Vol.2022-CSEC-97 No.13
Vol.2022-IOT-57 No.13
2022/5/20

機械学習を用いたセキュリティ対策セットのレコメンド技術

申河英[1]　金井遵[1]　上原龍也[1]　小池竜一[1]

概要: 近年のインフラシステムはサービス化により，インターネットに接続されていなかった従来のシステムに比べ，サイバー脅威にさらされる危険性が増加している．それにより，インフラシステムに対するセキュリティ対策が重要な課題となっている．一方，一般的にシステムに対する脅威は一つではなく，情報セキュリティの側面からも一つの脅威に対しても多層防御が求められる．しかしながら，複数のセキュリティ対策を効率的に導入するセキュリティ設計は，専門家の知見が必要不可欠な属人性が高いプロセスである．そのため，人的コストの上昇や開発期間の長期化の原因となっている．そこで，セキュリティ設計プロセスでの属人性を排除し，セキュリティ専門家でなくてもセキュリティ設計を可能にすることで，加速化されているインフラシステムのサービス化，開発過程での人的コストの軽減や開発期間の短縮が期待できる．本稿では，セキュリティ設計において人的コストの軽減や開発期間の短縮を実現するためのセキュリティ設計の自動化を目的とするセキュリティ対策レコメンド技術を提案する．レコメンド技術はシステム環境に適するセキュリティ対策の組み合わせを自動的にレコメンドすることで，セキュリティに関する深い知識がなくてもセキュリティ設計を可能とする．また，高精度のレコメンドを行うため，過去のセキュリティ設計データを学習した機械学習モデルを用いて，脅威に対して対策が採択される確率を予測する．予測したデータとユーザの要求度に基づいてセキュリティ対策組み合わせを評価する方法を提案し，提案手法を用いたレコメンド結果について精度評価を行う．

キーワード: サイバーセキュリティ，自動化，機械学習

Recommendation technology for cyber security measures sets utilizing machine learning

HAYEONG SHIN[†1]　JUN KANAI[†1]
TATSUYA UEHARA[†1]　RYUITI KOIKE[†1]

Abstract: In recent years, infrastructure systems have increased the risk of cyber threats compared to traditional systems that have been closed due to the use of services, so security measures against infrastructure systems have become an important issue. On the other hand, there are multiple threats in the system, and multiple layers of defense are required for each threat. However, security design, which efficiently introduces multiple security measures, is a highly personalized process that requires expert knowledge, so it is responsible for rising human costs and prolonged development periods. Therefore, by eliminating the personal knowledge of the security design process and enabling security design without a security expert, it is expected that accelerated infrastructure systems will be serviced, human costs will be reduced in the development process, and development time will be shortened. This paper proposes a security recommendation method that automatically recommends a combination of security measures suitable for the system environment to reduce human cost and reduce development time in security design. In order to make high-precision recommendations, the probability of adopting countermeasures against threats is predicted using machine learning models that have learned past security design data, and the accuracy is evaluated.

Keywords: Cyber Security, Automation, Machine Learning

1. はじめに

近年のインフラシステムはサービス化により，インターネットに接続されていなかった従来のシステムに比べ，サイバー脅威にさらされる危険性が増加している．それにより，インフラシステムに対するセキュリティ対策が重要な課題となっている[1].

一方，一般的にシステムに対する脅威は一つではなく，情報セキュリティの側面からも一つの脅威に対しても多層防御が求められる．しかしながら，複数のセキュリティ対策を効率的に導入するセキュリティ設計は，専門家の知見が必要不可欠な属人性が高いプロセスである．

このように，インフラシステムに対するセキュリティ対策の需要の増加に対し，セキュリティ人財の人力は限定されているため，セキュリティ設計プロセスでの人的コストの上昇や開発期間の長期化の原因となっている．

以上の背景から我々は，システム環境に適するセキュリティ対策の組み合わせをレコメンドするセキュリティ対策レコメンド技術（以降，レコメンド技術と呼ぶ）を研究している．レコメンド技術により，セキュリティ設計プロセスでの属人性を排除し，セキュリティ専門家でなくてもセキュリティ設計を可能とするセキュリティ設計の自動化が

1 (株)東芝研究開発センター
Corporate Research & Development Center, Toshiba Corporation.

実現できる．セキュリティ設計を自動化することで，セキュリティ設計での人的コストの軽減と開発期間の短縮が可能となり，急増しているインフラシステムのセキュリティ対策の需要に対処することができる．

本稿では，レコメンド技術の実現と高精度化のため，過去のセキュリティ設計事例と機械学習を用いる手法について，2 章で関連研究について述べ，3 章ではセキュリティ対策の課題について述べる．4 章では提案手法について述べ，5 章では提案手法の評価結果について報告し，6 章で考察し，7 章でまとめる．

2. 関連研究

セキュリティ対策の自動化において，機械学習の活用に関する多くの研究は，セキュリティ運用フェーズに重点を置いている．

セキュリティ設計の自動化に関する研究は R. Lagerstrom らの研究[2]が挙げられる．強化学習の SARSA アルゴリズムを用いたセキュリティ設計の自動化を提案している．特徴としては，利害関係者の間の機密性・可用性・完全性などのシステム要件や時間, コストなど項目の優先度に対し，妥協点を見つけるために効用理論を用いて，適切な報酬機能を定義していることである．初期の設計より良い設計を提案しながら，効用関数(累積報酬)が最大化するポリシーを探索する．

S. Vijayakumar らの研究[3]では，セキュリティ運用の側面でセキュリティソリューション修正の自動化を提案している．DevOps 方法論を用いてセキュリティ修正事項を検知，生成，パターン予測，ソリューションをレコメンドすることでセキュリティプロセス自動化を実現する．自動化データでディープラーニングモデルの改善をし，脅威を検知する機能を強化する．

我々の研究では，セキュリティ対策を導入する前の設計フェーズで，ユーザによる制約要件に重点を置いたセキュリティ対策の提案を自動化する．過去の設計データを学習した学習モデルとセキュリティ対策に関するデータベースを用いて，セキュリティ対策をレコメンドすることで，セキュリティ設計の自動化を目指す．

3. セキュリティ対策における課題

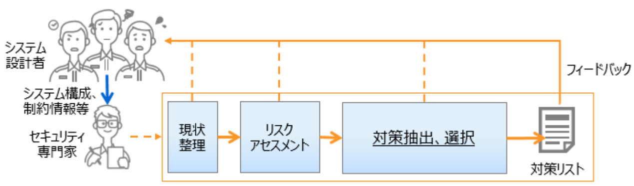

図 1 従来のセキュリティ対策の導入プロセス

図 1 に従来のセキュリティ対策の導入プロセスを示す．セキュリティ対策の導入プロセスでは現場のシステム設計者からシステム構成案を確認し，システムに存在するセキュリティ上の脅威を明らかにするリスクアセスメントを行う．その後，リスクアセスメント結果やユーザ要求，システム構成などの情報から導入するセキュリティ対策を決定するセキュリティ設計を行う．さらに対策の導入を行い，運用を開始する順で行われる．その中でもリスクアセスメントやセキュリティ設計はセキュリティについての深い知識を持つ人財が必要である．リスクアセスメントには様々な支援ツールがあるが，セキュリティ設計には決定的なツールが存在していないため，セキュリティの専門家でないとセキュリティ設計の実施が困難という課題がある．

特に，セキュリティ設計を実施する際は，セキュリティ対策を導入するシステム環境に対する理解に基づき，その環境に対するユーザの要求を満たすセキュリティ対策を選定する必要がある．ユーザの要求には，セキュリティ強度や機能，コスト，運用人財，既存環境への影響など（以降，制約情報と呼ぶ）が挙げられる．

4. 提案手法

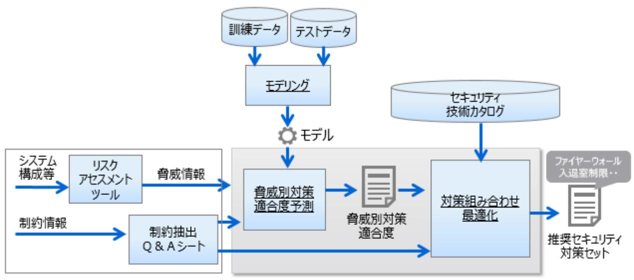

図 2 機械学習を用いたレコメンドアルゴリズムの全体像

図 2 は提案手法の全体像である．まず，ユーザはレコメンドシステムにセキュリティ対策を導入するシステム（以降，対象システムと呼ぶ.）の脅威情報と制約情報を入力する．さらにレコメンドシステムはユーザが入力した制約を持つ場合に脅威別に対策が採択される確率を予測するために学習済モデルを用いて,「対策適合度を示すスコア」を算出する．また，各セキュリティ技術を導入した際に与える影響が記載されたカタログ（以降，セキュリティ技術カタログと呼ぶ）の情報と制約情報の比較を行い「制約要件充足度を示すスコア」を算出する．続いて対策組み合わせ最適化では，制約情報の一部を用いたフィルタリングと上記の 2 つのスコアを用いたスコア計算を行いレコメンドする対策組み合わせ（対策セットと呼ぶこともある）の順位を付け，出力する．

本章の 4.1 節，4.2 節では提案手法を構成するデータについて述べ，4.3 節では機械学習アルゴリズム，4.4 節では対策組み合わせの最適化方式について述べる．

4.1 ユーザ入力データ

レコメンドアルゴリズムを活用するためにユーザが入

力すべきデータである，図 1 の脅威情報と制約抽出 Q&A シートについて述べる．

脅威情報（リスクアセスメント結果）

対策をレコメンドするためには，対象システムがどのような脅威を持っているのかについて明らかにする必要がある．リスクアセスメント支援ツールなどを用いて，対象システムの脅威を抽出し，対策を必要とする脅威情報を入力する．

制約抽出 Q&A シート

制約抽出 Q&A シートはセキュリティ要件と環境上の制約に対して項目別に要求度を相対的にレベル付けしたデータである．項目は表 1 のように構成されている．不要(0)，要(1)で表示するセキュリティ要件の 3 項目以外には要求大(1)，要求中(2)，要求小(3)の範囲内に記載するようになっている．

表 1　制約抽出 Q&A シートの項目

分類要件		要件	要求度
セキュリティ要件		セキュリティ制約 1	3~1
		セキュリティ制約 2	0，1
		セキュリティ制約 3	0，1
		セキュリティ制約 4	0，1
環境上の制約	コスト	制約 1	3~1
		制約 2	3~1
	運用人財	制約 3	3~1
		制約 4	3~1
		制約 5	3~1
	環境への影響	制約 6	3~1
		制約 7	3~1
		制約 8	3~1
		制約 9	3~1
		制約 10	3~1
		制約 11	3~1
		制約 12	3~1
	調達	制約 13	3~1

4.2 ナレッジデータ

レコメンドアルゴリズムを実現するため必要な構成データである，図 1 の訓練・テストデータとセキュリティ技術カタログについて述べる．

訓練データ・テストデータ

制約抽出 Q&A シートで対策のフィルタリング基準となるセキュリティ要件を除外した項目を特徴とし，その要件に対する対策の採択可否を教師データとする．

セキュリティ技術カタログ

脅威とその脅威に対する対策，制約抽出 Q&A シートの項目に対する対策の性質が「大，中，小」で相対的に記載されたデータである．制約抽出 Q&A シートの要求に対する充足度の判断基準となる．

4.3 機械学習アルゴリズムの選定

レコメンドシステムでは機械学習を用いて脅威別対策適合度（以降，適合度と呼ぶ）の予測を行う．

適合度を予測するモデルを作成するには，大きく 2 つの方向での学習方式が考えられる．

方式⑴ 既知のデータから特徴となりうるデータを特定し，その特徴による対策の採択結果を学習する（教師あり学習）

方式⑵ システムのセキュリティ設計情報から特徴を抽出し，抽出した特徴によるクラスタリングを行う（教師なし学習）

本研究では，特徴となりうる制約抽出 Q&A シートの制約要件のデータとそこに対する対策の採択結果のデータ持っている．そのため，まず方式⑴である教師あり学習を用いた実装及び評価を行う．

教師あり学習の中にも様々な学習アルゴリズムが存在している．また，学習モデルの精度はアルゴリズムだけでなく，データの質と量に多く影響される．そのため，レコメンド技術において求めるアルゴリズムの特性と，使用する訓練データの特徴についてまとめたものが表 2 である．

表 2　アルゴリズムの選定基準と訓練データの特徴

		詳細	重要度，特徴
アルゴリズムの特性	精度	未知のデータに対する予測精度	高
	速度	入力データの学習速度	低
	複雑度	アルゴリズムの複雑度 複雑度が高いほど結果の理解，説明容易性が低下	低い方が好ましい
訓練データの特徴	特徴量	予測，推論をするときデータから考慮すべき要素の数	10-15 個
	データ量	訓練データ規模	少量

今回入出力データは質的データを求めるため，教師あり学習の中でも分類アルゴリズムを用いる．表 3 には，表 2 に示した機械学習アルゴリズムの選定基準と訓練データの特徴を指標に，一般的に知られている分類アルゴリズムの特徴を示す．この特徴は，機械学習アルゴリズムの選択に際して考慮すべき要素とアルゴリズムの特性をまとめた文献やウェブ記事[5][6][7][8]を参考に整理したものである．

これらの比較はあくまで相対的な結果であるためデータによって結果が大きく変わることに注意する必要がある．そのため，レコメンド技術で使用する訓練データの特性（特徴量と規模）と類似する特徴のデータを用いて学習を行い，

そのモデルの精度を評価した研究があれば，その研究で活用されたアルゴリズムの特性データを参考にレコメンド技術で使用する学習アルゴリズムを選択することが有効だと考えた．

表 3　分類アルゴリズムの相対的特性

	精度	速度	複雑度	特徴量	データ量
KNN	高	低	低	少	少
ロジスティクス回帰	中	中	低	多	—
Naïve Bayes	中	高	低	多	—
決定木	低	—	中	少	—
Random Forest	高	中	中	少	多
GBM	高	中	中	少	多
SVM	高	中	高	—	少

—：カバー範囲が広い，影響が少ない

レコメンド技術の訓練データは図や自然言語などのデータに比べ特徴量は少ないと考えられる．また，データ量に対しては十分にあると仮定はしているが，設計事例は過去の情報を含めたとしても数十から数百事例と予想されるため，機械学習に用いる訓練データの数としては多いとは言い難い．そのため，特徴量とデータ量が「少」もしくは影響が少ないアルゴリズムである KNN と決定木，SVM を中心に，レコメンド技術と特徴が類似している研究について調査を行った．

その結果，分類アルゴリズムの中では主に決定木を用いる結果が多く，データ量が少なくても精度がある程度保証されていることが確認できた．その中でも Han らの研究[4]はレコメンド技術での機械学習の活用方式と性格が最も類似している．この研究はデータ収集方式，アンケート先，文化的性向，アンケートの形などの特徴からアンケート応答率を予測する研究である． 244 件の比較的少ないデータを学習データとテストデータに分けて決定木を用いて学習を行った結果，精度約 80%の予測をすることができた．レコメンド技術に対応した場合，環境上の制約を特徴として対策に対する適合度を予測し，確率が高い順に順位付けをする方向で応用することができると考えられる．

以上から本研究では，入出力データの特徴を考慮し，一番適していると考えられる決定木を用いて学習を行い，モデルを作成することにする．しかし，決定木は訓練データに過学習される傾向があり，予測の精度が低くなる可能性があるため，その場合は，KNN や SVM を用いることも考慮することとした．

4.4 対策組み合わせ最適化

図 3 は対策組み合わせ最適化のフローチャートを示す．対策組み合わせ最適化では，セキュリティ要件を充足する対策組み合わせに対して，図 4 のように環境上の制約要件充足度と対策の適合度によるスコア付けを行う．スコア付けられた対策組み合わせに順位を付与し，上位の対策組み合わせをレコメンドする．A と B は任意の係数であり，標準では A，B ともに 1.0 としている．

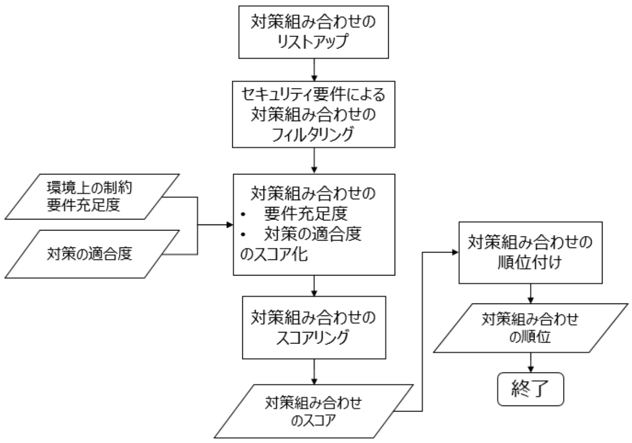

図 3　対策組み合わせ最適化のフローチャート

A×（環境上の制約要件充足度を示すスコア）
＋ B×（対策の適合度を示すスコア）
＝ 対策組み合わせのスコア

図 4　対策組み合わせのスコア計算

5. 評価

提案手法を用いて 2 件の事例に対してレコメンドの結果得られた対策セットについて評価を行う． 6 種類の脅威が存在すると仮定し，CASE①は脅威 A，脅威 C，脅威 E，脅威 F を持ち，CASE②は脅威 B，脅威 D，脅威 E，脅威 F を持つシステムであるとする．各 CASE に対して表 4 に示す要求度を充足し，かつセキュリティ専門家が実際導入すると判断する対策セットがレコメンドできたかについて確認を行う．

表 4　CASE①，CASE②の制約要件

分類要件		要件	CASE①要求度	CASE②要求度
セキュリティ要件		セキュリティ制約 1	3	3
		セキュリティ制約 2	1	1
		セキュリティ制約 3	0	1
		セキュリティ制約 4	0	0
環境上の制約	コスト	制約 1	1	3
		制約 2	1	2
	運用人財	制約 3	2	1
		制約 4	2	1

		制約 5	1	2
	環境への影響	制約 6	1	3
		制約 7	1	1
		制約 8	1	3
		制約 9	3	1
		制約 10	2	2
		制約 11	2	3
		制約 12	2	1
	調達	制約 13	3	3

まず，2 件の CASE に対する評価結果のまとめを表 5 に示す．評価項目は以下の 3 である．

- 採択可否の妥当性：レコメンドされた対策セットを構成する脅威別対策がセキュリティ専門家によって最終的に導入された対策であるか. ユーザの要求をベースとするが, 現場のフィードバックや専門家の判断によって実質的に導入が困難である対策を除外し, 長期的な観点で導入すべきである対策を含めるなどの知見が反映できているかを評価.
- 要件充足度の妥当性：レコメンドされた対策セットを構成する脅威別対策が，該当脅威に対処できる対策の中で何番目に適切な対策であるか. レコメンドされた対策セットを構成する個別対策が表 4 で示すユーザの要求度をどのぐらい充足しているかを評価.
- 組み合わせの妥当性：複数の脅威に対策できる対策が存在し，その対策がユーザの要求を充足する範囲内であれば，脅威別に異なる対策をレコメンドせずに同一な対策を含む対策セットを上位にレコメンドするか. ユーザの要求を充足する範囲内で導入される対策の複雑度を最小限にすることができるか, 脅威別個別対策ではなく，対策セットとしてレコメンドをする意味があるかを評価.

このような評価項目で評価を行った結果，2 件の CASE 両方改善点はあるが, 妥当な結果が出ることが確認できた. CASE①に対する詳細な結果は 5.1 節で，CASE②に対する詳細な結果は 5.2 節で説明する．

表 5　CASE①，CASE②の評価結果

	採択可否妥当性	要件充足度妥当性	組み合わせ妥当性
CASE①	○	○	○
CASE②	○	○	○

5.1 CASE①の評価結果

CASE①に対するレコメンド結果を表 6 に示しており，一つの行が一つの対策セットである．表 7 にはレコメンドされた対策が適切であるかを判断するための情報を示している．表 7 の「採択」列は専門家によって該当対策が採択された場合○で，採択されなかった場合，✕で表示している．また，表 7 の「要件充足度」列には該当対策がユーザの制約要件をどの程度満足しているかについて，対応すべき脅威の対策リストの中から比較を行い，順位付けした結果を示している．

① 採択可否の妥当性

5 位までの組み合わせを構成する対策は，脅威 F に対する対策である「対策 9」以外は全てセキュリティ専門家の判断によって採択された対策である．「対策 9」は不採択だが要件充足度 2 位である．これによって，対策の適合度のスコアより環境上の制約要件充足度のスコアの影響が高く計算される傾向があることが推測できる．

② 要件充足度の妥当性

脅威 E の場合，要件充足度が 4 位である「対策 6」と「対策 7」が上位の対策組み合わせとして含まれている．要件充足度がそれほど高くないにも関わらず,「対策 6」が上位の対策組み合わせに含まれる理由としては，脅威 A と脅威 E の複数の脅威をカバーできるためだと考えられる．しかしながら，今回の場合は脅威 A に対する「対策 6」の要件充足度の順位が 5 位であるため，より要件充足度が高い他の対策が選定されている．そのため，脅威 E の対策として「対策 6」が選定されるメリットがそれほど大きくないにも関わらず，上位の組み合わせに含まれてレコメンドされた点に対しては，改善の余地がある．

③ 対策組み合わせの妥当性

脅威 E の場合,「対策 6」と「対策 7」の要件充足度が同様だが,「対策 6」が脅威 A に対しても有効な対策であるため,「対策 7」より上位の対策組み合わせとして含まれたことが確認できる．

表 6　CASE①レコメンド結果

順位	脅威 A	脅威 C	脅威 E	脅威 F
1	対策 1	対策 3	対策 6	対策 8
2	対策 1	対策 3	対策 6	対策 9
3	対策 1	対策 3	対策 7	対策 8
4	対策 1	対策 3	対策 7	対策 9
5	対策 2	対策 3	対策 6	対策 8

表 7　CASE①評価表

	対応脅威	採択	要件充足度 (順位)
対策 1	脅威 A	○	1
対策 2	脅威 A	○	6
対策 3	脅威 C	○	1
対策 6	脅威 A 脅威 E	○	5(脅威 A) 4(脅威 E)
対策 7	脅威 E	○	4

対策 8	脅威 F	○	1
対策 9	脅威 F	✕	2

5.2 CASE②の評価結果

CASE②に対するレコメンド結果を表 8 に示しており，一つの行が一つの対策セットである．表 9 にはレコメンドされた対策が適切であるかを判断するための情報を示している．表 9 の「採択」列は専門家によって該当対策が採択された場合○で，採択されなかった場合，✕で表示している．また，表 9 の「要件充足度」列には該当対策がユーザの制約要件をどのぐらい満足しているかについて，対応すべき脅威の対策リストの中から比較を行い，順位付けした結果を示している．

① 採択可否の妥当性

5 位までの組み合わせを構成する対策は，脅威 D に対する対策である「対策 11」以外に全部セキュリティ専門家の判断によって採択された対策である．また，脅威 D に対して有効な唯一の対策である「対策 10」が上位にレコエンドされたあとに, 不採択だが要件充足度 1 位である「対策 11」がレコメンドされたため，レコメンドされたすべての組み合わせが妥当だと考えられる．

② 要件充足度の妥当性

脅威 E の結果を確認すると，要件充足度が高い順か対策の組み合わせも順位付けされていることを確認できる．

③ 対策組み合わせの妥当性

1 位から 3 位の脅威 D に対する対策結果を確認すると，脅威 B に対する対策である「対策 10」で対処できることを考慮し, 別途の対策が提案されていないことが確認できる．これで，レコメンド技術が対策組み合わせとしての対策の導入を考慮していることが確認できる．

表 8　CASE②レコメンド結果

順位	脅威 B	脅威 D	脅威 E	脅威 F
1	対策 10	左同	対策 4	対策 8
2	対策 10	左同	対策 5	対策 8
3	対策 10	左同	対策 12	対策 8
4	対策 10	対策 11	対策 4	対策 8
5	対策 10	対策 11	対策 5	対策 8

表 9　CASE②評価表

	対応脅威	採択	要件充足度 (順位)
対策 10	脅威 B 脅威 D	○	1（脅威 B） 2（脅威 D）
対策 11	脅威 D	✕	1
対策 4	脅威 E	○	1
対策 5	脅威 E	○	3
対策 12	脅威 E	○	4
対策 8	脅威 F	○	1

6. 考察

実際セキュリティ対策を導入する時，制約要件を充足する対策だとしても，セキュリティ専門家と実務者の判断により導入が困難であると判断する場合がある．また，現段階では脅威が存在しない，もしくはセキュリティ要件を充足しない対策だとしても，長期的にシステムの運用を考えた時，導入した方がいい対策なども存在することがある．

提案手法では対策組み合わせをレコメンドする際，制約要件の充足度を考慮する．加えて，過去のセキュリティ設計事例データを学習した機械学習モデルを用いて対象システムの制約要件での対策の適合度の予測し，対策セットのレコメンドの最終スコアに反映する．

このように過去のセキュリティ設計事例データを用いることで，制約要件の充足度に関わらず採択もしくは不採択される対策，つまり最終対策の採択まで生じるセキュリティ専門家とユーザの間のフィードバックについての情報を，対策組み合わせの選定アルゴリズムに反映することができる．したがって，より高精度な対策組み合わせの提案が可能になると期待できる．

最終スコア演算時, 係数 A と係数 B を同一にした場合に評価結果を出力した結果，適合度より要件充足度が重視される傾向があることを確認した．また，複数の脅威に対する対策があれば，専門家による採択可否や要件充足度より優先的に上位の対策組み合わせに含まれる傾向がある．それは「環境上の制約要件充足度を示すスコア」を計算する時，複数の脅威に対する対策であれば該当するすべての脅威に対して重複でスコアが加算されるためだと考えられる．

適合度より要件充足度が重視されることに対しては「対策の適合度を示すスコア」の係数である B をもっと高く調整することにより解決できる．しかし，複数の脅威に対処できる対策が優先で選定されることは「環境上の制約要件充足度を示すスコア」を算出する方法の問題である．そのため,「環境上の制約要件充足度を示すスコア」計算時，重複の脅威に対処可能な対策の評価方法を改善する必要がある．

これは，対象システムの環境にある脅威に対し，少ない数で対処ができる対策を優先し，導入対策を減らすことで効率を求めるか，もしくは個々の脅威に対する対策の要件充足度を優先し，セキュリティ強度を求めるかのバランス調整の問題であると考えることもできる．制約抽出 Q&A シートにセキュリティ要件とコストの項目を用いて「環境上の制約要件充足度を示すスコア」を計算する方法を調整することで，改善が可能だと考えられる．

7. おわりに

今回は，セキュリティ設計の人的コストと開発期間の削減をするために，セキュリティ設計を自動化する方法として，機械学習を用いた高精度なセキュリティ対策レコメン

ド技術を提案，実装し，評価を行った．

今後は，考察で述べた点について改善を行い，評価事例を増やすことでより明確な精度評価を行う．また，一つの脅威に対して複数の対策が効率的にレコメンドできるように実装を改善する予定である．そのあと，他の機械学習アルゴリズムを用いてモデルを生成し，精度比較を行うことでより高精度な対策レコメンド技術を目指す．

参考文献

[1] “2021 ICS CYBERSECURITY YEAR IN REVIEW”.https://www.dragos.com/year-in-review/#section-report, (参照 2022-03-29).
[2] R. Lagerstrom, P. Johnson and M. Ekstedt, "Automatic Design of Secure Enterprise Architecture: Work in Progress Paper," in 2017 IEEE 21st International Enterprise Distributed Object Computing Workshop (EDOCW), Quebec City, QC, Canada, 2017 pp. 65-70, doi: 10.1109/EDOCW.2017.19, keywords: {security;computer architecture;stakeholders;analytical models;tools;solid modeling;computational modeling}, url: https://doi.ieeecomputersociety.org/10.1109/EDOCW.2017.19, (参照 2022-03-29)
[3] S. Vijayakumar, K. S. P. Gowtham, N. Nigam and R. V. R. Singh, "An Novel Approach in Designing a Security Workbench with Deep Learning Capabilities and Process Automation," TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON), 2019, pp. 263-268, doi: 10.1109/TENCON.2019.8929691.
[4] Han, Jian & Fang, Miaodan & Ye, Shenglu & Chen, Chuansheng & Wan, Qun & Qian, Xiuying. (2019). Using Decision Tree to Predict Response Rates of Consumer Satisfaction, Attitude, and Loyalty Surveys. Sustainability. 11. 2306. 10.3390/su11082306.
[5] Chen, RC., Dewi, C., Huang, SW. et al. Selecting critical features for data classification based on machine learning methods. J Big Data 7, 52 (2020). https://doi.org/10.1186/s40537-020-00327-4, (参照 2022-04-07).
[6] “Azure Machine Learning のアルゴリズムの選択方法”, https://docs.microsoft.com/ja-jp/azure/machine-learning/how-to-select-algorithms, (参照 2022-04-07).
[7] “Which machine learning algorithm should I use?”, https://blogs.sas.com/content/subconsciousmusings/2020/12/09/machine-learning-algorithm-use/, (参照 2022-04-07).
[8] “Overcoming the Barriers to Production-Ready Machine Learning Workflows”, https://cdn.oreillystatic.com/en/assets/1/event/105/Overcoming%20the%20Barriers%20to%20Production-Ready%20Machine-Learning%20Workflows%20Presentation%201.pdf, (参照 2022-04-07).