スマートシティの政策課題と保険会社への影響

主席研究員　杉浦　友

目　　次

要旨

スマートシティにおいては、モビリティ、防災、エネルギー、医療といった様々な領域のインフラや機器をIoT技術によりネットワーク化し、センサー等を通じて収集した大量かつリアルタイムのデータを解析・活用することにより、都市問題の改善、公共サービスの効率化、ひいては市民の生活の質の向上が期待されている。その一方で、効果的なスマートシティ政策の実施のためには、インフラの連関性ゆえに増加する可能性がある、サイバー攻撃、プライバシー等のリスクに備えるとともに、政策決定プロセスへのステークホルダーの関与の促進を含む、諸課題に対処する必要がある。

保険会社にとっては、スマートシティ化の進展をビジネスチャンスにつなげるべく、スマートシティにおけるリスクの変容が商品・サービスの需要に及ぼす影響を長期的な視点で精査することや、リスク評価・リスク管理の知見を生かして都市政府の基盤・ルール整備に参画すること等が重要となりうる。

１．はじめに

世界的な都市化の進行・都市部への人口集中は、先進国・途上国を問わず、都市問題の深刻化を招いている。国連の持続可能な開発目標（Sustainable Development Goals：SDGs）の１つに「住み続けられるまちづくり」が掲げられているように、都市政府（自治体）にとって、自都市の財政、発展段階、地理的環境、リスク特性等に応じて効果的な解決策を講じることは、これまで以上に重要な課題となっている。

このような状況を背景として、モビリティ、治安、防災、エネルギー・資源、医療等に関わる、都市の様々なインフラに IoT[1]技術を取り入れ、それらを連関させることで、都市問題の改善、公共サービスの効率化、市民の生活の質の向上等を図る、スマートシティ[2]政策への注目が高まっている。スマートシティ政策は都市住民に望ましい変化をもたらす一方で、都市のリスクを変容させる可能性がある。そのため、都市政府はスマートシティ政策の実効性の確保に向けて、スマートシティ化（スマートシティへの移行）が都市政府および都市の住民・企業の抱えるリスクに及ぼす影響を特定・評価し、政策上の課題に対処する必要がある。また、リスク引受・リスク管理の専門家である保険会社にとっても、都市におけるリスク・損害の変化を踏まえて、商品・サービスの開発・提供や都市政府との連携のあり方を検討することが重要となりうる。

本稿では、スマートシティ政策の効果等を概説したうえで、スマートシティにおけるリスクの特徴、都市政策上の課題、および保険会社への影響について考察する。なお、本稿における意見は筆者の個人的見解であり、所属組織を代表するものではないことをお断りしておく。

２．スマートシティ政策の概観

本項では、スマートシティ政策の対象となる領域、スマートシティ化に期待される効果、および国内外のスマートシティ政策の動向を概説する。

（1）領域

スマートシティにおいては、様々なインフラに搭載したセンサー等で構成される大

---

[1] Internet of Things の略で、「モノのインターネット」と訳される。パソコンやスマートフォン等、インターネットとの親和性が高い機器のみならず、従来は必ずしもインターネットへの接続を前提としていなかったモノ（家電、車、建物・設備、インフラ等）をインターネット経由でサーバーやクラウドサービスにつなげる仕組を指す。詳細、大量かつリアルタイムのデータを双方向に通信、処理、分析、連携することにより、実効的・効率的なサービスの提供が実現するとされている。

[2] わが国国土交通省は、スマートシティを「都市の抱える諸課題に対して、情報通信技術（Information and Communicaion Technology：ICT）等の新技術を活用しつつ、マネジメント（計画、整備、管理・運営等）が行われ、全体最適化が図られる持続可能な都市または地区」と定義している（国土交通省「スマートシティの実現に向けて【中間とりまとめ】」（2018.8））。なお、関連する概念として、家屋内の電子機器・設備をネットワーク化することで、住民の生活環境の改善や利便性の向上を目指す「スマートホーム」や、電力インフラに IoT 技術を取り入れる「スマートグリッド」等が挙げられる。

量のデータ収集ポイントを経由して、リアルタイムの詳細なデータをより包括的・効率的で費用対効果が高い方法によって収集することが可能となる[3]。そのようなデータは、IoT、人工知能、機械学習等の技術を活用して解析され、都市政府が問題事象の発生の検知・予測、パターンの把握、相関・因果関係の分析等を進め、持続可能な解決・改善策を検討・実施したり、対処すべき問題の深刻度を比較し、効果的に予算を配分したりする際に有用となる。

スマートシティ政策は、都市の安全性の向上、災害リスクの制御、環境負荷の低減、公共サービスの利便性の向上、行政機能の高度化、限られたインフラ・財源の効率的・持続可能な管理・活用等を目的とし、その領域は多岐にわたる（図表１参照）。都市政府は、政策を進めるにあたって、自都市が抱える問題、それらの優先順位付け、および導入する技術の費用対効果等に応じて、どのインフラにどのような技術を取り入れるのかを決定する必要がある。

図表１　スマートシティで活用される技術の例（インフラ分野別）(注)

安全性	○犯罪予測　○リアルタイムの犯罪発生マッピング　○銃撃音検出システム ○スマート監視システム　○群衆管理　○緊急対応システムの最適化 ○自然災害早期警報システム　○個人用警報アラーム　○身体装着型カメラ ○ホームセキュリティシステム　○データ主導型の建物検査
モビリティ	○公共交通機関のリアルタイム情報　○交通インフラの予測的メンテナンス ○高度交通信号システム　○自動運転車　○リアルタイムナビゲーション ○様々な交通手段の情報の統合　○公共交通機関の乗車料金のデジタル決済 ○需要に合わせたマイクロ交通　○カーシェア・バイクシェア ○オンラインタクシー配車システム（個人・相乗り）　○通行料制度 ○スマートパーキング　○共同配送　○スマート宅配ロッカー
医療	○遠隔医療　○遠隔患者モニタリング　○オンライン医療検索・予定作成 ○統合型入退院管理システム　○データに基づいた妊婦・乳幼児の健康管理 ○ウェアラブル端末　○応急処置の警報　○感染症監視システム ○データに基づいた下水道等の公衆衛生の改善　○リアルタイムの大気質情報
エネルギー	○ビル自動操作システム　○家庭用エネルギー自動化システム ○家庭用エネルギー消費量のトラッキング　○スマート街路灯 ○需要連動型の電気料金設定　○配電自動化システム
水	○水道使用量のトラッキング　○水漏れ検知・抑制　○灌漑設備のスマート化 ○水質監視
廃棄物	○廃棄物のトラッキング・決済システム　○廃棄物収集ルートの最適化
経済開発・住宅	○商業登記の申請・認証のデジタル化　○納税申告のデジタル化 ○オンラインの職業再訓練プログラム　○オンラインの就活支援センター ○個人のニーズに応じた教育　○オープンソースの土地台帳管理データベース ○土地利用・建築の許可申請のデジタル化　○P2P の宿泊プラットフォーム
コミュニティエンゲージメント	○公共サービスのデジタル化　○市民向けエンゲージメントアプリケーション ○市民とのコミュニケーションを促進するプラットフォーム

（注）特に 2025 年にかけて重要度が増すと考えられる技術を示している。

（出典：McKinsey Global Institute, “Smart cities: Digital solutions for a more livable future”（2018.6）をもとに作成）

[3] 一部のインフラについては従来から大量のデータが収集されてきたものの、その多くの場合、体系的な整理や他のインフラのデータとの連携は不十分であったと考えられる（AXA XL, “Smart Cities: Mission Control”（2014.10）ほか）。

（2）効果

a. 都市問題・公共サービスの改善

スマートシティ化が都市問題の解決にもたらす効果の大小は、各都市のインフラの整備状況や問題の深刻度等に応じて異なるという点に注意が必要ではあるものの、図表 2 に例示するとおり、多くの都市においてスマートシティ政策の一定の成果が示されている。また、マッキンゼー・グローバル・インスティテュートは、既存のインフラや経済的・社会的な前提条件が異なる都市の類型を設定し、それらに数十のスマートシティ技術が活用された場合に期待できる効果を、図表 3 のとおり推計している[4]。

図表 2　スマートシティ政策の効果を示す主な事例

米国 ミズーリ州 カンザスシティ	駐車場の空き状況、交通パターン、および路面電車の位置に関するリアルタイムのデータの提供を、スマート信号、情報キオスク、および無料 Wi-Fi の整備とともに進めた結果、都市政府の運営・エネルギー費用が年間 400 万ﾄﾞﾙ削減された。
米国 ケンタッキー州 ルイビル	スマートフォンと連動する、ぜんそく患者用の吸入器を経由して、市内の発作の発生状況および大気汚染のレベルに関するデータを収集・分析し、患者（1,000 人以上）に対して関連情報の提供および警告を行った結果、取組開始から 1 年間で吸入器の緊急使用が 82%減少した。
メキシコ・ メキシコシティ	監視カメラ、銃撃音検出センサー、車両番号プレート検出器、スピーカー、カメラ付ドローン等をネットワーク化・配備した結果、通報から現場到着までの所要時間が 12 分から 4 分に短縮され、車両盗難件数が半減する等、治安が改善した。
中国・北京	大気汚染の発生源を監視するセンサーから収集したデータに基づき、交通の流れや建設プロジェクトを調整した結果、1 年以内に汚染のレベルが 20%低下した。
中国・深圳	総合的な交通制御システムにより、対象地域の交通量が前年比で 27.5%、交通事故警報件数が 90%減少した。また、疾病管理プラットフォームの整備により市内のインフルエンザの状況予測の正確性が 90%に達した。

（出典：Christine Wong, “Building the smart cities of the future”（Futurithmic, 2019.3）、Ping An, “Ping An Unveils First Smart City Integrated Platform and Solutions in China to Empower Development with Technology”（2018.8）、亀井卓也「諸外国スマートシティ動向とデータプラットフォームの実現に向けて」総務省先端技術 WG（第 5 回）配付資料（2016.4）ほかをもとに作成）

図表 3　スマートシティ政策の効果の推計

殺人、交通事故、火災による死亡者数	8～10%減少
犯罪発生件数	30～40%減少
疾病負荷（障害調整生命年 (注)）	8～15%減少
1 日あたりの通勤時間	15～20%（15～30 分）減少
温室効果ガス排出量	10～15%減少
水消費量	20～30%（1 人あたり 1 日 25～80 ﾘｯﾄﾙ）減少
緊急対応所要時間	20～35%減少

（注）早期死亡により失われる期間や疾病・障害により健康が失われる期間に係る指標である。

（出典：McKinsey Global Institute, “Smart cities: Digital solutions for a more livable future”（2018.6）をもとに作成）

[4] 高所得都市（米国・ニューヨーク等）、中所得都市（ブラジル・リオデジャネイロ等）、および低所得都市（ナイジェリア・ラゴス等）の 3 類型が設定されており、類型によって各分野の効果の大小は異なる（McKinsey Global Institute, “Smart cities: Digital solutions for a more livable future”（2018.6））。

b. 政策決定プロセスの変革

スマートシティ政策の効果を考えるうえでは、前記 a で取り上げたような既存の問題の解決という観点に加えて、都市政策に関する意思決定プロセスの変革という側面も注目に値する。スマートシティにおいては、インフラ・機器に搭載したセンサーやアナリティクス技術を活用することで、より多くのデータに基づいた効果的な意思決定が可能となるだけでなく、市民や企業等のステークホルダーとの情報の連携や、それらからの詳細な知見の取込が容易になるため、政策決定プロセスにおけるステークホルダーの関与が促進されうる。

デロイトの報告書[5]は、スマートシティ化の進展に伴い、都市政府にはデータを収集してエンドユーザー（市民、企業等）と共有するとともに、それらの集団的な知見を取り込む、プラットフォームとしての役割を強化し、都市問題の解決に向けた変革を推進することが求められると指摘している。このような政策アプローチのもとでは、市民がいわば政策の共同策定者となるため、より市民のニーズに合致したソリューションの創出が実現することが期待されている。また、スマートシティ政策の実施にあたっては、IoT の基盤となる高速インターネット網・5G（第 5 世代移動通信システム）等の確保が重要となるが、当該環境の整った都市は、新技術の実証・インキュベーションの場として活用され、起業家や最新デジタル技術に精通した企業を呼び込む可能性が高い。このような企業の知見を取り入れることが、さらに実効的・効率的な政策決定・実施をもたらすという効果も期待できる。

（3）動向

スマートシティ政策の採用は世界の様々な都市において確認されており、特に近年の傾向としては、人口密度が高い大規模な都市に加えて、中規模な都市での取組の増加が挙げられる[6]。IT 専門調査会社である IDC の予測[7]によると、主要な都市におけるスマートシティプロジェクトに係る支出額は 2023 年には合計で 1,895 億ﾄﾞﾙに達する。また、対象期間（2019 年から 2023 年）においてプロジェクトが実施される主な分野は、「レジリエンス（回復力）のあるエネルギーおよびインフラ」、「データに基づくセキュリティ」、および「インテリジェントな交通」であり、これらの優先分野に対する支出額が対象期間の総支出額の半分以上を占めると推定されている。スマートシティプロジェクトに対する投資額が特に大きい都市は、シンガポール、ニューヨーク、東京、

[5] William D. Eggers & John Skowron, “Forces of change: Smart cities” Deloitte Insights（Deloitte, 2018）

[6] Alicja Grzadkowska, “The rapid spread of smart cities exchanges old risks for new ones”（Insurance Business, 2019.1）

[7] 9 地域（米国、カナダ、日本、西欧、中欧・東欧、中東・アフリカ、ラテンアメリカ、中国、およびアジア・太平洋）の 180 以上の都市を対象としている（IDC, “Smart Cities Initiatives Forecast to Drive $189 Billion in Spending in 2023, According to a New Smart Cities Spending Guide from IDC”（2019.6））。

ロンドン、北京、上海であり、地域単位で見ると、米国、西欧、および中国[8]における支出額が対象期間中の総計の 70%超を占めるとされている。なお、対象期間中に最も支出額の伸びが予想される地域は、日本および中東・アフリカであり、年間平均増加率は約 21%に達するとされている。

わが国においては、2019 年に国土交通省がスマートシティのモデル事業を選定する等、スマートシティへの関心は高まりつつあると言える。その一方で、様々なインフラに IoT 技術等を導入し、ステークホルダーを意思決定のプロセスに実効的に取り込む総合的な都市政策というよりは、地域の抱える個別課題を技術主導で解決することを目指した、比較的小規模な取組あるいは企業による実証実験にとどまっている事例が多いとの指摘もある[9]。

３．リスクの特徴

前記 2（1）・(2）において記述したとおり、スマートシティにおいては、治安、災害、事故、健康等に係るリスクの軽減が見込まれる一方で、物理的なインフラの機能がデジタル技術に依存し、大量のデータが取り扱われるという特性ゆえに、財物、死亡・傷害、賠償責任等に係る損害が大規模化する可能性も指摘されている[10]。本項では、スマートシティにおけるリスクの特徴を、サイバー攻撃、プライバシー、およびインフラの不具合・人的ミスの観点から説明する。

（1）サイバー攻撃

スマートシティにおいては、センサーが増設され、様々な機器およびスマートグリッド等のインフラがインターネットを通じてつながることにより、インフラの外部との接続性およびインフラ間の連関性が高まる。これは、ハッカーやインターネット犯罪者がデータの窃取や公共サービスの運営の妨害を行う際の侵入地点が、潜在的に多く存在することを意味する。スマートシティのインフラに対するサイバー攻撃の主要な形態としては、ランサムウェアや DoS[11]等が考えられる。

---

[8] 中国では、保険、銀行、投資、インターネット金融、技術提供、プラットフォーム事業等を展開する平安グループが、スマートシティプロジェクトに積極的に関与している。2018 年 8 月時点の情報では、平安は国内の 200 以上の都市と提携し、2,000 以上の公共サービスに係るオンラインプラットフォームを提供している（Ping An, “Ping An Unveils First Smart City Integrated Platform and Solutions in China to Empower Development with Technology”（2018.8））。また、同社は、2018 年 11 月に戦略的提携契約を締結した海南省三亜市において、300 億元（約 4,530 億円。2020 年 4 月末時点の為替レートである 1 元＝15.1 円で換算した。）を投じて、スマートシティプロジェクトや関連する金融サービス・商品の開発等を進めるとしている（新華社通信「平安集团将在三亚投 300 亿元进行智慧城市等建设」（2018.11））。

[9] 日立コンサルティング「スマートシティに関する動向と今後の課題」（2019.4）ほか

[10] Mark S. Raffman, “‘Smart Cities' Raise Novel Issues and Novel Risks”（The Recorder, 2018.10）

[11] ランサムウェアは、攻撃対象のコンピュータシステムをウイルスに感染させ、適正な作動を損なわせたうえで、修復と引換に身代金を要求するプログラムであり、DoS（Denial of Service）は、攻撃対象のサーバーやネットワークに通信障害等を引き起こすものである。

都市政府のITシステムは、予算の制約もあり、アップデートやバックアップが不十分であることが多く、そのような脆弱性を突いたサイバー攻撃は増加傾向にある。特に米国では、都市政府がランサムウェアによって身代金を要求される事例が増えている[12]。身代金の支払を拒否した場合、インフラの停止・公共サービスの妨害といった被害が拡大するほか、例えば、公立病院の有する患者の医療記録へのアクセスの遮断や個人データの漏えい等に伴う、都市政府自体に対する潜在的な訴訟リスクを想定する必要が生じる[13]。また、身代金を支払った場合でも、攻撃・妨害が約束どおりに中止されなかったり、加害者側にさらなる攻撃のインセンティブを与えてしまったりするリスクがあるため、都市政府にとって対応の判断が難しい問題となっている。

すべての身代金支払の事例が公表されているわけではないと考えられるが、図表4に米国の都市政府への攻撃事例を示すとおり、ランサムウェア攻撃の結果、高額の身代金支払や復旧・交換費用が生じている。これらの都市のうち、リビエラビーチの人口は約3万5,000人、レイクシティの人口は約1万2,000人であり、小規模な都市であっても攻撃対象となりうることがわかる。両市の身代金支払は保険の補償範囲内であったため、免責金額（レイクシティの場合、1万ﾄﾞﾙ）以外は保険会社が負担したとされている[14]。なお、身代金を支払った場合でも、システム・インフラの補強が不可欠となるため、当該都市政府には財務的負担が生じる。

図表4　都市政府に対するランサムウェア攻撃の主な事例（注1）

メリーランド州 ボルチモア	○2019年に攻撃を受け、7万6,000ﾄﾞﾙの身代金支払を拒否した。 ○復旧費用は1,800万ﾄﾞﾙ以上に達すると推計されている（注2）。
ジョージア州 アトランタ	○2018年に攻撃を受け、5万1,000ﾄﾞﾙの身代金支払を拒否した。 ○復旧費用は1,700万ﾄﾞﾙ以上に達すると推計されている。
フロリダ州 リビエラビーチ	○2019年に攻撃を受け、60万ﾄﾞﾙの身代金を支払った。
フロリダ州 レイクシティ	○2019年に攻撃を受け、46万ﾄﾞﾙの身代金を支払った。

（注1）本表で示す金額は、ビットコイン等の暗号資産（仮想通貨）の相当額を含む。

（注2）同市は攻撃後に、補償限度額を1,000万ﾄﾞﾙとする保険を2本契約しており、それらの年間保険料は合計で83万5,000ﾄﾞﾙとされている（James Rundle, “Cities Warned Not to Rely on Cyber Insurance Alone”（The Wall Street Journal, 2019.10））。

（出典：Kate Fazzini, “City ransomware attacks and huge payouts mean a once-private corporate problem has gone public”（CNBC, 2019.6）、Wade Goodwyn, “Ransomware Attacks Create Dilemma For Cities: Pay Up Or Resist?”（NPR, 2019.7）ほかをもとに作成）

[12] 米国では2013年以降、少なくとも170の州、郡、市のシステムがランサムウェア攻撃を受けたとされている（Kyle Funk, Cooper Martin, Nicole DuPuis, Alan Shark & Dale Bowen, “Protecting Our Data: What Cities Should Know About Cybersecurity”（National League of Cities, 2019.10））。

[13] Frank Ready, “As cyberattacks increase, cities push risky strategy”（Legaltech News, 2019.7）

[14] Ian Duncan, “As Florida cities use insurance to pay $1 million in ransoms to hackers, Baltimore and Maryland weigh getting covered”（The Washington Post, 2019.7）ほか

（2）プライバシー

スマートシティにおいては、収集されるデータの量および質・粒度が大幅に変容する。収入、犯罪、移動、土地使用、駐車違反、廃棄物等に関する多様なデータの解析によって、高価値の知見の提供が可能となる一方で、官民連携により IoT 技術を取り込むというスマートシティの特性ゆえに、それらのデータが民間企業の収益を向上させるために転用されたり、都市政府による市民の監視[15]を強化する目的で使用されたりするなど、市民の望まない結果を生む可能性も指摘されている[16]。そのため、プライバシーやデータ共有・使用に係る潜在的な訴訟・賠償責任リスクに対処するために、収集するデータの種類、使用目的・範囲等を明確にして市民の理解を得るとともに、データの適切な保護・取扱を確保するガバナンス方針・態勢を確立することが必要となる[17]。

プライバシーが争点となった事例として、カナダ・トロントの都市政府と Alphabet（Google の親会社）の子会社である Sidewalk Labs 等による再開発計画が挙げられる。SideWalk Labs は、対象地域に最新の都市インフラを導入し、それらを専用 OS（オペレーティングシステム）で管理することを計画していた。同社は、町中に設置されるセンサーを介して、歩行者の通行からエネルギー消費の状況に至るまで様々なデータを収集し、例えば、歩行者・車両のデータの解析により、交通の流れをリアルタイムで調整することで、配達やごみの収集を含む、モビリティの最適化を実現させるとしていた。

この計画に対して、市民の同意を得ない民間企業による大量の公共データの収集・使用の是非、監視社会化の可能性、データ匿名化の十分性・タイミングの適切性、都市政府による SideWalk Labs の活動の統制の実効性、利益配分等に関して、市民の懸念が高まり、実施機関の理事等が計画に抗議して辞職する事態に発展した。その結果、SideWalk Labs は、データ収集・使用に係る透明性・監視態勢を確保するために、データガバナンスの主導権を都市政府が持つことに合意したほか、同地域で開発された技術の知的財産権や付随利益の帰属・配分等について、大幅な譲歩を余儀なくされた[18]。

---

[15] 多くの都市において、AI・顔認識システムを搭載した監視カメラが警察等の公的機関により活用されているが、欧米を中心に、過度の監視社会化、データの正確性・公平性、データ主体（市民）の権利等の観点から懸念する動きもあり、米国では 2019 年 5 月にカリフォルニア州サンフランシスコが大規模な都市としては初めて、警察等による顔認識技術の使用の禁止を決定した（Charlie Campbell, "'The Entire System Is Designed to Suppress Us.' What the Chinese Surveillance State Means for the Rest of the World"（Time, 2019.11）ほか）。なお、世界の 120 の大都市を対象とした調査によると、人口あたりの公共の監視カメラの設置数が多い都市のトップ 10 のうち 8 都市は中国に所在し（その他はイギリス・ロンドンと米国・アトランタ）、第 1 位の重慶には 1,000 人あたり約 168 台の監視カメラが設置されている（Paul Bischoff, "The world's most-surveilled cities"（Comparitech, 2019.8））。また、同調査は、中国では 2022 年には全国平均で約 2 人に 1 台の割合で公共の監視カメラが設置されていると予測している。

[16] Leyland Cecco, "'Surveillance capitalism': critic urges Toronto to abandon smart city project"（The Guardian, 2019.6）ほか

[17] Derek Porter, "Why Smart Cities Need Risk Management"（EfficientGov, 2018.11）

[18] Ian Austen, "You Can't Fight City Hall. But Maybe You Can Fight Google."（The New York Times, 2020.3）、Gillian Tett, "Google's smart city: dystopian nightmare or model for the future?"（Financial Times, 2019.11）ほか。なお、その後 2020 年 5 月に SideWalk Labs は、世界およびトロントの不動産市場における前例のない経済的な不確実性に鑑みて、根幹を変更せずに再開発計画を財務的に実行可能とすることが難しくなったとして、計画の中止を公表した。

（3）インフラの不具合・人的ミス

スマートシティでは IoT 技術等を取り込んだインフラのネットワークを活用することで、事故や災害の頻度が全体的に減少する一方、インフラ、センサー、およびソフトウェアの欠陥、機器間の連動の不具合、システム障害、不適切なデータ取扱、アナリティクスに係る人的ミス等を原因として、都市政府のインフラ・機器、第三者の財物、および車両等の損害、都市政府の職員や市民の負傷・死亡、情報漏えい等が生じる可能性がある[19]。そのような損害は低頻度ではあるものの、従来は１つのインフラ内の１つのミスとして対処できた事象の影響が、スマートシティでは他のインフラへ波及し、大規模化してしまう潜在性が指摘されている[20]。

４．政策課題

本項では、前記 3 で取り上げたスマートシティのリスク特性を踏まえて、都市政府がスマートシティ政策を実効的に進めるうえでの主な課題を考察する。

（1）総合的な都市政策への取込

スマートシティ政策の実効性を高めるためには、センサーやアプリ等の個別技術の導入、あるいは個別のインフラ・問題の改善に主眼を置くのではなく、総合的な都市政策の一環として、どのように技術を活用して都市を構成するインフラ要素を連関させ、都市全体のプラットフォームとしての機能を強化するべきかを検討することが鍵となる[21]。その際には、導入する技術が都市政府・市民のニーズに合致しているかを見極めるために、都市の直面する問題の把握、スマートシティプロジェクトの実施に必要な条件の特定、新技術の信頼性、機能性、維持、訓練要件、費用等に係る直接的な効果の精査、および新技術が既存の政策、リソース配分、セキュリティ態勢、その他の実務等に及ぼしうる間接的な効果の評価を含む、全体的な検証作業（デューディリジェンス）を実施する必要が生じる[22]。同時に、都市の有する複数のインフラ・システムの相互運用性を確保するために、標準的な API[23]を採用するなど、基盤・ルールを整備することも重要となりうる[24]。

---

[19] Travelers, “Infrastructure for the smart city”（2019）ほか

[20] 例えば、「ソフトウェアのバグにより、厳冬期に暖房システムが停止し、パイプの破裂・洪水が発生する」、「インフラを保護・監視するためのセンサーが故障し、建物、橋、ダム等が崩壊する」、「交通システム・ソフトウェアの設計ミスによって自動車事故が起こる」といった事態が想定されうる（Mark Breading, “Smart Cities and Insurance: Exploring the Implications”（SMA, 2017.8）、Mark S. Raffman, “'Smart Cities' Raise Novel Issues and Novel Risks”（The Recorder, 2018.10）ほか）。

[21] Thom Rickert, “Smart Cities and the Infrastructure Revolution”（Public Risk Magazine, 2019.1）

[22] Adam Rujan & Nicole Simpkinson, “Risk versus reward: Six considerations for smart cities”（Plante & Moran, 2018.8）

[23] Application Programming Interface の略で、主にウェブサイト上でソフトウェア（アプリケーション）の機能等を共有する仕組を指す。

[24] 日立コンサルティング「スマートシティに関する動向と今後の課題」（2019.4）ほか

なお、総合的な都市政策への取込にあたっては、多様なインフラごとのリスク・技術導入の効果やインフラの連関性を評価・検証し、政策のフィードバックループを確保するために、都市政府内の部門ごとのサイロ型のアプローチではなく、関係部門が密接に連携する横断型のアプローチが求められる[25]。

(2) リスク対策

a. リスク評価・管理

スマートシティ政策の実施にあたっては、その計画段階から、インフラ、コネクテッドデバイス、ネットワークシステム等の運用や収集したデータの保護・取扱の適切性を確保するために、リスク評価・管理態勢を整備することが重要となる。スマートシティ政策に関連する主なリスク評価・管理の要素としては、都市政府の有する重大な資産の把握、インフラ、土地使用、人材配置、規制の遵守等といった領域ごとのリスク評価、重大な情報を保管（バックアップ）、処理、移転するためのシステムごとのリスク評価、全職員を対象とするITセキュリティ方針に係る教育、外部委託先のベンダー・クラウド事業者の適切な点検、契約条件（責任の所在）の確認、サイバーセキュリティ態勢のモニタリング等が挙げられる[26]。

b. リスク移転（保険）

スマートシティのインフラ・システムの規模、複雑性、および連関性ゆえに大規模化しうる損害や、ネットワークを介して収集される大量のデータの不適切な保管・使用あるいは漏えいのリスク等に備えるために、保険を通じてリスクを移転することは有効な措置となりうる。一般的には、スマートシティ化が進んだ場合、都市政府が自都市のインフラ全体にわたる多様なリスクに対応するために、補償限度額が高く、補償範囲が広範な保険の手配が必要となると考えられる[27]。また、スマートシティプロジェクトにおける官民連携に際しては、想定される損害額がベンダーの負う契約上の賠償責任の上限額を大きく上回る事態等もありえるため、都市政府にとっては、契約条件を評価し、財務健全性を確保するために、不足分を保険で補完することも重要となりうる[28]。

スマートシティ化を進める都市政府が必要とする主な保険として、米国の大手保険会社であるトラベラーズは、サイバーリスクに対応する情報セキュリティ保険、財物・第三者への付随的損害へのエクスポージャーを補償する財物・自動車（対人・対物賠償、車両）保険、および人身傷害のエクスポージャーに対応する賠償責任保険（施設賠償責

[25] Gianni Minetti, “A smart city is an interoperable city”（Smart Cities World, 2019.9）ほか
[26] Kyle Funk, Cooper Martin, Nicole DuPuis, Alan Shark & Dale Bowen, “Protecting Our Data: What Cities Should Know About Cybersecurity”（National League of Cities, 2019.10）、Travelers, “Infrastructure for the smart city”（2019）ほか
[27] Mark S. Raffman, “'Smart Cities' Raise Novel Issues and Novel Risks”（The Recorder, 2018.10）
[28] Loqiva, “Lloyd's Networked World: Addendum”（2018.12）

任保険等）を挙げている。同社は、スマートシティが発達する中で、インフラの不具合に伴って都市政府が負う責任の全容の把握は難しく、すべてのリスクが付保可能というわけでもないという制約はあるが、都市ごとのセキュリティ上のニーズを踏まえて保険の選択肢を精査し、最良なリスク移転を確保することが重要であるとしている[29]。

なお、米国の都市政府の IT 担当者を対象とした調査[30]によると、当該政府の 68%がサイバー保険に加入しており、それらのうち 12%は補償限度額が 100 万ﾄﾞﾙ以下、35%は 100 万ﾄﾞﾙから 500 万ﾄﾞﾙ、11%は 500 万ﾄﾞﾙ以上であった。その一方で 42%が補償限度額について「わからない」と回答したこと等を踏まえると、リスク管理における保険の重要性に係る認識を都市政府内で高める余地は依然として大きいと考えられる。

c. 緊急対応

スマートシティ政策を進めるにあたっては、大規模停電、サイバー攻撃等に起因してインフラに問題が発生した場合に備えて、緊急時対応計画、インフラの連関性・接続性を制限する手段、バックアップの電力システム等を整備しておく必要がある[31]。なお、スマートシティにおいては、平常時はアルゴリズムがインフラの動作に係る意思決定を容易にするが、想定どおりにセンサーが作動しない場合等に備えて、都市政府職員が IoT 技術等に依存せずに意思決定を行い、当該設備を動かすための応急措置を講じられるように訓練しておくことも重要である[32]。

（3）ガバナンス

スマートシティでは、インフラ・機器およびソフトウェアを介して大量のデータが収集されるため、都市政府はそれらを保管、分類、分析、活用する方法を確保するとともに、個人を特定できる情報が適切に保護されていることを示すことで、エンドユーザー（市民、企業等）の信頼を醸成する必要がある[33]。また、スマートシティプロジェクトでは民間企業の技術の活用・資金調達[34]の観点から官民連携が進められるが、都市政府の公共性と提携企業の収益性のバランスを確保したうえで、提携企業が取り扱うことができるデータの種類・範囲、インフラ・システムの開発・運用に係る協調領域・競争

---

[29] Travelers, “Infrastructure for the smart city”（2019）

[30] 有効回答数は 165 であり、人口規模別では 5 万人未満の都市が 45%、5 万人から 15 万人の都市が 33%、15 万人以上の都市が 22%を占めた（Kyle Funk, Cooper Martin, Nicole DuPuis, Alan Shark & Dale Bowen, “Protecting Our Data: What Cities Should Know About Cybersecurity”（National League of Cities, 2019.10））。

[31] Derek Rice, “Smart City Networks Require Resiliency to Stay Connected in Severe Weather”（StateTech Magazine, 2019.2）ほか

[32] Travelers, “Infrastructure for the smart city”（2019）

[33] Alicja Grzadkowska, “The rapid spread of smart cities exchanges old risks for new ones”（Insurance Business, 2019.1）

[34] スマートシティプロジェクトに対する都市政府の関心は高いものの、単独でプロジェクトの資金を調達できる都市は 16%にすぎず、官民連携や国家からの補助金に頼らざるを得ないとの調査結果がある（Loqiva, “Lloyd's Networked World: Addendum”（2018.12））。

領域の区分け[35]、当該プロセスの管理方法等を決定することが重要となる[36]。前記 3(2)のトロントの事例に示されるように、このような官民連携のあり方に関するステークホルダーの理解の確保は、特に大規模なプロジェクトにおいて課題となりうる。

スマートシティ政策において適切なガバナンスを推進するためには、新技術を本格的に導入する前に、対応する方針・規制を整備し、運用上の一貫性を確保することも必要となりうる。例えば、米国ミズーリ州カンザスシティでは、低所得層地域に銃撃音検出センサーを設置する 6 か月前に、監視社会化・プライバシーに係る市民の懸念に対処すべく、収集されるデータの内容、収集の目的、およびデータの共有・開示の範囲等を明確化する方針を策定した[37]。

(4) ステークホルダーとの連携

スマートシティ政策を進めるにあたっては、政策決定プロセスにステークホルダーを取り込み、スマートシティ化によって得られる効果やリスク対策等に係る共通認識を構築することが、実効性を高める鍵となる[38]。とりわけ、IoT 技術等を導入するインフラの優先順位付けを行う際には、すべてのステークホルダー(市民・企業、提携企業、都市政府自体等)にとって透明性があり、それらが知見を共有できるオープンなプロセスを通じて、ステークホルダーがスマートシティ政策に対して有する多様な期待・利害関係を調整し、より良い意思決定につなげることが望ましいとされている[39]。

ステークホルダーの関与に関連して、スマートシティ化がデジタルディバイド[40]の拡大やコミュニティの衰退といった悪影響を生まないように注意することも重要である。例えば、スマートフォンの使用・インターネットへの接続を前提としたプロジェクトにおいて、低所得層がサービスを十分に受けられなくなる、あるいはサービスのデジタル化に伴う人的交流の減少が、都市の住みやすさや活気に資するコミュニティ意識を低下させるといった潜在性を懸念する見方がある[41]。一方で、コミュニティが既にそういった課題を抱えている場合に、IoT 技術等の活用が当該課題の解決に有効となる可能性もあり[42]、この観点からもステークホルダーのニーズに則した政策決定が肝要となる。

---

35 例えば、データ連携のための基盤の構築・運用は、費用最適化の観点から公的機関が主導し、個別のデジタルソリューション・システムについては、技術開発等の観点から提携企業の競争領域として扱うこと等が想定されうる(日立コンサルティング「スマートシティに関する動向と今後の課題」(2019.4))。

36 Christine Wong, "Smarter, safer and more inclusive communities"(Futurithmic, 2019.3)、William D. Eggers & John Skowron, "Forces of change: Smart cities" Deloitte Insights(Deloitte, 2018)ほか

37 Adam Rujan & Nicole Simpkinson, "Risk versus reward: Six considerations for smart cities"(Plante & Moran, 2018.8)

38 Tom Saunders & Peter Baeck, "Rethinking Smart Cities From The Ground Up"(Nesta, 2015.6)ほか

39 Bethan Moorcraft, "All stakeholders must work together on 'smart city' master plans"(Insurance Business, 2019.5)

40 IT を利用できる人と利用できない人の間に生じる格差を指す。

41 Christine Wong, "Building the smart cities of the future"(Futurithmic, 2019.3)

42 関連事例として、米国オハイオ州コロンバスでは、低所得層が多い地域において、妊婦向けにウェブベースのライドシェアプロジェクトを展開している(Skip Descant, "Columbus, Ohio, Turns to On-

５．保険会社への影響

本項では、スマートシティ化が保険会社にもたらしうる影響について、商品・サービスの提供および都市政府との連携の観点から考察する。

（1）商品・サービスの提供

a. 都市政府向け

保険会社は、スマートシティ特有のリスクに対応する、前記 4（2）b で取り上げたような保険を、都市政府のニーズに応じてパッケージ化[43]して販売するなどして、都市政府に対して適切なリスク移転を促すことができる。また、保険会社はリスク分析・管理の専門家としての知見や請求・支払等に関するデータを活用して、以下のような観点から、スマートシティ政策の立案・実施段階において、有益なリスクコンサルティング・ソリューションを提供することも可能であると考えられる[44]。

○ リスクモデル・アナリティクス等を活用したリスク評価・定量化によって、都市政府による顕在的・潜在的なリスクの特定、計測、および理解を支援する。
○ 公共セクターのリスク管理に係る、グローバルな動向・ベストプラクティスに関する知見を提供する。
○ スマートシティに特有のリスクの軽減・管理のための、都市政府向けソリューションを提供する。
○ スマートシティのプラットフォーム・サービスの利用者向けの保険の共同開発・提供等を通じて、スマートシティ政策の推進を支援する。

b. 個人・企業向け

スマートシティ化は都市のあらゆるインフラおよびその利用者である個人・企業の有するリスクに変化をもたらす可能性があるため、保険会社は、サイバーセキュリティ、自動車、財物、賠償責任（施設賠償責任、専門職業人賠償責任等）を含む広範な商品・事業種目への影響を、長期的な視点で評価する必要がある[45]。そのうえで、保険会社にとっては、スマートシティ化に伴う事故・災害リスクの変容や産業構造の変化を踏まえて、既存商品を改定したり、IoT 技術等を活用してスマートシティにおける需要に合致

Demand Transportation to Improve Medical Access”（Government Technology, 2018.11））。

[43] インフラの連関性を踏まえると、小規模のプロジェクトであっても影響が深刻化する可能性があるため、都市の規模に関係なく、広範な補償に対する需要は存在しうる。一方で、包括的なパッケージの保険料は、予算が限られる小規模な都市等にとって高額となる可能性もあり、そのような場合は取組ごとに保険料が設定される商品を優先順位に応じて選択することも想定される（Alicja Grzadkowska, “The rapid spread of smart cities exchanges old risks for new ones”（Insurance Business, 2019.1）ほか）。

[44] Derek Porter, “Why Smart Cities Need Risk Management”（EfficientGov, 2018.11）、Thom Rickert, “Smart Cities and the Infrastructure Revolution”（Public Risk Magazine, 2019.1）ほか

[45] Mark Breading, “Smart Cities and Insurance: Exploring the Implications”（SMA, 2017.8）ほか

した保険商品を開発したりすることが重要となると考えられる。

図表 5 は、スマートシティにおいて想定されうるリスク・損害の変化の例を保険分野別に示している。とりわけ自動車保険に関しては、自動運転車の開発および対応する交通インフラの整備の状況に応じて、新たなビジネスモデルを構築する必要が生じうる。そのようなビジネスモデルは、サイバーセキュリティ、車両に搭載されたソフトウェア・ハードウェア（アルゴリズム、センサー等）に対する製造物責任、およびインフラの不具合の 3 分野に対応する保険を含み、従来型の自動車保険の収入保険料が低下するのに対して、特にサイバーセキュリティに関する保険料は増加していくと推定されている[46]。

図表 5　スマートシティ化がもたらしうる変化の例（保険分野別）

自動車	自動運転車の増加、公共交通（モビリティ）の選択肢の増加、ライドシェアの増加、自動車所有率の低下、テレマティクスの普及等により、事故の減少、位置情報等を活用したオンデマンド保険の需要の拡大等が想定されうる。
財物	事故・問題を予見・検知し、自動的に対処する、スマートビル・スマートホームの普及等により、財物エクスポージャーの減少、建物ごとのより細分化された保険料設定の実現等が想定されうる。
健康・医療	環境（大気・水質）の改善、運動の選択肢の増加、交通事故の減少、治安の改善等により、死亡率・罹患率の低下、寿命の延伸等が想定されうる。
労災	通勤環境の改善、通勤時間の短縮化、職場事故の減少（例えば、ドローンや衛星画像の活用に伴う高リスク作業の減少）等により、労災リスクの軽減が想定されうる。

（出典：Alicja Grzadkowska, “The rapid spread of smart cities exchanges old risks for new ones”（Insurance Business, 2019.1）、Mark Breading, “Smart Cities and Insurance: Exploring the Implications”（SMA, 2017.8）ほかをもとに作成）

c. 課題

スマートシティに対応する商品・サービスの提供にあたっては、スマートシティに特有のリスクの評価や、保険契約の補償・免責範囲の見直し等に関して課題が生じうる。

（a）リスク評価

スマートシティにおける複雑なリスクを詳細かつ適切に分析し、定量化することは、保険会社が引受可能な補償範囲・条件を特定するための重要な基礎となる。しかし、スマートシティプロジェクトの実施やそこで使用される技術の進展のペースが速まる一方、スマートシティにおける損害および請求・支払のデータの蓄積やデータ分析の手法の開発はまだ十分とは言えず、長期的な損害シナリオやリスクモデルの構築に係る課題が存在することが指摘されている[47]。

---

[46] 米国市場では、従来型の自動車保険の収入保険料が 2026 年を境に減少に転じる一方で、それ以外の 3 分野に係る保険料規模は 2025 年には 150 億ﾄﾞﾙだが、2050 年には 340 億ﾄﾞﾙまで増加すると推定されている（Lawrence Karp & Richard Kim, “Insuring Autonomous Vehicles”（Accenture, 2017.5））。

[47] Thom Rickert, “Smart Cities and the Infrastructure Revolution”（Public Risk Magazine, 2019.1）ほか

保険会社がスマートシティにおけるリスクを分析する際には、物理的なインフラ、ネットワークに接続する機器、サイバー空間の複雑性、暗号化技術、官民連携における関係性等、様々な観点を取り込む必要があり、自社内で部門横断的な方法で取り組むとともに、リスクエンジニアや外部の技術提供会社と協働することが重要となると考えられる。また、保険会社は、データ共有・使用のメリット、影響、範囲、および方法等に関して、契約者の理解・同意を得たうえでデータを蓄積するとともに、共有可能な形式のデータセットへのオープンアクセスを可能とするデータリポジトリをデータサイエンス業界と共同開発するといった方策も検討しうる[48]。

（b）補償・免責範囲の見直し

インフラや設備に IoT 技術等を搭載した場合、リスク・損害の変容が想定されることから、保険会社は既存の保険契約の内容が契約者のニーズに合致したものであるか否かを契約者との間で確認する必要がある。また、保険会社が財務的責任を果たすために、制御可能かつ適切なレベルでの保険料率設定が可能なリスクのみを引き受けるという観点からも、既存商品・契約の適切性を判断することは重要である[49]。保険会社には、これらの観点を踏まえて、追加補償の設定・その可否の判断、サイレント・サイバーリスク[50]への対応を含む免責・除外の明確化等を行い、約款・補償範囲を見直す必要が生じうる。

（2）都市政府との協働

スマートシティ化は保険会社に対して、スマートシティにあわせた商品・サービスの提供の機会だけでなく、スマートシティ政策に官民連携のパートナーとして参画することでメリットを受ける機会も創出しうる。保険会社がリスク管理・引受・移転の専門家、機関投資家・インフラ資金提供者、データ保有者としての機能を発揮し、都市政府と連携することは、ウィンウィン（Win-Win）の効果をもたらすと考えられる。

スマートシティにおいて IoT 技術等を活用して収集される、例えば、自然・都市環境の変化、市民の行動パターン、犯罪等に関する、大量で粒度の高いリアルタイムのデータは、特に大規模な損害の頻度・深刻度を予測するための、より精度の高いリスクモデル・シナリオの構築に資する[51]。また、保険会社はリスク評価やデータ管理に係る知見を活用し、都市政府に対してスマートシティにおけるリスク・機会の特定やデータの解

---

48 Swiss Re, “How data will shape the new urban future”（2019.1）、Zurich Insurance, “Insurance in the age of the smart city”（2020.1）ほか

49 Bethan Moorcraft, “All stakeholders must work together on ‘smart city’ master plans”（Insurance Business, 2019.5）

50 補償・免責のいずれの対象にも明示的に含まれていないサイバーリスクを指す。詳細は損害保険事業総合研究所「欧米地域におけるサイバー保険関連動向」（2019.9）を参照願う。

51 Leonie Maria Tanczer, Ine Steenmans, Irina Brass & Madeline Carr, “Networked world: Risks and opportunities in the Internet of Things” Emerging Risk Report 2018（Lloyd’s, 2018）、Swiss Re, “How data will shape the new urban future”（2019.1）ほか

析・標準化に係るノウハウを提供することにより、プラットフォーム・ルール整備の段階からスマートシティ政策に深く関与することも想定されうる[52]。なお、前記３（2）で説明したとおり、都市政府がスマートシティプロジェクトにおいて収集したデータを民間企業と共有する場合には注意が必要であり、都市政府から保険会社への所定のデータセットに係る API の提供、スマートシティプロジェクトのプラットフォーム運営事業者を介した連携等、状況に応じて適切な方法を採用することが重要となる[53]。

そのほか、保険会社がスマートシティプロジェクトや実証実験[54]に当事者として参加することは、他の提携企業との協働による知見の獲得、今後も増加が見込まれるスマートシティ特有のリスクに対応して市場で先行する機会の獲得・拡大、リスク移転以外の革新的な商品・サービスの開発・提供等につながると考えられる。

６．おわりに

本稿で考察したとおり、スマートシティ政策の実施は深刻化する都市問題の改善や市民の生活の質の向上をもたらすことが期待されているが、その実効性を確保するためには、スマートシティに特有のリスクや都市政策上の諸課題に対処することが必要となる。

スマートシティにおいては様々な都市のインフラが連関するため、関連するリスクの大幅な変容が見込まれている。そのため、保険会社にとっては、これらの複雑なリスクを評価・分析し、スマートシティ化の進展や顧客（都市政府および個人・企業）のニーズの変化にあわせて、最適な商品・サービスを提供していくことが課題となる。その一方で、保険会社はスマートシティ政策に関して都市政府と連携することにより、政策課題の解決に貢献するとともに、より粒度の高いデータに基づいたリスクモデルの改善、直接的・潜在的な市場ニーズの把握、他の提携企業との協働等を通じてビジネスチャンスを獲得できる可能性もある。

世界規模でのスマートシティ化のさらなる進展が想定される中、わが国保険会社においても、海外の先駆例をはじめとするスマートシティ政策の動向および採用される技術がリスクに及ぼす影響等を注視し、自社が提供しうるリスクソリューションや都市政府との連携のアプローチについて整理等を進めることは検討に値すると考えられる。

---

[52] Thom Rickert, “Smart Cities and the Infrastructure Revolution”（Public Risk Magazine, 2019.1）

[53] Loqiva, “Lloyd's Networked World: Addendum”（2018.12）

[54] 関連事例としては、アクサ、パリ市、ルノー、日産自動車等が参加した、都市のモビリティに関する実証実験が挙げられる。アクサは、個人間での自動車貸借サービスへの保険提供の可能性の検討、およびモバイル機器の位置情報を使用した通勤パターンの分析に協力した（CityMakers, “CityMakers First Edition”（2018））。

＜参考資料＞

・外務省「「持続可能な開発目標」（SDGs）について」（2019.1）
・亀井卓也「諸外国スマートシティ動向とデータプラットフォームの実現に向けて」総務省先端技術 WG（第 5 回）配付資料（2016.4）
・国土交通省「スマートシティの実現に向けて【中間とりまとめ】」（2018.8）
・国土交通省「スマートシティモデル事業いよいよ始動～先行モデルプロジェクト等の選定～」（2019.5）
・新華社通信「平安集团将在三亚投 300 亿元进行智慧城市等建设」（2018.11）
・損害保険事業総合研究所「欧米地域におけるサイバー保険関連動向」（2019.9）
・中沢潔「北米（アメリカ、カナダ）におけるスマートシティの取組」ニューヨークだより（JETRO、2019.6）
・八山幸司「米国におけるスマートシティに関する取り組みの現状」調査レポート（JETRO、2015.10）
・日立コンサルティング「スマートシティに関する動向と今後の課題」（2019.4）
・マッキンゼー・グローバル・インスティテュート「スマートシティ：より快適な未来を実現するデジタルソリューション　エグゼクティブサマリー」（2018.6）
・Accenture, “The Global Future of Cyber Insurance - and the London Market's Pivotal Role”（2019.5）
・Adam Rujan & Nicole Simpkinson, “Risk versus reward: Six considerations for smart cities”（Plante & Moran, 2018.8）
・Alicja Grzadkowska, “Smart city technology helps communities mitigate against key risk”（Insurance Business, 2019.6）
・Alicja Grzadkowska, “The rapid spread of smart cities exchanges old risks for new ones”（Insurance Business, 2019.1）
・Amy J. Spencer, “Be Smart about Insurance for the Smart Grid: Coverage for Losses from Cyber Events - Part I”（Blank Rome, 2017.9）
・Anthony R. O’Donnell, “The Rise of ‘Smart Cities’ and Its Implications for Insurers”（Insurance Innovation Reporter, 2017.9）
・AXA, “CityMakers: 9 startups selected to reinvent urban mobility”（2017.9）
・AXA, “Smart Cities: Step into the city of the future!”（2017.3）
・AXA XL, “Smart Cities: Mission Control”（2014.10）
・Bethan Moorcraft, “All stakeholders must work together on ‘smart city’ master plans”（Insurance Business, 2019.5）
・Charlie Campbell, “‘The Entire System Is Designed to Suppress Us.' What the Chinese Surveillance State Means for the Rest of the World”（Time, 2019.11）
・Christine Wong, “Building the smart cities of the future”（Futurithmic, 2019.3）
・Christine Wong, “Smarter, safer and more inclusive communities”（Futurithmic, 2019.3）

・CityMakers, “CityMakers develops innovative urban mobility solutions”（2017.6）
・CityMakers, “CityMakers First Edition”（2018）
・Daniel L. Doctoroff, “Why we’re no longer pursuing the Quayside project - and what’s next for Sidewalk Labs”（Medium, 2020.5）
・Derek Porter, “Why Smart Cities Need Risk Management”（EfficientGov, 2018.11）
・Derek Rice, “Smart City Networks Require Resiliency to Stay Connected in Severe Weather”（StateTech Magazine, 2019.2）
・Donovan Vincent, “New Toronto rules for data collection won’t be in place before final vote on Sidewalk Labs’ smart city project”（Toronto Star, 2020.1）
・Elizabeth Woyke, “A smarter smart city”（MIT Technology Review, 2018.2）
・Frank Ready, “As cyberattacks increase, cities push risky strategy”（Legaltech News, 2019.7）
・Gianni Minetti, “A smart city is an interoperable city”（Smart Cities World, 2019.9）
・Gillian Tett, “Google’s smart city: dystopian nightmare or model for the future?”（Financial Times, 2019.11）
・Ian Austen, “You Can’t Fight City Hall. But Maybe You Can Fight Google.”（The New York Times, 2020.3）
・Ian Duncan, “As Florida cities use insurance to pay $1 million in ransoms to hackers, Baltimore and Maryland weigh getting covered”（The Washington Post, 2019.7）
・IDC, “Smart Cities Initiatives Forecast to Drive $189 Billion in Spending in 2023, According to a New Smart Cities Spending Guide from IDC”（2019.6）
・James Rundle, “Cities Warned Not to Rely on Cyber Insurance Alone”（The Wall Street Journal, 2019.10）
・Kate Conger, Richard Fausset & Serge F. Kovaleski, “San Francisco Bans Facial Recognition Technology”（The New York Times, 2019.5）
・Kate Fazzini, “City ransomware attacks and huge payouts mean a once-private corporate problem has gone public”（CNBC, 2019.6）
・Kyle Funk, Cooper Martin, Nicole DuPuis, Alan Shark & Dale Bowen, “Protecting Our Data: What Cities Should Know About Cybersecurity”（National League of Cities, 2019.10）
・Lawrence Karp & Richard Kim, “Insuring Autonomous Vehicles”（Accenture, 2017.5）
・Leonie Maria Tanczer, Ine Steenmans, Irina Brass & Madeline Carr, “Networked world: Risks and opportunities in the Internet of Things” Emerging Risk Report 2018（Lloyd’s, 2018）
・Leyland Cecco, “'Surveillance capitalism': critic urges Toronto to abandon smart city project”（The Guardian, 2019.6）
・Loqiva, “Lloyd's Networked World: Addendum”（2018.12）
・Marco Chown Oved, “Waterfront Toronto issues final offer to Sidewalk Labs: no guaranteed LRT, no expansion beyond Quayside”（Toronto Star, 2019.10）

・Mark Breading, “Smart Cities and Insurance: Exploring the Implications”（SMA, 2017.8）
・Mark S. Raffman, “'Smart Cities' Raise Novel Issues and Novel Risks”（The Recorder, 2018.10）
・McKinsey Global Institute, “Smart cities: Digital solutions for a more livable future”（2018.6）
・Patricia Mazzei, “Another Hacked Florida City Pays a Ransom, This Time for $460,000”（The New York Times, 2019.6）
・Patricia Mazzei, “Hit by Ransomware Attack, Florida City Agrees to Pay Hackers $600,000”（The New York Times, 2019.6）
・Paul Bischoff, “The world’s most-surveilled cities”（Comparitech, 2019.8）
・Ping An, “Ping An Unveils First Smart City Integrated Platform and Solutions in China to Empower Development with Technology”（2018.8）
・Scott Corwin, Jeff Hood, Anat Dinamani, John Skowron & Derek M. Pankratz, “Cities explore digital mobility platforms: Accelerating the realization of seamless, integrated transportation” Deloitte Insights（Deloitte, 2018）
・Skip Descant, “Columbus, Ohio, Turns to On-Demand Transportation to Improve Medical Access”（Government Technology, 2018.11）
・Swiss Re, “How data will shape the new urban future”（2019.1）
・Thom Rickert, “Smart Cities and the Infrastructure Revolution”（Public Risk Magazine, 2019.1）
・Tom Saunders & Peter Baeck, “Rethinking Smart Cities From The Ground Up”（Nesta, 2015.6）
・Travelers, “Infrastructure for the smart city”（2019）
・Wade Goodwyn, “Ransomware Attacks Create Dilemma For Cities: Pay Up Or Resist?”（NPR, 2019.7）
・William D. Eggers & John Skowron, “Forces of change: Smart cities” Deloitte Insights（Deloitte, 2018）
・Zurich Insurance, “Insurance in the age of the smart city”（2020.1）

＜参考ウェブサイト＞

・国土交通省　https://www.mlit.go.jp/
・AIR Louisville　https://www.airlouisville.com/
・Allianz　https://www.allianz.com/
・AXA　https://www.axa.com/
・Center for Smart Cities　https://www.ict-smart-cities-center.com/
・HDI Global　https://www.hdi.global/
・McKinsey & Company　https://www.mckinsey.com/
・Swiss Re　https://www.swissre.com/
・Travelers　https://www.travelers.com/
・Zurich Insurance　https://www.zurich.com/