セキュリティ構築方法論とその支援ツール

Security Design Methodology and Its Support Tool

秋山　浩一郎　　鬼頭　利之　　梅澤　健太郎
■AKIYAMA Koichiro　■KITO Toshiyuki　■UMESAWA Kentaro

ネットワークの発達に伴って情報システムが格段に便利になったが，その反面でシステムへの不正侵入やウィルスによるシステム障害などが後を絶たず，現代社会における一つの脅威となっている。

東芝は，これらの脅威に対して網羅的に防御可能な情報システムを構築するため，構築の段階で必要となる手続きをまとめたセキュリティ構築方法論を策定し，これを効率的に実施するための支援ツールを完成させた。

While the expanding network creates great convenience in the realm of information systems, network-caused security incidents such as virus attacks are constantly occurring. This is becoming a major threat in people's lives.

In response to this situation, Toshiba has formulated a security design methodology that shows the necessary steps in system design in order to comprehensively avoid such threats. We have also developed a system integrator support tool for efficient design of the target system.

1 まえがき

情報の電子化とネットワークの発達によって，情報システムが格段に便利になった。しかし，その一方で不正侵入やウィルス被害に代表されるようなセキュリティ事件の多発化，深刻化により，ネットワーク社会全体が脅威にさらされている。このような状況の下，情報システムの安全性を客観的に評価するための国際セキュリティ標準ISO/IEC 15408（国際標準化機構／国際電気標準会議規格15408）が策定された。

ISO/IEC 15408はCC（Common Criteria）とも呼ばれ，セキュリティを評価するための書式と手順を定めている。すなわち，ISO/IEC 15408では文書によって，評価の対象となる情報システムで守るべき資産（保護資産）とそれに対する脅威を明確にし，回避すべき脅威には適切な対策の実施を明示することが求められている。更に，これを第三者である評価機関が客観的な評価を行い，認証機関がこの評価が適正であることを認証することにより，その安全性が認証される。

一方で，評価の対象となる情報システムを分析し，安全なセキュリティ機能を作り込む設計技法に関しては，現在でも設計者の経験やセキュリティに関する知識に大きく依存している。このため，漏れのないセキュリティを構築するには，相当な経験と専門知識が必要となっている。東芝はこのような状況から，セキュリティ構築経験のある技術者のノウハウを形式知化することにより，セキュリティ構築の際に実施すべき手続きをまとめたセキュリティ構築方法論を策定した。また，この方法論を実践する際の作業効率化のために，支援ツールも開発したので併せて紹介する。

2 セキュリティ構築方法論の考え方

セキュリティ構築方法論の概要を**図1**に示す。

セキュリティ構築方法論によるシステム設計は，セキュリティ機能を除く外部仕様が決定された段階からスタートする。初めに，決められた外部仕様をセキュリティの観点から分析する（初期システム構成）。次に，システムの保護資産を決定し，初期システム構成で分析された結果に基づいて，個々の保護資産に関して存在する脅威を網羅的に洗い出す（保護資産洗出し，脅威分析）。更に，ここで洗い出された

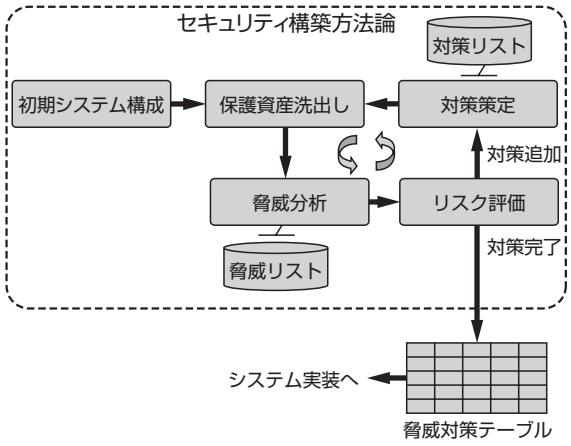


図1．セキュリティ構築方法論の概要 ― 五つの手続きから構成され，これらの手続きを踏むことによって，システムに存在する保護資産とその脅威を網羅的に分析する。

Overview of security design methodology

個々の脅威に関してリスク評価を行い，評価結果を参考にして対策すべき脅威を絞り，対策策定を行う(リスク評価，対策策定)。

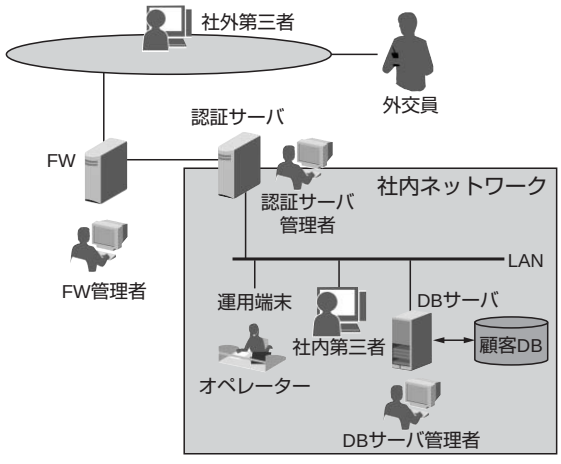
対策することによって新たに生じる保護資産(例えば，本人認証による対策で利用されるパスワードなど)を洗い出し，その脅威を前記の手段で網羅的に洗い出す。このように，保護資産洗出しから対策策定までのフェーズを数回繰り返すことによって，網羅的に安全対策を施した情報システムを構築することができる。更に，ここで得られた脅威と対策に関する対応関係を脅威対策テーブルに整理することにより，ISO/IEC 15408に対応した文書作成の基礎資料としても利用できる。

3 セキュリティ構築方法論

3.1 初期システム構成

このフェーズは，システム外部仕様をセキュリティの観点から分析することを目的としており，次の2ステップからなる。

⑴ システム構成要素と関与者の決定　　システムの外部仕様に基づいて，必要な機器(システム構成要素)とそれらがネットワーク(若しくは配線)でどのようにつながっているかを分析し，システムにかかわる人(関与者)を決定する。顧客管理システムの初期システムの例を**図2**に示す。ここでは，社内のオペレーターと社外の外交員が顧客データベース(DB)へアクセスすることを想定している。



FW：ファイアウォール

図2．初期システム(顧客管理システムの例) ― オペレーターと外交員がそれぞれ社内，社外から，業務上必要となる顧客情報の検索・登録ができるシステムである。社外からのアクセスを正当なものに制限するために，認証サーバやFWの導入を検討している。また，システムの構成要素としては，それを管理する管理者のほか，社内外にはシステムとは直接関係のない第三者も想定しなくてはならない。

Draft design for customer-related data management system

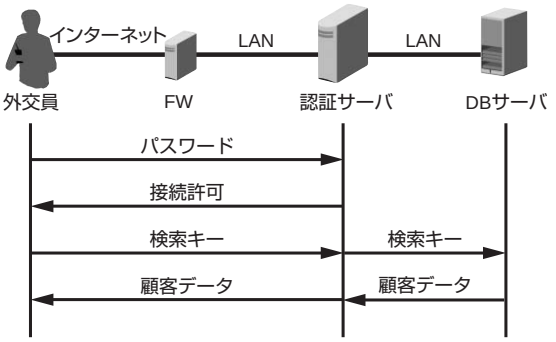


図3．処理フロー(顧客管理システムの例) ― 外交員がインターネットから顧客管理システムにアクセスして顧客情報を検索する場合の処理フローである。

Transaction flow for customer-related data search process

⑵ 処理フローの分析　　システムの機能ごとに，前記システムの構成要素とその間のネットワークをデータがどのように流れるかを分析する。顧客管理システムの検索処理における処理フローの例を**図3**に示す。

3.2 保護資産洗出し

保護資産とは，情報資産やシステム構成要素などのシステム資産のうち保護すべきものを言う。顧客管理システムの例では“顧客データ”や“システム可用性”などが保護資産となる。

3.3 脅威分析

ここで脅威とは，保護資産の機密性(秘密にしておくこと)，完全性(かってに変更されないこと)，可用性(利用可能なこと)のいずれかを損なう危険を言う。個々の脅威は“関与者(Who)が，どこ(Where)で，いつ(When)，何のため(Why)に，保護資産(What)に，何をする(How)”のように5W1Hで記述し，脅威対策テーブルにまとめる。脅威分析のポイントはその網羅性である。このためこの方法論では，これまでの構築経験から導き出した脅威事例を脅威リストに抽象化してDB化しており，この脅威リストを利用して，**図4**と以下に示す方法で脅威分析を行う。

まず，処理フロー図(図3)から保護資産，場所，関与者，時の4項目を検索項目として抽出する(①)。図4では保護資産＝顧客データ，場所＝LAN，関与者＝社内第三者，時＝登録時のように抽出されている。これらの項目を脅威リストに記載されていることば(キーワード)に置き換える(②)。この後，これらキーワードに合致した攻撃方法を脅威リストから抽出する(③)。更に，システム特有の脅威を付加(④)した後，これらの導出された脅威から可能性のある脅威に絞り込む(⑤)。

3.4 リスク評価

リスク評価では，脅威が導出された原因にさかのぼって分析できる，フォールトツリー分析に基づいて分析を行う。これにより，脅威分析で列挙された個々の脅威に対して，それ

が顕在化した場合のリスクを定量評価し，対策要否の参考となる評価値を算出する。分析者はこの評価値を参考にして，その脅威に対して対策が必要な場合は対策策定フェーズに移行する。一方，対策が必要となる脅威が出現しなくなった時点でセキュリティ構築は終了となる。

3.5 対策策定

対策が必要な脅威に対して具体的な対策を策定する。ここで，対策すべき脅威が脅威リストに掲載されている場合は，その脅威に対応する対策リストの項目を参照して選択できる。一方，脅威リストに掲載されていない脅威の場合は，対策を分析者自身が考案するか，セキュリティの専門家に策定してもらう必要がある。

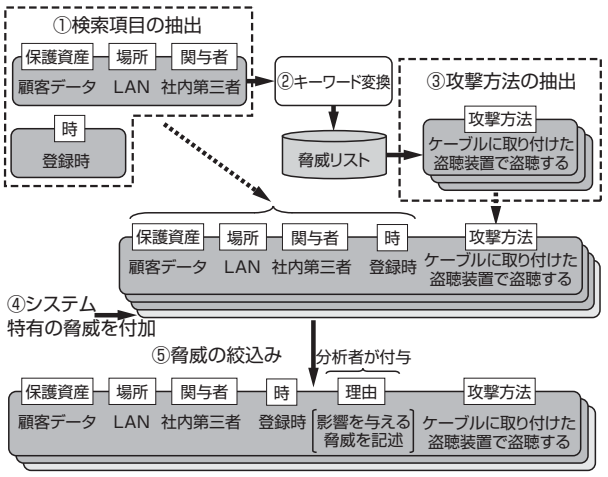


図4．脅威分析の流れ（顧客管理システムの例）— 処理フロー上に現れた保護資産に対応する脅威を，脅威リストを利用して網羅的に洗い出す。

Threat analysis procedure

4 セキュリティ構築支援ツール

セキュリティ構築方法論に基づいた分析では，分析者は分析対象システムが持っているすべての機能に対して，処理フローを決定する。更に，その処理フローに存在する保護資産，場所，関与者，時の組合せごとに，脅威リストを利用してもれなく脅威を抽出し，記録しなくてはならない。この一連の作業は，分析者にとって相当な負担となる。そこで，それを軽減するため分析を支援するセキュリティ構築支援ツールを作成した。ここでは，このツールを用いた分析例を紹介する。

システムの関与者と保護資産を登録する画面例を**図5**に示す。この画面は初期システム構成及び保護資産洗出しのフェーズで利用される。画面左の関与者リストには，初期システム構成で導出された関与者をその信頼度（5段階）とともに記録する。信頼度は関与者のこのシステムに対する信頼性のレベルを示す指標で，脅威分析で脅威を絞り込むときやリスク評価の際に利用される。

図5では，顧客管理システム（図2）を例に取って，DBサーバ管理者など業務契約関係にある関与者にもっとも高い信頼度5を，社外第三者などシステムと直接責任関係のない関与者にもっとも低い信頼度1を付与している。更に，画面右の保護資産リストには，処理フロー図から抽出された保護資産とその価値（脅威が発生した際の被害規模に相当）が表示される。

脅威分析の画面例を**図6**に示す。脅威分析は，処理フロー図を利用して検索項目（保護資産，場所，関与者，時）を抽出することから始める。分析者はここで抽出された検索項目を画面最上部の各フィールドに入力する。次に“キー

図5．関与者・保護資産登録の画面（顧客管理システムの例）— 初期システムで洗い出されたシステム関与者と，保護資産洗出しで認識された保護資産を登録する。

Participants/assets registration display

図6．脅威分析の画面（顧客管理システムの例）— 脅威リストを利用して脅威分析を行う。
Threat analysis display

ワード変換”のフィールドにおいて，プルダウンメニューを利用し，脅威リストに登録されているキーワードに変換する。キーワード変換後，脅威検索ボタンを押すことにより，検索項目のキーワードに合致する脅威が脅威リストから抽出され，画面中央に表示される。

次に表示された脅威の中から可能性のある脅威をクリックにより選択し，脅威対策テーブル登録ボタンを押すことにより脅威対策テーブルに登録する。ここで，当該検索項目における脅威リストにないシステム特有の脅威は画面下部の脅威対策テーブル登録フィールドを用いて登録する。

脅威分析が終了すると，脅威対策テーブルに登録されたそれぞれの脅威に対して，脅威どうしの因果関係にまで配慮したリスク評価を実施する。続いてリスク評価の結果を参考にし，対策が必要な脅威に対し対策リストを用いて対策を選択する。選択された対策によって新たな保護資産が生じる場合は，これを関与者・保護資産登録画面（図5）で登録する。なお，対策リストにはその対策から生じる新たな保護資産候補が記載されており，この支援ツールはそれら候補を表示し，そこから保護対象すべき保護資産を選択する方法で保護資産リストに付加することができる。

また，脅威対策テーブルなどの分析結果をCSV（Comma Separated Value）ファイルに保存し，他の市販ソフトウェアなどで編集して，その結果を再度読み込むことができる。このため，システムの分析を複数人で分担して結果をまとめることが可能である。また，類似システムの開発など過去の分析結果を流用する際にも，保存された脅威対策テーブルは有効である。

以上のように，この支援ツールによって，構築者の作業を軽減し，構築者が脅威リストや対策リストを効果的に利用して網羅的な分析ができる環境が提供できた。

5 あとがき

当社は，情報システムにセキュリティを作り込む手続きをまとめたセキュリティ構築方法論を策定し，その支援ツールを開発した。この方法論に則してシステム構築を行うことで，脅威を組織的かつ網羅的に挙げることができ，漏れのないセキュリティが実現できる。また，構築結果は脅威対策テーブルにまとめられ，ISO/IEC 15408の評価文書作成の際の基礎資料として利用することもできる。更に，開発した支援ツールによって構築者の作業効率を高めることもできる。現在，当社では，一部の製品の開発にこの方法論を用いたセキュリティ構築と分析を実施している。

文　献

(1) 小田原育也，ほか．セキュアシステムインテグレーション．東芝レビュー．**58**，8，2003，p.11－14.


秋山　浩一郎　AKIYAMA Koichiro
研究開発センター　コンピュータ・ネットワークラボラトリー　主任研究員。セキュリティ技術の研究・開発に従事。電子情報通信学会会員。
Computer & Network Systems Lab.


鬼頭　利之　KITO Toshiyuki
研究開発センター　コンピュータ・ネットワークラボラトリー。セキュリティ技術の研究・開発に従事。電子情報通信学会会員。
Computer & Network Systems Lab.


梅澤　健太郎　UMESAWA Kentaro
研究開発センター　コンピュータ・ネットワークラボラトリー。システムセキュリティの研究・開発に従事。情報処理学会会員。
Computer & Network Systems Lab.