

提案団体名：丸紅エアロスペース株式会社

○提案内容

(1) 自社の保有するスマートシティの実現に資する技術と実績等 ※スマートシティの実現に資する技術については、別紙3の(1)～(7)の技術分野への対応を記載ください	
技術の概要・実績等	技術の分野
<p>概要： ネットに接続できる都市のあらゆる既存アセット(機材・インフラ・人員)を連結させ各アセットの運用効果を高め、都市の様々な課題に対処するクラウド上のプラットフォーム。</p> <p>特徴： イスラエル企業(Octopus社)による本プラットフォームには顔認証システム(AnyVision社)、映像分析システム(Agent VI社)他、AIや機械学習といったイスラエルの最先端技術が組み込まれており、各種ISO、EU一般データ保護規則(GDPR)に準拠しています。</p> <p>実績： ペタフ・ティクヴァ市、キリアット・ビアリク市(イスラエル)、シンガポールの各スマートシティプロジェクト</p> <p>事例： シンガポールのスマートシティ指定地区における各種施設(病院、スポーツ施設、大学、オフィス、住宅)で使用。更には交通管理や都市インフラの監視、セキュリティ要員や特定の車両の位置情報の管理を行っています。</p>	4) データプラットフォーム
(2) (1)の技術を用いて解決する都市・地域の課題のイメージ ※課題については、別紙3の(ア)～(シ)の課題分野への対応を記載ください	
解決する課題のイメージ	課題の分類
<p>【A: 組織パフォーマンスの可視化とモニタリング】 本プラットフォームに連結した都市アセットから得られる情報を分析・相関させ、組織のパフォーマンス(業務遂行、安全管理、法令順守等)をリアルタイムに可視化。組織の責任者は組織の現状をリアルタイムに監視し、低下しているパフォーマンス領域の改善に注力することができます。</p> <p>【B: サイバー情報を融合させたセキュリティ】 インシデント発生に対し、サイバーセキュリティから事案が事実か虚偽か判断した上で、予めカスタマイズできるアルゴリズムに基づき、プラットフォームに連結した既存のセキュリティ機材を連動させて対処します。</p> <p>例) ビルの火災報知器が作動→サイバー攻撃による誤作動かミリ秒内で判断→真実であれば付近の監視カメラを起動し画像を消防本部へ送信→ビル内に警報、防火扉を閉じ延焼防止、消防隊派遣など予め設定している対処手順を自動で展開</p> <p>イスラエルのペタフ・ティクヴァ市では導入初年度に指令センター運営費25%削減、インシデント応答時間40%短縮、セキュリティ事案発生15%削減を達成。</p> <p>【C: 都市のインフラの効率的運用】 都市のあらゆるインフラを連結させ得られるデータを分析、相関させコスト効率を向上させます。</p> <p>例) 水道の配管システム、水道メーター等の関連インフラをプラットフォーム上で統合。得られるデータから、エネルギー消費の削減、予測保守による故障回避や、給水の問題発生時には噴水停止といったインフラ管理の最適化。</p> <p>【D: 交通データを分析し、都市交通の全体最適化】 公共、民間の交通データ、カメラによる交通量の監視、渋滞や事故情報などを相関させ、信号機の切り替え等により都市交通を全体最適化させます。</p> <p>【E: インフラや機材だけでなく人もセグメントに応じて都市機能と結びつけるポータルスマートフォンアプリ】 例) 市民セグメント: ・従来の市役所等の窓口業務をアプリで集約し市民に公的サービスを提供 ・市民へのコミュニケーションチャンネルとして情報提供(例: 交通情報、不審者等の安全情報を付近の人だけに通知) ・アプリに登録した市民の希望や経歴に応じてボランティア呼びかけ</p> <p>例) セキュリティ要員セグメント: ・センシティブ情報の提供。マップ上での全要員の配置の可視化やパトロールルートの指示などで偏りのないセキュリティ体制。実行すべきタスク指示、スマートフォンカメラを使った状況報告など“要員のセンサー化と最適化”</p>	【A】 シ) その他 【B】 ウ) 防災 ケ) セキュリティ 【C】 イ) エネルギー エ) インフラ維持管理 【D】 ア) 交通モビリティ 【E】 シ) その他

(3) その他

まとめ： 行政と技術を融合するプラットフォーム。都市のアセット（機材・インフラ・人）から得られるデータを関連付けて都市の課題を可視化し政策に反映。本システムの下で連動する都市アセットに政策とデータをフィードバックし最適化。

○部局名・担当者・連絡先（電話及びメール）

部局名	担当者	連絡先（電話）	連絡先（メール）
丸紅エアロスペース株式会社	小俣 基幸	03-5157-7508	Omata-M@asp.marubeni.co.jp



OCTOPUS

City Wise

スマートシティ・マネジメント



オクトパス・システムズ社 – 会社概要

物理およびサイバーセキュリティ技術の豊富な経験を持つ
セキュリティ専門家と技術者によるソフトウェア会社

- Octopus Systems LTD. - 2011年設立
- Octopus North American - 2016年カナダにて会社登記
- イスラエルとカナダの国際投資家によるバックアップ
- 優れた物理的セキュリティ方法論とサイバーセキュリティ技術を誇る
- ISO規格– ISO9001, ISO9003, 情報セキュリティISO27001, ITサービスISO20000
- 登録済みデータコントローラ
- 製品の受賞歴– フロスト&サリバン賞2016 –緊急時インフラ向けグローバル・コマンド&コントロール新製品イノベーション賞
- 特許出願中の統合アルゴリズム
- インストールはOctopus社または世界中のインテグレーション・パートナーによって実施
- 多くの重要なインフラ、企業、地方自治体におけるプロジェクトへの導入実績

課題

今日の都市には対処しなければならないタスクにあふれています

- 増え続ける都市のインフラとアセットの管理
- 数多くの部門にまたがる調整
- 多様な技術の管理と生み出される膨大なデータ
- 様々な種類の課題への対処
- 住民へ提供する高いレベルの公的サービス
- 犯罪、テロ、サイバー攻撃、異常気象、システム障害などの対応

- 高い運用コスト
- 個別対応で統合的な管理が難しい
- データ分析および相互参照がない
- 住民の関与なし
- 将来的には使えなくなる

タスク実行の遅延、住民とのコミュニケーション低下、都市のアセットの管理が非効率かつ高コスト化



OCTOPUS
control and command

OCTOPUSのソリューション



- 都市管理の費用対効果を向上。高度な分析機能によって都市のアセットを管理し、包括的に都市を運営するスマートシティ・ソリューション
- 公共設備でのエネルギー消費を削減し、コストを低減
- あらゆる都市システムにコマンドを送受信できるツール
- 様々な種類のセンサーとプロトコルをサポート
- 専用のモバイルアプリを通じた住民と行政のコミュニケーション

OCTOPUS CITY WISEの概要



開発目的: 都市のスマート化、安全上の監視、インフラ管理、住民とのコミュニケーション、インシデント時の要員の緊急派遣

クラウド上の指令センター機能: インシデント情報、データやビデオ、オープンソースインテリジェンス(OSINT)を集積

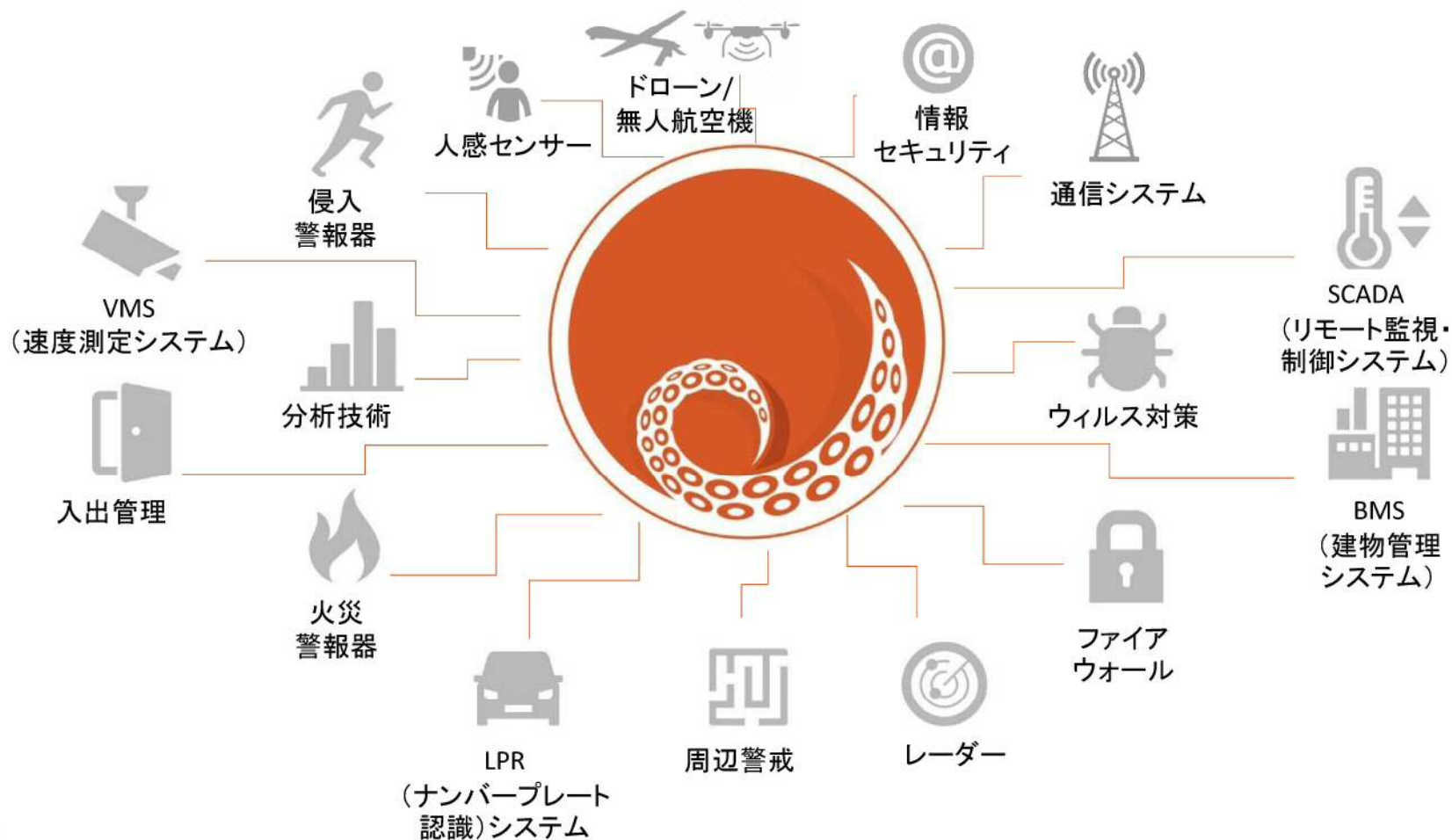
モバイルアプリによる住民と自治体の双方向コミュニケーション:

- 自治体→住民: 危険情報、自治体の取り組みや文化活動の通知
- 住民→自治体: 自治体サービスへのモバイルアクセス、発見したインシデントの報告や改善の提言

包括的な情報提供: 輸送、緊急サービス、地図、関心地点が一望できるモバイルアプリ

ルーチン管理: パトロール、メンテナンス、インフラやシステム管理、運用リスク管理などのルーチン業務を管理

安全に係る様々なアセットがOctopusの下で連携



脅威に対するインテリジェンスとの連携

- オープンソースインテリジェンス(OSINT)と連携
 - 犯罪情報
 - 情報源
 - ソーシャルメディア
 - 気象システム
 - 車両記録および登録
 - 背景とスクリーニングシステム
- インシデント発生時に周辺情報を関連付けて分析
- インテリジェンス、脅威、リスクの分析と管理が可能
- モバイルアプリ、SMS、電子メール(一斉通知)を通じて、インシデント関連情報を保安部隊、自治体職員、住民に提供



インシデント管理

相関: データ、イベント、アラームを分析・相関させ、実際の状況把握と優先順位付け

検証: 関連する情報を一つの図に集約し、状況を可視化

移動性: 当局者はモバイル機器によってインシデントをどこにいても管理可能



自治体の規則に準じた日常と危機への対処

- 自治体の政策や規制等に基づく、日常の運営や緊急事態対処の際の標準運用手順(SOP)を提供
- 都市の保守、安全に関する最適な手法を提供
- 事業継続とワークフロープロセスの自動化が導入可能



情報収集

様々なセキュリティ機材やシステムからのデータを自動的に集約



優先順位付け

インシデントの優先順位を決定するためにデータを分析して関連付け



管理と対処

セキュリティの全体像を俯瞰的に表示
事前設定された手順を自動で発動



応答

ユーザーの携帯電話を活用して迅速な対応(自治体のルールに準拠)



報告

コンプライアンス報告と後のトレーニングのために対処完了した事案を記録

日常のパトロールルートの作成

○ 車両

- システムは車両と事案発生時の現場への到着時間などの基準に基づいてパトロールルートを自動的に生成します。
- 予測される事を防ぐためルートは定期的に変更されます。
- 指令センターは車両位置を把握し、ルートから外れたり長時間の停車があると通知を受ける事ができます。

○ 要員

- セキュリティ要員は、モバイルアプリから位置情報に基づく、警戒場所のバーコードを受け取ります。
- 要員は警戒場所で実行するタスクを受け取り、実行後に結果を報告することができます。
- 要員が警戒場所を順番に、または時間通りに訪れない場合、指令センターから通知を受けます。

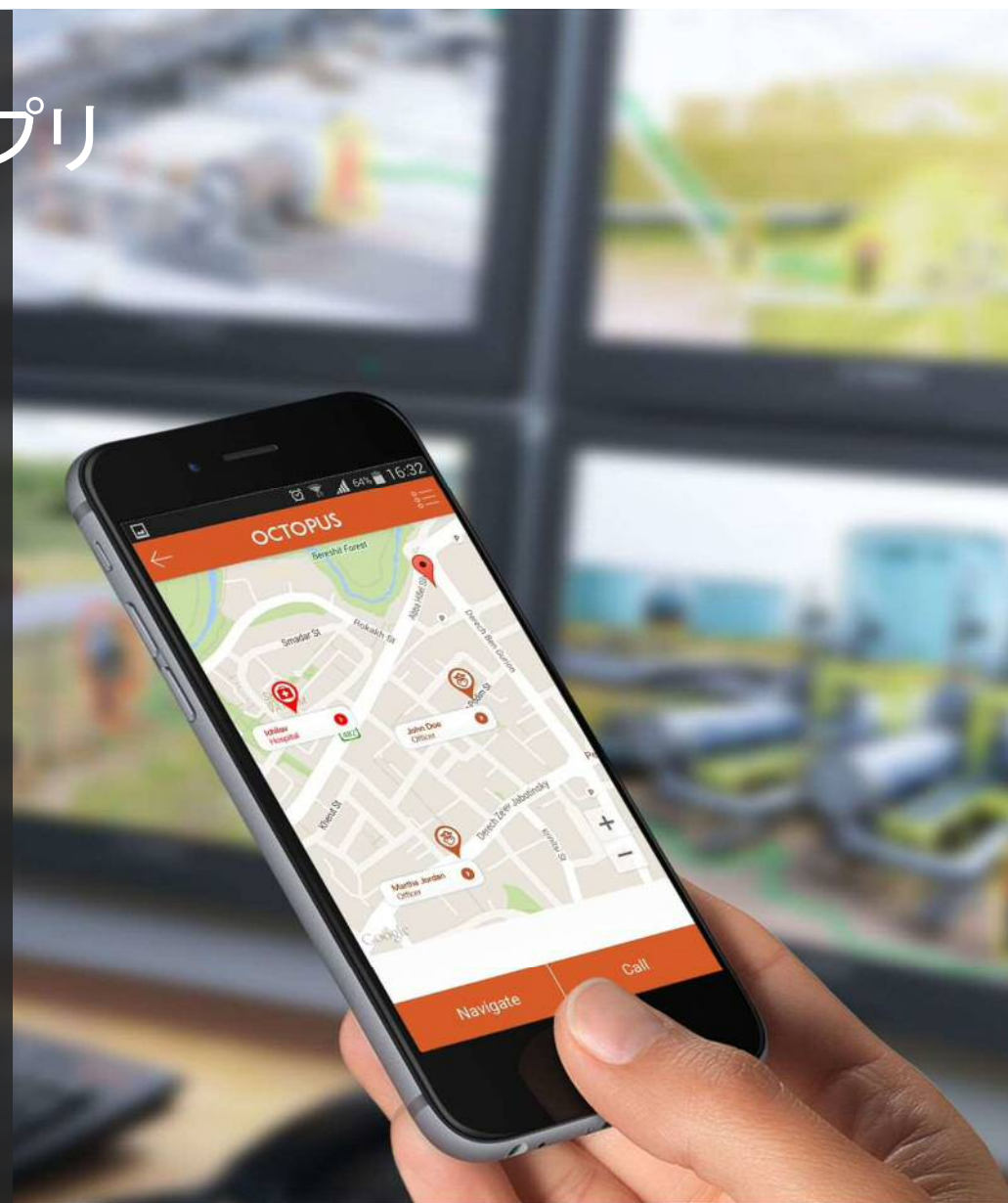
The image shows a map application interface with a legend panel on the right side. The legend panel is titled "Legend" and contains several categories with their respective counts:

- Cameras (9)
- Facilities (16)
- Alarms (181)
- Incident
- Guards (0)
- Scan points
- Cameras group
- Crime map
- Virtual fence (24)

The map in the background shows a city area with various streets and landmarks, including Norwalk, Yorba Linda, and Huntington Beach. A search bar and navigation controls are visible in the top right corner of the map.

自治体当局者向けモバイルアプリ

- アプリから全てのセキュリティ状況を確認
- 緊急時に即座に対応チームを派遣
- セキュリティ要員の管理 - インシデント、タスク、状況報告の双方向通信
- アプリから緊急通知を発信
- セキュリティ要員を不審者・物の情報・映像をアプリから本部に送信する“セキュリティ・センサー”化
- 現場状況と点検結果をアプリから報告
- 警備やパトロールのルートを最適化し要員に指示



重要拠点の警備

状況把握:

地上レーダー、電気フェンス、分析システム、その他のシステムからターゲット(不審者など)を把握

- ターゲットの方位と距離をリアルタイムに表示
- レーダーで検出したターゲットを連動するカメラでリアルタイムに撮影、追跡
- 昼夜兼用カメラの解析、熱カメラ、音響センサーなどからターゲットを探知
- 複数の監視プラットフォーム(ドローン、UAV、PTSD風船など)の画像を表示

状況分析:

収集した全てのデータを分析し、相関させ、効率的なインシデント管理を行い、対応の優先順位付けを支援

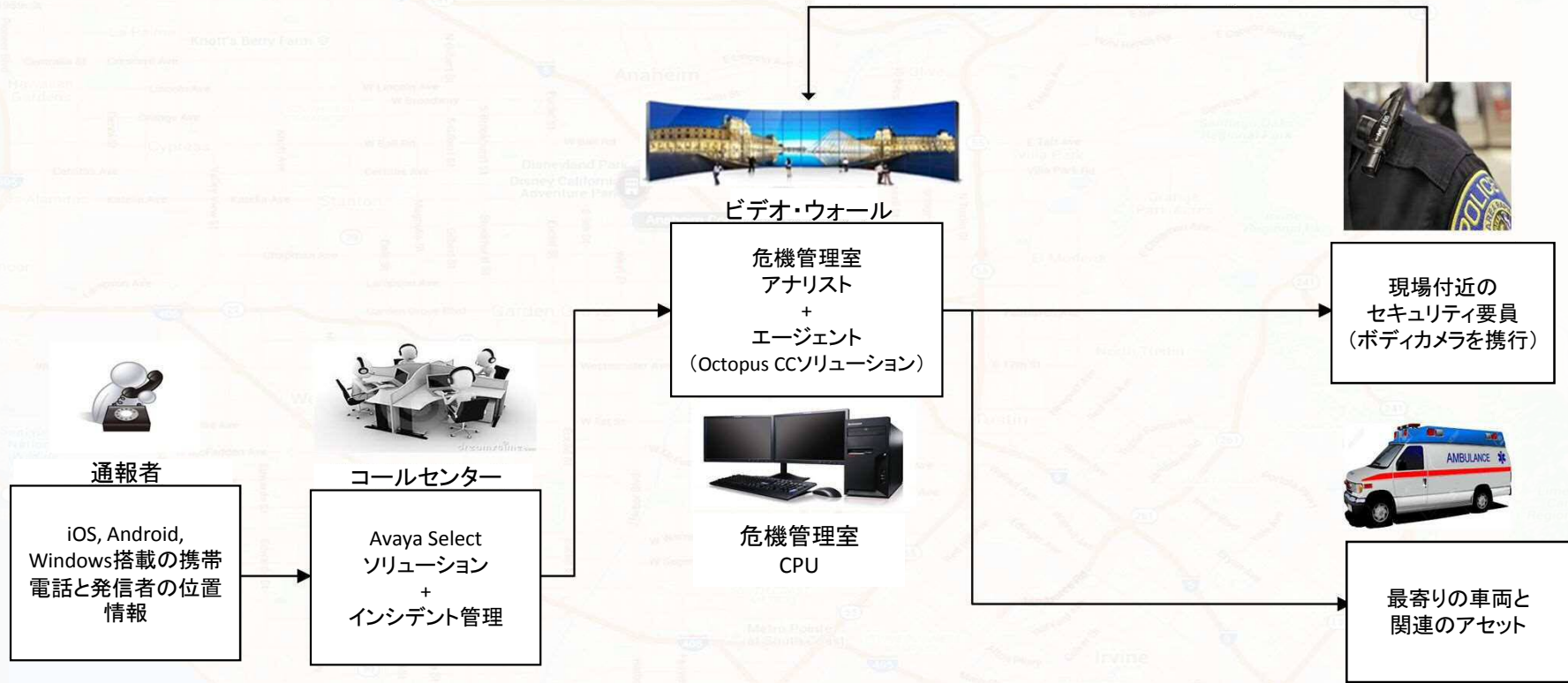
The screenshot displays a security monitoring interface. At the top, there is a navigation bar with icons for 'Full screen', 'Create new incident', 'Ask for guards location', 'Send alarm', 'Send an audio message', 'Pending requests', 'Compose', and 'Phone book'. Below this is a header for 'Open incidents' with a status summary: 135 Critical, 53 High, 17 Medium, 17 Normal, 9 Low. A 'Recently viewed' section and a 'Sort by: Severity' dropdown are also present.

The main area is a grid of incident reports. Each report includes an ID, a status icon (a red circle with a white target), a title, a timestamp, a source, and a responsible party. For example, incident 2049101 is a 'Panic button' triggered on 20/04/2016 at 10:25, sourced from 'Ilya Dembinsky', and assigned to the 'Organization Administrator'. Other incidents follow a similar pattern with different timestamps and sources.

Below the incident list is a satellite map of an area. A large purple semi-transparent area is overlaid on the map, labeled '地上レーダー' (Ground Radar). Several orange and black icons representing targets are scattered within this area. To the right of the map, there is a label 'ドローン 昼夜兼用カメラ 熱カメラ' (Drone Day/Night Camera Thermal Camera). At the bottom of the interface, there are four small video feeds: the first shows a wide outdoor scene with a timestamp '6 Wed 17:10:04'; the second is a dark, low-visibility thermal or night-vision feed with red bounding boxes around figures; the third shows a person climbing a fence; the fourth is a thermal image showing several figures in a dark environment.

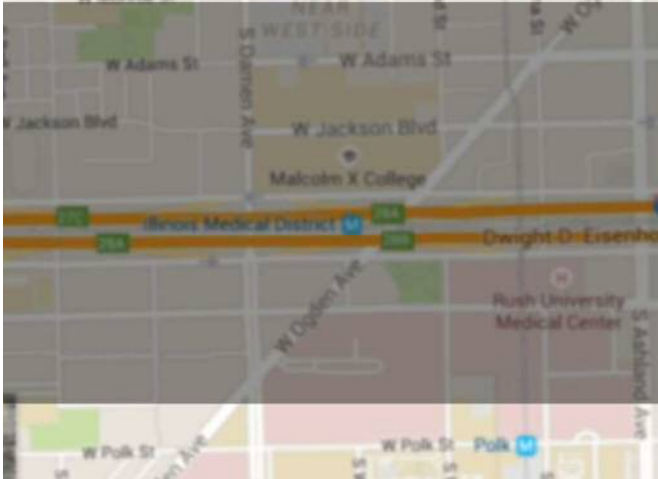
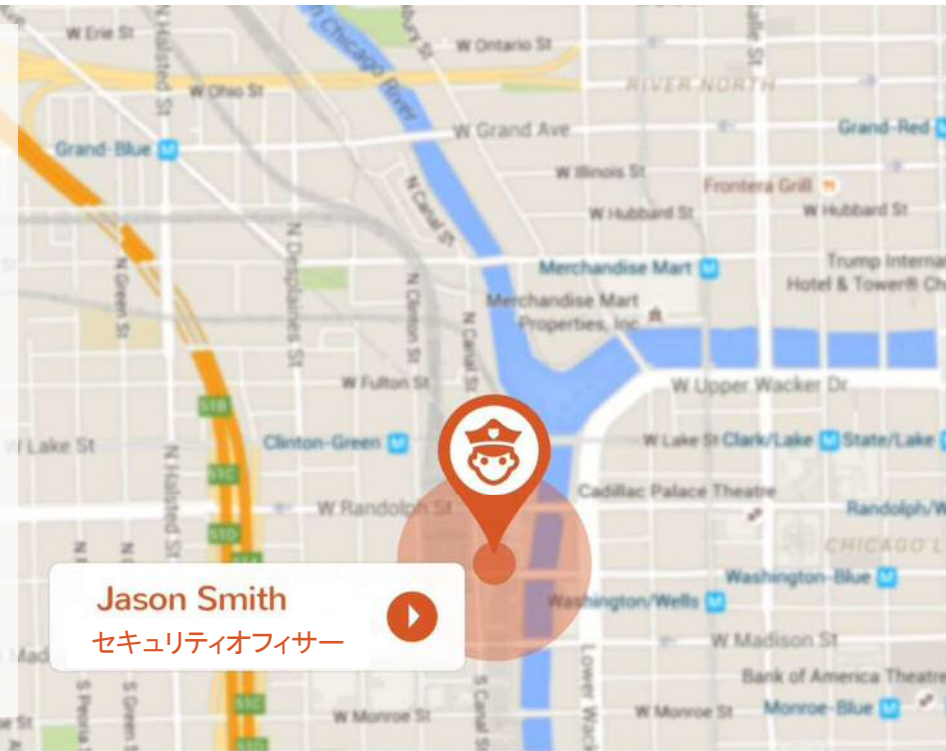
Octopus緊急コールセンター

セキュリティ要員がモバイル機器で応答



緊急派遣 (CAD)

- インシデントに最も近い緊急対応チームを手動または自動で派遣します。
- 対応要員は即座にインシデント概要の報告を受けとります。
 - インシデントの詳細
 - 写真と場所
 - ナビゲーション指示
- 指令センターはマップ上で緊急対応者の位置を追うことができます。
- カメラの映像は緊急対応者の位置情報に従って自動的にポップアップ表示されます



緊急時のコミュニケーションの一元化

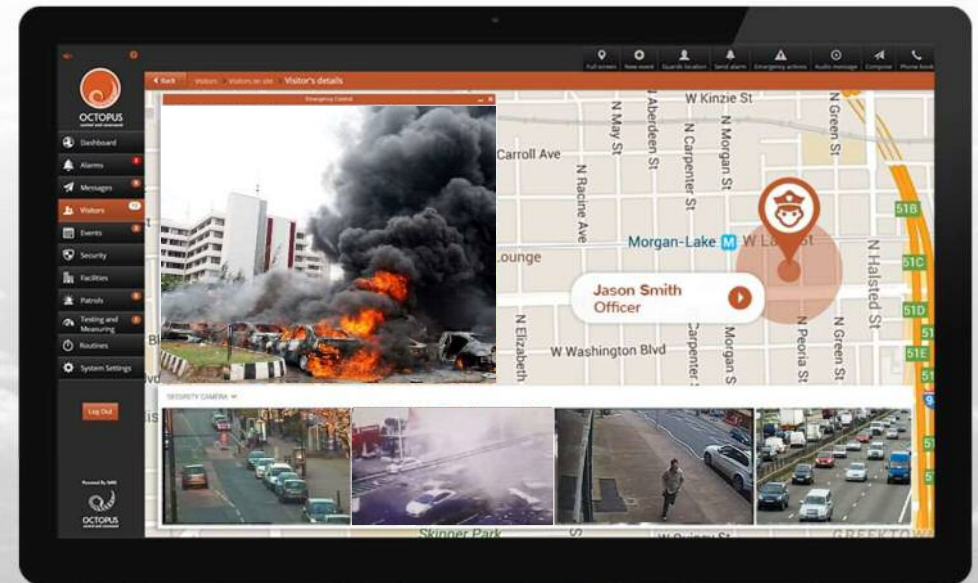
公的機関の緊急 連絡と一斉通知:

- モバイルアプリ
- PTT無線
- VoIP
- 固定電話
- 携帯電話
- 衛星
- SMS
- Eメール
- 電子メッセージボード
- 公表



シナリオ例：爆弾事案

- 1) ユーザーがモバイルアプリより指令センターに爆発の発生を報告
- 2) 報告者の位置情報から現場付近の防犯カメラ画像が指令センターに自動的に表示され、報告の真偽が確認
- 3) 予め設定された爆発物事案の対処手順が展開
- 4) 関連する潜在的な脅威の全てを把握するために、オープンソースのインテリジェンスを関連付け
- 5) システムは現場に最も近い救急隊員に急行命令
- 6) 一斉通報システムは、付近の全住民にモバイルアプリ、SMS、電子メールで避難指示
- 7) 緊急対応者はアプリから指令センターにライブビデオ送信
- 8) 緊急対応者はアプリからインシデントの対応状況報告



サイバー防衛

スマートシティでは多くのIPベースのシステムが利用され、サイバー攻撃を受けやすく業務に混乱を招く可能性があります。

- Octopus SIEM SOC : セキュリティ情報イベント管理 & セキュリティオペレーションセンター
- Octopus インフラ保護 : SCADAとIPデバイスをスキャンし、ハッキングから保護
- Octopus 電話ガーディアン : 自治体職員の携帯電話をハッキングから保護し、プロキシのホワイトリストとブラックリスト、なりすましへの対処を可能にします。
- サイバープロテクション、アンチウイルス、IT & ネットワークシステムと統合, IT & ネットワークシステム
 - ドメイン保護システム
 - ウイルス対策システムとエージェント
 - ファイアウォールとネットワークセキュリティ
 - トロイの木馬などのマルウェア攻撃からの保護
 - IT システム
- サイバーインシデント管理のための情報の関連付け
- サイバー脅威とリスクの分析と管理

スマートシティのソリューション

都市の全てのインフラとシステムを連結

- エネルギー、水
- 建物、インフラ、都市計画
- 交通機関
- 観光、レクリエーション、文化
- セーフティとセキュリティ
- 情報通信技術

連結したインフラやシステムから得られるあらゆるデータを分析し相関させて、コスト効率の良いインフラ管理を支援

110番、119番
緊急通報

電力・公共設備

ICT

セキュリティ・
安全

市民インフラ

上下水道

輸送機関
セキュリティ



新しい都市の姿

エネルギー：

- 都市の電力使用状況を分析し消費を管理

公共設備：

- 街灯の焼損時の交換指示、給水の問題発生時の噴水停止といったアクションの通知と管理

水：

- 配管システムや水道メーターなど、様々な情報源から履歴・リアルタイムデータを分析。公共・商業施設や住民からの使用の統計表示
- 予測保守による機材故障の回避、ポンプ制御によるエネルギー消費の削減などインフラの最適化
- センサーによる小～大規模の漏水を通知

下水：

- 汚水センサによる漏水、ポンプの稼働や処理状況、洪水制御システムなどを監視





新しい都市の姿

交通機関:

- 公共・民間交通データをリアルタイムに受信し分析
- カメラによる交通量の監視、特定エリアへの車両の出入り台数分析
- 交通事故、渋滞、交通違反に関するリアルタイム通知

セキュリティ:

- 公共施設、学校、企業からのアラームを受信
- 迅速な対処のため「重要拠点」を監視
- 指名手配人物や不審車両に関するリアルタイム通知を受信
- 住民からの保安上の危険と問題について通報をリアルタイムに受信

ビル管理:

- 建物や官民インフラにおける不具合通知を受信

住民サービス:

- モバイル上のポータルアプリで自治体のあらゆるサービスにアクセス

施設と安全管理

- 自治体の建物システムと統合し、自動的にデータと警報を受信
 - ゲート、ドア
 - 火災・ガス検知器
 - 電カメーター、UPS(無停電電源装置)、発電機
 - SCADA(リモート監視・制御システム)、テレメトリ、PLC(電子制御装置)
 - カメラ、セキュリティシステム
- 警報器等のセキュリティ機材の位置を示す建物のレイアウトマップ
- 避難と緊急時の計画と手順を管理。自動化されたワークフローを展開
- 施設メンテナンス、訪問者管理、およびセキュリティ構築をひとまとめに
- 人員と機材の特性を管理
- 資産管理 – 訪問者、資格、テスト、サービスレベルの管理
- 運用スタッフが実行すべきタスクを自動または手動で作成
- 状況と調査結果の報告
- 安全管理と性能監視

リスクとパフォーマンスのモニタリング

組織の状況把握:

Octopusのインテリジェンスにより組織のリスクとパフォーマンスを可視化。組織の責任者はリアルタイムに状況をモニタリング

情報収集・分析:

Octopusに連結するセキュリティ機材、サイバー、インフラおよび運用ソースからの情報を自動・手動で収集し、分析

個別設定可能な指標:

組織や拠点毎に事前に定義できるKPI(重要業績評価指数)に基づき、パフォーマンスとリスクを計算し、%で表示

詳細分析:

KPI算出の元データを掘り下げて、低いKPIの原因を調査

対処:

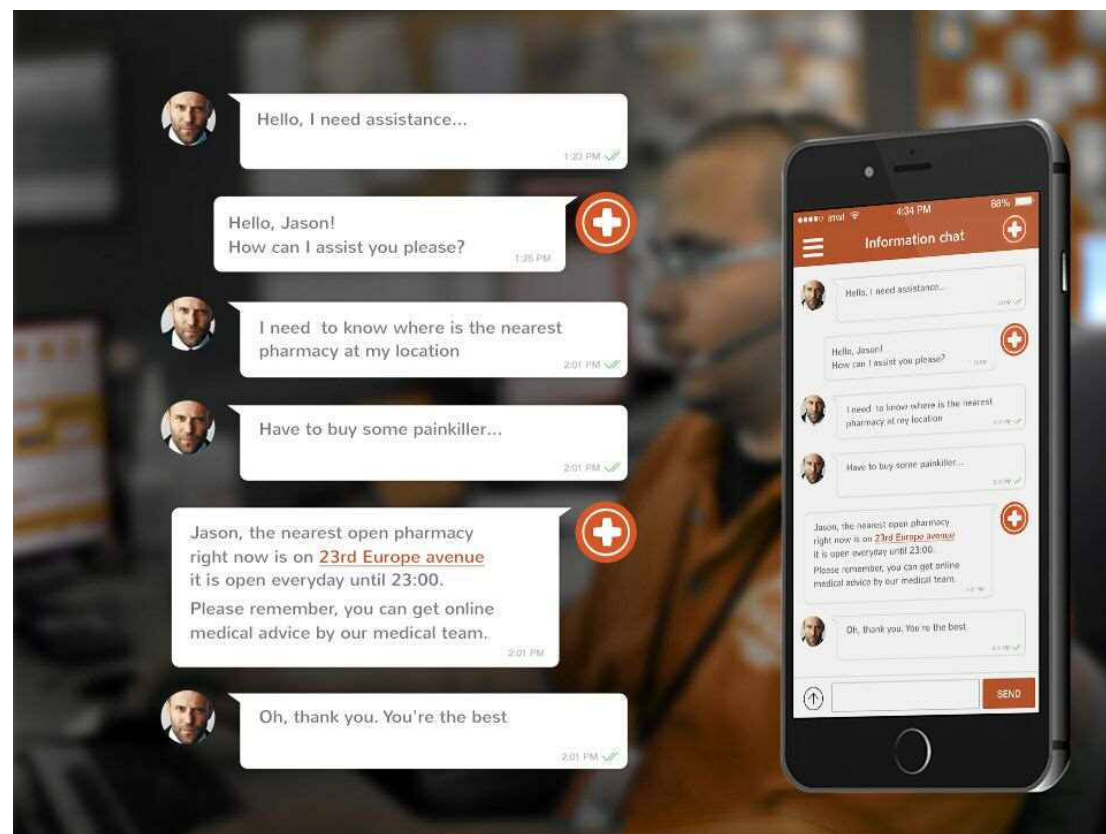
リスクのしきい値の超過時に自動で実行するアクションを設定



住民向けモバイルアプリ

モバイルアプリ：自治体と住民の双方向コミュニケーション

- 自治体の住民サービスをアプリに集約
- 住民はアプリを通じて住民サービスを楽しむ
 - 交通情報
 - 文化・観光イベント
 - グリーンプログラム
 - 健康管理
 - 地図
 - 自治体の施策
 - 支払い
 - その他
- 住民側から自治体へのコンタクト
 - 事故や危険の通報
 - 緊急電話
 - 街の改善提案
 - 街のチャットサービス利用



Octopusの構造

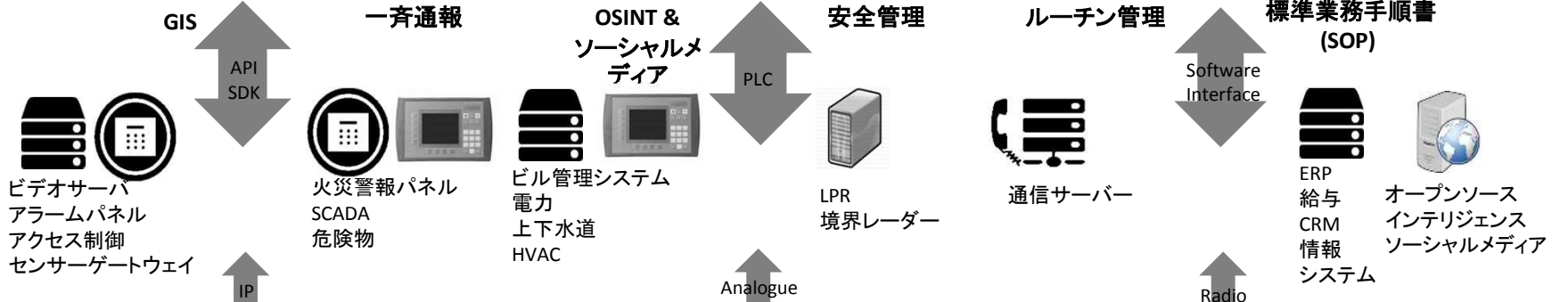
Octopus システム ユーザー



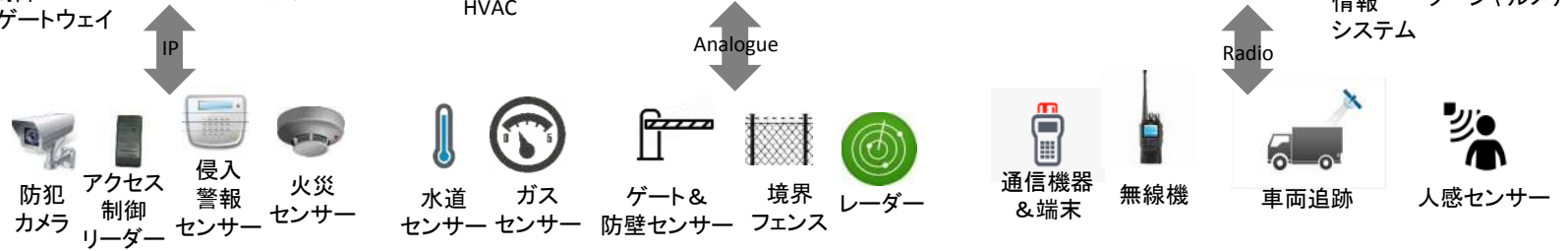
Octopus システム・コア・モジュール



統合サブシステム



外部セキュリティ 機材



セーフシティプロジェクトのケーススタディ



イスラエル
ペタフ・ティクヴァ市



Octopus City Wise
セーフ・シティ・プラットフォーム

都市の概要	機能要件	都市の目標
人口250,000人 コールセンターと指令センター有り	システムとセンサーの全てを緊急通報のインシデント対応に統合	高いレベルの住民サービスを維持しながら運用コストを削減
何千台もの防犯カメラ	全ての遠隔操作カメラを指令センターに接続	
何千台ものセンサーとデバイス	単一のプラットフォーム上で全てのオペレーションを統合	
	自治体職員と住民にモバイルアプリを提供	

Octopusプラットフォームの特性	Octopusメインモジュール	初年度に達成した効果
街の全ての防犯カメラ、アクセスコントロール、侵入警報、火災報知器を統合	クラウドベースのシステム 統合指揮統制 - ルールエンジン	指令センター運営コストを25%削減
インシデント管理手順、プロトコル、および規制管理	インシデント管理と業務手順	インシデントに対する応答時間を40%短縮
ビデオマトリックス	地理情報 モバイルアプリによる通報と要員派遣 施設管理 防犯カメラへの警察の遠隔アクセス	セキュリティ事案の発生を15%削減

OCTOPUS CITY WISEの概要と利点のまとめ

- 1. クラウドベースのソリューション:** 迅速で簡単なインストールで、単一のプラットフォームから複数の拠点を簡単・安全にコスト効率良く管理。クラウドでもオンプレミス(自社のサーバー)でも導入可能
- 2. 街の全てのニーズに答える単一プラットフォーム:** 単一のプラットフォームから、街固有のセキュリティと運用ニーズを満たす35のモジュール
- 3. 情報セキュリティソリューション:** 情報セキュリティモジュールを含む総合的なセキュリティ
- 4. スマートフォンやタブレットでの住民とのコミュニケーション:** 緊急時の一斉通報など住民とのコミュニケーションツールとなります。
- 5. 緊急時の即時対応:** 指令センターやモバイル機器から全てのセキュリティ部隊、ファーストレスポnder、緊急機関、自治体職員と迅速かつ簡単に連絡を取ります。
- 6. 公共施設のコスト削減:** エネルギー使用を最適化し、公共施設管理を自動化
- 7. セキュリティインテリジェンス:** 犯罪や行政のデータソース、オープンソースインテリジェンス、ソーシャルメディアを相関させたリアルタイムのリスク分析
- 8. ベストプラクティス:** システムが、都市の危機管理、物理&サイバーセキュリティ関連インシデントへの対処に対する最適・標準的な運用手順を提供
- 9. オープンアーキテクチャのシステム:** 主要なセキュリティ機器やインフラ関連のメーカーと連携することで、既存の設備をそのままに制御を一元化。何千ものセンサーを同時に機能させます。
- 10. 将来性:** 次世代のクラウドベースの映像システム、セキュリティシステム、サイバー防御システム、IoTとの接続
- 11. 共通運用:** 直感的で高度なユーザーインターフェイスにより、セキュリティと運用の状況を単一のプラットフォーム上でリアルタイムかつ包括的に把握し、状況認識力を強化

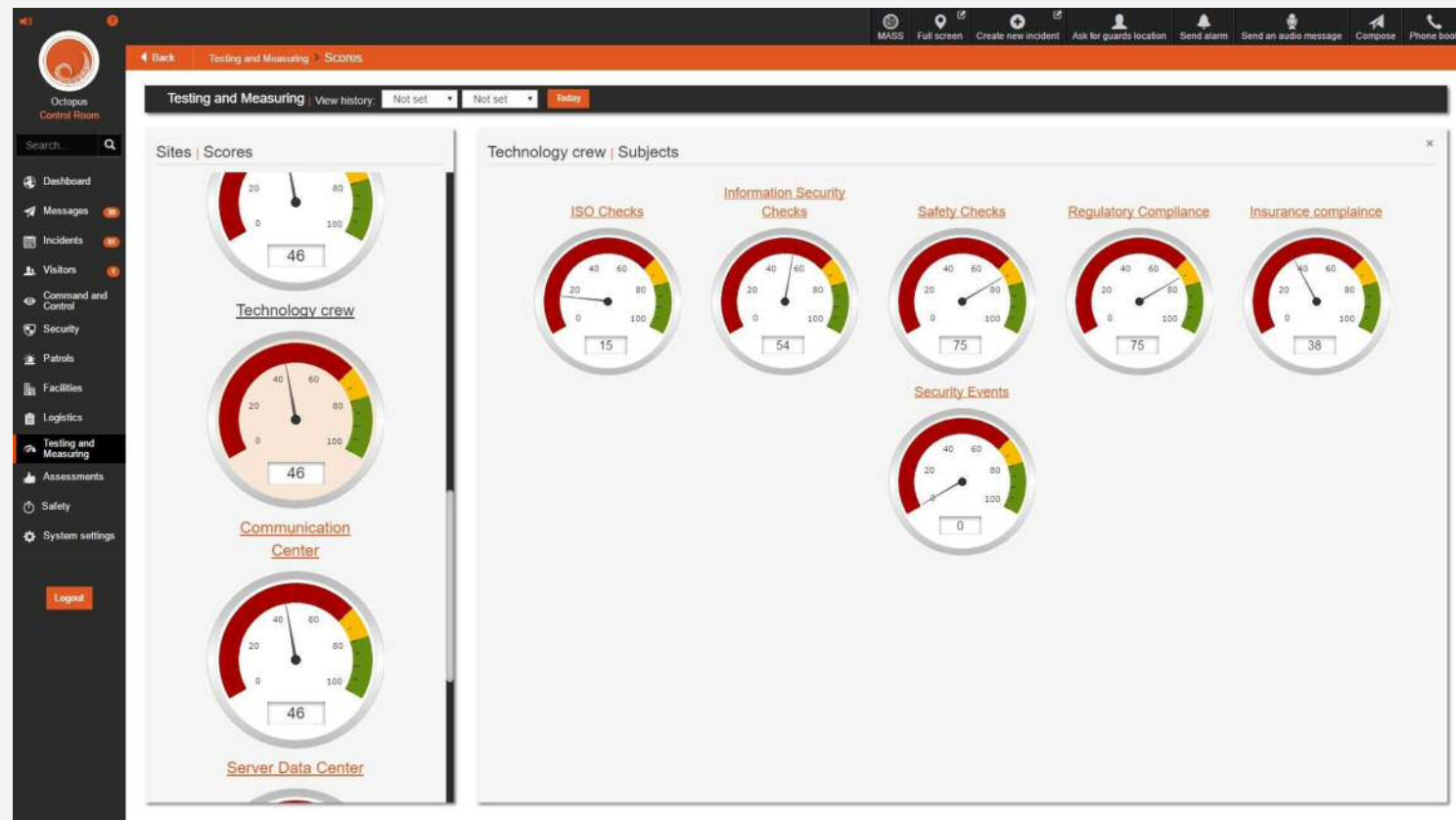


Octopus
**組織パフォーマンスの
モニタリングと評価システム**

2019年1月

Octopusパフォーマンス&モニタリングシステム

組織パフォーマンスを可視化して、リスクを監視し対処する



Octopusパフォーマンス&モニタリングシステム

組織の運営責任者の為の組織の状況把握システム

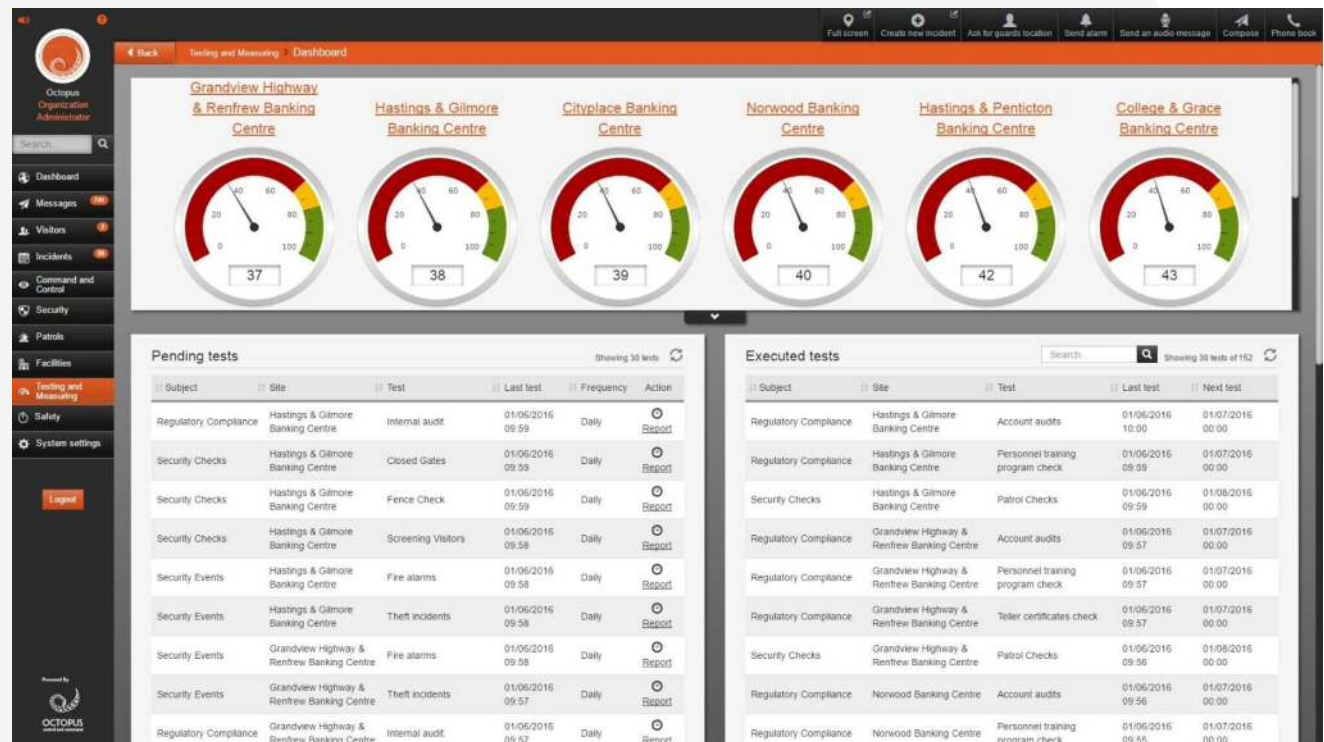
内部・外部の情報源より組織のパフォーマンスに係る情報を取得

モニタリングするパフォーマンスKPI例:

- セーフティ
- メンテナンス
- オペレーション
- セキュリティ
- 情報セキュリティ
- コンプライアンス
- ISO
- その他、組織が望む領域



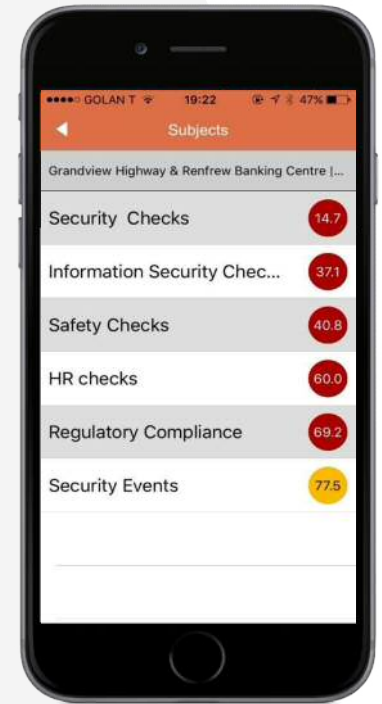
これらの状況やリスクレベルをKPI (重要業績評価指数)として監視



Octopusパフォーマンス&モニタリングシステム

主な特徴:

- **モニタリング対象KPI設定:** 定期メンテナンス、規制、ISO、安全検査、セキュリティ評価、サイバーコンプライアンス、ITとHR、従業員トレーニングと資格の認定など組織で定期的な監視が必要のあるKPIを設定します。
- **タスク管理:** 拠点や対象毎に任命されるスタッフに、モバイルアプリやウェブを通じて実行すべき検査タスクを実行すべき時期に通知します。
- **レポート管理:** スタッフが行った検査タスクの結果をモバイルアプリを介して報告することができます。
- **アクションアイテム管理:** 管理者は結果を確認し、未解決の問題は別のリストにて管理します。
- **運用可視化:** 管理者は、全ての施設の全てのパフォーマンスレベルをアプリで俯瞰的に見る事ができます。
- **演習:** 基準となるパフォーマンスレベルを明確化する為の演習を各拠点で行えます。
- **しきい値と対処手順のカスタマイズ:** 監視対象毎にパフォーマンスレベルのしきい値と、しきい値の逸脱時における対処手順の設定を行います。
- **弱点の把握:** 複数の拠点の比較や平均からパフォーマンスの低い、あるいはリスクの高い拠点や分野について認識することができます。
- **高度なユーザーインターフェース:** 様々なレベルの訓練を容易に行えます。
- **組織階層のマッピング:** タスクの実行者、報告相手を適切に任命します。



評価システム

- 評価、規則、試験、点検の全てを管理
- 評価を行うスタッフを任命
- スタッフはモバイルアプリまたはウェブサイトを通じて評価報告を行えます
- 評価結果は各拠点のパフォーマンス&モニタリングメーターに自動的に反映

The screenshot displays the 'Assessments' section of the Octopus Control room web interface. It features a sidebar with navigation options like 'Control panel', 'Messages', 'Incidents', 'Visitors', 'Command and Control', 'Security', 'Reports', 'Patrols', 'Buildings', 'Logistics', 'Performance and Measurement', 'Assessments', 'Safety', and 'System settings'. The main content area is divided into three panels:

- Assessments:** A table listing assessment types such as 'information security', 'Risk Management', 'Eligibility Form Operational technical security measures and physical protection', and 'Information security auditing and records (physical aspect)'. Each entry has an 'Add' button and action icons.
- Subjects:** A table listing subjects for the selected assessment, including 'Cameras (Tm's) and VMD', 'Digital Recording System', 'Burglar System', 'Panic buttons', 'Access Control System / Guest', 'POS rooms and safes', 'System Corzit', 'Determination vehicles LPR system', 'Equipment, accessories and related measures', and 'Physical protection measures'. Each entry has an 'Add' button and action icons.
- Questions:** A table listing questions for the selected subject, such as 'Upload Pictures: 4, 9, 16', 'Obtaining an image from a camera', 'Adjusting No. Camera location', 'Quality Watch (Focus / Zoom) motion detection and Details', 'Lack of lighting (all the cameras will be dark)', 'Long-term glare cameras (sun / headlights)', 'Movement of the camera and viewing angle', 'Obstruction / Interference of a foreign object', and 'Interference / noise viewing screen'. Each entry has an 'Add' button and action icons.

The screenshot shows the 'Assessment system' mobile app interface. It displays the following information:

- Header:** 'Assessment system' with a back arrow.
- Reviewer name:** 'Danny Security'.
- General Information:** 'The date of the evaluation: 05/06/2017 10:08'.
- Participants in the assessment:** 'Krissy'.
- General information about assessment:** A text input field.
- Cameras (Tm's) and VMD Weight:...** A section header.
- Upload Pictures: 4, 9, 16** with a 'Critical risk 10%' indicator.
- Buttons:** 'Save' and 'Save and close'.