セキュリティ研究開発
先進セキュリティ技術の研究開発

鍛 忠司
Kaji Tadashi

近年のサイバー攻撃は，ITシステムに加えインフラを実現するIoTシステムをも対象とし，その被害は社会全体に波及しつつある。このような状況にあって，日立は社会インフラを安全・安心に構築・運用することを使命とし，長年にわたりサイバーセキュリティの研究開発を継続して推進している。

本稿は日立が提案するセキュリティコンセプトであるH-ARCの実現に向けて実施している研究開発について概観する。これらの研究により，長期間にわたって安心して利用できる堅牢なIoTシステムを設計・開発し，システムに関わるステークホルダーと協調してサイバー攻撃への迅速な対応の実現をめざす。

1. はじめに

IT（Information Technology）システムを対象とするサイバー攻撃がより高度化している。企業活動のITへの依存度の高まりもあり，ITシステムへの攻撃による被害は経営リスクに直結するようになった。

さらに制御系分野においても，ITをベースにモノどうしを接続するIoT（Internet of Things）システムの登場により，従来はサイバー攻撃から疎遠であった領域においてもセキュリティ対策が必要になりつつある。このため，サイバーセキュリティの研究活動でも新たな課題に取り組むことが重要になっている。

本稿では，このような状況に対応するために実施している新たな研究開発の概要を，日立の提唱するセキュリティコンセプトを交えて述べる。

2. 日立の考えるセキュリティコンセプト「H-ARC」

社会インフラを支えるIT/IoTシステムにおいては，情報の保護だけでなく，あらゆる脅威をも想定して社会インフラがサービスを提供し続けられるかといった観点でもセキュリティに取り組む必要がある。また，ネットワークに接続されたデバイスが増えており，これまでに攻撃の対象とならなかったモノも被害を受ける可能性が高まっている。さらに，さまざまな機能を実現するためにIT/IoTシステムどうしの連携も始まっている。

このためわれわれは，IT/IoTシステムの情報セキュリティを確保するうえで，以下の3つの潮流への対応が必須と考えている。

(1) 脅威の多様化
(2) 事後対処の重要性
(3) 相互依存の拡大

これらの潮流に対応すべく，日立は2013年からH-ARCコンセプトを提唱している[1)]（図1参照）。

ITシステムの情報セキュリティを高めるためには，コ

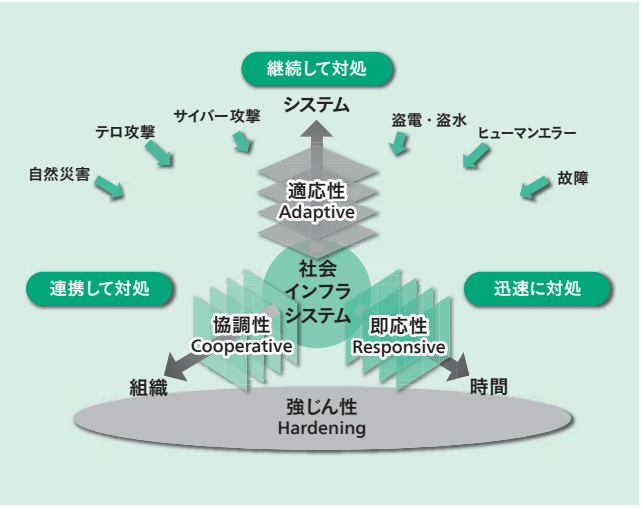


図1｜H-ARCコンセプト
従来からの強じん性という概念に加え適応性，即応性，協調性という観点からセキュリティの強化ポイントを明確化した。

ンポーネントのセキュリティ機能の実現と，システムのセキュリティ運用マネジメントの両輪を実施していくことが大切である。H-ARCコンセプトは機能とマネジメントの両面に関し，3つの潮流に対応するためのセキュリティの強化ポイントを示すものである。

3. H-ARCの特徴

本章では，H-ARCのめざすセキュリティの全体像を示す。

3.1 堅牢なシステムの実現

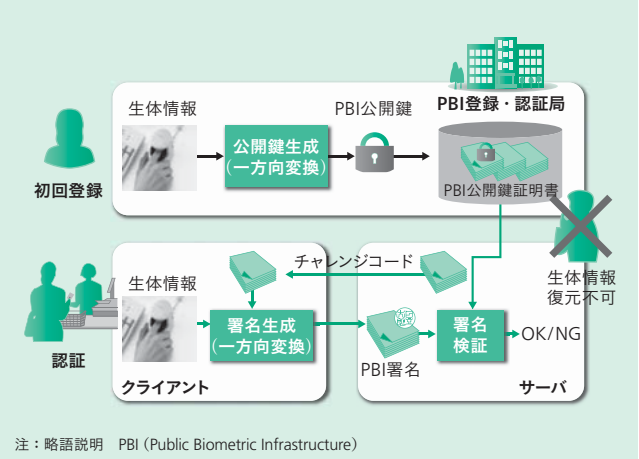
サイバー攻撃はシステム内の保護対象資産に対する機密性，完全性，可用性を侵害するために実行されるアクションである。このようなアクションに対抗するため，システムはより堅牢（ろう）な実装を行うことが必要である。

ITシステムにおけるサイバー攻撃対策は，ユーザーを識別・認証し，本人であることを確認してアクセスを許可することがまず基本となる。従来のシステムではユーザーのみが知りうるパスワードを提示させることにより本人を確認するユーザー名／パスワード認証や，本人が所持するIC（Integrated Circuit）カードを提示させ，その内部の本人識別情報は本人のみが引き出せるようにPIN（Personal Identification Number）コードで保護する方式が一般的である。

しかし現在のITシステムでは，ユーザーをだましてパスワードを教えさせる，いわゆるソーシャルエンジニアリングと呼ばれる手法や，フィッシングサイトといったパスワードをだまし取るサイトによる被害が多発している。また，安易なパスワードの推測や，手帳などに書いておいたパスワードを盗み見るなどの手口や，パスワードの再設定サイトを悪用する手口などがあり，従来技術で構築されたシステムは必ずしも堅牢と言えなくなってきている。

そこで日立は，攻撃者に盗み取られることのない生体情報と現時点で最も堅牢であるPKI（Public Key Infrastructure：公開鍵基盤）を組み合わせ，より堅牢な本人確認を可能とするPBI（Public Biometric Infrastructure）を開発した（図2参照）。

また，モノどうしが接続されるIoTシステムは，ITシステムよりも低コスト化への要求が強く，処理性能を犠牲にしても安価なハードウェアを用いて実現されることが多い。このため，現状のIoTシステムにおいては，通信路の秘匿化や相手との相互認証といった暗号技術で実現されるセキュリティ機能を搭載することが難しかった。そこで日立は，IoTシステムにおいて利用されるハードウェアを対象として，従来の暗号方式と比較して乏しいリソースだけでも動作可能な省リソース暗号方式を開発している。



注：略語説明　PBI（Public Biometric Infrastructure）

図2｜PBIの仕組み

生体情報を一方向変換して生成したPBI公開鍵を利用することにより，攻撃者のなりすましを防止する本人確認機構を実現した。

3.2 長期利用に対する保証

IoTシステムで使用されるデバイスは，PC（Personal Computer）やスマートフォンと異なり，システム実現コストを下げるために10年以上の長期間にわたって使用されることがある。一方でサイバー攻撃の手法は日々巧妙に進化しており，システムを攻略する新たな脆（ぜい）弱性が発覚した場合にはソフトウェアにパッチを当てるなどの継続した対処が必要となる。

しかし，商用，オープンソースを問わず，ソフトウェアのメンテナンスは期限が設けられている。ITシステムにおけるメンテナンス期間は通常5年程度であり，長期保証を行うためにはできる限り脆弱性をなくすとともに継続した対処を考慮した設計を行うことが重要である。そこで日立は，IoTシステムを対象とするセキュリティ設計技術を開発した。

IoTシステムにおけるデバイスはセンサーとアクチュエータを有し，サイバー空間だけではなくフィジカル空間とのインタラクションを持つものがある。従来のITシステムでは，守るべき対象はサイバー空間内の情報が中心であり，第三者に情報を盗まれないことと，情報を改ざんされないことを中心にセキュリティ設計が実施されている。このため，IoTシステムもしくはデバイスのセキュリティ設計として，ITシステムで採用されていた手法がそのまま適用可能かは疑問の余地があった。特にコネクティドカーのように，サイバー攻撃が行われると，人命に関わりかねないIoTデバイスにおいては，情報だけではなく，デバイスが提供する制御機能もまた重要な保護対象として考える必要がある。

日立は，ITシステム向けのセキュリティ設計技術を拡張し，デバイスの提供機能も保護対象と考えて脅威を抽出し，対策を検討することを特徴とするIoTシステム向けセ

キュリティ設計技術を開発した。この技術は，標準的なセキュリティ設計手順に基づき，「評価対象定義」，「セキュリティ課題抽出」，「対策目標の立案」，「セキュリティ要件の策定」の4フェーズにより構成される。そして，セキュリティ課題の抽出と，対策目標の立案を解析的かつ網羅的にに実施することで，策定した各セキュリティ要件が何を防止するためのものであるかを論理的に説明できる点を特徴とする。

具体的には，セキュリティ課題の中で特に脅威事象の抽出を，機能を含む各保護対象資産に対し，どこから（Where），誰が（Who），いつ（When），何のために（Why），何を行う（What）の観点から網羅的に実施する。また，故障木解析（Fault Tree）手法を応用し，抽出されたすべての脅威事象に対し，その脅威を起こす攻撃者の動機，手順，および攻撃が成立する条件を詳細に解析し，Treeの末端事象に対抗する方法を検討することにより，論理的に説明可能な対策目標を立案する（**図3**参照）。

3.3　速やかな対応の実現

ITシステムは，半世紀にわたってさまざまなサイバー攻撃にさらされてきた。このためITベンダはセキュリティ設計に関するノウハウを蓄積するとともに，攻撃を受けた後に迅速に対処する能力（インシデントレスポンス）を強化してきた。

標的型攻撃に代表される最近のサイバー攻撃では侵入の発覚を逃れるために，狙ったOS（Operating System）やアプリケーションがインストールされた環境でしか動作しないような細工が施された高度なマルウェアが増加している。また，これらのマルウェアは既存のパターンマッチングによるウイルス対策では，その半数が検知できないとも言われている。

そこで日立はこのようなマルウェアによる脅威へ早期の対策をするために，細工されたマルウェアを多種多様な解析環境で実際に実行させてみて振る舞いを観測し，マルウェアの挙動を自動で短時間に解明する技術の研究を進めている。例えばマルウェアによる攻撃者サイトへの情報送信など，本技術で解明した挙動に基づき，そのサーバへの接続を遮断するといった出口対策が行えるようになり，インシデントレスポンスの即応化に寄与する（**図4**参照）。

3.4　情報共有によるセキュリティ強化

IT/IoTシステムが相互に連携することによって利便性は向上するものの，あるサブシステムへの攻撃・災害による被害が他のサブシステムに波及し，システム全体への被害に拡大する懸念がある。これに対応するためには，前節で述べたインシデントレスポンスにおける状況分析（Orient）や判断（Decide）を活用し，連携して対処することが必要になってきている。

日立は異なるシステムや仕組みをつなぐことによって生み出される価値を，それらのシステムに関わるステークホルダー全体に提供し，新たな成長を促す「共生自律分散」コンセプトを提唱している[2)]。

共生自律分散システムにおいてサブシステム間，すなわち異なる組織や事業者間で互いに状況を的確に認識するには，ISAC（Information Sharing and Analysis Center）などの組織やインシデントレスポンスチーム間での情報共有が必要である。また，速やかな対応を実現するには，インシデントレスポンスに関わる情報の機械的な処理を可能にすることも重要である。現在，ITシステムに関してはOASIS（Organization for the Advancement of Structured Information Standards）/CTI（Cyber Threat Intelligence）/TC（Technical Committee）において情報根幹フォーマット

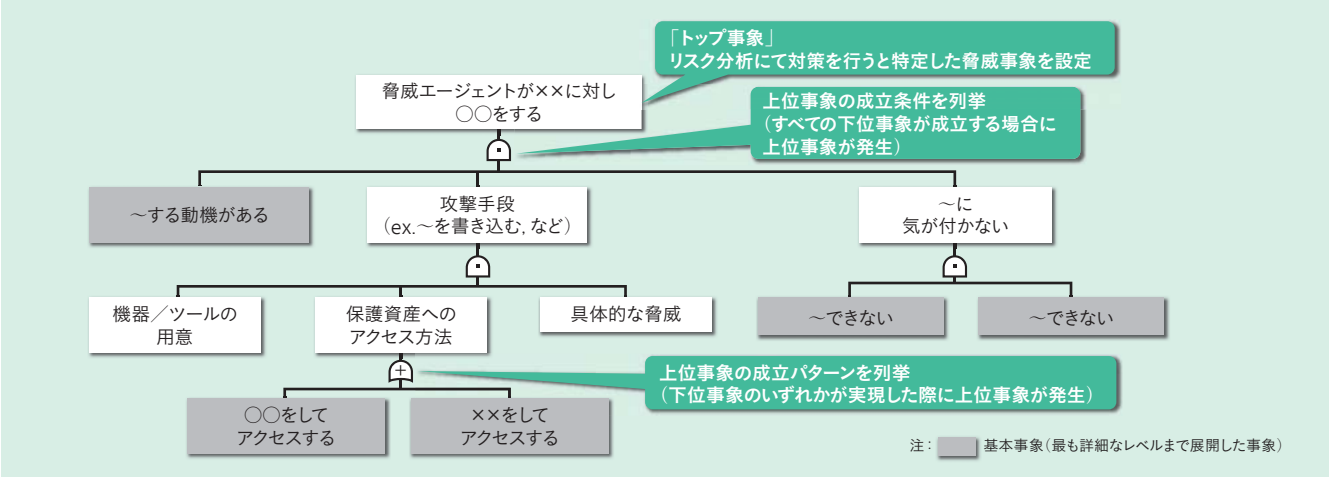
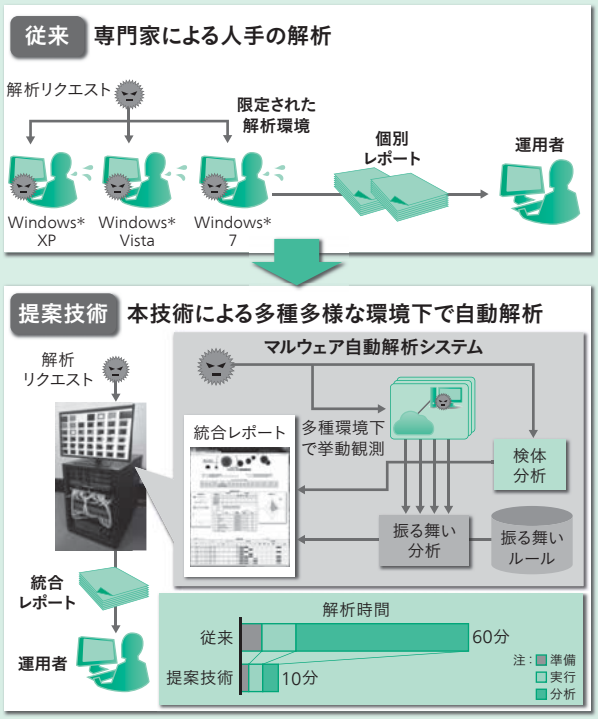


図3｜故障木解析（Fault Tree）を用いた脅威の対策目標立案
脅威事象が成立する要因を，動機，手順，成立条件の面から分析し，基本事象への対抗策を検討する。



注：＊Windowsは，米国Microsoft Corporationの米国およびその他の国における登録商標または商標である。

図4｜マルウェア自動解析技術

多種多様な環境下でのマルウェア自動解析により，環境によって振る舞いが変化するマルウェアの挙動を解明する。

として，STIX（Structured Threat Information Expression）/TAXII（Trusted Automated Exchange of Indicator Information）/CybOX（Cyber Observable Expression）といった規格が策定されつつあり，この規格をIoTシステムでも利用可能にする取り組みを開始したところである。

4. 標準化への取り組み

IoTシステムのセキュリティに関するさまざまな標準を策定する動きが加速している。Industry分野ではIEC（International Electrotechnical Commission）を中心に制御システム向けセキュリティ規格であるIEC62443の策定が進んでいる。またネットワークやITを中心とする分野ではIEEEやoneM2M（Machine to Machine），ISO（International Organization for Standardization），ITU-T（International Telecommunication Union Telecommunication Standardization Sector）などの標準化団体が連携しながらセキュリティ規格の策定を進めている。

日立は今までのIT/IoTシステム向けのセキュリティの標準化に対し，セキュリティコンセプトの確立に向けた貢献と，IoTシステムの特徴を鑑みたセキュリティ機能の実現に向けた貢献を実施している。

前者に関しては，IoT/ITシステムを取り巻く潮流に合わせ，単に堅牢なシステムを実現するだけではなく，長期利用に対する保証，速やかな対応の実現，情報共有によるセキュリティ強化を図るべくIECに対して貢献を進めている。また，日立は技術研究組合制御システムセキュリティセンターと協力して標準規格を用いた研究開発を行い，演習プログラムと普及啓発を進めている。

後者に関しては，CPU（Central Processing Unit）のスペックやメモリ搭載量が少なく，リアルタイムでの動作を要求されるIoTデバイスでセキュリティ機能を実装できるようにすることをめざし，省リソースで実行可能な暗号アルゴリズムをISO/IECに対して提案している。また，IoTデバイスどうしで相互認証やセキュアな通信路を利用するためには，軽量な暗号通信プロトコルが必要であり，ITU-Tにおいて標準方式を提案するとともにoneM2Mにおいて標準方式の策定に参画している。

5. おわりに

IT/IoTシステムは今後の社会インフラを支えていく基盤であり，サイバーテロへの対応を含めて最新の技術を活用した万全の対策を実施していくことが重要である。本稿では，IT/IoTシステムを支えるセキュリティの最新研究状況を，日立が提案するH-ARCコンセプトの観点から述べた。

低コストかつ長寿命のIT/IoTシステムにおいてサイバーセキュリティを確保するうえで，堅牢なシステムを実現する既存の技術を利用していくことは基本である。さらにシステム開発時において脅威を明確化し，長期間にわたって効力を発揮する最善の対策を実施していくこと，システム運用時に速やかな対処を実現すること，また，関連するステークホルダー間でセキュリティ関連情報を共有し，高度化するサイバー攻撃に対する備えを強化することが重要である。日立はこれらの観点に基づき，最新技術の研究開発を今後も推進し，安全・安心な社会インフラの実現に寄与していく。

参考文献

1） 三村，外：H-ARCコンセプトに基づく日立グループの社会インフラセキュリティ，日立評論，96，3，160～167（2014.3）
2） 入江，外：情報制御システム―共生自律分散で実現するオープンイノベーション―，日立評論，98，3，161～165（2016.3）

執筆者紹介

鍛 忠司
日立製作所 研究開発グループ システムイノベーションセンタ
セキュリティ研究部 所属
現在，企業向けIT・IoTシステムを対象とした情報セキュリティ技術の研究開発に従事
博士（情報科学）
IEEE CS会員