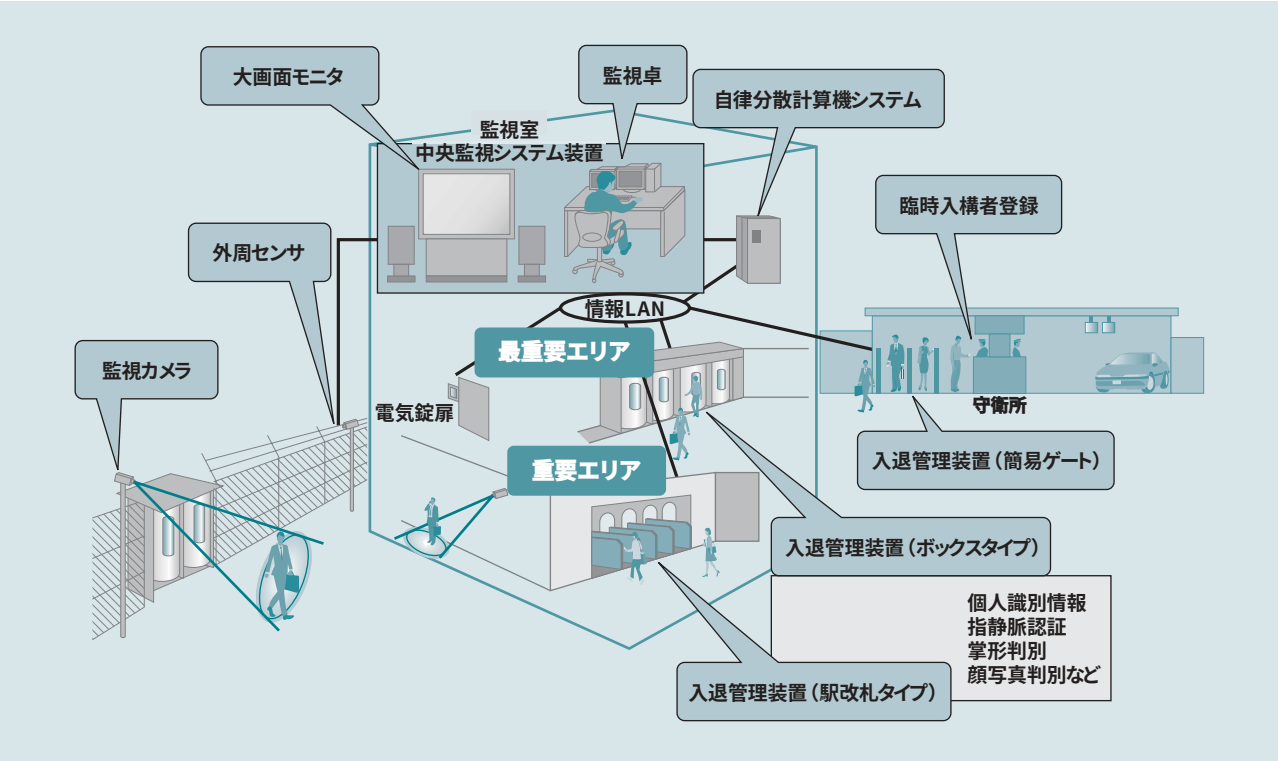
重要施設を守るフィジカルセキュリティソリューション

Physical Security Solution to Protect an Important Facility

久保田 龍治 Ryûji Kubota
石井 敦 Atsushi Ishii
河野 真作 Shinsaku Kawano
西川 良博 Yoshihiro Nishikawa
会沢 慎一 Shin'ichi Aizawa



注：略語説明 LAN（Local Area Network）

図1 PPSのイメージ

PPS（物的防護システム）は，抑止効果または敵の探知，敵のアクセス遅延，対処部隊による阻止の組み合わせのいずれかによって目標が達成される。具体的には，不法侵入を監視する「侵入監視システム」と，許可された人の出入りを制限する「出入管理システム」，さらにこれら両者のシステムを統括する「監視室システム」から構成する。

1. はじめに

「安全」は，火災，地震，善意の行為でのヒューマンエラーなどによる異常事態におけるシステムの運転状態などを表すのに用いられる。これに対し，「セキュリティ」は，悪意のある行為である攻撃を防御したり，検知するのに適用するシステムに用いられる。両者は重複する部分もあるが，安全とセキュリティシステムとの間で生じる葛藤の例として火災がある。例えば，施設内のアクセス制限された部屋で火災が発生し，負傷者が出た場合を想定すると，火災への対処として作動したスプリンクラーの水が，部屋の入り口の電気式ドアロックを短絡させ，救急スタッフの入室を妨害するといったことも起こりうる。これは安全とセキュリティシステムが，あらゆる条件で相互に動作するように設計されるべきであることを示す例である。

盗難，破壊，その他の悪意のある行為は二つの方法で阻止できる。第1番目は敵を抑止する（抑止効果）こと，第2番目は敵を打倒することである。抑止は敵による攻撃を失意させるのに非常に効果があるが，無差別にどの施設でも攻撃する敵に対しては効果がない。PPS（Physical Protection System：物的防護システム）では，「敵の抑止」は対策立案が難しいうえ，成功している抑止効果は敵が攻撃してこない限り，その有効性を確証できない。そこで，第2番目の機能である「敵の打倒」が考慮されることになる。ここでのPPSの基本的な機能は敵の検知，敵のアクセス遅延，およびセキュリティ員（監視部隊）による対処から成る。敵から玉，金，銀という資産を守る将棋で

**米国で発生した同時多発テロ以降，重要施設をはじめ多数の人が集まる施設などで
テロ対策を含めてセキュリティレベルが強化されており，PPSや機器へのニーズが高まっている。
2004年9月には国民保護法が施行され，危険性を内在する物質を有する施設などに対する攻撃が行われる事態や
多数の人が集合する施設に対する攻撃が行われる事態などへの緊急対処が想定されている。
日立製作所は，すでに，従来から開発してきたPPSを中核としたシステムを
重要施設である発電所，空港，図書館，高層ビルなどに適用してきている。**

は，飛車・角の大駒は敵から遠くに，歩は敵の近くに打つのが定石であるのと同様に，PPSでも検知はできる限りターゲットから遠くに，アクセス遅延はターゲットの近くであればいっそう優れた性能を発揮する。

ここでは，PPSの設計と評価方法，実施例，施設周辺のセキュリティシステム，および重要施設の例として港湾施設について述べる（**図1**参照）。

2．PPSの設計と評価方法

2.1 PPSの設計方法

（1）設計基礎脅威（DBT：Design Basis Threat）

脅威の定義は，目標を決定したり，PPSの有効性を評価するときに考慮される。敵についての必要な情報として，動機，ターゲットに応じた潜在的なゴール，戦術，員数，能力がある。脅威の定義には敵のタイプとして，外部者，内部者，内部者と外部者との衝突が想定される。

（2）ターゲットの明確化

ターゲットの明確化は，PPS設計そのものが何を防護すべきかを明確化することであり，防護すべきエリア，資産，行為を明確化することになる。

（3）PPSの設計

PPSの究極の目標は，公然または人目につかない悪意のある行為の達成を阻止することである。代表的な目標はクリティカルな装置の破壊，施設内部の資産や情報の盗難を防止すること，および人の防護である。PPSは抑止効果または検知，遅延，対処の組み合わせのいずれかによって達成されなければならない。

（a）検　　知

検知は敵の行為の発見である。この検知には公然，あるいは人目につかない行為の検出も含まれる。さらに，検知には警報の要因が攻撃によるものか，誤報によるものかを決定する評価も含まれる。

物的防護の検知の機能には出入制限を含む。出入制限は認可された人に入場を許可し，認可されていない人やモノの入場を検知する。出入制限の有効性の指標は処理速度（スループット），他人受入率，本人拒否率である。

（b）遅　　延

遅延はPPSの第2番目の機能である。これは敵の侵攻をスローダウンさせる機能である。遅延は人，バリア，錠，および遅延活動によって達成できる。もし，対処部隊が常駐し，十分に防御された場所にいるのであれば，遅延の要素として考慮できる。遅延の有効性の指標は，検知後敵が遅延の各要素をバイパスするのに要する時間である。

（c）対　　処

対処機能は対処部隊が敵の成功を阻止するための行為から成る。対処は妨害でもある。妨害は，敵の侵攻を停止させるために適切な位置に到着している十分な人数の対処部隊と定義される。これには敵の行為や対処部隊の配備についての正確な情報に関する監視部隊との連絡も含まれる。対処部隊の有効性の指標は，敵の行為についての報告を受信してから敵の行為を妨害するまでの時間である。

（4）PPS特有の設計上の概念

（a）深層防護

深層防護は，「安全」ではディフェンスインデプスが適用されるが，「セキュリティ」ではプロテクションインデプスが適用される。後者はゴールを達成するために，敵に数多くの防護的な装置をシーケンス的に回避させたり，打破させたりすることを要求することになる。

（b）タンパ防護

タンパ防護とは，ハードウェアやシステム設計がタンパリングによって無効にされるのを阻止する特性を持っていることである。具体的な適用事例としては，システムの妨害抵抗性（Tamper-Resistant）や抵抗表示（Tamper-Indicating）がある。

2.2 PPSの評価方法

通常のバリアの施設からの盗難という単純なシナリオでのタイムライン分析の例を**図2**に示す。シナリオは敵がフェンスの外側にいる時点から開始し，敵が盗んだ資産をフェンス外へ持

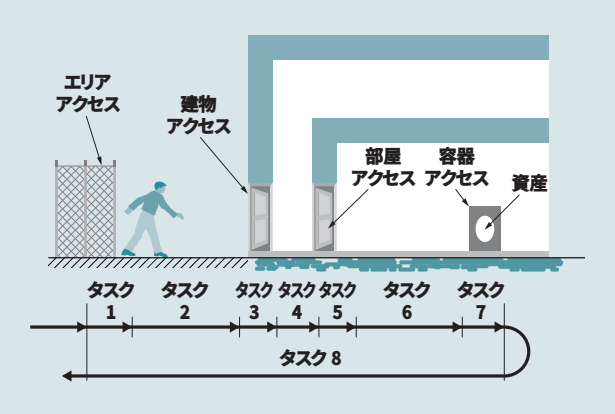


図2　タイムライン分析のイメージ図
敵が資産を盗むには，全部で8個のタスクを完遂しなければならないことを表す盗難パスを示す。

ち出した時点で完了する。この例では，対処部隊が妨害できなかったら，敵は約3分で盗難を完了できると仮定する。

各種の防護システムのゴールに必要な対処時間を例示するために，即座の警報評価能力を持つ周辺探知システムは，施設のフェンスの内側に存在すると仮定する。建物に侵入する前に敵を阻止することをゴールとすると，対処部隊は警報発令後約1分以内に到着しなければならない。また，ゴールが資産に対する敵の破壊行為の阻止とするならば，対処部隊は警報後約2分以内にその地点に到着しなければならない。ゴールを盗難後フェンスエリア内に敵を封じ込めることと仮定するならば，対処部隊は警報後約3分以内に到着しなければならないことになる。

実際の評価では，数百，数千のシナリオが想定されることから，ASD（Adversary Sequence Diagram）を作成し，最も低い阻止確率（最も敵が成功しそうなパス）を算出することになる。また，許容リスクを残留リスクと同程度まで低減する対策も必要である。最終的には，これらの評価を踏まえて，非常事態計画書を作成し，訓練などに反映させることが望まれる。

3. PPSの実施例

PPSは，許可されていない場所から敷地などに入るのを検知する侵入監視システムと，許可されたゲートなどから入ってくる人の入域資格などをチェックする出入管理システム，さらにこれら両システムを統括して監視する監視室システムから構成する。

侵入監視システムは，敷地境界に設置されたフェンス沿いの侵入監視センサと，その侵入監視センサ区間に対応した監視カメラから構成する。

出入管理システムは，人の出入を制限するゲートや扉があり，人の入域資格を確認するIDカードとカードリーダから構成する。

監視室は，上記システムを監視するためのモニタと各種情報を表示するコンピュータ，および各種操作ボタンを収納した監視卓から構成する。

3.1 侵入監視システム

侵入監視システムでは，さまざまな侵入監視センサが使用されている。侵入監視センサは，設置環境や設置場所の気候などに応じて最適なセンサを設置する必要がある。各種センサの比較表を**表1**に示す。また，センサによっては，センサチェック機能付きやセンサへのいたずら探知機能付きなど，同じ原理のセンサでも使い分ける。

監視カメラには多種類のカメラがあるので，設置される場所の照度や監視対象に応じて使い分ける。

センサが発報した際には，直ちに該当のカメラ映像が確認

表1　侵入監視センサの比較
鳥，動物，木々などの影響を考慮してセンサを設置する。

	フェンス（振動）センサ	テンションセンサ	赤外線センサ	パッシブ赤外線センサ	マイクロ波センサ
設置方式	バー取り付けあるいはフェンスに添加	地上自立型	地上自立型 対向設置	壁側壁あるいは建物側壁	地上自立型 対向設置
動作方式	ケーブル内部振動検知 残線・短絡検知	ケーブル振動検知 残線・短絡検知	赤外線ビーム送受信 ビーム遮断で検知	熱感知	マイクロ波検知
長　所	1警戒最大300 mで安定動作 目立つため抑止効果 侵入区域特定容易	1警戒最大50 mで安定動作 目立つため抑止効果 侵入区域特定容易	長距離で安定 設置は目立たない。 複数ビームでサイズ安定 複数ビームで誤報が少ない。	設置が比較的容易 面検知が可能	飛来物の影響が少ない。 耐候性に優れている。
短　所	長距離で若干誤報率が上がる。	長距離で若干誤報率が上がる。	設置・調整に手間 見通し確保が必要	検知範囲が狭い。 太陽光・熱源の影響 誤報の可能性が高い。	検知領域が不定 電磁波の影響大 草木などの揺れに弱い。 壁などに影響される。
センサ作動範囲	線検知（一次元）	線検知（一次元）	線検知（一次元）	面検知（二次元）	立体検知（三次元）
センサ設置間隔	～300 m	～50 m	～100 m	10数 m×10数 m	5～100 m
耐候性	雨，霧には強い。 風，積雪，低/高温に難	雨，霧には強い。 風，積雪，低/高温に難	風には強い。 雨，霧などに難	風，雨，雪，霧に比較的強い。	雨，雪，霧に強い。 風に弱い。
耐破壊性	破壊は簡単 ただし検知可能	壁の内側なら破壊は困難	壁の内側なら破壊は困難	低位置設置のため破壊は容易	壁の内側なら破壊は困難
メンテナンス	物理的な破損点検	物理的な破損点検	防護ガラスなどの定期清掃	防護ガラスなどの定期清掃	定期点検だけ
カメラとの連動	区間を小さくすれば可 ズームアップ可能	区間を小さくすれば可 ズームアップ可能	連動は可能だが位置の特定は不可	連動は可能だが，位置の特定は不可	連動は可能だが，位置の特定は不可
適切な設置場所	壁の上部	壁の上部	壁の内側	敷地内特定区域	壁からできるだけ離れた敷地内

できる。その方式はさまざまであるが，日立製作所は，発報信号を高速に伝達するために，自律分散方式のネットワークや画像フレームメモリを使用して，発報した際の画像を静止画で記録する方式を採用している。また，センサが発報した原因も多岐にわたって入力できる。さらに，センサの健全性を確認するために，最低1日1回センサチェックする。これら一連の情報は，ログファイルとして保存されており，いつでも検索できる。

3.2 出入管理システム

出入管理システムは，カードシステムと出入管理ゲートシステムに大別される。

カードシステムとして，これまで磁気カードが多数使用されていたが，今後は，データの容量も大きく保存データに対するセキュリティレベルも高いICカードが主流になると予測される。また，使い捨てのような使用方法では，二次元バーコードも多く使用されると考えられる。

出入管理ゲートは，ある程度の入域者数があり，人手による管理が困難な際に有効となる。出入管理ゲートも多様にあり，最もセキュリティレベルが高い強化扉から，駅の改札ゲートのような簡易なものまである。そして，重要なのは，監視員がゲートの近くにいるか，無人かによってゲート機能が異なるということである。特に無人運転する場合，ゲートには1人通過を確認する機能があるので，容易にゲートを飛び越えることなどができないようにしなくてはならない。

また，ゲートを通過する際に本人認証の目的で，個人識別装置を使用する場合もある。個人識別装置の比較を**表2**に示す。

日立製作所は，低誤報率で，使用時の抵抗感が少ないことなどから，指静脈認証装置を開発している。個人識別装置は，金融機関やパスポートなどに順次導入される予定であり，身近な装置になっていくと期待される（**図3**参照）。

出入管理システムで重要なことは，入域している人の現在の居場所を絶えずシステム側で把握することである。このことにより，カードの二重使用などが防げるとともに，問題が発生した場合でも，該当者の割り出しが迅速に行えるという長所がある。システム側で絶えず入域者の居場所を把握するために，自律分散システムを採用して処理の高速化を実現している。

3.3 監視室システム

監視室には，侵入監視システムの監視カメラ画像を確認するモニタが設置されている。1人の監視員が確認できるモニタ台数は3～4台程度であるため，通常は，各監視カメラの映像を一定周期で表示しているが，センサが発報した場合は該当のカメラ画像に自動的に切り替わる。

最新のシステムでは，各カメラ映像をフレームメモリなどの使用により，常時サイクリックに記録しておき，センサ発報によって常時サイクリックを止めることにより，センサ発報時の画像が確認でき，センサ発報原因を正確に把握できる。

図3　指静脈認証付き出入管理ゲート
指静脈認証は低誤報率であるため，出勤時でもゲートで待つ人の列は短い。

表2　個人識別装置の比較
生体認証のうち，生体内部情報を透過光で照合できるのは指静脈認証だけである。

分　類	装置の大きさ	照合対象の特徴	適用分野	課　題
指紋	数 cm²	特徴点（分岐・端点，ほか）	入出退，アクセス管理	ウェット肌，乾燥肌対応
掌形	数十 cm²	手の大きさ，長さ，比率	入出退管理	装置の小型化
虹彩	50×20×20～(mm)	目の虹彩（アイリス）の紋様	入出退管理	装置の小型化
顔	カメラ	顔の輪郭，目・鼻の位置	入出退管理	照明，撮影角度，背景の制約
音声	マイク	音声波形，発生速度，ほか	入出退管理	体調の影響
サイン	数 cm² タブレット	筆順，筆速，形状	アクセス管理	偽筆対策
指静脈	数 cm²	静脈形状，血流	入出退管理	体調の影響

4. 周辺設備の概要

重要施設のPPSの設備に付随する施設周辺のセキュリティシステムについて述べる。

4.1 入出門管理

重要施設の敷地周辺は外部に対して塀やフェンスで囲まれ，出入り口は限定されている。一方，施設に出入りする人は，必ずしも従業員だけではなく，関連会社や協力会社，あるいは敷地内の食堂などの施設で働く人など多岐にわたる。さらに，施設へのアクセス方法も自動車，オートバイ，自転車，徒歩などさまざまである。

出入り口では，警備員による入域許可証の確認などによって人の出入りが管理されるが，出退勤時など人の出入りがピークになる時間帯では，効率的な入域許可証と本人の一致確認が求められる。

許可された人だけを敷地内に入域させることは，セキュリティ確保上重要であるが，いっそう高度なセキュリティを確保

するには，入域した人が確実に退域したかといった「いつ」，「誰が」出入りしたかについてシステム的に管理することが有効である。

以上に述べたことから，入出門管理システムでは，以下の要件を満足するシステムの構築が重要であると考えられる。

(1)「いつ」，「誰が」出入りしたかを管理できるシステム

(2) 出退勤時の出入りのピーク時への対応を考慮した効率的な管理を可能とするシステム

(3) 自動車，徒歩など，アクセス方法の違いに対応が可能なシステム

リアルタイムでの人の管理を可能にする技術としては，RFID（Radio-Frequency Identification）や非接触ICカード，バーコード，指静脈などの生体認証技術の適用が考えられる。ここでは，アクティブあるいはパッシブRFIDを適用した場合の運用イメージについて述べる（図4参照）。

このシステムは，電源設備を有し，電波を発信することが可能なアクティブRFID，あるいはパッシブではあるが比較的離れた距離で交信可能なRFIDを貼り付けた入域許可証を発行し，タグリーダによって，入出門を管理するものである。

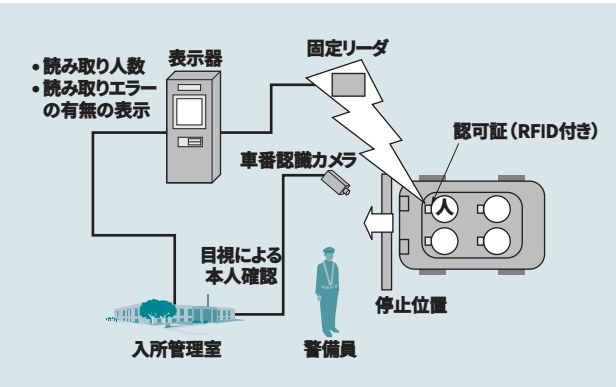
このシステムを採用することで，システム管理者による入出者の一元管理が可能となる。また，タグリーダの読み取り結果を表示器に表示させることで，読み取り人数や読み取りエラーなどを警備員に表示させることが可能である。さらに，車番認識装置を設置することで，自動車の管理も可能となる。

実際のシステム構築に際しては，出入りする人数や実際の運用方法など，対象施設固有の条件を考慮することが重要であり，今後も，顧客のニーズを反映した提案をしていく。

4.2 入所者位置管理

近年，敷地入り口での入出門管理だけでなく，敷地内の屋外における人の位置検知のニーズが高まっている。

適用可能な技術としては，GPS（Global Positioning System）



注：略語説明 RFID（Radio-Frequency Identification）

図4 RFIDを適用した入出門管理イメージ
比較的遠距離での利用が可能なアクティブRFIDとパッシブRFIDを適用した運用例のイメージを示す。

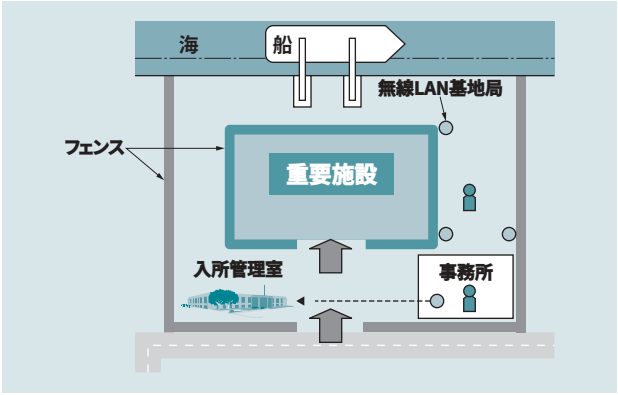


図5 無線LAN基地検知技術を適用した位置管理イメージ
高精度な位置検知を行うことで，高度な物的防護対策を実現する。

やRFID技術，あるいは無線LAN（Local Area Network）位置検知技術などの適用が考えられる。ここでは無線LAN位置検知技術を適用した場合の運用イメージについて述べる（図5参照）。

このシステムは，携帯用端末を所持している人を，無線LAN基地局で検知するものである。このシステムを採用することで，正確な人の管理が可能になり，許可されていないエリア通過時に未許可であることをアナウンスすると同時にシステム管理者へ通知することができる。また，万一の災害時に，敷地内にいる人の把握や効率的な避難誘導を可能にする。位置管理システムについても，入出門管理システムとの連携を考慮しつつ，顧客のニーズを反映した提案をしていく。

5. 港湾施設の概要

5.1 港湾セキュリティの背景

2001年9月11日の米国同時多発テロを契機として，世界では海上の安全を定めたSOLAS条約（The International Convention for the Safety of Life at Sea）が改正された。これを受け，国内では「国際航海船舶及び国際港湾施設の保安の確保等に関する法律」が施行され，2004年7月までに国際ふ頭における保安対策が義務づけられた。

5.2 国際港湾施設の保安措置の概要

国際港湾施設の保安措置の概要を図6に示す。

実施すべき保安措置は，(1)人的対応としては，保安措置の実施責任者である保安管理者を選任し，自己警備のための保安規定を作成して実施することにより，国の承認を受けること，(2)物的対応としては，制限区域を設定してフェンスや照明などの保安設備を設置することである。

自己警備では，施設への出入管理，貨物の取り扱い管理，施設内外の監視などを実施している。

人的な対応を支援する保安設備として，フェンスや照明のほかにカメラなどを設置する施設が多い。例えば，不正な侵

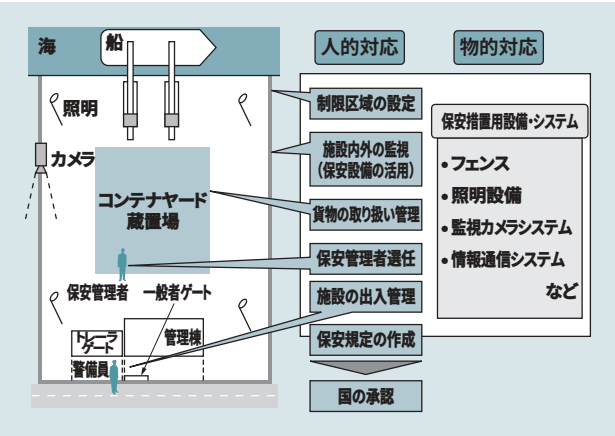


図6　港湾施設の保安措置の全体像
港湾施設の保安措置は，各保安措置が一体となって機能することによって実現されている。

入者は早期に監視室の警備員にカメラなどによって捕らえられ，直ちに保安規定に従い，電話や無線，放送を通じて対処が行われる。

カメラの映像は貨物の安全性を証明するための記録として活用するとともに，保安措置の見直しなどに利用する。停電などへの対応として無停電電源装置や非常用発電設備などの電源設備も装備している。

保安設備は，監視対象や監視区画，警備員の配置や対処のしかた，夜間の場合には照度など，施設の特徴に応じて配備している。

複数の施設の一体的な監視や，関係機関と連携して対処する場合，侵入や不審事象などの現場の情報伝達を最速化するため，共有する映像の数，配信先，ネットワーク形態，監視の運営形態や権限などの体制に応じて，映像配信制御装置，映像符号化伝送装置，セキュアネットワークなどを用いる。

5.3 今後の港湾セキュリティ

今後は，前述の保安設備に加えて，情報疎通と初動体制を早期に確立し，危機管理対策や意思決定などを支援するナビゲーションシステム，保安対策用テレビ会議システムなどが必要である。

貨物や手荷物については，港湾施設や税関などの水際で不審物を発見することを目的とした爆発物探知装置や薬物探知装置，X線検査装置が有効である。不審物の確認とあわせて，物流情報や画像情報と連携した記録も重要である。

施設の出入管理には，顔写真の付いた許可証などが現在使われているが，セキュリティ強化と物流効率化のため，ICカードやRFIDタグと連携し，日立の特長的な技術である指静脈認証による本人確認は有効である。

また，人だけでなく，車両，船舶，貨物にユニークなIDを付与し，ICカードやRFIDタグを活用したID管理と出入管理，ヤード管理との連携が必要になる。人，車両，船舶，貨物の「情報」と「物体」の情物一致により，業務の効率化と保安の強化を両立することを目的として，トレーサビリティが必要になる。

6. おわりに

ここでは，PPSについて，設計と評価方法およびその実施例の概要を述べた。

ヒューマンエラーの対策では，人の行為は善意と見なすことで対応できる。一方，盗難や破壊のような悪意のある行為は，ヒューマンファクタといった安全設計の考え方ではなく，PPS特有の設計法が要求される。

日立製作所は，長年の実績に基づき，世界トップクラスのフィジカルセキュリティソリューションを提案していく所存である。

参考文献

1）Mary Lynn Garcia : The Design and Evaluation of Physical Protection Systems, Elsevier Science（2001）

執筆者紹介

久保田 龍治
1979年日立製作所入社，ディフェンスシステム事業部 フィジカルセキュリティビジネス推進統括センタ 所属
現在，フィジカルセキュリティ事業の推進に従事
工学博士
日本原子力学会会員，日本人間工学会会員，日本人工知能学会会員，日本機械学会会員

西川 良博
1981年日立製作所入社，ディフェンスシステム事業部 フィジカルセキュリティビジネス推進統括センタ 所属
現在，重要施設のフィジカルセキュリティに従事

石井 敦
1992年日立製作所入社，電機グループ 社会・産業システム事業部 事業企画本部 情報システムエンジニアリング部 所属
現在，公共・社会分野向けシステムの取りまとめに従事

会沢 慎一
1993年日立製作所入社，トータルソリューション事業部 公共・社会システム本部 社会システム部 所属
現在，重要施設向けセキュリティ分野のソリューション拡販に従事

河野 真作
1993年日立製作所入社，トータルソリューション事業部 公共・社会システム本部 社会システム部 所属
現在，港湾・ガス・セキュリティ分野のソリューション拡販に従事