Deloitte.
デロイト トーマツ

2024年3月

信頼性の高いサイバーセキュアな スマートエコシステムの「オーケストレーション」

ハイパーコネクテッドなスマートエコシステムは、都市にどのようなメリットやリスクをもたらすのか

目次

目次の各項目をクリックし、移動してください

ここ数年、都市が掲げる達成目標や住民からのフィードバックに対しても、デジタル技術を活用することで、都市サービスの近代化、効率化、生活の質の向上を加速させています。

各家庭でのエネルギーの無駄遣いを検知するメーターから、最適な通勤に役立つ交通システムに至るまで、デジタルトランスフォーメーション（DX）への関心はあらゆる領域で見られています。しかし、このようなスマートソリューションを構築した後も、セキュアな状態を保ち続けるにはどうしたらよいのでしょうか。スマートシティを形成する何兆ものデジタル接続を、どのようにしてバッドアクター（セキュリティ攻撃者）から守ることができるのでしょうか。

サイバーセーフティとセキュリティは、全てのスマートシティにおける最優先事項です。その複雑性は気が遠くなるようなものですが、都市のサイバー領域がセキュアな状態であれば、住民、組織、訪問者に、新たな、より充実した機会を数多く提供することができるようになります。

サイバーファーストのアプローチは、安全かつセキュアなスマートシティを目指す、都市当局の指針となるでしょう。

巨大かつ複雑なスマートエコシステム

新しく作り出されるほとんどのものと同様に、スマートエコシステムの構築には、新しい課題や、独自レベルのインフラが伴い、カスタマイズされたサイバーセキュリティが必要になります。

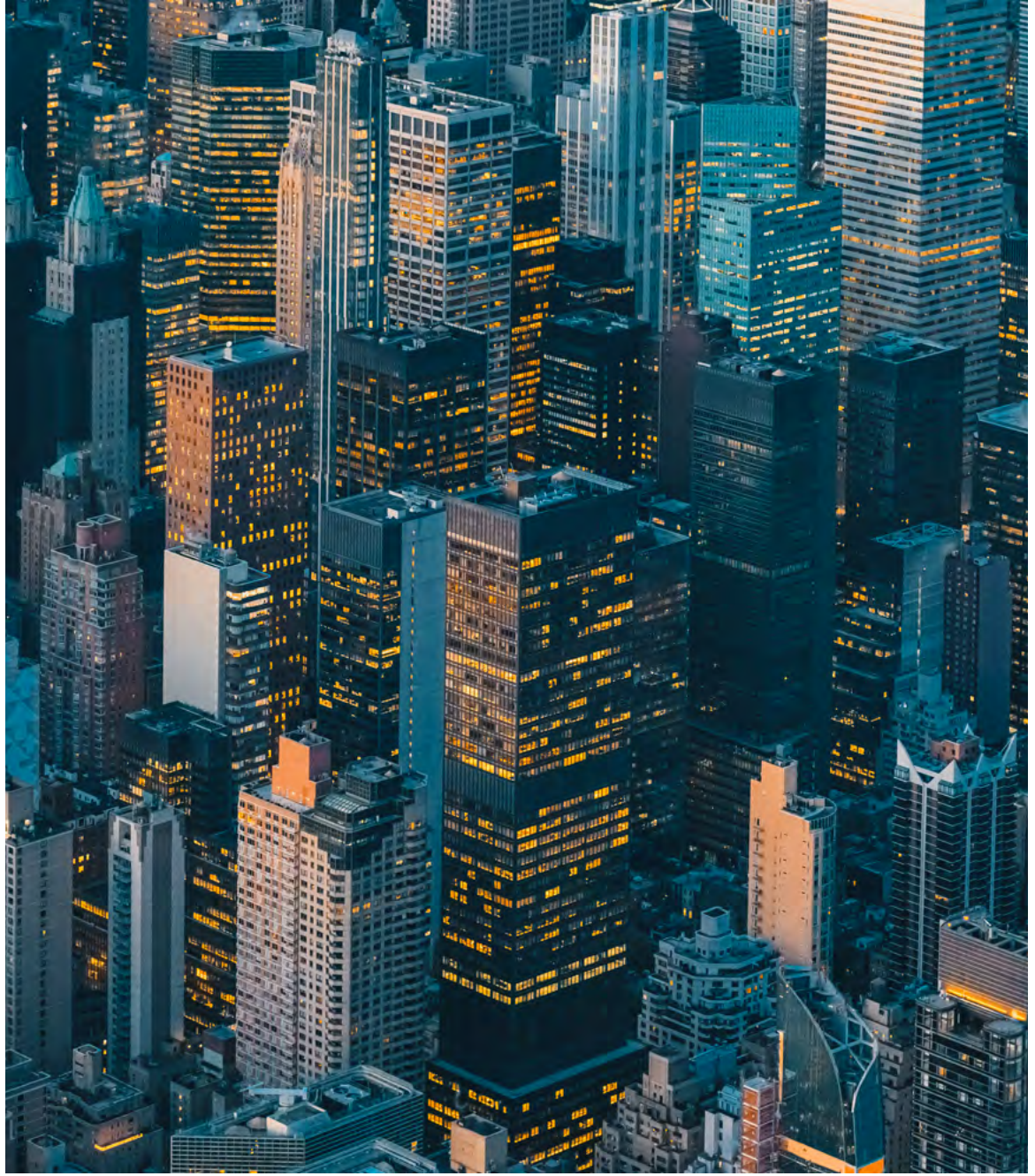
2050年までに10人中7人が都市部に暮らすようになるとの予想があることをご存じでしょうか。世界銀行が発行したグローバル予測[1]によると、都市人口は今後25年間で倍増すると指摘されています。世界中のあらゆる場所で、急速な都市化が続いていると言っても過言ではありません。今こそ、より成功した未来のために、持続可能かつサイバーセーフな都市化を実現するときなのです。

都市人口が急増することで、都市の既存インフラやあらゆる資源は必然的に圧迫され負担は増大していくでしょう。そうした中で都市やコミュニティは、限られた資源を効率的に利用しつつ、環境的、社会的、経済的な観点から持続可能な建造環境を維持するというバランスの取れた行動を取っていく必要があります。

では、都市化の準備を整えるために何ができるのでしょうか。スマートシティのコンセプトは、まさにこうした課題に対処するものです。スマートシティという言葉を耳にしたことがある方は多いと思いますが、都市を「スマート」にする要素にはどのようなものがあるのでしょうか。

スマートシティは、デジタル技術を活用することで公共資源の配分を改善し、市民の全体的な生活の質（QOL）を向上させます。また、複数のセクターや産業を集結させることで垣根を取り払い、それらを徐々に統合することで、コネクテッド化されたエコシステムを形成します。データとテクノロジーによって実現するこれらのエコシステムは、集合知を利用して、都市の様々な機能を最適化します。

スマートシティはスマートエコシステムの一種であり、何兆ものシステムやデバイスが接続され、情報を交換し、サイバー世界と物理世界の間に存在する障壁を取り除くことで物理的環境を制御する、デジタル接続の巨大なネットワークが存在しています。



スマートエコシステムは、スマートシティ、空港、交通網、発電所や病院に至る、デジタル接続されたあらゆる統合的な環境をカバーしています。

セクター

1

- モビリティ
- エネルギー
- 水
- 食品
- 衛生
- 廃棄物・リサイクル
- 建物・住宅
- 健康
- 産業
- 都市サービス
- インフラ
- 教育

テクノロジー

2

- 高度道路交通システム（ITS）
- 交通管理
- ヘルスケア関連アプリ
- モバイルソリューション
- 市民参加型ツール
- アナリティクス
- 自動化
- 人工知能
- ブロックチェーン
- IoT
- クラウドコンピューティング
- 量子

ステークホルダー

3

- 居住者・訪問者
- 政府・地域の規制当局
- 各セクターの組織
- ベンダー・サードパーティ

プロセスとオペレーション

4

- ガバナンス
- マネジメント
- オペレーション
- データ共有

スマートエコシステム開発は、自治体のリーダー層に地域コミュニケティの運営や効率性を改善するまたとない機会をもたらしています。その一方で、スマートエコシステムの開発には元来、情報セキュリティ、プライバシー、規制に関する無数の課題が内在しています。スマートエコシステムにおける情報技術（IT）、運用技術（OT）、モノのインターネット（IoT）の間で生じる融合性、相互運用性、統合性の高まりは、悪意ある攻撃者がステークホルダーに重大な損害を与える手段を提供し、極めて現実的かつ物理的な影響を及ぼすことになります。

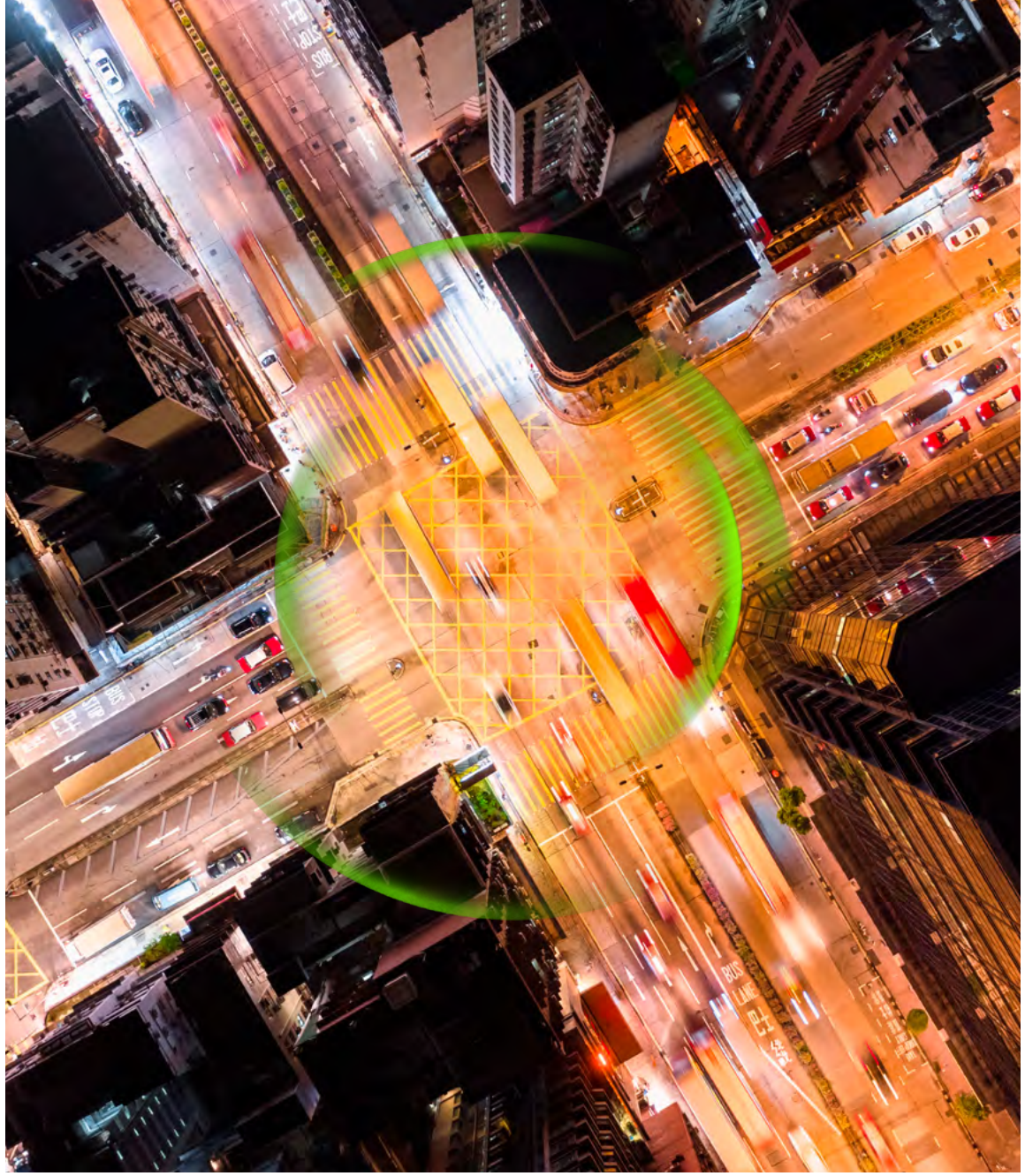
スマートエコシステムのあらゆる複雑性に対処するには、統合されたサイバー主導のアプローチが必要となります。個別で実施するサイロ型のアプローチは悪影響をもたらしかねません。スマートエコシステムにおいて、「スマート化」のための基本的かつ必須の推進力であるデジタル接続が拡大し続けるにつれて、デジタル的、物理的な影響はより深刻化する可能性があります。

従来型のサイバーセキュリティソリューションは、組織単体を監視するよう設計されています。しかし、スマートシティのようなスマートエコシステムは、ガバナンス関連の課題や技術的な問題が増加しているうえに、そのネットワークにはかつてないほど多くのステークホルダーやサードパーティが存在しています。したがって、従来の設計では対応できず、スマートエコシステムの管理者は、サイバーリスク環境を包括的に把握することができません。

従来の組織もガバナンス関連の連絡窓口も設置していますが、スマートエコシステムではその規模が全く異なります。例えば、米国のある主要都市では、スマートメーターの詳細から壊れた街灯に至るまで、1日5億件以上のデータイベントが収集されています[2]。そして様々な種類のインフラや周辺の状況に基づき、複数の異なるプレーヤーが独自のセキュリティとプライバシーのニーズを持って集結しています。一方、異なるIT、OT、IoT関連のガバナンス構造に対するセキュリティは、スマートエコシステム全体で管理していく必要があるのです。

スマートエコシステムの複雑性に対処するには、統合されたサイバーファーストのアプローチが必要となります。

デジタルインフラと物理的インフラの融合が進むにつれ、スマートエコシステムの脆弱性は高まります



スマートエコシステムのサイバーセキュリティについて考察してみましょう

まず注目すべきことの１つは、DXによってオンラインと物理的な世界のギャップが不明確になり、脅威のアタックサーフェスが指数関数的に拡大していることです。サイバー攻撃の影響は、もはやデータの損失や金銭的な損失にとどまらず、物理環境にも影響を拡大し得ることから、人々の生命に影響を及ぼす恐れがあります。

米国フロリダ州の水処理施設で起こったサイバー攻撃では、ハッカーが水中に含まれる水酸化ナトリウムの量を大幅に増やそうとしたことで、人々に深刻な健康被害が及ぶ恐れがありました。幸いなことに、初期の段階で発見されましたが、このインシデントによって、サイバー犯罪者がITシステムを介してOTをいかにコントロールできるかが浮き彫りになり、同じように病院の監視機器を危険にさらすサイバー攻撃が起これば、生死に関わる悲惨な状況に陥る事態にもなりかねないということです。

スマートエコシステムは、3つの主要な要因がもたらす複雑性に直面しています

各セクションの詳細については、このマークをクリックしてください

スマートエコシステムのハイパーコネクテッド領域におけるリスク要因を調査したところ、複雑性を生み出し、ときにはそれを悪化させる主要要因が3つ明らかになりました。

融合：サイバー世界と物理世界が出会う場所であり、ITシステムとOTがつながり、両世界の境界が曖昧になる瞬間でもあります。これによりOTは、ITと切り離されていたときには直面しなかった脅威に対して脆弱になります。

相互運用性：ここでは、新旧のシステムやプラットフォームが共存し、頻繁に相互作用する必要があります。スマートシティのエコシステムでは、多様で異なるシステムが数多く集結します。セキュリティの成熟度が異なる何百万個のデバイスやプロセスが個別に存在することを想像してみてください。
そしてそれらが相互に接続し、エコシステム全体にギャップを生み出す、一貫性のないセキュリティモデルが構築されてしまうことを想像してみてください。こうした状況は、潜在的なデータ侵害をもたらし、サイバー犯罪者に個人情報の盗用や運用妨害を行う機会を与えることになります。

統合：スマートエコシステムでは、IoTやデジタル技術を通じて、領域を超えたサービスが融合されます。この相互接続性は、特に各種セクター、産業、インフラがいかに統合されているかを考慮すると、おそらくスマートシティの最も魅力的な側面と言えるでしょう。しかし、このような相互接続性は相互依存性も生み出すことになります。

例えば、1つのサービス領域で発生した問題が、ドミノ倒しのように他の領域にすぐに連鎖し、結果的に生活に欠かせない重要なサービスの質の低下を招く可能性があります。ここで重要なのは、サイバーリスク環境に影響を与える主要な要因を把握することです。また、スマートシティの基礎を築く際には、上記を常に念頭に置き、リスクを軽減しつつ包括的なアプローチを取ることが不可欠となります。

1.

ITとOTインフラの融合

2.

レガシー技術とデジタル技術間の相互運用性

3.

セクター、プロセス、技術の統合と独立性

スマートエコシステムに対するサイバー攻撃事例

融合

サウジアラビアの石油化学プラントで、プラント内の有害化学物質レベルの監視やリリーフ弁の開閉といった自動プロセスを起動する安全計装システム（SIS）に障害が発生し、業務を緊急停止する事態に陥りました。後に、攻撃者グループがシステムに侵入し、遠隔でプラントを乗っ取ることに成功していたことが判明し、産業制御システムの安全性を脅かす脅威グループの出現が広く報告された最初の事例となりました。攻撃シナリオから、攻撃者グループはシステムに、プラント内の危険化学物質のクリティカルレベルを無視するよう命令できた恐れがあるとわかり、負傷や人命の損失につながりかねない事態となりました[3,4]。

米国アラバマ州の病院がランサムウェア攻撃を受け、コンピューターやヘルスセンサーが機能不全に陥りました。攻撃を受けている間に生まれた乳児は、コンピューターシステムがダウンしていたことから心拍の変化に気づくことができず、分娩中に窒息状態となり重度の脳損傷を受け、集中治療室で数カ月後に死亡しました。出産を担当した医師は、スタッフが監視システムを使用し変化に気づくことができていれば、帝王切開を実施していただろうと認めたことが報告されています[5]。

相互運用性

米国フロリダ州の水処理施設がハッカーの標的となり、水中に含まれる水酸化ナトリウムの濃度が一時的に引き上げられ、周辺地域に住むおよそ15万人に影響を与えうる事態が発生しました。観察力の鋭いエンジニアが異常に気付いたため実害は発生しませんでしたが、工場の各ワークステーションでは、Microsoftのサポートが終了した古いバージョンのWindows7が使用されており、リモートアクセスを介した脆弱性は深刻なものでした[6,7]。

イスラエルの半導体チップメーカーTower社がランサムウェア攻撃を受け、被害状況の把握にあたり、製造業務を停止する事態となりました。Cybereason社のセキュリティ調査担当者は、製造システムが感染したインシデントの主な問題は、古いオペレーティングシステムの使用であると報告しました。製造停止を自ら招いてしまうことを懸念し、旧システムの使用を継続する例は多くみられます[8]。

統合

ドイツの都市ポツダムがサイバー攻撃の標的となり、市民が情報やサービスを利用するための複数の公的ポータルが使用できなくなりました。自動車管理局、登記情報、インフラの危険性や欠陥の報告に使用するMaerkerプラットフォームなどが攻撃対象となりました[9]。

米国テキサス州最北部の都市であるボーガーは、サイバー攻撃の発生により市のオンライン業務が停止したと報告しました。統合されたネットワークやシステムを経由し、公共料金の支払処理、出生証明書や死亡証明書などのアーカイブへのアクセスといった全サービスに影響が及びました。またこの攻撃は、必要な記録にアクセスできなくなるなど、警察官の職務にも影響を与えました。さらにテキサス州の複数の自治体も、サードパーティの技術サービス請負業者を起因とする同様のランサムウェア攻撃を受けたと報告しており、最大20の自治体に影響が広がりました[10]。

スマートエコシステムの年数やデジタル成熟度が複雑性を左右します

スマートエコシステムにおけるサイバーセキュリティの複雑性に対処するうえで、環境年数、インフラのレベル、デジタル成熟度が重要な役割を果たしています。

様々な都市について考察してみましょう。何千年も前に確立した古代都市もあれば、古いものと新しいものが交差する分岐点に立つ都市や、最新の戦略と技術でゼロから建設される都市も存在します。また、かつては先駆けて近代化した都市でも、今では技術が老朽化し、アップグレードや新たな技術との統合が求められているような都市も存在します。

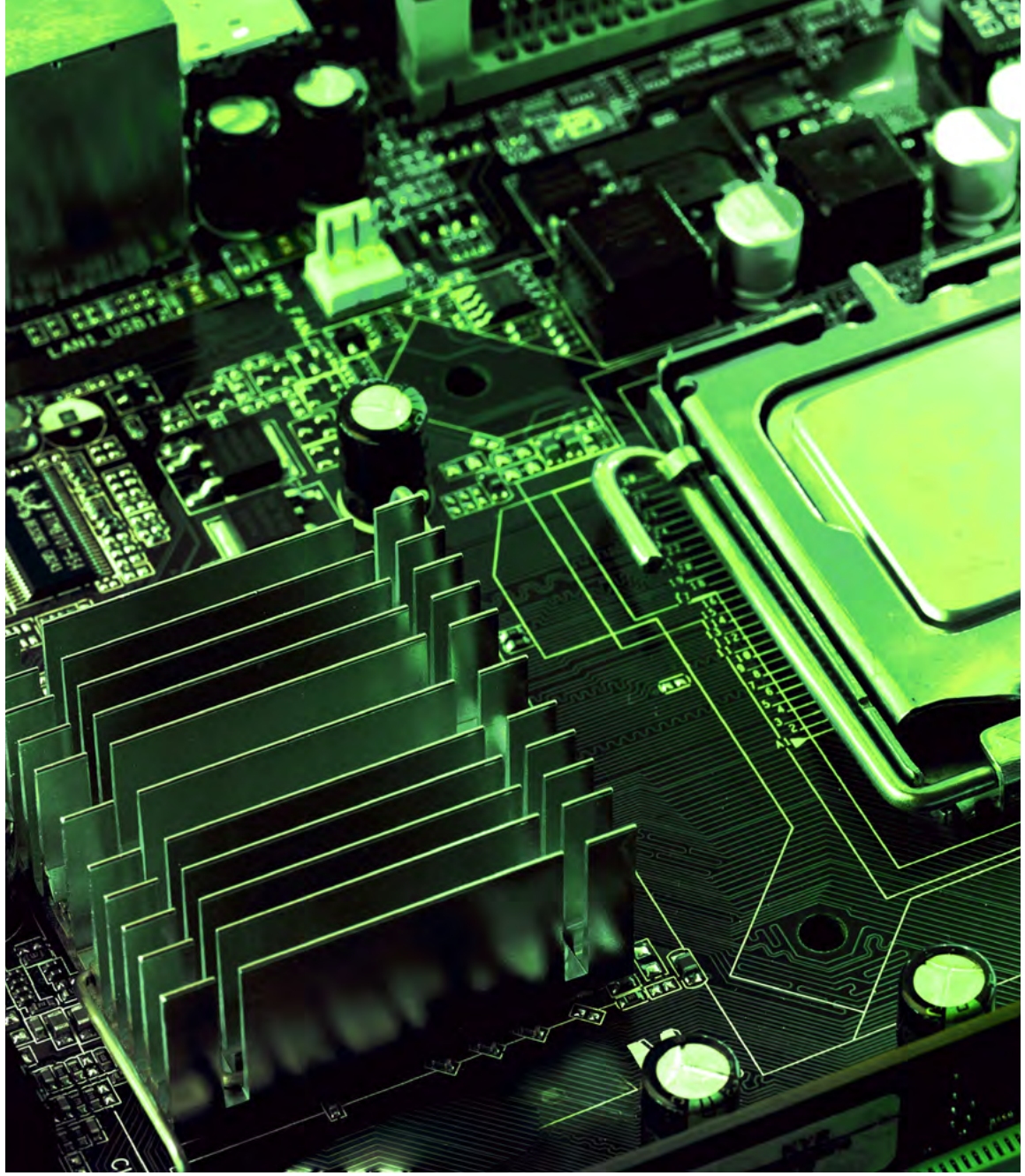
異なる技術を統合したデジタルモダナイゼーションの程度は様々ですが、エコシステム全体にわたるサイバーセキュリティフレームワークを包括的に適用していくことが必要になります。

「サイバーファースト」のアプローチが、スマートエコシステム全体の安全性とレジリエンスを強化します

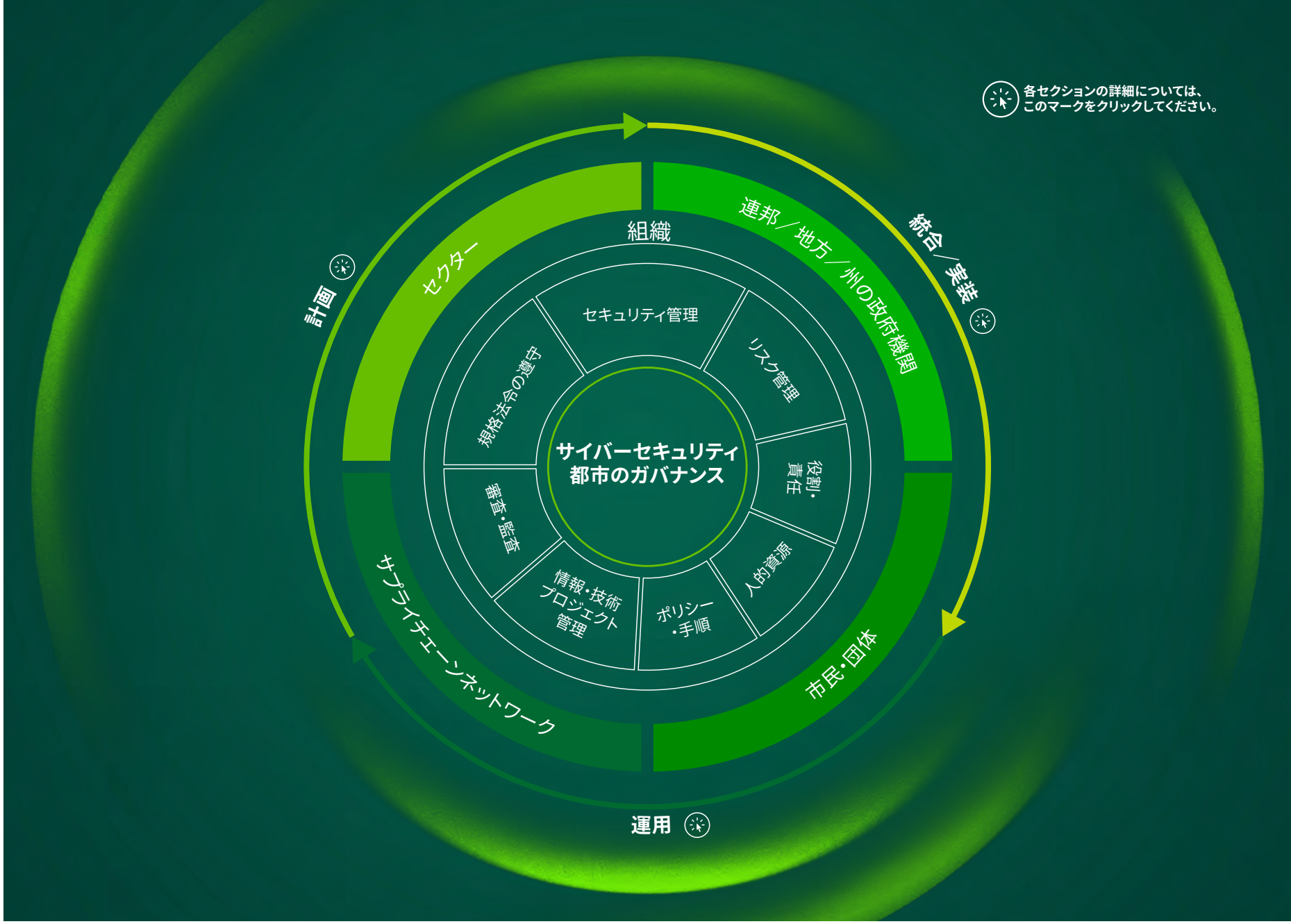
スマートシティの安全性とレジリエンスを確保するためにできること

ハイパーコネクテッド環境にあるスマートシティでサイバーセキュリティに必要となるのは、エコシステム全体を包括的に見渡す視点です。これには、エコシステムの各構成要素やサービスに加え、それらが相互に及ぼす影響に関するより精査の強化が含まれます。

「サイバーファースト」のフレームワークは、構想や要件決定を含む計画フェーズから、構築の統合／実装フェーズに移行し、最終的に運用フェーズに至るまで、スマートエコシステムのライフサイクル全体でサイバー制御を組み合わせたものです。



サイバーファーストのアプローチが、安全性とレジリエンスを強化します



サイバーファーストのフェーズ1：計画

スマートエコシステムを保護するためのサイバーファーストなアプローチは、計画フェーズから始まります。本フェーズでは、スマートエコシステムに転換していくための環境を選択します。

次に、環境の現状を把握するために、既存インフラのセキュリティとプライバシーに対する評価を行います。また、適用可能なプロジェクト基準や規制を決定し、サイバーセキュリティとプライバシーの目標像を定義します。

本フェーズの最後に、プロジェクトを前進させ、評価された現状と望ましい目標像の間に存在するギャップを埋めるために、高レベルのプロジェクトロードマップを策定します。本フェーズでの活動取り組みを通じて、重要インフラの設計、構築、統合を行うための基礎を形成します。

計画フェーズの構成要素：

- **コネクテッド化されたインフラに対するサイバーセキュリティ評価：**既存インフラの監査と同時に、規制要件に沿ってリスクの特定と評価を実施する。
- **目標像の設計とロードマップの策定:**レジリエンシーフレームワークや計画の策定を含む、スマートエコシステムのサイバーセキュリティプログラムを開発するためのロードマップを作成する。
- **ガバナンス、リスク、コンプライアンス（GRC）：**安全な調達、ポリシーと手順の策定、サードパーティリスク管理、セキュリティとデバイス管理を連携させるためのコミュニケーションフレームワークを含む、スマートエコシステムのセキュリティとプライバシーに関するガバナンスモデルを構築する。
- **資産の識別と分類：**潜在的な影響の重大度の評価結果に基づき、IT資産とOT資産の分類基準とカテゴリーを定義する。影響評価に基づくIT資産とOT資産のリスク／重要度の分類も適用される。

事例紹介：スマートシティの新規構築

ゼロから開発・構築されるスマートシティは、初期の構想フェーズの時点でサイバーセキュリティを重要概念として盛り込むことが可能です。新しいスマートシティは、都市のリーダー層、市民、訪問者、その他のステークホルダーを対象としたサイバーセキュリティ戦略や学習機会を初期設計に組み込み、ユーザーのフィードバックに基づいてサイバーセキュリティとデータプライバシーの概念を継続的に進化させることができます。

機会：

- **サイバー戦略ロードマップ：**計画フェーズでのサイバー戦略に関するロードマップの作成
- **コミュニティ向けの学習プログラム：**本継続的改善に向けた教育、連携、意識向上を通じ、コミュニティのイノベーションを促進するプログラムの開発

サイバーファーストのフェーズ2：統合／実装

計画フェーズが完了すると、統合／実装フェーズに入ります。スマートエコシステムのプロジェクトチームは、本フェーズにおいて、スマートエコシステム内のセキュリティやプライバシープログラムのためのアーキテクチャや高レベルな運用要素の構築に注力します。

次に、計画フェーズで作成したプロジェクトロードマップを見直し、より詳細な取り組みを盛り込んでいきます。これには、デジタル資産のインベントリ作成、デジタルアイデンティティの選定と導入、データ保護ツールとプロセスの特定、脆弱性管理と脅威インテリジェンスソリューションの決定、堅牢なトレーニングと啓発プログラムの構築が含まれます。その後、プロジェクトチームは、新しくコネクテッド化されたインフラを対象としたベースラインセキュリティリスク評価を実行することが可能です。

本フェーズを通じて、各構成要素を、計画フェーズで決定された適切な基準や規制に整合させていくことが不可欠です。統合／実装フェーズの構成要素：

- **セキュリティアーキテクチャとロードマップ：**セキュリティ技術運用モデル、サービスカタログ、セキュリティライブラリ、セキュリティ技術導入に関するロードマップの策定を含む、スマートエコシステムのセキュリティアーキテクチャを構築します。
- **デジタルアイデンティティ：**エコシステムデータへのアクセスを許可する前に、統合システムのアイデンティティを検証するための、スマートエコシステムのアイデンティティソリューションを開発します。
- **データ保護：**規制要件に合わせるために、データの暗号化、プライバシー、保管、転送などに関する制御を実施します。
- **脆弱性管理：**スマートエコシステムインフラにおける脆弱性を特定、分類、優先順位付け、修復、緩和するための管理プロセスの確立します。
- **脅威インテリジェンスのプラットフォーム：**監視要件の計画、特定、マッピングと、インフラ強化のための設計と実装を行います。

事例紹介：トンネルと橋

デロイトでは、アパラチア山脈を通る全長360マイルの道路を横断する際に通過する4つのトンネルのうちの1つである、長大なトスカローラ山脈トンネルの近代化に向け、ペンシルベニア州ターンパイク委員会（Pennsylvania Turnpike Commission、PTC）への支援を行いました。同委員会は典型的な土木関連の課題に直面していただけでなく、トンネル全体に配置されたコネクテッドデバイスの複雑なネットワークに直接関連する、様々なサイバーセキュリティリスクを管理する必要がありました。

本プロジェクトでは、トンネルの状態、温度、二酸化炭素やその他のガスの濃度を測定して報告する接続型の環境センサーの配置を始め、自動換気、照明、映像検出システム、データ収集とリモートでの監視を可能にする制御システムなどのデバイスやシステムが必要とされていました。

非常に多くの物理的デバイスがテクノロジースタックの一部となったことから、委員会は、サイバーセキュリティに対する将来を見据えた先手のアプローチを取る必要性を認識していました。エンジニアリングチームとセキュリティチームは、電力網で一般的に使用される規範的なサイバーセキュリティ基準をプロジェクトに合わせて調整し、使用することを決定しました。

プロジェクトの注目点：

- **プロアクティブなサイバーセキュリティ：**重要な仮想・物理インフラに関する先を見通した計画と、将来の設計業務のためのOTを伴う、設計におけるプロアクティブなサイバーセキュリティを実現
- **サイバー関連のコミュニケーション：**PTC運用、設計、エンジニアリング、構築チーム間でのサイバーセキュリティ関連の連携と、サイバー・物理空間向けの変更管理プロセスの標準化を実現

サイバーファーストのフェーズ3：運用

スマートエコシステムが最終第3フェーズである運用フェーズへと移行し始めると、管理者は、安全な運用、顧客からの信頼強化、ステークホルダーの価値を高めるためのレジリエンスの構築に注力します。

本フェーズでは、サイバーセキュリティ支援とマネージドサービスの強化、脅威の評価と監視の継続的な実施、セキュリティとプライバシーの改善機会の継続的特定などを実施します。

運用フェーズの構成要素：

- **脅威評価サービスの管理：**監査への準備度と技術評価、マニュアルの見直し、脆弱性スキャンの自動化、脅威の継続的／早期検出といったサービスを通じて、ユーザーは進行中のプロセス内の脅威に優先順位をつけて対処できるようになります。
- **セキュアオペレーションセンター：**スマートエコシステム内のサイバーセキュリティインシデントは継続的に監視、分析、解決されます。統合された一貫性のある監視を行うことで、インシデントをリアルタイムで解決することができます。
- **脅威インテリジェンス：**民間、公的機関、規制機関は、セキュアかつ中核的なプラットフォームを通じて、脅威インテリジェンスを調整し、脅威の緩和に向けた協業を行います。
- **リカバリとレジリエンス：**事業継続マネジメント、災害復旧、データのバックアップとリカバリ、インシデント対応に関するプロセスや手順を監視し、継続的に評価を実施します。これにより、サイバー攻撃、自然災害、システム停止などのインシデント発生時に、貴重なデータや機能が失われてしまうエコシステムの脆弱性を軽減することができます。

事例紹介：現代都市

現代都市では、サイバーセキュリティインフラを用いてレガシーシステムを近代化して運用するという、新旧システムの融合の機会の獲得が可能です。デロイトでは、世界中の都市やインフラ事業者に対して、アイデンティティとアクセス管理（IAM）、特権アクセス管理（PAM）、データ保護サービス、アプリケーションセキュリティ、インフラセキュリティ、脅威インテリジェンス、脅威ハンティング、脆弱性管理に関連する支援を行っています。デロイトが提供する「Digital Identity by Deloitte」というソリューションを使用することで、都市関連人材のアイデンティティガバナンス、アクセス管理、特権アクセス制御に係る変革が実現し、安全性、レジリエンス、市民からの信頼性向上が促進されます。

機会：

- **IAMロードマップ：**サイバー関連のアイデンティティとアクセス管理について、ステークホルダーによる短期・長期的な可視化とマッピングを実現
- **実証済みの導入設計：**ボトルネックの除去とユーザーエクスペリエンスの向上を行う標準化されたIAMソリューションの導入

行動しよう!

予見可能な未来に向け、急速な都市化は当面続くでしょう。世界中の都市で働く職員層は、この現実を受け入れることで、今日のバーチャルとフィジカルが融合する世界に内在する機会やリスクに対応する、安全な空間や場所を構築することができます。

デロイトでは、都市のリーダー層がスマートにセキュアな未来を保てるよう支援する体制を整えています。スマートシティへの進化と安全対策に関してぜひデロイトまでお問い合わせください。

著者

PIYUSH PANDEY

ANDRÉ CORREIA SOUSA

FREDERICO MACIAS

LISSA BARROWS

謝辞
著者は、アイデアや洞察の提供や講評についてPeter WirnspergerとPaul Beverleyに、そして本プロジェクトの研究開発において多大なる支援を提供したDeepali Kochhar、Rita Machado、Harris Block、Tanner Brooks、Larissa Dornに感謝の意を表しています。

各著者の経歴を見るには、
このマークをクリックして
ください

参照情報

1. The World Bank, "Urban Development," accessed August 17, 2023.
2. Merritt Maxim and Salvatore Schiano, Making Smart Cities Safe and Secure, Forrester, 2021, p. 4.
3. Samuel Gibbs, "Triton: hackers take out safety systems in 'watershed' attack on energy plant," The Guardian, December 15, 2017.
4. TrendMicro, "New Critical Infrastructure Facility Hit by Group Behind TRITON," April 11, 2019.
5. Kevin Poulsen, Robert McMillan, and Melanie Evans, "A Hospital Hit by Hackers, a Baby in Distress: The Case of the First Alleged Ransomware Death," The Wall Street Journal, September 30, 2021.
6. Casey Crane, "Hacker Breaches Florida Water Treatment Plant, Adds Lye to City's Water Supply," Security Boulevard, February 16, 2021.
7. Lee Mathews, "Florida Water Plant Hackers Exploited Old Software and Poor Password Habits," Forbes, February 15, 2021.
8. Meir Orbach, "Israeli chipmaker Tower confirms cyberattack forced it to shut down systems," Calcalist Tech, September 6, 2020.
9. Sergiu Gatlan, "City of Potsdam Servers Offline Following Cyberattack," Bleeping Computer, January 24, 2020.
10. Jake Bleiberg and Eric Tucker, "'Holy Moly!': Inside Texas' Fight Against a Ransomware Hack," Bloomberg News, The Associated Press, July 26, 2021.

Deloitte.
デロイト トーマツ

Designed and produced by 368 at Deloitte. J31276