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

三村 昌弘 Mimura Masahiro
新井 利明 Arai Toshiaki
中野 利彦 Nakano Toshihiko
服部 隆一 Hattori Ryuichi
佐藤 敦俊 Sato Atsutoshi

重要性の高まる社会インフラセキュリティ

社会インフラとは，国民の社会生活や企業の経済活動の基盤となる施設，設備，システムなどを指す。社会インフラは，電力，ガス，水道，鉄道をはじめとし，政府，金融，医療などのさまざまなサービスを社会に提供するものである（**図1**参照）。したがって，社会インフラには，24時間365日ノンストップで，あるいは，どんなときにも最低限必要なサービスを提供することが期待される。これは社会インフラシステムが持つ重要な特徴の1つと言えるだろう。

また，それらのサービスは独立して社会インフラに存在するのではなく，相互に依存し合う形で初めて成り立っている。例えば，鉄道は電力がなければ走れないが，電力会社の従業員が鉄道を使って通勤している場合もある。このように，社会インフラは全体が1つの複合的な巨大システムであり，そのスマートな運用を実現するためにICT（Information and Communication Technology）が積極的に導入・活用されている。ICTや環境技術によって社会全体の電力の有効利用を図ろうとするスマートシティはその一例である。

従来，「セキュリティ」と言えば，一般的には情報セキュリティ，つまり情報の保護（機密性の確保）を主な目的としていた。しかし，対象を社会インフラに拡大した場合，情報の保護だけでなく，あらゆる脅威に対して社会インフラがサービスを提供し

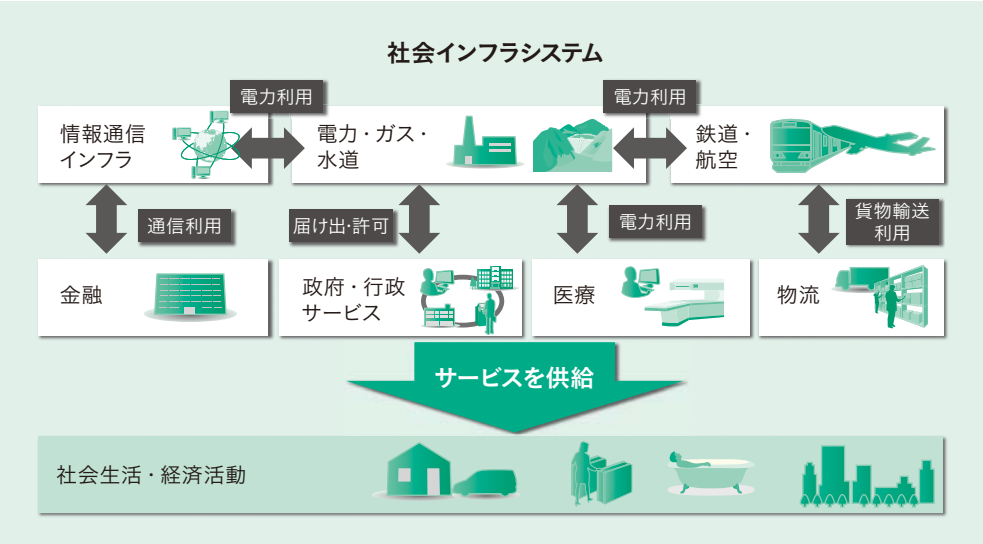


図1｜社会インフラシステム
社会インフラは，人々の社会生活や企業の経済活動の基盤となる施設・設備・システムであり，相互に依存し合うシステムで構成される巨大な複合システムである。

続けられるか（可用性の確保）といった観点でもセキュリティに取り組む必要があると考える。日立グループは，これを「社会インフラセキュリティ」として捉え，社会・技術の潮流に基づいて今後の社会インフラに求められるセキュリティ上の要件を「H-ARCコンセプト」として整理した。以下，社会インフラを取り巻く潮流，セキュリティ上の要件の抽出，H-ARCコンセプトについて述べる。

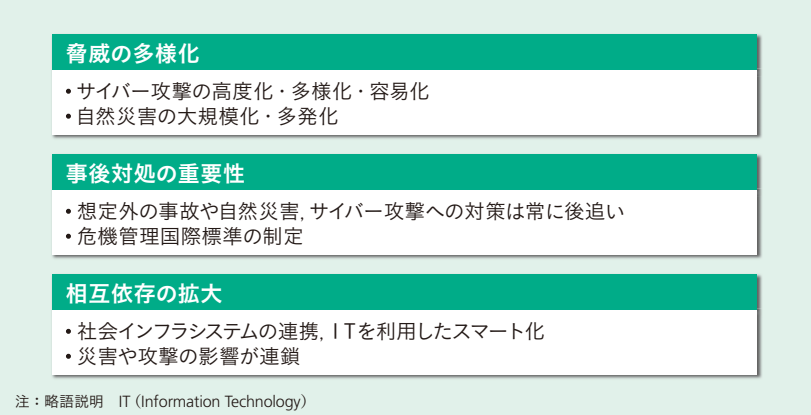


図2｜社会インフラセキュリティを取り巻く潮流
昨今の社会インフラセキュリティを取り巻く潮流として，「脅威の多様化」，「事後対処の重要性」，「相互依存の拡大」の3つを取り上げた。

社会インフラセキュリティを取り巻く潮流

社会インフラセキュリティを取り巻く潮流として，ここでは「脅威の多様化」，「事後対処の重要性」，「相互依存の拡大」の3つを取り上げる（**図2**参照）。

脅威の多様化

社会インフラを取り巻く脅威を見てみると，今世紀に入ってから想定外の自然災害，事故，攻撃が発生しており，特に攻撃に関しては単なる施設や設備を対象としたものだけでなく，ICTの領域，すなわちサイバー空間もその対象になっている。例えば，2010年に発生したウイルスStuxnetによる発電所への攻撃は，ICTと融合した重要施設への新たな脅威と考えられている。

また，サイバー攻撃の兆候を見てみると，広くは知られていない脆（ぜい）弱性を利用し，特定の組織や人物を狙う標的型攻撃，逆に不特定多数のユーザーが閲覧するサイトにマルウェアを仕込んでおく水飲み場型攻撃などの高度な攻撃が現れている。今後は，スキルを持った攻撃者が攻撃自体をサービスとして提供することにより，特殊なスキルを持たない人物でも容易に攻撃を実行できるサービス型攻撃に発展していくものと予想される。

一方，自然災害は，近年，多発・大規模化する傾向にある。例えば，カトリーナ（2005年）やサンディ（2012年）などの大型ハリケーンは，都市の冠水，広範囲に及ぶ停電，交通機関の麻痺（まひ），金融・自治体サービスの停止などの被害を引き起こした[1)]。また，日本では近年，これまではあまり注目されていなかった竜巻や局所的大雨（ゲリラ豪雨）が，家屋倒壊や浸水被害などをもたらしている。

このように社会インフラに対する脅威は多様化しており，これまで想定していなかった脅威への対策が必要になってきていると言える。

事後対処の重要性

通常，セキュリティでは多層防御という考え方が一般的である。これは，ある攻撃・災害に対していくつかの対策を用意しておき，いずれかの対策が機能することで被害を未然に防ぐものである。例えば，サイバーセキュリティの分野では，守るべき機密情報を含む情報システムに対して，機密情報を漏えいするウイルスの侵入を防ぐ「入口対策」と同時に，機密情報が情報システム外に送信されるのを防ぐ「出口対策」をとる方法などが知られている。これは，事前に知りえた情報を最大限に活用して事前対策をとろうとするものである。

しかし，先に述べたとおり社会インフラを取り巻く脅威は多様化する傾向にあり，今後起こりうるすべての攻撃・災害に対策をとることは現実的ではない。そのため，多層防御によって想定しうる対策をとっていたとしても，想定外の攻撃・災害による被害が発生することを前提とし，被害が発生した後の事後対処を検討しておく必要がある。例を挙げると，被害の発生自体はな

くせないものの，攻撃・災害に迅速に対処することによって被害の拡大や波及を抑える減災の考え方がこれに相当する。

このような事後対処の重要性に関する潮流は，国際標準の動向にも見て取れる。例えば，情報セキュリティマネジメントの国際規格であるISO/IEC 27000シリーズでは，2011年に事業連続性（BCP：Business Continuity Plan）に関するガイドラインを策定している（ISO/IEC 27031:2011 Guidelines for information and communication technology readiness for business continuity）。これは，「情報セキュリティは絶対ではなく，事故は起こりうる」という考え方から，情報サービスの継続に関わる実施施策をガイドラインとしてまとめたものである。また，ISO 22320 Societal security－Emergency management－Requirements for incident responseでは，効果的な危機対策を実現するための最小限の要件を示し，緊急事態への対処能力を高めようとしている。

相互依存の拡大

冒頭に述べたように，社会インフラのサービスは相互に連携しており，全体が1つの複合的な巨大システムであると捉えることができる。現在では，さらにサービスの利便性や効率を高める目的で，IT（Information Technology）を介したサービス間連携がより緊密になる方向に進んでいる。例えば，鉄道の相互乗り入れやグローバルに展開したサプライチェーンなどが挙げられる。いずれも消費者の利便性や企業の生産効率の向上に寄与するものであり，今後もスマートシティのように異業種間を高度に連携した社会インフラが発展していくものと予想される。こうしたサービス間の相互依存の拡大は，複合的なサービスを高度化すると同時に，攻撃・災害による被害を連鎖させる可能性も高めてしまう。1か所での鉄道事故が相互に乗り入れる路線全体に影響して利便性を低下させたり，2011年のタイの洪水のように，ある地域での自然災害の影響が世界的に波及し，HDD（Hard Disk Drive）やそれを組み込む最終製品のコストに影響したりした例がある[2)]。

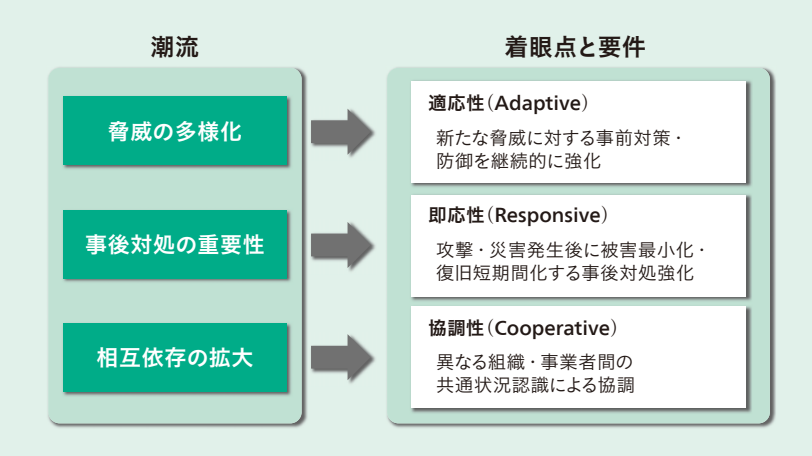


図3｜社会インフラセキュリティの要件
社会インフラセキュリティに求められる要件を，「適応性（Adaptive）」，「即応性（Responsive）」，「協調性（Cooperative）」という3つに整理した。

社会インフラセキュリティの要件

前章で述べた社会インフラを取り巻く潮流から，社会インフラセキュリティに求められる要件を整理した（図3参照）。多様化する新たな脅威に対する事前対策や防御を継続的に強化する適応性，攻撃・災害が発生したときに被害の最小化や復旧の短期間化につなげる即応性，異なる組織や事業者間の連携と共通状況認識によって攻撃・災害に対処する協調性の3つである。以下，それぞれの要件について述べる。

適応性（Adaptive）

多様化する攻撃・災害といった脅威に対策し続けるためには，大きく2つの観点が必要になる。

1つは，新たな脅威が発見されるたびに，対応する事前対策を継続的に保護対象のシステムに取り入れていく仕組みである。これは，セキュリティ管理の手法として広く知られているPDCA（Plan，Do，Check，Act）の考え方である。具体的には，新たな脅威の把握，対策方法の立案，導入計画の策定，対策の導入・評価を継続的に実施することで，新たな脅威の発見に対応する。

もう1つの観点は，保護対象システムと

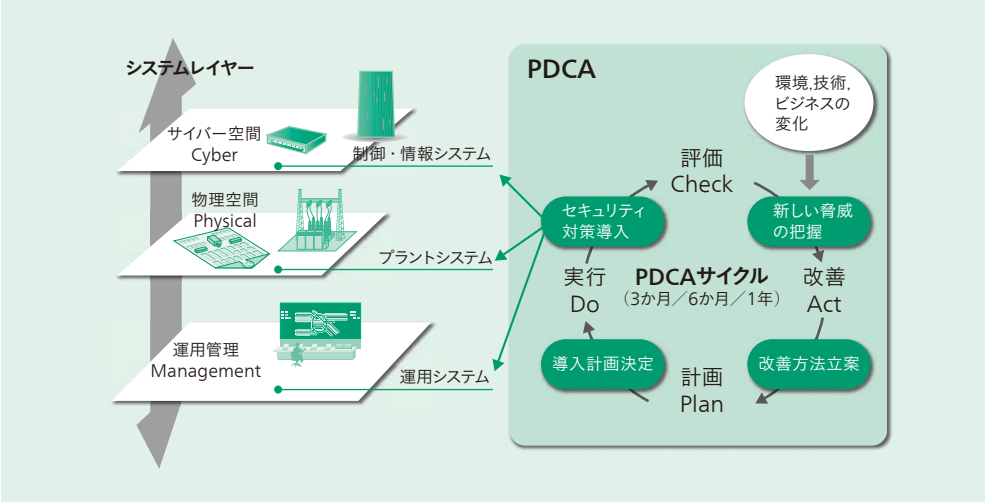


図4｜適応性（Adaptive）
新たな脅威に対する事前対策・防御を継続的に強化し，サイバー空間，物理空間，運用管理の各レイヤーでPDCA（Plan, Do, Check, Act）サイクルを適用する。

してあらゆるレイヤーを対象にするということである。社会インフラシステムに限らず，システムはおおよそ3つのレイヤー，すなわちサイバー空間，物理空間，運用管理に分けることができる。社会インフラシステムへのあらゆる攻撃・災害に対策していくには，単一のレイヤーだけで十分とは限らない。多層防御の考え方を導入すれば，ある1つの攻撃・災害に対して，3つすべてのレイヤーで対策が打たれていることが望ましい。

適応性（Adaptive）という概念は，多様化して常に新たな脅威が発生する状況において，システムのあらゆるレイヤーに対してPDCAによる継続的な対策を行うことを意味している（**図4**参照）。

即応性（Responsive）

事後対処の重要性の高まりにより，前節に述べた適応性で攻撃・災害を未然に防ぐ事前対策だけではなく，攻撃・災害の発生後にできるだけ被害を最小化したり，復旧を短期間化したりする即応性（Responsive）の概念が必要になる。これを実現するために，PDCAとは異なる以下のようなプロセスを考える（**図5**参照）。

まず，常にシステムの状況や周囲の環境を監視（Observe）し，状況の変化を検知できる仕組みが必要になる。監視すべきシステムの状況はアプリケーションによって異

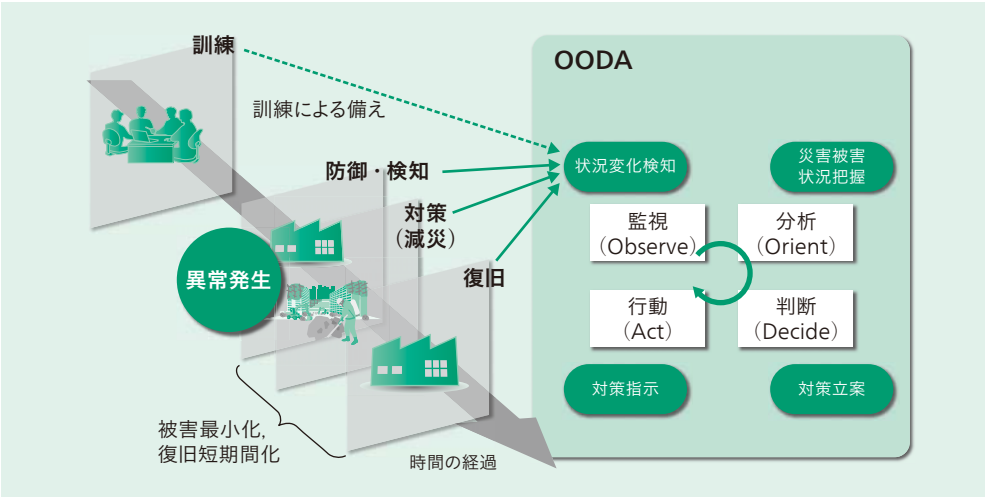


図5｜即応性（Responsive）
攻撃・災害の発生後に被害を最小化し，復旧を短期間化するための事後対処を強化する。状況変化に迅速に対処するプロセス（OODA：Observe, Orient, Decide, Act）を支援する。

なるが，例えば，サイバーセキュリティなら新たな脆弱性の発見やウイルスの侵入など，防災なら避難所に避難している人数の変化や電気・ガス・水道のサービス提供の停止／再開などが状況変化に相当する。

次に，状況変化を検知したら，状況を分析（Orient）し，被害状況を把握あるいは予測する必要がある。先の例で言えば，脆弱性やウイルスの情報から情報漏えいの発生可能性（リスク）を予測する，避難所の人数と停止しているサービスから，避難所での二次被害を予測する，などがある。

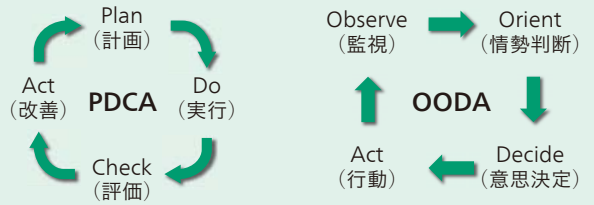
さらに，被害の状況やその予測から，次にとるべき対処行動を決定（Decide）する。対処行動としては，例えば情報漏えいリスクのあるシステムの一時的な停止，飲料水や暖房器具の緊急配布などが挙げられる。最後に，決定した対処を行動（Act）に移し，実行する。

これら一連のプロセスは，もともとリアルタイムの意思決定を行うモデルとして米国空軍が1970年代に考案したものである[3]。2000年前後から，指揮統制（Command and Control）のプロセスとして研究がなされるようになってきた。長期スパンで問題発見とシステム／運用対策を繰り返し，システム／運用自体を改善していくPDCAサイクルとは異なり，今現在のシステム／運用のリソースの中で最良の対処を行うことに主眼を置いている。

攻撃・災害発生後の事後対処を改善するには，PDCAのような長期的・計画的な対応では間に合わず，リアルタイムあるいはそれに近い時間的スパンで，状況の監視・分析と対処の決定・実行を行い（OODA），被害の最小化や復旧の短期間化を実現する即応性が必要になると考える。

これは，OODAの各タスクをサポートするITの導入によって実現されうるが，一方で人間の作業を完全にITに置き換えることもできない。代表的なのは判断（Decide）のタスクである。したがって，即応性の実現には人間系の作業の迅速化も同時に必要になる。これについては，平時における訓練によって仮想的にOODAループを経験させ，人の練度を向上することで対応できるであろう。

PDCAとOODAの違いを図6に示す。



フェーズ	事前対策	事後対処
サイクル	長い（6か月～）	短い（リアルタイム～）
対象	• セキュリティリソースの変更・追加 • セキュリティコンポーネント追加 • アプリケーションソフトウェア更新 • 組織・規則	• セキュリティリソースへの指令（変更・追加はしない。） • 設定値・パラメータの変更・調整 • ミドルウェアなどのパッチ更新

図6｜PDCAとOODA
PDCAは，脅威に備え，定期的にセキュリティ施策を見直して改善するプロセスである。それに対し，OODAは，脅威発生時に迅速に対処することで被害を最小化するプロセスである。

協調性（Cooperative）

社会インフラシステムの相互依存性の進展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，社会インフラ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，サブシステム間，すなわち異なる組織や事業者間で互いの状況を的確に認識し，前節で述べたOODAにおける状況分析（Orient）や判断（Decide）に活用する協調性（Cooperative）の概念が必要になる（図7参照）。それには，各組織の状況を表すのに使用している表現を意味のレベルで共通化し，かつ機械可読の状態で情報交換できる仕組みや，さまざまな組織が持つ情報を一元的に表示・管理することが求められる。これは，防衛分野では共通状況認識（COP：Common Operational Picture）と呼ばれており，指揮統制における主要な機能の1つとされている[4]。

H-ARC コンセプト

適応性（Adaptive），即応性（Responsive），協調性（Cooperative）という，前章で述べた社会インフラセキュリティに求められる3つの概念をまとめて，日立グループは

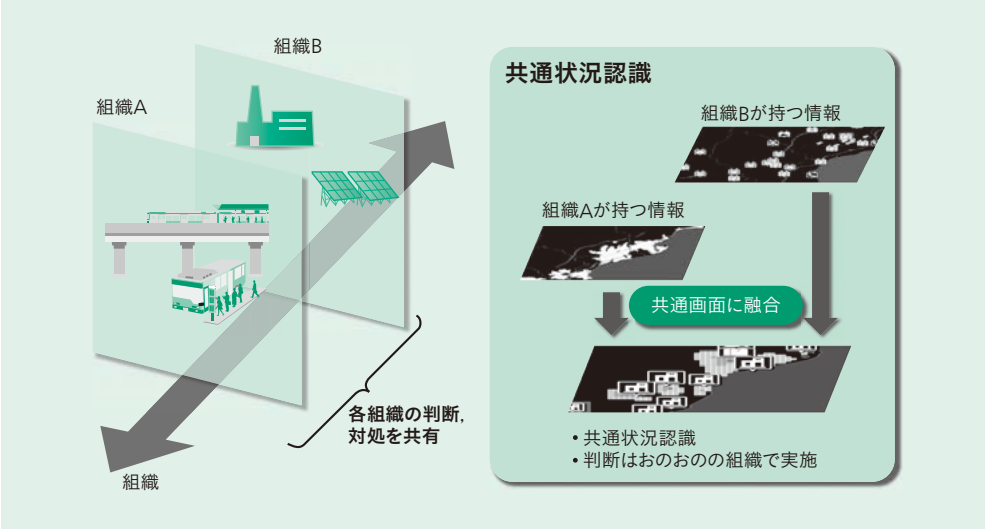


図7｜協調性（Cooperative）
異なる組織や事業者が取得した情報を共有し，それを視点を変えて可視化することで連携した対処を可能にする。

H-ARCコンセプトと呼んでいる（図8参照）。H-ARCコンセプトは，社会インフラを取り巻く3つの潮流（脅威の多様化，事後対処の重要性，相互依存の拡大）から，今後必要となるセキュリティ上の概念として導出したものである。また同時に，それぞれがシステムレイヤー，時間，組織の3つの軸における対策あるいは対処に位置づけられている。

社会インフラシステムは，平時の稼働はもちろんのこと，有事の際にも最低限必要なサービスを提供する「可用性」を期待されており，この点で常に極めて多くの脅威にさらされている。これらの脅威から社会インフラシステムを守るには，広範囲にわたる対策が必要になる。H-ARCコンセプトは，社会インフラセキュリティとして対策を検討する際の観点を提供することができると考える。

セキュリティ製品・ソリューション・サービス

日立グループは，物理空間，サイバー空間におけるセキュリティ製品をはじめ，H-ARCコンセプトを具現化するソリューションを保有している。

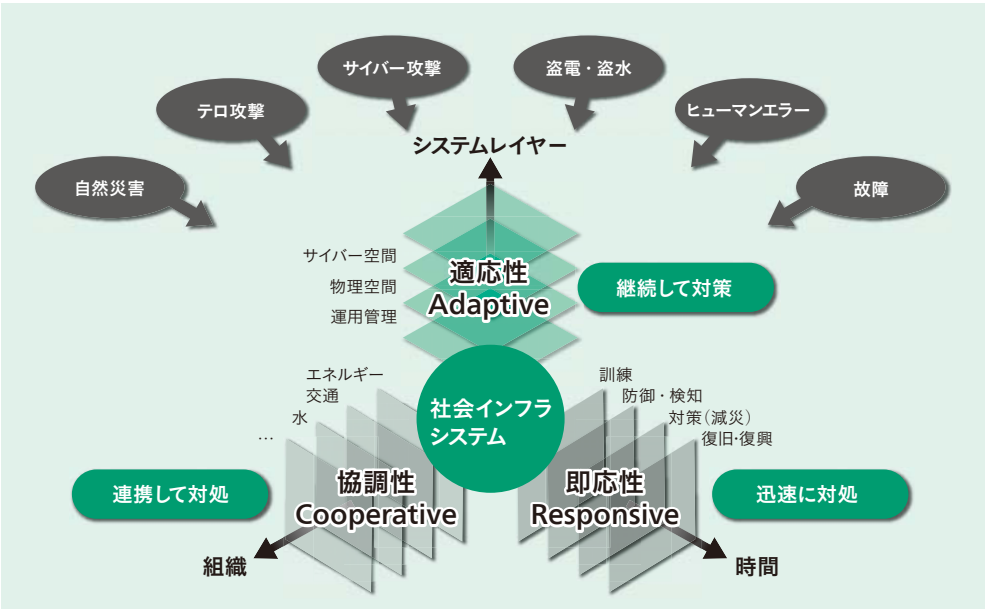
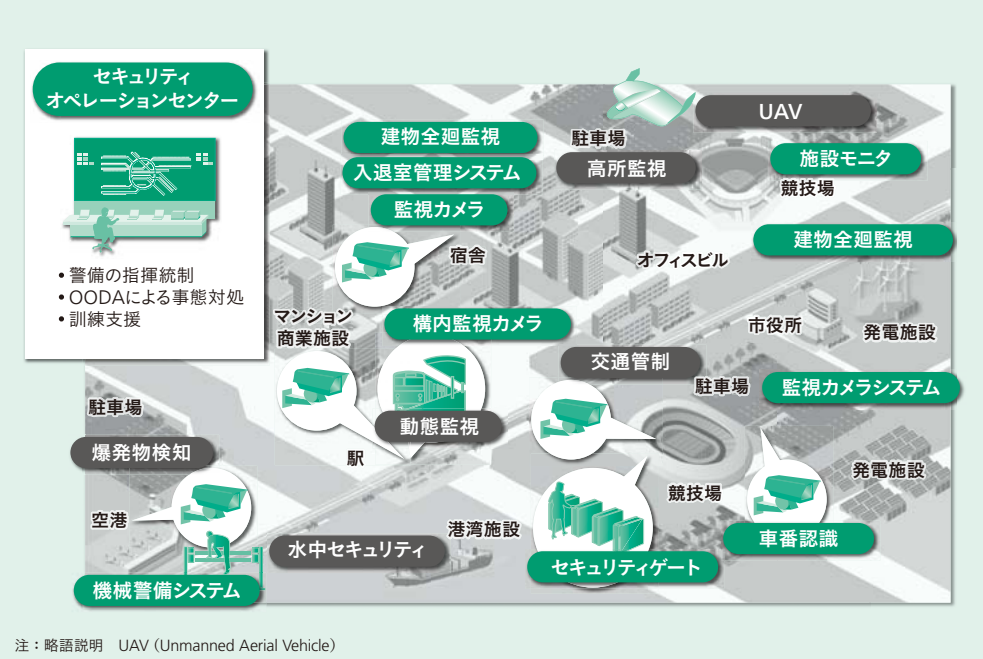


図8｜H-ARCコンセプト
システムレイヤー，時間，組織という3つの軸で対応することで，社会インフラのセキュリティを実現する。



注：略語説明　UAV（Unmanned Aerial Vehicle）

図9｜都市まるごと安全・安心ソリューション

都市に流入する航空機，船舶，車両，人を対象に，水際でのセキュリティチェックを実現する。

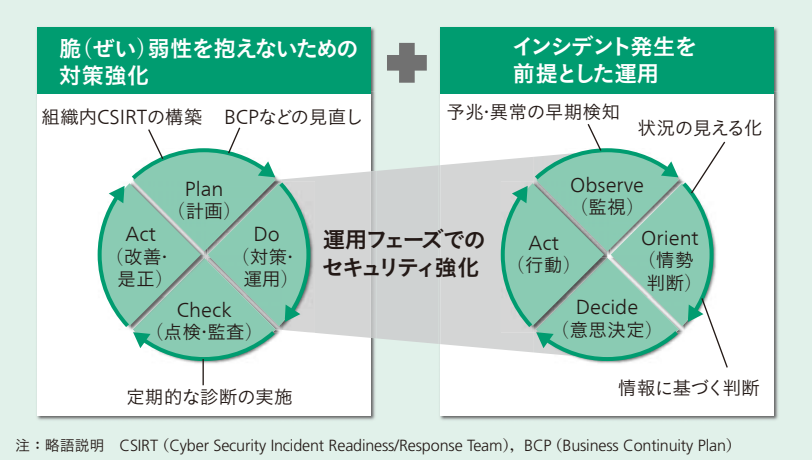
物理空間におけるセキュリティ分野では，都市に流入する航空機，船舶，車両，人を対象に，水際でのセキュリティチェックを実現する都市まるごと安全・安心ソリューションを提供している（図9参照）。具体的には，空港や駅などにおける不審者の行動を監視する空港／駅セキュリティソリューション，海洋の船舶を検出・確認・分類する海洋警備ソリューションなどから構成される。これらのソリューションは，さまざまなレイヤーで事前対策を施す適応性を実現するものである。

サイバーセキュリティ分野では，適応性に即応性を加えたマネージド・セキュリティ・サービスが代表的である（図10参照）。このサービスは，脆弱性を抱えないための対策強化として，CSIRT[a]の構築や見直しといった計画（Plan）から，対策・運用（Do），点検・監査（Check），改善・是正（Act）までのPDCAサイクルに加え，監視（Observe），分析（Orient），判断（Decide），行動（Act）という一連の流れにより，迅速かつ合理的な意思決定や施策を実現するOODAループの概念も採用している。これにより，セキュリティ対策の強化と迅速化を実現している。

制御セキュリティ分野では，IEC 62443[b]に基づいて制御システムの堅牢（ろう）性を適応性，即応性，協調性の3つの軸で評価する指標を提案し，制御システムおよび制御コンポーネントの2つのレイヤーでそれぞれの指標を満たすための要件とその対応策を示している。具体的には，社会インフラシステムのセキュリティをライフサイクル全体で確保する「2×3セキュリティ実現モデル」に基づき，開発フェーズにおけるセキュリティ施策でセキュリティ強靭（じん）性要件と適応性要件を，運用フェーズにおけるセキュリティPDCAサイクルで即応性要件と協調性要件をそれぞれ達成

(a) CSIRT
Cyber Security Incident Readiness/Response Teamの略。企業や組織内で，情報セキュリティに関するインシデントに対処する組織の総称。

(b) IEC 62443
制御システムセキュリティに関する国際標準規格。制御システムのセキュリティでは，業界分野ごとに標準規格が策定されているが，汎用的な標準規格であるIEC 62443シリーズに統合する動きが広がっている。



注：略語説明　CSIRT（Cyber Security Incident Readiness/Response Team），BCP（Business Continuity Plan）

図10｜マネージド・セキュリティ・サービスの考え方

PDCAサイクルとOODAループにより，サイバー空間におけるセキュリティ対策の強化と迅速化を実現する。

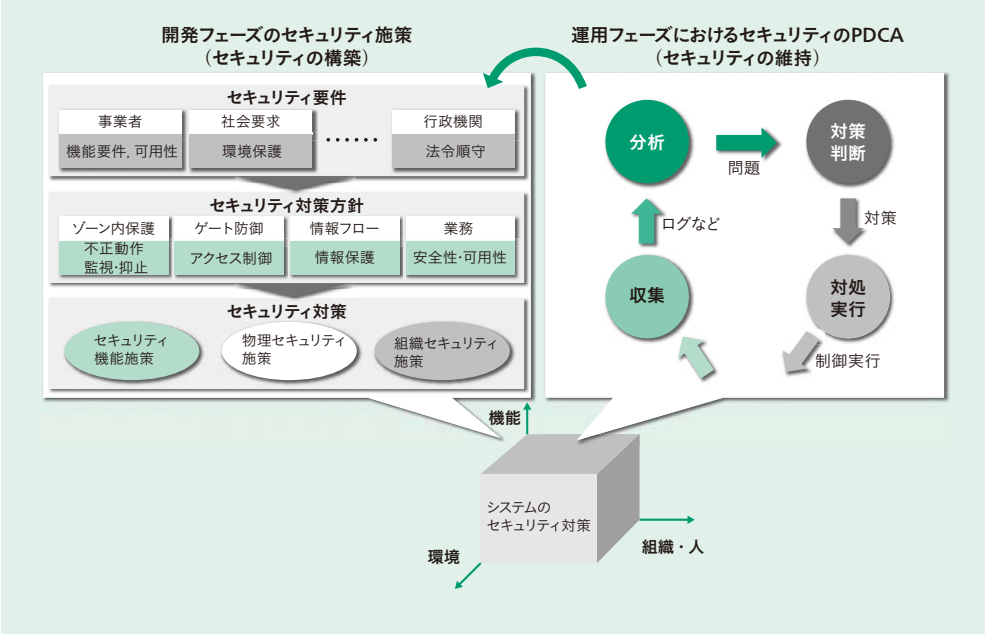


図11｜2×3セキュリティ実現モデル

2つのフェーズを3つの軸で評価し，社会インフラシステムのセキュリティをライフサイクル全体で確保するモデルである。

している（図11参照）。

さらに安全・安心な社会インフラへ

ここでは，社会インフラセキュリティに必要となるセキュリティ上の概念であるH-ARCコンセプトと，物理空間･サイバー空間・制御システム上のそれぞれで実現するソリューションについて述べた。

今後も，日立グループはH-ARCコンセプトに基づいた製品，ソリューション，サービスを提供し，社会インフラシステムの安全・安心の向上に寄与していく。

参考文献

1） 西村：ハリケーン・カトリーナによる被害，電子情報通信学会技術研究報告，信学技報106，220，13～16（2006）
2） 清水：タイ洪水によるHDDサプライチェーンへの影響，Future SIGHT，55号，32～36（2012）
3） T. Grant: Unifying Planning and Control using an OODA-based Architecture, Proceedings of SAICSIT（2005）
4） H. Minners: Conceptual linking of FCS C4ISR systems performance to information quality and force effectiveness using the CASTFOREM high resolution combat model, WSC 2006（2006）

執筆者紹介

三村 昌弘
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，企業向け情報システムを対象としたソリューション，セキュリティ，生産性技術の研究開発に従事
博士（工学）
情報処理学会会員

中野 利彦
日立製作所 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

佐藤 敦俊
日立製作所 デザイン本部 情報デザイン部 所属
現在，社会インフラシステム，スマートシティ関連のデザイン業務に従事

新井 利明
日立製作所 ディフェンスシステム社 所属
現在，ディフェンスシステム社のCTOとして，技術全般の取りまとめに従事
工学博士

服部 隆一
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 事業企画部 所属
現在，セキュリティを中心とするサービス分野の事業企画業務に従事