原子力防災とセキュリティ

Nuclear Security and Incident Response

谷村 和彦 Tanimura Kazuhiko
伊藤 久幸 Ito Hisayuki
木村 博幸 Kimura Hiroyuki

東日本大震災の発生以降，これまで以上に厳格な原子力防災機能の強化が求められている。また，テロ防止を目的として2011年に改訂されたIAEAの新たな勧告への対応も，今後は必要になると想定される。

日立グループは，これまでの原子力事業で培った原子力発電所の信頼性確保に関するノウハウに加え，防衛事業で培った指揮統制・訓練機能のノウハウ，危機管理関連技術・製品を有している。これらを活用し，新しい原子力防災やセキュリティ機能など，今後の原子力発電所の安全・安心のさらなる向上に寄与していく。

1. はじめに

現在，原子力エネルギーの利用をめぐって各方面で活発な議論が続けられているが，新原子力政策大綱においては，シビアアクシデント（過酷事故）発生時の原子力防災機能の強化が課題として挙げられている。

一方，国際的には新興国の発展や温暖化対策の有効な手段の一つとして，原子力エネルギーの利用が，今後推進されていくと考えられる。

原子力エネルギーの利用においては，厳格な安全性を実現するためのシステムの作り込みは当然として，万一の災害時には，その被害を最小限に抑えるための原子力防災機能の強化も求められる。また，自然災害や事故ばかりでなく，テロ（テロリズム）などの人為的攻撃に対してもいっそうのセキュリティ機能の強化が必要である[1)]。

このような中，米国同時多発テロ事件（9.11テロ）を受け，IAEA（International Atomic Energy Agency：国際原子力機関）から，核テロ防止を目的にした項目が追加された「核物質及び原子力施設の物理的防護に関する核セキュリティ勧告（INFCIRC/225/Revision5）」（以下，核セキュリティ勧告Rev.5と記す。）の改訂版が2011年に発行された。

ここでは，今後の原子力発電所の安全・安心のさらなる向上をめざし，核セキュリティ勧告Rev.5への対応を視野に，防衛・安全保障事業の経験で得た指揮統制や訓練機能のノウハウを適用した新しい原子力防災機能，およびセキュリティシステムに関する技術について述べる。

2. 原子力防災とセキュリティの位置づけ

原子力防災とセキュリティの位置づけを**表1**に示す。原子力防災の目的は国民保護法（武力攻撃事態等における国民の保護のための措置に関する法律）（2004年施行）に基づく「国民保護」であり，セキュリティの目的は，IAEA勧告によると，「盗取，妨害破壊行為，無許可立入及び不法移転（中略）……その他の悪意を持った行為から核物質その他の放射性物質あるいはそれらの関連施設を防護すること」と定義されている[2)]。

以前からこれらのシステム整備は，個別に進められてきた。個別に計画，整備するシステムにおいても，ツールであるシステムや装置，設計は共有できる部分もあり，むだな冗長と有効な冗長の整理，相互バックアップや相互補完

表1｜原子力防災とセキュリティの位置づけ
原子力防災の目的は国民保護であり，セキュリティの目的は核物質／核物質関連情報の防護である。

項目	原子力防災	セキュリティ
想定対象脅威	・自然災害 ・プラント事故 （・武力攻撃／テロ攻撃）	・武力攻撃／テロ攻撃 ・サイバー攻撃
防護対象	・国民	・核物質／核物質関連情報
対象ユーザー	・国（政府） ・地方公共団体（自治体） ・電力（原子力）事業者	・電力（原子力）事業者 ・治安部隊（警察，海上保安庁）
既存機能	・放射線管理 ・放射線監視（自治体／事業者）	・原子力PPS （IAEA勧告Rev.4対応）
次世代システムに共通する要件	・指揮統制（共通状況認識，M&S技術） ・訓練（訓練用シナリオ，机上訓練／指揮所訓練／実動訓練） ・サイバーセキュリティ	

注：略語説明　PPS（Physical Protection System），IAEA（International Atomic Energy Agency），M&S（Model and Simulation）

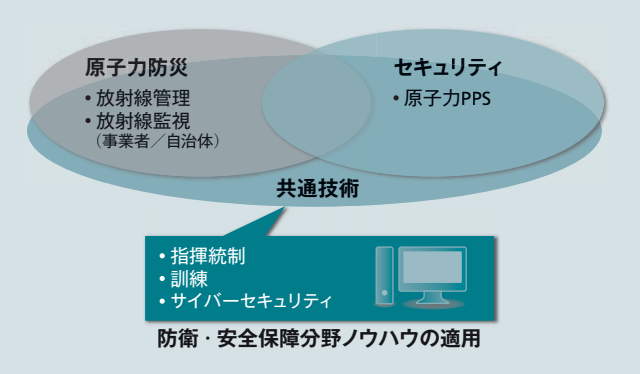


図1｜防衛・安全保障分野のノウハウの適用
原子力防災とセキュリティに防衛・安全保障分野のノウハウを適用し，安全・安心のさらなる向上を図る。

がその一例である。また，東日本大震災や9.11テロの経験を踏まえ，防災やセキュリティシステムを運用する組織が，より迅速かつ効果的に機能するための「指揮統制」,「訓練」機能の充実や，悪意の情報盗取・攻撃からシステムを守る「サイバーセキュリティ」の強化も必要である（**図1**参照）。

3. 原子力防災

防衛分野では，机上訓練，指揮所訓練，実動訓練など，さまざまな訓練体系で日常的に訓練を行い，隊員や組織の練度向上を図っている。その結果として，いかなる状況でも，的確に対処できる能力を維持しており，その効果は，東日本大震災での災害派遣に関する数々の報道で紹介されたとおりである。

原子力施設におけるシビアアクシデントが発生した場合の緊急対策においても，防衛・安全保障分野で培った指揮統制，訓練，サイバーセキュリティなどのノウハウを参考に，シビアアクシデントへの対処機能の充実を図ることは有効である。

(1) 指揮統制

指揮統制の基本コンセプトの一つに，COP（Common Operational Picture：共通状況認識）がある。逐次変化する状況を，リアルタイムに関係者全員が共有することで，指揮者は，次に行うべき適切な命令を下し，現場は，次に行うべき作業の準備を想定することができる。情報提供に際しては，各自の役割や職務に応じた情報を提供することにより，大量の情報に埋もれてしまうことを防いでいる。

COP表示対象としては，既存のプラント状況や放射線状況に加え，図面／CAD（Computer-aided Design）データ，タスキングリスト（緊急時に編成される班別にタスクやイベント，タスク進行状況をリアルタイムに表示），航空／衛星写真のほか，後述するセキュリティの情報などが考えられる（**図2**参照）。

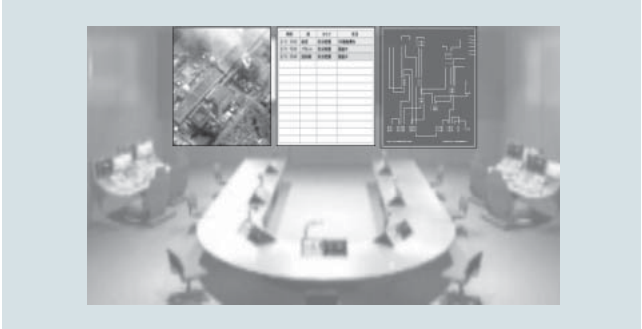


図2｜指揮統制のイメージ
基本コンセプトの一つに，指揮所と現場で，変化する状況をリアルタイムに共有するCOP（Common Operational Picture：共通状況認識）機能がある。

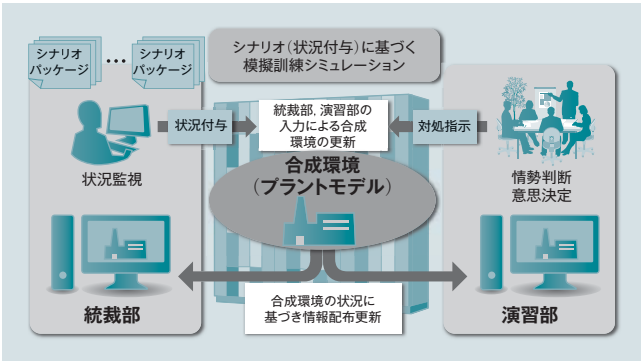


図3｜訓練のイメージ
訓練目的別に作成するシナリオに基づく訓練を実施し，訓練効果を高める。

(2) 訓練

訓練は，事態発生時に的確に対応するために極めて重要な要素である。訓練には，机上で問題を討議して解決策を導出する「机上訓練」，シミュレーションによるロールプレイを中心とした意思決定を訓練するための「指揮所訓練」，現場の対処を実際に訓練するための「実動訓練」などの種類がある。それぞれの訓練目的を明確にするとともに訓練体系を整理することが重要であり，目的や訓練体系を整理した後，訓練目的別にシナリオパッケージとしてまとめる。作成したシナリオパッケージは，訓練時の訓練進行プロセスや状況付与に活用する。

また，指揮統制のCOP表示には訓練モード機能を設け，付与された状況を実際の表示と同じような画面を見ながら支援することにより訓練効果を高めている（**図3**参照）。

4. セキュリティ

4.1 セキュリティの動向

1980年の核物質防護条約に始まったセキュリティの重点は，当初，国際輸送時の防護にあった。その後，旧ソ連（ソビエト社会主義共和国連邦）の崩壊による核関連物質の移転や9.11テロなどを踏まえ，輸送時の防護だけではなく各国に存在する核関連物質や原子力施設も防護の対象とするように変更され，2005年に核物質防護条約が改定された[3)]。わが国においても，同年12月に「原子炉等規制

法（核原料物質，核燃料物質及び原子炉の規制に関する法律）」が改正され，これに基づいて核物質防護対策が強化された。2010年4月には，第1回核セキュリティ・サミットが米国・ワシントンD.C.で開催され，IAEAは2010年11月に核セキュリティ勧告 Rev.5を発行した。

なお，核セキュリティ勧告Rev.5によれば，原子力施設などの核物質を保有・管理する事業者などには，その一義的責任において物理的防護に関するリスク分析を行い，これを踏まえたシステムを整備するとともに，妨害・破壊などの行為発生後までの危機管理計画の拡充，体制の整備が要求されている。

4.2　核セキュリティ勧告Rev.5の要点[1), 3)]

核セキュリティ勧告Rev.5では，原子力施設のセキュリティに対して，以下のような要求が追加された。

(1) 遅延措置設計の必要性

立地選定および設計段階からの核セキュリティの考慮

(2) 外部脅威／内部脅威連携を考慮した対応

(3) 遠隔攻撃やサイバー攻撃への対処

(4) 核セキュリティ文化の導入

(5) フォースオンフォース（武力対抗）演習

性能試験の定期的実施・机上訓練の推奨

(6) 計量管理情報の共有

(7) 予備警報ステーションの設置

(8) 中央警報ステーションの冗長化

4.3　セキュリティのシステムソリューション

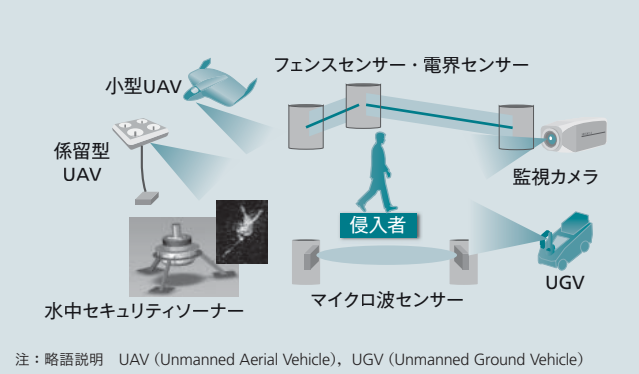
前述した核セキュリティ勧告Rev.5に対するセキュリティ強化に関しては，防衛や社会インフラ安全保障の一環で提供している以下のソリューションを適用することが可能と考える。

(1) 遅延措置設定のフレキシビリティ

防護区域の新設や変更では，等級別手法の適用により，各種センサーの設置，変更などが想定される。また，アクセス管理のためのゲートなどの設置は，さまざまなセンサーやゲートの中から適したものを選択できる（**図4**参照）。

これらは，必要箇所に分散配置する自律分散サーバに接続する。自律分散アーキテクチャで，IEC61508（電気／電子／プログラマブル電子の機能安全に関する国際規格）シリーズに適合したフォールトトレランスなシステム設計により，機器の増設・改変時にもシステム全体の必要十分な機能性能を確保しつつ運用を継続することができる（**図5**参照）。

指揮所においては，各種センサー情報と映像監視を連動させるとともに，多数の監視カメラ映像から区域内の人物・移動体の異常行動や特徴を抽出して自動追尾することにより，監視員の目視負荷軽減を図る（**図6**参照）。



注：略語説明　UAV（Unmanned Aerial Vehicle），UGV（Unmanned Ground Vehicle）

図4｜監視用各種センサーの概要
監視用センサーは，区域や目的に応じて，さまざまなセンサーの中から適したものを選択する。

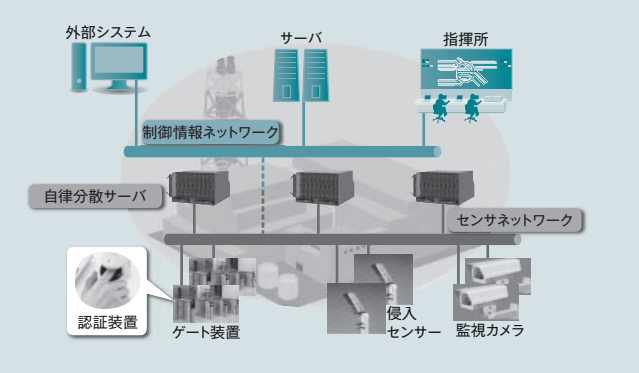
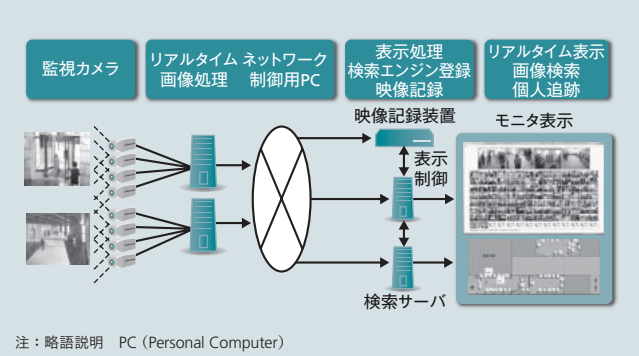


図5｜自律分散アーキテクチャによる高信頼設計
自律分散アーキテクチャによるフォールトトレランスなシステム設計を実施する。



注：略語説明　PC（Personal Computer）

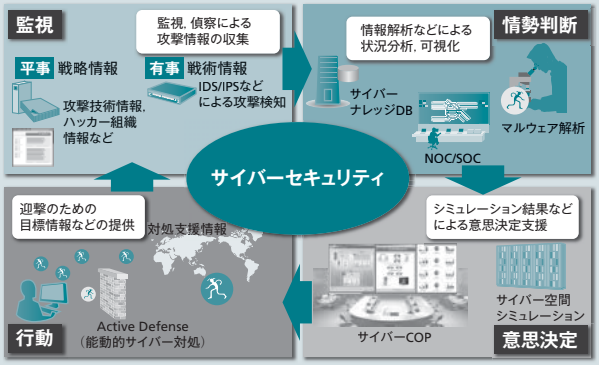
図6｜大規模映像監視
多数の監視カメラから人物などの異常行動や特徴を抽出して自動追尾する。

(2) サイバーセキュリティ

近年，特定の組織や集団を対象にしたサイバー攻撃が頻発する中で，重要インフラへのサイバー攻撃に対する防護を強化していく必要がある。また，内部脅威に関しては，例えばHDD（Hard Disk Drive）など機器内部の情報全体を暗号化し，特定の取扱者以外には秘匿するソリューションが適用可能である（**図7**，**図8**参照）。

(3) フォースオンフォース（武力対抗）演習

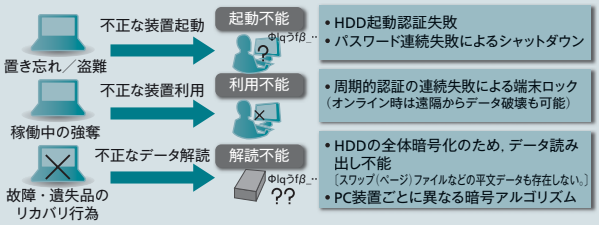
米国などで実施している武力対抗演習に相応な水準の実動訓練を効果的に行うためには，ウェアラブル端末やセン



注：略語説明　IDS（Intrusion Detection System），IPS（Intrusion Prevention System），DB（Database），NOC（Network Operation Center），SOC（Security Operation Center）

図7｜サイバーセキュリティ

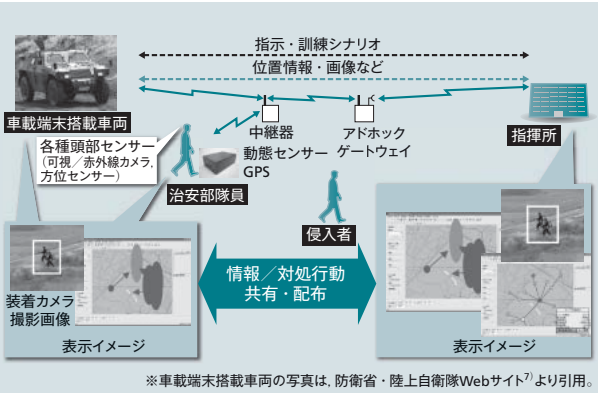
監視，情勢判断，意思決定，行動というサイバーセキュリティサイクルを構築し，サイバー攻撃に備える。



注：略語説明　HDD（Hard Disk Drive）

図8｜ハードディスク暗号の適用

ハードディスク暗号を適用し，盗難などの脅威に備える。



注：略語説明　GPS（Global Positioning System）

図9｜実動訓練における情報共有

ウェアラブル端末やセンサー，アドホック通信などを応用した個人装備の適用による訓練を実施することが有効である。

サー，アドホック通信などを応用した個人装備の適用も有効と考える。治安要員や警備員が身に着けることにより，リアルタイムでの情報共有と，迅速かつ的確な指揮命令を支援する（**図9**参照）。

5.　おわりに

ここでは，今後の原子力発電所の安全・安心のさらなる向上をめざし，核セキュリティ勧告Rev.5への対応を視野に，防衛・安全保障事業の経験で得た指揮統制や訓練機能のノウハウを適用した新しい原子力防災機能，およびセキュリティシステムに関する技術について述べた。

シビアアクシデントの際に効率よくオペレーションを実行するには，防衛システムの指揮統制のような考え方を適用することが有効と考える。また，日頃からの訓練は重要であり，住民の安全・安心に対するデモンストレーションや現実に起きた場合の教訓として生かされるべきである。

東日本大震災のような大規模災害においては，防災システムとセキュリティシステムの情報連携や統合運用が必要となる場面も想定される。核セキュリティ勧告Rev.5の中央警報ステーションの冗長化の要求などに，原子力防災とセキュリティシステムの相互バックアップの観点を取り入れて検討することなどは，その一例として考えられる。

日立グループは，今回提案したソリューション以外にも，プラントのセンサー情報を利用した異常予知検知技術・予防保全技術を含めたエンタープライズアセットマネジメント，ウェアラブル端末，コンテナ型データセンターなど，原子力発電所の危機管理に利用できる技術を保有している。また，動力炉，炉心制御，発電・送配電制御，放射線管理，環境監視システムなど，原子力発電を巡るさまざまなシステムを提供し，原子力発電所のさらなる安全・安心の向上に寄与できるものと考えている。

参考文献など

1)　IAEA：49th IAEA General Conference（2005）Documents,（2005.9）
2)　IAEA：Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities（2011.1）
3)　木村：核セキュリティの基礎知識，社団法人日本電気協会新聞部（2012.3.14）
4)　外務省：2012年ソウル核セキュリティ・サミット，ソウル・コミュニケ（2012.3）
5)　原子力委員会 原子力防護専門部会：我が国の核セキュリティ対策の強化について（2012.3）
6)　United States Nuclear Regulatory Commission：The NRC Incident Response Plan, NUREG-0728（Rev.4）（2005.4）
7)　防衛省・陸上自衛隊：装備，車両，http://www.mod.go.jp/gsdf/equipment/ve/1_9.html

執筆者紹介

谷村 和彦
1981年日立製作所入社，ディフェンスシステム社 情報システム本部 所属
現在，指揮統制分野と危機管理分野のシステム事業化に従事

伊藤 久幸
2003年日立製作所入社，インフラシステム社 情報制御システム事業部 原子力制御システム設計部 所属
現在，原子力施設の情報システム開発に従事

木村 博幸
2003年日立製作所入社，日立GEニュークリア・エナジー株式会社 原子力制御計画部 所属
現在，原子力施設の計測制御システム計画に従事