Vol.2013-DPS-154 No.35
Vol.2013-CSEC-60 No.35
2013/3/15

セキュリティ標準に基づいた セキュリティレベル評価技術の検討

芦野佑樹[†1]　森田陽一郎[†1]　小泉純[†1†2]　岡村利彦[†1]

IT システムの大規模化に伴い，セキュリティ対策は複雑化している．セキュリティ対策を行う際は，IT システムを構成する全てのコンピュータリソースに対して，適切なセキュリティ機能を割り当てる必要がある．IT システムの設計段階において，システムエンジニアには，物理層からアプリケーション層までの幅広いセキュリティの知識が必要である．そこで，筆者らは IT システムのセキュリティ機能の設計に必要な知識の拠り所として，セキュリティ標準が活用できるのではないかと考えた．セキュリティ標準とは，IT システムを運用する組織体制や技術的対策の確認項目を含んだ監査基準が記載されている．この記載内容に基づいた IT システムのセキュリティ機能の設計が行われることが望ましいが，セキュリティ標準には，セキュリティ機能の設計に関する具体的な内容が無い．そのため，システムエンジニアは，セキュリティ標準に記載内容から，具体的なセキュリティ機能，セキュリティ機能を実行するコンピュータリソースの特定，セキュリティ機能に必要なパラメータに解釈する必要があり，セキュリティ標準に対する専門的な知識が新たに必要になってしまう．そこで，筆者らは，IT システムの設計時において，セキュリティ標準に基づいたセキュリティ機能の設計ができるように，(1)セキュリティ標準のナレッジ化，(2)システムモデルとセキュリティモデルの二つのアプローチによる，セキュリティレベル評価技術を考案したので報告を行う．

Study of Evaluating Security Level of IT System Based on Security Guidelines

YUKI ASHINO[†1]　YOICHIRO MORITA[†1]　JUN KOIZUMI[†1†2]
TOSHIHIKO OKAMURA[†1]

As IT systems have become large and complicated, their security design has been also getting difficult. To build a secure system, a system engineer must have an extensive knowledge on security, and it is difficult for them to evaluate what security level the designed system achieves. We consider that security standards can be also used to assess security levels on a design stage. However, because they are written in very general descriptions from the view of audit criteria, it is difficult for an engineer to design a system according to a security standard. In this paper, to realize security-standard based system design, we propose the methods of security standard knowledge base, system model description with security functions and security level assessment by combining them. We show a prototype design and how the proposed methods work.

1. はじめに

IT システムの大規模化に伴い，セキュリティ対策は複雑化している．セキュリティ対策を行う際は，IT システムを構成する全てのコンピュータリソースに対して，適切な設定を行う必要がある．しかしながら，IT システムを構成する一台のサーバ(コンピュータリソース)に対するセキュリティ対策でさえ，入退室管理といった物理的な対策の他，ファイアウォールに代表されるネットワーク対策，オペレーティングシステムのセキュリティパッチ対策，ウェブサーバプログラムの設定など，物理層からアプリケーション層まで幅広く漏れの無い対策が求められている．また，このようなセキュリティ対策は，そのコンピュータリソースの役割や接続されているネットワークの種類などによって異なる場合がある．IT システムの設計段階において，システム全体に対して技術的なセキュリティ対策(セキュリティ機能設計)を実施するためには，システムエンジニアに対して，IT システム全体を把握した上で物理層からアプリケーション層に至る幅広いセキュリティに関する知識が必要であった．

そこで，筆者らは IT システムのセキュリティ機能の設計を行う上で必要な知識の拠り所として，セキュリティ標準が活用できるのではないかと考えた．セキュリティ標準とは，IT システムを運用する組織体制や技術的対策の確認項目を含んだ監査基準が記載されている．代表的なセキュリティ標準には，国際標準化機構(ISO)と国際電気標準会議(IEC)が共同で策定する情報セキュリティに関する規格群である ISO/IEC27000 シリーズ，内閣官房情報セキュリティセンターが策定する政府機関統一基準[1]，クレジットカード業界が策定する Payment Card Industry Data Security Standard(PCI-DSS)[2]などが存在する．この記載内容に基づいた IT システムのセキュリティ機能の設計が行われることが望ましい．しかしながら，セキュリティ標準は，あらゆる IT システムに対応できるよう一般的な記述になっているため，セキュリティ機能の設計に関する具体的な内容が無い．そのため，システムエンジニアは，セキュリティ標準に記載内容から，具体的なセキュリティ機能，セキュリティ機能を実行するコンピュータリソースの特定，セキ

†1 NEC 情報ナレッジ研究
Knowledge Discovery Research Laboratories, NEC Corporation
†2 2012 年 09 月に没
Passed away in September 2012.

ュリティ機能に必要なパラメータに解釈する必要があり，セキュリティ標準に対する専門的な知識が新たに必要になってしまう．

そこで，筆者らは，IT システムの設計時において，システムエンジニアがセキュリティ標準に基づいたセキュリティ機能の設計ができるように，(1)セキュリティ標準のナレッジ化，(2)システムモデルとセキュリティモデルの二つのアプローチによる，セキュリティレベル評価技術を考案した．本稿では，第 2 章で代表的なセキュリティ標準とその課題点を述べ，第 3 章では提案する技術について述べる．また，第 4 章で，関連研究について言及した後，第 5 章でまとめを行う．

2. セキュリティ標準とシステム設計

2.1 セキュリティ標準について

本節では，代表的なセキュリティ標準について述べる．

ISO/IEC27000 は，国際標準化機構(ISO)と国際電気標準会議(IEC)が共同で策定する情報セキュリティに関する規格群であり，ISMS(Information Security Management System)の情報セキュリティに関するガイドラインを提供することを目的として策定している．記述内容については，リスクの分析や体制の整備およびその監査方法が中心である．

政府機関統一基準は，政府機関のとるべきセキュリティ対策に統一性を持たせ，政府機関全体の情報セキュリティの強化・拡充を図ることを目的としていたドキュメント群である[3]．その中には，IT システムの対策技術に特化して記述された政府機関の情報セキュリティ対策のための統一技術基準がある[4]．このドキュメントには，セキュリティ要件として，主体認証機能，アクセス制御機能，権限管理機能，証跡管理機能，保証のための機能，暗号と電子証明の 6 つの要件を明確に定義しており，各要件には具体的な確認項目を記述している．

PCI-DSS は，クレジットカード情報や決済店舗とデータセンター間の取引情報を保護するために大手クレジットカード会社が策定したセキュリティ基準である．IT システムのセキュリティ対策が具体的に記されているだけでなく，適用するべきセキュリティ技術の具体的な設定方法についても記載がなされている．PCI-DSS は，全部で 12 章の構成を持っており，ファイアウォール，通信路暗号化などの章が存在する．全体を通じて，ISO27000 シリーズよりも具体的なセキュリティ対策が記述されている．

2.2 セキュリティ機能設計

システムエンジニアが， 図 1 に示すような会員向けの情報を配信するウェブベースのシステム(ウェブシステム)のセキュリティ対策を設計する際，どのような工程で設計を行うのかについて述べる．なお，図 1 中のクライアントとは，一般ユーザが所有する PC でありブラウザを介してウェブサーバにアクセスするものとする．

一般的に，設計段階における IT システムのセキュリティ対策の設計は，(設計行程 1)IT システムで取り扱う情報資産の整理，(設計行程 2)資産に対する脅威の整理，(設計行程 3)セキュリティ要件の整理，(設計行程 4)技術的対策の行程を経る[5][6].

(設計行程 1)において，ウェブシステムで取り扱う情報資産は，会員向け情報と定める．その結果を基に，(設計行程 2)では，会員向け情報資産についての脅威を整理する．ここで得られる脅威は，会員への成りすましとする．その脅威を基に(設計行程 3)では，セキュリティ対策の基本的な方針であるセキュリティ要件を整理する．成りすましに対しては，権限のある者がアクセスしてきたことを認証する主体認証である．最後の(設計行程 4)の行程で，セキュリティ要件を実現するための方式(実現方式)を定める．例えば，ウェブシステムの利用想定が，一般的な PC からブラウザを介したアクセスを想定しているのならば，主体認証に対しては ID とパスワードによる認証(ID/PW 認証)となる．

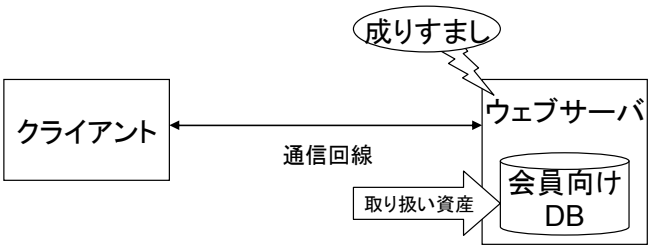

図 1 ウェブシステム
Figure 1 Web System

2.3 セキュリティ標準に基づくセキュリティ機能設計

本節では，システムエンジニアが，セキュリティ機能の設計を行う際に，セキュリティ標準を拠り所とした際の課題点について述べる．なお，ここで参照するセキュリティ標準は，政府機関統一基準とする．

政府機関統一基準では，1.5.2.4(1)(a)(ア)に，要保護資産を取り扱う IT システムに対しては，主体認証を行うよう記述されている．したがって，表現は異なるものの，前述したとおり(設計行程 1)～(設計行程 3)に至る作業についての記述は存在している．しかし，(設計行程 4)のみがセキュリティ標準に記述されている内容を反映しようとすると次に述べるような難しさが存在する．したがって，システムエンジニアが，セキュリティ標準に基づくセキュリティ機能設計を行う際には，多くの工数がかかってしまう．また，IT システムの構成を変更した際は，その都度，評価を行う必要があった．

Vol.2013-DPS-154 No.35
Vol.2013-CSEC-60 No.35
2013/3/15

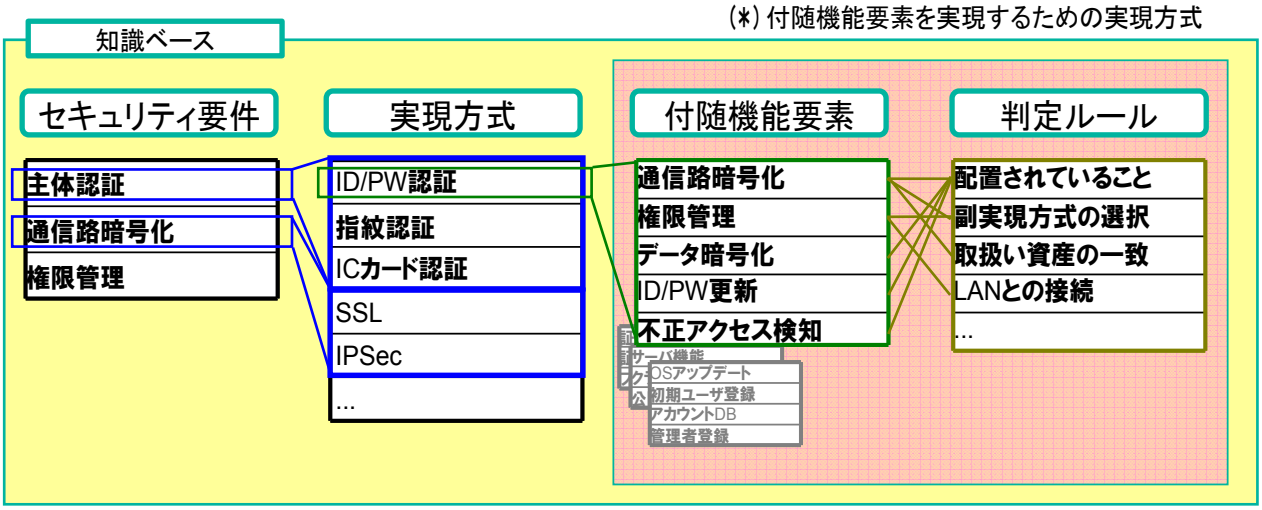

図 2　セキュリティ標準の 4 層構造
Figure 2　Four Layers of Security Standards

2.3.1 (問題 1)セキュリティ要件と実現方式問題

例えば，政府機関統一基準では 2.2.1.1 に主体認証に必要な技術的な要素が記載されている．2.2.1.1 には，(a)～(l)およびその子項目を含め 28 項目の記述が存在する．この 28 項目は，あらゆる主体認証の実現方式に対応できるよう一般的な記述となっている．そのため，システムエンジニアが実現方式に ID/PW 認証を選択した場合は，それに応じた解釈が必要である．例えば，2.2.1.1(1)(b)(ア)では，主体認証情報を保存する際は暗号化するよう指定があるが，これを，パスワードの暗号化やハッシュ化して保存する，と解釈する．現在の所，セキュリティ要件と実現方式や，実現方式とセキュリティ標準内の項目を対応させたデータは存在しない．したがって，システムエンジニアは，セキュリティ要件と実現方式および実現方式とセキュリティ標準内の項目のマッピング作業を行う必要がある．筆者らはこの問題を，セキュリティ要件と実現方式のマッピング問題(問題 1)と名付けた．

2.3.2 (問題 2)パラメータ指定の問題

例えば，政府機関統一基準 1.4.1.1(2)(c)(エ)には，主体認証情報は容易に推定されないものを設定するように記載がある．これは，実現方式 ID/PW 認証では，容易に推定されないパスワードを設定させるようにする必要があると解釈できる．例えば，8 文字以上で英数字をまぜたパスワード以外は設定できないようにするといった機能を搭載する必要性を意味している．また，使用するべき暗号アルゴリズムについては，1.5.2.5(1)(a)(ア)にて政府推奨のものであるよう記述がある．このように，実現方式には取り得るパラメータが存在する．しかし，セキュリティ標準には，実現方式ごとの具体的なパラメータの記述は存在しない．したがって，システムエンジニアは，実現方式ごとの取り得るパラメータをセキュリティ標準から解釈する必要がある．筆者らは，この問題を，パラメータ指定の問題(問題 2)と名付けた．

2.3.3 (問題 3)副実現方式の選択問題

あるセキュリティ機能を選択したことにより新たなセキュリティ要件が要求されてしまう場合である．例えば，ID/PW 認証に関して，2.2.1.1(1)(b)(イ)には，主体認証情報が通信回線上を流れる場合は暗号化するよう求めている．暗号に関する記述は 1.5.2.5 において，暗号と電子署名の標準手順が存在する．これらの内容は，ID/PW 認証の ID やパスワードは通信路上で暗号化すると解釈できる．このように，あるセキュリティ要件に記述されている付随した要素が，別の新たなセキュリティ要件を求めている場合がある．この場合，新たなセキュリティ要件に応じて実現方式(副実現方式)を選択する必要がある．したがって，システムエンジニアは，セキュリティ標準に記述されている内容から，関連する項目を見つけ，かつ，具体的にどのような実現方式を採用するべきなのか決定する作業が必要である．筆者らはこの問題を，副実現方式の選択問題(問題 3)と名付けた．

2.3.4 (問題 4)構成変更に伴う再評価問題

セキュリティ標準に基づいたセキュリティ機能設計は，ある IT システムの構成に対して行われるものである．したがって，構成が変更された場合は，その構成に対してセキュリティ標準と照らし合わせる必要がある．設計段階において，設計対象である IT システムの構成が変更されることは，頻繁に発生することが予想される．仮に，(問題 1)～(問題 3)について工数をかけて解決できたとしても，構成変更

を行うたびに評価を行っていては，時間とコストが多くかかってしまうことは自明である．筆者らはこの問題を，構成変更に伴う再評価問題(問題 4)と名付けた．

3. 提案手法

筆者らは,2.3 節で述べた四つの問題を解決するために，二つの解決アプローチを考案した．一つは，セキュリティ標準を 4 層モデルとして表現することである.もう一つは，IT システムの構成を表現するシステムモデルと，セキュリティ対策を表現したセキュリティモデルである．

この二つのアプローチを基に，セキュリティ標準を基にした IT システムのセキュリティ対策の評価結果を出力するセキュリティレベル評価技術を考案した．

3.1 節でセキュリティ標準の 4 層モデルについて述べ，3.2 節でシステムモデルとセキュリティモデルを入力としたセキュリティレベル評価技術について述べる．最後に，このセキュリティレベル評価技術のプロトタイプの開発を通じて三つの問題についてどのように解決できたのかを 3.3 節で述べる．

3.1 4 層モデルによるセキュリティ標準のナレッジ化

セキュリティ標準は，一般に章・節・項で構成されている．これらはツリー構造で表現できるが，IT システムの設計に適した構造および表現にはなっていない．そこで，筆者らはセキュリティ標準の構造を，セキュリティ要件，実現方式，付随隋機能要素，判定ルールの 4 層構造とし，それぞれの間にリンク構造を持たせた(図 2)．本文では，この構造を持つデータをナレッジと呼ぶことにする．その結果，三つの問題を解決に向けたデータ構造を構築することができた．以下に，4 層モデルについて述べる．

3.1.1 (第 1 層) セキュリティ要件

システムに求められるセキュリティの要件を表現したものである．代表的なセキュリティ要件には，主体認証，アクセス制御，権限管理，証跡管理，暗号技術などがある．セキュリティ要件の下位には，実現方式が存在する．

3.1.2 (第 2 層) 実現方式

セキュリティ要件を実現する実現方式を表現したものである．セキュリティ標準には，実現方式について具体的な言及がされていないことが多い．例えば，政府機関統一基準では，主体認証の実現方式について具体的な物は一切挙げられておらず，主体認証情報の例として「パスワードなどがある」と記載されているに過ぎない．そこで，セキュリティ要件に関連した実現方式をまとめることにより，システムエンジニアがセキュリティ要件を選択した際，必要な実現方式を列挙することができるようになるため, (問題 1)に対して支援が可能であると考えられる．

セキュリティ要件と実現方式の例としては，主体認証に対して「IC カード認証」「指紋認証」「ID/PW 認証」などがある．実現方式の下位には，実現方式が確実に動作するために必要な条件を記載する付随機能要素が存在する．

3.1.3 (第 3 層) 付随機能要素

セキュリティ標準の付随した要素は，実現方式に依存した記述はされていない．そこで，セキュリティ標準の付随した要素を実現方式に依存した表記にしたものが，付随機能要素である．例えば，実現方式 ID/PW 認証の付随機能要素の例としては，ID/PW を盗聴や改ざんから守るための通信路暗号化がある．この付随機能要素の下位には，この付随機能要素の合格する条件が記載された判定ルールとリンクされている．

3.1.4 (第 4 層) 判定ルール

付随機能要素を合格するために必要な条件を表現したものである．この判定ルールには，大きく分けて，入力するべきパラメータの指示と，副実現方式の選択指示に分類される．入力するべきパラメータの指示とは，付随機能要素に設定するべきパラメータの種類を定義したものである．例えば，ID/PW 認証の内，パスワードに最低限必要な文字数などがある．これにより，システムエンジニアは，付随機能要素に対する必要なパラメータを知ることができるようになるため, (問題 2)に対する対応が図れるものと考えられる．また，副実現方式の選択指示とは，付随機能要素を実現する上で，新たな実現方式を選択するよう指示を与えるものである．例えば，ID/PW 認証の場合，ID やパスワードを保護するために暗号化して送付する場合は，通信路を暗号化するための実現方式(副実現方式)を採用するよう指示をするものである.これにより,システムエンジニアは,付随機能要素には副実現方式が必要であることを知ることができることから, (問題 3)に対して対応が図れるものと考えられる．

3.2 セキュリティレベル評価技術方式

筆者らが提案するセキュリティレベル評価技術は，付随機能要素に設定されたパラメータを判定ルール基づいて評価を行い，合格または不合格を判定するものである．

セキュリティレベル評価には，システムモデル入力フェーズ，セキュリティモデル入力フェーズ，評価フェーズ，出力フェーズの 4 つのフェーズが存在する．全体のフローおよび入出力のデータについて図 3 に示した．

システムモデル入力フェーズでは，システムエンジニアが IT システムのコンピュータリソースの構成を表現するシステムモデルを入力する．例えば，第 2 章のウェブシステムの例を取ると，クライアントとウェブサーバの 2 つの

コンピュータリソースを設け，その間と通信回線で結ぶという表現をデータ化したものをシステムモデルとして入力する(図 4 中のシステムモデル).

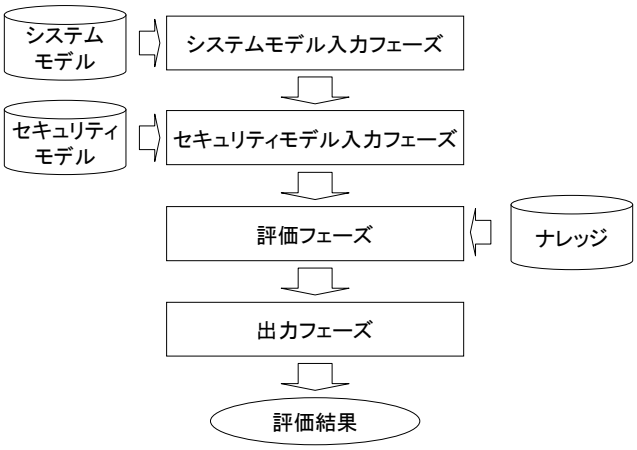

図 3　セキュリティレベル評価技術の全体フロー
Figure 3 Outline of Security Level Evaluation

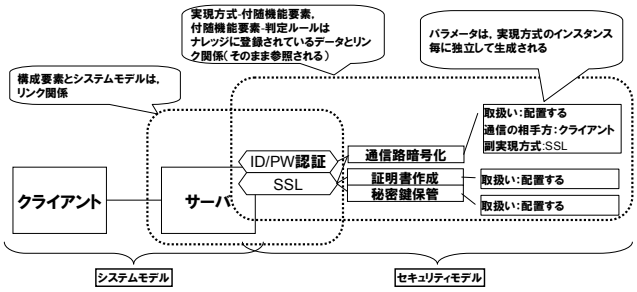

図 4　システムモデルとセキュリティモデルの例
Figure 4　System Model and Security Model

セキュリティモデル入力フェーズでは，システムモデル上のコンピュータに対して，実現方式，付随機能要素およびそのパラメータをリンクさせたセキュリティモデルを入力する．例えば，ウェブシステムのウェブサーバに，実現方式である ID/PW 認証を割り当てる. ID/PW 認証の付随機能要素である通信路暗号化のパラメータには，通信の相手方，および，副実現方式があった場合は，それぞれクライアント，SSL を入力する．また，ウェブサーバには，実現方式 SSL が割り当てられている．以上，実現方式，付随機能要素のパラメータをセキュリティモデルとして，入力する(図 4 中のセキュリティモデル).

評価フェーズでは，入力された付随機能要素に関連付けられた判定ルール毎に行う．判定する際は，パラメータの正当性をシステムモデル・セキュリティモデルの両方を見て評価する．例えば，通信相手を設定するよう指示されているにも関わらず，セキュリティモデルに設定されていない場合は不合格となる．また，通信相手の設定が行われていたとしても，システムモデル上にそのコンピュータリソースが存在していない場合や，経路をたどってもたどり着けない場合は不合格として扱う．また，副実現方式が選択されていたとしても，選択した実現方式を改めて評価した結果，不合格の付随機能要素が含まれていた場合は不合格として扱う.

出力フェーズでは, 評価した結果を可視化する. 例えば, 付随機能要素毎に合格・不合格の結果を出力する.

3.3 セキュリティレベル評価ツール

3.1 節および 3.2 節で述べたアプローチに基づいたセキュリティレベル評価を行うツールは，図 5 に示すような構成になる.

システムエンジニアが使うことを想定しているので，エディタ機能として IT システムの構成を入力するシステムモデルインタフェースと，システムモデルに対してセキュリティ機能を設計するためのセキュリティモデルインタフェースの編集を行えるようエディタを設ける.

入力支援機能は，システムエンジニアに対して適切なセキュリティモデルの入力ができるよう支援する．例えば，システムエンジニアが，システムモデル上のあるコンピュータリソースに対してセキュリティ要件を入力する．その時，入力支援機能は，ナレッジに対してセキュリティ要件に対応する実現方式一覧を取得する．その一覧を入力候補としてエディタ側に反映される．そのため，2.3.1 で述べた(問題 1)セキュリティ要件と実現方式の対応付けの問題に対しては，対応できるものと考えられる．システムエンジニアがある実現方式を選択した際，入力支援機能は，実現方式に関連付けられている付随機能要素および判定ルールをナレッジから取得する．判定ルールには，入力すべきパラメータに関する情報を含んでいるため，セキュリティモデルインタフェースに対して，入力パラメータのダイアログを出すことが可能である．そのため，2.3.2 で述べた(問題 2)パラメータ指定の問題についても，対応できるものと考えられる．また，副実現方式が必要である場合は，判定ルールで指定しているセキュリティ要件を基に実現方式一覧をナレッジから取得することができるため，セキュリティモデルインタフェースに対して，副実現方式の候補を提示することもできる．したがって，2.3.3 で述べた(問題 3)副実現方式の選択問題についても対応できるものと考えられる.

評価エンジンによって，セキュリティレベル評価を行うタイミングは，エディタに対する入力があるごととし，その評価結果は，評価結果インタフェースを介して行う．評価結果インタフェースは，エディタに対しても出力する．そのため，システムエンジニアは，どのセキュリティモデルがセキュリティ標準と照らして満足していないのかを知ることができるようになる．また，システムモデルの変更に追随して評価結果を出力することが可能なので, 2.3.4 で

Vol.2013-DPS-154 No.35
Vol.2013-CSEC-60 No.35
2013/3/15

述べた(問題 4)に対しても対応できるものと考えられる．

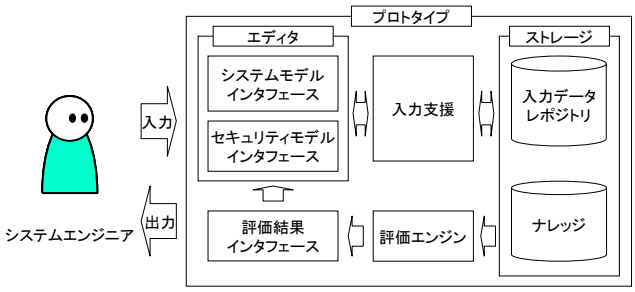

図 5　プロトタイプの概要

Figure 5　Outline of Proto-type

3.4 プロトタイプ

3.3 節で述べた機能の一部をプロトタイプとして実装することで，提案技術の有効性を評価する．プロトタイプでは，予めシステムモデルが入力されているものとした．また，予め WWW/AP サーバには，実現方式 ID/PW 認証が割り当てられているものとした．図 6 は，エディタの出力例である．

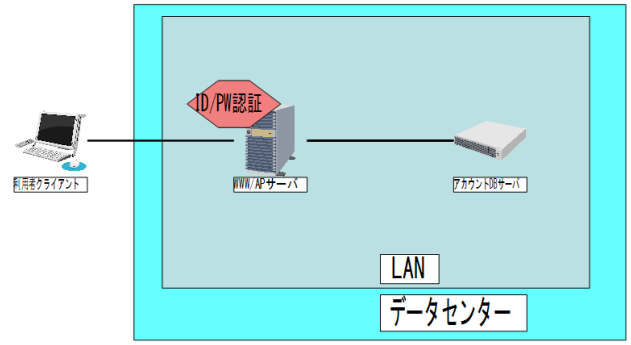

図 6　操作画面

Figure 6　Screenshot of Editor

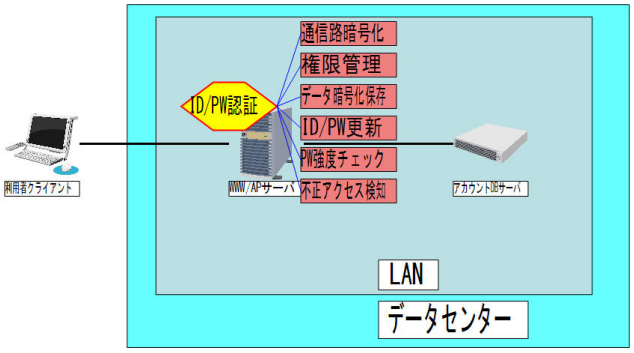

図 7　付随機能要素出力例

Figure 7　Sub-requirements

セキュリティモデルを入力する際に，実現方式にリンクしてある付随機能要素およびその入力するべきパラメータをエディタに出力するため，入力支援プログラムは以下のように処理を行う．

入力支援機能は，セキュリティモデルに入力された実現方式に従い，ナレッジからその実現方式にリンクしている付随機能要素一覧を取得する．さらに，付随機能要素にリンクしている判定ルールを取得し，入力するべきパラメータを取得する．図 7 は，ID/PW 認証を WWW/AP サーバに割り当てた際の出力である．通信路暗号化などの付随機能要素が表示されている．

付随機能要素に入力するべきパラメータは，判定ルールに記述されている内容から入力支援機能によって，エディタに表示することができる．図 8 は，図 7 にある通信路暗号化の付随機能要素をクリックした際に表示されたプロパティウィンドウである．判定ルールでは，副実現方式を入力するよう定義されているため，プロパティウィンドウには，副実現方式を選択するよう指示されている．このように，システムエンジニアは，付随機能要素のパラメータについては，画面に表示されている必須項目に従ってパラメータを設定して行けばよい．したがって，付随機能要素に対して何を入力しなければならないのかについて，自らセキュリティ標準の解釈をしなくて済み，また，間違いのない入力ができるようになった．

図 8　付随機能要素のパラメータ入力

Figure 8　Sub-requirement parameters

システムモデルおよびセキュリティモデルのデータを変更すると同時にセキュリティレベル評価を実行できる．そのため，編集した内容がどのようにセキュリティレベル評価に影響を与えたのかを瞬時に判別することができる．図 9 では，合格している付随機能要素は緑に，不合格の付随機能要素は赤い色で表現した．不合格の場合，どの判定ルールで不合格であったのかを評価エンジンが把握できるので，合格するための条件を表示することもできる(図 9 中の吹き出し)．例えば，通信路暗号化については，副実現方式を選択することが求められていたことがわかる．

出力結果は，図 10 に示すような出力をする．セキュリティレベルの数値は，実現方式の持つ付随機能要素の数を分母とし，その内で合格している付随機能要素を分子のパーセンテージ（合格率）とした．また，付随機能要素が副実

現方式を選択していた場合は，副実現方式が持つ全付随機能要素が分母に組み込んで算出するようにした．合格率が0%から100%未満を，赤から黄のグラデーショで表現した．100%合格している場合は緑色とした．

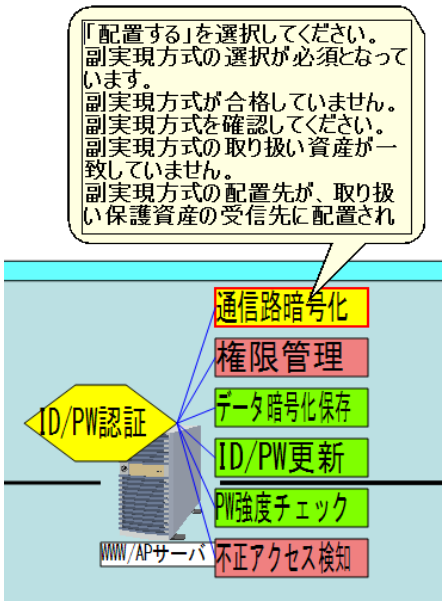

図 9　付随機能要素に対するガイド
Figure 9　Guide of Sub-requirements

図 10　出力結果
Figure 10　Result of Security Evaluation

この出力結果は，システムエンジニアに対して，IT システムのセキュリティ機能の状況を俯瞰することができるようになり，漏れの無いセキュリティ機能設計をするための支援するできるものと考えらえる．

4. 関連研究

本研究の関連研究としては，ナレッジ化と脆弱性診断の2つに分けられる．

ナレッジ化については，高橋らが行っているセキュリティ標準のデータベース化の研究がある[7]．高橋らは，セキュリティ標準内の項目が別の項目を参照している点に着目し，参照関係のデータベース化を試みている．また，この参照関係を基に，ある項目がどの項目に対しての影響度の定式化についても試みている．他項目への影響については，3.1 節で述べた 4 層モデルによるセキュリティ標準のナレッジ化において，副実現方式に近い発想であると考えられる．ただし，このデータベースの構造では，実現方式や判定ルールが存在しないため，そのままではセキュリティレベル評価に利用することはできない．

脆弱性診断は，実際に構築された IT システムの脆弱性を確認する目的で用いられる [8][9]．脆弱性診断ツールは，CVE[10]などのサイトで公開されている脆弱性情報を基に，構築済みの IT システムに対して実際に攻撃を行い，その攻撃が成功するかどうかを確認することにより，脆弱性の有無を診断する．セキュリティレベル評価は，IT システムが構築される前のセキュリティ対策の設計であり，脆弱性診断ツールは構築後の脆弱性診断であるため，使われる段階が異なると考えられる．したがって，セキュリティレベル評価とは補完し合う位置づけであると考えられる．

5. おわりに

IT システムのセキュリティ機能の設計を行うシステムエンジニアには，物理層からアプリケーション層までの幅広いセキュリティ知識が必要であった．セキュリティ対策を行う際の拠り所として，セキュリティ標準が存在するが，セキュリティ機能の設計に関して具体的な記述が存在していない．そこで，筆者らは，システムエンジニアがセキュリティ標準に基づいたセキュリティ機能の設計ができるように，セキュリティレベル評価技術を考案した．また，考案した技術を基にプロトタイプを開発し，IT システムのセキュリティ機能設計に活用できる可能性があることを確認することができた．

今後は，ナレッジ化の構築や，入力インタフェースについての検討を重ねていきたいと考える．

謝辞　本論文は，2012 年 9 月に他界した小泉純氏が，生前に筆者らへ指導してくださった内容を基に作成されたものである．この場をお借りして，小泉氏に謹んでご冥福をお祈りするとともに，本論文を捧げる．

参考文献

1) 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群(平成 24 年度版)」について, http://www.nisc.go.jp/active/general/kijun24.html
2) Payment Card Industry Security Standards Council: PCI SSC Data Security Standards, https://www.pcisecuritystandards.org/security_standards/
3) 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

Vol.2013-DPS-154 No.35
Vol.2013-CSEC-60 No.35
2013/3/15

ティ対策のための統一規範,
http://www.nisc.go.jp/active/general/pdf/kihan24.pdf
4) 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技術基準(平成 24 年度版),
http://www.nisc.go.jp/active/general/pdf/k305-111.pdf
5) 中塩 慎一: ゼロから学ぶアーキテクチャ設計, IT アーキテクトのためのシステム設計完全ガイド 2008, 日経 BP, pp.54-59 (2007).
6) 大西 克美: できるエンジニアのセキュリティチェックポイント, プロジェクトを成功に導くシステム開発のスキルアップ教本, 日経 BP ムック, pp.100-113 (2007).
7) 高橋雄仁, 勅使河原可海: 国際標準の参照関係に基づくセキュリティ評価方式における非専門家への対応策提示機能の検討, DICOMO 2011, pp.127-134 (2011).
8) Nessus, http://www.tenable.com/products/nessus
9) Metasploit, http://www.metasploit.com/
10) MITRE: Common Vulnerabilities and Exposures (CVE), http://cve.mitre.org/