組込みシステムの定量的なセキュリティリスク評価手法の提案

安藤 英里子† 森田 伸義† 萱島 信†

†日立製作所 横浜研究所
244-0817 神奈川県横浜市戸塚区吉田町 292 番地
{eriko.ando.yf, nobuyoshi.morita.gj, makoto.kayashima.hh}@hitachi.com

あらまし 車載システムをはじめとする組込みシステムのネットワーク化により新たな脅威が現れ，それらに対応するセキュリティ機能が求められている．適切なセキュリティ機能の実現には，脅威のリスク評価に基づいた過不足ないセキュリティ要件の抽出が重要となる．従来のリスク評価手法は，脅威の発生確率など評価者のセキュリティ知識に依存するものが多く，結果が評価者の主観に左右されやすい．そこで，本稿では，発生確率の代わりに攻撃容易性を用いた定量的な手法を提案する．攻撃容易性は，仕様書等に記載される情報を用いて定義することで客観性を持たせる．

A Proposal of the quantitative risk assessment technique in embedded systems

Eriko Ando† Nobuyoshi Morita† Makoto Kayashima†

†Hitachi, Ltd., Yokohama Research Laboratory
292, Yoshida-Cho Totsuka-Ku, Yokohama-Shi, Kanagawa-Ken 224-0817, JAPAN
{eriko.ando.yf, nobuyoshi.morita.gj, makoto.kayashima.hh}@hitachi.com

Abstract Security functions in embedded systems such as automotive systems are necessary, because networking of these systems causes new threats. The extraction of security requirements based on risk assessment is important to implement appropriate security functions. The existing risk assessment techniques are subjective, because they depend on evaluator's knowledge and utilize probability of threats. In this paper, we propose an objective risk assessment technique. This technique utilizes the information described in specification documents to compute the risk values. The risk assessment technique makes it possible to quantify the risk of threats in the target system and to design the security requirements.

1 はじめに

近年，制御システム，情報家電，自動車などの組込みシステムに情報処理システムが利用され，インターネットなど外部ネットワークとつながるようになりつつある[1][2][3]．組込みシステムのネットワーク化に伴い，悪意ある第三者からの攻撃対象となる危険性が出てくる．実際に，外部ネットワークから車載システムを遠隔操作できることが実証され

ている[4]．ECU（Electronic Control Unit）につながる車載システムへの攻撃は人命に関わるため，セキュリティは不可欠である．

既に様々なセキュリティアタックにさらされている IT システムでは，システムの設計，開発，運用にわたり，セキュリティ対策手法が検討されてきた．システムの設計，開発に関しては，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）[5] に基づいて，システムが必要とするセキュリティ要件定義をおこない，システムのセキュリティ機能を正しく設計，実装，検査する対策が実施されている．また，運用に関しては，リリースされたシステムにおいて，後日発覚したセキュリティ問題に対応するために，インシデントレスポンスの仕組み[6]がある．

組込みシステムはITシステムと比較して，現時点では攻撃事例が少なく，対策を経験した人材が少ないことから，セキュリティ設計，開発，運用のそれぞれの対策が十分におこなわれているとは言えない．

そこで本稿では，車載システムを対象とし，セキュリティ設計段階でのセキュリティ要件抽出に必要となるリスク評価手法を提案する。組込みシステムの設計段階におけるリスク評価手法としては，脆弱性評価手法CVSS（Common Vulnerability Scoring System）を応用した定量的なリスク評価手法が提案されている[7]．本稿ではこの手法を車載システム向けに適用した場合について述べる．

第 2 章では，対象となる車載システムとリスク評価の必要性を，第 3 章では，従来のリスク評価手法を車載システムに適用する場合の課題を述べる．第 4 章では CVSS をベースとしたリスク評価手法を車載システム向けに適用した場合について述べる．

2　車載システム

2.1　概要

本稿で対象とする車載システムの構成を図 1 に，機能を表 1 に示す．カーナビにはユーザが入力した目的地までのルートを検索するナビゲーション機能のほかに，スマートフォン経由でテレマティクスセンタからお知らせや ECU への制御データなどを受信し，ユーザや ECU に通知するインポート機能，走行距離などの車両データをテレマティクスセンタに送信するエクスポート機能がある．また，保守端末や SD メモリカードから地図やプログラムを更新する機能もある．カーナビと ECU との通信は CAN(Controller Area Network)を介しておこなわれる．

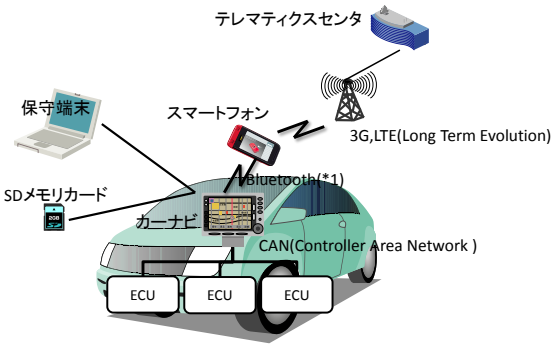

図 1　車載システム

表 1 機能概要

機能	概要
ナビゲーション	地図をもとに目的地までのルートを検索する
インポート	テレマティクスセンタからデータを受信し、ユーザまたは ECU に送る
エクスポート	テレマティクスセンタへデータを送信する
保守機能	地図およびプログラムを更新する

2.2　セキュリティ設計手順

2.1 節で述べたような車載システムにおいて，外部ネットワークから車載システムを遠

隔操作できることが実証されている[4]．車の安全に関わる ECU と連携する車載システムでは，脅威が発生した場合，人命に関わる危険性があり，従来の IT システムよりも被害が大きくなる可能性が高い．したがって，セキュリティ対策は必要である．IT システムにおいて，セキュリティを設計する際には，以下の手順で進める[5]．

(1) システムのモデル化
対象システムと保護資産をモデル化する．

(2) 脅威分析とリスク評価
対象システムに対して発生しうる脅威を分析し，各脅威のリスクを評価する．

(3) 対策目標の立案
脅威分析とリスク評価の結果に基づき，対策する脅威を明確にし，対策目標を決める．

(4) セキュリティ機能要件の選択
ISO/IEC15408 の Part2 [9]に記載されたセキュリティ機能要件集から対策目標の具現化に必要な項目を選択する．

本稿ではセキュリティ設計手順のうち，リスク評価を対象とする．

3 従来のリスク評価手法と課題

ITシステムにおいては，様々なリスク評価の手法がある．表2に主なリスク評価のアプローチを示す[10]．

表 2 リスク評価のアプローチ

アプローチ	概要
ベースライン アプローチ	既存のシステムの基にセキュリティ対策規準を策定し、チェックする
非形式的 アプローチ	専門家の知識や経験を活用してリスク分析をおこなう
詳細リスク分析アプローチ	構造化された解析的手法に基づいて分析をおこなう
組み合わせ アプローチ	ベースラインと詳細リスク分析を組み合わせる

ベースラインアプローチは，ベースとなる既存の組込みシステムの対策基準が見当たらないため，車載システムへの適用は難しい．また，組込みシステム分野の情報セキュリティに関する知識や経験が十分な人材が少ないため，非形式的アプローチも適するとは言えない．詳細リスク分析アプローチは，資産を明確化した上で，「資産価値」，資産に対する「脅威」「脆弱性」でリスク評価するため，評価対象に適合したリスク評価が可能である．詳細リスク分析アプローチに分類される手法の１つに，ETSI TS 102 165-1 [11] があり，組込みシステムに対しても利用が検討されている[12]．ETSIでは，以下のパラメータを用いてリスク値を定義する．

(1) 影響度
「組織への影響度」と「攻撃対象の範囲」の2つのパラメータの組合せで表す．まず，各パラメータを3段階で評価し，その組合せを更に3段階に分類し，1~3の数値で表す．

(2) 攻撃可能性
「攻撃に要する時間」，「攻撃者のスキル」，「知識」，「攻撃の機会」，「必要な装置」の5つのパラメータを用いて表す．各パラメータは表3に示すように区分され，各値の合計値を3段階に分類し，1~3の数値で表す．

それぞれ1~3の数値で表した「影響度」と「攻撃発生可能性」の積でリスク値を求め，リスク値を3段階に分類する．

ETSIのリスク評価では，「資産価値」を「影響度」という指標で，「脅威」「脆弱性」を「攻撃可能性」という指標で評価する．

ETSIのリスク評価を車載システムの設計段階で用いる場合，以下のような課題がある．

(1) 設計段階での評価
「影響度」を構成するパラメータ「組織に対する影響度」は，構築されたシステムを考慮する必要があり，システムを構成する各製品を設計する段階では評価が難しい．

(2) 区分の客観性
「攻撃可能性」を構成するパラメータ「攻

撃に要する時間」は設計段階では客観的評価しにくく，区分結果が評価者に依存する．

そこで，本稿では車載システム向けに，製品の設計段階で決定可能なパラメータを用いた評価者に依存しないリスク評価手法を提案する．

表 3　攻撃可能性のパラメータ

パラメータ	区分	値
攻撃に要する時間	≦day	0
	≦1 week	1
	≦1 month	4
	≦3 month	13
	≦6 month	26
	＞6 month	26以上
攻撃者のスキル	素人で可能	0
	熟練が必要	2
	エキスパートのみ	5
必要な知識	公開情報のみ	0
	制限された情報	1
	センシティブ情報	4
	クリティカル情報	10
攻撃できる機会	不必要/無制限	0
	容易	1
	中間	4
	困難	12
	不可能	12以上
装置	標準品	0
	特製	3
	オーダーメード	7

4　車載システム向けリスク評価手法

4.1　CVSS を拡張したリスク評価手法

第3章で述べた課題に対応する新たなリスク評価手法として，CVSS [8] を応用したリスク評価手法を提案する．CVSSは，米国家インフラストラクチャ諮問委員会（NIAC：National Infrastructure Advisory Council）のプロジェクトが 2004年10月に原案を作成した情報システムの脆弱性に対するオープンで汎用的な評価手法で，ITシステムでは広く利用されている．2005年6月CVSS v1が，2007年6月CVSS v2が公開されている．

CVSSは，実在のソフトウェアやシステムで発覚した脆弱性に対し，そのソフトウェアを利用するシステムの運用管理者が脆弱性対策をいつ実施するか意思決定を行うために利用される．CVSSでは，以下の3つの基準を用いて脆弱性を評価する．

(1) 基本値

脆弱性そのものの特性を評価する基準で，時間の経過や利用環境により評価結果が変化しないものである．基本値は，「AV：攻撃元区分」「AC：攻撃条件の複雑さ」「Au：攻撃前の認証要否」「C：機密性への影響」「I：完全性への影響」「A：可用性への影響」の6つのパラメータより算出する．

(2) 現状値

脆弱性の現在の深刻度を評価する基準で，脆弱性への対応状況に応じ，時間の経過とともに評価結果が変化する．対応状況に関するパラメータは，「E:攻撃される可能性」，「RL：利用可能な対策のレベル」，「RC：脆弱性情報の信頼性」の3項目がある．

(3) 環境値

製品利用者の利用環境も含め，最終的な脆弱性の深刻度を評価する基準で，脆弱性に対して想定される脅威に応じ，製品利用者毎に評価結果は変化する．「CD：二次被害の可能性」，「TD：影響を受ける対象システムの範囲」，「CR：機密性の要求度」，「IR：一貫性の要求度」，「AR：可用性の要求度」の５つのパラメータにより構成される．

CVSS も ETSI と同様に，実在するソフトウェアやシステムで発覚した脆弱性のリスクを評価する指標として開発されたものであり，システム設計時に利用することを想定したものではない．そこで，セキュリティ設計時にCVSS を活用できるようにするため，以下の2 つの要件を付け加える．

(1) 基本値の活用

CVSS の基本値は脆弱性そのものの特性を評価する基準であり，対象システムの設

計に起因する基本的なパラメータで評価する．一方，現状値および環境値は，脆弱性が発生した時点での深刻度を評価する規準であり，システム設計段階では評価できない．そこで，CVSS の基本値を活用し，リスク値として算出する．

基本値の各パラメータは，表 4 に示すように数値が割当てられており，以下の算出式から基本値を算出する．

$$\text{基本値} = ((0.6\times\text{影響度}) + (0.4\times\text{攻撃容易性}) - 1.5) \times f(\text{影響度})$$

$$\text{攻撃容易性} = 20\times AV\times AC\times Au$$

$$\text{影響度} = 10.41\times(1-(1-C)\times(1-I)\times(1-A))$$

$$f(\text{影響度}) = \begin{cases} 0 & (\text{影響度が } 0) \\ 1.176 & (\text{影響度が } 0 \text{ 以外}) \end{cases}$$

表 4　CVSS 基本値のパラメータ

パラメータ	区分	値
AV ：攻撃元区分	ローカル	0.395
	隣接	0.646
	ネットワーク	1.0
AC ：攻撃条件の複雑さ	高	0.35
	中	0.61
	低	0.71
Au ：攻撃前の認証要否	複数	0.45
	単一	0.56
	不要	0.704
C ：機密性への影響	なし	0.0
	部分的	0.275
	全面的	0.660
I ：完全性への影響	なし	0.0
	部分的	0.275
	全面的	0.660
A ：可用性への影響	なし	0.0
	部分的	0.275
	全面的	0.660

(2) パラメータ区分解釈の明示化

評価者によってパラメータの区分結果が変わらないように定義する必要がある．パラメータ区分の解釈は対象システムによって変わる可能性があり，本稿では車載システム向けに定義する．

4.2　車載システム向けパラメータ区分

4.2.1　前提条件

セキュリティ設計に入る前にシステム設計書は準備されているものとする．また，2.2 節で示したセキュリティ設計手順で，システムのモデル化と脅威分析は実施済みとする．その結果，システムのモデル図と脅威一覧表が存在するものとする．

4.2.2　システムのモデル図と脅威一覧表の定義

評価者がリスク評価のパラメータ区分を決定しやすいように，システムモデル図と脅威一覧表を定義する．

(1) システムのモデル図

システムのモデル図はシステム設計書をもとに作成する．まず，システムを構成するモジュールと関与人物を抽出し，各モジュール間または関与人物とのインタフェースとデータの流れを明確化する．これは，パラメータ「AC：攻撃の複雑さ」「Au：認証の要否」を客観的に評価するためである．詳細は 4.2.3 項で述べる．第 2 章の車載システムのモデル図を図 2 に示す．

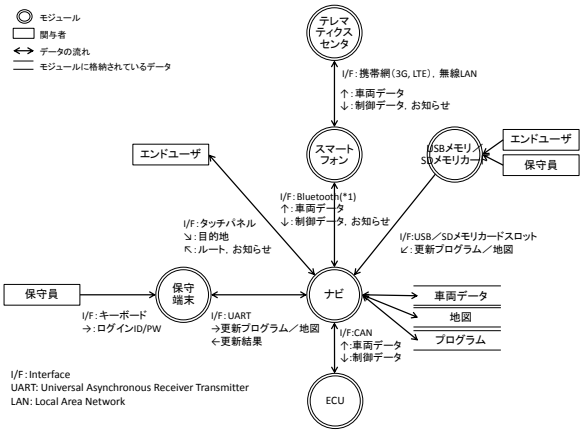

図 2　システムモデル図

(2) 脅威一覧表

脅威分析手法は本稿の対象外だが，抽出された脅威は，「情報資産」「攻撃経路」

「攻撃者」「脅威事象」が明確に分かるように記載する．これは，「AV：攻撃元区分」「Au：認証の要否」「C：機密性への影響度」「I：完全性への影響度」「A：可用性への影響度」を客観的に評価するためである．詳細は 4.2.3 項で述べる．第 2 章の車載システムの脅威の一例を表 5 に示す．

表 5 脅威一覧表の例

脅威 No.	資産	攻撃経路	攻撃者	攻撃タイミング	動機	脅威事象
1	制御データ	3G/LTE	第三者	定常利用時	故意	テレマティクスセンタになりすまし，不正な制御データをECUに送る
2	目的地／ルート	Bluetooth	第三者	定常利用時	故意	スマートフォン経由でカーナビにウィルスを送り，目的地／ルートを漏洩させる
3	地図	UART	保守員	保守時	過失	保守端末経由で古いバージョンの地図を更新する
	…	…	…	…	…	…

4.2.3 パラメータ区分の定義

車載システム向けに，パラメータ区分を定義する．

(1) 攻撃元区分

本パラメータは攻撃対象の資産に対して，どの経路で攻撃がおこなわれるかを評価する（表 6）．したがって，脅威一覧表の攻撃経路からどの区分に該当するかを客観的に判断できる．

表 6 攻撃元区分の定義

区分	定義
ローカル	対象資産への物理的アクセスが必要 例）USB メモリ，SD メモリカード，UART，カーナビのタッチパネル，CAN
隣接	対象資産があるモジュールの近くへの接近が必要　例）Bluetooth(*1)
ネットワーク	対象資産があるモジュールへの接近不要 例）3G, LTE

(2) 攻撃条件の複雑さ

攻撃者から対象資産までのモジュール数で攻撃条件の複雑さを評価する（表 7）．本パラメータは攻撃者から資産が存在するモジュールまでのモジュール数をシステムモデル図から数えることでわかるため，評価者の主観には依存しない．例えば，表 4-2 の脅威 No.1 の場合，テレマティクスセンタ, スマートフォン, カーナビ, ECU と 4 つのモジュールを経由するため，区分は高となる．

表 7 攻撃条件の複雑さ区分の定義

区分	定義
高	対象資産までのモジュール数が 3 つ以上
中	対象資産までのモジュール数が 2 つ
低	対象資産までのモジュール数が 1 つ

(3) 攻撃前の認証要否

本パラメータは攻撃する前に発生する認証回数で評価する（表 8）．これはシステムのモデル図と脅威一覧表の攻撃者および脅威事象から客観的に評価できる．例えば，図 2 のモデル図を見ると，保守端末にはログイン認証があることが分かる．したがって，保守端末を使う脅威事象の場合，認証回数は 1 回となる．ただし，攻撃者が保守員の場合はログイン権限があるため，認証回数は 0 回となる．

表 8 攻撃前の認証要否区分の定義

区分	定義
複数	脅威発生までに認証が 2 回以上発生する
単一	脅威発生までに認証が 1 回発生する
不要	脅威発生までに認証が発生しない

(4) 機密性，完全性，可用性への影響度

本パラメータは脅威一覧表の「情報資産」と「脅威事象」から評価する．

車載システムにおいて，機密性が求められる情報資産は「プライバシー情報」と「知的財産」に分類される．車載システムは自社／他社の知的財産が存在するため，表 9 に示すように定義する．

完全性と可用性への影響度は ASIL（Automotive Safety Integrity Level）を活用する．ASIL は自動車の安全水準レベルを規定するものであり，危害度（S：Severity），曝露確率（E：Exposure），

制御可能性（C：Controllability）の 3 つのパラメータの組合せから QM，A~D の 5 段階で評価される．QM は通常の品質管理レベルが求められ，A~D では D が最も高い安全レベルが求められる．そこで，表 10 に示すように完全性と可用性を定義する．完全性と可用性に同じ区分を用いることで，機密性以上に，安全に影響を及ぼすものはリスク値として高い値を示すようになる．

表 9　機密性への影響度区分の定義

区分	定義
なし	機密性がない資産
部分的	自社の知的財産
全面的	プライバシー情報，他社の知的財産

表 10　完全性，可用性への影響度区分の定義

区分	定義
なし	ASIL QM に該当する資産
部分的	ASIL A,B に該当する資産
全面的	ASIL C,D に該当する資産

4.3　従来手法との比較

4.2 節で示すとおり，本稿で適用した手法は，車載システム向けにパラメータ区分を定義し，システムのモデル図および脅威一覧表から明確に評価できるものであり，従来の ETSI のリスク評価手法より設計段階で客観的なリスク値を求めることが可能になる．

本稿で提案した手法は，「影響度」「攻撃容易性」の指標でリスク値を求めている一方，詳細リスク分析アプローチは「影響」「脅威」「脆弱性」でリスク評価する手法である．本手法の「攻撃容易性」では，「AV：攻撃元区分」と「AC：攻撃条件の複雑さ」が脅威を，「AC：攻撃条件の複雑さ」「Au：攻撃前の認証要否」が脆弱性を表すと解釈でき，これも ETSI の手法と同様に詳細リスク分析アプローチの１つと言え，定量的な評価が可能な手法であると言える．

5　まとめと今後の課題

本稿では，車載システムの設計におけるセキュリティ対策を向上させるため，実装すべきセキュリティ要件の洗い出しに必要となるリスク評価手法の検討をおこなった．IT システムに用いられている従来のリスク評価手法は，セキュリティ対策の経験を十分にもった人材がまだ少ない車載システムには適用が難しい．もしくは，システムの設計時で利用するには，評価者の主観に依存する．したがって，設計段階での車載システム向けリスク評価手法としては適していない．そこで，CVSS を拡張したリスク評価手法を提案した．具体的には，CVSS の指標のうち，脅威そのものの特性を評価する基準値をリスク値として利用することで，設計段階でのリスク値算出が可能にする．そして，基準値のパラメータ区分をシステムの設計書をもとに決定可能になるように定義し，評価者に依存しない客観的なリスク値の算出が可能であることを示した．

今後はセキュリティ機能を実装するプロセスが妥当であることを検証する手法も必要と考えている．具体的には以下のような項目が挙げられる．

(1)　他の手法とのリスク値結果の比較による本手法の妥当性確認

(2) 情報セキュリティへの経験度合いによらない脅威分析手法の研究開発

参考文献

[1] IPA, 2010年度 制御システムの情報セキュリティ動向に関する調査報告書,
https://www.ipa.go.jp/files/000014121.pdf
[2] IPA, 情報家電におけるセキュリティ対策検討報告書,
https://www.ipa.go.jp/files/000014114.pdf
[3] IPA, 2012年度 自動車の情報セキュリティ動向に関する調査,
https://www.ipa.go.jp/files/000027274.pdf

[4] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno, Comprehensive Experimental Analyses of Automotive Attack Surfaces, USENIX Security, August 10–12, 2011. http://www.autosec.org/pubs/cars-usenixsec2011.pdf
[5] ISO, Information technology – security techniques – evaluation criteria for it security – part 1: Introduction and general model, 2005.
[6] CSIRT, 日本コンピュータセキュリティインシデント対応チーム協議会ホームページ, http://www.nca.gr.jp/
[7] 萱島 信, 森田 伸義, 安藤 英里子, セキュリティ機能実装の妥当性検証手法の提案, SCIS(Symposium on Cryptography and Information Security) 2013
[8] IPA, 共通脆弱性評価システム CVSS 概説, https://www.ipa.go.jp/security/vuln/CVSS.html
[9] ISO, Information technology – security techniques – evaluation criteria for it security – part 2: Security functional requirements, 2005.
[10] 土居 範久, 情報セキュリティ事典, 共立出版,2003
[11] ETSI, Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis, ETSI TS 102 165-1 V4.2.3, 2011
[12] C. Laurendeau and M. Barbeau, "Threats to Security in DSRC/WAVE," ADHOC-NOW Lecture Notes in Computer Science, Volume 4104, 2006

(*1) Bluetooth®は、Bluetooth SIG,INC. の登録商標です.