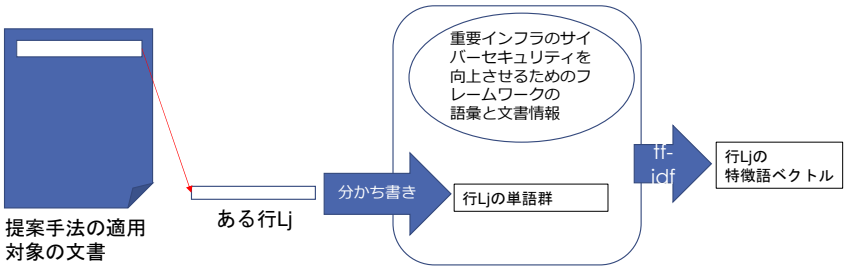


図 6　手順：提案手法の適用対象の文書のある行の特徴語ベクトルの作成

Figure 6　Schematic diagram of the proposal: Creating feature word vector of a document being applied the proposal

5. カテゴリの特徴語ベクトル $\mathbf{c_i}$ との間のコサイン類似度を計算した後，カテゴリ毎に算出したコサイン類似度の総和を取り，提案手法のあるカテゴリとの類似性を示すスコア $S_i(C_i)$ を計算した（図 7）.

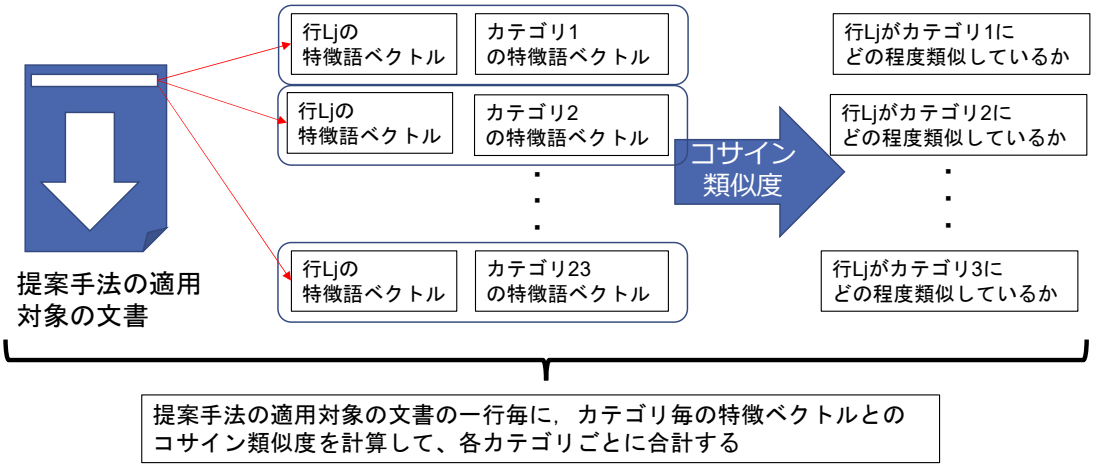


図 7　手順：カテゴリ C_I 毎に文書全体でコサイン類似度の総和を取る

Figure 7　Schematic diagram of the proposal: Take the sum of the cosine similarity across the document for each category for the score of $S_i(C_i)$

4.4. 提案手法の評価

提案手法がどれほど人による分析結果と一致するかを確認するために，情報セキュリティ対策に関する 4 つのガイドラインに対して，質的データ分析を実施した結果を用いて提案手法を適用した結果を評価した．質的データ分析では，各ガイドラインの文章に対してフレームワークコアのカテゴリをコードとしたテンプレートコーディングを行った．コーディングとは文書に繰り返し現れる表現や要素に対してコードや符号と呼ばれる説明を割り当てることで，背後にある体系的な解釈を見出す手法である．テンプレートコーディングでは，事前にコーディングに用いる語群（コード群）を定義してコーディングを行う．この質的データ分析の結果は，人の感覚・判断に基づいて作成されたものであり，この結果と提案手法の結果を比較することで，提案手法により，人の感覚・判断と近い内容分析

を行えることを確認する．

4.4.1. 評価に用いる解析対象の文書

提案手法の評価を行うにあたって，以下 4 つのガイドラインに対して提案手法を適用した（表 8）．

「中小企業の情報セキュリティ対策ガイドライン　第 2.1 版」［64］は，中小企業の IT 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 年に法改正など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．

個人情報保護委員会［65]によって公開されている「中小企業向けはじめてのマイナンバーガイドライン」［66]は，中小企業の担当者が「特定個人情報の適正な取扱いに関するガイドライン」［67]を読む前に概要を学習することを想定して作成された文書であり，今回検証の対象とした文書の中で最もページ数が少ない．

「中小企業 BCP（事業継続計画）ガイド」［68］は，2008 年に中小企業庁により Web サイト上［69]に発行された中小企業が行うべき事業継続計画について記載した文書である．CSF においても事業継続と災害復旧に対する言及は存在するため，今回解析・評価対象に含めた．

日本ネットワークセキュリティ協会［70]により Web サイト［71］上で公開されている「出社してから退社するまで中小企業の情報セキュリティ対策実践手引き(改訂版)」［72]は，中小企業で一般的な業務に潜む情報セキュリティ上のリスクを洗い出し，評価，対策することを支援するための文書である．評価に用いた文書の中で最もページ数が多いが，第 2 部（p.20 以降）については，1 ページにつき 1 項目分の説明で統一されている．

表 8　解析・評価対象とした文書一覧

Table 8　Documents used in test and analysis.

ID	文書名	項目	ページ数
1	中小企業の情報セキュリティ対策ガイドライン　第 2.1 版	リスクアセスメントやポリシー策定などセキュリティ対策の導入についての文書	54
2	中小企業向けはじめてのマイナンバーガイドライン	マイナンバーに関する関する法令や運用についての文書	8
3	中小企業 BCP（事業継続計画）ガイド	災害時の事業継続計画についての文書	43
4	出社してから退社するまで通称企業の情報セキュリティ対策実践手引き(改訂版)	一般的な業務に潜むセキュリティ上のリスクを洗い出し，評価対策することを支援する文書	110

4.4.2. 質的コーディングによる評価用のデータの作成

提案手法の精度を測定するためには，「解析対象の文書の内容を人がどのように理解しているか」を定量的に表すことが必要とされる．そこで本研究では，質的コーディングの方法を用いて文書の内容を人の手で分析・定量化することで，提案手法の評価に用いるデ

ータとした．

質的コーディングとは，質的データ解析の方法の一つで，文書に表れる表現に対してコード（符号）を割り当てることで，文書の内容について整理を行う手法である．事前にコーディングに用いる語群（コード群）を定義するテンプレートコーディングと，繰り返し文書を読みながら都度コードを作成していくオープンコーディングに大別される．

提案手法の評価を行うには，提案手法と比較可能な形式で文書の質的解析を行う必要がある．そこで，CSF のフレームワークコアのサブカテゴリをコード群として，解析対象にした 4 つの文書に対してテンプレートコーディングを実施した．この結果を提案手法の結果と比較することで，提案手法の評価が可能になる．

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) 複数のサブカテゴリ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) コード群に適切なコードが存在しないと思われる場合には，その文に対してコードの割り振りは実施しない．

こととした

例えば，「中小企業の情報セキュリティ対策ガイドライン」の中にある「パソコンにはウイルス対策ソフトを入れてウイルス定義ファイルを自動更新するなどのように，パソコンをウイルスから守るための対策を行っていますか？」という文には「悪質なコードを検出できる」というコード（符号）を割り振っている．この例では，文中に「悪質なコード」などの単語は表れていないが，「ウイルス」が「悪質なコード」を指していると読み取れ，その検出技術の導入を促しているため，このコードが適切であると判断した．

また，本研究での提案手法の解析結果を見ることでコーディング結果に影響が出ないように，各解析対象の文書に対して提案手法を適用する前に，質的コーディングを実施し，この結果に対し，セキュリティガイドラインに詳しい協力者に依頼しレビューを実施した．全体の約 2 割のセンテンスで質問とフィードバックがなされたが，CSF のフレームワークコアの定義について説明することで解消された． 指摘されたカテゴリとしては，「PR.IP 情報を保護するためのプロセス及び手順に関するもの」が特に多かった．これは，このカテゴリが多様な内容を含んでおり，他の機能との関連性が高いためであると考えられる．実際に PR.IP のカテゴリに含まれるサブカテゴリは 12 個あり，各カテゴリに含まれるサブカテゴリ数の平均 4.5 個に対して 3 倍程度広い範囲をカバーしていると考えられる．

各文書に対してどのようなコードが割り当てられたかを 表 9 に記載をした．サブカテゴリについては識別子で記載している．

定量評価を実施するため，コードが割り当てらてられた文の数について，カテゴリごとに和をとり，質的コーディングによる記述数を表すスコア SQ_i (C_i) とした．

表 9　テンプレートコーディングの実施結果

Table 9　Results of template coding with sub-categories of Cybersecurity Framework

機能	カテゴリ	サブカテゴリ	文書 ID			
			1	2	3	4
ID	AM	1	3	0	4	8
		2	5	0	0	8
		3	3	0	0	1
		4	1	0	1	6
		5	16	0	10	2
		6	10	4	3	6
	BE	1	5	0	4	1
		2	1	0	2	0
		3	1	0	3	0
		4	1	0	5	0
		5	0	0	3	0
	GV	1	18	5	4	6
		2	13	4	5	6
		3	20	4	0	1
		4	1	0	0	0
	RA	1	3	1	0	3
		2	8	0	0	2
		3	0	0	0	1
		4	14	0	10	3
		5	6	0	2	4
		6	10	0	5	4
	RM	1	0	0	0	3
		2	3	0	2	5
		3	2	0	4	4
	SC	1	18	0	8	9
		2	1	1	0	0
		3	3	0	0	7
		4	4	0	0	0
		5	0	2	3	0
PR	AC	1	4	3	0	13
		2	2	2	1	12
		3	0	0	0	12

機能	カテゴリ	サブカテゴリ	文書 ID			
			1	2	3	4
DE	AE	1	0	0	0	0
		2	0	0	0	0
		3	0	0	0	1
		4	0	0	0	0
		5	0	0	0	0
	CM	1	0	0	0	8
		2	1	0	0	10
		3	0	1	0	9
		4	6	1	0	10
		5	0	0	0	3
		6	0	0	0	0
		7	0	0	0	4
		8	0	0	0	1
	DP	1	0	0	0	0
		2	0	0	0	1
		3	0	0	0	1
		4	0	0	0	1
		5	0	0	0	2
RS	RP	1	3	0	0	4
	CO	1	4	0	7	2
		2	2	0	2	1
		3	3	0	0	0
		4	5	0	0	0
		5	3	0	0	0
	AN	1	0	0	0	0
		2	1	0	0	0
		3	0	0	0	0
		4	0	0	0	0
		5	1	0	0	0
	MI	1	1	0	0	0
		2	1	0	0	0
		3	0	0	0	0

		4	2	1	0	5
		5	0	0	0	3
		6	0	0	0	2
		7	0	0	0	4
	AT	**1**	15	1	4	9
		2	6	7	2	1
		3	2	0	3	0
		4	13	0	5	0
		5	3	0	0	0
	DS	**1**	1	1	1	6
		2	0	1	0	4
		3	2	2	0	1
		4	0	0	2	5
		5	7	4	0	27
		6	0	0	0	2
		7	0	0	0	1
		8	0	0	0	1
	IP	**1**	0	0	0	0
		2	0	0	0	0
		3	0	0	0	8
		4	2	0	6	12
		5	1	0	1	1
		6	2	3	0	4
		7	23	0	0	0
		8	1	0	0	0
		9	1	0	6	3
		10	0	0	2	1
		11	3	1	0	3
		12	29	1	0	9
	MA	**1**	0	0	0	0
		2	0	0	0	0
	PT	**1**	1	0	0	2
		2	0	0	0	4
		3	0	0	0	0
		4	1	0	0	6
		5	0	0	0	3

	IM	**1**	4	0	0	1
		2	6	0	0	4
RC	**RP**	**1**	2	0	13	3
	IM	**1**	4	0	2	1
		2	5	0	7	4
	CO	**1**	0	0	3	0
		2	0	0	2	0
		3	0	0	2	2

4.4.3. 提案手法と質的コーディングの結果

提案手法のスコア $S_i(C_i)$ を，カラーコード表示（緑：低⇔赤：高）とともに表 3「各文書に対する提案手法と質的コーディングの実施結果」の a）から d）の「提案手法による解析」の「スコア」に記載した．また，フレームワークコアの機能ごとにスコアの平均値を

計算し「機能ごとの平均値」として記載している．質的コーディングによるスコア SQ_i (C_i)についても，表 10 の「質的コーディング」の「スコア」に記載をし，「機能ごとの平均値」についても同様に計算して記載した．

「提案手法による解析」の「スコア」や「機能ごとの平均値」に，それぞれの文書の特徴が見て取れる．例えば，表 10 a）の「中小企業の情報セキュリティ対策ガイドライン第 2.1 版」は，Identify（特定）と Protection（防御）の機能に関連したカテゴリのスコアが高く，リスクアセスメントやポリシーの作成などの対策の準備段階に重点が置かれていることが予測される．実際，この文書では，リスクアセスメントとセキュリティポリシー作成を促している．一方で，表 10 c）の「中小企業 BCP（事業継続計画）ガイド」では，Identify（特定）の「資産管理」のカテゴリや Recovery（復旧）の機能に含まれるカテゴリのスコアが高く，資産の洗い出しや，復旧計画などについて記載されていることが予測される．実際，この文書には名前の通り，災害復旧計画を含む BCP（事業継続計画）の要素が多く記述されている．

本研究では，提案手法の提示内容の妥当性の評価を行うために事前にテンプレートコーデ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．

$S_i(C_i)$，SQ_i (C_i)について，下式で，正規化を行った．正規化後のスコアは表 10 の「正規化スコア」に記載をした．

$$N(X) = \frac{X - x_{min}}{|x_{max} - x_{min}|} \cdots\cdots \text{式 7}$$

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．表 3 上で，正規後のスコアの差分の絶対値 $|N(S_i) - N(SQ_i)|$ を正規化後のスコアの差として表記する．この値の平均は 0.27，中央値は 0.21，第三四分位は 0.39 であり，これが 0.5 を超えるものについては，特に正解から大きく外れていると考えられるため，次の議論と制限の 4.5 章で検討を行う（表 10 中，太字と二重下線で強調）．

提案手法のスコアを要素として持つベクトルを $\mathbf{M}$ とし，質的コーディングによるスコアを要素として持つベクトルを $\mathbf{Q}$ とする．

$$\vec{M} = (S_1(C_1),\ \ldots,\ S_{23}(C_{23}))\,,\ \vec{Q} = (SQ_1(C_1),\ \ldots,\ SQ_{23}(C_{23})) \cdots\cdots \text{式 8}$$

表 10　各文書に対する提案手法と質的コーディングの実施結果

Table 10 Results of the proposed procedure and template coding for each document with color scale

a)　中小企業の情報セキュリティ対策ガイドライン第 2.1 版

	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	スコア	正規化スコア	カテゴリ	正規化後のスコアの差	スコア	正規化スコア	機能ごとの平均値
Identify（特定）	63.4631	60.58109	0.6017	資産管理	0.0112	38	0.6129	28.3333
		62.66334	0.6294	ビジネス環境	0.5003	8	0.1290	
		64.10374	0.6485	ガバナンス	0.1902	52	0.8387	
		67.09194	0.6882	リスクアセスメント	0.0269	41	0.6613	
		63.7634	0.6440	リスク管理戦略	0.5633	5	0.0806	
		62.57506	0.6282	サプライチェーンリスク	0.2088	26	0.4194	
Protection（防御）	70.2238	43.9369	0.3806	アクセス制御	0.2516	8	0.1290	20.1667
		73.78872	0.7771	意識向上およびトレーニング	0.1481	39	0.6290	
		90.56535	1.0000	データセキュリティ	0.8387	10	0.1613	
		89.1779	0.9816	情報を保護するためのプロセスおよび手順	0.0184	62	1.0000	
		59.64659	0.5893	保守	0.5893	0	0.0000	
		64.22752	0.6501	保護技術	0.6179	2	0.0323	
Detection（検知）	33.1768	26.96574	0.1552	異常とイベント	0.1552	0	0.0000	2.3333
		49.67934	0.4569	セキュリティの継続的なモニタリング	0.3440	7	0.1129	
		22.88544	0.1010	検知プロセス	0.1010	0	0.0000	
Response（対応）	36.2112	40.64815	0.3369	分析	0.3047	2	0.0323	6.8000
		44.90455	0.3935	コミュニケーション	0.1193	17	0.2742	
		26.56475	0.1499	改善	0.0114	10	0.1613	
		40.69605	0.3376	低減	0.3053	2	0.0323	
		28.24251	0.1721	対応計画	0.1238	3	0.0484	
Recovery（復旧）	20.9207	15.28354	0.0000	改善	0.1452	9	0.1452	3.6667
		29.58491	0.1900	コミュニケーション	0.1900	0	0.0000	
		17.89355	0.0347	復旧計画	0.0024	2	0.0323	

b) 中小企業むけ初めてのマイナンバーガイドライン

	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	スコア	正規化スコア	カテゴリ	正規化後のスコアの差	スコア	正規化スコア	機能ごとの平均値
Identify（特定）	13.1319	14.50888	0.9173	資産管理	0.6096	4	0.3077	3.5000
		13.59565	0.8527	ビジネス環境	0.8527	0	0.0000	
		13.20291	0.8248	ガバナンス	0.1752	13	1.0000	
		15.67625	1.0000	リスクアセスメント	0.9231	1	0.0769	
		10.78312	0.6535	リスク管理戦略	0.6535	0	0.0000	
		11.02435	0.6706	サプライチェーンリスク	0.4398	3	0.2308	
Protection（防御）	7.7915	7.611298	0.4288	アクセス制御	0.0327	6	0.4615	4.5000
		8.446021	0.4880	意識向上およびトレーニング	0.1274	8	0.6154	
		8.609577	0.4995	データセキュリティ	0.1158	8	0.6154	
		8.5153	0.4929	情報を保護するためのプロセスおよび手順	0.1083	5	0.3846	
		6.209951	0.3296	保守	0.3296	0	0.0000	
		7.357107	0.4108	保護技術	0.4108	0	0.0000	
Detection（検知）	2.8879	2.521282	0.0684	異常とイベント	0.0684	0	0.0000	0.6667
		3.968102	0.1708	セキュリティの継続的なモニタリング	0.0170	2	0.1538	
		2.174301	0.0438	検知プロセス	0.0438	0	0.0000	
Response（対応）	5.1365	4.617821	0.2169	分析	0.2169	0	0.0000	0.0000
		9.342579	0.5515	コミュニケーション	0.5515	0	0.0000	
		3.164115	0.1139	改善	0.1139	0	0.0000	
		5.386191	0.2713	低減	0.2713	0	0.0000	
		3.171816	0.1144	対応計画	0.1144	0	0.0000	
Recovery（復旧）	3.2189	1.555793	0.0000	改善	0.0000	0	0.0000	0.0000
		6.522643	0.3517	コミュニケーション	0.3517	0	0.0000	
		1.578266	0.0016	復旧計画	0.0016	0	0.0000	

c) 中小企業 BCP（事業継続計画）ガイド

	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	スコア	正規化スコア	カテゴリ	正規化後のスコアの差	スコア	正規化スコア	機能ごとの平均値
Identify（特定）	35.8055	49.7153	1.0000	資産管理	0.0000	18	1.0000	13
		35.8844	0.6664	ビジネス環境	0.2781	17	0.9444	
		29.1137	0.5030	ガバナンス	0.0030	9	0.5000	
		36.8698	0.6901	リスクアセスメント	0.2543	17	0.9444	
		32.1633	0.5766	リスク管理戦略	0.2433	6	0.3333	
		31.0864	0.5506	サプライチェーンリスク	0.0605	11	0.6111	
Protection（防御）	19.8708	12.3003	0.0974	アクセス制御	0.0419	1	0.0556	5.5
		17.769	0.2294	意識向上およびトレーニング	0.5484	14	0.7778	
		20.7976	0.3024	データセキュリティ	0.1357	3	0.1667	
		28.8285	0.4961	情報を保護するためのプロセスおよび手順	0.3372	15	0.8333	
		17.3627	0.2196	保守	0.2196	0	0.0000	
		22.1665	0.3354	保護技術	0.3354	0	0.0000	
Detection（検知）	12.3075	12.6695	0.1063	異常とイベント	0.1063	0	0.0000	0
		15.9913	0.1865	セキュリティの継続的なモニタリング	0.1865	0	0.0000	
		8.26154	0.0000	検知プロセス	0.0000	0	0.0000	
Response（対応）	23.5848	26.3673	0.4368	分析	0.4368	0	0.0000	1.8
		35.2885	0.6520	コミュニケーション	0.1520	9	0.5000	
		15.8842	0.1839	改善	0.1839	0	0.0000	
		20.3853	0.2925	低減	0.2925	0	0.0000	
		19.9985	0.2831	対応計画	0.2831	0	0.0000	
Recovery（復旧）	47.5215	45.2986	0.8935	改善	0.3935	9	0.5000	9.666667
		48.3188	0.9663	コミュニケーション	0.5774	7	0.3889	
		48.9473	0.9815	復旧計画	0.2593	13	0.7222	

d) 出社してから退社するまで中小企業の情報セキュリティ対策実践手引き(改訂版)

	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	スコア	正規化スコア	カテゴリ	正規化後のスコアの差	スコア	正規化スコア	機能ごとの平均値
Identify（特定）	208.2439	232.312	0.8955	資産管理	0.2876	31	0.6078	15.0000
		211.0702	0.7960	ビジネス環境	0.7764	1	0.0196	
		231.5448	0.8919	ガバナンス	0.6370	13	0.2549	
		201.8335	0.7527	リスクアセスメント	0.4193	17	0.3333	
		188.1098	0.6884	リスク管理戦略	0.4531	12	0.2353	
		184.593	0.6719	サプライチェーンリスク	0.3582	16	0.3137	
Protection（防御）	194.1280	203.8884	0.7623	アクセス制御	0.2377	51	1.0000	27.3333
		157.5106	0.5450	意識向上およびトレーニング	0.3489	10	0.1961	
		254.6157	1.0000	データセキュリティ	0.0784	47	0.9216	
		209.3266	0.7878	情報を保護するためのプロセスおよび手順	0.0161	41	0.8039	
		146.5039	0.4934	保守	0.4934	0	0.0000	
		192.9226	0.7109	保護技術	0.4168	15	0.2941	
Detection（検知）	76.9775	72.72001	0.1477	異常とイベント	0.1281	1	0.0196	17.0000
		114.1258	0.3417	セキュリティの継続的なモニタリング	0.5406	45	0.8824	
		44.08675	0.0135	検知プロセス	0.0845	5	0.0980	
Response（対応）	76.7417	91.13232	0.2340	分析	0.1555	4	0.0784	2.4000
		102.5866	0.2876	コミュニケーション	0.2288	3	0.0588	
		50.26428	0.0425	改善	0.0425	0	0.0000	
		82.27769	0.1925	低減	0.1925	0	0.0000	
		57.44748	0.0761	対応計画	0.0219	5	0.0980	
Recovery（復旧）	64.1140	41.19798	0.0000	改善	0.0588	3	0.0588	4.0000
		97.00023	0.2615	コミュニケーション	0.1634	5	0.0980	
		54.14372	0.0607	復旧計画	0.0214	2	0.0392	

このベクトル $\mathbf{M}$, $\mathbf{Q}$ は計測手法が異なるため，直接の比較は難しい．そこで類似性にのみ注目し，コサイン類似度とピアソン積率相関係数を各文書で計算した．その結果を表 11 の「カテゴリ」として示す．また，機能ごとの平均値についても同様の計算したものを表 11 の「機能」として示す．機能で見た場合コサイン類似度のへ平均は 0.907，カテゴリで見た場合の平均は 0.761 とであった．また，相関係数も機能では強い正の相関を示す数値であり，カテゴリでも正の相関を示す数値であった．したがって，提案手法による結果と

質的コーディングによる結果には類似性が見られるため，人の感覚にそった妥当性のあるものであると考えられる．

表 11　提案手法の結果と質的 コーディングの結果の間のコサイン類似度とピアソン積率相関係数

Table 11　Cosine Similarity and Pearson product-moment correlation coefficient between results of the proposed procedure and template coding

文書名	コサイン類似度		ピアソン積率相関	
	カテゴリ(23)	機能(5)	カテゴリ(23)	機能(5)
中小企業の情報セキュリティ対策ガイドライン　第 2.1 版	0.768	0.932	0.605	0.902
中小企業向け初めてのマイナンバーガイドライン	0.637	0.866	0.424	0.761
中小企業 BCP（事業継続計画）ガイド	0.846	0.918	0.704	0.810
出社してから退社するまで中小企業の情報セキュリティ対策実践手引き(改訂版)	0.792	0.912	0.607	0.699

4.5.　議論と制限

評価結果をもとに本研究で行った提案の制限と改善方法について議論を行う．

4.5.1.　記述内容の正確性と十分性についての制限

本研究の提案手法では，あるカテゴリもしくは機能についての記述があるかないか（多いか少ないか）について表現することは可能だが，記述内容の正確性や十分性を表現することはできない．

これは，本質的にはテキストマイニングを行ったことによる制限だが，CSF のフレームワークコアでは，サブカテゴリの項目まで用いて詳細まで判定することで，問題の緩和を行える可能性がある．

ただし，本研究では，サブカテゴリでの特徴語ベクトルの作成の検討は行っていない．これは，特徴語ベクトル作成には，文書量が不十分であると思われたためである．そのため，サブカテゴリでの解析を実施するためには，「フレームワークコア」の「参考情報」を用いるなどして，文書量を増やすなどの改善策を検討する必要があると考える．「参考情報」は，各サブカテゴリについて期待される成果を達成するための，既存の標準・ガイドライン・ベストプラクティスについてまとめたものである．CSF では，項目番号やページのみが表記され，実際の内容については対象の文書を確認する必要がある．そのため，この方法を取る場合には，CSF の枠組みからさらに，他の標準・ガイドライン・ベストプラクティスなどの各文書への拡張が必要になる．この場合，各文書のどの部分を採用するかなどそれぞれの文書に対して改めて検討を行う必要が出てくると考えられる．

4.5.2. 誤差が発生したケースについての検討

この節では，正規化したスコアの差分が 0.5 を超えたカテゴリ，つまり，表 10 中で太字二重下線を用いてマークした項目について検討を行う．

4.5.3. 同一機能内のカテゴリの特徴語が類似しているために誤差が発生したケース

太字二重下線でマークした項目のうち，「中小企業 BCP（事業継続計画）ガイド」の「意識向上とトレーニング」のカテゴリと，「出社してから退社するまで中小企業の情報セキュリティ対策実践手引き (改訂版)」の「セキュリティの継続的なモニタリング」のカテゴリ以外のものは，提案手法のスコア $N(S_i)$ が，質的コーディングのスコア $N(SQ_i)$ を大きく超えていることで差が発生している．

この原因を検討するため，カテゴリの上位の特徴語について実際に確認した．表 7 によると各機能で見た場合には，上位の特徴語が類似していることが確認できる．例えば，Identify （特定）の機能に属するカテゴリは全て，「リスク」や「ビジネス」といった単語を上位の特徴として持っている．つまり，本研究の提案手法では，同一の機能に属するカテゴリ同士ではスコアの差が発生しにくいという制限が存在すると考えられる．

これは，カテゴリ C_i について記述された部分を抽出する際に，C_i が属する機能についての記述も対象に含めた影響であると考えられる．そのため，カテゴリに関連した記述の抽出をする際に機能についての文を含めないように調整することで改善される可能性がある．

4.5.4. 特徴語の可能性がある単語が特徴語ベクトルに含まれていないために誤差が発生したケース

「中小企業 BCP（事業継続計画）ガイド」の「意識向上とトレーニング」のカテゴリと，「出社してから退社するまで中小企業の情報セキュリティ対策実践手引き（改訂版)」の「セキュリティの継続的なモニタリング」のカテゴリでは，質的コーディングのスコア $N(SQ_i)$が提案手法のスコア $N(S_i)$を大きく超えていることで差が発生している．

この差の原因を推測するため，「出社してから退社するまで中小企業の情報セキュリティ対策実践手引き（改訂版)」の「セキュリティの継続的なモニタリング」のカテゴリ内のサブカテゴリの質的コーディングの結果を確認した．このカテゴリ内で最も多くコードとして割り振られたのは，「発生する可能性〜（中略）〜物理環境をモニタリングしている」のサブカテゴリと「悪質なコードを検出できる」の 2 つであった．どちらも割り振られた文の数は 10 個である．

このうち「悪質なコードを検出できる」がコードとして割り振られた文の 1 つに「コンピューター(PC，サーバー)をアンチウイルスソフトウェアで定期的(1 週間に 1 度 程度)にスキャンする」という文がある．この文の特徴語ベクトル L_j を計算したところ，「スキャン」は上位の特徴語としてあらわれたが，「アンチウイルス」ないし「ウイルス」は特徴語として出現しなかった．同様に残りの 9 個の文についても検証したところ，「ワーム」，

「スパイウェア」,「トロイの木馬」,「ボッド」などの用語も特徴語として抽出されなかった．以上より，質的コーディングの際，コーディングの手がかりとなるが，提案手法の特徴語ベクトルに含まれていない単語があり，これがスコア差を生んでいると考えられる．

また，実験結果には明示的に表れていないが，他のカテゴリにおいても実際にコーディングを実施した結果と特徴語を比較してみると，特徴語と思われるのにも関わらず特徴語ベクトル中には出現していない単語がある事例が確認された．

例えば,「中小企業の情報セキュリティ対策ガイドライン　第 2.1 版」のコーディングで「ビジネス環境」のカテゴリに属するコードが,「業務上の関係者（顧客，取引先，委託先，代理店，利用者，株主など）からの信頼を高めるには，…(中略)…，整理しておくことが重要です.」という文に割り振られている．この文に対して同様に特徴語ベクトル L_j を計算すると,「関係」,「業務」,「顧客」,「経営」,「利用者」などの単語については，上位の特徴語としてあらわれていたが,「委託」の単語が特徴語ベクトルに存在していないことが確認できた．

これは，特徴語ベクトルの作成に利用した CSF の翻訳版である「重要インフラのサイバーセキュリティを改善するためのフレームワーク」の文書中に該当の単語自体が表れていなかったことが原因である．そのため，この問題については特徴語ベクトル作成時に利用する文書数を増やすか，適切な類義語や関連語を追加することで改善できると思われる．文書数を増やす方法としては，4.5.1 項で検討した「参考情報」を用いる方法があるが，各参考情報のどの部分を採用するかなどそれぞれの文書に対して改めて検討を行う必要がある．類義語や関連語を用いる場合，情報セキュリティ分野の専門用語を適切に扱うことができる辞書を用いる必要がある．

4.6. 本部の結論

提案手法の結果と質的データ分析の結果を，コサイン類似度で比較したところ，フレームワークコアの機能で見た場合平均 0.907，カテゴリで見た場合平均 0.761 となった．また，ピアソン積率相関係数で計算した場合の平均でも機能では 0.793 で強い正の相関を示し，カテゴリでも 0.585 で正の相関を示した（表 11）．

また，提案手法の有利性を示す目的で，4 つのガイドラインに対して提案手法と k 平均法によるクラスタリングとトピック分析を行った結果との比較を行った．クラスタリングとトピック分析では，文書の内容について分類し内容の類推を行うことは可能であったが，セキュリティとは関係のない分類が発生したり，その分類の内容に重複や偏りが生じたりするため，体系的な分類に基づいた内容の提示が難しいことを確認した．

以上より，CSF に基づいて文書の内容を体系的に表現する手法について提案を行うことができたと考える．

また， 本研究における教材の改善をするために，CSF のフレームワークコアと AH の類似性に着目し，フレームワークコアに基づいて教材の情報を提示する．そのため，この提

案手法により，情報セキュリティに関連する文書や文章の内容とフレームワークコアとの関連性を顕わにすることができることは，本研究における教材の改善に必要な要素である．

５．実験のための教材の作成と予備実験

本研究では，第４部で主に目的とした体系的に学習できるように文書内容の分析し表示する方法の提案することの他，教材のインタフェース改善を行い，それが学習者のメンタルモデルにどのように影響を及ぼし，また，メンタルモデルが学習効果とどのように関係するのかを明らかにすることも目的としている．そのためには，インタフェースの異なる教材を用いた実験が必要となる．そこで，5.1 章では，教材のインタフェースの影響について確認するための実験に用いる教材の改善を第 4 部の提案手法を用いて行い，5.2 章では，その教材を用いて予備実験を行う．

5.1. Cybersecurity Framework に基づいた教材の改良

この章では，教材のインタフェースの改善を実施する．この章の内容は 2020 年の HCII でポスター発表を実施した「Improving the training material of the information security based on Cybersecurity」 [73]に基づいているが，「節・項」に対する提案手法の結果の評価や対応付けの方法について，より詳しく記載を行った．これは，1.3 章の研究の流れの説明では，「3) 提案手法を利用して教材の改良する」に該当する．

5.1.1. 概要

この章では，第４部で文書全体に適用していた手法を，文書内の「章」や「節・項」に援用することで，「中小企業の情報セキュリティ対策ガイドライン　第 3 版」 [74]の章や節・項と，Cybersecurity Framework (CSF)のフレームワークコアの関係性を明らかにして，その結果の妥当性の検討を行った．また，その結果を用いて教材の作成を行った．

具体的には，「中小企業の情報セキュリティ対策ガイドライン　第 3 版」の「章」と「節・項」に対して，第４部で提案した手法を適用して，その文がフレームワークコアのどの機能と強く結びついているのかを分析した．また，第４部と同様に質的データ分析による結果を「章」や「節・項」ごとに作成してピアソン積率相関係数を用いて相関性を比較した．「章」で見た場合は，質的データ分析の結果と提案手法の結果の相関係数は機能でもカテゴリでも強い相関が確認された．「節・項」で見た場合には，機能では相関が，カテゴリでは弱い相関が確認された．

この評価結果を参考に，提案手法の適用結果を用いて「中小企業の情報セキュリティ対策ガイドライン 第３版」とフレームワークコアのカテゴリと機能との対応付けを行い，その情報に基づいて，インタフェースを変更した教材の作成を行った．3.3 章で説明したように CSF のフレームワークコアは AH と類似した構造をもっているため，このインタフェースを用いることで AH に基づいた学習を促すことができると考えられる．

5.1.2. 目的

3.3 章で検討した通り，CSF のフレームワークコアと AH には類似性がある．そこで，CSF のフレームワークコアを AH として，既存の教材についてユーザーインタフェースの改善を行う．AH に基づくことで学習者に包括的かつ体系的なメンタルモデルを浸透させ，学習効率を向上させることができると考えている．

この際，1.1.6 節でも確認した通り情報セキュリティに関するガイドラインは数多く出版されていることから，これらのガイドラインやドキュメントに対して共通して用いることのできるアプローチを目指す．

5.1.3. 教材の改善手法

今回改善する教材では，CSF のフレームワークコアを AH として想定して，3.1 章で述べた EID のアプローチに基づいて既存の教材の内容を変えず構成やユーザーインタフェースを変えることを目指している．そのため，改善の対象とする文書とフレームワークコアとの対応関係を明確にする必要がある．

5.1.3.1. 利用した文書について

ここではユーザーインタフェース改善のために AH として用いた CSF の翻訳である重要インフラのサイバーセキュリティを改善するためのフレームワーク」と，教材として改善の対象とする「中小企業の情報セキュリティ対策ガイドライン　第 3 版」について述べる．本実験で用いる教材は，これら二つの文書を用いて作成されている．

(1) 枠組みとなる文書：「重要インフラのサイバーセキュリティを改善するためのフレームワーク」

第 4 部の提案手法と同じく CSF の翻訳版である「重要インフラのサイバーセキュリティを改善するためのフレームワーク」を文書内容の解析の枠組みとして用いた．3.2 章で説明を行った通り，CSF とは，NIST が重要インフラにおけるセキュリティ対策をまとめるために作成したフレームワークで，サイバーセキュリティ領域の規格，ガイドライン，ベストプラクティスを集約し，さまざまなセキュリティ対策を体系的，構造的に全体像を把握できるようになっている．第 4 部での分析と同じく，IPA（日本）が発行した日本語に翻訳されたバージョンである「重要インフラのサイバーセキュリティを改善するためのフレームワーク　1.1 版」を使用した．

(2) 改善対象の文書：「中小企業の情報セキュリティ対策ガイドライン　第 3 版」

本研究において改善の対象とする教材として，「中小企業の情報セキュリティ対策ガイドライン　第 3 版」を用いた．「中小企業の情報セキュリティ対策ガイドライン　第 3 版」は，2021 年 11 月現在 IPA が Web サイト [75]上で公開している「中小企業の情報セキュ

リティ対策ガイドライン」の最新の版で，2019 年 3 月に 2.1 版を更新する形で公開された．2.1 版と同じく日本の中小企業の情報セキュリティ担当者がセキュリティポリシーを作成し，利用可能なセキュリティ対策を決定することを支援するために作成されている．2.1 版と同じく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が，2.1 版と構成が変更された部分が存在する．2.1 版では管理実践編において，取り組みやすい「情報セキュリティ 5 か条」について述べた後，付録のシートに基づいた自社診断の実施方法について説明し，すぐにリスク分析に基づいたセキュリティポリシーの策定の説明を始めるが，3 版では，取り組みを「できるところから始める」,「組織的な取り組みを開始する」,「本格的に取り組む」,「より強固にするための方策」という形で，3.4.2 節で説明した CIS Control 8 の実装グループのような段階的な実践を意識した構成になっている．また，リスク管理をメインに据えた 2.1 版とは異なり，紹介程度ではあるが具体的な対策の内容も多く記載されている．

「中小企業の情報セキュリティ対策ガイドライン第 3 版」は現在も更新されている新しいガイドラインであり，主に情報セキュリティに課題を抱えていると考えられる中小企業向けにかかれたものである．そのため，今回のインタフェース改善の実験の事例として採用したが，この改善アプローチそのものは「中小企業の情報セキュリティ対策ガイドライン　第 3 版」以外にも適用可能であると考えられる．

5.1.3.2. 章や節・項とフレームワークコアとの関係性の分析手法の提案

CSF のフレームワークコアを AH として既存の教材についてユーザーインタフェースの改善を行うためには，フレームワークコアと既存の教材の内容の対応付けが必要になる．

そこで，第 4 部で検討したフレームワークコアに基づいて文書の内容を CSF のカテゴリを要素とするベクトル的に表現するための手順を，文書そのものではなく，文書内の「章」や「節・項」ごとに適用し，内容の評価と対応関係の明確化を行った(図 10)．

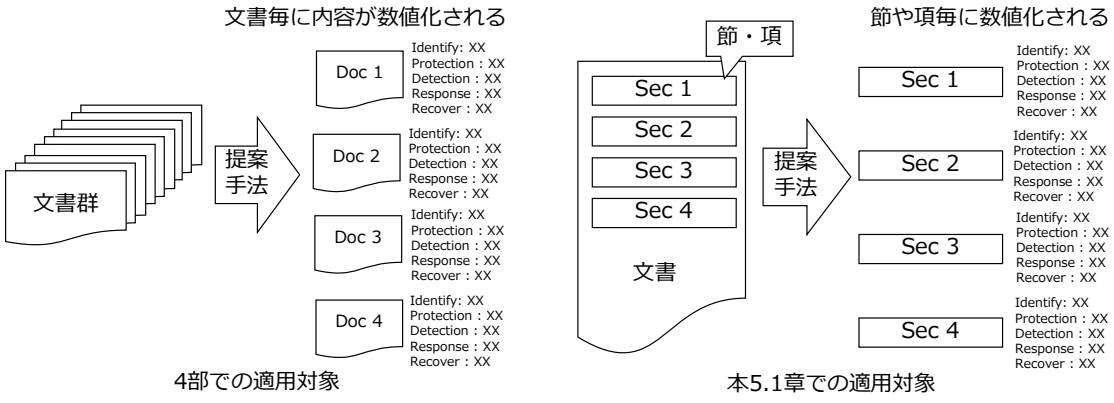


図 8　第 4 部と 5.1 章での提案手法の適用対象の違い

Figure 8　Difference of the target between Capter4 and Section 5.1

「章」については，目次に定義されているものをそのまま採用した．ただし，ガイドラインの利用方法の解説についての項目である「本ガイドラインの対象」,「本ガイドラインの全体構成」,「本ガイドラインの活用方法」については，分析対象から除外した．これはこれらの項目が情報セキュリティ対策と関係のない文書についての情報を提供しているのが表題から明らかなためである．「節・項」については，本文中の番号や項目名で分割されている内容で分割を行っている．

解析対象の文書中のある「章」か「節・項」に存在する行 L_j が，フレームワークコアのあるカテゴリ 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，CSF の記述を基に作成したカテゴリ C_i の特徴語ベクトル $\mathbf{c_i}$ と，ある行 L_j に対して CSF 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．

「章」か「節・項」の中にカテゴリ C_i に関連する記述がどの程度あるかを表すスコア $S_i(C_i$;章，節・項）は，$\mathbf{l_j}$ と $\mathbf{c_i}$ のコサイン類似度の総和となるので，下式で評価することができると考えられる．

$$S_i\left(C_i\text{: 章，節・項}\right) = \sum_j \frac{\vec{l}_j \cdot \vec{c}_i}{|\vec{l}_j||\vec{c}_i|} \cdots\cdots\text{式 9}$$

具体的には，下記の手順でスコア $S_i(C_i$;章, 節・項）の計算を行った．基本的には，4 部に記載されている提案手法と同じだが,「章」や「節・項」ごとに総和を取る．

1．CSF の翻訳版である「重要インフラのサイバーセキュリティを改善するためのフレームワーク」内で各カテゴリ C_i について記述されている部分を実際に読んで確認し，カテゴリごとに抽出した．また，カテゴリ C_i が属している機能に関する記述も同様に実際に読み抽出し，あるカテゴリ C_i の文書の一部として取り扱った（図 5 の 1.を参照).
2．抽出した各カテゴリと機能の文書集合に対して，Mecab を用いて標準のシステム辞書で分かち書きと形態素解析を実施して名詞を取り出し，名詞だけの集合に変換した（図 5 の 2.を参照).
3．名詞句による文書集合に対して，それぞれのカテゴリ C_i 毎に，TF-IDF による特徴語ベクトル $\mathbf{c_i}$ を作成した（図 5 の 3.を参照).
4．適用対象の「章」か「節・項」から 1 行ごと文字列を抜き出して,「重要インフラのサイバーセキュリティを改善するためのフレームワーク」の語彙と文書頻度を用いて，特徴語ベクトル $\mathbf{l_j}$ を計算した．
5．カテゴリの特徴語ベクトル $\mathbf{c_i}$ との間のコサイン類似度を計算した後,「章」か「節・項」の範囲でカテゴリ毎に算出したコサイン類似度の総和を取り，提案手法のあるカテゴリとの類似性を示すスコア $S_i(C_i$;章・節) を計算した（図 9).

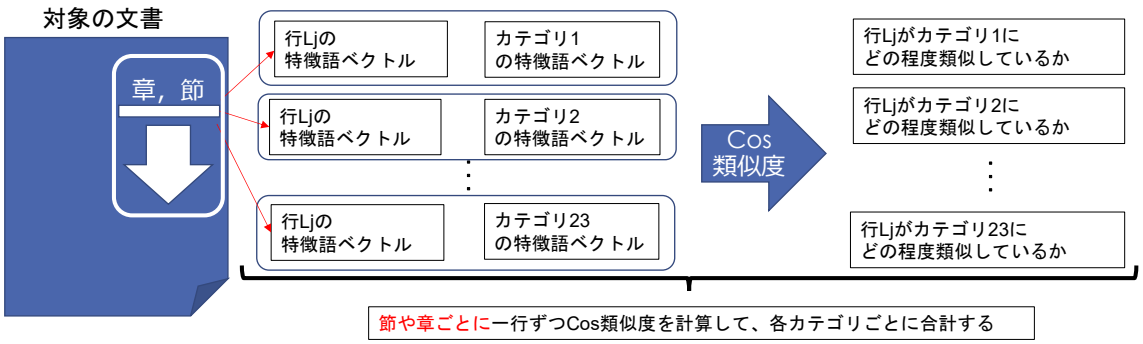


図 9　手順：カテゴリ C_I 毎に「章」や「節・項」でコサイン類似度の総和を取る

Figure 9　Schematic diagram of the proposal: Take the sum of the cosine similarity across the chapter or section for each category for the score of $S_i(C_i)$

5.1.4.　結果とその妥当性の確認

提案手法の結果の妥当性を測るために，人が文書の内容をどのように認識しているかを定量的に評価した結果と比較を行った．第 4 部での「中小企業の情報セキュリティ対策ガイドライン」の解析は第 2.1 版に基づいて実施したため，「中小企業の情報セキュリティ対策ガイドライン　第 3 版」に基づいて，第 4 部と同様に文書単位での分析も再実施し，テンプレートコーディングについても再度実施した．

5.1.4.1. テンプレートコーディングの実施

4.4.2 節と同じく，CSF のフレームワークコアのサブカテゴリをコード群として，「中小企業の情報セキュリティ対策ガイドライン　第 3 版」に対してテンプレートコーディングを実施した．

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) 複数のサブカテゴリ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) コード群に適切なコードが存在しないと思われる場合には，その文に対してコードの割り振りは実施しない．

こととした．

テンプレートコーディングは 2 名で実施され，Cohen's Kappa は，8.1 であった．これは，Krippendorff ら [76]の基準に基づくと「ほぼ一致」しており，Landis と Koch ら [77]の基準に基づいても「明確な結果」がある．

Cohen's Kappa [78]は，質的分析において 2 名の評価者の間でそれぞれ評価を行った結果がどの程度一致しているかを表す指標で，実際の一致率から偶然一致する確率を取り除いて補正を行ったものであり，下式で表現される．

$$\kappa = \frac{p_0 - p_e}{1 - p_e} \quad \cdots\cdots\text{式 10}$$

ここで，p_0 は相対的に観測された一致率を表し，p_e は偶然一致する確率を表す．

5.1.4.2.「章」と「節・項」に対する機能単位での提案手法と質的分析の結果

提案した分析手法を「章」に対して機能単位で適用した結果を表 12 に示す．この提案手法の結果は，文書内の「章」がある CSF のフレームワークコアの機能にどれだけ類似しているかを示していると考えられる．

今回の結果では，識別と防御がすべての「章」で一番高い項目となっており，この 2 つがどの「章」でも主たる内容になっていると考えれられる．また，テンプレートコーディングの結果を，表 13 に示す．こちらも識別と防御がすべての「章」で一番高い項目となっており，この 2 つがどの「章」でも主たる内容になっていると考えれられる．

提案手法を「節・項」に対して機能単位で適用した結果を表 14 に示す．「章」に比べると各文書の長さが短いため，個々の値は小さくなっている．全体の傾向としては識別と防御が高く出ているが，「2.4.1.2　②緊急対応体制の整備」などの項目はその内容に従って，対応と判定されていることが確認できた．同様の対象に対してテンプレートコーディングの結果を，表 15 に示す．テンプレートコーディング結果でも似たような傾向が確認された．

同様に提案手法を「章」と「節・項」に対してカテゴリ単位で適用した場合の提案手法とコーディングの結果については付録 1 に記載する．

表 12　各章に対して機能単位で提案手法を適用した結果

Table 12　Text mining analysis results for chapters with functional view

		識別	防御	検知	対応	復旧
0	経営者の皆様へ	1.140	1.130	0.250	0.339	0.185
1.1	情報セキュリティ対策を怠ることで企業が被る不利益	2.605	2.756	0.689	1.645	0.756
1.2	経営者が負う責任	2.634	3.308	0.462	1.044	0.419
1.3	経営者は何をしなければならないのか？	3.660	3.140	1.003	1.625	0.789
2.1	実践編の進め方	1.268	0.829	0.344	0.308	0.124
2.2	できるところから始める	1.184	1.530	0.521	0.518	0.641
2.3	組織的な取り組みを開始する	7.694	10.026	2.638	5.453	2.288
2.4	本格的に取り組む	10.712	7.576	2.536	7.162	1.857
2.5	より強固にするための方策	34.700	39.219	9.182	15.055	7.560

表 13　各章に対して機能単位でテンプレートコーディングを実施した結果

Table 13　Template coding results for chapters with functional view

ID	表題	識別	防御	検知	対応	復旧
0	経営者の皆様へ	3	3	0	0	0
1.1	情報セキュリティ対策を怠ることで企業が被る不利益	7	9	0	1	2
1.2	経営者が負う責任	6	1	0	0	0
1.3	経営者は何をしなければならないのか？	6	6	0	1	0
2.1	実践編の進め方	1	1	0	0	0
2.2	できるところから始める	1	4	1	0	0
2.3	組織的な取り組みを開始する	5	3	0	0	0
2.4	本格的に取り組む	22	9	0	3	0
2.5	より強固にするための方策	53	27	5	2	0

表 14　各節・項に対して機能単位で提案手法を適用した結果

Table 14　Text mining analysis results for sections with functional view

ID	表題	識別	防御	検知	対応	復旧
0	経営者の皆様へ					
1	経営者編					
1.1	情報セキュリティ対策を怠ることで企業が被る不利益					
1.1.0	序文	0.8976	0.6681	0.1654	0.2287	0.0968
1.1.1	(1) 金銭の損失	0.3005	0.7666	0.1601	0.4126	0.2501
1.1.2	(2) 顧客の喪失	0.6717	0.5691	0.1752	0.2189	0.0672
1.1.3	(3) 業務の喪失	0.4127	0.3382	0.0995	0.4611	0.2929
1.1.4	(4) 従業員への影響	0.3225	0.4141	0.0889	0.3239	0.0487
1.2	経営者が負う責任					
1.2.1	(1) 経営者などに問われる法的責任	0.5608	0.6903	0.0933	0.2622	0.1110
1.2.2	(2) 関係者や会社に対する責任	0.5324	0.5403	0.0957	0.2839	0.1256
1.3	経営者は何をしなければならないのか？					
1.3.1	認識すべき「3 原則」	0.6326	0.5781	0.1213	0.1806	0.1373
1.3.1.1	原則 1　情報セキュリティ対策は経営者のリーダーシップで進める	0.7894	0.6680	0.2441	0.2875	0.1273
1.3.1.2	原則 2　委託先の情報セキュリティ対策まで考慮する	0.8133	0.8222	0.1916	0.3102	0.0698
1.3.1.3	原則 3 関係者との情報セキュリティに関するコミュニケーションはどんな時も怠らない	0.6207	0.4522	0.1748	0.5787	0.2242
1.3.2	実行すべき「重要 7 項目の取り組み」					
1.3.2.0	序文	0.4553	0.5095	0.1125	0.1839	0.1488
1.3.2.1	取組 1　情報セキュリティに関する組織全体の対応方針を決める	0.6723	0.7602	0.2642	0.8141	0.1261
1.3.2.2	取組 2　情報セキュリティ対策のための予算や人材を確保する	0.2855	0.9324	0.2507	0.6558	0.4304

1.3.2.3	取組３　必要と考えられる対策を検討させて実行を指示する	0.8398	0.5968	0.3074	0.5376	0.2246
1.3.2.4	取組４　情報セキュリティ対策に関する適宜の見直しを指示する	0.4368	0.4878	0.1926	0.3290	0.2190
1.3.2.5	取組５　緊急時の対応や復旧のための体制を整備する	0.2416	0.3723	0.0781	1.0674	0.6050
1.3.2.6	取組６　委託や外部サービスの利用の際にはセキュリティに関する責任を明確にする	0.3907	0.6306	0.1662	0.2841	0.1389
1.3.2.7	取組７　情報セキュリティに関する最新動向を収集する	0.1389	0.4676	0.2081	0.1942	0.0185
2.	管理者編					
2.1	情報セキュリティ対策管理実践の勧めから					
2.1.0	本文	1.2681	0.8294	0.3439	0.3078	0.1236
2.2	できるところから始める					
2.2.1	① OS やソフトウェアは常に最新の状態に	0.5683	0.6547	0.2649	0.2225	0.1317
2.2.2	② ウイルス対策ソフトを導入しよう	0.3753	0.3586	0.1291	0.1027	0.1426
2.2.3	③ パスワードを強化しよう	0.0667	0.1326	0.0582	0.0797	0.1346
2.2.4	④ 共有設定を見直そう	0	0.2027	0	0	0.0872
2.2.5	⑤ 脅威や攻撃の手口を知ろう	0.0611	0.1251	0.0210	0.0158	0
2.3	組織的な取り組みを開始する					
2.3.1	(1) 情報セキュリティの基本方針の作成と周知	0.6666	0.3861	0.1857	0.3399	0.1898
2.3.2	(2) 実施状況の把握	0.5907	0.7397	0.3426	0.5227	0.1990
2.3.3	(3) 対策の決定と周知	0.4318	0.6424	0.2685	0.4511	0.2010
2.4	本格的に取り組む	1.6834	0.8123	0.2745	0.3927	0.1325
2.4.1	（１）責任分担と連絡体制の整備					
2.4.1.1	① 責任分担と連絡体制の整備	0.9235	1.1129	0.3165	0.3152	0.1789
2.4.1.2	② 緊急時対応体制の整備	0.5621	0.7748	0.3493	1.4531	0.2712
2.4.2	（２）IT 利活用方針と情報セキュリティの予算化	0.6321	0.5322	0.1159	0.2943	0.0853
2.4.3	（３）　情報セキュリティ規程の作成	1.4932	0.3252	0.0973	0.3422	0.1306
2.4.3.1	① 対応すべきリスクの特定	1.3528	0.6290	0.2018	0.7493	0.0708
2.4.3.2	② 対策の決定	1.4699	0.4261	0.1451	1.3997	0.1844
2.4.3.3	③ 規程の作成	0.3981	0.4167	0.1797	0.4942	0.1230
2.4.4	（４）委託時の対策	0.7028	1.0299	0.2800	0.6627	0.1376
2.4.5	（５）点検と改善	0.6737	0.8151	0.2877	0.5698	0.1850
2.5	より強固にするための方策					
2.5.1	（１）情報収集と共有					
2.5.1.1	① 情報収集の方法	0.2808	0.1676	0.0836	0.0759	0
2.5.1.2	② 情報共有の枠組み	0.4045	0.3717	0.0622	0.3634	0.0906
2.5.2	（２）ウェブサイトの情報セキュリティ					
2.5.2.1	① ウェブサイトの運営形態の検討	0.8478	0.7987	0.3044	0.3827	0.3136
2.5.2.2	② ウェブサイトの構築	0.3596	0.5281	0.2226	0.3562	0.1781
2.5.2.3	③ ウェブサイトの運営	0.7340	0.9585	0.3925	0.4017	0.2204

2.5.3	（3）クラウドサービスの情報セキュリティ					
2.5.3.1	① クラウドサービスの選定	0.5363	0.6974	0.1122	0.1094	0.1385
2.5.3.2	② クラウドサービスの運用	1.0961	0.7829	0.2178	0.3162	0.3527
2.5.3.3	③ クラウドサービスのセキュリティ対策	0.5453	0.8064	0.3299	0.3961	0.3199
2.5.4	（4）セキュリティサービス例と活用					
2.5.4.1	① 情報セキュリティコンサルテーション	0.7975	0.8989	0.1307	0.3174	0.1811
2.5.4.2	② 情報セキュリティ教育サービス	0.2292	1.0582	0.2576	0.1693	0.1550
2.5.4.3	③ 情報セキュリティ監査サービス	0.9156	0.6980	0.2223	0.1668	0.1567
2.5.4.4	④ 脆弱性診断サービス	0.1903	0.4307	0.1003	0.2652	0.0729
2.5.4.5	⑤ デジタルフォレンジックサービス	0.2001	0.3661	0.0240	0.4184	0.0680
2.5.4.6	⑥ セキュリティ監査・運用サービス	0.1762	1.2275	0.5411	0.3263	0.2283
2.5.5	（5）技術的対策例と活用					
2.5.5.1	①ネットワーク脅威対策	0.5599	1.1140	0.5137	0.3527	0.1188
2.5.5.2	②コンテンツセキュリティ対策	0.7286	1.3138	0.7223	0.6255	0.2247
2.5.5.3	③アクセス管理	0.9036	1.2364	0.0435	0.0831	0.1502
2.5.5.4	④システムセキュリティ管理	1.3048	1.0380	0.1643	0.3526	0.1309
2.5.5.5	⑤暗号化	0.6210	1.0080	0.0467	0.4084	0.0179
2.5.5.6	⑥データの破棄	0.7909	0.4499	0.0380	0.1840	0.0252
2.5.6	（6）詳細リスク分析の実施方法					
2.5.6.0	序文	2.1093	0.8570	0.2195	0.6279	0.1541
2.5.6.1	手順１　情報資産の洗い出し	1.5312	0.9563	0.1111	0.2563	0.0651
2.5.6.2	手順２　リスク値の算定	1.3225	0.7057	0.2058	0.5168	0.2060
2.5.6.3	手順３　情報セキュリティ対策の決定	1.6096	0.8630	0.3244	0.6245	0.2569

表 15　各節・項に対して機能単位でテンプレートコーディングを実施した結果

Table 15　Text mining analysis results for sections with functional view

ID	表題	識別	防御	検知	対応	復旧
0	経営者の皆様へ					
1	経営者編					
1.1	情報セキュリティ対策を怠ることで企業が被る不利益					
1.1.0	序文	3	1	0	0	0
1.1.1	(1) 金銭の損失	1	2	0	0	0
1.1.2	(2) 顧客の喪失	1	3	0	0	1
1.1.3	(3) 業務の喪失	1	2	0	1	0
1.1.4	(4) 従業員への影響	1	1	0	0	1
1.2	経営者が負う責任					
1.2.1	(1) 経営者などに問われる法的責任	2	0	0	0	0
1.2.2	(2) 関係者や会社に対する責任	2	1	0	0	0
1.3	経営者は何をしなければならないのか？					
1.3.1	認識すべき「3 原則」	0	1	0	0	0
1.3.1.1	原則 1　情報セキュリティ対策は経営者のリーダー	1	1	0	0	0

	シップで進める					
1.3.1.2	原則 2　委託先の情報セキュリティ対策まで考慮する	3	1	0	0	0
1.3.1.3	原則 3 関係者との情報セキュリティに関するコミュニケーションはどんな時も怠らない	1	2	0	1	0
1.3.2	実行すべき「重要 7 項目の取り組み」					
1.3.2.0	序文	1	0	0	0	0
1.3.2.1	取組 1　情報セキュリティに関する組織全体の対応方針を決める	2	1	0	0	0
1.3.2.2	取組 2　情報セキュリティ対策のための予算や人材を確保する	1	1	0	0	0
1.3.2.3	取組 3　必要と考えられる対策を検討させて実行を指示する	4	1	0	0	0
1.3.2.4	取組 4　情報セキュリティ対策に関する適宜の見直しを指示する	0	1	0	1	1
1.3.2.5	取組 5　緊急時の対応や復旧のための体制を整備する	0	0	0	1	1
1.3.2.6	取組 6　委託や外部サービスの利用の際にはセキュリティに関する責任を明確にする	2	0	0	0	0
1.3.2.7	取組 7　情報セキュリティに関する最新動向を収集する	1	1	0	0	0
2.	管理者編					
2.1	情報セキュリティ対策管理実践の勧めから					
2.1.0	本文	1	1	0	0	0
2.2	できるところから始める					
2.2.1	① OS やソフトウェアは常に最新の状態に	0	1	0	0	0
2.2.2	② ウイルス対策ソフトを導入しよう	0	0	1	0	0
2.2.3	③ パスワードを強化しよう	0	1	0	0	0
2.2.4	④ 共有設定を見直そう	0	2	0	0	0
2.2.5	⑤ 脅威や攻撃の手口を知ろう	1	0	0	0	0
2.3	組織的な取り組みを開始する					
2.3.1	(1) 情報セキュリティの基本方針の作成と周知	1	1	0	0	0
2.3.2	(2) 実施状況の把握	0	1	0	0	0
2.3.3	(3) 対策の決定と周知	4	1	0	0	0
2.4	本格的に取り組む	4	0	0	0	0
2.4.1	（1）責任分担と連絡体制の整備					
2.4.1.1	① 責任分担と連絡体制の整備	1	2	0	0	0
2.4.1.2	② 緊急時対応体制の整備	0	1	0	3	0
2.4.2	（2）IT 利活用方針と情報セキュリティの予算化	2	0	0	0	0
2.4.3	（4）　情報セキュリティ規程の作成	1	0	0	0	0
2.4.3.1	① 対応すべきリスクの特定	4	0	0	0	0
2.4.3.2	② 対策の決定	3	0	0	0	0

2.4.3.3	③ 規程の作成	1	1	0	0	0
2.4.4	（4）委託時の対策	2	1	0	0	0
2.4.5	（5）点検と改善	0	4	0	0	0
2.5	より強固にするための方策					
2.5.1	（1）情報収集と共有					
2.5.1.1	① 情報収集の方法	1	0	0	0	0
2.5.1.2	② 情報共有の枠組み	0	1	0	1	0
2.5.2	（2）ウェブサイトの情報セキュリティ					
2.5.2.1	① ウェブサイトの運営形態の検討	2	0	0	0	0
2.5.2.2	② ウェブサイトの構築	3	1	0	0	0
2.5.2.3	③ ウェブサイトの運営	0	3	0	0	0
2.5.3	（3）クラウドサービスの情報セキュリティ					
2.5.3.1	① クラウドサービスの選定	2	0	0	0	0
2.5.3.2	② クラウドサービスの運用	7	0	0	0	0
2.5.3.3	③ クラウドサービスのセキュリティ対策	4	0	0	0	0
2.5.4	（4）セキュリティサービス例と活用					
2.5.4.1	① 情報セキュリティコンサルテーション	3	1	0	0	0
2.5.4.2	② 情報セキュリティ教育サービス	0	1	0	0	0
2.5.4.3	③ 情報セキュリティ監査サービス	0	0	0	0	0
2.5.4.4	④ 脆弱性診断サービス	0	1	0	0	0
2.5.4.5	⑤ デジタルフォレンジックサービス	0	0	0	1	0
2.5.4.6	⑥ セキュリティ監査・運用サービス	0	0	3	0	0
2.5.5	（5）技術的対策例と活用					
2.5.5.1	①ネットワーク脅威対策	0	4	0	0	0
2.5.5.2	②コンテンツセキュリティ対策	0	0	2	0	0
2.5.5.3	③アクセス管理	0	3	0	0	0
2.5.5.4	④システムセキュリティ管理	0	3	0	0	0
2.5.5.5	⑤暗号化	0	1	0	0	0
2.5.5.6	⑥データの破棄	0	1	0	0	0
2.5.6	（6）詳細リスク分析の実施方法					
2.5.6.0	序文	5	0	0	0	0
2.5.6.1	手順１　情報資産の洗い出し	2	0	0	0	0
2.5.6.2	手順２　リスク値の算定	3	0	0	0	0
2.5.6.3	手順３　情報セキュリティ対策の決定	5	0	0	0	0

5.1.4.3. 提案手法の妥当性について

第 4 部の議論によって提案手法の結果についてある程度の妥当性が認められると考えるが，本節では，「章」と「節・項」についての分析においてどの程度認められるか改めて確認した．また，第 4 部の解析の時点では第 2.1 版だった文書が第 3 版になっているため，文書全体の評価についても改めて評価を実施した．

「文書全体」と各「章」と「節・項」ごとに，提案手法の結果とテンプレートコーディ

ングの結果との間のピアソン積率相関係数を計算し平均値をとったものが，表 16 である．文書全体に対する適用結果を確認すると，機能単位では機能レベルで見た場合でもカテゴリレベルで見た場合でも強い正の相関を示しており，これは第 4 部で「中小企業の情報セキュリティに関するガイドライン第 2.1 版」に対して，提案手法を適用した場合の結果と同じ傾向である．

「章」で見た場合には，機能レベルでは強い正の相関，カテゴリレベルでは正の相関が確認され，「節・項」で見た場合には，機能レベルでは正の相関，カテゴリレベルでは弱い正の相関が確認された．

表 16　提案手法の結果と質的コーディングの結果の間のピアソン積率相関係数

Table 16　Pearson product rate correlation coefficient between the results of the proposed method and the results of qualitative coding

文書名	カテゴリ（23）	機能（5）
文書全体	0.710	0.970
章の平均	0.543	0.862
節・項の平均	0.225	0.503

5.1.4.4.　結果の妥当性の検証についての議論と制限

この予備実験の「中小企業の情報セキュリティ対策ガイドライン　第 3 版」に対するテンプレートコーディングは，2 名で行われた．両名とも CSF とその翻訳版である「重要インフラのサイバーセキュリティを改善するためのフレームワーク」と「中小企業の情報セキュリティ対策ガイドライン」の第 2.1 版及び第 3 版について学習済みの状態であり，1 名は第 4 部において「中小企業の情報セキュリティ対策ガイドライン　第 2.1 版」に対してテンプレートコーディングを実施し，1 名はその結果に対するレビューを行っている．そのため，両名ともコードについて検討する際に前回の結果の影響を受けた可能性がある．

提案手法の結果とテンプレートコーディングの結果に相関が確認されたことより，提案手法の結果を手がかりにして，文書の各「章」や「節・項」とフレームワークコアのカテゴリがどのような関係にあるかを把握することができると考えられる．

特に，ある「節・項」がフレームワークコアのどの機能に関連しているか，ある「章」がフレームワークコアのどのカテゴリに関連しているかという観点では，強いないし中程度の相関が見えているため，信頼を持って適用が可能であると考えられる．しかしながら，ある「節・項」がどのカテゴリに関連しているかという観点では弱い相関しか見られなかったため，提案手法の結果については慎重に適用する必要があると考えられる．

「節・項」については，文書上目次で明示的に定義されていなかったため，文章中に現れる項目ごとに分割を行っている．そのため，本来執筆者が意図していない分割になっている可能性がある．また，項の単位で見た場合には，手法の紹介で留められている場合があり，その場合では文章の長さが短い可能性がある．今回の文書での 1 つの「節・項」の

文章の長さは 100 字程度であるが一方で，短い「節・項」では，数十字程度であった．テンプレートコーディングの結果を正しいと考えた場合，「節・項」において相関が弱くなったのは，文章の短さが提案手法の結果に悪い影響を与えたためであると考えられる．

また，「節・項」単位で見た場合には，テンプレートコーディング上割り当てられるカテゴリは平均 2 個程度多くても 6 個であり殆どの値が 0 となる．一方で提案手法においては殆どの場合，一つの単語の評価により複数のカテゴリに加算がされるため，大半の値が 0 となるようなことは殆どなかった．そのため，類似性を評価するピアソン積率相関係数では弱い相関となった可能性が考えられる．これは評価方法の制限である．

5.1.5. 教材の作成

分析結果を基にして，「中小企業の情報セキュリティ対策ガイドライン　第 3 版」にフレームワークコアの情報を付加し，ユーザーインタフェースを改善した教材を設計した．

5.1.5.1. 対応付け

これらの「章」や「節・項」と CSF のフレームワークコアとの関係性の分析結果を基にして，「章」や「節・項」に主に関連するカテゴリと副次的に関連するカテゴリを選定した．

前 5.1.4 節の検討の結果から強い相関が確認できたため，「章」がどの機能と結びついているかという判断は提案手法の結果をそのまま採用した．

また，「章」がどのカテゴリと結びついているかという判断は，相関が確認されたため，提案手法の結果に基づいて決定することとした．具体的には，カテゴリ全体の約 3 割にあたる上位 7 つのカテゴリから，主たる内容に当たりそうなカテゴリと，副次的な内容に当たりそうなカテゴリを選択的に割り当てた．この際，分析結果のスコアを 23 次元ベクトルとして考え規格化した後の数値が，0.2 を下回るものは上位 7 位に含まれていても採用しなかった．主に関連があると思われるカテゴリは最低 1 個，最大 2 個まで設定可能として，副次的に関連があると思われるカテゴリは最低 0 個，最大 3 個まで設定可能とした．

「章」についてカテゴリを割り当てたものを表 17 に記載する．主に関連があると思われるカテゴリは，主カテゴリ，副次的に関連があると思われるカテゴリは副カテゴリとして分類した．

「節・項」については，「節・項」がどのカテゴリと最も結びついているかという判断は，前 5.1.4 節の検証で弱い相関しかみられなかったためそのまま適用することを避けて，上位 7 つのカテゴリの中から選択的に採用しつつも，適用するものがないと思われる場合や，追加の必要を感じた場合には適宜カテゴリを追加した．最終的に，提案手法に基づかないで追加したカテゴリは全体の 35%程度であった．「節・項」についての結果は表 18 に記載する．この際，提案手法に寄らず追加されたカテゴリについては表中下線で記載する．

表 17　フレームワークコアのカテゴリと章の対応付け [2]

Table 17　Map chapters to categories of framework core

ID	主カテゴリ ID	副カテゴリ ID
0	ID.GV	PR.AT, PR.IP
1.1	ID.RA	PR.AT, PR.IP
1.2	ID.GV	ID.RA, PR.AT
1.3	PR.IP,PR.AT	ID.BE, ID.GV
2.1	ID.GV	PR.AT
2.2	PR.AC	ID.RA, PR.IP, DE.CM
2.3	ID.GV, PR.AT	PR.IP
2.4	ID.AM,ID.RA	ID.GV,PR.AT,
2.5	ID.AM,ID.RM,ID.SC	ID.GV, PR.AC, PR.IP

表 18　フレームワークコアのカテゴリと節・項の対応付け

Table 18　Map chapters to categories of framework core

ID	主カテゴリ ID	副カテゴリ ID
0		
1.		
1.1		
1.1.0	ID.RA	ID.GV
1.1.1	ID.RA	PR.AT, ID.GV
1.1.2	ID.RA	
1.1.3	ID.RA	
1.1.4	ID.RA	
1.2.		
1.2.1	ID.GV	ID.RA, PR.AT
1.2.2	ID.RA	ID.GV, PR.AT
1.3.		
1.3.1	PR.AT	
1.3.1.1	ID.BE, PR.AT	
1.3.1.2	ID.SC	ID.BE, ID.AM
1.3.1.3	ID.SC, RS.CO	PR.AT, PR.IP
(1) 実行すべき「重要 7 項目の取り組み」		
1.3.2.0	ID.GV	
1.3.2.1	ID.GV	
1.3.2.2	ID.GV	PR.IP
1.3.2.3	ID.RA [3]	PR.IP
1.3.2.4	PR.IP	DE.DP, RS.IM, RC.IM

2 引用元の論文 [76] 上の Table 5 を訂正．ID-1.3 と ID- 2.4 の副カテゴリにある ID.SC と PR.IP を削除

3 引用元の論文 [83]　上の Table 7 の PR.IP から ID.RA に訂正.

1.3.2.5	RS.RP, RC.RP	PR.IP
1.3.2.6	ID.SC	ID.AM
1.3.2.7	ID.RA	PR.IP
2		
2.1		
2.1.0	ID.GV	PR.AT
2.2		
2.2.1	PR.IP	
2.2.2	DE.CM	
2.2.3	PR.AC	
2.2.4	PR.AC	
2.2.5	ID.RA	
2.3		
2.2.3.1	ID.GV	PR.AT
2.2.3.2	PR.IP	
2.2.3.3	ID.RA, ID.RM	ID.GV, ID.AM, PR.AT
2.4	ID.GV	ID.RA, ID.BE
2.4.1		
2.4.1.1	ID.AM, PR.AT	
2.4.1.2	RS.CO, PR.IP	
2.4.2	ID.AM	
2.4.3	ID.GV	
2.4.3.1	ID.RA,ID.RM	ID.AM,ID.GV
2.4.3.2	ID.RM	ID.RA
2.4.3.3	ID.GV, PR.IP	
2.4.4	ID.SC	PR.AT, ID.AM
2.4.5	PR.IP	
2.5		
2.5.1		
2.5.1.1	ID.RA	
2.5.1.2	PR.IP,RS.CO	
2.5.2		
2.5.2.1	ID.AM	
2.5.2.2	ID.RA, ID.RM	PR.IP
2.5.2.3	PR.PT, PR.DS	PR.AC, PR.IP
2.5.3		
2.5.3.1	ID.AM, ID.SC	
2.5.3.2	ID.RM, ID.RA	ID.SC, ID.GV, ID.AM
2.5.3.3	ID.SC, ID.GV	ID.AM, PR.IP
2.5.4		
2.5.4.1	ID.GV,PR.IP	ID.RA, ID.RM

2.5.4.2 [4]	PR.AT	
2.5.4.3	ID.RA, ID.RM	
2.5.4.4	PR.IP	
2.5.4.5	RS.AN	
2.5.4.6	DE.CM	DE.DP, DE.AE
2.5.5		
2.5.5.1	PR.PT	PR.DS, PR.AC
2.5.5.2	DE.CM,DE.AE	
2.5.5.3	PR.AC	
2.5.5.4	PR.MA	PR.IP
2.5.5.5	PR.DS	
2.5.5.6	PR.IP	
2.5.6		
2.5.6.0	ID.RM/RA	
2.5.6.1	ID.AM	ID.RA
2.5.6.2	ID.RA	
2.5.6.3	ID.RM	

5.1.5.2. 対応付けの議論

一部の「節・項」においては 7 つの候補の中に適切だと思われるカテゴリが存在しなかったため，別のカテゴリを割り当て追加した．ここでは，それらの「節・項」のうち追加したカテゴリが過半数になってしまった「節・項」について議論する．

5.1.5.2.1. 「取組 1 情報セキュリティに関する組織全体の対応方針を決める」

「中小企業の情報セキュリティ対策ガイドライン　第 3 版」の 1.3.2.1. 項に当たる「取組 1．情報セキュリティに関する組織全体の対応方針を決める」に対して，提案手法で高い関連を示したカテゴリは，RS.IM，PR.IP，RS.CO,RS.AN，PR.AT，RS.RP，PR.DS であり，防御ないし対応の機能に属するカテゴリであった．しかしながら，この項目は実際の文章では，以下のように組織全体の対応方針について述べている．

> *情報セキュリティ対策を組織的に実施する意思を，従業員や関係者に明確に示すために，（中略）情報セキュリティに関する基本方針を定め宣言します.*
>
> *―中小企業の中小企業の情報セキュリティ対策ガイドライン　第 3 版*

これはカテゴリで言うと，識別（ID）のガバナンス（GV）の以下の ID.GV-1 のサブカ

4 引用元の論文 [83]　上の Table 7　を訂正．元の表では，Information security audit service で，PR.PT となっているが，正しくは，「教育サービス」で，PR.AT.

テゴリ―について述べているものと思われる．

> *ID.GV-1:　組織のサイバーセキュリティポリシーが定められ周知されている．*
>
> *―重要インフラのサイバーセキュリティを改善するためのフレームワーク　1.1 版*

従って，項目としては，ID.GV を付与した．

防御ないし対応の機能として関連付けられた原因としては，「対応」という単語が機能としての対応に属するカテゴリ，「セキュリティ」という単語が防御に属するカテゴリの上位の特徴語となっていることが挙げられると考えられる（表 7 も参照）．文がある程度の長さを持っていれば，特定の単語の影響を強く受けることはなくなると考えられるが，今回の事例では，40 字程度の文に対する適用であったため，これらの単語の影響が際立ったものと考えられる．

5.1.5.2.2.　「取組 4. 情報セキュリティ対策に関する適宜の見直しを指示する」

「中小企業の情報セキュリティ対策ガイドライン　第 3 版」の 1.3.2.4. 項に当たる「取組 4　情報セキュリティ対策に関する適宜の見直しを指示する」に対して，提案手法で高い関連を示したカテゴリは，PR.AT，RC.CO，ID.SC，PR.IP，DE.CM，RS.CO，ID.RA のカテゴリであった．しかしながら，この項目は実際の文章では，下記のようにポリシーやプロセスの評価と見直しについて述べている．

> *（前略）情報セキュリティ対策について、実施状況を点検させ取組 1 で定めた方針に沿って進んでいるかの評価をします、（中略）基本方針なども適宜見直しを行い、致命的な被害に繋がらないよう、対策の追加や改善などを行うように責任者担当者に指示します。*
>
> *―中小企業の中小企業の情報セキュリティ対策ガイドライン　第 3 版*

CSF 上で，ポリシー，プロセスの評価に触れているのは，サブカテゴリの，PR.IP-7，DE.DP-5 とカテゴリである．従って，PR.IP，DE.DP，RS.IM，RC.IM のカテゴリを割り振った．

他のカテゴリが強く関連付けられた原因は，前項 5.1.5.2.1 と同一であると考えられる．文の長さは，40 字程度であり，PR.AT の「責任」，ID.SC の「評価」，RC.CO の「被害」などの単語に過敏に反応したと考えられる．

5.1.5.2.3.　「①OS やセキュリティソフトは最新の状態にしよう！」

「中小企業の情報セキュリティ対策ガイドライン　第 3 版」の 2.2.1 項に当たる「 ①OS

やセキュリティソフトは最新の状態にしよう！」に対して，提案手法で高い関連を示したカテゴリは，DE.CM, PR.DS, ID.BE, ID.AM, ID.GV, ID.SC, ID.RM であった．主にデータ保護や検知のためのモニタリング，識別関連の項目として分類されてしまっているが，実際の文章は，下記のように修正プログラムの定期的な適用を促すものとなっている．

> *（前略）お使いの OS やソフトウェアには修正プログラムを適用する、もしくは最新版を利用するようにしましょう。*
>
> *―中小企業の中小企業の情報セキュリティ対策ガイドライン　第 3 版*

これは防御（PR）のガバナンス（IP）の以下の PR.IP-12 のサブカテゴリ―について述べているものと思われる．

> *PR.IP-12:　脆弱性管理計画が，作成され，実施されている．*
>
> *―重要インフラのサイバーセキュリティを改善するためのフレームワーク　1.1 版*

従って，項目としては，PR.IP を付与した．

他のカテゴリが強く関連付けられた原因は，前項 5.1.5.2.1 と同一であると考えられる．文の長さは，30 字程度であった．この節・項の特徴語について確認したところ，カテゴリの上位 10 個の特徴語に含まれるものは，「セキュリティ」しかなかったため，これに反応したものと思われる．

5.1.5.2.4.　「①規程の作成」

「中小企業の情報セキュリティ対策ガイドライン　第 3 版」の 2.4.3.3 項にあたる「①規程の作成」に対して，提案手法で高い関連を示したカテゴリは，　RS.MI, RS.IM,DE.CM,PR.PT,RS.CO,PR.AT,ID.SC であり対応の機能に属するカテゴリについて述べているように見えるが，実際の文章は，下記のようにセキュリティポリシーを策定，改善する内容であった．

> *②で決定した対策を文書化した規程を作成します。決定した対策を一から文書化するのは経験がないと難しいため、「情報セキュリティ関連規程(サンプル)」(付録 5)を参考に、自社に適した規程にするために修正を加えます(表 7)。*
>
> *サンプル文中の赤字、青字部分を自社向けに修正すれば，自社の規程が完成します。なお、サンプルに明記されていなくても必要な対策や有効な対策があれば、追記を行ってください。*

―中小企業の中小企業の情報セキュリティ対策ガイドライン　第 3 版

そのため，ID.GV と PR.IP を割り当てた．それぞれ

ID.GV-1:　組織のサイバーセキュリティポリシーが定められ周知されている.

PR-IP-7：防御プロセスは改善されている.

―重要インフラのサイバーセキュリティを改善するためのフレームワーク　1.1 版

が該当すると考えられる．

他の事例と異なり，この「節・項」の文の長さは，約 60 字程度であった．このカテゴリの上位 10 単語をみると「セキュリティ」が含まれており，それに反応した可能性があったが，他の高いスコアが出たカテゴリとずれがあった．そこで，それ以外の単語について調査するため，この「節・項」の特徴語とカテゴリ毎の特徴語を比較した結果，「一」という一般語でこれらのカテゴリのスコアに加算がされていることを確認した．これは，TF-IDF の実施時にフィルタが不十分であったため混入したと考えられる．

5.1.5.2.5.　「⑥データ破棄」

元の教材の 2.5.5.6 項 「⑥データ破棄」に対して，提案手法で高い関連を示したカテゴリは，ID.AM，PR.DS，ID.RM，ID.BE，ID.GV，ID.RA，ID.SC であり識別の機能について述べているように見える．しかしながら，実際の文章は，以下のようにデータ破棄ポリシーについて説明している．

情報システムを使わなくなった場合、システム内にデータを保存したまま放置したり、破棄したりするとそれが情報漏えいの原因となるため、速やかにデータの消去を行う必要があります。

―中小企業の中小企業の情報セキュリティ対策ガイドライン　第 3 版

これは防御（PR）のガバナンス（IP）の以下の PR.IP-6 のサブカテゴリ―について述べているものと思われる．

PR.IP-6:データは，ポリシーに従って破棄される.

―重要インフラのサイバーセキュリティを改善するためのフレームワーク　1.1 版

したがって，PR.IP を割り当てた．

実際に割り当てたカテゴリとは異なるカテゴリが強く関連付けられた原因は，他の場合と基本的には同一であると考えられる．文の長さは，約 40 字程度であり，単語「リスク」に過敏に反応したため，識別に属するカテゴリが多く含まれたと考えられる．一方で，この「節・項」について関連性が高いと思われる資産管理とデータセキュリティのカテゴリについては，上位に正しく挙げられていた．PR.IP の「情報を保護するためのプロセスおよび手順」では，様々なセキュリティポリシー，プロセスについて言及されているため，データについての文章で，関連のある別カテゴリのスコアが高くなってしまった可能性がある．

5.1.5.2.6. 対応付けの限界と応用について

本研究では，「中小企業の情報セキュリティ対策ガイドライン　第 3 版」を対象として，フレームワークコアのカテゴリとの対応付けを実施したが，このアプローチ自体は，「中小企業の情報セキュリティ対策ガイドライン　第 3 版」に依存しておらず，他の情報セキュリティ対策の文書教材に対しても応用可能だと考えられる．

一方で，前項までの対応付けが上手くいかなかった「節・項」の議論をまとめると，現時点では以下の様な問題があると考えられる．

1) 50 字前後を境に本来適用されるべきカテゴリが上位にあらわれなくなる．

2) 一部の特徴語ベクトルに一般語が含まれている

この内，2)については TF-IDF を実施する前に事前にわかる範囲の一般語を除外するようにフィルタを適切に設定することで解消可能であると考えられるが，1)については，解析対象の文章が短すぎるために発生する問題で，文の類似性を利用するアプローチで共通する問題であり改善には詳細な検討が必要な課題であると考える．

5.1.5.3. インタフェースの設計

前項で検討した表 17 と表 18 の情報に基づいて教材の作成を行った．今回の実験においては，「中小企業の情報セキュリティ対策ガイドライン　第 3 版」の内容の変更を可能な限りさけるため，CSF のフレームワークコアとの関係性を外挿するような形で関係性を明示した．

5.1.5.3.1. インタフェース概要

作成した教材のユーザーインタフェースを図 12 に示す．画面の左側には，フレームワークコアのカテゴリがリストアップされ（図 12 の B），その隣には，「中小企業の情報セキュリティ対策ガイドライン　第 3 版」の目次がリストアップされ（図 12 の C），画面右側に本文が表示されている（図 12 の D）．目次の項目にマウスカーソルを合わせると，その項目がどのカテゴリに関連しているかを示す線が表示される（図 12 の A）．

実線はそのカテゴリと関連性が高く（表 17 と表 18 の主カテゴリ），破線はそのカテゴリと副次的に関連性がある（表 17 と表 18 の副カテゴリ）ことを表す．C に表示される目次は，クリックすることでより詳細な目次が展開される．「中小企業の情報セキュリティ対策ガイドライン　第 3 版」の目次の項目やカテゴリや機能の各項目をクリックすると，本文表示部分（図 12 の D）に説明が表示される．「中小企業の情報セキュリティ対策ガイドライン　第 3 版」の本文は，元の文書と同一である．カテゴリや機能の説明文は，CSF のものを参考に作成されており，「中小企業の情報セキュリティ対策ガイドライン　第 3 版」の各「章」や「節・項」との関連性についても記載されている．教材の作成には，Adobe 社の販売する Adobe XD [79]を用いて行った．これはプロトタイプ作成のための製品で，文字の細かな調整や動的表示を実装する上で制限がかかるが，今回の改良案ではそれらの制限を超えるような機能を付ける予定はなかったため，実装の簡便さを優先してこの環境で作成を行った．

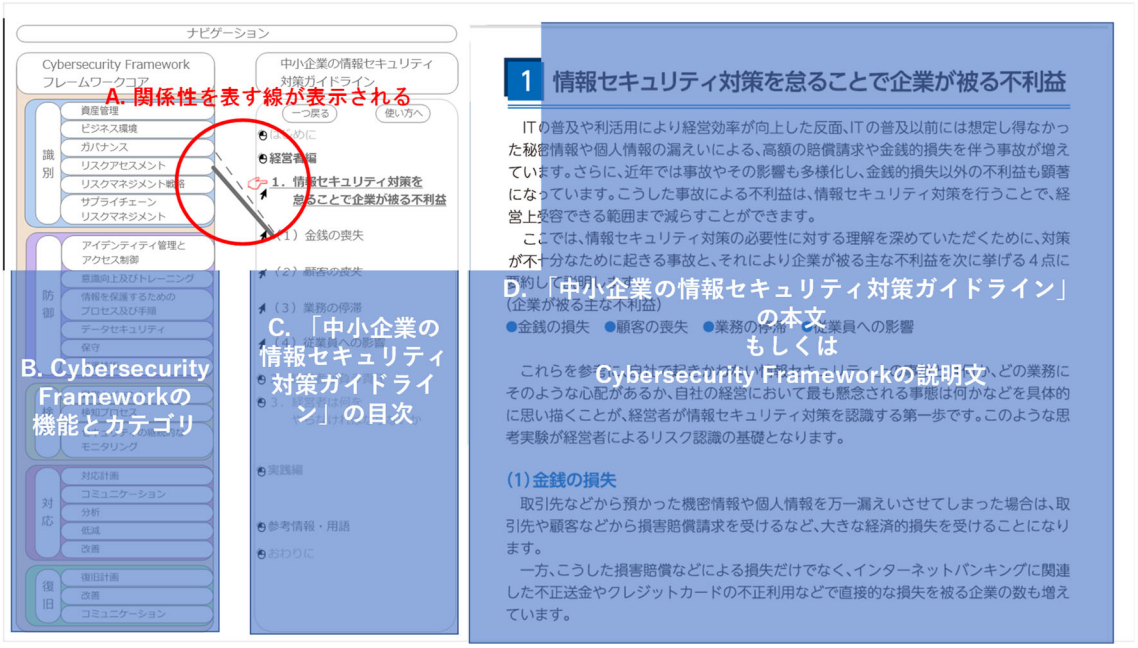


図 10　教材のインタフェース（各部分の説明付き）

Figure 10 Interface of the material with explanation

5.1.5.3.2.　教材の動作事例

ここでは，教材の基本的な画面の遷移について一つずつ紹介していく．

(1) アイコンについての説明

教材を開いた一番初めのページにはこの教材の使い方についての説明が記載されている．本教材では，学習者は図 10 の C 部にある目次をクリックしながら D 部の説明を読み進めていくことになるが，目次の項目に 3 種類の印が付与されていることがあるため，これらについて説明を行っている（図 11）．一つ目は，赤い矢印の印でこれは現在いるセクションをさしている．二つ目は，右クリック部が黒く表示されたマウスの印で，これはその目次がクリック可能なことを示す．最後に，黒い矢印の印でこれはマウスオーバーすることで，フレームワークコアとの関係性が表示されること示している．

図 11　教材のインタフェース：教材の使い方

Figure 11 Interface of teaching materials: How to use page

(2) 図 10 の C 部の目次をクリックすることによる「中小企業の情報セキュリティ対策ガイドライン」の本文の表示／より詳細な目次の表示

クリック可能な目次のクリックを行うと，対象のセクションの説明が図 10 の D 部に表示される．また，場合によっては，そのセクションのより詳細な目次が図 10 の C 部に表示される．図 12 の例では，図 11 の目次の内容よりも，「1 情報セキュリティ対策を怠ることで企業が被る不利益」のセクションについて，より詳細な項目である (1) 金銭の喪失，(2) 顧客の喪失，(3) 業務の停滞，(4) 従業員への信頼 の 4 つが表示されており，D 部には「1 情報セキュリティ対策を怠ることで企業が被る不利益」の説明文が記載されている．

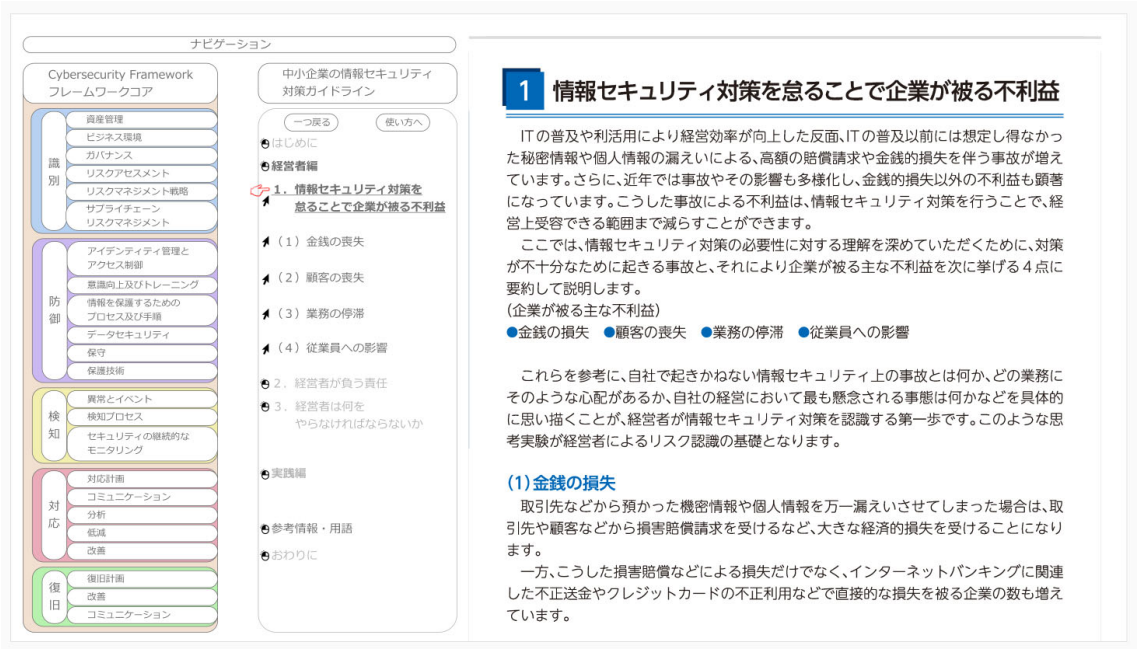


図 12　教材のインタフェース：本文の表示・詳細な目次の表示

Figure 12 Interface of teaching materials: Description and detail items

(3) 図 10 の C 部の目次をマウスオーバーすることによる関連性の表示

黒い矢印の印がつけられている項目をマウスオーバーすることで，図 10 の B 部のフレームワークコアとの関連性が表示される．この際，実線は主にかかわる項目を示し，破線は副次的にかかわる項目を示している．図 13 では，「1 情報セキュリティ対策を怠ることで企業が被る不利益」のセクションをマウスオーバーしており，主としてリスクアセスメント（また副次的にはガバナンス）に関連していることが表示されている．

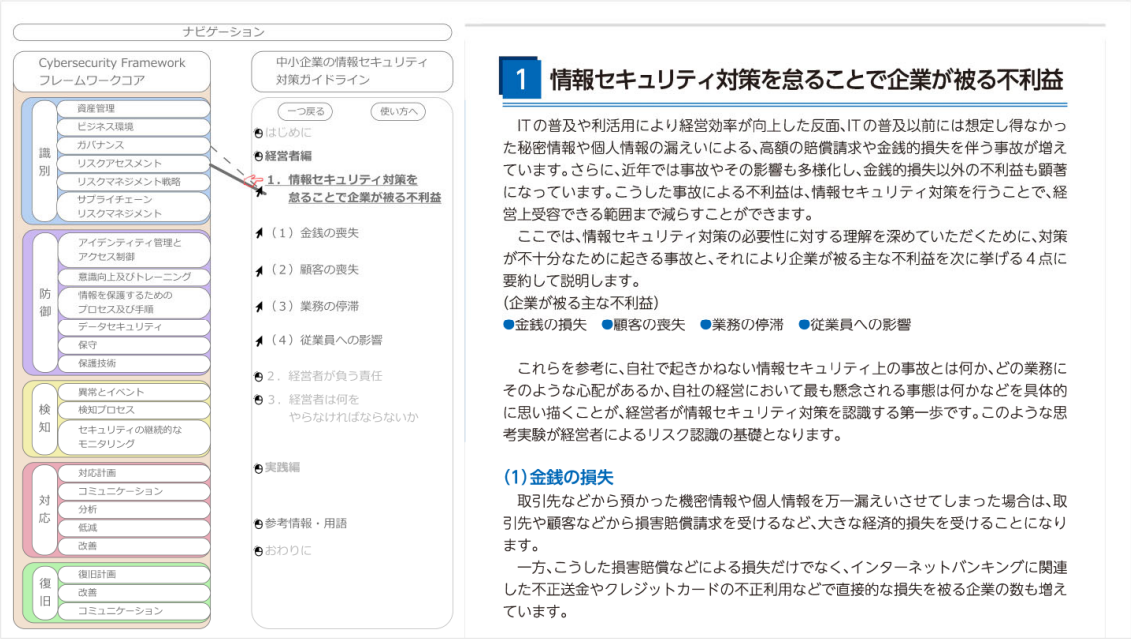


図 13　教材のインタフェース：関連性の表示

Figure 13 Interface of teaching materials: Relationship of CSF framework core and items

(4) 図 10 の B 部の項目をクリックすることによる CSF のフレームワークコアのカテゴリの表示

図 10 の B 部のカテゴリの項目をクリックすることで，そのカテゴリについての解説の文章が表示される．図 14 では，リスクアセスメントのカテゴリがクリックされておりその説明が表示されている．元の画面に戻る場合には，グレイアウト部をクリックすることで戻ることができる．また，説明の下部には，「中小企業の情報セキュリティ対策ガイドライン」の関連する項目が表示されており，クリックすることで対象の項目の説明文へ遷移することができる．

図 14　教材のインタフェース：Cybersecurity Framework のフレームワークコアの説明

Figure 14 Teaching material interface: Description of the category of Cybersecurity Framework

(5) 図 10 の B 部の項目をクリックすることによる CSF のフレームワークコアの機能の表示

また，図 10 の B 部の機能についてクリックすると，機能についての説明を確認することができる．図 15 の例では，リスクアセスメントが属する識別の機能の説明を表示している．この機能の説明の下部には，その機能に属するカテゴリが表示されており，それをクリックすることで，各カテゴリの説明に遷移することができる．

図 15　教材のインタフェース：Cybersecurity Framework の機能の説明

Figure 15 Interface of teaching materials: Description of the function of Cybersecurity Framework

5.1.6.　結論

この 5.1 章では，第 4 部で文書全体に適用していた手法を，文書内の「章」や「節・項」に援用することで，「中小企業の情報セキュリティ対策ガイドライン　第 3 版」の「章」や「節・項」と，CSF のフレームワークコアの関係性を明らかにし，それに基づいて教材の作成を行った．

適用結果に基づいて教材を作成する前に第 4 部での評価と同様にテンプレートコーディングとの比較を行って，人手による分析の結果との相関について検討した．テンプレートコーディングは 2 名で実施されて，Cohen’s Kappa は 8.1 であった．ピアソン積率相関係数を計算したところ，「章」で見た場合は，質的データ分析の結果と提案手法の結果の相関係数は機能でもカテゴリでも強い相関が確認された．「節・項」で見た場合には，機能では相関が，カテゴリでは弱い相関が確認された．

「節・項」が弱い相関となる原因としては，「節・項」の文が短いため，含まれる単語

数が少なく，また，テンプレートコーディングの結果に 0 が含まれる割合が多くなる一方で提案手法では 1 単語に対して複数のカテゴリに対して加点がされるため，類似性の比較が難しくなってくるためと考えられる．また，特に文が短い場合に（５０字前後を境に）適切なカテゴリに結びつけることができない事例を確認した．

「節・項」とカテゴリの関係については，弱い相関となっていたため，第 4 部の手法の適用結果をそのまま利用するのではなく，分析結果を参考にしつつもカテゴリの追加が必要と思われる部分については適宜追加した．最終的には追加が必要だったカテゴリは全体の 35%程度であった．

この評価結果を参考に，提案結果の適用結果を用いて「中小企業の情報セキュリティ対策ガイドライン　第 3 版」とフレームワークコアのカテゴリと機能との対応付けを行って，その情報に基づいて，インタフェースを変更した教材の作成を行った．

このアプローチは，「中小企業の情報セキュリティ対策ガイドライン　第 3 版」に依存しない方法であるため，他の情報セキュリティ対策関連の文書に対しても適用できる可能性があると考える．

5.2. 作成した教材を用いた予備実験

この章では，前章で作成した改善後の教材を用いた対照実験のために実施された予備実験について記述する．この章の内容は 2021 年の HCII で口頭発表を行った「Study on the Impact of Learning About Information Security Measures on Mental Models: Applying Cybersecurity Frameworks to Self-learning Materials」 [80]に基づいている．これは，1.3 章の研究の流れの説明では，「4）改良された教材を用いた実験について設計して予備実験を通して調整する」 に該当する．

5.2.1. 概要

この予備実験では，設計した実験の手順で学習者のメンタルモデルと学習の効果について観測が可能か、また実験のサンプルサイズはどの程度必要かを確認することを目的とした．

前章でユーザーインタフェースの改良を行った教材とその元となった「中小企業の情報セキュリティ対策ガイドライン　第 3 版」を用いて，実際に 13 人の実験参加者に対して実験を行った．予備実験への参加者はセキュリティ教育を受けていない人，セキュリティ関連の仕事に 1 年から数年携わっている人を対象とした．

実験の参加者は 2 つのグループに分けられ，統制群には情報セキュリティ対策に関する標準的な教材として「中小企業の情報セキュリティ対策ガイドライン　第 3 版」と CSF についての説明補助教材を用いて学習を行ってもらい，実験群には，改良された教材を用いて学習を行ってもらった．自己学習の前後で，学習の効果を確認するためのテストと半構造化インタビューを実施して，自己学習の前後でのテストの得点の変化とメンタルモデル

の変化を調査した.

情報セキュリティ対策の概要について，役割型，時間軸型，フレームワーク型，未構造型の 4 つのメンタルモデルの型があることを確認した．また，サンプル数は少ないが，あるセキュリティ対策がフレームワークコアのどの機能と関連性が高いかを問う選択式の質問では，統計的に有意な差が見られることを確認できた.

5.2.2. 目的

この予備実験では，以下の 3 点を目的として，実際に実験参加者を募って，それぞれ検討を行った.

1. 計画しているインタビュー手順により実験参加者の情報セキュリティ対策に対するメンタルモデルについて描き出すことが可能であるかを確認すること
2. 計画しているテスト内容において学習の前後で有意な差が確認されること．つまり，教材に関わらず学習の効果について確認のできる問題設計になっていることや天井効果やフロア効果の影響の有無の確認すること.
3. 実験群と統制群の間で，統計的に有意な差がでるサンプルサイズについて見積もること.

5.2.3. 実験

5.2.3.1 では，実験参加者の募集と属性について説明し，5.2.3.2 では，実験の流れについて説明を行う.

5.2.3.1. 実験参加者の募集と分布

この予備実験では，筆者の知人の情報技術に関係のない会社員や学生 5 名，筆者が所属するセキュリティ製品会社の社員 4 名，LINE の Open Chat 機能で募集した実際のセキュリティ担当者の 4 名の計 13 名が実験に参加した（表 19）．ソーシャルメディア上での呼びかけの様子を図 15 に示す.

また，日本プライバシー認証機構の実施するセキュリティに関する講習会や，東京商工会議所で実施された人材育成に関する講習会で本実験に関するチラシの配布を実施してもらった（図 16）．しかしながら，チラシによる応募者は予備実験の検証の段階では集まらず，本実験に参加してもらう形をとった.

実験は 2 つの段階に分けて行われた．第 1 段階では，筆者が所属するセキュリティ製品会社の社員 4 名と情報技術に関係のない会社員や学生 1 名の参加者（ID-1 から 5）による実験を行い，その結果を分析した.

第 2 段階では，37 問の選択形式の問題と正誤問題を新たに追加した．実験は，情報技術に関係のない会社員や学生 4 名と，SNS で募集した実際のセキュリティ担当者 4 名の参加者（ID-6 から 13）により実施された． ここで新たに追加された正誤問題については，第

5.2 章の分析では用いていないため，第 6 部に詳細を記載する．

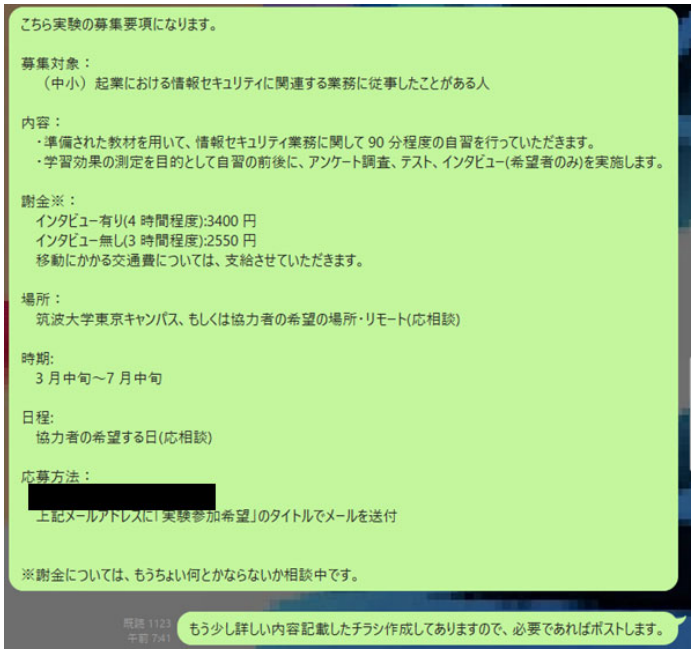


図 16　ソーシャルメディア上での声掛けの様子

Figure 16 Recruitment on social media(Line Open Chat)

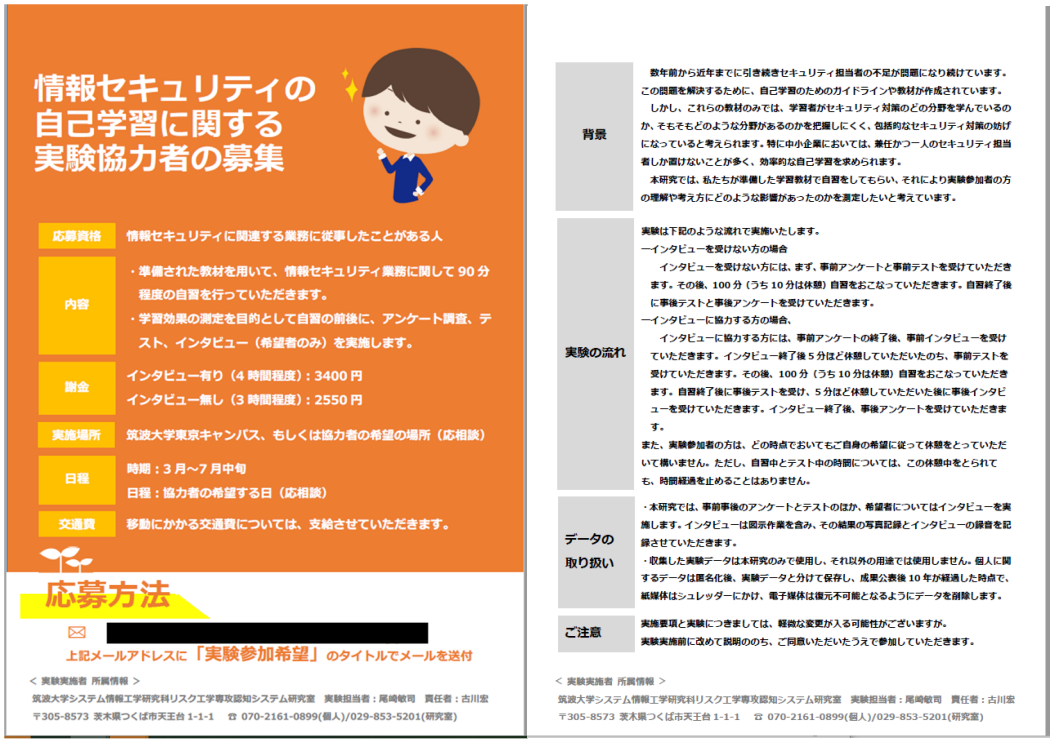


図 17　予備実験時に配布した実験参加者募集のチラシ

Figure 17 Flyer for recruiting experiment participants

表 19　実験参加者の情報

Table 19　Profile of Participants

ID	セキュリティ関連業務の経験	年齢	段階	企業規模	条件	実施方法
1	1 年	20 代	1	300–1000 人	統制群	対面
2	1 年	20 代	1	300–1000 人	実験群	対面
3	1 年	20 代	1	300–1000 人	統制群	遠隔
4	1 年	20 代	1	300–1000 人	実験群	遠隔
5	経験なし	20 代	1	n/a	実験群	対面
6	経験なし	20 代	2	n/a	統制群	遠隔
7	経験なし	20 代	2	n/a	統制群	対面
8	経験なし	20 代	2	n/a	実験群	対面
9	経験なし	20 代	2	n/a	実験群	遠隔
10	5–10 年	40 代	2	100–300 人	統制群	遠隔
11	5–10 年	30 代	2	50–100 人	実験群	遠隔
12	3–5 年	30 代	2	1000– 人	実験群	遠隔
13	3–5 年	20 代	2	50–100 人	統制群	遠隔

5.2.3.2. 実験の流れ

予備実験では，参加者は 2 つのグループに分けられ，統制群の参加者は，情報セキュリティ対策に関する標準的な教材として「中小企業の情報セキュリティ対策ガイドライン第 3 版」と CSF についての説明補助教材を用いて学習を行い,実験群の参加者は,改良された教材を用いて学習を行った． 自己学習の前後で，学習の効果を確認するためのテストと半構造化インタビューを実施して，自己学習の前後でのテストの得点の変化とメンタルモデルの変化を調査した（図 17）.実験は，対面と遠隔の 2 つの方式で実施された.

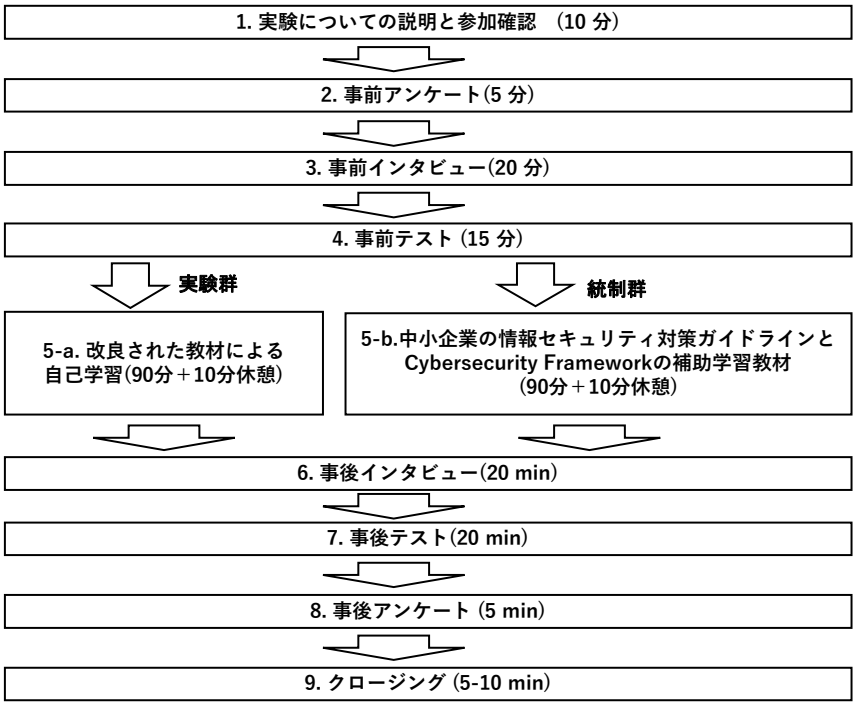


図 18　実験の流れ

Figure 18 Experiment Design

5.2.3.2.1.　事前・事後のインタビュー

インタビューは学習者の情報セキュリティ対策に対するメンタルモデルについて導き出すことを目的に実施しており，自己学習前と自己学習後のメンタルモデルを比較するために，自己学習前と自己学習後の 2 度，同じ内容でインタビューを行った．それぞれ図 17 では，事前，事後と記載されている．

インタビューは，シート上に置かれた付箋を用いて，セキュリティ対策の構成要素を列挙し整理するという作業を通して聞き取りを行う半構造化形式で行われた．この作業では，実験参加者は以下の手順で作業を実施した．

1）セキュリティ対策の要素を列挙する．
2）各構成要素のグループに分け名づけを行う．
3）名付けたグループについて,各グループがどのように連携して，情報セキュリティ対策を構成しているのか説明を行う．

作業が止まった場合には，事前に決めた声掛けを行うことで，作業を促した．自己学習後のインタビューでは，参加者の繰り返しの作業を避ける目的で，自己学習前のインタビューで作成した付箋の再利用を認めた．

この作業の結果は画像として保存され，インタビュー中の発言も録音された．インタビュースクリプトを表 20 に示す．

遠隔方式でのインタビューでは，実際の付箋紙の台紙ではなく，画面共有が行えるオン

ライン作図ソフト Cacoo [81]を使って作業を実施した．

表 20　インタビュースクリプト

Table 20　Interview script.

	用途
1．リストの作成	あなたが企業におけるセキュリティ対策に必要だと思っていることや要素，セキュリティ対策の達成のために必要だと思っている手段・手法は何ですか？それぞれの要素ごとに付箋に書き出して台紙上に張ってください．まず，5 分ほど時間を取って実施してください．
作業が止まった場合の呼びかけ例	間違えても問題ありませんので思いつくことを何でも書いていただいて大丈夫です．技術的なものでも，精神的なものでも構いません．
2-1．分類	それらの要素は互いにどのように関係していて，どのようなグルーピングが可能でしょうか？
2-2．名づけ	各グループに名前を付けるとしたらどのような名前でしょうか？ご記入お願いします．
作業が止まった場合の呼びかけ例	1．ご自分の好きな基準で分けて大丈夫ですよ． 2．一旦，仮で名付けていただいて後で修正していただくのでも大丈夫ですよ．
3．グループ間の関係性の説明	全体として各グループがどのようにセキュリティ対策を構成しているのかを台紙上に書き込みながら説明してください．説明中思いついたことがあれば，新たな付箋を使って要素を追加しても構いません．
作業が止まった場合の呼びかけ例	・まとめていただいたグループ間ではどのような関係がありますでしょうか？ ・グルーピングをしていくなかで新たに必要なものは見つかりましたでしょうか？

5.2.3.2.2.　テストの実施方法

テストは，学習効果を測ることを目的としており，実際のセキュリティ対策に関連する 30 問の正誤問題とともに，回答に対する確信の度合いを 5 段階で尋ねた．この回答に対する確信の度合いを，本研究では確信度と呼称する．

確信度を回答させたのは，テストで設定した正誤問題の内容は難しいものではなく類推で答えを導き出すことも可能であるためである．問題の難易度を高く設定しなかった理由としては，実践では，詳細な知識よりも基本的な理解に基づく類推や判断が重要になると考えたためである．

確信度については，実際のビジネス環境を想定して定義づけを行った．本研究では，最も確信がある場合には，「業務上その質問を受けた場合に，迷うことなくその場で答えることができる」と定義し，最も確信がない場合には，「業務上その質問を受けた場合に，その場で答えず質問を持ち帰り検討するが調べるのに時間が掛かる」と定義した．各段階については表 21 に示す．

さらに第二段階の実験では，30 問の正誤問題に加えて，あるセキュリティ対策がフレームワークコアのどの機能に貢献しているかを問う多肢選択問題を 37 問分用意した．これは，ある情報セキュリティ対策を提示して，それが，5 つの機能（識別，防御，検知，対応，復旧）のうちどれに貢献するものか，1 つまたは 2 つを選択する質問である．第一段階の実験が終了した段階で，テストの得点において実験群と統制群で差が出ないことが予測されたため正誤問題に問題の追加を行い，さらに，情報セキュリティ対策とフレームワークコアの関係性についての理解というより踏み込んだ観点での設問を，正誤形式よりも

差が出やすい多肢選択式で追加した．ただし，第 5.2 章では追加の正誤問題についてはサンプル数の少なさからサンプルサイズの推定に利用できないと考えられたため解析の対象としなかった．テスト実施時のスクリプトを表 22 に，予備実験の分析に用いた 30 問の正誤問題を表 23 に，選択問題を表 24 に記載する．

表 21　確信度の定義

Table 21　Definition of the degree of confidence

確信度	表現	今回のテストでの目安
5	強い確信がある	職場において，あなたがセキュリティ担当者の立場でその質問を受けた場合に，全くの迷いなくその場で応えることが出来る．
4	確信がある	職場において，あなたがセキュリティ担当者の立場でその質問を受けた場合に，多少の迷いや不安が生じるが，最終的には資料を確認することなくその場で回答を行うことが出来る．
3	やや確信がある	職場において，あなたがセキュリティ担当者の立場でその質問を受けた場合に，その場で推測して答えることが出来るが，正式な回答は後程資料を確認してから行う．
2	確信がない	職場において，あなたがセキュリティ担当者の立場でその質問を受けた場合に，その場では答えずに質問を持ち帰り，資料を確認した後に回答する．しかし，心当たりはあるため調査にそれほど時間はかからない．
1	全く確信がない	職場において，あなたがセキュリティ担当者の立場でその質問を受けた場合に，その場では答えずに質問を持ち帰り，資料を確認した後に回答する．このとき，何も心当たりを持っていないため調査に時間がかかる．

表 22　テストのスクリプト

Table 22　Script for test section

	用途
テスト開始時	これから事前テストを開始します．時間は 20 分です． このテスト自体は現在の理解度を把握するためのものです。あまり気を張らずに受けていただければと思います．
延長の確認	時間ですが，最後まで解けましたでしょうか？ もし終了していないようでしたら，最大 10 分延長することが可能です．
テスト終了時	では，テストを終了してください．

表 23　正誤問題一覧

Table 23　Ture False Questions in Test

	設問	正答
	自己学習前，自己学習後で共通する 30 問	
1	個人情報漏洩の場合，通常システム自体が停止するような攻撃は受けないため，社内情報システムの運営に影響を与えることはない．	×
2	内部班による情報漏洩は従業員のモラルが原因なので，経営者が責任を取る必要はない．	×
3	セキュリティ事故（情報漏洩，改ざん消失，機能低下など）の影響は，顧客と自分の会社のみでなく，取引会社などの関係者にも影響を与える．	○
4	個人情報の漏洩により禁固刑を受ける可能性がある．	○
5	セキュリティ対策は IT 担当者の課題なので，経営者がセキュリティ対策について意思決定する必要はない．	×

6	委託先のセキュリティについて管理責任を問われることがあるのでその点にも注意を払う必要がある.	○
7	経営者は，社外の業務上の関係者に，適切に自社のセキュリティに対する取り組みやセキュリティ事故発生時の対応を説明できるようにする必要がある.	○
8	担当者を任命しているので，経営者が情報セキュリティに関する組織全体の対応方針を決める必要はない.	×
9	平時は業務を優先する必要があるため，情報セキュリティ対策のための資源（予算と人材）を確保する必要はない	×
10	経営者として，担当者に対して必要と考えられる対策を検討させて，その実行を指示する必要がある.	○
11	脅威の動向に合わせて，情報セキュリティ対策に関する事柄を随時見直す必要がある.	○
12	業務委託や外部サービスを用いる場合に，規約等で情報セキュリティ対策が定まっていることが多いため，担当者に指示をだしてまで責任範囲を意識した選定を行う必要はない.	×
13	実際にインシデントが発生した場合には，その場その場での判断が重要になるため，緊急時の連絡先や被害発生時の対処について準備しておく必要はない.	×
14	社内の人間に使用されても問題ないので，PC のロック機能は利用していなくても問題はない.	×
15	重要情報をメールで送るときにも，本文中に情報を記載したほうが良い.	×
16	重要情報を送付する際には，宛先にミスがないように複数人でのダブルチェックを実施したほうが良い.	○
17	情報管理の大切さなどを定期的に説明する機会を持つ必要がある.	○
18	利害関係者については契約に記載されているので，改めて彼らのセキュリティ上の役割と責任を確認する必要はない.	×
19	情報管理の大切さについて話をする際には，パソコンなどの IT 機器やソフトウェアの取り扱いについて言及するだけで良い.	×
20	情報資産の整理は，機密性・完全性・可用性の観点で実施される	○
21	完全性が損なわれたということは，その情報資産が適切に扱われておらず，改ざんや破損された可能性があることを意味する.	○
22	可用性が損なわれた場合に，業務影響がでることはない.	×
23	リスクは，資産そのものの（もしくは問題が発生した場合の）重要度とその被害が発生する可能性の２つの要素で算定される.	○
24	リスクへの対応には，低減，回避，転移３つの考え方がある.	×
25	リスクの転移とは，自社よりも有効な対策を行っている（もしくは補償能力のある）サービスを利用するなどして，自社のリスクを代替してもらうことである.	○
26	パソコンにアンチウィルスソフトをインストールする行動は，リスクへの対応のうち「回避」に該当する.	×
27	通常時でもセキュリティインシデント発生時でも，経営者や従業員それぞれの役割は変わることはない.	×
28	情報セキュリティ対策ポリシーをチェックする際には，対策を実施できていないことをとがめることが目的ではないことを周知するのが望ましい.	○
29	現場の業務との整合性が取れない場合には，必要に応じてポリシーを変更する必要がある.	○
30	新たな情報セキュリティ脅威や，社内システムの変化に合わせてポリシーを変更する必要があ	○

	る.	

表 24　選択問題一覧

Table 24　multiple-choice questions in Test

設問		機能
2. Cybersecurity Framework のフレームワークコアの観点では，「中小企業のセキュリティ対策」で紹介されている情報セキュリティ 5 か条は，それぞれ何を目的とした対策でしょうか？　一つ選んで選択してください．また，それぞれの回答に対する確信度を記入してください.		
1	OS やソフトウェアは常に最新の状態にする	PR
2	ウイルス対策ソフトを導入してウイルス定義ファイルを最新にする	DE
3	パスワードは破られにくい，長く複雑なものを使う	PR
4	重要情報に対する適切なアクセス制限を行う	PR
5	新たな脅威や攻撃の手口を知り，社内共有する仕組みがある	PR
6	電子メールの添付ファイルや URL リンクを介したウィルス感染に気を付ける	PR
7	電子メールや FAX の宛先の送信ミスを防ぐ取組を実施している	PR
8	重要情報は電子メールの本文には書かず，添付ファイルに書いてパスワードで保護するなど漏洩対策を行っている	PR
9	無線 LAN を安全に使うために適切な暗号化方式を設定するなどの対策をしている	PR
10	インターネットを介したウイルス感染や SNS への書き込みなどのトラブルへの対策をしている	PR
11	パソコンやサーバのウイルス感染，故障や誤操作による重要情報の消失に備えてバックアップを取得している	PR
12	紛失やとうなんを防止するため，重要情報が記載された書類や電子媒体は机上に放置せず，書庫などに安全に保管してる	PR
13	重要情報が記載された書類や電子媒体を持ち出す時は，盗難や紛失の対策をしている	PR
14	離席時にパソコン画面の覗き見や勝手な操作ができないようにする	PR
15	関係者以外の事務所への立ち入りを制限している	PR
16	退社時にノートパソコンや備品を施錠保管するなど盗難防止対策をしている	PR
17	事務所が無人になる時の施錠忘れ対策を実施している	PR
18	重要情報が記載された書類や重要なデータが保存された媒体を破棄する時は，復元できないようにしている	PR
19	従業員に守秘義務を理解してもらい，業務上知り得た情報を外部に漏らさないなどのルールを守らせている	ID, PR
20	従業員にセキュリティに関する教育や注意喚起を行っている	PR
21	個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしている	ID, PR
22	重要情報の授受を伴う取引先との契約書には，秘密保持条項を規定している	ID
23	クラウドサービスやウェブサイトの運用などで利用する外部サービスは，安全・信頼性を把握して選定している	ID
24	セキュリティ事故が発生した場合に備え，緊急時の体制整備や対応手順を作成するなど準備をしている	RC, RS
25	情報セキュリティ対策をルール化し，従業員に明示している	ID, PR

3. 下記の Cybersecurity Framework のフレームワークコアの観点では,「中小企業のセキュリティ対策」で紹介されているセキュリティサービス例と技術的対策例は,それぞれ何を目的とした対策でしょうか？		
3.1. サービス		
1	情報セキュリティコンサルテーション	ID, PR
2	情報セキュリティ教育サービス	PR
3	情報セキュリティ監査サービス	ID
4	脆弱性診断サービス	PR
5	デジタルフォレンジックサービス	RS
6	セキュリティ監査・運用サービス	DE
3.2. 具体的な対策		
1	① ネットワーク脅威対策	PR
2	② コンテンツセキュリティ対策	DE
3	③ アクセス管理	PR
4	④ システムセキュリティ管理	PR
5	⑤ 暗号化	PR
6	⑥ データの破棄	PR

5.2.3.2.3. 自己学習

自己学習においては，比較実験のため実験群と統制群で，異なる教材を用いて学習を行った．実験群と統制群を決める際には，事前テストの結果をもとに会社規模，業務経験の分布に極端な差がでないよう可能な限り注意した．

実験群では，5.1 章で作成した教材を用いて自己学習を実施し，統制群では,「中小企業の情報セキュリティ対策ガイドライン　第 3 版」と,「CSF についての補助学習教材」を用いて実験を行った.「CSF についての補助学習教材」の内容は，5.1 章で作成した教材の CSF についての説明に基づいている．本研究では，ユーザーインタフェースの違いによる学習効果やメンタルモデルへの影響を把握することを目的としているため，実験群と対象群に提供するインタフェース以外の文章情報を可能な限り一致させることを目的に追加の教材として提供した．

実験参加者にはすべての項目を読むように指示し，項目を一覧にしたチェックシートを渡して，学習時間内で読み残しがないように記入管理を実施してもらった．このチェックシートは，実験群と統制群で共通のものを使用した．これは，どちらの教材も文章情報は同じであり学習項目も同一のためである．

学習は，間に 10 分間の休憩を挿む 90 分間で実施されたが，学習者から時間が足りないという申告があった場合には，最大で 30 分間学習時間を延長した．自己学習セクションを実施する際のスクリプトを表 25 に記載する．

表 25　自己学習のスクリプト

Table 25　Script for self-learning section

	用途
自習開始時	これから自習用の教材を用いて自習を進めていただきます. 教材は、NISC のサイバーセキュリティフレームワークと IPA から発行されている中小企業のセキュリティ対策ガイドラインがもとになっています.
配布資料の確認確（実験群）	まず，URL（もしくはアプリ）が，開けることを確認してください. 平板画面の中央部の目次の項目にマウスを置き矢印が表示されることを確認してください. 学習を進める際には，お渡ししたチェックシートに読み終わり次第チェックを入れながら学習を進めてください.
配布資料の確認確（統制群）	まず，PDF が 2 つあり開けることを確認してください．PDF の一つは，中小企業の情報セキュリティ対策ガイドライン，もう一つは，フレームワークコア説明資料 と表題がついていることを確認してください. 学習を進める際には，お渡ししたチェックシートに読み終わり次第チェックを入れながら学習を進めてください.
延長の確認	時間ですが，最後まで読み切れましたでしょうか？ もし終了していないようでしたら，最大 30 分延長することが可能です.
学習終了時	では，自己学習を終了してください.

5.2.3.2.4.　事前・事後のアンケート

事前アンケートは参加者のプロファイルについて把握するために実施され，事後アンケートは，事前知識についての確認と実験のクロージングを目的として実施された.

事前アンケートの内容は，実験群と統制群を均等に振り分ける際に参考にされた.

表 26　アンケート項目

Table 26　Questions and answer options of pre- and post- questionnaires

質問	選択肢
事前アンケート	
あなたの所属する会社の業種をお答えください	日本標準産業分類に基づいた選択肢から選択
あなたの所属する会社の従業員数をお答えください.	1-5/ 5-20/ 20-50/ 50-100/ 100-300/ 300-1000/ 1000 人　以上
あなたの現在の業務についてお答えください	セキュリティの専任担当／セキュリティの担当とIT業務の兼任／セキュリティの担当とIT業務以外の業務の兼任
セキュリティ担当業務としての業務経験年数をお答えください	1 年未満/ 1-2/ 3-5/ 6-10/ 10 年以上
あなた以外に，情報セキュリティの担当者はいますか	いる（　）人　／いない
1 週間あたりどのくらいの時間自習を行っていますか	1 週間あたり　1 時間未満／1～7 時間／7 時間～14 時間／それ以上
そのうち何割程度が情報セキュリティに関連していますか	ほとんど関係ない／少し関係がある／半分程度環形がある／大体が関係している／ほとんどが関連している

セキュリティ対策を検討・実施する際に何を参考にしているか教えてください	自由記入
事後アンケート	
セキュリティ対策について，今後どのような分野を学習したいと考えていますか	自由記入
実験実施前から，IPA の発行している「中小企業の情報セキュリティ対策ガイドライン」を知っていましたか	利用したことがある／読んだことがある／名前は知っている／知らない
実験実施前から，米国国立標準研究所（NIST）の発行している「重要インフラのサイバーセキュリティ対策」通称サイバーセキュリティフレームワークを知っていましたか	利用したことがある／読んだことがある／名前は知っている／知らない
今回，2 パターンの教材を用いて実験を行っています．これらの双方の教材について提供を希望しますか？	はい／いいえ
今回実施した事前テストと事後テストのあなた自身の結果について提供を希望しますか？	はい／いいえ
実験全体を通してお気づきの点，気になった点がございましたらご記入ください	自由記入

5.2.3.2.5. 研究倫理

この実験は，筑波大学工学部情報システム学科の研究倫理委員会で承認された．実験参加者には，実験中に使用される ID が割り当てられ収集されたデータは ID に基づいて管理された．実験参加者は，研究に参加する前に研究の目的，実験中に参加者が行うこと，収集されたデータの取り扱いについて説明を受け，説明内容について記載された同意書に署名を行った．この際，同意の取り消し方についても説明が行われた．署名された同意書は別個に保管され，実在の人物とのリンクを避けるため，実験の分析に用いている ID についての情報は含まれていない．報酬については，筑波大学の基準に従い 3400 円を支払った．インタビュー実施前，テスト実施前，自己学習の開始前に，数分から数十分の休憩時間を設け，さらに，実験参加者の求めに従い，必要に応じて実験を休止して休息の時間を設けた．

5.2.4. インタビュー結果とその分析

インタビューについては，実験結果に対してコーディングを行い学習者のメンタルモデルが読み取れるか確認を行った．また，テストの結果については，検定と効果量の計算を行い，テスト設計の妥当性と適切なサンプルサイズについて検討する．

5.2.4.1 インタビューの分析

インタビューの分析では，作業の結果得られた図を整理したのち，項目に対してコーディングを実施した．この際，録音した音声データを書き起こしたものも利用している．

インタビュー結果の例として，図 18 に ID-6 の実験参加者の事前インタビューのタスク

の実施結果を示す

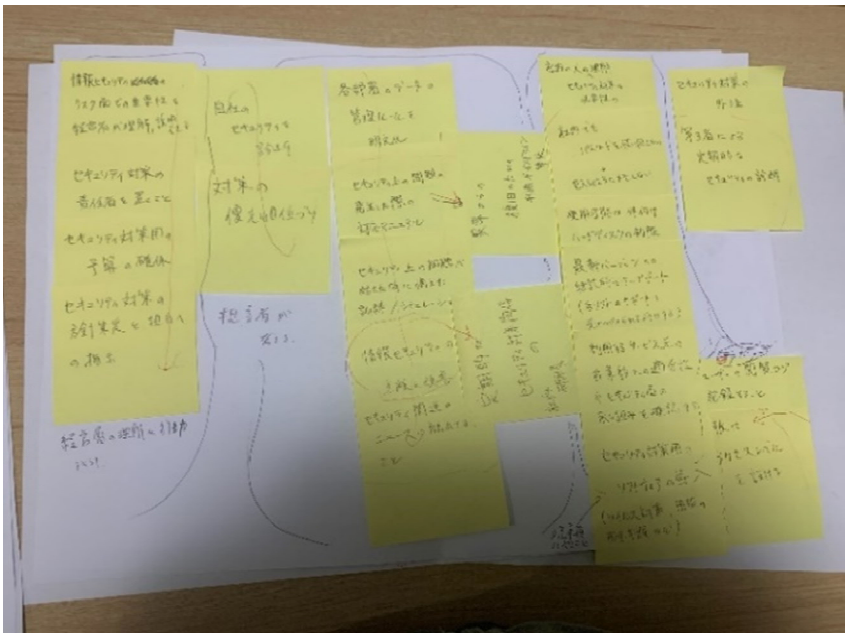


図 19　ID-6 の実験参加者の自己学習前のインタビュータスクの実施結果

Figure 19 Task results in interview of ID-6 before self-learning

5.2.4.1.1.　図の項目の整理

得られた実験結果について，名付けてもらったグループをグループ，個々の付箋はセキュリティ項目として定義して，表形式で整理をした．ID-6 の実験参加者の整理結果を表 27 に示す．この際，整理の簡略化のため，グループ間の関係性についての説明については表中には含まなかったが，この情報については，音声データの書き起こしと共にコーディングを実施する際に利用された．

表 27　ID-6 の作業結果を表に整理

Table 27 Organize the results of the ID-6 task to a table

グループ	セキュリティ項目
経営層の理解と行動	情報セキュリティのリスク面での重要度を経営者が理解説明できる．
	セキュリティ対策の責任者をおくこと
	セキュリティ対策用の予算の確保
	セキュリティ対策の方針策定と担当者への指示
担当者が考える	自社のセキュリティ診断

	対策の優先順位づけ
	各部署のデータの管理ルールを明文化
	セキュリティ上の問題の発生した際の対応マニュアル
	セキュリティ上の問題が起きた時に備えた訓練／シミュレーション
	異常からの復旧のための手順ガイドライン策定
	情報セキュリティの点検と改善
	敵的なセキュリティ関係者の社内研修
	セキュリティ関連のニュースに触れておく
従業員がやること	社内の人のセキュリティ対策の必要性の理解
	社内でもパスワードを使いまわさない，見えるところにメモしない
	使用可能な外付けハードディスクの制限
	最新バージョンへの継続的なアップデート
	利用するサービス先の自業務との適合性やセキュリティの取り組みを確認する
	セキュリティ対策用のソフトウェアの導入
	ユーザーの閲覧ログを記録する
	情報にアクセスレベルを設ける．
N/A	セキュリティ対策の外注
	第三者による定期的なセキュリティ診断

5.2.4.1.2. 項目に対するコードディングの実施

得られた結果の粒度を揃えることを目的として，前目 5.2.4.1.1 で整理したセキュリティ項目に対するオープンコーディングを 2 名で実施した．この際，各セキュリティ項目の文脈を理解するために図上に記載された情報のほか音声データの書き起こしを合わせて利用した．

2 名によるコーディングの結果について各コードの項目の調整を行った後，Cohen's kappa が計算され，その結果は 0.68 となった．これは，Krippendorff ら [76]の基準に基づくと「かなりの一致」であり，Landis と Koch ら [77]の基準に基づいても「暫定的な結果」がある．異なった部分は議論により解消された．最終的に得られたコードを表 28 に示す．

表 28 予備実験におけるコーディング結果

Table 28 Coding results in preliminary experiments

コード	コード
リスク評価	ポリシーの見直しと改善
攻撃の調査	（セキュリティについての）訓練と気づき
関係者への情報共有	サードパーティのセキュリティ
対応計画（の作成）	脅威やセキュリティの知識の獲得
復旧計画（の作成）	要員と予算の確保（責任範囲の確定）
外部サービスによるセキュリティ	アカウント管理
セキュリティソフト導入	アクセス制御
データ漏洩ポリシー（の作成）	資産管理

（強固な）暗号化	リスク管理
データ復旧	リスクアセスメント
セキュリティ事故監視／異常監視	セキュリティポリシーの作成
ロギング	セキュリティ水準の確認
バージョンアップ管理	攻撃の軽減

5.2.4.1.3.　コーディング後の図形の分類

前目 5.2.4.1.2 で同じコードに割り当てられたセキュリティ項目は 1 つにまとめられたのち，セキュリティ対策を頂点とする階層構造で整理された．一つ目の層には参加者の定めたグループ名が記載され，2 層目にはセキュリティ対策についてのコードが記載されている．矢印などの記号については，そのまま残される．参加者 ID-6 の学習後の結果について整理したものを例として図 19 に示す．

整理された図におけるグループ間の構造と項目の数，時間経過や順序を表す矢印の有無，項目をまとめるグループ名に着目して，得られた結果を「未構造型」「時間軸型」「役割型」「フレームワーク型」の 4 つの型に分類した．まず，得られた図において，項目数が少なくグループが定義できないか，グループ数が 1 つしかないものを，構造化されていない未構造型として判別した．次に，時間経過や順序を表す矢印や番号付けが存在するか確認し，存在する場合には時間軸型と判別した．その後，グループ名に着目し，それらが時間経過に関連している場合には時間軸型，人の属性や立場や役割を表している場合には役割型，特定のセキュリティ関連のフレームワークに該当する名前である場合にはフレームワーク型として分類した．特に，フレームワーク型の場合には，インタビュー中にそのフレームワークに対する言及があるかも確認した．

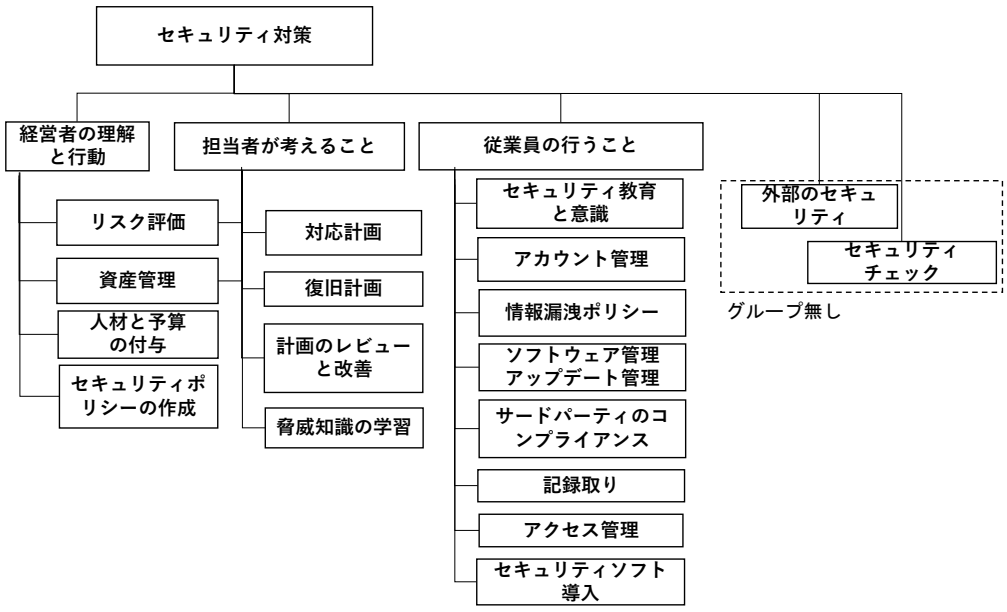


図 20　ID-6 の実験参加者の自己学習前の要素整理後の結果

Figure 20 Analysis results of the ID-6 before self-learning.

5.2.4.1.4.　インタビューに基づくメンタルモデルの分析

この予備実験では，前目の分類によって，学習者のメンタルモデルとして，「役割型」，「時間軸型」，「フレームワーク型」，「未構造型」の 4 つの型が確認された．この目では，これらの型について説明を行う．

役割型のメンタルモデルでは，セキュリティ項目は，誰がどの対策を行うかという観点で整理され，多くの場合，経営層，セキュリティ担当，その他の従業員という役割が登場する．時間軸型のメンタルモデルでは，セキュリティ項目は，どの段階で行われるべき対策かという観点で整理され，時間の経過を表現する矢印が記入されている．フレームワーク型では，セキュリティ項目は，既存のフレームワークに基づいて整理された．予備実験では，Cyber Kill Chain と CSF の 2 種類の枠組みが確認された．未構造型では，セキュリティ項目はグループとして整理されておらず，また要素の数も少ない傾向がみられた．

(1) 役割型のモデル

この型のメンタルモデルでは，誰が何を実施すべきかという観点から，セキュリティ対策は整理される．この型のモデルの例としては，先の図 19 が挙げられる．ID-6 は，対策を「経営者の理解と行動」，「担当者が考えること」，「従業員の行うこと」に分類した．この分類の中に，「経営者」，「担当者」，「従業員」という用語が含まれるため，役割に着目した役割型と判断した．

自己学習前のインタビューでは，参加者 ID-6 がこのモデルを適用していることを確認した．この時には，ID-6 は，「会社全体の取り組み」，「部署ごとの取り組み」，「セキュリティ担当者の取り組み」の 3 つのグループに分類している．

一方で，自己学習後のインタビューでは，ID-5，-6，-8，-9 の参加者が，この役割型のモデルを適用していることを確認した．同様に ID-6，-8，-9 は，グループ名に「経営者」，「情報セキュリティ担当者」，「従業員（個人）」という単語が現れ，これら 3 つの役割の視点からセキュリティ構成要素を構成しようとしたが，ID-5 は「経営者」と「従業員（個人）」の 2 つの視点しかなかった．

(2) 時間軸型のモデル

時間軸型のモデルでは，セキュリティ対策は段階や時間軸に沿って整理される．自己学習前のインタビューでは，参加者 ID-1，-2，-3，-7，-11，-13 がこの型のメンタルモデルを持っていた．この型の例として，図 21 に ID-3 の自己学習前の結果を示す．この型の作業結果には，流れや時間軸を示すために，矢印が書き込まれることが多かった．また，ID-1，-3，-11，-13 の作業結果では，時系列で並べるとループバックが生じている場合もあった．これは，セキュリティ対策にはプロセスの改善が必要なものもあるためだと考えられる．自己学習後のインタビューでも，ID-1，ID-7，ID-10 の参加者は，このモデルを使って関係性やグループ化を表現していた．

ID-1 の学習前のインタビューの結果（図 22）では，明確なグループ化はされず構成要素が時系列に沿って列挙されていただけであったが，明確に実行順序に従っていたため，時間軸型として扱うことにした．

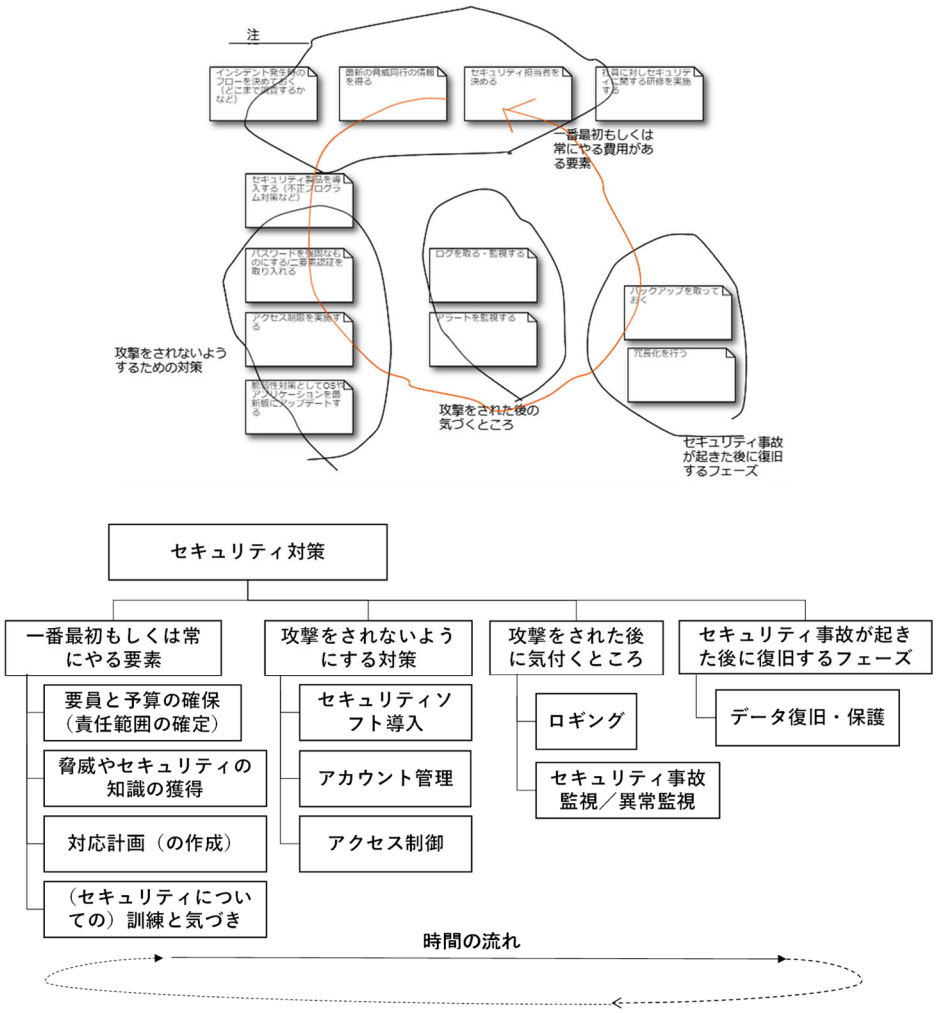


図 21　ID-3 の自己学習前の時間軸型のメンタルモデルの例

Figure 21 Timeline -based model (lower) and the task result (upper) of ID-3 before self-learning

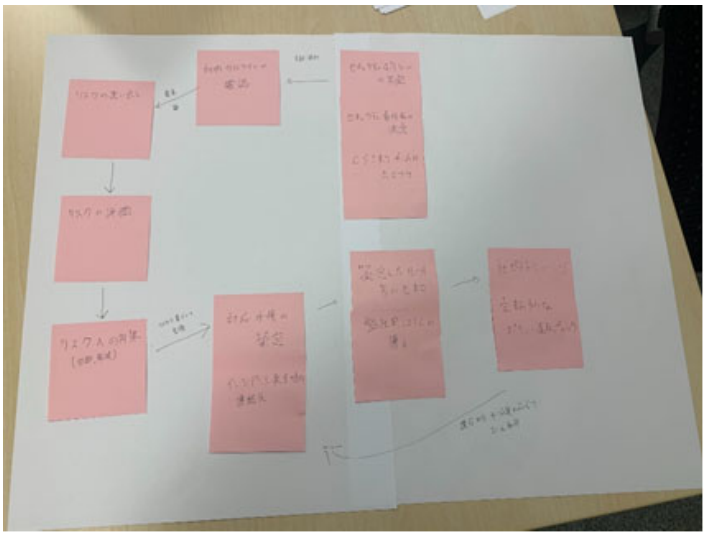


図 22　ID-1 の自己学習前の作業実施結果

Figure 22 Results of the ID-1s task before self-learning

(3) フレームワーク型

フレームワーク型では，特定の情報セキュリティに関する枠組みに基づいてグルーピングや整理を行われる．今回の予備実験では，フレームワーク型のメンタルモデルは 2 種類確認された．1 つは Cyber Kill Chain に基づいたもので自己学習前のインタビューで確認され，もう 1 つは CSF のフレームワークコアに基づいたもので自己学習後のインタビューで確認された．

Cyber Kill Chain 型

ID-4 の参加者は，自己学習前のインタビューで，Cyber Kill Chain に基づいて，グループの名づけを試みて，その関係を説明した．この参加者は，最初に「Cyber Kill Chain で要素を挙げます」と宣言して，リストアップ作業を始め，その後クルーピングを実施した．しかしながら，実際には Cyber Kill Chain よりも単純な分類となっていた．

本来，Cyber Kill Chain は，偵察，武器化，デリバリー，エクスプロイト，インストール，C&C，目的の実行の 7 つの段階に分けられるが，ID-4 の参加者は，これを 3 つのフェーズに再編し，「侵入防止」，「感染拡大防止」，「攻撃からの回復」と名前を変え，偵察と武器化が消えた分類を使用した（図 22）．

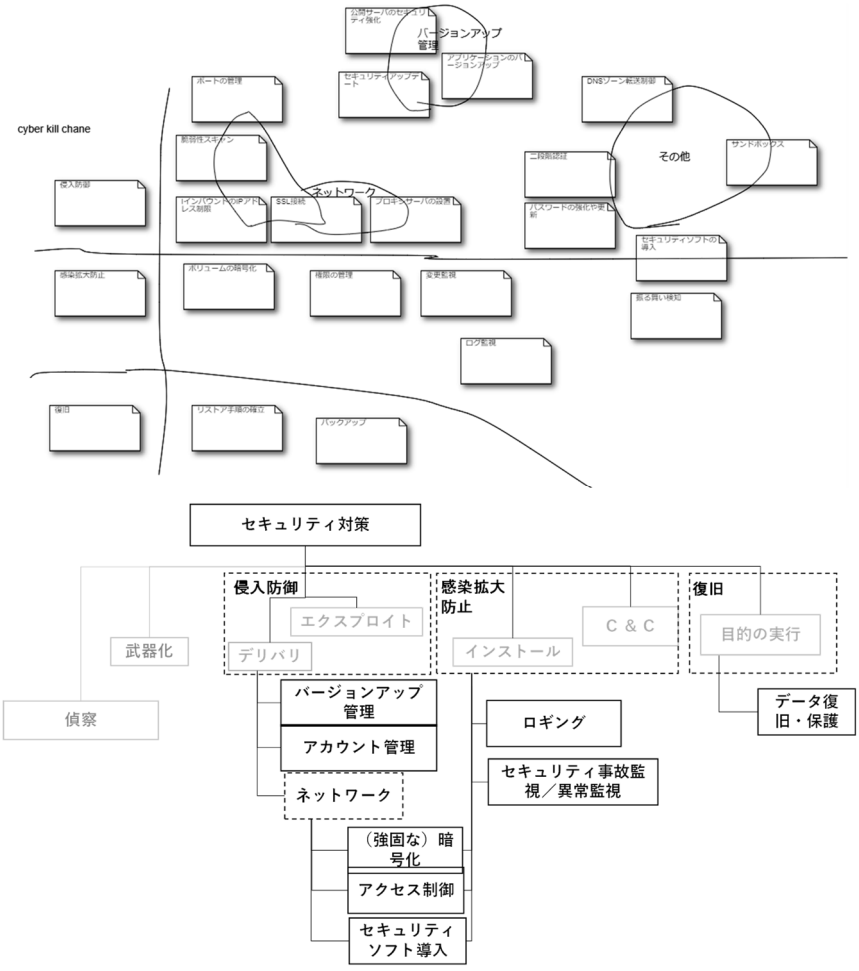


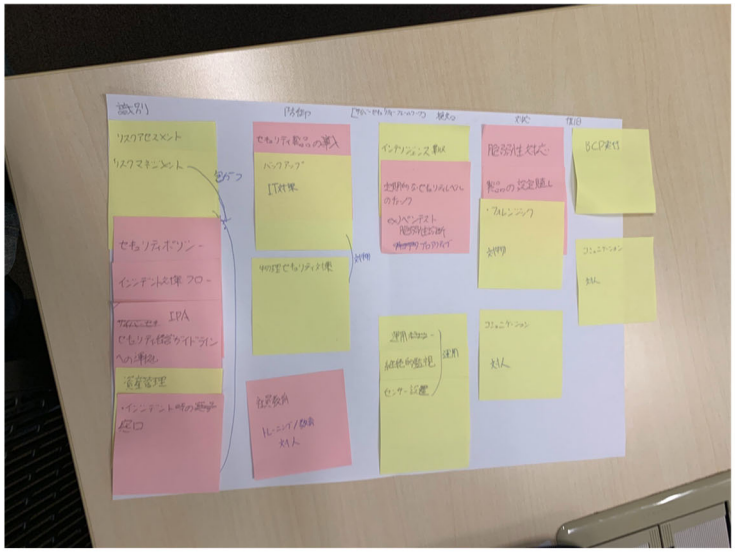
図 23　ID-4 の自己学習前の Cyber Kill Chain によるフレームワーク型のメンタルモデルの例

Figure 23 Framework-based model of Cyber Kill Chain (lower) and the task result (upper) of ID-4 before self-learning

CSF 型

ID-2，ID-3，ID-4，ID-11 の実験参加者は，自己学習後のインタビューで，CSF のフレームワークコアを使って項目をリストアップし，その関係を説明した．

参加者は，フレームワークコアがこの課題に使えることに言及し，先にグループを定義したのちに項目のリストアップを実施して，その後，自己学習前のインタビューで記述した項目についても組み合わせようとした．図 23 に ID-2 の自己学習後の CSF のフレームワーク型の例を示す．この参加者の例では，赤い付箋は，自己学習前のインタビューで作成されたもので，自己学習後のインタビューにおいてグループ分けの段階で CSF の枠組みの中に組み込まれた．



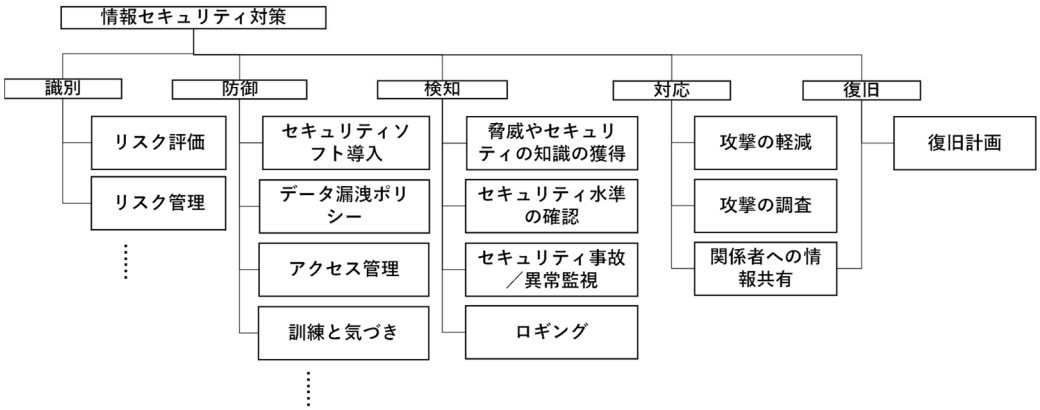
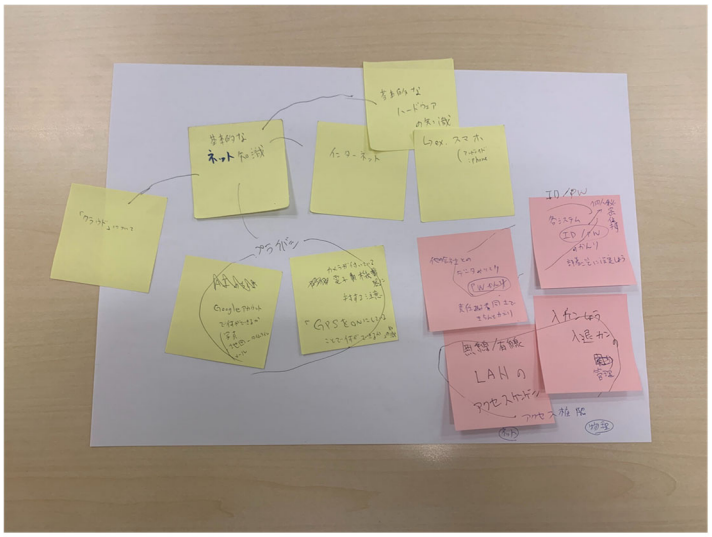


図 24　ID-2 の自己学習後の Cybersecurity Framework に基づいたフレームワーク型のメンタルモデルの例

Figure 24 Framework based model of the framework core (lower) and the task result (upper) of ID-2 after self-learning

(4) 未構造型

整理後にグループが存在しないか，1 つのグループのみが存在する場合，未構造型として判別した．情報セキュリティに関する教育を受けていない参加者（参加者 ID-5，ID-8，ID-9）は，セキュリティ対策の項目をうまく列挙できなかったり，整理ができなかったり，グルーピングは部分的にできても，体系的なグルーピングに失敗した結果，この型に分類された．このモデルは，自己学習前のインタビューセッションでのみ確認された．図 24 に ID-5 の学習前の結果を示す．この例では，赤色の付箋は技術的な部分を，黄色の付箋は知識的な部分を意味しており，いくつか項目がリストアップされているが，コーディングの結果，3 つのコードに集約されてしまい，未構造型として判定された．



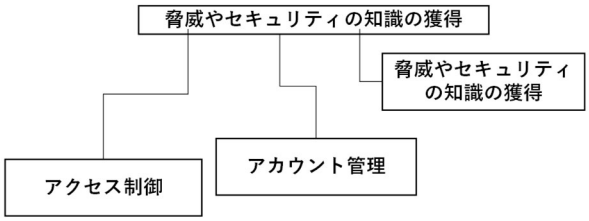


図 25　ID-5 の自己学習前の未構造型のメンタルモデルの例

Figure 25 Unstructured model (lower) and the task result (upper) of ID-5 before self-learning

(5) 自己学習によるメンタルモデルの型の変化

自己学習前と後の実験参加者のメンタルモデルの型について表 29 に示す．自己学習の前後でメンタルモデルが変化する事例が確認された．

セキュリティの業務経験のある参加者では，一部の実験参加者（ID2，3，4，11）が，他の型から CSF のフレームワーク型に移行し，セキュリティ教育を受けていないグループの参加者の一部（参加者 ID5，8，9）では，未構造型から役割型に変化した例を確認した．未構造型のモデルを持っていた参加者も，学習によって構造化されたメンタルモデルを獲得するほか，すでに特定の型で構造化されたメンタルモデルを持っている場合でも学習により他の型を獲得できることが確認された．

表 29　予備実験におけるメンタルモデルの型の変化

Table 29　Changes of the type of mental model in preliminary experiments

メンタルモデル	事前インタビュー時	事後インタビュー時
フレームワーク CSF		2,3,4,11
フレームワーク Cyber Kill Chain	4	
時間軸	1,2,3,7,10,11,13	1,7,10,13
役割	6,12	5,6,8,9,12
未構造	5,8,9	

この予備実験では統制群と実験群で学習前に確認されたメンタルモデルの型に偏りが発生してしまっているため，実験群と統制群の間での適切な比較は難しいと考えられる．実験群では，学習後に CSF のフレームワークコア型に移行した例が 3 例確認されたが，統制群では 1 例であったため，インタフェースの違いにより学習後の型の変化にも違い発生している可能性があると考えらえる（表 30）.

表 30　予備実験における実験参加者のメンタルモデルの型

Table 30　The type of mental models of each participant in the preliminary experiment

メンタル モデルの型	統制群		実験群	
	学習前	学習後	学習前	学習後
フレームワーク型　CSF		3		2,4,11
フレームワーク型 Cyber Kill Chain			4	
役割型	1,3,7,10,13	1,7,10,13		
時間軸型	6	6	12	5,8,9,12
未構造型			5,8,9	

5.2.4.2. テストの分析

テストの得点では，正解の場合は 1 点を加点して，不正解の場合は 0 点とした．一方，確信度の計算では，問題に正解した場合は，回答の確信度を合計に加え，不正解の場合は，回答の確信度分を減算した．誤った対策を信じることで，誤った行動につながる可能性があるため，ペナルティとして減算を行っている.

第 2 段階に追加された 37 問の選択問題の場合，テストの得点については，完全に正しい答えには 2 点，部分的に正しい答えには 1 点，誤った答えには 0 点を与えた．確信度の計算では，部分的に正解した場合でも完全に正答した場合でも確信度分を加点し，誤答だった場合は，確信度分の減点を行った．実験参加者の得点と確信度について，表 31 に示す.

表 31　テストの得点と確信度

Table 31　Test score and degree of confidence

	正誤問題 30 問				選択問題　37 問(第二期)	
ID	自己学習前		自己学習後		自己学習後	
	得点	確信度	得点	確信度	得点	確信度
1	25	87	30	138	N/A	N/A
2	29	110	29	133	N/A	N/A
3	27	113	28	134	N/A	N/A
4	29	117	28	130	N/A	N/A
5	28	129	28	130	N/A	N/A
6	27	66	27	108	32	17
7	29	90	30	108	30	23
8	27	68	30	144	46	78

9		27	115	29	128	46	103
10		25	100	26	110	17	-14
11		27	73	30	122	48	82
12		27	105	29	136	45	93
13		28	90	29	132	36	40
平均	実験	27.7	107.8	28.6	131.9	46**	90.5**
	統制	26.8	89	28.8	121.6	31**	20**
	全体	27.3*	98.4*	28.7*	126.7*	38.5	55.25
標準偏差	実験	1.60	15.54	1.63	14.39	8.22	22.55
	統制	0.83	25.00	0.89	7.53	1.26	11.28
	全体	1.32	20.05	1.25	11.75	10.82	42.12

テストの得点と確信度について，自己学習の前と後で対応のある t 検定を行ったところ，自己学習の前後でテストの得点と確信度が有意に向上した（P-value = 0.042 < 0.05;表 31 の*）．したがって，用意した問題セットで学習の効果は確認可能であると考えられる．

実験群と統制群の間で， t-検定を行ったところ，あるセキュリティ対策がどのセキュリティの機能に寄与しているかを問う選択問題では，サンプル数が少ないながら有意な差が示された（P-value = 0.002 < 0.05; 表 31 の**）．これにより，少なくとも選択問題では，有意差が確認できる可能性があることが確認できた．

天井効果について平均値と標準偏差の和で確認したところ，この予備実験においては確認されなかった．

また効果量Δについても計算を行った．その効果量から検出力を 80%として有効な実験に最低限必要なサンプルサイズを推定したところ，25 名程度の参加者が必要であることが確認された（表 32）．

表 32　効果量Δと推定サンプルサイズ

Table 32　Effect size Δ and estimated sample size

	予備実験 サンプルサイズ	事後実験群 平均	事後統制群 平均	効果量Δ	推定 サンプルサイズ
正誤問題 30 問　得点	13	29	28.3	0.82	19～20
正誤問題 30 問　確信度	13	131.9	121.6	0.71	25～26
選択問 37 問　得点	8	46	31	2.1	N/A
選択問題 37 問　確信度	8	90.5	20	3.2	N/A

5.2.5.　議論と制限

5.2.5.1. 統計学的な観点での制限

この予備実験は年齢や地域に偏りがあり，サンプルサイズも小さかった．そのため，本研究の結論は，テストとインタビューの分析結果の両方において，限られた環境下でしか再現・適用できない可能性がある．特に，インタビューデータは自己申告による質的なも

のであり，コーディングの手法を用いて分析されているため，他の研究者が異なる結論を出す可能性がある．実験参加者の募集についても，公募により参加したのは第二段階のセキュリティ業務に経験のある 4 名のみであり，それ以外の参加者は筆者の知人によるものであり，この点でも偏りが存在する可能性がある．

5.2.5.2. インタビューの制限

観察されたメンタルモデル，つまり作業結果やそこから整理された結果は，もともと実験参加者の中に存在したものではなくインタビュー中により導出されたものである．これは情報セキュリティに関する教育を受けていない，あるいは業務経験のない参加者を対象としたインタビューでは特に顕著である．インタビューでは，事前にスクリプトを決めて必要以上に実験参加者の考えや作業に介入しないようにした．

また，インタビューのプロトコルの設定が十分ではなかったため，ID-1 のように付箋同士の説明は行ってもグループの作成を行わない場合があった．本実験ではこのような例を避けるために，グループの作成については必ず行ってもらうようにする．

5.2.5.3. 質的コーディングの制限

この予備実験のオープンコーディングは，2 名で行われた．両名とも CSF とその翻訳版である「重要インフラのサイバーセキュリティを改善するためのフレームワーク」と「中小企業の情報セキュリティ対策ガイドライン」の第 2 版及び第 3 版について学習済みの状態であり，5.1 章において，「中小企業の情報セキュリティ対策ガイドライン　第 3 版」に対して，CSF のフレームワークコアによるテンプレートコーディングを行っている．そのため，両名ともコードについて検討する際にフレームワークコアに影響を受けて定義した可能性がある．

5.2.5.4. メンタルモデルの分類についての制限

この予備実験ではコーディングの対象として，付箋に記載された情報セキュリティ対策の要素のみを対象としていた．それにより，粒度を揃えることで，上手く体系付けを行えていない未構造型について確認することができた．また，矢印の有無や番号の有無により実行順序を示す時間軸型や，利用するフレームワークに言及がある場合のフレームワーク型については形式的に分類できた．

しかしながら，それ以外の場合では，グループ名を参照し分類に利用しているため，主観性が含まれるものとなっている．そこで，実際の情報セキュリティ担当者に対する実験では，グループ名に対してもコーディングを行い，グループのコードを定義して体系的に分類することとした．

5.2.5.5. テストの制限

事前テストは，参加者の自己学習中の学習戦略に影響を与えた可能性がある．特定の範囲にのみ集中して学習が行われるのを避けるため，チェックリストを準備して全分野について学習を進めてもらうように留意した．

また，第 2 段階で新たに 37 問を追加したが，テストの実施時間については変更を行わなかったため，第 2 段階のグループの正誤問題の得点に影響が出た可能性がある．しかしながら，第 1 段階と第 2 段階で共通する 30 問の正誤問題の得点に有意な差が見られなかったため，この影響は限定的なものであると考えられる．すべての参加者が余裕をもってテストを終了していたため，本実験では正誤問題の数を増やすことにした．

5.2.5.6. メンタルモデルの型の変化についての議論

学習によるメンタルモデルの型の変化は，役割型とフレームワーク型（CSF 型）への変化のみが確認された．これは，「中小企業の情報セキュリティ対策ガイドライン　第 3 版」が役割に基づいた視点で書かれており，そこに CSF のフレームワークコアについての情報を追加したためであると考えられる．

また，情報セキュリティ業務経験者のみが CSF 型に変化しており，これは実験群，統制群に関わらず発生した．この事実は，情報セキュリティ対策の経験者であれば，フレームワークコアの存在を知ることでメンタルモデルの変更を試みることができるかもしれないことを示唆している．

一方で，情報セキュリティに関する知識のない参加者は未構造型から役割型のメンタルモデルへと移行した事例が多く確認された．これは，「中小企業の情報セキュリティ対策ガイドライン　第 3 版」が，経営者と担当者という役割の観点で章分けされているため，その影響を受けた可能性が考えられる．

フレームワーク型では，その枠組みを正しく利用できていない事例が確認された．例えば，ID-4 は Cyber Kill Chain に基づいたモデルを使おうとしたが，偵察と武器化について言及するのを忘れ，いくつかのステップを 1 つのグループに統合してしまい，本来の Cyber Kill Chain とは異なる構造になっていた．同様の問題は，CSF 型でも発生した．特に，自身で列挙した構成要素を機能やカテゴリに結びつけようとすると，本来 CSF で定義されているものと異なる分類になる場合があった．これは枠組みへの理解が不十分なことにより発生していると考えられ，繰り返しの学習によって改善する可能性があると考えられる．

5.2.5.7. テストの制限についての議論

サンプル数は少なかったが，実験群と統制群の間には，テストの得点の合計点と確信度の合計点について Welch の t-検定を用いて有意な差が検出された．したがって，どちらの

教材を使った学習においても一定の学習効果は表れていると考えられる．

統計的な有意性はないが，自己学習後，時間軸型であった参加者は，役割型やフレームワーク型の参加者に比べると得点が低い傾向が確認された．そのため，学習により身についたメンタルモデルの型が学習の効果に影響を与えている可能性があると考えられる．

5.3. 本部の結論

情報セキュリティ担当者の学習効率を高め，包括的で適切なメンタルモデルを導入するために，フレームワークコアとの関係を明示した教材を作成した．

その教材を用いて，情報セキュリティに関する体系的な教育を受けていないグループ，セキュリティ関連業務に約 1 年間従事したことのあるグループ，そして実際のセキュリティ担当者のグループを対象に，実験設計について確認するための予備実験を行った．

この実験では，インタビュー手順により実験参加者の情報セキュリティ対策に対するメンタルモデルについて描き出すことが可能であること，テスト内容において学習の前後で有意な差が確認されると期待される設計になっていること，統計的に有意な差がでるサンプルサイズについて見積もることを目的とした．

インタビューでは，自己学習により学習者のメンタルモデルがどのように変化するのかを確認することを目的として，情報セキュリティ対策の構成要素を整理，分析した．その結果，セキュリティ対策の捉え方として，大きく役割型，時間軸型，Cyber Kill Chain によるフレームワーク型，CSF によるフレームワーク型，そして未構造型があることを確認した．また，自己学習によってこれらの型は変化することが確認された．CSF によるフレームワーク型への変化は情報セキュリティ業務の経験者でしか確認できなかった．セキュリティの知識のない学習者に CSF のフレームワークコアに基づく型を浸透させるには，今回作成した教材のように単に関係性やつながりを示すだけではなく，資料の構造を大幅に変更し，よりフレームワークコアに基づいた構成を提供する必要があると考えられる．

また，実験の設計について検討するため，テストによって学習効率の向上が統計的に検出されるかどうかの推定も試みた．選択問題についてウェルチの t-検定を行ったところ，実験群と統制群の得点と確信度の間に統計的に有意な差が見られた．このことから，情報セキュリティ業務経験者のみを対象とした本実験でもテストを通して有意差が確認できることが期待される．また，天井効果の影響がないことが確認された．

今回の実験結果の効果量から必要なサンプルサイズを計算すると，統計的妥当性を得るためには約 25 名の参加が必要となることが確認された．

今後の研究では，今回の予備実験の結果を踏まえて，実験の設計を再検討し，約 25 名の情報セキュリティ担当者を対象に実験を行い，改良された教材により効率的な学習ができるようになったことを検証する．

6．改良後の教材の効果とメンタルモデルの学習効果への影響

この部では，改良後の教材の効果とメンタルモデルの学習効果への影響について述べる．これは，1.3 章の研究の流れの説明では，「5) 実験を行いその結果について分析する」に該当する．

6.1. 概要

第 6 部では，本実験として情報セキュリティ関連業務に 1 年以上携わっている実験参加者 26 名に，改良された教材を使ってインタビュー，テスト，調査を行った．実験の方法は，基本的に 5.2 章で実施した方法と同様である．

その結果，予備実験と同じように，役割型，時間軸型，フレームワーク型，未構造型のメンタルモデルの 4 つの基本的なメンタルモデルが観察された．しかし，今回の実験では，Cyber-kill chain に基づいたモデルは確認されず Cybersecurity Framework (CSF)に基づいた型（フレームワーク（CSF）型）のみ確認された．また，本実験では，2 種類の基本的なメンタルモデルが 1 つのモデルに統合された混合型のメンタルモデルのケースも 2 例確認され，例えば，ID-13 番の参加者は役割型に基づいた表現の上に実行順序や時間経過を表すような矢印を加えることで 2 つのモデルを組み合わせた表現を行った．

改良された教材を用いた実験群は，統制群に比べて自己学習後のテストの得点が有意に向上した．また，メンタルモデルの型で分類したグループについて，一元配置分散分析とボンフェローニ法による多重比較手順で有意差を確認したところ，フレームワーク型のグループは他の型のグループより有意に，質問に正しく自信を持って答えた．これにより教材を通して CSF によるフレームワーク型のメンタルモデルを身に着けさせるのが望ましいという示唆を得たと考えられる．また，実験群の学習者は学習後フレームワーク型に変化したものが統制群よりも多く，CSF のフレームワークコアを AH として改良した教材のほうが適切なメンタルモデルを身に着けさせより高い学習効果を上げていたと考えられる．ただし，実験群の学習者が統制群よりも多くフレームワーク型に変化したという点については，統計的に有意ではなかった．

6.2. 目的

この予備実験では，以下の 2 点を目的として，フレームワークコアを AH として改良を行った教材を用いて予備実験の結果を基に調整した実験を実施して，それぞれ検討を行った．

1．改善後のユーザーインタフェースが，学習時の学習者のメンタルモデルにどのような影響を与えるか
2．改良した自己学習用教材が，通常の教材と比べて高い学習効果を示しているか
3．メンタルモデルと学習効果の間に関係性が見られるか

6.3. 実験

6.3.1. 実験参加者の募集と分布

実験参加者の募集は，2020 年の 7 月ごろから予備実験での声掛けから継続して行われた．手法は予備実験と同じく，ソーシャルネットワークサイト上での声掛けと著者の知人を介しての募集を実施した．講習会での募集については，COVID-19 の影響により実質的に中断されているが，予備実験の頃から募集をかけていた関係で，講習会でのチラシ配布からの参加者が 3 名存在する．

ソーシャルネットワークサイトについては，予備実験でも利用した LINE Open Chat に加えて，Twitter の Direct Message での声掛けなどを実施した（図 25）．ソーシャルネットワークサービス上での声掛けでは，予備実験で用いたチラシを提供した（図 16：ただし，期間の情報は募集時期に合わせて更新している）．

アンケートの自由記述によると参加者の中には，特定の業務（ネットワーク監視やセキュリティプランニングなど）にしか関係していない人もいるが，ほとんどの人は複数の情報セキュリティ業務を担当していた．

ID-1 から 4 は予備実験の参加者であり，その実験結果を利用している．実験参加者の詳細な情報については，表 33 に記載する．表中の業務内容については，「システム（のセキュリティの）保守・運用」，「セキュリティ導入（支援）」，「システム監視」，「有事の対応」，「ポリシー作成運用・教育」の四つに大別して記載した（「システム監視」，「有事の対応」は同時に現れていたため，表 33 中では，「システム監視・対応」とまとめて記載されている）．これらの分類は，Cybersecurity Workforce Framework の Category（業務分野）に基づいてまとめており，それぞれ順に Operate and Maintain，Securely Provision，Protect and Defend，Investigate に対応している．Analyze と Collect and Operate に該当するような業務は，今回の参加者では明示的には確認されなかった．これらの業務はセキュリティの調査研究を行うものであり，エキスパート層に着目している本研究の対象外である．

参加者数は，予備実験における効果量を基にテストの結果が統計的に有意になるようにサンプルサイズを見積もり 25 名以上となるように募集をした．

実験は，基本的にオンラインのミーティングツールを使って行われたが，一部は対面で行われた（ID-6,7,1216,25）．COVID-19 の対策として，対面での実施の際には，マスクは外さず，十分な距離を保ち，定期的に消毒と換気を行った．

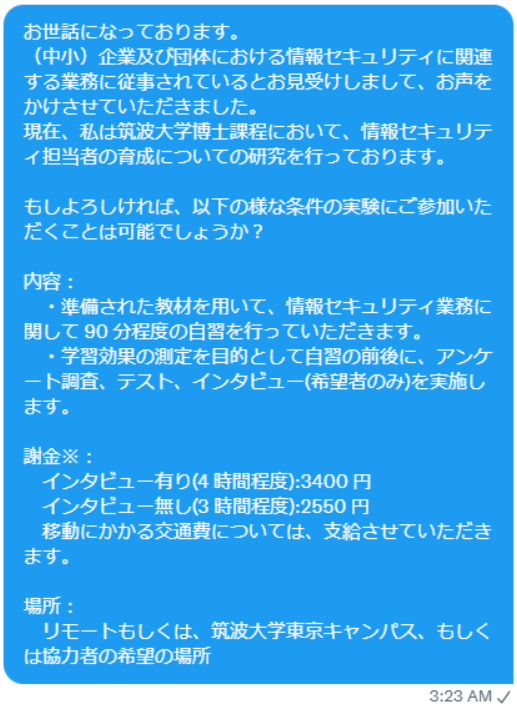


図 26　Twitter Direct Message 上での声掛けの様子

Figure 26 Recruitment on Twitter Direct Message

表 33　実験参加者の情報と実験条件

Table 33　Demographics and experiment conditions

ID	業務年数	企業規模	業務内容	募集	グループ
1	6～10年	100～300人	システム（のセキュリティの）保守・運用，セキュリティ導入（支援）	SNS	統制
2	6～10年	50～100人	ポリシー作成運用，教育，セキュリティ導入（支援）	SNS	実験
3	3～5年	1000 人～	解答なし	SNS	実験
4	3～5年	50～100人	システム（のセキュリティの）保守・運用，システム監視・対応	SNS	統制
5	6～10年	100～300人	セキュリティ導入（支援），システム（のセキュリティの）保守・運用	SNS	統制
6	6～10年	100～300人	システム（のセキュリティの）保守・運用，セキュリティ導入（支援）	チラシ	統制
7	3～5年	50～100人	システム（のセキュリティの）保守・運用，ポリシー作成運用，教育	SNS	実験
8	3～5年	100～300人	システム（のセキュリティの）保守・運用，ポリシー作成運用，教育	SNS	実験
9	1～2年	50～100人	システム（のセキュリティの）保守・運用	SNS	統制
10	3～5年	100～300人	システム（のセキュリティの）保守・運用，システム監視・対応	SNS	統制
11	3～5年	100～300人	システム（のセキュリティの）保守・運用セキュリティ導入（支援）	チラシ	実験

12	3〜5年	100〜300人	システム（のセキュリティの）保守・運用セキュリティ導入（支援）	チラシ	実験
13	6〜10年	300〜1000人	システム監視，対応，セキュリティ導入（支援）	知人	統制
14	3〜5年	50〜100人	ポリシー作成運用，教育，セキュリティ導入（支援），システム（のセキュリティの）保守・運用	知人	統制
15	6〜10年	300〜1000人	システム（のセキュリティの）保守・運用	知人	実験
16	3〜5年	50〜100人	ポリシー作成運用，セキュリティ導入（支援），システム（のセキュリティの）保守・運用	SNS	統制
17	1〜2年	300〜1000人	システム監視，対応，セキュリティ導入（支援）	知人	実験
18	1〜2年	300〜1000人	システム監視，対応，セキュリティ導入（支援）	知人	実験
19	3〜5年	100〜300人	システム（のセキュリティの）保守・運用，システム監視・対応，ポリシー作成運用，教育	知人	統制
20	6〜10年	100〜300人	システム（のセキュリティの）保守・運用，システム監視・対応	知人	統制
21	3〜5年	100〜300人	セキュリティ導入（支援），システム（のセキュリティの）保守・運用，システム監視，対応	知人	実験
22	6〜10年	50〜100人	ポリシー作成運用，セキュリティ導入（支援），システム（のセキュリティの）保守・運用，システム監視・対応	SNS	実験
23	3〜5年	300〜1000人	システム監視・対応，セキュリティ導入（支援）	知人	統制
24	3〜5年	300〜1000人	システム監視・対応，セキュリティ導入（支援）	知人	統制
25	6〜10年	100〜300人	システム（のセキュリティの）保守・運用，システム監視・対応	知人	実験
26	6〜10年	100〜300人	システム（のセキュリティの）保守・運用，システム監視・対応	知人	実験

6.3.2. 実験フロー

実験は，自己学習によるメンタルモデルの変化を把握するための半構造化インタビューと，学習効果の変化を測定するためのテストの 2 つ手法を用いた．それぞれ，自己学習の前と後の 2 回実施した(図 27)．手順については，予備実験の手順 5.2.3.2 と基本的に同じである．テストの問題については予備実験の第二段階の形式に基づいている．第一段階の正誤問題 30 問に加えて，事前テスト・事後テストで共通の問題を 10 問，事後のみの問題をさらに 20 問，新たに追加した(表 34)．そのため，本実験におけるテストの全体の構成は，事前テストは正誤問題が 40 問，事後テストは，正誤問題が 60 問と選択問題が 37 問となっている．また，事前アンケートにおいて，実験参加者の具体的な業務内容について記述する自由記入欄を設けた．予備実験の 4 名の業務内容については別途，聞き取りを行った．

図 27　実験の流れ

Figure 27　Experiment Process

表 34　追加問題一覧

Table 34　Ture False Questions in Test

	設問	正答
	自己学習前，自己学習後で共通して追加した 10 問	
1	Web サイトを構築後に，サーバ OS やソフトウェアに対して脆弱性パッチの適用をする必要はない.	×
2	Web サイトの運用形態によって，自社で担当すべきセキュリティ対策の範囲や対象が異なる.	○
3	クラウドサービスのセキュリティ対策を適切に実施するには，あらかじめ必要なセキュリティ対策を検討して，それらを備えたクラウドサービスを選定する必要がある.	○
4	クラウドサービスのセキュリティは，事業者が実施してくれるため，利用者として対策を検討・実施する必要はない.	×
5	デジタルフォレンジックサービスを利用することで，攻撃を事前に防ぐことができる.	×
6	脆弱性診断サービスを利用して事前に脆弱性を洗い出し対応することで，実際の攻撃を受ける前に対応することができる.	○
7	自社の情報セキュリティマネジメントやリスク対策の運用状況を検証・評価し，助言を受けるのには，情報セキュリティ監査サービスが有効である.	○
8	ウイルス対策などのコンテンツセキュリティ対策を充実することで，危険なウェブサイトやファイルからの感染を防いだり，検知することができる.	○
9	通信やデータを適切に暗号化することで，のぞき見や改ざん漏洩などを防止することができる.	○
10	サーバ等に誰がログインしたかや，どのデータに対してアクセスがあったかなどのログ情報	×

	は，監査目的では有効であるがサイバー攻撃の分析などに使われることはない	
	自己学習後で共通して追加された 20 問	
1	公的機関の情報を把握したり，積極的にコミュニティへ参加するなど，情報セキュリティに関する最新動向を収集する必要がある．また業界団体や委託先等への共有を行うのが望ましい．	○
2	重要情報を机の上に放置せず書庫などの定められた場所に保管することは，セキュリティ対策として有効である．	○
3	重要情報が勝手に変更されていることに気付けるように，電子署名などの仕組みを導入したほうが良い．	○
4	重要情報が保存されたハードウェアはバックアップをとり，何かあった場合でも復元できるようにしている．	○
5	従業員を雇用する際には，守秘義務や罰則規定があることを知らせる必要がある．	○
6	情報資産台帳には，社内の情報資産のうち最低限重要なものが記載されていれば良く，すべての資産を洗い出す努力をする必要はない．	×
7	策定したポリシーは正社員のみが順守すればよく，アルバイトにまで周知する必要はない．	×
8	セキュリティ事故が発生した場合の対応方法を事前に作成してまとめておく必要がある．	○
9	監査やログの記録の対象はポリシーに従って決定されている必要がある．	○
10	アンチウィルスソフトで検知が発生した場合には，すでに検体は削除されているので調査の必要はない．	×
11	Web サーバのセキュリティを考える際には，ウェブサーバが置かれているネットワークのルータや FW で，公開すべき通信ポート以外のポートを閉じるなどの対応が必要である．	○
12	選定したクラウドサービスで利用されているデータのバックアップの必要性について検討する必要はない．	×
13	重要なデータを扱うサービスなどにおいては，自社のセキュリティポリシーに従って，多要素認証を行わなければならない．	○
14	脆弱性検査を行って見つけた脆弱性は，その脆弱性のリスクについて検討したうえで対応の方針を決めればよい．	○
15	適切にネットワークを分離することで，ネットワークの脅威に対する軽減することができる．	○
16	データや通信の暗号化は，暗号化方式の種類に関係なく，実施されていれば必ずのぞき見や改ざん，漏洩などを防ぐことができる．	×
17	社員の情報セキュリティリテラシーの向上のために情報セキュリティ教育サービスを利用することができる．	○
18	自社の情報セキュリティ対策は，自分たち自身で行う必要があるため，コンサルテーションサービスなどの利用はできない．	×
19	セキュリティ監視・運用サービスを利用すれば，自社の情報セキュリティ運用について自分たち自身で考える必要はない．	×
20	デジタルフォレンジックサービスは，法廷紛争の観点で利用されるほか，セキュリティ事故の対応の方針を決定するために利用されることがある．	○

6.4. 結果と分析

6.4.1. インタビューの分析結果

今回の実験では，予備実験と同様に，情報セキュリティ対策の概要説明を通じて，役割，

時間軸型，フレームワーク（CSF）型，および未構造のモデルの 4 種類のメンタルモデルを確認した．また，2 人の参加者のインタビューでは，4 種類のうち 2 種類のモデルが混合されたモデルが観察された．1 つは CSF 型と役割型の混合モデル，もう 1 つは役割型と時間軸型の混合モデルである．

6.4.1.1. インタビューの分析手法

インタビュー内で作成した図をオープンコーディングにより，実験参加者間の項目の粒度を揃えて整理し，共通項を元に分類を行った．録音された音声データは書き起こされ，オープンコーディングの際に利用された．図 28 に ID-5 の実験参加者の自己学習前の結果を示す．

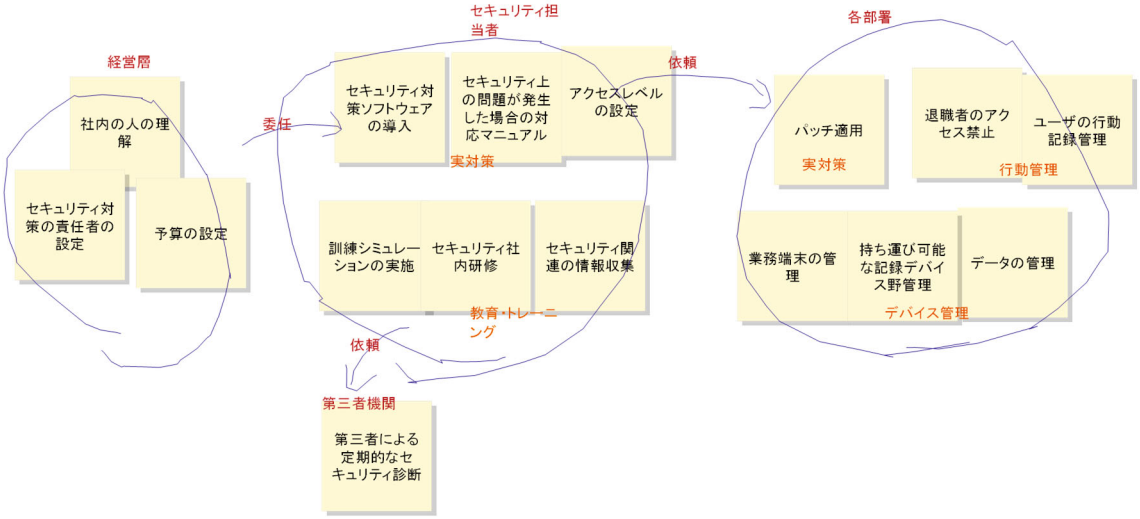


図 28　ID-5 の実験参加者の自己学習前のインタビュー結果

Figure 28　Task result of ID-5 before self-learning

まず，各被験者のインタビュー中に作成された図について，グループと付箋にかかれた項目の整理を行った．名付けてもらったグループをグループとして，個々の付箋はセキュリティ項目として定義して，表形式で書き表した．ただし，予備実験とは異なり，今回の実験では，グループ内でさらに分類などが行われている場合が存在したため，それらはサブグループとして取り扱った．

整理の結果を表 35 に示す．次に，実験参加者間の項目の粒度を揃えることを目的にコーディングを実施した．

表 35　図 27 の項目を整理した表

Table 35　Table organizing the Figure 27

グループ	サブ グループ	セキュリティ項目 （付箋の項目）
経営者		社内の人の理解
		セキュリティ対策の責任者の設定
		予算の設定
セキュリティ担当者	実対策	セキュリティ対策ソフトウェアの導入
		セキュリティ上の問題が発生した場合の対策マニュアル
		アクセスレベルの設定
	教育・トレーニング	訓練シミュレーションの実施
		セキュリティ社内研修
		セキュリティ関連の情報収集
各部署	実対策	パッチ適用
	行動管理	退職者のアクセス謹慎
		ユーザーの行動記録管理
	デバイス管理	業務端末の管理
		持ち運び可能な記憶デバイスの管理
		データの管理
第三者機関		第三者による定期的なセキュリティ診断

インタビュー中の説明や発言も参考として，付箋の記載内容とグループ名に対して，2 名によるオープンコーディングを行った．本実験では，予備実験とは異なりグループ名やそれ以外の表中に現れる説明全てに対して，コードを割り振るようにした．

各コードの項目について調整を行った後，2 名のコーディングの Cohen's kappa を計算したところ 0.71 であり，Krippendorff ら [76]の基準に基づくと「かなりの一致」，Landis と Koch ら [77]の基準に基づいても「暫定的な結果」があるとされた．コードの振り分けとコードの内容について意見が一致しなかった部分については議論を行い最終的な調整が行われた．得られたコードを表 36 に示す．コードは，割り当てられる対象に従って，3 つに形式的に分類された．要素向けコードとは，実験参加者によって付箋に記載された各要素に対して割り振られたコードである．グループ向けコードとは，主に実験参加者によって名付けられたグループ名に対して割り振られたコードである．補足コードとは，グループ内で各要素を分類しなおしたり，各要素やグループについての説明が行われた際に現れたコードである． また，グループ向けのコードについては，その表現に基づいてさらに「時間的表現」,「行動的表現」.「役割的表現」,「フレームワーク的表現」の 4 つに分類した．

コーディングの結果，同一コードにまとまった付箋やグループは 1 つに整理された．図 28 に整理された ID-5 の自己学習前のインタビュー結果について示す．この図中には，コード一覧にあるコード以外の要素やグループ名は表れず同じ粒度に基づいて各被験者の実験結果を比較することができる．

表 36　コード一覧

Table 36　Code List

形式的分類	表現による分類	
グループ向けコード	時間的表現	初めにすべきこと※
		攻撃される前にすべきこと※
		攻撃された後にすべきこと※
	行動的表現	評価※
		方針・体制づくり※
		対策の実施と運用※
		有事の対応※
	役割的表現	経営者の取組
		セキュリティ担当者の取り組み
		部署ごとの取り組み
		全社員（個人）の取り組み
		第三者の取り組み
	フレームワーク的表現	識別
		防御
		検知
		対応
		復旧
要素向けコード	N/A	物理セキュリティ
		セキュリティへの理解と協力
		ガバナンス
		要員と予算の確保（責任範囲の確定）
		セキュリティポリシーの作成
		リスク評価と管理
		資産管理
		アカウントとアクセス管理
		脅威やセキュリティの知識の獲得
		サードパーティのセキュリティ
		（セキュリティについての）訓練と気づき
		セキュアなシステム設計
		セキュリティ製品の導入
		ソフトウェアの運用と管理
		データ保護と管理
		外部サービスによるセキュリティ
		対応計画
		（行動などの）ロギング
		セキュリティ事故監視／異常監視
		攻撃の調査と軽減
		セキュリティ水準の確認
		ポリシーの見直しと改善
		復旧計画
		関係者とのコミュニケーション
補足コード		システムとツール
		環境とルール
		人と知識
		手の付けやすい対策
		手の付けにくい対策

※番号付けや矢印などの順序表現と共に確認された

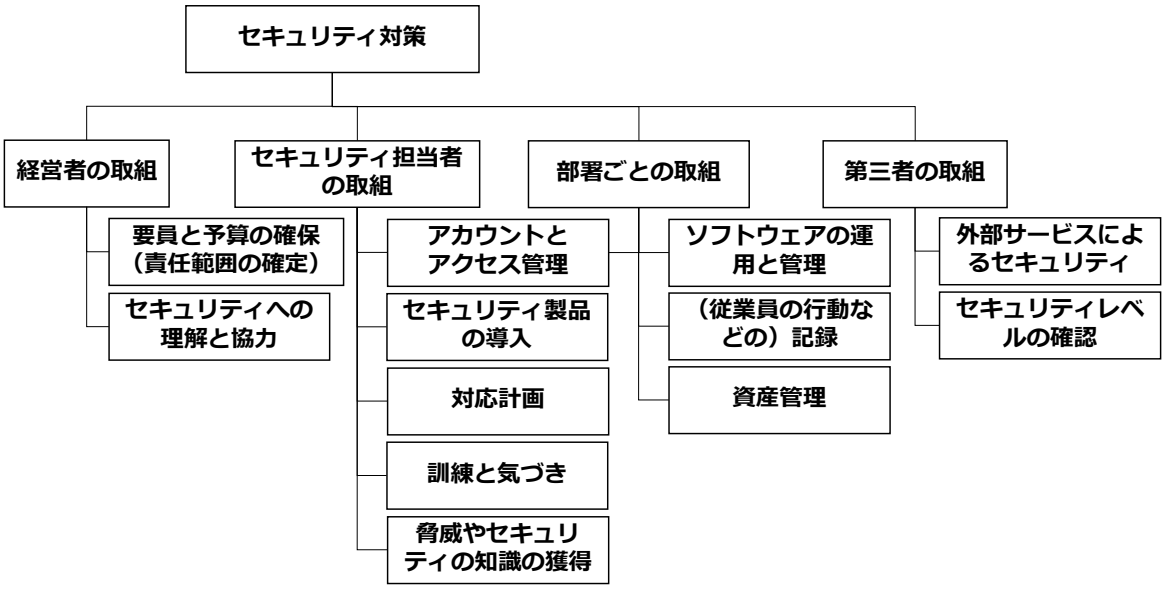


図 29　ID-5 の実験参加者の自己学習前のインタビューのコーディングの結果

Figure 29　Coding result of ID-5 before self-learning

グループ向けのコードについて着目すると，学習者は「時間的表現」,「行動的表現」.「役割的表現」,「フレームワーク的表現」な観点を保持していることが分かる．そこで，グループ間の構造と項目の数，時間経過や順序を表す矢印の有無，項目をまとめるグループ名に着目して，モデルの分類を試みた．行動的表現はすべて矢印と共に現れていたため，時間的・順序的表現を重視していると考え，時間軸型としてまとめたため，最終的に構造化できなかった場合を含む 4 つの型に分類された．具体的な分類の手順を図 30 に示す．まず，得られた図において，項目数が少なくグループが定義できないか，1 つしかないものを，構造化されていない未構造型として判別した．次に，時間経過や順序を表す矢印や番号付けが存在するか確認し，存在する場合には時間軸型と判別した．その後，グループ名に着目し，それらが時間経過を表している場合（つまり，時間的表現に属するグループコードの場合）は時間軸型，人の属性や立場や役割を表している場合（役割的表現に属するグループコードの場合）は役割型，特定のセキュリティ関連のフレームワークに該当する名前に該当する場合（フレームワーク的表現に属するグループコードの場合）はフレームワーク型と判別した．特にフレームワークの場合には，インタビュー中にそのフレームワークに対する言及があるかも確認した．今回の実験では，定めた手順に従って分類した結果，どこにも属さないものは現れなかった．つまり，行動的表現に属するグループコードは全て矢印と共に現れていた．

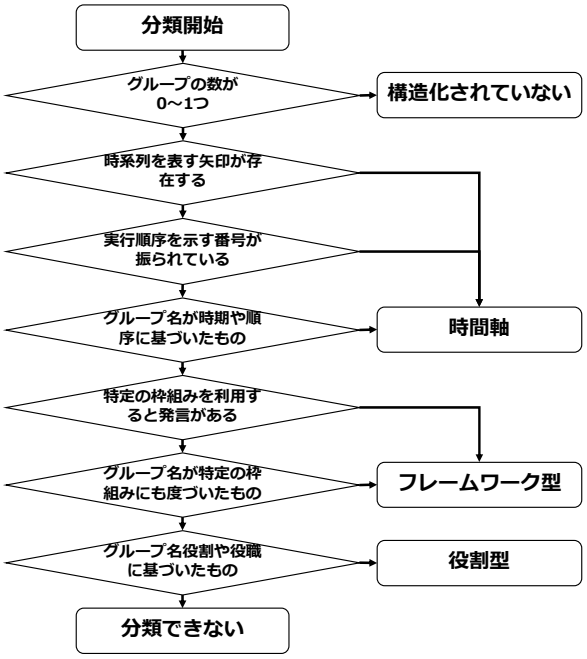


図 30　型の分類のフローチャート

Figure 30　Flowchart for categorizing a type of mental model

6.4.1.2. メンタルモデルの 4 つの型

本実験では 4 つの異なる型のメンタルモデルを確認した.

6.4.1.2.1.　役割型のモデル

この型では，誰がどのような対策を実施するべきかという視点に基づいて，セキュリティ対策を分類する．本実験では，グループ名として，役割的表現である「経営者の取り組み」,「情報セキュリティ担当者の取り組み」,「部署ごとの取り組み」,「全社員（個人）の取り組み」,「第三者の取り組み」が現れるものを役割型とした．図 27 で記載した ID-5 の実験参加者の自己学習前のインタビューのコーディング後の結果は，この典型である．実験参加者は， セキュリティの要素を「経営者の取り組み」,「セキュリティ担当者の取り組み」,「部署ごとの取り組み」,「第三者の取り組み」の 4 つに分類しており,「アカウントとアクセス管理」に関する活動は，セキュリティ担当者と各部署が共同して行うものであると認識していると読み取れる.

6.4.1.2.2.　時間軸型のモデル

この型では，セキュリティ対策を時間経過や実行順序に基づいて分類する．セキュリティ対策の構成要素をいくつかの段階に分けて，時間軸に沿って段階ごとに整理する

この型では，要素とグループやグループ間の関係性の説明の際に，時間経過を表す矢印が書き込まれ，時間の流れや順序で各要素は表現された．セキュリティ対策の中には，プ

ロセスの改善や振り返りを必要とするものがあるため，時系列で並べるとループバックが発生することもある．具体的には，時間的表現である「初めにすべきこと」,「攻撃される前にすべきこと」,「攻撃された後にすべきこと」といったコードが割り当てられる純粋に時系列に基づいた名づけがされたものや，行動的表現である「評価」,「方針・体制づくり」,「対策の実施と運用」,「有事の対応」といったコードが割り当てられる一般的なグループの名づけに実行順序を示す矢印が書き加えられたものを時間軸型としている．

実験の参加者の半数以上が学習前にはこの型のモデルを使用していた．図 30 は ID-11 の実験参加者の自己学習前のインタビューの結果であり，図 31 はその分析結果である．

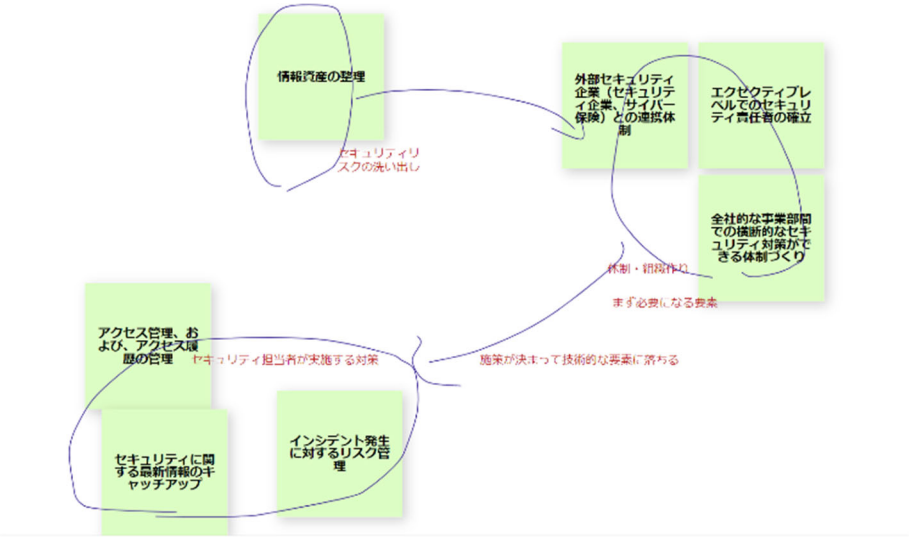


図 31　ID-11 の実験参加者の自己学習前のインタビューの結果

Figure 31　Task result of ID-11 before self-learning

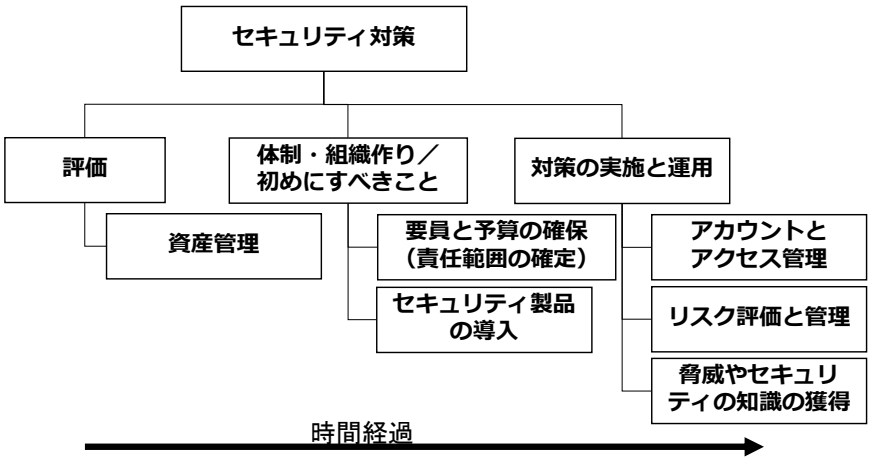


図 32　ID-11 の実験参加者の自己学習前のインタビューのコーディングの結果

Figure 32　Coding result of ID-11 before self-learning

6.4.1.2.3.　フレームワーク（CSF）型のモデル

この型では，フレームワークに基づいて要素を分類し，その関係を説明する．グループ名として，フレームワーク的表現である「識別」,「防御」「検知」,「対応」,「復旧」が用いられているものを，フレームワーク(CSF)型とした．多くの場合，説明の際に明示的にCSF への言及が確認された．

予備実験では，分類に用いられるフレームワークとして CSF 以外に，自己学習前に Cyber kill chain の枠組みに基づいたモデルが確認されたが，本実験では，自己学習後に CSF に基づく型のみが確認された．実験参加者のうち，統制群では 1 名が，実験群では 4 名が，自己学習の後この型に変化していた．

図 32 は，ID-12 の実験参加者の自己学習後のインタビューの結果であり，図 33 はその分析結果である．

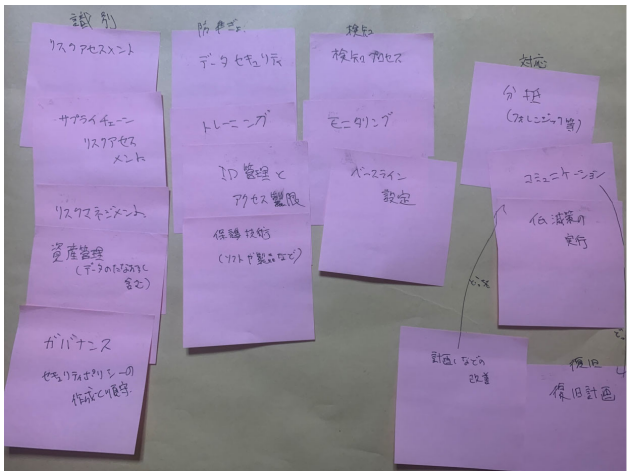


図 33　ID-12 の実験参加者の自己学習後のインタビューの結果

Figure 33　Task result of ID-12 before self-learning

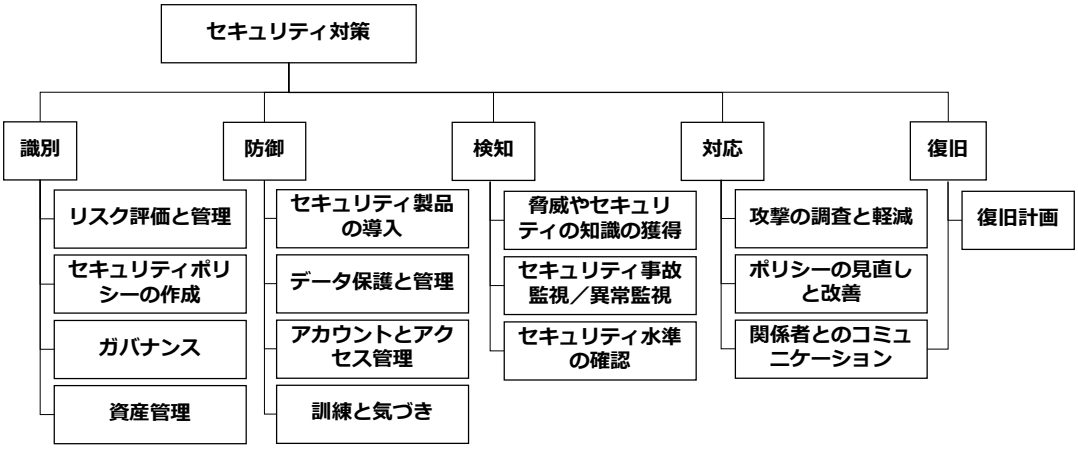


図 34　ID-12 の実験参加者の自己学習後のインタビューのコーディングの結果

Figure 34　Coding result of ID-12 before self-learning

6.4.1.2.4.　未構造のモデル

実験参加者の中には，セキュリティ対策の要素をうまく列挙できなかったり，要素を整理できなかったりする人がいた．この場合，グループ化は不十分となり，グループと構成要素の間に関連性を見いだせない場合がほとんどであった．また，この型に該当する事例では，グループ名として，要素向けとしているコードを割り振る事例がみられた．このモデルは，自己学習前でのみ観察された．

図 34 は ID-19 の実験参加者の自己学習前のインタビューの結果であり，図 35 はその分析結果である．この実験参加者は，データの保護の観点で要素を挙げたが 4 つの要素しか上げることができず，コーディングの結果，要素向けコードである「データ保護と管理」のグループとしてまとめられた．

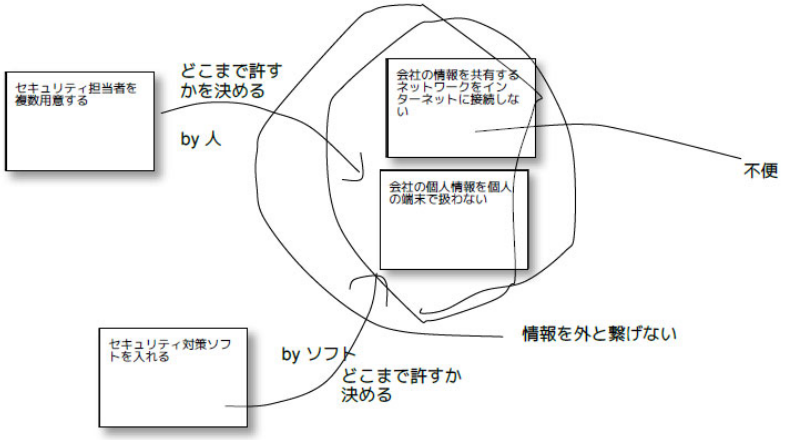


図 35　ID-19 の実験参加者の自己学習前のインタビューの結果

Figure 35　Task result of ID-19 before self-learning

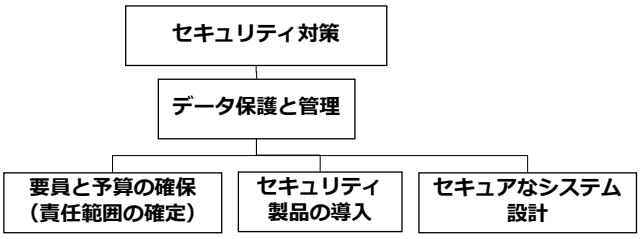


図 36　ID-19 の実験参加者の自己学習前のインタビューのコーディングの結果

Figure 36　Coding results of ID-19 before self-learning

6.4.1.3. 混合型のモデルについて

今回の実験では，4 つの型のうち二つが組み合わさったものが 2 例確認された

6.4.1.3.1.　フレームワーク型と役割型

参加者 ID-11 の学習後のインタビューで，フレームワーク型と役割型が組み合わさったものが確認された．図 36 は ID-11 の実験参加者の自己学習後のインタビューの結果であり，図 37 はその分析結果である．ID-11 は，まず CSF に基づいて手法を説明し，その後，役割に基づいて要素を「経営者の行動」と「情報セキュリティ担当者の行動」という二つの基準で再分類した．

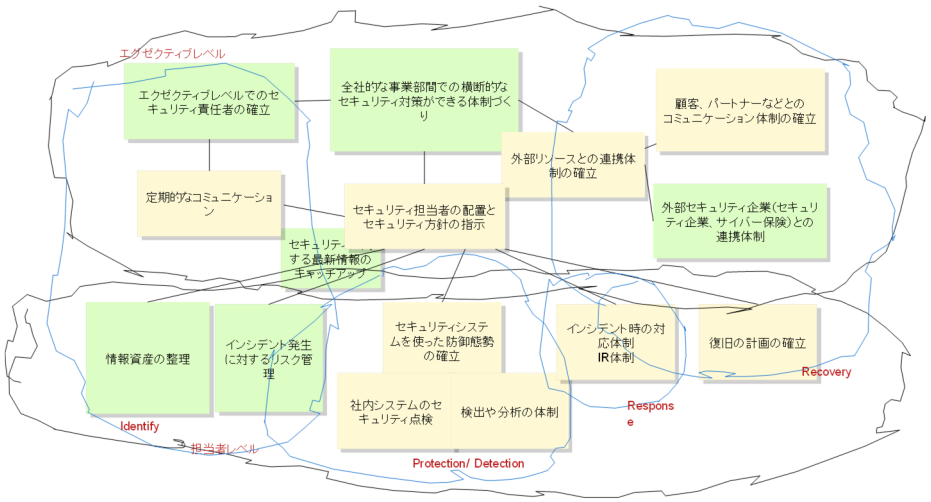


図 37　ID-11 の実験参加者の自己学習後のインタビューの結果

Figure 37　Task result of ID-11 before self-learning

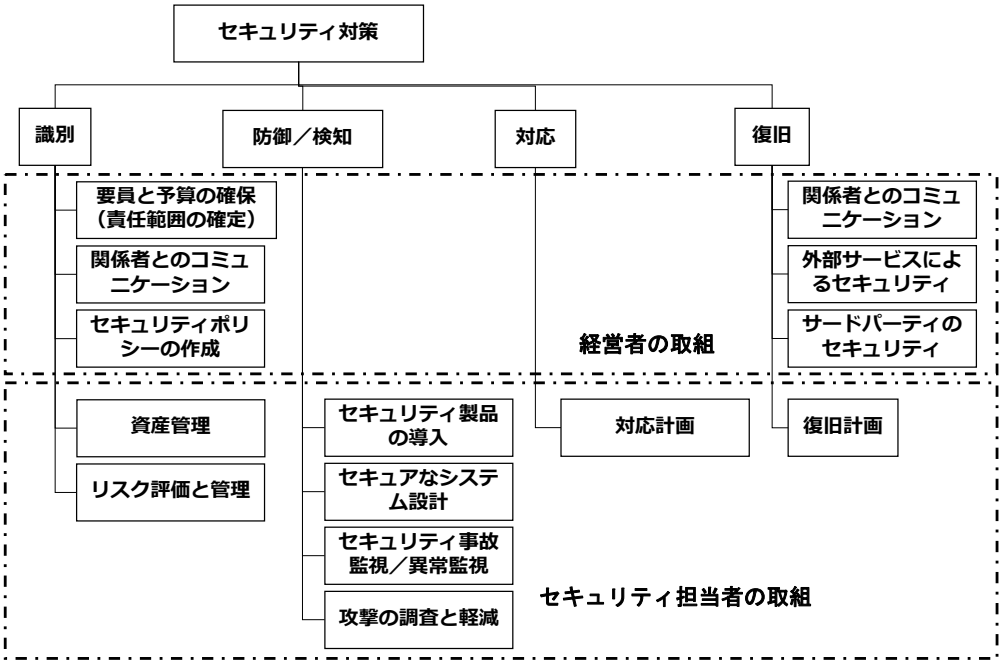


図 38　ID-11 の実験参加者の自己学習後のインタビューのコーディングの結果

Figure 38　Coding results of ID-11 after self-learning

6.4.1.3.2.　役割型と時間軸型

このモデルは，ID-13 の学習後のインタビューで確認された（図 38）． ID-13 は，要素を「全社員（個人）の取り組み」,「経営者の取り組み」,「セキュリティ担当の取り組み」の 3 つに分類した．そして，モデルに時間を表す矢印を加え，時間順になるように付箋の位置を調整して，それに時間に関するグループ名を追加した．解析後の結果を図 39 に示す,

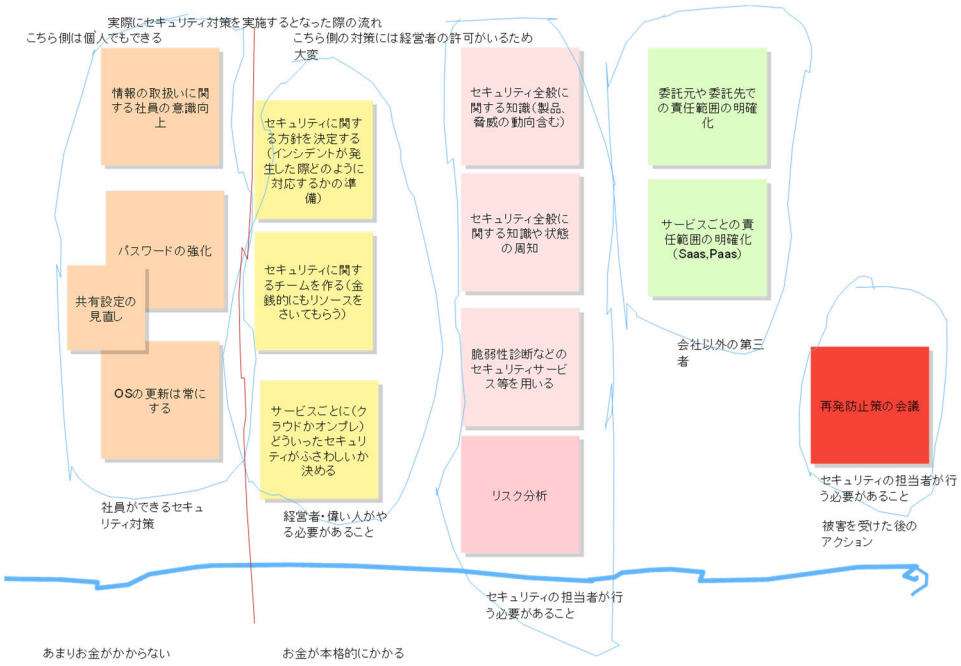


図 39　ID-13 の実験参加者の自己学習後のインタビューの結果

Figure 39　Task result of ID-13 before self-learning

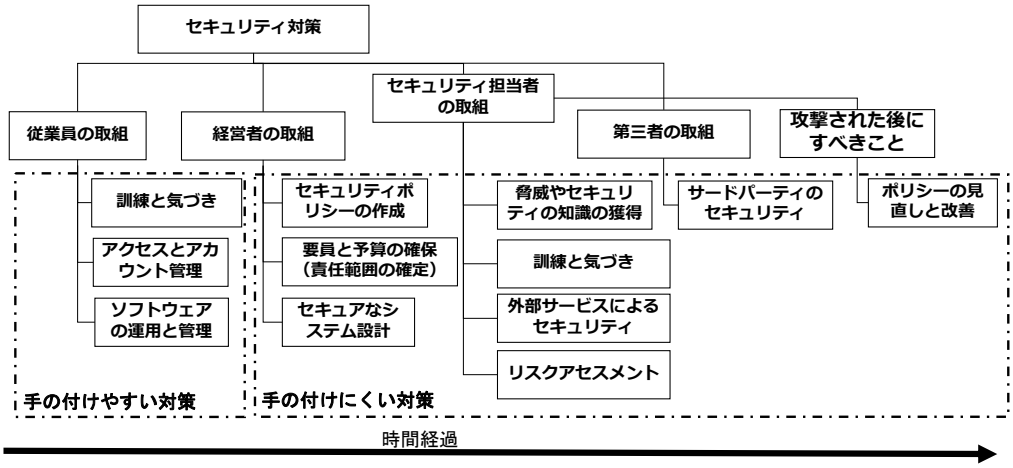


図 40　ID-13 の実験参加者の自己学習後のインタビューのコーディングの結果

Figure 40　Coding results of ID-13 after self-learning

6.4.1.4. メンタルモデルの型の変化について

実験参加者の学習前と学習後のメンタルモデルについて表 37 に示す．複数の型が組み合わさっている場合には，副次的な型は（）で表現する．学習の前後で，実験参加者の一部のメンタルモデルの型が変わっていた．学習前は，未構造のメンタルモデルを持っていた人も，学習によって他の型を獲得した．型が変更しなかった場合でも，学習者は多くの場合，学習後のインタビューで新しいグループや要素を追加しており，学習によりモデルを進化していることが確認された．

表 37　実験参加者のメンタルモデルの型

Table 37　The type of mental models of each participant

メンタル モデルの型	統制群		実験群	
	学習前	学習後	学習前	学習後
フレームワーク型		9		2,11,12,22
役割型	5,13	5,13,14	3,7,18,22	3,7, (11),17,21,26
時間軸型	1,4,6,9,10, 14,16,20,23	1,4,6,10,(13),16, 19,20,23,24	2,11,12, 15,21,25,26	8,15,18,25
未構造型	19,24		8,17	

今回の実験では，予備実験と同様に，情報セキュリティ対策の概要説明を通じて，役割，時間軸型，フレームワーク（CSF）型，および未構造型モデルの 4 種類のメンタルモデルを確認した．また，2 人の参加者のインタビューでは，4 種類のうち 2 種類のモデルが混合されたモデルが観察された．1 つは CSF 型と役割型の混合モデル，もう 1 つは役割型と時間軸型の混合モデルである．ほとんどの情報セキュリティ担当者が時間軸型のモデルを使用していた．

実験群では，フレームワーク（CSF）型への変化が 4 例確認されたのに対して，統制群では，1 例のみであった．これについて実験群と統制群の間で検定を行った．本実験はサンプルサイズが小さく期待数が 5 未満のものが現れる可能性があるため，Cochran’s rule [82]に従い χ^2 検定ではなく，Fisher の正確検定 [83]を用いて検定を行った．その結果，有意差は確認されなかった(p=0.1609, 効果量 h=0.61)．

6.4.2.　テストの結果と統計的分析

6.4.2.1. テスト結果の計算方法

テストの結果については，予備実験と同じように計算を行った．テストの得点では，正解の場合は 1 点を加点して，不正解の場合は 0 点とした．一方，確信度の計算では，問題に正解した場合は，回答の確信度を合計に加え，不正解の場合は，回答の確信度分を減算した．誤った対策を信じることで，誤った行動につながる可能性があるため，ペナルティとして減算を行っている．

選択問題では，完全に正しい答えには 2 点，部分的に正しい答えには 1 点，誤った答え

には 0 点を与えた．確信度の合計は，問題が（部分的にでも）正解した場合は，確信度を合計に加えた．不正解だった場合は，確信度を減算した．

表 38 に各群の平均と標準偏差と 95%信頼区間について記載する．個々の参加者の結果については，表 39 に記載する．天井効果の影響を平均と標準偏差の和で確認したところ本実験においても確認されなかった．

表 38　平均・標準偏差・95%信頼区間

Table 38　Statistics of test score and degree of confidence

条件			グループ	平均	標準偏差	95%信頼区間	
						最小	最大
学習前	共通正誤問題 40 問	得点	統制	36.4	2.0	35.2	37.6
			実験	36.8	2.0	35.6	38.0
			全体	36.6	2.0	35.8	37.4
		確信度	統制	131.2	29.9	113.1	149.2
			実験	140.8	33.1	120.8	160.7
			全体	136.0	31.3	123.3	148.6
学習後	共通正誤問題 40 問	得点	統制	37.5	2.0	36.3	38.8
			実験	38.7	1.2	38.0	39.4
			全体	38.1	1.7	37.4	38.8
		確信度	統制	160.3	19.7	148.4	172.2
			実験	177.4	9.8	171.5	183.3
			全体	168.8	17.5	161.8	175.9
	全正誤問題 60 問	得点	統制	56.4	2.9	54.6	58.2
			実験	58.4	1.4	57.5	59.2
			全体	57.4	2.5	56.4	58.4
		確信度	統制	240.7	29.4	222.9	258.4
			実験	267.0	18.3	256.0	278.0
			全体	253.8	27.5	242.8	264.9
	選択問題 37 問	得点	統制	34.4	10.4	28.1	40.7
			実験	48.2	6.6	44.2	52.2
			全体	41.3	11.1	36.8	45.8
		確信度	統制	38.6	40.6	14.1	63.2
			実験	98.6	20.8	86.0	111.2
			全体	68.6	44.0	50.8	86.4

表 39　各参加者の得点と確信度

Table 39 Test score and degree of confidence

ID	学習前		学習後			
	共通 40 問		全体 60 問		選択 37 問	
	得点	確信度	得点	確信度	得点	確信度
1	33	130	51	210	17	-14
2	35	82	60	276	49	82
3	36	152	58	270	45	95
4	36	148	56	256	36	40
5	36	85	56	218	34	29
6	38	106	59	198	32	29
7	37	88	60	279	46	92

8	36	152	56	261	47	103
9	38	164	60	289	50	112
10	39	160	58	268	39	79
11	39	173	59	274	46	99
12	37	149	59	281	59	137
13	35	137	54	233	40	52
14	33	104	55	256	21	-25
15	40	195	59	286	40	81
16	38	152	60	288	29	29
17	39	170	58	266	40	71
18	38	110	57	232	54	101
19	35	78	58	224	44	63
20	36	152	52	210	19	-21
21	33	122	56	227	55	101
22	35	134	59	281	59	143
23	39	166	59	237	45	69
24	37	123	55	242	41	60
25	35	143	60	276	46	96
26	38	160	58	262	41	81

6.4.2.2. 学習教材に基づく分析

実験群と統制群に対して，有意水準 0.05 の片側 Welch の t-検定を行った．さらに，改良された教材の効果を学習教材で検証するために，効果量 r を算出した．学習前のテスト結果では，実験群と統制群の間に統計的に有意な差は見られなかった．

学習後のテストでは，共通問題（40 問），追加問題（20 問），真偽判定問題（60 問），選択問題（37 問）の各問題において，確信度とテストの得点の両方で統計的に有意な差が認められた．各グループの統計量と t 検定の結果を表 40 に示す．また，検出力について，効果量 d を用いて有意水準 0.05 として計算を行い記載した．

学習後の実験群は，統制群と比較して，既知の質問と未知の質問の両方に自信を持って正しく答えることができ，CSF の機能と実際の情報セキュリティ対策との関係について理解を深めることができたと考えられる．

表 40　実験群と統制群に対する t 検定の結果

Table 40　Welch’s t-test results between experiment group and control group

			t 値	自由度	効果量 r	効果量 d	p 値	検出力
学習前	共通 40 問	得点	0.487	24	0.1	0.20	0.315	0.13
		確信度	0.778	24	0.16	0.30	0.222	0.19
学習後	共通 40 問	得点	1.774	19	0.38	0.73	0.046*	0.56
		確信度	2.804	18	0.55	1.10	0.006*	0.86
	全 60 問	得点	2.224	17	0.47	0.88	0.020*	0.70
		確信度	2.742	20	0.52	1.07	0.006*	0.84

	選択問題 37 問	得点	4.046	20	0.67	1.58	0.000*	0.98
		確信度	4.738	18	0.74	1.86	0.000*	0.99

6.4.2.3. モデルの型に基づく分析

学習により身についたメンタルモデルと学習効果の関係性を確認するために，観察されたメンタルモデルの型の観点で追加の分析を行った．事前学習と事後学習のモデルの種類に基づいて，新たなグループを定義した．具体的には，事前学習では，未構造型（サンプルサイズ 4)，役割型（サンプルサイズ 6)，時間軸型（サンプルサイズ 16）の三つのグループを定義し，事後学習では，CSF 型（サンプルサイズ 5)，役割型（サンプルサイズ 8)，時間型（サンプルサイズ 13）の三つのグループを定義した．各グループの学習後と学習前のテストの統計と結果も表 41 に示した．

設問の各項目における各グループの結果について，有意水準 0.05 の一元配置分散分析（一次元配置 ANOVA）を行った（表 42)．一次元配置 ANOVA の効果量の大きさは二乗相関比（η^2）を用いて算出した．検定の結果，事前テストと事後テストで共通して出題された 40 問の正誤問題，事後テストのみ出題された 20 問を含む全 60 問の正誤問題と 37 問の選択問題の確信度には，グループの間で有意差が確認された．

さらにどちらのグループの平均値が高いかを明らかにするために，ボンフェローニ法を用いた多重比較を行った．今回の事例では，比較するグループの数は 3 で，有意水準は 0.05 であるため，メンタルモデルのグループの組み合わせごとに，有意水準 0.0167 の片側ウェルチの t-検定を行った．学習前のテストでは，どのグループ間にも，有意な差は見られなかったが，学習後のテストでは，20 問の追加問題の CSF 型と役割型のグループの間，役割型と時間軸型のグループの間以外では，有意な差が確認された（表 43)．したがって，CSF 型の群は学習後に他の 2 群よりも高い得点を獲得したものと考えられる．また，検出力について，効果量 d を用いて有意水準 0.0167 として計算を行い，その結果も表 43 に記載した．

表 41　各型によるグループの平均・標準偏差・95%信頼区間

Table 41　Statistics of test score and degree of confidence in groups of mental model types

			グループ	標本サイズ	平均	標準偏差	95%信頼区間	
							最小	最大
学習前	共通 40 問	得点	未構造	4	36.2	1.2	34.3	38.0
			役割	6	36.8	1.7	35.0	38.5
			時間軸	16	36.7	2.3	35.4	37.9
		確信度	未構造	4	130.8	40.1	66.9	194.6
			役割	6	117.7	27.7	88.6	146.7
			時間軸	16	144.1	29.0	128.7	159.6
学習後	共通 40 問	得点	CSF	5	39.4	0.5	38.7	40.1
			役割	8	37.8	1.5	36.5	39.0
			時間軸	13	37.8	2.0	36.6	39.1

		確信度	CSF	5	185.8	6.8	177.4	194.2
			役割	8	167.5	13.0	156.6	178.4
			時間軸	13	163.2	19.3	151.5	174.8
	全体 60 問	得点	CSF	5	59.4	0.5	58.7	60.1
			役割	8	56.9	2.0	55.2	58.5
			時間軸	13	56.9	2.9	55.2	58.7
		確信度	CSF	5	280.2	5.8	273.0	287.4
			役割	8	251.4	22.4	232.7	270.1
			時間軸	13	245.2	29.9	227.2	263.3
	選択問題 37 問	得点	CSF	5	52.6	6.0	45.1	60.1
			役割	8	40.3	9.9	32.0	48.5
			時間軸	13	37.6	10.9	31.0	44.2
		確信度	CSF	5	114.6	25.6	82.8	146.4
			役割	8	62.0	42.6	26.4	97.6
			時間軸	13	55.0	40.6	30.5	79.5

表 42　一次元配置分散分析の結果

Table 42　the one-way ANOVA results of mental model groups

			F 値 F(2,23)	効果量 η^2	p 値
学習前	共通 40 問	得点	0.157	0.1	0.856
		確信度	1.724	0.13	0.201
学習後	共通 40 問	得点	1.833	0.14	0.183
		確信度	3.707	0.24	0.040*
	全体 60 問	得点	2.278	0.17	0.125
		確信度	3.589	0.24	0.044*
	選択問題 37 問	得点	4.211	0.27	0.028*
		確信度	4.370	0.28	0.025*

表 43　ボンフェローニ法による多重比較の結果

Table 43 The results of multiple comparison procedure

		組合せ	t 値	自由度	効果量 r	効果量 d	p 値	検出力
学習前 共通 40 問	得点	未構造 - 役割	0.596	5	0.26	0.39	0.288	0.055
		未構造 - 時間軸	0.060	6	0.2	0.23	0.477	0.041
		役割 - 時間軸	0.692	18	0.16	0.05	0.249	0.021
	確信度	未構造 - 役割	0.568	5	0.25	0.40	0.297	0.055
		未構造 - 時間軸	0.627	4	0.30	0.43	0.282	0.079
		役割 - 時間軸	1.973	9	0.55	0.92	0.040	0.376
学習後共通 40 問	得点	CSF - 役割	2.843	10	0.59	1.30	0.009*	0.465
		CSF - 時間軸	2.569	15	0.55	0.91	0.011*	0.304
		役割 - 時間軸	0.126	18	0.03	0	0.451	0.016
	確信度	CSF - 役割	3.329	11	0.71	1.64	0.003*	0.673
		CSF - 時間軸	3.691	16	0.68	1.33	0.001*	0.583
		役割 - 時間軸	0.617	19	0.14	0.25	0.272	0.054
学習後全体 60 問	得点	CSF - 役割	3.436	9	0.75	1.54	0.004*	0.614
		CSF - 時間軸	2.973	14	0.62	0.99	0.005*	0.353
		役割 - 時間軸	0.046	19	0.01	0	0.482	0.016
	確	CSF - 役割	3.462	8	0.77	1.58	0.004*	0.640

	信度	CSF - 時間軸	4.023	14	0.73	1.34	0.001*	0.596
		役割 - 時間軸	0.536	18	0.13	0.23	0.299	0.049
学習後選択問題 37 問	得点	CSF - 役割	2.799	11	0.64	1.42	0.009*	0.539
		CSF - 時間軸	3.704	13	0.72	1.51	0.001*	0.706
		役割 - 時間軸	0.571	16	0.14	0.26	0.288	0.055
	確信度	CSF - 役割	2.780	11	0.64	1.41	0.009*	0.535
		CSF - 時間軸	3.713	12	0.73	1.59	0.001*	0.752
		役割 - 時間軸	0.372	14	0.10	0.17	0.358	0.038

6.4.2.4. その他の要因についての分析

ここでは，アンケートの結果から，教材やモデルの型以外の影響の有無について検定を行った．特定の業務内容がテスト結果に影響を与えるかという観点で，特定の教務とそれ以外という分類で t 検定を行った．統計的な情報を表 44 に，検定の結果を表 45 に示す．「ポリシーの作成・教育」の業務経験がある参加者では，学習前のテスト結果の比較において，経験がない参加者に比べてテストの得点と確信度が有意に低くなっていることが確認された．

また，募集方法，業務経験年数，企業規模（人数）に基づいてグループ分けを行った．各統計情報を，表 46，表 47，表 48 に記載する．また，一次元配置 ANOVA を実施したところ有意な差は確認されなかった（表 49）．

表 44　業務経験毎の平均・標準偏差・95%信頼区間

Table 44 Statistics of test score and degree of confidence grouped by security experience

		業務経験	標本サイズ	平均	標準偏差	95%信頼区間	
						最小	最大
学習前共通 40 問	得点	システムのセキュリティの保守・運用	19	36.42	2.1	35.4	37.4
		システムのセキュリティの保守・運用 以外	6	37.00	1.7	35.2	38.8
		セキュリティ導入の支援	13	36.54	2.2	35.2	37.9
		セキュリティ導入の支援 以外	12	36.62	1.9	35.4	37.8
		システム監視，有事の対応	11	36.73	2.1	35.3	38.1
		システム監視，有事の対応 以外	14	36.47	2.1	35.3	37.7
		ポリシー作成・教育	7	35.57	1.6	34.1	37.0
		ポリシー作成・教育 以外	18	36.95	2.1	35.9	38.0
	確信度	システムのセキュリティの保守・運用	19	136.6	31.9	121.2	152.0
		システムのセキュリティの保守・運用 以外	6	134.3	31.8	100.9	167.7
		セキュリティ導入の支援	13	128.6	30.7	110.0	147.2
		セキュリティ導入の支援 以外	12	143.3	32.5	122.7	163.9
		システム監視，有事の対応	11	137.9	27.9	119.2	156.6
		システム監視，有事の対応 以外	14	134.5	35.4	114.1	154.9
		ポリシー作成・教育	7	112.9	32.6	82.8	143.0
		ポリシー作成・教育 以外	18	144.5	27.5	130.8	158.2
学習後全体 60 問	得点	システムのセキュリティの保守・運用	19	57.42	2.6	56.2	58.7
		システムのセキュリティの保守・運用 以外	6	57.29	2.1	55.1	59.5
		セキュリティ導入の支援	13	57.08	2.7	55.4	58.7
		セキュリティ導入の支援 以外	12	57.69	2.3	56.2	59.2
		システム監視，有事の対応	11	57.18	1.8	56.0	58.4
		システム監視，有事の対応 以外	14	57.53	3.0	55.8	59.3

		ポリシー作成・教育	7	58.29	2.1	56.3	60.2
		ポリシー作成・教育 以外	18	57.05	2.6	55.8	58.3
	確信度	システムのセキュリティの保守・運用	19	254.9	30.4	240.2	269.6
		システムのセキュリティの保守・運用 以外	6	250.9	19.0	231.0	270.8
		セキュリティ導入の支援	13	247.0	28.9	229.5	264.5
		セキュリティ導入の支援 以外	12	260.6	26.2	244.0	277.2
		システム監視，有事の対応	11	247.5	18.5	235.1	259.9
		システム監視，有事の対応 以外	14	258.4	33.4	239.1	277.7
		ポリシー作成・教育	7	266.4	21.9	246.1	286.7
		ポリシー作成・教育 以外	18	249.2	28.7	234.9	263.5
学習後選択問題 37 問	得点	システムのセキュリティの保守・運用	19	40.00	12.4	34.0	46.0
		システムのセキュリティの保守・運用 以外	6	44.86	5.2	39.4	50.3
		セキュリティ導入の支援	13	39.00	12.2	31.6	46.4
		セキュリティ導入の支援 以外	12	43.62	10.2	37.1	50.1
		システム監視，有事の対応	11	43.73	6.0	39.7	47.8
		システム監視，有事の対応 以外	14	39.53	14.0	31.4	47.6
		ポリシー作成・教育	7	42.14	12.9	30.2	54.1
		ポリシー作成・教育 以外	18	41.00	11.0	35.5	46.5
	確信度	システムのセキュリティの保守・運用	19	66.00	50.6	41.6	90.4
		システムのセキュリティの保守・運用 以外	6	75.71	17.9	56.9	94.5
		セキュリティ導入の支援	13	55.77	46.7	27.5	84.0
		セキュリティ導入の支援 以外	12	81.46	40.2	55.9	107.0
		システム監視，有事の対応	11	73.91	20.0	60.5	87.3
		システム監視，有事の対応 以外	14	64.73	57.4	31.6	97.9
		ポリシー作成・教育	7	69.57	54.5	19.2	120.0
		ポリシー作成・教育 以外	18	68.26	41.9	47.4	89.1

表 45　特定の業務経験の有無のテストの結果への影響の t 検定

Table 45 The t-test results of test score grouped by work experience

		業務経験	t 値	自由度	効果量 r	p 値
学習前共通 40 問	得点	システムのセキュリティの保守・運用	0.87	9	0.28	0.2022
		セキュリティ導入の支援	0.16	23	0.03	0.4387
		システム監視，有事の対応	0.27	22	0.06	0.3934
		ポリシー作成・教育	1.83	14	0.44	0.0443
	確信度	システムのセキュリティの保守・運用	0.39	8	0.14	0.3535
		セキュリティ導入の支援	1.10	23	0.22	0.1409
		システム監視，有事の対応	0.37	23	0.08	0.3590
		ポリシー作成・教育	2.24	10	0.58	0.0245
学習後全体 60 問	得点	システムのセキュリティの保守・運用	0.26	9	0.09	0.4018
		セキュリティ導入の支援	0.58	23	0.12	0.2834
		システム監視，有事の対応	0.33	22	0.07	0.3732
		ポリシー作成・教育	1.36	18	0.31	0.0948
	確信度	システムのセキュリティの保守・運用	0.79	13	0.21	0.2208
		セキュリティ導入の支援	1.17	23	0.24	0.1264
		システム監視，有事の対応	0.96	21	0.20	0.1744
		ポリシー作成・教育	1.72	14	0.42	0.0537
学習後選択問題 37 問	得点	システムのセキュリティの保守・運用	1.28	19	0.28	0.1081
		セキュリティ導入の支援	1.00	23	0.20	0.1631
		システム監視，有事の対応	1.10	18	0.25	0.1432
		ポリシー作成・教育	0.25	10	0.08	0.4047
	確	システムのセキュリティの保守・運用	0.38	23	0.08	0.3523

	信度	セキュリティ導入の支援	1.41	23	0.28	0.0855
		システム監視，有事の対応	0.69	17	0.16	0.2506
		ポリシー作成・教育	0.12	9	0.04	0.4527

表 46　募集方法の平均・標準偏差・95%信頼区間

Table 46 Statistics of test score and degree of confidence grouped by recruiting procedure

			グループ	標本サイズ	平均	標準偏差	95%信頼区間	
							最小	最大
学習前	共通40問	得点	SNS	11	36.27	1.7	35.1	37.4
			チラシ	3	38.00	1.0	35.5	40.5
			知人	12	36.50	2.2	35.1	37.9
		確信度	SNS	11	131.55	31.5	110.4	152.7
			チラシ	3	142.67	33.9	58.3	227.0
			知人	12	138.33	28.8	120.1	156.6
学習後	全体60問	得点	SNS	11	57.64	2.8	55.8	59.5
			チラシ	3	59.00	-	-	-
			知人	12	56.75	2.4	55.2	58.3
		確信度	SNS	11	263.27	26.5	245.5	281.1
			チラシ	3	251.00	46.0	136.6	365.4
			知人	12	245.92	20.3	233.0	258.8
	選択問題37問	得点	SNS	11	41.00	11.6	33.2	48.8
			チラシ	3	45.67	13.5	12.1	79.2
			知人	12	40.50	11.4	33.3	47.7
		確信度	SNS	11	71.82	45.6	41.2	102.5
			チラシ	3	88.33	54.8	-47.8	224.4
			知人	12	60.75	43.8	32.9	88.6

表 47　業務年数ごとの平均・標準偏差・95%信頼区間

Table 47 Statistics of test score and degree of confidence grouped by the length of service of security

			グループ	標本サイズ	平均	標準偏差	95%信頼区間	
							最小	最大
学習前	共通40問	得点	1-2 年	3	38.33	0.6	36.9	39.8
			3-5 年	13	36.54	2.0	35.3	37.8
			5-10 年	10	36.10	2.0	34.7	37.5
		確信度	1-2 年	3	148.00	33.0	65.9	230.1
			3-5 年	13	135.92	30.3	117.6	154.2
			5-10 年	10	132.40	34.5	107.7	157.1
学習後	全体60問	得点	1-2 年	3	58.33	1.5	54.5	62.1
			3-5 年	13	57.62	1.8	56.5	58.7
			5-10 年	10	56.80	3.4	54.4	59.2
		確信度	1-2 年	3	262.33	28.7	191.1	333.6
			3-5 年	13	258.69	20.8	246.1	271.3
			5-10 年	10	245.00	34.5	220.3	269.7
	選択問題37問	得点	1-2 年	3	48.00	7.2	30.1	65.9
			3-5 年	13	42.54	10.0	36.5	48.6
			5-10 年	10	37.70	12.9	28.5	46.9
		確信度	1-2 年	3	94.67	21.2	42.0	147.4
			3-5 年	13	72.46	41.1	47.6	97.3
			5-10 年	10	55.80	51.0	19.3	92.3

表 48　企業規模ごとの平均・標準偏差・95%信頼区間

Table 48　Statistics of test score and degree of confidence grouped by company size

			グループ	標本サイズ	平均	標準偏差	95%信頼区間	
							最小	最大
学習前	共通40問	得点	50-100 人	7	36.00	1.8	34.3	37.7
			100-300 人	12	36.25	2.1	34.9	37.6
			300-1000 人	6	38.00	1.8	36.1	39.9
			1000 人-	1	36.00	-	-	-
		確信度	50-100 人	7	124.57	33.0	94.1	155.1
			100-300 人	12	134.17	30.6	114.7	153.6
			300-1000 人	6	150.17	32.2	116.4	183.9
			1000 人-	1	152.00	-	-	-
学習後	全体60問	得点	50-100 人	7	58.57	2.1	56.6	60.6
			100-300 人	12	56.83	2.8	55.0	58.6
			300-1000 人	6	57.00	2.1	54.8	59.2
			1000 人-	1	58.00	-	-	-
		確信度	50-100 人	7	275.00	13.8	262.3	287.7
			100-300 人	12	242.42	30.5	223.0	261.8
			300-1000 人	6	249.33	21.9	226.4	272.3
			1000 人-	1	270.00	-	-	-
	選択問題37問	得点	50-100 人	7	41.43	13.3	29.1	53.7
			100-300 人	12	39.92	12.8	31.8	48.0
			300-1000 人	6	43.33	5.6	37.5	49.2
			1000 人-	1	45.00	-	-	-
		確信度	50-100 人	7	67.57	56.7	15.1	120.0
			100-300 人	12	65.17	49.3	33.8	96.5
			300-1000 人	6	72.33	17.2	54.3	90.4
			1000 人-	1	95.00	-	-	-

表 49　参加者の分布に基づく一次元配置分散分析の結果

Table 49 the one-way ANOVA results based on demographics

			F 値	p 値	効果量 η^2
応募方法 SNS チラシ 知人	共通40問	得点	F(2,23)=0.9036	0.4190	0.079
		確信度	F(2,23)=0.1997	0.8203	0.017
	全体60問	得点	F(2,23)=1.1068	0.3476	0.096
		確信度	F(2,23)=1.1806	0.3250	0.103
	選択問題37問	得点	F(2,23)=0.2519	0.7795	0.022
		確信度	F(2,23)=0.5011	0.6123	0.044
業務経験年数 1-2 年 3-5 年 5-10 年	共通40問	得点	F(2,23)=1.5301	0.2377	0.133
		確信度	F(2,23)=0.2707	0.7652	0.024
	全体60問	得点	F(2,23)=0.5388	0.5906	0.047
		確信度	F(2,23)=0.8540	0.4388	0.074
	選択問題37問	得点	F(2,23)=1.1717	0.3276	0.102
		確信度	F(2,23)=0.9992	0.3836	0.087
企業規模 50-100 人 100-300 人 300-1000 人 1000- 人	共通40問	得点	F(3,22)=1.4351	0.2595	0.196
		確信度	F(3,22)=0.8048	0.5046	0.11
	全体60問	得点	F(3,22)=0.7886	0.5132	0.108
		確信度	F(3,22)=2.7051	0.0701	0.369
	選択問題37問	得点	F(3,22)=0.1499	0.9286	0.02
		確信度	F(3,22)=0.1435	0.9327	0.02

6.4.3. 議論と制限

6.4.3.1. 実験参加者の制限

本研究は，サンプルサイズについて予備実験で検討を行った上で実施された実験であるが，テストとインタビューの分析結果の両方において，限られた環境下でしか再現・適用できない可能性がある．そこで，募集方法や経験などによる実験参加者の層による影響について確認する．

業務経験の観点では，今回の実験では多くの参加者が複数の業務の経験があった．経験がある順で並べると，システムのセキュリティについての保守・運用者（19 名）が最も多く，次いでセキュリティ導入（支援）(13 名)，システム監視・対応（11 名)，ポリシー作成運用，教育（7 名）と続いた．保守運用経験者の割合が多いが，研究の対象としていない調査や研究に関わる業務を以外の分野が網羅されていることが確認された．6.4.2.4 項の業務経験毎の検定によると，自己学習前の比較で、「ポリシーの作成・教育」の業務経験がある参加者は，経験がない参加者に比べて有意に得点が低かった．しかし，自己学習後においては，この有意差は確認できなかったため，自己学習により差が解消されたと考えられる．効果量 r について確認すると，「ポリシー作成・教育」に関する効果量は選択問題を除き中から大程度を示していた．しかし，それ以外の業務については，効果量はほんどないもしくは小程度であった．したがって，本実験において特に「ポリシー作成・教育」の経験の有無はテストの結果に影響を与えている可能性があると考えられるが，他の要因による効果は少ないと考えられる．一方で，「ポリシー作成・教育」の経験の有無について，各分布を確認すると，実験群で 4 名，統制群で 3 名，CSF 型，役割型，時間軸型では，2 名、2 名，3 名とほぼ均等に分布していたため，その影響はある程度抑えられていると考えらえる．

また，それ以外の要因（実験参加者の募集方法，業務経験年数，企業規模（人数））についても一次元 ANOVA による有意差は確認できなかった．効果量 η^2 について，確認すると，中以上（0.06 以上）の値を取っているものが多数みられ，テストの結果に影響を与えている可能性がある．しかしながら，これらの要因については，実験群と統制群で分布に乖離がないように注意しているため，実験群と統制群の比較においては，その影響はある程度抑えられていると考えられる（表 50)．

表 50　実験群と統制群の参加者の分布

Table 50 the number of participants for each category.

		実験群人数	統制群人数
勤続年数	1～2 年	2	1
	3～5 年	6	7
	6～10 年	5	5
規模	50～100 人	3	4
	100～300 人	6	6

	300〜1000 人	3	3
	1000 人〜	1	0
募集方法	SNS	5	4
	チラシ	2	6
	知人	6	3

6.4.3.2. テストの得点と確信度の制限と議論

自己学習後のテスト結果では，すべてのテストの得点とすべての確信度について，片側ウェルチの t-検定を用いて，実験群と統制群の間に有意な差が検出された．このことから，改良された教材は，より高い学習効果を持ち，この教材を用いた学習者は，セキュリティ対策がどの機能と結びついているかをより理解できていると考えられる．

実験で確認されたメンタルモデルに基づいて分類したグループに対して，一元配置の ANOVA とボンフェローニ法を用いた多重比較を行った．

学習前のテスト結果は，未構造型グループ，役割型グループ，時間軸型グループの 3 つに分けられ，一元配置の ANOVA による検定が行われたがグループ間に有意な差はなかった．学習後のテストの結果は， CSF 型，役割型，時間軸型の 3 つのグループに分けられ，一元配置の ANOVA で検定が行われ，グループ間に有意な差が確認された．多重比較手続きの結果では，CSF 型のメンタルモデルのグループは，他の 2 つのグループよりもテストの得点と確信度が高い傾向にあることが示唆された．その結果，CSF 型のメンタルモデルを持つ人は，他の 2 つの型のメンタルモデルを持つ人より，より自信を持って的確に質問に答え，CSF のフレームワークコアとセキュリティ対策の関係もよく理解していると考えられる．これにより，学習者が CSF のフレームワークコアを適切なメンタルモデルとして身に着けることで，学習に良い影響があることが示唆されたと考える．

6.4.3.3. インタビューにおける制限と議論

観察されたメンタルモデルは，インタビューによる介入の影響を受けたものである．そのため，本来実験参加者が持っていたモデルよりも発展，整理されたものになっている可能性がある．また，インタビューのデータは，自己申告による質的なものであり，コーディングにより分析されたため，他の研究者は違う結論を見出す可能性がある．

インタビューを元にコーディングを実施する場合，一般的にコーディングの分析が十分だと判断できるまで実験を進めるが，本研究においては，テストの実施による検定とあわせて行ったため，予備実験で求めた推定サンプルサイズに基づいて，参加者数を求めている．しかしながら，セキュリティ関連のメンタルモデルを検討する先行研究 [30] [31]においても，約 20〜30 名程度の実験参加者に基づいて質的解析を行っているため，その影響は限定的であると考えられる．

また，今回の質的分析を実行した 2 名については，前提知識として CSF と「中小企業の情報セキュリティ対策ガイドライン」の第 2.1 版および第 3 版について読了済みである他，

予備実験においても同様な手順でコーディングを実施している．そのため，コードや分析にバイアスがある可能性がある．

補足コードについては，その取り扱いについて特に議論された．今回の実験では，ある要素やグループが，道具的な側面を持つか（「システムとツール」）や，外的な制限や決まりごとに関連するか（「環境とルール」），人が要因となるものか（「人と知識」）に言及され，グループの名づけや補足的な説明に用いられた．これらのコードは，活動理論 [84]における「ルール」,「媒介する人工物」,「分業」に類似しており，枠組みの一つとして取り扱うかどうか，議論が行われた．今回の実験においては，単独でこの形式の分類が現れることはなく，あくまで補足的な情報として扱われていたため，また，全ての項目がそろって現れることがなかったため，今回の分析においては，単独の型として扱わず，補足的な付加情報として扱うという結論にいたった．しかしながら，複数の型が組み合わさった事例が今回の実験で確認されたことから，今回の実験では明確に表れてこなかっただけで活動理論に基づく型のメンタルモデルが存在する可能性がある．

また，特に時間軸型の実験参加者において，実行のしやすさ（「手の付けやすい対策」,「手の付けにくい対策」）について説明がなされることがあった．これらの補足コードは実行順序の説明を行う際に順序を定義する基準として用いられることが多かった．これについては，単体で現れず常に，時間軸型のモデルでのみ確認されたことから，補足的な説明要因だと判断した．

個々のコードにおいて，議論が行われたものでは，「要員の確保と責任範囲決め」と「セキュリティへの理解と協力」が挙げられる．これらのコードは，責任者の取り組みという観点でインタビュー中に現れることが多く，理解と協力，要員確保，責任範囲決めの 3 点が一体となって語られる場合が多く付箋としても区別が難しいものが多かった．議論の結果，理解と協力というのは経営者以外でも求められる事例がある点，要員確保と責任範囲決めはどちらも人事的な要素であり不可分だという結論に至り，現在の「要員の確保と責任範囲決め」と「セキュリティへの理解と協力」というコードに決定された．

6.4.3.4. 統計学的な制限

インタビューを伴う実験であるため実験参加者数を多くは確保できていないが，このサンプルサイズは，同様の手順で実施した予備実験の効果量をもとに検出力を 0.8，有意水準 0.5 として計算したサンプルサイズに基づいて決定しているため，影響は限定的であると考えられる．また，今回の実験の結果を基に検出力について計算を行ったところ，確信度と選択問題の項目で高い検出力が確認できた．そのため，少なくともこれらの項目では高い確率で帰無仮説を正しく棄却できると考えられる．

本実験では，改良された教材と通常の教材の効果の差を確認する目的で実験参加者数を決めたため，メンタルモデルのグループに対する多重比較分析をするためのサンプル数が十分ではない可能性がある．そこでボンフェローニ法について効果量 d に基づいて，検出

力の計算を行った．その結果，各型の比較においても，今回着目している CSF 型と他の型との間の比較では，確信度と選択問題の項目で 0.5 以上の検出力が現れており，比較的高い確率で帰無仮説を正しく棄却できると考えられる．

一方で，時間軸型と役割型と未構造型の比較については，検出力が低くタイプ I の誤りに陥っている可能性が十分にあると考えられる．CSF 型と他の 2 つの型の間については，有意な差がある可能性が高いが，他の 2 つの型の間の優劣については判断を行うことができないと考えられる．

6.4.3.5. 混合モデルについて

本実験では，セキュリティ対策の概要については，役割型モデル，時間軸型モデル，フレームワーク（CSF）型モデル，構造化されていないモデルの 4 種類のメンタルモデルが観察され，特に，2 種類のメンタルモデルが組み合わされて 1 つのモデルに統合された事例も確認された．1 つは，CSF 型モデルに役割の情報が加えられたもので，もう 1 つは，役割型モデルに時系列情報を加えたものであった．これらのケースは，情報セキュリティの担当者が複数の視点からメンタルモデルを持ち，それらを統合できることを示唆している．

CSF と役割の混合モデルを用いた参加者 ID-11 は，CSF モデルを用いた参加者よりも得点が低かったため，回答内容について確認したところ，外部のサードパーティのサービスと CSF の機能との関係を問う設問で，ID-11 が誤答したことが確認された．一方で，ID-11 の事後インタビューでは，「第三者の取組」というグループがなかったことより，ID-11 が第三者のサービスについてよく学んでいなかった，あるいは意識していなかったことが示唆される．したがって，このギャップは，混合モデルの特性というよりも，ID-11 の自己学習のミスだと考えられる．また，役割型と時間軸型の複合モデルを持つ ID-13 については，他の役割型と大きく変わらない結果だった．そのため，複合モデルについては，主に用いられている型のほうが有効に働いているものと考えられる．

6.4.3.6. メンタルモデルの変化の仕方について

自己学習によってメンタルモデルの変化が起こることも観察された．実験前には，ほとんどのセキュリティ担当者が時間軸型のモデルを持っていた．これは，普段から業務を順番に計画・実行しているため，時間軸に基づいてセキュリティ対策を容易に想像できるからだと推測される．

学習教材によって学習者のメンタルモデルが変化することも確認された．例えば，実験群では 4 例がフレームワーク型に変化しているのに対して，統制群では 1 例がフレームワーク型に変化している．先行研究の暗号通貨ツール [33]における示唆と同じく，教材のユーザーインタフェースによって，学習者のメンタルモデルが受ける影響が異なる可能性があると考えられる．今回の実験においては Fisher の正確検定で有意な差は確認されなかっ

たが，効果量 h が中程度であったことから，十分な検出力を得る分だけのサンプルサイズで実験を行えばこの有意差を検出できる可能性があると考えられる．

6.4.4. 結論

情報セキュリティ担当者の学習効率を向上させ，包括的で適切なメンタルモデルを導入するために，自己学習中に学習者のメンタルモデルについて確認し，学習者のメンタルモデルと学習効率がどのように関係しているかを解明することを目的に，CSF のフレームワークコアとの関係を明示した教材を作成し比較実験をおこなった．

セキュリティ対策の構成要素に関するインタビューにより，セキュリティ対策の概要を把握するためのモデルとして，役割型，時間軸型，フレームワーク（CSF）型，構造化されていないモデルの 4 種類の型があることを確認した．また，2 種類の型が組み合わされて 1 つのモデルに統合されている混合モデルも観察された．自己学習によるメンタルモデルの変化が観察され，実験群では，統制群よりも CSF 型のモデルへの移行数が多くみられた（ただし，Fisher の正確検定で有意な差は確認されなかった)．

また，テスト結果について，片側ウェルチの t-検定を行った．その結果，実験群と統制群の間には，テストの得点と確信度の両方で統計的に有意な差が見られ，改良後の教材は，理解の促進に効果があると考えられる．

その原因について検討するため，学習後に観察されたメンタルモデルでグループを定義し，一元配置の ANOVA とボンフェローニ法による多重比較を行った．その結果，フレームワーク型のグループと他の 2 つのグループでは有意な差が確認され，フレームワーク型のグループでは CSF コアと実際のセキュリティ対策との関係をよりよく理解し，確かな自信を持って質問に正解することができたと推測された．

そのため，改良された教材は，学習者のメンタルモデルを CSF に基づいたものに変える傾向があり，他の 2 つのメンタルモデルよりも，より適切で包括的なセキュリティ対策の理解を提供していると思われる．

7．総括

7.1. 結論

本研究ではセキュリティ対策の学習者のメンタルモデルに着目し，以下の 3 点を目的として研究を行った．

1） 学習者が既存のガイドラインなどを教材として体系的に学習できるよう，情報セキュリティに関する教材の内容を，体系的な枠組みに基づいて提示すること

2） 教材のユーザーインタフェースを実際に改善するアプローチについて提案すること

3） 教材の改善の効果の確認として，以下の 2 点を明らかにすること

3-1）教材（のインタフェース）が学習者のメンタルモデルにどのように影響を及ぼすか

3-2) メンタルモデルが学習効果とどのように関係するのか

目的の 1）について，TF-IDF によるテキストマイニングにより，対象とする文書の内容を CSF のフレームワークコアに基づいて表示する手法を提案し，その評価を行った．この手法を適用することで，学習者は情報セキュリティに関する文書教材について，フレームワークコアにおけるどのカテゴリや機能に重きを置いた資料なのか把握することができ，CSF に基づいた体制化方略によって自己学習に効果的に行うことができると考える．

目的の 2）について，AH に基づくインタフェースを持った教材の作成のために，前述の提案手法を「中小企業の情報セキュリティ対策ガイドライン　第 3 版」の「章」や「節・項」ごとに適用することにより，文書内の各「章」や「節・項」とフレームワークコアとの関係性を明らかにし，その結果を基に教材のインタフェースの改善を行った．この際用いたアプローチは，「章」や「節・項」の文の短さに制限があると考えられるが，情報セキュリティに関する文書であれば，特定の文書によらず適用可能だと考える．

目的の 3) について，改善した教材を用いて，改善前の教材との比較を行う対照実験を行った．一度，予備実験を行いテスト問題やインタビューの分析方法について調整を行った後，本実験を行った．その結果，学習者のメンタルモデルには，大きく役割型，時間軸型，フレームワーク型，未構造型の 4 つが存在することが確認され，学習によってそれらが変化することを確認した．この際，AH に基づいて改良された教材を用いた実験群では約 3 割が CSF によるフレームワーク型に変化した，一方で，改善前の教材を用いた対象群では 1 割しか変化しなかった．ただし，この点について今回の実験では Fisher の正確検定で有意差は確認されなかった．

また，自己学習後のメンタルモデルの型に基づいて多重比較検定を行ったところ，フレームワーク型のみ有意差が確認された．これにより，フレームワーク型のグループではフレームワークコアと実際のセキュリティ対策との関係をよりよく理解し，確かな自信を持って質問に正解することができたと推測された．

本研究の貢献として，以下が挙げられる．

1）第 4 部において，体系的な文書内容の表現方法の提案を行った
2）5.2 章において，学習者の情報セキュリティ対策に対する 4 つのメンタルモデルの型について明らかにし，第 6 部において特に情報セキュリティ担当者でもそれが変わらず，時間軸型のモデルを持つ場合が多いことを確認した．
3）5.2 章と第 6 部において学習によりメンタルモデルの型が変化することを確認し，特に第 6 部では，改善後の教材を情報セキュリティ担当者が学習した場合，より高い割合で，教材のインタフェースの改良に用いられた CSF を反映したフレームワーク型に変化することを確認した（ただし，Fisher の正確検定で有意な差は確認されなかった）．
4）第 6 部において，フレームワーク型のメンタルモデルを身につけられた場合，他の型に比べて学習の効果が最も高くなることを明らかにした．
5）5.1 章で，既存の教材を適切なメンタルモデルを学習者に身に着けられるインタフェースに改善した．この教材のインタフェースの改善アプローチは，今回用いた教材以外にも利用可能だと考えられる．

7.2. 今後の課題と展望

第 4 部の CSF に基づいて文書の内容を表現する研究の今後の課題として，CSF に基づいた文書内容の提示を行うことで学習効率がどの程度向上するのか，単一の文書における効果については今回の研究で確認されたと考えられるが，複数の文書を用いた学習方略に対する影響については今回の研究では取り扱っていない．そのため，複数の教材を組み合わせた学習による実験の実施が必要であると考える．

第 4 部の提案手法の改善の観点では，fastText [85]，doc2vec [86] などの他のテキスト解析の方法を TF-IDF の代わりに用いることも可能であると考えている．また，文書量の増加や類義語・関連語を利用した精度の向上についても検討することができる．

また，第 4 部の展望として，応用の観点では，セキュリティ分野でも異なるフレームワークを用いて，異なる観点での体制化を試みることが考えられる．例えば，Cybersecurity Workforce Framework を用いることで役割の観点から再整理を行ったり，MITRE ATT&CK を用いることで攻撃者側の観点で再整理を行うことができる可能性がある．提案手法の適用対象としては，本研究においては文書教材を対象としているが，映像教材についても，教材中の発話をスクリプト化することにより，この手法を適用することができる可能性がある．また，異なる分野でも，1）専門性が高く使用される用語が決まっており，2）その分野についての包括的な構造モデルが提示されている分野であれば，同様の手法を用いてそのモデルに基づいた表現を行うことができる可能性があると考えている．

5.1 章の研究の課題として，適用範囲の制限の明確化とより精度の高い対応付けの方法の検討があげられる．本研究においては，50 字前後から提案手法による対応付けが上手くいかなくなる事例を確認したが，より適切な対応付けの方法を検討するためには，まず，これが定量的にどのような関係性になっているのか評価を行う必要がある．この際可能で

あれば，複数の文書において実施できるのが望ましいと考える．

また，展望として，このアプローチ自体は，今回教材として用いた「中小企業の情報セキュリティ対策ガイドライン　第 3 版」以外でも利用可能であると考える．そのため，他のセキュリティ関連文書に対して同様に教材を作成して検証することも検討できると考える．また，今回の研究では，一つの教材のみを対象に改良を行っているが，CSF との対応において相互補完性が高い複数の教材を組み合わせることで，情報セキュリティ対策を包括するような一つの教材にまとめ上げることができる可能性があると考えられる．

第 6 部（及び 5.2 章）の課題として，今回確認されたメンタルモデルの変化がどのくらい続くのか，得られた学習効果がどのくらい続くのかという観点ついては，本研究では調査を行っていない．これには継続的な調査が必要となり今後の課題とする．また，本研究においては，すでに情報セキュリティ業務を担当したことがある人材を対象に実験を行っているが，エキスパート層の育成という観点では，全く情報セキュリティ業務に触れていない一般的な IT 運用者が情報セキュリティについて学ぶ可能性があると考えられる．そこで，情報セキュリティに触れていない IT 運用者に対する影響についても検討する必要があると考える．

また，展望として， CSF の教材以外のインタフェースへの適用が考えられる．例えば，セキュリティインシデント対応に強く関連する Endpoint Detection and Response ツールのユーザーインタフェースを CSF のフレームワークコアを AH として設計することで，ツールの利用により適切なメンタルモデルを身に着けられる可能性があると考える．

謝辞

本研究は，本学筑波大学大学院システム情報工学研究科後期博士課程在学中に，筑波大学の古川 宏 准教授のご指導とご助力のもと行ったものです．5 年の長期履修という機会を頂戴したにもかかわらず仕事と学業の兼ね合いが上手くいかず，発表前や投稿前に先生にご負担をかけることになってしまうことが多く自分の至らなさを恥じるばかりでした．私の求めに応じた先生の丁寧で的確なご指導には大変感謝しております．

筑波大学の亀山 啓輔 教授，面 和成 准教授の両先生には，達成度評価という場を通して（日々の活動を含む）研究について見直す機会を頂戴いたしました．このような振り返りの場を通しての先生方のご助言がなければ，この 5 年間研究を続けることはできていなかったと思います．深く感謝を申し上げます．

東邦大学の金岡 晃　准教授には，先生の主催するセキュリティ心理学とトラスト研究会での発表機会を頂戴するとともに，ユーザブルセキュリティという分野を知る機会を頂戴いたしました．研究テーマについての掘り下げが不十分なまま入学をしてしまい，なかなか方針が定まらない中，先生の主催するセキュリティ心理学とトラスト研究会や勉強会を通してユーザブルセキュリティという分野に触れる機会を得たことで光明を得ることができた思っております．深く感謝を申し上げます．

日本プライバシー認証機構、東京商工会議所のご担当者様には突然のお願いにもかかわらずメールでの相談や対面でのご相談の機会を頂戴し，実験参加者募集のチラシの配布にご協力いただきました．深く感謝を申し上げます．また，ご相談に載ってくださった他団体の皆様にも改めて，深く感謝を申し上げます．

トレンドマイクロ社からは，学費援助プログラムと研究・学習の場の提供により多大なるご助力を頂戴いたしました．援助プログラムのご担当者の方にはさまざまなご配慮を頂戴し頭の上がらぬ思いです．深く感謝を申し上げます．また，自主的な学習会である Advanced Security Learning & Research（ASLR）のみなさまには，研究発表の練習に付き合っていただいたり，アドバイスを頂戴したり一部実験募集やレビューについてご助力をいただいたり，研究を進めるうえで大変助けになりました．ASLR がなければ，博士論文の執筆に至ることはできなかったと考えます．深く感謝を申し上げます．

本研究の過程において，たくさんの皆様にご教示，ご協力をいただきました．ここに記して深く感謝の意を表します．

参考文献

[1] ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary.
[2] JIS Q 27000：2019. 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－用語.
[3] ISO 7498-2 : 1989. Information processing systems－ Open Systems Interconnection－Basic reference model－ Part2 : Security architecture.
[4] JIS X 5004-1991. 開放型システム間相互接続の 基本参照モデル－安全保護体系.
[5] ISO/IEC 27032:2012. Information technology — Security techniques — Guidelines for cybersecurity.
[6] “平成二十六年法律第百四号 サイバーセキュリティ基本法,”.https://elaws.e-gov.go.jp/document?lawid=426AC1000000104. [アクセス日: 27 11 2021].
[7] 独立行政法人情報処理推進機構　技術本部 セキュリティセンター, “「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/. [アクセス日: 23 11 2021].
[8] 独立行政法人情報処理推進機構 技術本部 セキュリティセンター, “「情報セキュリティ人材の育成に関する基礎調査」 - 調査報告書 -,” 2012 年 4 月 .
[9] 独立行政法人情報処理推進機構 技術本部セキュリティセンター, “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）,” 2014 年 7 月 30 日.
[10] “「情報セキュリティ事故対応ガイドブック」の公開,” . http://lab.iisec.ac.jp/~hiromatsu_lab/sub07.html. [アクセス日: 23 11 2021].
[11] “情報セキュリティ事故対応に関わるアンケート調査,” 情報セキュリティ大学院大学, 2022 年　3 月.
[12] “J-CSIP「標的型攻撃／新しいタイプの攻撃の実態と対策」の一部訂正とお詫びについて,” . https://www.ipa.go.jp/security/J-CSIP/presentation2_errata_01.html. [アクセス日: 27 11 2021].
[13] 独立行政法人情報処理推進機構 技術本部 セキュリティセンター, “標的型攻撃／新しいタイプの攻撃の実態と対策,” 2011.
[14]　　経済産業省 商務情報政策局, “産業分野におけるサイバーセキュリティ政策,” . https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/001_05_00.pdf. [アクセス日: 27 11 2021].
[15] “情報セキュリティ 10 大脅威 2021,” . https://www.ipa.go.jp/security/vuln/10threats2021.html. [アクセス日: 27 11 2021].
[16] “平成十五年法律第五十七号　個人情報の保護に関する法律,” . https://elaws.e-gov.go.jp/document?lawid=415AC0000000057. [アクセス日: 27 11 2021].

[17] “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,” . https://www.nisc.go.jp/conference/cs/jinzai/wg2/index.html. [アクセス日: 23 11 2021].
[18] 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, “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　～「戦略マネジメント層」の育成・定着に向けて～,”
[19] “産業横断サイバーセキュリティ検討会,” . https://cyber-risk.or.jp/.[アクセス日: 23 11 2021].
[20] “報告書　産業横断サイバーセキュリティ検討会,” . https://cyber-risk.or.jp/cric-csf/report/.[アクセス日: 23 11 2021].
[21] 一般社団法人サイバーリスク情報センター　産業横断サイバーセキュリティ人材育成検討会, “「産業横断サイバーセキュリティ人材育成検討会」　第二期最終報告書,”.
[22] “Web Archiving Project－セキュリティ関連コンテンツ一覧,” . https://warp.da.ndl.go.jp/info:ndljp/pid/9968513/www.meti.go.jp/policy/netsecurity/secdoc/secdoc_list.html. [アクセス日: 27 11 2021].
[23] “サイバーセキュリティ政策,” . https://www.meti.go.jp/policy/netsecurity/index.html. [アクセス日: 27 11 2021].
[24] “サイバーセキュリティ経営ガイドライン,” . https://www.meti.go.jp/policy/netsecurity/mng_guide.html. [アクセス日: 27 11 2021].
[25] 克. 鈴木, 教材設計マニュアル　独学を支援するために, 北大路書房, 2002 年.
[26] Kenneth Craik , The Nature of Explanation, 1943.
[27] “The Mental Models Global Laboratory,” . https://www.modeltheory.org/. [アクセス日: 1 12 2021].
[28] 土井 俊央, 村田 厚生, 味間 智志, “メンタルモデル構築のし易さから見たタッチパネルＧＵＩの画面構成の評価,” デザイン研究, 64 巻, 3 号, pp. 31-40, 2017.
[29] NIST, CYBERSECURITY FRAMEWORK . https://www.nist.gov/cyberframework. [アクセス日: 23 11 2021].
[30] K. Krombholz, K. Busse, K. Pfeffer, M. Smith , E. V. Zezschwitz, “If HTTPS Were Secure, I Wouldn’t Need 2FA-End User and Administrator Mental Models of HTTPS,” : IEEE Symposium on Security and Privacy (SP) Proceedings, USA, 2019.
[31] J. Wu, D. Zappala, “When is a Tree Really a Truck? Exploring Mental Models of Encryption,” 14th SOUPS Proceedings, 395–409, USA, 2018.
[32] K. R. Fulton, R. Gelles, A. McKay, R. Roberts, Y. Abdi, M. L. Mazurek, “The Effect of Entertainment Media on Mental Models of Computer Security,”: 14th SOUPS Proceedings,79–95, USA, 2019.

[33] A. Mai, K. Pfeffer, M. Gusenbauer , E. Weippl, K. Krombholz, “User Mental Models of Cryptocurrency Systems - A Grounded Theory Approach,”: 16th SOUPS Proceedings, 341–358, USA, 2020.
[34] M. Katsantonis, P. Fouliras, I. Mavridis, “Conceptual Analysis of Cyber Security Education based on Live Competitions,” : IEEE EDUCON Proceedings,, USA, 2017.
[35] K. Yonemura, K. Yajima, R. Komura, J. Sato, Y. Takeichi, “Practical security education on operational technology using gamification method,” : IEEE ICCSCE Proceedings, Malaysia, 2017.
[36] M. Yamauchi, M. Sakakura, T. Oshima, H. Sunahara, “Design and evaluation for cybersecurity incident handling exercise considering interorganizational communication,” Computer Software, vol.38, no.1, pp. 18-30, 2021.
[37] C. W. Yooa, G. L. Sandersb, R. P.Cervenya, “Exploring the Influence of Flow and Psychological Ownership on Security Education, Training and Awareness Effectiveness and Security Compliance,” Decision Support Systems, vol.108, p. 107–118, 2018.
[38] 孫 英敬, 山口 由紀子, 嶋田 創, 高倉 弘喜, “技術能力に注目した情報セキュリティ教育課程開発のためのカリキュラム分析,” 情報処理学会論文誌, 58 巻, 5 号, pp. 1163-1174, 2017.
[39] “National Institute of Standars and Technology,” . https://www.nist.gov/. [アクセス日: 23 11 2021].
[40] R. Petersen, D. Santos, K. Wetzel, M. Smith, G. Witte, “National NIST Special Publication 800-181 Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework,” U.S. Department of Commerce, USA, 2017.
[41] R. Petersen, D. Santos, K. Wetzel, M. Smith, G. Witte, “NIST Special Publication 800-181 Workforce Framework for Cybersecurity (NICE Framework),” U.S. Department of Commerce, USA, 2020.
[42] K. J. Vicente, J. Rasmussen., “Ecological Interface Design: Theoretical Foundations,” IEEE Transactions on Systems, Man, and Cybernetics, vol.22, non.4, p. 589–606, 1992.
[43] K. J. Vicente, “Ecological Interface Design: Progress and Challenges,” Human Factors, vol.44, non.1, pp. 62-78, 2002.
[44] C. M. Burns , J. Hajdukiewicz, ”Ecological Interface Design, Boca Raton”: CRC Press, 2004.
[45] H. Furukawa, “A learning method to support user's understanding about complex systems based on functional models: an empirical study on young and elderly users of mobile phones,” : Proc. UKSim 13th International Conference on Computer Modelling and Simulation pp.370-375, Cambridge, United Kingdom, 2011.

[46] “セキュリティ関連 NIST 文書,” . https://www.ipa.go.jp/security/publications/nist/index.html. [アクセス日: 23 11 2021].
[47] National Institute of Standards and Technology (翻訳監修　独立行政法人　情報処理推進機構, 重要インフラのサイバーセキュリティを改善するためのフレームワーク　1.1 版, https://www.ipa.go.jp/files/000071204.pdf. [アクセス日: 23 11 2021].
[48] ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems — Requirements.
[49] JIS Q 27001:2014. 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.
[50] “CIS Critical Security Controls Version 8,” . https://www.cisecurity.org/controls/v8/. [アクセス日: 23 11 2021].
[51] E. M. Hutchin, M. J. Cloppert , R. M. Amin, “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains,” . https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf. [アクセス日: 30 11 2021].
[52] “Cyber Kill Chain,” . https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html. [アクセス日: 23 11 2021].
[53] “MITRE ATT&CK,” . https://attack.mitre.org/. [アクセス日: 23 11 2021].
[54] B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington , C. B. Thomas, “MITRE ATT&CK: Design and Philosophy,” . https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf. [アクセス日: 1 12 2021].
[55] B. J. Zimmerman. “Becoming a self-regulated learner: Which are the key subprocesses?,” Contemporary Educational Psychology, vol.11, non.4, pp. 307-313, 1986.
[56] B. J. Zimmerman, “A social cognitive view of self-regulated academic learning,” Journal of Educational Psychology, vol.81, non.3, p. 329–339, 1989.
[57] 松. 光奉, “学習内容の体制化と図作成方略が現在完了形の学習に及ぼす効果,” 教育心理研究, 55 巻, pp. 414-425, 2007.
[58] 尾崎敏司, “情報セキュリティに関連するガイドラインの Cybersecurity Framework に基づいた文書内容の可視化手法の提案とその評価,” 情報処理学会論文誌,　60 巻, 12 号, pp. 2196-2210, 2019.
[59] G.Salton, E.A.Fox , H.Wu, “Extended Boolean Information Retrieval,” CACM, vol.26, non.11, pp. 1022-1036, 1983.
[60] D. Park, S. Kim , J. Lee, J. Choo, “Nicholas Diakopoulos, and Niklas Elmqvist, ConceptVector: Text Visual Analytics via Interactive Lexicon Building using Word

Embedding,” IEEE TRANSACTIONS ON VISUALIZATION AND COMPUTER GRAPHICS, vol.24, non.1, pp. 361-370, 2018.
[61] 赤石 美奈, “文書群に対する物語構造の動的分解・再構成フレームワーク,” 人工知能学会論文誌, 21 巻, 5A 号, pp. 428-438, 2006.
[62] scikit-learn, “scikit-learn Machine Learning in Python,” . https://scikit-learn.org/stable/. [アクセス日: 23 11 2021].
[63] T. Kudo, K. Yamamoto, Y. Matsumoto, “Applying Conditional Random Fields to Japanese Morphological Analysis,” : Proceedings of the 2004 Conference on Empirical Methods in Natural Language Processing, pp.230-237, 2004.
[64] “中小企業の情報セキュリティ対策ガイドライン 2.1 版,” . https://www.tokyo-kosha.or.jp/support/josei/setsubijosei/documents/29_cyber_guide02.pdf. [アクセス日: 27 11 2021].
[65] 個人情報保護委員会. https://www.ppc.go.jp/.
[66] 個人情報保護委員会事務局, “中小規模事業者向け はじめてのマイナンバーガイドライン,” . https://www.ppc.go.jp/files/pdf/chusho_my_number_guideline.pdf. [アクセス日: 23 11 2021].
[67] 個人情報保護委員会, “特定個人情報の適正な取扱いに関するガイドライン,” . https://www.ppc.go.jp/legal/policy/. [アクセス日: 23 11 2021].
[68] 中小企業庁, 中小企業ＢＣＰ（事業継続計画）ガイド, 平成 20 年 3 月.
[69] “中小企業 BCP 策定運用方針,” . https://www.chusho.meti.go.jp/bcp/. [アクセス日: 23 11 2021].
[70] NPO　日本ネットワークセキュリティ協会, “NPO　日本ネットワークセキュリティ協会,” . https://www.jnsa.org/. [アクセス日: 23 11 2021].
[71] “出社してから退社するまで中小企業の情報セキュリティ対策実践手引き （西日本支部 出社してから退社するまでのリスク対策ワーキンググループ）,” . https://www.jnsa.org/result/2013/chusho_sec/index.html. [アクセス日: 23 11 2021].
[72] NPO ネットワークセキュリティ協会　西日本支部, 出社してから退社するまで中小企業の情報セキュリティ対策実践手引き　改訂版, 2014.
[73] S. Ozaki, “Improving the training material of the information security based on Cybersecurity,” : HCII Proceedings 2020 -Posters, Heidelberg, 2020.
[74] 独立行政法人情報処理推進機構セキュリティセンター, “中小企業の情報セキュリティ対策ガイドライン　第 3 版,” . : https://www.ipa.go.jp/files/000055520.pdf. [アクセス日: 28 11 2021].
[75] 独立行政法人情報処理推進機構　セキュリティセンター, “中小企業の情報セキュリティ対策ガイドライン,” . https://www.ipa.go.jp/security/keihatsu/sme/guideline/. [アクセス日: 28 11 2021].

[76] K. Krippendorff, “Content Analysis. An Introduction to its Methodology”, Beverly Hills, CA: Sage Publications, 1980.
[77] J. R. Landis, G. G. Koch, “The Measurement of Observer Agreement for Categorical Data,” Biometrics, vol.33, non.1, 1977.
[78] J. Cohen, “A coefficient of agreement for nominal scales,” Educational and Psychological Measurement, vol.20, non.1, p. 37–46, 1960.
[79] “Abobe XD | UI/UX デザインと共同作業ツール【アドビ公式】,” . : https://www.adobe.com/jp/products/xd.html. [アクセス日: 26 12 2021].
[80] S. Ozaki , H. Furukawa, “Study on the Impact of Learning About Information Security Measures on Mental Models: Applying Cybersecurity Frameworks to Self-learning Materials,” : Proc. of HCI for Cybersecurity, Privacy and Trust, 2021.
[81] “Cacoo,” . https://cacoo.com/ja/. [アクセス日: 29 11 2021].
[82] W. G. Cochran, “Some methods for strengthening the common $\chi 2$ tests,” Biometrics, vol.10, pp. 417-51, 1954.
[83] R. A. Fisher , “On the interpretation of $\chi 2$ from contingency tables, and the calculation of P,” Journal of the Royal Statistical Society , vol.85 , non.1, pp. 87-94, 1922.
[84] Y. Engeström , “Learning by Expanding: An Activity-Theoretical Approach to Developmental Research”. Helsinki: Orienta-Konsultit.1987（ユーリア エンゲストローム, 百合草 禎二（訳）, 庄井 良信（訳）, 松下 佳代（訳）, 保坂 裕子（訳）, 手取 義宏（訳）, 高橋 登（訳）, 山住 勝広（訳）, 拡張による学習―活動理論からのアプローチ, 東京: 新曜社, 1999.
[85] “fastText,” . https://fasttext.cc/. [アクセス日: 9 12 2021].
[86] Q. Le, T. Mikolov, T. , “Distributed Representations of Sentences and Documents,” Proceedings of the 31st International Conference on Machine Learning, vol.32, non.2, pp1188-1196, 2014.

付録 1. 枠組みを用いないテキストマイニング手法の適用結果の検討

現在，文書の内容分析については多くの手法が提案されており，そのほとんどが枠組みに基づかない手法である．本付録では，枠組みを用いない手法を第 4 部で解析の対象とした文書に対して適用をして，CSF に基づいて評価することにより，どのような問題が考えられるのか検討を行う．すべての手法を試すのは不可能であるため，特に代表的な手法と思われるクラスタリングとトピック分析を実施して評価した．具体的には，解析対象の 4 つの文書それぞれについて，TF-IDF と k 平均法を用いたクラスタリング，と Latent Dirichlet Allocation (LDA) [87]によるトピック分析を用いて文書内容の分類を行い，フレームワークコアの機能との関連性に基づいてその分類結果について検討した．

付録 1.1. Cybersecurity Framework の機能の特徴語の抽出

枠組みを用いないテキストマイニングの結果が，CSF のフレームワークコアのどの機能に類似しているかを比較するために，TF-IDF を用いて，機能ごとの特徴語を計算した．計算では，4.3.2 節で「重要インフラのサイバーセキュリティを改善するためのフレームワーク　1.1 版」から抽出したカテゴリ C_i についての記述をそれぞれの機能ごとにまとめて，機能についての文書とし，機能の文書の間で TF-IDF の計算をおこなった．特徴語ベクトルの次元は 376 次元で，各カテゴリの上位 10 の単語については，表 51 として記載した．

表 51　機能ごとの特徴語 上位 10 個

Table 51　Top 10 words extracted for each Function by TF-IDF

文書名	機能毎の特徴語　上位 10 個　()は TF-IDF の値
Identify(識別)	ビジネス(0.35377) ,リスク(0.34304) ,管理(0.32180) ,サイバーセキュリティリスク(0.26164) ,組織(0.22458),順位(0.17688),優先(0.17688) ,理解(0.17275) ,機能(0.17033) ,特定(0.17029)
Protection(防御)	保護(0.48204) ,防御(0.31241),アクセス(0.28507) ,情報(0.20460) ,制御(0.19916) ,技術(0.19916) ,トレーニング(0.19525) ,向上(0.19135) ,意識(0.18744) ,保守(0.17182)
Detection(検知)	検知(0.70770),異常(0.28660) ,モニタリン(0.27327) ,サイバーセキュリティイベント(0.23486) ,イベント(0.21521) ,継続(0.18919) ,タイムリー(0.16286),発見(0.15633) ,機能(0.14898) ,セキュリティ(0.12722)
Response(対応)	対応(0.62111) ,サイバーセキュリティイベント(0.23948) ,分析(0.23292) ,低減(0.23186) ,対処(0.20609) ,機能(0.19641) ,支援(0.18868) ,検知(0.18706) ,実施(0.16572) ,計画(0.15965)
Recovery(復旧)	復旧(0.64329) ,計画(0.26673) ,機能(0.23887) ,サイバーセキュリティイベント(0.20397) ,阻害(0.16710) ,軽減(0.16710) ,実現(0.16710) ,状態(0.16710) ,改善(0.14121) ,策定(0.13481)

付録 1.2. TF-IDF と k 平均法によるクラスタリング

今回の提案手法では TF-IDF を用いているため，同様に TF-IDF を用いたクラスタリングを行いその結果についての検討を行った． 各解析対象の文書を対象に TF-IDF を用いて特徴語ベクトルを作成し，k 平均法 [88]を用いてクラスタリングを行った．k 平均法は非

階層型のクラスタリングのアルゴリズムで，最初に n 個のデータ x_i(i=1,…,k)にランダムに k 個のクラスタを割り振った後，各クラスタの中心 C_j (j=1,…,k)と各 x_i の距離を求め x_i に最も近いクラスタに割り当て直すことを，x_i の割り当てが変化しなくなる（もしくは変化量が一定の閾値を下回る）まで繰り返すことで k 個のクラスタを得る．そのため，k 平均法は対象の集合を指定した個数のクラスタに分割することができる．今回の実験では，TF-IDF による特徴語ベクトルの空間に対して，クラスタの数は CSF の機能の数に合わせて 5 と設定して，k 平均法によるクラスタリングを実施した．

具体的には，解析対象の文書それぞれに対して，以下の手順で解析を実施した．手順の図示を図 41 記載する．

1)文書中の 1 行を一つの文章とし，Mecab を用いてその標準辞書で分かち書きと形態素解析を行い名詞の文書集合を作成した．

2)作成した文書集合を用いて正規化した TF-IDF を計算し，各文書の特徴語ベクトルを作成した．

3)scikit-learn を用いて，クラスタの数を 5 として設定して，k 平均法によるクラスタリングを実施した．

各クラスタの特徴について把握するために，各クラスタの中心における特徴語ベクトルのうち，上位 10 個を抽出した．この結果は，表 52 の「各クラスタの特徴語上位 10 個」に記載する．

この検証において k 平均法の距離尺度で非類似度であるユーグリッド距離を利用しているようにみえるが，本研究における TF-IDF の定義から，実際には提案手法と同じくコサイン類似度を用いた分析となっている．

ユーグリッド空間でベクトルX_1，X_2を考えて，この 2 つの距離を正規化すると以下の関係が成立する．

$$\|\mathrm{X}_1 - \mathrm{X}_2\|_2^2 = \mathrm{X}_1^{\mathrm{T}}\mathrm{X}_1 + \mathrm{X}_2^{\mathrm{T}}\mathrm{X}_2 - 2\mathrm{X}_1^{\mathrm{T}}\mathrm{X}_2 = 2 - 2\cos(\mathrm{X}_1, \mathrm{X}_2) \quad \text{.....式 11}$$

右辺の $\cos(\mathrm{X}_1, \mathrm{X}_2)$ がコサイン類似度である．従って，コサイン類似度を最大化するためには，正規化した距離が最小になるようにすれば良いことが分かる．4.3.1 節での TF-IDF の scikit-learn でのデフォルトでの定義より，本研究では正規化した値を採用しているため，実際には、ユーグリッド距離によるクラスタリングではなくコサイン類似度によるクラスタリングになっている．

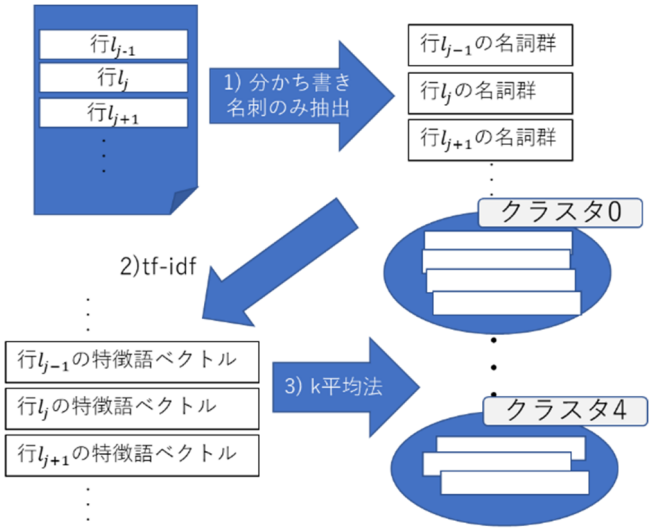


図 41　TF-IDF と k 平均法によるクラスタリングとの手順

Figure 41　Schematic diagram of the experimental procedure for TF-IDF and k-means cluster

表 52　各文書での TF-IDF と k 平均法によるクラスタリングの結果

Table 52　Results of the TF-IDF and k-means clustering for each document

文書名	ID	クラスタに属する文章割合	各クラスタの特徴語上位 10 個　() はクラスタの中心からの距離
中小企業のサイバーセキュリティ対策ガイドライン 第2.1版	0	0.69885	情報(0.02856),場合(0.01983),個人(0.01821),評価(0.01783),利用(0.01698),事故(0.01675),管理(0.01552),発生(0.01536),経営(0.01527),業務(0.01375)
	1	0.17449	対策(0.18686),セキュリティ(0.16468),情報(0.14280),実施(0.04883),ポリシー(0.04310),必要(0.03864),組織(0.02491),実行(0.02390),経営(0.02285),検討(0.02228)
	2	0.05314	重要(0.32306),度(0.20306),取組(0.12208),情報(0.08597),管理(0.04146),資産(0.03906),算定(0.03883),値(0.03826),判断(0.03647),記入(0.03273)
	3	0.03100	ガイドライン(0.3846),中小(0.37181),企業(0.35302),セキュリティ(0.26426),情報(0.23549),対策(0.22681),不利益(0.04112),ポリシー(0.03777),重要(0.02922),策定(0.02353)
	4	0.04252	リスク(0.43500),値(0.15342),大(0.08709),算定(0.06775),実施(0.05376),対策(0.05018),分析(0.04246),小(0.03734),もの(0.03488),資産(0.03139)
中小企業向けのサイバーセキュリティお取引先様へのお願いガイド	0	0.56809	等(0.06108),社(0.04444),会社(0.03704),ルール(0.02963),保管(0.02653),提供(0.02368),ページ(0.02114),取得(0.02106),策定(0.02014),漏えい(0.02007)
	1	0.21401	委託(0.6672),先(0.1712),再々(0.1253),必要(0.07223),監督(0.06806),許諾(0.06631),者(0.05391),場合(0.04593),最初(0.03182),同様(0.02976)
	2	0.08560	個人(0.2094),番号(0.1587),情報(0.1108),必要(0.1107),特定(0.1003),等(0.09197),廃棄(0.06397),適切(0.06290),場合(0.05693),監督(0.05212)
	3	0.07393	措置(0.37213),安全(0.3684),管理(0.3613),物理(0.1227),人的(0.08918),技術(0.08678),組織(0.08295),適正(0.07380),取扱い(0.07067),者(0.05513)
	4	0.05837	者(0.28143),事業(0.2021),取扱(0.15215),事務(0.14225),担当(0.13453),規模(0.13401),中小(0.10849),等(0.06162),情報(0.06053),特定(0.05778)
中小企業BCP（事業継続計画）ガイド	0	0.76885	員(0.19636),従業(0.17962),企業(0.14986),中小(0.10533),等(0.03995),安否(0.038226),ｂｃｐ(0.03527),確認(0.03290),家族(0.03027),時(0.02902)
	1	0.05068	事業(0.24649),復旧(0.15476),中核(0.15051),目標(0.09285),継続(0.09193),時間(0.09128),計画(0.03599),時(0.03017),経営(0.02677),特定(0.02575)
	2	0.01545	担当(0.60588),社員(0.40559),調達(0.09212),輸送(0.07909),搬送(0.07853),経理(0.07722),調整(0.07675),加工(0.07088),避難(0.02913),用(0.02585)

	3	0.07169	緊急(0.01327),時(0.01282),等(0.01163),社(0.01146),工場(0.01139),ｂｃｐ(0.01122),連絡(0.01102),確保(0.01023),代替(0.00961),資金(0.00939)
	4	0.09333	bcp(0.39292),企業(0.12469),導入(0.10977),策定(0.06965),運用(0.05710),済み(0.05058),サイクル(0.04360),中小(0.04050),発動(0.03278),会社(0.03135)
出社して社で業セテ実き小情報リテ策引き中のキュ対手践(改訂版)	0	0.71998	情報(0.04748),影響(0.02871),性(0.02829),実体(0.02775),備考(0.02570),運用(0.02518),ポイント(0.02488),処(0.02321),サービス(0.02247),保存(0.02198)
	1	0.03205	管理(0.18360),記憶(0.17526),媒体(0.17464),策(0.16805),メモリ(0.15172),usb(0.15063),関連(0.14567),アプリケーション(0.13664),ネットワーク(0.13356),項目(0.07300)
	2	0.11500	対策(0.42138),セキュリティ(0.24812),人的(0.19670),技術(0.19415),目的(0.16577),現状(0.15350),レベル(0.14550),情報(0.00560),記述(0.00461),シート(0.00405)
	3	0.08805	責任(0.70439),実施(0.69439),参考(0.00934),本人(0),管理(0),員(0),従業(0),システム(0),外(0),要因(0
	4	0.04492	者(0.40052),本人(0.31734),管理(0.26461),員(0.25278),従業(0.25248),システム(0.22107),外(0.17806),要因(0.17748),偶発(0.12668),訪問(0.12284)

付録 1.3. k 平均法によるクラスタリングの適用結果の検討

各クラスタリングの特徴語を基に各クラスタのラベルを考案した．この結果を表 14 の「ラベル」に記載した．付けられたラベルを見る限りでは，どの文書においても概ねその文書の代表的な話題を表現しているように見える．その一方で，これらのラベルは，CSF のフレームワークコアの機能と比較すると下記のような印象をうけた．

1) セキュリティ対策に関係のない分類がある

2)（一文書内での）分類に偏りがある

3) 体系立てられた分類にはなっていない

そこで，各クラスタと各機能の間の関係性を把握するため各クラスタの中心での特徴語ベクトルと 4.3.2 節で計算した機能の特徴語ベクトルの間のコサイン類似度を計算し，それらの傾向の類似性について確認を行った．その結果を，カラーコード表示（緑：低⇔赤：高）とともに表 53 に記載する．

表 53　各クラスタの中心の特徴語ベクトルとワークコアの機能の特徴語ベクトルのコサイン類似度

Table 53　Cosine Similarity between feature words vector of cluster center and one of Function of Framework Core

文書名	a) 中小企業の情報セキュリティ対策ガイドライン				
クラスタID	0	1	2	3	4
ラベル	個人情報の管理	セキュリティ対策ポリシー	資産管理	企業向けのガイドラインによる対策	リスク管理
Identify(特定)	0.2325	0.1159	0.2029	0.1129	0.3405
Protection(防御)	0.2718	0.2911	0.2025	0.1514	0.0945
Detection(検知)	0.1103	0.1921	0.0384	0.0917	0.0408
Response(対応)	0.1991	0.1607	0.0404	0.0488	0.0920
Rcovery(復旧)	0.1242	0.1021	0.0267	0.0339	0.0322

文書名	b) 中小企業向けはじめてのマイナンバーガイドライン				
クラスタID	0	1	2	3	4
ラベル	情報の管理	委託先の監督	個人番号	物理的な安全管理	事業者の取り扱い
Identify(特定)	0.0625	0.0251	0.1267	0.2287	0.1346
Protection(防御)	0.1506	0.0185	0.1234	0.1165	0.0580
Detection(検知)	0.0381	0.0071	0.0672	0.0173	0.0202
Response(対応)	0.0598	0.0190	0.0825	0.0237	0.1077
Rcovery(復旧)	0.0628	0.0116	0.0382	0.0240	0.0581

文書名	c) 中小企業BCP（事業継続計画）ガイド				
クラスタID	0	1	2	3	4
ラベル	事業継続計画での従業員の安否確認	中核事業の復旧計画	輸送調達搬送などの調整	工場における緊急時のBCP	企業でのBCP導入
Identify(特定)	0.0817	0.1552	0.0002	0.1115	0.0660
Protection(防御)	0.0262	0.0449	0.0093	0.1214	0.0208
Detection(検知)	0.0128	0.0607	0.0000	0.0571	0.0145
Response(対応)	0.0490	0.0547	0.0044	0.1450	0.0199
Rcovery(復旧)	0.0505	0.2993	0.0048	0.1372	0.0531

文書名	d) 出社してから退社するまで中小企業の情報セキュリティ対策実践手引き				
クラスタID	0	1	2	3	4
ラベル	情報運用の影響	IT環境の管理	セキュリティ対策	実施責任	システムの管理
Identify(特定)	0.1954	0.1525	0.0446	0.0118	0.1411
Protection(防御)	0.2811	0.0817	0.1817	0.0979	0.0548
Detection(検知)	0.0895	0.0095	0.1247	0.0635	0.0180
Response(対応)	0.1236	0.0076	0.0739	0.1163	0.0302
Rcovery(復旧)	0.0974	0.0069	0.0541	0.0745	0.0661

まず，「中小企業向けはじめてのマイナンバーガイドライン」のクラスタ ID1 の「委託先の監督」や，「中小企業 BCP（事業継続計画）ガイド」のクラスタ ID2 の「輸送・調達・搬送などの調整」のように，どの機能とも類似性の低い項目が確認された．これらは 1) のセキュリティ対策に直接関係のない分類であると考えられる．

また，例えば「中小企業の情報セキュリティ対策ガイドライン」では，5 つすべてのクラスタで，Identify(特定)の機能との間で他の機能に比べて相対的に高い類似性を示しており，それにより 2)のような分類に対する偏りを感じたものと考えられる．

一つの機能と強く類似しているクラスタは，3 つのみ（「中小企業の情報セキュリティ対策ガイドライン」のクラスタ ID4 の「リスク管理」，「中小企業向けはじめてのマイナンバーガイドライン」のクラスタ ID3 の「物理的な安全措置」，「中小企業 BCP（事業継続計画）ガイド」のクラスタ ID1 の「中核事業の復旧計画」）であり，残りのクラスタは，複

数の機能と類似した部分もっていると考えられる．CSF は一つの体系化されたセキュリティ対策の枠組みであるため，これから外れていることで，3)の体系化されていないという印象を得たものと考えられる．

付録 1.4.トピック分析

クラスタリングを適用した場合と同様に，潜在的なトピックの存在を仮定するトピック分析の手法を対象の文書に適用した結果について検討を行った．トピック分析とは，文書が複数の潜在的なトピックから確率的に生成されると仮定するトピックモデルに基づいたテキストマイニング手法である．トピックモデルは，文書が複数の潜在的なトピックから確率的に作り出されていると仮定したモデルのことで，文書内の各単語は特定のトピックが持つ確率モデルに従って出現すると仮定される．トピックモデルにおいては，一つの文書を複数の似たトピックに関連付けることが可能になる．各解析対象の文書に対して gensim [89]を用いて LDA によるトピック分析を実施した．LDA は，日本語では潜在的ディリクレ配分法と呼ばれる手法で，トピックの分布にディレクトリ分布を仮定してベイズ推定を行うトピックモデルの一種である．LDA によるトピック分析では，ある個数のトピックが文書内に潜在していると仮定して解析をおこなう．今回の実験では，CSF の機能の数に合わせて 5 つとした．

具体的には，解析対象の文書それぞれに対して，以下の手順で解析を実施した．手順の図示を図 42 に記載する．

1） 文書中の 1 行を一つの文章とし，Mecab を用いてその標準辞書で分かち書きと形態素解析を行い名詞の文書集合を作成した．
2） 作成した文書集合に対して，gensim を用いて，LDA によるトピックモデルを作成した．
3） この際トピックの数は 5 としている．

各トピックの特徴について把握するため，トピックの出現確率が高い上位 10 個の特徴語を抽出した．その結果については表 54 の「各文書でのトピック分析の結果」に記載する．

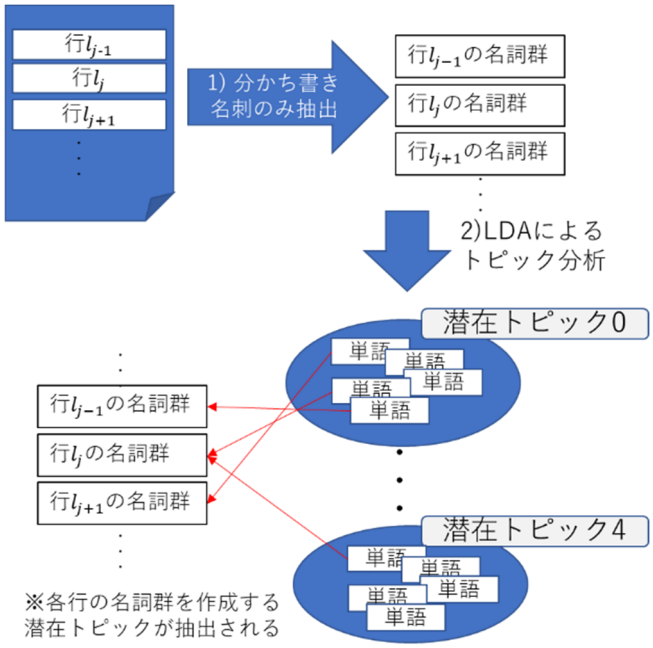


図 42　トピック分析の手順

Figure 42　Schematic diagram of the experimental procedure for topic analysis

表 54　各文書でのトピック分析の結果

Table 54　Results of the topic analysis for each document

文書名	ID	トピック分布	各トピックの特徴語上位 10 個　（）はそのトピックでの単語の修験頻度
中小企業情報セキュリティ対策ガイドライン	0	0.0667	必要(0.03955),管理(0.02585),組織(0.02514)攻撃(0.02100),委託(0.01817),確認(0.01786),リスク(0.01638),実施(0.01587),重要(0.01480),脅威(0.014730)
	1	0.6675	利用(0.03893),重要(0.03505),管理(0.03068),脅威(0.02035),ポリシー(0.02032),脆弱(0.02032),必要(0.01894),資産(0.01735),自社(0.01605),責任(0.01422)
	2	0.06778	実施(0.03551),企業(0.03373),場合(0.03120),可能(0.02179),先(0.01930),ガイドライン(0.01745),ウイルス(0.01654),中小(0.01630),実行(0.01516),事業(0.01432)
	3	0.73175	企業(0.05300),ガイドライン(0.04213),中小(0.03897),リスク(0.02880),値(0.02081),場合(0.01717),発生(0.01711),重要(0.01607),度(0.01406),漏えい(0.01405)
	4	0.06706	個人(0.03154),経営(0.02648),自社(0.02088),事故(0.01992),従業(0.01659),員(0.01600),責任(0.01545),利用(0.01483),管理(0.01449),資産(0.01429)
中小企業初めてのマイナンバーガイドライン	0	0.05007	委託(0.06955),場合(0.06889),監督(0.06856),番号(0.05833),先(0.05220),提供(0.05138),廃棄(0.04385),保管(0.04346),必要(0.04140),担当(0.03498)
	1	0.05000	事務(0.08497),取扱(0.08290),委託(0.05833),適切(0.05212),担当(0.04812),取得(0.04766),必要(0.04037),保険(0.03253),監督(0.03251),利用(0.02945)
	2	0.79787	措置(0.10067),管理(0.10059),安全(0.10047),事業(0.04735),中小(0.03960),規模(0.03957),物理(0.03956),対応(0.03948),方法(0.03204),漏えい(0.03172)
	3	0.05137	特定(0.15691),番号(0.08457),事業(0.06538),事務(0.05024),取扱い(0.0419),管理(0.03704),適正(0.03370),機器(0.02946),安全(0.02780),廃棄(0.02557)
	4	0.05069	委託(0.09275),必要(0.06774),場合(0.05529),事業(0.05428),事務(0.03986),員(0.03558),従業(0.03521),廃棄(0.03385),先(0.03144)書類(0.03068)
中小企業BCP（事	0	0.10089	時(0.06236),緊急(0.05439),復旧(0.04648),員(0.03791),従業(0.03744),事業(0.03609),災害(0.02606),確保(0.02197),目標(0.01958),時間(0.01899)

業継続計画）ガイド	1	0.10001	情報(0.03419),継続(0.02883),資源(0.02657),事業(0.02526),代替(0.02395),訓練(0.02310),場所(0.02305),データ(0.01999),企業(0.01996),バックアップ(0.01971)
	2	0.59841	例(0.05541),記入(0.02587),行(0.02416),様式(0.02287),連絡(0.02228),工場(0.02161),方法(0.02036),企業(0.02009),時(0.01942),機械(0.01868)
	3	0.10013	BCP(0.04445),確保(0.02999),対策(0.02871),企業(0.02646),緊急(0.02187),協力(0.02100),家族(0.01749),要員(0.01705),代替(0.01506),取引(0.01421)
	4	0.10056	企業(0.03914),事業(0.03366),電話(0.03129),連絡(0.02546),影響(0.02354),経営(0.02178),ＢＣＰ(0.02119),中小(0.01906),代替(0.01860),先(0.01848)
出社してから退社するまで中小企業の情報セキュリティ対策実践手引き	0	0.20000	セキュリティ(0.07954),ネットワーク(0.07023),アプリケーション(0.05325),媒体(0.04930),記憶(0.04798),利用(0.03683),レベル(0.03652),メモリ(0.03496),USB(0.03278),現状(0.03144)
	1	0.20000	管理(0.10552),システム(0.06640),本人(0.06300),従業(0.04803),員(0.04802),対策(0.03959),業務(0.03949),外(0.03151),要因(0.03144),技術(0.02334)
	2	0.20000	サービス(0.06010),セキュリティ(0.04434),サーバ(0.042746),PC(0.03802),対策(0.03712),ファイル(0.02906),影響(0.02758),リスク(0.02727),机上(0.02623),目的(0.02515)
	3	0.20000	情報(0.11040),機器(0.04279),機密(0.03590),スマート(0.03535),完全(0.03448),可用性(0.03306),電子(0.03220),デバイス(0.03169),適法(0.02880),コピー(0.02776)
	4	0.20000	資料(0.07814),参考(0.07308),付き(0.07241),番号(0.06903),保存(0.05582),ポイント(0.04547),運用(0.04463),理(0.04406),備考(0.04055),監査(0.01896)

付録 1.5.トピック分析の結果の適用結果の検討

トピック分析の結果についても同様の方法で比較を実施した．特徴語から検討したトピックについては，表 55 の「トピック」の項目に記載した．

トピック分析の結果においては，クラスタリングの場合とは異なり，1）セキュリティ対策に直接関係のない分類があることはなかったが，2)の一つの機能に対する偏りがクラスタリングの場合と同じく，「中小企業の情報セキュリティ対策ガイドライン　第 2.1 版」に発生しているのが確認された．また，ほとんどのトピックが複数の機能と類似性を持っており，同様に少なくとも一つの体系には従っていない分類になっていることが分かる．

表 55　トピックの出現頻度のベクトルと機能の特徴語ベクトルのコサイン類似度

Table 55　Cosine Similarity between appearance frequency vector of words of each topic and the feature words vector of Function of Framework Core

文書名	a) 中小企業の情報セキュリティ対策ガイドライン				
トピックID	0	1	2	3	4
トピック	包括的な管理の必要性	ポリシーに基づいた管理の重要性	中小企業におけるガイドライン実施	中小企業のリスク管理ガイドライン	経営者と従業員の責任
Identify(特定)	0.3413	0.2846	0.2226	0.2812	0.2417
Protection(防御)	0.1896	0.2469	0.1285	0.1580	0.2139
Detection(検知)	0.0558	0.0582	0.0899	0.0579	0.0551
Response(対応)	0.1126	0.1099	0.2160	0.1412	0.1301
Rcovery(復旧)	0.0740	0.1019	0.1112	0.0864	0.0856

文書名	b) 中小企業向けはじめてのマイナンバーガイドライン				
トピックID	0	1	2	3	4
トピック	委託先の番号管理の監督	事務における適切な情報の取り扱い	物理的な安全管理	番号と事業・事務	委託先の従業員
Identify(特定)	0.0593	0.0859	0.2144	0.2363	0.1263
Protection(防御)	0.0766	0.0529	0.0736	0.0678	0.0504
Detection(検知)	0.0294	0.0376	0.0075	0.0348	0.0211
Response(対応)	0.0506	0.0606	0.1312	0.0238	0.0565
Rcovery(復旧)	0.0279	0.0330	0.0286	0.0104	0.0197

文書名	c) 中小企業BCP（事業継続計画）ガイド				
トピックID	0	1	2	3	4
トピック	緊急時の目標復旧時間と従業員確保	事業継続のための情報管理と訓練	工場における事例．連絡先の管理	事業継続計画と緊急時の関係性	事業継続計画における連絡先
Identify(特定)	0.0794	0.1505	0.1011	0.0994	0.1340
Protection(防御)	0.0499	0.1340	0.0915	0.0805	0.0668
Detection(検知)	0.0354	0.0843	0.0291	0.0633	0.0348
Response(対応)	0.0630	0.0659	0.0527	0.1027	0.1068
Rcovery(復旧)	0.2396	0.1022	0.0378	0.1013	0.1009

文書名	d) 出社してから退社するまで中小企業の情報セキュリティ対策実践手引き				
トピックID	0	1	2	3	4
トピック	IT環境でのセキュリティ	従業員を含めたシステム管理	サーバ/サービスでのリスク対策	スマートデバイスに関するCIA	監査のための参考資料
Identify(特定)	0.0692	0.2134	0.0471	0.0273	0.0593
Protection(防御)	0.1933	0.1424	0.1182	0.1896	0.0322
Detection(検知)	0.0811	0.0543	0.2156	0.0408	0.0125
Response(対応)	0.0455	0.0448	0.0902	0.0237	0.0167
Rcovery(復旧)	0.0121	0.0301	0.1515	0.0324	0.0209

付録 1.6. 枠組みを用いないテキストマイニングとの比較評価まとめ

今回，TF-IDF と k 平均法によるクラスタリングとトピック分析の二つの方法で分類を行い，その結果を確認したが，どちらにおいても，文書内容を表す分類結果を得ることはできるが，分類結果の偏りが発生し，（少なくとも一つの）体系に従っていない分類になっていることが確認された．このような分類に基づいて学習を進めると誤った体系化が行われ，教材そのものの学習効果に悪影響がある可能性が考えるほか，他の教材と組み合わせた学習者の方略にも悪い影響があると考えられる．

しかしながら，体制化方略は，理論や枠組みに基づいて学習要素を相互に関連付けて整理する学習方略であり，体系だった理論や枠組みに基づいて学習要素が相互に関連付けられ整理された形で提示されることが要求される．

提案手法においてはCSFの枠組みに従ってテキストマイニングを行うため，体制化方略の要求である「体系だった理論や枠組み」による情報提示を行うことができる．これにより，枠組みを前提としないテキストマイニングの方法では体制化方略を促すための最低限の要求を満たすことができない可能性があることがあり，今回の研究の目的を達成するためには適切ではないと考えられることが事例的に確認された．

付録 参考文献

[87] D. M. Blei, A. Y. Ng , M. I. Jordan, “Latent Dirichlet allocation,” Journal of Machine Learning Research, vol.3, pp. 993-1022, 2003.
[88] J. MacQueen, “Some Methods for classification and Analysis of Multivariate Observations,” Proceedings of 5th Berkeley Symposium on Mathematical Statistics and Probability, p. pp. 281–297, 1967.
[89] “gensim,” . https://radimrehurek.com/gensim/. [アクセス日: 23 11 2021].

付録 2.「章」と「節・項」に対するカテゴリ単位での提案手法と質的分析の結果

ここでは，カテゴリ単位で提案手法を適用した結果と質的分析を実施した結果を記載する．本文中の表16のカテゴリに対する評価はこの結果に基づいている．

5.1.3節の提案手法を「章」に対してカテゴリ単位で適用した結果を表56と表57の2つの表に分けて示す．この結果では，防御（PR）のIPにあたるカテゴリが全体に高めに出ていることが分かる．このカテゴリは「情報を保護するプロセス及び手順」を表し，以下のように定義されている．

> *（目的，範囲，役割，責任，経営コミットメント，組織間の調整について記した）セキュリティポリシー，プロセス，手順が，維持され，情報システムと資産の防御の管理に使用されている．*
>
> *—重要インフラのサイバーセキュリティを改善するためのフレームワーク 1.1版*

この記述より，防御の機能以外のその他の機能にも関わるような内容が多いと考えられ，それにより全体に高い値が出ていると考えられる．また，同様の対象にテンプレートコーディングを実施した結果を，表58に示す．こちらにおいても，防御のIPの項目は多く出現していた．

提案手法を「節・項」に対してカテゴリ単位で適用した結果を表 59 と表 60 の 2 表に分けて示す．テンプレートコーディングの結果を，表 61 に示す． これらの表については，表記の簡略化のため，ID を用いて行と列の項目を記載する．列は表 3 に記載されているカテゴリの ID を用いており，「章」や「節・項」の ID は，表 14 に記載されているものを用いる．

表 56　各章に対してカテゴリ単位で提案手法を適用した結果（識別，防御）

Table 56　Text mining analysis results for sections with functional view

	識別（ID）						防御（PR）					
	AM	BE	GV	RA	RM	SC	AC	AT	DS	IP	MA	PT
0	0.22	0.20	0.20	0.22	0.15	0.15	0.12	0.21	0.19	0.31	0.12	0.18
1.1	0.45	0.38	0.38	0.61	0.4	0.38	0.32	0.52	0.47	0.64	0.36	0.45
1.2	0.46	0.49	0.58	0.51	0.29	0.3	0.43	0.66	0.51	0.82	0.38	0.52
1.3	0.53	0.76	0.71	0.58	0.53	0.55	0.26	0.67	0.5	0.9	0.28	0.53
2.1	0.22	0.2	0.23	0.24	0.19	0.19	0.07	0.17	0.14	0.18	0.11	0.15
2.2	0.16	0.23	0.19	0.25	0.18	0.16	0.27	0.23	0.29	0.28	0.25	0.22
2.3	1.44	1.57	1.17	1.34	1.11	1.05	0.65	2.04	1.84	1.97	1.52	1.99
2.4	1.69	1.74	1.74	1.96	1.86	1.72	0.84	1.6	1.4	1.5	0.87	1.37
2.5	5.77	6.35	5.43	5.6	6.26	6.29	5.12	5.38	8.19	6.78	5.4	7.35

表 57　各章に対してカテゴリ単位で提案手法を適用した結果（検知，対応，復旧）

Table 57　Text mining analysis results for sections with functional view

	検知(ID)			対応(RS)					復旧(RC)		
	AE	CM	DP	AN	CO	IM	MI	RP	CO	IM	RP
0	0.06	0.13	0.06	0.06	0.16	0.03	0.05	0.04	0.12	0.02	0.04
1.1	0.18	0.36	0.15	0.35	0.39	0.24	0.35	0.32	0.33	0.17	0.25
1.2	0.08	0.24	0.14	0.14	0.56	0.08	0.21	0.05	0.36	0.04	0.02
1.3	0.23	0.48	0.3	0.28	0.73	0.2	0.23	0.18	0.63	0.07	0.09
2.1	0.1	0.17	0.08	0.08	0.08	0.04	0.05	0.05	0.05	0.03	0.04
2.2	0.16	0.25	0.11	0.12	0.17	0.07	0.1	0.06	0.42	0.12	0.1
2.3	0.76	1.26	0.62	1.16	1.4	0.78	1.16	0.95	0.98	0.6	0.7
2.4	0.76	1.15	0.63	1.47	1.52	1.36	1.49	1.32	0.87	0.47	0.51
2.5	2.84	4.07	2.27	3.64	3.77	2.06	3.32	2.27	3.48	1.93	2.15

表 58　各章に対してカテゴリ単位でテンプレートコーディングを実施した結果

Table 58　Text mining analysis results for sections with functional view

	識別(ID)							防御(PR)					検知(DE)			対応(RS)					復旧(RC)		
	AM	BE	GV	RA	RM	SC	AC	AT	DS	IP	MA	PT	AE	CM	DP	AN	CO	IM	MI	RP	CO	IM	RP

0	0	0	2	1	0	0	0	2	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
1.1	0	0	1	6	0	0	0	4	1	4	0	0	0	0	0	1	0	0	0	0	1	0	1
1.2	0	0	4	2	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.3	1	2	1	0	0	2	0	3	0	3	0	0	0	0	0	0	1	0	0	0	0	0	0
2.1	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.2	0	0	0	1	0	0	3	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0
2.3	1	0	2	1	1	0	0	2	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
2.4	6	2	4	5	2	3	0	4	0	5	0	0	0	0	0	0	3	0	0	0	0	0	0
2.5	13	1	8	12	5	14	7	2	3	9	2	4	1	3	1	0	1	1	0	0	0	0	0

表 59　各節に対してカテゴリ単位で提案手法を適用した結果（識別，防御）

Table 59　Text mining analysis results for sections with functional view

	識別(ID)						防御(PR)					
	AM	BE	GV	RA	RM	SC	AC	AT	DS	IP	MA	PT
0												
1												
1.1												
1.1.0	0.12	0.14	0.14	0.20	0.16	0.14	0.09	0.12	0.11	0.21	0.06	0.08
1.1.1	0.03	0.03	0.03	0.11	0.05	0.05	0.12	0.10	0.16	0.13	0.11	0.15
1.1.2	0.15	0.11	0.10	0.12	0.09	0.10	0.04	0.16	0.09	0.11	0.07	0.10
1.1.3	0.08	0.05	0.05	0.13	0.06	0.05	0.03	0.07	0.03	0.08	0.07	0.06
1.1.4	0.07	0.06	0.06	0.06	0.04	0.04	0.05	0.06	0.07	0.11	0.05	0.06
1.2												
1.2.1	0.08	0.11	0.10	0.14	0.06	0.07	0.13	0.12	0.10	0.15	0.10	0.10
1.2.2	0.09	0.17	0.10	0.06	0.06	0.06	0.03	0.20	0.06	0.15	0.04	0.05
1.3												
1.3.1	0.02	0.04	0.04	0.02	0.03	0.02	0.02	0.02	0.01	0.10	0.01	0.02
1.3.1.1	0.11	0.16	0.14	0.12	0.13	0.13	0.06	0.12	0.13	0.19	0.06	0.11
1.3.1.2	0.12	0.15	0.16	0.11	0.10	0.17	0.06	0.21	0.15	0.15	0.10	0.15
1.3.1.3	0.08	0.17	0.08	0.09	0.09	0.12	0.04	0.13	0.06	0.12	0.04	0.07
1.3.2												
1.3.2.0	0.07	0.11	0.09	0.06	0.06	0.05	0.02	0.12	0.06	0.18	0.04	0.08
1.3.2.1	0.09	0.13	0.12	0.10	0.10	0.13	0.05	0.17	0.15	0.19	0.11	0.11
1.3.2.2	0.04	0.05	0.05	0.04	0.05	0.06	0.05	0.17	0.17	0.17	0.12	0.24
1.3.2.3	0.12	0.13	0.13	0.20	0.13	0.12	0.04	0.17	0.11	0.10	0.08	0.09
1.3.2.4	0.05	0.08	0.07	0.09	0.04	0.11	0.04	0.15	0.07	0.09	0.06	0.07
1.3.2.5	0.02	0.04	0.03	0.03	0.05	0.06	0.03	0.07	0.04	0.09	0.05	0.08
1.3.2.6	0.04	0.05	0.05	0.09	0.08	0.08	0.04	0.16	0.08	0.13	0.09	0.13
1.3.2.7	0.01	0.01	0.02	0.10	0.01	0.01	0.04	0.09	0.09	0.09	0.05	0.12
2.												
2.1												

2.1.0	0.22	0.20	0.23	0.24	0.19	0.19	0.07	0.17	0.14	0.18	0.11	0.15
2.2												
2.2.1	0.07	0.07	0.07	0.03	0.06	0.07	0.04	0.06	0.11	0.06	0.03	0.06
2.2.2	0.01	0.01	0.01	0.02	0.01	0.01	0.02	0.01	0.01	0.03	0.04	0.02
2.2.3	0.00	0.00	0.00	0.00	0.00	0.00	0.09	0.00	0.00	0.01	0.11	0.00
2.2.4	0.02	0.01	0.01	0.01	0.01	0.01	0.02	0.01	0.04	0.03	0.01	0.02
2.2.5	0.01	0.05	0.02	0.06	0.01	0.01	0.02	0.01	0.01	0.01	0.01	0.01
2.3												
2.3.1	0.13	0.14	0.12	0.10	0.09	0.09	0.04	0.09	0.06	0.10	0.03	0.06
2.3.2	0.11	0.09	0.10	0.13	0.08	0.09	0.04	0.19	0.12	0.15	0.14	0.11
2.3.3	0.05	0.07	0.12	0.05	0.11	0.07	0.03	0.16	0.10	0.13	0.08	0.11
2.4	0.30	0.26	0.27	0.31	0.30	0.25	0.12	0.15	0.18	0.16	0.07	0.14
2.4.1												
2.4.1.1	0.15	0.21	0.20	0.13	0.12	0.12	0.11	0.32	0.17	0.25	0.10	0.17
2.4.1.2	0.08	0.17	0.10	0.07	0.08	0.08	0.06	0.21	0.10	0.18	0.10	0.12
2.4.2	0.11	0.07	0.07	0.15	0.12	0.10	0.04	0.09	0.10	0.09	0.08	0.13
2.4.3	0.26	0.21	0.22	0.24	0.31	0.25	0.06	0.05	0.08	0.06	0.02	0.05
2.4.3.1	0.19	0.19	0.30	0.24	0.23	0.21	0.09	0.11	0.11	0.15	0.05	0.12
2.4.3.2	0.20	0.23	0.20	0.23	0.33	0.27	0.08	0.05	0.13	0.06	0.06	0.05
2.4.3.3	0.05	0.08	0.04	0.08	0.07	0.09	0.04	0.09	0.06	0.07	0.04	0.11
2.4.4	0.11	0.12	0.12	0.16	0.10	0.11	0.07	0.23	0.19	0.19	0.14	0.20
2.4.5	0.11	0.11	0.12	0.11	0.09	0.13	0.09	0.17	0.14	0.16	0.08	0.17
2.5												
2.5.1												
2.5.1.1	0.05	0.06	0.06	0.04	0.04	0.04	0.01	0.04	0.03	0.03	0.02	0.03
2.5.1.2	0.08	0.07	0.07	0.07	0.05	0.07	0.02	0.12	0.09	0.05	0.04	0.05
2.5.2												
2.5.2.1	0.18	0.14	0.11	0.13	0.16	0.13	0.09	0.15	0.14	0.15	0.11	0.17
2.5.2.2	0.07	0.08	0.06	0.07	0.03	0.04	0.04	0.07	0.14	0.12	0.07	0.08
2.5.2.3	0.13	0.11	0.16	0.10	0.12	0.11	0.10	0.17	0.20	0.17	0.11	0.21
2.5.3												
2.5.3.1	0.10	0.08	0.07	0.08	0.10	0.10	0.03	0.11	0.12	0.16	0.12	0.14
2.5.3.2	0.20	0.19	0.18	0.13	0.21	0.19	0.08	0.16	0.12	0.18	0.12	0.13
2.5.3.3	0.08	0.08	0.19	0.08	0.12	0.12	0.05	0.08	0.14	0.19	0.10	0.14
2.5.4												
2.5.4.1	0.12	0.12	0.12	0.10	0.09	0.23	0.18	0.16	0.17	0.14	0.10	0.16
2.5.4.2	0.02	0.06	0.04	0.02	0.02	0.05	0.08	0.31	0.18	0.17	0.11	0.20
2.5.4.3	0.13	0.11	0.14	0.12	0.19	0.22	0.06	0.13	0.18	0.12	0.09	0.12
2.5.4.4	0.06	0.03	0.01	0.07	0.01	0.01	0.03	0.05	0.14	0.08	0.07	0.07
2.5.4.5	0.05	0.05	0.02	0.02	0.02	0.04	0.04	0.03	0.10	0.04	0.09	0.07
2.5.4.6	0.04	0.04	0.04	0.01	0.03	0.03	0.07	0.22	0.23	0.25	0.20	0.26
2.5.5												

2.5.5.1	0.11	0.09	0.10	0.08	0.09	0.08	0.25	0.10	0.17	0.19	0.17	0.24
2.5.5.2	0.10	0.10	0.10	0.15	0.15	0.12	0.30	0.17	0.19	0.18	0.21	0.26
2.5.5.3	0.14	0.13	0.14	0.13	0.19	0.17	0.47	0.10	0.15	0.14	0.20	0.18
2.5.5.4	0.24	0.21	0.23	0.24	0.19	0.19	0.15	0.11	0.23	0.16	0.23	0.17
2.5.5.5	0.12	0.09	0.08	0.11	0.12	0.10	0.18	0.11	0.23	0.15	0.13	0.21
2.5.5.6	0.17	0.13	0.12	0.12	0.13	0.11	0.05	0.04	0.16	0.06	0.07	0.06
2.5.6												
2.5.6.0	0.32	0.29	0.34	0.32	0.46	0.38	0.13	0.12	0.16	0.19	0.12	0.14
2.5.6.1	0.28	0.21	0.21	0.25	0.28	0.31	0.14	0.09	0.35	0.14	0.11	0.13
2.5.6.2	0.22	0.17	0.17	0.28	0.28	0.21	0.11	0.09	0.18	0.12	0.10	0.10
2.5.6.3	0.22	0.22	0.22	0.28	0.37	0.30	0.11	0.13	0.20	0.16	0.12	0.15

表 60　各節に対してカテゴリ単位で提案手法を適用した結果（検知，対応，復旧）

Table 60　Text mining analysis results for sections with functional view

	検知(DE)			対応(RS)					復旧(RC)		
	AE	CM	DP	AN	CO	IM	MI	RP	CO	IM	RP
0											
1											
1.1											
1.1.0	0.05	0.08	0.04	0.05	0.07	0.02	0.07	0.02	0.06	0.02	0.02
1.1.1	0.04	0.08	0.04	0.09	0.07	0.07	0.07	0.10	0.10	0.06	0.09
1.1.2	0.04	0.09	0.05	0.03	0.06	0.02	0.07	0.04	0.02	0.02	0.03
1.1.3	0.03	0.06	0.01	0.10	0.09	0.08	0.10	0.10	0.11	0.07	0.11
1.1.4	0.02	0.06	0.02	0.07	0.10	0.05	0.04	0.06	0.03	0.01	0.01
1.2											
1.2.1	0.02	0.05	0.03	0.03	0.12	0.02	0.09	0.02	0.08	0.01	0.01
1.2.2	0.02	0.03	0.05	0.03	0.15	0.02	0.07	0.01	0.11	0.01	0.01
1.3											
1.3.1	0.01	0.02	0.02	0.02	0.11	0.01	0.01	0.01	0.09	0.01	0.01
1.3.1.1	0.06	0.13	0.05	0.06	0.09	0.07	0.04	0.02	0.10	0.02	0.01
1.3.1.2	0.05	0.09	0.05	0.06	0.09	0.03	0.11	0.03	0.04	0.02	0.02
1.3.1.3	0.03	0.06	0.08	0.09	0.28	0.07	0.05	0.10	0.18	0.01	0.03
1.3.2											
1.3.2.0	0.02	0.04	0.05	0.03	0.11	0.01	0.04	0.01	0.14	0.01	0.00
1.3.2.1	0.06	0.12	0.08	0.17	0.17	0.21	0.10	0.16	0.08	0.02	0.03
1.3.2.2	0.07	0.12	0.06	0.14	0.14	0.09	0.17	0.11	0.15	0.13	0.15
1.3.2.3	0.12	0.11	0.08	0.12	0.17	0.06	0.11	0.08	0.13	0.04	0.05
1.3.2.4	0.05	0.09	0.06	0.07	0.09	0.07	0.05	0.05	0.13	0.06	0.04
1.3.2.5	0.03	0.02	0.03	0.23	0.20	0.21	0.18	0.24	0.25	0.16	0.19
1.3.2.6	0.04	0.08	0.05	0.06	0.06	0.02	0.12	0.03	0.06	0.04	0.05
1.3.2.7	0.10	0.08	0.03	0.04	0.11	0.01	0.03	0.01	0.01	0.01	0.01

2.											
2.1											
2.1.0	0.10	0.17	0.08	0.08	0.08	0.04	0.05	0.05	0.05	0.03	0.04
2.2											
2.2.1	0.04	0.07	0.02	0.03	0.02	0.02	0.02	0.01	0.05	0.05	0.04
2.2.2	0.01	0.02	0.02	0.01	0.01	0.01	0.03	0.01	0.05	0.05	0.04
2.2.3	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.09	0.00	0.00
2.2.4	0.01	0.01	0.00	0.00	0.02	0.00	0.00	0.00	0.00	0.00	0.00
2.2.5	0.02	0.01	0.01	0.01	0.07	0.01	0.01	0.01	0.14	0.01	0.00
2.3											
2.3.1	0.04	0.09	0.05	0.06	0.14	0.05	0.05	0.04	0.12	0.04	0.03
2.3.2	0.14	0.13	0.07	0.14	0.10	0.05	0.13	0.10	0.08	0.04	0.08
2.3.3	0.07	0.13	0.07	0.09	0.11	0.10	0.08	0.06	0.11	0.04	0.05
2.4	0.08	0.13	0.06	0.08	0.08	0.05	0.11	0.07	0.07	0.02	0.04
2.4.1											
2.4.1.1	0.07	0.15	0.09	0.08	0.11	0.03	0.06	0.04	0.11	0.03	0.04
2.4.1.2	0.13	0.10	0.12	0.28	0.32	0.32	0.22	0.31	0.14	0.05	0.07
2.4.2	0.05	0.05	0.02	0.06	0.05	0.07	0.08	0.03	0.03	0.02	0.03
2.4.3	0.02	0.05	0.02	0.08	0.07	0.06	0.09	0.05	0.05	0.05	0.04
2.4.3.1	0.07	0.08	0.04	0.18	0.15	0.15	0.11	0.16	0.06	0.00	0.01
2.4.3.2	0.05	0.06	0.03	0.27	0.24	0.31	0.25	0.33	0.13	0.02	0.04
2.4.3.3	0.03	0.11	0.03	0.09	0.10	0.12	0.13	0.06	0.04	0.04	0.04
2.4.4	0.08	0.13	0.07	0.14	0.15	0.08	0.18	0.11	0.04	0.04	0.06
2.4.5	0.08	0.14	0.07	0.11	0.15	0.09	0.12	0.09	0.09	0.06	0.04
2.5											
2.5.1											
2.5.1.1	0.05	0.02	0.01	0.01	0.07	0.00	0.00	0.00	0.00	0.00	0.00
2.5.1.2	0.03	0.02	0.01	0.07	0.14	0.04	0.09	0.02	0.09	0.00	0.00
2.5.2											
2.5.2.1	0.08	0.13	0.09	0.08	0.16	0.04	0.04	0.05	0.14	0.09	0.09
2.5.2.2	0.06	0.10	0.06	0.07	0.04	0.03	0.15	0.07	0.05	0.05	0.07
2.5.2.3	0.11	0.19	0.09	0.11	0.08	0.05	0.11	0.06	0.09	0.06	0.06
2.5.3											
2.5.3.1	0.03	0.06	0.02	0.02	0.05	0.01	0.02	0.01	0.07	0.03	0.04
2.5.3.2	0.06	0.10	0.06	0.07	0.12	0.03	0.05	0.04	0.18	0.08	0.09
2.5.3.3	0.12	0.13	0.08	0.11	0.09	0.05	0.06	0.08	0.12	0.10	0.10
2.5.4											
2.5.4.1	0.04	0.07	0.02	0.10	0.07	0.05	0.06	0.04	0.07	0.06	0.05
2.5.4.2	0.07	0.13	0.06	0.07	0.04	0.02	0.02	0.02	0.05	0.05	0.05
2.5.4.3	0.05	0.14	0.03	0.04	0.04	0.03	0.04	0.02	0.05	0.06	0.05
2.5.4.4	0.03	0.07	0.00	0.07	0.04	0.03	0.09	0.03	0.03	0.02	0.03
2.5.4.5	0.01	0.01	0.00	0.15	0.07	0.07	0.05	0.07	0.02	0.02	0.02

2.5.4.6	0.16	0.22	0.16	0.13	0.04	0.03	0.08	0.04	0.08	0.08	0.07
2.5.5											
2.5.5.1	0.17	0.16	0.18	0.08	0.12	0.04	0.05	0.06	0.10	0.00	0.02
2.5.5.2	0.22	0.23	0.27	0.13	0.12	0.09	0.17	0.13	0.09	0.07	0.07
2.5.5.3	0.02	0.02	0.01	0.02	0.04	0.01	0.01	0.00	0.09	0.03	0.03
2.5.5.4	0.06	0.09	0.01	0.10	0.05	0.05	0.11	0.04	0.06	0.03	0.04
2.5.5.5	0.02	0.02	0.01	0.05	0.07	0.12	0.11	0.06	0.01	0.01	0.01
2.5.5.6	0.02	0.02	0.01	0.02	0.05	0.01	0.10	0.01	0.01	0.00	0.01
2.5.6											
2.5.6.0	0.07	0.08	0.07	0.20	0.09	0.08	0.15	0.11	0.06	0.03	0.06
2.5.6.1	0.04	0.06	0.01	0.05	0.07	0.03	0.07	0.03	0.02	0.01	0.04
2.5.6.2	0.08	0.08	0.04	0.11	0.09	0.07	0.14	0.11	0.11	0.03	0.07
2.5.6.3	0.08	0.17	0.07	0.12	0.10	0.11	0.20	0.10	0.08	0.08	0.09

表 61　各節に対してカテゴリ単位でテンプレートコーディングを実施した結果

Table 61　Text mining analysis results for sections with functional view

	識別(ID)						防御(PR)						検知(DE)			対応(RS)					復旧(RC)		
	AM	BE	GV	RA	RM	SC	AC	AT	DS	IP	MA	PT	AE	CM	DP	AN	CO	IM	MI	RP	CO	IM	RP
0																							
1																							
1.1																							
1.1.0	0	0	1	2	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
1.1.1	0	0	1	1	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
1.1.2	0	0	0	1	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	1	0	0
1.1.3	0	0	0	1	0	0	0	1	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0
1.1.4	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
1.2																							
1.2.1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.2.2	0	0	1	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.3																							
1.3.1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.3.1.1	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.3.1.2	1	1	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
1.3.1.3	0	1	0	0	0	0	0	1	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0
1.3.2																							
1.3.2.0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.3.2.1	0	0	2	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.3.2.2	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
1.3.2.3	0	0	0	2	2	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
1.3.2.4	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0	1	0

1.3.2.5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0
1.3.2.6	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.3.2.7	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
2.																							
2.1																							
2.1.0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.2																							
2.2.1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
2.2.2	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
2.2.3	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.2.4	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.2.5	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.3																							
2.2.3.1	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.2.3.2	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
2.2.3.3	1	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.4																							
2.4.1	0	1	1	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.4.1.1	1	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.4.1.2	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	3	0	0	0	0	0	0
2.4.2	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.4.3	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.4.3.1	1	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.4.3.2	0	0	0	2	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.4.3.3	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
2.4.4	1	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.4.5	0	0	0	0	0	0	0	1	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0
2.5																							
2.5.1																							
2.5.1.1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.5.1.2	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0
2.5.2																							
2.5.2.1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.5.2.2	0	0	0	1	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
2.5.2.3	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0
2.5.3																							
2.5.3.1	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.5.3.2	1	0	1	1	1	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.5.3.3	1	0	1	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
2.5.4																							
2.5.4.1	0	0	1	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
2.5.4.2	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

2.5.4.3	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.5.4.4	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
2.5.4.5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
2.5.4.6	0	0	0	0	0	0	0	0	0	0	0	0	2	1	1	0	0	0	0	0	0	0	0
2.5.5																							
2.5.5.1	0	0	0	0	0	0	1	0	1	0	0	2	0	0	0	0	0	0	0	0	0	0	0
2.5.5.2	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0
2.5.5.3	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.5.5.4	0	0	0	0	0	0	0	0	0	1	2	0	0	0	0	0	0	0	0	0	0	0	0
2.5.5.5	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.5.5.6	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
2.5.6																							
2.5.6.0	4	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.5.6.1	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.5.6.2	0	0	0	1	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.5.6.3	4	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0