モデルポリシー(案)

Cyber Accountability

G20 Global Smart Cities Alliance

本モデルポリシーは、G20 グローバル・スマートシティ・アライアンスのポリシーフレームワークにおける「**セキュリティとレジリエンス**」原則の基礎のひとつに位置づけられるものです。本書の採用と実施のための実践的なサポートを提供する補足的なコンテンツは、当社のウェブサイト[1]に掲載されています。

Foreword

現代の都市はサイバー攻撃の脅威に直面しています。例えば、2016 年には、米国の 4 分の 1 の都市が、1 時間ごとにサイバーセキュリティ攻撃を受けていたとのことです[2]。また、2019 年には、米国の地方政府は 163 件のランサムウェア攻撃によるセキュリティ侵害により、180 万ドル(約 1 億 8 千万円)以上の身代金を支払い、セキュリティ侵害の回復に数千万ドル(約数十億円)を費やしたという報告もあります[3]。(2018 年の報告と比較すると、約 150%増加しており、損害が深刻化していることを示しています。)

スマートシティに用いられる技術は社会的なメリットとともにサイバー攻撃に対するリスクの増加ももたらします。スマートシティ化に伴う情報システムと運用技術（OT）システ

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

[2] Deloitte, Making Smart Cities Cyber Secure.

[3] Cities Today, Should Cities Pay Cybercriminals?

ムの統合によって、サイバー攻撃者に多数の「入口」を提供することにつながるからです。また、都市の中に異なる種類の技術プラットフォームやデバイスが混在する状態は、隠れた脆弱性を生み出す可能性があります。特に、デバイス管理のための共通の標準がない場合、そうした脆弱性は増える傾向があります。

例えば、相互接続されたデバイスは、2019 年には 84 億台でしたが、2020 年末には 200 億台へ急増すると予想されています[4]。システム統合が進んだ都市でこうしたデバイスがサイバー攻撃を受けると、その被害は単なるデータの損失や財政的な影響、風評被害のリスクにとどまりません。システム間でカスケード効果が発生し、緊急対応や輸送、電力網、教育などのサービスが全面的に中断される、という社会的コストが生じるおそれすらあります。

加えて、都市は今、スマートシティ化による市民サービスの向上に加え、高度に分散化され、どこからでも仕事ができるようになった労働環境という、新たな運用上の現実にも対処することを求められはじめました。従来のサイバーセキュリティのアプローチ - システムをサイロ化し、サイロの境界をネットワーク監視することでサイバーセキュリティを確保するアプローチ - は、あらゆるものがお互いにつながっている現在の環境においては、もはや効果的ではありません。

例えば、OT システムは、障害が発生した場合には物理的な影響が大きくなる可能性のあるインフラを制御しているシステムであり、従来は隔離されたネットワーク内に構築してきました、。このような OT システムの分野でも、IoT の導入、クラウドへの移行、および第三者の他システムとのデジタル統合が進み、OT システムは今やリスクの高い領域となっています。

このように都市が技術の導入に力を注いだ結果として、サイバー攻撃にさらされうる「入口」は拡大し続け、そこからあらゆるシステムに攻撃が可能となっています。都市のシステムは攻撃に対してより脆弱になっているとさえ言えるのです。

政府にサイバーセキュリティに対するより高度な対応が求められるようになり、多くの都市が最高情報セキュリティ責任者（CISO）またはそれに類する役職を任命してきています。この責任者は、スマートサービスの効果的なサイバーセキュリティの設計と展開を評価・指示・監視し、セキュリティの不備に対する責任を負う役職です。都市に CISO という特定の役職を設けることは重要ではなく、サイバーセキュリティのアカウンタビリティについて都市が確固たるモデルを持つことが重要で、都市のサイバーセキュリティを改善し、ひいては高いサイバーセキュリティを確保した都市を実現するための基礎を築くことにつながります。

---

[4] World Economic Forum, 2018. Our Exposure to Cyberattacks is Growing – We Need to Become Cyber Risk Ready

本ポリシーの目的は、世界中のすべての都市に適用可能なサイバーセキュリティ・アカウンタビリティ・モデルを定義することにより、都市と市民が保有する情報資産及び運用資産を保護することにあります。都市がサイバーセキュリティを維持・構築するにあたって優先順位をつける際に参照できる枠組みを提供することを目指しています。

都市のガバナンス構造に差異があることは認識した上で、あらゆる都市に参考となるアカウンタビリティの明確な規定を作成するという意欲的な取組みであると考えています。

How to use this Accountability model policy

このポリシーを策定したチームの調査やインタビューの結果、都市の CISO は、自分が直接管理していないシステム（中央の IT 部門以外の部門が調達したり、管理したりしているもの）についても、責任を問われる可能性があることがわかりました。我々は、アカウンタビリティ(説明責任)は一人の人間が果たすのが最善であると考えていますが、都市のガバナンス構造の変更には時間がかかることも認識しています。一人の人間が説明責任を負う形はめざすべき姿とも言えます。本ポリシーは、一人が説明責任を負う体制を想定して書かれていますが、中央の IT チーム／CISO のオフィスと業務部門の間でアカウンタビリティを共有するする場合にも適用できると考えています。

つまり、都市がこの「アカウンタビリティ」ポリシーを実装するにあたっては自由度があるのです。必要な責任事項がすべて網羅され、誰が何の責任を負うのかが明確であれば、複数の責任者(Senior Officer)が共同で「アカウンタビリティ」を担っても構わないでしょう。ただ、複数の役割を設けるのであれば、その役割の間での協力の程度が明確に定義され、担うべき責任全体が共有され、それらが更新され続けている必要があります。例えば、役割間で、サイバーセキュリティに関する KPI や関連するスケジュール、明確なエスカレーションの階層などについて意識共有がされている必要があります。

このポリシーは、内部文書/公開文書のいずれかのポリシーを策定する場合や、都市におけるサイバーセキュリティの責任を負う役職の職務定義を策定する場合の基礎資料としてご活用ください。

Contents

モデルポリシー(案)

定義

サイバーセキュリティとは？

サイバー空間における情報の機密性/完全性/可用性を保持することです。

ここでのサイバー空間は、人やソフトウェアサービスがデバイスやネットワークを介してインターネット上で相互に作用しあう複雑な環境であり、如何なる物理的な形も存在しません[5]。

サイバーレジリエンスとは？

サイバーセキュリティは、データやデータインフラの機密性/完全性/可用性を保護することでサイバー攻撃に対する被害を和らげるために重要な役割を担います。しかしながら、サイバーセキュリティだけでは不十分です。

サイバーレジリエンスは、セキュリティ侵害が発生した場合にも ICT システムがサービスを提供し続けることを指し、サイバーセキュリティのさらに一段先の段階に進んだ概念と言えます[6]。

[5] Note 1: In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.
Note 2: Adapted from the definition for information security in ISO/IEC 27000:2009.
[6] McKinsey, 2018. Smart City Resilience: Digitally Empowering Cities to Survive, Adapt and Thrive.

スマートシティにおけるサイバーセキュリティ、サイバーレジリエンスとは？

都市にとってのサイバーレジリエンスは、リスクに対する準備/対応/見直しの能力であると考えることができます。サイバーレジリエンスを構築することは、サイバー攻撃や自然災害に直面した場合の都市機能の維持や復興に重要な役割を果たします[7]。

物理的およびデジタルインフラの統合、インターオペラビリティの確保、さらには都市のシステムやデータの相互接続は、今まさに多くの都市で取り組まれている内容です。スマートシティにおけるセキュリティ(機密性/完全性/可用性/レジリエンス)の目的は、(データを守るという)既存の IT システムに対する目的のみならず、(システムやプロセスの安全性や機能維持を担保するという)OT システムに対する目的も設定されるべきです。IT と OT のセキュリティ目標を組み合わせることが、都市がより安全でレジリエントな運用環境を実現することにつながると言えます[8]。

(本書における)「アカウンタビリティ」では、IT と OT の両方を担当する一人の責任者を置く形態、またはそれぞれの領域（IT と OT）で責任者を置く形態が含まれるでしょう。何が適切な形態であるのかは、都市が自身の権限において決める必要があります。

スマートシティにおける責任とアカウンタビリティとは？

都市においてサイバーセキュリティがよく維持されているとは、ある最高責任者あるいはその都市の中のキーパーソンのグループがあらゆるセキュリティ侵害に対して最終責任を負うということです。この責任者(ら)は、スマートシティの個々の施策やサービスに対して効果的なセキュリティ対策が設計/実装されているかを評価、監督し、監視しなければなりません。また、何らかのセキュリティ侵害が発生した場合の対処、復旧にも責任を持たなければなりません[9]。

1. はじめに

1. 本ポリシーは「サイバーセキュリティのアカウンタビリティに関するポリシー」であって、[公文書/内部規定]として発行されることにより効力を発揮するものです。

[7] Ibid
[8] Deloitte, Making Smart Cities Cyber Secure.
[9] Governance Principles of COBIT 5

2. 目的

1. [都市]は、すべての情報および物理的インフラ(物理的およびクラウドインフラ、デバイス、ネットワーク、データ、アプリケーション、ユーザを含みますが、それだけに限定されるものではありません)のサイバーセキュリティとサイバーレジリエンスの確保に責任を持ちます。

2. 本ポリシーの目的は、[都市]におけるサイバーセキュリティのアカウンタビリティのモデルを規定することにあります。ここでは、一人または複数の最高責任者が、サイバーセキュリティに関する意思決定を行い、サイバー攻撃による[都市]のブランド低下、業務の混乱、財務上の損失、法的責任、市民の信頼喪失といった被害から[都市]を守る責任と権限を持ちます。その意思決定を的確に実施するためには監督やリソース確保に対する最終決定権限と責任が必要になります。

3. 主たる責任項目 (必須項目)

1. リーダーシップとアカウンタビリティ

a. スマートシティのサイバーセキュリティを含め、都市におけるサイバーセキュリティは、都市の最高幹部レベルが責任を負うものです。

b. 一人の最高責任者が、すべての IT および OT インフラ(ユーザやデバイス、ネットワーク、データ、アプリケーションなどを含みます)に対するサイバーセキュリティを適用する最終決定権限と責任を持ちます。

c. 上記最高責任者は、都市の最高幹部の一人であるか、都市の最高幹部チームに対して直接報告する権限を有する者とします。

d. 最高責任者は、市が定義したパフォーマンス指標に基づいて、サイバーセキュリティ関連のすべての事項を報告する責任を有します。

e. 上記最高責任者はサイバーセキュリティに関する全体的な枠組みとポリシーを定め、1 年に 1 度以上、都市の最高幹部チームの確認と承認を受けるものとします。

f. 上記最高責任者は、法務チームと協力し、すべてのポリシーや指示が関連法規や国際標準に準拠していることを担保しなければなりません。

g. 上記最高責任者は、既存のすべての IT および OT 製品/サービス/調達/内部のアプリケーション開発に関してサイバーセキュリティ面での最終意思決定を行う権限を有します。これには、都市における IT/OT 製品やサービスへの多額の投資・調達も含まれます。

h. 上記最高責任者は、既存のインフラ(デバイス、ユーザ、ネットワーク、データ、アプリケーションを含む)の構成情報を作成・維持することに対して責任を有し、既存の資産のセキュリティを確保するために構成情報の内容と IT インフラの全体像を理解していなければなりません。上記最高責任者は、インフラに対する脅威の全体像、様々なシステムの依存性、ユーザのアクセス権、誰が構成情報管理の責任者であるのか、に対しても一定の理解を有しなければなりません。

i. 新たなシステムを構築する場合には、最高幹部チームが予算承認を行う前に、上記最高責任者は、文書化されたサイバーセキュリティ観点での評価(それには、どのような IT プログラムや、内外部のリソースを利用するのか、を含みます)を事前に付議しなければなりません。正規の手続きにより予算が執行される場合、上記最高責任者がその責任を負います。一方、コロナパンデミックのような非常時で正規の手続きによらず予算が執行される場合、最高幹部チームがその責任を負います。

j. 最高責任者は、サイバー攻撃の記録を保持したり、プライバシー規制に対しても技術的な実行責任を有します（例：プライバシー影響評価の実施、ビジネスプロセスおよび技術ソリューション内でのプライバシー・バイ・デザイン原則の実施）。

2. 情報資産に対するセキュリティ

a. 上記最高責任者は、第 1 項に定義されているすべての IT/OT インフラについて、最低限遵守すべき内容を示したポリシーを実行する最終決定権限と責任を有します。また、サイバーセキュリティ（市の情報資産の管理に関する事項を含む）に関する運用上の意思決定に対する承認を行う最終決定権限と責任を有します。

3. センサーや IoT デバイス等の物理的な資産に対するセキュリティ

a. 最高責任者は、IT インフラ(公共空間に設置するデータ収集用のデバイスやデータセンタ、オフィスやリモートデバイス等)の物理セキュリティに対する直接的な責任は有しないかもしれません。そのような場合でも、最高責

任者は、その IT インフラの物理セキュリティが維持されるよう、民間やインフラオーナー等の第三者を含む物理面の責任者と密に連携しなければなりません。

4. セキュリティ対策の改訂

a. 最高責任者の権限下、セキュリティ責任者は、監査の結果やセキュリティ国際標準の策定/改訂を鑑み、情報セキュリティに関する文書を、年に一度(あるいは、都市が必要と認める場合にはより頻繁に)更新しなければなりません。

5. セキュリティインシデントの予防

a. 最高責任者は、セキュリティインシデントを防止するためのガバナンスやプロセス、ポリシー、システム、技術を実装する最終決定権限と責任を有しています。

b. 最高責任者は、市の幹部、議会、職員、請負業者を対象に、市全体のサイバーセキュリティに関する意識向上と訓練を行う責任を有します。訓練実績を記録し、最低でも年に一度は評価しなければなりません。

6. セキュリティインシデントの対処

a. サイバーセキュリティポリシーには、インシデント対処の具体的な計画を盛り込まなければなりません。この計画では、インシデントの深刻さに応じた操作やコミュニケーションの対応が規定され、対応者の対応内容が定義される必要があります。

b. 最高責任者は、すべての基幹システムのオンライン/オフラインバックアップ機能などの復旧アプリケーションを含む、適切な災害復旧プログラムが実施されていることを確認する責任を有しています。

c. 最高責任者は、すべてのセキュリティインシデントをレビューし、再発を防止するための措置を講じなければなりません。

d. 最高責任者は、(ポリシーに規定された)重大なインシデントが発生した場合には、文書によって速やかに最高幹部チームに報告しなければなりません。

e. 情報セキュリティの侵害を確認した場合、(最高責任者の配下の)セキュリティ責任者はサイバー攻撃の記録を保持し、関係当局/部署と適切なコミュニケーションをとらなければなりません。

f. 重大なインシデントが発生した場合には、最高責任者は、コミュニケーション/メディア関係部署と連携し、組織内外の主要な窓口となる必要があります。

4. 重要な責任事項(推奨項目)

1. 情報セキュリティとリスク管理の訓練

a. セキュリティ責任者は、最高責任者の権限の下、年に一度(あるいは都市が必要と考える場合にはより頻繁に)、情報セキュリティとリスク管理の訓練を実施し、その記録を残さなければなりません。

2. セキュリティ監査

a. セキュリティ責任者は、最高責任者の権限の下、職員または第三者に情報セキュリティ対策の実施状況についての定期的な監査を実施するように指示し、市全体の他のコンプライアンスチームと緊密に連携しなければなりません。

3. 委託先に対するセキュリティ基準の策定

a. 最高責任者の権限下、セキュリティ責任者は、業務委託先のリスクアセスメントと審査に関するポリシーを策定しなければなりません。

4. サイバーセキュリティに対する市民教育

a. 最高責任者の権限の下、セキュリティ責任者は、市民が都市の Web サイトから容易に情報を見つけ活用できるよう、オンラインリソースの参照先を管理しなければなりません。

謝辞

リード

Yalena Coleman Applied Data & Technology, Connected Places Catapult

メンバー

Abhik Choudhury Tata Consulting

David G & Tom C UK National Centre for Cyber Security

Daniel Dobrygowksi Cyber Security Centre, World Economic Forum

Eleri Jones Head of PETRAS National Centre of Excellence for IoT Cybersecurity, UCL

Gökay Bekşen Principal Advisor, Istanbul Metropolitan Municipality

Greg McCarthy Chief Information Security Officer, City of Boston

Saj Huq Director, London Office for Rapid Cybersecurity Advancement

Sandy Tung Programme Manager, Greater London Authority

Lee Xiadong CEO, Fuxi Institution

Michael Lake CEO, Leading Cities

Murray Rosenthal Senior Security Policy Analyst, City of Toronto

Tadashi Kaji World Economic Forum Fellow, Hitachi

Thad Eidman Chief Operating Officer, Acreto Security

貢献者/レビュー者

Kush Sharma CISO, City of Toronto

Mirel Sehic Cyber Security Director, Honeywell

Nathan Pawl CEO, Blacksands

G20 Global Smart Cities Alliance について

2019 年 6 月に設立された「G20 グローバル・スマートシティ・アライアンス」は、スマートシティ技術の責任ある倫理的な利用のための共通の原則セットをめぐって、自治体、地域、国の政府、民間パートナー、都市の住民を結びつけるものです。世界経済フォーラム（官民協力国際機関）がアライアンスの事務局を務めています。

アライアンスを通じて、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を成功させるために必要なモデル政策を特定するために、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