2017年6月20日

日本マイクロソフト株式会社
パナソニック株式会社

センシング技術とクラウド技術の融合で安心・安全な社会を目指す

日本マイクロソフトとパナソニック、パブリックセーフティ分野のシステム構築で協業開始

日本マイクロソフト株式会社（本社：東京都港区、代表取締役 社長：平野 拓也、以下：日本マイクロソフト）とパナソニック株式会社（本社：大阪府門真市、代表取締役 社長：津賀 一宏、以下：パナソニック）は、このほど、安心・安全な社会を目指し、両社が保有するセンシング技術とクラウド技術を融合したパブリックセーフティ分野でのシステム構築に向けた協業を開始しました。

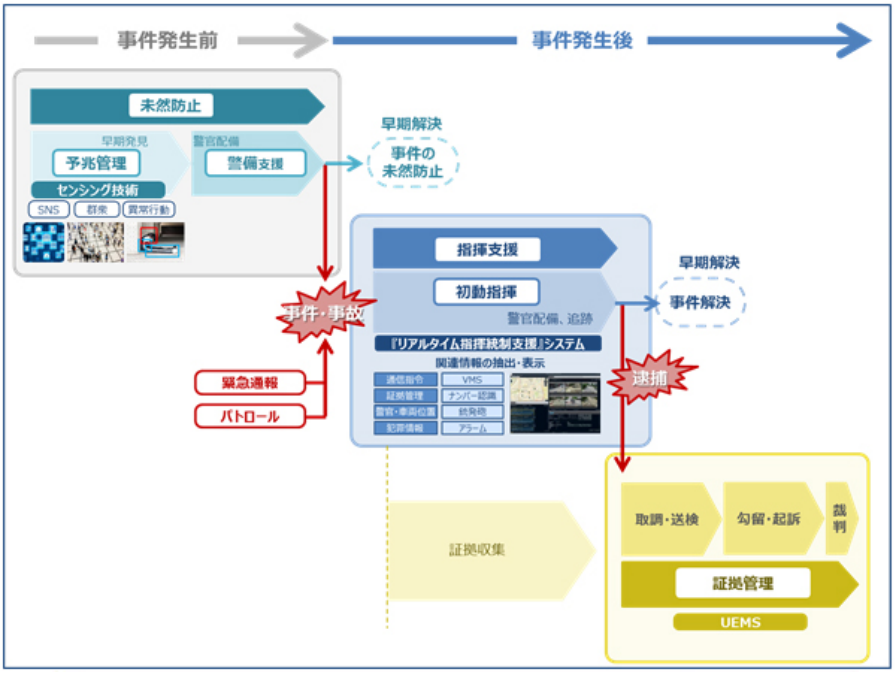
国内外で多様化する安全保障上のリスクの高まりや事件・事故の多様化に対して、ITを活用した防犯・治安への取り組みが進んでいます。それに伴い、防犯カメラ映像や事件・事故などのデジタルデータが飛躍的に増加する中、それらのデータをさらに有効活用し、犯罪捜査やテロ・犯罪の未然防止等に役立てる、より高度なソリューションが求められています。

そこで、日本マイクロソフトとパナソニックは、世界の主要都市の警察機関などで実績のある関連情報を抽出表示し警察官や保安担当者の意思判断スピードを向上させるマイクロソフトの『リアルタイム指揮統制支援』システム（※1）と、パナソニックが北米の警察で急拡大を目指すウエアラブルカメラ映像などの『証拠管理』システムパッケージ「UEMS(Unified Evidence Management System)」（※2）を、海外での経験を生かして日本国内向けに、マイクロソフトのクラウドプラットフォーム「Microsoft Azure（以下：Azure）」上で連携させます。
加えて、パナソニックの画像・音声認識などのIoTセンシング技術を融合することで、異常事態発生の『予兆』を検知『予兆管理』から『指揮支援』『証拠管理』にわたる統合システムを開発し、事件・事故の未然防止と早期解決につなげます。
具体的には、群衆の異常行動などを検知すると、関連地域の地図やリアルタイムのカメラ映像、過去事件情報などを一元的に活用して、警察官を現場へ速やかに配置させることで、事件の未然防止につなげることが可能になります。

本システムは、異常、危険の予知検出から、事故の未然防止、そして現場での指揮支援、証拠管理が必要となる駅や空港などの公共エリア全般で役立つものと考えています。
日本マイクロソフトとパナソニックは、パブリックセーフティ分野で連携し、営業活動やイベントを通して、本システムの導入を推進し、2020年に向けて、日本の安心安全な街づくりの実現に貢献していきます。

＜補足資料＞

【実現するシステムイメージ】



【システム技術の概要と特長】

※1『リアルタイム指揮統制支援』システム（日本マイクロソフト）
『リアルタイム指揮統制支援』システムは、センサーおよびシステムからのリアルタイム脅威情報管理、既存のデータベースのデータの関連付け検索、VMSやGISとの統合したマイクロソフトの複数の製品、技術を組み合わせて構築されるシステムです。
2013年から、マイクロソフトは世界中の多数の行政機関と提携して、それぞれの機関のIT環境に沿った本システムを開発導入してきました。警察機関の保有するシステムなどの既存システム、データソース、および市中に配備されたセンサーからのアラートや監視カメラ画像管理システムと連携して動作します。各種センサーなどの通知を統合し、捜査のためにデータベースを人物や場所、時間などを軸に統合検索ができるシステムです。これにより警察官や保安担当者は迅速な意思決定をできるようになります。

※2 証拠管理システム「UEMS(Unified Evidence Management System)」（パナソニック）
パナソニックが開発した証拠管理システム「UEMS(Unified Evidence Management System)」は、オンプレミスのWindowsサーバ、もしくはMicrosoft Azure上で動作するシステムで、データの格納、再生、公開、エクスポート、グループ化といったデータ操作、これらのデータ

を扱うユーザー管理、接続される機器の管理を行うことが可能な司法警察業界向けコンテンツマネジメントシステムです。
警察が犯罪捜査にあたって証拠として扱うさまざまな映像・音声・テキストといったデジタルデータは、高いセキュリティ性をもって管理される必要があるとともに、管理にあたってはそのデータの「完全性」すなわち取得された以降で改ざんや不整合が生じていないことを保証する必要があります。パナソニックのUEMSは、証拠となるデジタルデータを、それぞれの属性を示す情報（メタ情報）とともに、データ自身のライフサイクル（事件発生から立件・裁判・結審まで）に沿って、システム内に取り込んだ時から、常に改ざん検知機能を働かせることで、その完全性を担保するとともに、データが紐づけられた事件の種別によって必要な保存期間を自動的に設定し、不要となったデータは速やかにアクセス不可とするなど、安全性・秘匿性にも配慮した機能を備えています。

※3 IoTセンシング技術（パナソニック）
センシング情報を安全に効率よく収集し、顔認証、異常行動等の高度な分析を可能にする主要技術です。

（1）ディープラーニング技術
画像、音声認識等で、システムそのものがデータの特徴を学習し、より確実な分析精度で特徴の識別・判別・推測を行います。パナソニックではアルゴリズム自身の最適化と強化で総合性能向上を実施しています。顔照合技術は機械学習機能と誤りを抑制する類似度計算手法を組み合わせた独自アルゴリズムで、米国国立標準技術研究所（NIST）が公開しているベンチマークデータセットにおいて、世界最高水準の性能を実現し、人間の目でも顔の判別が困難な左右90度近い向き、照明の明暗が強い環境、サングラス・マスクなどの一部顔が隠れているような状態でも顔照合を行うことができます。

（2）エッジコンピューティング技術
センシングデータをIoT機器で分散処理し伝送経路上の負荷低減を図る技術です。ビッグデータや映像情報のリアルタイム性と情報分析要求の高まりで通信経路のデータ量が増加し帯域整備が追い付かない状況になりつつあります。特に情報量が大きな画像、音声のディープラーニング処理では、それに適したプロセッサをIoT機器（エッジ）側に配置し、伝送する情報をメタデータと呼ばれる属性情報に絞り込むことで、ネットワーク上の負荷を大幅に低減し、必要な情報だけを素早く効率的に伝送することが可能になります。

（3）IoT暗号セキュリティ技術
パナソニックはインターネットに繋がれるIoT機器を、不正侵入、改ざん、なりすまし等、サイバー攻撃のリスクから守るため、パソコン並みのセキュリティレベルをIoT機器のプロセッサー性能でも実現する暗号・認証モジュールをソフトウエアで実現し、セキュリティカメラや決済端末などIoT機器への実装実績を積み重ねてきました。この方式は秘密鍵が外部に漏洩するリスクがなく、改ざんが著しく困難で、証拠性が非常に高い安全な運用を実現します。また、この暗号モジュールは、暗号アルゴリズムが正しく実装され、暗号鍵、ID、パスワード等の重要情報の安全性が確保されていることを保証する米国第三者認証制度であるFIPS CMVP認証を取得しています。

（商標について）

以上