車載通信システム向けサイバーセキュリティ対策立案手法の提案

山内知奈津[1]　河内尚[1]　安藤英里子[1]

概要： デジタル技術の活用が進む車載通信システムは，様々なユースケースや機器による複雑な構成のため，サイバーセキュリティ対策が必要十分に対策立案されているか把握することが難しいという課題と，必要十分な対策を設計実装するには既存以上の開発工数を要するという課題がある．本研究では，ユースケースとシステム構成を包含する対象システムを定義し，IEC62443 のセキュリティ要件に沿った対策 DB を整備して，対策 DB と連携したセキュリティ設計自動化技術を開発した．その結果，セキュリティ機能の設計工数を従来比 1/10 の工数（従来：6 カ月→3 週間）に短縮した．

Proposal of Method to Create Cyber-security Countermeasures for In-vehicle Communication System

CHINATSU YAMAUCHI[1]　TAKASHI KAWAUCHI[1]　ERIKO ANDO[1]

1. はじめに

近年，自動車や鉄道車両といった車載機器の分野では，メンテナンスの効率化や運行管理の高度化を目ざし，運用データをセンタと通信して取得・分析するサービスおよびシステムの開発が進んでいる．このような車載通信システムは，車載機器と運用データを外部に設けたセンタとで構成される．一方で，車載通信システムにおける一般通信回線の利用は,サイバー攻撃の攻撃対象となる危険性が伴う．従来の IT 分野と同様のサイバー攻撃事例が報告されるようになり，サービスに影響がでる事例も報告されるようになってきた．そのため，通信サービスを利用するシステムや機器の発注条件にセキュリティ設計と対策の実施が求められるようになってきている．それに伴いシステム開発現場では，多種多様な車載機器に対応させるセキュリティ設計の工数増加と短納期化が課題となっている．

本研究では，車載通信システムに対して実施するセキュリティ設計において,「対策立案を必要十分に立案する」「分析，対策立案にかかる工数」という 2 点の課題を解決し，想定されるセキュリティ上の脅威の明確化と，設計者のノウハウによらない対策立案を実現するセキュリティ設計手法を提案する．

2. セキュリティ対策手法の提案

2.1 セキュリティ設計の概要

IT 分野においては一般的に，システムの設計，開発に関して ISO/IEC15408 として国際標準化された“セキュリティ評価のためのコモンクライテリア(CC: Common Criteria)”[1][2][3]に基づき，必要なセキュリティ要件定義をおこない，セキュリティ機能を正しく設計，実装，検査する評価枠組みが運用されている．制御システム分野においては，所謂「V 字モデル」に沿った要件分析／定義，アーキテクチャ設計，プログラム設計，プログラム実装，単体／結合テスト，システムテスト，運用テストの認証枠組みが整備されている[4].

脅威分析に基づいて実施されるセキュリティ設計のフローを図 1 に示す．設計フロー①～④の概要を以下に説明する．

図 1　セキュリティ設計フロー

① 評価対象の定義：保護資産を規定し，脅威分析を行う対象システムを明確化する

② セキュリティ課題の定義：リスク分析法を用いて，対策が必要な脅威を抽出し，脅威のリスク評価を行う

③ 対策方針の策定：Fault Tree 解析を用いて脅威の発生要因を分析し，脅威緩和策を立案する

1　(株) 日立製作所　研究開発グループ
Hitachi, Ltd. Research & Development Group

④ 費用対効果の分析：脅威緩和策に基づいて，費用対効果の分析を行い，開発仕様を策定する

これまでに著者らは，セキュリティ設計のノウハウが十分でない評価者でも必要な脅威のリスク評価を適切に実施できることを目的に，設計フローの②を自動化するセキュリティリスク評価ツールを開発した[5][6]. 本稿では③対策方針の策定の自動化に関して報告する．

2.2 課題

セキュリティ設計手法で③においてセキュリティ対策を立案する際には，図 1 の②-1 で抽出された脅威に対し，脅威を発生させる原因を論理的に分析する Fault Tree 解析を実施する．そして Fault Tree 解析の結果をもとに，各脅威事象の発生原因である末端事象（基本事象）に対して，それぞれの末端事象を抑止・予防・検出・回復する対策目標を検討して対策方針を立案する.そして対策方針に対して，具体的なセキュリティ対策を設計する．しかし，設計フロー③を行う際には以下２つの課題がある．

(1) 分析者の知識量と主観に依存しない必要十分な対策立案

Fault Tree 解析は，脅威が発生しうる手順や条件を分析者が想起し，樹状に展開していく手法のため，分析者の知識量や主観に依存し，分析者によって導き出される末端事象が異なってしまう．そのため，ノウハウの少ない分析者が実施すると立案する対策方針の品質（セキュリティ強度）が低くなることや，脅威に対して対策方針の抜け漏れが発生することが起こる．

(2) 脅威に対する対策立案の工数

Fault Tree 解析は，樹状分析であることから末端事象の件数が膨大になりがちである．さらに，対策方針を立案する際に，脅威の異なる末端事象に対して同じ効果が見込める対策方針や，類似の対策方針が存在する．そのため，膨大な末端事象それぞれに対策方針を立案後，重複する対策方針をマージする必要があり，対策方針の立案とマージの作業工数削減が望まれる．

例えば，ある車載器の脅威分析で抽出した脅威項目数は 11385 件であり，手動で脅威分析を実施するには約 30 日の工数，Fault Tree 解析で対策方針を列挙して重複対策方針をマージするには約 15 日の工数，セキュリティ要件の列挙には 10 日の工数が必要であり，合計 60 日(3 ヶ月)の工数を要していた．

3. 対策立案の自動化技術

セキュリティ設計自動化技術の開発では，ユースケースとシステム構成を包含するシステム定義，対策リストの定義，対策リストを活用した対策 DB を整備すると共に，DB 連携 Fault Tree 分析および対策立案自動化技術を実施した．

3.1 ユースケースとシステム構成を包含するシステム定義および対策リスト定義

汎用 IoT システムのユースケースと構成から，車載通信システムとシステムコンポーネントが有する資産および攻撃者を定義した．そして，定義した評価対象（以後，TOE(Target of Evaluation)と呼ぶ）に対して，攻撃者が資産に対して脅威を防止する対策をマッピングし，脅威－対策リストを作成した．さらに，リストアップした脅威－対策リストをマージし，8 種の脅威とそれを防止する 34 種の対策を対応させた脅威－対策リストを定義した（図 2）．

脅威(対策番号)	基本的対策(対策方針)
○機器機器本体上のDoS、権限昇格、なりすまし、漏洩及び改竄(A-2, B-2, C-2, D-2, E-2, F-2, G-2)	ソフトウェアに対するセキュリティパッチの適用
	不必要なサービス・モジュールの停止、削除
	異常動作時の汎用サービスの停止、異常範囲の切断
	アクセス制限により動作可能範囲を限定する
	認証機能の利用（ユーザID/パスワード設定、デフォルト設定の排除、機器認証）
	ログを利用したSOCサービス、IRTサービスによる監視
○機器機器－無線通信網-ネットワーク間における漏洩及び改竄(B-3, C-3, D-3, G-3, B-4, C-4, D-4, G-4)	情報システム安全対策基準（経済産業省）、情報通信ネットワーク安全・信頼性基準（総務省）への対
	通信相手の認証、ホワイトリスト、ブラックリストなどの通信範囲の制限
	外部通信データの暗号化(TLS, SSH等の暗号プロトコル)
	通信路上のデータ暗号化(MEP等の無線通信通信固有の暗号プロトコル)
○リモートサイト内サーバ上での漏洩及び改竄(B-5, C-5, D-5, G-5)	情報システム安全対策基準（経済産業省）、情報通信ネットワーク安全・信頼性基準（総務省）への対
	認証機能の利用(利用時のユーザ認証等)
	保存する情報資産の暗号化機能
	サーバ上の情報へのアクセス管理機能
○なりすまし(A-1, A-5)	人－機器機器間での認証機構のセキュリティ強度の向上
	機器機器－サーバ間での認証機能(電子証明書等)
	外部から受信したデータ異常検知（ハッシュ、チェックサム、センサデータ等の異常監視）
○権限昇格(A-2, A-5)	ソフトウェアに対するセキュリティパッチの適用
	不必要なサービス・モジュールの停止、削除
	認証機能の利用(利用時のユーザ認証等)
	搭載する情報資産の暗号化機能
	暗号鍵情報など本体に保存しなければならない情報を格納する媒体の耐タンパー性確保
	機器機器上の情報へのアクセス管理機能
	書換えデータ異常検知（ハッシュ、チェックサム）
○DoS(A-3, A-4)	外乱に強い通信方式の採用
	短距離通信方式Fの異常検知による機能停止
	USB等の汎用Fの異常検知による機能停止
○否認(A-1)	認証機構のセキュリティ強度向上(バイオメトリクス認証)
○機器機器本体上の漏洩及び改竄(U-1,U-2,V1,V-2,W-1,X-1,E-2,Z-1,A2-1,B2-1,C2-1 -2, B-2,C-2)	認証機能の利用（ユーザID/パスワード設定、デフォルト設定の排除、機器認証）
	搭載する情報資産の暗号化機能
	暗号鍵情報など本体に保存しなければならない情報を格納する媒体の耐タンパー性確保
	機器機器上の情報へのアクセス管理機能
	書換えデータ異常検知（ハッシュ、チェックサム）
	接続情報の漏えい防止策

図 2　脅威－対策リスト

3.2 対策 DB 連携 Fault Tree 解析および対策立案自動化技術

提案するセキュリティ設計手法では CVSS リスク評価および 5W 法による脅威分析を実施する．5W 法では，5W の各項目「攻撃経路」「攻撃者」「攻撃タイミング」「動機」「攻撃方法」の掛け算の結果となる脅威事象を出力する．TOE で起きる脅威事象を脅威分析により作成し，脅威事象すべてに対して，「動機」，「攻撃手段」，「検知可否」を出力する Fault Tree 解析を実施し，脅威が発生する原因事象を出力する（図 3）．

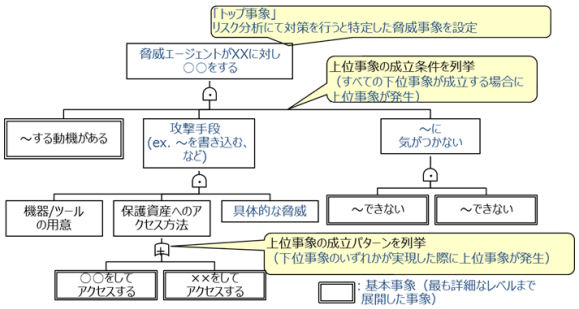

図 3　Fault Tree 解析

本稿では，5W の各項目に対して，「AND」，「OR」，「NOT」

検索を行うテキストエンジンと，エンジンが用いる対策 DB を開発した（図 4）．そして，テキストエンジンは「AND」，「OR」，「NOT」検索条件である登録リンクワードに沿って，FT 事象（トップ事象）と「動機」，「攻撃手段」，「検知可否」を自動で出力し，Fault Tree および構成する原因事象に対して，対策 DB から対策を立案する．立案した Fault Tree の脅威，原因事象，対策の例を図 5 に示す．

	Not			And			Or			Basic event unit	Type of countermeasure	Countermeasure
1							Accidentally			Have a motive to attack	Environment(Non-IT)	OEN_SecurityManual(b-1,c-1)
2							Accidentally				IT	O_LogAnalysis(a-6)
3							Intentionally			Not detection of the attack	IT	O_LogAnalysis(a-6)
4	Using a non-regular interface						device	Using a regular interface		Equipment / tools available	IT	O_ProtectionofConnectionInfo(h-6)
5	Using a non-regular interface						device	Using a regular interface		Equipment / tools available	Environment(Non-IT)	OEN_PromotingNoUnauthorizedManUseTool

図 4　対策 DB

What	リスク値	対策番号	FT基本事象	対策目標	対策種別	セキュリティ対策方針
正規の相手になりすまして改ざんした情報をTOEに送信する。正規の相手になりすまして情報を読み取る	7.3	1	過失によりwhat事象を起こせる製品仕様となっている	過失による行動を防止	環境(Non-IT)	情報システム安全対策基準（経済産業省）、情報通信ネットワーク安全・信頼性基準（総務省）への対応(b-1,c-1)
		2	過失によりwhat事象を起こせる製品仕様となっている	過失による行動を防止	IT	ITを利用したSOCサービス、IRTサービスによる監視(a-6)
		27	機器とセンタ間の通信のプロトコル、メッセージフォーマットが分かっている	通信プロトコルを解読されないようにする	環境(IT)	メッセージ等を最小限に減らし、通信プロトコルの解析が困難になるようにする
		28	機器の保存データが平文である	機器の保尊データを暗号化する	IT	保存する情報資産の暗号化機能(c-3,e-4,h-2)
		29	機器にアクセスできる	操作員を特定する	IT	認証機能の利用(利用時のユーザ認証等)(c-2,e-3)
		36	誤ったバージョンのデータ/プログラムを書き込む	ソフトウェアの環境を最新にしておく	IT	ソフトウェアに対するセキュリティパッチの適用(a-1,e-1)
		37	誤ったバージョンのデータ/プログラムを書き込む	古いソフトウェアのを削除しておく	IT	不必要なサービス・モジュールの停止、削除(a-2,e-2)
		38	不整合な組合せの地データ/プログラムを書き込む	データ/プログラムの組合せが整合している場合のみ書き換えを可能にする	IT	書換えデータ異常検知（ハッシュ、チェックサム)(e-7, h-5)
		39	操作員が確認する手段がない	操作員を確認する	IT	認証機能の利用(利用時のユーザ認証等)(c-2,e-3)
		40	保存する情報が暗号化されていない	保存する情報資産の暗号化機能を実装する。	IT	保存する情報資産の暗号化機能(c-3,e-4,h-2)
		41	異常な機器が検知しない	データ/プログラムを機器が検証する	IT	車載情報機器上の情報へのアクセス管理機能(e-6,h-4)

図 5　脅威に対する対策の立案（一部）

4. 車載通信システムにおける評価結果

本稿では，5 個の機能で構成される車載通信システム TOE を作成し，TOE が保持する 29 個の資産に対して，3 個の IF に接続された不正機器，半導体を想定し，そのシステムに対してセキュリティ設計の対策立案を実施した．

セキュリティ設計の結果，本システムでは 756 件の脅威事象，84 件の対策が一致する脅威事象（マージ結果）が出力された．そして，この 84 件の脅威事象に対して 3.2 節で述べた対策 DB 連携 Fault Tree 解析および対策立案自動化技術を適用した結果，34 種，541 件の対策を立案することができた．

分析項目	結果出力数
脅威事象	756件
脅威事象（マージ後）	84件
対策	541件（34種）

図 6　車載通信システムにおける分析結果

分析結果は，2.2 節の課題に対応する以下の 2 項目で評価した．

(1) 対策立案の必要十分性

手作業で分析した結果と比較した．その結果，本手法で出力した対策の脅威と対策とのマッピングロジックの一貫性を確認するとともに，必要十分な対策が出力されていることを確認した．

(2) 対策立案の工数

想定した車載通信システムと同規模，同種のシステムに対する従来のセキュリティ設計の工数と比較した．従来は，脅威事象項目に対して「動機」，「攻撃手段」，「検知可否」の原因事象項目を作成しマージするのに平均 2 カ月，セキュリティ機能設計時に原因事象項目に対して対策を立案するのに平均 2 カ月がかり，脅威事象項目，原因事象項目，および対策項目をリストアップして関連付け，対策の整合性を確認するまでの作業に合計平均 6 カ月の工数がかかっていた．本手法を適用した結果，脅威分析，FT 解析，セキュリティ設計時の工数を合計 1 日に短縮することができ，セキュリティ設計工数を従来比 1/10 の工数（従来：6 カ月→3 週間）に短縮できた．

5. おわりに

本稿では，想定されるセキュリティ上の脅威の明確化と，設計者のノウハウによらない対策立案を実現するセキュリティ対策立案自動化手法を提案した．そして本手法を適用することにより，必要十分な対策を立案するとともに，セキュリティ設計の工数を従来比 1/10 の工数に短縮できることを確認した．図 7 にセキュリティ設計工数の低減効果を示す．

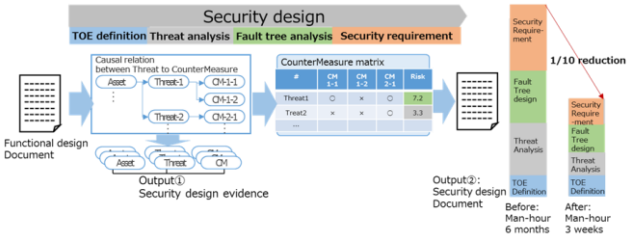

図 7　セキュリティ設計工数の低減効果

参考文献

[1] ISO/IEC 15408-1, Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model, 2009

[2] ISO/IEC 15408-2, Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional components, 2008

[3] ISO/IEC 15408-3, Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance components, 2008

[4] 織茂,津原,山本,佐々木, ”情報システムにおけるセキュリティ対策立案のための計画手法,” 情報処理学会論文誌, Vol.41, No.1, pp.177--187, January 2000.

[5] 安藤英里子，森田伸義，河内尚，萱島信，薦田憲久，藤原融，“車載システム向けセキュリティリスク評価支援システム”，電気学会情報システム研究会，IS-17-031，pp. 17-22，2017 年 5 月

[6] Eriko Ando, Takashi Kawauchi, Norihisa Komoda, and Toru Fujiwara, “Security Risk Assessment Supporting System in Connected Car Systems”, in Proc. of 15th International Conference on Applied Computing, pp.389-394, Oct. 2018.