D-023

情報セキュリティ工学データベースシステム ISEDS の API の実現と応用

Implementation and Applications of an Application Program Interface for Information Security Engineering Database System: ISEDS

堀江 大輔† 後藤 祐一† 程 京徳†
Daisuke Horie Yuichi Goto Jingde Cheng

1. はじめに

高安全性情報システムは，一旦開発された後も，安全性を最善の状態に保つために，その情報システムに対する脅威から情報資産を守る機能，すなわちセキュリティ機能を改善し続ける必要がある．しかし，情報システムに対する脅威の多くは悪意ある人間によって能動的に作り出されるものであるため，セキュリティ機能を保守するためには開発時には考慮できなかった新たな脅威に対してセキュリティ機能の改善を迅速かつ適切に行う必要がある．よって，セキュリティ機能の開発から保守までを一貫して行うことは困難であり，これを一貫して支援するツールが求められている．

我々は，高安全性情報システムにおけるセキュリティ機能の開発から保守までを一貫して支援する汎用的なツールとして情報セキュリティ工学データベースシステム ISEDS を開発しており [6,7]，迅速かつ適切なセキュリティ機能の改善を支援するために不可欠な ISEDS の連携ツール群を提案した [6]．

しかし，現在のところ，ISEDS の連携ツールを開発するためには，連携ツールごとに共通な ISEDS への操作に対して，連携ツールごとに何度もソースコードを記述する必要がある．また，ISEDS のスキーマが更新された際には，新しいスキーマに対応して連携ツールを実装し直す必要がある．このため，ISEDS の連携ツールにおいて，ISEDS を利用することは簡単ではない．

本研究では，ISEDS を利用した連携ツールを簡単に開発することができるようにするために，ISEDS に格納されているデータを連携ツールから利用できるようにするための API を実現する．また，API の利用事例としてセキュリティ機能の設計仕様書作成支援ツールの開発を行い，API を用いて ISEDS のデータを簡単に利用できることを示す．

2. 情報セキュリティ工学データベースシステム ISEDS

ISEDS は，様々なセキュリティ機能の開発から保守までを一貫して支援するために，セキュリティ機能に関するデータを管理するデータベースシステムである．

ISEDS は，情報システムが満たすべきセキュリティ基準に関するデータ（以後，基準データ）を管理する [6]．利用者は，基準データを検索することで，セキュリティ基準を満たすセキュリティを備えた情報システムの開発に役立てることができる．また，既存のセキュリティ機能の保守においてセキュリティ基準の版間の差異を検索することで，セキュリティ基準の更新に対応することができる．また，ISEDS は様々な情報システムにおけるセキュリティ機能の開発や保守の事例に関するデータ（以後，事例データ）も管理する [6]．利用者は，事例データを検索することで，既存の情報システムにおけるセキュリティ機能に関するデータを，新しいセキュリティ機能の開発や既存のセキュリティ機能の保守に役立てることができる．また，ISEDS は各利用者による個々のセキュリティ機能の開発や保守を支援するために，各利用者がセキュリティ機能の開発や保守の際に定義するデータ（以後，個別データ）も管理する [6]．利用者は，個別データを格納しておき，後から検索することで，その利用者が過去に行った開発や保守に関するデータを，新しいセキュリティ機能の開発や既存のセキュリティ機能の保守に役立てることができる．

また，ISEDS が管理するデータの検索を実現するために，データの検索，データの更新支援，データの自動削除を行う連携ツールが提案されている．また，セキュリティ機能を迅速かつ適切に改善するために，セキュリティ機能の要求定義書や設計仕様書などの仕様書の作成を支援する仕様書の作成支援ツールが提案されている．また，既存のセキュリティ機能の保守において，セキュリティ機能がセキュリティ基準を満たしているかどうかを確認するために，仕様書の自動添削と検証支援を行う連携ツールが提案されている．

セキュリティ機能の開発者や保守者は，ISEDS とその連携ツール群を用いてセキュリティ機能に関するデータを簡単に検索したり，仕様書の作成や添削，検証を行うことで，様々なセキュリティ機能の開発から保守までを一貫して行うことができる．

しかし，現在のところ，ISEDS の連携ツールを開発する際に ISEDS を利用することは簡単ではない．一つは，ISEDS の連携ツールを開発するためには，連携ツールごとに共通している ISEDS への操作であっても，連携ツールごとに何度もソースコードを記述しなければならないためである．連携ツールから ISEDS を利用する際の操作の多くは検索や格納など共通しているが，連携ツールを開発する際にはこれらの操作を実行するために SQL クエリを作成，実行するためのソースコードをそれぞれ記述しなければならず，これは労力が必要であるし，何度も同じソースコードを記述する過程において記述ミスも起こりやすい．また，もう一つは，ISEDS のスキーマが更新された際には，新しいスキーマに対応して連携ツールを実装し直さなければならないためである．個別データに関して，利用者が独自の社内基準や独自の方法論に基づい

† 埼玉大学大学院 理工学研究科

た開発事例に関するデータなどを管理しようとする可能性がある．このようなデータの追加や変更に対応するために，個別データを管理するための個別 DB のスキーマは頻繁に更新されることが想定される．個別 DB のスキーマが変更された場合は，連携ツールにおいて SQL クエリを作成および実行するためのソースコードを個別 DB のスキーマに合わせて記述しなければならない．このため，個別 DB のスキーマが更新された際には，連携ツールを実装し直す必要がある．

3．ISEDS の API の実現

連携ツールの開発者が簡単に ISEDS を利用し，既に提案されている連携ツールや独自に提案した新たな連携ツールを開発することができるようにするために，我々は ISEDS における API を実現した．具体的には，近年 Web アプリケーションの開発に頻繁に利用されており，現在 ISEDS の実現に用いられている PostgreSQL や HTML との親和性が高い PHP のメソッドライブラリとして実現した．

3.1 ISEDS が管理するデータの特徴

ISEDS が管理する個別データは頻繁に追加や変更されるため，これに対応するために個別 DB のスキーマは頻繁に更新される．また，基準データは，ISO/IEC 15408 [1,5] や ISO/IEC 17799 [4] のように一つの親データに対して複数の子データが属する階層構造を備えるものが存在する．

ISEDS のメソッドライブラリは，これらの特徴を持つデータを利用するために，連携ツールが備えるべき操作を実現する必要がある．

3.2 ISEDS に対する連携ツールの操作

前節で説明した特徴を持ったデータを管理する ISEDS への連携ツールが備えるべき操作について説明する．

連携ツールが ISEDS に対して実行し得る操作は，基準データと事例データに対しては検索のみであり，個別データに対してはスキーマ変更と検索，格納，更新，そして削除のみである．

個別 DB のスキーマは，利用者が新たに社内基準や独自の方法論を用いた開発事例に関するデータを管理する場合，頻繁に変更されることが想定されているため，この変更を簡単に行えるようにするためにスキーマ変更が必要な操作として挙げられる．また，ISEDS が管理する全てのデータを検索する操作が必要となる．更に，ISEDS が管理する基準データは階層構造を備えるものが想定されているため，ある基準を満たすために満たさなければならない詳細化された基準を検索するなど，一つの親データに属する全ての子データを一括して検索する操作が必要となる．更に，ISEDS が管理する事例データや個別データは，既存のデータを再利用することを目的としているため，新たな情報システムの開発や既存の情報システムの保守の保守には，開発および保守しようとしている情報システムと類似する情報システムや，新たに発見された脅威と類似する既存の脅威を検索するなど，利用者が開発および保守したい情報システムの仕様と類似する既存の仕様データを検索する操作が必要となる．また，ISEDS を用いて個別データを管理するために，個別データの格納と更新，削除の操作が必要となる．

ISEDS のメソッドライブラリは，以上の操作を実現しなければならない．また，個別データの追加に対して個別 DB のスキーマが更新されても，連携ツールを大きく変更したりすることなく利用できるものである必要がある．

3.3 実現したメソッドライブラリ

我々は，前節で挙げた ISEDS への操作を実現するメソッドライブラリを実現した．表 1 は，我々が実現したメソッドライブラリが提供するメソッドの分類と，対応する既存の連携ツール，それぞれの群のメソッド数を表したものである．

表 1: 各メソッド群と連携ツールの対応状況

メソッド群	既存の連携ツール	メソッド数
スキーマ更新	-	9
データ検索	検索，作成支援， 自動添削，検証支援	6
データ更新	更新支援	2
データ削除	自動削除	3

それぞれのメソッド群について，以下で説明する．

スキーマ更新メソッド群: 個別 DB のスキーマの更新を行うためのメソッドを提供する．このメソッド群が提供するメソッドは以下である．

Create_Entity(A, B, C, D): データベース A 上に，C というカラムを持ち，テーブル D を外部参照する実体テーブル B を作成する．

Create_Relational(A, B, C, D): データベース A 上に，テーブル B とテーブル C を外部参照し，カラム D を持つ関連テーブルを作成する．

Drop_Table(A, B): データベース A 上からテーブル B を削除する．

Add_Column(A, B, C, D): データベース A 上のテーブル B の C 番目のカラムとして，D というカラムを挿入する．

Drop_Column(A, B, C): データベース A 上のテーブル B のカラム C を削除する．

Alter_Column(A, B, C, D): データベース A 上のテーブル B のカラム C を，D というカラムに変更する．

Add_Reference(A, B, C): データベース A 上のテーブル B の外部参照先としてテーブル C を追加する．

Drop_Reference(A, B, C): データベース A 上のテーブル B の外部参照先からテーブル C を削除する．

Alter_Reference(A, B, C, D): データベース A 上のテーブル B の外部参照先をテーブル C からテーブル D へと変更する．

データ検索メソッド群: 基準，事例および個別データを検索するためのメソッドを提供する．このメソッド群が提供するメソッドは，以下である．

Select_Single(A, B, C, D): データベース A 上のテーブル B のカラム C から，キーワード D を含むレコードを検索し，レコードを配列として返す．

Select_Bundle(A, B, C, D, E): データベース A 上で，検索条件 E に基づいてテーブル C から検索を行い，検索されたレコードと関連するレコードを，テーブル群 B から出力方法 D に基づいて一括して出力し，レコードを配列として返す．

Select_List(A, B): データベース A 上のテーブル B から全てのレコードを配列として返す．

Select_Analogous(A, B, C, D, E): データベース A 上のテーブル B のカラム C から，単語ごとに重要度 E が重みづけさ

れた文字列 D と類似する文字列を含むレコードを選び，レコードとその類似度数を配列として返す．文字列 D に含まれる単語ごとの重要度は E によって指定され，類似度数を算出する際に，文字列 D の要約となる単語に対して重みを設定することができる．

Select_Recursive(A, B, C, D, E): データベース A 上のテーブル B からテーブル C を経由した自己参照検索を，検索条件 D，出力条件 E に基づいて行い，検索結果として出力されたレコードを配列として返す．

Select_Compliance(A, B): データベース A 上のテーブル群 B に格納されているレコードから階層構造を上層へと辿り，親データが削除されているレコードを検索し，レコードを配列として返す．

更新メソッド群: 個別データを格納および変更するためのメソッドを提供する．このメソッド群が提供するメソッドは，以下である．

Insert_Single(A, B, C): データベース A 上のテーブル B にレコード C を格納する．

Update_Single(A, B, C, D): データベース A 上のテーブル B から検索条件 C に基づいて検索されるレコードを，レコード D へと変更する．

削除メソッド群: 個別データを削除するためのメソッドを提供する．このメソッド群が提供するメソッドは，以下である．

Delete_Single(A, B, C, D): データベース A 上のテーブル B のカラム C から，キーワード D を含むレコードを削除する．

Delete_Bundle(A, B, C D): データベース A 上のテーブル C から検索条件 D に基づいて検索を行い，検索されたレコードと関連するレコードを，テーブル群 B から一括して削除する．

Delete_Analogous(A, B, C, D, E, F): データベース A 上のテーブル B のカラム C から，単語ごとに重要度 E が重みづけされた文字列 D と類似する文字列を検索し，各レコードの類似度数を計算し，閾値 F より高いものを削除する．

4. API を用いた設計仕様書作成支援ツールの開発

我々が実現した API を用いた応用事例として，セキュリティ機能の設計仕様の評価基準に関する国際標準である ISO/IEC 15408 に準拠した設計仕様書の雛形を自動作成するツールをこの API を用いて開発した．

4.1 国際標準 ISO/IEC 15408

ISO/IEC 15408 は，セキュリティ機能の設計仕様を評価するための基準として，セキュリティ機能が満たすべき機能の要件（SFR: Security Functional Requirements）と，セキュリティ機能の保証手段が満たすべき保証の要件（SAR: Security Assurance Requirements）を規定している．

ISO/IEC 15408 は，情報システムの設計仕様書において以下に挙げる仕様を記述しなければならないと規定している．

- 評価対象となる情報システムもしくは情報システムの分野（TOE: Target of Evaluation）
- 情報システムに対する脅威やセキュリティポリシーを含むセキュリティ課題（SP: Security Problem）
- 環境における条件を守り，環境に存在する脅威に対抗するためのセキュリティ対策方針（SO: Security Objective）
- セキュリティ対策方針を達成するために満たすべき SFR と SAR
- SFR を満たすために実装すべきセキュリティ機能の要約仕様（TSS: TOE Summary Specification）
- SP, SO, SFR, SAR, TSS 間の関連性とその根拠（Rationale）

また，これらのデータを記述した ISO/IEC 15408 認証取得済みの設計仕様書が各 ISO/IEC 15408 公式ウェブサイトにて公開されている．

4.2 設計仕様書の作成支援処理の流れ

設計仕様書作成支援ツールは，利用者がツールと対話的にセキュリティ機能の設計仕様書を作成するために，設計仕様書の雛形を自動生成するツールである．このツールにおける設計仕様書の作成支援処理の流れを図 1 に示す．

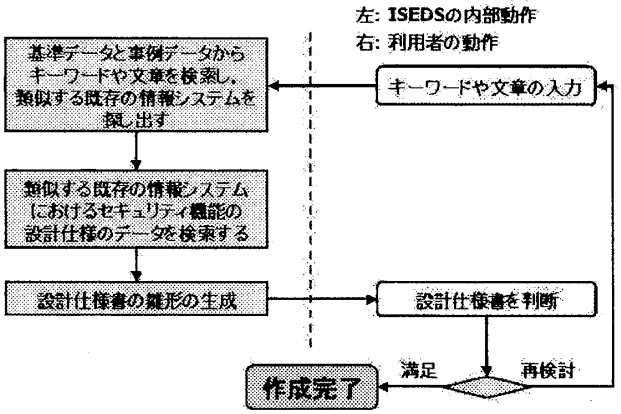

図 1: 設計仕様書の作成支援処理の流れ

利用者は設計したい情報システムの概要となるキーワードや文章を用意する必要がある．これに対し，ISEDS は設計仕様書の TOE データからキーワードや文章を検索し，設計したい情報システムと類似する既存の情報システムを探し出す．更に，この類似する既存の情報システムにおける設計仕様のデータを検索し，検索されたデータを用いて設計仕様書の雛形を生成し，出力する．これに対し利用者は，経験則やテストなどを用いて出力された設計仕様書に記述されている設計仕様が高いセキュリティを満たすものであるかどうかを判断する．その結果，設計仕様書が不十分であると判断した場合には，再度概要を変更して雛形を作成するか，もしくは手作業で設計仕様書の修正を行わなければならない．このように，利用者は ISEDS と対話的に確認や単語入力を適宜行うことで，ISO/IEC 15408 が規定しているセキュリティ機能の要件を満たした設計仕様書の作成を行うことができる．

4.3 設計仕様書作成支援ツールの実装

表 2 は，設計仕様書作成支援ツールの内部処理の流れである．まず，設計したい情報システムと類似する TOE を検索し，採用する TOE を決定する．次に採用する TOE の設計仕様を検索し，重複する設計仕様データを除去する．最後に，設計仕様データを設計仕様書の形式に整形し，ファイルとして出力する．

表 2: 設計仕様書支援ツールの内部処理の流れ

	操作	メソッド
1	類似する TOE の検索	Select_Analogous
2	採用する TOE の決定	-
3	設計仕様データの検索	Select_Bundle
4	重複データの除去	-
5	仕様書ファイル出力	-

設計仕様書支援ツールの内部処理のうち，ISEDS を操作する必要があるのは類似する TOE の検索と設計仕様データの検索である．類似する TOE の検索では，利用者が入力する情報システムの概要と，概要に含まれる単語の重要度を指定することで，設計したい情報システムと類似する TOE を検索する必要がある．また，設計仕様データの検索では，採用する TOE を指定することで，それらの TOE の設計仕様データを検索する必要がある．

設計したい情報システムと類似する既存の TOE を検索するために，Select_Analogous メソッドを用いる．各引数は以下のように与える．

Select_Analogous(事例 DB, TOE, TOE 概要, 設計したい情報システムの概要, 単語と重要度の組):

検索するデータベースは事例データを管理する事例 DB，検索するテーブルは TOE，検索するカラムは TOE の概要を格納するフィールドである TOE 概要として固定する．設計したい情報システムの概要と，概要に含まれる単語とその重要度はユーザが入力したものをそのまま引数として与える．これにより，既存の TOE に対して，設計したい情報システムとの類似度数を算出し，配列として返される．

採用された TOE の設計仕様データを検索するために，Select_Bundle メソッドを用いる．各引数は以下のように与える．

Select_Bundle(事例 DB, 設計仕様，TOE，空集合, 採用された TOE の番号):

検索するデータベースは事例 DB，出力するテーブルは，設計仕様である SP, SO, SFR, SAR, TSS, Rationale を指定し，検索するテーブルは TOE，出力方法は特に指定しないため空集合として固定する．また，検索の条件としては，採用された TOE の番号を与える．これにより，採用された TOE の SP, SO, SFR, SAR, TSS, Rationale のデータが一括して配列として返される．

このように，本研究で実現した API を用いることで，設計仕様書作成支援ツールを簡単に開発することができた．また，本研究にて開発した設計仕様書作成支援ツールをウェブ上にて公開している [3].

また，開発した設計仕様書の作成支援ツールを用いて，実際に設計仕様書の雛形を作成した．本研究では設計対象として IP ルータを想定し，設計対象のプロフィールと設計対象の概要，概要に含まれる重要な単語とその重要度の組を入力した．この結果，既存の二つの TOE に記述された設計仕様データを用いた設計仕様書の雛形が出力された．

このようにして，今回我々が実現した API を用いて，設計仕様書の作成支援ツールの開発を支援できた．

5. おわりに

本研究では，ISEDS の連携ツールを開発するための汎用的な API として，ISEDS が管理しているデータを連携ツールから簡単に利用できるようにするための PHP のメソッドライブラリを実現した．連携ツールの開発者は，この API を用いることで，ISEDS の連携ツールを簡単に開発することができる．また，実現した API を用いて，設計仕様書作成支援ツールを開発することで，API の応用事例を示した．

今回実現した API は，ISEDS のスキーマに依存しないため，新たなデータに対応する連携ツールの開発にも対応している．新たなデータに対しても，類似データの検索や階層構造データの一括検索など，ISEDS が管理するデータに特化した操作を利用した連携ツールの開発を支援することができる．

今後は，ISO/IEC 15408 以外のセキュリティ基準や，セキュリティ機能の開発や保守の事例に関するデータを ISEDS に格納し，今回開発した API を用いてこれらのデータに特化した連携ツールを開発する．また，従来の統合開発環境をセキュリティ機能の開発や保守に応用し，ISEDS が管理するデータを効率的に提供し，様々なセキュリティ機能の開発から保守までを一貫して，統合的に支援する情報セキュリティ工学環境の構築を行う．

[参考文献]

[1] Common Criteria Project: common criteria portal. http://www.commoncriteriaportal.org/.
[2] The Electronic Government Council: MAGERIT. http://www.csae.map.es/
[3] 埼玉大学大学院理工学研究科先端情報システム工学研究室：情報セキュリティ工学データベースシステム ISEDS. http://www.aise.ics.saitamau.ac.jp/iseds/.
[4] 田渕治樹：国際セキュリティ標準 ISO/IEC 17799 入門，オーム社雑誌局，1 edition (2000).
[5] 独立行政法人情報処理推進機構：IT セキュリティ評価及び認証制度（JISEC）. http://www.ipa.go.jp/security/jisec/index.html.
[6] 堀江 大輔, 森本 祥一, 後藤 祐一, 程 京徳: 情報セキュリティ工学データベースシステム ISEDS の開発と応用, 満田成紀・羽生田 栄一編, ソフトウェアエンジニアリング最前線 2006, pp. 59-66, 近代科学社, 2006 年 10 月.
[7] 森本祥一，堀江大輔，程　京徳：ISO/IEC 15408 に基づく情報セキュリティ要求管理データベース，日本データベース学会 Letters，Vol.4, No.3, pp.13–16 (2005).