O-021

セキュリティ機能の設計手法とその支援ツールの実装
The method for security design and its support tool

鬼頭　利之 *　秋山　浩一郎 *　小島　健司 †　梅澤　健太郎 *
KITO Toshiyuki　AKIYAMA Koichiro　KOJIMA Kenji　UMESAWA Kentaro

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りつつある．その一方で，情報システムのセキュリティインシデントの多発化，深刻化により多大な損害をもたらしている．このような状況を反映し，国際セキュリティ標準（ISO/IEC 17799[1], ISO/IEC 15408[2] など）が策定されるなど，情報資産（保護資産）やシステムに対する脅威を的確に把握し，避けるべき脅威には適切な対策を実施し，かつそれを第 3 者によって保証されることが必要となってきた．

しかしながら，情報システムにセキュリティ機能を作りこむ設計技法は設計者の設計経験やセキュリティの知識に大きく依存し，経験やセキュリティの専門知識が十分ではない設計者には容易に行うことができない．そのため，設計技法を体系的・容易に実現する設計手法が求められるようになっている．

そこで，本論文では，保護資産・脅威・対策の関係を把握・蓄積でき，設計者の設計経験やセキュリティの知識に依存しない設計手法を提案する．また，設計者が本設計手法を実施する際に，必要となる支援ツールを作成したので，併せて報告する．

2. 提案設計手法

2.1 概　要

提案設計手法 (図 1 上) は，システムの概要を整理する論理設計段階と，論理設計段階において整理したシステムの概要に沿ってセキュリティ機能を作り込んでいくシステム設計段階の 2 段階から構成され，これらを通じて保護資産・脅威・対策の関係を木構造により表す ACT ツリーを作成する：

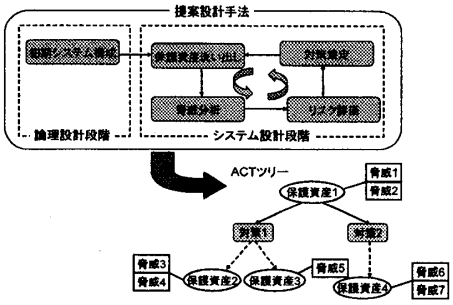

図 1: 提案設計手法の全体図

論理設計段階では，初期システム構成のフェーズにおいてシステムを構成する要素やデータの流れをセキュリティの観点で整理する．システム設計段階では，システムにおいて保護すべき対象となる保護資産を洗い出す保護資産の洗い出しと，その保護資産に対する脅威をすべて導出する脅威分析，各脅威に対してリスク分析・評価を行うリスク評価，脅威に対する対策を決定する対策策定といった 4 つのフェーズをこの順で繰り返す．

また，本設計手法を適用することにより生成される ACT ツリー (図 1 下) は，保護資産を親ノード，その保護資産を保護する対策を子ノード，対策によって導出される保護資産を孫ノードというように続き，さらに，各保護資産に関連する脅威をその保護資産と対応付けることによって形成される．これにより分析結果を体系的にまとめ，セキュリティ設計の論理関係を把握し，保護資産・脅威・対策の関係をセキュリティ設計ノウハウとして蓄積することができる．

2.2 論理設計段階

論理設計段階の初期システム構成のフェーズでは，システムの概要を確認するために以下の 2 ステップを行う．

(1)システム構成要素と関与者の決定

システム構成からサーバや運用端末などのシステム構成要素とそれらがどのように接続され，システム内にどのような関与者がいるかを図 2 のように初期システム構成図として洗い出す：

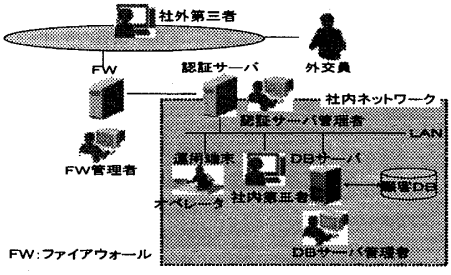

図 2: 初期システム構成図の例

(2)処理フローの決定

システムの処理過程で，システム構成要素中のデータの流れを図 3 のように処理フロー図としてまとめる：

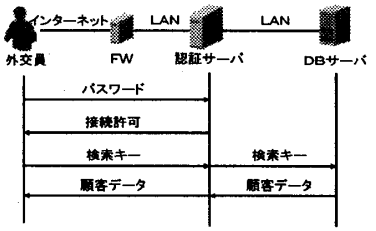

図 3: 処理フロー図の例

2.3 システム設計段階

システム設計段階は，保護資産洗い出し，脅威分析，リスク評価，対策策定の 4 フェーズからなり，一定レベルの安全性が確保できるまでこれらをこの順で繰り返す．

(1)保護資産洗い出し

* （株）東芝　研究開発センター, TOSHIBA Corporation R&D Center
† 東芝ソリューション株式会社, TOSHIBA Solutions Corporation

保護資産は，初期システム構成から初期の保護資産を決定する１次保護資産の決定および対策策定から保護資産を導出されるｎ次保護資産のどちらかによって洗い出される．前者は処理システム構成図，処理フロー図を利用して保護資産を抽出する．例えば，図２，３では，パスワードや顧客データが１次保護資産に当たる．一方，後者は脅威分析とその対策により保護資産を決定する．例えば，脅威に対して暗号化という対策を施した場合は，復号鍵がｎ次保護資産として抽出される．

(2)脅威分析

本設計手法では，脅威を「関与者（Who）がどこにある（Where）保護資産（What）をいつ（When）どのような目的（Whey）でどうする（How）」といった5W1Hの形式で記述する．また，様々な脅威を盛り込んだ脅威リストを作成した：

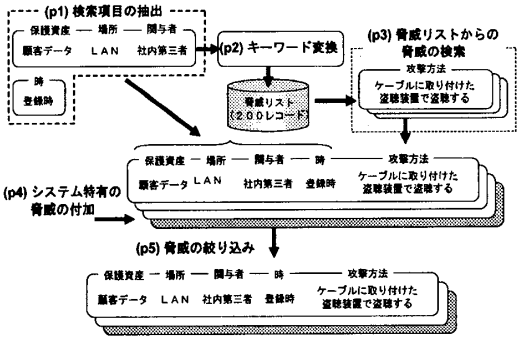

図 4: 脅威分析の流れ

脅威分析では，この脅威リストを利用し，以下の手順により脅威を導出する（図４）：

p1) 検索項目の抽出
p2) キーワード変換
p3) 脅威リストからの脅威の検索
p4) システム特有の脅威の付加
p5) 脅威の絞り込み

まず，処理フロー図から「関与者」,「保護資産」,「(保護資産のある）場所」「時」の４項目の少なくとも１項目を抽出する (p1)．例えば，関与者が社内第三者，保護資産が顧客データ，場所がLAN，時が登録時という項目が抽出されたとする．これらの項目を脅威リストに記載されている言葉に置き換える (p2)．この後，これらの言葉によって攻撃方法を脅威リストから抽出する (p3)．本例では,「ケーブルに取り付けた盗聴装置で盗聴する」という攻撃方法などが抽出されている．さらに，システム特有の脅威を付加し (p4)，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 (p5)．

(3)リスク評価

リスク評価では，脅威が導出された原因に遡って解析するフォールトツリー分析に基づいた分析手法を利用する．これにより，脅威分析で列挙された個々の脅威に対して，脅威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．

この評価値を参考にして，当該脅威に対して対策が必要なら対策策定フェーズに移行する．一方，対策が必要な脅威が出現しなくなった時点で設計終了となる．

(4)対策策定

リスク評価の結果，対策すべきと判断された脅威に対しては対策を決定することになるが，このガイドラインとすべく対策リストを作成した．対策リストは脅威リストに掲載されている各脅威に対応する対策を列挙したもので，暗号化，アクセス制御といった技術対策と「罰則を含む業務規則で禁止する」のような管理対策が含まれている．

さて，脅威に対して何らかの対策が採用された場合，前述のように，その対策によって新たな保護資産が生じることがある．例えば，ある脅威に対して暗号化を行うという対策が適用されたとする．このとき，暗号化された顧客情報を復号する鍵が新たな保護資産として導出され，これを２次保護資産として保護資産洗い出しのフェーズへ戻る．なお，この保護資産は対策リストに対策との対となるよう記録されているため，対策リストより導出することができる．

3. 支援ツールの実装

本設計手法を利用する分析者を支援するツールの実装を試みた．ここでは，一例として，LAN 上の顧客データを登録する際に社内第三者によって引き起こされる脅威（一部）を抽出する際の画面を示す（図５）：

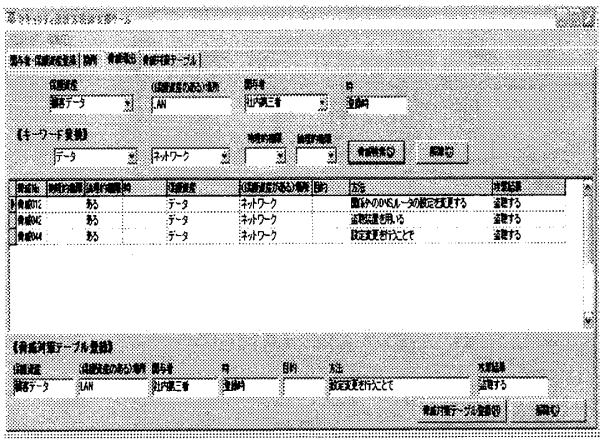

図 5: 支援ツールを利用した脅威分析

4. まとめ

本論文では，情報システムにセキュリティ機能を作りこむ設計手法を提案した．本設計手法により，設計者の経験に依存していた設計手法を形式知化し，ACT ツリーによって設計ノウハウを蓄積することができるようになり，設計経験やセキュリティの知識が十分ではない設計者でも情報システムにセキュリティ機能を作りこむことができるようになった．さらに，本設計手法を実施する際に，設計者の作業を支援するツールを作成した．

参考文献

[1] ISO/IEC 17799：Code of Practice for Information Security Management, 2000.

[2] ISO/IEC 15408：Information Technology - Security techniques - Evaluation criteria for IT security, 1999.