

融合セキュリティ管理・監視システム

Converged Security Management (CSM)



セキュリティの動向

変化するセキュリティ市場

- ・ 現在情報セキュリティ市場は新製品開発段階と市場に商品が普及する成長期を経て、他部門との融合化現象が展開される成熟期に突入
- ・ ITシステムセキュリティ、ネットワークセキュリティ、個人情報セキュリティで自動車・医療・金融などの産業だけでなく社会の間接インフラ・セキュリティに幅広く適用される“知識情報セキュリティ産業”に跳躍

情報セキュリティ産業

- One Person
- One Computer

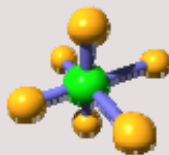
ITシステムセキュリティ



2,528

- One Person
- Many Computer

ネットワークセキュリティ



6,261

- One Person
- Many Information

個人情報セキュリティ



7,482

知識情報
セキュリティ産業

ITセキュリティ技術/製品間融合

ITセキュリティ+物理セキュリティ融合

IT 融合産業セキュリティ

(単位:億ウォン,年度)

未来デジタル時代のセキュリティ脅威と弱点

サイバー攻撃で国家ネットワーク体系を掌握
(映画“ダイハード4の中にファイアー セール ”)

1

交通管理コンピュータネットワーク占領

- ・ 信号灯かく乱
- ・ 鉄道管理システム誤作動

2

証券及び通信コンピュータネットワーク掌握

- ・ 株価暴落及び残高操作
- ・ 放送の悪意的利用

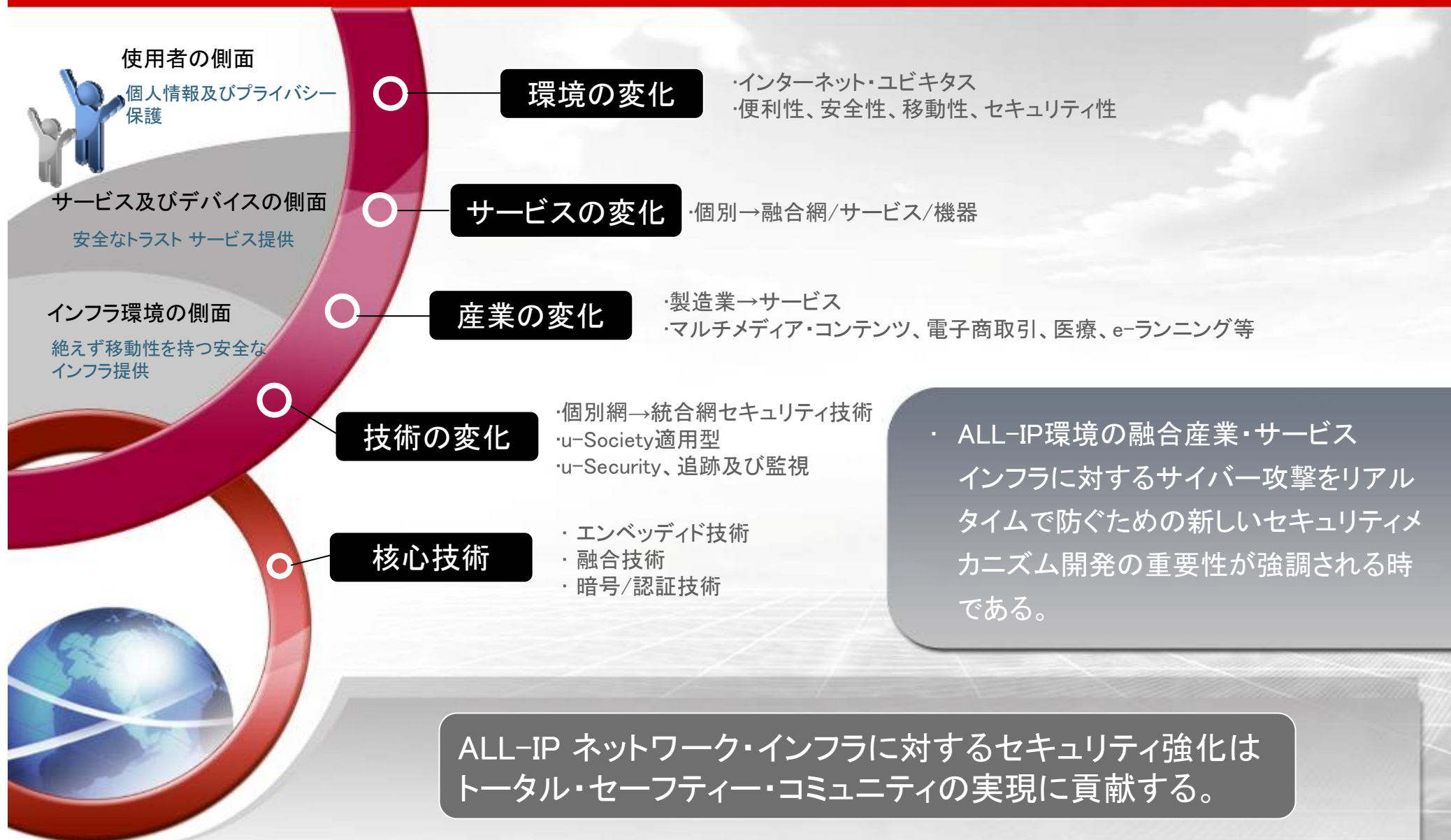
3

公共施設統制権確保

- ・ ガス、首都、電気などの公共サービスに対する統制

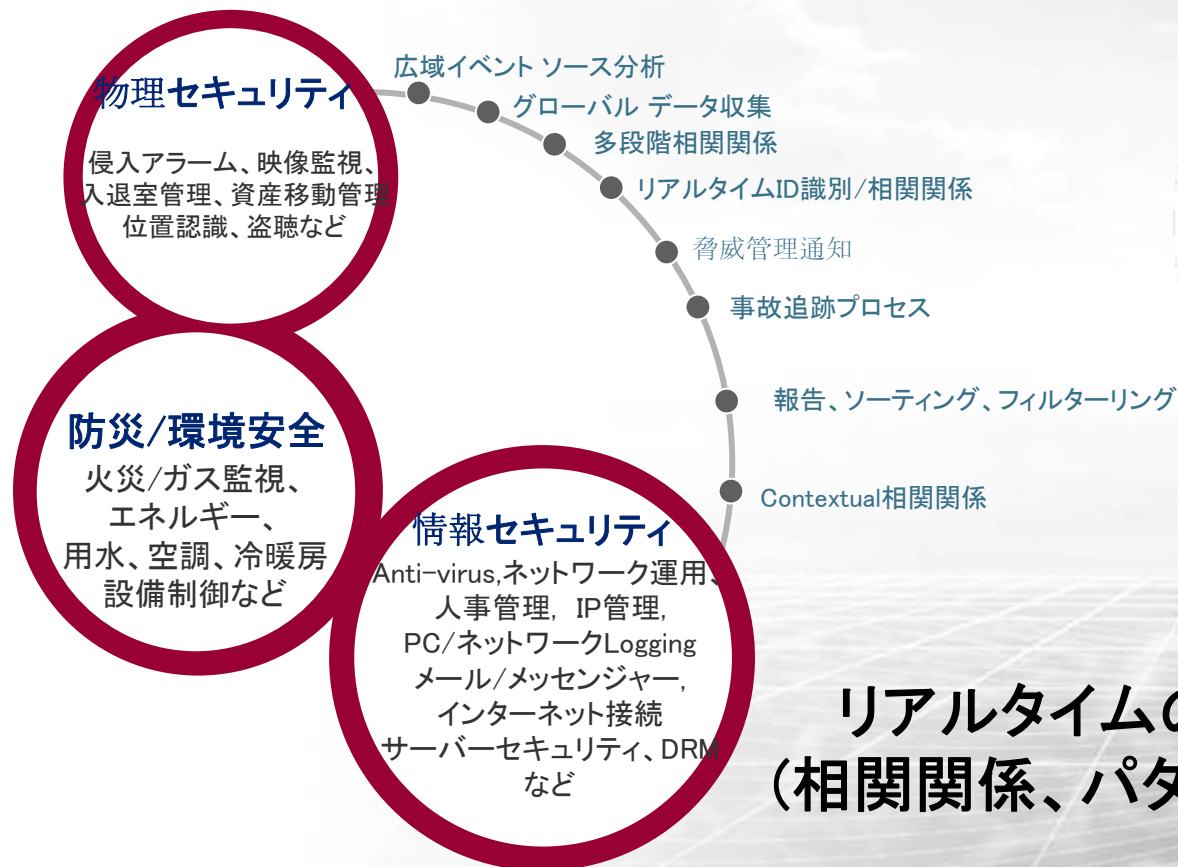


融合セキュリティ管理・監視の必要性



融合セキュリティ管理・監視システムの概要

- ・ 個別で単純モニターされた信号を融合/分析して、意味あるセキュリティ脅威の管理情報に加工
- ・ →全社的なセキュリティ脅威の事前予測及び積極的な統制が可能
- ・ 物理セキュリティ + 情報セキュリティ + 防災/環境安全信号を融合/分析
- ・ →リアルタイムでのセキュリティ脅威モニター及び、経営陣の意志決定の支援

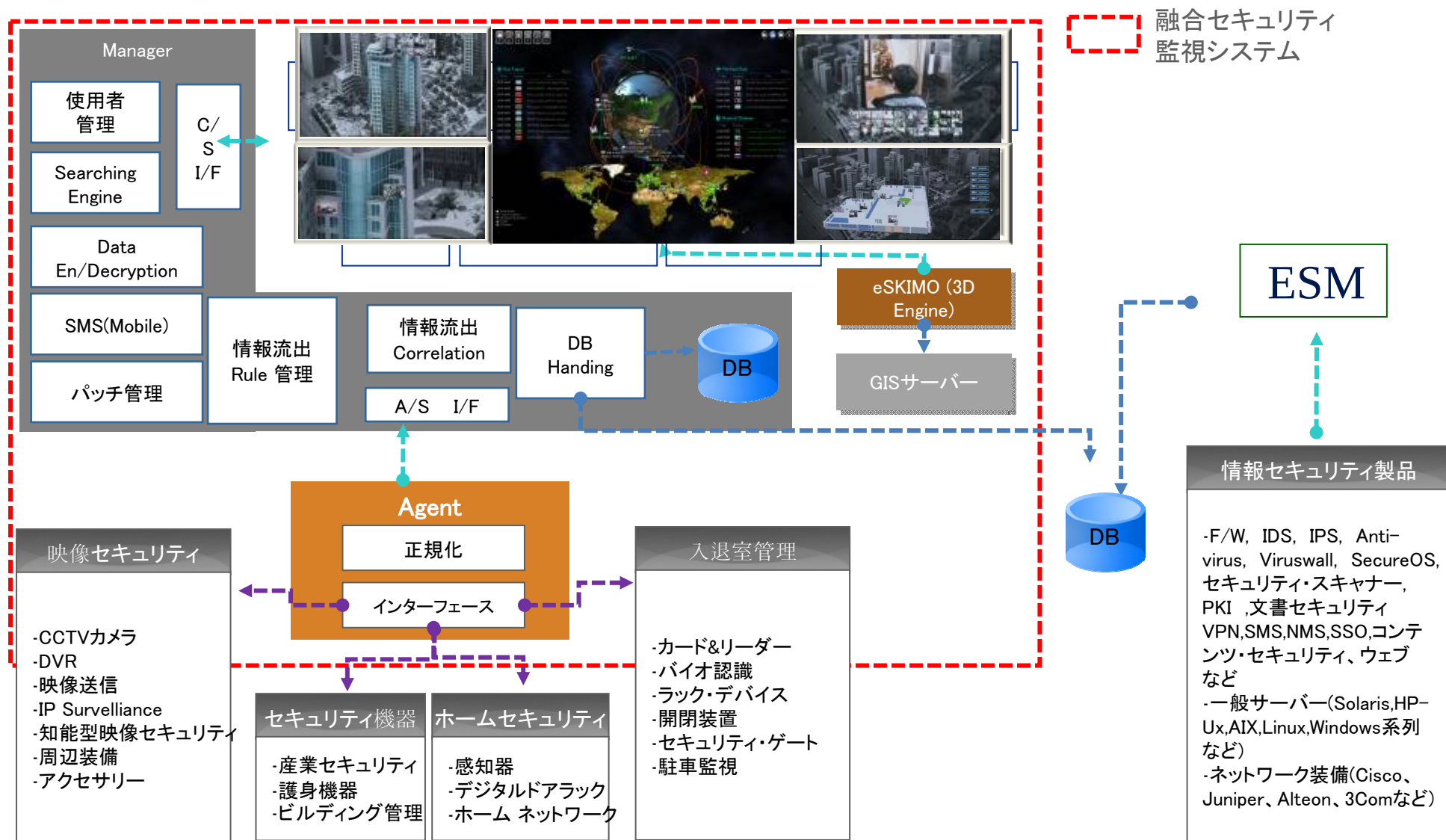


セキュリティ脅威予測 及び 早期対応・事故調査・レポート

- ・セキュリティ脅威検知
- ・リアルタイム報告
- ・レポート産出
- ・3D ディスプレイ
- ・事業への影響分析
- ・法規遵守報告
- ・正常でないパターン検知
- ・脅威関連資料

リアルタイムの情報融合/分析
(相関関係、パターン、アノマリ分析)

融合セキュリティ管理・監視システムのアーキテクチャー



融合セキュリティ管理・監視システムの特長点

融合セキュリティ管理・監視システムの画面



便利なユーザ インターフェース

ユーザー中心の分かりやすい3D GUI構成及び多様な形態のwindows GUIで、運営状態と障害状況を動的に表現

システムの柔軟性

企業の環境によって多様な形態のセキュリティ監視システムの構成が容易

システムの拡張性

分散環境及び中央集中型環境の運営方式が可能で、同一製品群に対するアド・オン機能の支援

強力な システム連動性

世界的に多様なセキュリティ・システム及び防災/環境安全装備との連動が可能

接近の容易性

いつでもどこでもネットワークを通じて、サーバーに接続して迅速な状況監視や情報分析が出来るようにサポート

保守費用節減

障害感知を自動で行うため、頻繁な管理の必要無し

融合セキュリティ管理・監視システムの主要機能

- **表現管理:**3D、GIS、E-MAPを利用した監視メイン画面、イベント状況表示、運営者中心の選択的画面構成
- **画面管理:**拡大、縮小、移動、回転、視野角、調整機能

融合
監視

運営
管理

- **構成管理:**個別環境に対するローカルマネージャー、分散環境に対するマスターマネージャー
- **拡張性:**大規模のインフラ構成に伴うサーバーの垂直的、水平的拡張が可能

LIGER-1

- **オブジェクト生成:**3次元オブジェクト生成機能、オブジェクトテクスチャ指定機能
- **オブジェクト調整:**オブジェクト追加、移動、削除、コピー機能

オブジェ
クト編集

連動
管理

- **連動方式:**Log File、API、Syslog、SNMP、Serial、TCP/IPなどすべての連動方式の支援
- **連動製品:**多数のセキュリティ製品(物理セキュリティ、情報セキュリティ、施設安全)連動技術の保有

融合セキュリティ管理・監視システムの導入効果

リアルタイムの障害検知を通しての迅速な対応

- 各種IT装備及び設備に対する障害発生をリアルタイムで検知
- 正確な障害ポイントを把握して、障害処理時間の短縮
- 迅速な障害対応処理を通してのサービス障害時間短縮

温度、湿度、漏水など適正な室内環境を維持して、IT装備の障害防止

- 温度変化の管理を通しての障害予防
- グラフ形式で温度変化の推移を分析して、適正温度の維持
- 漏水センサーを利用したリアルタイムでの漏水検知

設備の監視とセキュリティ・システム間の連動監視を通しての高度な障害対応

- 設備の障害が発生時、事故現場のカメラと自動連動
- 撮影映像と入退室記録を事故処理の証拠として活用可能

システム管理及び保守コストの節減

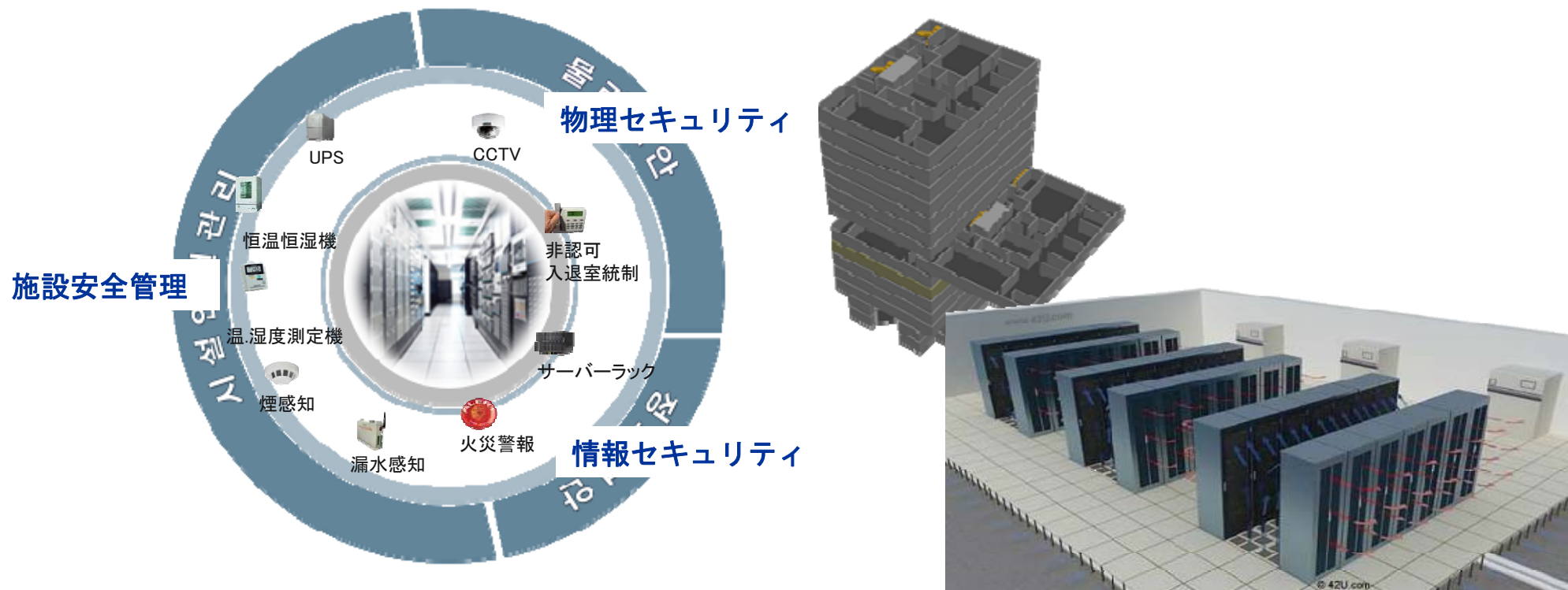
- リアルタイムで障害を感知するため、定期的な施設管理の必要無し
- 事前予防、迅速な障害処理による保守コストの節減
- システム自動化による管理人コストの節減

ユーザーのプロファイリング分析を通しての内部情報の流出防止

- 特定使用者と関連した情報を短時間で把握
- 物理セキュリティ・イベントと情報セキュリティ・イベントの融合分析を通して、事件に対する正確性向上
- 体系的な証拠収集及び監査費用と時間を節約

融合セキュリティ管理・監視システム（サーバールーム監視）

- ・ 3D鳥瞰図でN/Wセキュリティ及び入退室セキュリティ、映像監視、FMS (UPS、恒温恒湿など)を統合的にモニタリングできる統合監視システム



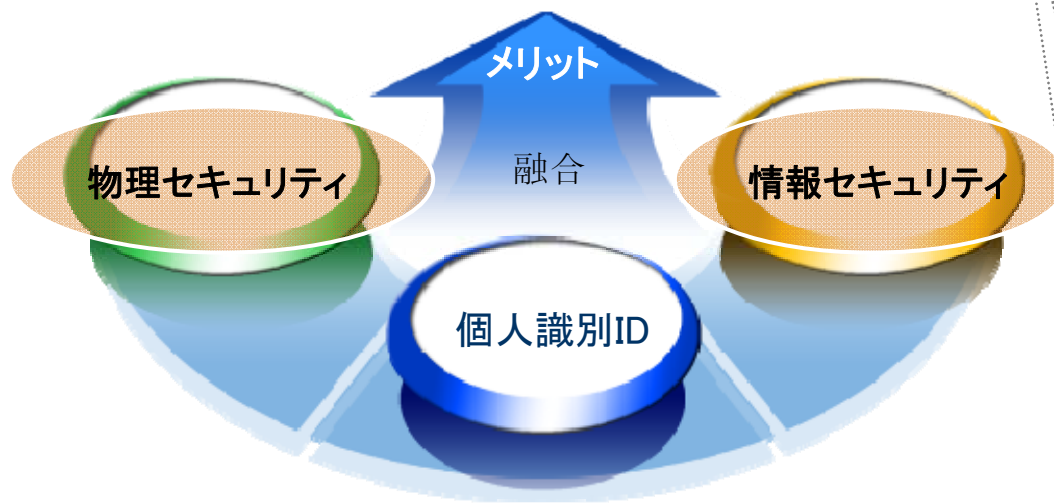
期待効果

- ・ 実写の鳥瞰図を通して、多様なIT装備と設備の障害発生時にリアルタイムでの検知及び予測による対応能力の向上
- ・ 設備の障害が発生時、事故現場のカメラと自動連動による障害対応
- ・ 情報セキュリティと物理セキュリティ及び施設管理システムの自動化による管理費用の節減

融合セキュリティ管理・監視システム [内部情報流出監視]

- ・ 物理セキュリティ・イベントと情報セキュリティ・イベントの間に共通の認識手段生成

特定個人の物理的・論理的
正体と位置を動機化



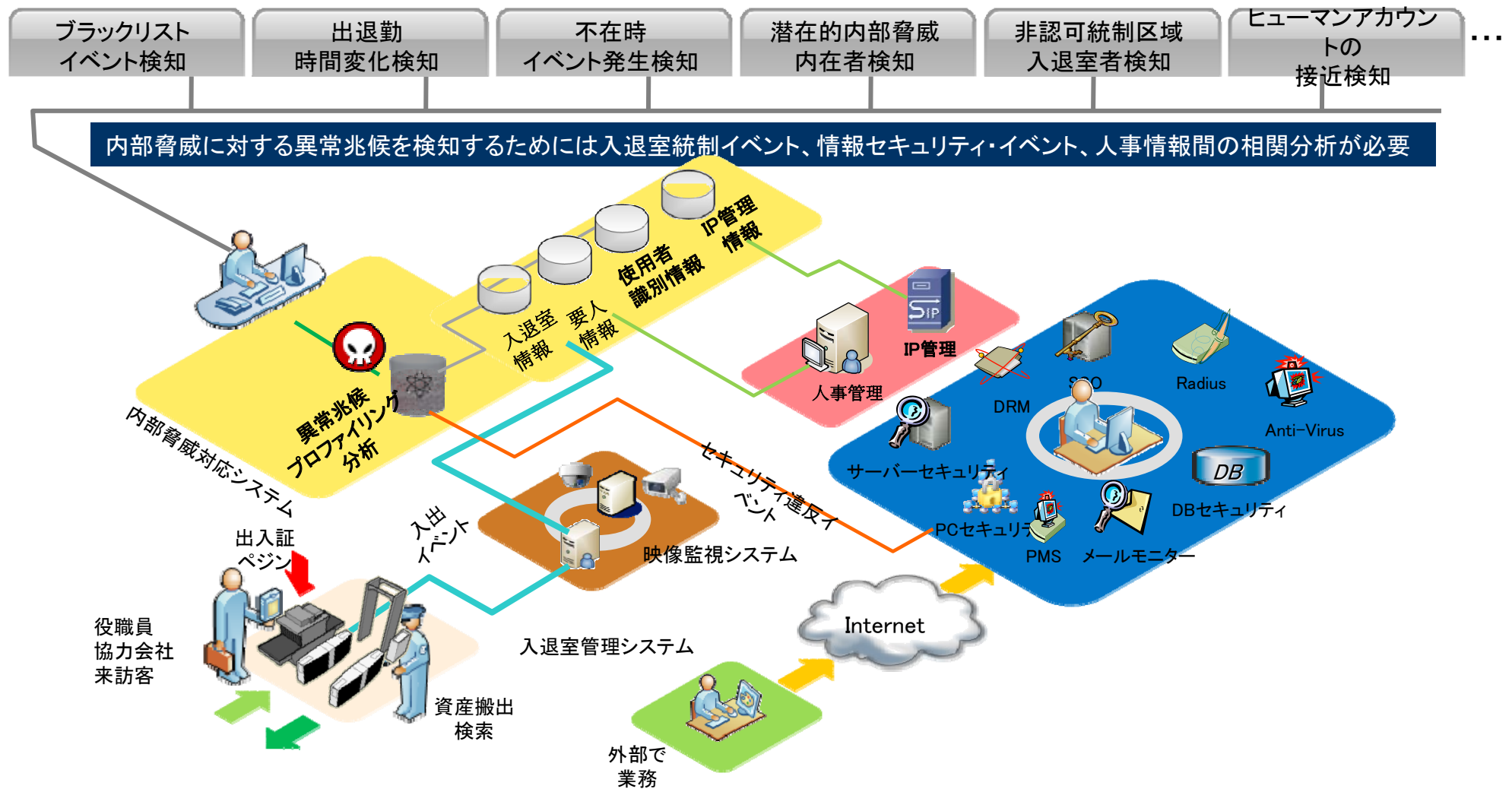
- ・ 位置識別時に特定国家、住所、建物、門を識別

- ・ 接近試みの承認または失敗の可否のログ記録

- ・ 誰かが自分が違う場所にいるかのように見せかけようと試みたのか、適切に糾明

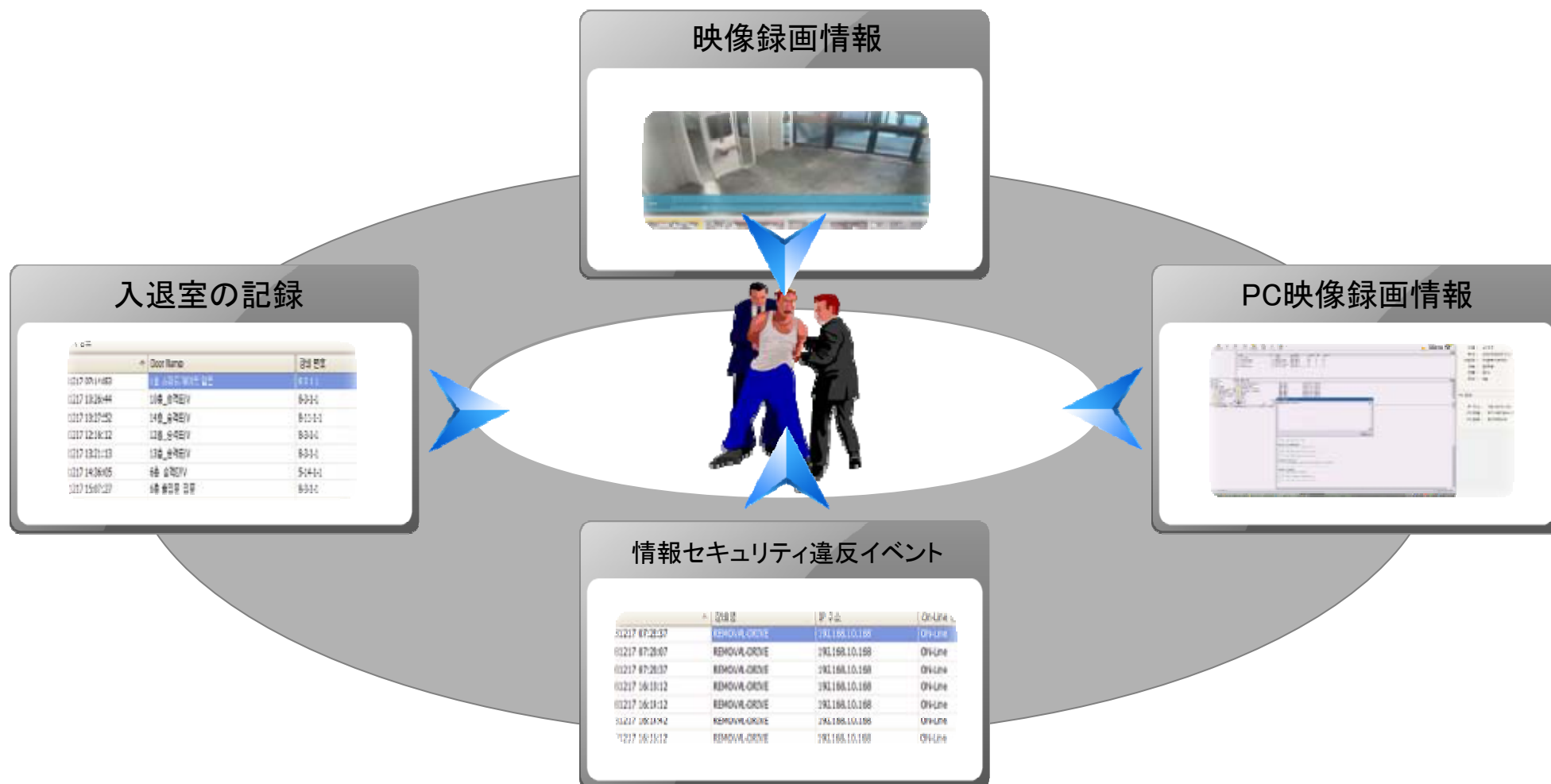
★特許獲得:単一使用者識別を通した改良化されたセキュリティ監視システム及びその方法(2009年)

融合セキュリティ管理・監視システム [内部情報流出監視]



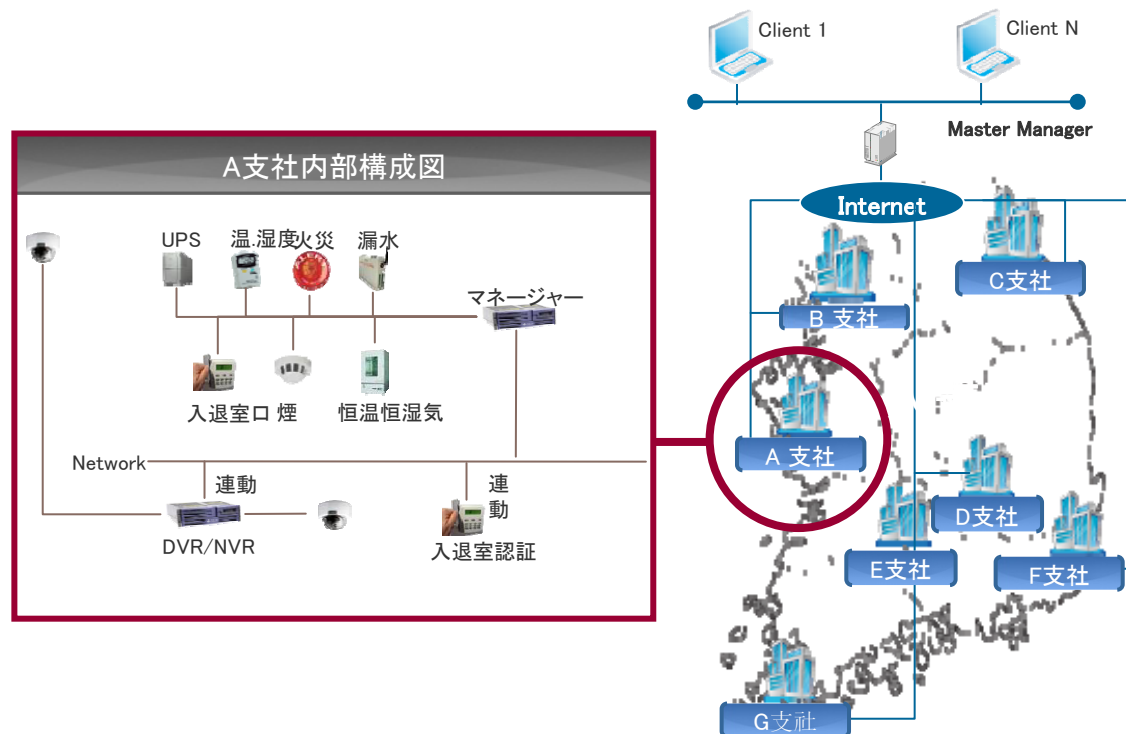
融合セキュリティ管理・監視システム [内部情報流出監視]

・内部脅威に対する監査体系の構築



融合セキュリティ管理・監視システム（施設監視）

- 映像監視及び火災発生監視、侵入監視を効果的に遂行できるよう運営者中心の統合監視画面を構成して迅速で正確な状況対応ができるシステム



主要機能

- 施設周辺と内部のCCTV及び施設管理センサーの位置をマッピングし、3D画面でモニタリング
- イベント発生時施設センサー及びCCTV位置、発生時間、場所をモニター画面に表示し、警報を出す。警光灯作動とスピーカーを通して自動的に状況伝播
- E-MAP上にCCTV監視範囲及び巡回査察経路の表示
- 建物周辺及び内部断面図の管理(生成、修正、削除、複写)機能



期待効果

- 現場映像及び装備位置情報などを立体的な3D画面で構成して、各種イベント状況を迅速で直観的に表示することによって監視運営の便宜性が向上
- 一元化されたセキュリティ統合(物理セキュリティ、施設管理)運営を通してのセキュリティ事故の発生頻度が減少
- 物理セキュリティ、施設管理を統合監視することでセキュリティ要員コストの節減

融合セキュリティ管理・監視システムの適用分野

電力,エネルギーなど基盤施設の総合監視

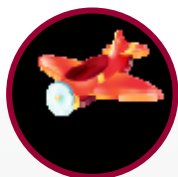


融合セキュリティ管理・監視システムの適用分野

主要施設(ダム、橋梁、堤防など)総合監視



河川堤防



空港



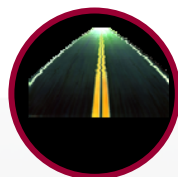
鉄道橋量



鉄道斜面



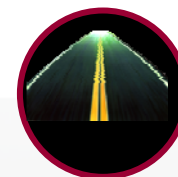
鉄道トンネル



道路橋梁



道路斜面



道路トンネル

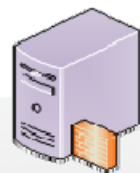


地下鉄

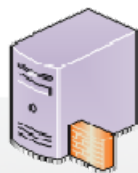
安全監視センサー・イメージ映像



Raw Data



河川堤防
施設管理



鉄道
施設管理



道路
施設管理



空港
施設管理

安全管理ネットワーク統合運営システム

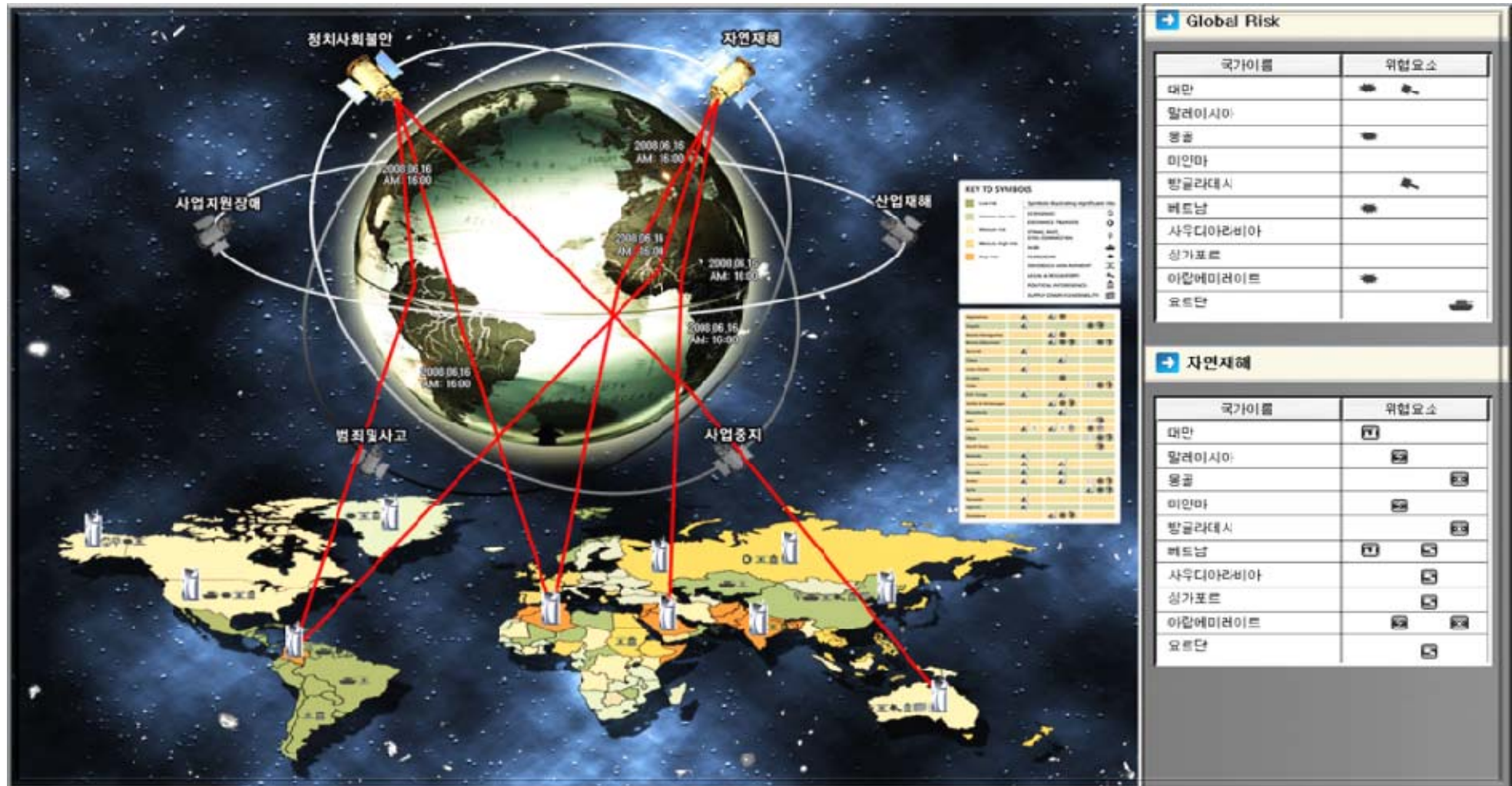
- 分析データ
- 映像データ
- 異常兆候検知データ



災害対応シナリオ システム

融合セキュリティ管理・監視システムの適用分野

Global事業場環境の大規模企業





ありがとうございました。



崔 正濬 (チェ ジョンジュン)
株式会社イグルーセキュリティ日本支社
Email: jjchoi@igloosec.com
Phone: 03-3459-6323 , 080-3080-5469