

概要

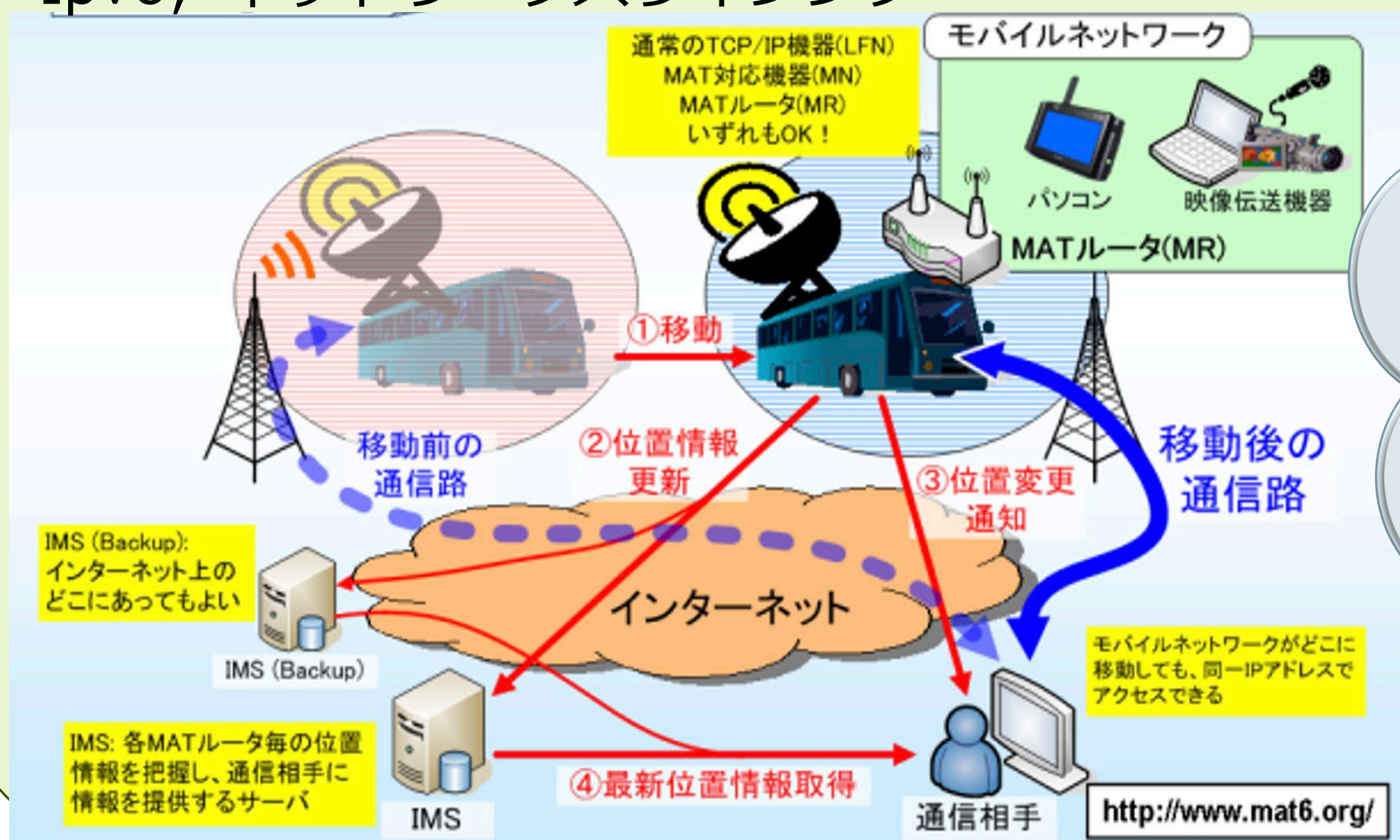
情報通信の基盤となるインターネット、モバイル通信、クラウド、仮想化技術の最新技術は勿論のこと、情報通信によって生み出される人同士のコミュニケーションまで含めた新しい基盤技術に関する研究をしています。本グループでは、次世代ネットワーク技術だけでなく、誰もが安心してネットワークサービスを楽しむ世界を目指しセキュリティ技術分野における研究も行っています。

先端ネットワーク

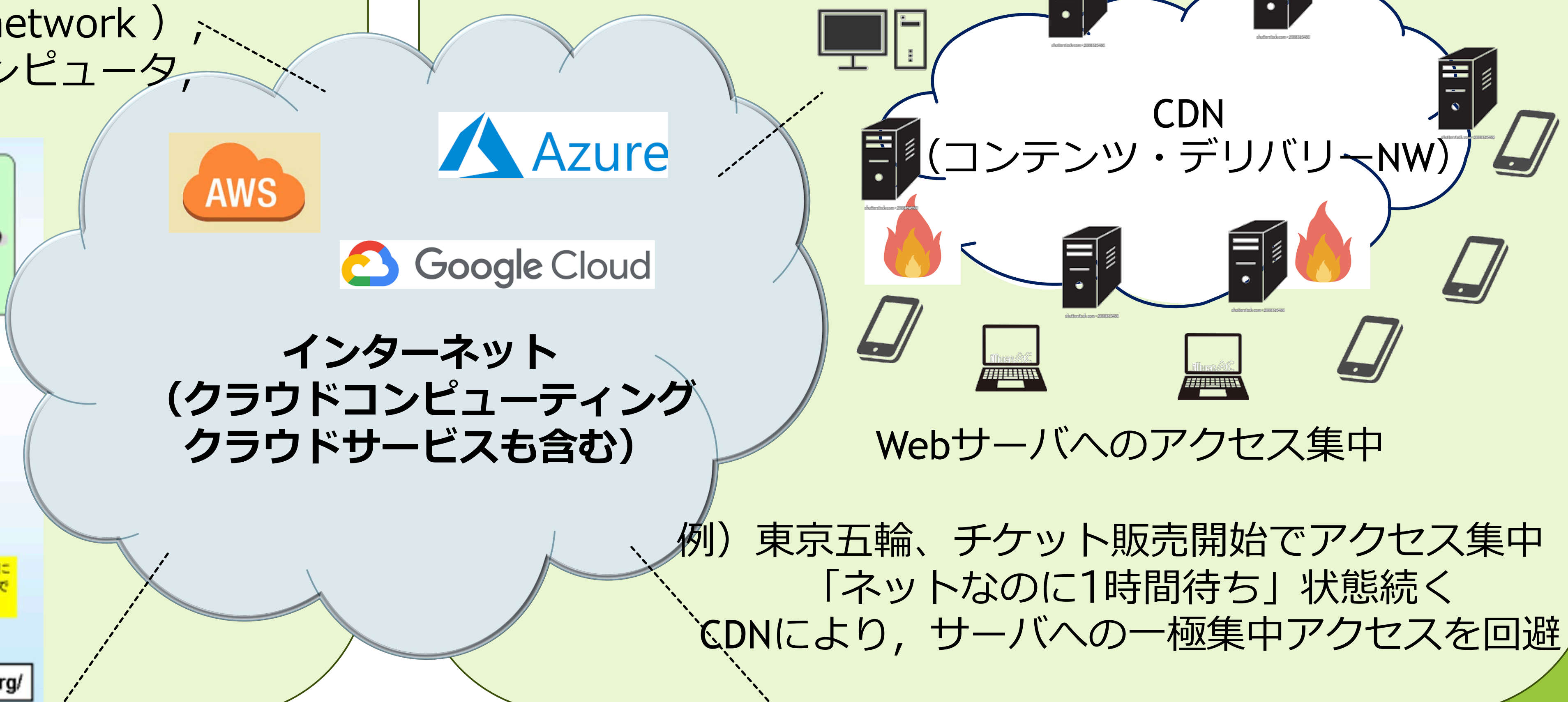
次世代NW基盤技術

いつでもどこでも高速、高信頼、低遅延、多接続を実現するネットワーク基盤を作る！

- ・ Bluetooth MANET, VANET (vehicle ad hoc network)
- ・ 移動透過通信技術, 仮想化, クラウド, エッジコンピュータ, Ipv6, ネットワークスライシング



Webサービス



情報ネットワーク(パソコンやサーバの繋がり) → 社会生活との結びつきが強い

例: 某映画が放送されると某SNSの処理が遅くなる

ユーザーの集団的な行動が 情報ネットワークの大規模な障害に繋がる!

情報ネットワークと社会ネットワークを併せた大規模で複雑であるネットワークの構造を分析

情報ネットワークの安定運用技術に応用しよう!

SNS関連

ネット炎上, バズ事象の因果律の解明

情報ネットワーク側からの制御

モバイルタイルディスプレイ ストリーミング

複数の端末(例えばAndroidやiPhoneなど)を用いて、1枚の画面を構成し、動画を再生する

amazon prime video, YouTube, NETFLIX, U-NEXT

4分割

複数人で動画を見たいとき、一人一人の端末を用いて大画面で見ることができる

ネットワーク・セキュリティ

暗号アルゴリズム

数学の力で情報漏洩、データの改ざん、なりすまし被害などあらゆる脅威から身を守る

共通鍵/公開鍵暗号、電子署名、秘密計算、ブロックチェーン、耐量子計算機暗号、etc.

データ作成者保証

暗号資産

個人情報秘匿化

いろんなサービスを実現

セキュア分散通信

不正アクセスや故障に強いセキュアな分散通信技術を確立する

一般的な通信方法: [基地局, ゲートウェイ]・通信データが集まる

不正アクセスや故障に対する弱点

セキュア分散通信: [通信端末]・スマートフォン・センサその他

WSN (Wireless Sensor Network)

図3 複数のGWをもつWSNの概念図

図4 ノードSから各GW候補が属するサブネットまでの最短経路

セキュリティシステム

セキュリティの仕組みを導入した新しい情報処理技術の実現やICTサービスの提案を行う

公開鍵認証基盤、プライバシー保護、電子商取引、デジタル著作権管理、etc.

デジタルコンテンツの編集制御機能の例

正当な編集 (例: A3を削除)

不正な編集 (例: A2を削除)

オリジナルコンテンツ: A1, A2, A3, A4

削除用署名集合: σ1, σ2, σ3, σ4

Aggregate署名: σ (= σ1 × σ2 × σ3 × σ4)

認証・認可

「あなたが誰であるか」を確認する ⇒ 認証

- 1) IDと本人である証拠を提示
- 2) 本人であるか証拠を問い合わせ
- 3) 本人であることを確認
- 4) 本人と確認したことを通知

認証サーバ, ユーザ情報データベース

「あなたはそれを動かしてよい人か」を確認する ⇒ 認可

- 1) 使用権限の許可を申請
- 2) 使用権限があるか確認する
- 3) 使用権限の有無の結果を示す
- 4) 権限がないことを通知

認証サーバ, ユーザ情報データベース

サイバーテロ対策

ネットワークやコンピュータを監視し、不正な攻撃から情報や人を守る

IDS/IPS, ファイヤーウォール, DoS対策, アンチウイルス機能、etc.

サイバー攻撃対策の例

インターネット, DMZ, イン트라ネット

不正者

不正アクセス検知システム

UTMで攻撃遮断

不正から防御

安心安全なICT環境を実現