電力分野の事例
日立が考える電力制御システムセキュリティ

村上 正博 Murakami Masahiro
花見 英樹 Hanami Hideki
今野 博充 Konno Hiromichi
岡本 竜一 Okamoto Ryuuichi
石場 光朗 Ishiba Mitsuaki

広域運用，小売全面自由化，発送電分離などの電力システム改革により，電力システムをつなぐネットワークは今後，より広範囲なものとなると見込まれる。このため，電力制御システムにおけるセキュリティ対策の重要性と，それに対する関心が高まっている。
日立では，長年培ってきた電力制御の経験と実績から，「電力制御セキュリティのあるべき姿」を見定め，制御・人（行動）・情報の視点でセキュリティリスクを分析し，制御技術と情報セキュリティ技術を最大限に活用したセキュリティ施策を検討している。本稿では，電力制御セキュリティに対する日立の考え方と取り組み事例を紹介する。

1. はじめに

広域運用，小売全面自由化，発送電分離などの電力システム改革により，電力をつなぐネットワークは，需要家から発電事業者まで電力そのものに加えて，電力量などの情報を伝送する通信回線がより広範囲につながることとなる。電力設備は安全性が最優先で，かつ電力の安定供給が求められ続けるため，攻撃者の進化に対処できるセキュリティ施策を行っていく必要がある。

ここでは，電力の安定供給に貢献するための電力制御セキュリティに対する日立の考え方と取り組み事例を紹介する[1)]。

2. 電力インフラにおけるセキュリティ脅威

2.1 サイバー攻撃の巧妙化・多様化

2010年のイラン核施設へのサイバー攻撃以降，全世界で原子力発電所や送変電システムなどの重要インフラ設備を狙ったサイバー攻撃の被害が，多数報告されている（図1参照）。

現在報告されている重要インフラ設備へのサイバー攻撃の手法は，情報搾取などを目的とした単純なサイバー攻撃ではなく，制御システムへ侵入し制御情報を入手・解読し，攻撃対象機器を決めて設備を確実に制御不能とすることを目的としているものが散見され，重要インフラ設備は，この極めて悪質でかつ巧妙なサイバー攻撃の脅威にさらされていると言える。

2.2 電力制御システムを取り巻くリスク

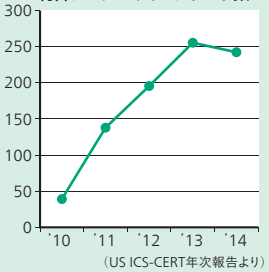
電力制御システムへのサイバー攻撃の脅威は，悪意を持った人間の侵入などによるフィジカル攻撃や，USB機器などの外部媒体からの侵入と，インターネット回線から情報ネットワークを経由し制御ネットワークへ侵入する高度なサイバー攻撃などが想定される。

国内の電力制御システムは，従来はメーカー独自技術を採用し，かつ閉鎖された専用の制御ネットワークで構築されていたため，インターネット回線からのサイバー攻撃の

実被害を伴う重要インフラへの攻撃が増加・巧妙化

- 制御システムへのサイバー脅威は増加傾向
- 攻撃対象を入念に調査したうえで攻撃を最適化 ➡ 実被害が顕在化

制御システムのインシデント数



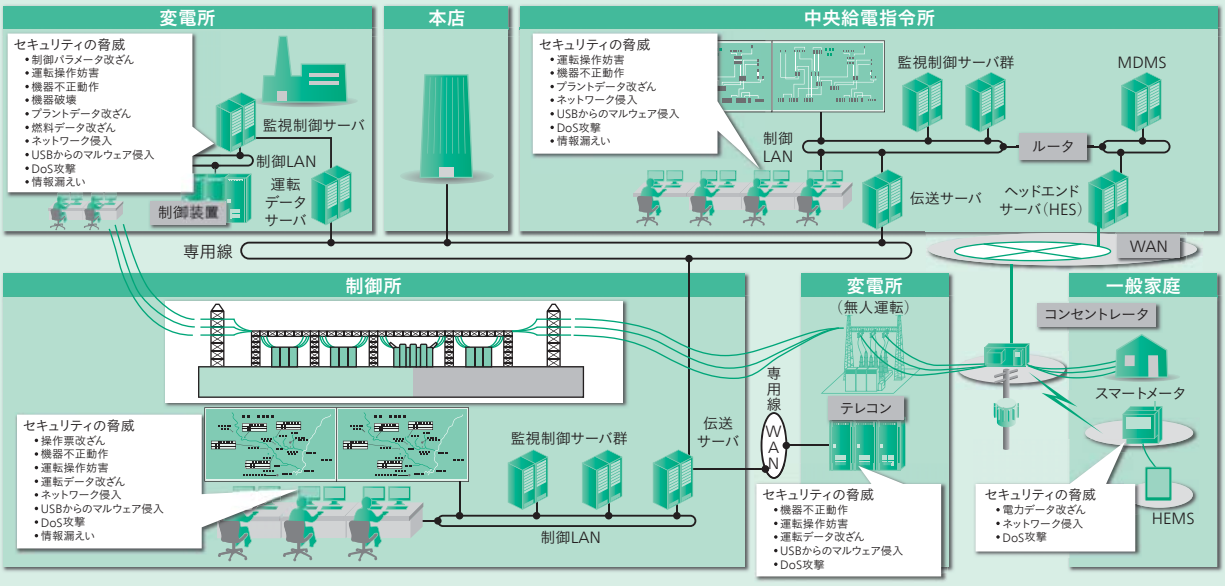
（US ICS-CERT年次報告より）

重要インフラへのサイバー攻撃事例

日付	攻撃対象（地域） 被害内容	損害額
2010/7	核施設（イラン） 設備破壊	NR
2012/3	金融機関（全世界） 情報漏えい	$80M
2012/8	オイル会社（中東） 設備破壊	NR
2013/3	放送局，金融機関（韓国） システム停止	$800M
2015/6	公共機関（日本） 情報漏えい	NR
2015/12	発電所（ウクライナ） システム停止	NR

注：略語説明　ICS-CERT（Industrial Control Systems Cyber Emergency Response Team），NR（Not Reported），US（United States）

図1｜重要インフラでのセキュリティインシデント
重要インフラへの攻撃が増加し，影響範囲も拡大している。



注：略語説明　DoS (Denial of Service)，USB (Universal Serial Bus)，LAN (Local Area Network)，WAN (Wide Area Network)，MDMS (Meter Data Management System)，HES (Head End System)，HEMS (Home Energy Management System)

図2｜電力制御システムのセキュリティリスク例

重要インフラ設備が多数ネットワークに接続され，それぞれセキュリティ脅威がある。重大なインシデントが発生した場合の影響は，局所的な一部機器動作異常などの単体障害から，発電所や変電所などの重要設備障害，さらには広範囲な電力システム障害へと拡散するリスクを秘めている。

リスクは非常に低かった。しかし現在は，ビッグデータ活用や利便性向上を目的として，情報系システムとファイヤウォールなどのセキュリティ機器を介して接続されることも増えてきている。それに伴って，高度なサイバーアタック技術に習熟している者による攻撃にさらされるリスクも増加している。

電力制御システムで想定されるサイバー攻撃は，制御情報の搾取・ネットワークへのDoS (Denial of Service) 攻撃だけでなく，制御信号改ざんや機器不正動作による，重要インフラ設備の安定稼働を妨げることを目的とした攻撃が想定される（図2参照）。

3. 日立が考える電力制御システムセキュリティ

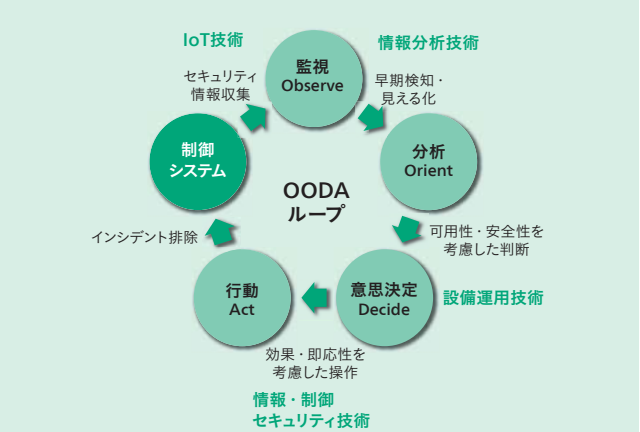
3.1 セキュリティコンセプト

セキュリティ対策においては，国際標準規格・業界標準規格に対応するとともに，特に電力事業者に対しては，その機器の重要性（安全性や被害の大きさ）に応じてレベル分けを行い，必要な対策を実施することが大切である。

日立は適応性 (Adaptive)・即応性 (Responsive)・協調性 (Cooperative) という3つのセキュリティ要件を「H-ARCコンセプト」として整理し，電力制御システムセキュリティにも適用している。

昨今の高度なサイバー攻撃に対抗するためには，開発フェーズでの十分なセキュリティ設計と検知・防御機能の実装，運用フェーズにおけるセキュリティ対策と対処，サイバー攻撃に対する体制構築，ICS-CERT (Industrial Control Systems Cyber Emergency Response Team) などの関係機関との連携による情報共有，攻撃時に正確に対処できる定期的な訓練の重要性が増してきている。

運用フェーズでは，開発フェーズのセキュリティレベルを維持するだけでなく，最新のセキュリティナレッジを蓄積することでセキュリティシステムを維持・成長させていく必要がある。そのために，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し，発生している問題を迅速に検知し，必要に応じて確実に対処していく（図3参照）。すなわち，計画から改善・是正までのPDCA (Plan, Do, Check, Act) サイクルに加え，監視 (Observe)，分析



注：略語説明　IoT (Internet of Things)

図3｜電力制御システムの可用性を高めるセキュリティコンセプト

監視 (Observe)，分析 (Orient)，意思決定 (Decide)，行動 (Act) というOODAループにより，サイバー攻撃から重要インフラ設備を守る。

(Orient)，意思決定 (Decide)，行動 (Act) というOODAループを適用し，攻撃への迅速かつ的確な意思決定を行い，セキュリティ対策の強化を実現する[2), 3)]。

3.2　セキュリティマップの導入

重要インフラにセキュリティ対策を施すうえで最も重要なことは，堅ろう性を確保しつつ可用性を維持することであり，「守るべきところを見定め確実に守る」ことである。これに対し，電力制御システムに対するフィジカル攻撃とサイバー攻撃の両方を想定し，あらかじめインシデント発生時の機器単位の対応方法・行動基準を定める必要があると考える。

この対応として，電力システム全体を各ゾーンに分割し，制御面からリスク分析した「制御セキュリティ」と，システム機器への物理的なフィジカル攻撃とネットワークなど情報機器へのサイバー攻撃を合わせた「システムセキュリティ」の両面からリスク分析を行い，ゾーンごとに影響度合いを評価しマッピングした「セキュリティマップ」の作成が必要である。

3.3　セキュリティポリシーの策定

セキュリティマップで定義した方針に従い，さらに中央給電指令所や発電所などの各制御システムに分解し，個別にセキュリティポリシーを策定することとした(図4参照)。

作成にあたっては，電力制御システムを熟知している経験を生かし，「自分たちが攻撃者になったら，システムをどう攻めるか」という視点であらゆる攻撃パターンを検討し，次にその攻撃に対して，「どうすればシステムを守れるか」という視点でシステム機器の防御方法を個別に整理した。

これにより，セキュリティマップとセキュリティポリシーで電力システムを構成するおのおのの設備での対応を策定することにより，電力制御システムの安定稼働に寄与できると考える。

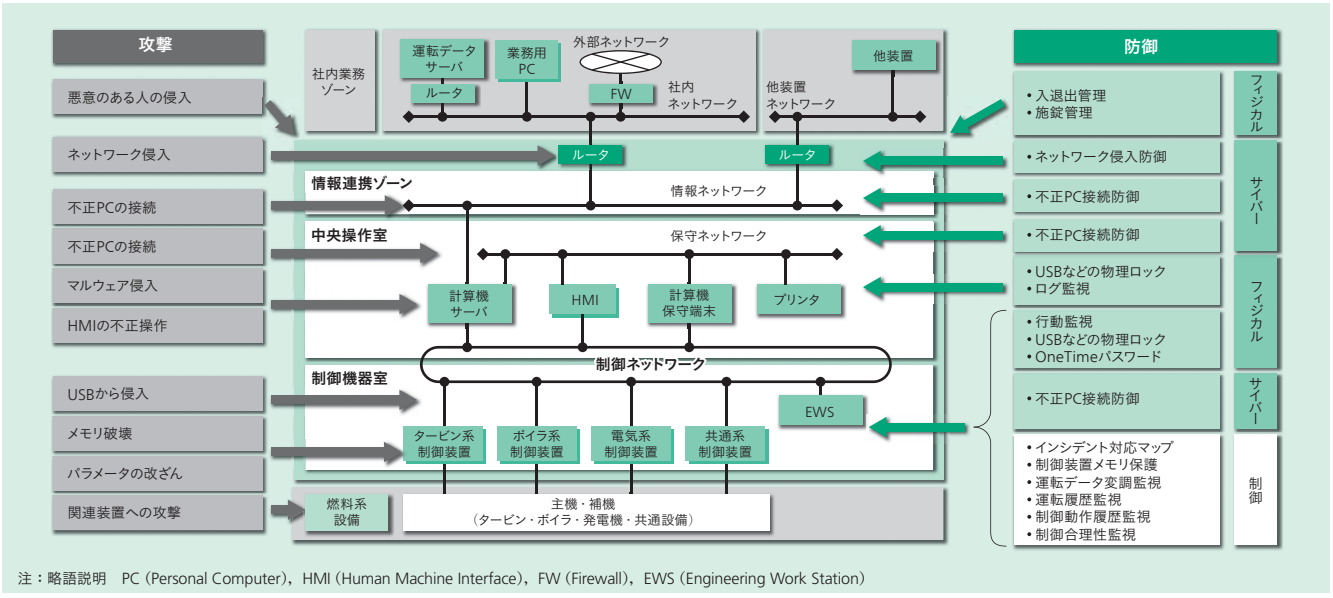
4.　セキュリティソリューション

4.1　電力系統監視制御システム

電力系統監視制御システムは，これまでクローズドな制御系ネットワークで運用されてきた。今後は徐々にオープンな制御系ネットワークへ移行され，外部とのネットワーク相互接続機会が増加する見通しである。このような状況の中，電力系統監視制御システムへのサイバー攻撃による大規模停電が懸念されており，適切な対処が求められている。従来，電力系統監視制御システムにおけるセキュリティ対策としては，他拠点のシステムや各種支援系システムとの接続点にファイヤウォールを設置する不正侵入対策が施されていたが，昨今のサイバー攻撃への脅威と，それに対する関心の高まりから，IDS (Intrusion Detection System：不正侵入検知装置) やホワイトリスト制御，IDカードによるアクセス権管理など，セキュリティ対策強化の動きが活発化している。

4.2　発電所と監視制御システム

原子力発電所では，従来から原子炉等規制法に従い，フィジカルセキュリティについての対策を実施してきている。今後は福島第一原子力発電所事故を踏まえた作業員安



注：略語説明　PC (Personal Computer)，HMI (Human Machine Interface)，FW (Firewall)，EWS (Engineering Work Station)

図4｜制御システムセキュリティポリシー
制御システムに対して，セキュリティポリシーの策定により，すべての攻撃手法を洗い出し，その攻撃手法に対して検知・防御を施すことにより電力システムを守る。

全への取り組みを強化していく。サイバーセキュリティについても，従来からファイヤウォール，データダイオードなどの適用を実施してきているが，今後は，設計基礎脅威を策定して深層防護まで考慮している米国のセキュリティ対策における先行事例などを参考にしながら，国際的な水準まで対策を強化していく。

火力・水力発電所においても，従来から制御系ゾーンと情報系ゾーンを分離したゾーニングを施し，外部とのインタフェース部分にはファイヤウォールなどのセキュリティ機器が導入され制御システムを外部攻撃から防衛している。

火力・水力発電所は，複数の制御ベンダで構築された制御システムであり，さまざまな施策が必要となる場合がある。これに対し，制御ベンダに依存しない手法を選択する必要があり，制御セキュリティの国際規格であるIEC62443を考慮し，セキュリティ対策を構築する。日立は，制御面での対策として「保護」,「制御」,「運転データモニタリング」で対応するとともに，EDSA（Embedded Device Security Assurance）認証を取得した機器によるハードニングと，フィジカルセキュリティとサイバーセキュリティの組み合わせをもってセキュリティを強化していく。

4.3　フィジカルセキュリティ

重要設備および監視・制御設備への物理的アクセスの統制は，直接的な不安全行為の防止は当然ながらサイバーセキュリティのリスク低減にも有効であり，フィジカルセキュリティとサイバーセキュリティは相互に補完される。アクセスの統制にあたっては，アクセスする人員を分類し設備へアクセス可能な人員を最小限にすること，それと同時に危険物の持ち込み防止およびモバイルメディアやデバイスの持ち込み管理をすることを実施する。

発電所は広い敷地および建屋が特徴であり，作業員の位置を把握しておくことはセキュリティ管理の面で重要であり，また災害時の作業員の誘導にも活用できる。

送配電設備は設置場所が広範囲に広がっているため，フィジカルセキュリティと一体運用で入出管理および制御システムへのログイン認証の集中管理をしている。

5.　おわりに

電力インフラを支え続けている電力制御システムは，送配電設備や発電設備の監視制御による運用の最適化に貢献するだけでなく，フィジカル・サイバー攻撃などの新しい脅威と戦いながら，電力の安定供給を担っていく必要がある。

日立は，電力制御システムだけでなく，電力供給設備および制御技術，フィジカルセキュリティ技術，サイバーセキュリティ技術を熟知しており，顧客設備への攻撃に対する対処を多重かつ多層で構築可能である。さらに，制御装置のハードウェア，ソフトウェア両面での堅ろう性向上と，進化し続ける制御系・情報系のサイバー攻撃にも，日立社内のCSIRT（Computer Security Incident Response Team）のサポートにより対処し続けることが可能であり，顧客の設備を守り，電力の安定供給と経営課題解決に貢献していく。

参考文献など

1）　経済産業省：2015年版ものづくり白書，
http://www.meti.go.jp/report/whitepaper/mono/2015/honbun_html/index.html
2）　中野，外：社会インフラを支える制御システムセキュリティ，日立評論，96，3，205～209（2014.3）
3）　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）
4）　ZDNet Japan：IT企業に求められるエコシステムの形成（2015.2），
http://japan.zdnet.com/article/35060584/
5）　堀井，外：電力供給安定化と広域連系を可能にする電力系統技術への取り組み，日立評論，94，11，788～793（2012.11）
6）　日立製作所：自律分散システム，
http://www.hitachi.co.jp/products/infrastructure/product_solution/platform/middleware/autonomy_dispersion/index.html
7）　H. Kuwahara: Experience teach us the future of autonomous decentralized systems, International Symposium on Autonomous Decentralized Systems/ Keynote Address, 169-175（1997）

執筆者紹介

村上 正博
日立製作所 サービス&プラットフォームビジネスユニット
電力システム本部 発電・電力制御システム設計部 所属
現在，IoT（Internet of Things）を活用した電力インフラO&Mサービス設計業務に従事

花見 英樹
日立製作所 サービス&プラットフォームビジネスユニット
電力システム本部 原子力制御システム設計部 所属
現在，原子力制御システムおよび制御セキュリティシステムの設計・開発に従事

今野 博充
日立製作所 サービス&プラットフォームビジネスユニット
電力システム本部 発電・電力制御システム設計部 所属
現在，IoTを活用した電力インフラO&Mサービス設計業務に従事

岡本 竜一
日立製作所 サービス&プラットフォームビジネスユニット
電力システム本部 電力システム設計部 所属
現在，電力系統システムの設計業務に従事

石場 光朗
日立製作所 サービス&プラットフォームビジネスユニット
電力システム本部 原子力制御システム設計部 所属
現在，原子力制御システムの設計業務に従事