社会インフラの安全・安心を確保するサイバーセキュリティ技術

Cyber Security Technologies for Social Infrastructure Systems

鍛 忠司 Kaji Tadashi
山田 勉 Yamada Tsutomu
中野 利彦 Nakano Toshihiko
芹田 進 Serita Susumu

近年，サイバー攻撃の脅威があらゆる社会インフラシステムへ拡大する傾向が顕著になっている。
日立グループは「2×3コンセプト」という考え方の下，設計・開発・構築・運用のフェーズごとにセキュリティガイドラインを策定している。また，制約の厳しい制御機器やフィールドデバイスなどを含む社会インフラの隅々までセキュリティを確保するため，高速暗号実装技術，省電力ストリーム暗号「Enocoro※1)」，機器認証技術などを開発している。さらに，昨今の高度なサイバー攻撃に対し，大量のログや通信データを分析してシステム内に潜伏するウイルスを検知するなど，セキュリティ運用の負荷を軽減する技術を開発している。

1. はじめに

IT（Information Technology）を活用して社会インフラを効率化する取り組みがグローバル規模で進展しており，社会インフラのネットワーク化が加速している。このような社会インフラのネットワーク化に伴い，従来は企業情報システムの領域にとどまっていたサイバー攻撃の脅威が，あらゆる社会インフラシステムへ拡大する傾向が顕著になっている。特に，2010年にStuxnetウイルスが登場して以降，特定組織を対象に，複数の攻撃手法を組み合わせ，執ようかつ継続的に行われる「標的型攻撃」の被害が現実のものになってきている。

社会インフラシステムは，こうした高度なサイバー攻撃に対抗しながら運用を続けていく一方で，万が一の事態が発生した場合には「安全な状態」（システム停止状態など）に確実に移行することが必要である。そのためには，脅威に対して定められた状態遷移から逸脱しないよう，開発段階からセキュリティ機能を実装することが重要になる。

しかし，サイバー攻撃は日々進化しており，システム寿命の長い社会インフラシステムでは設計当初の想定を超える脅威が出現することも考慮しなければならない。そのため，昨今では，運用時におけるセキュリティ対策・対処が重要性を増してきている。また，社会インフラシステムでは，フィールドに設置される機器は処理能力や消費電力などのシステムリソースに厳しい制約がある機器が多く，セキュリティ対策の実装が困難な場合が多い。

ここでは，セキュリティ確保に対する日立グループの考え方と，社会インフラシステム全体にセキュリティ対策を実施するためのセキュリティ技術，および，安全・安心な運用を支えるセキュリティ技術について述べる。

2. 日立グループセキュリティの考え方 —2×3セキュリティ保証モデル—

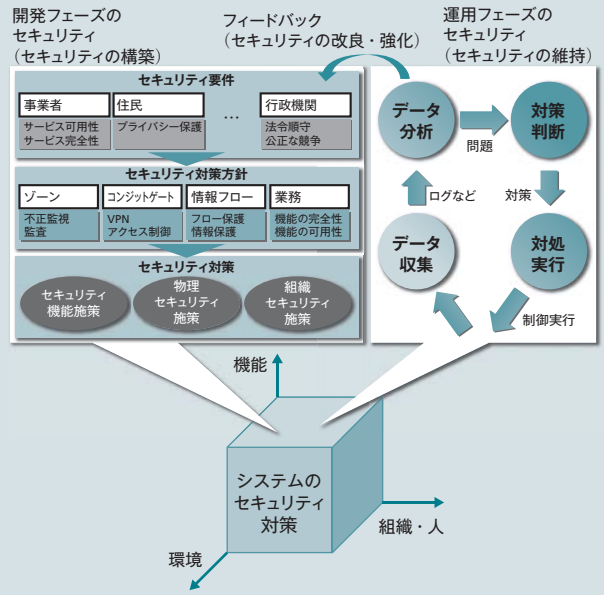
社会インフラシステム，特にその中の制御システムのセキュリティを確保するには，開発段階のセキュリティ機能の実装と，運用段階のセキュリティ対策・対処の両方が必要不可欠である。このための基本的な考え方が，「2×3セキュリティ保証モデル」[1)]である。

「2×3セキュリティ保証モデル」は，システムライフサイクルの2つのフェーズ（開発フェーズと運用フェーズ）において，機能，環境，組織・人という3つの観点で脅威に対策・対処し，漏れのないセキュリティを持続的に実現するという考え方である（**図1**参照）。

2.1 開発フェーズのセキュリティ

開発フェーズでは，システムのセキュリティを構築することを目的として，セキュリティ上の脅威を洗い出し，機能，環境，組織・人の3つの観点の対策を多層的に組み合わせ（多層防御），システムの機能の一部として組み込んでいく。

※1) Enocoroは，独立行政法人情報通信研究機構の委託研究「大容量データの安全な流通・保存技術に関する研究開発」（2005年度～2007年度）の開発成果を発展させたものである。



注：略語説明　VPN（Virtual Private Network）

図1｜2×3セキュリティ保証モデル

開発と運用の2つのフェーズで，機能，環境，組織・人の3つの観点から，脅威に対策・対処し，漏れのないセキュリティを実現する。

多層防御のセキュリティ機能を設計するには，IEC（International Electrotechnical Commission：国際電気標準会議）のIEC 62443[2]で提唱しているセキュリティコンセプトに基づき，システムを同一のセキュリティポリシーを適用する範囲（ゾーン）に分割し，ゾーンごとに必要なセキュリティ対策を検討・実装する必要がある。また，ゾーン間を安全なパイプ（コンジット）で接続し，その出入り口（コンジットゲート）にセキュリティ対策を施すことで，ゾーン内への不正者の侵入を防止する。

日立グループは，上述のシステム構成に着目したセキュリティ対策に加え，社会インフラシステムが提供するサービス（業務）単位で，業務を構成する機能の健全性や可用性，機能間で処理される情報フローの適切な保護などのセキュリティ対策も必要と考え，設計・開発・構築するためのセキュリティガイドラインを整備している。このガイドラインは，システムの重要度や顧客要件に応じて適切なセキュリティ対策を実装するためのものであり，NIST（National Institute of Standards and Technology：米国国立標準技術研究所）の発行するSP（Special Publications）800シリーズ，IECのIEC 62443シリーズなど，国内外の主要なセキュリティ規格に対応している。

2.2　運用フェーズのセキュリティ

運用フェーズでは，開発フェーズで構築したセキュリティを維持し続けることを目的として，システムのセキュリティ上の健康状態を把握し，発生している問題に迅速に対処していく。

昨今の高度なサイバー攻撃に対抗するためには，開発フェーズで十分なセキュリティ機能を実装するだけではなく，運用フェーズにおけるセキュリティ対策・対処が重要性を増してきている。運用フェーズでは，開発フェーズで構築したセキュリティを維持し続けることを目的として，システムのさまざまなポイントからデータを収集・分析することでシステムのセキュリティ上の健康状態を把握する。その結果，発生している問題を迅速に検知し，対処していく。さらには，運用フェーズから開発フェーズにフィードバックを行い，システムのセキュリティを改良・強化していく。

3.　社会インフラの隅々を覆うためのセキュリティ技術

高度なサイバー攻撃に対抗するには，社会インフラの隅々にセキュリティ対策を実施することが必要である。

一方，社会インフラシステムでは処理能力や消費電力などのシステムリソースに厳しい制約がある機器も多い。

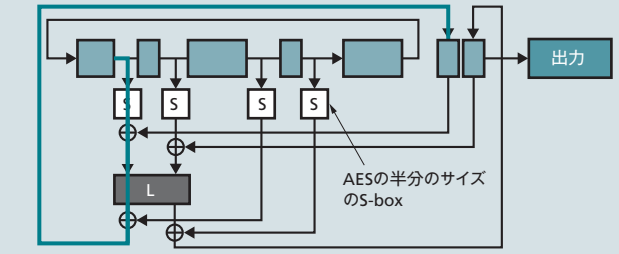
日立グループは，社会インフラシステムの隅々までセキュリティ対策を適用するため，こうしたリソース制約の厳しい機器にも適用可能な暗号技術，認証技術などを開発している。

3.1　省電力ストリーム暗号「Enocoro」

「Enocoro（エノコロ）」は2007年に開発した省電力ストリーム暗号であり，2012年には，小型機器向け暗号の国際標準規格であるISO/IEC 29192にも採択[3]されている。

Enocoroでは，暗号処理の構成要素の一つであるS-box（Substitution box）をAES（Advanced Encryption Standard）の半分のゲートサイズに抑えるとともに，低消費電力ロジックセルを有効活用するためにクリティカルパスを短縮している（**図2**参照）。

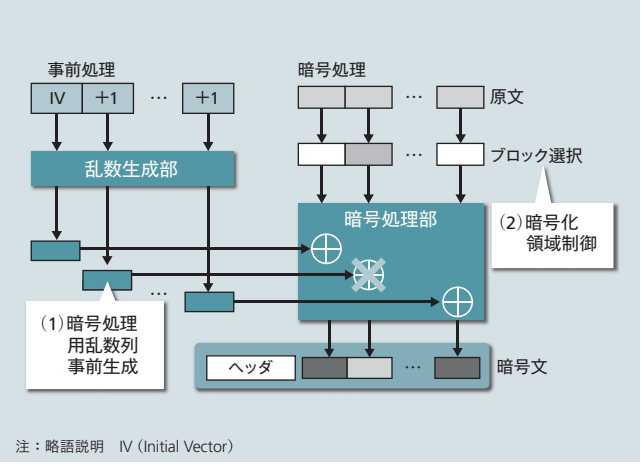
この結果，Enocoroはデータ暗号のデファクトスタン



注：略語説明　S（S-box：Substitution box），L（線形変換），
AES（Advanced Encryption Standard）

図2｜Enocoroの基本構造

S-boxをAESの半分のゲートサイズに抑えるとともに，低消費電力ロジックセルを有効活用するためにクリティカルパスを短縮している。



注：略語説明　IV (Initial Vector)

図3｜軽量暗号実装技術の概要

暗号化に必要な乱数列を事前に生成し，暗号化する領域を必要最小限に絞ることで高速・低負荷な暗号処理を実現している。

ダード（実質標準）であるAESと比べて，$\frac{1}{10}$程度の消費電力で暗号化処理を実現することができる。

3.2　軽量暗号実装技術

制約条件の厳しい機器での暗号通信実現にあたっては，前述のように軽量な暗号アルゴリズムの開発に加え，軽量かつ高速に実装する暗号実装技術も重要である。

日立グループは，暗号化に必要な乱数列を事前に生成することに加えて，暗号化する領域を必要最小限に絞ることにより，高速・低負荷軽量暗号処理を実現する技術を開発している（**図3**参照）。

この技術を用いると，標準暗号AESを用いた場合でも標準的に実装した場合に比べて約20倍の高速化を達成できる。具体的には，1,500バイトのデータを約40マイクロ秒で暗号化することができるため，従来は暗号化に要するオーバーヘッドが大きすぎることから暗号化通信が困難と思われていた領域へも適用可能となる。

4.　システム運用負荷を軽減するためのセキュリティ技術

システムの運用フェーズでは，システムのセキュリティ上の健康状態を把握し，発生している問題に迅速に対処していくことが必要である。

しかし，最近のサイバー攻撃は，攻撃活動を秘匿するためのさまざまな技術が用いられており，システム内に潜伏する攻撃者を見つけることは非常に困難になっている。

日立グループは，大量のログや通信データを数理工学の知見に基づいて分析し，問題を発見する技術の開発に取り組んでいる。具体的には，システム内に潜伏するコンピュータウイルスを検知する技術や，システムのセキュリティ状態を評価する技術を開発している。

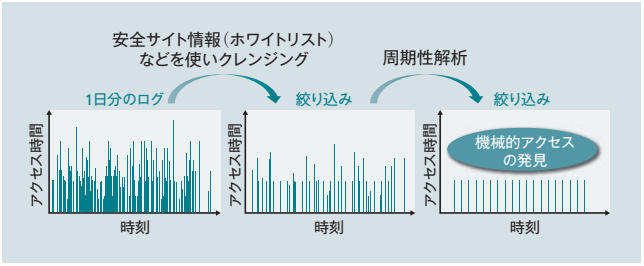


図4｜ログ分析による不正通信検知技術

コンピュータウイルスがC&C（Command and Control）サーバと定期通信するという特性を踏まえ，ログを周波数解析することで大量のログから機械的アクセスを発見する。

4.1　ログ分析による不正通信検知技術

コンピュータウイルスは，一般的なプログラムとは異なる特性を備えている。例えば，コンピュータウイルスは，C&C（Command and Control）サーバと呼ばれる指令サーバと定期的な通信を行い，観測した情報を送信したり，攻撃命令を受けたりする。

日立グループは，このようなコンピュータウイルスが備える特性を分析するとともに，その特性を踏まえ，大量に出力されるログからウイルス活動らしきログを自動的に抽出する技術を開発している。例えば，C&Cサーバと定期的に通信するという特性を利用し，ログを周波数解析することで，大量のログの中から機械的アクセスを発見する技術を開発した（**図4**参照）。

4.2　パケット分析による不正通信検知技術

ログ分析だけではなく，パケットの内容を解析して検査を行うDPI（Deep-packet Inspection）方式による不正通信検知技術も開発している。

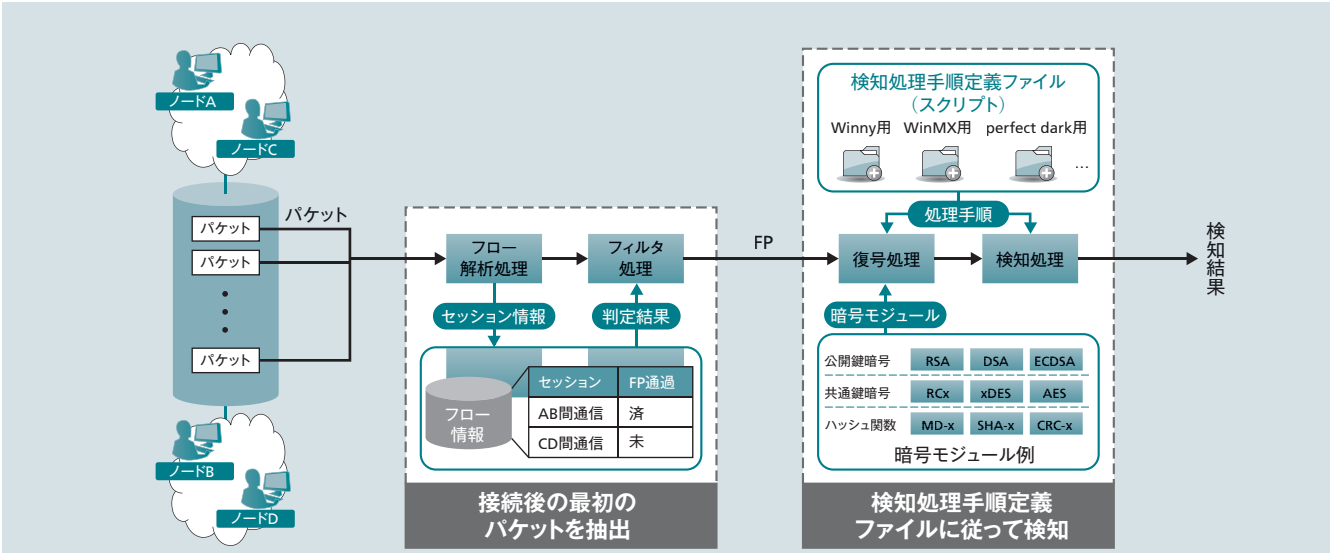
DPI方式は，複雑な演算処理が必要となる場合が多いため，大量データを処理するには処理負荷が大きくなるという課題がある。この技術では，ネットワークを流れるパケットを事前に絞り込みながら，検知処理手順定義ファイルに従って解析することにより，課題を解決し，広帯域のネットワークにおけるリアルタイムな不正通信の検知を実現した。

この技術をP2P（Peer to Peer）型ファイル共有ソフトウェアの通信検知に適用※2)し，10 Gビット/sのトラフィックの中から99.78％の高精度でこのソフトウェアの通信を検知することを確認している[4]（**図5**参照）。

4.3　システムのセキュリティ状態評価技術※3)

システムの規模が大きくなるにつれて，大小さまざまな

※2）この研究は，総務省委託研究「ネットワークを通じた情報流出の検知及び漏出情報の自動流通停止のための技術開発」の一環として実施された。
※3）この技術は，総務省委託研究「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　FP (Fast Packet)，RSA (Rivest Shamir Adleman)，DSA (Digital Signature Algorithm)，ECDSA (Elliptic Curve Digital Signature Algorithm)，DES (Data Encryption Standard)，MD (Message Digest)，SHA (Secure Hash Algorithm)，CRC (Cyclic Redundancy Check)

図5｜パケット分析によるP2P通信検知技術の概要
分析対象とするパケットを選択的に絞り込みながら，パケットを復号し，通信内容を解析することで高精度なP2P (Peer to Peer) 通信検知性能を達成している。

事象が日常的に発生するため，すべての事象が持つセキュリティ上の意味を運用者が正しく把握し，対処することは困難になっていく。

日立グループは，社会インフラシステムのような大規模システムで発生する事象を「設計段階で想定したセキュリティ性能に影響を与えるか」という観点で捉え，セキュリティ状態を評価する技術を開発している[5)]。

具体的には，例えば情報漏えいなどのセキュリティインシデントが発生した状態を「設計段階で想定したセキュリティ性能（ある情報の機密性を守ること）を維持できなくなった状態」と捉え，システムで発生した事象が与える影響度からセキュリティ状態を算出し，可視化する。

セキュリティ状態を評価することで，運用者は予兆にいち早く気付くことができるとともに，多くの予兆の中からさらに深刻な事態につながる予兆を選別できる。

5. おわりに

ここでは，セキュリティ確保に対する日立グループの考え方と，社会インフラシステム全体にセキュリティ対策を実施するためのセキュリティ技術，および，安全・安心な運用を支えるセキュリティ技術について述べた。

今後も，日立グループは，進化を続ける脅威に対抗するセキュリティ技術の研究開発を推進し，誰もが安心して利用できる安全な社会インフラの実現に貢献していく。

参考文献など

1) H. Endo：HITACHI Security Concept for Industrial Control Systems, 33rd Annual Conference of the Canadian Nuclear Society (CNS2012) (2012.1)
2) IEC 62443-2-1：Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program (2010.11)
3) IEC-News release：IEC and ISO adopt lower power encryption standard Enocoro stream cipher (2012.11)
http://www.iec.ch/newslog/2012/nr1912.htm
4) 日立ニュースリリース，10ギガビット/秒のブロードバンド上でP2P型ファイル共有ソフトのトラヒックを検知するソフトウェアを開発 (2010.7)
http://www.hitachi.co.jp/New/cnews/month/2010/07/0701.html
5) S. Kai：Development of Qualification of Security Status Suitable for Cloud Computing System, MetriSec '12 Proceedings of the 4th international workshop on Security measurements and metrics, pp.17-24 (2012.9)

執筆者紹介


鍛 忠司
1996年日立製作所入社，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（情報科学）
IEEE Computer Society会員


山田 勉
1994年日立製作所入社，日立研究所 エネルギー・環境センタ エネルギーマネジメント研究部 所属
現在，組込み計算機・ネットワークアーキテクチャ，制御系セキュリティの研究開発に従事
IEEE会員，ISA会員，電子情報通信学会会員，計測自動制御学会会員
技術士（情報工学部門）


中野 利彦
1980年日立製作所入社，インフラシステム社 情報制御プラットフォーム開発本部 制御プラットフォーム設計部 制御セキュリティセンタ 所属
現在，社会インフラシステムのセキュリティ開発に従事
博士（工学）
電気学会会員


芹田 進
2007年日立製作所入社，横浜研究所 情報サービス研究センタ サービスイノベーション研究部 所属
現在，ビッグデータ利活用を支えるセキュリティ技術の研究開発に従事