都市丸ごと安全・安心ソリューション

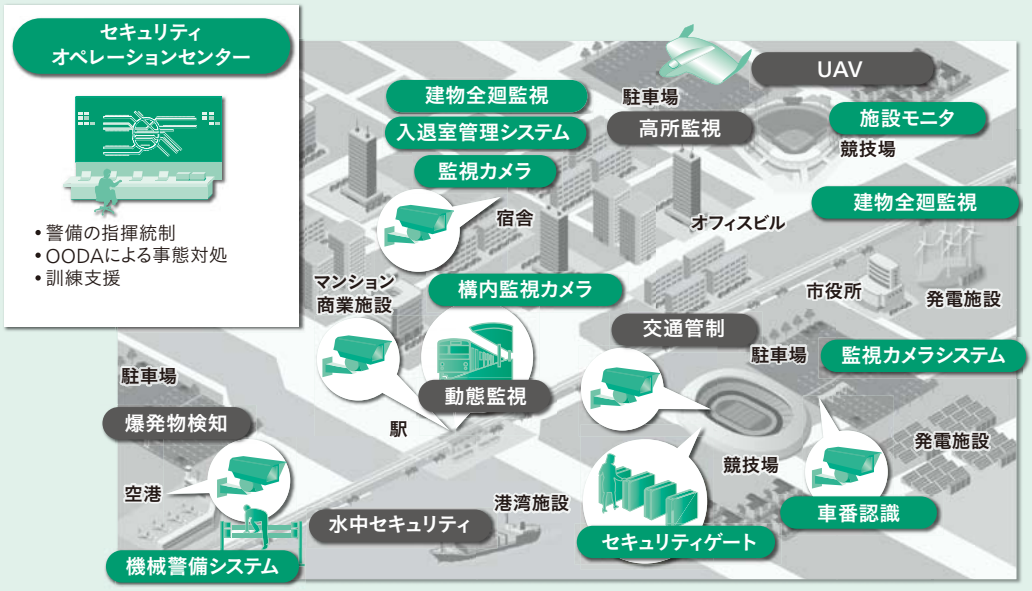
小野 郁宏 Ono Ikuhiro
相模 太 Sagami Futoshi
中本 健司 Nakamoto Kenji

都市の機能を支える社会インフラシステムは，人々の便利で快適な生活のためにますます高度化・複雑化し，相互に依存し合う巨大な複合システムとなっている。一方，社会インフラシステムの安定稼働に影響を与える自然災害，感染症，犯罪，サイバーテロなどの脅威が増大しつつあり，人々の安全・安心を守る社会インフラセキュリティへの期待が高まっている。
日立グループは，防衛・社会インフラセキュリティシステムの構築経験やノウハウを生かし，今後の社会インフラセキュリティシステムの在り方を検討してきた。これらを基に，さらなる安全・安心な社会インフラの提供に寄与している。

1. はじめに

都市は，エネルギー施設，交通機関，金融機関などの複雑なシステムが高度に協調し，快適で便利な生活を送ることができる空間を提供している。しかし，2011年の東日本大震災のような自然災害，2001年の米国同時多発テロ事件，2003年の中国における感染症，近年では重要インフラへのサイバー攻撃などのリスクにより，大きな影響が出ることが危惧されている[1)]。

従来は設備ごとにセキュリティ対策が実施されていたが，今後はシステム全体を俯瞰（ふかん）したシステムコンセプトが必要になると考える。特に大規模なナショナルイベントの開催時には，みずからの思想を世界にアピール



注：略語説明　OODA（Observe, Orient, Decide, Act），UAV（Unmanned Aerial Vehicle）

図1｜社会インフラセキュリティのイメージ
複雑なシステムが高度に協調する都市においては，増大するさまざまな脅威から人々の安全・安心を守るセキュリティ対策が求められる。

することを目的としたテロ活動などが発生することが懸念されており，これを防止する対策が望まれている[2)]。

ここでは，日立グループの社会インフラセキュリティコンセプト（H-ARCコンセプト）の適用イメージと，それらに対応したセキュリティソリューションについて述べる（図1参照）。

2. 社会インフラセキュリティコンセプトの適用イメージ

まず，社会インフラシステムにおいてH-ARCコンセプトを具現化した場合の新たな付加価値と適用イメージについて述べる。

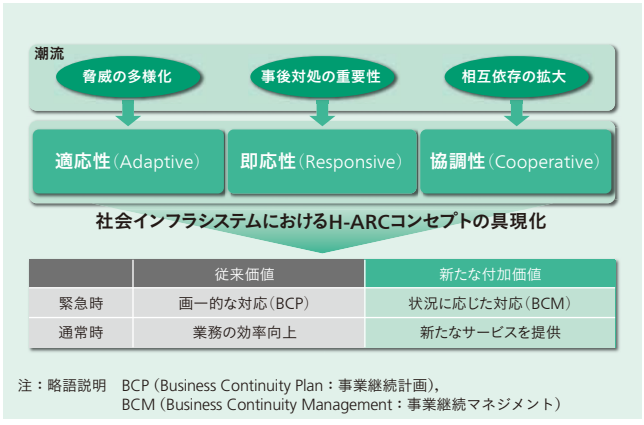
日立グループは，社会インフラセキュリティを取り巻く潮流として，「脅威の多様化」，「事後対処の重要性」，「相互依存の拡大」の3つを挙げ，今後必要となるセキュリティ上の概念として，「適応性（Adaptive）」，「即応性（Responsive）」，「協調性（Cooperative）」に焦点を当てたH-ARCコンセプトを導出した。

このコンセプトは，緊急時の事業継続計画をつかさどる従来のBCP（Business Continuity Plan）に，OODA（Observe, Orient, Decide, Act）ループの概念を加え，状況に応じた対応を可能するBCM（Business Continuity Management）に進化させるものである。通常時は，従来の業務の効率向上のほか，システムや組織の連携による新たなサービスの提供も可能になる（図2参照）。

次に，コンセプトを採用したシステムイメージについて述べる。

まず，組織間の協調性を確保するため，運用管理，ID管理，共通状況認識（COP：Common Operational Picture）などのセキュリティ・サービスを共通基盤として位置づけることにより，各社会インフラシステムアプリケーション間の連携を強化することが可能になる。各社会インフラシステムで発生した事象に対しては，監視（Observe），分析（Orient），判断（Decide），行動（Act）のループを回し，被害が最小となる事態対処法を決定することにより，即応性を確保できる。なお，このような仕組みにより，発生事象が，一部のシステムに限定されたものか，相互に関係したものかなどを判断することができる。

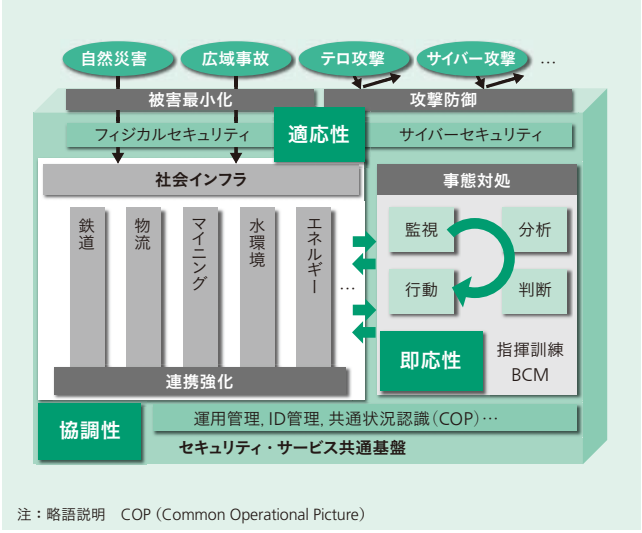
以上の構成をフィジカルセキュリティとサイバーセキュリティに展開することにより，物理空間とサイバー空間を超えて統合されたシステムの構築が可能となる（図3参照）。



注：略語説明　BCP（Business Continuity Plan：事業継続計画），
BCM（Business Continuity Management：事業継続マネジメント）

図2｜H-ARCコンセプトを具現化した場合の新たな付加価値

適応性（Adaptive），即応性（Responsive），協調性（Cooperative）に焦点を当てた日立グループの社会インフラセキュリティコンセプト「H-ARCコンセプト」は，緊急時，通常時において新たな付加価値を生み出すことが可能である。



注：略語説明　COP（Common Operational Picture）

図3｜H-ARCコンセプトのシステムイメージ

H-ARCコンセプトを具現化するシステムイメージを示す。

3. コンセプトを具現化するソリューション

ここでは，前述のコンセプトを具現化した都市向けのセキュリティソリューションを紹介する。なお，サイバーセキュリティ，制御セキュリティなどについては別稿で述べる。

一般に都市は外部との交通が発達しており，都市に流入する航空機，船舶，車両，人を対象に水際でセキュリティチェックをすることが高効率であるため，この観点で述べる。

3.1 空港トータルセキュリティソリューション

近年の空港では，一般乗客のチェックインや搭乗までの時間短縮によるサービス向上が顕著になってきている。

空港のセキュリティは，2001年9月の米国同時多発テロ事件を境に大幅に強化されたが，それ以降にも2005年7月のロンドン同時爆破テロ事件，2007年6月の英国車爆弾テロ未遂および空港施設へのテロ事件，2011年のドモジェドヴォ空港爆破事件など，交通機関などを標的としたテロ事件が世界各地で後を絶たない状況が続いている。

空港では，不特定多数の利用客が滞留する一般エリア，

特定者のみが出入りを許される制限エリアなどさまざまな区分がなされている。空港会社が警察や消防と連携しながら管理運営を行っているが，空港ビル内ではショッピングなどの滞留やスムーズな搭乗処理と，犯罪の巧妙化・凶暴化に対応する必要がある。つまり，犯罪者や不審者の早期発見・追跡と，付近の旅客・空港関係者の安全確保を，過剰なセキュリティを意識させずに両立することが重要と考える。

日立グループは，空港の安全・安心を守るため，トータルセキュリティに効率的な画像検索・画像追跡といった映像関係ソリューション，犯罪者の行動パターンを予測するソリューションなどを組み合わた，大規模監視ソリューションとしてのサービス提供を順次進めている（**図4**参照）。

3.2　海洋警備ソリューション

近年，国内の凶悪犯罪では，海外から持ち込まれた薬物・銃器などの関与も考えられる。また，国際テロ組織が，船舶から陸上施設または他の船舶に攻撃を加える事案，武器や大量破壊兵器関連物資などを密輸入する事案，テロリストを密入国させる事案などの発生が危惧されている。

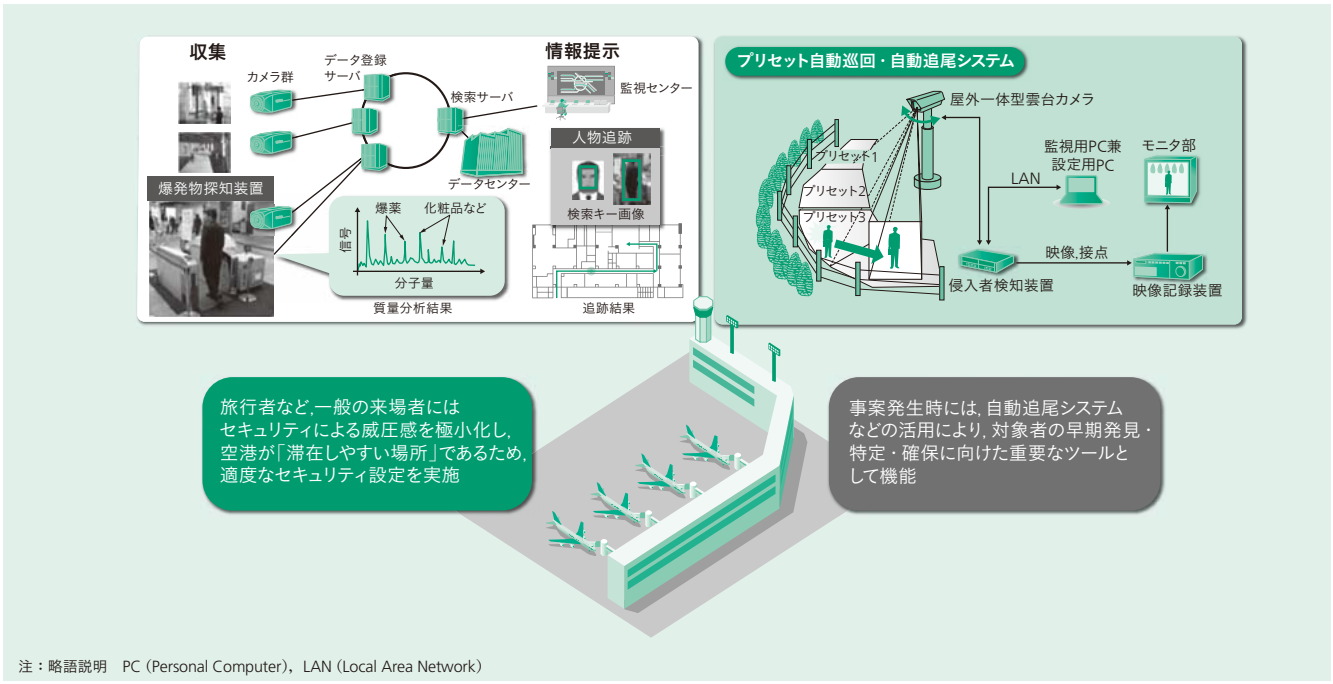
日本では，2002年7月に発効した「1974年の海上における人命の安全に関する条約（SOLAS74）」により，(1) 国際航海に従事する300総トン以上のすべての船舶，(2) 国際航海に従事するすべての旅客船，(3) 国際航海に従事しない500総トン以上のすべての船舶に，船舶自動識別装置（AIS：Automatic Identification System）の搭載が義務づけられている。そのため，船舶の識別符号，種類，位置，針路，速力，航行状態およびその他の安全に関する情報を自動的に送受信し，沿岸の船舶の動態を把握することが可能となっている[5]。

しかし，AISの搭載を義務づけられていない小型船舶があること，操業中の大型漁船は漁場の機密保持を目的に停泊できるため，船員による故意の停泊が容易であることなどにより，AIS情報によって全搭載義務船舶の動態を把握することはできないという課題がある[6]。

日立グループの海洋警備ソリューションは，海洋監視のための船舶の検出から，確認，分類，対応，解決までをトータルに支援するシステムである。検出・確認・分類フェーズでは，VTS（Vessel Traffic Services）・AIS情報を取り込み，沿岸に設置されたレーダ情報や航空機からのSAR（Specific Absorption Rate）情報など他のセンサーからのデータと相関を取ることにより，船舶などを識別し，精度の高い情報で状況を把握することができる。また，小型船舶にレーダおよびカメラを追加することで，レーダ覆域外の不審船を追尾・監視することができる。これらの情報を単一のCOPに統合表示することで情報共有を可能としている。対応・解決フェーズにおいては，チャット，ホワイトボード機能によるリスクの優先度や対応調整機能を有している（**図5**参照）。

3.3　水中セキュリティソリューション

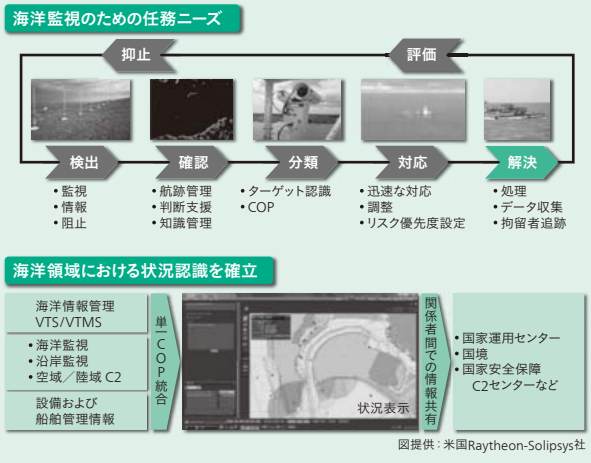
日本沿岸部には，空港施設，発電所および石油備蓄施設



注：略語説明　PC（Personal Computer），LAN（Local Area Network）

図4｜空港トータルセキュリティソリューション

通常時には，過剰なセキュリティを意識させない適度なセキュリティ設定で運用するが，異常時には自動追尾システムなどの活用による対象者の早期発見・特定・確保に向けた重要ツールとして機能する。



注：略語説明　VTS（Vessel Traffic Services），VTMS（Vessel Traffic Management System）

図5｜海洋警備ソリューション

海洋警備のためのニーズをサポートし，海洋領域における状況認識を確立する。

などの重要施設が存在し，それらの施設の水中からの脅威に対するセキュリティを充実させることは極めて重要であると考える。

海中では可視光や電波を含む電磁波は減衰量が大きいため，水中からの侵入を検知する方法としては，音波を用いたソーナーセキュリティシステムが有効である。適用するソーナー種別としては，遠距離での監視追尾用にはパッシブソーナーを適用し，近距離での目標識別用にはイメージングソーナーを適用することで，導入コストを低減でき，セキュリティとしても有効なシステム形態を取れると考える。

日立製作所は，2005年度から2007年度の間，東京大学生産技術研究所海中工学国際研究センターによる水中セキュリティソーナーシステムの研究に参画した。3年間の研究期間中に，実海面での試験評価を重ねた結果，研究開発したシステムが実際の水中潜入監視に有効であることが確認された（**図6**参照）。

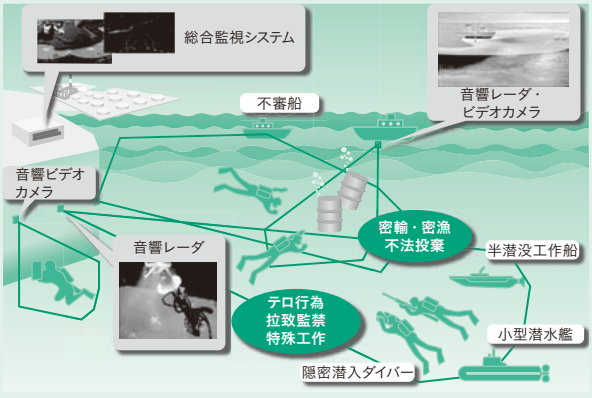


図6｜水中セキュリティソーナーシステムの運用構想

水中セキュリティソーナーシステムの運用構想を示す。

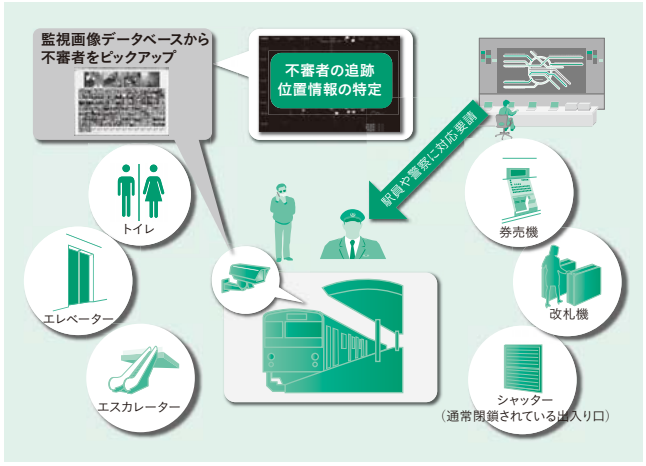


図7｜駅セキュリティソリューション

監視画像の応用技術とセンシング技術を用いて，不審者の検知・追尾が可能である。

3.4　駅セキュリティソリューション

2012年5月，東京地下鉄株式会社副都心線の渋谷駅で男性が刃物で切りつけられて大けがをした事件は，殺人未遂事件として捜査した警視庁によって数日で犯人が逮捕され，解決に至った。逮捕の決め手となったのは，東京地下鉄の駅に設置された監視カメラと渋谷駅近くの路上に設置されている防犯カメラの映像であった。

このように，駅では防犯目的での監視カメラの設置は進みつつあるが，抑止効果の一歩先に進む必要がある。それは，安全システムへの昇華である。高速画像処理の応用による不審者の事前検知ならびに追跡による周辺乗客の安全確保が，将来の安全システムの一端を担うと考えられる。限られたプラットフォームのスペースに大量の乗客が流れ込む日本の鉄道網の現状から，大量輸送を妨げるような安全システムの導入は難しい。そこで，監視画像の応用技術とセンシング技術を用いて，乗客や駅員に危険を知らせるなどの対策が可能である（**図7**参照）。

3.5　施設セキュリティソリューション

施設セキュリティは，イベントホールや大規模小売店舗，オフィスビル，工場，研究所，データセンター，マンションや老人福祉施設など，形状もそこに居合わせる人々も多種多様である。同様に，不特定多数の人々が集まる場所，特定の人々のみが利用する場所と，施設に応じたセキュリティが検討され，施されている。

東日本大震災を契機に，自治体や企業は，非常時の安否確認の重要性を再認識した。

安否確認をさらに発展させた，セキュリティシステムとの融合が進んでいる。在館者や工場内在席者の即時把握を目的とした，入退場管理と安否確認の組み合わせである。この組み合わせは，規模の大小に関わらず，工場での火災

などの事故発生時の安否確認に役立つものとして注目されている。

日立グループは，従来，大規模ビルやデータセンター向けにはローカル管理型のシステムを製作・納入してきた。一方で，マンションや小規模オフィス，老人福祉施設といった，高額の投資が難しい業態にある施設には，パブリッククラウドを活用したソリューションを提供してきた。パブリッククラウドの活用により，当該施設の利用者は高額の投資を抑え，維持管理に必要なコストの削減や運用の効率化が可能になる。例えば，マンション共用部の設備や，IC（Integrated Circuit）化されたマンションの鍵を24時間365日維持・管理していくことは，24時間対応の管理事務所に依存せずに行うことが困難である。しかし，日立グループのパブリッククラウドとサポート体制を活用することで，安価に実現することができる。また，パブリッククラウドは，それ自体を管理サービスとして位置づけることで，ローカル管理型では困難であった安価なオペレーティングシステム更新も可能であり，関係者から注目されている。

今後の取り組みでは，パブリッククラウドやプライベートクラウドをロケーションに応じて活用し，大規模ビルやマンション単体ではなく，商業地区やビル群といった特定規模のエリアを一括管理し，高いセキュリティを維持しつつ，これまで以上の効率的な運用をめざしている。国土交通省が推進する「エリアマネジメント」をさらに発展させた形態であり，セキュリティ管理をはじめ，エネルギーの効率運用などすべてをプライベートクラウドあるいはパブリッククラウドで一括管理するものである[7]。

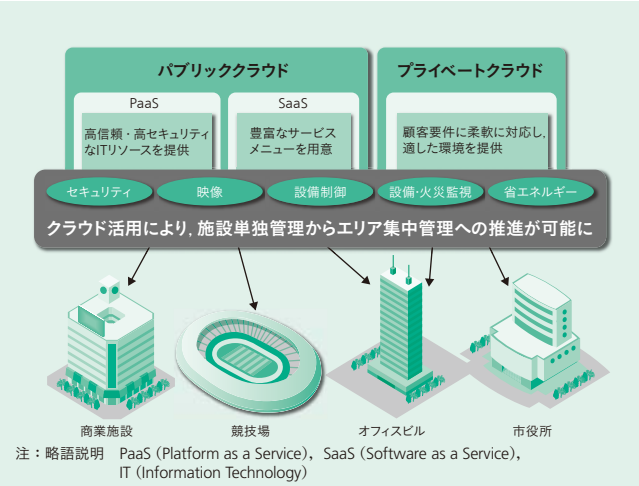


図8｜施設セキュリティソリューション
クラウド活用により，施設単独からエリア集中管理への推進が可能となる。

この取り組みは，情報の一元管理が可能なプライベートクラウドを適用したエリアマネジメントによる，従来の形態では難しかったビッグデータの活用を将来的な展望としている。それにより，エリア内部での過去の事案から該当者を記録し，該当者がエリア内に入場していることを管理者に注意喚起してトレースしていくといった新たなセキュリティ対策や，事案が発生する前に危険を予見して予防策を講じるといった管理手法の構築が期待できる（図8参照）。

4. おわりに

ここでは，日立グループの社会インフラセキュリティコンセプト（H-ARCコンセプト）の適用イメージと，それらに対応したセキュリティソリューションについて述べた。

ここで述べた各ソリューションは，安全・安心な社会の実現に貢献するものと考えられる。

参考文献など

1) 独立行政法人情報処理推進機構：標的型サイバー攻撃の事例分析と対策レポート（2012.1），
https://www.ipa.go.jp/files/000024536.pdf
2) 一般財団法人東京オリンピック・パラリンピック競技大会組織委員会：立候補ファイル，テーマ11-大会の安全，セキュリティ及び医療サービス
3) 厚生労働省健康局水道課：水道分野における情報セキュリティガイドライン（改訂版），
http://www.mhlw.go.jp/topics/bukyoku/kenkou/suido/houkoku/dl/guideline.pdf
4) 日本工業規格JISQ22320（社会セキュリティ－緊急事態管理－危機対応に関する要求事項）（2013）
5) 海上保安庁：AISを活用した航行支援システム，
http://www.kaiho.mlit.go.jp/syoukai/soshiki/toudai/ais/ais_index.htm
6) 日本海難防止協会：AISが安全運航に果たす役割，海と安全，No.545（2010）
http://nikkaibo.or.jp/pdf/545_2010.pdf
7) 国土交通省：エリアマネジメントの支援情報，
http://tochi.mlit.go.jp/tocsei/areamanagement/web_contents/shien/index_01.html

執筆者紹介


小野 郁宏
日立製作所 ディフェンスシステム社 マーケティング本部 事業開発センタ 所属
現在，危機管理分野，防災分野のシステム事業化に従事


相模 太
日立製作所 インフラシステム社 都市システム本部 セキュリティエンジニアリング部 所属
現在，統合セキュリティのソリューションビジネスに従事


中本 健司
日立製作所 インフラシステム社 都市システム本部 セキュリティエンジニアリング部 所属
現在，統合セキュリティのソリューションビジネスに従事