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

An Information Security Requirement Management Database Based on the International Standard ISO/IEC 15408

森本 祥一♥　堀江 大輔♦
程 京徳♠

Shoichi MORIMOTO　Daisuke HORIE
Jingde CHENG

情報システムの大規模化や多様化に伴い，情報システムに対するセキュリティ要求はますます複雑化している．今後，情報セキュリティ工学へのデータベース技術の応用は不可欠となることが予想される．ソフトウェア工学，特に要求工学の分野では，ソフトウェア要求を管理するデータベースなどは提案されているが，それらはセキュリティ要求に特化したものではない．本稿では，情報システムに対するセキュリティ要求を管理するデータベースを提案する．実現方式としては，情報技術セキュリティ評価の国際標準である ISO/IEC 15408 により定義されている情報システムが備えるべきセキュリティ機能の要件と，これらが用いられている認証済み公開仕様書の構造に基づいて設計を行った．このデータベースにより，あらゆる情報システムにおけるセキュリティ要求を管理し，セキュリティを考慮したシステム開発を支援することができる．

With the scale-spreading and diversification of information systems, security requirements for the systems are being complicated more and more. It is desirable to apply database technologies to information security engineering. On the other hand, in software engineering, especially in requirement engineering, some software requirement management databases have been proposed. However, the databases cannot be directly applied to analysis and management of security requirements. This paper proposes an information security requirement management database based on the international standard ISO/IEC 15408, because ISO/IEC 15408 defines the security functional requirements that should be applied to validate an information system. The database can manage security requirements of information systems and can aid development of information systems that need high security.

♥ 学生会員　埼玉大学大学院理工学研究科博士後期課程
morimo@aise.ics.saitama-u.ac.jp
♦ 学生会員　埼玉大学工学部情報システム工学科
horie@aise.ics.saitama-u.ac.jp
♠ 正会員　埼玉大学大学院理工学研究科
cheng@aise.ics.saitama-u.ac.jp

1. はじめに

今日，情報システムは，我々の生活のあらゆる局面に利用されるようになり，またその規模も拡大の傾向にある．一方で，コンピュータウィルスやコンピュータ犯罪による被害も，年々増加している．このような現状を受け，情報システムにおけるセキュリティ要求も最早人手により管理しきれないほどに増加し，また複雑化してきている．

ソフトウェア工学，特に要求工学の分野では，増大するソフトウェア需要に備え，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[1]や，リポジトリ[2]といったソフトウェア開発の各工程において得られる知見や経験の再利用・有効活用を目的としたデータベース等が既に提案されている．これらと同様，開発者の負担を軽減し高いセキュリティを備えたシステムを開発するために，大規模化・多様化している情報システム開発において発生するセキュリティ要求を，データベースにより情報セキュリティ工学の視点から管理することが望ましい．

しかしながら，情報システム開発においてセキュリティを考慮するにあたり，セキュリティ要求をどのように分析し定義するか，という一般的・工学的な手法は確立していない．そこで我々は，国際標準である情報技術セキュリティ評価基準ISO/IEC 15408 [3]に着目した．ISO/IEC 15408では，評価対象のシステム（TOE: Target of Evaluation）でどのようなセキュリティ要求があり，それらの要求をどのように実装し，保証できているかを記述した仕様書に基づいて，評価する．つまりこれらの仕様書作成の過程では，情報システムにおけるセキュリティ要求を分析し，定義している．本稿で提案するデータベースは，これらの分析過程における情報を格納しておき，必要に応じて参照できるようにすることで，高いセキュリティを達成した情報システム開発を支援する．また，新たなセキュリティ要求の定義・更新も可能にする．

2. ISO/IEC15408 におけるセキュリティ要求

本稿で提案するデータベースの基礎となる ISO/IEC 15408 におけるセキュリティ要求分析・定義について説明する．

2.1 セキュリティ機能要件

ISO/IEC 15408 は，「Part1: 概説と一般モデル」，「Part2: セキュリティ機能要件」，「Part3: セキュリティ保証要件」から構成される．Part1 では，用語の定義や評価の流れ，評価に必要な仕様書の構成等が解説されている．Part2 では，情報システムにおいてセキュリティ対策として実装すべき機能に関する要件（SFR: Security Functional Requirements）が 11 分野 251 項目に渡り規定されている（表 1）． つまり，これらは情報システムにおけるセキュリティ要求である．Part3 では，SFR がシステムに正しく実装されていることを保証するための 10 分野の要件が規定されている．

表 1　セキュリティ機能要件クラス
Table 1　The Security Functional Requirement Classes.

SFR クラス名	識別子	SFR クラス名	識別子
セキュリティ監査	FAU	プライバシー	FPR
通信	FCO	TSF の保護	FPT
暗号サポート	FCS	資源利用	FRU
利用者データ保護	FDP	TOE アクセス	FTA
認証と識別	FIA	セキュリティ管理	FMT
高信頼パス/チャネル	FTP		

SFR は，一番上からクラス・ファミリ・コンポーネント・エレメントという階層構造を成し，図 1 に示す各要素から構成される. エレメントは, 不可分のセキュリティ要件である. コンポーネントは，選択可能な最小のエレメントのセットであり，コンポーネント同士の依存関係も存在する．ファミリは，セキュリティ対策方針を共有するが，重点または厳密さが異なるコンポーネントのグループ，クラスは，共通の対象を共有するファミリのグループである．これらのうち最下層のエレメントにおいて，情報システムが備えるべきセキュリティ機能についての 251 の要件が直接的に述べられている.

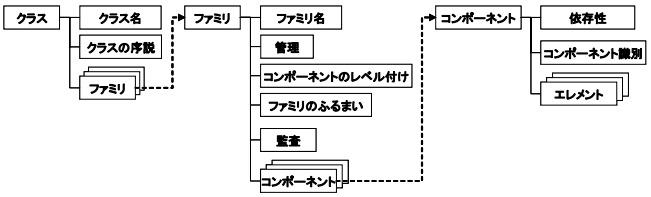

図 1　セキュリティ機能要件の階層構造
Fig.1 The Hierarchical Structure of the Security Functional Requirements.

実際のSFRは以下のようになっている．（一部省略した.）

> **FMT_SMR**　セキュリティ管理役割
> **FMT_SMR.1** セキュリティ役割
> セキュリティ役割は，TSF が認識するセキュリティに関する役割を特定する.
> **下位階層**　なし
> **FMT_SMR.1.2**
> TSF は，利用者を役割に関連づけなければならない.
> **依存性**　FIA_UID.1 識別のタイミング

原文中のTSFとは，システムのセキュリティ機能（TOE Security Functions）である．クラスFMTのFMT_SMRというファミリは「セキュリティ管理役割」というファミリ名であり，そこに含まれるコンポーネントFMT_SMR.1はコンポーネントFIA_UID.1に依存性があることが明記されている．そしてエレメントFMT_SMR.1.2において実際の要件が自然言語で記述されている.

2.2 ISO/IEC 15408 に準拠した公開仕様書の構成

ISO/IEC 15408 の評価を受けるためには，TOE ごとに Security Target と呼ばれる仕様書を作成しなければならない．また，製品・システム単位ではなく，情報システムにおける分野ごと（例：OS，DBMS，IC カード等）の仕様書である Protection Profile の評価・認証も行われている.

これら 2 種類の仕様書では，開発者はまず各システム・分野においてどのような脅威が想定されるのかを以下のように記述・列挙しなければならない.

> **T1** 外部ネットワークから内部ネットワークへの不正アクセス
> 外部ネットワークの利用者は，内部ネットワークに侵入し，内部ネットワークの保護資産の改ざん，破壊，又は漏洩を図る恐れがある.

次に，この列挙したそれぞれの脅威に対抗するためのセキュリティ対策方針を以下のように述べなければならない.

> **O.AC** 外部ネットワーク利用者の制限
> TOE は，TOE 又は TOE を経由して内部ネットワークにアクセスしようとする外部ネットワークの利用者を制限する.

1 つの脅威に対して複数の対策方針で対抗することもあれば，逆に 1 つで複数の脅威に対抗できる対策方針もあるため，脅威と対策方針の関係は多対多となっている．また，列挙したセキュリティ対策方針が，251 の SFR のうちどれに該当するのかを明記しなければならない．1 つの対策方針が複数の SFR に該当する場合もあれば, 複数の対策方針で 1 つの SFR に対応している場合もあるため，これらの関係も多対多である．更に，セキュリティ対策方針によって必要性が明らかになった SFR を, 実際にどのような機能を用いて具体的に実装するのかを TSF として以下のように述べなければならない.

> **SFP_IPPF**　IPパケットフィルタリング機能
> IPパケットフィルタリング機能は以下の機能を提供する.
> **IPPF.1**
> IPパケットフィルタリング機能は，…
> **IPPF.2**
> 上記のどの条件にも合致しなかった場合，…

TSF はまず大きな機能単位の分類（上記の SFP_IPPF）があり，その下に個々の小さな機能（IPPF.1 と IPPF.2）が具体的に記述され, それぞれの下位機能がどの SFR を実装しているかが明記される. つまり 1 つの上位 TSF に対して複数の下位 TSF が存在し，1 つの下位 TSF は複数の SFR を実装していることもあれば，複数の下位 TSF で 1 つの SFR を実装している場合もある.

ISO/IEC 15408 に準拠した公開仕様書では，以上のような過程で TOE のセキュリティ要求を分析し，定義している.

3. 設計と実現

情報システムのセキュリティ要求を管理するデータベースを実現するにあたって，セキュリティ要求をどのように管理するかを定義する必要がある．そもそもセキュリティ要求とは，「あるシステムのある局面において，どのようなセキュリティ対策を施す必要があるか」であるが，前述のように，一般的なセキュリティ要求分析のための手法が存在しないため, 開発者やシステムによって様々な定義の仕方があり得る. 逆に，これらを統一して定義さえしておけば，恣意的な開発を防ぐことができる．本研究では，セキュリティ要求の分析過程として, 前述の ISO/IEC 15408 に準拠した公開仕様書作成の過程に従うこととした．加えて，ISO/IEC 15408 Part2 ではどの SFR をどのようなシステムに用いるべきか明確に定義されておらず, Security Target や Protection Profile 作成において, 必要な SFR の選択は開発者の判断に委ねられる. しかしながら，選択のための明確な指標がないため，選んだ SFR に過不足があるのか開発者は判断することができない. 以上のことから, 本稿で提案するデータベースでは, ISO/IEC 15408 に準拠した公開仕様書作成の過程で述べられる想定される脅威・セキュリティ対策方針・TSF と，全ての SFR の情報，そしてこれらの各情報間の関連性を関係データベースに格納することとした.

3.1 スキーマ設計

2章で明らかにしたデータベースの構成要素（エンティティ）を以下に列挙する.

a. TOE（Security Target，またはProtection Profile），
b. 脅威，**c.** セキュリティ対策方針，**d.** TSF（上位レベル），
e. TSF（下位レベル），**f.** クラス，**g.** ファミリ，
h. コンポーネント，**i.** エレメント

これらのエンティティ間の関連のカーディナリティを以下の表 2 に示す.

表 2　エンティティ間の関連のカーディナリティ
Table 2　The Cardinality of the Entity Relationships.

	a	b	c	d	e	f	g	h	i
a	-	1:n	1:n	1:n	-	-	-	-	-
b	n:1	-	m:n	-	-	-	-	-	-
c	n:1	m:n	-	-	-	-	-	-	m:n
d	n:1	-	-	-	1:n	-	-	-	-
e	-	-	-	n:1	-	-	-	-	m:n
f	-	-	-	-	-	-	1:n	-	-
g	-	-	-	-	-	n:1	-	1:n	-
h	-	-	-	-	-	-	n:1	m:n	1:n
i	-	-	m:n	-	m:n	-	-	n:1	-

この表2を元に，以下の図2に示すモデルを設計した．図2は，Microsoft Visio Professionalにより作成した，IDEF1X・リレーショナル表記法によるデータベースモデル図である[4]．エンティティ間の関連を示す矢印は，矢の向いている先が多を示す．また，PKは主キーを，FKは外部キーを示す．

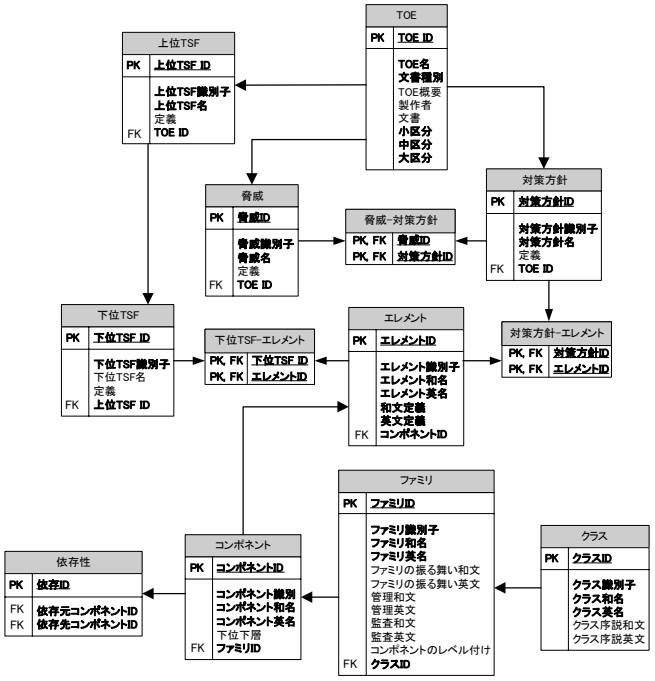

図 2 情報セキュリティ要求管理 DB のデータベースモデル図
Fig.2 The Database Model Diagram of the Security Requirement Management Database.

図2について簡単に説明する. 以下の文中における斜字体は, 図2中のスキーマの属性を示す．TOEスキーマは要素として，一意の番号（*TOE_ID*），TOEの名前（*TOE名*），Security TargetかProtection Profileを区別するための*文書種別*, TOEがどのようなシステムであるかを説明する文（*TOE概要*），仕様書の*製作者*, 仕様書自体のバイナリデータを格納する*文書*, そのシステムはどのような分野に属するかを示す*大区分*, *中区分*, *小区分*を持つ．*大区分*は現在は“IT製品”という区分のみで，*中区分*は“ソフトウェア”か“ハードウェア”か，*小区分*は“デジタル複合機”, “DBMS”, “ICカード”といったTOEごとの具体的な性質を示す. TOEスキーマは, 複数の上位TSF・脅威・対策方針スキーマと関連を持つ．脅威スキーマには，一意の番号（*脅威ID*），脅威名の英語の頭文字などから便宜上付けられた*脅威識別子*（例:前述のT1），脅威の名称（*脅威名*），前述の脅威T1における『外部ネットワークの利用者は，～恐れがある．』のように脅威の具体的内容を記述した原文（*定義*），どのTOE仕様書で述べられた脅威なのかを示すための外部キー*TOE_ID*を持つ．対策方針スキーマと上位TSFスキーマは，脅威スキーマと同様に*対策方針ID*, *対策方針識別子*・*対策方針名*・*定義*・*TOE_ID*と，*上位TSF_ID*・*上位TSF識別子*・*上位TSF名*・*定義*・*TOE_ID*を持つ．下位TSFスキーマは，*下位TSF_ID*・*下位TSF識別子*・*下位TSF名*・*定義*と, どの上位TSFに属するのかを示す外部キー*上位TSF_ID*を持つ．脅威と対策方針，対策方針とエレメント，下位TSFとエレメントの多対多の対応関係は，それぞれスキーマを作成し実現した．クラス，ファミリ，コンポーネント，エレメントの各スキーマは， ISO/IEC 15408 Part2で定義された図1の各要素に加えて, それぞれどの上位階層のスキーマに属すかを示す外部キーを持つ．コンポーネント同士の依存性は，依存元と依存先の*コンポーネントID*の対応関係を格納するスキーマを別に作成することで実現した.

3.2 実現

3.1 節で設計したスキーマを実際に PostgreSQL8.1 で作成した．そして ISO/IEC 15408 Part2 に記述された全ての SFR の情報と，認証済み公開仕様書の情報を格納する．日本で ISO/IEC 15408 の認証を行っている IPA では，2005 年 11 月末時点で認証済み製品 35，確認リスト 20 の仕様書が公開されている[5]．国際的には，Security Target は 657，Protection Profile は 125 公開されている[6]．現時点ではこれらの情報を利用できる．これにより，既に ISO/IEC 15408 認証済みの公開仕様書において，どのような脅威・対策・機能があり，どの SFR を使用しているか検索でき，これらの情報を指標にして，ISO/IEC 15408 に準拠したシステム開発の負担を軽減することができる.

4. 機能と評価

本稿で提案したデータベースでは, 情報システムにおけるセキュリティ要求を，ISO/IEC 15408に倣って情報システムの分野や性質・想定される脅威・脅威に対する対策方針・対策方針を実装する機能・SFRと，これらの関連性として定義することを前提とする. 本データベースを用いることにより，利用者は情報システム開発におけるセキュリティ要求という抽象的な概念をやみくもに分析し定義することなく，統一的に系統立てて分析し管理できる．また，格納した情報を以下のように利用し，システム開発の負担を軽減できる.

TOEスキーマを起点として「どのようなシステムでどのような脅威が想定され，そのためにどのような対策方針が必要で, どのようなTSFが必要でどのようなSFRを使っているか」が検索できる．例えば『データベース分野の製品ではどのような脅威が想定されており，どのような対策・セキュリティ機能があり，どのSFRが必要か』という検索ができる.

```
例 1 SELECT T.脅威名, T.定義 FROM TOE, 脅威 T
WHERE TOE.小区分 LIKE '%データベース%' AND
TOE.TOE_ID = T.TOE_ID
```

脅威スキーマを起点として「どのような脅威がどのようなシステムで起こり得，どのような対策があり，どのようなTSFが必要で，どのSFRを使っているか」が検索できる．例えば『なりすましは，どのようなシステムで起こり得，どのような対策・セキュリティ機能あり，どのSFRが必要か』等が検索できる.

例 2 SELECT O.対策方針名, O.定義 FROM 脅威 T, 対策方針 O, 脅威_対策方針 R WHERE T.定義 LIKE '%なりすまし%' AND T.脅威 ID = R.脅威 ID AND R.対策方針 ID = O.対策方針 ID

対策方針スキーマを起点として「どのような対策がどのようなシステムに必要で，どのような脅威に対抗し，どのようなTSFが必要でどのSFRを使っているか」が検索できる．例えば『IPアドレスの隠蔽は，どのようなシステムに必要で，どのような脅威に対抗し，どのような機能として実装され，どのSFRが必要か』等が検索できる．

例 3 SELECT E.エレメント和名, E.和文定義 FROM 対策方針 O, エレメント E, 対策方針_エレメント R WHERE O.定義 LIKE '%IP アドレスの隠蔽%' AND O.対策方針 ID = R.対策方針 ID AND R.エレメント ID = E.エレメント ID

TSFスキーマを起点として「どのようなTSFがどのようなシステムに必要で，どのような脅威に対抗し，どのような対策に使われ，どのSFRを実装しているか」が検索できる．例えば『IPパケットフィルタリング機能は，どのようなシステムに必要で，どのような脅威に対抗し，どのような対策に必要で，どのSFRを実装しているか』等が検索できる．

例 4 SELECT TOE.大区分, TOE.中区分 TOE.小区分 FROM 下位 TSF L, 上位 TSF H, TOE WHERE L.定義 LIKE '%IP パケットフィルタリング%' AND L.上位 TSF_ID = H.上位 TSF_ID AND H.TOE_ID = TOE.TOE_ID

上記以外にも，SFR の各スキーマを起点として，どの SFR がどのようなシステム・脅威・対策方針・TSF に使われているかを検索でき，SFR の階層構造から同じファミリの SFR を使う，依存性のある全ての SFR を調べる等，様々な検索が考えられる．また，システム開発の過程で，利用者が新たに TOE・脅威・対策方針・TSF を定義し，各スキーマにそれぞれの情報を格納し，新たな情報として利用することもできる．

加えて，我々は既にISO/IEC 15408を基準として情報システムの仕様がセキュリティ要求を満たしているかどうかを検証する技法を提案した[7,8]．この検証技法では，我々があらかじめ形式言語で記述したSFRを用いて，形式手法により数学的に厳密に情報システムの仕様を検証できる．この検証技法により，本稿で提案したデータベースを用いて開発したシステムの仕様が，要求したSFRを実際に満たしているか検証することができる．また，この検証技法の問題点は，検証者の判断で検証対象のシステムに必要な検証基準（形式化したSFR）を選択しなければならない点であったが，本稿で提案したデータベースを用いることで，この問題を解決できる．

5. おわりに

本稿では，情報システムにおけるセキュリティ要求を管理するデータベースを提案した．まず，管理する対象であるセキュリティ要求の定義として，情報技術セキュリティ評価基準 ISO/IEC 15408 における SFR と，認証済み公開仕様書の構造を採用した．次に SFR と認証済み公開仕様書においてデータベースに格納すべき対象を分析し，データベースモデル図によりスキーマ設計を行った．そして設計したデータベースによりどのような管理が実現できるかを評価した．このデータベースを用いることにより，情報システム開発におけるセキュリティ要求という抽象的な概念を一貫性して定義し，データベースに格納して管理することができる．また，既に認証済みの仕様書において述べられた想定される脅威，必要な対策方針や TSF, SFR を様々な角度から検索することができる．これらの情報を参照することで，ISO/IEC 15408 の評価を受けるかどうかに関わらず，ISO/IEC 15408 に準拠する高いセキュリティを達成した情報システム開発を支援することができる．その情報システムのセキュリティは，少なくとも国際標準に基づいているということができる．我々は，現在本稿で提案したデータベースを Web 上で公開する準備をしている[9]．また本稿で提案したデータベースの拡張として，SFR や認証済み公開仕様書の構造を XML で表現し，そのままネイティブ XML データベースへ格納し利用できる Web サービスやインタフェースの開発を検討している．

[文献]

[1] 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).

[2] Software Engineering Institute: "Software Engineering Information Repository", http://seir.sei.cmu.edu/

[3] ISO/IEC 15408 Standard: "Information Technology -- Security Techniques -- Evaluation Criteria for IT Security --" (1999).

[4] 松本聡: "アイデフワンエックス(IDEF1X)―リレーショナル・データモデルの新しい表現法", 日経 BP 社 (1996).

[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/

[6] Common Criteria Portal Org: "Public Files", http://www.commoncriteriaportal.org/public/files/

[7] 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を用いた情報セキュリティ仕様の検証技法", 第二回システム検証の科学技術シンポジウム予稿集, pp.12-23, 大阪, 2005 年 10 月.

[8] Morimoto, S., Shinjiro, S., Goto, Y., and Cheng, J.: "A Security Specification Verification Technique Based on the International Standard ISO/IEC 15408", Proceedings of the 21st Annual ACM Symposium on Applied Computing (SAC06), Dijon, France, April (2006).

[9] 埼玉大学 工学部 情報システム工学科 先端情報システム工学研究室: "ISO/IEC 15408 関連研究", http://queen.aise.ics.saitama-u.ac.jp/

森本 祥一 Shoichi MORIMOTO

埼玉大学大学院理工学研究科博士後期課程在学中. 2000 埼玉大学大学院理工学研究科博士前期課程修了．情報セキュリティ工学，ソフトウェア工学の研究に従事．日本データベース学会，情報処理学会，電子情報通信学会，日本ソフトウェア科学会，ACM 各学生会員.

堀江 大輔 Daisuke HORIE

埼玉大学工学部情報システム工学科在学中．情報セキュリティ要求管理データベースの研究・開発に従事．日本データベース学会学生会員.

程 京徳 Jingde CHENG

埼玉大学大学院理工学研究科情報数理科学専攻教授. 1989 九州大学大学院博士課程修了，工学博士．ソフトウェア工学，知識工学，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, 情報処理学会, 日本ソフトウェア科学会, ACM, IEEE-CS，IEEE-SMC，IEEE，AAAI 各正会員.