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

堀江大輔[†] 森本祥一[††]
後藤祐一[†] 程京徳[†]

高安全性が要求される情報システムにおけるセキュリティ機能は設計・実現から運用・保守まで一貫して行われなければならない．しかし，情報システムにおけるセキュリティ機能の設計から保守までを一貫して支援するツールはこれまで存在していなかった．本論文では，様々なセキュリティ機能の設計から保守までを一貫して支援するために我々が提案した情報セキュリティ工学データベースシステムISEDSの開発と応用について述べる．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や，セキュリティ機能の開発や保守の公開事例に関するデータや，各利用者がセキュリティ機能を開発し保守する際に自ら定義するデータを管理する．利用者は，ISEDSに格納されているデータを検索したり更新したりすることができるばかりでなく，ISEDSとその連携ツール群を用いて，セキュリティ機能の仕様書を簡単に作成や添削，検証することもできる．本研究では，まず，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をISEDSが扱うセキュリティ基準の1つとして採用し，ISEDSの機能のうち，ISO/IEC 15408に関連のあるデータを管理し，利用するための機能を実現した．

Development and Applications of ISEDS: An Information Security Engineering Database System

Daisuke Horie,[†] Shoichi Morimoto,[††] Yuichi Goto[†] and Jingde Cheng[†]

Security facilities of information systems with high security requirements have to be designed, implemented, used, and maintained consistently and continuously. However, there was no tool that can support all activities in designing, developing, and maintaining security facilities of information systems consistently and continuously. This paper presents the development and applications of ISEDS, an Information Security Engineering Database System we are developing. ISEDS manages data about information security criteria, data about cases of development and maintenance of security facilities, and data defined by its various users. Developers, users, and maintainers of information systems can retrieve and update these data and also easily generate, correct and verify specifications about security facilities with additional tools of ISEDS. We adopted the international standard ISO/IEC 15408 for information security evaluation as one of security criteria that ISEDS deals with, and implemented functions of ISEDS and its additional tools to manage and use data related to ISO/IEC 15408.

1. はじめに

高安全性が要求される情報システムは，いったん開発された後も，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設計から保守までを一貫して行うことは困難な作業であり，これを一貫して支援するツールが求められている．

一方，ソフトウェア工学の分野において，様々な高信頼性ソフトウェアの開発活動についてデータベースを用いて支援しており，ソフトウェア開発における要求を管理するデータベース[5]や，ソフトウェア開発過

† 埼玉大学大学院理工学研究科
Graduate School of Science and Engineering, Saitama University
†† 産業技術大学院大学産業技術研究科
Advanced Institute of Industrial Technology, School of Industrial Technology

程に得られる情報を管理するリポジトリ[8] などがすでに提案されている．一方，情報セキュリティ工学の分野においては，認証システムの仕様を再利用するために構造化し，そのデータを管理するデータベースがすでに提案されている[1]．しかし，このデータベースはセキュリティ機能の一分野である認証システムしか扱うことができず，また，開発の支援のみに特化している．他にも，セキュリティ評価のための方法論である MAGERIT に基づくセキュリティ要求を再利用するために管理するリポジトリが提案されている[10]．しかし，このリポジトリはセキュリティに関する要求定義やリスク分析，対策の決定の支援しか行うことができない．このように，セキュリティ機能の設計から保守までを一貫して支援する汎用的なデータベースは国内外においてこれまで存在していなかった．

我々は，セキュリティ機能が満たすべきセキュリティ基準やセキュリティ機能の開発や保守における公開事例など，セキュリティ機能に関する様々なデータを構造化し，管理する汎用的なデータベースシステム ISEDS（Information Security Engineering Database System）を提案した[17]．しかし，従来の ISEDS はセキュリティ機能の設計を支援することのみに特化しており，設計から保守までを一貫して支援することができなかった[3),6),17)]．

そこで本研究では，高安全性情報システムにおけるセキュリティ機能の設計から保守までを一貫して支援する汎用的なデータベースシステムとして ISEDS の開発を行う．また，迅速かつ適切なセキュリティ改善の支援を行うために，ISEDS の連携ツール群の開発を行う．このために，セキュリティ機能の設計から保守までを一貫して支援する汎用的なデータベースシステムとしての ISEDS とその連携ツール群に対する要求の再定義を行い，ISEDS とその連携ツール群の機能のうち，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 に関するデータを管理し利用するための機能を実現する．

2 章では，本研究で開発する ISEDS とその連携ツール群について説明し，実現すべき利用形態と利用法，想定される応用事例について述べる．3 章では，ISEDS とその連携ツール群が満たすべき要求と機能について述べる．4 章では，情報セキュリティ評価の国際標準である ISO/IEC 15408 に関するデータを管理するための ISEDS とその連携ツール群の機能の実現について述べる．5 章では，今回実現した ISEDS とその連携ツール群の利用事例について述べる．6 章では，今回実現した ISEDS とその連携ツール群について考察を行う．7 章ではまとめを述べる．

2. 情報セキュリティ工学データベースシステム ISEDS

2.1 情報セキュリティ工学データベースシステム ISEDS

ISEDS は，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 は以下のデータを管理する．

基準データ：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である．セキュリティ基準の例としては，情報セキュリティ評価の国際標準である ISO/IEC 15408 や，セキュリティ管理対策の国際標準である ISO/IEC 17799 や ISO/IEC TR 13335 などがあげられる．ISEDS は，これらをはじめとするセキュリティ基準が規定している要件やそれらの形式的記述，セキュリティに関する用語とその意味のデータを管理する．

事例データ：様々なセキュリティ機能の開発や保守の公開事例に関するデータである．これは，既存の様々なセキュリティ機能の要求定義，設計，実装を含む開発や保守の際に得られた仕様明細，図表，ソースコード，試行データである．事例データは，セキュリティ基準に基づいて評価され，認証を取得したセキュリティ機能の仕様に関するデータを含む．

個別データ：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である．これは，セキュリティ機能の要求定義，設計，実装を含む開発や保守において，各利用者が開発や保守の際に得た仕様明細，図表，ソースコード，試行データである．

また，セキュリティを迅速かつ適切に改善するために，ISEDS とその連携ツール群によって，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．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，既存の仕様書の添削や検証を支援する．さらに，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更新に対応するために，セキュリティ基準の版間の差異を提示する．

利用者は，基準データを検索し，参照することで，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を開発し，保守することができる．また，事例データを検索し，参照することで，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保守に役立てることができる．また，個別データを格納しておき，後から検

索し，参照することで，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．さらに，仕様書の作成や添削，検証を行うことで，既存のセキュリティ機能の保守におけるセキュリティ機能の改善を迅速かつ適切に行うことができる．

このようにして，セキュリティ機能の開発者や保守者は，様々なセキュリティ機能の設計から保守までを一貫して行うことができる．

2.2 ISEDS の使用者

ISEDS の使用者は，利用者と管理者の 2 種類に分けることができる．

利用者は，ISEDS を用いてデータを検索し，セキュリティ機能の開発や保守を行う．ISEDS の利用者は，セキュリティ機能の考案者，運用者，開発者，保守者などである．考案者や運用者は，ISEDS を用いてセキュリティ機能に関する要求の分析を行う．開発者や保守者は，ISEDS を用いてセキュリティ機能に対する要求の確認やセキュリティ機能の実装，および実装されたセキュリティ機能が高いセキュリティを備えているものであるかどうかの分析を行う．すべての利用者は，情報セキュリティ工学と情報システム開発に関する一般的な知識さえあれば，ISEDS を利用することができる．

管理者は，ISEDS の設置および運用を行う．ISEDS の管理者はデータベース管理システムとウェブサーバの設置と運用ができなければならない．

2.3 実現すべき利用形態

ISEDS が実現すべき利用形態は，大きく 2 種類に分けられる．

1 つ目は，複数の利用者が単一の ISEDS を共同で利用する利用形態である．基準データや事例データは汎用的であり，広く公開されたデータであるため，その漏洩が致命的となることはない．このため，これらのデータを単一の ISEDS で一元管理し，利用者がその ISEDS を共同で利用することが考えられる．

2 つ目は，組織もしくは個人ごとに ISEDS を運用し，データをその組織もしくは個人の下でのみ管理する利用形態である．ISEDS が管理するデータは，汎用的なデータだけではなく，各利用者が開発や保守の際に定義した個別データを含む．このため，これらのデータが改竄されたり，部外者によって閲覧されたりすることは致命的となるため，これらのデータを他人に委ねることを好まない利用者が存在することが考えられる．よって，組織もしくは個人が独自に ISEDS を管理し，組織内もしくはその個人のみがこれらの個別データを扱えるようにすることが考えられる．

2.4 実現すべき利用法

利用者が，ISEDS とその連携ツール群を用いて，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おいて行う利用法として，以下の 8 つの利用法を実現すべきである．

利用法 1：利用者は，セキュリティ基準が規定している情報セキュリティに関する用語とその説明を検索し，ISEDS を情報セキュリティに関する辞書や辞典のように利用する．

利用法 2：利用者は，セキュリティ基準が規定している要件や，それらの形式的記述を検索する．

利用法 3：利用者は，既存の様々なセキュリティ機能の開発や保守の際に定義された仕様明細，図表，ソースコード，試行データを検索する．

利用法 4：利用者は，利用者自身が開発や保守の際に定義した仕様明細，図表，ソースコード，試行データを ISEDS に格納しておき，後から検索する．

利用法 5：利用者は，開発や保守したい情報システムの概要となる単語や文章を ISEDS の連携ツールに入力し，ISEDS が管理しているセキュリティ基準と事例に基づいて，セキュリティ基準が規定している要件を満たすセキュリティ機能の仕様書を ISEDS の連携ツールと対話的に作成する．

利用法 6：利用者は，ISEDS を用いずに作成したセキュリティ機能の仕様書を ISEDS の連携ツールに入力し，セキュリティ基準や事例と照合させて，その仕様書を自動的に添削させる．

利用法 7：利用者は，ISEDS を用いずに作成したセキュリティ機能の仕様書を ISEDS の連携ツールに入力し，セキュリティ基準が規定している要件を満たしているかどうかを形式的に検証させる．

利用法 8：利用者は，ISEDS が管理しているセキュリティ基準の版間の差異を参照する．

2.5 想定した応用事例

前節であげた利用法に基づき，以下の 2 つの応用事例を想定した．

応用事例 1：ISEDS に加えて，高信頼性ソフトウェアの開発を支援するデータベースを統合したデータベースシステムを開発する．ソフトウェア開発における要求を管理するデータベースや，ソフトウェア開発過程で得られる情報を管理するデータベースなどは，ソフトウェア開発に関するデータを提供することができる．ISEDS は利用法 2 と 3 に基づき，セキュリティ機能の基準や事例に関するデータを提供することができる．これにより，高信頼性と高安全性の両方を備えたソフ

トウェアの開発全般を支援することができる．

応用事例 2：高安全性情報システムにおけるセキュリティ機能を保守するために，ソフトウェアの動的なセキュリティテストの手法がすでに提案されている[9]．この手法では，ソフトウェアに対する攻撃を自動的に検出し，攻撃の情報を取得する．この情報に基づき，情報システムの保守者はテストを行い，ソフトウェアのセキュリティ機能を改善する．一方，ISEDS は利用法 5 に基づき，情報システムへの攻撃に対してセキュリティ機能の仕様書の迅速な作成を支援することができる．このため，動的なセキュリティテストの手法におけるセキュリティ機能の改善に ISEDS を利用することで，ソフトウェアのセキュリティ機能をより迅速に改善することができる．

3. 要求と機能

3.1 ISEDS とその連携ツール群に対する要求

セキュリティ機能の設計から保守までを一貫して支援するためには，前章で述べた利用形態と利用法を実現しなければならない．このために ISEDS とその連携ツール群が実現すべき要求を最低限要求と定義し，以下に述べる．

R1-1：利用法 1 において，利用者が ISEDS を情報セキュリティに関する辞書や辞典のように利用することができるようにするために，セキュリティ基準が規定している情報セキュリティに関する用語とその説明のデータを検索できなければならない．

R1-2：利用法 2，5，6，7 において，セキュリティ機能の開発や保守を汎用的に支援するために，セキュリティ基準が規定している要件や，それらの形式的記述のデータを検索できなければならない．

R1-3：利用法 3，5，6 において，セキュリティ機能の開発や保守を汎用的に支援するために，開発や保守の事例に関するデータを検索できなければならない．

R1-4：利用法 4 において，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，各利用者が開発や保守の際に定義するデータを格納および検索できなければならない．

R1-5：利用法 5 において，利用者が選択したセキュリティ基準を満たす仕様書を作成することができるようにするために，利用者と対話的に仕様書を作成することができなければならない．

R1-6：利用法 6 において，ISEDS を用いずに作成された既存の仕様書に記述されている仕様が，利用者が選択したセキュリティ基準に対して不足もしくは冗長でないかどうかを確認するために，利用者が入力したセキュリティ機能の仕様書を自動的に添削できなければならない．

R1-7：利用法 7 において，ISEDS を用いずに作成された既存の仕様書が，利用者が選択したセキュリティ基準を満たすものであるかどうかを検証するために，利用者が入力したセキュリティ機能の仕様書の検証を支援することができなければならない．

R1-8：利用法 8 において，ISEDS が扱うセキュリティ基準が更新され，新たな版が公開された場合に，旧版に準拠したセキュリティ機能を新版に対応するように改善するために，セキュリティ基準の版間の差異を提示することができなければならない．

R1-9：利用法 1，2，3，4 において，利用者が参照したいデータだけを選んで検索できるようにするために，データの種類，範囲，条件，関連性を利用者が自由に指定して，それぞれのデータの検索範囲を絞り込んで検索できなければならない．

R1-10：すべての利用形態において，ISEDS が管理するデータの改竄，漏洩，紛失を防ぐために，妥当なセキュリティ対策が施されていなければならない．

ISEDS は，実用的に利用するために満たすべき要求として，以下の基本的要求を満たさなければならない．

R2-1：すべての利用法において，利用者が簡単に ISEDS を操作できるようにするために，データベースを操作するための特別な知識なしでも ISEDS を操作できるようにしなければならない．

R2-2：すべての利用形態において，管理者や利用者が，いつでも，どこからでも ISEDS を操作できるようにするために，ウェブを通して ISEDS を操作するための機能を提供しなければならない．

ISEDS は，利用者に，より高い利便性を提供するために満たすべき要求として，以下の発展的要求を満たさなければならない．

R3-1：利用法 4 において，利用者がより簡単にデータを格納できるようにするために，仕様書から自動的にデータを抽出して格納できなければならない．

R3-2：利用法 4 において，各利用者が開発や保守の際に定義して ISEDS に格納したデータを簡単に削除できるようにするために，利用者がこれらのデータを削除する際，そのデータの削除によって整合性が失われるすべてのデータを自動的に削除できなければならない．

R3-3：利用法 4 において，各利用者が開発や保守の際に定義したデータを ISEDS に格納する際に，すでに格納されているデータと新しく格納するデータとの

間に矛盾が生じるか否かを判定し，利用者に報告できなければならない．

R3-4：組織もしくは個人ごとに ISEDS を運用し，データをその組織もしくは個人の下でのみ管理する利用形態において，組織内で個別データを共有する場合，個別データの改竄，漏洩，紛失を防ぐために，組織における ISEDS の管理者が組織内における部門や個人に対してデータへのアクセス権限を設定できなければならない．

3.2 要求を満たす機能

前節であげたそれぞれの要求を満たすために，ISEDS とその連携ツール群は以下の機能を実現しなければならない．

F1-1：R1-1，R1-2 を満たすために，セキュリティ基準に関するデータを検索できるようにする．

F1-2：R1-3 を満たすために，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検索できるようにする．

F1-3：R1-4 を満たすために，各々の利用者が開発や保守の際に定義するデータを格納および検索できるようにする．

F1-4：R1-5 を満たすために，情報システムに関連する単語や文章を入力することで，目的に対応する基準データや，利用者が開発および保守したい情報システムと類似する情報システムの事例データを検索し，検索されたデータから利用者が選択したセキュリティ基準を満たす仕様書の雛形を自動的に作成できるようにする．

F1-5：R1-6 を満たすために，添削したい情報システムの仕様書を入力することで，目的に対応する基準データおよび添削したい情報システムと類似する情報システムの事例データを検索し，検索されたデータと仕様書と比較し，仕様書を自動的に添削できるようにする．

F1-6：R1-7 を満たすために，検証したい情報システムの仕様書を入力することで，目的に対応するセキュリティ基準が規定している要件の形式的記述のデータを検索し，検索されたデータから仕様書を形式的に検証できるようにする．

F1-7：R1-8 を満たすために，ISEDS が格納しているセキュリティ基準の版間の差異を一覧表示し，見やすく表示できるようにする．

F1-8：R1-9 を満たすために，メニューから選択肢を選択したり，文字入力によりキーワードを指定したりすることで，データの種類，範囲，条件，関連性を利用者が指定して，検索範囲を絞り込んで ISEDS が管理する全データを検索できるようにする．

F1-9：R1-10 を満たすために，ISEDS に格納されるデータに対するアクセス制御を行うことができるようにする．

F1-10：R1-10 を満たすために，管理者サーバやデータベース管理システムにおいて物理的，論理的な安全性，信頼性対策の手段を提供する．

F2-1：R2-1 を満たすために，GUI を用いたウェブユーザインタフェースを用意し，利用者が簡単に ISEDS を操作し，簡単に結果を参照できるようにする．

F2-2：R2-2 を満たすために，ウェブを通して ISEDS を操作できるようにする．

F3-1：R3-1 を満たすために，入力された仕様書を読み取ることで，半自動的にデータを抽出し，ISEDS に格納できるようにする．

F3-2：R3-2 を満たすために，データが削除される際，その削除によって整合性が失われる他のすべてのデータを検索し，それらのデータを自動的に削除できるようにする．

F3-3：R3-3 を満たすために，各利用者が開発や保守の際に定義したデータを ISEDS に格納する際に，すでに格納されているデータと新しく格納するデータを比較して矛盾を検知できるようにする．

F3-4：R3-4 を満たすために，各利用者で独自にアカウントを設定し，そのアカウントごとに各データへのアクセス制御を行うことができるようにする．

4. ISO/IEC 15408 に関するデータを管理するための機能の実現

本研究では，ISEDS が管理するデータの対象の 1 つとして，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 に関するデータを採用する．ISO/IEC 15408 は，ISO と IEC によるジョイント組織により制定された．また，内閣官房の情報セキュリティセンターから公表された「政府機関の情報セキュリティ対策のための統一基準」において，政府機関で使用される情報システムの評価において ISO/IEC 15408 を利用することが決定され，国内において重要度が高まっている[15]．また，前章で述べた ISEDS とその連携ツールのすべての機能のうち，ISO/IEC 15408 に関するデータを管理するための機能を実現する．

ISO/IEC 15408 はセキュリティ機能の設計仕様の基準であり，ISO/IEC 15408 に関するデータを管理するための機能を利用することでセキュリティ機能の

設計を支援することができる．また，セキュリティ機能を保守する際には，新たな脅威に対抗するためにセキュリティ機能の再設計を迅速かつ適切に行うことが重要となるため，ISO/IEC 15408 に関するデータを管理するための機能を利用することで，設計仕様書の作成や添削，検証を支援することにより，セキュリティ機能の保守において迅速かつ適切な再設計を支援することができる．また，ISO/IEC 15408 に準拠した情報システムの保守において，ISO/IEC 15408 が更新された際に，旧版と新版の差異を提示することにより，最新版の ISO/IEC 15408 に対応したセキュリティ機能の再設計を支援することができる．

4.1 ISO/IEC 15408 に関するデータ

ISO/IEC 15408 は，情報システムにおける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 で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評価手段が満たすべき保証の要件（SAR: Security Assurance Requirements）が規定されている．SAR に関しては，特定の SAR の組合せを満たすことによる評価保証レベル（EAL: Evaluation Assurance Level）を，セキュリティ機能の実装の厳密さの度合いとして規定している．また，ISO/IEC 15408 ではセキュリティに関する用語についてその定義と意味を規定している．ISEDS は，SFR，SAR および用語のデータを ISO/IEC 15408 に関する基準データとして管理する．また，情報システムが ISO/IEC 15408 による評価，認証を受ける際には，セキュリティ機能の設計仕様を記述した設計仕様書を作成しなければならない．ISO/IEC 15408 は，この仕様書に記述すべき設計仕様を規定している．具体的には，ISO/IEC 15408 による評価，認証を受ける際には，セキュリティ機能の設計者はトップダウン式に設計を行い，以下にあげる仕様を記述しなければならない．

- 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）
- TOE が運用される環境における脅威やセキュリティポリシ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

また，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おいて公開されている[2]．ISEDS は，この ISO/IEC 15408 認証取得済みの設計仕様書に記述されている設計仕様のデータを ISO/IEC 15408 に関する事例データとして管理する．また，設計者が定義した上記の仕様に関するデータを ISO/IEC 15408 に関する個別データとして管理する．

現在，ISO/IEC 15408 は最新版である 2.3 版と 3.1 版が公開されており[2]，日本語版も公開されている[14]．ISO/IEC 15408 の版によって，設計仕様書に記述すべき設計仕様や SFR と SAR の数，内容が異なる．

4.2 ISO/IEC 15408 に関するデータを管理するための機能コンポーネント

ISO/IEC 15408 に関するデータを管理し利用するために，ISEDS とその連携ツール群は**図 1** に示すとおり，ISEDS 本体であるデータベース群と，連携ツールとして，最低限機能を実現するデータの検索機能コンポーネント，仕様書の作成支援機能コンポーネント，仕様書の自動添削機能コンポーネント，仕様書の検証支援機能コンポーネントと，基本的機能を実現するウェブユーザインタフェース，発展的機能を実現するデータの格納支援機能コンポーネント，データの自動削除機能コンポーネントという 8 つの機能コンポーネントより構成される．

また，それぞれの機能コンポーネントと要求，機能の対応を**表 1** に示す．また，F1-9，F1-10 に対しては，各機能コンポーネントにセキュリティ対策を施す

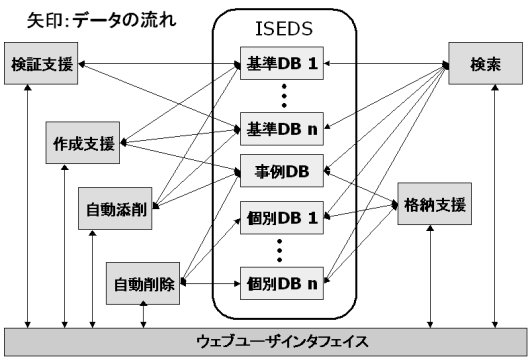

図 1 ISO/IEC 15408 に関するデータを管理するための機能コンポーネント
Fig. 1 Functional component to manage the data about ISO/IEC 15408.

表 1 機能コンポーネントと要求，機能の対応と実現状況
Table 1 Progress and correspondence about the functional components, the requirements and the function.

機能コンポーネント	対応する機能	対応する要求
データベース群	F1-1，F1-2 F1-3	R1-1，R1-2 R1-3，R1-4
検索	F1-7，F1-8 F2-1	R1-8，R1-9 R2-1
作成支援	F1-4	R1-5
自動添削	F1-5	R1-6
検証支援	F1-6	R1-7
ウェブユーザ インタフェース	F2-1，F2-2 (F3-4)	R2-1，R2-2 (R3-4)
格納支援	F3-1，(F3-3)	R3-1，(R3-3)
自動削除	F3-2	R3-2

ことで，ISEDS のセキュリティ機能を実現する．また，今回は最低限機能と基本的機能の実現を行い，発展的機能に関しては F3-1 と F3-2 のみ実現した．それぞれの機能コンポーネントについて，以下で述べる．

データベース群：TOE，SP，SO，TSS，SFR，SAR および，これらの関連性に関するデータを格納する．

まず，ISO/IEC 15408 の新しい版が公開された場合に現状のデータを維持しつつ新しいデータに対応するために，基準データを版ごとに分けて管理することとした．また，新たにユーザが追加された場合に現状のデータを維持しつつ新しいデータに対応するために，個別データを利用者ごとに分けて管理することとした．これにより，ISO/IEC 15408 の新たな版が公開されたり，ユーザが追加されたりしたとしても，従来のデータベースには触れることなく，新たな版を管理するためのデータベースを追加することができる．また，新たな版においてスキーマが同じならば，従来のスキーマをまったく変更することなく新たな版を管理するためのテーブルを追加することができる．このために，基準データ，事例データ，個別データをそれぞれ基準 DB，事例 DB，個別 DB というデータベースに分けて管理することとした．

また，管理者と利用者に対して，それぞれデータベースへの操作権限を**表 2** に示す．

また，それぞれの DB について，最も一般的に普及しており種類が豊富であるリレーショナルデータベースで実現することとした．このために，ISO/IEC 15408 に関するデータの ER モデルを作成する．まず，TOE は実体である．次に，SP は実体であり，個々の TOE に対して複数想定されるものである．よって TOE と SP との関係は 1 対多である．次に，SO は実体であり，1 つもしくは複数の SP に対して達成されるものである．また，1 つの SP に対抗するために，1 つもしくは複数の SO が達成される．よって，SP と SO との関係は多対多である．次に，SFR は実体であり，1 つもしくは複数の SO を達成するために実現されるものである．また，1 つの SO を達成するために，1 つもしくは複数の SFR が実現される．よって，SO と SFR の関係は多対多である．次に，SAR は実体であり，1 つもしくは複数の SO を達成するために実現されるものである．また，1 つの SO を達成するために，1 つもしくは複数の SAR が実現される．よって，SO と SAR の関係は多対多である．次に，TSS は実体であり，1 つもしくは複数の SFR を実現するために実装されるものである．また，1 つの SFR を実現するために，1 つもしくは複数の TSS が実装される．よって，SFR と TSS の関係は多対多である．

これらの実体およびこれらの実体が持つすべての属性を格納できるようにスキーマ設計を行った．また，データ間の関連性と依存性を実現し，検索できるようにスキーマ設計を行った．**図 2** は，データベース群の ER 図である．

また，ISO/IEC 15408 第 2.3 版と第 3.0 版の英語版と日本語版によって規定されている SFR と SAR の基準データを ISO/IEC 15408 文書から必要な箇所を抜き出して基準 DB に格納した．また，ISO/IEC 15408 認証取得済みの設計仕様書に記述されている事例データを，日本語版については ISO/IEC 15408 認証取得済みの設計仕様書から必要な箇所を抜き出して，英語

表 2 ISEDS への操作の権限
Table 2 Access authorization of ISEDS.

	格納	検索	削除
基準 DB	管理者	すべての利用者	-
事例 DB	管理者と 一部の利用者	すべての利用者	管理者と 一部の利用者
個別 DB	すべての利用者	格納した 利用者	格納した 利用者

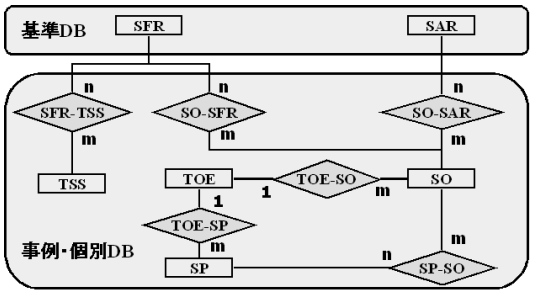

図 2 ISO/IEC 15408 に関するデータベース群の ER 図
Fig. 2 ER diagram of databases about ISO/IEC 15408.

表 3 ISO/IEC 15408 に関するデータのレコード数
Table 3 Number of the records of the data about ISO/IEC 15408.

	2.3 版	3.0 版	未格納
基準データ	2,851	2,447	0
形式化された基準データ	635	0（未形式化なため）	0
事例データ（仕様書 64 件）	4,631	0（未公開なため）	300

版についてはデータの格納支援機能コンポーネントを用いて事例 DB に格納した．15408 が規定している設計仕様に基づき各利用者が定義する個別データに関しては各利用者が格納するものであるため，本研究では格納は行わない．格納したデータ数を**表 3** に示す．

データの検索機能コンポーネント：利用者が，SQL に関する知識なしでも，検索したいデータベースの種類，データの種類，テーブル，属性，キーワード，数値などの検索範囲と検索結果の条件を指定して全データを検索するための機能を提供するコンポーネントである．

利用者は，検索したいデータベースの種類，データの種類，テーブル，属性，キーワード，数値などの検索範囲と検索結果の条件をプルダウンメニューやチェックボックスなどから選択する．検索機能コンポーネントは，この操作に基づいて動的に SQL 文を生成し，データベースへと送る．これにより，利用者はデータベースを操作するための特別な知識なしでもデータの検索を行うことができる．

また，ISO/IEC 15408 の規定は，版によって異なっている．この違いを比較するため，各版ごとの用語の定義の違いや，各 SFR と SAR の版ごとの有無を表示したり，特定の SFR や SAR の版ごとの定義の違いなどを提示したりすることができる．

設計仕様書の作成支援機能コンポーネント：利用者が，ISEDS と対話的にセキュリティ機能の設計仕様書の雛形を作成するための機能を提供するコンポーネントである．

この設計仕様書の作成支援機能コンポーネントの処理の流れを**図 3** に示す．まず，利用者は設計したい情報システムの概要となる単語や文章を用意し，この単語および文章とデータ使用の厳密さの度合いを入力する．データ使用の厳密さの度合いは，作成する設計仕様書の雛形に使用する設計仕様として，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の設計仕様をどれだけ隈なく使用するかを決定する値である．また，正確性に関して，出力される設計仕様書の雛形が高いセキュリティを備えるものになるかどうかは，利

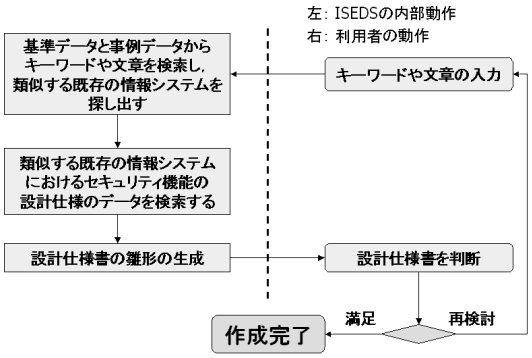

図 3 設計仕様書の作成支援処理の流れ
Fig. 3 Flow of the document creation.

用者の意図をよく反映した単語や文章が選ばれているかどうかに依存するため，利用者は慎重にこの単語や文章を選択し，入力する必要がある．これに対し，作成支援機能コンポーネントは ISEDS が管理している基準データと事例データの中から，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．このために，入力された単語や文章を概要に含む情報システムのデータを検索する．単語や文章が複数入力された場合は，それぞれの単語や文章について検索を行い，より多くの単語を概要に含む情報システムのデータを類似性が高い情報システムのデータと見なす．さらに，データ使用の厳密さの度合いに基づき，作成する設計仕様書の雛形に使用する情報システムを決定する．最後に，この情報システムの設計仕様である SP や SO，SFR，SAR，TSS 間の関連性のデータを図表化して整形し，SP や SO，SFR，SAR，TSS のデータとともに設計仕様書の雛形として出力する．

具体的な類似性判定の流れは以下のようになっている．

(1) 利用者は，単語とその重要度，データ使用の厳密さの度合いを入力する．
(2) ある既存の情報システムを 1 つ選び，それぞれの単語を，情報システムにおける名称や分野，概要など，複数の検索対象から検索する．
(3) 単語が発見された場合，その単語の重要度と検索対象の重要度に応じた得点を加算する．
(4) すべての単語と検索対象の組合せについて検索を行い，総得点をその既存の情報システムの得点とする．
(5) 既存のすべての情報システムにおいて，この得点を計算する．
(6) この得点が多いものほど類似性が高いとし，すべての情報システムのうちの最高得点とデータ

使用の厳密さの度合いから，データ使用の閾値を決定する．

(7) 閾値を超える得点を得た情報システムの設計仕様をもとに，新たな設計仕様書を作成する．

また，情報システム l の得点 P_l および閾値 P_{border} の算出式は以下のようになっている．

$$P_l = \sum_{i=1}^{n}\sum_{j=1}^{m}(K_i A_j t)$$

$$P_{border} = P_{max}(1-(L/100))$$

K_i（$i = 1, 2, \ldots, n$）はキーワード i の重要度であり，利用者が入力するものである．n は，利用者が入力したキーワード数である．

A_j（$i = 1, 2, \ldots, m$）は検索対象 j のそれぞれの重要度であり，作成支援機能コンポーネントの開発者によってあらかじめ設定されている．m は検索対象数である．

t はキーワード i が情報システム l における検索対象 j から検索されれば 1，検索されなければ 0 となる．

P_{max} はすべての情報システムの得点 P_l の最大値である．

L はデータ使用の厳密さの度合いであり，利用者が 0 から 100 までの値を選択することができ，この値が高いほど閾値 P_{border} は低くなり，より多くの設計仕様書に記述されている設計仕様を使用して設計仕様書の雛形が作成される．

さらに，作成支援機能コンポーネントはこの類似する既存の情報システムが想定している SP や，満たすべき SFR などの設計仕様のデータを検索し，検索されたデータから設計仕様書の雛形を生成して出力する．妥当性に関して，作成された雛形は少なくとも ISO/IEC 15408 が保証するだけのセキュリティを備えるために十分に足りる設計仕様を備えているが，複数の設計仕様書が使用された場合に，異なる設計仕様書から抽出された設計仕様間に矛盾が生じる可能性が存在する．また，作成支援機能コンポーネントに入力したキーワードが，利用者が設計したい情報システムをよく反映したものでない場合は，ISO/IEC 15408 の認証を得た設計仕様をもとにしていても，利用者の意図を反映していない正確性の低い設計仕様書が出力される場合もあるため，利用者が望む設計仕様が選ばれているかどうかは，利用者が入力するキーワードに依存する．このため利用者は，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．この結果，設計仕様書が不十分であると判断した場合には，再度キーワードを変更して雛形を作成したり，手作業で設計仕様書の修正を行ったりしなければならない．この判断や修正の工程の労力や妥当性・正確性は，利用者の能力に依存する．この作業を繰り返し，設計仕様が高いセキュリティを満たすものであると判断した場合は，設計仕様書の作成が完了したと見なす．このように，利用者は設計仕様の作成支援機能コンポーネント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．

設計仕様書の自動添削機能コンポーネント：入力された設計仕様書を，利用者が選択したセキュリティ基準や，その基準に準拠した事例と自動的に照合し，添削された仕様書を出力する機能を提供するコンポーネントである．

この設計仕様書の自動添削機能コンポーネントの処理の流れを**図 4** に示す．まず，利用者は添削したいセキュリティ機能の設計仕様書の TXT ファイルを準備しなければならない．この TXT ファイルをウェブからアップロードすることで，設計仕様書を入力する．これに対し自動添削機能コンポーネントは，入力された設計仕様書から，情報システムの概要となる部分を抽出する．さらに，設計仕様書の作成支援機能コンポーネントと同様に，この概要に含まれる単語や文章を基準データや事例データから検索することで，添削したい設計仕様書が記述している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．さらに自動添削機能コンポーネントは，この類似する既存の情報システムが満たすべき SFR や SAR のデータを検索し，検索された設計仕様のデータと，設計仕様書に記述された設計仕様を照合する．この結果，基準データや事例データからは検索されたにもかかわらず，入力された

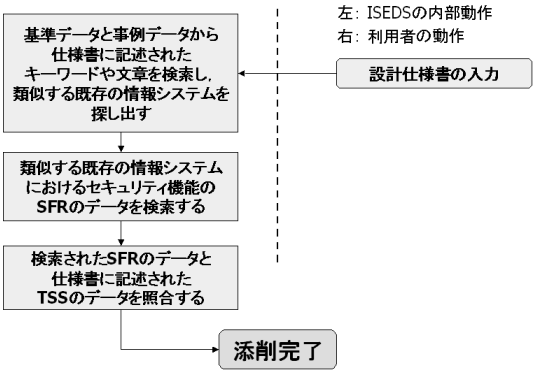

図 4 設計仕様書の自動添削処理の流れ
Fig. 4 Flow of the document correction.

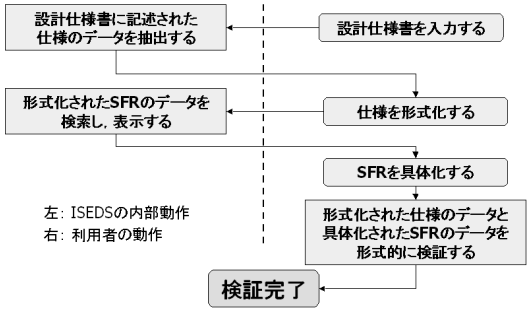

図 5 設計仕様書の検証支援処理の流れ
Fig. 5 Flow of the document verification.

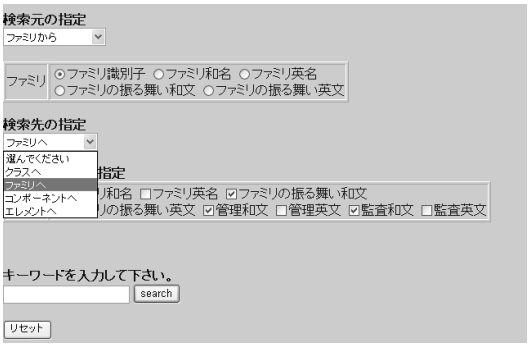

図 6 ISEDS のウェブユーザインタフェースの外観
Fig. 6 Overview of the web user interface of ISEDS.

設計仕様書に記述されていない SFR や SAR は，不足している仕様として追加を促す．また，基準データや事例データからは検索されていないにもかかわらず，入力された設計仕様書に記述されている SFR や SAR は，冗長な仕様として削除を促す．

設計仕様書の検証支援機能コンポーネント：入力された設計仕様書を読み取り，セキュリティ機能である TSS のデータと，各 TSS を実現するために満たすべき SFR の形式的記述のデータを自動的に検索する機能を提供するコンポーネントである．

ISO/IEC 15408 が規定している SFR に基づき，セキュリティ機能の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形式的に検証する技法がすでに提案されている[7),18)]．この技法では，形式化し具体化した SFR と，形式化した設計仕様を定理証明とモデル検査により検証する．この技法による設計仕様書の検証を支援する検証支援機能コンポーネントの処理の流れを**図 5** に示す．

まず，利用者は添削したいセキュリティ機能の設計仕様書の XML ファイルを準備しなければならない．この XML ファイルをウェブからアップロードすることで，設計仕様書を入力する．

これに対し検証支援機能コンポーネントは，入力された設計仕様書から，セキュリティ機能の仕様となる部分を抽出する．利用者は，抽出された仕様を Z 記法により形式化する．この際，PP（Protection Profile）と呼ばれる設計仕様書の雛形を UML によりモデル化し，これを用いて設計仕様書を記述する方法[16)] を用いることで，UML 化された仕様を半自動的に形式化する手法が提案されている．また，検証支援機能コンポーネントは，形式化された SFR のデータを検索し，表示する．また各 SFR は，設計対象となる情報システムに依存する部分をパラメータとしており，このパラメータは，設計対象に対応するように具体的に設定しなければならない．利用者は，この形式化された SFR を，検証したいセキュリティ機能に対応するように具体化する．これにより，利用者は，形式化された仕様と，形式化し具体化された SFR を，定理証明とモデル検査により形式的に検証することができる．

ウェブユーザインタフェース：2.4 節で想定したすべての利用法を，いつでも，どこからでも，簡単に実行することができるように，GUI を用いた ISEDS のインタフェースを提供するコンポーネントである．

ISEDS のウェブユーザインタフェースの外観を**図 6** に示す．利用者は，このウェブユーザインタフェースを通して検索，格納支援，自動削除，作成支援，自動添削，検証支援の各機能コンポーネントを呼び出すことができる．また，これらの機能を実行した結果を，GUI により見やすい形で表示する．このウェブユーザインタフェースは 2.3 節で想定した 2 種類の利用形態の両方で利用することができる．また，ウェブユーザインタフェース上でユーザの認証を実現した．

データの格納支援機能コンポーネント：入力された設計仕様書に記述されているデータを半自動的に読み取ることで，利用者と対話的に ISEDS へとデータを格納する機能を提供するコンポーネントである．

設計仕様書は，仕様書の著者ごとに様々な表記法や記述法で記述されており，これらの仕様書に記述されたデータを完全に自動的に読み取ることは困難である．そこで，利用者は設計仕様書の XML ファイルを準備しなければならない．

利用者は，この XML ファイルを入力し，さらにこの XML ファイルのタグをどのように読み取るかを指定させる．これに対し，ISEDS はこの XML ファイルのタグを読み取り，TOE のプロフィールや SP，SO，SFR，SAR，TSS の名称や定義，関連性などのデータを自動的に抽出する．さらに．抽出されたデータが正確に抽出されているかどうかを適宜格納者に確認さ

せる．このように，利用者が格納支援機能コンポーネントと対話的に格納を行うことで，仕様書に対する汎用性とデータ抽出の精度を向上させている．

データの自動削除機能コンポーネント：データが削除された場合，そのデータを根拠としているすべてのデータをトップダウン式に検索し，削除する機能を提供するコンポーネントである．

まず自動削除機能コンポーネントは，ISEDS に格納されている個別データを表示する．これに対し利用者は，表示されているデータの中から削除したいデータを選択する．これに対し自動削除機能コンポーネントは，選択されたデータと，このデータを削除することによって整合性が失われるすべてのデータ，このデータを根拠しているすべてのデータを検索し，自動的に削除する．

たとえば，ある TOE が削除された場合は，その TOE の設計仕様である SP，SO，TSS およびそれぞれのデータ間の関連性のデータを自動的に検索し，削除する．また，SP が削除された場合は，その SP に対応する SO や TSS およびそれぞれのデータ間の関連性のデータを自動的に検索し，削除する．

5. 実現した ISEDS の連携ツールの利用事例

本研究で実現した ISEDS の連携ツールの利用事例について述べる．ここでは，ISEDS の連携ツールである設計仕様書の作成支援機能コンポーネントを利用して，設計したい情報システムの設計仕様書の雛形を出力させる．まず，ISEDS が管理している事例データを検索し，設計したい情報システムにおける概要を記述する．さらに，この概要を仕様書の作成支援機能コンポーネントに入力することで，この概要で表される情報システムの設計仕様書の雛形を出力させる．

ISO/IEC 15408 では，設計対象（TOE）の概要，SP，SO，SFR，SAR，TSS およびこれらの関連性を定義し，設計仕様書に記述しなければならないと規定されている．既存の手法で設計仕様書を作成する場合は，**図 7** 左に示されるとおり，設計したい情報システムの概要からトップダウン式に仕様を一から洗い出し，定義しなければならず，これには十分なセキュリティ機能開発の経験と，多くの時間や費用が必要となる[19)]．また，ISO/IEC 15408 文書や ISO/IEC 15408 認証取得済み設計仕様書などの公開されている文書を参考にして設計仕様書を作成する場合には，図 7 中央に示されるとおり，ISO/IEC 15408 文書（合計 300 ページ以上）から必要な箇所を探し出したり，ISO/IEC 15408 公式ウェブサイトで公開されている認証取得済

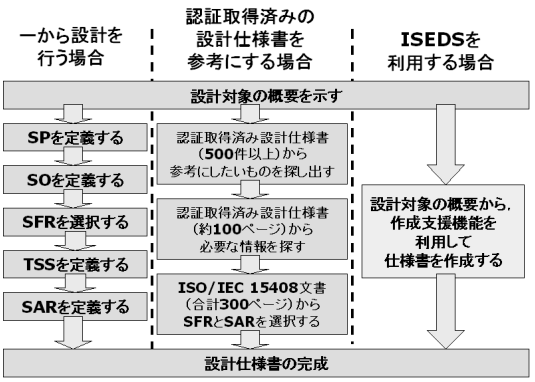

図 7 設計仕様書作成の流れ
Fig. 7 Flow of the document creation.

み設計仕様書（500 件以上）から参考にしたい設計仕様書を探し出したりし，さらに探し出された設計仕様書（約 100 ページ）から必要な情報のみを探し出して読まなければならず，これには非常に労力が必要となる．これに対して，仕様書の作成支援機能コンポーネントを利用すれば，図 7 右に示されるとおり，利用者は作成支援機能コンポーネントに概要を入力し，その結果出力された設計仕様書の雛形を修正することで設計仕様書を作成することができる．実際には，入力するキーワードの選択や出力された仕様書の雛形を修正する作業が必要ではあるが，ISEDS を用いれば仕様書の雛形の作成を非常に少ない労力で行うことができるため，全体的な労力を大きく削減することができる．

以下では利用事例をあげて，設計仕様書の作成支援機能コンポーネントを利用した設計仕様書作成の流れについて説明する．

本研究では設計対象として IP ルータを想定し，この設計対象の評価保証レベルを EAL1 と設定した．ISEDS には，すでに SFR と SAR に関するデータが基準 DB へと格納済みである．また，公開されている ISO/IEC 15408 認証取得済み設計仕様書 64 件に関するデータが事例 DB に格納済みである．これらのデータを用いて，利用事例を示す．

設計仕様書を作成する場合には，まず設計者は設計したい情報システムの概要を記述しなければならない．そこで，この IP ルータの概要を記述するために，検索機能コンポーネントを用いて情報システムの性質をよく表す概要を書くために参考となる文章を検索する．**図 8** はデータの検索機能コンポーネントのインタフェースである．まず，図 8 上部のラジオボタンから，検索するデータの範囲を指定する．ここでは，言語は英語，ISO/IEC 15408 の版を第 2 版，検索対象とし

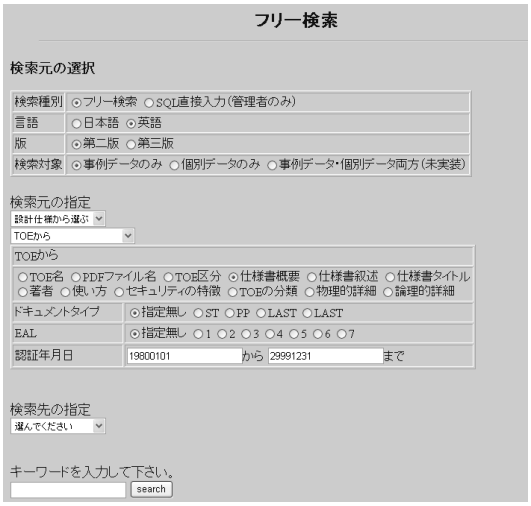

図 8 データの検索機能コンポーネントの外観
Fig. 8 Overview of the retrieval function.

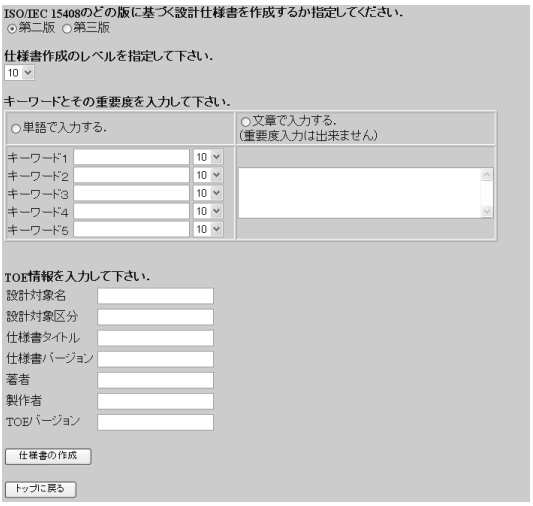

図 10 仕様書の作成支援機能コンポーネントの外観
Fig. 10 Overview of the creation function.

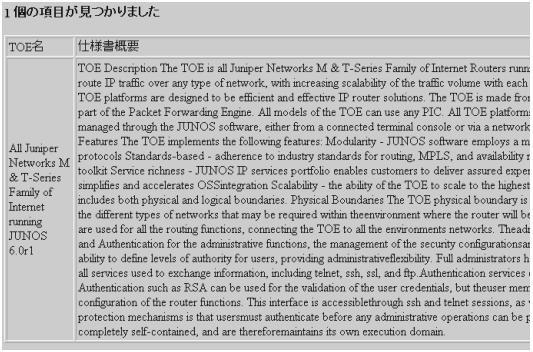

図 9 データの検索機能の出力結果画面
Fig. 9 Result of the retrieval function.

て事例データのみを選択した．また，図 8 中部のプルダウンメニューから，キーワードを検索する対象を指定する．ここでは，設計対象である TOE から，仕様書概要を選択し，ドキュメントタイプと EAL，仕様書の認証年月日は特に指定せず全範囲を検索することとした．また，図 8 下部のプルダウンメニューから，結果として表示したい対象を指定する．ここでは，設計対象である TOE から，仕様書概要を選択した．最後に，図 8 最下部のテキストボックスには，検索したいキーワードを入力する．ここでは，「IP Router」と入力した．これらの必要なデータを入力し，「送信」ボタンをクリックした．これにより，仕様書概要に「IP Router」という単語を含むすべての TOE の仕様書概要を表示することができる．この検索結果が**図 9** である．この検索の結果，Packet Forwarding Engine と Routing Engine という 2 つの機能コンポーネントを備えた IP ルータの概要を検索することができた．この検索された IP ルータの概要をもとに，設計対象の概要を記述した．

さらに，この設計対象の概要として，「IP Router」「Packet Forwarding Engine」「Routing Engine」という 3 つの単語から，作成支援機能コンポーネントを利用して仕様書を作成する．**図 10** は仕様書の作成支援機能コンポーネントのインタフェースである．まず，図 10 上部のラジオボタンから，仕様書の雛形を作成するための対象とするデータの範囲を指定する．また，設計したい情報システムと関係性を持つデータに対して，関係性の高低に応じてどこまで厳密に仕様書に使用すべきかというデータ使用の厳密さの度合いを指定する．ここでは，ISO/IEC 15408 第 2 版に基づくデータを対象として指定し，また，データ使用の厳密さの度合いを 40 と入力した．また，図 10 中部のキーワード入力欄には，設計対象の概要となる単語群とその重要度を入力する．単語ごとの重要度は，10 段階から設定することができ，設計したいシステムを的確に表す単語は重要度を高く設定することができる．ここでは，「IP Router」「Packet Forwarding Engine」「Routing Engine」という 3 つの単語を入力し，それぞれの単語の重要度をそれぞれ IP Router が 9，Packet Fowarding Engine が 4，Routing Engine が 4 として，キーワード入力欄の右のプルダウンメニューから選択した．また，図 10 下部のテキストボックスには，設計仕様書名や EAL，作成年月日，著者，製作者など，設計対象独自の設定情報を入力する．ここでは，設計対象名を「Test IP Router 1.0」，EAL

が「1」，著者が「Daisuke Horie」，製作者は「AISE Lab.」と入力した．これらの必要なデータを入力し，「送信」ボタンをクリックした．

この結果，設計仕様書の雛形が出力された．もし利用者が，この雛形には想定されるべき一部の脅威が想定されておらず，それらの脅威に対抗するためのセキュリティ対策方針やセキュリティ機能が備えられていないと判断した場合には，利用者自身が雛形の一部を修正したり，新たに単語や重要度，データ使用の厳密さの度合いを入力しなおしたりして，再度雛形の作成を行う．この工程を繰り返し，仕様書が高いセキュリティを満たすものであると判断できるまで，仕様書の作成と修正を繰り返す．今回は，新たにデータ使用の厳密さの度合いを 80 と設定し直し，再度雛形の作成を行った．その結果出力された設計仕様書の雛形をウェブ上に公開している[12)]．

このようにして，今回実現した ISEDS とその連携ツール群を用いて，セキュリティ機能の設計仕様書の作成を支援することができる．

6. 考　　察

認証システムの仕様を管理するリポジトリや MAGERIT に基づくセキュリティ要求を管理するリポジトリは，セキュリティ機能の要求定義や設計，実装などの開発の支援に特化している．これに対し ISEDS では，仕様書の迅速かつ適切な作成を支援する連携ツールによって，セキュリティ機能の設計から保守までを一貫して支援することができる．

仕様書の作成支援機能コンポーネントを利用すれば，利用者は作成支援機能コンポーネントに概要を入力し，その結果出力された設計仕様書の雛形を修正することで設計仕様書を作成することができる．

仕様書の作成支援機能コンポーネントを用いた場合の仕様書作成の労力に関して，作成支援機能を利用した場合においても，キーワードの選択や仕様書の修正に多くの労力が必要ではあるが，ISEDS の連携ツールを用いれば仕様書の雛形の作成が非常に少ない労力で行うことができる．これにより，従来の仕様書を一から作成する場合に比べ，仕様書の雛形を作成する段階までの労力が大幅に削減される．これにより，利用者が行う作業としてはキーワードの選択と仕様書の雛形を叩き台として雛形を修正する作業のみとなるため，全体的な労力は大きく削減される．例として，6 章で述べた利用事例においては，キーワード選択と仕様書の判断や修正の工程をほぼ省いたものの，概要の検索とキーワード入力に費やした 10 分間程度の時間で，2 件の ISO/IEC 15408 文書と 3 件の ISO/IEC 15408 認証取得済み設計仕様書から必要なデータを抜き出し，設計仕様書の雛形を作成することができた．

仕様書の作成支援機能コンポーネントを用いて作成した仕様書の妥当性に関して，ISO/IEC 15408 認証取得済みの設計仕様書をもとに作成された仕様書である．よって，その設計仕様は，少なくとも ISO/IEC 15408 が保証するだけのセキュリティを備えているといえる．しかし，今回実現した仕様書の作成支援機能コンポーネントは，複数の既存の仕様書から設計仕様を抜き出し，新しい設計仕様書を作成する．この際，余分な設計仕様が使用されたり，選択された複数の既存の仕様書間の設計仕様に矛盾が生じたりしている可能性が存在する．この場合は，キーワードが利用者の意図をよく反映しているかどうかに関係なく，出力された設計仕様書の雛形に対して，ISO/IEC 15408 の保証はあるということはできない．よって，余分な設計仕様や矛盾する設計仕様は，仕様書の修正の工程において取り除く必要がある．また，今後の課題として，設計仕様書の作成支援機能コンポーネントにおいて，採用する仕様書を単一の仕様書のみとするか，複数の仕様書を使用する場合にはその仕様書間の矛盾を検知する機能を追加することを検討している．

正確性に関して，仕様書の雛形の作成の際に利用者の意図をよく反映した設計仕様が選ばれているかどうかは，利用者が入力するキーワードに依存する．このため，利用者は意図をよく反映したキーワードを慎重に選ぶ必要があり，また，出力された雛形を適宜修正する必要がある．しかし，ISEDS の検索機能コンポーネントによって過去の事例から，利用者の意図をよく反映したキーワードの候補を検索することができる．また，仕様書の作成支援機能コンポーネントによって短時間で仕様書の雛形の作成を行うことにより，修正のために何度も雛形を作り直すこともできる．

作成した設計仕様書への具体的な定量的，定性的評価については，我々は現在セキュリティ機能の設計や開発，テストを行うための十分な環境を持っておらず，現在は格納されているデータ数も少ないため，今回は方法の提案のみを行い，実際の評価は今後の課題とする．具体的な方法としては，図 7 左および中央に示される方法で実際に仕様書を作成し，仕様書の作成支援機能コンポーネントを用いた仕様書の作成との時間や費用の差や，設計仕様書の差分をとることで，時間，費用，妥当性，正確性の評価を行う．また，ISEDS にデータが格納されていない ISO/IEC 15408 認証取得済みの情報システムを仮想し，作成支援機能を用いて

この情報システムの設計仕様書を作成することで，この情報システムの実際の設計仕様書と，作成された仕様書を比較することで，評価を行う．

7. おわりに

本論文では，セキュリティ機能の設計から保守までを一貫して支援する汎用的なデータベースシステムとして，ISEDS とその連携ツール群について，利用形態と利用法，応用事例，要求，機能を定義した．また，ISEDS が扱うセキュリティ基準の 1 つとして ISO/IEC 15408 を使用し，ISO/IEC 15408 に関するデータを管理するための ISEDS とその連携ツール群の機能の実現について述べた．さらに，ISEDS の連携ツールの利用事例として，今回実現した仕様書の作成支援機能コンポーネントを用いて，具体的な情報システムとして IP ルータにおけるセキュリティ機能の設計仕様書の作成について述べた．今回実現した ISEDS とその連携ツール群のプロトタイプはウェブ上に公開している[11]．この ISEDS とその連携ツール群はセキュリティ機能の仕様書の作成を支援することができ，セキュリティ機能の設計から保守までを一貫して支援する国内外で初のデータベースシステムである．

今後は，ISO/IEC 17799 や ISO/IEC TR 13335 などの ISO/IEC 15408 以外のセキュリティ基準およびセキュリティ機能の開発や保守の公開事例に関するデータを管理するための機能を実現する．例として，ISO/IEC 17799 では，IT セキュリティ管理実施基準というセキュリティ対策方針とセキュリティ管理項目を規定しており[13]，2.4 節で述べた利用法 2 に基づき，この管理実施基準を検索することができる機能を設ける．また，ISO/IEC TR 13335 では，IT セキュリティマネジメントの概念およびモデル[4] を示しており，2.4 節で述べた利用法 1 に基づきこれらの概念の意味を検索することができる機能を設ける．

また，より高いセキュリティを満たす情報システムの開発や保守を支援するために，ISEDS の連携ツールを充実させる．例として，今回開発したデータの検索機能コンポーネントでは，「『なりすまし』という脅威を想定している情報システムがなりすまし以外に想定している脅威を検索したい」などの複雑な検索を一度の操作で実現することはできない．そこで，このような複雑な検索について，利用者の要求を洗い出し，必要に応じて実現する．また，セキュリティ機能の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形式的に検証する技法[7),18)] を取り入れ，仕様の形式化や，SFR の具体化を支援する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設計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．

また，仕様書の作成支援機能コンポーネントにおいて，ISO/IEC 15408 が規定している PP と呼ばれる設計仕様書の雛形を UML によりモデル化し，これを用いて設計仕様書を記述する方法がすでに提案されている[16]．この技法では，モデル化された PP を用いてセキュリティ機能の設計を行うことにより，簡単かつ適切に設計を行うことができる．このモデル化された PP のデータを ISEDS により管理し，この技法を利用することで，設計仕様書の作成を支援する機能を検討中である．

また，ISEDS を 1 つの機能コンポーネントとし，ソフトウェアの総合開発や，動的なセキュリティテストにおけるセキュリティ機能改善への応用を検討している．

参考文献

1) Castano, S., Martella, G. and Samarati, P.: A New Approach to Security System Development, *Proc. 1994 workshop on New security paradigms*, pp.82–88, ACM (1994).
2) Common Criteria Project: common criteria portal. http://www.commoncriteriaportal.org/
3) Horie, D., Morimoto, S. and Cheng, J.: A Web User Interface of the Security Requirement Management Database Based on ISO/IEC 15408, *Computational Science — ICCS 2006: 6th International Conference, Reading, UK, May 28-31, 2006, Proc., Part IV*, Lecture Notes in Computer Science, Vol.3994, pp.797–804, Springer-Verlag (2006).
4) ISO/IEC: ISO/IEC TR 13335. http://www.bsi-global.com/Security/ITSec/BSISOIEC13335-1:2004.xalter
5) Jiao, J. and Tseng, M.: A Requirement Management Database System for Product Definition, *Journal of Integrated Manufacturing Systems*, Vol.10, No.3, pp.146–154 (1999).
6) Morimoto, S., Horie, D. and Cheng, J.: A Security Requirement Management Database Based on ISO/IEC 15408, *Computational Science and Its Applications — ICCSA 2006: International Conference*, Lecture Notes in Computer Science, Vol.3982, pp.1–10, Springer-Verlag (2006).
7) Morimoto, S., Shigematsu, S., Goto, Y. and Cheng, J.: Formal Verification of Security Spec-

ifications with Common Criteria, *Proc. 22nd Annual ACM Symposium on Applied Computing*, pp.1506–1512, ACM (2007).
8) Software Engineering Institute: Software Engineering Information Repository. https://seir.sei.cmu.edu/seir/
9) Stytz, M. and Banks, S.: Dynamic Software Security Testing, *IEEE Security & Privacy*, Vol.4, No.3, pp.77–79 (2006).
10) Toval, A., Nicolas, J., Moros, B. and Garcia, F.: Requirements Reuse for Improving Information Systems Security: A Practitioner's Approach, *Requirements Engineering*, Vol.6, No.4, pp.205–219 (2002).
11) 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.saitama-u.ac.jp/iseds/
12) 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：ISEDS を用いて作成した設計仕様書雛形事例 1. http://www.aise.ics.saitama-u.ac.jp/iseds/japanese/generated_specifications.html
13) 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 (2000).
14) 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
15) 内閣官房情報セキュリティセンター：政府機関の情報セキュリティ対策のための統一基準. http://www.nisc.go.jp/active/general/kijun01.html
16) 森本祥一，程　京徳：UML によるプロテクションプロファイルのモデル化とその形式的検証，電子情報通信学会論文誌「情報・システム」，Vol.J89-D, No.4, pp.726–742 (2006).
17) 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).
18) 森本祥一，重松真二郎，後藤祐一，程　京徳：ISO/IEC 15408 に基づく定理証明とモデル検査による情報セキュリティ仕様の検証技法，日本ソフトウェア科学会「コンピュータソフトウェア」，Vol.23, No.3, pp.117–133 (2006).
19) 山里拓己，吉府研治，伊東真理：ISO/IEC 15408 セキュリティ評価の意義と適用，NEC 技報，Vol.58, No.2, pp.33–37 (2005).

(平成 18 年 11 月 30 日受付)
(平成 19 年 5 月 9 日採録)

堀江　大輔（学生会員）

平成 18 年埼玉大学工学部情報システム工学科卒業．平成 19 年同大学院理工学研究科博士前期課程数理電子情報系専攻情報システム工学コース修了．修士（工学）．現在，同博士後期課程在学中．ソフトウェア工学および情報セキュリティ工学の研究に従事．日本データベース学会学生会員．

森本　祥一（正会員）

平成 11 年埼玉大学工学部情報システム工学科卒業．平成 13 年同大学院理工学研究科博士前期課程情報システム工学専攻修了．平成 13 年日本電気航空宇宙システム（株）入社．平成 15 年同社退職．平成 18 年埼玉大学大学院博士後期課程情報数理科学専攻修了．博士（工学）．平成 18 年産業技術大学院大学産業技術研究科研究員．平成 19 年同助教．ソフトウェア工学および情報セキュリティ工学の研究に従事．電子情報通信学会，日本ソフトウェア科学会，日本データベース学会，ACM 各会員．

後藤　祐一（正会員）

平成 13 年埼玉大学工学部情報システム工学科卒業．平成 15 年同大学院理工学研究科博士前期課程情報システム工学専攻修了．平成 17 年同博士後期課程情報数理科学専攻修了．博士（工学）．平成 17 年埼玉大学工学部助手．平成 19 年同大学院理工学研究科助教．知識工学の研究に従事．人工知能学会，ACM，IEEE-CS 各会員．

程　　京徳（正会員）

昭和 57 年中国清華大学計算機科学技術系卒業．昭和 61 年九州大学大学院工学研究科修士課程情報工学専攻修了．平成元年同博士後期課程情報工学専攻修了．工学博士．平成元年九州大学工学部助手．平成 3 年同助教授．平成 8 年九州大学大学院システム情報科学研究科教授．平成 11 年埼玉大学大学院理工学研究科教授．ソフトウェア工学，知識工学および情報セキュリティ工学の研究に従事．ACM 上級会員（Senior Member），IEEE-CS, IEEE-SMC，IEEE 各会員．