デジタル庁「国・地方ネットワークの将来像及び実現シナリオに関する検討会」第二回会議 (2023/11/02)

登 提出資料 #2 (意見書の補足スライド)
～ 厳格なシステムと自由なシステムの概念の説明 & 安全・確実な既存システム移行＋進化の両立の提案 ～

IPA 独立行政法人 情報処理推進機構
産業サイバーセキュリティセンター
サ イ バ ー 技 術 研 究 室

2023/11/01

登　大遊
Daiyuu Nobori, Ph.D.
Email: d-nobori@ipa.go.jp

DN

【1】パブリッククラウド技術・ゼロトラスト製品は、現在は、まだ開発途上である。各社の製品・サービスのセキュリティ・レベルは、現時点では、従来の閉域網思想 (例: 自治体 NW の LGWAN 接続系) で実現できている長年の実績を有する日本の行政システムのセキュリティ水準に大きく劣る。折角安定しているセキュアな業務システム群を、性急にモダン化して、クラウド化・インターネット化することは、安全性のリスクが大きく、避けたほうが良いと考える。ゼロトラスト原則に合わせた認証・ACL 設定・ログ収集の強化と、コストダウンが可能な場合の IaaS (VM) を活用したクラウド化を、個別のシステム責任者の判断で進めるべきである。

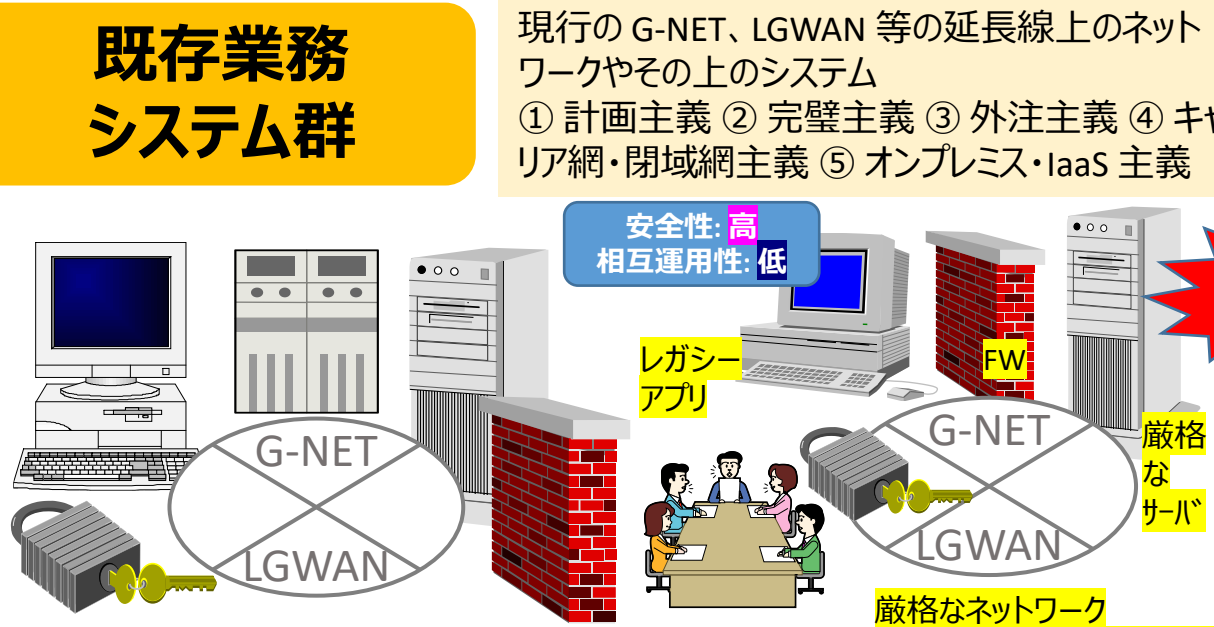
既存業務システム群

現行の G-NET、LGWAN 等の延長線上のネットワークやその上のシステム
① 計画主義 ② 完璧主義 ③ 外注主義 ④ キャリア網・閉域網主義 ⑤ オンプレミス・IaaS 主義

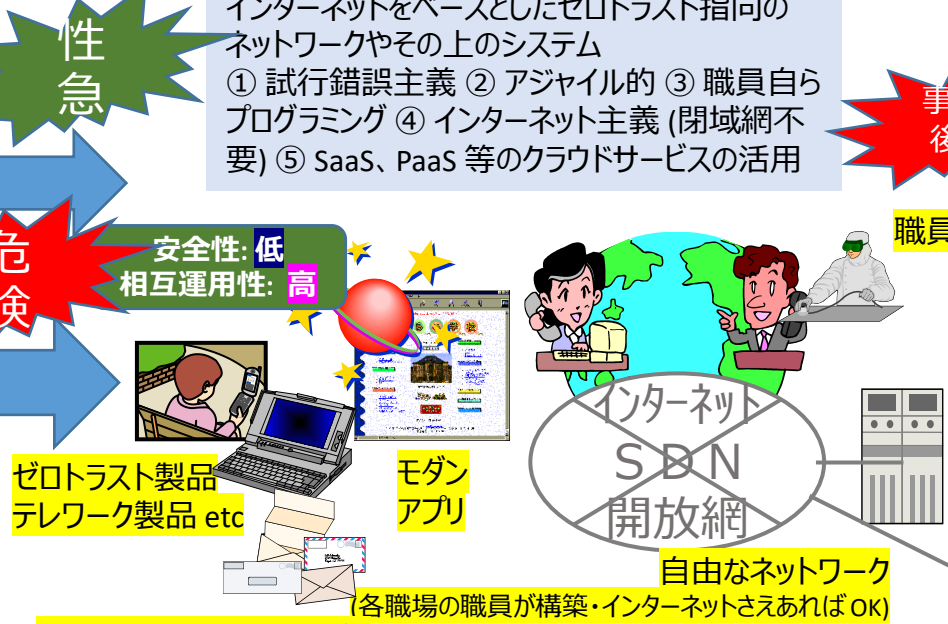
性急

インターネットをベースとしたゼロトラスト指向のネットワークやその上のシステム
① 試行錯誤主義 ② アジャイル的 ③ 職員自らプログラミング ④ インターネット主義 (閉域網不要) ⑤ SaaS、PaaS 等のクラウドサービスの活用

事故・後悔



危険



職員によるプログラミング

IaaS に限らない発展途上技術 (各種 PaaS、SaaS) を用いたパブリッククラウド活用
(自由なガバクラ)

職員によるサーバ構築

モダンなパブリッククラウド技術・ゼロトラスト製品への性急な移行によって生じる重大なリスクの詳細は、「国・地方ネットワークの将来像及び実現シナリオに関する検討会」第二回会議 (2023/11/02) 提出資料 (意見書) 2023/10/30 (登 大遊) の「第 1 章」 参照。これらの技術は開発途上であり、安全性具備にはまだまだ時間を要する。

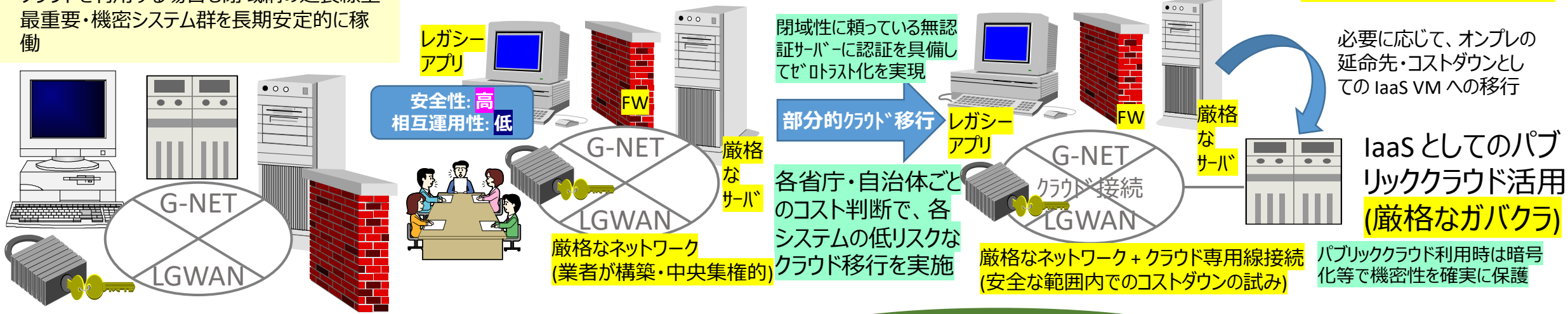
2023 年 (現在) → 2030 年以降

【2】そこで、現行の業務システムやネットワーク (G-NET、LGWAN) を現代化するステップにおいては、性急にすべてをモダンクラウド化またはインターネット化するのではなく、以下のような「安全で緩やかな進化」を行なうべきである。
①サーバー: オンプレミス → そのまま延命、VM (プライベートクラウド) 化、または、コストダウン見込みが高い場合のみパブリッククラウド化 (オンプレサーバーから IaaS をベースとした、「厳格なガバクラ」。ただしストレージの機密性対策必須)
②認証系: 従来どおりオンプレ的な認証サーバー群 (AD 等) を安全に利用 (機密性対策の上クラウド IaaS に移行してもよい)
③ゼロトラスト化: 無認証・脆弱なサーバーに個別に認証設定を施し、ACL 設定とログ管理の徹底によりゼロトラスト原則を実装 (これは、現在のシステムを元に十分に対応可能。これまで認証やセキュリティ対策を怠っていたサーバーを補強)
④ネットワーク: G-NET や府省内 WAN については国の内部問題なので国主導で最適化し (NGN 等を活用)、LGWAN については現状のアーキテクチャ (キャリアの広域イーサ + IPsec) を大きく改造することなく可能な範囲でコストダウン (品質重視)

「厳格なシステム」

- 現在のシステムをできるだけ安定させて延命
- クラウドを利用する場合も閉域網の延長線上
- 最重要・機密システム群を長期安定的に稼働

現行の G-NET、LGWAN 等の延長線上のネットワークやその上のシステム
① 計画主義 ② 完璧主義 ③ 外注主義 ④ キャリア網・閉域網主義 ⑤ オンプレミス・IaaS 主義



【３】一方、皆、新しい技術・製品も色々と試したい。例えば現在発展中のクラウドネイティブのアプリ開発、サーバーレス、新ネットワーク技術など (いわばハイカラな技術) も、次々に試すべきである。これにより、ゼロトラスト的なさまざまな創意工夫を凝らした職員主体の DX の実現とアプリ開発が可能になるためである。このような、行政職員の創造的・試行錯誤的な活動を【２】で述べた安定志向によって阻害してはならない。
だが、【２】で述べた既存業務システムのセキュアな運用の継続と機密性・可用性は、上述のような新たな試みよりも絶対優先であろう。【２】のシステムの安全に継続に万一失敗すると、国の統治機能に影響が生じ、国民共同の利益が脅かされるためである。【２】は枯れた技術のみで運用する。

そこで、いかにして、既存業務システムの保護と、新しい技術の試行錯誤とを両立するかが問題となる。
既存の業務システム (厳格なシステム) と、原則としてネットワーク的に独立した、「自由なシステム」 という概念とネットワークを生み出し、ハイカラ技術を導入して試す場合は、「自由なシステム」の枠内で試す。仮想ネットワーク技術、SDN 技術、プライベートクラウドシステム、およびパブリッククラウド上の PaaS・SaaS ベースのメールサービス基盤、ファイル共有基盤、端末管理基盤、ID 認証基盤といった新しいものは、現在日本国内外で進化・開発中であり、多様なものが 2030 年頃までに生み出されるであろう。「自由なシステム」とは、それらをいちはやく試して実運用し、必要に応じて技術開発をする技術検証と人材育成基盤である。製品進化と、「自由なシステム」の上で行政職員たちにより確立される運用ノウハウによって、市場製品に内在する機密性・可用性・安定性・プロプライエタリ性・ベンダロックイン (クラウドロックイン) 等の問題を、克服することができる。そのような克服がなされた領域ごとに、従来の「厳格なシステム」→「自由なシステム」への安全な移行が実現可能となる。

「自由なシステム」

- さまざまな開発途上製品・サービス・アーキテクチャの採り入れが可能な自由な NW
- 職員による自由な発想のアプリ開発、DX や AI 活用等

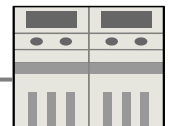
インターネットをベースとしたゼロトラスト指向のネットワークやその上のシステム
① 試行錯誤主義 ② アジャイル的 ③ 職員自らプログラミング
④ インターネット主義 (閉域網不要) ⑤ SaaS、PaaS 等のクラウドサービスの活用

ゼロトラスト製品
テレワーク製品 etc

モダンアプリ

自由なネットワーク
(各職場の職員が構築・インターネットさえあれば OK)

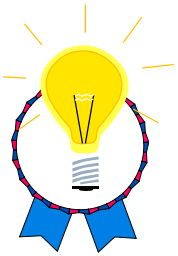
職員によるプログラミング



IaaS に限らない発展途上技術 (各種 PaaS、SaaS) を用いたパブリッククラウド活用
(自由なガバクラ)

職員による
サーバ構築

ｸﾗｳﾄﾞﾍﾞｰｽのﾒｰﾙやﾌｧｲﾙ共有,
ID 基盤 (機密性は劣るが便利)



- 2030 年前後までにｾﾞﾛﾄﾗｽﾄ製品・ｸﾗｳﾄﾞ技術のｾｷｭﾘﾃｨや運用ノウハウが進歩することを期待
- この頃までに、十分な安全性を検証

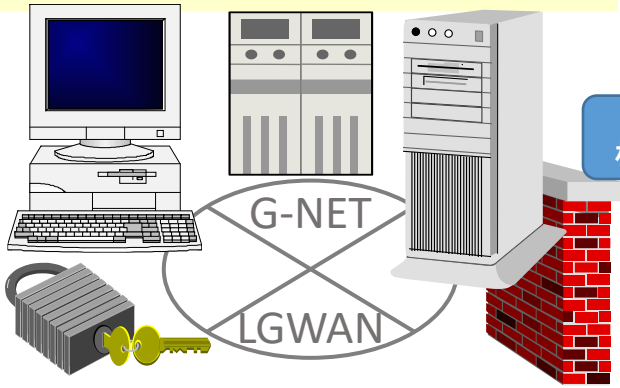
2023 年 (現在)

2030 年以降

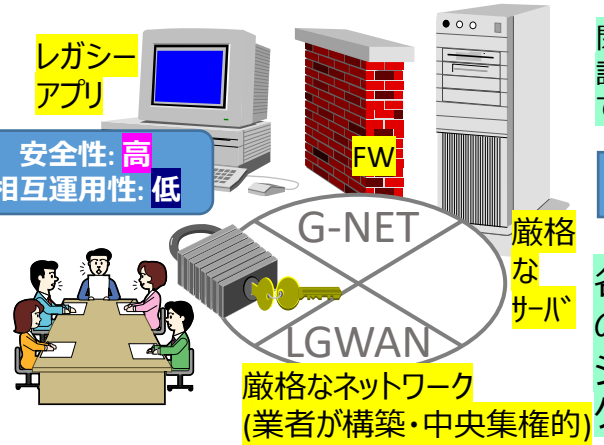
独立行政法人
情報処理推進機構
サイバー技術研究室 登

「厳格なシステム」

- 現在のシステムをできるだけ安定させて延命
- クラウドを利用する場合も閉域網の延長線上
- 最重要・機密システム群を長期安定的に稼働



現行の G-NET、LGWAN 等の延長線上のネットワークやその上のシステム
① 計画主義 ② 完璧主義 ③ 外注主義 ④ キャリア網・閉域網主義 ⑤ オンプレミス・IaaS 主義

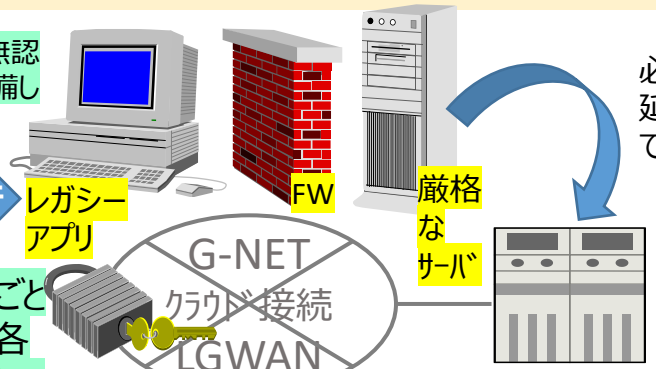


厳格なネットワーク
(業者が構築・中央集権的)

閉域性に頼っている無認証サーバーに認証を具備してゼロトラスト化を実現

部分的クラウド移行

各省庁・自治体ごとのコスト判断で、各システムの低リスクなクラウド移行を実施



厳格なネットワーク + クラウド専用線接続

必要に応じて、オンプレの延命先・コストダウンとしての IaaS VM への移行

IaaS としてのパブリッククラウド活用
(厳格なガバクラ)

パブリッククラウド利用時は暗号化等で機密性を確実に保護

「自由なシステム」

- さまざまな開発途上製品・サービス・アーキテクチャの採り入れが可能な自由な NW
- 職員による自由な発想のアプリ開発、DX や AI 活用等

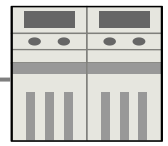
インターネットをベースとしたゼロトラスト指向のネットワークやその上のシステム
① 試行錯誤主義 ② アジャイル的 ③ 職員自らプログラミング
④ インターネット主義 (閉域網不要) ⑤ SaaS、PaaS 等のクラウドサービスの活用

ゼロトラスト製品
テレワーク製品 etc

自由なネットワーク
(各職場の職員が構築・インターネットさえあれば OK)

職員によるプログラミング

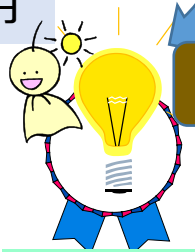
IaaS に限らない発展途上技術 (各種 PaaS、SaaS) を用いたパブリッククラウド活用
(自由なガバクラ)



職員によるサーバ構築

クラウドベースのメールやファイル共有, ID 基盤 (機密性は劣るが便利)

「厳格なシステム」を「自由なシステム」に移行



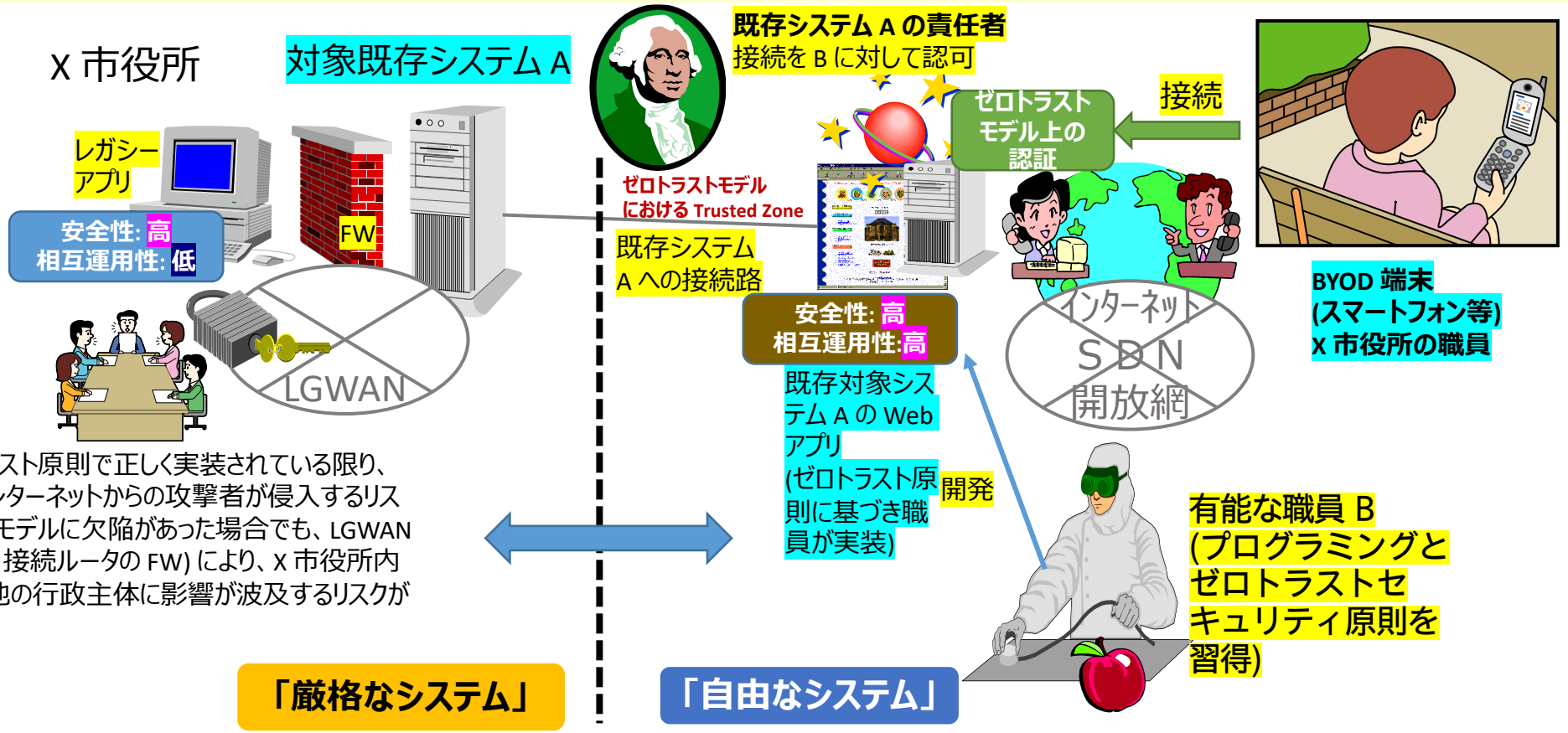
↑最終理想形態

2030 年前後までにゼロトラスト製品・クラウド技術のセキュリティや運用ノウハウが進歩することを期待し、「自由なシステム」が「厳格なシステム」と同等程度の十分な安全性を検証した後に、「厳格なシステム」を必要に応じて「自由なシステム」に移行

2023 年 (現在)

2030 年以降

【5】「厳格なシステム」と「自由なシステム」は、完全に独立し無関係という訳ではない。各領域の既存の厳格なシステムの各責任者 (府省庁、自治体等における既存の特定の業務システムの責任者) の判断で、既存の特定の厳格なシステムと、自由なシステムとの間で、ゼロトラスト原則に基づいた相互運用を許容する。これにより、組織内の職員に対して、とても安全な、モダンな利便性の高い組織内ソフトウェア開発の機会を提供し、行政主体内における高度な IT 人材育成が実現できる。この手法は、「厳格なシステム」を完全モダン化することが困難・不可能でも機能する優れた手法である。「厳格なシステム」の安全性をそのままに、「自由なシステム」によるゼロトラスト原則の Web アプリの実現を可能とする。たとえば、X 市役所のある行政職員 B が、「自由なシステム」の思想に基づき、既存の X 市システム A にインターネット経由でゼロトラスト原則に基づいた認証を経て安全に BYOD スマートフォンでアクセスできるシステム (既存の厳格なシステムへの操作を行う Web アプリ型のゲートウェイ) を開発したとする。この場合、その職員は、「自由なシステム」でその Web アプリをデプロイし、これを、「厳格なシステム」 A の対象サーバーに個別に接続する。ゼロトラスト原則が適用されている限り、Web アプリはユーザーからの認証を必須とし、ゼロトラスト上の Trusted Zone が「厳格なシステム」の対象サーバーとの接続部分に相当する。「自由なシステム」は、このように、システムオーナーの責任と判断による、レガシーな個別の「厳格なシステム」に対する、ゼロトラスト原則に基づくインターネットからのアクセスの安全・容易な実現に寄与する。



開発 Web アプリがゼロトラスト原則で正しく実装されている限り、既存対象システム A にインターネットからの攻撃者が侵入するリスクはない。仮にゼロトラストモデルに欠陥があった場合でも、LGWAN の隔離の仕組み (LGWAN 接続ルータの FW) により、X 市役所内部に影響は隔離される。他の行政主体に影響が波及するリスクがない。

【６】「自由なシステム」は、単なる概念・考え方であり、「G-NET」や「LGWAN」のような具体的なシステムや NW が中央集権的に存在している必要はない。自由なシステムにおけるコンピュータ・ネットワークは、ゼロトラストモデルを基本とするものであるから、最小限度のものとして、単純な IPv4, IPv6 インターネット接続路やサーバー運用が可能な一定数の固定 IP アドレスがあれば良い。ゼロトラストモデルにおける Trusted Zone 内の通信路を組織横断で構築するためのセキュアな L2 閉域路や、パブリッククラウドとの専用線接続経路があると、尚良い。
しかし、これらを各行政主体で用意するのは大変であるし、それぞれが独立して用意するとなると、組織間の相互運用実験も困難となる。自由なシステムは、人材育成基盤でもある。しかし人材育成が十分でない場合、NW の用意が困難という、ニワトリが先かタマゴが先かの状態の組織もある。そこで、自由なシステムの基礎として、自由な行政主体専用の合同ネットワークを作るべきである。合同 NW は物理的な設備・予算は最小限とし、既存のリソースを活用して、ほとんどお金をかけずに使う。重要な点は、合同ネットワークは組合的なものであり、いずれの参加組織も、完全対等で、主体性があり (自らの一部である)、同時に、いずれの参加組織によっても単独で支配権がない (デジタル庁が独占支配する訳でもない) という点である。参加希望者がいる各行政主体から出席する者で合議体・中立的に運営するのである。これにより、各参加組織とそのメンバーは、自分の物として、NW 運営にかなり主体的に参加する意欲が生じる。
このような「自由な合同ネットワーク」を１つ作ることが必要と考えられる。発起方法を含めてアイデアをいただきたい。