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

川西 康之[1,2]　西原 秀明[2]　相馬 大輔[2]　吉田 博隆[2]　畑 洋一[1,2]

概要：近年，産業制御システムにおける情報通信技術の適用が進展中であり，制御機器およびシステムの低コスト化等を促す一方で，2010 年の Stuxnet ウイルスによるイラン原子力発電所への攻撃など，セキュリティ脅威が深刻な問題となりつつある．本論文では，産業制御システムにおけるデータロガーに対するセキュリティ設計の検討を行う．我々は情報システムで実績がある ISO/IEC15408 に準拠するフレームワークに基づき，車載システムのセキュリティ設計ガイドライン JASO TP15002 を制御機能の保護という観点で適用した．結果，データロガーへの脅威を網羅的に抽出し，リスク値評価により優先される対策を明らかにした．

キーワード：産業制御システム，データロガー，セキュリティ設計，脅威抽出，リスク評価

1. はじめに

産業制御システムは，制御対象に関する情報を中央で監視することにより状況を把握し，分散した対象を制御するシステムである [16] ．具体的には，電力，ガス，水道，石油などの生産システムが挙げられる．産業制御システムでは，運用時には，センサから吸い上げられた情報を基に，制御コントローラでアクチェータに制御指示を出すという一連の処理により，制御処理が行われる．保守時には，操作者が保守端末（HMI）を通じて，制御対象プロセスのモニタリングや制御コントローラのパラメータ設定を行い，さらに，遠隔による診断保守により，制御対象プロセスの異常・障害の防止を行い，それらを検知した場合には回復を行う．

近年，産業制御システムにおいても，OS，アプリケーション，通信プロトコル等について，一般 IT システムで使用されている情報通信技術と同じものの適用が進展中である．これらにより，制御機器およびシステムの低コスト化を促す等のメリットが期待されている．産業制御システムの一翼を成すシステムとして，データロガーシステムが挙げられる．データロガーはセンサ等から収集した各種データを蓄積する装置であり，生産プロセスにおける様々なデータを蓄積することにより，品質向上，生産コスト削減，効率的な生産現場の構築を目的として用いられる．近年，産業制御システムへのネットワーク化の進展に伴い，データロガーは通信機能を搭載することにより，PLC から成る制御ネットワークからの情報を中継することが可能となり，現場の工場のインターネットへの窓口としてのゲートウェイのような役割を担うようになってきている．

一方で，2010 年の Stuxnet ウイルスによるイランの原子力発電所への攻撃 [2][15] や 2016 年のウクライナの発電所 [21] への攻撃等において見られるように，産業制御システムにおいても，セキュリティ脅威が深刻な問題となりつつある．2017 年 5 月には，JVN (Japan Vulnerability Note) のポータルサイトにおいて，特定のデータロガーにおけるコマンドインジェクションの脆弱性 (JVNDB-2017-004293) が公開 [11] され，不正の情報取得，情報の改ざん，およびサービス運用妨害状態にされる等の悪影響の可能性が指摘された．このような背景から，産業制御システム製品の脆弱性を修正することは急務であるが，システムのライフサイクル (企画・設計・開発・運用・廃棄) における企画段階 (調達段階) から情報セキュリティの観点を意識し，調達仕様にセキュリティ機能を必要十分な形で搭載するための方法論である，SBD（Security By Design）の重要性も指摘されている [14].

本論文では，データロガーシステムを対象としたセキュリティ設計を検討する．我々のセキュリティ設計方式の検討に際しては，厳格なリアルタイム性要求や，完全性と可用性等のセキュリティ保護観点の重要性等の類似性に着目とし，自動車システム向けのセキュリティ設計ガイドライ

1　住友電気工業株式会社
2　国立研究開発法人産業技術総合研究所　情報技術研究部門
住友電工－産総研サイバーセキュリティ連携研究室

ンである自動車技術会のテクニカルペーパー TP15002[10] に基づき，我々が提案した方式 [9] を採用した．本検討の結果として，データロガーへの脅威を網羅的に抽出し，リスク値評価により対策を優先すべき脅威を明らかにした．

一方，上記の検討において，採用したリスク評価方式に関しては，産業制御システム向けに最適かは明確ではないという課題がある．このため，我々は組込み向け脆弱性スコアリングシステム規格 CWSS[7] をベースとし，産業制御システムに最適なリスク評価を行うための方式を検討中であり，現時点までに検討方式と CRSS によるリスク評価方式との定量比較を行った．

本論文の構成は以下である．2 章において，本論文の理解に必要な技術説明を行い，3 章において，本セキュリティ設計検討で用いる方式を提案する．4 章において，提案方式を用いたデータロガーシステムのセキュリティ設計における，モデル定義，脅威抽出，リスク評価について，得られた結果を説明する．5 章において，産業制御システム向けリスク評価の最適化の検討について状況を報告し，6 章で結論を述べる．

2. セキュリティ設計に関する事前準備

2.1 セキュリティ設計の全体像

一般的な情報システムにおいては，セキュリティ脅威に対抗するセキュアなシステムを設計するためのシステマティックな方式論，即ち，セキュリティ設計が ISO/IEC15408[4] 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している．セキュリティ設計とは，システム仕様を入力とし，セキュリティ対策方針を出力する作業プロセスである．プロセスの過程において，TOE(Target of evaluation) 定義，脅威抽出，リスク評価等を実施することが一般的である．我々は，IT システムで実績がある ISO/IEC 15408 記載のセキュリティ対策方針策定をゴールとする．

一方，産業制御システムにおいては，IEC62443[3] や UL2900-2-2[22] 等の規格の策定において，セキュリティガイドラインやセキュリティ対策が，各ネットワークレイヤー毎に検討されている状況である．産業制御システムの分野においては，これらの規格を踏まえることにより，保護対象の制御機器に最適な対策の策定が期待できる．

2.2 JASO TP 15002

自動車技術会 (JASO) は 2012 年より，自動車システムのセキュア設計の標準的なガイドラインを検討し，その成果を 2015 年にテクニカルペーパー TP 15002 として出版した [10]．特に JASO TP 15002 では，サーバ，デバイスなどからの自動車制御 ECU への通信の不正な操作やアクセスからの防御を考察している．

JASO TP 15002 では，システムのセキュア設計は「TOE 定義」，「脅威分析」，「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」の 5 つのフェーズからなり，そのうち TOE 定義，脅威分析，リスク評価の 3 つがセキュリティ評価に関係する．これらのフェーズにおいて実施される作業と成果物について概説する．

2.2.1 フェーズ 1: TOE 定義

評価対象 (TOE) を明確にモデル化する．このモデルは TOE の保護資産と TOE のモジュール間におけるデータの流れを明示したデータフロー図 (DFD) からつくられる．よって，このモデルは TOE のネットワーク構造と攻撃のエントリポイントを示す．このフェーズでは，各保護資産について守るべき CIA の観点が割り当てられる．自動車システムにおいては，一般に機能が想定通り正しく動作することが重要であるので，一貫性または可用性が確保されるべきである．同様にデバイス間通信あるいはシステム外部との通信においては機密性または一貫性が確保されるべきである．TOE のライフサイクルやモジュールといった分析・評価に関連する情報もこのフェーズで規定される．最終的にセキュリティ評価に関する全ての情報が整理され，関係者間で共有されることとなる．

2.2.2 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が網羅的に列挙される．まず，分析における前提が同定され，次にエントリポイントごとに起こりうる，好ましくない動作が検討される．好ましくない動作に対しては，5W の観点 (“Who”, “When”, “Where”, “Why”, “What”) でその状況が同定される．また組織におけるセキュリティ方針もこのフェーズで明確に述べられる．

2.2.3 フェーズ 3: リスク評価

このフェーズでは，フェーズ 2 で同定された脅威のリスクを算定し評価する．JASO TP 15002 ではリスク評価方式として CRSS と RMSA の二つが参照されているが，本稿ではケーススタディで採用した CRSS による評価について説明する．

CRSS は CVSS v2 [5] ベースのリスク評価方式である．フェーズ 2 で同定された個々の脅威に対して，攻撃容易性と影響度の二つを数値として評価し (これらの分類と評価値については表 3 と表 4 を参照のこと)，その値をもとにリスク値を算出する．更に，脅威をそのリスク値をもとにレベル III(critical)，レベル II(warning)，レベル I(caution) のいずれかに分類する．

なお，現在，CVSS については，CVSS v3 [5] が公開されており，必要な特権レベルとユーザ関与レベルが新たに導入された．本検討では，JASO 規格を準拠するという意味で CVSS v2 を採用した．

以上により，TOE に対する脅威とセキュリティリスク評価結果の一覧が成果物として得られる．

2.3 既存手法

産業制御システムのためのセキュリティ設計については，2000 年代中頃より様々な方法論が提案されている．これまでに提案されている方法論は，抽象的な攻撃導出，その詳細化・分析，詳細な脅威のリスクを評価を対象としており，JASO TP 15002 のフェーズ 2: 脅威抽出およびフェーズ 3: リスク評価 (またはその一部) に相当する．[1], [17], [19] は Attack Tree などの木構造を基にした分析手法を提案している．また，リスク評価には，[1] は攻撃に必要なスキル，攻撃の影響，攻撃検知の容易性の 3 つ，[17] は攻撃による経済的な影響とそれから算出される脆弱性評価を用いている．一方，[19] は攻撃のリスク評価だけでなく，脅威への対策の評価も実施している．攻撃のリスクは return on attack (ROA) で評価し，対策を return on investment (ROI) で評価している．これら木構造を用いた方法論では，攻撃のリスク評価に構成された木を用いるという特徴がある．[13] は攻撃者を基に攻撃の詳細化・分析を行い，攻撃ごとに必要とされる時間やステップなどのコストをリスクとして評価している．この手法は詳細に攻撃方法を分析するもので，これを用いることで多段攻撃の分析も可能になると考えられる．[18] は攻撃の種類とシステムに起こりうる影響を列挙し，それらの組み合わせることで脅威を導出している．また，脅威によりに起こる経済的な損失をリスクとして評価している．[12] は UML のユースケース図を拡張した脅威抽出，リスク評価，対策導出の手法である．リスクはインシデントに対し，それを引き起こす攻撃シナリオの発生頻度とインシデントによる asset への影響の大きさにより評価される．

本論文で提案する手法は，これまで提案されてきた方法論で対象としてきた，抽象的な脅威の抽出方法からそのリスク評価の全てを対象としている．また，これまでに提案されてきた手法では，複数の側面からそのリスクを評価しているものは少ない．本論文ではより詳細にリスクを評価するために抽出された脅威に対し複数の側面から評価を行うことを提案している．しかし，これは評価方法が複雑になり，コスト増加が懸念される．このコスト増加の抑制については，現在検討中である．

3. 提案方式

3.1 実際のセキュリティ設計における課題

理論的には前節の通りであるが，実際のシステムにおいて，セキュリティ設計を実施する際には大きく分けると以下の 3 つの課題に纏められると我々は考えている．

一点目の課題は，セキュリティ設計における設計工数の全体最適化である．例えば，脅威抽出フェーズにおいて，詳細情報の記述や脅威件数を多くすることに注力しすぎる等のリスクはあるが，５つのフェーズから成る設計全体において，脅威と対策の対応表のような主要な目標成果をいかにして，小さい工数で達成するかが課題と考える．

二点目の課題は，設計の妥当性の確認であり，セキュリティ設計の実施者が正しく妥当な設計と検証を行っているかを，実施者の共同作業者や管理者等がいかにして，容易に確認するかが課題と考える．

三点目の課題は，複数のセキュリティ設計間の整合性の確保である．セキュリティ設計は，複数回に渡る可能性はありうる．例えば，他社機器も含む全体システムの設計と，自社機器のみを含むサブシステムの設計である．前者は，粒度は粗いが全体を俯瞰する意味で重要であり，後者は，自社製品に具体的にどのようなセキュリティ機能を搭載し，実装していくかという観点において重要である．上記二つのセキュリティ設計は，相関があり，各モジュールに課される前提は（環境の）対策方針に関して，いかにして整合性を担保するかが課題である．

3.2 資産コンテナ方式によるセキュリティ評価

本セキュリティ設計において，我々が自動車システム向けに提案した方式 [9] を採用する．それは JASO TP 15002 記載の方法論を詳細化し， CRSS を検討方式として採用している．具体的には，脅威の記述における５つの観点における “What”に関し，攻撃の終着点を表現する “At”と攻撃が侵害する保護資産を表現する “Asset”の観点において，記述内容を詳細化する．以降，“At”を資産コンテナ，提案方式を資産コンテナ方式と呼称する．

また，資産コンテナ方式は自動車システム向けなので，産業制御への適用は非自明と考える．したがって，セキュリティ設計の各フェーズにおいて，本方式適用のための詳細な検討を行った．例えば，フェーズ 1 のモデル定義においては，評価対象データロガーシステムについて，TOE とそれ以外を分ける境界線の妥当性，攻撃者が利用する通信インターフェースであるエントリポイント，一つの機器における物理的あるいは論理的観点からの複数のモジュール定義，それらのモジュール間の結線構造に関する検討を実施した．

4. ケーススタディ

これよりケーススタディとして，工場などの制御システムにおけるキーコンポーネントであるデータロガーを例に，JASO TP15002 を元にした我々の提案方式である資産コンテナ方式について説明し，データロガーにおいて何が主要な脅威となるかを明らかにする．

4.1 フェーズ 1: モデル定義

図 1 が制御システム内のデータロガーの機能モジュールをモデル化したものである．

図中の赤い丸印がエントリポイントで，外部からコンポーネント内のモジュールにアクセスできる入り口である．

「シリアル」とあるのが保守の際にだけ使用する保守用シリアルポート，「イーサネット」が外部のネットワークへつながっている通信ポート，「Modbus シリアル」が制御システムの装置と繋がった PLC とのアクセス用のバスである．

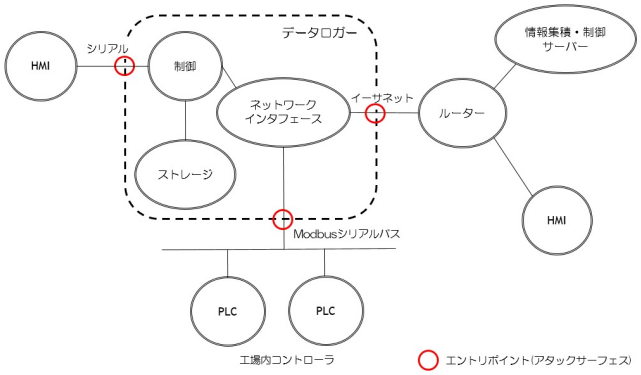

図 1　フェーズ 1: TOE 定義

TP15002 を本来のターゲットである自動車ではなく制御システムのコンポーネントに適用するにあたり，課題となるのはモデル内のモジュールの粒度であった．自動車の場合，各機能ごとに ECU という物理的なモジュールに分かれており，実際の構成に合わせたトポロジーが作りやすいが，データロガーのような小規模の装置では機能モジュールの境界はファームウェアの関数などの境界であり曖昧となる．モジュール構成は攻撃の難易度を判断する重要な要因であるので，粗過ぎず細か過ぎず根拠を持って定める必要があった．

ケーススタディでは保守用シリアルポートで本体の動作に携わる資産を取り扱う制御モジュール，運用時にネットワークやシリアルバスを介して外部とアクセスするネットワークインタフェースモジュール，そして PLC の状態をログとして保存するストレージモジュールの 3 つに分割した．ストレージに関しては外部記憶メディアを用いているケースもあるが，運用時の着脱はまれであるため，今回のケーススタディにおいては内蔵ストレージ扱いとした．

表 1　フェーズ 1: 機能モジュールリスト

#	モジュール名	守るべき資産	機密性	完全性	可用性
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 インタフェース	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		○	

守るべき資産については，装置の設定情報，装置の機能を実現するファームウェアを制御モジュールが持ち，通信および認証にかかわる機能と認証情報をネットワークインタフェースが持つ．PLC のステータスデータはログデータとしてやり取りをするためにモジュール間で共有する各機能モジュールが持つ守るべき資産について，機密性 (C)，完全性 (I) および可用性 (A) の何を持つのか定義したものが表 1 である．

4.2　フェーズ 2: 脅威抽出

表 2 が TOE モデルに関して想定される脅威をリストにしたものの一部である．脅威の抽出に関しては前章で述べた通り，エントリポイント (“Where”)，資産コンテナ (“At”)，および守るべき資産 (“Asset”) の組合せについて総当たりにし，残りの “W” についてのバリエーションを加えることで表を完成させる．

表 2　フェーズ 2: 脅威リスト (抜粋)

脅威 #	Where	Who	When	Why	What	(At	Asset)
1	シリアル	保守員	保守時	過失で	誤設定する	制御	設定情報
12	イーサネット	第三者	運用時	故意に	有害なソフトを駆動		ファームウェア
20	Modbus	運用者	運用時	過失で	データを消去		PLC ステータス
21	シリアル	保守員	保守時	過失で	故障させる	ネットワーク インタフェース	通信機能
32	イーサネット	運用者	運用時	過失で	情報を漏らす		PLC ステータス
35	イーサネット	第三者	運用時	故意に	故障させる		認証機能
41	Modbus	保守員	保守時	故意に	情報を漏らす		認証情報
47	Modbus	運用者	運用時	過失で	データを消去	ストレージ	PLC ステータス

表 2 は抽出した脅威の一部について抜粋して表にしたものであるが，実際は制御モジュールに関する脅威が 20 件，ネットワークインタフェースモジュールに関する脅威が 21 件，ストレージモジュールに関する脅威が 6 件と，計 47 件の脅威が抽出できた．表の読み方であるが，例えば脅威 #35 については「運用時に第三者が故意にイーサネット経由でネットワークインタフェースモジュールの認証機能を故障させる」という脅威である．

4.3　フェーズ 3: リスク評価

前節で示した脅威リストについて具体的にリスク評価を行った．リスク評価においては前述の CRSS に準拠した．表 3 および表 4 が作成した数値化指標である．

表 3　フェーズ 3: 攻撃容易性 (AE) の分類

パラメータ	考え方	区分 (ランク)	判断基準	数値
AV:攻撃元区分	脅威からの距離	ローカル (L)	シリアル, Modbus	0.395
		隣接 (A)	(Wifi など)	0.646
		ネットワーク (N)	イーサネット	1.000
AC:攻撃条件の複雑さ	資産に達するまでに介するモジュール数	高 (H)	3 以上	0.350
		中 (M)	2	0.610
		低 (L)	1	0.710
Au:攻撃前の認証要否	資産に達するまでに必要な認証回数	複数 (M)	複数	0.450
		単一 (S)	単一	0.560
		なし (N)	不要	0.704

表 3 はエントリポイントに至る物理的な距離やトポロジー的なモジュール間の距離で攻撃の難易度を決める指標である．例えば「攻撃条件の複雑さ」は TOE のモジュール間のトポロジーにより決まるものである．

また表 1 で説明した資産の CIA については，表 4 にあるように「なし」，「軽微」，および「甚大」という資産が損

表 4　Phase3: 影響度 (EF) の分類

#	モジュール名	守るべき資産	C:機密性への影響			I:完全性への影響			A:可用性への影響		
			なし (0.0)	軽微 (0.275)	甚大 (0.660)	なし (0.0)	軽微 (0.275)	甚大 (0.660)	なし (0.0)	軽微 (0.275)	甚大 (0.660)
1	制御	設定情報	○				○		○		
		ファームウェア			○			○	○		
		PLC ステータス	○				○		○		
2	ネットワークインタフェース	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	○				○		○		

なわれた際の被害の大きさにより 3 つのランクを設けている．後半の 2 つについては，「軽微」は資産が損なわれた結果データロガー単体の機能不全が起きるが制御システムの稼働には影響を及ぼさない脅威，「甚大」はデータロガーを踏み台に PLC が遠隔操作される，重要パスワードの流出など，システムおよびその外部に波及しうる脅威としてランク付けした．

そして TOE モデルに基づきデータロガーの脅威についてリスク評価を行った結果，47 の脅威を抽出 (一部を表 2 に記載) し，CRSS に基づくリスク値評価により，9 個の脅威を最も高いリスク (レベル III)，20 個を次に高いリスク (レベル II)，そして 18 個を比較的低いリスク (レベル I) に分類した．レベル III の脅威については表 5 にまとめた．

表 5　フェーズ 3: 重大脅威 (リスク値がレベル III(7 以上) のもの)

脅威 #	Where	What (At	Asset)	AV	AC	Au	C	I	A	リスク値
13	イーサネット	制御	ファームウェア	N	L	N	甚大	甚大	なし	9.43
30		ネットワークインタフェース	通信機能	N	L	N	なし	甚大	甚大	9.43
31				N	L	N	なし	甚大	甚大	9.43
34			認証機能	N	L	N	なし	甚大	甚大	9.43
35				N	L	N	なし	甚大	甚大	9.43
36			認証情報	N	L	N	甚大	甚大	なし	9.43
37				N	L	N	甚大	甚大	なし	9.43
11		制御	ファームウェア	N	M	N	甚大	甚大	なし	8.77
12				N	M	N	甚大	甚大	なし	8.77

表 2 で説明例とした脅威#35 が表 5 にあるので，これを例に表の内容について説明すると，脅威#35 という「運用時に第三者が故意にイーサネット経由でネットワークインタフェースモジュールの認証機能を故障させる」脅威は，「ネットワーク経由でいつでも (AV=N)，直接モジュールを (AC=L)，認証機能を持たないポートから (Au=N) 攻撃が行え，攻撃対象である認証機能は完全性 (I) と可用性 (A) に甚大な被害を受ける」というリスクが考慮され，数値化により 9.43 点という同点 1 位の高いリスクであることがこの表では示されている．

以上，JASO TP15002 のフェーズ 1 からフェーズ 3 までの手順により，制御システムのデータロガーについて脅威の抽出とリスク評価が行われ，イーサネットを通じてネットワークインタフェースを経由した制御モジュールもしくはネットワークインタフェース自身への攻撃が最も高いレベル III の脅威であることが明らかとなった．表 5 の CVSS v2 の基本値を見ていくと，モジュール構成が簡単であったり認証機能が弱いことにより攻撃条件の複雑さ (AC) と攻撃前の認証要否 (Au) のランクが共に低くなっており，これらの改善が必要であることが読み取れる．

5. CWSS を用いたリスク評価の最適化の検討

5.1 CWSS の概要

CWSS(Common Weakness Scoring System) は ITU-T X.1525[7] として標準化されている組込みシステムの弱点を数値化するシステムで，TP15002 で採用している CRSS がベースとしている CVSS v2 に対してより広義の脆弱性を示すものとして多くのパラメータを定義しており，脆弱性を数値化しその深刻さを評価するものである．

CWSS は基準，攻撃可能性，環境の 3 つのカテゴリにおいて合計 16 個のパラメータを定義し，リスク値算出のための数値を与えている．表 6 がそれぞれのパラメータの内容で，それぞれ 4 ～ 7 段階にランク付けされる．

表 6　CWSS パラメータ

グループ	パラメータ	内容
基準	Technical impact (TI)	攻撃により対象の機能をどこまで掌握できるか (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か (無い ～ 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無い)
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)，限定された構成や条件下なら “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，任意に実施可能であれば “H” (High)，特定の条件下で実施可能であれば “M” (Middle)，まれな条件下でのみ実施可能であれば “L” (Low)，攻撃不可能であれば “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程度に応じて “H” (High)，“C” (Common)，“L” (Limited) とする

5.2 CWSS ベースのリスク評価の検討

表 8 が前章のケーススタディで示した，データロガーのレベル III の脅威に関して，同様に CWSS パラメータで計算した結果である．CWSS パラメータに関しては JASO TP15002 のフェーズ 4 における原因分析にかかる内容もあり，今回のケーススタディでは分類が難しいパラメータ 6 つについては固定値としたが，CRSS の 6 個に比べて 10

個が比較に有効で，CRSS よりも脅威のランク付けがより細分化される結果となった．

固定値としたパラメータについて表 7 に補足する．パラメータは 0 ～ 1 の値を取り，1 となる条件が最もリスクがあるものとなっている．

表 7 固定値とした CWSS パラメータ

パラメータ	コード	値	固定値とした根拠
AL	A(Application)	1.0	攻撃の結果により装置の全機能が掌握されることを想定した．
IC	N(None)	1.0	脆弱性から守る仕組みの有無については脅威が起こる原因の精査が必要なため，最も厳しい条件 (仕組みは無い) とした．
FC	T(Proven True)	1.0	所見の信頼性に関しては，今回のテストケースでは最も厳しい条件 (攻撃が確実に実行できる) とした．
IN	A(Automated)	1.0	データロガーの運用では常時誰かが操作しているわけではないので，限定的な条件を持たない最も厳しい条件 (他者の相互作用は不要) とした．
SC	R(Rare)	0.5	今回のテストケースでは TOE にある限定された構成のみでの運用であるため，この条件とした．
P	W(Widespread)	1.0	波及範囲に関しては今回のテストケースでは判断が困難で，最も厳しい条件 (広範囲に波及する) とした．

表 8 リスク値の比較: CWSS vs CRSS

脅威	基準		攻撃可能性				環境				リスク値	
#	TI	AP	RP	RL	AV	AS	BI	DI	EX	EC	CWSS	CRSS
13	H	A	N	N	I	N	C	M	H	N	75.8	9.43
30	L	A	A	A	I	N	L	M	M	I	13.2	9.43
31	M	A	L	N	I	W	M	L	H	I	23.3	9.43
34	L	A	A	A	I	N	L	M	M	I	13.2	9.43
35	M	A	L	N	I	W	M	L	H	I	23.3	9.43
36	L	A	A	A	NA	NA	L	H	H	N	33.7	9.43
37	M	A	L	N	I	W	L	L	H	I	18.1	9.43
11	H	A	A	A	I	W	L	L	M	I	15.4	8.77
12	C	A	L	N	I	W	C	M	H	I	38.3	8.77

表 8 は，固定値とした 6 つを除外した 10 個のパラメータとスコアを示した．CRSS の結果と CWSS の結果ではスコア順位が入れ替わっている脅威もあり興味深く，今後の検討事項とし，我々の評価方式に組み入れるなどの研究を進めたい．

なお，パラメータが増えることがコストの増加につながるという懸念があり，検討ではその解消をどうやって実現するかについても進めたい．リスク分析の手順で重要なのはパラメータを数値化する際の評価指標を如何に明確に具体的にできるかであると考える．CRSS と比較して CWSS で難しいと思えたのがパラメータの数よりもむしろそれらのランク付けであり，TOE のリスク評価のプロジェクト単位で厳格な評価指標を決め，パラメータの数値化が出来さえすればリスク値の計算に時間はほとんどかからないため，コストの増加は懸念すべきことではなくなると思われ，今後の検討で具体化する．

6. おわりに

産業制御システムの一翼を成すデータロガーシステムを対象とし，車載システムの設計方式を適用した網羅的な検討を行い，高いリスクの脅威を明らかにした．結果として，本方式は，脅威抽出フェーズには，高い親和性を確認できたが，モデル定義フェーズについては，産業制御システム固有の観点で再度詳細な検討を必要とし，リスク評価フェーズについては，方式の最適性についての課題が残った．今後の課題として，CWSS ベースのリスク評価の優位性検証を CRSS や CVSS v3 等のとの比較により行う．

参考文献

[1] J. Eric Byres, M. Franz, and D. Miller. ”The use of attack trees in assessing vulnerabilities in SCADA systems.” Proceedings of the international infrastructure survivability workshop. 2004.

[2] N. Falliere, L. O Murchu, and E. Chien, “W32.Stuxnet Dossier”, Symantec Security Response, Feb. 2011.

[3] IEC TS 62443-1-1:2009 Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models

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

[5] ITU-T X.1521: Cybersecurity information exchange, Vulnerability/state exchange, Common vulnerability scoring system

[6] ITU-T X.1524: Cybersecurity information exchange, Vulnerability/state exchange, Common weakness enumeration

[7] ITU-T X.1525: Cybersecurity information exchange, Vulnerability/state exchange, Common weakness scoring system

[8] S. Karnouskos: ”Stuxnet Worm Impact on Industrial Cyber-Physical System Security”. In: ”37th Annual Conference of the IEEE Industrial Electronics Society (IECON 2011), Melbourne, Australia”, November 2011.

[9] Y. Kawanishi, H. Nishihara, D. Souma and H. Yoshida, “Detailed analysis of security evaluation of automotive systems based on JASO TP15002, “ DECSoS: Dependable Smart Embedded Cyber-physical Systems and Systems-of-Systems, LNCS 10489, 2017, Springer (to appear).

[10] 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.

[11] JPCERT コーディネーションセンターと独立行政法人情報処理推進機構 (IPA)「脆弱性対策情報データベース JVN iPedia」

[12] M. S. Lund, B. Solhaug and K. Stolen, Model-Driven Risk Analysis, The CoRAS Approach, Springer-Verlag Berlin Heidelberg, 2011.

[13] E. LeMay, W. Unkenholz, D. Parks, C. Muehrcke, K. Keefe and W. H. Sanders, ”Adversary-driven state-based system security evaluation.” Proceedings of the 6th International Workshop on Security Measurements and Metrics. ACM, 2010.

[14] 内閣サイバーセキュリティセンター（NISC)，「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」の策定について」，2015.

[15] B. Meixell and E. Forner, “Out of Control: Demonstrating SCADA Exploitation”, Black Hat 2013.

[16] NIST Special Publication 800-82 Revision 2 Guide to Industrial Control Systems (ICS) Security

[17] S. C. Patel, J. H. Graham and P. A.S. Ralston, Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements, International Journal of Information Management Vol. 28, pp.483-491, 2008.

[18] S. Patel and J. Zaveri. ”A risk-assessment model for cyber attacks on information systems.” Journal of Com-

puters 5.3, pp.352-359, 2010.
[19] A. 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.
[20] A. Roy, D. S. Kim, K. S. Trivedi: ACT: Towards unifying the constructs of attack and defense trees, Security and Communication Networks, 2011:3:1-15
[21] SANS, "Analysis of the Cyber Attack on the Ukrainian Power Grid", March 2016
[22] UL 2900-2-2: Outline of Investigation for Software Cybersecurity for Network-Connectable Products, Part 2-2: Particular Requirements for Industrial Control Systems, 2016.