Model Policy

Privacy Impact Assessment

G20 Global Smart Cities Alliance

本モデルポリシーは G20 Global Smart Cities Alliance の基本原則である **Privacy & Policy** に属する一つのポリシーです。本ポリシーの実装に伴う補完的な情報については、GSCA のウェブサイト[1]にも記載をしています。

Background / 背景

世界中の都市は驚異的なスピードで成長しており、経済的な機会や快適さを求める住民が集まっています。市政府は、市民中心のサービスを可能にするテクノロジーや「スマートシティ」ソリューションを導入し、より持続可能で、包括的で、開かれた都市へと発展させることで、その継続的な成長に対応しています。こ

[1] Visit https://globalsmartcitiesalliance.org/

れらの目標を達成するためには、あらゆる規模の都市とコミュニティが、これらのテクノロジーによって生成された個人とコミュニティに関するデータが適切に保護され、保護されていることを確認しなければなりません。

データの収集は、公共料金の支払いからウェブページの閲覧、市道を歩く姿や、公共交通機関の利用、自動車の運転といった様々な日常生活をサポートする都市運営の中で行われています。例えば、センサーやコネクテッドデバイスが常時接続され、データが流れることで、交通システムの管理や、公共インフラ全般におけるリアルタイムメンテナンス、全自動の公共サービス、透明性のあるガバナンスとオープンデータの実現、公共エリアでの救急サービスのサポートなど、スマートテクノロジーの利用は行政と市民の双方に便益をもたらします。たとえ、これが善意の取り組みであったとしても、個人のプライバシーを侵害するリスクを生み出し、監視への恐れを高めることによって都市生活の利点を否定し、個人が公共空間に関わることへの阻害にも繋がりかねません。

新たに台頭したテクノロジーやビジネスシステム、法律や規制の変化と複雑化、さらには世間の注目を浴びるようになったことから、都市は、プライバシーとデータ保護を積極的かつ体系的に活動に組み込むための適切な措置を講じることが求められています。プライバシーは、伝統的に、さまざまな権利を包含するより広い概念として理解されている一方、データ保護とは、個人データの収集、使用、処理に関連し、個人を保護することを意味します。

都市は、事業を遂行するためにデータを利用・共有するという自らの必要性と、より広範な公共の福祉や個人のプライバシーの利益との間で、公共の信頼を構築し維持する方法でバランスを取らなければなりません。市民の信頼が得られなければ、スマートシティ技術の恩恵を享受し続けることはできません。都市は、個人、地域社会、技術提供者が責任を持ってデータを利用することで、個人や地域社会のプライバシーリスクを最小限に抑えながら、その恩恵を最大限に享受できるような政策と実践に投資しなければならないのです。

プライバシー影響評価（PIA）ポリシーを実施することで、都市はプライバシーリスクを特定、評価、対処するための一貫した方法を確立することができます。世界各国では、プライバシーやデータ保護に対する文化的・法的なアプローチに大きな違いがあるため、モデルとなる PIA ポリシーを作成するのは複雑な作業となります。本ポリシーでは、従うべきプロセスと考慮すべき問題点を規定することで、都市がより自信を持って、地域社会の期待に沿った形でプライバシーリスクを検討し、対処する可能性を高めることができると期待しています。

Contents / コンテンツ

Model Policy / モデルポリシー **3**
Objectives / 目的 3
Foundations for Privacy Impact Assessments / PIA の基本要件 4
1. Organizational Values and Risk / 組織の価値観とリスク 4
2. Scope and Timing / 範囲とタイミング 5
3. Tools and Components / ツールと構成要素 7
4. Roles and Responsibilities / 役割と責任 8
5. Monitoring and Recordkeeping / 監査と記録 11
6. Transparency & Engagement / 透明性とエンゲージメント 12
Fundamentals of a Privacy Impact Assessment / PIA の構成要素 13
Additional Guidance & Resources / 追加情報 **16**
Acknowledgements / 謝辞 **17**

Model Policy / モデルポリシー

Objectives / 目的

市は、必要なサービスを提供するために情報を収集することと、特に革新的なスマートシティ技術を導入する場合には、市民のプライバシーを保護することとの間に公正なバランスを見出すように努めなければなりません。プライバシー影響評価（PIA）は、不可欠なプライバシー評価ツールです。PIA は、収集から廃棄に至るまでのデータのライフサイクル全体を通して、プライバシーリスクを特定し、管理するための一連のプロセスで構成されています。スマートシティにおける技術の取得や使用に先立って PIA を実施することは、透明性と説明責任を高め、市民の信頼を支え、潜在的なプライバシー侵害を回避し、コンプライアンスを改善して法的リスクを軽減します。PIA の実施によってデータや技術に関し、市職員、そのパートナー、市民による、より確かで一貫した意思決定を可能にすることができます。

市の PIA ポリシーは、プライバシーリスクの特定と軽減において、対処すべき問題と従うべきプロセスを特定すべきです。具体的には、PIA ポリシーは、以下に留意する必要があります。

- PIA ポリシーはデータと技術の具体的な目的、潜在的なプライバシーリスクと軽減策を明確にし、市と地域社会の価値観、優先順位、法的権利と照らし合わせて評価すべきです。
- PIA ポリシーは、プロジェクト全体とデータのライフサイクルとが一致している必要があります（これには、部門を超えて発生する調達、データセキュリティ、アクセシビリティ、公的記録に関する事が含まれます）。
- PIA ポリシーは、特定の時点で「個人」または「個人を特定できる」と見なされるデータだけでなく、テクノロジーまたはサービスによって収集されるすべてのデータに対処する必要があります。
- PIA ポリシーは個人情報の取り扱いに関する社内外のコミュニケーションと協力を促進し、市が特定の技術への再考や、地域社会、パートナー、技術提供者に通知する際に、明確な理解が得られるようにします。
- PIA ポリシーは、個人のプライバシーや社会全体への悪影響を最小限に抑えつつ、倫理的な意思決定を支援し、データの有益な利用を最適化することで、イノベーションを加速させます。
- [より参加型のオプション]: データとテクノロジーの実践に関する市民の参加と意思決定のために、ワークショップや集会など、多様な機会を設けることも重要です。

> **Examples（具体的な事例）：**
>
> - http://www.longbeach.gov/globalassets/health/healthy-living/office-of-equity/clb_toolkitbook_singlepages
> - https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/691383/Consultation_Principles__1_.pdf

Foundations for Privacy Impact Assessments / PIA の基本要件

本セクションでは、PIA ポリシーの具体的な目標である、個人および地域社会の社会的利益を最大化し、リスクを最小化するという全体の目的を達成するための基本的な要件について記載します。

1. Organizational Values and Risk / 組織の価値観とリスク

a. 都市は、PIA プロセスにおいて、特定の技術やサービスが評価される際の公共の価値、優先順位、プライバシーの原則を明示的に示すべきである。

Examples（具体的な事例）：

- NYC's IOT Guidelines
- Seattle's Privacy Principles
- Barcelona's Digital Service Standards
- India's Data Smart Cities Strategy

b. 市は、PIA プロセスにおいて特定の技術やサービスが評価される際の法的基準や権限、既存の市の方針や原則を明確に示すべきである。

c. PIA は、リスクと利益を評価する際には、倫理、公平性、行政による関与など、法令遵守以外の考慮事項を考慮に入れるべきである。これらの考慮事項には、個人への影響だけでなく、グループへの影響も含まれるべきである

d. [より高い成熟度のオプション]: PIA プロセスには、上記で特定された価値観に基づいて算出されたスコアリングモデルの適用を含んでも良い。

Examples（具体的な事例）：

- https://wellington.govt.nz/~/media/about-wellington/emergency-management/files/covid-19/wcc-privacy-impact-assessment-digital-contact-tracing.pdf?la=en

e. [より参加型のオプション]: 市の職員や、市民、特に社会的弱者を巻き込み、広範な市民の価値観、原則、リスクのしきい値を決定する。モデル化においては、市民協議会、市民ボランティア活動、市民集会等の議論や、市財政や予算編成における電子投票、草案の公開注釈、ソーシャルメディア等の活用を含む。

2. Scope and Timing / 範囲とタイミング

a. 初期評価（または完全な PIA の必要性を判断するための他のしきい値分析）は、以下のタイミングで実施すべきである。

i. あらゆる新技術の開発又は調達において、可能な限り早期に実施する。［具体的には、プライバシー保護を調達基準や開発規範に組み込む事を含む］。設計・実装後に

プライバシーリスクを低減するためのシステム改修を行うことは、よりコストがかかることが証明されている。

ii. 既存のプロセスやシステムの重要な変更を計画する場合に実施する。これには、新たにデータ活用を行う場合や何らかの変更といったプロジェクトが更新されたタイミングを含む。

b. 市の規則や政策で要求されている場合、または初期評価で以下のように判断された場合には、完全もしくは部分的な PIA を実施すべきである。

i. 個人を特定する可能性のあるデータのための新しい技術、新しい目的、または新しいプロセスが導入される場合。

ii. システム内の他の情報と個人情報との物理的または論理的な分離に影響を及ぼす可能性のある方針、業務プロセス、またはシステムの大幅な変更が計画されている場合。

iii. 機密性の高いデータが処理される場合、または技術やサービスにより高リスクのデータ処理が可能になる場合［例えば、個人のスコアリング／プロファイリング、系統的なモニタリング、大規模処理、複数のソースからのデータのマージまたはマッチング、子供または社会的弱者をターゲットとしたもの、身体的危害のリスク、または新しい技術の使用や既存技術の新規適用など］

iv. 技術またはシステムが自動的もしくは半自動的に、個人に対し、影響を及ぼすような意思決定を行う場合。

c. 必要に応じ、データ収集が可能となる技術を、市内に実装する前に、もしくは市の意思決定プロセスに実装する前に、PIA を実施すべきである。

d. PIA は、収集時に 法的に「個人的」または「個人を特定できる」とみなされるデータが収集されるときだけでなく、技術やサービスによって収集されたすべてのデータを評価するために実施すべきである。

e. PIA は包括的なプライバシープログラムの一部に過ぎないため、データを収集しないこと、プライバシー保護に関する技能訓練、規制、各地方自治体や当局の方法の中での PIA の監査と公表といった各種の取り組みを並行して行うべきである。

3. Tools and Components / ツールと構成要素

a. 市は、完全な PIA [または非個人データの倫理的影響評価]の完了など、さらなる検討が必要かどうかを明らかにするために、予備的な初期評価またはその他のしきい値分析を策定し、実施すべきである。

b. 初期評価では、システム、製品、またはサービスによって引き起こされるプライバシーリスクの初期評価が行われるべきである。これには、詳細なデータフロー図や、予備的なデータと使用特性等が含まれる。

> **Examples（具体的な事例）：**
>
> - Helsinki Initial Assessment
> - Seattle's PIA Policies
> - Toronto's PIA Policies

c. 完全な PIA が必要であると判断された場合、その完全な PIA には以下の点が含まれるべきである（詳細は下記「PIA の構成要素」を参照）。

i. プライバシーリスクの評価 - プライバシーリスク評価を実施することで、システム、製品、またはサービスに起因するプライバシーリスクを特定し、それらに優先順位をつけて、リスクへの対応方法について十分な情報に基づいた意思決定を行える。

ii. リスク対応の決定 - 評価されたリスクにどのように対応するかを決定する際には、市は組織の価値観とリスク許容度の決定を参考にすべきである。対応方法としては、以下のようなものが含まれる。

- **軽減**（リスクは、データの最小化などの技術的・政策的措置により、許容可能なレベルにまで下げることが可能）。
- **移転/共有** （リスクは契約や保険などにより他の当事者と共有される。同意取得は、個人のリスク共有の形態の一つであり、個人は、その情報の提供に関して同意を求められる前に、関連するリスクがどういうものか合理的に理解可能となる） 。
- **回避** （都市は、リスクが便益を上回る場合には、特定の技術を使用しないことを選択したり、 特定の種類のデータ処理を行わないことを選択したりできる）。

- **保有**（都市は、悪影響の可能性や影響が低く、利益が大きい場合には、リスクを受け入れることを選択できる）。

iii. 市が設定すべき要件と管理権限

- **法的義務の適用**（組織としてのプライバシーに関する要求事項は、市が遵守する法令、プライバシーに関する価値観および政策を示す手段である。組織としてのプライバシーに関する要求事項は、法的環境（例えば、法律、規制、方針、文化的価値観、関連する基準、 プライバシー原則など）やリスク低減が可能と判断されたリスクなど、様々なものから導き出されます。

- **軽減可能なリスクへの対処**

d. 市は、PIA の実施およびプライバシーリスクの評価のための専門的なガイダンス、テンプレート、ツールについて、各地のデータ保護当局やその他のプライバシーおよびデータ保護の専門家に相談すべきである（下記の追加ガイダンスを参照）。

> PIA を実施するにあたって確実な方法は、最初にワークショップを行う方法であり、必要なすべての利害関係者によって行います。責任の割り当ては、最初の会議で行われます。最初の会議の後に行う、影響評価に関するワークショップ（複数回になる場合があります）では、専門家は事前に担当範囲についての整理をしておきます。なお、データの文書化をツールにしていく作業は、共同で行うことができます。

4. Roles and Responsibilities / 役割と責任

a. チーフ/シティ・プライバシー・オフィサー（CPO）などの指名された上級職員（必要に応じて専任のプライバシー・チームのサポートを受ける）は、以下の点について責任を負うべきである。

i. 市の初期評価と PIA ツールのための適切なテンプレート、リソース、コンポーネントの開発。

ii. PIA の実施に関する基準と実施に伴うリソースの資格要件を設定すること。

iii. 初期評価の見直し、またはその他 PIA が必要な場所を決定すること（既存の PIA の再検討を含む）。

iv. プライバシーへの影響を低減するための要件や勧告を提供することを含む、PIA の実施と承認を行うこと。

v. PIA の過程で提起されたプライバシー及びセキュリティ上の懸念を解決するために、他の関係者と連絡を取り合うこと。

vi. 特定されたプライバシーリスクに対する市の対応を決定すること。

b. 庁/部局/プログラム担当者は以下の点について責任を負うべきである。

i. 提案された技術とその利用に関する適切な情報と文書の提供（例：技術の機能性、ビジネスケース、提案された目的、継続的なプライバシーとセキュリティ保護のためのコストなど）。

ii. 初期評価の実施、および必要に応じた完全な PIA の実施の支援。

iii. 提案された技術に関連するリスクを軽減するために、必要に応じて、PIA で特定されたデータの利用及び管理計画、並びにすべての適切な保護措置を実施すること。

iv. PIA の方針が職員に伝達され、職員が PIA プロセスに参加するための十分な時間と資源が与えられていることを確認すること。

v. プライバシーに影響を与える可能性のある技術の使用に先立ち、必要に応じて PIA を認可し、承認すること。

c. 市長や最高技術責任者などの幹部または上級職員は、以下のような PIA ポリシーの遵守を監督する権限を持つべきである。

i. PIA ポリシーが全職員に伝達され、実施されることを確認すること。

ii. プライバシーとセキュリティ要件を尊重しつつ、情報が可能な限り共有され、アクセスできるようにすること。

iii. 指名されたプライバシー担当上級職員及びその他の職員が日常的に PIA を実施できるように、適切な予算及び組織構造を提供すること。

iv. 適切な説明責任措置（例えば、エスカレーション手順、スタッフの研修と認識、報告システム、プライバシーに関連した苦情や潜在的な脅威の受け付けなど）を開発し、実施すること。

v. PIA ポリシーの有効性と成果を監視すること。

vi. スマートシティプロジェクトのスケジュールと PIA のスケジュールの整合性を見直すこと。

d. 特定の技術やサービスの性質を考慮して、必要に応じ、以下のような追加の市職員や外部の利害関係者に相談すべきである。

i. PIA プログラムに助言し、各部局の参加を促すことができる市幹部や市議会議長等の代表者

ii. 技術システムの設計、データセキュリティリスクの評価及び軽減を支援する CISO 又はその他の IT 専門家

iii. 適用されるデータ保護規則を含む法的基準の遵守を確実にするための、市の弁護士または法律顧問

iv. データが開示される範囲を明確にするための（意図的にまたは法律で）公的記録に関する担当者とオープンデータに関する担当者

v. 調達担当者

vi. データまたは技術に関し別の視点をもたらす他都市の公務員

vii. 特定分野の外部専門家

viii. 技術パートナー

ix. 影響を受けるコミュニティのメンバー

e. [より成熟したオプション]: 上級プライバシー担当者は、データ保護、リスク管理、セキュリティの専門家によってサポートされ PIA を実施する。データプライバシーチームは、市全体のプライバシーチャンピオン（PIA プロセスを支援する特定分野の専門家）ネットワークによってサポートされ PIA の実施プロセスを支援する。PIA チームは、組織の知識とベストプラクティスを構築し、市全体で

より一貫性のあるプライバシーの意思決定をサポートし、PIA のプロセスと結果を改善する機会を明確にする。

> **Examples（具体的な事例）：**
>
> - Toronto RMIS w/in I&T division
> - Seattle privacy champions

f. [より参加型のオプション]: 外部の機関または組織が、意見、勧告、コミュニティの専門性の活用、または PIA 実施の承認を行うために従事する。このグループには、プライバシーやデータ保護の専門家やコミュニティのメンバーなど、多様な利害関係者の代表者が含まれる。

> **Examples（具体的な事例）：**
>
> - Seattle Surveillance Working Group
> - Oakland Privacy Advisory Commission

5. Monitoring and Recordkeeping / 監視と記録

a. すべての初期評価と PIA は、書面で完全に文書化され、市の記録保持の規則に従って維持されなければならない。

b. PIA レビューの結果、除外されると判断された技術も、記録され、文書化されなければならない。

c. もし市に複数の PIA がある場合は、PIA を種類に応じて分類することができる。

d. 地方自治体は、かつては個人を特定できないと考えられていたデータが時間の経過とともに個人を特定できるようになるのを防ぐために、[3 年に 1 度] 程度、IoT テクノロジーまたはサービスによって生成されたすべてのデータを一緒に評価することで、都市は将来に渡りより確かな評価ができるよう、PIA プロセスの見直しまで含めた運用を策定すべきである。

e. 個人情報保護のために指名された上級職員は、PIA ポリシーを毎年（必要であればそれよりも早く）見直し、必要に応じて更新すべきである。

f. 市の部局、課、プログラム、およびパートナーやサービス提供者は、PIA 方針の遵守度を評価すべきである [内部監査、プログラムレビュー、またはプログラム評価の実施など]

g. 市がプライバシーに関する苦情を受けた場合や、プライバシー侵害が発生した場合には、プライバシー担当の上級職員が調査を行い、必要に応じて状況を改善する。

h. [より成熟度の高いオプション]: 都市は、データを処理するシステム／製品／サービスの目録を作成し、維持するべきである。これには、システムやその構成要素に関する所有者や運用の役割、データの出所、発明されたシステムのデータアクション、データアクションの目的、データ処理環境が記載される。

> **Precedents（先行事例）：**
>
> - Seattle's inventory of surveillance tech
> - Amsterdam's IoT Registry
> - Barcelona's Sentilo
> - City of Boston's pilot of Digital Transparency in the Public Realm
> - NIST privacy framework

6. Transparency & Engagement / 透明性とエンゲージメント

a. 可能な限り、都市は、すべての PIA を、アクセスしやすく、外部に向けたウェブサイトで公開すべきである。

> **Precedents（先行事例）：**
>
> - Seattle PIA and SIR inventory
> - Wellington DCTT PIA

b. 市は、組織や個人がデータの処理方法や関連するプライバシーリスクについて信頼できる理解を持ち、対話を行うことができるよう、適切な活動を開発し、実施すべきである。

c. 都市は、スマートシティ技術に関連したデータ処理の目的、慣行、プライバシーリスクを、関連する PIA に基づいて知らせるための仕組み（通知、内部報告書、公開報告書など）を開発すべきである。

d. [より参加型のオプション]: データ処理および関連するプライバシーリスクに関する個人からのフィードバックを得るための仕組み（調査やフォーカスグループなど）が確立され、実施される。

> **Supplementary guidance（追加ガイダンス）：**
>
> - PIA では、頭字語、スラング、または外部の聴衆にあまり知られていないその他の用語の使用を避ける必要があります。さらに、回答は、トピックに不慣れな聴衆がアクセスできるように、主に非技術的な言語を使用して作成する必要があります。
> - サイネージは、関連する地域のプライバシー規制に準拠するために、必要に応じてその場で提供する必要があります[また、データの収集および処理活動を一般に知らせるために、IoT テクノロジーの新規導入や新規展開を検討する必要があります]。

Fundamentals of a Privacy Impact Assessment / PIA の構成要素

このセクションでは、データとテクノロジーによる公共の利益を最大化しながら、都市とそのパートナーが潜在的なプライバシーリスクを効果的に特定、軽減できるようにするため、PIA で取り組むべき基本的な問題や疑問点を説明します。

PIA は、以下で説明するように、明確で分かりやすい必要があります。

1. テクノロジーの使用や説明責任を負う対象である、市の部局やプログラム、パートナーやサービス提供者を特定すること。

2. 設計または取得するテクノロジーについて、それらの一般的な能力や機能、生成される可能性が高いデータの種類、収集された個人情報のソースと正確性の説明について記述すること。（市の部局が提案した用途以外で合理的に予測可能な監視能力を含む）

3. 個人やコミュニティ、社会一般に対する想定価値や便益（それらを証明するデータや研究）を含む、テクノロジーの目的や利用案を記述すること。テクノロジーが解決しようとしている問題や、侵害性の低い代替技術の有無についても記述すること。

4. 必要に応じて、提案されたテクノロジーに関する個人データを収集、利用、開示するための市の権限を記述すること。

5. テクノロジー評価が行われている、公共の価値や原則、法的基準、組織的リスクフレームワークについて記述すること。

6. 提案されたテクノロジーの使用に関する潜在的なプライバシーリスクを評価、記述すること（リスクが発生する可能性や個人、コミュニティへの潜在的な影響の重大性を含む）

7. 組織の価値観とリスク許容度 [リスクの軽減や移転・共有、回避、受容など] を踏まえて、特定されたリスクへの市の対応を記述すること。

8. 提案されたテクノロジーの利用について、以下のような、明確な利用方針とデータ管理ポリシーを記述すること。:

    a. テクノロジーがいつ、どのように提供され、使用されるか、誰によって行われるか（必要に応じ、誰がどのような条件で、データの所有権やライセンス権を持つのかの記述を含む）

    b. テクノロジーを統制する追加の規則（犯罪捜査目的など、テクノロジーを使用する前に満たすべき法的基準を含む）

    c. データをどのように安全に保存し、破棄し、非識別化するか.

    d. データが識別可能、識別不可能な形態で、どのくらいの期間保持されるか

    e. データへのアクセスをどのように監視および管理するか（アクセスログや監査を含む）

    f. 技術やデータを共有するかどうか、共有する場合はどのような条件か（パートナーやサービス提供者、他の政府機関、研究者、公文書要求、オープンデータなどの日常的な共有と、緊急事態の場合の両方を含む）

    g. テクノロジーを扱い、データにアクセスする全ての職員が、市のポリシーを遵守してテクノロジーを使用することを保証するため、どのようなトレーニングと説明責任の施策を行うのか

    h. データの機密性、完全性、可用性を確保するために、どのような保護策があるか（ランサムウェアやマルウェア、IoT 脆弱性などの脅威からの保護を含む）

i. テクノロジーの使用に関する潜在的なプライバシーリスクの軽減を目的とした、その他の法的、組織的、物理的、技術的な保護策

9. 実施された地域活動と今後の地域活動計画、受け取ったコメントと市の回答、テクノロジーの取得と使用から生じる可能性のある近隣住民への影響と差別的効果についての市の結論を記述すること。

10. データの使用方法やデータの管理プロセスを変更する可能性のある、緊急事態や防衛上の理由についても記述すること。

11. テクノロジーによる、市民の権利と自由に与える潜在的な影響と、社会的弱者への潜在的な差別的効果の影響が、どのように考慮、軽減されるかを記述すること。

12. テクノロジーの運用に関するプライバシーおよびデータ保護の維持コスト（人件費、法令遵守、監査、データ保持、セキュリティコストなど）のための資金調達ついて記述すること。

Additional Guidance & Resources / 追加情報と資料

Examples of City PIAs / 各都市の PIA ポリシー

- Helsinki Data Register and DPIA tools
- Huron County Privacy Impact Assessment Policy
- Santa Clara County Surveillance Use Policies
- Seattle PIA Reviews and Surveillance Reports
- Toronto Privacy Impact Policy
- Wellington Digital Contact Tracing PIA

Guidance on conducting a PIA or DPIA / PIA と DPIA 実施ガイダンス

- The former Article 29 Working Party's Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" (2017) + EU member state DPIA whitelists and blacklists (2019)
- French DPA/CNIL -- Privacy Impact Assessment resources *(available in French and English),* including guidance, templates, knowledge bases, IoT examples, infographic, and a free software tool (2018)
- Spanish DPA/AEPD's modelo de informe de Evaluación de Impacto en la Protección de Datos (EIPD) dirigido a Administraciones Públicas (2019) *(available in Spanish)*
- Australian OAIC -- Public Sector Chief Information Officer Council (PSCIOC) Guide to undertaking privacy impact assessments
- New Zealand Privacy Commissioner -- Privacy Impact Assessment Handbook
- Canadian OPC -- PIAs guidance
- Bureau of Justice Assistance -- U.S. Department of Justice, Guide to Conducting Privacy Impact Assessments: for State, Local, and Tribal Justice Entities (2012)
- NIST Privacy Framework A Tool for Improving Privacy through Enterprise Risk Management
- Sidewalk Labs, Responsible Data Use Assessment - Digital Innovation Appendix Section 2.2.3, page 237 - 295
- UN Global Pulse, Risks, Harms, and Benefits Assessment
- SynchroniCity: Delivering an IoT enabled Digital Single Market for Europe and Beyond

Acknowledgements / 謝辞

Co-leads / 執筆者代表

Kelsey Finch, Senior Counsel, Future of Privacy Forum

Michael Mattmiller, Director of Government Affairs, Microsoft

Task Force Members: / 参加メンバー

Pasquale Annicchino, Lex Digital and Archimede Solutions

Sean Audain, Wellington City Council

Chandra Bhushan, Quantela

Dylan Gilbert, Privacy Policy Advisor, NIST

Naomi Lefkovitz, Program Manager, NIST

Jacqueline Lu, Co-Founder, Helpful Places

Eugene Kim, Associate Director, Privacy and Data Governance, Sidewalk Labs

Dan Wu, Immuta

Contributors and reviewers: / 貢献者および批評者

Hector Dominguez-Aguirre, City of Portland

Dilip Krishnaswamy, VP of New Tech R&D, Reliance Jio

Masaru Yarime, Ph.D., Associate Professor, Division of Public Policy (PPOL), Hong Kong University of Science and Technology

About the G20 Global Smart Cities Alliance

2019 年 6 月に設立された「G20 Global Smart Cities Alliance for Technology Governance」は、スマートシティテクノロジーの責任ある倫理的な利用のための共通原則を、自治体・政府、民間企業、市民の連携を目指すものです。官民協力の国際機関である世界経済フォーラムがアライアンスの事務局を務めます。

本アライアンスでは、政府、民間企業、市民社会のグローバルな専門家が、倫理的なスマートシティの実現に必要なモデルポリシーを策定するために、世界中の政策をまとめ、分析しています。

アライアンスのモデルポリシーやその詳細については、こちらをご覧ください。
https://globalsmartcitiesalliance.org/

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland
Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
info@globalsmartcitiesalliance.org
https://globalsmartcitiesalliance.org/

Cover: Forum Stock Images