



2018年版

プレゼンテーション

Genetec編

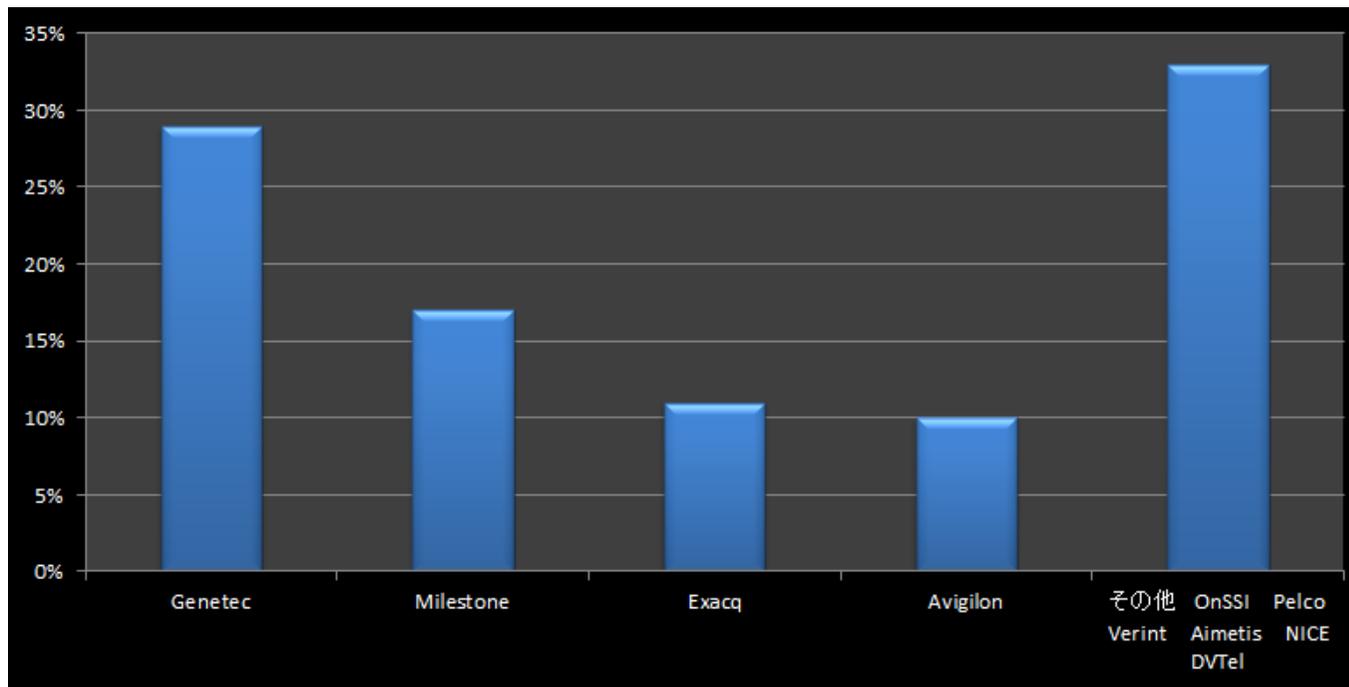
## わたしたちのSolution

# Genetec スイーツ

### エンタープライズへの約束

1. カバナンス
2. セキュリティ
3. シームレスなモニタリング・コミュニケーション
4. クオリティとプロフィット

## 出典IPVM 最も好きなVMSランキング



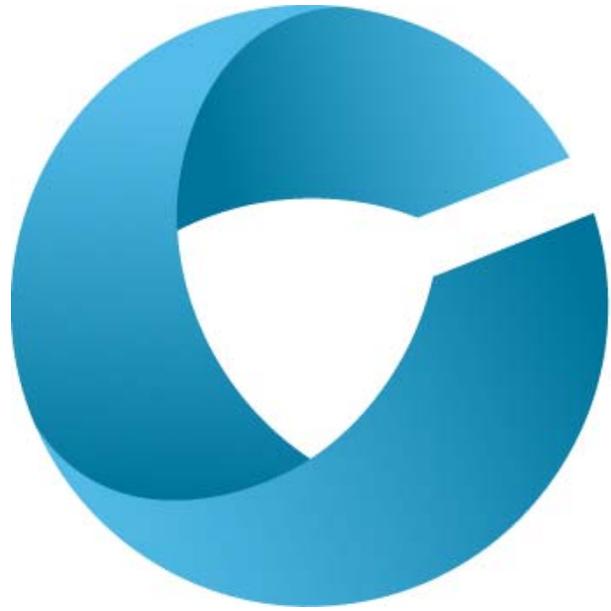


1997年創業 カナダ モントリオール

# Genetec

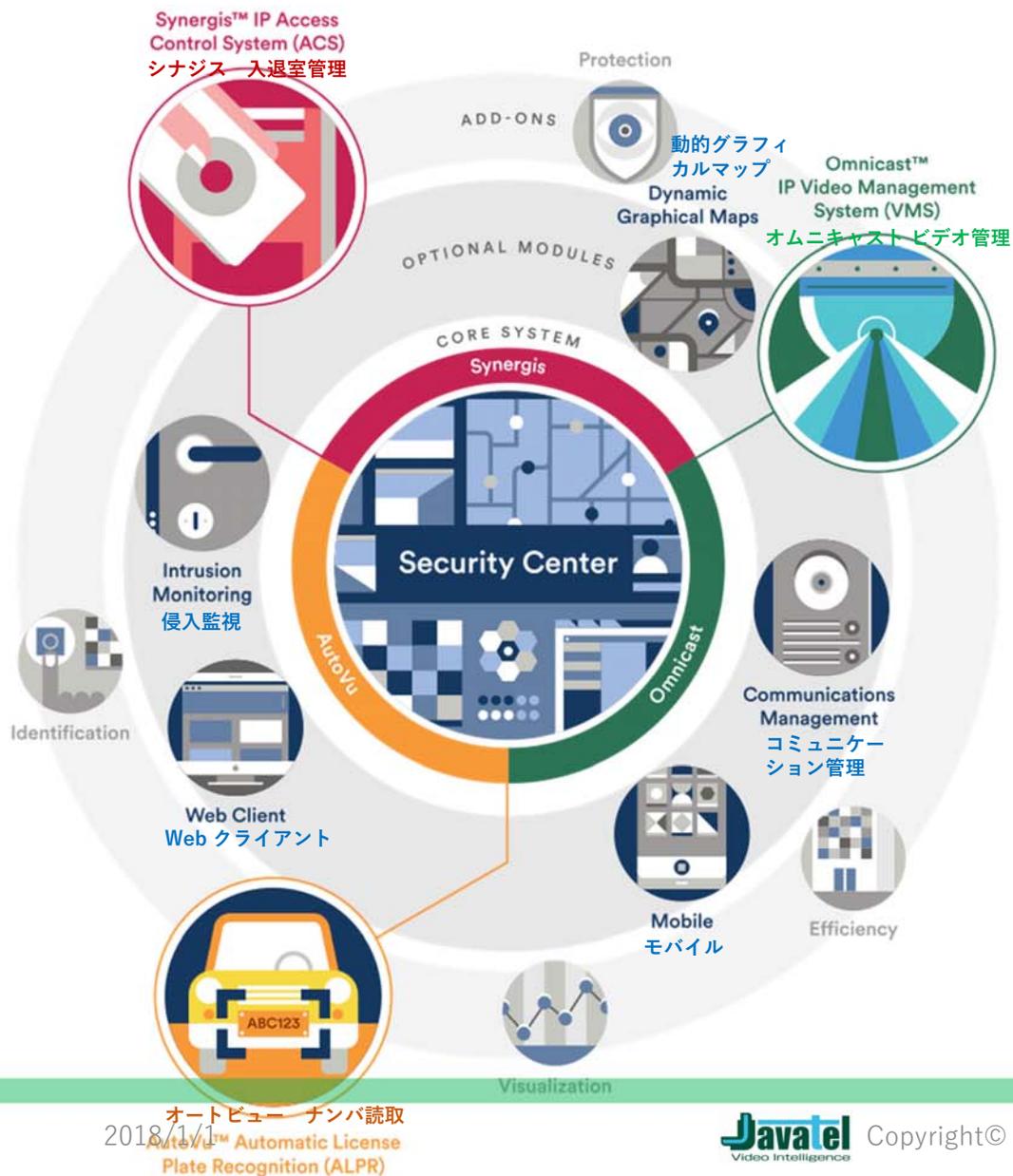
Genetecの創設者兼社長兼CEO、Pierre Racz Genetecが何年も成長してきた。Pierre Raczは、彼は生粋のエンジニアであるという点で、典型的な成長企業のCEOではありません。彼は根底にテクノロジーのマスターを持っていますが、彼と彼の会社であるGenetecが市場の鋭い感覚を持っています。Racz氏はまた、新技術に慣れ、純粋な起業家の舞台を過ぎて会社を成長させ、業界をリードするビデオ管理ソフトウェア会社を運営しているという点で、非典型的です。





# Security Center

統一セキュリティ・  
プラットフォーム



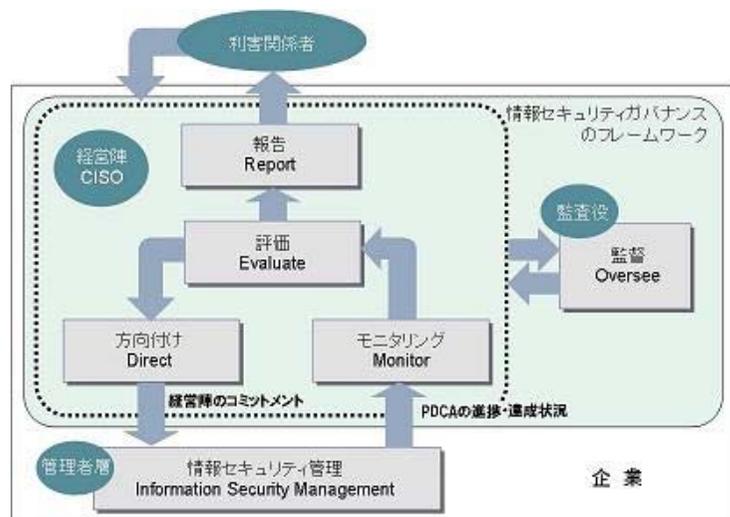
ガバナンスの為にはシームレスなセキュリティ管理は喫緊の課題

Security Centerはこの課題に対して全方位の解決策を提供する、非定型インフォメーションのプラットフォーム

## 情報セキュリティガバナンスとは、

「企業における情報セキュリティガバナンスのあり方に関する研究会報告書」において、「コーポレート・ガバナンスと、それを支えるメカニズムである内部統制の仕組みを、情報セキュリティの観点から企業内に構築・運用すること」と定義されました。

平成20年6月公開の「産業構造審議会情報セキュリティ基本問題委員会 中間とりまとめ (PDF形式: 323 K B) PDFファイル」の中で、「企業経営の主目標は、株主、顧客、取引先、従業員、社会等の利害関係者に対して責任を果たすこと、つまり、「企業価値の向上」及び「社会的責任の遂行」にあり、これを支える重要な取組の一つにリスク管理が位置づけられる。様々なリスクの内、情報資産に係るリスクの管理を狙いとして、情報セキュリティに関わる意識、取組及びそれらに基づく業務活動を組織内に徹底させるための仕組み\*を構築・運用することを情報セキュリティガバナンスと位置づける。(\*経営者が方針を決定し、組織内の状況をモニタリングする仕組み及び利害関係者に対する開示と利害関係者による評価の仕組みを指す)」と、その概念の一層の明確化を図りました。



非定型的な情報の典型が**物理セキュリティ**であることは自明でこれを如何に制するかが重要課題となる。

コントロールされた物理セキュリティのイベントアクションは**重要なメタデータを蓄積**させる。

モニタリングは従業員の不正行為を発見するためだけでなく、会社のセキュリティ上の規則が機能していることを確認するために行うものです。安全を確認することで、経営者も従業員も、初めて安心することができます。確認を行わず漠然と安心してしまふことは、すなわち油断です。情報セキュリティガバナンスを企業、企業グループに確立することで、安心して本来業務に取り込むことができます。

# 統一されたセキュリティ、妥協することなく



統一とは、セキュリティにおいて御用される言葉です。Genetecでは、人と建物を保護する真の統一セキュリティシステムを構築しています。

しかし、しばしば企業が統一について語るとき、彼らは実際には、複数の独立した製品、ベンダー、サーバー、トレーニングプログラム。

これらのタイプの考慮事項を管理するにはコストがかかる  
そして複雑な妥協 - それはただの寄せ集めで統一ではありません。

より良いアプローチが存在します。Genetec Security Centerは、よりスマートに作業する能力を提供する包括的なセキュリティプラットフォームです。

これにより、セキュリティを管理し、アクセスを監視し、車両を追跡し、単一のインターフェースで1つのシステムを使用することができます。

それは、全部と全員が一緒に働く統一されたプラットフォームです。

セキュリティセンターには、アクセスコントロール、ビデオ監視、自動ナンバープレート認識 (ALPR)、通信、および侵入検知が組み込まれています。  
より大きな画像を表示することで、状況認識の向上、操作効率の向上、生産性の向上を実現します。

**オープンなアーキテクチャにより、セキュリティを強化することができます。  
あなたのビジネスに合ったデバイスとアドオンを備えたセンター - あなたのセキュリティはあなたの組織と共に成長します。**

# 保安要員(オペレータ)は過負荷になっています

セキュリティ事業者は、複数のベンダーによって構築された2つ、3つまたはそれ以上のセキュリティアプリケーションを切り替えることがしばしば期待されています。余分な作業負荷は、有効性を妨げ、不必要なストレスを引き起こし、エラーにつながります。場合によっては、6つ以上の監視および管理アプリケーションを処理することを要求される場合もあります。

アップキープとアップグレードを導入すると、セキュリティとITチームがどのように忙殺され、それほど効果的ではないかを理解するのは簡単です。



セキュリティアプリケーションに複数のユーザーインターフェイスを使用するのではなく、「ガラスの単一のペイン」に移動することができます。

それはあなたが1つの場所ですべてを設定し、監視することができます。

さまざまな種類のタスクに精通しており、オペレーターにより効果的に作業を行うためのツールを提供します。

# 統合システムは、リソースを消耗

どのオペレータにとっても、さまざまなシステムでさまざまなタスクを学習しマスタリングすることで、他の場所でよりうまく時間を費やすことができます。

シンプルなアクティビティでは、さまざまなシステムを行き来してインシデントを解決することがよくあります。

重要な情報が失われ、オペレータが効果的に反応できないことを意味する可能性があります。

## 統合と統一の意味は大きく違う



統一されたシステムは、オペレータに時間を提供し、1つの使い慣れた直感的なインターフェイスでコアセキュリティタスクを実行します。

セキュリティ管理者にとって、余分なサポートやメンテナンス契約、互換性、アップグレード、複数のシステムのトレーニングなどの追加的な負担が必要です。

# セキュリティをビジネスの中心に置く



あなたのセキュリティオペレーターが従業員から電話を受けるのを想像してください。彼らは安全な戸口にあり、アクセスカードを紛失しています。

カード所有者の身元を確認し、ライブビデオと保存された画像を比較し、インターコムを介して会話することはすべて貴重な時間を要します。

セキュリティセンターでは、オペレーターはよりスマートで迅速に作業することができます。

アクセスコントロール、ビデオ、およびインターコムに1つのインターフェイスを使用することで、必要なすべてのタスクを簡単かつ効率的に簡単に完了できます。

これは、セキュリティ担当者が日常的かつ重大な状況に効果的かつ確実に対処しながら、完全な視点を得ることを意味します。

簡単に言えば、より迅速でより簡単な意思決定と調査が可能になります。

# より良い意思決定を する能力

1つのサイトまたは複数のサイトのいずれかで保護する人と資産がある場合、事業者は一度に複数のことを実行する能力が必要です。

セキュリティセンターでは、作業者が任意の数の同時タスクを実行できるコラボレーティブなタスクベースのアプローチを使用し、同時に特定のアクティビティに集中します。



フェデレーション™機能によるマルチサイトの監視とレポート機能により、セキュリティセンターは集中管理された操作を提供し、機密データを保護しながらセキュリティを強化します。中断のないアクセスを提供し、組織を動かすことができます。

# 完全なセキュリティ アプローチを構築する



大規模なマルチサイト組織を安全に保つことは大きな仕事です。ビデオ監視と訪問者アクセスの管理から脅威と警報への対応まで、セキュリティチームは十分に対処しなければなりません。Corpincという名前の組織のシナリオを詳しく見てみましょう。



**> 4,200**  
過去3年間にGenetec認定インテグレータによってグローバルに展開された完全に統合されたシステムの数

**80%**  
ビデオと統合されたSynergisアクセス制御システムの割合

# 完全なセキュリティ アプローチを構築する

世界中のサイトから何千人もの従業員が働いているため、Corpinclは主要な国際機関です。

安全な環境を維持するための責任は、セキュリティチームにあります。しかし、成長がインフラ投資を上回っているため、セキュリティへの混乱を招いています。



包括的なセキュリティ戦略の欠如は、時間が経つにつれて、セキュリティシステムが異種の方法で導入され、管理されることを意味しました。

チームは6つのセキュリティ製品を使用していました。これは意味のあるコラボレーションや努力に苦勞していました。

彼らの統一されていない旧式のビデオ監視システムは、使用するのが困難で時間がかかりました。

# 完全なセキュリティ アプローチを構築する



「各サイトはサイロで作業していましたが、セキュリティ担当者は過負荷状態になり、リソースが引き伸ばされました。」

欲求不満な調査のために作られた粒状の画像で、システムは信頼できませんでした。彼らは観察し報告することができ、他には何もない。インシデントは、分析されるべき接続されたデータではなく、ワンタイムイベントとして扱われました。

また、統合に関する問題のため、複数のシステムがインシデントに関連するデータに関連付けることはありませんでした。各サイトはサイロ内で作業していましたが、セキュリティ担当者は過負荷になり、リソースが引き伸ばされました。これは、セキュリティ環境の危険な不完全な見方と、脅威に自信を持って一貫して対応できないことにつながりました。

物事をさらに挑戦するために、コントロールルームは乱雑になりすぎてしまった。非常に多くのアプリケーションが稼働しているため、すべてのアプリケーションを管理するために複数の画面とスタッフが必要でした。

サイロとは業務プロセスや業務アプリケーション・システムなどが、外部との連携を持たずに自己中心的で孤立している様を示す言葉。

silosとは家畜の飼料や穀物などの貯蔵庫ないしは弾道ミサイルの地下格納庫のことで、英語では「窓がなく周囲が見えない」という意味がある。ここから、組織が縦割り構造になっていて各業務部門の活動が連動を欠いていることを「サイロ型業務」、コンピュータ業務システムにおいてアプリケーションやデータが部門や個人ごとに孤立していることを「サイロ型システム」「アプリケーション・サイロ」「データ・サイロ」などという。

# 完全なセキュリティ アプローチを構築する



Corpinc社のセキュリティディレクターがGenetecに来たとき、彼女はチームが直面した問題について説明しました。

私たちは、統一されたシステムを導入することで、状況を変え、誰もが簡単に生活できるような徹底的なセキュリティ戦略を提供することを認識しました。

# 完全なセキュリティ アプローチを構築する



3/4

アプリケーション間で共通のセキュリティ活動の割合（アクセス、ビデオ、ALPR、侵入） - まだ一部のエンドユーザーは、異種のシステムで動作しています

## 大きい & 小さい

統一されたシステムはすべてのサイズで提供され、大規模な展開だけではありません。Genetecの**平均統一システム**は、30リーダー(ACS)と40カメラから構成されています

「統一されたシステムは、単純なセキュリティ以上のものを提供します。  
ビジネス機能と柔軟性を提供します。」

セキュリティセンターに入ります。Certified Genetec Integratorと協力して、顧客は業務を変革しました。今日の日常生活をより簡単に直感的に理解できるようになりました。それはチームにすべてのサイトのグローバルなビューを提供する統一されたプラットフォームを与えました。

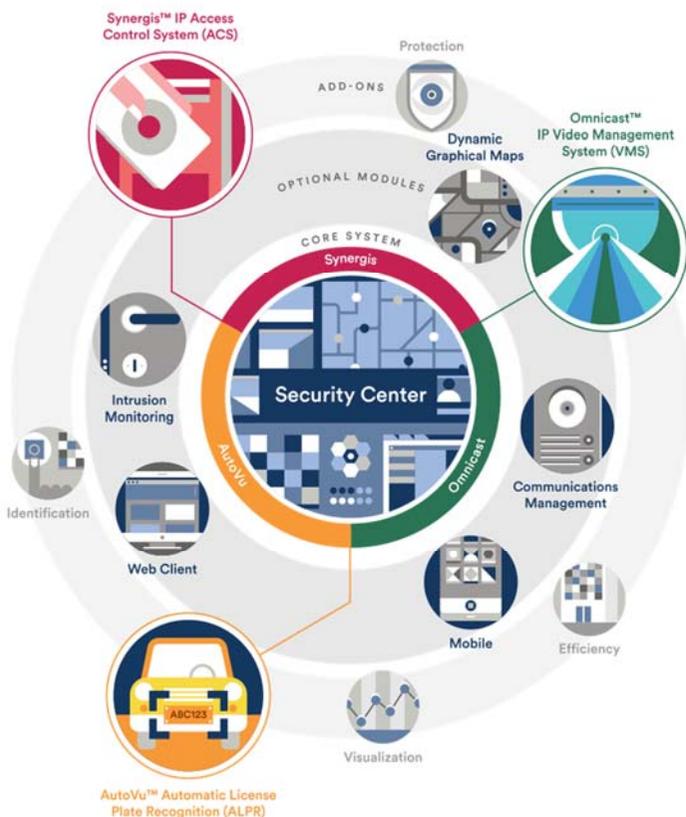
彼らは、アラームを監視し、ビデオを見て、インシデントをより簡単に報告し、施設のアクセス要求から緊急時の対応まですべてを調整することができます。

Corpincは、世界各地の小規模のリモートオフィスが独自に50~100台のカメラシステムを運用することを可能にしていましたが、地域オフィスを本社に連動させることができませんでした。

Security CenterはCorpincの機能性と柔軟性を提供し、ビデオ監視、アクセス制御、自動ナンバープレート認識、スマートな分析などの集中監視、通信、監査を1つのプラットフォームで行うことができます。

この統一されたセキュリティアプローチにより、組織リソースが節約され、運用効率が向上し、環境に関する重要な情報が提供されました。

# 統一されたGenetecの経験



セキュリティセンターは、ビデオ監視、アクセス制御、自動ナンバープレート認識の3つのコアシステムと、オプションのモジュールとパートナーアドオンを統合しています。セキュリティセンターは、モジュラーソリューションとして、時代に応じて強化できるコアセキュリティ機能を提供します。。



**Omnicast**<sup>TM</sup>

# ビデオ管理ソリューション



# あなたの環境を 知的に見る



セキュリティを向上させながらビデオでよりスマートに作業しても、ネットワークや人に負荷がかかるとは限りません。

より多くのセキュリティカメラを追加し、高解像度のビデオに依存し、保持時間を長くすると、セキュリティシステムに負担がかかります。サイバーセキュリティのリスクとプライバシーの懸念は、それをさらに困難にします。

セキュリティセンター  
Omnicastは、人と資産を効果的に保護する手段を提供するビデオ管理システムです。

信頼性の高い有用なエビデンスを取得するだけでなく、環境を把握し理解することができます。統合セキュリティプラットフォームであるGenetec Security Centerのコアシステムの1つです。

Omnicastは、1つのサイトを監視していても、複数の場所で操作を監視していても、オープンで、柔軟で、スケーラブルです。それはあなたの選択したカメラをサポートし、ネットワーク上でシームレスに動作します。インテリジェントなストリーミングと帯域幅の最適化により、ネットワークとストレージのコストが削減されます。

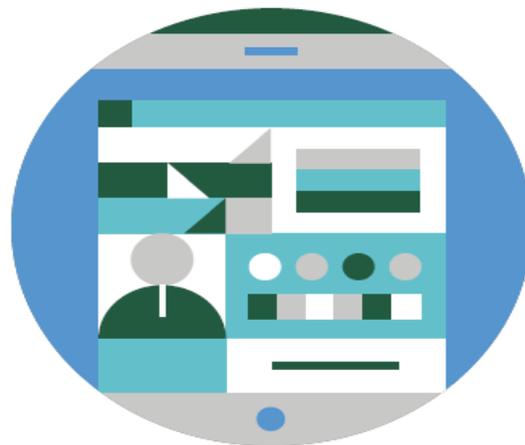
Omnicastは、カメラのフィードとセキュリティアラームの中断のないビューを使用して、オペレータが状況を迅速に評価して対応できるようにします。彼らは強力な検索とレポートツールを提供し、机や携帯端末からでも迅速に調査に取り組み、人やネットワークへの負担を軽減します。

他のセキュリティシステムとのビデオ監視を統一します。  
単一の直感的なインターフェ이스の背後にある複数のニーズに対応することで、すべての操作を制御します。  
さらに重要なことに、状況に即座に反応することができます。



### あなたの組織と共に進化する

Omnicastは、お客様のニーズやビジネスの変化に合わせて組織に適応する柔軟でオープンなアーキテクチャを採用しています。非常に小規模な企業から非常に大規模な企業まで、あらゆる組織で機能するように拡張され、条件が進展するにつれてビデオシステムがペースを維持することを確実にします。



### 単一の統合プラットフォーム

Security Centerを使用してセキュリティシステムを統一する場合は、ビデオ、アクセスコントロール、および自動ナンバープレート認識 (ALPR) のためのインターフェイスを1つだけ使用します。アプリケーション間のジャンプ時間を短縮しながら、よりスマートに作業します。インタラクティブマップを使用して施設をナビゲートし、カメラやその他のデバイスを監視します。さらに、ビデオをSIP通信と侵入検知に結びつけることで、より多くの成果を上げることができます。



### 全て見る

Federation™を使用して、複数のリモートシステムとサイトを1つの仮想システムの一部であるかのように監視します。いつでもどこからでもビデオ監視システムにアクセスできます。ビデオを録画し、組織全体で共有します。カメラを制御し、アラームを監視し、アクセス制御と車両活動を追跡して、あなたの状況に関する共通の操作イメージを提供します。

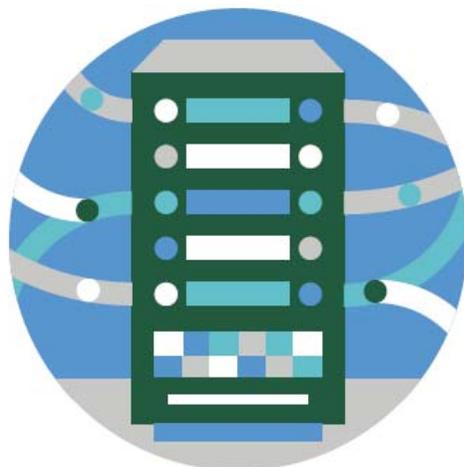
監視システムを拡張し、変化するチームの要求に適応してください。新しいテクノロジーをすぐに利用できるにする。また、柔軟な購入オプションを利用することもできます。



### 最も必要なときに利用可能

ライブや録画されたビデオが必要なときにアクセスできるようにする。サーバーへの接続が失われた場合でも、ビデオに途切れることなくアクセスできます。

Omnicastはフェイルオーバーと冗長性を内蔵しているため、録画をネットワーク障害や物理的な損傷から保護します。正常性監視通知は、システムの正常性と稼働時間に関するリアルタイムの更新を提供するので、常に意識しています。



### ハードウェアに適合

セキュリティセンターOmnicastは自然にあらゆるハードウェアに適合し、何千もの業界をリードするカメラ、エンコーダ、ストレージ機器、センサなどをお客様の選択に応じて提供します。

OmnicastソフトウェアがあらかじめロードされているGenetecのセキュリティライセンスを採用することで、より短時間で稼働させることができます。完全にテストされ、検証され、最適なパフォーマンスを発揮しながらリスクを軽減します。



### ネットワーク上のホームで

Omnicastはあなたのネットワークを容易にします。あまりにも多くのあなたはそれがそこにあることをほとんど知らない。あなたが最も必要とするまで。20年の経験を基に、当社の次世代ビデオエンジンは、インテリジェントなストリーミングと帯域幅管理により、あまり洗練されていないソリューションで遭遇するネットワーク過負荷を克服します。

# お客様のご意見



Omnicastは革新的で確立された市場をリードするビデオ管理システムです。

しかし、私たちの言葉をそれだけにとどめてはいけません。ここには幸せな顧客がいます。

「新しいセキュリティシステムは大きな味方です。ホールトラフィックとドア、駐車場とバスループを監視するために毎日使用しています。また、学生の規律上の問題に対処する際にも非常に役立ち、両親に事実を伝えるのに役立ちます。」

Hilton Central  
School District

「このシステムは非常に良く設計されており、建物全体をこの小さなチームで管理することができ、積極的な検出とレポート機能を備えたインテリジェントなソリューションが必要でした」

Brisbane City Hall

「以前のアナログシステムとは異なり、個人に接続する必要がありました。DVRのビデオを見つけるために、私たちのカメラのすべてがプールにあります。日付と時間で検索したり、マウスのクリックで早送りや巻き戻しができます。それはすべて滑らかで簡単です。」

Homemakers  
Furniture

「Genetecはこのプロジェクトを達成するのに非常に敏感で、全く新しいシステムをインストールする必要がなかったため、このカスタムアプリケーションを通じてたくさんのお金を節約することができました。」

Tampa International  
Airport

# Omnicast in action

Omnicastの活動あらゆる規模の組織は、Omnicastを使用して、セキュリティを強化し、業務を簡素化し、インテリジェントなデータを収集する能力を獲得します。ここでは、利益を得ることができるビジネスの種類いくつかを詳しく見ていきます。



## Omnicastのカスタマーストーリー

Omnicastは、小規模な喫茶店、大規模なオフィス、国際空港など、組織を保護し、盛大に育つために必要な活力を提供します。

### A large enterprise

この世界的な小売業者は、店舗、流通センター、および何千ものカメラを管理していますが、拡張はセキュリティ投資を上回っていました。彼らの既存のシステムは、マルチサイト機能とグローバルに分散したエンティティへのアクセスが欠けており、追いつくことができませんでした。故障したカメラを交換するだけの簡単なことは、検出されず、長時間の呼び出しを意味する可能性があります。Omnicastの集中監視、効率的なマルチサイトストリーム管理、およびスケラビリティが答えでした。

即座のメリットは、全世界の緊急の問題に積極的に取り組むために、すべてのカメラとコンポーネントの稼働時間をユーザーに明確に見せるリアルタイムヘルスマモニタリングでした。



## Omnicastのカスタマーストーリー

Omnicastは、小規模な喫茶店、大規模なオフィス、国際空港など、組織を保護し、盛大に育つために必要な活力を提供します。



### A coffee shop

侵入者事件の増加は、店舗閉鎖後に店舗周辺で何が起こっていたのかをコーヒーショップのマネージャJeffに確信させた。彼はまた、彼の古い学校のDVRよりもスマートなシステムが必要でした。新しいOmnicastシステムで既存のカメラを使用することは、時間外の動きと近くの車両の検出に続いてモバイルアラートを受け取ることを意味しました。

有料の定期購入は、手頃な価格でより強力なビデオオプションを提供しました。そして、彼が警察に与えた映像は、加害者が見つかったことを保証した。



## Omnicastのカスタマーストーリー

Omnicastは、小規模な喫茶店、大規模なオフィス、国際空港など、組織を保護し、盛大に育つために必要な活力を提供します。



### An international airport



毎年何百万人もの乗客が移動し、監視するための広範な境界があるため、国際空港では安全が最も重要です。

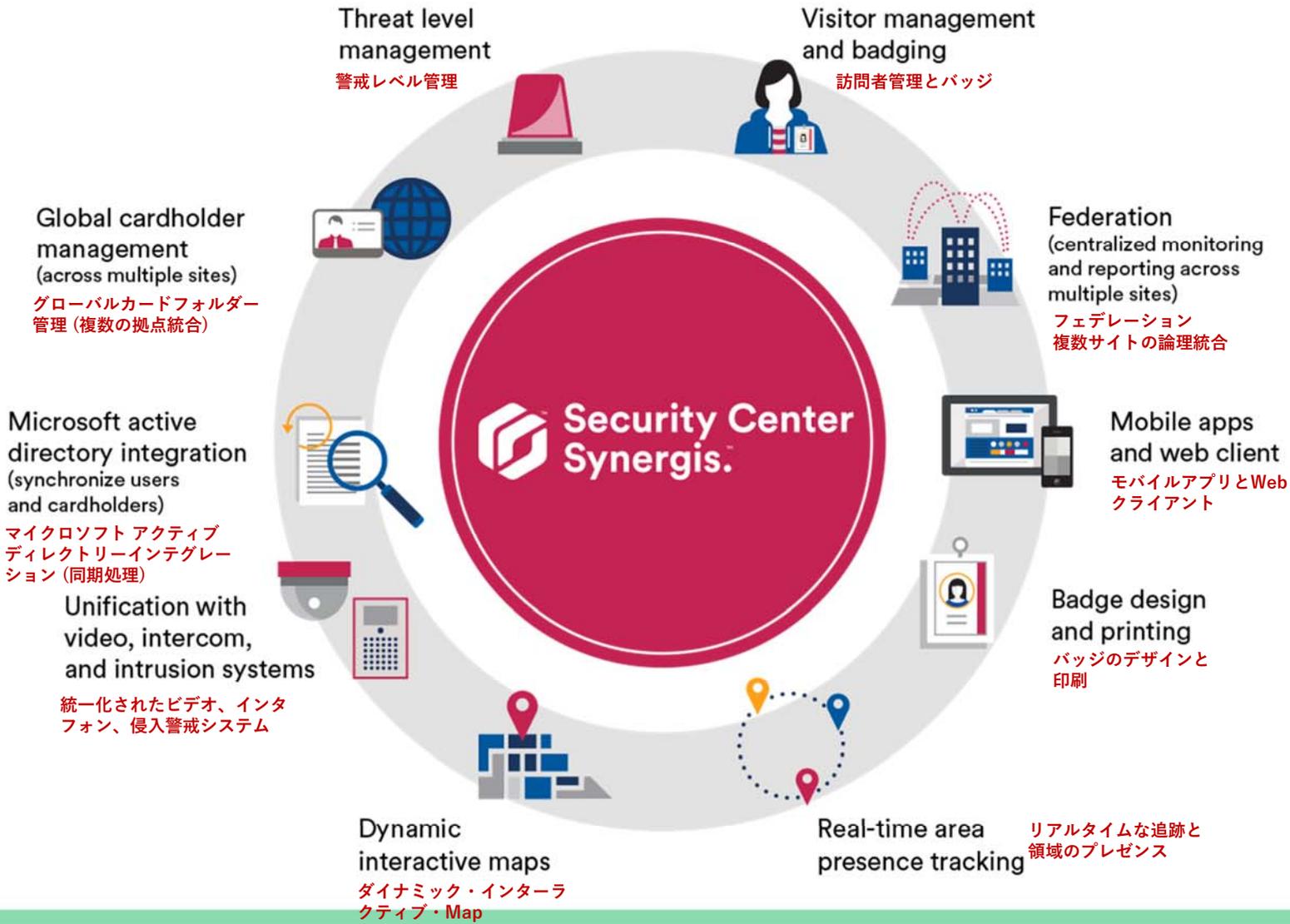
セキュリティチームの主な任務の1つは、空港の不動産の監視を継続的に維持することです。そのため、彼らはビデオ監視に大きく依存しています。

彼らは侵入者や迷惑な侵入者から破壊的な人まで、さらに悪い点で空港を安全にするために正確なリアルタイムのビデオを必要としています。Omnicastは、セキュリティ以外に、車両が違法に駐車されていないことを確認し、空港交通の流れを改善するのに役立ちます。Omnicastをそのような貴重なツールにするために、施設をより良く機能させる方法に対するセキュリティと洞察の組み合わせです。



# synergis

## アクセスコントロール ・ソリューション



# 閉じたドアの後ろのセキュリティ



あらゆる組織が繁栄するためには、安全で歓迎すべき作業環境を提供することが必要です。しかし、セキュリティと自由な動きのバランスを見つけることは必ずしも容易ではありません。あまりにも制限的で、それは人の流れを妨げる。あまりにも容認しすぎて、セキュリティが損なわれています。

セキュリティセンターSynergisは、適切なバランスを見つけるのに役立つアクセスコントロールシステムです。重要なエリアや重要なエリアへのアクセスを制限し、シームレスな移動を可能にします。あなたの人や資産を自信を持って保護するために、すべての活動を完全に把握することができます。アクセスを制限したり建物全体をロックダウンしたりすることで、瞬時に脅威に対処するチームを装備します。

Synergisは柔軟性と適応性があります。ハードウェアの選択を可能にすることで、独自のハードウェアを必要とする従来のアクセス制御モデルを改善します。Genetec Security Centerプラットフォームを使用すると、ビデオ、通信、侵入などのシステムとのアクセス制御が統合された統一された包括的なセキュリティ戦略を採用することができます。したがって、コラボレーションと共有を強化し、運用の効率を高め、新たな脅威から組織を保護します。

**Synergisを使用すると、組織を保護し脅威に対処する権限があり、適切に装備されています。**



#### 自信を持って対応する

セキュリティの状況を常に把握しておくことで、適切なタイミングで適切な決断を下すことができ、自信を持って対応することができます。状況が発生するとすぐに、セキュリティ担当者に通知し、脅威レベルを引き起こしたり、ドアや建物を閉鎖したりするなど、すばやく対応してください。そして、どんなシナリオにでも率先して備えて、あなたは決して不意をつかれません。



#### サイバーセキュリティの強化

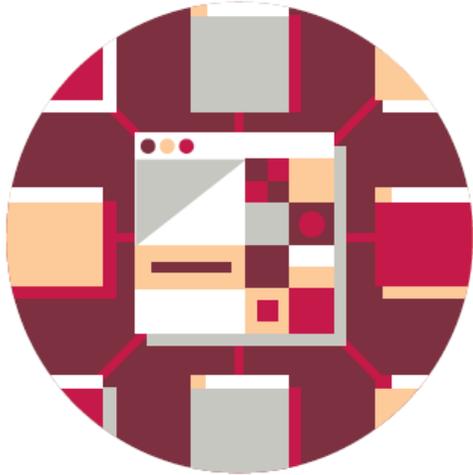
サイバー脅威の環境が進展するにつれて、組織はカード保有者を保護する必要があります。安全なコミュニケーションを維持し、サイバー攻撃から他の重要なデータを守ることができます。リーダーからSynergisソフトウェアまでのネイティブエンドツーエンド暗号化と高度なクレームベース認証により、セキュリティが即座に強化され、組織のプライバシーが保護されます。



#### 統一されたシステム

セキュリティ環境をより深く理解した上で、明確かつタイムリーな意思決定を行います。セキュリティセンターを通じたビデオ、侵入、および通信によるアクセスコントロールを統合すると、意識のレベルが上がり、運用効率が向上します。1つのパネルですべてを監視するだけでなく、直接調整された方法で行動します。

## 近代的なアクセス制御エクスペリエンスは、 総所有コストを削減します。



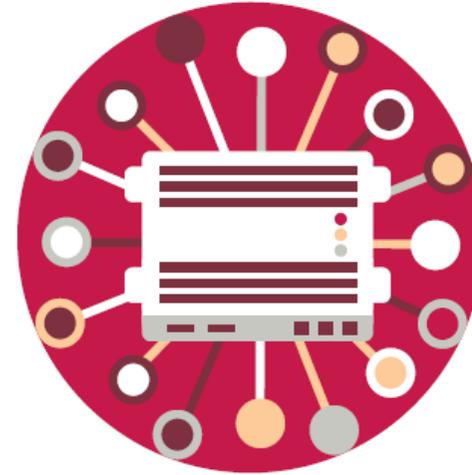
### ハードウェアの選択

Synergisは、従来の独自のアクセス制御とは異なります。  
広範に展開されているアクセスコントローラーと電子ロックの絶えず増大するアレイをサポートすることにより、投資の長期的な実行可能性を守りつつ、新たな柔軟性を提供します。



### 単一のカードアプローチに移行する

あなたの人々があなたの場所を旅行する際、グローバルなカード会員管理の一貫した経験が重要です。  
カード所有者と資格情報を一元的に管理し、自動的に変更を同期させ、単一のカード方式に移行することで、同僚が訪問者のように感じる必要がなくなります。冗長な活動を排除することで、コストを削減し、運用効率を向上させます。

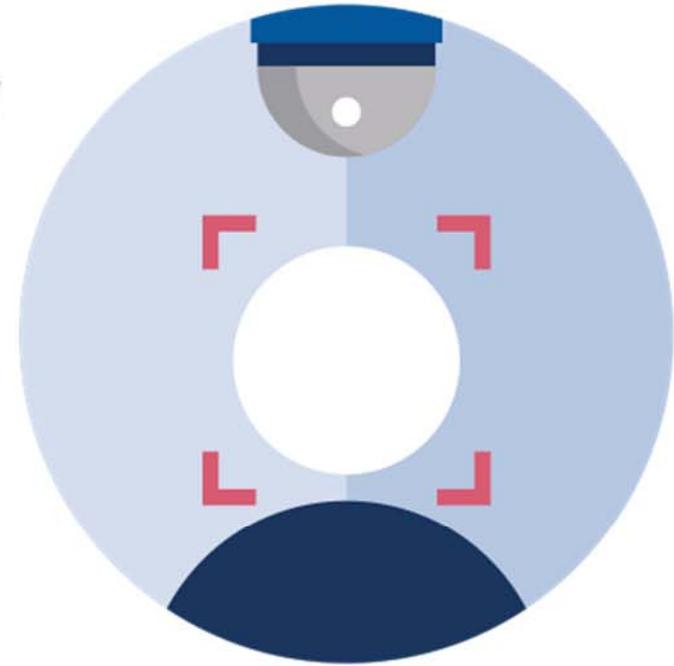


### インフラストラクチャの維持

Synergis Cloud Linkアプライアンスは、組織が1つまたは複数のサイトに展開する際に、すべての場所に展開します。  
必要なハードウェアの量を制御し、接続、通信、およびセキュリティを合理化します。スケーラブルで効率的なアーキテクチャにより、すぐに節約の恩恵を受けることができます。



追加編集中



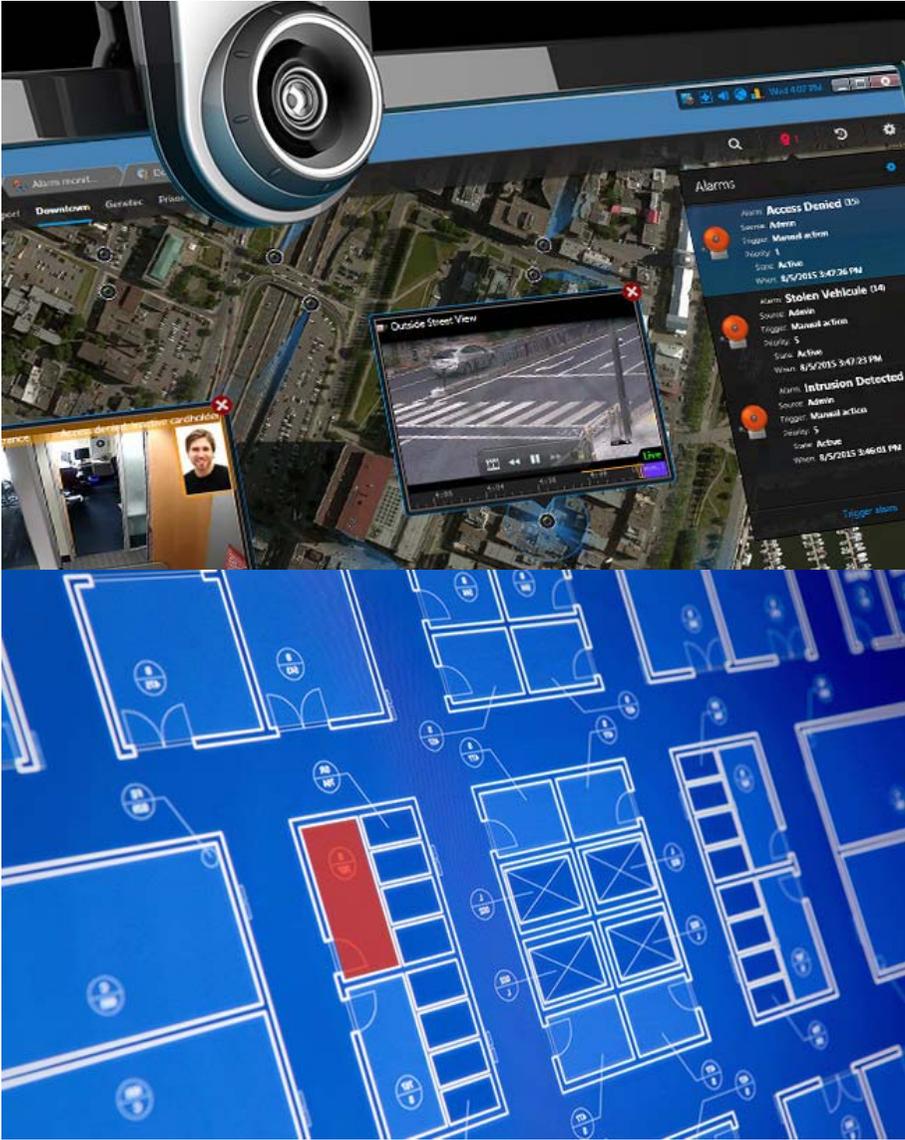
# Our optional modules

**Plan Manager**は、インタラクティブでグラフィカルなマッピングを提供し、セキュリティ環境の視覚化と管理を可能にします。設備を動的にナビゲートし、より多くのカメラとドアを監視します。これは、小規模および大規模のマルチサイト環境の両方に完全かつリアルタイムのカバレッジを提供します。

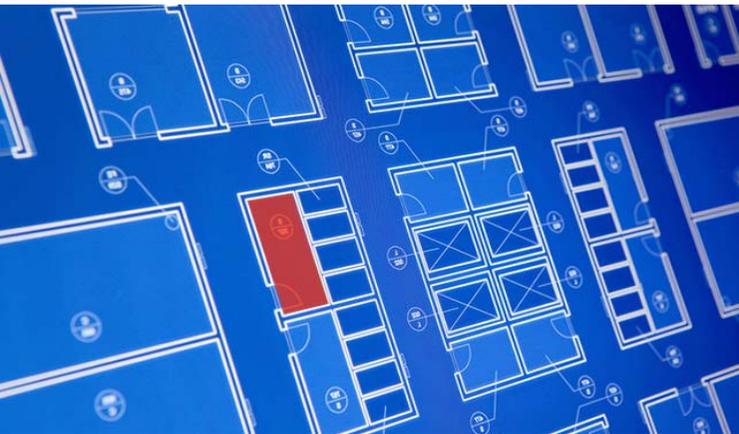
# ダイナミック・インタラクティブ・Map

## セキュリティ環境の視覚化

Plan Managerはセキュリティセンターのモジュールで、セキュリティ環境の視覚化と管理を効率化するためのインタラクティブでグラフィカルなマッピングを提供します。設備を動的にナビゲートし、より多くのカメラ、ドア、自動ナンバープレート認識（ALPR）カメラ、侵入、およびその他のセキュリティアプリケーションを監督する能力を備えたPlan Managerは、小規模から大規模のマルチサイトから完全かつリアルタイムのカバレッジを提供します環境。



# ダイナミック・インターラクティブ・Map



## 進化したモニタリング戦略

伝統的なセキュリティ監視は、セキュリティデバイスのリストまたはツリーを調査し、ライブイベントストリームを視聴し、タイルでビデオを見るオペレータの周りに確立されています。長い間規範と考えられていましたが、より直感的なアプローチが出てきました。グラフィカルマップは、セキュリティ環境に関する独自の視点を提供します。視覚的に視覚的には、より豊かなオペレータ体験をもたらす。最先端の地図技術は、ライブイベントやアラーム、ビデオ、カード会員写真、ナンバープレートを表示するだけでなく、コマンドと制御機能のすべてのスイートを組み込む必要があります。

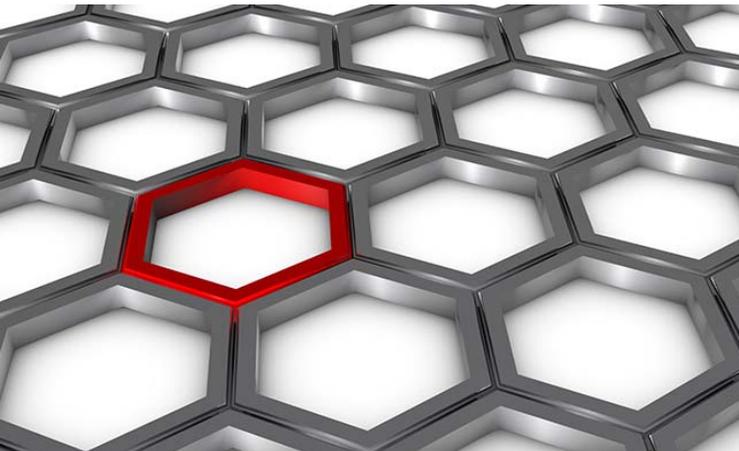
## あなたの現実に適応する地図

組織のプロセスは、しばしばセキュリティプラットフォームに適合しています。プラットフォームがサポートできるものに基づいてマップを構築します。チームがセキュリティ環境を最も正確に表現していない場合、計画どおりの効果を発揮することはできません。地図技術はあなたのニーズに適応する必要があります。最新のツールとテクノロジーを利用することで、複数のマップレイヤーを定義したり、新しいタイプのオブジェクトやデバイスを追加したり、カスタムコントロールを作成したり、操作上の現実に合わせてマップをカスタマイズすることができます。

## コラボレーションを高める

ビデオの録画、アクセスの制御、アラームの管理だけでなく、セキュリティプラットフォームはコラボレーションを促進する必要があります。複数の地理的な場所にまたがる複数のサイトを監視する場合、チームワークはかなり複雑になる可能性があります。マップは、サイト間で簡単に共有できるようにすることで、より大きなコラボレーションの触媒になることができ、オペレータは同じマップセットで作業することができます。このような状況が発生した場合、セキュリティ担当者はより効果的に作業し、同じ環境や状況を視覚化し、同僚と協力して事件や脅威に対応することができます。

# ダイナミック・インターラクティブ・Map 主な特徴



## 集中管理された複数サイト管理

組織が複数のリモートサイトにまたがっており、セキュリティ担当者が各地のセキュリティを管理する必要がある場合、マップはより実用的で直観的な監視方法を提供します。Plan Managerでは、GISマップと多層テクノロジーのサポートにより、鳥瞰図のためのすべての施設を地理的に視覚化することができます。また、特定の地理的領域、建物、床、

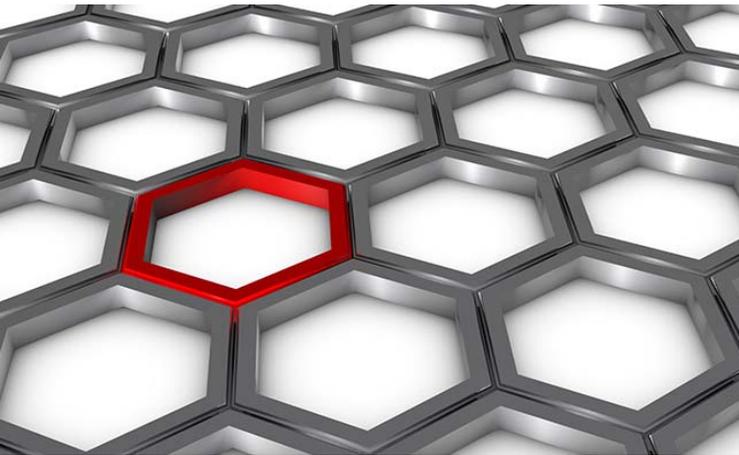
## コマンドと制御によるイベント監視

Plan Managerは、セキュリティデバイスのライブステータスの監視以外にも、従来のイベントリストまたはビデオタイルに対する代替のリアルタイムモニタリングインターフェイスを提供します。Plan Managerを使用すると、セキュリティオペレータは、アクセス制御 (ACS)、ビデオ、ALPR、侵入などのイベントを展開しながら表示することができます。また、行動を促すと、ドアのロック解除、PTZカメラの制御、アラームの管理など、マップ内で直接行動を起こすことができます。

## 埋め込みマップベースのアラーム管理

Plan Managerには、アラームの監視と管理が組み込まれています。アラームがトリガされると、オペレータはアラームの正確な位置に瞬時に注意を引くリアルタイムのビジュアルキューを受信します。一度そこにいれば、複数のレイヤーをすばやくズームして、ビデオでより詳細で詳細なビューを取得できます。オペレータはアラームに応答し、マップから直接応答するか、応答を保証するために同僚に転送します。

# ダイナミック・インターラクティブ・Map 主な特徴



## マルチサイトの視覚化

- ◆GISベースの地図を使用してすべての場所を監視することにより、新しいレベルの認識に到達する
- ◆特定の地理的領域、建物、床、およびより流動的な部屋をズームインする
- ◆サイト間の遠隔地の地図を作成して共有する（フェデレーション）
- ◆地図のショートカットやお気に入りのビューを指定して、特定のサイト、建物、エリアにすばやくアクセスする
- ◆複数のディスプレイ（ビデオウォール）にわたるマップにまたがって視覚化を拡張する
- ◆単一の場所からすべてのサイトにわたる侵入装置およびイベントを監視する



## 監視と制御

- ◆すべてのセキュリティアプリケーションの動的で統合されたビューを提示するマップを展開する
- ◆ライブまたは録画されたビデオ、カード所有者写真によるACSイベント、ナンバープレートによるALPRヒットを見る
- ◆PTZカメラを制御し、ドアのロックを解除し、すぐに対応する
- ◆マップ内のポイントを選択し、すべてのPTZカメラがその場所にすばやく向くように監視します（スマートクリック）
- ◆マップ内のエリアをハイライト表示して、ディスプレイタイトルに関連するカメラ（Lasso）に即座に設定します。
- ◆Genetecソフトウェア開発キット（SDK）を使用して、現実の地図をカスタマイズする



## アラーム管理

- ◆アラームがマップからリアルタイムで直接トリガされたときに表示する
- ◆すべての施設、サイト、地理的な場所で発生したアラームを管理する
- ◆アラームが生成された瞬間に即座にビジュアル通知を受信
- ◆マップ内のアラームに直接応答する：アラームを確認する、転送する、またはスヌーズする
- ◆相関関係のあるビデオに即座にアクセスしてアラームを有効にする
- ◆すべてのセキュリティアプリケーションのためのマップベースのアラーム管理の集中

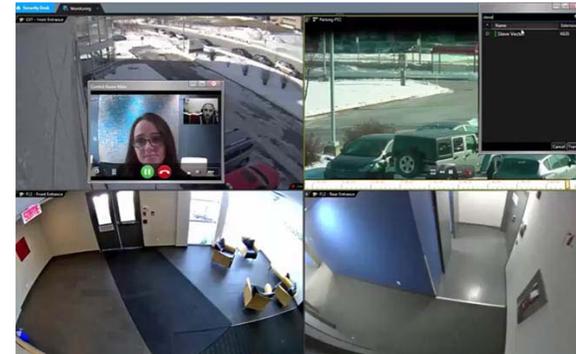
# Our optional modules

**Sipelia Communications Management**は、オペレータとインターコムデバイス間のSIPベースの通信を可能にします。セキュリティセンターで統一されると、インターコム通信はセキュリティアプリケーションにリンクされ、セキュリティチームの意識を大幅に向上させ、コラボレーションを促進します。

## セキュリティと通信管理の統一

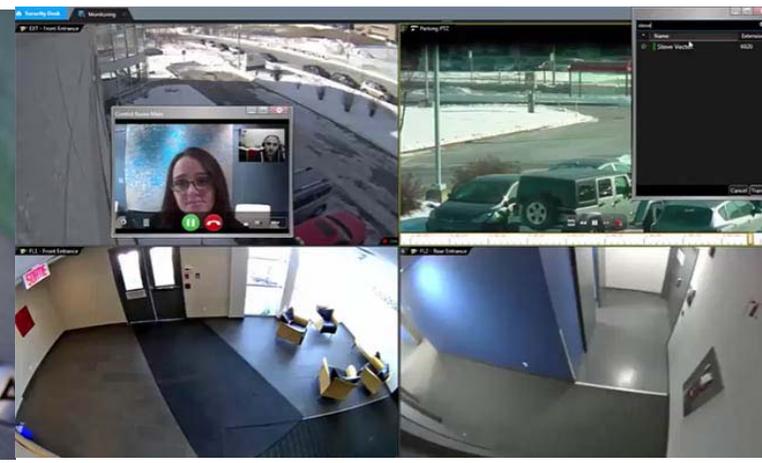
### Sipelia™ Communications

**Management**は、組織全体に展開されたオペレータとインターコムデバイス間のSIPベースの通信を可能にするセキュリティセンターのモジュールです。セキュリティセンターで統一されると、インターコム通信はセキュリティアプリケーションと緊密に連携し、セキュリティチームの意識を大幅に改善し、コラボレーションを促進します。



異なった考えをしてみてください。

# Sipelia Communications Management



## 通信はセキュリティの重要な側面

個別の物理的セキュリティと通信システムを使用することで、予期しない脅威や緊急通報にオペレータが対応する必要がある場合、多くの課題が発生する可能性があります。コミュニケーション管理を戦略の不可欠な要素にするための措置を講じることで、より包括的なセキュリティへのアプローチにつながります。物理セキュリティアプリケーションとの通信を統合することで、オペレータは、ビデオ、アクセスコントロール、および侵入システムからの物理的なセキュリティデータを直感的に補う情報のストリームを得ることができます。

## 専有通信の落とし穴

新しい電話システムを導入する場合、組織はVoIPやSIP標準に基づいて構築されたIP電話のようなオープンなソリューションを選択する傾向があります。つまり、多くの組織が引き続き独自のインターコムソリューションに依存しています。独自のインターコムシステムを導入することで、組織は時間の経過とともにコミュニケーション戦略を進化させることができます。SIPベースのデバイスを採用することで、既存のIPネットワークをより有効に活用し、設置コストを削減し、SIPベースのインターコムデバイスを既存のIPベースの電話機やセキュリティシステムに接続するなどの新しい可能性を開くことができます。

## コラボレーションの強化

ビデオ会議は家庭やオフィスでは一般的になっていますが、この形式のビデオ対応の対話は一般的にセキュリティスペースにはありません。組織が複数のコミュニケーションツール（スマートフォン、モバイルアプリ、ワークフォン、ワークステーションアプリ）に依存している場合、オペレータは通常、インシデントに応答する際の効率が低下します。セキュリティアプリケーションに組み込まれたビデオ対応の通信により、通信事業者は、単一のセキュリティおよび通信アプリケーション内で、同僚と共同作業しながらインシデントに対応することができます。

## サンプルアプリケーション

## Sipelia Communications Management



### 緊急電話管理

単一の建物を確保している場合でも安全を確保している場合でも、ビデオと緊急コールステーションの統合を使用して、緊急コールをより適切に管理できます。スタッフは、緊急コールの着信に回答したり、応答中にライブビデオを表示したり、発生した状況に対処するための適切な処置を取ることができます。

### 駐車場入口制御

アクセスコントロールリーダーやナンバープレートの認識機能を使用して駐車場へのアクセスを制御する場合でも、駐車場の入り口を制御する場合でも、お客様のチームは応募要請に回答して、単一のユーザーアプリケーションからパーキングゲートとドアを手動で開くことができます。

### 従業員ロストカードの状況

アクセスコントロールドアとビデオカメラにリンクされたインターコムコールステーションは、従業員が従業員の失ったカード要求にどのように反応するかを合理化します。着信を受け入れ、ライブビデオとカード所有者のプロファイルを通じて発信者の身元を確認し、セキュリティセンターのユーザーアプリケーションからのアクセスを許可します。

## 主な特徴

## Sipelia Communications Management



### 組み込みSIPサーバ

完全に埋め込まれたSIPエンジンにより、Sipeliaコミュニケーションサーバーは、インターコムステーションやインターコム交換サーバーを含むSIP対応エッジデバイスを独自に管理します。Sipeliaサーバーはすべての通話をルーティングし、ビデオ通話の記録と再生（オプション）を可能にします。SIPを使用して、Commend、Zenitel、Code Blue、Castel、およびAxisからさまざまな標準ベースのデバイスを導入することもできます。

### フルコール管理

オペレータは、同じ統一されたアプリケーションで、アクセス制御、ビデオ、およびALPRシステムの管理を可能にする組み込みコールダイアログを使用して、コールを開始、応答、転送することができます。カメラおよびリーダに関連付けられたドアステーションからの着信コールは、オペレータがカメラおよびドア制御用のコマンドに動的にアクセスできるようにする。カスタマイズ可能な電話帳、最近の通話リスト、ダイヤルパッドにより、操作性がさらに向上し、オペレータは他のオペレータやリモートインターコムドアステーションに電話をかけることができます。

### オペレーター間ビデオ通話

オペレータが日常的なタスクと脅威の両方の応答に外部通信アプリケーション/デバイスを使用する必要がなくなるため、ユーザ間ビデオコールはチームワークを強化します。ビデオチャットと同様に、この機能により、セキュリティインターフェイスがIPソフトフォン（SIPクライアント）に進化するにつれ、オペレータはセキュリティセンタークライアントアプリケーションでビデオコールを開始できます。これにより、同僚とのビデオ通信が大幅に簡素化され、オペレータは情報を共有してあらゆる状況に対応することができます。

## 主な特徴

## Sipelia Communications Management



### 利用可能な機能

- ◆ アクセス制御、ビデオ、ALPR、侵入およびその他のセキュリティアプリケーションとの統一された通信
- ◆ サードパーティのSIP対応ドアステーション、マスターステーション、交換サーバー、モバイルアプリに接続
- ◆ SIPトランクの設定を含む、SIPプロトコルを使用するすべての通信を管理します。
- ◆ コールキューを管理し、複数の受信者を持つ個々のユーザまたはリンググループへのコールをルーティングします。
- ◆ オプションで、ビデオにリンクされたコールセッションを記録する

### 利用可能な機能

- ◆ セキュリティセンター内の埋め込みコールダイアログにより、オペレータはコールの開始、応答、転送、キャンセルを行うことができます
- ◆ 視覚的および可聴的なコール通知により、オペレータは着信コールをすぐに通知できます
- ◆ 連絡先リスト、最近の通話リスト、電話帳、およびダイヤルパッドは、オペレータが通話を発信する方法を容易にします
- ◆ 複数のオペレータが着信コールを受信できるようにカスタムリンググループを作成する
- ◆ コールレポート機能を使用すると、ユーザーは通信アクティビティを調査し、関連付けられたビデオでコールセッションを再生できます

### 利用可能な機能

- ◆ オペレータは、同僚や同僚との間で音声のみまたはビデオ通話を確立できます
- ◆ すべてのビデオ通話は、セキュリティセンター統一ユーザーアプリケーション内に配置されているため、外部アプリケーションを一切必要としません
- ◆ USBヘッドセットやマイクを含む市販の機器で動作
- ◆ 将来の再生とレビューのためのオプションのコール録音
- ◆ タスクシェアリングで使用すると、スタッフは意識とコラボレーションのレベルをさらに高めます

## Supported Partners



Axis Communications



Code Blue



Commend



Talkaphone



TOA



Vingtor Stentofon  
(Zenitel)



2N



All Intercoms Partners

# Our optional modules

## **Security Center Mobile** (セキュリティセンターモバイル)

モバイルアプリを使用してセキュリティセンターにリモートアクセスできます。ライブまたは録画されたビデオの表示、リモートカメラの制御、アクセス制御イベントとシステムアラームのレビュー

# Our optional modules

## **Security Center Web Client** (セキュリティセンターWebクライアント)

Webブラウザを使用できるどこからでもセキュリティシステムを制御できます。カメラの監視、アクセス制御イベントとシステムアラームの検索とレビュー、ビデオのエクスポート、カード所有者と訪問者の管理を行います。



統一されたアプリのアプローチ

リアルタイムアラーム管理

より広い範囲

安全なモバイル戦略

あなたの好みのデバイス



### 主な機能\*

- ビデオの表示、PTZカメラの制御、ブックマークの追加、スナップショットの保存
- カード所有者の写真と関連するビデオでアクセス制御イベントを監視する
- 遠隔からドアのロックを解除し、ロック解除スケジュールを管理する
- リモートデバイスからSecurity Centerサーバーに**ビデオをストリーミング**する
- 失敗したログインとデバイスアクティビティを監視し、制限されたデバイスを特定する
- 変化するセキュリティ条件に対応して**脅威レベル**を管理する

\*ベンダーによって異なります

# Our built-in key features

## **Security Center Federation** (セキュリティセンター連盟)

複数のリモートサイトおよびロケーションにわたって集中管理された監視、レポート、およびアラーム管理を提供し、グローバルセキュリティを合理化します。

## Security Center Federation (セキュリティセンター連盟)

### 主な利点

- 集中監視、レポート、アラーム管理で施設を一括表示
- ローカルサイトやリモートサイトの運用を保ちつつ組織のグローバル化を支援
- 単一サイトから複数のサイトを監視することで無駄をなくし、セキュリティコストを削減
- すべてのリモートシステムへの接続に単一の統合プラットフォームとインターフェースを使用することで、標準化を促進
- サイト間の連携およびセキュリティ設備やインフラの共有を促進
- プライバシーを侵害することなく、公的な治安機関との協力や情報共有方法を単純化

### すべての拠点を一括表示し、社内セキュリティを強化する

[Security Center Federation™](#) は複数拠点や組織の集中監視、レポート、アラーム管理を行い、同時にピーク時以外の業務を合理化します。

Federation はカメラ、ドア、ナンバープレート認識ユニット、侵入パネル、およびこれに関連するすべてのイベント、アラーム、ナンバープレート認識の該当データをサイト間で同期する、高度に拡張性の高いアーキテクチャを備えています。情報がリアルタイムで自動的に同期されるため、各サイトに個別に接続したり、サイト間でデータを手動で同期したりするといった手間のかかる作業が不要になります。

Federation は拡張を前提に構築されているため、何千ものリモート入退室管理システム、ビデオ監視システム、ナンバープレート認識サイトへの接続が可能です。



# Our built-in key features

## **Global Cardholder Management(グローバルカード会員管理)**

さまざまな場所で簡単にカード所有者を同期させることができます。  
複数のサイトにまたがってアクセスする1枚のカードを発行し、コストと労力を同時に削減します。

## 主な利点

- シングルカード方式に移行することで運用コストを削減
- 可能な限りスムーズなカード会員管理モデルへの移行を実現
- 必要に応じてリモートサイトの自律性を許可する
- 主要タスクの自動化による人的ミスやセキュリティ上の欠陥の排除
- セキュリティセンターのWebクライアントでいつでもどこからでもグローバルなカード所有者と資格情報を管理できます

## Security Center Federation (セキュリティセンター連盟)

### マルチサイト共有の強化とグローバルなカード会員管理プロセスの近代化

グローバルなカードホルダー管理により、複数のサーバーを同期させて複数の独立したSynergis™アクセス制御システム間で、カード所有者、カード会員グループ、資格情報、バッジテンプレートを管理できます。新しく作成または変更されたカード所有者と資格情報は、場所に関係なく、参加しているすべてのサイトと同期して組織全体の共有と標準化を促進できます。変更は、中央または遠隔地で開始することができます。マルチサイト、マルチナショナル、マルチテナントの展開に最適です。あるサイトの変更がすぐに他のすべてのサイトに反映されることを知っていれば、安全です。



# Our built-in key features

## Intrusion Panel Integration(侵入パネルの統合)

不正なアラームや関連するコストを排除するだけでなく、侵入状況とアラームをビデオとアクセス制御とともに監視することができます。

日本では警備会社が供給しているもの以外は殆ど普及していない。警戒状態と非警戒状態をプログラム端末から設定する。家庭用として普及したが、オフィスでもそれなりに普及しているが、オフィスではACSに置き換えられている。

# Our built-in key features

## Failover(フェイルオーバー)

フェイルオーバーは、システムの中断を伴わずにハードウェア障害を許容できる連続的なサーバーアクセスを提供します。

競合他社と違い、 built-inでFailoverをサポートします。  
SQLはBackup, Mirror, Always Onで利用可能です。  
高額なクラスタリングは不要です。

最新の5.7ではアクセスコントロールもbuilt-inでFailoverをサポート

# Our built-in key features

## Threat Level Management(脅威レベル管理)

脅威レベル管理

セキュリティ条件の変化に対応してシステムの動作をすばやく変更できます。

## Threat Level Management(脅威レベル管理)

### 主な利点

- 組織がさまざまな脅威の状況に積極的に備え付ける能力を提供する
- 瞬時にセキュリティ状況の変化に対応することができます
- 潜在的な脅威への標準化された対応の実装を容易にし、セキュリティを強化する
- アクセス制御ドアによる物理的な入口点の完全な制御を提供します\*
- ビデオ監視のような他のシステムへのアクセス制御を超えた脅威管理の拡張
- あなたは、組織の特定のニーズに適応する完全にカスタマイズ可能な脅威レベルは

### 瞬時にセキュリティ状況の変化に対応

セキュリティセンターの脅威レベル管理機能により、セキュリティ条件や潜在的な脅威に対応して、セキュリティシステムの動作を素早く変更することができます。

[Synergis™Cloud Linkアプライアンス](#)で

制御されるドアからの入力を選択的に制限したり、記録品質やフレームレートなどの[Omnicast™](#)ビデオカメラの動作を変更したり、オペレータを制限したりすることができますあなたのセキュリティソフトウェアにアクセスすることができます。



# Our built-in key features

## Cloud Archives

クラウドアーカイブはあなたに与えます  
クラウドにビデオ録画を格納する能力

## Cloud Archives (クラウドアーカイブ)

### 主な利点

- インシデントやクリティカルなイベントをクラウドに転送することにより、安全でオフサイトの場所にビデオエビデンスが保存されるようにする
- レビューが必要なときはいつでも、セキュリティセンターシステムからオンプレミスまたはクラウドに保存された録画ビデオを迅速に取得します。
- 保存期間の増加やクラウドに多くの録画が転送されるにつれて、クラウドストレージ容量をシームレスに増加させる
- 資本支出の削減、オンサイトストレージハードウェアのメンテナンスコストの削減

### ストレージハードウェアへの投資を削減

監視システムの存続期間中の追加ストレージの必要性は、多くのイベントから発生する可能性があります。システムが拡大したり、ビデオ保存ポリシーが進化したり、冗長アーカイブやその他の高可用性メカニズムが導入されると、組織は追加のストレージハードウェアに多額の投資をする必要があります。

クラウドアーカイブはGenetecのユニークなサービスで、組織は既存のセキュリティセンターシステムを引き続き活用しながら、クラウド内のビデオ録画を維持することができます。このハイブリッドクラウドサービスにより、お客様は追加のハードウェアを購入する必要なく、ストレージ容量を増減する柔軟性が向上します。セキュリティセンターのオペレータは、クラウドアーカイブのビデオにシームレスにアクセスできるため、社内またはクラウドにあるアーカイブビデオをすばやく表示および検索できます



# Our built-in key features

## Active Directoryの統合

セキュリティセンターの管理者やカード所有者のアカウントとWindowsアカウントを同期させるため、貴重な時間を節約し、人的ミスを排除します。

## Active Directoryの統合

### 主な利点

- セキュリティソフトウェアと物理的な施設へのアクセスを最新のものにする
- 組織全体の協力、データの共有、一貫性の促進
- ユーザー管理を合理化し、人為的なエラーを式から排除します。
- カード保有者の管理を簡素化し、チームの生産性を向上
- 自動化された同期により、従業員のアクセスを管理するための煩雑な書類や電子メールが不要になります。
- セキュリティセンター内にセキュリティグループが表示され、グループの迅速な選択が

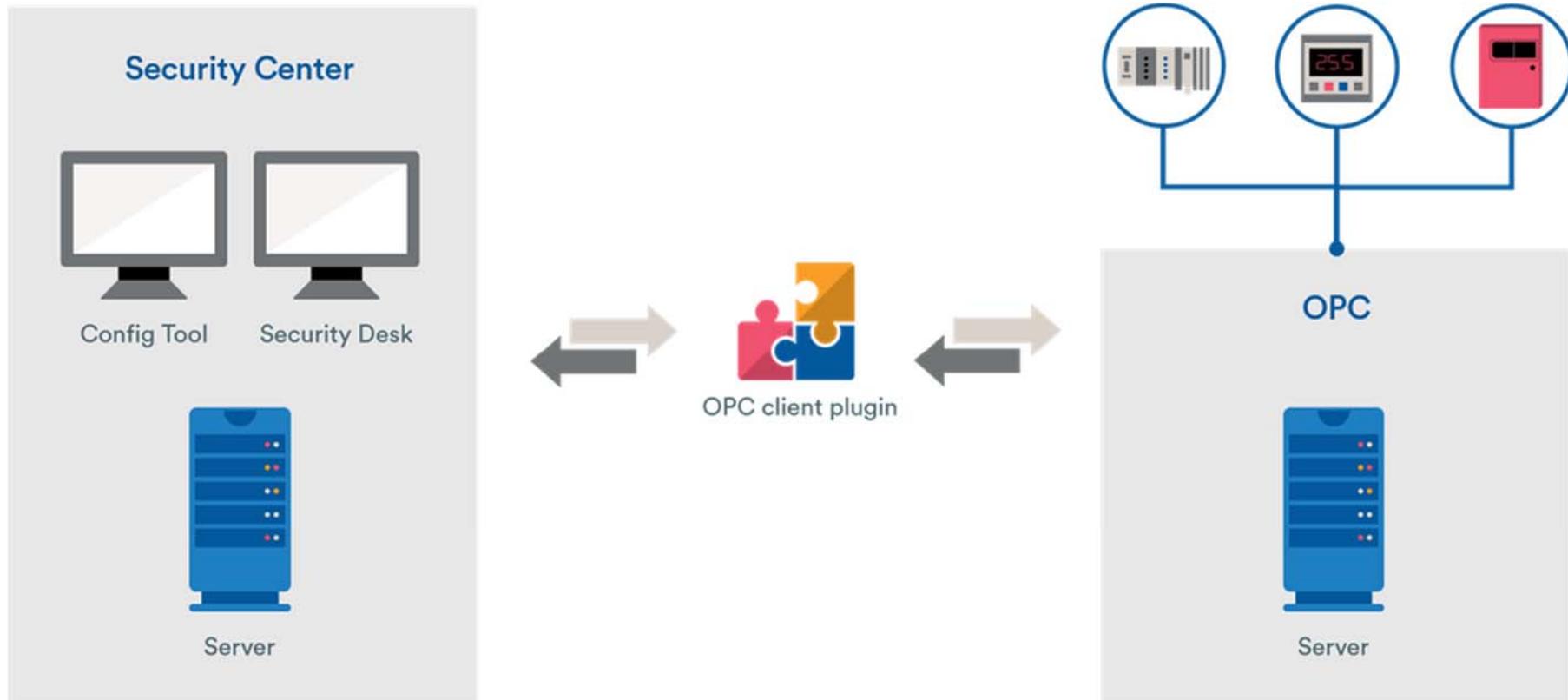
### ITディレクトリと物理的なセキュリティシステムを完璧に調和させる

Microsoft Active Directoryとの統合により、Windowsユーザーアカウントとセキュリティセンターの管理者およびカード所有者アカウントとの一元管理と同期が容易になります。Active DirectoryにWindowsユーザーを追加すると、セキュリティセンターユーザーおよび/またはカード所有者が自動的に作成されます。同期化は自動化されているため、全体的なプロセスが効率的で、一般的な手作業による介入やエラーを排除します。Active DirectoryとSecurity Centerとの統合により、Synergis™ アクセスコントロール、Omnicast™ ビデオ監視、AutoVu™ ナンバープレート認識システムのリンクを1回だけ構成すれば、貴重な時間を節約できます。



# Our built-in key features

# OPC プラグイン





物理的な違反のリスクを減らす  
組織のセキュリティを強化し、セ  
キュリティ侵害のリスクを軽減する  
ため、Security Centerの統合プラット  
フォームには、**NECのNeoFace®Watch**  
顔認識テクノロジーが統合されていま  
す。



世界最高レベルの顔認証が  
今すぐご利用頂けます。



追加の監視機能とフォレンジック機能  
を備えたセキュリティオペレータを強  
化する

この統合により、セキュリティオペ  
レータは、既知の監視リストに対して  
個人のライブビデオをチェックするこ  
とができ、リアルタイムのアラートが  
提供されます。また、効率的な調査の  
ために自動的に顔マッチイベントを  
ブックマークします。



顔認証ならお任せください。

アクセスコントロール用なら  
FaceStation 2

汎用用途なら  
AllGoVision / NEC NeoFace

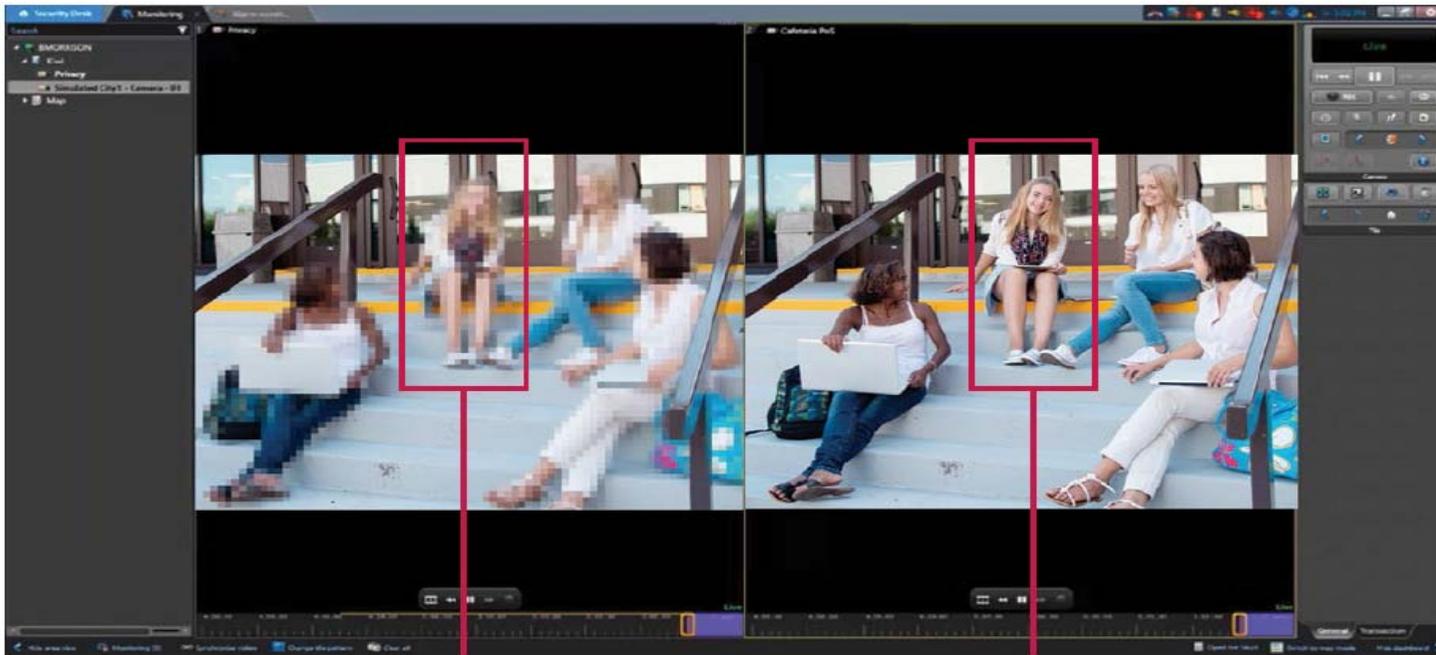


## Kiwi Security の組み込み標準サポート P/N VAPPRIPR

## オペレータは参照する必要があるものを参照

権限を使用すると、元の映像を確認できるオペレータを簡単に制御できます。インシデントが発生すると、許可されたオペレータはセキュリティセンターの監視インターフェイスから直接アクセスし、調査が遅くならないようにします。オリジナルの録音は、不正なアクセスを防ぐために証明書やチップカードを使用して暗号化することもできます。

ライセンスは永続と一年間、一か月から選定できます。カメラ毎にライセンスが必要です。



人々のリアルタイム  
匿名化

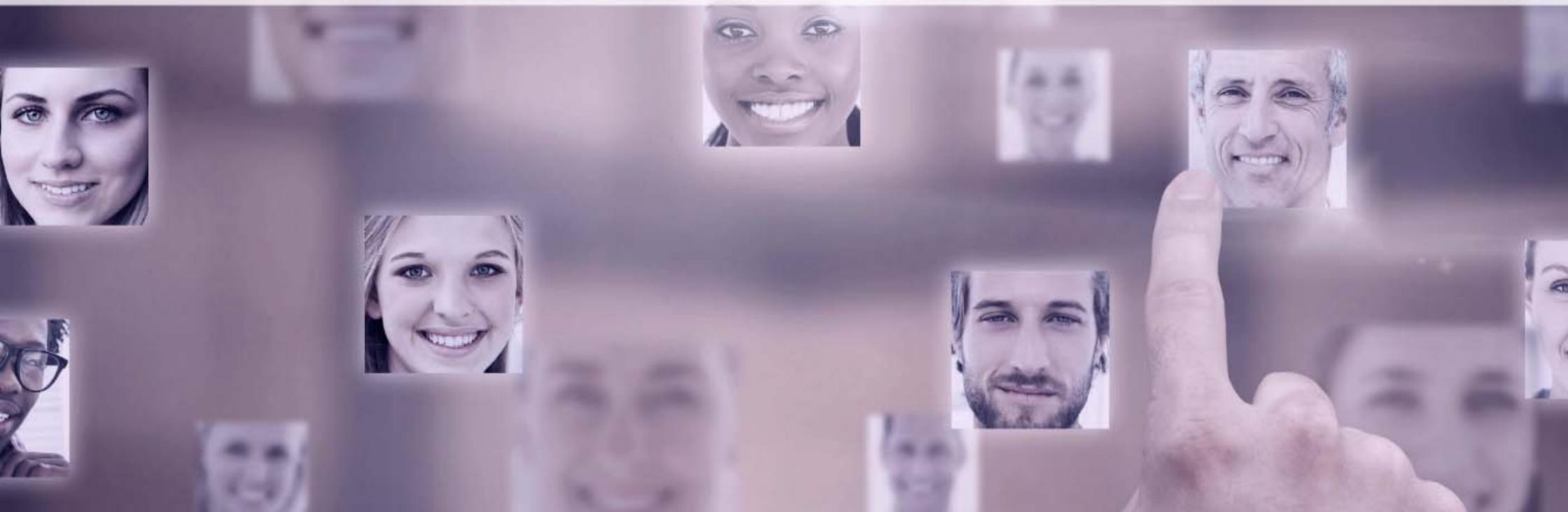
許可されたオペレーターだけが  
元のビデオを見ることができる。





## 顔コレクター

ビデオストリームにおける顔のリアルタイム収集





# 侵入検知器

あなたの周辺の自動保護





# オブジェクト検出器

オブジェクトの正確な視覚検出





# ビデオエンハンサー

関連イベントのクリアビュー





# アクティビティビジュアライザ

アクティビティ、動作、滞留時間の概要





# 人のカウンター

人の光カウント

複数の人が同時にエリアを通過しても、カウントは安定しています。3Dセンサを使用すると、**99.5%**を超える精度を達成できます。



# キュー検出器

キューの自動分析

KiwiVision®キュー検出器は、初期段階で過密状態を検出するために、キューと待機領域を自動的に分析します。

待ち行列や群集が発生した場所であればどこでも使用でき、分析結果を適用して顧客の増加を効果的に管理できます。

Kiwi Security の組み込み標準サポート  
P/N VATPSAN6 6スポット  
P/N VATPSANA 制限無



# 駐車スペースアナライザ

駐車場の視覚分析



KiwiVision® 駐車スペースアナライザは、駐車スペースが占有されているか、個々の駐車時間、駐車禁止ゾーンに駐車されている車両を検出します。

パーキングスペースアナライザは、パーキングエリアの管理に理想的なソリューションです。既存のカメラは、追加のセンサを実装する必要なしに機能をアップグレードすることができます。



# トラフィックアナライザ

視覚的なカウントと車両の分類

KiwiVision<sup>®</sup> トラフィックアナライザは自動的にカウントし、道路上の車両を分類しています。

車両が自由に定義できるエリアを通過すると、自動的にカウントされ、分類されます。Traffic Analyzerは、**トラック**、**バス**、**乗用車**、**オートバイ**を確実に区別することができます。得られた結果を統計的に評価し、エクスポートすることができます。



# 車両カウンター

車両の視覚的なカウント

KiwiVision®車両カウンターは自動的に道路上の車両をカウントします。

車両が自由に定義できるエリアを通過すると、自動的にカウントされ、分類されます。得られた結果を統計的に評価し、エクスポートすることができます。

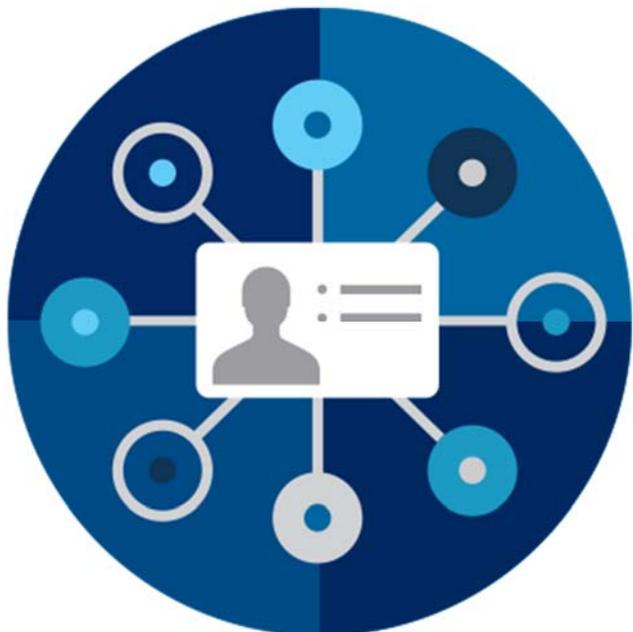


## 方向制御装置

光方向検出

KiwiVision®Direction Controllerは、制限された方向に移動するオブジェクトを自動的に検出します。

人または車両（自由に定義可能）が制限された方向に移動するとすぐに、イベントまたはアラームがトリガーされます。Directionコントローラーのアルゴリズムは、たとえオブジェクトの高さがわずか20ピクセルであってもわずかな動きまで検出することができます。



## 物理的なアクセス制御機能を拡張する

deister proxSafeの統合により、物理的なアクセスはドアの制御を超えます。セキュリティセンターの機能は、**キーキャビネット、武器ロッカー、ラジオロッカー**、その他の物理的資産にまで及んでいます。



アイテム管理システム「proxSafe」は、鍵やUSBメモリ、携帯電話など、貴重な情報機器アイテムの貸出・返却をキータグと利用者ID情報で自動化するシステムです。

- RFIDタグでアイテムを管理し、ICカードで利用者を把握
- スタンドアロン、ネットワーク経由で使用可能
- カードリーダー「proxMagic」で各種仕様のカードに対応
- 1台のキャビネットに32本のキータグを管理
- 1台のターミナルで最大1024本のキータグを管理
- オートシャッター機能でアイテムを保護(屋内仕様)
- キャビネットは簡単に壁面に設置可能
- ネットワーク経由で遠隔管理
- バッテリーバックアップで停電時もアクセス可能

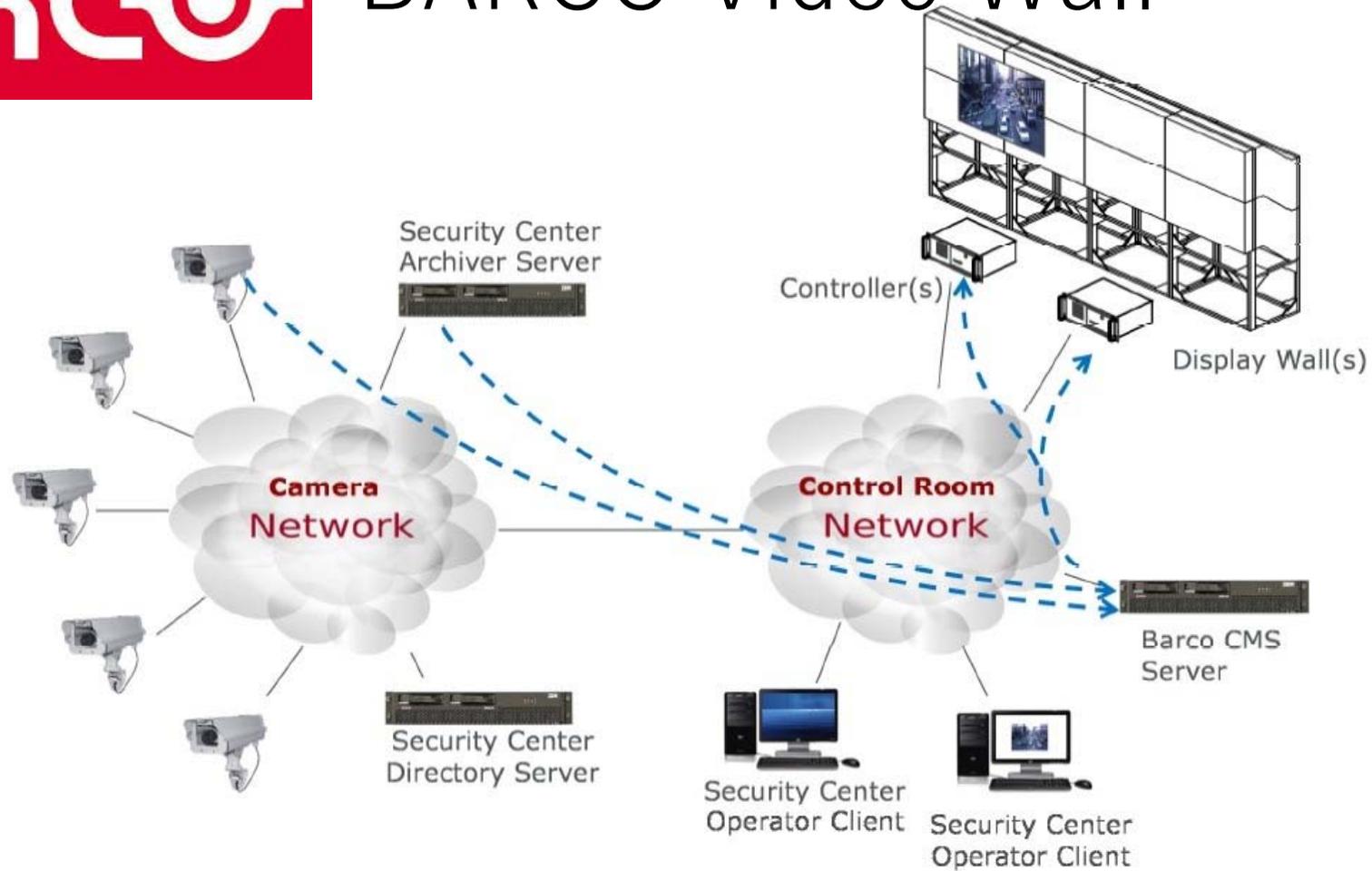


## 物理的な資産の管理、監視、保護

proxSafeプラグインは、オペレータが主要な管理イベントに関連付けられたカード所有者を視覚的に識別できるようにすることで、セキュリティを強化します。電子キー管理がSecurity Centerに統合され、deister proxSafeイベントの監視が簡素化されました。



# BARCO Video Wall



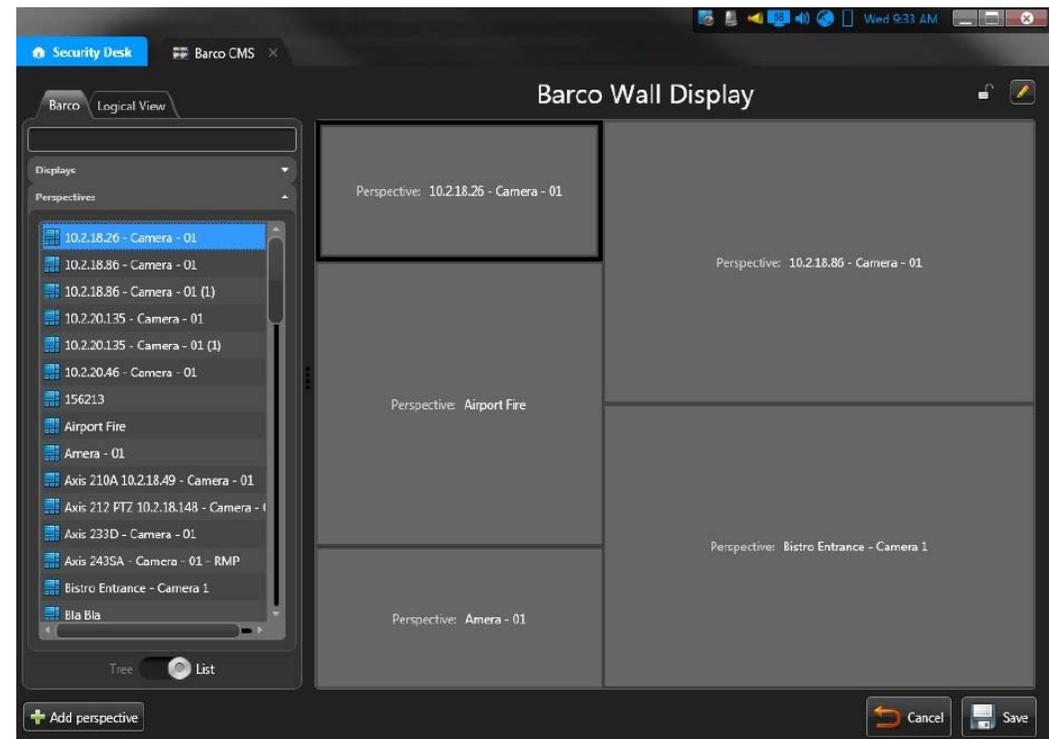


# BARCO Video Wall

## GenetecとBarco

GenetecセキュリティセンターにはBarco CMSの可視化機能が組み込まれています

単一のプラットフォームで統一されたIPビデオ監視、アクセス制御、ナンバープレート認識の世界的リーダーであるコントロールルームとGenetec incのための視覚化の世界的なサプライヤーであるBarcoは、協力とソフトウェアの統合に関する長い歴史を持っています。両社は、最新のソフトウェアプラットフォームに基づいた統合の主要な更新に投資して、共同顧客コミュニティの価値を最大限に高めています。より良い成果の実現、迅速な共有、迅速な解決





# BARCO Video Wall





# BARCO Video Wall

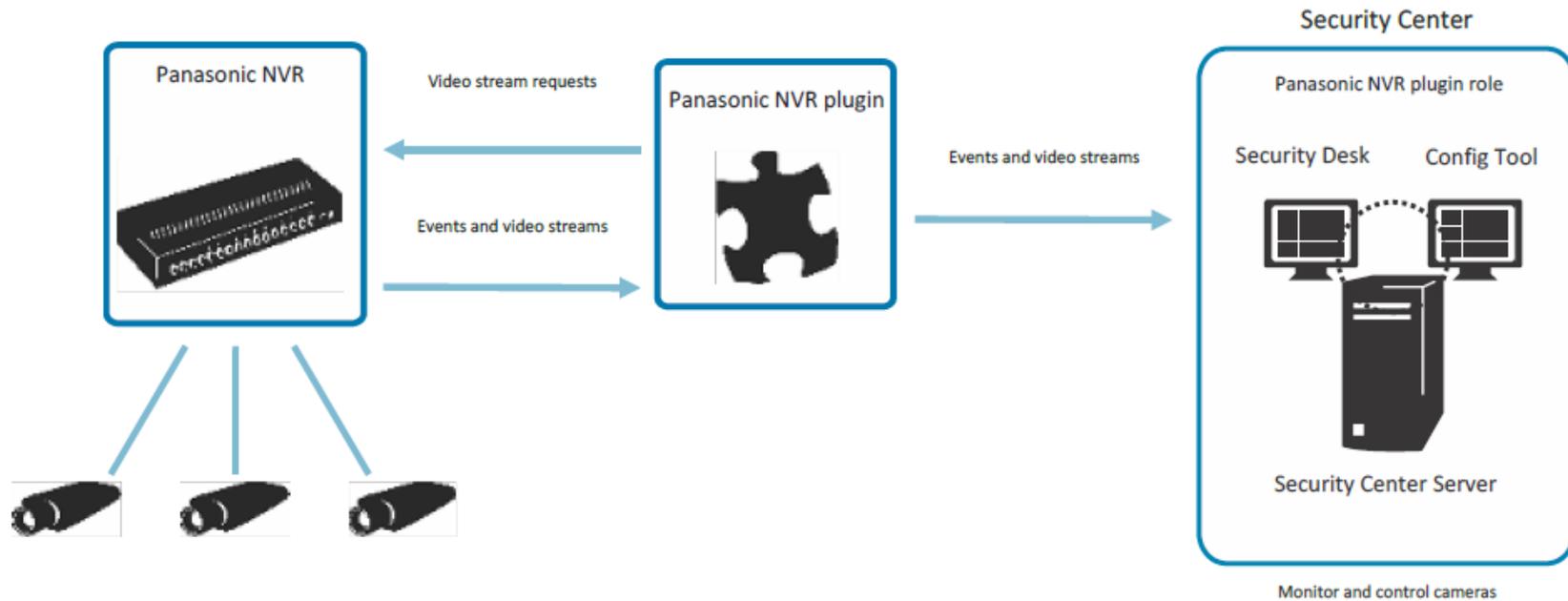




# BARCO Video Wall



## Panasonic NVR



Panasonic DVRプラグインは、Panasonic DVRをセキュリティセンターに統合するために使用されます。Panasonic DVRプラグインの役割。プラグインはカメラからイベントとビデオストリームを受信します。パナソニックDVRに接続し、セキュリティセンターに中継します。プラグインも受信します。セキュリティからのビデオストリームリクエストとユーザコマンド（カメラやPTZコントロールなど）センターに送信し、Panasonic DVRに送信します。

# Southwest Microwave MicroPoint

## Southwest Microwave MicroPoint



3m毎の位置情報

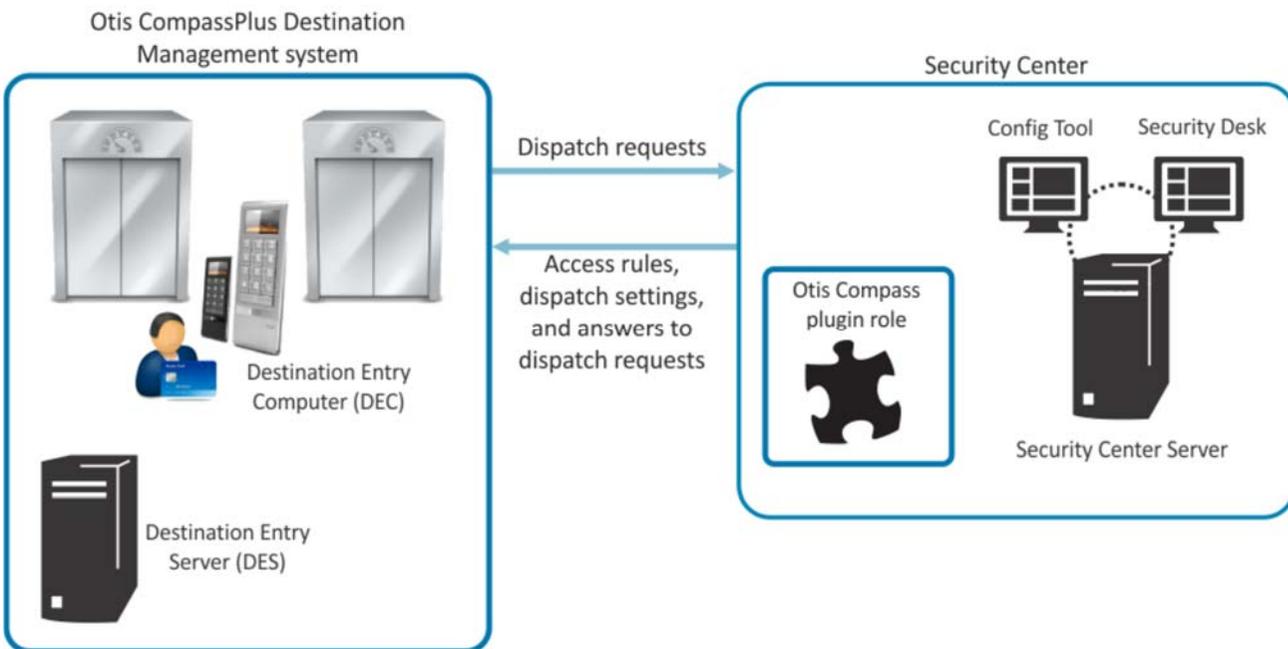
Genetec Security Centerは、Southwest MicrowaveのINTREPID MicroPoint周辺フェンス検出システムとの完全な統合を提供します。現場で実証済みのこのシステムにより、オペレータは周辺フェンスからアラームを受信し、セキュリティセンターのイベントに関連する監視ビデオを監視できます。

フェンスセンサーは、セキュリティオペレータに違反や改ざんイベントのリアルタイム通知を提供し、侵入試行を即時に監視し対応することができます。業界最高性能のフェンスセンサーとして、MicroPointは風、雨、車両交通などの無害な外乱を無視して、侵入の試みを3メートル以内に正確に位置付けます。

MicroPointプラグインは、システム管理者が周辺を監視しているカメラを完全に制御できるようにします。たとえば、複数のフェンスセクション（ゾーン）を監視するために1台のカメラを割り当てることができます。侵入試行がゾーン内でアラームをトリガーするとすぐに、カメラは妨害の正確な位置にズームするようにプリセットすることができます。オペレータ画面にカメラを表示したり、ビデオ録画を自動的に開始したり、セキュリティ担当者に電子メール通知を自動化するなど、アラームがトリガされたときに追加のアクションを実行することもできます。

MicroPointシステムのすべての侵入イベントおよび改ざんイベントは、迅速かつ効率的なビデオ検索およびイベント分析を確実に行うために、Security Centerプラグインデータベースに格納されています。

# Otis Compassプラグイン



## 日本オーチス、エレベーター次世代運行管理システム「CompassPlus™」 第46回機械工業デザイン賞「審査委員会特別賞」受賞

日本オーチス・エレベータ株式会社（代表取締役社長 ステファン・ド・モントリポール、本社 東京都文京区、以下 日本オーチス）が提供するエレベーター次世代運行管理システム（群管理システム）「CompassPlus™（コンパスプラス）」が、2016年7月15日発表されました第46回機械工業デザイン賞（日刊工業新聞社主催）にて「審査委員会特別賞」を受賞いたしました。

### Otis Compassプラグインとは何ですか？

Otis Compassプラグインは、オーチスCompassPlus™を統合したサードパーティのセキュリティセンタープラグインです

セキュリティセンターの宛先管理システムを使用して、エレベーターの発送設定と

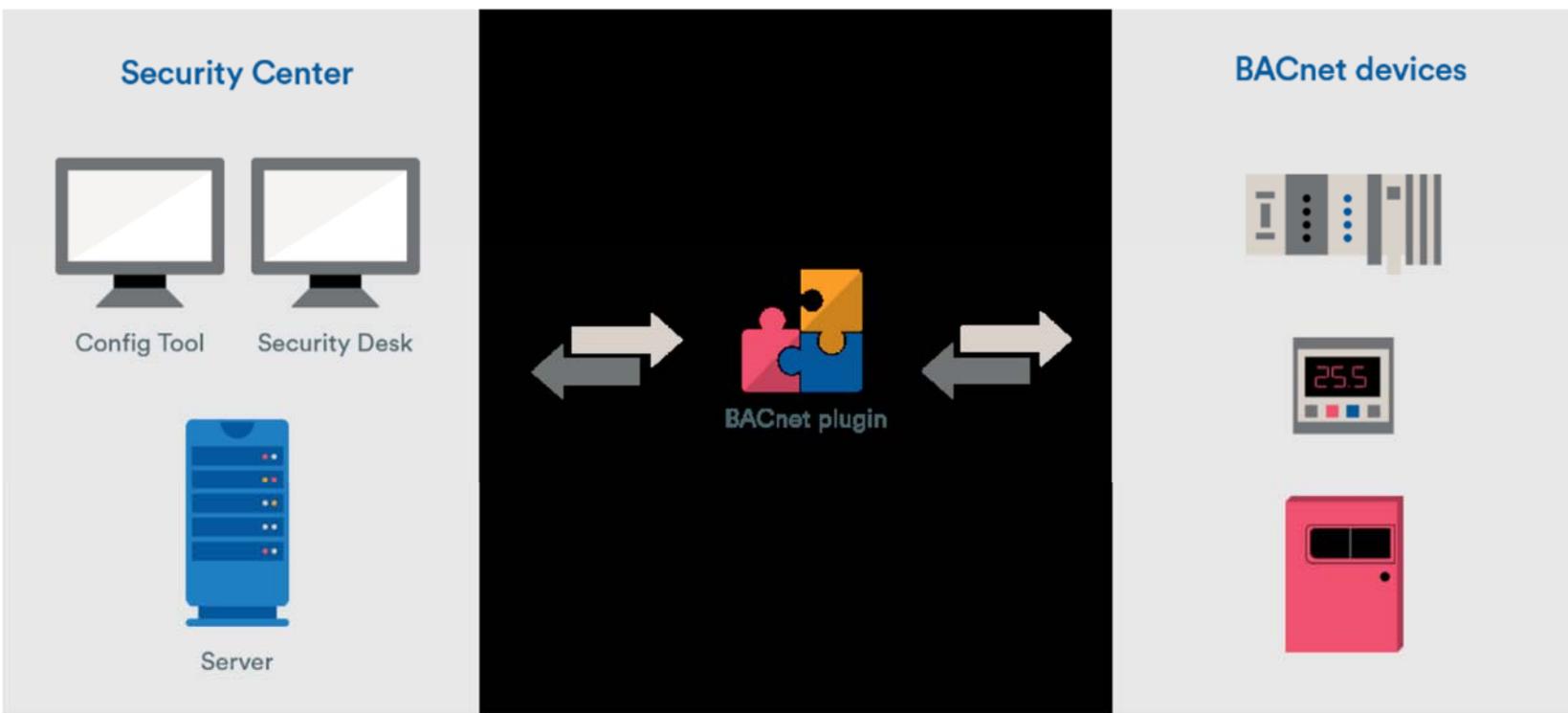
セキュリティセンターでエレベーターを管理することができます。プラグインを使用すると、次のことができます。

- Otis Compassプラグインの役割をCompassPlus™システムに接続します。
  - セキュリティセンターのCompassPlus™システムから宛先エントリデバイスを同期させます。
  - セキュリティセンターでエンティティ（フロア、着陸など）を作成して、その物理的な建物に合わせます
  - CompassPlus™システムによって管理されます。
  - 宛先エントリコンピュータ（DEC）のエレベーターディスパッチオプションを設定する。コンピュータの操作、許可されたフロア、アクセスルールなどが含まれます。
  - デフォルトフロアをカード所有者およびカード会員グループに割り当てます。また、特別フロアCompassPlus™システム。
  - DECのアクセスルールからカード所有者およびカード会員グループを除外する。
  - カスタムイベントとしてSecurity DeskのCompassPlus™イベントを受信して監視する。
  - CompassPlus™システムのエレベーターカーをセキュリティセンターのエレベーターエンティティにマップし、監視します
  - セキュリティデスクのエレベーターカーに関連するイベント。
  - 次のSecurity Deskレポートを使用して、過去のCompassPlus™システムのイベントを調査します。
  - エリア活動報告
  - エレベーター活動報告
  - カード会員アクティビティレポート
  - Otis Compassアクティビティレポート（プラグイン固有のレポート）
  - セキュリティデスクから手でエレベーターを発送する。
  - フロアのアクセス制御モードをSecurity Deskからロックおよびロック解除することによって変更します。
  - 乗客のグループに異なる発送規則を提供するために、建物を複数の区画に分割する。
- セキュリティセンターのスケジュール、アクセスルール、およびその他のエンティティの構成の詳細については、「セキュリティセンター管理者ガイド」を参照してください。イベントの監視の詳細については、監視タスクまたはSecurity Deskレポートの使用については、「Security Deskユーザーガイド」を参照してください。あなたはこれらにアクセスできます
- Config ToolまたはSecurity DeskでF1キーを押してガイドを表示します。
- CompassPlus™の用語がセキュリティセンターでどのように使用されているか
- CompassPlus™システムのエレベーター用語は、セキュリティセンターで次のように表されています。

# BACnetプラグイン

<http://www.bacnet.org/>

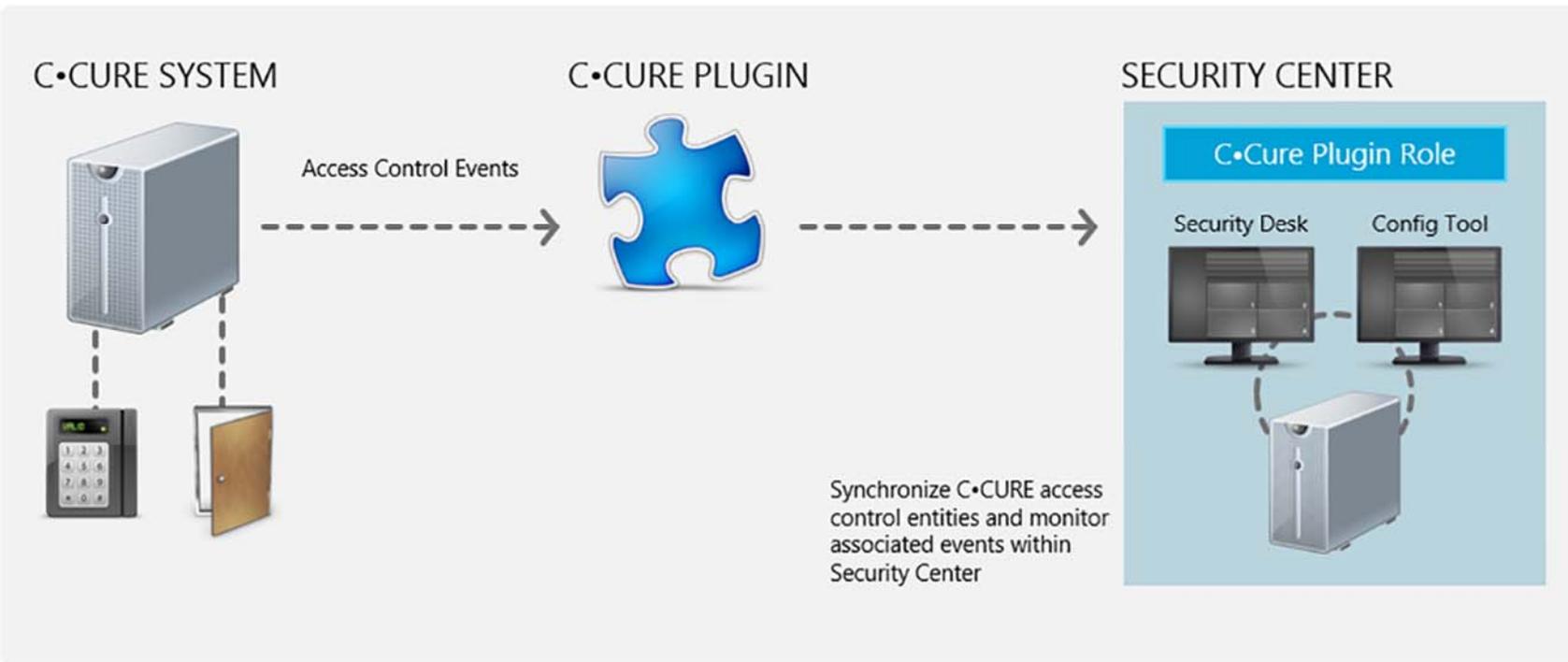
## BACnetプラグイン3.0とは何ですか？



BACnetプラグインを使用すると、セキュリティセンターでBAC（Building Automation and Control）デバイスやセンサーのネットワークを統合できます。プラグインを使用すると、次のことができます。

- 暖房、換気、空調制御、照明制御、アクセス制御、火災検知システムとそれに付随する機器の建物センサーを監視する。
- センサーからステータスを受信し、セキュリティセンターで自動的にイベントを生成します。
- センサーの状態をリアルタイムで表示します。
- トレンドの特定に役立つ履歴データのレポートを生成する。

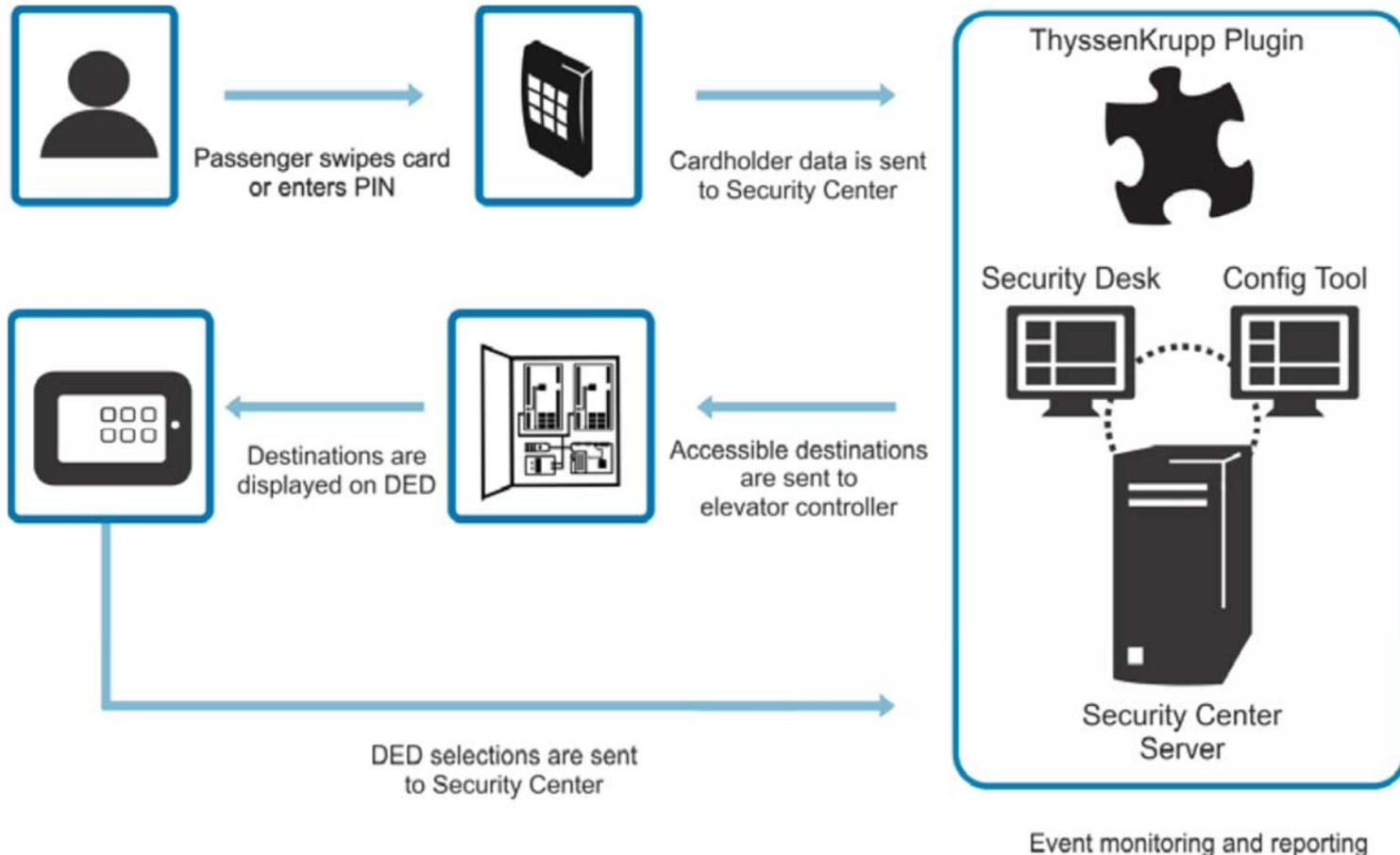
# C.Cure 9000



## ソフトウェアハウスC.Cure 9000とセキュリティセンタープラグイン

セキュリティ情報の管理を容易にするために、組織はビデオ監視とアクセス制御システムの統合を強化する必要があります。GenetecのC-CURE 9000プラグインは、Genetec Security CenterとSoftware House Cとの統合を提供します。C-CURE 9000アクセスコントロールソリューションにより、セキュリティセンター内のC-CUREアラーム、カード保有者、および資格情報を監視し、ライブおよび記録されたアクセスコントロールイベント。C-CUREプラグインは、C-CUREクライアントアプリケーションからセキュリティセンタービデオを表示する機能も提供します。

# ThyssenKruppプラグイン



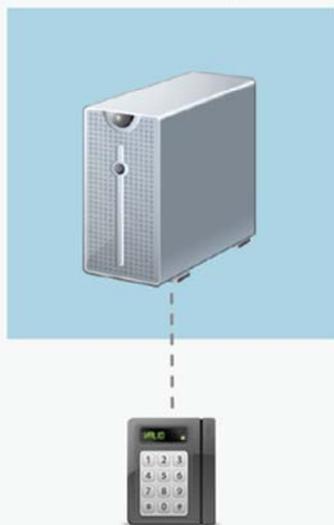
**ThyssenKruppプラグイン**は、セキュリティセンターの ThyssenKrupp Destination Dispatchエレベータシステムを Pluginルールを使用して統合します。テナントがカードをスワイプしたり、アクセスコントロールユニットのピン番号を入力したりすると、カード保有者のデータはセキュリティセンターに送られます。プラグインは、アクセス可能な着陸、エレベーター、エレベーターのドアのリストを ThyssenKruppエレベーターコントローラーに送信します。このコントローラーはThyssenKrupp DEDパネルに表示します。テナントは、DEDを使用して目的地を選択し、その選択に関連するイベントが監視され、レポートの作成に使用されるセキュリティデスクにライブで報告されます。

# Lenel OnGuard

## セキュリティセンターOnGuardおよびビデオトランスレータプラグイン

OnGuardプラグインとVideo Translatorプラグインは、Genetec™セキュリティセンターとLenel OnGuardアクセスコントロールシステムとの統合を提供します。オペレータは、OnGuardのアクセス制御エンティティ、アラーム、およびセキュリティセンター内のイベントを監視し、ライブおよび記録されたアクセス制御イベントから関連するビデオを表示できます。Video Translatorプラグインは、OnGuardクライアントアプリケーションからセキュリティセンタービデオを表示する機能を提供します。

OnGuard™ System



Alarm Acknowledgements and commands

Access Control Entities, Alarms and Events

OnGuard Plugin

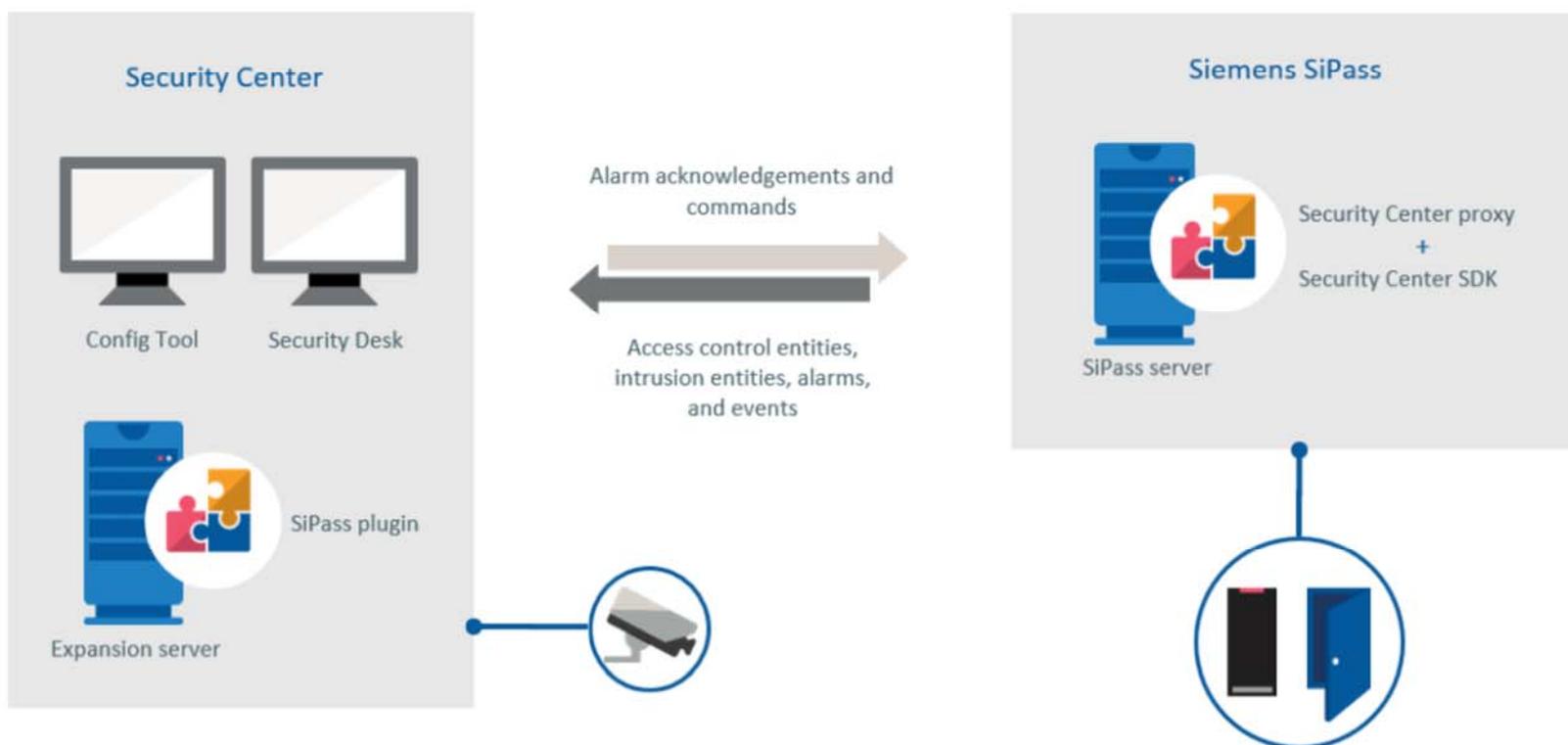


SECURITY CENTER System



Monitor Access Control Entities, Alarms and Events

## Siemens SiPass



### セキュリティセンター-SiPass Plugin 3.1

Security Center SiPassプラグインは、SiemensのSiPassアクセスコントロールシステムとGenetec Security Centerとの間のシームレスな統合を提供し、オペレーターがSecurity Desk内のSiPassアクセスコントロールイベントに関連するカード所有者およびクレデンシャル情報とともにライブおよび録画ビデオを見ることができます。

SiPassプラグインは、SiPassのアラームとイベントを監視し、応答し、レポートを生成し、Security Deskからアクションをトリガーする機能も提供します。

\*このプラグインはSiemensのみで販売されています

# Our partner add-ons

## Identification:

識別：顔認識、バイオメトリクス、IDスキャン。  
アクセスカードが不足している場合は、シームレスで侵入しないで安全な生体認証でエントリを制御します。  
顔認識技術によって人々を特定し、マルチファクタ認証を使用してセキュリティを強化します。

# Our partner add-ons

## Visualization:

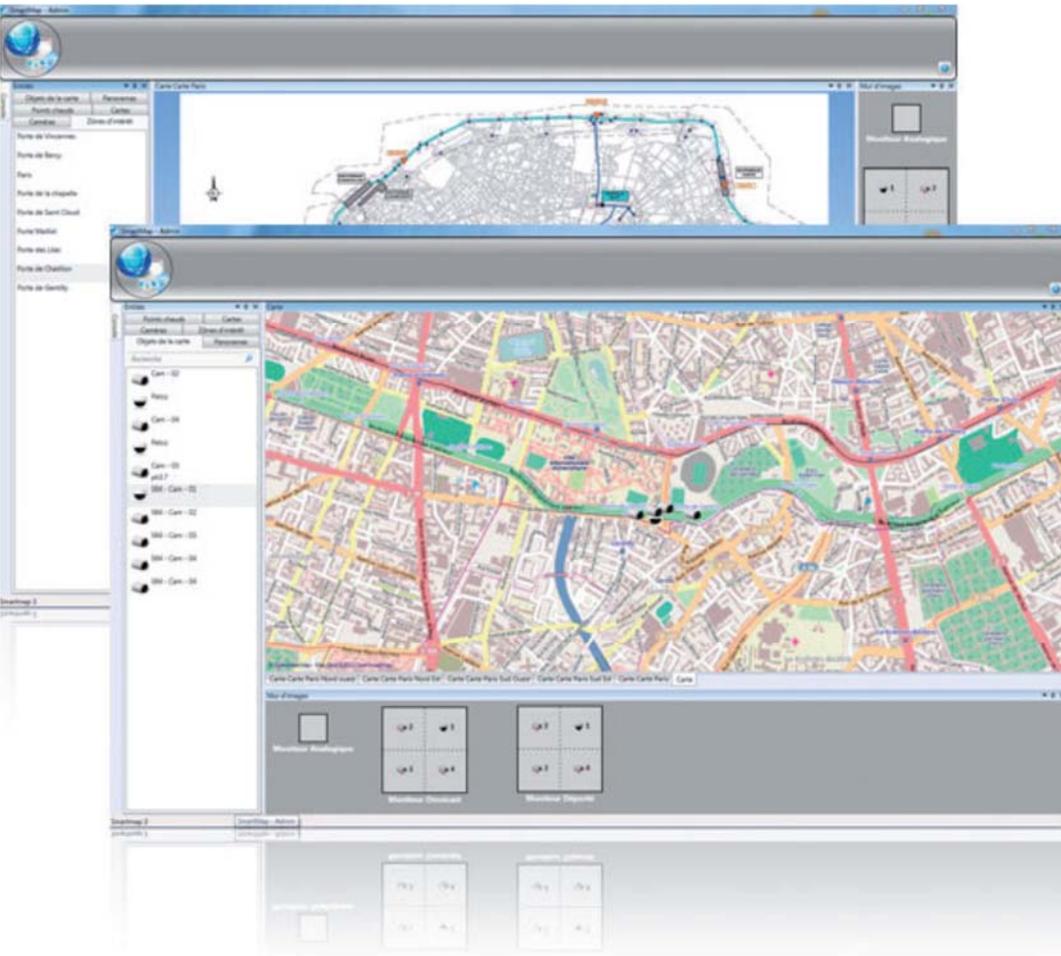
ビジュアライゼーション：ビデオウォール、ダッシュボード、AutoCAD

セキュリティ環境のインテリジェントで構造化されたビューを取得します。より多くのビデオ、画像、およびデータを表示するビデオ壁を持つ大きな画像を参照してください。セキュリティセンターとのシームレスな統合により、全体の状況認識が強化されます。

## Visualization:



## Visualization:



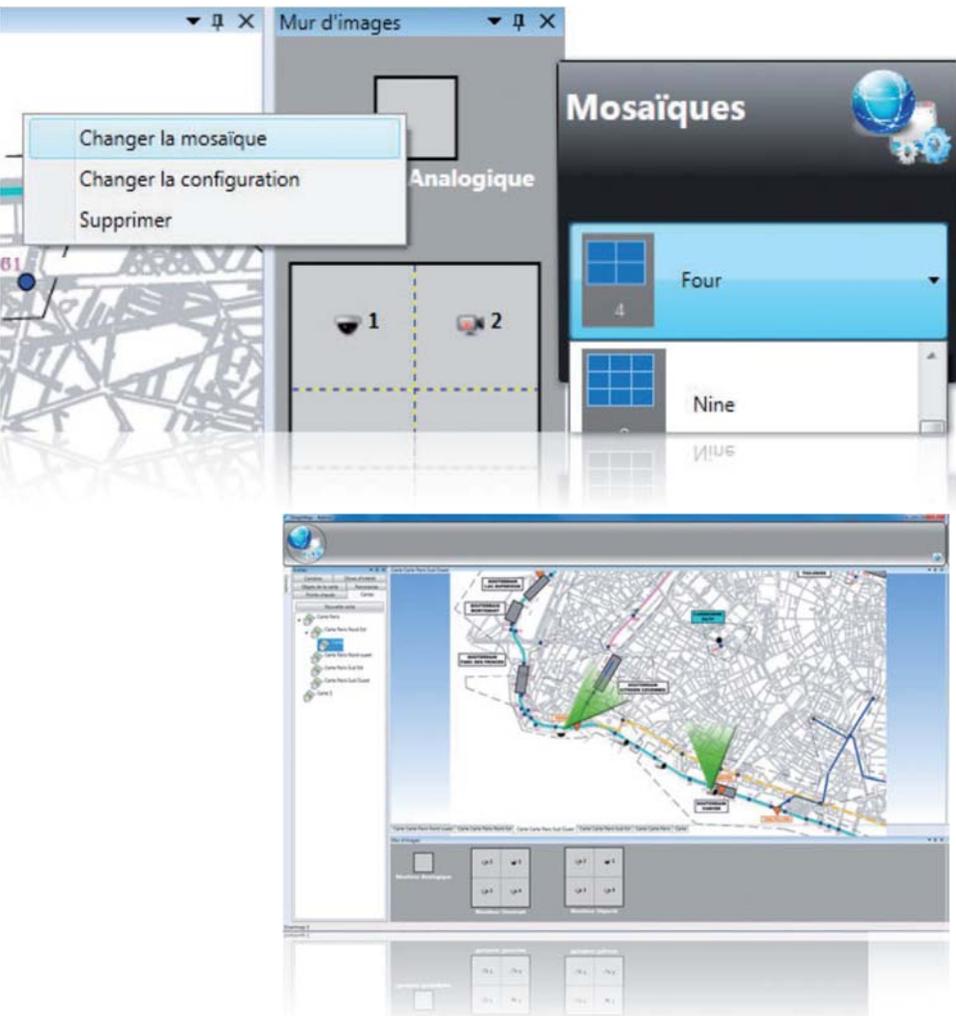
### Dynamic mapping

マッピングは、Google Maps、OpenStreetMap、Bing Mapなどのソースからエクスポートされ、マウスホイールを使用してさまざまなズームレベルを含む動的なインターフェイスを簡単に調整できます。

### Custom static map

このグラフィカルインターフェイスにより、BMPまたはJPEGファイルをSmartMapに統合することができます。また、AutoCADのアーキテクチャプランを使用することもできます。これらのマップは、ユーザーのためのマップとカメラのツリービューから利用できます。

## Visualization:



### Management of video wall

SmartMapを入手して既存のシステムに統合することで、ビデオウォールの動作を最適に監視および制御できます。マウスを1回クリックするだけで、デジタルカメラまたはアナログカメラの表示を監視できます。あなたのビデオウォールはあなたが自由に設定できる表示エリアを提供します。

### Display of the field of view

SmartMapと互換性のあるPTZカメラは、カメラが見た正確なエリアの地図上の表現から利益を得ます。監視する領域を瞬時に見ることができます。

## Visualization:

### Camera positioning

SmartMapは、180° マルチレンズカメラの視点からPTZカメラの位置を制御する機能を提供します。簡単なマウスクリックで、180° のビデオ画像にあるターゲットをズームするようにPTZカメラを制御することができます。

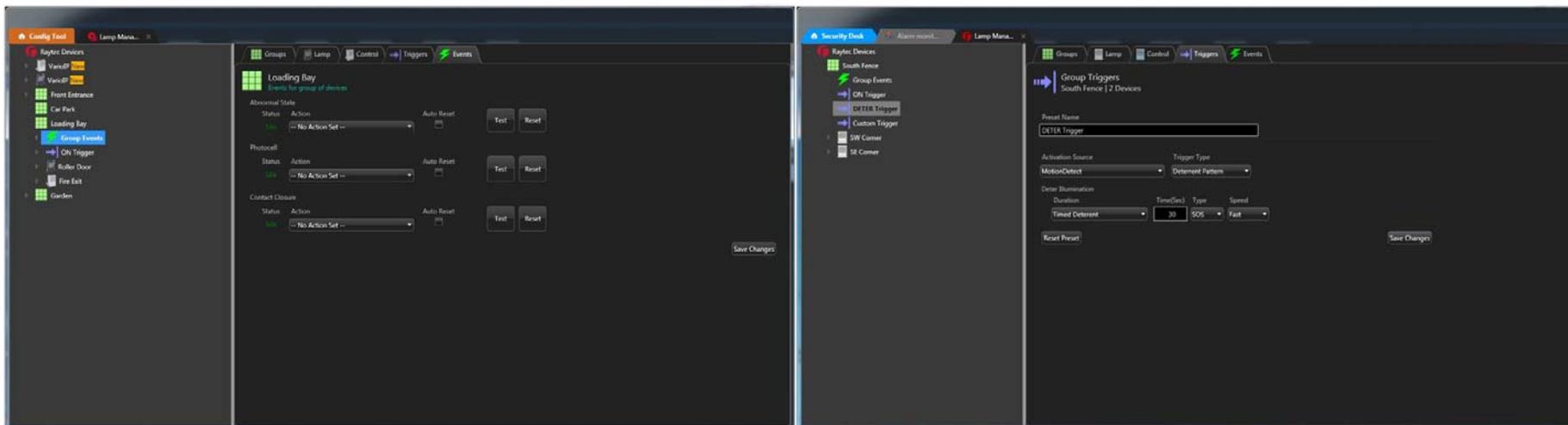




## Raytec VARIO2 IPネットワークイルミネータ



VARIO2 IPネットワークイルミネータのRaytec®シリーズは、Genetecのセキュリティセンターと完全に統合される世界初の監視照明です。簡単なプラグインソフトウェアを介して有効にすると、VARIO2 IPは簡単に応答するように設定できますか？セキュリティセンタプラットフォーム内の多数の異なるシステムデバイスによって駆動される複数のアラームに対応し、現場のイベントに対する最も視覚的で瞬時に対応します。



## Genetec Security CenterのVuWallのプラグイン

Genetec Security CenterのVuWallのプラグインにより、Matroxのセキュリティ監視用の強力なデコードが始まります

VuWallプラグインにより、セキュリティシステムビルダーは、[Matrox®Mura IPX高密度デコードカード](#)を統合して、数百のIPカメラを1つのビデオウォールに同時にデコードすることができます。このプラグインにより、システムオペレータはGenetecソフトウェアインターフェイス内の強力なVuWall2ビデオウォールソフトウェア機能セットにアクセスして、すべてのIPソースを管理することもできます。

新しい統合は、包括的でありながらも、セキュリティと監視に対するエレガントなアプローチを表しています。使い慣れたGenetecソフトウェアインターフェイスの下で作業することで、システムオペレータは簡単なドラッグ&ドロップ機能によってタイルレイアウトやムーブIPXでデコードされたコンテンツをビデオウォール上に遠隔で表示および制御できます。オペレータは、ライブビデオカメラのシーケンスを表示する必要があるか、ビデオサーバーからストリームを再生する必要があるかに関係なく、ビデオウォール上のビデオフィードを完全に制御できます。プラグインは、ビデオコンテンツに加えて、マップやWebページ、コントロールデータなどの非ビデオコンテンツを管理することもできます。これらのコンテンツは、すべてのソースとプリセットを制御して壁に表示することができるため、完全なエンドツーエンドネットワーク化されたソリューション



## AXIS Perimeter Defender 高セキュリティで拡張性に優れた周辺保護 Genetec Plugin



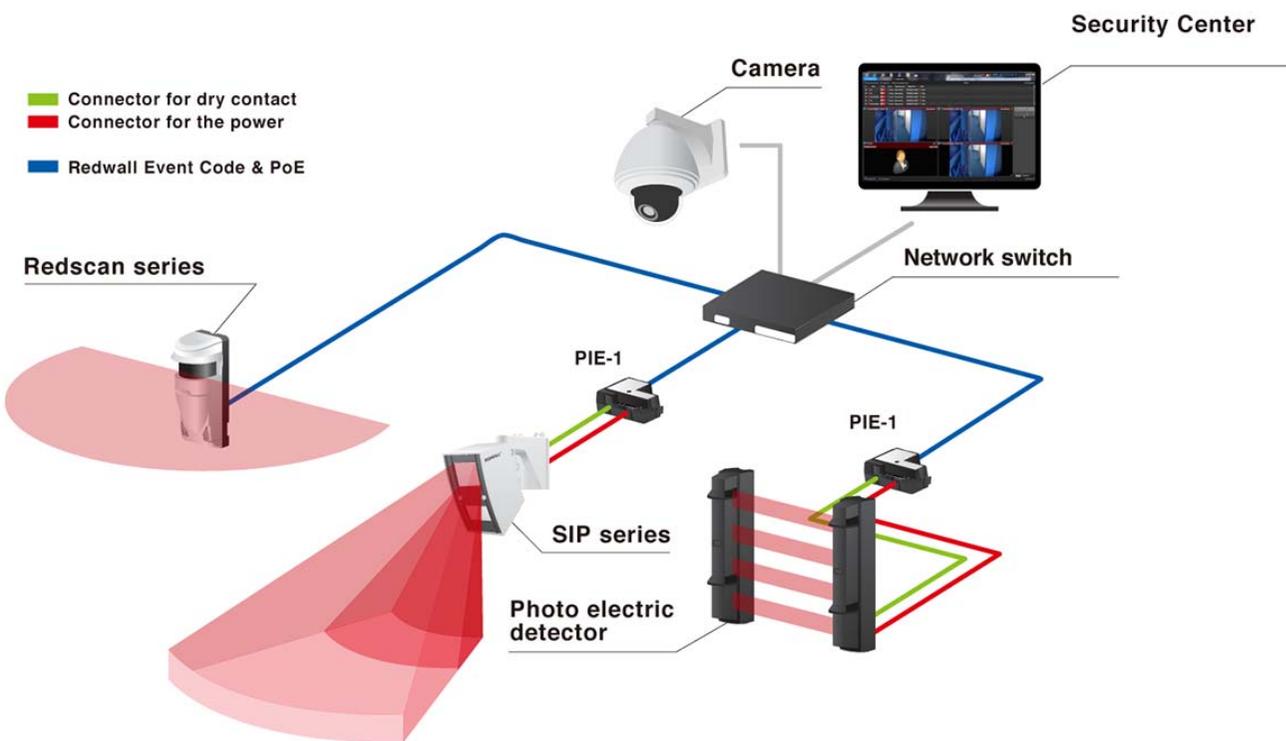
- 優れた検知精度と信頼性
- 拡張性の高い周辺保護
- 複数の検知シナリオ
- i-LIDS認定
- 簡単に直観的な設置



AXIS Perimeter Defenderは、施設の周辺でセキュリティの活動開始範囲を強化します。これは、化学プラント、発電所、刑務所、重要なインフラなど高セキュリティな施設において、物理的なアクセスコントロールを強化する場合に適しています。Axisのネットワークカメラ、ホーンスピーカー、およびビデオ管理ソフトウェアと合わせて使用することにより、AXIS Perimeter Defenderは効率のよい周辺保護における、映像による総合的なソリューションを構成します。また、立入制限区域監視用のプライマリ検知システムとして、i-LIDSの認定を受けています。

# Optex IP検出器による効果的な周辺セキュリティの実現

## Genetec Plugin



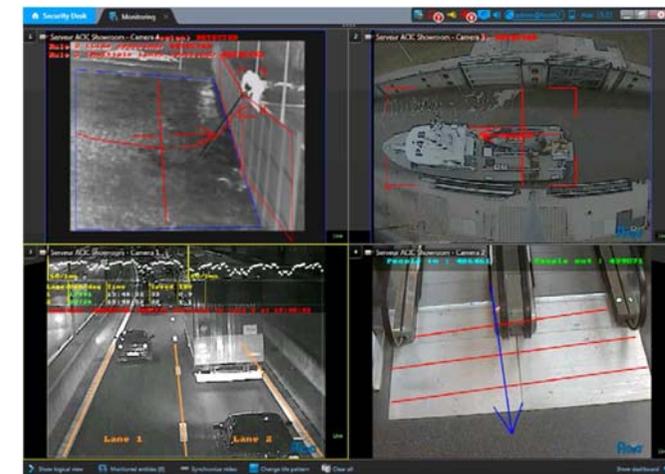
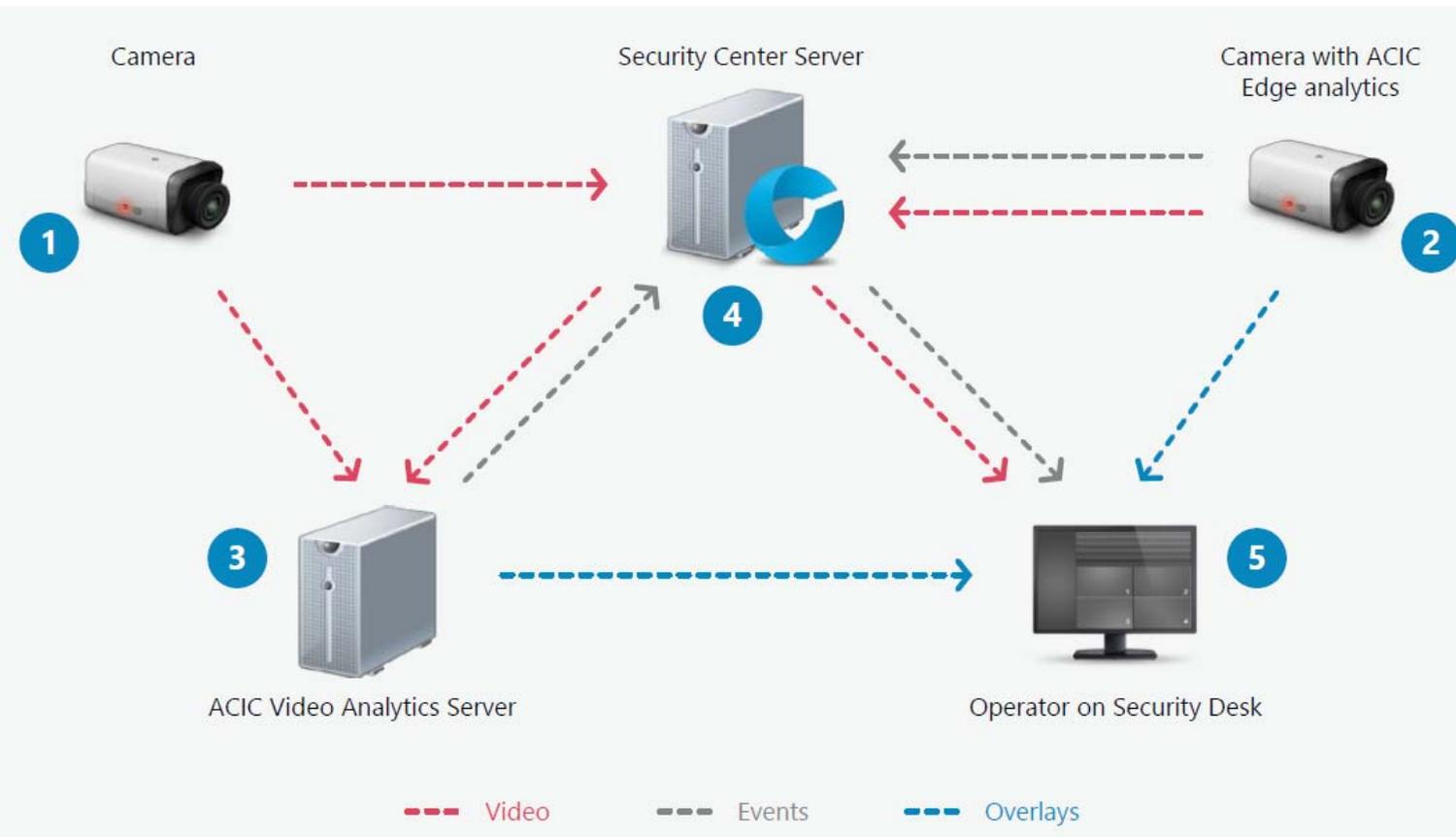
### Optex IP検出器による効果的な周辺セキュリティの実現

境界セキュリティのための効果的なIPビデオ監視を実現するには、多層の統合ソリューションが必要です。過酷な環境条件での動き検出のレベルを最大化し、誤警報率を改善することは、エンドユーザにとって重要な要素です。Optexの最先端のIP検出技術とGenetecビデオ管理ソフトウェアを統合することにより、境界セキュリティのための最高レベルのIPビデオ監視を提供することができます。

# ACIC ActivityDetectionおよびセキュリティセンター Genetec Plugin

## サポートされるアナリティクス

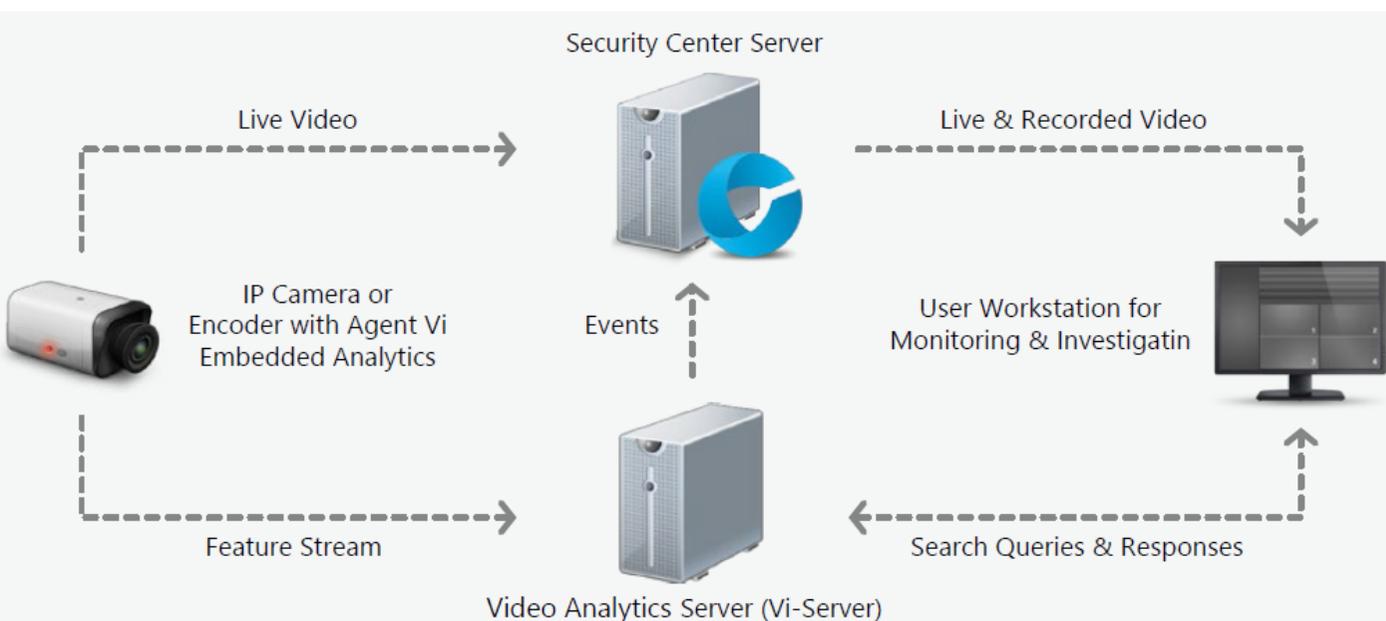
- ▶バーチャル・トリップワイヤー
- ▶移動方向
- ▶人数カウント
- ▶ロイター
- ▶車両特性
- ▶車両挙動
- ▶交通管理
- ▶持ち去り/放棄
- ▶カメラの改ざん
- ▶画像安定化
- ▶自動PTZトラッキング
- ▶落書き検出



## Agent Vi Video Analytics Solutions Genetec SDK

### サポートされるアナリティクス

- ▶ バーチャル・トリップワイヤー
- ▶ テイリング
- ▶ ムーブメントの方向
- ▶ 高度な動き検出
- ▶ 人数/群衆密度
- ▶ ロイター
- ▶ 車両特性
- ▶ 車両挙動
- ▶ 交通管理
- ▶ キュー管理
- ▶ 休止時間
- ▶ パスマップ
- ▶ ヒートマップ
- ▶ カメラの改ざん
- ▶ 画像安定化
- ▶ 自動PTZトラッキング
- ▶ 持ち去り/放置



## AllGoVision Video Analytics Solutions Genetec SDK



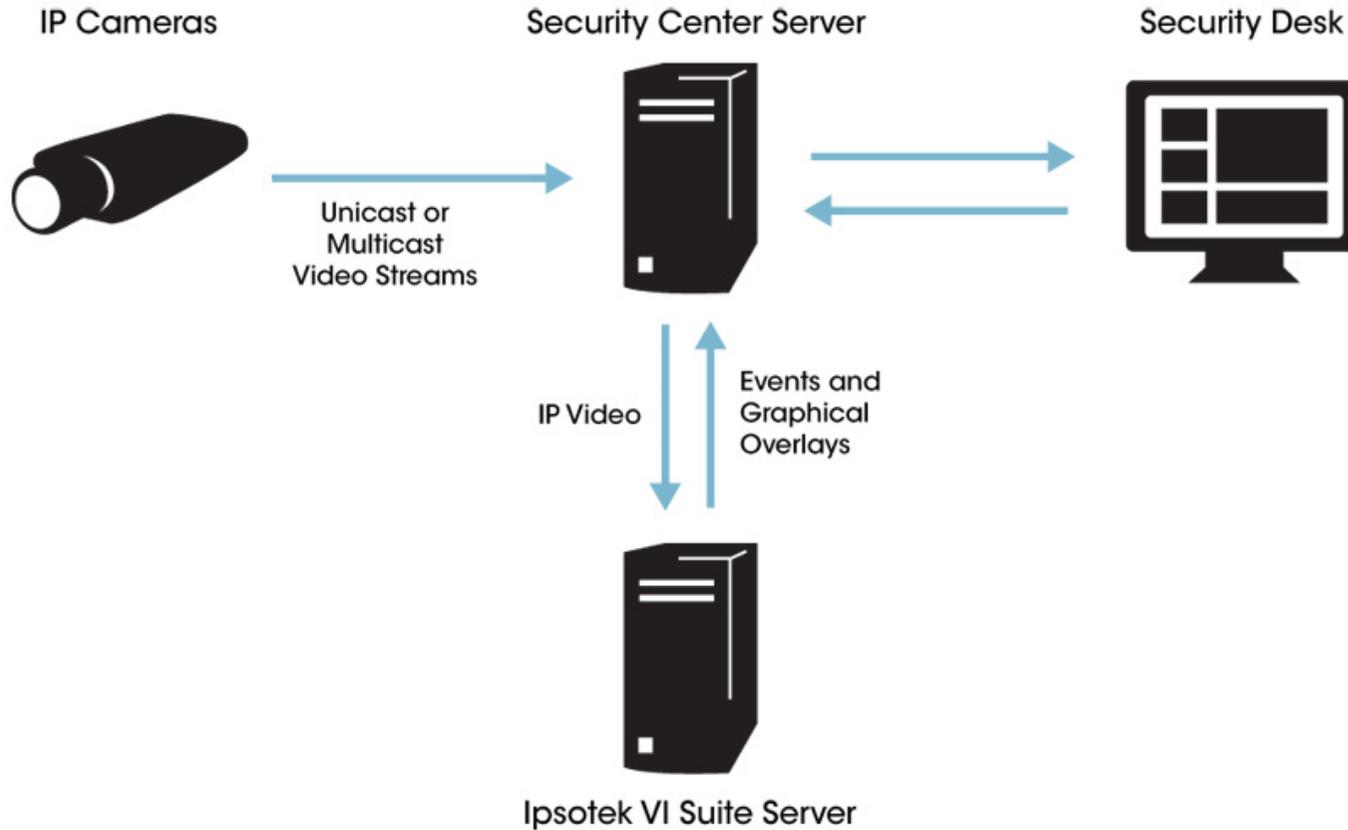
### サポートされるアナリティクス

- ▶ バーチャル・トリップワイヤー
- ▶ テイリング
- ▶ ムーブメントの方向
- ▶ ロイター
- ▶ プライバシーマスキング
- ▶ 車両分類
- ▶ 車速
- ▶ 車両の向き/間違った方向検出
- ▶ 車両数
- ▶ 持ち去り/放置
- ▶ オブジェクト分類
- ▶ ジオロケーション
  
- ▶ 顔認識

ジャバテル 国内代理店



# Ipsotek VISuiteとセキュリティセンター統合 Genetec Plugin



## Ipsotek VISuiteとセキュリティセンター統合

Ipsotekは、ビデオコンテンツ分析ソリューションVISuiteの基盤となる特許取得済みシナリオベース検出技術を開発しました。IpsotekのVI Suiteは、Genetecの統合セキュリティプラットフォームであるSecurity Centerと統合され、不審なイベントや動作を自動的に検出して対応する複雑なツールをユーザに提供します。セキュリティセンターでビデオイメージを使用して、数百台のカメラのコンテンツを分析し、リアルタイムでオペレーターの注意を掴んで、セキュリティセンターに直接アラームを送信します。セキュリティセンターでは、特定のイベントアラームを事前に設定したり、追加されたビジネスインテリジェンス用のレポートを生成することもできます。