モバイルネットワークにおける利用者認証の現状・課題・研究動向

2021年11月29日

（株）IT企画　才所敏明
（株）ZenmuTech
toshiaki.saisho@advanced-it.co.jp
http://www.advanced-it.co.jp

共　著　者

辻井重男
中央大学研究開発機構

櫻井幸一
九州大学　大学院システム情報科学研究院
＆サイバーセキュリティーセンター
（株）国際電気通信基盤技術研究所

謝辞　本研究の一部は　一般財団法人テレコム先端技術研究支援センターの研究助成を受けている。

はじめに

（1）現在はインターネット（依存）社会
- ＊1974年のTCP/IP発表：インターネットの歴史は高々半世紀
- ＊今やインターネット無しでは
  産業界の経済活動や国民の生活活動も成り立たない
- ＊社会の安心・安全は，
  インターネット上の活動の安心・安全に強く依存する時代

（2）インターネットの最大の課題は，利用者の確実な認証（本人確認）機能の欠如
- ＊もともと研究者間のコミュニケーションツールとしての利用を想定
- ＊世界各国の不特定多数の人々が利用する現在，
  インターネット上のさまざまの事故・事件の氾濫を招き，大きな社会問題

（3）モバイル端末がインターネット利用の主役へ

＊1G（1979年）➔2G（1993年）➔3G（2001年）

➔4G(2010年）➔5G（2020年）➔Beyond5G/6G（2030年？）

＊1985年ショルダーホン発売

＊2010年にはインターネット利用でモバイル端末がPCを上回る

（4）モバイルネットワークのセキュリティ

＊事業者による有料サービスとして発展

一定レベルの利用者認証機能は実装されている

＊しかし，利用者認証にかかわるセキュリティ要件である，

利用者の確実な本人確認

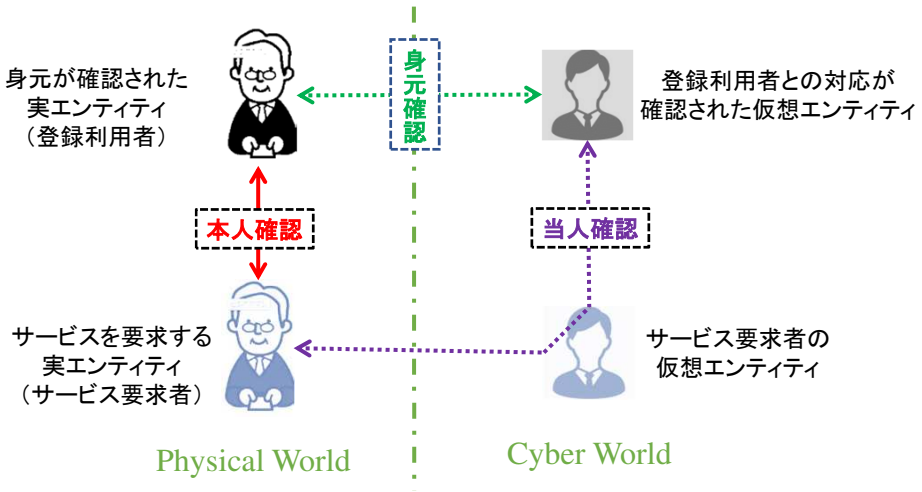
利用者の匿名性確保

不正・不法な利用者の特定・追跡の仕組み

の面ではまだまだ課題も多い．

➔モバイルネットワークサービス事業者が実施する
利用者認証にかかわるセキュリティについて，
5Gの現状，Beyond5G/6Gに向けた検討課題，研究動向等調査

利用者認証（本人確認）

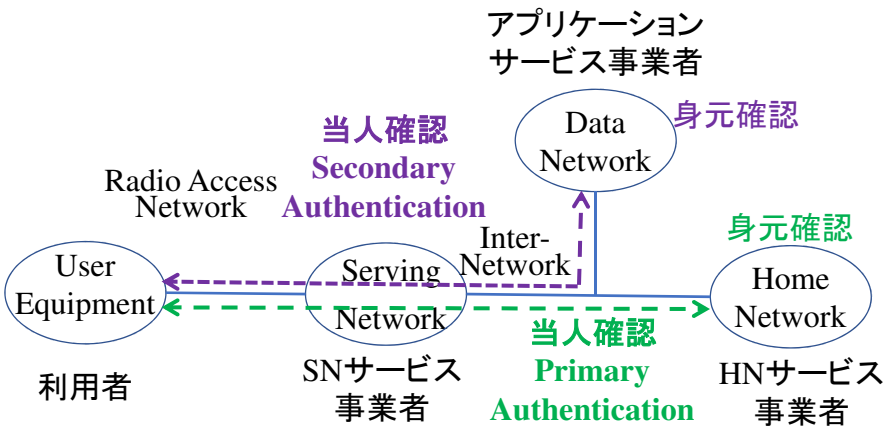


本人確認＝身元確認＋当人確認

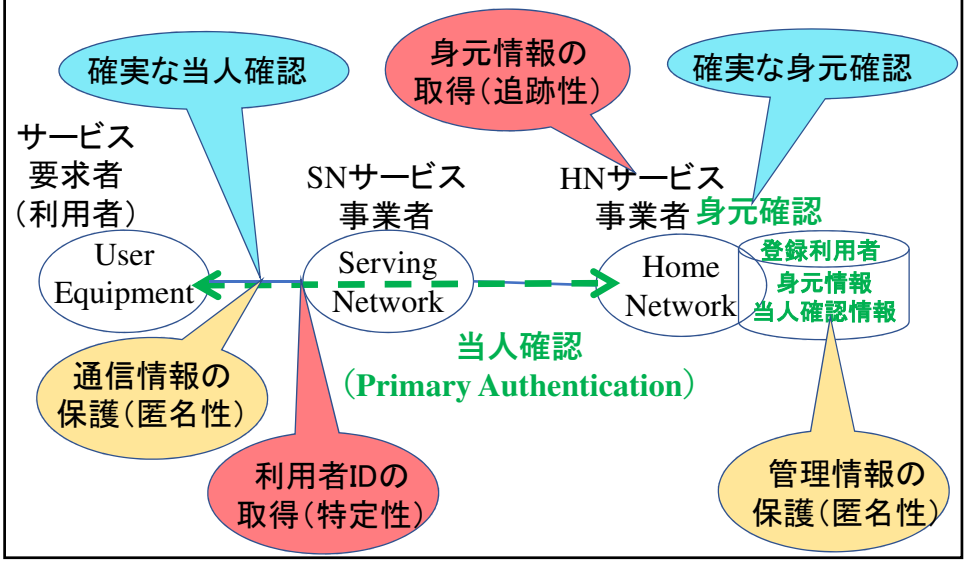
身元確認・当人確認の保証レベル（NIST Special Publication 800-63A,B）

保証レベル	身元確認方法の要件・特徴（IAL）	当人確認方法の要件・特徴（AAL）
1	本人確認不要（自己申告での登録でよい）	単要素認証でOK
2	識別に用いられる属性をリモートまたは対面で確認する必要あり	2要素認証が必要、2要素目の認証手段はソフトウェアベースのものでOK
3	識別に用いられる属性を対面で確認する必要があり、確認書類の検証担当者は有資格者	2要素認証が必要、かつ2要素目の認証手段はハードウェアを用いたもの（ハードウェアトークン等）

モバイルネットワークにおける利用者認証

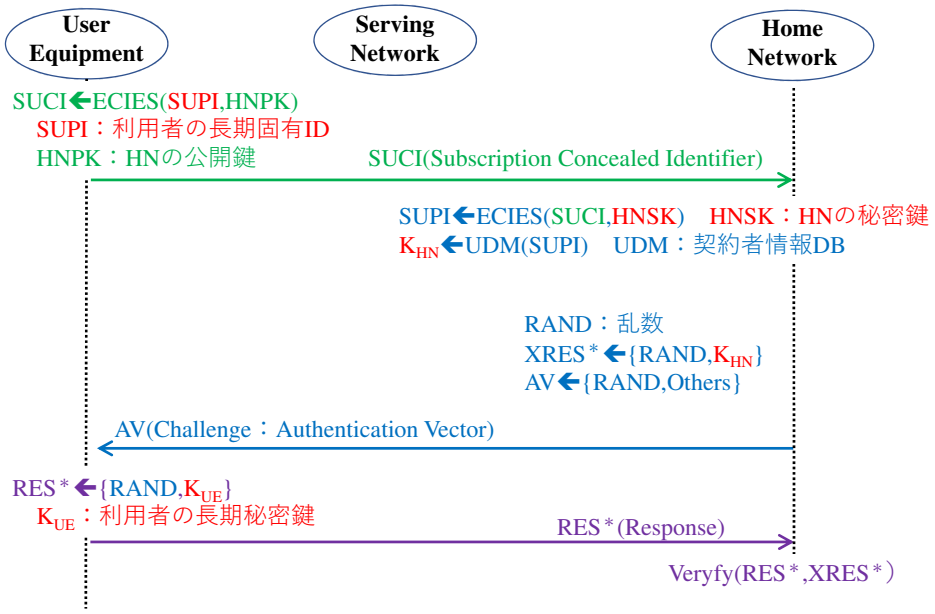


モバイルネットワークサービスにおける利用者認証の主要なセキュリティ要件



セキュリティ要件	5Gの現状	
確実な本人確認	身元確認	各国の公的機関や民間組織で発行される証明書等による身元確認。身元確認方法や身元確認の信頼性のレベルは各国で異なっている
	当人確認（5G-AKA）	
利用者の匿名性		
利用者の特定・追跡性		

5G-AKAプロトコル（超概要）



セキュリティ要件	5Gの現状	
確実な本人確認	身元確認	各国の公的機関や民間組織で発行される証明書等による身元確認。身元確認方法や身元確認の信頼性のレベルは各国で異なっている
	当人確認（5G-AKA）	UEは利用者固有ID（SUPI）をSN経由でHNへ送信、HNが契約利用者を特定。利用者固有IDに対応する長期秘密鍵（K）をUEが保有するかどうかをHNが確認。
利用者の匿名性	管理情報	利用者情報は契約するHNサービス事業者が管理。各国の法制度やガイドライン等に基づき管理・保護され、保護の確実性については各国で異なっている。
	通信情報	利用者固有ID（SUPI）は、HNの公開鍵を利用した暗号化後、HNへ送信。長期秘密鍵（K）は、乱数およびハッシュ関数によりワンタイム化し、UEへ送信。
利用者の特定・追跡性	特定	暗号化された利用者固有ID（SUCI）から利用者固有IDの特定（復号）は困難。特定可能なHNサービス事業者の協力により利用者の特定は可能。
	追跡	利用者の追跡に必要な利用者情報はHNサービス事業者が管理。利用者固有IDを特定できれば、HNサービス事業者の協力により利用者の追跡は可能。

セキュリティ要件	Beyond5G/6Gの課題・研究動向	
確実な本人確認	身元確認	HNサービス事業者が確保すべき身元確認の信頼性レベルおよびその評価・認定方法等のガイドライン策定が望ましい。（参考：NISTのSP 800-63A）
	当人確認	
利用者の匿名性		
利用者の特定・追跡性		

Beyond5G/6Gに向けた当人確認に関する研究動向

A：5G-AKAの脆弱性・課題対応研究（[3]～[8]）

指摘されている5G-AKAの脆弱性・課題例：

利用者のプライバシー情報（SUPI等）の漏洩

Compromised SN Malicious SN

セッションのlinkability（複数セッションの利用者の同一性特定）

ロケーション情報の漏洩

リプレイアタックによるなりすまし等

B：量子コンピュータ対応研究（[9]～[12]）

指摘されている5G-AKAの脆弱性・課題例：

公開鍵暗号方式ECIESの利用（利用者固有ID（SUPI）の保護）

➔Shorアルゴリズムによる安全性への脅威

128ビットの鍵長の暗号鍵の使用

（利用者固有ID（SUPI）、利用者長期秘密鍵（K）の保護）

➔Groverアルゴリズムによる安全性への脅威

C：Blockchain技術の応用研究（[14]～[16]）

UEとHN間の当人確認プロセスにBlockchainを利用

5G-AKAは、モバイルネットワークを構成する多くの機器を経由

狙い

①UEとHN間の通信を少なくし，応答性能向上，ネット負荷軽減

②モバイルネットワーク上を流れる情報からの

利用者に関する情報の漏洩リスクの軽減

D：バイオメトリクス技術の応用研究（[17]～[20]）

当人確認の高度化を目指したバイオメトリクス技術の利用

①従来からの静的生体特徴を利用したバイオメトリクス認証

②動的生体特徴を利用したバイオメトリクス認証，

連続的利用者認証を可能とする当人確認

セキュリティ要件	Beyond5G/6Gの課題・研究動向	
確実な本人確認	身元確認	HNサービス事業者が確保すべき身元確認の信頼性レベルおよびその評価・認定方法等のガイドライン策定が望ましい。（参考：NISTのSP 800-63A）
	当人確認	IMSI catcher等の4Gで指摘されていた主な脆弱性については対応。5G-AKAの脆弱性・課題対応および新方式提案等の研究開発が活発化。
利用者の匿名性	管理情報	HNサービス事業者が確保すべき身元情報の保護レベルおよびその評価・認定方法等のガイドライン策定が望ましい。（参考：国際規格ISO27001、ISO29100）
	通信情報	(当人確認方式の課題・研究の一環として推進中)
利用者の特定・追跡性	特定	HNサービス事業者が契約利用者かどうかを確認できる情報は今後もUEから送信される必要があり事業者の協力により，利用者固有IDの特定は可能と考えられる。（合法的傍受の仕組みは今後も必要）
	追跡	利用者の追跡に必要な利用者情報は今後もHNサービス事業者が管理。利用者追跡に必要な身元情報への合法的アクセスの仕組みは今後も必要。

まとめ

（1）モバイルネットワークサービスの利用者認証を構成する
①HNサービス事業者による身元確認
②UEとHN間で実施される当人確認
における、主要な三つのセキュリティ要件
①確実な本人確認
②利用者の匿名性
③利用者の特定・追跡性
について、
①5Gの現状（対応状況）
②Beyond5G/6Gにむけての課題や研究動向
を、整理・考察した。

（2）Beyond5G/6Gにおける利用者認証にかかわるセキュリティ課題は,
①技術的側面
②社会的側面
の両面から検討が必要
（3）技術的側面では、
①現状（5G）の分析・評価による課題抽出と克服策の研究開発
②Beyond5G/6Gの具体化に伴う新たなセキュリティ課題への対応
③新技術開発・実用化の進展に伴う新たな克服策の可能性探求
それぞれの視点からの検討が必要
（4）社会的側面では、
①個人の権利を尊重した匿名性
②社会の安心・安全の維持のための不正・不法な利用者の特定・追跡性
の両立に関する国民の合意形成が必要であり、
①各国の主権の尊重
②グローバルなモバイルサービスの安心・安全を確保するための国際連携
に関する国際的合意形成も必要

終

（ご清聴、ありがとうございました。）