サイバーセキュリティの動向と最新対策技術

武本 敏 Takemoto Satoshi
萱島 信 Kayashima Makoto
宮崎 邦彦 Miyazaki Kunihiko
福澤 寧子 Fukuzawa Yasuko

社会インフラを支えるITシステムは，情報系システム，制御系システム，およびそれらを高度に融合したCyber Physical Systemsとして発展を遂げている。その一方で，不正アクセスは高度化・大規模化し，従来は安全と考えられていた制御系システムも深刻なサイバー攻撃に直面してきている。
日立グループでは，Secureplazaおよびマネージド・セキュリティ・サービスによるセキュリティソリューション，Cyber Physical Systemsを視野に入れた制御系システムのセキュリティ対応，HIRTによるインシデント対応，進化する標的型攻撃などに対抗するマルウェア解析など，総合的なサイバーセキュリティを提供している。また，安全・安心な社会インフラの実現のために，先進的な研究開発に取り組んでいる。

1. はじめに

近年，IT（Information Technology）システムはクラウドコンピューティングと携帯情報端末を中心に急速な進展を遂げており，サイバーセキュリティ技術が果たす役割はますます大きくなっている。クラウドコンピューティングの普及は，オンデマンドで大規模リソースを確保できるなどの利便性が高まる一方で，クラウドのシステム管理者による不正アクセスやデータの漏えいといった問題も懸念されている。また，情報系と制御系のシステムが融合したCyber Physical Systemsは，スマートグリッドやスマートシティなどの新たな社会インフラの創出を期待させるが，昨今は，従来は想定されなかった制御系システムへのサイバー攻撃が顕在化している。例えば，制御系システムに侵入して制御装置に異常をきたすマルウェアStuxnetや，人命に影響を及ぼしかねない自動車や医療機器などの組込み機器への不正アクセスなどが報告されている。その手法としては，人間の心理的な隙や行動のミスを利用して攻撃し，被害を及ぼすソーシャルエンジニアリングが台頭してきている。

一方，ITシステムやそれを構成する製品の開発や部品調達の現場では，オープン化やグローバル化，COTS（Commercial off-the-shelf）化が進み，サプライチェーンが構築されている。この状況下では，セキュリティに関わる開発や管理も国内外のサプライヤーに委ねられるため，サプライチェーン全体でいかにセキュリティを確保するかという問題にも直面している。

以上のような動向を踏まえ，日立グループは，サイバーセキュリティに対し，総合的なサービス・製品，技術の提供に取り組んでいる。具体的には，コンサルティングからセキュリティ施策や運用サービスまでを提供するSecureplaza[1)]およびマネージド・セキュリティ・サービス，Cyber Physical Systemsを視野に入れた制御系システムのセキュリティ，HIRT（Hitachi Incident Response Team）による製品やソリューションの脆（ぜい）弱性対策とインシデントへの対応，環境を選ぶマルウェアを自動的に解析する多種環境動的解析システムなどである（それぞれについては別稿を参照）。

日立グループが提供するセキュリティサービス・製品への適用を視野に入れて取り組んでいる先進的な研究開発として，ここでは，形式手法を用いたセキュリティ検証技術，安全なクラウドコンピューティング環境を実現する技術，組込みシステムのセキュリティ評価技術について紹介する。

2. 形式手法を用いたセキュリティ検証技術

形式手法は，数理論理学的な基盤の上で，仕様やプログラムに不具合や不整合がないことを機械的に検証する技術

である。例えば，航空，鉄道，自動車などの分野においては，国際規格などで形式手法を利用した開発が推奨されるなど，高い安全性・信頼性が要求される分野において特に注目されている技術である。日立グループにおいても，効率的な形式手法適用を支援するソフトウェア公開[2]や，自動車制御ソフトウェア向け形式検証技術の研究開発[3]などに取り組んでいる。

形式手法の特徴は，ある範囲において不具合がないことを網羅的に示せる点にある。この特徴は，どのような攻撃者が存在するか分からない状況であっても安全であることの保証が期待されるセキュリティの検証を行ううえでも有用である。形式手法を用いたセキュリティ検証技術の代表例として，暗号プロトコルの安全性評価技術が挙げられる。

暗号プロトコルは，さまざまな暗号機能（暗号化，電子署名など）を組み合わせて安全な通信路を確立するための技術であり，TLS（Transport Layer Security），IPsec（Security Architecture for Internet Protocol）などの例が代表的である。これらは，インターネット上での通信をはじめとした日々のさまざまな通信の安全性を支えるうえで必要不可欠になっている。

しかし，暗号プロトコルが安全であることの検証は容易ではない。部品として利用される暗号機能そのものが安全であることは当然求められるが，それだけでは不十分である。

次の手順は，Needham–Schroeder public-key protocolと呼ばれる，鍵共有のための暗号プロトコルの手順を示している。

（1）A → B: $\{Na, A\}_{Kb}$

（2）B → A: $\{Na, Nb\}_{Ka}$

（3）A → B: $\{Nb\}_{Kb}$

Nxはエージェント X が生成する乱数，$\{\cdot\}_{Kx}$ はXの公開鍵Kxで括弧内のデータを暗号化することを示す。

この手順に従ってプロトコルの実行が完了したとき，Na，NbがAとBの間で秘密裏に共有された鍵となる。このプロトコルは，1978年に提案されて以来，20年近く安全であると考えられてきた。しかし，A，Bとは異なる攻撃者が，AとBのやり取りに入り込むことでNa，Nbを知ることができるという攻撃が1996年にLoweによって発見された。この攻撃は，部品として使っている暗号関数 $\{\cdot\}_{Kx}$ を破ることなく実行可能である。

このような比較的単純な仕様であってもプロトコルの安全性を検証することが難しいのは，プロトコルが，複数のエージェントによって並行的，かつ，非決定的に実行されるためである。起こりうるすべての状態を抜けや漏れのないように確認することは一般には困難となる。

Loweは，上述の攻撃に関する一連の研究の中で，FDR（Failures-Divergence Refinement）という形式手法ツール（モデル検査ツール）を使用して攻撃の確認と改良プロトコルの安全性検証を行った。現在では，モデル検査法，定理証明法などの形式手法に基づく検証手法・ツールが多数開発・提案され，WiMAX※1)や欧州鉄道通信規格などの実用的なプロトコルの安全性についての評価も進んでいる。

ところで，このような形式手法を用いた暗号プロトコル検証手法・ツール相互の関係は必ずしも明確ではなく，評価結果を実際上どのように理解すればよいかは明らかではなかった。

そこで，日立グループは，2006年ごろから暗号プロトコルの安全性評価基準についての国際標準づくりを進めてきた。独立行政法人情報通信研究機構や独立行政法人産業技術総合研究所と共同で，ISO/IEC JTC/1 SC/27 WG/3においてProject Editorとして標準化を推進した結果，2011年にISO/IEC 29128（Verification of Cryptographic Protocols）が発行された。この規格では，プロトコル評価を行ううえで，共通的に必要になると考えられる記述事項（プロトコル仕様，攻撃者モデル，セキュリティ要件，自己評価）を規定し，また，検証の度合いに応じてPAL1（非形式的な議論），PAL2（形式的な手証明），PAL3（ツールによる有限チェック），PAL4（ツールによる無限チェック）の4つのプロトコル保証レベルを定義している。

また，2013年12月には独立行政法人情報通信研究機構，日立製作所，株式会社KDDI研究所，日本電信電話株式会社によって暗号プロトコル評価技術コンソーシアム（CELLOS：Cryptographic Protocol Evaluation toward Long-lived Outstanding Security）が設立された[4]。これは，暗号プロトコルの安全性に関する国際的に信頼できる情報の集約と共有，ICT（Information and Communication Technology）システムに即した議論，それらから得た安全性情報の公開，安全な暗号プロトコルの普及促進を目的とした組織である。国内外の大学や研究機関，関係企業が参画し，日本のみならず，国際的な協力体制で活動を推進している。

3. 安全なクラウドコンピューティング環境を実現する技術

クラウドコンピューティングの利用は，オンデマンドでの大規模リソースの確保など，多くの利便性をもたらす。一方で，データをクラウドに預けるユーザーは，クラウド側のシステムを見ることができないため，システム管理者

※1）WiMAXは，WiMAX Forumの登録商標である。

を含む不正アクセス者による情報漏えいに対応しなければならない。そこで，クラウド側での処理は，秘匿した情報をベースに行う「生体情報を用いた電子署名技術」と，「秘匿情報処理技術」を研究開発している。

3.1　生体情報を用いた電子署名技術

従来の認証強化技術として，IC（Integrated Circuit）カードなどのハードウェアトークンの利用や公開鍵暗号基盤（PKI：Public Key Infrastructure）の活用などがある。これらは，セキュリティの強化につながる反面，利便性や費用対効果の面で課題がある。また，これまでの生体認証ではICカードなどの耐タンパ装置を用いるか，センター集中型で認証情報を厳密管理しなければならないなどの課題があった。そこで，生体情報（テンプレート）を復元できない形に変換することで，プライバシーを保護しつつ安全に公開し，認証や署名に利用可能とする，テンプレート公開型生体認証基盤（PBI：Public Biometrics Infrastructure）[5]を開発した※2)（図1参照）。

PBIは，秘密鍵に誤差を許容する新しい電子署名方式により，生体情報を取得するたびに必ず発生してしまうアナログデータの誤差が一定の範囲内であれば，誤り訂正処理と適切な閾（しきい）値の設定で署名検証（認証）を可能としている。また，電子署名を検証する公開鍵（公開テンプレート）からは元の生体情報を復元できないことから，生体情報の漏えいや偽造を防止しつつ，誰もが署名検証（認証）することができる。さらに，今回の開発技術は，数学的に安全性が証明されているWaters署名※3)と呼ばれる署名方式に安全性を帰着させることで，どのような攻撃を受けても決して破れないことを証明できている。

この方式の活用により，厳密なユーザー認証を必要とする決済システムや電子行政システムなどのクラウド化，それらの関係する複数のシステム間のID連携が低コストで実現する。

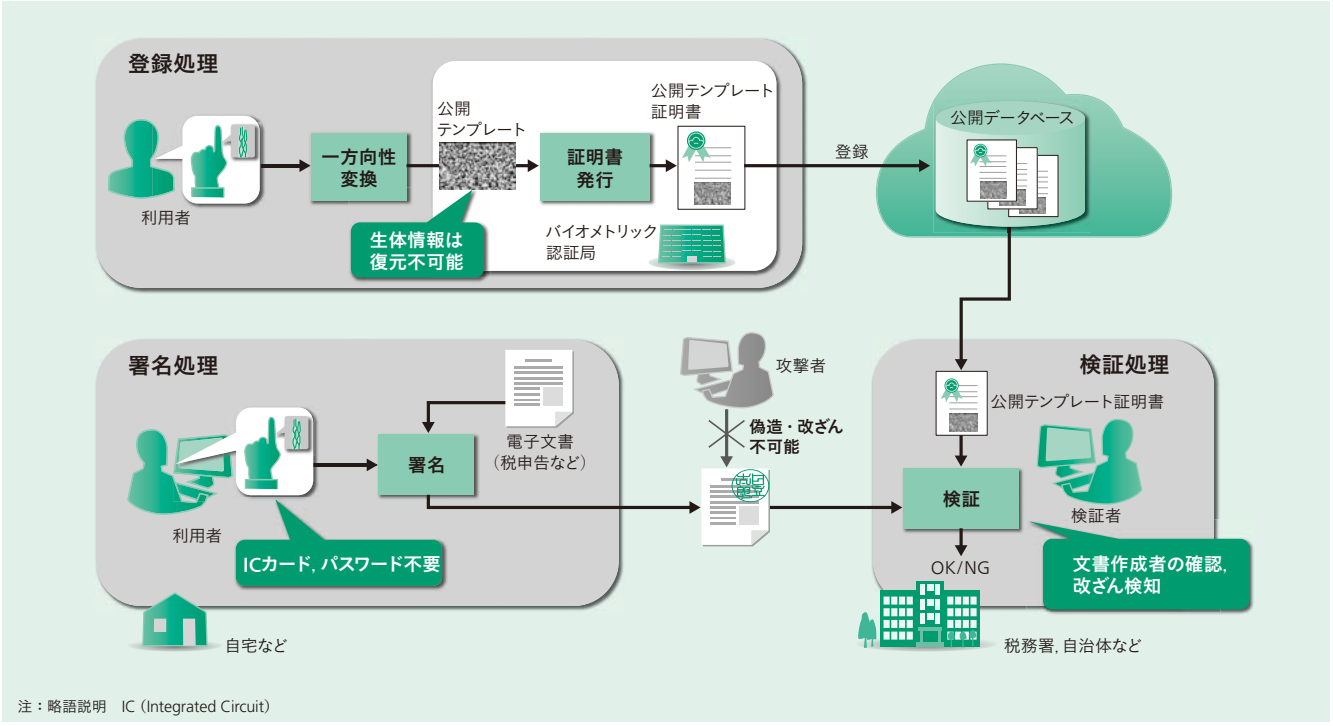
3.2　秘匿情報処理技術

システムで用いるデータの機密性を確保する場合は，従来，データの暗号化が一般的に用いられるが，データ処理時には復号しなければならず，その際にシステム管理者やマルウェアなどにデータをのぞき見られるリスクがある。

このリスクの低減策として，日立グループは，高速検索可能暗号方式[6]を開発した※4)（図2参照）。共通鍵暗号方式をベースにすることによる高速性と，準同型暗号技術の応用によって異なる暗号文間の比較を実現した高い安全性を確保している。

また，この技術を応用し，複数の分析キーワードが暗号

※2）この技術は総務省から受託した「災害に備えたクラウド移行促進セキュリティ技術の研究開発」の成果を含む。
※3）2005年にBrent Watersが発表した電子署名方式。電子署名方式の安全性の定義として広く受け入れられているEU-CMA（選択平文攻撃に対する存在的偽造不可能性）を満たすことが，CDH（Computational Diffie-Hellman）仮定と呼ばれる数学的な仮定の下で証明されている。
※4）この技術は総務省から受託した「災害に備えたクラウド移行促進セキュリティ技術の研究開発」の成果を含む。



注：略語説明　IC（Integrated Circuit）

図1｜テンプレート公開型生体認証基盤
厳密なユーザー認証を必要とする決済システムや電子行政システムなどのクラウド化，それらの関係する複数のシステム間のID連携を低コストで実現することにつながる。

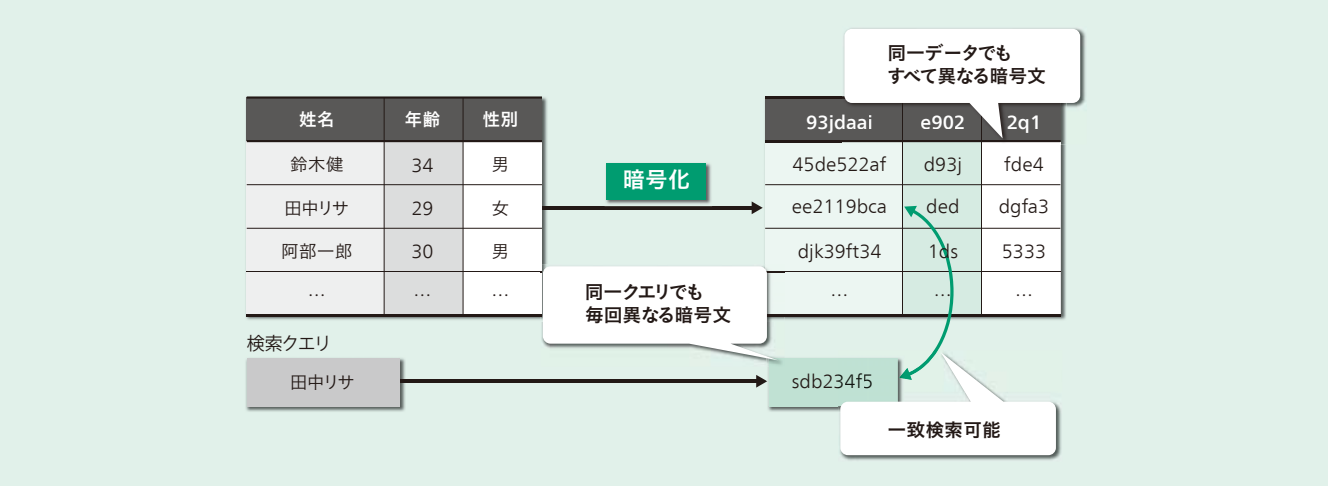


図2｜検索可能暗号の主な特徴

共通鍵暗号方式や準同型暗号技術を応用することで，高速性と安全性を確保している。

化データベース中に出現する頻度を求め，それらを比較して相関ルールを調べる秘匿分析技術[7]を開発し，実用化を進めている。

4. 車載組込みシステムのセキュリティ検証技術

近年，自動車などの組込み分野においても，IT分野で広く使われているネットワークやデバイス，OS（Operating System）などが活用され始めており，サイバー攻撃に対する備えが重要になっている。ネットワークを介して車載組込みシステムを遠隔操作した実証例もあり，攻撃によって人命に影響が及ぶ危険性が想定される自動車においては，自動車セキュリティの早期確立が求められている。

早くから自動車セキュリティの検討を行っている欧州では，第7次研究開発枠組み計画（FP7）において，HSM（Hardware Security Module）の規格を提案するとともに，HSMを搭載する車載組込みシステムを対象とするセキュリティ評価の検討を開始している。

このため，日立グループは，1980年代に培ったプラントの安全性解析技術をベースにしたセキュリティ評価技術を車載組込みシステムに適用した。また，日本国内におけるセキュリティ評価技術の標準化に参画し，脅威抽出およびリスク評価手法を提案している。

この車載組込みシステム向けセキュリティ評価技術の中核となる脅威事象の抽出およびリスク評価手法について以下に述べる。

4.1 評価対象システムの定義

セキュリティの脅威事象は，評価対象システムにおいて，「どの保護資産に，どんな脅威エージェントが，何を起こすのか」で記述することができる。

車載組込みシステムでは，従来から保護資産として認識されている「情報」に加え，エンジンやブレーキなどを制御する「機能」，および組込みシステムの「ファームウェア」も保護資産として定義した。これらの保護資産の在りかと，保護資産に対するデータフローを整理した「データフローダイアグラム」によってシステムモデルを作成する。

脅威エージェントとしては，自動車の製造から，新車および中古車の購入者による利用を経て廃棄されるまでの製品ライフサイクル全体における関与者を整理する。これは，車載組込みシステム内の機密情報が，通常の利用時だけでなく，製造工程や納車時，整備点検時などでも格納・参照されることを考慮するためである。

何を起こすのか，すなわち攻撃内容は，評価対象のエントリーポイントごとに事象を整理するとともに，保護資産のタイプに応じて「機密性」，「完全性」，「可用性」の侵害に分けて検討する。例えば，車載情報システムの「機能」は，意図したとおりにきちんと動作することが重要であり，完全性と可用性の喪失は避けなければならない。また，ITS（Intelligent Transport Systems）車載器がセンターサーバとの間でやり取りする情報は，盗聴・改ざんされていないことが重要であり，機密性と完全性の喪失は避けなければならない。

4.2 脅威事象の抽出

評価対象に対し，4つの観点を用いて脅威事象を抽出す

表1｜脅威事象を抽出する観点

評価対象システムの定義で整理したシステムモデル，ライフサイクル，攻撃内容を4つの観点に当てはめる。

観点	説明
Where	攻撃を実行するエントリーポイントを明確化
Who	脅威エージェントを明確化
When	脅威発生の機会を明確化
What	攻撃の具体的な内容を明確化

る（表1参照）。

前節で述べた評価対象システムの定義で整理したシステムモデル，ライフサイクル，攻撃内容をこれらの観点に当てはめることにより，「どの保護資産に，どんな脅威エージェントが，どのようなタイミングで何を起こすのか」を網羅的に抽出することができる。

4.3 リスク評価

ITシステムの脅威に対するリスク評価は，脅威事象をどのように実施するかによって決まる攻撃コストと保護資産の価値によって算出する手法が一般的であった。これは，攻撃事例が多数あり，それらの事例を実現するために必要な実行時間や攻撃者の能力など，攻撃方法のコストについてのコンセンサスが得られている場合には有効な方法である。

車載組込みシステムにおいては，まだ研究レベルでの攻撃事例がいくつか判明している段階であり，ITシステムのようにさまざまな攻撃手法のバリエーションは存在しない。このため，攻撃方法のコストを見積もることは困難であると考えている。そこで，ITシステムの脆弱性の深刻度評価に用いられているCVSS（Common Vulnerability Scoring System）を参考に，脅威のリスクを評価する手法を開発した。

この手法は，抽出した脅威事象に対して機密性，完全性，可用性の観点から保護資産に資産価値を割り当てるとともに，脅威エージェントがどれだけ保護資産に接近する必要があるか，およびアクセスする際の関門の有無によって算出した攻撃の容易度からリスク値を計算する。この手法では，車載組込みシステムのようにセキュリティの脅威に対するノウハウが蓄積されていない分野においても，脅威事象および評価対象システムの定義内容から解析的にリスク値を算出することが可能である。また，保護資産の価値に関しても，「機能」を保護資産として捉え，完全性や可用性の喪失が重大な結果をもたらす機能に対しては資産価値を高く見積もるように調整することで，人命などへの影響を考慮したリスク評価を可能にするものである。

5. おわりに

ここでは，社会インフラを支えるITシステムを取り巻くサイバーセキュリティの動向と，動向を見据えた先進的な研究開発の取組みについて述べた。

今後も，新たなセキュリティソリューションの提供と，そのための技術開発に取り組み，それらを通じて，安全・安心な社会インフラの実現に貢献したいと考えている。

参考文献など

1) セキュリティソリューション Secureplaza：日立，
http://www.hitachi.co.jp/Prod/comp/Secureplaza/index.html
2) 日立ニュースリリース，社会インフラシステム向けの高信頼で高効率なソフトウェア開発技術を公開（2013.2），
http://www.hitachi.co.jp/New/cnews/month/2013/02/0212a.html
3) 日立ニュースリリース，形式手法を用いた自動車制御ソフトウェアの高信頼検査技術を開発（2013.4），
http://www.hitachi.co.jp/New/cnews/month/2013/04/0416a.html
4) 日立ニュースリリース，「暗号プロトコル評価技術コンソーシアム」の設立について（2013.12），
http://www.hitachi.co.jp/New/cnews/month/2013/12/1219b.html
5) 日立ニュースリリース，生体情報を用いた電子署名技術の開発に成功（2013.2），
http://www.hitachi.co.jp/New/cnews/month/2013/02/0218.html
6) 日立ニュースリリース，クラウド上での情報漏えい防止に貢献する検索可能暗号技術を開発（2012.3），
http://www.hitachi.co.jp/New/cnews/month/2012/03/0312.html
7) 日立ニュースリリース，暗号化したままデータ分析を行う秘匿分析技術を開発（2014.1），
http://www.hitachi.co.jp/New/cnews/month/2014/01/0121b.html

執筆者紹介

武本 敏
日立製作所 情報・通信システム社 サービスプロデュース統括本部 セキュリティ先端技術本部 セキュリティ先端技術部 所属
現在，セキュリティ先端技術の技術開発およびその事業化に従事

萱島 信
日立製作所 横浜研究所 情報サービス研究センタ エンタープライズシステム研究部 所属
現在，情報セキュリティ技術の研究開発に従事
博士（工学）
電子情報通信学会会員，情報処理学会会員，人工知能学会会員

宮崎 邦彦
日立製作所 横浜研究所 情報サービス研究センタ エンタープライズシステム研究部 所属
現在，形式手法，情報セキュリティ技術の研究開発に従事
博士（情報理工学）
電子情報通信学会会員，情報処理学会会員

福澤 寧子
日立製作所 横浜研究所 情報サービス研究センタ エンタープライズシステム研究部 所属
現在，情報セキュリティ技術の研究開発に従事
博士（工学）
電気学会会員，電子情報通信学会会員，情報処理学会会員