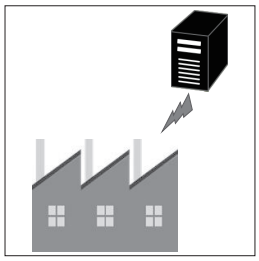


セキュリティ設計におけるリスクの定量化

A Study on Quantification of Risk Assessment in Security Design

川西　康之*
Yasuyuki Kawanishi

畑　洋一
Yoichi Hata

西原　秀明
Hideaki Nishihara

相馬　大輔
Daisuke Souma

吉田　博隆
Hirotaka Yoshida

近年、制御システムにて生産プロセスの効率化・自動化を図る目的で情報系システムと通信接続し、データのやりとりを行う運用が増えつつある。その一方でStuxnet※1による発電所への攻撃等が起こり、制御システムのセキュリティ対策が喫緊の課題となり、制御機器の開発においても最初からセキュリティを考慮した設計を求める動きが生まれている。本研究では設計手順の効率化・属人性の排除を目指し、国立研究開発法人産業技術総合研究所と連携して継続研究を行っている。本論文では、複数フェーズからなるセキュリティ設計におけるリスク評価のフェーズに焦点を当て、既存の脆弱性評価システムを応用し、制御機器・システムに最適なリスク評価の定量化手法についての検討結果について、データロガーをキー要素とする制御システムのケーススタディを交えつつ報告する。

For further automation and efficiency improvement of production, industrial control systems have been increasingly connected to other information systems to exchange data. Under this circumstance, establishing security measures for control systems against malware (such as Stuxnet, which attacked power plants) is an urgent issue. Therefore, security design has been taken into consideration at the beginning of the system development. In collaboration with the National Institute of Advanced Industrial Science and Technology (AIST), we have been applying security design guidelines for automobiles to control systems, aiming to improve the efficiency of design procedures without depending on personal knowledge or experience. Focusing on the risk-assessment phase in security design consisting of multiple phases, this paper proposes a quantification method optimized for the risk assessment of control devices and systems by utilizing an existing vulnerability assessment system. This paper reports on the security design results using the method, providing a case study on a control system equipped with a data logger as the key element.

キーワード：制御システム、セキュリティ設計、リスク評価、CWSS

1. 緒　　言

近年、制御システムへ情報通信技術の適用が進んでいる。情報機器・システムにおいて普及している、情報ネットワーク、汎用OS、通信インターフェイス等の情報通信技術が制御機器に適用された結果、フィールド機器が生成し、送信するセンシングデータの収集、制御サーバ等におけるデータの解析、HMI※2による保守員のシステムメンテナンス、システムの最上位の情報ネットワークにおけるシステム全体の監視、制御へのフィードバックといった、一連の制御プロセスに対して効率化・自動化が図られている。

また、自動車業界においては、コネクティッドカーというシステムモデルにおいて、車載機器がインターネット通信、ITS通信、WiFi通信することにより、車と車の衝突防止や、車－センタ間等での遠隔ソフトウェア更新等の、多様なサービスを提供する製品開発が進んでいる。

制御システム・機器においては、2010年のStuxnetによる発電所への攻撃[1]、2017年のデータロガーの情報セキュリティ脆弱性（JVNDB-2017-004293）[2]などの事例から、制御機器の開発におけるサイバーセキュリティ確保の必要性と緊急性は明らかである。情報システム・機器に関しては、事業等に依拠するコスト制約下で、セキュリティ対策を体系的に漏れなく実施するためのプロセスとしてセキュリティ設計がよく知られている。実際に、ISO/IEC 15408規格[3]で、セキュアな製品開発において、製品開発前にシステム仕様書からセキュリティ要件を導き出す検討フェーズとして「TOE※3定義」、「脅威同定」、「リスク評価」、「セキュリティ対策方針策定」、「セキュリティ要件選定」等から構成されるプロセスを実施するよう定めている。

このような規格を適用し、必要に応じ実施手段の具体化や最適化を行いつつ、制御機器や車載機器の開発に適したセキュリティ設計手法を確立することが喫緊の課題であり、自動車業界では取組みが近年盛んに実施されている。2015年に自動車技術会（JSAE）から自動車の標準的なセキュリティ設計ガイドラインとして、JASO TP15002[4]がリリースされ、2017年に出版された車－センタ間等での遠隔ソフトウェア更新等におけるITU-T X.1373勧告[5]においても、本設計手法が用いられている。

まず当社の自動車関連製品のセキュリティ設計に適用できるかを見極めるため、我々はJASO TP15002を架空の自動車モデルに適用して効率化に関するいくつかの知見を得た[6]。この自動車業界のガイドラインは手順が具体的か

つ汎用性を持つため、工場などの制御システムにも適用できるか検討を試み[8]、脅威抽出からリスク分析に至るプロセスで属人性を排除し半自動化することで作業コストの削減を狙える方式の実現に向けた研究を継続している。

本論文ではJASO TP15002のリスク評価に焦点を当て、制御機器・システムに適した定量化を行えそうな評価スコアリングシステムとして、ソフトウェア脆弱性評価システムCWSSを応用したリスク評価の定量化手法RSS-CWSSを考案し、既存方式CRSSと比較検討した。本論文で実施したデータロガーに関するケーススタディでは、RSS-CWSSはCRSSに比べ評価値が適度に分散することが確認でき、脅威の優先順位付けに効果があることを明確化できた。

第二章で本論文に関連する準備を行う。第三章では前節の内容に従って課題を同定し、第四章で提案手法を述べる。第五章では提案手法を用い、データロガーのセキュリティ設計のケーススタディを実施し、第六章で結論を示す。

2. 準　　備

2−1　セキュリティ設計

セキュリティ設計は製品開発前に仕様書を元にセキュリティ要件を盛り込むプロセスのことで、ISO/IEC15408規格として整備され、対応する国際認証スキームもコモン・クライテリアとして確立されている。産業制御システムにおいては、IEC62443[7]やUL2900-2-2[8]等の規格において、ガイドラインやフレームワークが検討されている。

自動車分野における前出のJASO TP15002は、Lundらが行っているモデルベースのリスク分析アプローチ[9]のような仕様書からのモデル化、脅威抽出、リスク分析、対策方針の導出と、セキュリティ要件を導出するためのプロセスをわかりやすく規定し、外部からの自動車制御ECUへの通信の不正な操作やアクセスなどの攻撃を可視化し、対策の導出を容易にしている。このガイドラインが自動車以外のシステムに適用できそうだと考えたのが我々の研究動機である。**図1**がJASO TP15002の処理フローである。

各フェーズにおいて実施される作業について説明する。

フェーズ1：TOE定義。TOEの保護資産とデータの流れを明示した**図3**のようなデータフロー図（DFD）を作り、資産の重要性や外との攻撃の入り口となるエントリポイント、そしてシステムの開発、販売、運用などのフェーズやそれぞれ関わる人を定義する。

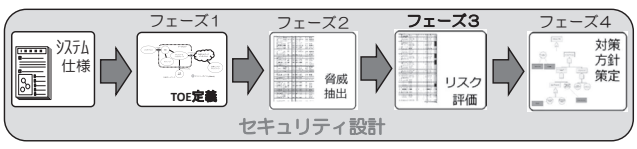


図1　セキュリティ設計の処理フロー

フェーズ2：脅威抽出。このフェーズでは、TOEに起こる脅威とその状況を網羅的に列挙する。具体的には**表1**のように、TOEに起きる好ましくない動作を5Wの観点（“Who”，“When”，“Where”，“Why”，“What”で記述する。“What”の記述方法に関しては、以下事前研究に記す「資産コンテナ方式」を用いている。

表1　JASO TP15002で記述する脅威のリストの例

#	脅威	Where	Who	When	Why	What	(At	Asset)
1	T.制御_ファームウェア_イーサネット_第三者_購買_故意_脆弱性解析	イーサネット	第三者	購買時	故意に	ファームウェアを入手し脆弱性を解析	制御	ファームウェア
2	T.ネットワークIF_通信機能_イーサネット_オペレータ_通常運用_過失_誤操作	イーサネット	オペレータ	通常運用	過失により	故障させる	ネットワークIF	通信機能
3	T.ネットワークIF_通信機能_イーサネット_第三者_通常運用_故意_サーバ侵入	イーサネット	第三者	通常運用	故意に	サーバーに侵入する	ネットワークIF	通信機能
4	T.ネットワークIF_認証機能_イーサネット_オペレータ_通常運用_過失_誤操作	イーサネット	オペレータ	通常運用	過失により	故障させる	ネットワークIF	認証機能
5	T.ネットワークIF_認証機能_イーサネット_第三者_通常運用_故意_誤操作	イーサネット	第三者	通常運用	故意に	故障させる	ネットワークIF	認証機能
6	T.ネットワークIF_認証機能_イーサネット_オペレータ_通常運用_過失_情報漏洩	イーサネット	オペレータ	通常運用	過失により	情報を漏洩させる	ネットワークIF	認証情報
7	T.ネットワークIF_認証機能_イーサネット_第三者_通常運用_故意_情報盗難	イーサネット	第三者	通常運用	故意に	情報を盗む	ネットワークIF	認証情報
8	T.制御_ファームウェア_イーサネット_オペレータ_通常運用_過失_誤データ上書	イーサネット	オペレータ	通常運用	過失により	誤ったファームウェアを上書きする	制御	ファームウェア
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
47	T.制御_設定情報_Modbus_オペレータ_通常運用_過失_誤データ上書	Modbusシリアル	オペレータ	通常運用	過失により	誤ったデータを書込む	制御	設定情報

フェーズ3：リスク評価。このフェーズでは、フェーズ2で抽出した脅威を定量化し優先順位を付ける。JASO TP15002で参照しているリスク評価方式のひとつであるCRSS（CVSS based Risk Scoring System）による評価を例に説明する。CRSSはCVSS v2[10]ベースのリスク評価方式であり、フェーズ2で抽出された個々の脅威に対し**表2**にあるメトリックについてどの分類に含まれるか選択し、重み値を計算式に当てはめてリスク値を算出する。そしてリスク値により脅威をレベルⅢ（critical)、レベルⅡ（warning)、レベルⅠ(caution)、もしくは脅威なしのいずれかに分類するという手順を取る。

表2　リスク計算値メトリックの振分け条件定義の例

メトリック	分類	条件	値
攻撃元区分(AV): 攻撃者の距離	ローカル(L)	シリアル, Modbusシリアル	0.395
	隣接(A)	−	0.646
	ネットワーク(N)	イーサネット	1.000
攻撃条件の複雑さ(AC): 突破するモジュール数	高(H)	3以上	0.350
	中(M)	2	0.610
	低(L)	1	0.710
攻撃前の認証要否(Au): 攻撃に要する認証回数	複数(M)	2以上	0.450
	単一(S)	1	0.560
	不要(N)	0	0.704

#	モジュール名	守るべき資産	機密性(C)			完全性(I)			可用性(A)		
			なし	小	甚大	なし	小	甚大	なし	小	甚大
			0	0.275	0.66	0	0.275	0.66	0	0.275	0.66
1	制御	設定情報	✔				✔		✔		
		ファームウェア			✔			✔	✔		
		PLCステータス	✔					✔	✔		
2	ネットワークIF	通信機能	✔					✔			✔
		PLCステータス	✔					✔	✔		
		認証機能	✔					✔			✔
		認証情報			✔			✔	✔		
3	ストレージ	PLCステータス	✔					✔	✔		

表3　リスク値の算出と優先順位付けの例

#	脅威	AV	AC	Au	AE	EF-C	EF-I	EF-A	EF	Risk Value
1	T.制御_ファームウェア_イーサネット_第三者_購買_故意_脆弱性解析	N	L	N	10.0	甚大	甚大	なし	9.2	9.43
2	T.ネットワークIF_通信機能_イーサネット_オペレータ_通常運用_過失_誤操作	N	L	N	10.0	なし	甚大	甚大	9.2	9.43
3	T.ネットワークIF_通信機能_イーサネット_第三者_通常運用_故意_サーバ侵入	N	L	N	10.0	なし	甚大	甚大	9.2	9.43
4	T.ネットワークIF_認証機能_イーサネット_オペレータ_通常運用_過失_誤操作	N	L	N	10.0	なし	甚大	甚大	9.2	9.43
5	T.ネットワークIF_認証機能_イーサネット_第三者_通常運用_故意_誤操作	N	L	N	10.0	なし	甚大	甚大	9.2	9.43
6	T.ネットワークIF_認証機能_イーサネット_オペレータ_通常運用_過失_情報漏洩	N	L	N	10.0	甚大	甚大	なし	9.2	9.43
7	T.ネットワークIF_認証機能_イーサネット_第三者_通常運用_故意_情報盗難	N	L	N	10.0	甚大	甚大	なし	9.2	9.43
8	T.制御_ファームウェア_イーサネット_オペレータ_通常運用_過失_誤データ上書	N	M	N	8.6	甚大	甚大	なし	9.2	8.77
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
47	T.制御_設定情報_Modbus_オペレータ_通常運用_過失_誤データ上書	L	M	N	3.4	なし	小	なし	2.9	1.85

フェーズ4：セキュリティ対策方針の導出。このフェーズでは脅威の原因をツリートポロジーに分解して、その枝葉それぞれへの対策方針を導出する。安全分析におけるフォールト・ツリー解析（FTA）に似たこのツリーをアタック・ツリー（AT）と呼ぶ[11]、[12]。そして脅威と対策方針の対応関係が判るマトリクスを作成する（**表4**）。脅威のツリー分析は全ての脅威に対して行うか、コストや時間の理由によりリスク値の高い脅威の一部に行うかはガイドラインには明記されておらず、そこに我々はフォーカスを当て研究を行っている。

表4　セキュリティ対策方針マトリクスの例

		セキュリティ対策方針															
		評価対象							環境								
		1	2	3	5	7	10	11	4	6	8	9	12	13	14	15	16
		O.制御コマンドの検疫	O.ファームウェアアクセス防止	O.ファームウェア暗号化	O.IPアドレスフィルタリング	O.パスワードの強化	O.TCP/IPポートフィルタリング	O.マルウェア感染防止	OE.セキュアなファームウェア開発	OE.運用管理の徹底	OE.設定データ管理の徹底	OE.システム構築手順の徹底	OE.機器用途の限定	OE.信頼できるオペレータ	OE.教育	OE.ファームウェアバージョン管理	OE.入室/物理アクセス制限
脅威	1	X	X	X					X								
	2				X	X	X			X	X	X					
	3	X			X	X	X			X	X						
	4	X			X	X	X			X	X						
	5	X			X	X	X			X	X						
	6					X		X					X	X	X		
	7	X			X	X	X	X					X		X		
	8		X							X						X	
	9	X	X	X					X						X		
	10				X	X	X				X						
	11	X			X	X	X			X					X		
	12				X		X			X	X						
	13	X			X	X	X			X							
	14									X						X	
	15	X		X					X						X		
	16	X		X					X						X		
	17	X			X		X								X		
	18	X			X		X								X		
	19	X			X		X								X		
	20									X	X						
	21									X	X						
	22	X												X	X		
	23					X					X						
	24									X							
	25	X		X					X						X		X

2−2　脆弱性評価

脆弱性評価とは、既存システムの持つ脆弱性を定量化するもので、これを仕様書段階である開発初期のセキュリティ設計に適用しようというのがJASO TP15002の試みである。代表的な脆弱性評価システムは以下の通りである：

- CVSS v2（Common Vulnerability Scoring System）：2007年に策定されたITU-T X.1521標準[10]であり、複数の装置が連結された情報システムを意識した脆弱性評価手法である。
- CWSS（Common Weakness Scoring System）：2015年に公開されたITU-T X.1525標準[13]であり、「弱さ」とあるように、より広範囲でのシステムの脆弱性を定量化する評価手法である。

2−3　CWSSのメトリック

CWSSは基本、攻撃可能性、環境の3つの観点から定められた合計16個のメトリックを定義する（**表5**）。

表5　CWSSメトリック[13]

分類	メトリック	内　容
基本	Technical impact（TI）	攻撃により対象の制御をどれだけ掌握できるか（Critical〜None）
	Acquired privilege（AP）	攻撃が成功した結果として、攻撃者はどの程度のユーザー権限を得られるか（管理者〜ゲストユーザー）
	Acquired privilege layer（AL）	攻撃が成功した結果として、攻撃者はどういった機能を掌握できるか（アプリケーションのサービス、システムのOS提供機能、ネットワークアクセス機能など）
	Internal control effectiveness（IC）	脆弱性から守る仕組みがシステムなりアプリケーションに備わっている（ない〜完全に守られている）
	Finding confidence（FC）	脆弱性に関する所見の信頼性（攻撃が届く、攻撃は届くが条件は限定的である、所見は誤りで脆弱性はない）
攻撃可能性	Required privilege（RP）	攻撃を仕掛けるのにどの程度の権限を掌握しておく必要があるか（不要〜管理者権限）、例えばログイン不要なら "N"、ゲストユーザーからでいいなら "L" など
	Required privilege layer（RL）	攻撃対象の何のサービスに対して優位性があるか、例えば攻撃にアプリケーションの機能を使えるなら "A"、システムやOSの共通機能が使えるなら "S"、ネットワークにアクセスできるだけでいいなら "N" など
	Access vector（AV）	攻撃元はどこか、例えばインターネットからなら "I"、イントラなら "P"、Wifiなどからなら "A" など
	Authentication strength（AS）	認証機能の強さ、パスワードが簡単なものでないか、単一の認証ではないかなど、
	Level of interaction（IN）	システム利用者からの一定の「協力」（通常操作、不用意な操作を含む）を必要とするか
	Deployment scope（SC）	脆弱性がどの程度の範囲で存在するのか、例えばどんなプラットフォームやシステム構成でも顕在するものなら "A"（All）、よく使う構成にのみなら "M"（Moderate）、割と特殊な構成や条件下なら "R"（Rare）など
環境	Business impact（BI）	システム操業など、ビジネスやミッションにどの程度支障が出るか（Critical〜None）
	Likelihood of discovery（DI）	脆弱性の見つけやすさのパラメータ。脆弱性を見つけるのにリバースエンジニアリングなどの高度な技術が必要かどうか、長期間の調査が必要かどうかなど
	Likelihood of exploit（EX）	攻撃のチャンスがどれだけあるか、いつでも試せるなら "H"（High）、実施タイミングはその時の状況次第なのが "M"（Middle）、レアケースでしかチャンスが来ないのは "L"（Low）、チャンスが全く無いのは "N"（None）
	External control effectiveness（EC）	攻撃対象の外側にあるシステムなりサービスで、攻撃を困難にしている機能が付与されていないか、
	Prevalence（P）	この脆弱性がどの程度頻繁に、広範囲に出現しうるか、例えば同じ構成の機器なら必ず出るものなら "W"（Widespread）とし、頻度や条件が限定されるにつれて "H"（High）、"C"（Common）、"L"（Limited）とする

2−4　セキュリティ設計におけるリスク評価

セキュリティ設計におけるリスク評価とは、製品リリース前にシステム仕様から脅威を抽出し、客観的な定量化により優先順位付けすることである。JASO TP15002では前出の脆弱性評価システムCVSS v2を応用したリスク評価方式であるCRSS方式を例示しており、本来製品リリース後

に使う脆弱性評価システムが、製品リリース前のリスク評価にも使えることを示した。

2−5　事前研究

2017年のDECSoS会議[6]にて、まず我々はJASO TP15002を自動車のTOEに適用した際の課題を抽出し、リスク分析の省力化に関する提案を行った。脅威の対策を導出する最も工数のかかる作業を行う前に、リスク分析により対象とする脅威をコストに見合う数に絞り込むという提案で、そのために脅威を定める5Wの何に着目し、定量化するかという課題を提示した。そして解決手段として、“What”（どうなった）を「“At”（どこ）の“Asset”（資産）が侵害された」と分解して“Where”（どこから）と組み合わせることで、攻撃経路（“Where”～“At”）と攻撃される資産（“Asset”）の重要性から脅威の抜け漏れを防ぎリスクを定量化する手法を提案した。これら“Where”、“At”、“Asset”の関係が**図2**に示すように資産を入れる器とその口に喩えることができるので、我々はこの手法を「資産コンテナ方式」と命名した。

図2　「資産コンテナ方式」の考え方[6]

上記提案手法は、攻撃者側の観点や攻撃シナリオからリスクを評価する方式に比べ以下の利点を持つ：

- 評価者の知見に依存する、属人性を排除できる。
- 装置やシステムの仕様から導出できる組合せのみ考慮すればよく、脅威の抜け漏れを防げる。
- 5Wより観点の少ない3つのメトリックで一意に判断できるので、リスク分析の工数が削減できる。

また自動車の車載機器と制御システムの制御機器は、保護資産が制御機能を含み、完全性と可用性に重きが置かれている等、共通点が多く存在するため、2017年のCSS会議[14]において、我々はJASO TP15002を産業制御システムに適用する試みとして行った、データロガーのケーススタディの結果を報告した。具体的には**図3**のようなデータロガーのTOEを作成し、47件の脅威を抽出した。

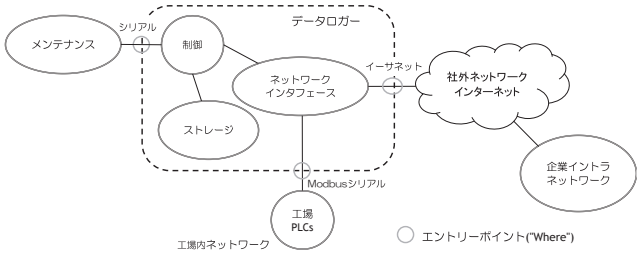


図3　データロガーのTOE[14]

3.　課　　題

前節で述べたように、JASO TP15002は制御システムに適用できる。しかしリスクの定量化方式CRSSは、CVSS v2という古い標準に準拠しているということもあり、より制御機器の特性に沿ったものを求め、文献（14）のさらなる検討を試みた。

今回の試みとして、同じTOEを用いてCRSSに対抗する新たな定量化手段を考案し、比較検討を行った。比較においてはフェーズ4のセキュリティ対策方針選定を進めた際の作業量の差を見ることにし、有効な対策が出揃うまでにアタック・ツリー分析を行った脅威の数が少ない方が優れた定量化方式であるという評価基準を採用した。

CRSSをリスク定量化に用いた際の傾向として、リスク値がうまく分散せず、複数の脅威が横並びで優先順位が付けにくいというものがあった。具体的には文献（14）のリスク定量化の際に、リスク値が1位の脅威が7件、14位のものが6件、20位のものが8件並んだ。その結果脅威の絞り込みがうまく行かず、フェーズ4における必要な分析件数が全脅威の半数程度となり、改善の余地があった。

4.　リスク評価の定量化に関する検討手法

上記課題を解決する新しい定量化手法として、CWSSのメトリックが適用できるかを試みた。この応用方式を、RSS-CWSS（Risk Scoring System based on CWSS）と呼称する。

4−1　CWSSベースのリスク評価方式RSS-CWSS

我々はRSS-CWSSを、**表5**のメトリックのうち、**表6**の6つを除く10個を用いたリスク評価方式と定義した。

表6　固定値としたCWSSメトリック

メトリック	コード	値	設定内容
AL	A (Application)	1.0	攻撃成功により、装置の全機能が掌握される
IC	N (None)	1.0	脆弱性から守る仕組みはない
FC	T (Proven True)	1.0	所見の信頼性は高く、攻撃が確実に実行できる
IN	A (Automated)	1.0	攻撃に他者の相互作用は不要
SC	R (Rare)	0.5	TOEにある限定された構成のみで起きるリスク
P	W (Widespread)	1.0	攻撃の影響は広範囲に波及する

4－2　CWSSの計算式

RSS-CWSSの元となるCWSSのリスク値は0から100までの値を取り、次の計算式に従って各メトリックの取る重み変数を掛け合わせて算出する[13]：

リスク値＝BaseFindingSubscore×
AttackSurfaceSubscore×EnvironmentSubscore

BaseFindingSubscore＝
[(10×TI+5(AP+AL)+5×FC)×f(TI)×IC)]×4.0
TI＝0の場合f(TI)＝0、それ以外はf(TI)＝1

AttackSurfaceSubscore＝
[20(RP+RL+AV)+20×SC+15×IN+5×AS]/100.0

EnvironmentSubscore＝
[(10×BI+3×DI+4×EX+3×P)×f(BI)×EC)]/20.0
BI＝0の場合f(BI)＝0、それ以外はf(BI)＝1

5.　検討結果

5－1　RSS-CWSSの導入結果

ケーススタディにおいて各方式を適用し比較を行った。

メトリックの数がCRSSの6に対し、RSS-CWSSでは10と増えたことにより、リスク値の分散が向上した。一例を挙げると**表7**にあるように、CRSSの評価結果ではリスク値1位で7つも並んでいた脅威が、RSS-CWSSの結果では5つのクラスタに分散した。

表7　脅威のリスク値の分散

脅威No.	CRSS	RSS-CWSS
13	9.43	75.8
36		33.7
31		23.3
35		
37		18.1
30		13.2
34		

図4は、フェーズ4でリスク値の高い順にセキュリティ対策方針を抽出した際に、それぞれの対策方針が何番目の脅威で初めて抽出されたかを、線で繋いだものである。これによると対策方針が全部出揃ったのはCRSS方式では25件目、RSS-CWSS方式では14件目であり、課題で述べた評価基準において後者の方が優れた結果となった。

よって、リスク定量化のメトリックやその個数をうまく選んだRSS-CWSS方式がリスク分析フェーズにおけるリスク値をうまく分散させ、効果的な脅威の絞り込みを行い後段のフェーズの作業量を減らせることが確認できた。

5－2　結果の考察

リスク分析の定量化方式によりばらつきに違いが出ることについて、検討結果では単純にメトリックの数の大小で差が出たと考えられたが、実際はそれだけではなく、メトリックの定義された内容がリスク評価するシステムに合っているかということも重要である。例えば資産が攻撃を受けることでのインパクトを示すメトリックが技術的なTIだけでなく事業に関するBIを持つ（**表5**参照）RSS-CWSSでは攻撃経路が限られたデータロガーでもリスク値に差が出やすい。つまり、単にメトリクスが多いだけでなく、システムの構成要素を明確に差別化できるメトリックを多く持つリスク評価方式を用い、メトリックの重み変数をシステムの現状に合わせて偏らないように分類するのが重要であると言える。

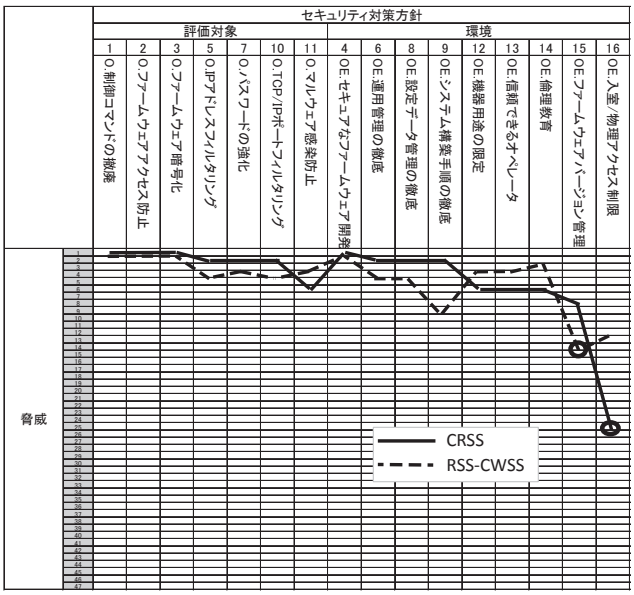


図4　対策方針全抽出に必要な脅威の分析量の比較

6.　結　　言

制御システムを対象としたセキュリティ設計手順について紹介し、省力化と属人性の排除を目的とする、リスク評価前後のプロセスと定量化手法の改良に関する検討結果を報告した。制御システム向けに脆弱性評価手法CWSSを応用したリスク評価手法RSS-CWSSを考案し、対策方針導出フェーズまで追跡検討を行ったことで、RSS-CWSSが分析件数の軽減を実現し、そしてリスク定量化での適切なメトリックの選択により、リスク値を適度に分散させることで、効果的な脅威の絞り込みが実現することを確認できた。

用語集

※1　Stuxnet

2010年にイランの核施設を攻撃したマルウェア（悪意のあるソフトウエア）で、亜種を含め産業制御システムに大きな被害を与えた。

※2　HMI

操作盤等のヒューマン・マシン・インタフェース。

※3　TOE

Target of Evaluation：セキュリティ設計における評価対象のことで、設計対象をモデル定義化したもの。

参考文献

(1) S.Karnouskos, “Stuxnet Worm Impact on Industrial Cyber-Physical System Security.” In: “37th Annual Conference of the IEEE Industrial Electronics So-ciety (IECON 2011), Melbourne, Australia”（November 2011）
(2) JPCERT コーディネーションセンター、情報処理推進機構（IPA）、脆弱性対策情報データベースJVN iPedia
(3) ISO/IEC 15408-1:2009 Information technology Security techniques Evaluation criteria for IT secu-rity Part 1: Introduction and general model
(4) 自動車技術会、JASO TP15002:2015、自動車の情報セキュリティ分析ガイド（2015）
(5) ITU-T X.1373 : Secure software update capability for intelligent transportation system communication de-vices
(6) Y. Kawanishi, H. Nishihara, D. Souma and H. Yoshida, “Detailed analysis of security evaluation of auto-motive systems based on JASO TP15002,” DECSoS: Dependable Smart Embedded Cyber-physical Systems and Systems-of-Systems, LNCS 10489, 2017, Springer
(7) IEC TS 62443-1-1:2009 Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models
(8) UL 2900-2-2: Outline of Investigation for Software Cybersecurity for Network-Connectable Products, Part 2-2: Particular Requirements for Industrial Control Systems（2016）
(9) M. S. Lund, B. Solhaug and K. Stolen, Model-Driven Risk Analysis, the CoRAS Approach, Springer-Verlag Berlin Heidelberg (2011)
(10) ITU-T X.1521 (04/2011): Cybersecurity information exchange, Vulnerability/state exchange, Common vulnerability scoring system
(11) Roy, D. S. Kim, and K. S. Trivedi, “Cyber security analysis using attack countermeasure trees.” Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research. ACM (2010)
(12) Roy, D. S. Kim, and K. S. Trivedi, ACT: Towards unifying the constructs of attack and defense trees, Security and Communication Networks, 2011:3:1-15
(13) ITU-T X.1525: Cybersecurity information exchange, Vulnerability/state exchange, Common weakness scoring system
(14) 川西康之、西原秀明、相馬大輔、吉田博隆、畑洋一、「産業制御システムデータロガーに対するセキュリティ設計の検討」、CSS2017

執筆者

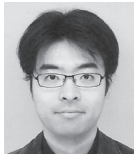
川西　康之*：サイバーセキュリティ研究開発室 主席

畑　　洋一：サイバーセキュリティ研究開発室 室長

西原　秀明：（国研）産業技術総合研究所 博士（理学）

相馬　大輔：（国研）産業技術総合研究所 博士（情報科学）

吉田　博隆：（国研）産業技術総合研究所 博士（工学）



*主執筆者