ISO/IEC 15408 に基づくセキュリティターゲット作成支援ツール POSTA の開発

―セキュリティ設計仕様書の雛形を自動生成―

１． 背景

現在，情報システムのセキュリティ機能が正しく設計され，正しく動作するものであることを評価するための制度として，情報セキュリティ評価の国際標準である ISO/IEC 15408 に基づく IT セキュリティ評価制度が世界的に実施されている．この制度においては，システム本体と，その設計仕様書であるセキュリティターゲット（ST)，情報システムが ST の記述通りに設計されていることを示す証拠資料に対して，評価機関が ISO/IEC 15408 に基づき設計仕様を評価し，認証機関がその評価結果を受けてその情報システムが安全なものであると認証し，認証された ST を公開している．認証を得たシステムは，ISO/IEC 15408 を満たすセキュリティを備えているということができる．

しかし，ISO/IEC 15408 による認証を取得するためには，設計したいシステムの設計仕様を一から定義しなければならず，セキュリティ機能に関する豊富な知識を持つ設計者が必要である．また，システムの設計から ST の作成までを含めて数千万円の費用や半年の時間が必要となることもある．

このような現状を受けて，経験の少ない設計者でも，高い安全性を備えた情報システムの設計および ST 作成を簡単に行えるようにすることが求められている．これにより，セキュリティ機能を一から設計できるだけの経験や知識を持った設計者がいなくても，セキュリティ機能を設計することができる．また，システムを開発している企業にとっては設計コストの削減と開発サイクルの効率化による利益の増大が期待される．

２． 目的

本プロジェクトの目的は， セキュリティ機能の設計者が情報システムのセキュリティ機能を設計するとき，高い安全性を備えた情報システムの ST を簡単に作成できるように支援することである．この目的を達成するために本プロジェクトでは，公開されている ISO/IEC 15408 認証取得済み ST を元にして，ST の雛形を自動生成するツール POSTA を開発する．

３．　開発の内容

本プロジェクトにおいて開発した POSTA は，利用者が入力したシステムのキーワードに対して，そのシステムの ST の雛形を自動生成するツールである．セキュリティ機能の設計者は，設計しようとしているシステムのキーワードを入力するだけで雛形を簡単に生成することができる．この雛形はプログラムによって機械的に生成されたものであるので，人間の手による確認および修正が必要となるものの，設計者はこの雛形を叩き台として修正するだけで対象システムの ST を作成することができる．これにより，セキュリティ機能の設計全体に必要な時間と費用は大きく削減される．また，設計者は最低限キーワードの選定と雛形の修正を行うことができる能力を持っていれば，ST を作成することができる．また，POSTA は Web 上で公開されており，利用者はいつでも，どこからでも Web ブラウザを通して POSTA を利用することができる．

具体的には，POSTA は「ST 管理機能」「類似システム判定機能」「設計仕様品質保持機能」「設計仕様整形機能」の四つの機能から構成される．四つの機能に基づく POSTA の内部処理の流れを図１に示す．

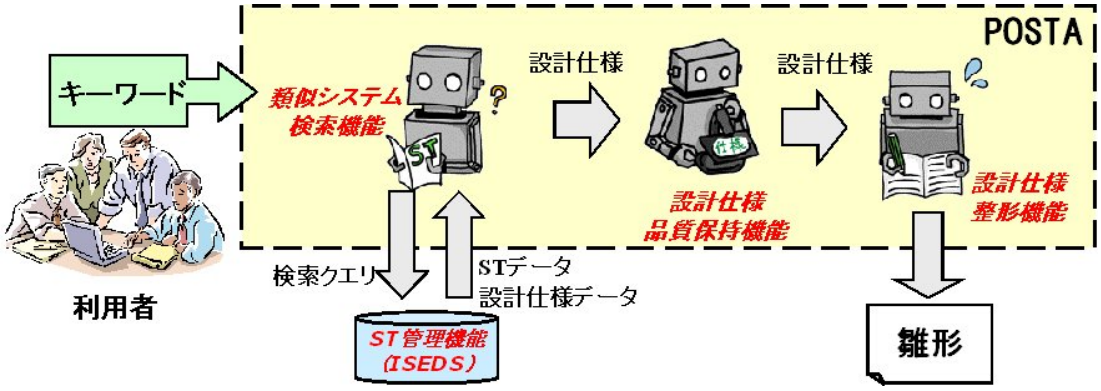

図１：POSTA の各機能と内部処理

まず POSTA は，利用者が入力したシステムのキーワードに基づき，ST 管理機能を用いて予め管理している ISO/IEC 15408 認証取得済み ST の中から，類似システム検索機能によって設計したい情報システムと類似する情報システムの ST を探し出し，探し出された ST に記述されている設計仕様を用いて新たな ST の雛形を生成する．この際，採用された ST が複数存在する場合は，それらの設計仕様間に不整合が存在する場合があるため，設計仕様品質保持機能によって不整合を除去する．最後に，設計仕様整形機能によって設計仕様を ST の形式に整形して出力する．

POSTA による雛形生成の特徴としては，以下の三つの点が挙げられる．

・ISO/IEC 15408，CEM 3.1，IEEE 830 に基づく高い安全性を備えた雛形を生成できる

・ST 用に調整されたアルゴリズムを用いて適切な雛形を生成できる

・キーワードを入力するだけで簡単に雛形を生成できる

図２は，POSTA のインタフェイスの一部と，POSTA によって出力された雛形の例である．現在 POSTA の試用版を以下の URL にて公開している

http://iseds.aise.ics.saitama-u.ac.jp/posta/

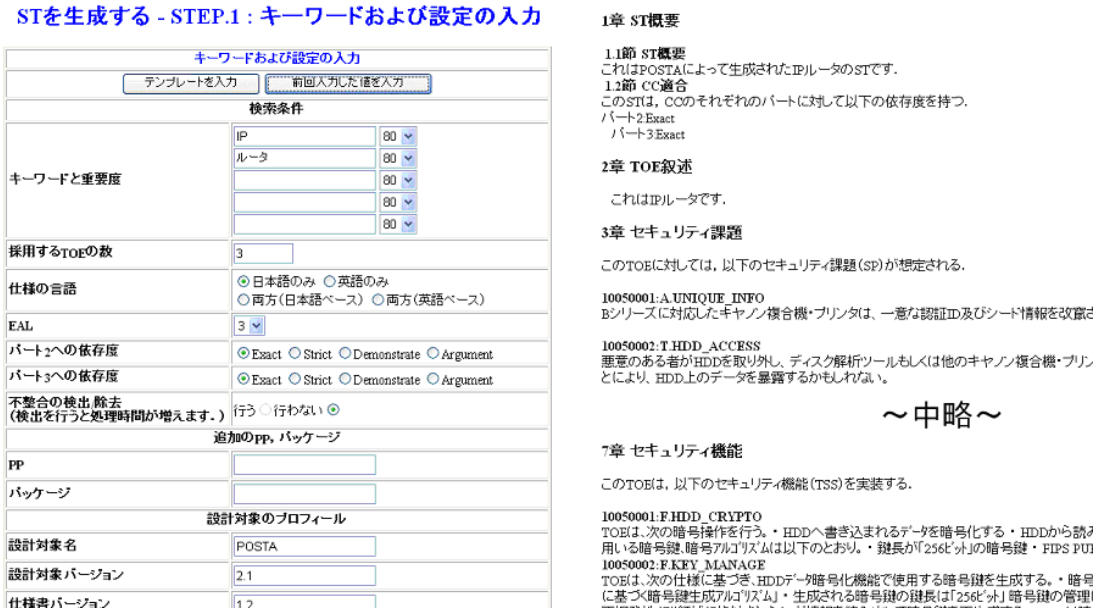

図２：POSTA のインタフェイス（左）と生成された雛形の例（右）

４． 従来の技術（または機能）との相違

POSTA は，キーワードを入力するだけで ST としての必須条件を満たす雛形を生成することができ，従来のセキュリティ機能の設計支援ツールや ST 作成支援ツールに比べ，工程を広範囲に自動化するツールであり，情報システムのセキュリティに関する設計仕様書の雛形を自動生成する世界初のツールである．

５． 期待される効果

POSTA は，ソフトウェアにおけるセキュリティ機能開発活動に対して，以下の波及効果を与える．

POSTA によって生成される雛形は，少なくとも ISO/IEC 15408 を満たすセキュリティを備えていると言える．これにより，POSTA を用いて開発した製品の安全性を消費者にアピールすることができる．

POSTA は，雛形の自動生成を行うことによりセキュリティ機能の設計に必要な労力を大幅に削減させることができる．ST を簡単に作成できるようにすることで，ISO/IEC 15408 の認証申請を従来よりも簡単に行うことができ，中小企業にとって高いものであった ISO/IEC 15408 認証取得の敷居を下げることが見込まれる．ISO/IEC 15408 の認証を取得するシステムが

増えれば，人々にとってより安心な社会の実現に貢献することが期待される．

また，情報システムの保守においては，一度受けた攻撃に対してすぐにセキュリティ機能を設計し直し，脆弱性を解消する必要がある．これに対し，POSTA は，セキュリティ機能の設計に必要な時間を削減することができる．よって，POSTA はセキュリティ機能の保守における迅速な再設計を支援することができる．

６．　普及（または活用）の見通し

POSTA の利用者としては，ソフトウェアにおけるセキュリティ機能の設計者を想定している．普及の見通しには，ISO/IEC 15408 自体の普及が大きく関係する．現在，日本における ISO/IEC 15408 の認証取得システムは 150 を超え，更に年間 60 件以上ものシステムが認証されている．また，諸外国においても認証取得済みシステムは 800 を超え，年々認証されるシステム数は増加する傾向にある．今後 ISO/IEC 15408 が普及し，一般的なシステムでも認証を取得するようになれば，世界中のセキュリティ設計者が POSTA の利用者として想定される．

７．　開発者名（所属）

堀江大輔（埼玉大学 大学院理工学研究科 先端情報システム工学研究室）

関連 URL：http://iseds.aise.ics.saitama-u.ac.jp/posta/