

第12回DPF研究会 2023年3月17日

# ネットワークによるトラスト Trust-Enhanced Networking

*Trust in the Network is...  
Trust-ing the Future!*

富士通株式会社  
データ&セキュリティ研究所  
シニアディレクター  
関屋 元義

Thank you to the Team



Fujitsu Cybersecurity Center  
of Excellence in Israel

FUJITSU



## ChatGPTに聞いてみました

MO DPF研究会 って何ですか



「DPF研究会」とは、データプラットフォーム構築促進協議会（Data Platform Forum）が主催する研究会の一つで、データプラットフォーム（DPF）に関する技術研究を行う団体です。



知って  
いれば  
わかる



MO デジタルサービス・プラットフォーム技術 特別研究専門委員会って何ですか



「デジタルサービス・プラットフォーム技術特別研究専門委員会」とは、総務省が設置した専門委員会で、デジタルサービス・プラットフォームに関する技術的な研究を行うことを目的としています。



MO サイバーのトラストへのネットワークの役割は？



ネットワークは、サイバーのトラストに重要な役割を果たします。サイバートラストは、情報セキュリティに関する信頼を確立することを目的とした概念であり、ネットワークは情報セキュリティの実現に不可欠な役割を果たします。

⇒ネットワークで得られるフィジカルの情報をトラストに活用できないか？

リアル



- ✓ 目に見えるものは事実
- ✓ 現場に足を運び確かめる
- ✓ 直接目を合わせて会話

空間も時間も有限

サイバー

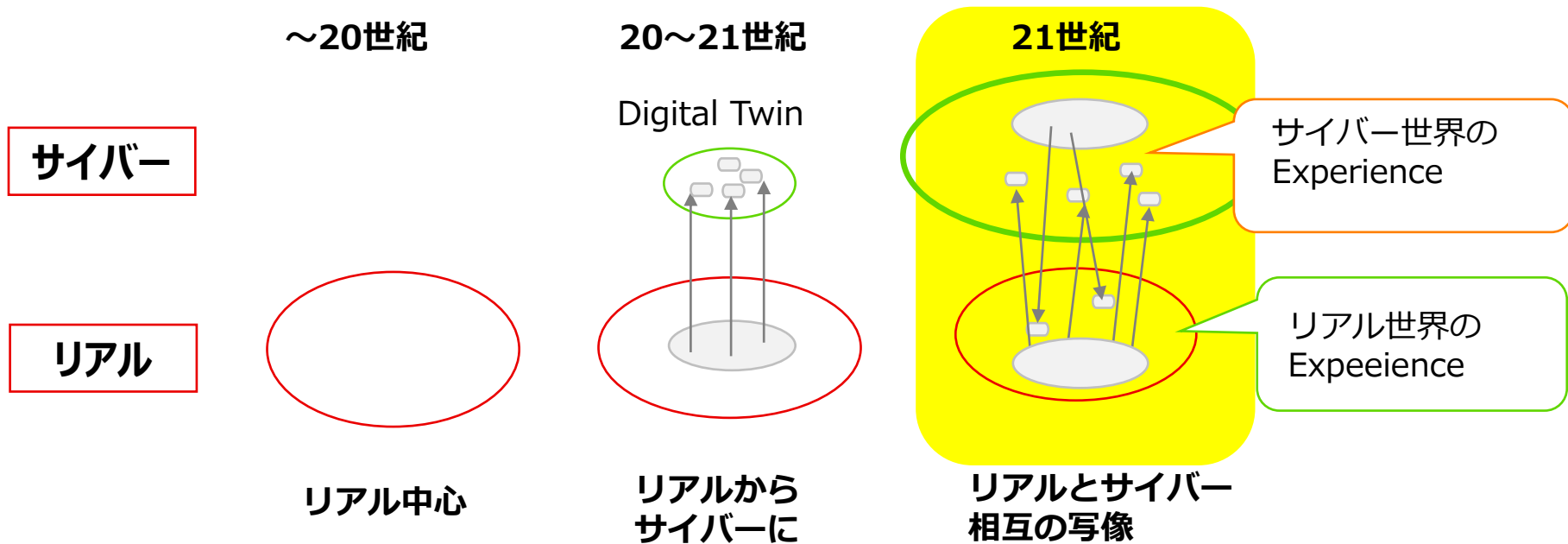


- ✓ ネットの動画で知る
- ✓ ネットを通じてどこにでも行ける
- ✓ ネットを通じて会話

制約を受けない、可能性は無限

サイバー世界の“自由”が新しい体験（Experience）を生む。。

# リアルの制約からの解放->新しいExperience



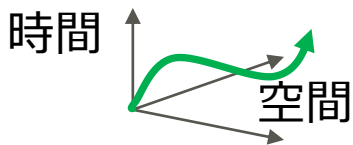
21世紀

サイバー世界のExperience > リアル世界のExperience

# 求められる “トラスト”

- サイバー世界が大きく広がるとともに安心・安全に関する不安。。

実世界の制約（時間・距離）から解放



デジタルの世界で  
自由に飛び回る

サイバー世界のExperience  
リアル世界とは違う感動

デジタルツイン  
デジタルの世界に 人・モノ・コトを写像

不安。。



サイバー世界の新鮮な体験



安心して楽しむために求められる“トラスト”

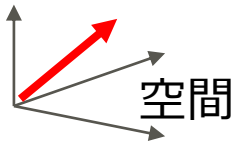
## “制約がない”サイバーのメリット + 安心・安全（トラスト）

方向1



サイバー世界の秩序  
となる次元のようなもの？

時間

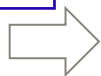


空間

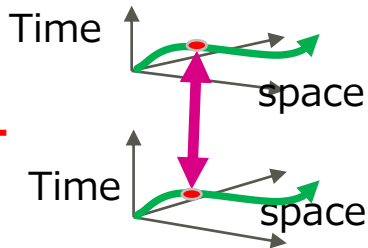
例えば **ブロックチェーン技術**  
デジタルの世界でコトを分散共有。  
コトの因果関係を保存 秩序の基準

## 本日の話

方向2



リアル世界と紐づけ

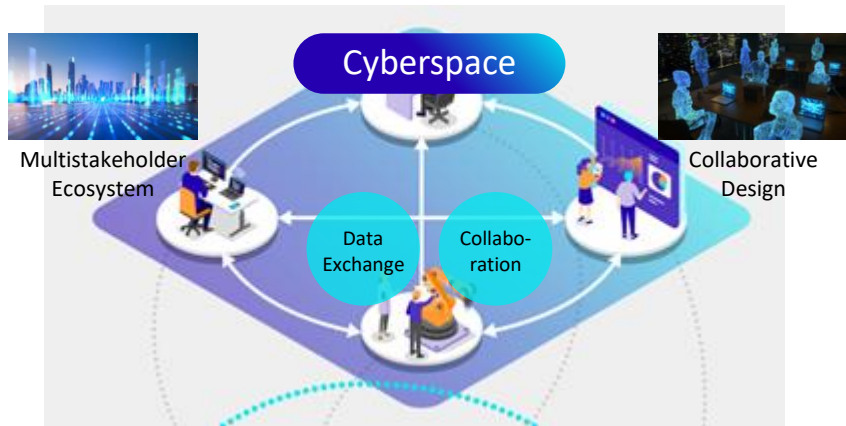


リアル空間と関連づけることで  
**時空間の制約**を“トラスト”に利用

場所・時間の情報

- 地域、国を超えた多様なステークホルダーと新たに共創する機会が増加。

- サイバー空間であっても、経済安全保障、データ越境移転などのルールを守りながらビジネスを活性化する必要



## ○情報通信白書平成29年 第1部 特集 データ主導経済と社会変革より

○ <https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h29/html/nc123110.html>

### <グローバル>

- 2005年から2014年にかけて、越境データの帯域は、4.7Tbps(毎秒テラビット)から211.3Tbpsへと **10年間で約50倍拡大**  
(Mckinsey Global Instituteの分析)
- 北米とEU間のデータ流通に係る帯域が世界の越境データ流通を牽引

### <日本>

- 我が国を起点とした越境データの状況国外ISP等と交換されるトラフィック(帯域)について  
In(国外から国内へ)Out(国内から国外へ)ともに大きく増加。  
特にInは**2004年から2016年の間で約50倍**



## ○ 情報通信白書平成29年 越境データに関する規制等の法制度の動向

- <https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h29/html/nc123120.html>
- 「データローカライゼーションとは、例えばインターネット上のサービス等について、当該サービスを実行する物理的なサーバーはサービスを提供する国内で運用しなければならない、すなわちサービス提供に必要なデータはすべて当該国内に存在しなければならないという考え方に基づくルールであり、その対象はパーソナルデータや産業データなど、目的や理由に応じて整理されるものである。」

# Trust-Enhanced Networking (TEN)

## リアル世界の制約を活かしてトラストを強化

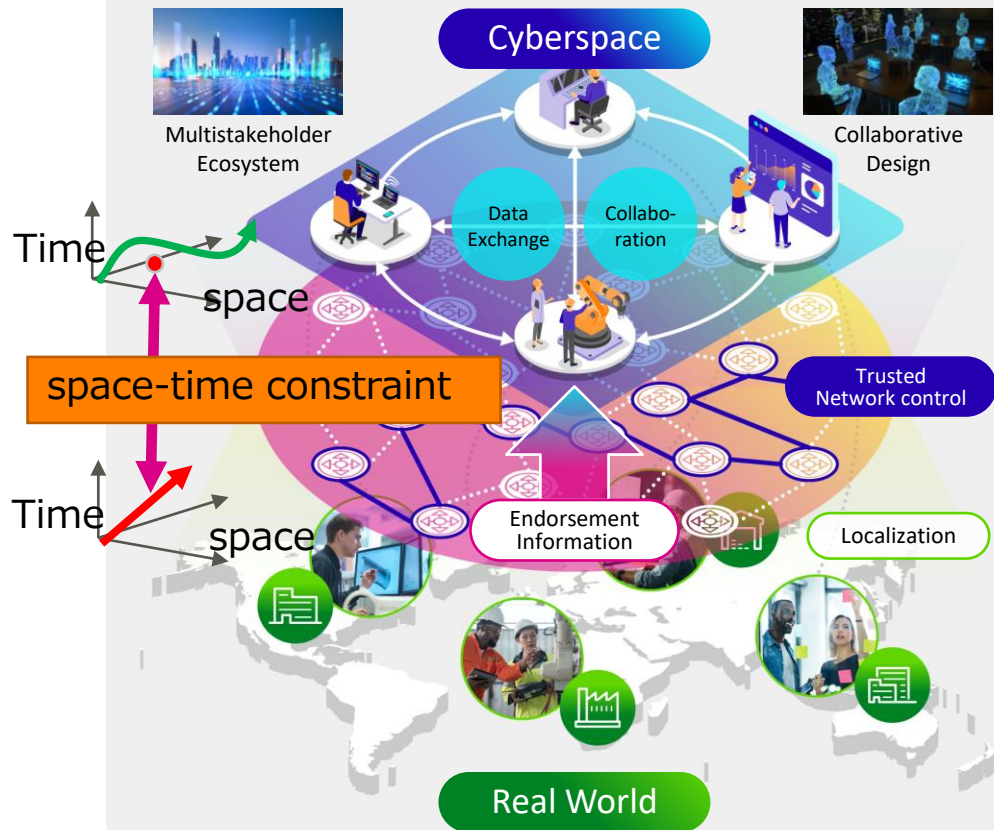
### サイバーとリアルを繋ぐ ネットワークによるトラスト

メタバース/Web3.0といった今後のサイバーでの活動の  
トラストを、リアルな位置などのフィジカルの  
裏付けをネットワークが提供し強化

FUJITSU | CBG  
Fujitsu Cybersecurity Center  
of Excellence in Israel

### 新しいネットワークの役割

- データ/デバイスのリアルな位置を検証しサイバーに提供
- ネットワーク自体がトラストに制御 (信頼する経路を経由)
- ネットワークの先のリアルの実体・実物を検証



# Trust-Enhanced Networking (TEN)

## リアル世界の制約を活かしてトラストを強化

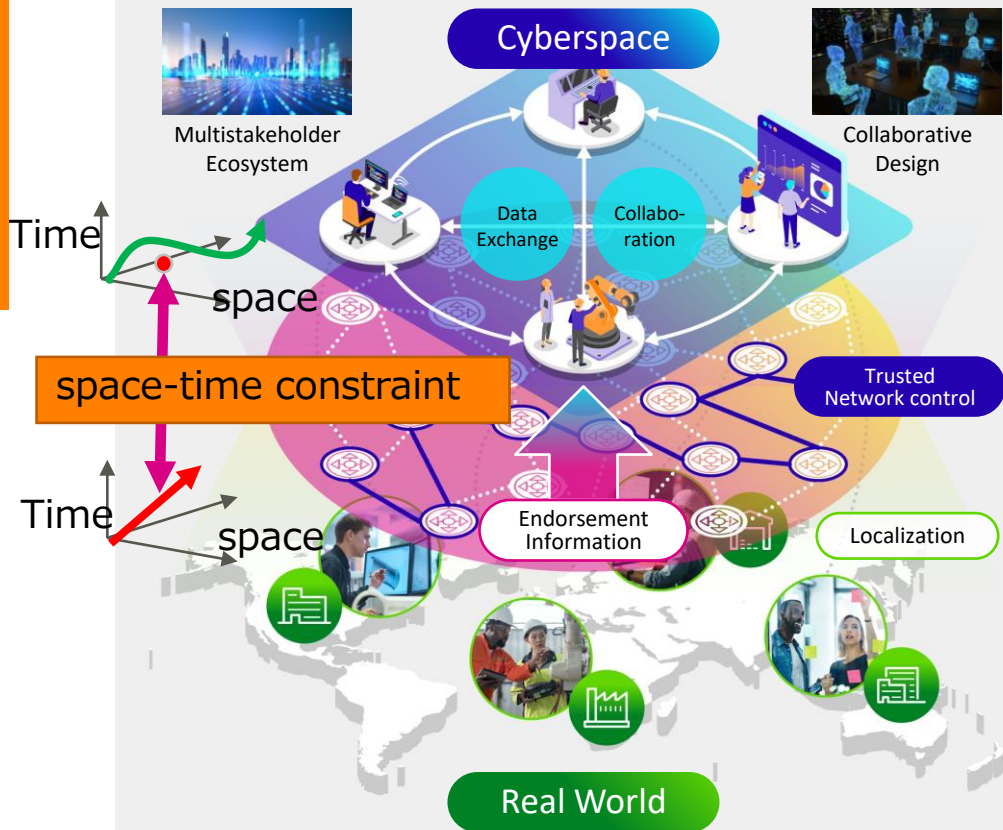
### サイバーとリアルを繋ぐ ネットワークによるトラスト

メタバース/Web3.0といった今後のサイバーでの活動の  
トラストを、リアルな位置などのフィジカルの  
裏付けをネットワークが提供し強化

FUJITSU | CBG  
Fujitsu Cybersecurity Center  
of Excellence in Israel

### 新しいネットワークの役割

- データ/デバイスのリアルな位置を検証しサイバーに提供
- ネットワーク自体がトラストに制御 (信頼する経路を経由)
- ネットワークの先のリアルの実体・実物を検証可能に



# Trust-Enhanced Networking (TEN) Robust localization

ネットワークを通じた位置情報の検証



Fujitsu Cybersecurity Center  
of Excellence in Israel

# Robust Localization

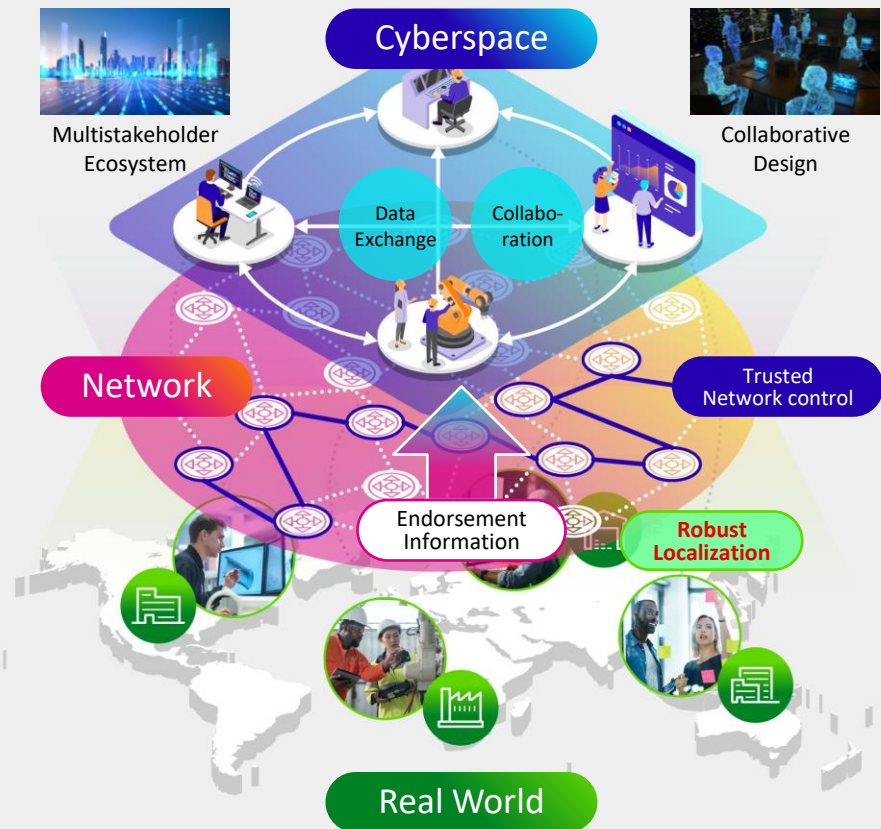
## part of Trust-Enhanced Networking (TEN)

### 1. Robust Localization

- 複数のアンカーポイントを使用したプロービングを発展、サイバースペースのデータの位置を検証

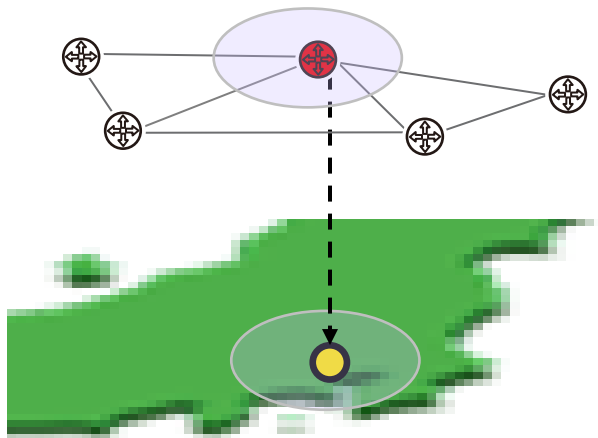
### 2. Trusted Network Control

- ユーザーと利用者を地理的に（意図しない/疑わしい地域を回避）信頼できる経路でデータ転送



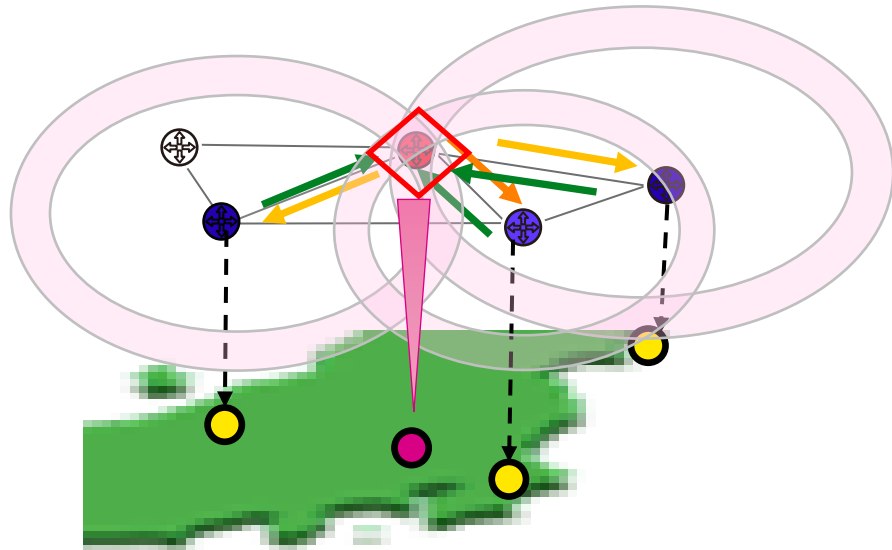
## ○IP-Base Passive

地理情報とアドレスが対応しているランドマークの記録にもとづき直接位置を推定



## ○IP-Base Active

ランドマークを起点にターゲットに対し距離(遅延)を測定、ターゲットの位置を推定



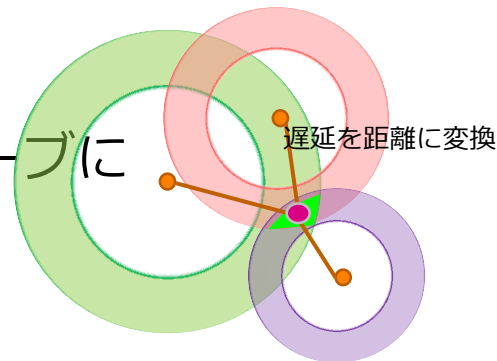
- パブリックレジストリ、データベースをもとに位置を特定
  - Pros 簡単に使える
  - Cons 低いカバレッジ、精度（数百km-千km）
  - 例 Whois、AS 番号、DNS  
MaxMind（2002年）、IP2Location（2002年）

<https://www.maxmind.com/en/home>

<https://www.ip2location.com/>

## ○ ランドマークからのプローブやクエリーを使ったGeolocation 遅延時間ベースが主流

- Pros Passiveに比べて高精度（数十km – 数百km）
- Cons 複数のプローブが必要、ターゲットがプローブに反応しない。 精度がトポロジーに依存など



- GeoPing (2001) : 複数ランドマークから目標までの遅延を測定し推定
- GeoTrack (2001) : 既知のDNS（位置）から目標までの経路をもとに推定
- Constraint-Based geolocation(CBG) (2004)  
複数多地点（ランドマーク）からのDelayを使い距離変換を補正する  
アルゴリズム。実験にRipeを活用
- Topology-aware geolocation (TBG) (2006)  
経路情報も加えてCBGをさらに高精度化



# Street-Level Geolocation Based on Router Multilevel Partitioning (Zhao et al 2019)

- 本研究のアプローチ

- 広いエリアから階層にわけて絞り込むことで精度を改善**

- ターゲットまでの経路を分析し、ターゲットを含むCityの境界を特定絞り込む。複数のランドマークからターゲット周辺のルータを調べ、近傍のルータを中心にサービスレンジを設定、その重なりからターゲットを特定

- 効果 従来アルゴリズムに比べて精度で10-20%改善（平均誤差数km）

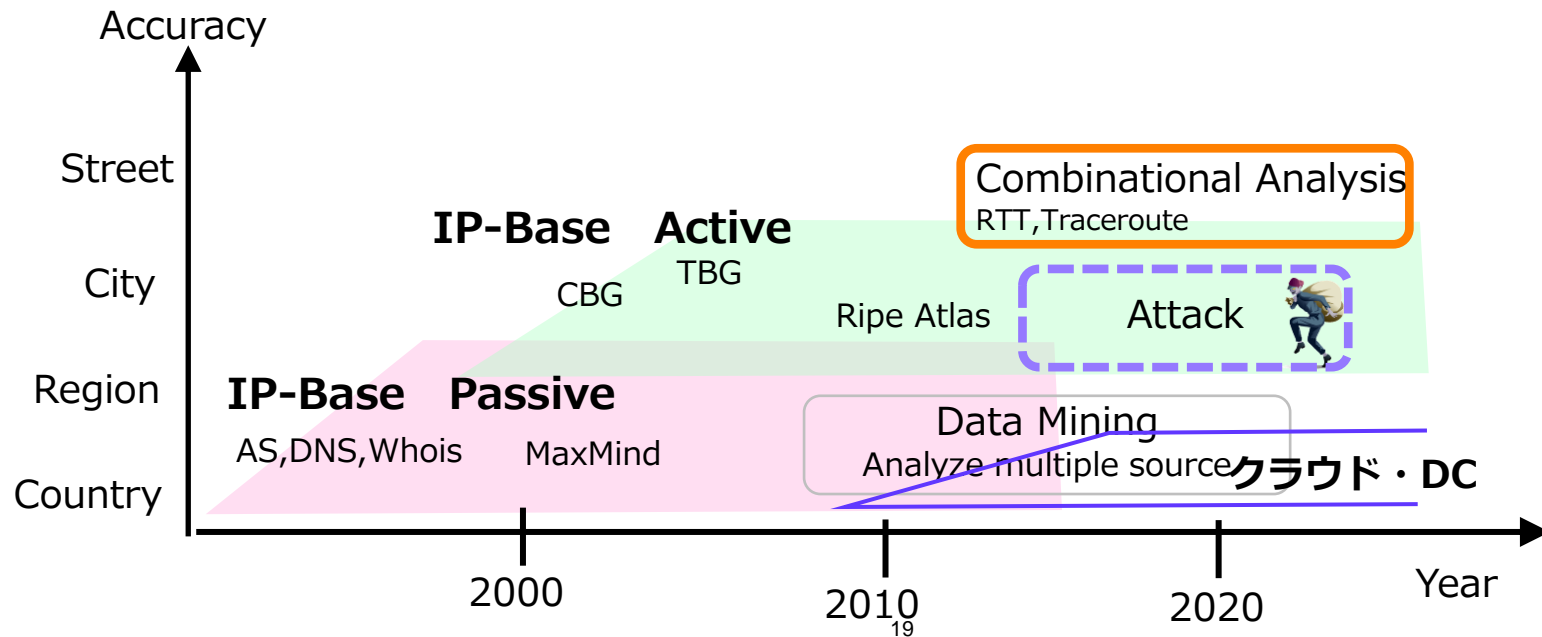
## ○RIPE NCCが運営するインターネットの接続性・到達性を計測する プローブのグローバルネットワーク

- 2010年に、RIPE NCC（欧州地域のIPアドレスを管理する非営利組織; JPNICのEU版）が開始
- 集計結果に基づいてインターネットマップ、データツール、視覚化を提供
- アクティブなプローブ数：11980（2022年10月末）
- ユーザはプローブを使って測定その結果は共有される  
ping, traceroute, SSL/TLS, DNS, NTP and HTTP (to selective targets)

<https://atlas.ripe.net/>

# ネットワークのGeolocationのヒストリー

- 大別して2つの手法：PassiveとActive（プローグ）
- 精度の向上を狙うための複合的な技術から偽装・隠蔽・攻撃などへ
- クラウド（DC）の普及とともにクラウド上のGLの研究が始まる



- ネットワークを通じたGeolocationは長い歴史
- Passiveな手法からActiveなDelay測定、さらに組み合わせなどで高精度化
  - Activeな測定を行う基盤となるプローブネットワーク（例 Ripe Atlas）
- 一方で、クラウドの普及によりGeoLocationは困難な要因が増加
  - DCの位置は公開されない
  - DCはCSPのインフラに隠れてIP-Geolocationの従来手法はつかえない
- さらに、近年は遅延偽装（攻撃）の研究がおこなわれている。

長い間 Geolocationの技術は研究されてきたが、高精度で  
使いやすく、簡単な方法はいまだに課題

## ○ 精度の課題

### ○ IP-Based Passive (Geolocation DB)

- 数百kmの誤差 (IP2Loc, InfoDB等の分析)

CityLevelでClaimしているルータの実際の位置との差分を調査

IP Geolocation Databases: Unreliable? Ingmar Poesse et.al ACM SIGCOMM Computer Communication Review 2011

### ○ IP-Based Active 例 CBG (Constraint -based geolocation)

- 誤差中央値 150 km 米国、100 km 西ヨーロッパ 2割は数百km

Bamba Gueye, et,al Constraint-Based Geolocation of Internet Hosts IEEE/ACM TRANSACTIONS ON NETWORKING 2006

## ○ 隠蔽・偽装の課題

- VPNやProxyにより隠蔽可能。

### ○ 偽装の課題：Delay測定を偽る手法

- レスポンス時間をあえて長くしRTTを偽る
- パケットの生成時間を書き換えて返す
- Fake パケットを発信時間を推定してそのタイミングで返す

## ○ クラウド・DC内部のLocationの課題

**狙い** データの所在、運ばれる経路を阻害要因を回避して高い精度で検証可能にする

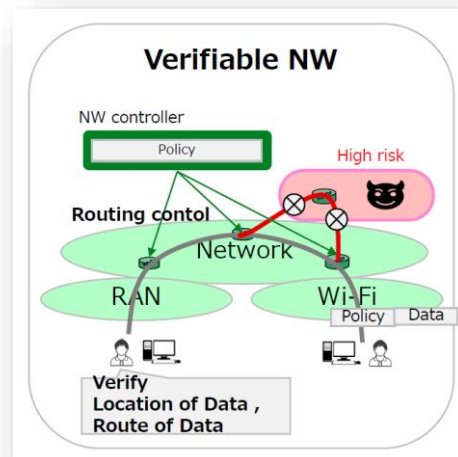
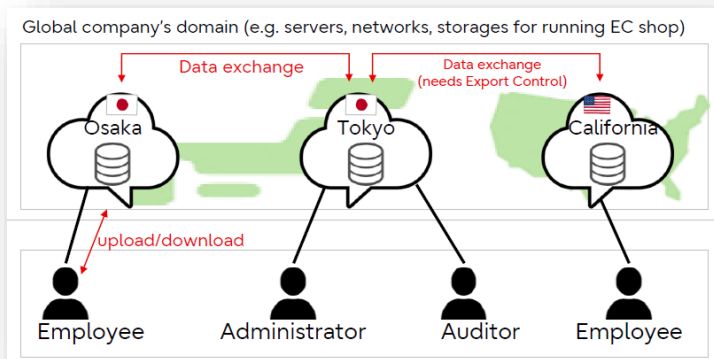
## 正確なGeo Locatingを阻害する要因

- VPN/Proxy
- 遅延による位置偽装、複雑なトポロジー
- 経路ハイジャック、ワームホールアタック
- クラウド
- マルチ・ドメイン



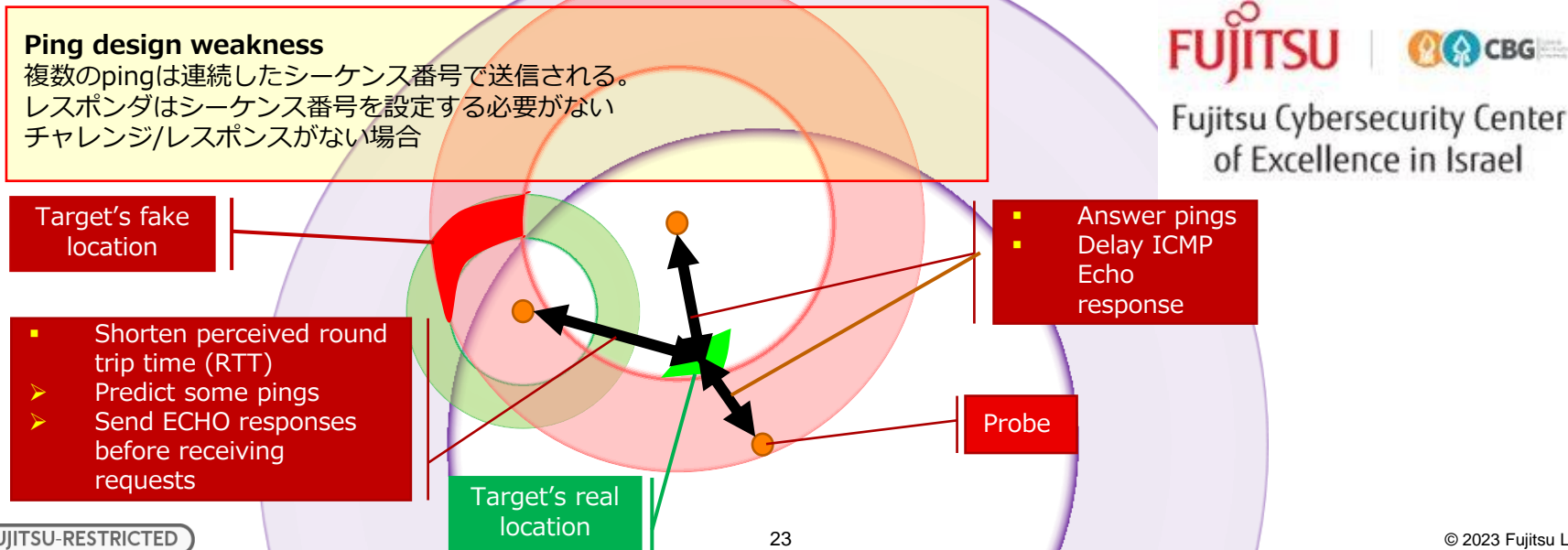
検知・回避して正確に測定する方法はないか？

**Robust Localization**



# 超信頼なGeolocation実現に向けて

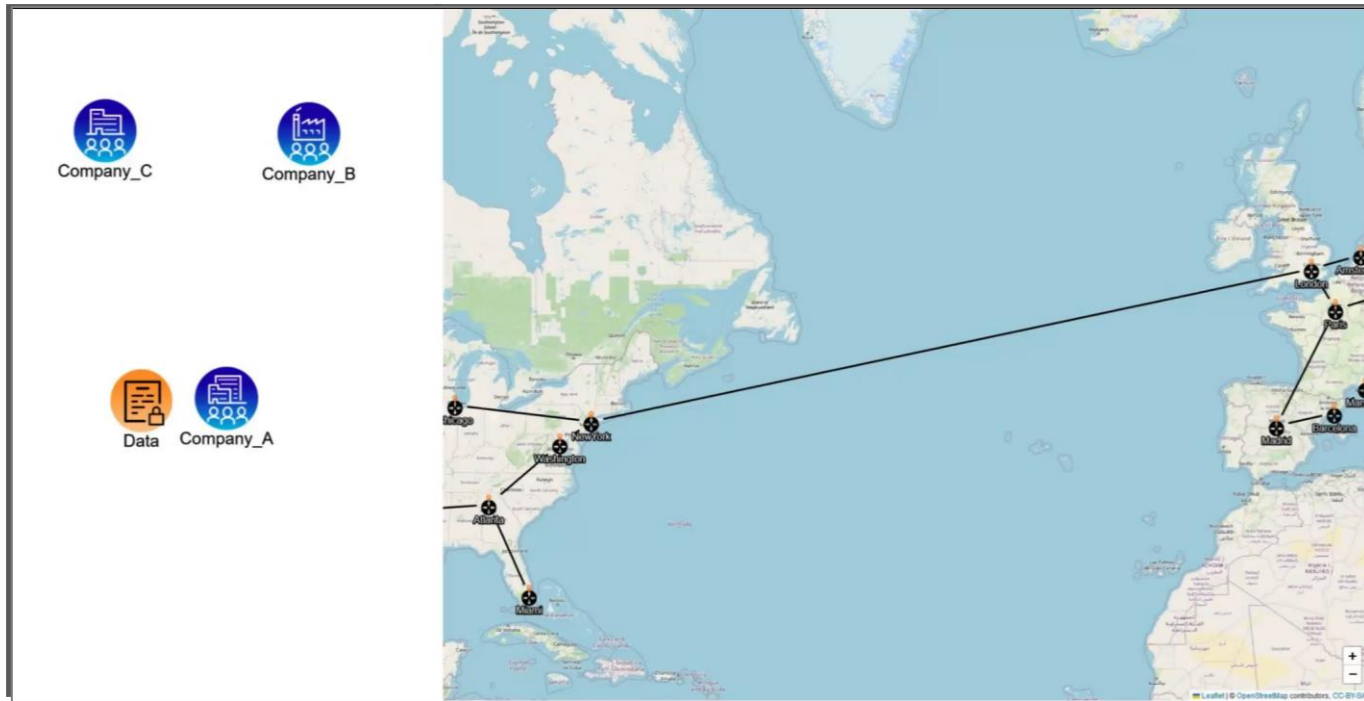
- 遅延時間に基づく複数プローブのアプローチは確実な一方で、セキュリティリスクへの対応が課題
  - spoofing , topology obfuscation, route hijacking, wormhole attack etc.
- この課題の克服に向け、イスラエル Ben-Grion大学と共同研究を推進



## シナリオ 1:

相互の所在地を検証し、メタバース上で安心して取引相手とマッチング

- 企業Aはビジネスパートナーを探している（企業B,Cなどが候補）
- センシティブな情報を扱う事業のため、地理的な情報を含めてパートナーのアイデンティティを確認する必要がある



Entities in B2B metaverse

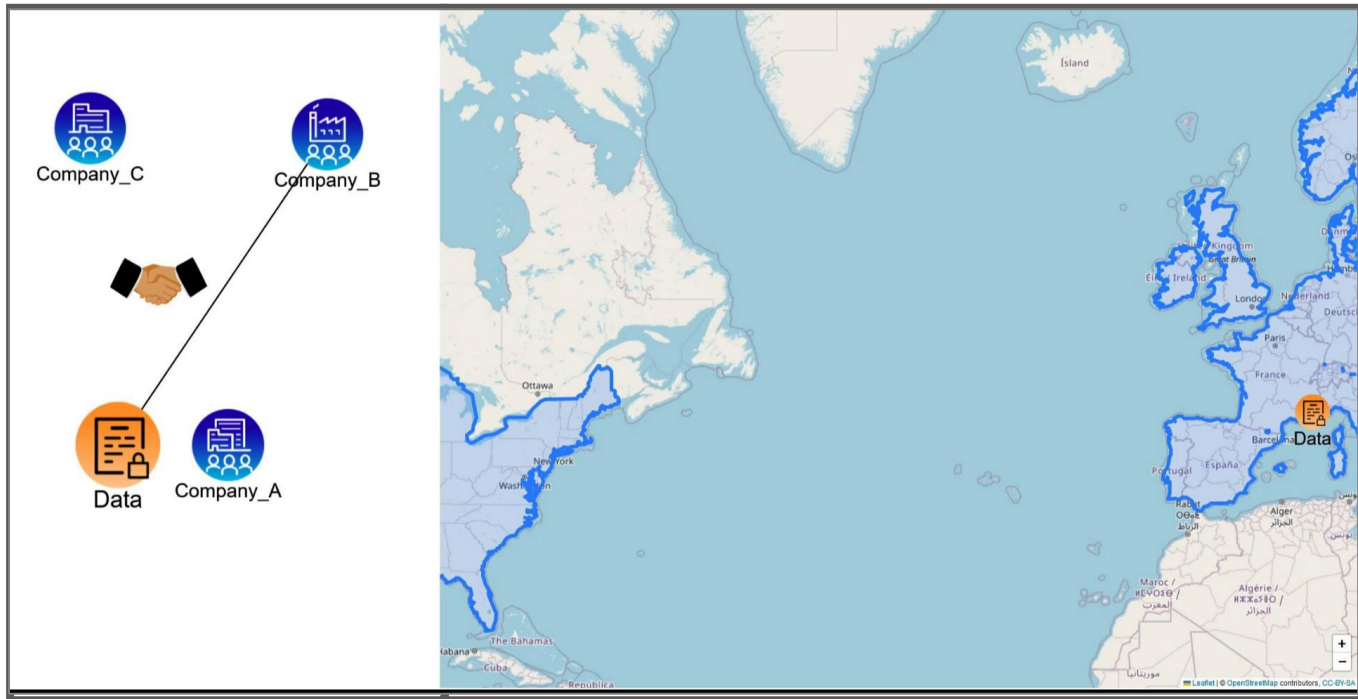
Physical information provided by the network



# 利用例: “トラストな経路で機密データを転送”

**シナリオ 2:**  
データ転送経路を検証  
しながら、安心して  
B2B取引を実施

- 企業Aは企業Bにデータを送りたい
- データには機密情報を含むため、転送時に決められた地域の外には出てはいけない



Entities in B2B  
metaverse

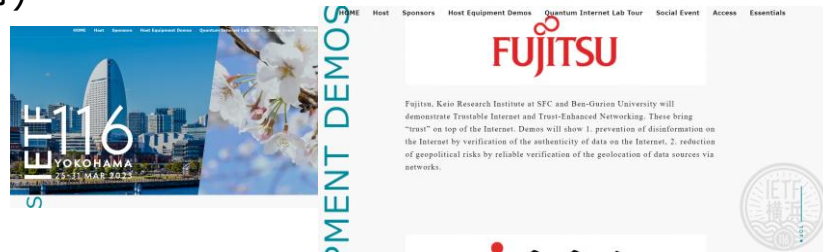
Physical information provided by the  
network

# わたしたちの取り組み



イスラエルのベングリオン大学  
内にNWセキュリティ分野の技  
術革新に取り組む新拠点を設立  
“Trust-Enhanced Networking”  
コンセプトに関するホワイト  
ペーパーを発行 (2022年12月)

IETF116 Yokohama2023.3月  
にてベングリオン大学と共同展示



[参考]  
IETFではインターネットのデータの確からしさを検証可能にするTrustable Internetを慶應大学と共同展示

「Trustable Internet」について

「Trustable Internet」によるアプローチでは、インターネット上のデータの確からしさを検証可能にする。検証可能なインターネットが元のデータの確からしさとして期待可能な信頼を付与し、利用者の間で共有する (Endorsement Layer) をインターネットの最上層に追加することでデータの確からしさを確保可能とする新しいアプローチです。この層は、既存のインターネットに実装を及ぼす実装可能な。インターネット利用者は従来のWebアプリケーションを使用し、必要に応じてデータの確からしさを検証可能な信頼の取得が可能です。

確からしさの物理的属性と結合可能な信頼性は、データ生成者人と検証可能な信頼性 (匿名 (人・法人) の名前、所属、資格、または生成した場所、場所、日時など) のほか、データ生成者と共有されるもの (専門家のような第三者によるアーケの検証・評価など)、さらにインターネットの信頼性といったフィジカル属性から導かれる可能性があります。これらの信頼性を (Endorsement Layer) と呼ぶアプローチに賛同し、信頼可能なインターネット上のデータを提供する際に、Endorsement Layer、その信頼性を提供、検証した。また確からしさを確保するために必要信頼をログアウトすることで、信頼性がデータの確からしさを検証可能になります。

2022年10月13日  
慶應義塾大学研究科  
富士通株式会社

Web/App  
Endorsement Layer  
Internet

付加 関与 リクエスト

情報取得

グラフの起点

信頼可能なデータ

※「Endorsement Layer」のイメージ

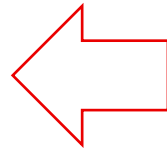
インターネット上のデータの確からしさを汎用的かつ容易に確認可能な「Trustable Internet」のコンセプトに関するホワイトペーパーを公開

- ネットワークはデータを運ぶだけでなく、サイバーに信頼をもたらす重要な役割を担う “Trust-Enhanced Networking” のコンセプトを紹介
  - サイバー上での活動を安心して行えるように、ネットワークが実世界における物理的なお墨付き情報を取得・提供

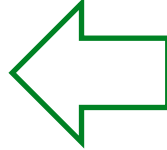
MO DPF研究会 って何ですか

「DPF研究会」とは、データプラットフォーム構築促進協議会（Data Platform Forum）が主催する研究会の一つで、データプラットフォーム（DPF）に関する技術研究を行う団体です。

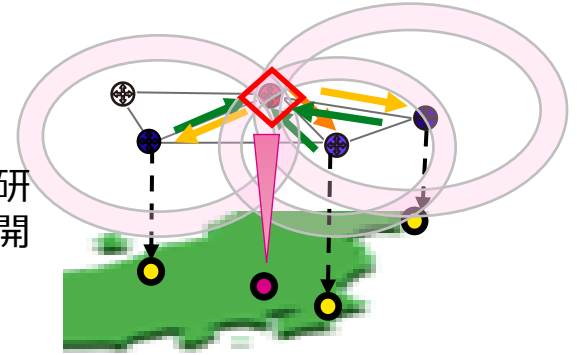
信頼できない



正しい！！



3月17日に  
オンラインで研  
究会を川崎で開  
催している！



DPF研究会の皆様と可能性をご議論させていただければ幸いです。  
(ChatGPTも交えて)

- [1] Fujitsu whitepaper on Trust-Enhanced Networking. <https://www.fujitsu.com/global/about/research/article/202212-trust-enhanced-networking.html>, 2022.
- [2]. IP Geolocation Databases: Unreliable? Ingmar Poese et.al ACM SIGCOMM Computer Communication Review 2011
- [3] Shichang Ding, Fan Zhao, and Xiangyang Luo. A street-level ip geolocation method based on delay-distance correlation and multilayered common routers. Security and Communication Networks, 2021, 2021.
- [4] Qiang Li, Zhihao Wang, Dawei Tan, Jinke Song, Haining Wang, Limin Sun, and Jiqiang Liu. Geocam: An ip-based geolocation service through fine-grained and stable webcam landmarks. IEEE/ACM Transactions on Networking, 29(4):1798– 1812, 2021.
- [5] Fan Zhao, Rui Xu, Ruixiang Li, Ma Zhu, and Xiangyang Luo. Street-level geolocation based on router multilevel partitioning. IEEE Access, 7:59237–59248, 2019.
- [6] Jing-ning Chen, Fen-lin Liu, Ya-feng Shi, and Xiangyang Luo. Towards ip location estimation using the nearest common router. Journal of Internet Technology, 19(7):2097–2110, 2018.
- [7] Hao Jiang, Yaoqing Liu, and Jeanna N Matthews. Ip geolocation estimation using neural networks with stable landmarks. In 2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pages 170–175. IEEE, 2016.
- [8] Michael J. Freedman Mythili Vutukuru, Nick Feamster, Hari Balakrishnan Geographic Locality of IP Prefixes Internet Measurement Conference 2005
- [9] Bamba Gueye, Artur Ziviani, Mark Crovella Constraint-Based Geolocation of Internet Hosts IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 14, NO. 6, DECEMBER 2006
- [10] Qiang Li, Zhihao Wang, Dawei Tan, Jinke Song, Haining Wang, Limin Sun, and Jiqiang Liu. Geocam: An ip-based geolocation service through fine-grained and stable webcam landmarks. IEEE/ACM Transactions on Networking, 29(4):1798– 1812, 2021.
- [11] Fan Zhao, Rui Xu, Ruixiang Li, Ma Zhu, and Xiangyang Luo. Street-level geolocation based on router multilevel partitioning. IEEE Access, 7:59237–59248, 2019.
- [12] Jing-ning Chen, Fen-lin Liu, Ya-feng Shi, and Xiangyang Luo. Towards ip location estimation using the nearest common router. Journal of Internet Technology, 19(7):2097–2110, 2018.

- [13] Hao Jiang, Yaoqing Liu, and Jeanna N Matthews. Ip geolocation estimation using neural networks with stable landmarks. In 2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pages 170–175. IEEE, 2016.
- [14] Michael J. Freedman, Mythili Vutukuru, Nick Feamster, Hari Balakrishnan. Geographic Locality of IP Prefixes. Internet Measurement Conference 2005
- [15] Bamba Gueye, Artur Ziviani, Mark Crovella. Constraint-Based Geolocation of Internet Hosts. IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 14, NO. 6, DECEMBER 2006
- [16] Fan Zhang, Fenlin Liu, Rui Xu, Xiangyang Luo, Shichang Ding, and Hechan Tian. Street-level ip geolocation algorithm based on landmarks clustering. CMCCOMPUTERS MATERIALS & CONTINUA, 66(3):3345–3361, 2021.
- [17] Shuodi Zu, Xiangyang Luo, Siqi Liu, Yan Liu, and Fenlin Liu. City-level ip geolocation algorithm based on pop network topology. IEEE Access, 6:64867–64875, 2018.
- [18] Yang Zhang, Dongzheng Jia, Shijie Jia, Limin Liu, and Jingqiang Lin. Splitter: an efficient scheme to determine the geolocation of cloud data publicly. In 2020 29<sup>th</sup> International Conference on Computer Communications and Networks (ICCCN), pages 1–11. IEEE, 2020.
- [19] Dongzheng Jia, Yang Zhang, Shijie Jia, Limin Liu, and Jingqiang Lin. Dpvgeo: Delay-based public verification of cloud data geolocation. In 2020 IEEE Symposium on Computers and Communications (ISCC), pages 1–7. IEEE, 2020.
- [20] Dong Lai Fu, Xin Guang Peng, and Yu Li Yang. Trusted validation for geolocation of cloud data. The Computer Journal, 58(10):2595–2607, 2015.
- [21] Katharina Kohls and Claudia Diaz. {VerLoc}: Verifiable localization in decentralized systems. In 31st USENIX Security Symposium (USENIX Security 22), pages 2637–2654, 2022.
- [22] Abdelrahman Abdou, Ashraf Matrawy, and Paul Oorschot. Accurate manipulation of delay-based internet geolocation. pages 887–898, 04 2017.
- [23] Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor: The secondgeneration onion router. Paul Syverson, 13, 06 20

# Thank you

A large, stylized graphic element is positioned in the center of the slide. It consists of two interlocking loops, one on the left and one on the right, that resemble a figure-eight or infinity symbol. The loops are filled with a gradient of blue, transitioning from a darker shade on the left to a lighter shade on the right. The graphic is partially overlaid by the "Thank you" text on the left and the "Please contact the following" text below it.

If you have any questions about the content, please contact  
Please contact the following

[sekiya.motoyosh@jp.fujitsu.com](mailto:sekiya.motoyosh@jp.fujitsu.com)