米国における防犯・治安と IT に関する取り組みの現状

八山　幸司
JETRO/IPA New York

1　はじめに

今月（2015 年 11 月 13 日）パリで同時多発テロが発生して多くの犠牲者がでた。まず、この場をお借りして、犠牲になられた方々に対し哀悼の意を表したい。またパリ以外でも最近テロが頻発し、日本でいつおきてもおかしくない状況であり、今後ますますテロや犯罪に対して警戒を高めていくことが必要である。これまで犯罪捜査・治安の取り締まりやテロ・犯罪の未然防止のために様々な技術が投入されてきたが、IT を活用することによる、より高度な防犯・治安の取り組みが進んできている。これまで監視カメラや犯罪データを使った取り組みは取り締まりのサポート的な役割として使われてきたが、近年では、ネットワーク化された数千台の監視カメラが地域を監視し、ビッグデータを使った分析が犯罪の発生する地域を事前に予測するなど、IT が防犯と治安の要になろうとしている。さらに、IoT の発達によりホームセキュリティもスマート化が進み、利便性が高く強固なセキュリティが実現している。今号では、高度な IT を取り入れた犯罪対策を進める、米国の防犯・治安分野の IT 化について紹介する。

最初に、米国における IT を活用した防犯と治安の事例について紹介する。かつては高い犯罪率で有名であったニューヨークだが、様々な取り組みによって現在では米国でも最も安全な大都市の 1 つになっており、特に近年では最新の IT を取り入れた地域警戒システムや顔認識技術等さらなる取り組みを進めている。他州の警察機関でも IT の活用が進み、ビッグデータを使った犯罪予測や飛行機を使った監視システムは複数の警察機関で利用されている。

次に、防犯と治安に関連した市場について紹介する。監視カメラと関連したサービスの市場では、IP ベースの製品の普及によって 2020 年までに 489.5 億ドルに拡大すると見られ、特にクラウドを活用したサービスに注目が集まっている。ホームセキュリティの市場も 2018 年までに 24 億ドルに達すると見られ、IoT の普及によりすでに多数の企業が参入し始めている。

最先端技術では、動体解析、映像解析、セキュリティロボットについて紹介する。マサチューセッツ工科大学は壁の向こう側にいる人物の動きを高い精度で知ることが出来る技術や、映し出された物体の映像解析により周囲の音を再現することに成功している。Placemeter 社では、詳細な交通量の計測が出来るシステムを開発しており、人の流れが多いイベント会場などでの使用が期待されている。セキュリティロボットでは、Knightscope 社の建物内外を警備する自律ロボットや、Liquid Robotics 社の自家発電しながら海中を自律航行できるロボットについて取り上げる。

最後に、防犯・治安と関連する米国における監視とプライバシーの問題について取り上げる。米国のプライバシー問題はテロ対策を目的とした監視活動と大きく結びついており、人々のプライバシーに対する考え方は、同時多発テロやスノーデン事件などをきっかけに大きく変化してきた。また、監視システムの全国的な運用指針は示されていないことから、各警察機関では憲法に記された原則に基づいた取り組みが進められている。高速道路の自動精算システム E-ZPass についても本来の目的外の使用が疑われており、非難の声が上がっている。

米国はテロ対策を目的として犯罪に対して強い姿勢で取り組み続け、様々な IT を防犯と治安に導入してきた。しかしながら、スノーデン事件を機に政府がプライバシーをおろそかにしているのではないかという声が上がり、監視システムとプライバシーのバランスの難しさについて改めて認識することとなった。一方で、テロ対策以外にも銃問題や人種問題など多くの課題を抱えていることから、依然として強固な監視システムに

頼ることは避けられない状態となっている。IT を使った防犯と治安について新しい段階へ進もうとする米国の取り組みを紹介する。

図表 1:ニューヨーク・タイムズスクエアの警備の様子

（2015 年 11 月 18 日に筆者撮影）

ニューヨークの代表的な繁華街であるタイムススクエアは常に多くの警察と監視カメラで重点的に警備されている。**図表 1** の写真は、パリのテロの後、IS がニューヨークでのテロを示唆する映像を公開した日に撮影したものだが、特に警備が強化されていることがわかる。

2　米国における IT を活用した防犯・治安の事例

米国では犯罪捜査に様々な技術が投入されているが、治安維持を目的とする警察も最先端の IT を用いた監視システムを導入している。特に、長年にわたって犯罪に対して強い姿勢で取り組んできたニューヨーク市警察は、その有効性から犯罪取り締まりのモデルケースとなっている。その他にも、ビッグデータ、アナリティクス、高画質カメラを用いた上空からの監視など、各警察機関で最新の IT を導入した取り組みが進められている。

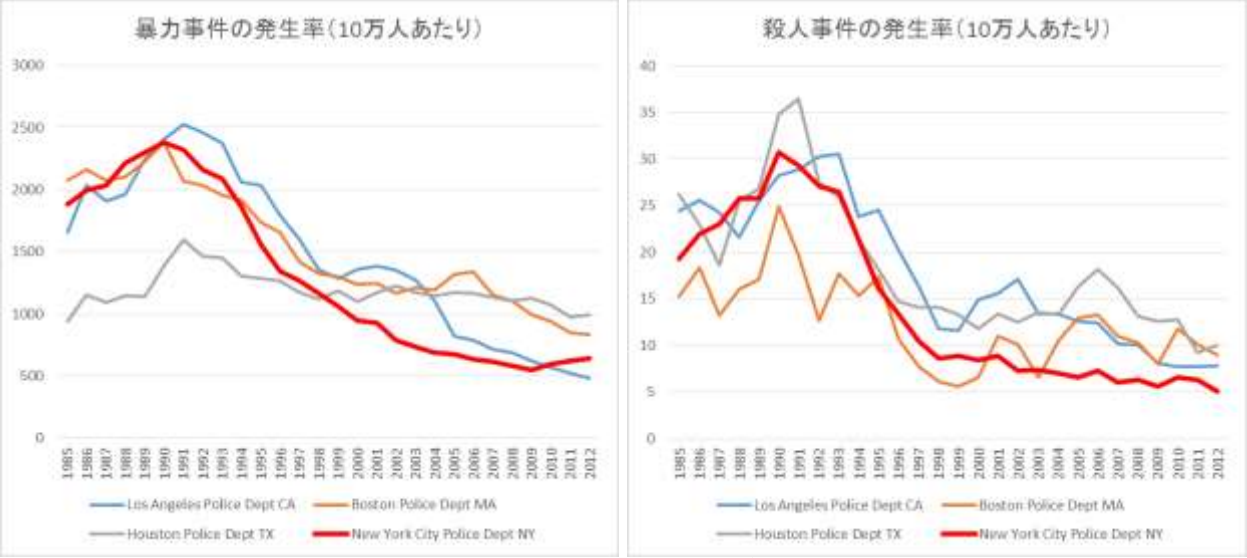
（1）　ニューヨーク市警察における取り組み

a.　ニューヨークにおける犯罪の傾向

犯罪件数の多いニューヨークでは、ニューヨーク市警察が様々な IT を使った犯罪防止に取り組んでおり、全米で最も進んだ防犯・治安のためのシステムを確立している[1]。1990 年までニューヨークの暴力事件と殺人事件の発生率は全米でもトップクラスであったが、1994 年に就任したジュリアーニ市長による取り組みにより、犯罪発生率は急激に減少していった[2]。ジュリアーニ市長が退任した 2001 年以降も犯罪発生率は減少し、現在ではニューヨーク市は全米の大都市の中でも安全な街の 1 つとなっている。

図表 2 は、米国の大都市（ニューヨーク、ロサンゼルス、ボストン、ヒューストン）における 10 万人当たりの犯罪発生率を示したもので、左が暴力事件で右が殺人事件の発生率となっており、赤い線がニューヨーク市警察のデータとなっている。**図表 3** は、米国の 50 万人以上の大都市における 1992 年と 2012 年の暴力事件と殺人事件の発生率ランキングとなっている。

図表 2：米国の大都市における暴力事件と殺人事件の発生率



出典：FBI を基に作成[3]

[1] http://creative.nydailynews.com/smokingguns
[2] http://voices.washingtonpost.com/fact-checker/2007/11/rudy_the_crime_buster.html
[3] http://www.ucrdatatool.gov/Search/Crime/Local/LocalCrimeLarge.cfm

図表 3:米国の主要都市における暴力事件と殺人事件の発生率ランキング(1992 年、2012 年)

暴力事件の発生率(10 万人あたり)

	1992	2012
1	ボルチモア	デトロイト
2	ワシントン D.C.	メンフィス
3	デトロイト	ボルチモア
4	ロサンゼルス	ミルウォーキー
5	**ニューヨーク**	ナッシュビル
6	ダラス	インディアナポリス
7	ボストン	ワシントン D.C.
8	フォートワース	フィラデルフィア
9	ポートランド	ヒューストン
10	サンフランシスコ	オクラホマ
26		**ニューヨーク**

殺人事件の発生率(10 万人あたり)

	1992	2012
1	ワシントン D.C.	デトロイト
2	デトロイト	ボルチモア
3	ボルチモア	フィラデルフィア
4	ダラス	メンフィス
5	シカゴ	シカゴ
6	フォートワース	ミルウォーキー
7	ロサンゼルス	オクラホマ
8	メンフィス	ワシントン D.C.
9	ヒューストン	ダラス
10	**ニューヨーク**	インディアナポリス
18		**ニューヨーク**

出典:FBI を基に作成[4]

b. Domain Awareness System

近年、ニューヨーク市警察は様々な IT を駆使してさらなる治安強化・犯罪の取り締まりに力を入れている。代表例が 2012 年にニューヨーク市警察が Microsoft 社と共同で開発した地域警戒システム(Domain Awareness System:DAS)であり、これは犯罪取り締まりのために必要な機能を提供する包括的なシステムとなっている。具体的には、DAS は監視カメラをネットワーク化させることで、必要な地域の映像を 7,000 個におよぶ警察所有と商業施設の防犯カメラや、パトカーの車載カメラの映像から呼び出すことができるという特徴をもつ[5]。DAS の詳細な機能は明らかにされていないが、例えば、赤いシャツを着た人間だけを表示するように指示をすれば、全ての監視カメラから該当する映像だけを抜き出すことなどが可能であるという[6]。道路上や警察車両に取り付けられたナンバープレート読み取り装置から特定車両の位置情報を確認することもでき、車両の位置情報は過去数ヶ月にわたって検索が可能となっている[7]。

また、DAS は監視カメラや車両の位置情報に加え、ソーシャルメディアで発砲を示唆する投稿や過去の犯罪データといった様々な情報までを集約し、その情報を犯罪の種類などに分類した上で、犯罪捜査の戦略司令室であるリアルタイム・クライム・センター(Real Time Crime Center:RTCC)の画面上に映し出して管理できるようにもなっている。さらに RTCC では DAS を使い、複数の事件の関連性やギャングの活動といった犯罪捜査や、事件が発生しそうな地域には事前にパトカーを巡回させるなど、様々な犯罪の取り締まりを進めることとなる[8]。

2015 年 6 月には DAS のモバイル版の試験運用も開始されており、巡回中の警察官は専用アプリが入ったタブレットを使って DAS の情報を利用できるようになっている。これにより、例えば、逃走した車を追跡す

[4] http://www.ucrdatatool.gov/Search/Crime/Local/LocalCrimeLarge.cfm
[5] http://creative.nydailynews.com/smokingguns
[6] http://www.huffingtonpost.com/len-levitt/thee-rant-turns-ugly_b_1852092.html
[7] http://www.nyc.gov/portal/site/nycgov/menuitem.c0935b9a57bb4ef3daf2f1c701c789a0/index.jsp?pageID=mayor_press_release&catID=1194&doc_name=http://www.nyc.gov/html/om/html/2012b/pr291-12.html&cc=unused1978&rc=1194&ndi=1
[8] http://creative.nydailynews.com/smokingguns
http://www.pcworld.idg.com.au/slideshow/443894/pictures-human-face-big-data/?image=5

る警察官は、タブレット上でナンバープレートの読み取り機から送られた情報を検索し、リアルタイムで特定の自動車の位置情報を確認することなどが可能となる。巡回中に通報を受けた場合でも、通報者や地域の犯罪歴、逮捕状の有無、銃器の使用許可など、これまでよりも詳しい情報を得ることが可能となり、活動の幅を広げるものとなっている。通信は通常の携帯電話回線を使用するが政府の暗号接続を使用しており、タブレットを紛失した場合には遠隔からデータを消去できる機能も搭載されている[9]。

図表 4 は、Domain Awareness System（DAS）の管理画面とモバイル版を示したものとなっている。

図表 4：Domain Awareness System（DAS）の管理画面とモバイル版

出典：The Guardian、The Wall Street Journal[10]

[9] http://www.wsj.com/articles/new-nypd-tablets-help-fight-crime-1403834389
[10] http://www.theguardian.com/cities/2014/jun/25/predicting-crime-lapd-los-angeles-police-data-analysis-algorithm-minority-report
http://www.wsj.com/articles/new-nypd-tablets-help-fight-crime-1403834389

c. ハイテクパトカー

ニューヨーク市警察ではパトカーにも様々な技術を投入している。ニューヨーク市警察が 2013 年 12 月に発表したパトカーは、多くのセンサーやカメラを使い様々な警察の活動を自動化している。例えば、車の後部に取り付けられた赤外線スキャナーは周囲の車のナンバープレートを読み取る機能を持っており、盗難車や手配中の車であるかどうか自動で判別する。さらに放射能検知器も取り付けられており、これらの情報は車内のコンピューターに映し出して確認することもできる。フロントガラス付近に取り付けられた車載カメラは、リアルタイムで映像を警察の指令所に送ることができ、警察内部の連携など様々な活動をシームレスに行うことができるようになっている。このハイテクパトカーは実験段階ではあるものの、導入に向けた取り組みが進められている[11]。

図表 5 は、ニューヨーク市警察のハイテクパトカーとなっている。

図表 5:ニューヨーク市警察のハイテクパトカー

出典:The Wall Street Journal[12]

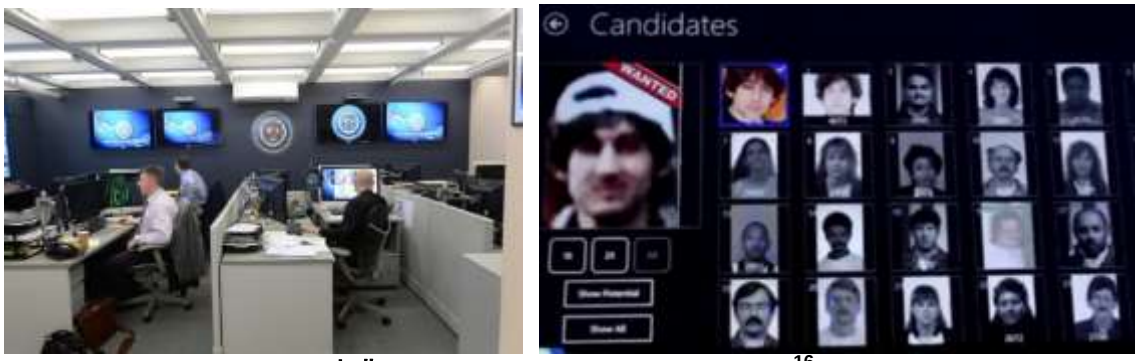
d. IT を使った捜査システム

ニューヨーク市警察は通常の事件捜査にも IT を取り入れている。2011 年からは顔認識システムを使った犯罪者の追跡を行っており、ニューヨーク市警察内に顔認識システムを扱う専門のチームが、監視カメラや Facebook などのソーシャルメディアから集められた画像と犯罪捜査官から送られてきた画像の照合を行っている。画像の照合プロセスは、専用のシステムが顔の 3D イメージを作成し、特徴が近い 200 人のマグショット[13]が自動で抽出され、さらにその中から専門チームが手作業で傷跡や入れ墨といった身体的な特徴を照合していくという形となっている。これまでに 4,400 件の捜査で顔認識システムが使用され、照合する画像の多くは鮮明ではないものの、これまでに 1,000 人以上の顔を一致させているという[14]。プライバシーの観点から DAS に顔認識機能は搭載されていないものの、かなり近い機能のものが開発中とされており、ニューヨークで顔認識を使った犯罪捜査はさらに進むと見られている[15]。

[11] http://www.wsj.com/articles/SB10001424052702304475004579278122995687950?alg=y
[12] http://www.wsj.com/articles/SB10001424052702304475004579278122995687950?alg=y
[13] 容疑者が逮捕された際に撮影される顔写真。
[14] http://creative.nydailynews.com/smokingguns
[15] http://gothamist.com/2012/08/08/photos_the_nypds_new_ultimate_domai.php#photo-1

図表 6 は、左はニューヨーク市警察の顔認識の専門チームとなっており、右は顔認識システムを製作している企業によるデモ画面となっている。

図表 6:ニューヨーク市警察の顔認識専門チーム

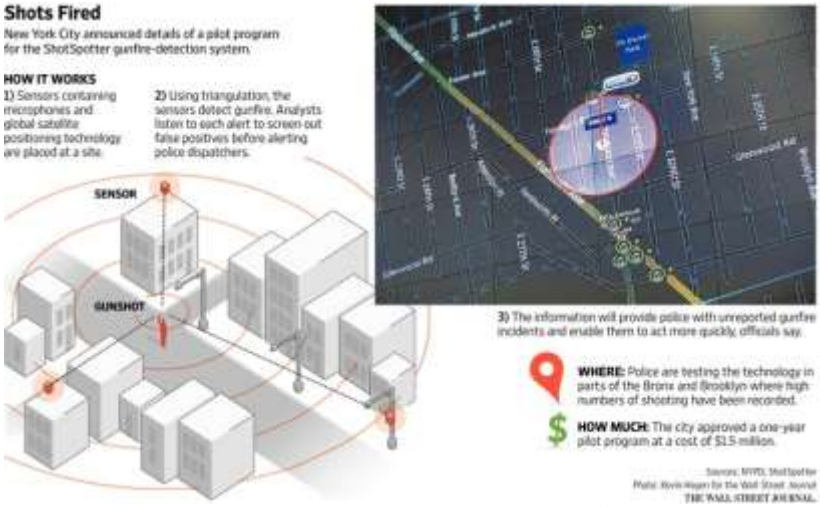


出典:New York Daily News、Yahoo![16]

2015 年 3 月には発砲があった場所をリアルタイムで特定することが可能な銃声検知システム(Gunshot detection system)の導入が発表された。ShotSpotter と呼ばれる同システムは、街中に取り付けられたマイクが銃声を検知すると、複数のマイクの音声データを統合させることで発砲位置を特定する仕組みとなっている。現在 ShotSpotter は試験運用中のため DAS と連動しておらず、発砲位置を特定すると担当官が情報を確認してから DAS へ情報が送られるようになっているが、将来的には統合される予定となっている。統計によると、ニューヨークにおける発砲事件の 75%が警察へ通報されていないことがわかっているが、ニューヨーク市内 300 ヶ所にマイクを設置して 15 平方マイルをカバーし、実際に同システムを使うことにより、通報が無くても発砲を検知することに成功している[17]。

図表 7 は、銃声検知システムとなっている。

図表 7:銃声検知システム



出典:The Wall Street Journal[18]

[16] http://creative.nydailynews.com/smokingguns
https://en-maktoob.screen.yahoo.com/nypd-used-facial-recognition-hammer-183046841.html
[17] http://www.wsj.com/articles/new-york-police-try-out-new-tool-to-detect-gunfire-1426556033?KEYWORDS=ShotSpotter
http://www.engadget.com/2015/03/17/nypd-gunshot-detection-system/
[18] http://www.wsj.com/articles/new-york-police-try-out-new-tool-to-detect-gunfire-

（2） ビッグデータを使った犯罪予測

米国におけるビッグデータを使った犯罪予測（Predictive policing）は、複数の大都市で運用が始まっており一定の成果を上げている。例えば、カリフォルニア州のロサンゼルス市警察は、2012 年からベンチャー企業 PredPol 社と共同で犯罪予測システムの開発を進めてきた。同システムはロサンゼルス市警察の 1,300 万件におよぶ過去の犯罪データを使い、繁華街などの固定要因（Fixed factor）と発砲事件などの変動要因（Variable factor）を加えることで、次に犯罪が発生する可能性の高い地域を予測している。例えば、ギャングによる発砲事件があれば報復のために同じ地区で新たな発砲事件が起きる可能性が高く、高級住宅街で空き巣被害があれば被害宅から 1 マイル以内で再度空き巣被害が発生する可能性があるということになり、人間の行動を数理モデルで説明することで、使用する要因の 1 つ 1 つを犯罪発生率へとつなげている[19]。

PredPol 社の犯罪予測システムは、警察官が勤務（シフト）に入るたびに 10～20 ヶ所の犯罪が起こる可能性の高い地域を提示する形となっており、その地域の巡回に勤務時間の 10～15%の時間を費やすだけでこれまでよりも犯罪を抑えることができるという。ロサンゼルス市警察では同システムを使うことで、強盗事件を 33%、暴力事件を 21%、空き巣被害を 12%削減させることができたとしている。同社のシステムは今や全米 60 の警察機関で利用されており、ワシントン州シアトル（Seattle）やジョージア州アトランタ（Atlanta）といった大都市でも導入されている[20]。

図表 8 の左は PredPol が映し出されたロサンゼルス市警察の指令所となっており、右が PredPol のマップ画面となっている。

図表 8：ロサンゼルス市警察の指令所（左）と PredPol のマップ画面（右）

出典：The Guardian、WAVE[21]

また、ニューヨーク市警察も 2013 年からベンチャー企業 Azavea 社の犯罪予測ソフトウェア Hunchlab の試験運用を続けている。Hunchlab も様々な要因を基に犯罪を予測するものとなっており、1 日から季節ごとまでの時期的な周期、天候、バス停やバーなどの施設、地域経済、過去の犯罪データといった様々な要

1426556033?KEYWORDS=ShotSpotter

[19] http://www.forbes.com/sites/ellenhuet/2015/02/11/predpol-predictive-policing/
http://www.alleywatch.com/2014/08/catch-me-if-you-can-big-data-and-crime-prevention/

[20] http://www.forbes.com/sites/ellenhuet/2015/02/11/predpol-predictive-policing/
http://www.theguardian.com/cities/2014/jun/25/predicting-crime-lapd-los-angeles-police-data-analysis-algorithm-minority-report

[21] http://www.theguardian.com/cities/2014/jun/25/predicting-crime-lapd-los-angeles-police-data-analysis-algorithm-minority-report
http://news.wabe.org/post/concerns-arise-over-new-predictive-policing-program

因から犯罪が発生する一定のパターンを見つけ出す仕組みをとっている。ニューヨーク市警察は 2000 年代前半から、リアルタイムでデータを統合し犯罪対策の戦略管理ができる IBM 社の CompStat と呼ばれるシステムを利用してきたが、Hunchlab を導入することで統計データからだけでは読み取れない犯罪が発生するパターンを分析し、犯罪予測に弾みをつける狙いだという。2015 年 7 月にはニューヨーク市警察全体のシステム向上の計画が発表され、データセンターの設計、犯罪予測システムの導入、CompStat のアップグレードに合わせて 5,500 万ドルが見積もられている[22]。

このほか、テネシー州では交通事故の減少を目的として交通事故予測アルゴリズムを活用するといった動きがある。C.R.A.S.H.（Crash Reduction Analyzing Statistical History）と呼ばれるこの交通事故予測アルゴリズムは、天気、スポーツイベント、地域のお祭り、過去の事故データを総合的に分析することで、事故の発生が予測される場所や時間までを特定することが可能となっている。同システムは交通事故に関連しない情報を自動で取り除く機能を持っており、6 ヶ月の運用の間に 72%という精度で交通事故を予測するという成果を出しているという[23]。

（3） 飛行機やドローンの活用

軽飛行機やドローンを使って上空からリアルタイムで監視するシステムが登場している。例えば、Persistent Surveillance Systems 社が開発した監視システムは、軽飛行機に超高解像度カメラを取り付けて、上空から 25 平方マイル（約 64 平方キロメートル）を監視することができるものとして注目を集めている。Google マップの衛星画像のようなものであるが、大きな違いはリアルタイムで対象地域を見ることができるという点にあり、1 秒ごとに録画された映像を確認することで人や自動車の細かい追跡が可能となっている。上空を飛行している軽飛行機からの撮影であるが、人工衛星からの画像のように座標を固定することができ、最大 6 時間にわたって同じ地域を監視し続ける形をとっている。

このシステムの大きなメリットは、個人を特定するような情報を拾うことがないため、プライバシーを侵害することなく監視活動を行うことができるという点にある。上空からの監視は従来の監視システムとは違い、対象地域のすべての人の動きを追跡することができる一方で、建物の中に入り込むことや個人特定につながる情報収集は行われないため、取り締まりを強化しつつプライバシー侵害の可能性を少なくできるという。同システムはメリーランド州ボルチモア（Baltimore）、オハイオ州デイトン（Dayton）、カリフォルニア州コンプトン（Compton）で試験運用中となっており、コンプトンでは実際にひったくり犯の足取りを追うことに成功している[24]。また、地域監視だけでなく、パイプラインなどの重要インフラや被災地の被害状況の確認などへの応用も期待されている[25]。

図表 9 は、Persistent Surveillance Systems 社の地域監視システムとなっている。

[22] http://www.capitalnewyork.com/article/city-hall/2015/07/8571608/nypd-testing-crime-forecast-software
[23] http://www.timesfreepress.com/news/local/story/2014/aug/01/new-software-predicts-when-and/263323/
[24] http://gizmodo.com/police-are-testing-a-live-google-earth-to-watch-crime-1563010340
[25] http://www.pss-1.com/#!hawkeye-ii-applications/c1i6o

図表 9：Persistent Surveillance Systems 社の地域監視システム

出典：Dailymail、Persistent Surveillance Systems[26]

ドローンの利用も少しずつ進んでいる。米国では 2011 年に初めて SWAT チーム（警察特殊部隊）が国内でドローンを使った逮捕に成功しており、国境警備隊（United States Border Patrol）が数年前から国境の警備にドローンを使用しているが、これらのケースで使われたドローンは飛行機型で、国土安全保障省（Department of Homeland Security：DHS）から貸与された機体となっている[27]。警察機関でドローンを使用する場合は州政府の法整備が必要であるため、導入は進んでいるものの取り締まりには使用できない状態となっており[28]、各警察機関は実用化に向けたテストを重ねている[29]。しかしながら、少しずつではあるものの様々な取り組みは出てきており、2015 年 5 月には湿地帯に逃げ込んだ容疑者を、警察が消防署から借りたドローンを使って容疑者の捜索にあたった[30]。2015 年 8 月にはノースダコタ州が初めて非致死性の

[26] http://www.dailymail.co.uk/news/article-3151641/Catching-crimes-moment-happen-Small-company-capable-filming-cities-24-7-Big-Brother-future-American-surveillance.html
http://www.pss-1.com/#!hawkeye-ii-resolution/ccm3
[27] http://www.wsj.com/articles/inspector-general-criticizes-u-s-border-drone-program-1420576272
http://www.usnews.com/news/articles/2014/01/15/north-dakota-man-sentenced-to-jail-in-controversial-drone-arrest-case
[28] http://www.bloomberg.com/news/articles/2015-01-13/police-drones-aimed-at-berkeley-s-skies-rankle-privacy-activists
[29] http://www.bloomberg.com/news/articles/2015-01-13/police-drones-aimed-at-berkeley-s-skies-rankle-privacy-activists
[30] http://www.wpr.org/law-enforcement-farming-drones-are-becoming-increasingly-popular-tool

武器であればドローンに搭載することを承認する法案を可決させるなど、ドローンを使った犯罪の取り締まりに向けた動きが進んでいる[31]。その他、2014 年 11 月にジョージア州アトランタ（Atlanta）で行われたデモ行進で逮捕者が出た際に、警察とデモ隊がもみ合っている様子をジャーナリストがドローンを使って撮影しており、その映像が法廷で証拠として採用されるなどドローンの有効性を示した例となっている[32]。

図表 10 は、アトランタのデモ行進で警察とデモ隊を追いかけるドローンとなっている。

図表 10：警察とデモ隊を撮影するドローン

出典：Bloomberg[33]

3　防犯と IT の市場

警察の監視システムが高度化する一方で、企業や個人が使用する防犯設備も IT を活用したシステムが主流となってきている。特にインターネットを活用した防犯システムが注目を集めており、IP ベースの監視カメラとクラウドを使うことで利便性を高め、IoT を活用したスマートホームの中にもホームセキュリティが統合されてきている。

（1）　監視カメラと関連システムの市場

監視カメラの市場はインターネットを利用する IP カメラを中心に拡大が見込まれている。米調査会社 Grand View Research 社によると、監視カメラと関連のクラウドサービス（Video Surveillance As A Service：VSaaS）の世界市場は 2012 年の 123.5 億ドルから 2020 年には 489.5 億ドルにまで拡大すると見られており、特にインターネットを利用する IP ベースの監視システムが市場を後押しするとされている。従来のアナログ方式の監視システムに比べ映像の扱いやすさが IP ベースの大きなメリットであり、映像を使った機器の管理、映像解析技術の発達、VSaaS による映像の検索の容易さに注目が集まっている。こ

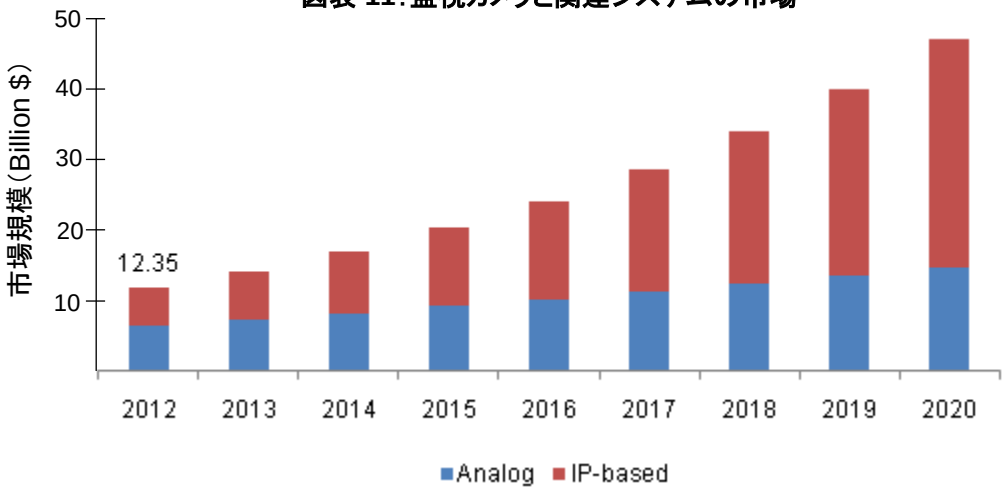
[31] http://www.engadget.com/2015/08/27/north-dakota-cops-will-be-first-in-nation-to-use-weaponized-dron/
[32] http://www.11alive.com/story/news/2015/09/22/drone-footage-lawsuit/72634970/
[33] http://www.bloomberg.com/news/articles/2015-01-13/police-drones-aimed-at-berkeley-s-skies-rankle-privacy-activists

のため監視システムの市場には IP ベースの監視システムを活用するための遠隔監視サービス、クラウドインフラ、VSaaS などに投資が集まると見られている[34]。

分野別に見ると交通機関や商業施設が市場を最も大きく占め、この 2 つの分野ではクラウドや映像管理システムの需要が高いためと見られている。その他には、オフィス、住居、再開発事業者（デベロッパー）、銀行などで VSaaS の導入が進むと予測されている。また、企業の IT コストの削減が進む中で、高解像度カメラの映像や映像解析技術のデータを管理するためのシステムやソフトウェアが必要になってくると見られている[35]。

図表 11 は、監視カメラと関連システムの市場となっている。

図表 11：監視カメラと関連システムの市場



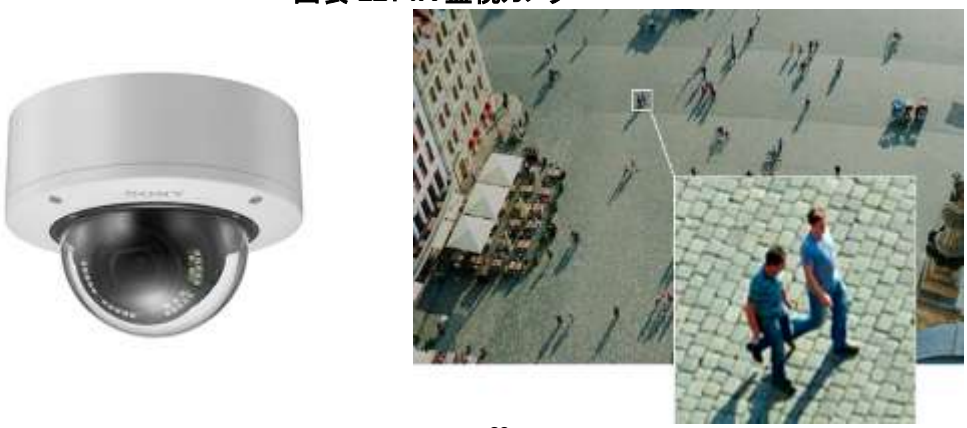
出典：Grand View Research[36]

また、4K 解像度を持つ監視カメラも登場してきており、市場に大きな変革をもたらし今後のトレンドになると期待されている。4K 監視カメラは HD 解像度の 4 倍の解像度をもっており、撮影した映像の詳細まで分析ができるだけでなく、遠くの対象物でも高画質の撮影ができるため離れた場所から広い範囲を撮影できるというメリットがある。この 4K 監視カメラは、顔認識システムのような多くの対象を撮影するシーンに対して特に有用であり、例えば、空港の入国審査で並んでいる人を顔認識が可能な解像度で撮影する場合、約 20 メートルの列に対して HD 監視カメラが 3 台必要とするところを 4K 監視カメラであれば 2 台でさらに長い列までカバーできる[37]。すでに様々な企業から 4K 監視カメラは発売されているが、高解像度の映像はデータが膨大となるため、データの容量を抑える新しい映像圧縮技術やデータ転送のための高速ブロードバンド回線が不可欠であり、これらの利用環境が整備されるとともに 4K 監視カメラも大きく普及すると見られている[38]。

図表 12 は、4K 監視カメラによる監視のイメージとなっている。

[34] http://www.grandviewresearch.com/industry-analysis/video-surveillance-industry
[35] http://www.grandviewresearch.com/industry-analysis/video-surveillance-industry
[36] http://www.grandviewresearch.com/industry-analysis/video-surveillance-industry
[37] http://www.ifsecglobal.com/building-business-case-4k-video-surveillance/
[38] http://www.sdmmag.com/articles/90911-state-of-the-market-video-surveillance

図表 12：4K 監視カメラ



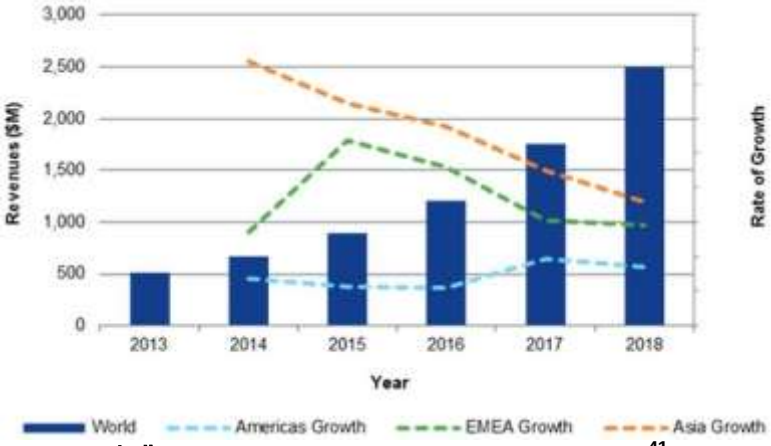
出典：Sony[39]

（2） ホームセキュリティの市場

米調査会社 IHS 社によると、ホームセキュリティの市場は 2014 年の 6 億 7,000 万ドルから 2018 年には 24 億ドルに拡大すると予測されている。現在のところホームセキュリティは単体として販売されていることが多いものの、将来的にはホームオートメーションの一部に組み込まれていくことで活用が広まっていくと見られている。また、これまでホームセキュリティは専門のセキュリティ事業者により提供されるケースが多かったが、インターネットを利用したサービスが可能になったことで、インターネットプロバイダやケーブルテレビ会社といった様々な企業が参入してきているほか、多くのユーザーを持つ Apple 社や Google 社がホームオートメーションのプラットフォームを構築してきたことで、ユーザーは様々な製品を選ぶことができるようになりつつあり、こうした点も市場を拡大させる要因になると見られている[40]。

図表 13 は、ホームオートメーション市場の予測となっている。

図表 13：ホームオートメーションの市場



出典：SECURITY SALES & INTEGRATION[41]

[39] http://www.pro.sony.eu/pro/lang/en/eu/product/video-security-ip-cameras-minidomes/snc-vm772r/overview/
http://www.sony.fi/pro/article/video-security-4k
[40] http://www.securitysales.com/article/why_the_residential_security_market_will_never_be_the_same
[41] http://www.securitysales.com/article/why_the_residential_security_market_will_never_be_the_same

近年ではインターネットを活用した個人向けのホームセキュリティが中心とってきていることから、ケーブルテレビ会社や通信企業などがホームセキュリティの市場に参入してきている。例えば、米大手ケーブルテレビ会社 Time Warner Cable 社が提供しているサービスでは、様々なホームセキュリティの機能がセットになっている。家の中に設置されたセキュリティカメラは人物を検知すると画像付きでメールやテキストメッセージで通知されるようになっており、不審者の侵入だけでなく子供が学校から帰宅したかなどを確認できる。また、カメラの映像はクラウド上に保存されるため、2 台のカメラの映像を最大 10 日前までに戻って確認することが可能である。
また窓やドアの開閉検知センサー、窓ガラス破壊検知センサー、モーションセンサーなどを設置することで不審者を検知できるが、住民による予期しないセンサーの検知を防ぐために在宅時、外出時、就寝時によって検知する範囲をプログラムすることもできる。この他、空調や照明の管理といったスマートホームの機能も提供されており、これら全てを専用端末もしくはスマートフォンやパソコンから一括して管理できるようになっている。スマートホームセキュリティはインターネット回線を使用するようになっているが、家のインターネット回線が使用不能の時は携帯電話回線を使用し、停電時には各機器がバッテリーで稼働するなどバックアップ体制も整っている[42]。

図表 14 は、ホームセキュリティを示したものとなっている。

図表 14:ホームセキュリティの例

出典:Time Warner Cable、Comcast[43]

[42] http://www.timewarnercable.com/en/intelligenthome/overview.html
https://www.timewarnercable.com/content/dam/residential/pdfs/intelligenthome/ih-product-brochure.pdf
[43] http://www.timewarnercable.com/en/intelligenthome/overview.html
http://corporate.comcast.com/media-center/home-media

4　最先端技術

（1） トラッキング技術、映像解析技術

マサチューセッツ工科大学（Massachusetts Institute of Technology：MIT）は 2013 年 12 月、微弱な無線電波を対象物に放射し、対象物に当たって反射した電波を捉えることで対象物の位置や形状がわかるという WiTrack と呼ばれる技術を発表した。驚くべきはその精度であり、およそ 10～20 センチメートルの精度で対象物の位置を特定できるほか、対象物を 3 次元的にも捉えることができるため対象物の動きまでもわかるという。さらに、無線電波は壁を通過することができるため壁の向こう側にいる人物の位置や動きを特定することなども可能であり、使用する電波の強度は通常の Wi-fi の 100 分の 1、携帯電話の 1,000 分の 1 程度となっている。実験では対象者が部屋に入って壁に向かって指をさすだけで隣の部屋の照明を点灯させることに成功しており、壁越しに人物の位置と動きを正確に特定できることが確認されている。将来的にはゲーム、ホームオートメーション、ヘルスケアなどに加えて、監視システムなどに応用できると見られている[44]。

図表 15 は、WiTrack の実験の様子となっている。

図表 15：WiTrack の実験の様子

出典：MIT[45]

また 2014 年 8 月には、同工科大学から、被写体のわずかな動きから周囲の音を再現することができる映像解析技術ビジュアルマイクロフォン（Visual Microphone）も発表された。この技術は映像に映し出された物体のわずかな動きを増幅させるというもので、見た目では判別できない表情のわずかな変化や機械の動きを増幅させ、物体の状態をより詳細に分析するものである。さらに研究では、観葉植物やごみ袋といった軽い物体の振動を増幅させることで周囲の音を再現することに成功している。また 1 秒間に 6,000 フレームの撮影が可能なハイスピードカメラを使用することで、部屋の中で流れている音楽を再現することに成功している。1 秒間に 60 フレームの撮影しかできない通常のデジタル一眼レフカメラでも CMOS センサーの特性を利用することで、ある程度の再現が出来たという。将来的には様々な物体の振動を分析できるようにすることを目的としており、監視カメラの映像などから様々な情報を取り出すことが期待されている[46]。

[44] http://news.mit.edu/2013/new-system-allows-for-high-accuracy-through-wall-3-d-motion-tracking-1211
http://www.silverdoctors.com/wifi-device-can-see-through-walls-track-a-human-by-using-body-as-an-antenna-array/
[45] http://news.mit.edu/2013/new-system-allows-for-high-accuracy-through-wall-3-d-motion-tracking-1211
[46] http://www.engadget.com/2014/08/04/visual-microphone/
https://www.ted.com/talks/michael_rubinstein_see_invisible_motion_hear_silent_sounds_cool_creepy_we_can_t_dec

（2） 人の流れを監視する技術

車輌に加えて通行人の流れを監視することができる技術なども登場している。ニューヨークのベンチャー企業 Placemeter 社は車道や歩道上の交通量を調べることが可能なソフトウェアを開発しており、実用化へと進みつつある。同社のソフトウェアはカメラの映像から歩行者、自動車、歩道上の売店など交通量を構成する要素ごとに分類して統計を取っていくようになっており、自動車だけでも乗用車、バス、トラック、タクシーなど 11 種類に分けてカウントされる。また、進行方向やスピードに加え、歩行者がどのビルに入ったかまでも分析されるため、歩行者数に対する商業施設の利用状況がわかるようになっている。同社のビジネスモデルも特徴的で、計測用のカメラを設置して調査に協力する地域住民には最大で月に 50 ドルが支払われるようになっており、計測方法も、使用しなくなったスマートフォンなどを窓に設置するだけとなっている。なお、利用者からは 1 箇所の計測につき月額 149 ドル（年間契約であれば月額$99）を徴収している[47]。

図表 16 は、Placemeter 社の交通量計測システムとなっている。

図表 16：Placemeter 社の交通量計測システム

出典：Citylab、The Washington Post[48]

この Placemeter 社のサービスは様々な場面への活用が期待されている。イベントなどで長蛇の列が出来た場合には、来場客に通知して人の流れをコントロールするといった使い方や、展示物に来場者がどれだけの時間とどまっているかなどを知ることができる。また、高画質カメラを使用していれば歩行者の性別を75～80%の確率でわかるため、ショーウィンドウのデザインや小売店の出店場所の選定に使用される[49]。

大規模なイベントを効率的に運用するために Placemeter 社のサービスを活用した例も出ている。2015 年 10 月にニューヨークで開かれた市民マラソン大会 New York Road Runners（NYRR）では、スタートとゴールになっているスタジアムにどれだけの見学者が集まったか計測した。平均的な市民ランナーのスピードからどの時間帯にゴールする人数が多くなるか予測し、それに合わせて集まる見学者数を計測し、予測と実

ide#t-458903
[47] http://techcrunch.com/2015/06/23/placemeter-uses-computer-vision-to-help-businesses-and-cities-measure-vehicle-and-pedestrian-traffic/
http://www.citylab.com/tech/2014/08/the-view-from-your-window-is-worth-cash-to-this-company/375471/
[48] http://www.citylab.com/tech/2014/08/the-view-from-your-window-is-worth-cash-to-this-company/375471/
https://www.washingtonpost.com/news/innovations/wp/2015/06/23/placemeter-launches-in-bid-to-provide-retailers-cities-with-better-data/
[49] https://www.washingtonpost.com/news/innovations/wp/2014/06/16/five-interesting-things-that-result-from-gobs-of-foot-traffic-data/

際の数を確認している。これらのデータを活用することで、警備員や売店などを効率的に運用することができると見ている[50]。

（3） セキュリティロボット

a. 商業施設での防犯ロボット

防犯のために様々なロボットを利用するケースが登場している。2014 年 1 月に Knightscope 社が発表したロボット K5 は、決められた範囲を自律的に行動して警備できるものとなっている。K5 には 360 度を監視することが可能なカメラや赤外線・熱感知センサーが搭載されており、1 分間に 300 の自動車のナンバープレートを読み取ることができるほか、人の動作を分析して攻撃的な行動をしているかまで識別することができるという。2015 年 5 月にはカリフォルニア州のショッピングモールで試験運用を行うなど実用化を進めている[51]。サービスが開始されれば 1 時間あたり 6.25 ドルでレンタルされる予定であり、通常、1 時間 20 ドルかかる警備員のコストを大きく削減することが可能と見られている[52]。

図表 17 は、Knightscope 社の K5 となっている。

図表 17：Knightscope 社の K5

出典：CBS[53]

b. 海中警備ロボット

海中を自律航行することで環境や海上での犯罪を監視するロボットも登場している。2014 年 8 月には Liquid Robotics 社から、海中を自律航行可能なロボット Wave Glider SV3 が発表された。このロボットは太陽光発電や波の力を使って自家発電を行うことが可能であり、長期間にわたって自律航行が可能となっている。同ロボットには多くのセンサーが取り付けられているため、ガスやオイルといった環境汚染につながる物資の監視、海上でのドラッグの取引や密入国の防止、魚群探知など様々な利用方法が期待されている。また、Wave Glider SV3 はクラウドのように使用することを想定した設計となっているため、海上にいながら Wave Glider SV3 上にソフトウェアを送ることができ、複数のユーザーが 1 台のロボットを使って様々なデータを受け取ることができるようになっている[54]。

図表 18 は、Liquid Robotics 社の Wave Glider SV3 となっている。

---

[50] http://blog.placemeter.com/2015/10/15/placemeter-x-nyrr/
[51] http://www.paloaltoonline.com/news/2015/08/09/robots-deployed-to-protect-and-serve
[52] http://venturebeat.com/2015/10/22/i-for-one-welcome-our-new-surveillance-robot-overlords/
[53] http://sanfrancisco.cbslocal.com/2014/11/18/crime-fighting-robots-go-on-patrol-in-silicon-valley-k5-knightscope-mountain-view-stacy-stephens-autonomous-security-guard/
[54] http://www.cnet.com/news/liquid-robotics-launches-autonomous-sea-faring-data-center/
http://www.cnet.com/news/hundreds-of-floating-robots-could-soon-surveil-the-oceans/

図表 18：Wave Glider SV3

出典：CNET[55]

5　監視とプライバシーの問題

（1）　米国における監視システムとプライバシー

a.　テロ対策法とプライバシー保護

米国におけるプライバシー問題は同時多発テロとスノーデン事件をきっかけに大きく変化し、現在でも議論が続いている。2001 年 9 月 11 日に発生した同時多発テロの発生後、テロの取り締まりを目的とした米国愛国者法（USA PATRIOT Act）が制定され、国家安全保障のため情報収集が個人のプライバシーよりも優先されるきっかけとなった。米国愛国者法は様々な内容で構成されているが、最も大きな変更点に「外国情報監視法（Foreign Intelligence Surveillance Act：FISA）」と「電気通信におけるプライバシー保護法（Electronic Communications Privacy Act）」の大幅な改正があり、政府による情報収集のためにこの 2 つの法律で定められていたプライバシーに対する法的保護の内容が大きく縮小された[56]。

次にプライバシーに関する転換点となったのは 2012 年 12 月に起きたエドワード・スノーデン氏（Edward Snowden）による国家安全保障局（National Security Agency：NSA）の大規模な情報収集活動の暴露であり、国民の見えないところで政府が想像以上の情報収集を行っていたことが問題となった。この事件によって国家安全保障とプライバシー保護のバランスについて議論が巻き起こり、同時多発テロ以降、テロ対策を常に優先してきた連邦政府が変化し始めた[57]。米国愛国者法は 2015 年 6 月 1 日に期限切れとなり失効したが、翌日の 6 月 2 日にオバマ大統領が後継となる米国自由法（USA Freedom Act）に署名している。同法では政府による情報収集は継続することを認める一方で NSA による一般市民への情報収集を大きく制限することが定められており、一定のプライバシー保護のバランスを取った内容となっている[58]。

b. 警察機関におけるプライバシー保護の取り組み

米国における監視システムの全国的な運用指針は示されておらず、法執行機関によるプライバシー保護への取り組みは憲法で記された原則に基づいたものとなっている。米国のプライバシー保護は権利章典（Bill of Rights）[59]の修正第 4 条（Fourth Amendment）の中で規定されている。その内容によると、個人が第三

[55] http://www.cnet.com/news/hundreds-of-floating-robots-could-soon-surveil-the-oceans/
[56] http://today.uconn.edu/2015/09/privacy-security-and-the-legacy-of-911/
[57] http://today.uconn.edu/2015/09/privacy-security-and-the-legacy-of-911/
[58] http://thehill.com/policy/national-security/243850-obama-signs-nsa-bill-renewing-patriot-act-powers
[59] アメリカ合衆国憲法の基本的人権が規定された修正第 1 条から修正第 10 条までを指したもの。修正第 4 条では法執行機関による捜査と令状について記されている。

者と情報を共有した場合、その個人は共有した情報に対し「プライバシーの合理的な期待（reasonable expectation of privacy）」を持っていないと見なされるため、法執行機関は令状を取らずにそれらの情報を取得できる[60]。しかしながら、デジタル時代では情報の発信が不可欠であり、携帯電話の通話記録や位置情報などは個人の活動を特定できる情報であるにもかかわらず、捜査上で取得するのに令状を必要としないということになる。このため、実際に令状無しで取得された通話記録や位置情報の違法性が様々な裁判で争われている[61]。

全国的な監視システムの運用指針は示されておらず、上記のような背景から、各警察機関では権利章典の修正第 4 条を侵害しないプライバシー保護の取り組みに基づいて監視活動が進められている。例えば、ニューヨーク市警察では 2009 年に Domain Awareness System（DAS）の運用に関するプライバシーのガイドラインを発表しており、DAS 運用の項目で、DAS の監視活動はプライバシーの合理的な期待がない場所で公的な活動にのみに使用されると規定されている[62]。

図表 19 は、DAS のプライバシーガイドラインとなっている。なお、目的外のデータの使用や共有について承認を出す担当部署はデータの種類によって異なる。

図表 19：DAS のプライバシーガイドライン

項目	内容
使用目的	• テロリストや工作員の活動の監視 • テロリストによる工作活動の検知 • テロ攻撃の検知 • その他の地域警戒活動 • 警察の即応時間の短縮 • 新しいセキュリティ技術を統合するためのプラットフォーム構築
運用	• DAS はプライバシーの合理的な期待がない場所で公的な活動の監視にのみ使用 • DAS 上では顔認識システムを使用しない • DAS 上の一部となっている警察所有の監視カメラすべてに、DAS で使用していることを書いた看板を設置する。また商業施設のカメラを DAS で使用している場合にも同様の看板の設置を勧める
データの保存期間	• 映像：保存期間は 30 日間 • メタデータ：保存期間は 5 年 • ナンバープレート：保存期間は 5 年間 • 環境データ：無期限
データの使用	• 上記の使用目的以外でのデータの使用には担当部署から承認を得る必要がある
データの共有	• データの共有は法執行または防犯・治安の目的に限られる。ただし、裁判所など司法からの要請は除く • 第三者機関とのデータの共有には、担当部署からの承認が必要
データ保護	• DAS のデータへアクセスが可能な指令所へ立ち入ることができる人物は、ニューヨーク市警察のスタッフ、承認を受けた訪問者、協力機関・組織の代表者に限る • データに直接アクセスできるのは、ニューヨーク市警察の中で承認を受けたスタッフと協力機関・組織の代表者に限る

出典：New York City[63]

[60] http://today.uconn.edu/2015/09/privacy-security-and-the-legacy-of-911/
[61] https://www.washingtonpost.com/world/national-security/us-appeals-court-no-warrant-needed-for-stored-cellphone-location-data/2015/05/05/c290e28e-f34d-11e4-b2f3-af5479e6bbdd_story.html
http://www.forbes.com/sites/danielfisher/2015/05/07/court-rules-nsa-phone-surveillance-illegal-but-saves-bigger-questions-for-later/
[62] http://www.nyc.gov/html/nypd/downloads/pdf/crime_prevention/public_security_privacy_guidelines.pdf
[63] http://www.nyc.gov/html/nypd/downloads/pdf/crime_prevention/public_security_privacy_guidelines.pdf

（2） E-ZPass を使った車両追跡

高速道路の自動精算システムを使った一般道での車両追跡が議論を巻き起こしている。ニューヨーク州からワシントン D.C.とイリノイ州シカゴ（Chicago）まで伸びる高速道路（フリーウェイ）では、E-ZPass と呼ばれる自動精算システムが利用されている。E-ZPass は、日本の ETC と同様に料金所で自動的に通行料を支払うシステムであるが、日本のようにカードを挿入する必要もなく、簡易な通信機器を車両のフロントガラスに取り付けるだけという利便性の高いものとなっている。しかし、高速道路の通行料金精算を目的とした本システムが、ニューヨークの都心部では料金所のない場所でも E-ZPass を使って通過した車両の情報収集にも利用されており、ニューヨーク州運輸局（New York Department of Transportation）も交通量監視のために E-ZPass を使用していることを明らかにしている[64]。

さらに 2015 年 4 月、米国自由人権協会（American Civil Liberties Union：ACUL）によると、ニューヨークの都市部以外でも料金所から離れた場所で E-ZPass の読み取りが行われていることがわかった。同団体は情報公開法（Freedom of Information Act）に基づいてニューヨーク都心部で E-ZPass が使われている 149 箇所の情報を取得したが、それ以外の場所でも E-ZPass の読み取り機を使った同様の取り組みが進められていると公表した。同団体は、ニューヨーク州運輸局が E-ZPass を本来の目的である料金精算以外に使用する場合にはプライバシーポリシーやデータの使用目的をユーザーへ明確に説明するべきだと非難し、また、ユーザーにオプトアウトの選択肢を与えるべきだと述べている[65]。

図表 20 は、E-ZPass のデバイスと、読み取り機が設置されたニューヨーク周辺となっている。

図表 20：E-ZPass（左）と読み取り機が設置された箇所

出典：MassDOT、American Civil Liberties Union[66]

[64] http://www.forbes.com/sites/kashmirhill/2013/09/12/e-zpasses-get-read-all-over-new-york-not-just-at-toll-booths/
[65] https://www.aclu.org/blog/free-future/newly-obtained-records-reveal-extensive-monitoring-e-zpass-tags-throughout-new-york
[66] https://www.aclu.org/blog/free-future/newly-obtained-records-reveal-extensive-monitoring-e-zpass-tags-throughout-new-york
https://www.massdot.state.ma.us/highway/TrafficTravelResources/EZPassMAProgram/HowEZPassWorks.aspx

6　終わりに

近年テロの脅威はさらに大きなものとなっており、防犯・治安への対応は益々重要になってきている。特に米国ではセキュリティは最も大きな関心事の一つであるが、日本でも今後、伊勢志摩サミットや東京オリンピック・パラリンピックをはじめ、世界的に注目されるイベントが開催されることから、米国と同様に防犯・治安への対応は一層大きな課題になってくると思われる。

今回紹介したように、米国では様々な先端 IT が防犯・治安の分野で実用化され、そして大きな効果をあげていることから、今後ますます新しい技術の開発や実用化が進むものと思われる。IT 産業にとっても、防犯・治安関連は今後大きな成長分野になってくるものと思われる。

防犯・治安面における危機感が高い米国における IT 化の取り組みは、日本にとっても大いに参考になるのではないだろうか。