国際標準に基づく汎用的情報セキュリティ工学環境の構築

代表研究者	程　京徳	埼玉大学大学院理工学研究科教授
共同研究者	後藤祐一	埼玉大学大学院理工学研究科助教
共同研究者	森本祥一	産業技術大学院大学助教
共同研究者	堀江大輔	埼玉大学大学院理工学研究科大学院生

1 研究の背景と目的

インターネットの普及と情報化社会の高度化に伴って、情報システムに対する安全性要求がますます高まっており、今日、ほとんどの情報システムの設計と開発においては、情報セキュリティに対する要求を考慮しそれらを保証する機能を実現しなければならない状況になってきた。また、悪意のある攻撃者らの知識や技能も時間と共に増えるので、高安全性が要求される情報システムにおいては、次々と新たな攻撃方法を編み出す攻撃者の存在を常に考慮しなければならない。情報システムの設計者、開発者、運用者、保守者は、責務として、システムに情報セキュリティ機能を実装するばかりではなく、システムが攻撃を受けたとき、情報セキュリティ機能が適切かつ迅速に動作することを常に保証しなければならなく、システムが攻撃を受けて正常に稼働できないとき、迅速に回復することをも保証しなければならない。従って、高安全性情報システムが一定以上の安全性を常に保つために、その設計や開発だけなく運用や保守をも一貫してかつ継続的に行わなければならない。しかし、現在、これらの作業を一貫してかつ継続的に行うための系統的な方法論がまだ確立されていない。

一方、情報セキュリティ工学は多くの面でソフトウェア工学と本質的に違っているので、従来のソフトウェア工学環境が提供できる支援は高安全性が要求される情報システムの設計、開発、運用、保守にとって不十分である。しかし、現在、情報セキュリティ機能の設計・実現から運用・保守までを一貫して国際標準に基づいて継続的、系統的、統合的に支援できる情報セキュリティ工学環境は全くない。

本研究では、高安全性が要求される情報システムにおける情報セキュリティ機能の設計・実現から運用・保守までを一貫かつ継続して支援するために、ISO/IEC 国際標準規格に基づいて、情報セキュリティ工学データベース、情報セキュリティ機能保証技法および支援ツール群を開発し、それらを統合する汎用的情報セキュリティ工学環境 ISEE(Information Security Engineering Environment)を開発している。また、将来、ISEE と従来のソフトウェア工学環境とを統合し、高信頼性、高安全性が要求される情報システムの設計、開発、運用、保守を支援できる工学環境を構築することを目指している。

2 国際標準に基づく情報セキュリティ工学環境の必要性

システムの信頼性は要求される機能を確実に実現する保証（の程度）であることに対して、システムの安全性は障害を確実に防ぐ保証（の程度）である［1]。情報システムの安全性に関しては、攻撃者が能動的に知識を獲得し新しい技術や攻撃法を編み出せるため、ある時点では充分な安全性を備えていたシステムであっても、一定の時間がたつと充分な安全性を保っているとはいえない。よって、高安全性が要求されるシステムに対して、その運用・保守において、設計・開発時に想定されなかった脆弱性や攻撃法がないかどうかを常に考慮しなければならない。従って、高安全性情報システムにおいては、一度設計し開発され、運用・保守方法が適切に決定されたとしても、充分ではなく、常に、運用・保守方法を更新したり、セキュリティ機能を改善し追加したりすること、即ち、絶えず保守を継続することが必要である。

また、システム全体の信頼性は一般的にシステムの各構成部分の信頼性の全体、すなわち総和によって決められることに対して、システム全体の安全性は常にシステムの最も脆弱な構成部分あるいは構成部分間の最も脆弱な連結の安全性によって決められる［88, 89]。攻撃者はいつもシステムのうち最も脆弱な部分を突いて攻撃を行う。一旦攻撃が成功すると、そこからデータが流出されたり、改竄されたり、他のセキュリティ機能が無効化されたり、システム全体の安全性が破壊されてしまう。よって、最も脆弱な部分の安全性が、システムが備えるべき安全性を下回っていれば、システム全体の安全性は不十分となってしまう。また、システムの設計、開発、運用、保守のどの段階においてもただ１つの作業が適切に行われなく脆弱点を生じる

ことになったとしても、システム全体の安全性も不十分となってしまう。従って、高安全性情報システムにおいては、全ての構成部分の設計、開発、運用、保守における全ての作業を、一定以上の安全性を保証できる標準規格に基づき一貫した手法て行うことにより、全ての構成部分および構成部分間連結の安全性を一定以上の強固さに維持することが必要である（Fig. 1を参照されたい）。

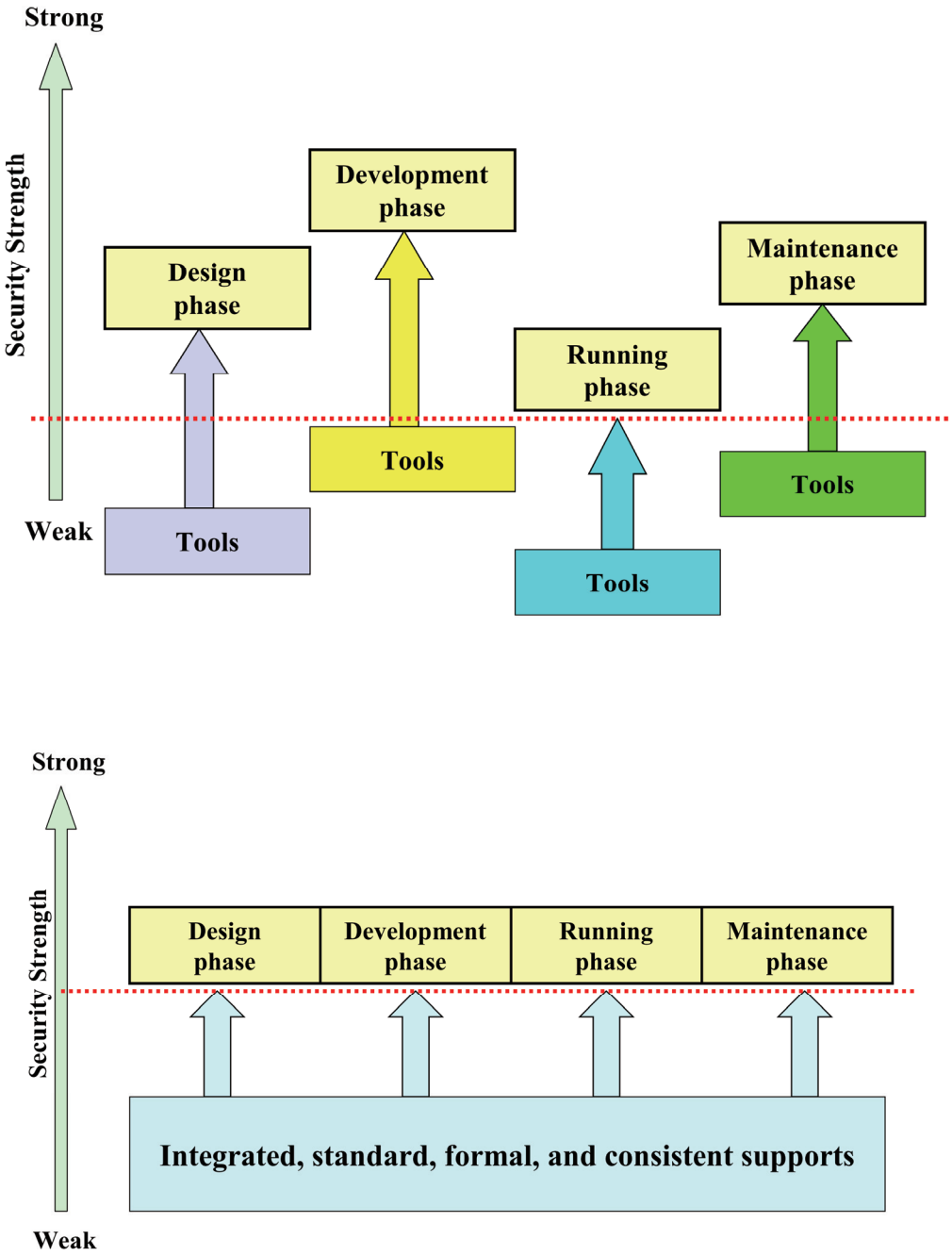

Fig. 1　Ensuring the whole security of the target system anytime consistently and continuously by integrated, standard, formal, and consistent supports

一方、ソフトウェア工学の分野においては、高信頼性が求められるシステムの設計、開発、運用、保守を支援するために、様々なソフトウェア工学環境が実現され、利用されている［8-10］。しかし、既存のソフト

ウェア工学環境は、ソフトウェアの信頼性の確保に重点を置いているため、システムの安全性や能動的な攻撃者の存在を殆ど考慮していない［7］。また、システムの個々の構成部分の設計、開発、運用、保守における個々の作業も，必ずしも一定の標準規格に基づいて一貫した手法で支援していない［7］。よって、従来のソフトウェア工学環境は、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、開発、運用、保守を一貫かつ継続して支援するためには不十分である。

従って、高安全性情報システムに要求される安全性を常に維持するために、情報セキュリティ工学において特有の問題である能動的な攻撃者の存在を考慮し、セキュリティ機能の設計・開発から、運用・保守までを国際標準規格に基づいて一貫かつ継続して行えるように支援する情報セキュリティ工学環境が必要である。

3 ISEE: 国際標準規格に基づいた汎用的情報セキュリティ工学環境

3-1 ISEE の構築における基本的な考え

我々は、下記の基本的な考えに基づいて、国際標準規格に基づいた汎用的情報セキュリティ工学環境 ISEE を構築している（Fig. 2 を参照されたい）［6］。

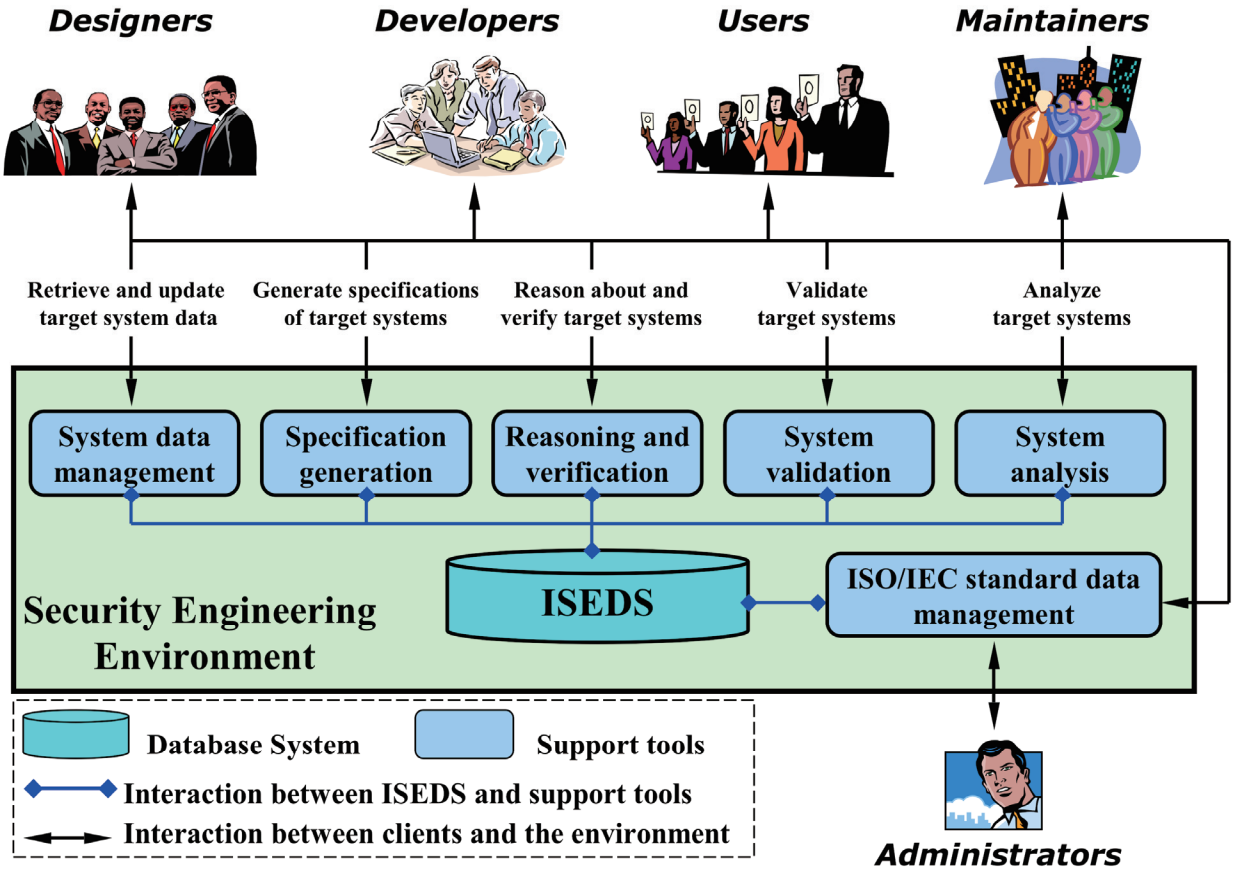

Fig. 2　Security engineering environment based on ISO/IEC standards

（1）ISEE は、システムのセキュリティ機能の設計、開発、運用、保守に対する支援を絶えずに継続するために、永続的計算システム［2-5］であるべきである。

（2）ISEE は、セキュリティ機能の設計と開発だけでなく、運用、保守、廃棄も支援すべきである。

（3）ISEE は、利用者がセキュリティ機能の設計、開発、運用、保守、廃棄における様々な作業を ISO/IEC 国際標準規格の規定に従って行うことを支援すべきである。

（4）ISEE は、利用者が標準規格や情報やデータを共有し、また共通な基準・情報・データに基づいて、セキュリティ機能の設計、開発、運用、保守、廃棄における様々な作業を行うことを支援すべきである。

（5）ISEE は、利用者がセキュリティ機能の設計、開発、運用、保守、廃棄における様々な作業を適切な

順序で行うことを支援すべきである。

（6）ISEEは、利用者がセキュリティ機能の設計、開発、運用、保守における様々な作業をISO/IEC国際標準規格に基づく形式的手法を用いて行うことを支援すべきである。

（7）ISEEは、利用者がセキュリティ機能の保守（更新、追加、停止、復旧、削除など）を迅速に行うことを支援すべきである。

3-2 セキュリティ機能の設計、開発、運用、保守、廃棄における様々な作業の詳細化

ISEEに対する具体的な要求を分析し定義するためには、ISEEの支援対象であるセキュリティ機能の設計、開発、運用、保守、廃棄における様々な作業を明確にしなければならない。そこで我々はソフトウェアライフサイクルプロセスに関するISO/IEC国際標準規格であるISO/IEC 12207［34］に着目した。ISO/IEC 12207は、機能性、信頼性、保守性、生産性、ユーザビリティ、安全性などの品質を備えたソフトウェアの企画および設計、開発、運用、保守、廃棄の作業をそれぞれいくつかのプロセスとして詳細化し、一連のプロセスを包括したソフトウェアライフサイクルプロセスを定義している。

我々は、ISO/IEC 12207が規定する作業のうちセキュリティ機能および情報システムの安全性に直接関係する作業を以下のように分類した。

・セキュリティ機能もしくはその関連文書（要求定義文書、仕様規定文書、設計文書、プログラムのソースコード、テスト関連文書、保守関連文書、マニュアルなど）を作成する作業
・セキュリティ機能もしくはその関連文書を管理する作業
・セキュリティ機能もしくはその関連文書を検証および検収、レビューする作業
・セキュリティ機能もしくはその関連文書を修正する作業
・セキュリティ機能もしくはその関連文書を参照する作業
・情報システムの情報資産、操作者、管理者、周辺機器、外部環境などを分析もしくは管理する作業
・情報システムを廃棄する作業

また、ISO/IEC 12207が規定する作業のうちISEEが支援すべき作業、およびISO/IEC 12207が規定していないが我々の分析に基づいて明らかにした、ISEEが支援すべき作業を以下のように明確に列挙した。

・脅威管理（risk management）
・ソフトウェア要求分析（software requirements analysis）
・ソフトウェア基本設計（software architectural design）
・ソフトウェア詳細設計（software detailed design）
・ソフトウェア実装（software implementation）
・ソフトウェア構築（software construction）
・ソフトウェア統合（software integration）
・ソフトウェア適格性テスト（software qualification testing）
・ソフトウェア品質保証（software quality assurance）
・ソフトウェア検証（software verification）
・ソフトウェア検収（software validation）
・ソフトウェアレビュー（software review）
・基盤管理（infrastructure management）
・人的資源管理（human resource management）
・品質管理（quality management）
・情報管理（information management）
・ソフトウェア文書管理（software documentation management）
・ソフトウェア構成管理（software configuration management）
・環境管理（environment management）
・ソフトウェア導入（software installation）
・ソフトウェア操作（software operation）
・ソフトウェア保守（software maintenance）
・ソフトウェア問題解決（software problem resolution）
・ソフトウェア復旧（software recovery）
・ソフトウェア廃棄（software disposal）

更に、ISEEは利用者がセキュリティ機能の設計、開発、運用、保守、廃棄を、それぞれ適切なISO/IEC国際標準規格に基づいて行うことを支援できるために、我々はISEEの支援対象となる作業と、ISOにおいて情報シ

ステムのセキュリティ技術の標準化を担当するSC27（Sub Committee 27）が規定しているISO/IEC国際標準規格［14-33, 35, 37-87］が規定している作業との対応関係を以下のように（Tab. 1を参照されたい）明確にした。但し、ソフトウェア構築、ソフトウェア統合、ソフトウェア構成管理、ソフトウェア問題解決、ソフトウェア廃棄の作業に関しては、安全性の観点から重要な作業ではあるが、これらの作業に関して規定するISO/IEC国際標準規格は未だない。

Tab. 1　Correspondence relations among tasks and ISO/IEC standards

Classification	Tasks	ISO/IEC Standards
Design	Risk Management	15408
	Software Requirements Analysis	15408, 19790
	Software Architectural Design	15408, 15446, 15816, 15945, 15947, 18028
	Software Detailed Design	7064, 9796, 9798, 10118, 13888, 14888, 18014
Development	Software Implementation	9797, 10116, 10118, 15946, 18031, 18032, 18033
	Software Construction	No
	Software Integration	No
Design and Development	Software Qualification Testing	15408, 15443, 18045, 19790, 19791
	Software Quality Assurance	21827
	Software Verification	15408, 15443, 18045, 19790, 19791
	Software Validation	15408, 15443, 18045, 19790, 19791
	Software Review	15408, 15443, 18045, 19790, 19791
Management	Infrastructure Management	13335, 27001, 27002, 27006
	Human Resource Management	13335, 27001, 27002, 27006
	Quality Management	13335, 27001, 27002, 27006
	Information Management	11770
	Software Documentation Management	13335, 27001, 27002, 27006
	Software Configuration Management	No
	Environment Management	11770, 13335, 14516, 27001, 27002, 27006
	Software Installation	13335, 27001, 27002, 27006
	Software Operation	13335, 18043, 27001, 27002, 27006
Maintenance	Software Maintenance	7064, 9796, 9797, 9798, 10116, 10118, 13888, 14888, 15408, 15446, 15816, 15945, 15946, 15947, 18014, 18028, 18031, 18032, 18033, 18044
	Software Problem Resolution	No
	Software Recovery	24762
Abolition	Software Disposal	No

我々は，ISO/IEC 12207 に定義されたソフトウェアライフサイクルプロセスを参考にして、情報システムのセキュリティ機能の設計、開発、運用、保守、廃棄における様々な作業を順序付けした（Fig. 3 を参照されたい）。このような順序で、各作業を繰り返し行えれば、対象システムの安全性を一貫して維持することができる。

3-3 ISEE の要求定義

我々はISEEが満たすべき具体的な要求を以下のように定義した。

R-1: ISEEは、永続的な計算環境として、集中的にも分散的にも利用できる手段を利用者に提供しなければならない。

R-2: ISEEは、セキュリティ機能の設計、開発、運用、保守、廃棄におけるあらゆる作業に対して支援を利用者に提供しなければならない。

R-3: ISEEは、ISO/IEC国際標準規格を格納、更新、検索、参照する手段を利用者に提供しなければならない。

R-4: ISEEは、ISO/IEC国際標準規格に基づいて認証済みのシステム開発において作成された文書を格納、更新、検索、参照する手段を利用者に提供しなければならない。

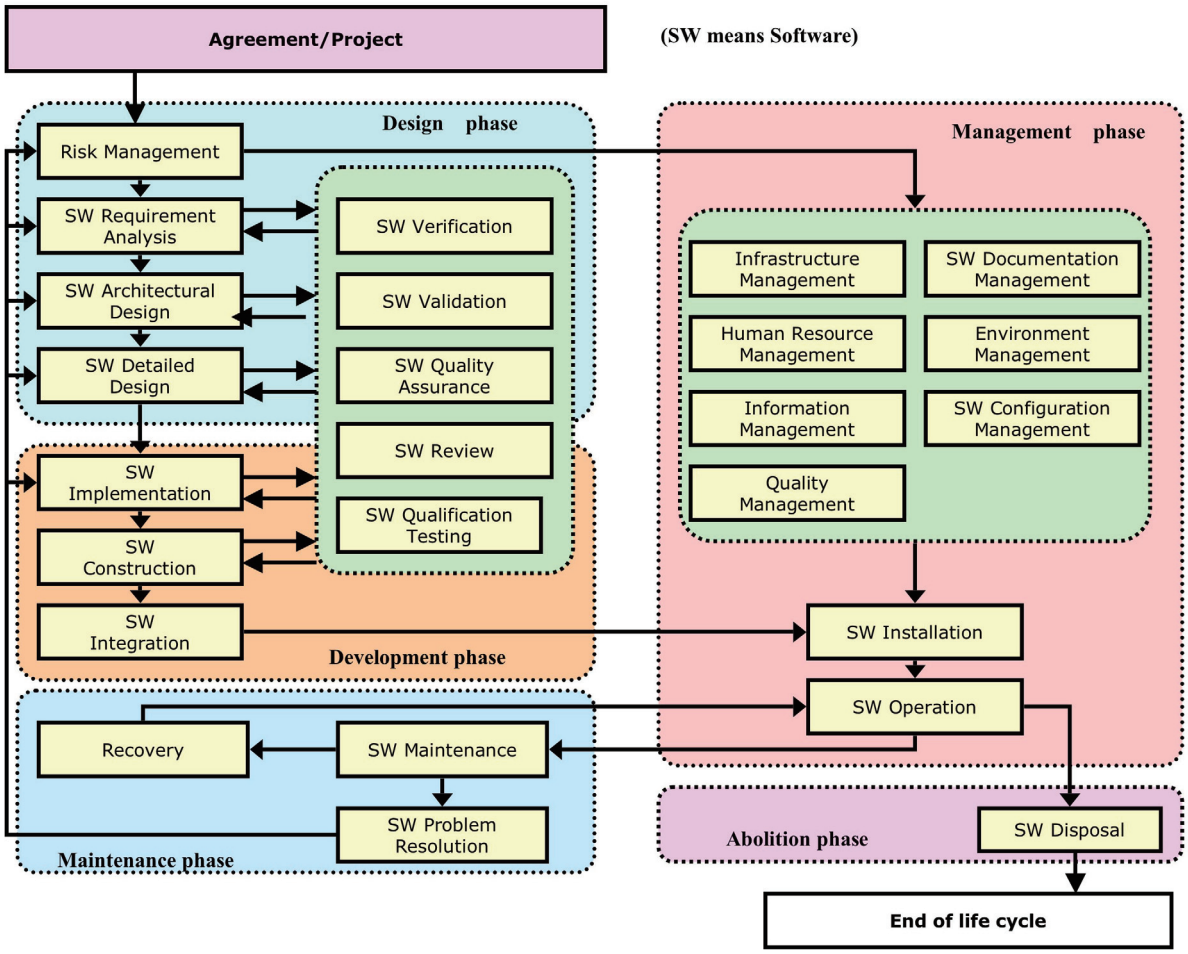

Fig. 3　Tasks with a right order in design, development, management, and maintenance

R-5: ISEEは、ISO/IEC国際標準規格に基づく認証に必要な文書を簡単かつ迅速に作成する手段を利用者に提供しなければならない。

R-6: ISEEは、セキュリティ機能の設計、開発、運用、保守、廃棄におけるあらゆる文書を、ISO/IEC国際標準規格に基いて形式的あるいは非形式的に検証、検収、レビューする手段を利用者に提供しなければならない。

R-7: ISEEは、個々の対象システムに関するあらゆるデータを格納、更新、検索、参照する手段を個々の利用者に提供しなければならない。

R-8: ISEEは、個々の対象システムに関するデータをアクセス権限の持つ利用者同士間に自動的に共有する手段を利用者に提供しなければならない。

R-9: ISEEは、個々の対象システムに関するデータに対する情報セキュリティ制御を行う手段を利用者に提供しなければならない。

R-10: ISEEは、セキュリティ機能の設計、開発、運用、保守、廃棄におけるあらゆる作業に対する支援を適切かつ迅速に提供しなければならない。

R-11: ISEEは、その自身の高い信頼性と高い安全性を常に維持しなければならない。

3-4 ISEE の利用形態とアーキテクチャー

ISEE のデータベース ISEDS（後述）が格納しているデータのうち、多くの一般公開データもあれば、対象システムの情報セキュリティに関する高度機密データもある。従って、我々は ISEE の可能な利用形態を２つ想定している。一つ目は、ISEE を WEB 上で一般公開して、不特定多数の利用者がネットワークを経由して、ISEE を分散的に利用する形態である。この場合、責任を持って ISEE を管理する個人か組織が必要である。二つ目は、会社もしくは団体ごとに ISEE を単独で管理し集中的にもしくは分散的に利用する形態である。また、前者の利用形態に対して、多くの利用者も ISEE プロジェクトに参加し、共同で ISEE の継続開発と保守

を行うことを期待できる。

Fig. 4 は、現在我々が開発している ISEE のアーキテクチャーを示している。

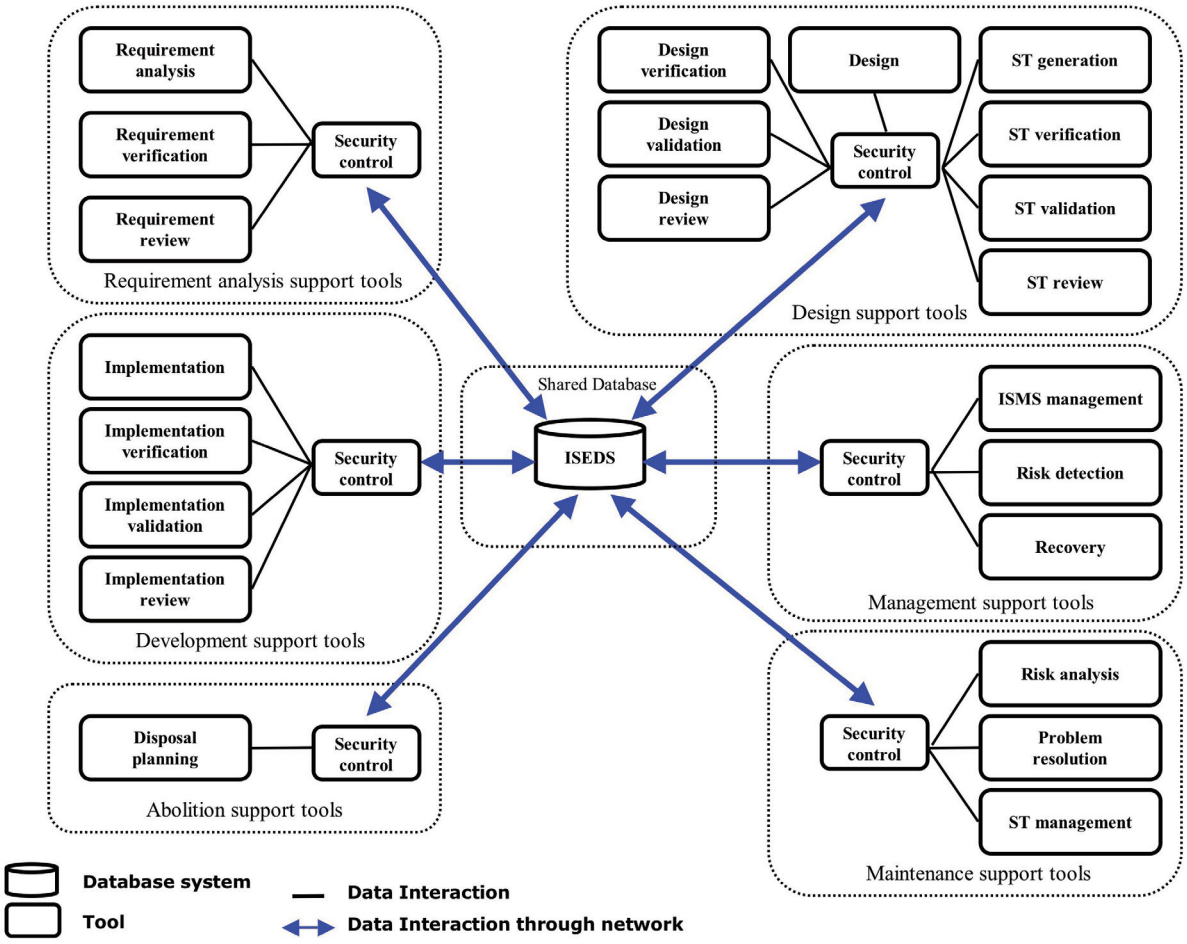

Fig. 4 Components of ISEE and the relationships among them

3-5 ISEE の各構成部分の開発

情報セキュリティ工学データベースシステム ISEDS (Information Security Engineering Database System) は、ISEE において最も中心的かつ重要な構成部分である [11, 85, 92, 93]。ISEDS は情報システムのセキュリティ機能に関する様々なデータを管理するデータベースシステムであり、利用者がそれを用いて以下のデータを格納、更新、検索することができる。

ISO/IEC国際標準規格に関するデータ：情報システムにおけるセキュリティ機能の設計、開発、運用、保守、廃棄に関係のあるISO/IEC国際標準規格データである。これらの国際標準規格は、テキストのまま格納されたものもあれば形式的記述言語で形式化されたうえ格納されたものもある。

システム事例に関するデータ：実際に開発された様々な情報システムのセキュリティ機能の設計、開発、運用、保守の公開事例に関するデータである。例えば、要求定義文書、仕様規定文書、国際標準規格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文書、設計文書、テストや検証に関する文書、プログラムソースコード、保守記録文書などである.

個別対象システムに関するデータ：各利用者が対象システムのセキュリティ機能の設計、開発、運用、保守の際に定義、生成した、一般公開せず、利用権限が制限されているデータである。

これらのデータの構造化、形式化、電子化により、データの検索と参照の効率化ばかりではなく、本来様々な媒体で保存され、散乱されているデータの形では全くできなかった、様々な目的で生成されたデータ間の一貫性に対する検証、およびセキュリティ機能の設計・開発から運用・保守までにおける様々な作業の自動化が可能になり、情報セキュリティ工学における系統的な方法論の樹立に役に立つ。従って、ISEDSは、ISEE

の様々な利用者や支援ツールにとって、仕事の共通の土台である同時に、情報セキュリティ機能の設計・実現から運用・保守までにおける様々な作業の一貫性の維持およびこれらの作業の自動化にとっても極めて重要な役目を果たす。

利用者は、ISEDSを「情報セキュリティ工学の百科事典」として利用し、用語や国際標準規格における事項を検索し参照することことができる。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、新しい情報システムの設計と開発や新しいセキュリティ機能の設計と開発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、対象システムの設計・実現から運用・保守までにおける様々な作業の一貫性を維持することができ、過去に行った設計や開発や保守に関するデータを、既存のセキュリティ機能の保守や新しいセキュリティ機能の設計と開発に役立てることもできる。

一方、ISEDSに格納されている様々なデータに基づいて、ISEEはいろいろな支援ツールを利用者に提供することができる。現在、我々は、ISEDSのデータを充実すると共に、ISEDSのデータに基づいて利用者に支援するツール群を開発している。

情報技術セキュリティ評価国際標準規格ISO/IEC 15408は、情報技術セキュリティの観点から、情報技術に関連した製品およびシステムが適切に設計され、その設計が正しく実装されているかどうかを評価するための国際標準規格である。ISO/IEC 15408に基づいて、情報システムのセキュリティ強固さの度合いを、設計・仕様書や開発プロセスなど様々な視点から系統的に評価できる。調達者は、導入しようとしているシステムを共通の基準で比較し、必要なセキュリティ強固さに応じて必要な機能を具備しているかどうかをチェックすることができる。一方、開発者は、セキュリティ対策やセキュリティ機能の設計・開発をISO/IEC 15408に基づいて行うことにより、考慮漏れのない安全なシステムを設計・開発することができる。従って、ISO/IEC 15408は、適用範囲が広い、多くの利用者にとって役に立つ国際標準規格である。現在、世界において、多くの国々はISO/IEC 15408を政府調達基準、即ち、政府が利用するIT関連製品のセキュリティ機能・品質をチェックするための基準としている。日本では、政府が利用するIT関連製品のセキュリティ機能・品質をチェックするために「情報セキュリティ評価認証体制」が2001年4月にスタートし、ISO/IEC 15408を政府調達基準としている。

我々は、情報セキュリティ機能保証技法を調査、研究し、ISEDSをはじめISEEの様々な支援ツールを設計、開発する際に、まず、情報技術セキュリティ評価国際標準規格ISO/IEC 15408を最も重視すべき基準とした [6, 11, 84-87, 90-93]。現在、ISEDSにはISO/IEC 15408の最新（英語、日本語）版ばかりではなく、古い（英語、日本語）版も格納しており、テキスト版ばかりではなく、Z表記法[36]で形式された版も格納している [11, 85, 92, 93]。利用者は、最新版のISO/IEC 15408に基づいて、セキュリティ機能の設計・開発を行うことができ、古い版のISO/IEC 15408に基づいて設計、開発したセキュリティ機能を、ISO/IEC 15408の最新版と古い版との差分を調べながら、更新・改善することもできる。また、ISEDSにはISO/IEC 15408に基づいて既に認証され公開されたセキュリティ設計仕様書も多く格納している。

情報システムがISO/IEC 15408に基づいて認証されるには、まずセキュリティ設計仕様書(Security Target, ST) を作成しなければならない。しかし、このセキュリティ設計仕様書作成という仕事は容易なことではない。我々は、多くの利用者がセキュリティ設計仕様書をもっと容易に作成するために、セキュリティ設計仕様書雛形生成ツールGEST(GEnerator of Security Targets)を開発した。また、セキュリティ設計仕様書作成・保守支援エディターも現在開発している。GESTは、利用者に指定された条件（言語、ISO/IEC 15408版、評価保証レベルEAL、キーワードなど）およびISEDSに保存されている認証済みのセキュリティ設計仕様書に基づいて、セキュリティ設計仕様書の雛形を生成し出力する。利用者は、指定条件を繰り返し修正し、GESTを用いて、自分が作成したいセキュリティ設計仕様書に最も近い雛形を手に入れることができる。セキュリティ設計仕様書作成・保守支援エディターは、セキュリティ設計仕様書の構造エディターであり、ISO/IEC 15408に規定されているセキュリティ設計仕様書の構造に従いながら、セキュリティ設計仕様書の作成、編集、修正を利用者に支援することができる。

形式的手法を用いてセキュリティ機能の設計を行うのは、セキュリティ強固さを保証する最も有効な技法である。しかし、必ずしも全てのセキュリティ関連の国際標準規格を完全に形式化できるというわけではなく、たとえある国際標準規格が完全に形式化されたとしてもそれに基づく検証法を簡単に構築できるというわけでもない。更に、検証法自身の使いやすさはその実用性に大きな影響を与える。我々は既にISO/IEC 15408に基づく設計仕様の形式的検証法を提案した [86, 87, 90, 91]。しかし、この技法は数学、論理学、形式的手法に関して高度な知識が要求されるので、初心者にとって、必ずしも使いやすい技法と言えない。そこで、我々は、セキュリティ設計仕様書検証支援ツールFORVEST(FORmal VErification Support Tool of security

specifications）を開発した。FORVESTにより提供した支援で、利用者にとって、従来必要であった９種類の知識のうち、７種類の知識が不要になり、２種類の知識の必要性の程度も軽減されている。即ち、FORVESTを使えば、我々の設計仕様の形式的検証法をもっと簡単に実施することができる。

上記で述べた、ISEEの既に開発されたツールは、情報システムにおけるセキュリティ機能の設計・開発にとって役に立つばかりではなく、セキュリティ機能の適切かつ迅速な保守にとっても非常に役に立つ筈である。

現在、我々は、ISEEの他の多くの支援ツールの要求分析、機能定義、設計、開発を行っており、順次に公表していく予定である。

4 成果と展望

本研究では、高安全性が要求される情報システムにおける情報セキュリティ機能の設計・実現から運用・保守までを一貫かつ継続して支援するために、ISO/IEC 国際標準規格に基づいて、情報セキュリティ工学データベース、情報セキュリティ機能保証技法および支援ツール群を開発し、それらを統合する汎用的情報セキュリティ工学環境 ISEE を開発している。ISEE は世界において初めての情報セキュリティ工学環境である。

ISEE を利用すれば、情報通信システムの設計者と開発者は、設計・開発の最初段階から ISO 国際標準規格および認証済みセキュリティ仕様の公開事例に基づいて、安全性の高い情報通信システムを設計し開発することができる。また、情報通信システムの運用者と保守者は、新たな脅威に対して情報セキュリティ機能の改善を適切かつ迅速に行うことができる。本研究の成果は、情報セキュリティ工学基盤技術として、情報セキュリティ工学という新しい工学分野の更なる発展の基礎になる。

将来、ISEE と従来のソフトウェア工学環境とを有機的に統合し、高信頼性、高安全性が要求される情報システムの設計、開発、運用、保守を支援できる工学環境を構築することもできる。

【参考文献】

[1] R. J. Anderson: Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd ed., John Wiley & Sons, 2008.

[2] J. Cheng: Connecting Components with Soft System Buses: A New Methodology for Design, Development, and Maintenance of Reconfigurable, Ubiquitous, and Persistent Reactive Systems, Proc. 19th International Conference on Advanced Information Networking and Applications, Vol. 1, pp. 667-672, IEEE Computer Society Press, 2005.

[3] J. Cheng: Comparing Persistent Computing with Autonomic Computing, Proc. 11th International Conference on Parallel and Distributed Systems, Vol. II, pp. 428-432, IEEE Computer Society Press, 2005.

[4] J. Cheng: Persistent Computing Systems as Continuously Available, Reliable, and Secure Systems, Proc. 1st International Conference on Availability, Reliability and Security, , pp. 631-638, IEEE Computer Society Press, 2006.

[5] J. Cheng: Persistent Computing Systems Based on Soft System Buses as an Infrastructure of Ubiquitous Computing and Intelligence (Invited Paper), Journal of Ubiquitous Computing and Intelligence, Vol. 1, No. 1, pp. 35-41, 2007.

[6] J. Cheng, Y. Goto, S. Morimoto, and D. Horie: A Security Engineering Environment Based on ISO/IEC Standards: Providing Standard, Formal, and Consistent Supports for Design, Development, Operation, and Maintenance of Secure Information Systems, Proc. 2nd International Conference on Information Security and Assurance, pp. 350-354, IEEE Computer Society Press, 2008.

[7] P. T. Devanbu, and S. Stubblebine: Software Engineering for Security: A Roadmap, International Conference on Software Engineering, Proc. Conference on The Future of Software Engineering, pp. 227-239, ACM Press, 2000.

[8] K. Dittrich, D. Tombros, and A. Geppert: Databases in Software Engineering: A Roadmap, International Conference on Software Engineering, Proc. Conference on The Future of Software Engineering, pp. 291-302, ACM Press, 2000,

[9] A. Finkelstein, and J. Kramer: Software Engineering: A Roadmap, International Conference on Software Engineering, Proc. Conference on The Future of Software Engineering, pp. 3-22, ACM Press, 2000.
[10] W. Harrison, H. Ossher, and P. Tarr: Software Engineering Tools and Environments: A Roadmap, International Conference on Software Engineering, Proc. Conference on The Future of Software Engineering, pp. 261-277, ACM Press, 2000.
[11] D. Horie, S. Morimoto, N. Azimah, Y. Goto, and J. Cheng: ISEDS: An Information Security Engineering Database System Based on ISO Standards, Proc. 3rd International Conference on Availability, Reliability and Security, pp. 1219-1225, IEEE Computer Society Press, 2008.
[12] IEEE Computer Society: IEEE Standard 610, IEEE Standard Computer Dictionary – A Compilation of IEEE Standard Computer Glossaries, IEEE Computer Society Press, 1990.
[13] IEEE Computer Society: IEEE Standard 610.12-1990, IEEE Standard Glossary of Software Engineering Terminology, IEEE Computer Society Press, 1990
[14] ISO: ISO/IEC 7064:2003, Information technology – Security techniques – Check character systems.
[15] ISO: ISO/IEC 9796-2:2002, Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms.
[16] ISO: ISO/IEC 9796-3:2006, Information technology – Security techniques – Digital signature schemes giving message recovery – Part 3: Discrete logarithm based mechanisms.
[17] ISO: ISO/IEC 9797-1:1999, Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher.
[18] ISO: ISO/IEC 9797-2:2002, Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function.
[19] ISO: ISO/IEC 9798-1:1997, Information technology – Security techniques – Entity authentication – Part 1: General.
[20] ISO: ISO/IEC 9798-2:2008, Information technology – Security techniques – Entity authentication – Part 2: Mechanisms using symmetric encipherment algorithms.
[21] ISO: ISO/IEC 9798-3:1998, Information technology – Security techniques – Entity authentication – Part 3: Mechanisms using digital signature techniques.
[22] ISO: ISO/IEC 9798-4:1999, Information technology – Security techniques – Entity authentication – Part 4: Mechanisms using a cryptographic check function.
[23] ISO: ISO/IEC 9798-5:2004, Information technology – Security techniques – Entity authentication – Part 5: Mechanisms using zero-knowledge techniques.
[24] ISO: ISO/IEC 9798-6:2005, Information technology – Security techniques – Entity authentication – Part 6: Mechanisms using manual data transfer.
[25] ISO: ISO/IEC 10116:2006, Information technology – Security techniques – Modes of operation for an n-bit block cipher.
[26] ISO: ISO/IEC 10118-1:2000, Information technology – Security techniques – Hash-functions – Part 1: General.
[27] ISO: ISO/IEC 10118-2:2000, Information technology – Security techniques – Hash-functions – Part 2: Hash-functions using an n-bit block cipher.
[28] ISO: ISO/IEC 10118-3:2004, Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions.
[29] ISO: ISO/IEC 10118-4:2000, Information technology – Security techniques – Hash-functions – Part 4: Hash-functions using modular arithmetic.
[30] ISO: ISO/IEC 11770-1:1996, Information technology – Security techniques – Key management – Part 1: Framework.
[31] ISO: ISO/IEC 11770-2:2008, Information technology – Security techniques – Key management – Part 2: Mechanisms using symmetric techniques.
[32] ISO: ISO/IEC 11770-3:2008, Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques.

[33] ISO: ISO/IEC 11770-4:2006, Information technology – Security techniques – Key management – Part 4: Mechanisms based on weak secrets.
[34] ISO: ISO/IEC 12207:2008, Systems and software engineering – Software life cycle processes.
[35] ISO: ISO/IEC 13335-1:2004, Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management.
[36] ISO: ISO/IEC 13568:2002, Information Technology – Z formal specification notation – Syntax, type system and semantics.
[37] ISO: ISO/IEC 13888-1:2009, Information technology – Security techniques – Non-repudiation – Part 1: General.
[38] ISO: ISO/IEC 13888-2:1998, Information technology – Security techniques – Non-repudiation – Part 2: Mechanisms using symmetric techniques.
[39] ISO: ISO/IEC 13888-3:1997, Information technology – Security techniques – Non-repudiation – Part 3: Mechanisms using asymmetric techniques.
[40] ISO: ISO/IEC 14888-1:2008, Information technology – Security techniques – Digital signatures with appendix – Part 1: General.
[41] ISO: ISO/IEC 14888-2:2008, Information technology – Security techniques – Digital signatures with appendix – Part 2: Integer factorization based mechanisms.
[42] ISO: ISO/IEC 14888-3:2006, Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms.
[43] ISO: ISO/IEC 15408-1:2005, Information Technology – Security Techniques – Evaluation Criteria for IT Security – Part 1: Introduction and general model.
[44] ISO: ISO/IEC 15408-2:2008, Information Technology – Security Techniques – Evaluation Criteria for IT Security – Part 2: Security functional components.
[45] ISO: ISO/IEC 15408-3:2008, Information Technology – Security Techniques – Evaluation Criteria for IT Security – Part 3: Security assurance components.
[46] ISO: ISO/IEC 15816: 2002, Information technology – Security techniques – Security information objects for access control.
[47] ISO: ISO/IEC 15945:2002, Information technology – Security techniques – Specification of TTP services to support the application of digital signatures.
[48] ISO: ISO/IEC 15946-1:2008, Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General.
[49] ISO: ISO/IEC 15946-2:2002, Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures.
[50] ISO: ISO/IEC 15946-3:2002, Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 3: Key establishment.
[51] ISO: ISO/IEC 15946-4:2004, Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 4: Digital signatures giving message recovery.
[52] ISO: ISO/IEC 18014-1:2008, Information technology – Security techniques – Time-stamping services – Part 1: Framework.
[53] ISO: ISO/IEC 18014-2:2002, Information technology – Security techniques – Time-stamping services – Part 2: Mechanisms producing independent tokens.
[54] ISO: ISO/IEC 18014-3:2004, Information technology – Security techniques – Time-stamping services – Part 3: Mechanisms producing linked tokens.
[55] ISO: ISO/IEC 18028-1:2006, Information technology – Security techniques – IT network security – Part 1: Network security management.
[56] ISO: ISO/IEC 18028-2:2006, Information technology – Security techniques – IT network security – Part 2: Network security architecture.
[57] ISO: ISO/IEC 18028-3:2005, Information technology – Security techniques – IT network security – Part 3: Securing communications between networks using security gateways.

[58] ISO: ISO/IEC 18028-4:2005, Information technology – Security techniques – IT network security – Part 4: Securing remote access.
[59] ISO: ISO/IEC 18028-5:2006, Information technology – Security techniques – IT network security – Part 5: Securing communications across networks using virtual private networks.
[60] ISO: ISO/IEC 18031:2005, Information technology – Security techniques – Random bit generation.
[62] ISO: ISO/IEC 18032:2005, Information technology – Security techniques – Prime number generation.
[62] ISO: ISO/IEC 18033-1:2005, Information technology – Security techniques – Encryption algorithms – Part 1: General.
[63] ISO: ISO/IEC 18033-2:2006, Information technology – Security techniques – Encryption algorithms – Part 2: Asymmetric ciphers.
[64] ISO: ISO/IEC 18033-3:2005, Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers.
[65] ISO: ISO/IEC 18033-4:2005, Information technology – Security techniques – Encryption algorithms – Part 4: Stream ciphers.
[66] ISO: ISO/IEC 18043:2006, Information technology – Security techniques – Selection, deployment and operations of intrusion detection systems.
[67] ISO: ISO/IEC 18045:2008, Information technology – Security techniques – Methodology for IT security evaluation.
[68] ISO: ISO/IEC 19790:2006, Information technology – Security techniques – Security requirements for cryptographic modules.
[69] ISO: ISO/IEC 21827:2002, Information technology – Systems Security Engineering – Capability Maturity Model.
[70] ISO: ISO/IEC 24762:2008, Information technology – Security techniques – Guidelines for information and communications technology disaster recovery services.
[71] ISO: ISO/IEC 27000:2009, Information technology – Security techniques – Information security management systems – Overview and vocabulary.
[72] ISO: ISO/IEC 27001:2005, Information technology – Security techniques – Information security management systems – Requirements.
[73] ISO: ISO/IEC 27002:2005, Information technology – Security techniques – Code of practice for information security management (Redesignation of ISO/IEC 17799:2005).
[74] ISO: ISO/IEC 27005:2008, Information technology – Security techniques – Information security risk management.
[75] ISO: ISO/IEC 27006:2007, Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management Systems.
[76] ISO: ISO/IEC TR 14516:2002, Information technology – Security techniques – Guidelines for the use and management of Trusted Third Party services.
[77] ISO: ISO/IEC TR 15443-1:2005, Information technology – Security techniques – A framework for IT security assurance – Part 1: Overview and framework.
[78] ISO: ISO/IEC TR 15443-2:2005, Information technology – Security techniques – A framework for IT security assurance – Part 2: Assurance methods.
[79] ISO: ISO/IEC TR 15443-3:2007, Information technology – Security techniques – A framework for IT security assurance – Part 3: Analysis of assurance methods.
[80] ISO: ISO/IEC TR 15446:2009, Information technology – Security techniques – Guide for the production of Protection Profiles and Security Targets.
[81] ISO: ISO/IEC TR 15947:2002, Information technology – Security techniques – IT intrusion detection framework.
[82] ISO: ISO/IEC TR 18044:2004, Information technology – Security techniques – Information security incident management.

[83] ISO: ISO/IEC TR 19791:2006, Information technology – Security techniques – Security assessment of operational systems.
[84] S. Morimoto and J. Cheng: A Security Specification Library with a Schemaless Database," in Y. Shi, G. D. v. Albada, J. Dongarra, and P. M. A. Sloot (Eds.), "Computational Science - ICCS 2007: 7th International Conference, Beijing, China, May 27-30, 2007, Proceedings, Part III," Lecture Notes in Computer Science, Vol. 4489, pp. 890-893, Springer-Verlag, 2007.
[85] S. Morimoto, D. Horie, and J. Cheng: A Security Requirement Management Database Based on ISO/IEC 15408, in M. Gavrilova, et al (Eds.), "Computational Science and Its Applications - ICCSA 2006: International Conference, Glasgow, UK, May 8-11, 2006, Proceedings, Part III" Lecture Notes in Computer Science, Vol. 3982, pp. 1-10, Springer-Verlag, May 2006.
[86] S. Morimoto, S. Shigematsu, Y. Goto, and J. Cheng: Formal Verification of Security Specifications with Common Criteria, Proc. 22nd Annual ACM Symposium on Applied Computing, pp. 1506-1512, ACM Press, 2007.
[87] S. Morimoto, S. Shigematsu, Y. Goto, and J. Cheng: Classification, Formalization and Verification of Security Functional Requirements, in V. Geffert et al. (Eds.), "SOFSEM 2008: Theory and Practice of Computer Science, 34th Conference on Current Trends in Theory and Practice of Computer Science, Novy Smokovec, High Tatras, Slovakia, January 19-25, 2008, Proceedings," Lecture Notes in Computer Science, Vol. 4910, pp. 622-633, Springer-Verlag, 2008.
[88] OECD, Guidelines for the Security of Information Systems, 1992.
[89] OECD, Guidelines for the Security of Information Systems and Networks, 2002.
[90] 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 (フォーマルアプローチ論文特集号), pp. 726-742, 電子情報通信学会, 2006 年 4 月.
[91] 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, 日本ソフトウェア科学会, 2006 年 7 月.
[92] 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, 日本データベース学会, 2005 年 12 月.
[93] 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ISEDSの開発と応用, 情報処理学会論文誌, Vol. 48, No. 4, pp. 2684-2698, 情報処理学会, 2007 年 8 月.

〈発 表 資 料〉

題　　名	掲載誌・学会名等	発表年月
A Security Engineering Environment Based on ISO/IEC Standards: Providing Standard, Formal, and Consistent Supports for Design, Development, Operation, and Maintenance of Secure Information Systems	Proceedings of the 2nd International Conference on Information Security and Assurance, pp. 350-354, IEEE Computer Society Press	April 2008
FORVEST: A Formal Verification Support Tool of Security Specifications with ISO/IEC 15408	Proceedings of the 4th International Conference on Availability, Reliability and Security, pp. 624-629, IEEE Computer Society Press	March 2009
GEST: A Generator of ISO/IEC 15408 Security Target Templates	Studies in Computational Intelligence, Vol. 208, pp. 149-158, Springer-Verlag	May 2009
A New Model of Software Life Cycle Processes for Consistent Design,	Proceedings of the 8th IEEE/ACIS International	June 2009

Development, Management, and Maintenance of Secure Information Systems	Conference on Computer and Information Science, pp. 897-902, IEEE Computer Society Press	
ISEE: An Information Security Engineering Environment	Proceedings of International Conference on Security and Cryptography, pp. 395-400, INSTICC Press	July 2009
Development of ISEE: An Information Security Engineering Environment	Proceedings of the 7th IEEE International Symposium on Parallel and Distributed Processing with Applications, IEEE Computer Society Press	August 2009