都市空間の安全・安心を支える セーフティ・オペレーション

広明 敏彦

要 旨

ホームグロウンテロのような新たなタイプの犯罪は、従来の目視によるブラックリスト照合を中心としたモニタリングだけでは防ぐことが難しくなっています。今後は、ホワイトリスト照合に加え、各種AI技術を活用することで、人間だけでは発見や予知が難しい未知の異常を素早く検知し、新たなタイプの犯罪にも対処が可能になると考えられます。また、システムの設計も、防犯を主眼としたものから、平時における現場の管理を中心としたものへとシフトすることで、より多くの価値が創出できると見込まれます。本稿では、これら都市空間の安全・安心を支える監視ソリューションや、その基礎となる技術の進化に関するNECの見解を概説します。

KeyWords
映像監視／ビデオサーベイランス／パブリックセーフティ／センシング／見える化／認識技術／人工知能(AI)／データマイニング／犯罪・テロ防止

1. はじめに

世界的に都市への人口集中が続いているといわれて久しく、都市部に暮らす人口の比率は7割を超し、2050年にはその割合が9割近くに達するという予測もあります。その急速な都市化に社会インフラの整備が追い付いておらず、交通渋滞などのさまざまな社会問題が生じていますが、都市型犯罪の増加もそうした問題の1つです。

都市には農村や国外から多様な人が集まり、かつ所得格差や貧困などの要因も加わることで、地域への帰属や仲間意識が希薄になりやすくなっています。その結果として、地域全体としてのコミュニティ形成や自治、見守りが困難となり、犯罪への心理的な障壁も低くなっていると考えられています。また、犯罪者にとっても、人口が集中している都市はターゲットを探しやすく、テロなどの破壊の効果も高いなど、犯罪を実行する場として有利に働きます。

犯罪増加への対策には、警備力や警察力の強化が挙げられますが、各自治体の財政状況から、一般に警察官の大幅な増員は困難です。その解決策として、近年、ITを活用した監視や警備の増強への関心が高まってきています。その典型例がビデオカメラによる監視システムの導入です。ロンドンなどが代表例としてよく知られており、市内の各地に監視用のビデオカメラを配置し、防犯センターで監視員が集中的に各地から送られてきた監視映像をモニタリングし、異常発生をいち早く察知、対処しています。現在、ロンドン市内には約60万台を超えるカメラが設置され（英国全体では500～600万台と推計）、防犯や犯罪捜査に貢献しているといわれています[1)]。

しかし近年、新たなタイプの犯罪による脅威が、安全で安心な都市での暮らしの実現に暗い影を落とし始めています。それら犯罪は、従来の監視体制、すなわち、エリアが限定的で、かつ、目視を中心としたモニタリングでは対処が困難です。また、社会に対するより大きなマイナスのインパクトは、都市への脅威にとどまらず、むしろ国家に対する脅威として位置付けられるべきものとなってきています。その対処には、組織や機関、国家の壁を越えて連携しながら、より広域を常時、素早く細やかに監視・警戒する仕組みが求められます。

2. 新たなタイプの脅威

近年、若者や社会との関わりが薄く社会的に疎外感を抱いている者が、インターネットなどを通じてテロ組織などの過激な思想に触れ、その影響を受けてテロを含む凶

悪な犯罪を行う問題が生じています。例えば、2013年に起きた米国ボストンでのマラソン大会における事件に見られるように、自国民が自国民を対象にテロ行為をする「ホームグロウン・テロリスト」や、個人が組織に属さずに単独で大規模なテロ攻撃を行う「ローンウルフ」といった新たな形態のテロが起こるようになってきました[2)]。これからはインターネットの更なる普及を背景に、世界規模でこの種の犯罪の増加傾向は強まってくると考えられます。

この新たな形態のテロへの対策を困難としているのが、犯罪を起こす印象が薄い人間を実行犯として選ぶようになってきている点です。実行犯が初犯や低年齢の子供の場合には、従来のような、被疑者をブラックリストに登録して対象人物を限定し、その人物の発見に注力するといった対策では防ぎきれなくなります。

更に、犯罪を計画する者とテロ組織との接触も、インターネットを経由する場合には察知が困難なため、犯罪を防ぐには、凶器や爆弾の準備活動、あるいは犯罪を想起させる不審な行動などを察知し、犯罪を起こす可能性を推定して警戒する必要があります。しかし、これら活動は、一般人による大多数の正常な活動に埋もれてしまうため、異常な活動としての発見や分離が困難です。

テロ組織の活動も巧妙化しており、例えば2009年7月に起きたインドネシア・ジャカルタにおけるホテルへのテロ攻撃に関しては、ホテル側が正面エントランスにおいて金属探知機や荷物検査を厳重に行っていたにもかかわらず、テロリストが花屋を装い、従業員通用口から爆弾を事前に持ち込んでいたことが判明しています[3)]。

このように、犯罪の多様化と広域化が進むなか、これら新たな犯罪の脅威に対抗するためには、これまでの常識的な想定を越えて、より広範囲を常時、細やかに見守ることができる、高度で柔軟な犯罪対策が必要になっています。他方、犯罪はいつどこで起こるかがはっきり分からず、際限なくその対策に高いコストが掛けられないという実情もあり、新たな防犯対策に対しても、効率や経済性に対する十分な配慮が求められます。

3. 脅威への対抗策

3.1 ホワイトリストの活用

前述のように、これまでは、犯罪歴がある、あるいは犯罪組織への所属が疑われる人物のブラックリストを作成し、その登録者を早期に発見・追跡して行動を観察することで、犯罪の計画や実行を阻止するという対策が一般的でした。ブラックリストの登録者数は、一般人の数に比べて十分に少なく、その点で、出入国時や施設でのゲートにおけるブラックリスト照合による監視は、効率の面でも極めて有効な対策となっていました。

しかし、ホームグロウンテロのように、ブラックリスト照合では防げないタイプのテロに対しては、基本的にはまったく逆のタイプの対策、すなわち、不特定多数の人物を対象にその行動の不審性の有無を評価するような、網羅的な監視が必要となります。その一例に、ホワイトリストをベースとした対策が挙げられます。

ホワイトリストとは、身元が定かであり危険性が無いと判定された人物のリストのことです。多数派となるホワイトリスト登録者をいち早く特定して追跡対象から除外し、かつ、その結果としてホワイトリストに登録されていない人物（グレーリスト）に対する観察や解析により多くのIT資源を投入し、その挙動を細やかにモニタリングしながら、犯罪を起こす可能性の判断精度を高めることを目指します（**図1**）。

最も単純な例としては、対象者を事前に審査し、その合格者に対して何らかの認証手段（IDカードなど）を、保全義務（紛失したり盗まれたりしないなど）を課して付与し、その認証手段の登録者一覧をホワイトリストとするものがあります。出入り口にゲートを設置して、関係者が全員、カードによる認証を行うというのも一種のホワイトリスト型の対策といえます。

このIDカードの代わりにバイオメトリクス（指紋認証や顔認証）などを活用し、更に、立ち止まらずに済むウォークスルー型の認証もあわせて実現できれば、カードを常に携行して入退場のたびに機械へカードをかざすといった積極的な認証行為が不要になります。一般に、認証用ゲート

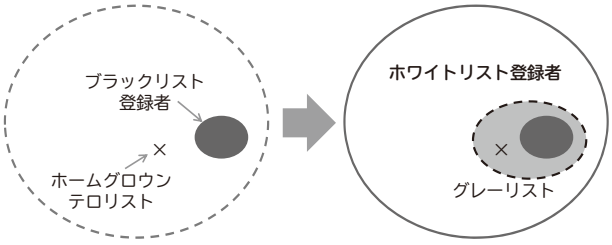


図1　ブラックリスト照合からホワイトリスト照合へ

の設置は人の流れを妨げ、混雑の原因となりやすく、かつ、その設置コストも高額です。そのため、人の往来が激しい場所においてホワイトリスト型の対策を行うには、ゲート設置を必要としない、あるいは人の流れを妨げないウォークスルー型の認証の実現が望まれます。

ただし、このようなホワイトリスト照合を実現するためには、その前提として、ブラックリスト照合の場合よりもはるかに多数のホワイトリスト登録者に対して、精度の高い個人認証を高速に行える必要があります。また、プライバシーの問題も十分に配慮し、個人を特定する情報の厳密な管理策を講じるほか、個々人への利益の還元も図るなどして、ホワイトリスト照合を用いた犯罪やテロ対策への理解を得ることなども不可欠です。

より完全な安全性が求められる場合には、ホワイトリスト型対策に加えて、更にホワイトリスト対象者をも含む全員の行動を観察し、その不審性を評価することになります。この場合は、前述した固有の認証手段を前提としないので、IDカードの偽造や盗難によるなりすましまで想定した対策となります。しかし、対象者全員の行動を長時間にわたり観察することは処理負荷が膨大となるため、大規模な監視には不向きといえます。実際には、立ち入りが限定された少人数のみを対象としたり、ホワイトリスト登録者向けの監視は重要項目のみに絞り込んだりといったことが必要になります。

3.2 犯罪の予測・予知

2002年に公開されたSF映画『マイノリティー・リポート』[4]には、近未来における管理社会が興味深く描かれています。この作品では、犯罪を予知できる3人の超能力者によって未来殺人者を事前に特定し、その未来殺人者が殺人を犯す前に逮捕できるシステムの確立で、殺人犯罪がまったく起こらなくなった社会が描かれています。また、作品中では計画的な殺人と激情的で突発的な殺人とが区別され、激情的な殺人は直前でなければ予測できないとされています。

現実の世界においても、突発的な事件はやはり予測が困難だろうといえます。しかし、犯罪の計画や、犯罪へつながる確度が高く、その予兆と判断がつく行動・イベントが特定できるものは、ある程度の犯罪の予測が可能になると見込まれます。したがって、ITを活用した犯罪の予測や予防について考える場合も、“予兆”と見なせる特定の振る舞いやイベントをいち早く発見することが最初の目標となります。

まず、計画性のある犯罪の予測について、犯罪計画の察知は、例えばテロ行為であれば、準備段階において爆発物の材料の入手や、犯罪実行に向けた臨時の移動手段の確保、更には現場の下見活動などを発見することが挙げられます。そのほか、凶器となる物品の購入、犯罪組織との接触、インターネット上での犯罪予告書き込みなども、犯罪の兆しとしての手掛かりとなり得ます。これら犯罪につながる典型的な準備活動や事前行動に関する知識は、一種の犯罪モデルを成立させ、かつ、このモデルに基づく犯罪の予測や予知の実現につながります。また、要人が集まる国際会議や大型のスポーツイベント・フェスティバルなどはテロの標的になりやすいため、まずは、これら重要イベント向けの対策技術を優先的に開発し、イベント会場やその周辺において、人的あるいはITによる警備資源や警察活動を、動的かつ迅速に制御し展開できるように支援することが求められます。

他方、計画性のない犯罪の予測について、突発的な犯罪やまったく新たな手口による犯罪は、従来のデータとしての蓄積が無く、したがって犯罪発生のモデルも作りにくいため、その予測自体も困難です。犯罪の発生場所の事前予測や特定ができないため、可能な限り広域を監視しながら、何らかの異変を素早く検知するような対策とならざるを得ません。そのため、ITを活用することで複数の現場をモニタリングし、各地における新たな異常の発生や、異常につながるようなわずかな変化をいち早く捉え、かつ、これら新規の異常が犯罪へ発展するのかについて、その可能性をより早い段階において正しく予測して判定することを目指します。

ここで重要となるのが、監視システムにおいても、人間が行っているのと近いレベルで「現場における違和感」を検知することです。違和感とは、平常や平時からわずかに逸脱した状況の知覚、あるいはそれに基づく異常性や不快感、危険性などを認知することです。つまり、平時の観察の蓄積に基づき「正常状態」の範囲を定義し、その範囲からどの程度まで逸脱した状況を「異常」と判定してアラートを挙げるのかという問題になります。これは、環境の正常さを正しく判定できるモデルを構築して、そのモデルに基づき、発生頻度が少ない異常やまったく新規に発生したような異常をも判定できるようにすることだといえ、犯罪のように発生頻度が低いイベントを検知する場合には重要

な考え方となります。このような異常性の判定には「インバリアント分析技術」[5]などが応用できると考えられ、犯罪の予知・予測に対してもこれら技術の適用が期待されます。

また、上記の考え方の背景には、機械学習技術は本質的に大量の学習データを必要とするため、学習データを得にくい異常イベントよりも、得やすい平常系のイベントをベースにした方が有利であることが深く関係しています。現場環境の観察を自動化し、正常か異常かを判定するようなシステムを構築する場合には、一般的に機械学習技術を利用しなければなりません。しかし、機械学習の性能は、基本的に学習データの良し悪しに強く依存するので、発生頻度が少ない犯罪に対しては、学習用データが十分に確保できません。したがって、検知精度が高められないことが予想できます。学習データをシミュレーション合成によって生成する方法も考えられますが、犯罪のあらゆる可能性をシミュレーションすること自体が難しい課題であり、それよりも日常状態を判定し、そこからの逸脱を検知する方が合理的なアプローチだといえます。

4. 経済性への配慮

4.1 平時の管理を中心としたシステム設計

セーフティ向けの監視システムは、従来、異常の検知を目的とした設計が中心でした。そのため、ほとんど発生しない「異常」なイベントを正しく検知できるのか、また、その検知精度自体をいかにして正しく評価するのか、という難題が常に付きまとっていました。しかし、仮に犯罪の多発地域であっても、犯罪が起こった有事よりも、犯罪が起こらない平時の時間が長いはずです。むしろ現場では、犯罪や異常の検知よりも、本来の業務の効率化に向けて、人や物品を正確に管理することの方が重要だという場合が少なくありません。また、前述のように、異常とは正常の裏返しのイベントであり、正常状態であることを正確に把握できているのであれば、異常の検知もまた正確に行える可能性が高まります。

システムの投資回収の側面から見ても、システムの目的や機能を、いつ発生するかが分からない異常に限定して設計するのは有効とはいえません。平時における機能をメインとし、同時に有事にも対応するシステムとして設計する方が、投資対効果の面で有利となります（**図2**）。例えば、従業員を管理するためのシステムは、従業員以外の判別にも使えるため、外部の人間の侵入防止としても働きます。また、環境下の物品の全品管理が可能であれば、登録に無いものは異物として検知が容易になります。それは、都市全体の安全・安心に向けたセーフティシステムでも同様で、都市の平常時における効果的な管理や制御を目的とした機能と、発生頻度が少ない犯罪・テロを防ぐことを目的とした機能とが統合した、両者が共存するようなシステム設計が有望視されます。

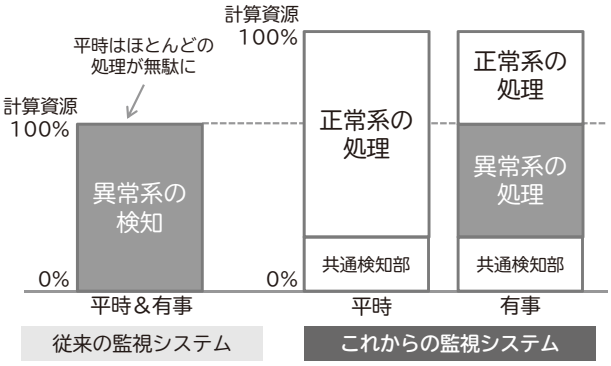


図2　平時向け用途を中心としたシステム設計

ただし、平時向けの用途と有事向けの用途では、直接的な受益者や管理者が異なるため、双方の機能が統合されたシステムの実現は多くの困難を伴います。システムを利用する関係者間の調整が不可欠で、特に、異なる機関や会社間での情報共有はさまざまな問題が生じやすいため、システム側で安全性と利便性とをうまく両立させる仕組みを提供することが求められます。

4.2 都市をまるごと管理

ホームグロウンテロやローンウルフといった新たな脅威へ対抗するには、都市全域あるいは国全体を想定したレベルで、主要都市や重要施設、道路、鉄道などの交通インフラをカバーし、犯罪の予兆をも素早く検知できる監視システムの実現が望まれます。

しかし、これを設置場所が定まった固定的なセンサーを中心に実現しようとすると、センシング範囲を確保するために各地に多数のセンサーを配置しなければならず、多大な設置コストが掛かります。むしろ、固定的なセンサーと移動型のセンサーとを組み合わせ、より広域を効果的に管理できる仕組み作りが有効になります。移動型センサーには、自動車やドローンなどにセンサーや通信手段を搭

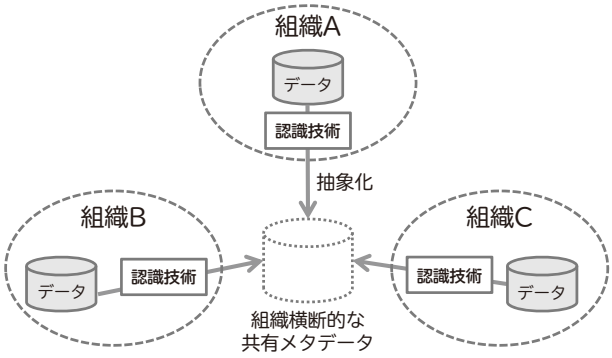


図３　組織横断的な監視データ共有の例

載する以外にも、スマートフォンなど携帯型端末上のセンサーの活用も考えられます。

また、既設の固定型センサーも、組織同士が連携して監視情報を共有できる仕組みを作ることで、より広域を監視できるようになります。しかし、そのためには、各組織が保有するデータを適切に抽象化して、モニタリングに必要な情報を共有できるようにする各種認識や解析技術の活用が求められます。例えば、各組織のセンシングデータをそのまま共有するのではなく、認識技術を介して共通の構造を持つ抽象度が揃ったメタデータへ変換し、それを共有するような方法がこれに当たります（**図3**）。

5. おわりに

都市空間の安全･安心を支える次世代の監視ソリューションや、それを支える技術・システムの今後の進化について、NECのビジョンを概説しました。従来の目視によるブラックリスト照合を中心としたモニタリングでは、初犯者を中心とした新たなタイプの犯罪を防ぐことが難しく、今後は豊富な計算資源の利用を前提としたホワイトリスト照合に加え、各種AI技術の活用により新たな異常を素早く検知し、従来は人間だけでは発見や予知が難しかった新たな犯罪への対処が可能になっていくと考えられます。また、システムの設計思想も、防犯を主眼としたものから、平時における現場の管理を中心としたものへシフトすることで、より多くの価値を生み出すシステムが実現できると見込まれます。

NECはこれらビジョンに基づき、世界各国における都市や国家の安全・安心を支えるための、新たな技術やシステム、ソリューションの開発を進めていきます。

参考文献

1）セキュリティ産業新聞：イギリス・ロンドン市における防犯カメラの現状について，第８回日本防犯設備協会特別セミナー，2008.10
http://www.secu354.co.jp/contents/seminar/08/seminar-081010-4.htm
2）公安調査庁：「ホームグロウン・テロリスト」の脅威，国際テロリズム要覧（Web版）
http://www.moj.go.jp/psia/ITH/topic/2015_topic_01.html
3）友次晋介：都市部へのテロ対策の課題 ―アジア太平洋国土安全保障サミット報告―，RISTEX CT Newsletter Issue 第８号，2010.2
https://www.ristex.jp/aboutus/enterprize/trust/terrorism/pdf/NewsLetter08.pdf
4）20th Century Fox：Minority Report
http://www.foxmovies.com/movies/minority-report
5）NEC：ビッグデータ活用を支える最先端AI技術
http://jpn.nec.com/bigdata/analyze/index.html

執筆者プロフィール

広明 敏彦
データサイエンス研究所
所長代理

NEC 技報のご案内

NEC技報の論文をご覧いただきありがとうございます。
ご興味がありましたら、関連する他の論文もご一読ください。

NEC技報WEBサイトはこちら

NEC技報(日本語)　　NEC Technical Journal(英語)

Vol.69 No.1　AIによる社会価値創造 ～NEC the WISEの世界～

AIによる社会価値創造特集によせて
AI時代における社会ビジョン ～人々の働き方、生き方、倫理のあり方～
NECが目指すAIによる社会価値創造

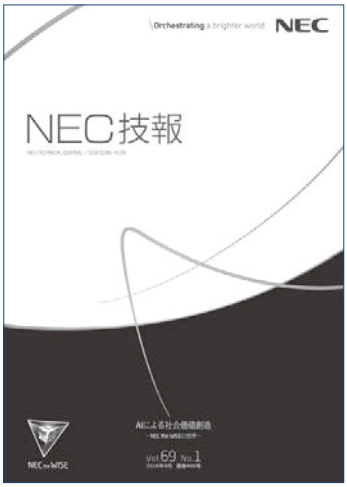
◇ 特集論文

NECが目指す社会価値創造像
都市空間の安全・安心を支えるセーフティ・オペレーション
新たな消費エクスペリエンスを提供するリテール産業オペレーション
都市交通サービスにおける「NEC the WISE」
第四次産業革命を支えるインダストリー・オペレーション

NECが誇る最新のAI技術
リアルタイム監視を実現する動画顔認証技術
社会インフラの保全を効率化する光学振動解析技術
IoTの活用を広げる物体指紋認証による個体識別
未知のサイバー攻撃を自動検知する自己学習型システム異常検知技術（ASI）
防犯カメラ映像から未登録の不審者を見つけ出す時空間データ横断プロファイリング
きめ細かなマーケティングの実現に向けた顧客プロフィール推定技術
要因分析エンジンを用いた工場・プラントでの品質管理
予測から意思決定へ ～予測型意思決定最適化～
REFLEXによるバス運行の動的最適化

最先端のAI技術開発におけるNECのオープンイノベーション活動
脳の「ゆらぎ」を応用した超低消費電力のコンピュータで「おもろい社会」を実現
アナログ回路の活用により本物の脳を再現する「ブレインモルフィックAI」とは
AIとシミュレーションを組み合わせ、データに乏しい状況でも意思決定を可能に

AI技術ブランド「NEC the WISE」



Vol.69 No.1
（2016年9月）

特集TOP