5Gモバイルシステムとセキュリティ

IDF 第17期第1回「技術」分科会

Huawei Technologies Japan K. K.

2020. 7.15

Security Level:

自己紹介

赤田正雄　CTO/CSO, Huawei Technologies Japan

1983年　東京大学 工学部 情報工学 修士
第５世代コンピュータ（推論・AIマシン）の研究室で分散OSの研究。
パケット通信装置試作、ミニコンへの分散OSカーネル実装など。

1983年～　NEC入社 交換機開発部門。D70交換機加入者回路開発。

1985年～　NEC 半導体部門。
D70交換機用CODEC開発（ DSPアーキテクチャ・回路設計、DSPソフト設計、LSIレイアウト設計等）。
スケジューリングエンジン付ATMスイッチLSI、B-ISDN用CMOS-LSI試作　等。

1990年～　交換機開発部門。商用装置開発に従事。
論理合成、FPGA等、新たな開発環境を商用装置設計に導入。
PSTN、ISDN、ATM新ノード等各種NTT向け基幹装置のアーキテクチャ、ハード設計。ITU-T、TTC等で標準化活動。

2000年～　モトローラ（2011年にNokia Siemens Networksが吸収）入社。
モバイルAll IPトライアル。
WiMAXトライアル。 OFDM、MIMOなどモバイル・無線領域へ。
LTE商用化。5G検討（ミリ波、ビームフォーミング）。

2015年～　サムスン電子ジャパン入社。　ネットワーク部門 技術責任者。

2018年～　ファーウェイジャパン入社。

Huawei会社紹介

Huawei　世界有数のICTインフラ機器とスマート端末メーカー

あらゆる人、家庭、組織にデジタル化の価値を提供し、
すべてがつながったインテリジェントな世界を実現する

19.4万
従業員

9.6万+
研究開発従事者

170+
国と地域

61
世界TOP500

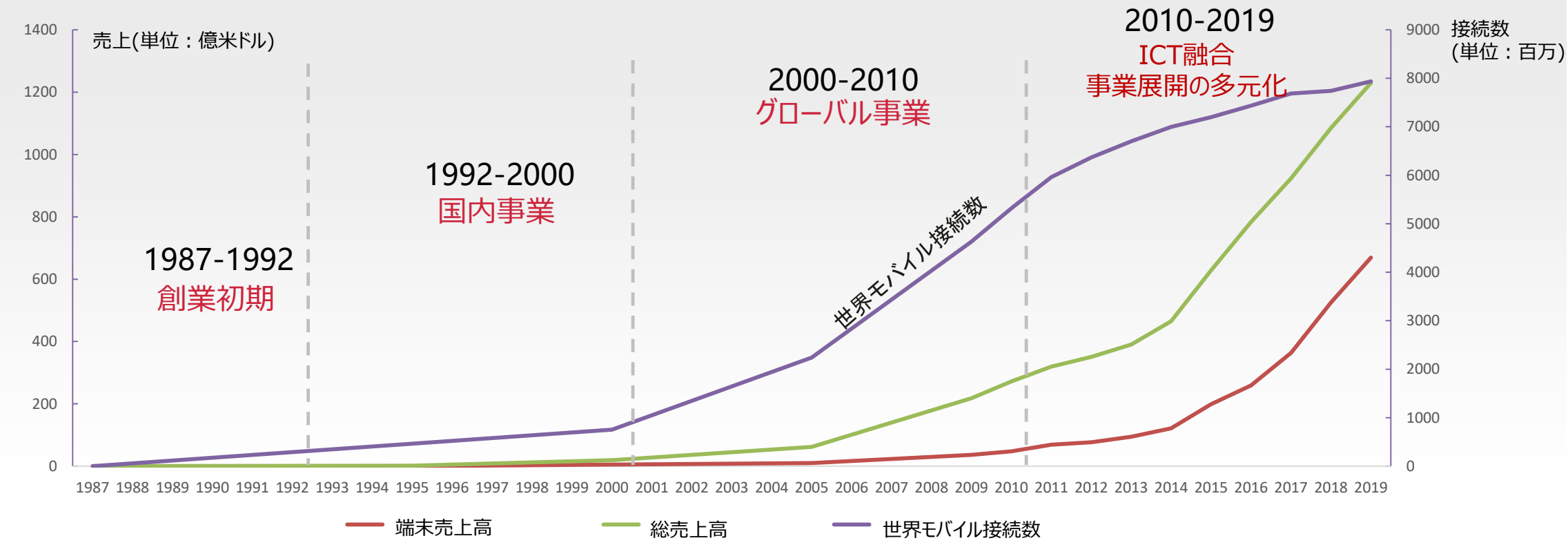
3つの顧客グループ向けにICTソリューションとサービスを提供

グローバルなリソース配置と経営の現地化

- 170か国以上で事業を展開し 、160以上の国籍からなる19万人以上の多様な価値観を持つ従業員を雇用（現地採用率：70%）
- ファーウェイのグローバル・バリュー・チェーンにより、世界全体でスムーズな能力の移転が可能であり、現地の優れた人材を育成・確保し、雇用創出と経済成長に貢献
- 世界各国でグローカル化を促進、現地経営陣がエンド・ツー・エンドで経営責任を負えるよう、相応の決定権を委譲
- 共存共栄の理念に基づきグローバル産業チェーンを構築し、各国において責任ある企業市民となる

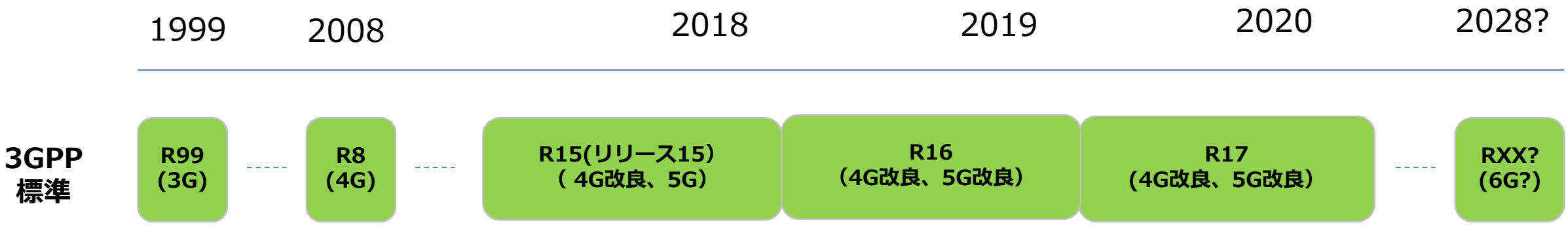
発展の歩み

- 1987に創業者である任正非氏が21,000人民元を集め、深圳にファーウェイを設立。
- 交換機の代理販売からスタートし、製品の研究開発、技術革新に取り組みながら、中国の改革開放政策やICT産業の発展がもたらした機会を捉え、年間売上高1,000億米ドルを超えるグローバル企業に成長。



5Gモバイル通信システムとグローバル市場動向

5Gモバイル技術標準　各国商用導入状況



3GPP　“3rd Generation Partnership Project “

https://www.3gpp.org/

・世界の標準化団体
　ARIB(日), ATIS(米), CCSA(中),ETSI(欧州),
　TSDSI(印), TTA(韓),TTC(日)
による協力プロジェクト。

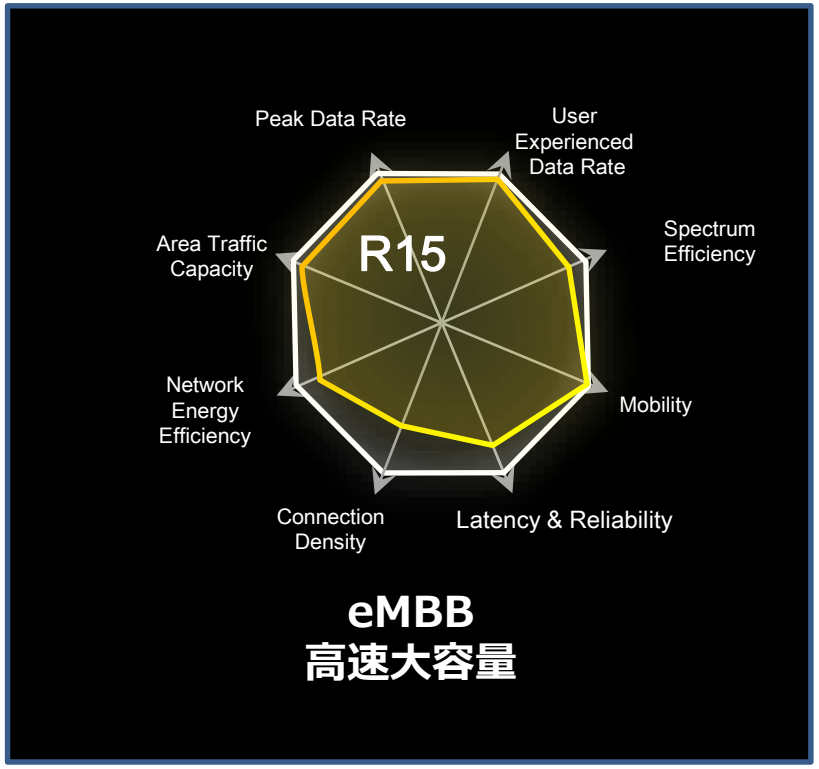
・2Gまでは各国で互換性が無かった携帯電話の技術標準を
3G, 4G, 5Gで継続的にグローバル標準化。

・モバイルネットワークの
　無線アクセス、コアネットワーク、サービス機能
各領域に対して技術標準を策定。

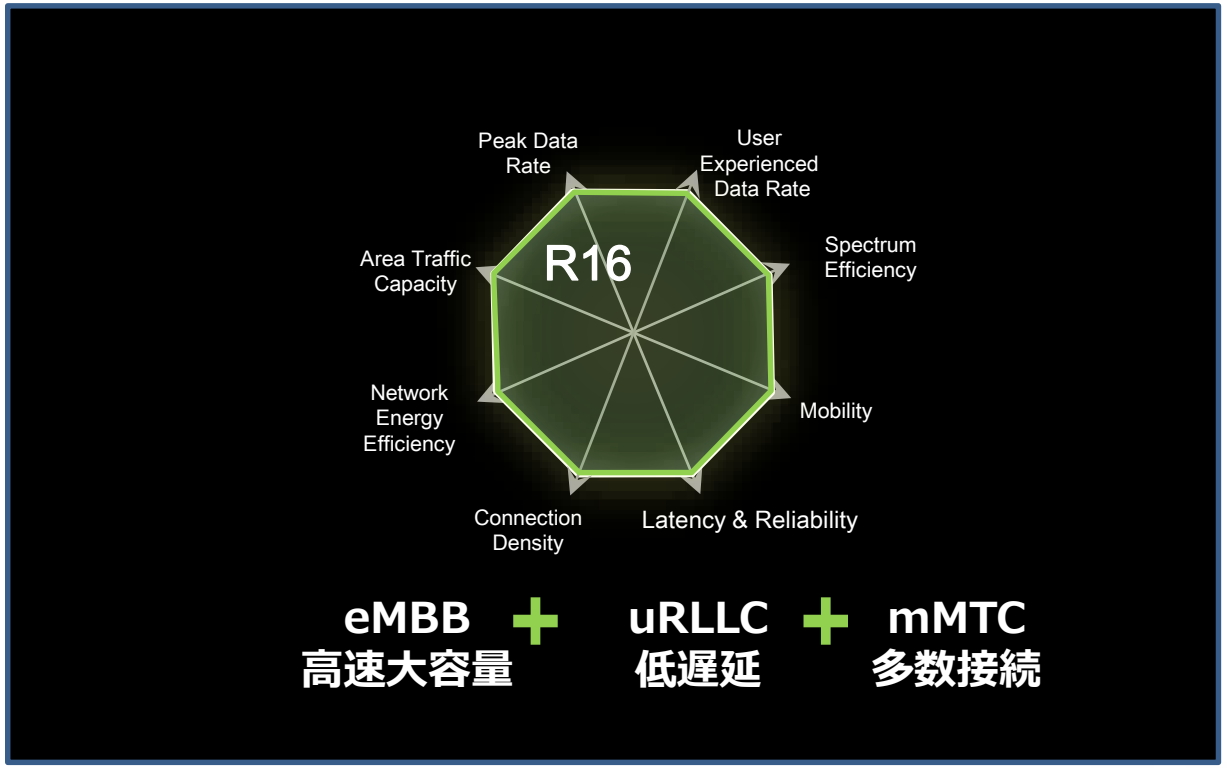
	5G商用サービス開始時期	5G基地局数
	韓国: 3社 2019/4/3	~6万局(19年/9)
	中国: 3社 2019/11/1	~20万局(20年/5)
	日本: 2020/3末	~2500局(20年/7)
	米国: Verizon社 2019/4/3	
	英国: EE社　2019/5/30 スイス: Sunrise社 2019/5/2 …	

3GPP標準　段階的に拡充（R15, R16, R17, …）

R15：
eMBB（高速大容量）フォーカス



R16：
5G全要件（高速大容量・低遅延・多数接続）サポート



モバイル通信の無線技術世代

5Gはこれまでの世代交代ような新規多重技術で定義されていない
従来技術の組合せ、
　　周波数領域の拡大（6GHz以上）：ビームフォーミング
　　空間多重技術（Massive MIMO）の進展
により「高速大容量」を実現

モバイル通信　無線技術世代の進歩

1G	周波数多重(FDMA)	
2G	時間多重(TDMA)	ディジタル化
3G	コード分割多重(CDMA)	コード多重
4G	周波数と時間による多重(OFDMA) 空間多重（SDMA)	 MIMO
5G	周波数領域の拡大（6GHz以上） 空間多重技術の進展（6GHz以下）	ビームフォーミング Massive MIMO

モバイル通信サービスは10年かけて世代交代・成熟

・2001年　3G商用開始
→「映像」が俎上に

2001/10/01
「FOMA、10月１日に本格サービス開始」
「本サービス開始後の展開としては、年内に映像クリッピングサービスが対応端末の発売により開始され、今年度末までに**映像配信サービス**と**音楽配信サービス**、および**映像をその場でメール送信できるサービス**などが提供される予定。」

NTTドコモ・立川敬二社長

<出典https://k-tai.watch.impress.co.jp/cda/article/news_toppage/5883.html >

・2010年　4G商用開始
→「低遅延」「クラウド」が俎上に

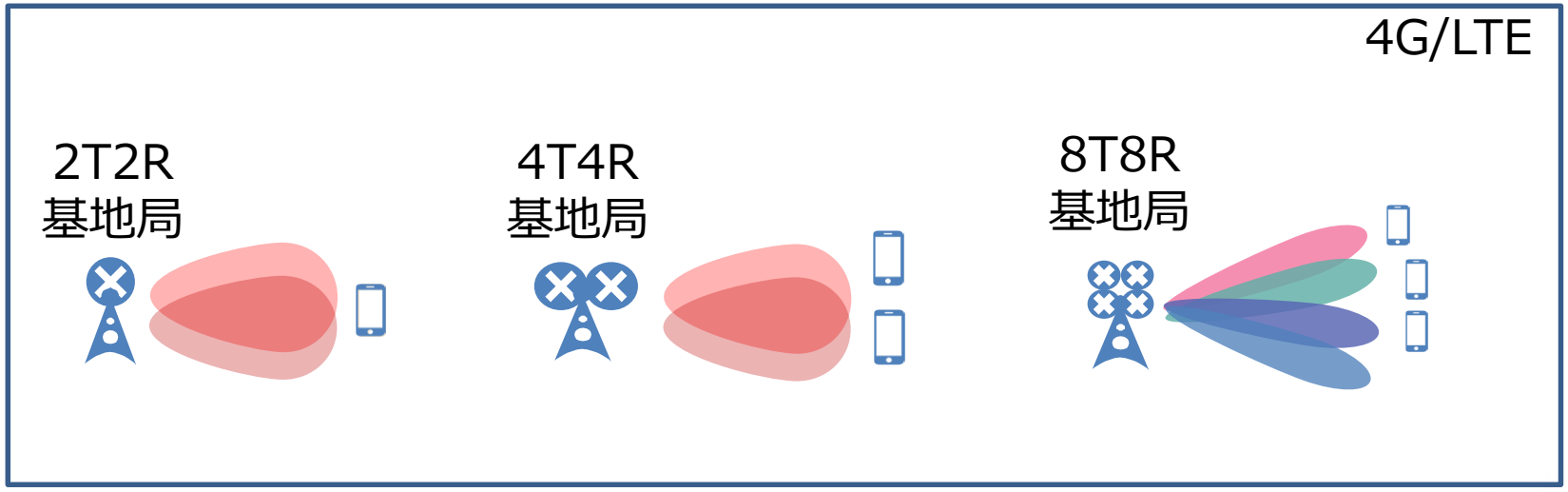
2010/12/20
「ドコモの「Xi」スタート」
「Xiが社会に新しい生活スタイルをもたらし、**豊かな生活の社会基盤**になると確信している”
“Xiでは、高速性もさることながら、**低遅延によりネットワークと端末が緊密に連携する、クラウドサービスの可能性が広がる**」

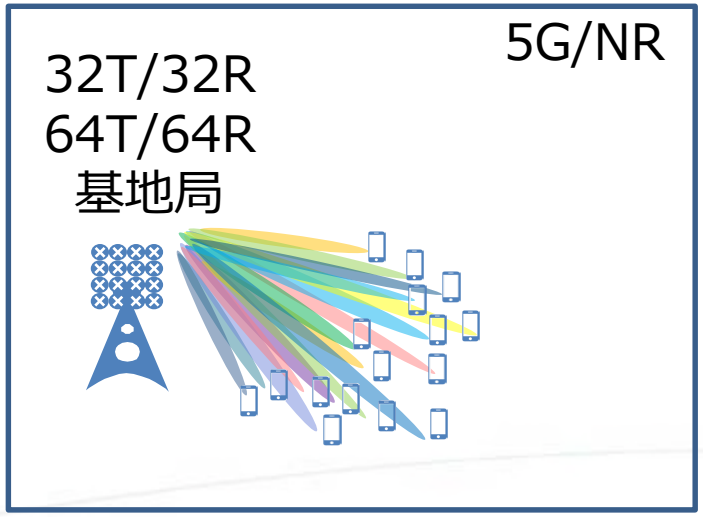
“メリークロッシィ！”のかけ声で「Xi」開始スイッチをオンに。左からITCネットワーク代表取締役社長の寺本一三氏、ドコモ山田社長、森田政務官、富士通山本社長

<出典　https://k-tai.watch.impress.co.jp/docs/news/416928.html >

高速大容量を実現する32T32R、64T64R AAU(Massive MIMO)

5G AAU→Active Antenna Unit
アンプ内蔵アンテナ
LTE基地局に比較してビーム数が飛躍的に増大
基地局通信容量・通信速度も増大
動的な狭いビーム幅の制御により4Gと同等のエリアカバレッジ





韓国LGU+　Huawei 5G基地局を4か月で10,000局展開

省スペース	重量制限	電源制限
ビル屋上 新規支柱一本	支柱一本の許 容荷重	既存電源設備 に5G機器収容 の余裕なし

3.5GHz帯(80MHz幅）Massive MIMO(32T32R)
AAU:アンテナ一体型無線機

既存LTE基地局設置場所に、
支柱一本で5G基地局を追加設置

20Kg 1人で可搬

小型ブレード電源

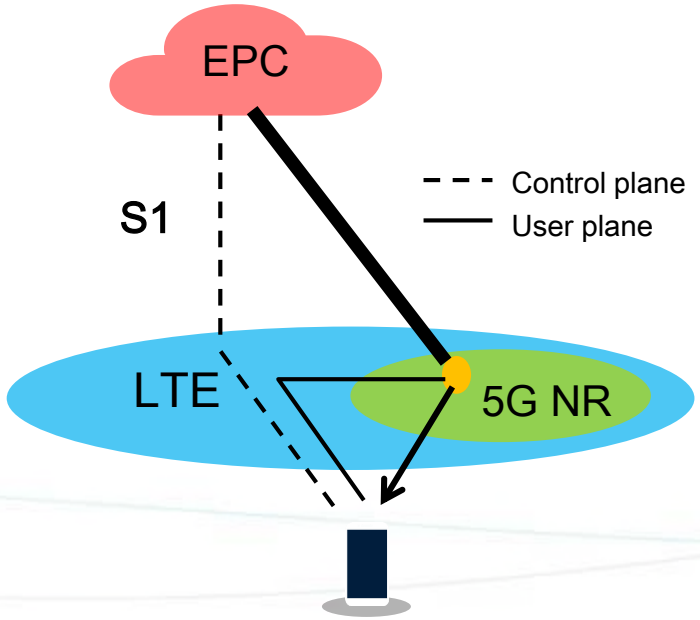
2人・2時間で設置

5Gのネットワーク構成　NSAとSA

現在商用導入が進んでいる5GはNSA
　4Gネットワークに5G無線（NR：New Radio）を付加
　コアネットワークは4G（EPC）

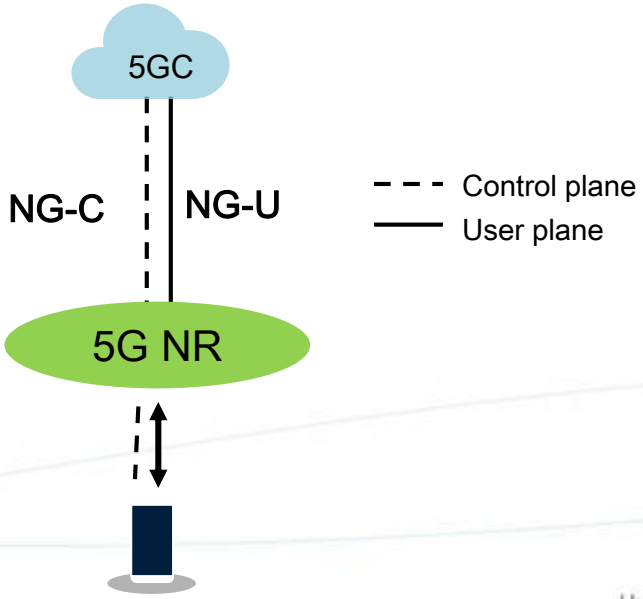
NSA (Non Standalone)

LTEが5G動作を補助
eMBBサービス対応
4Gコア(EPC)



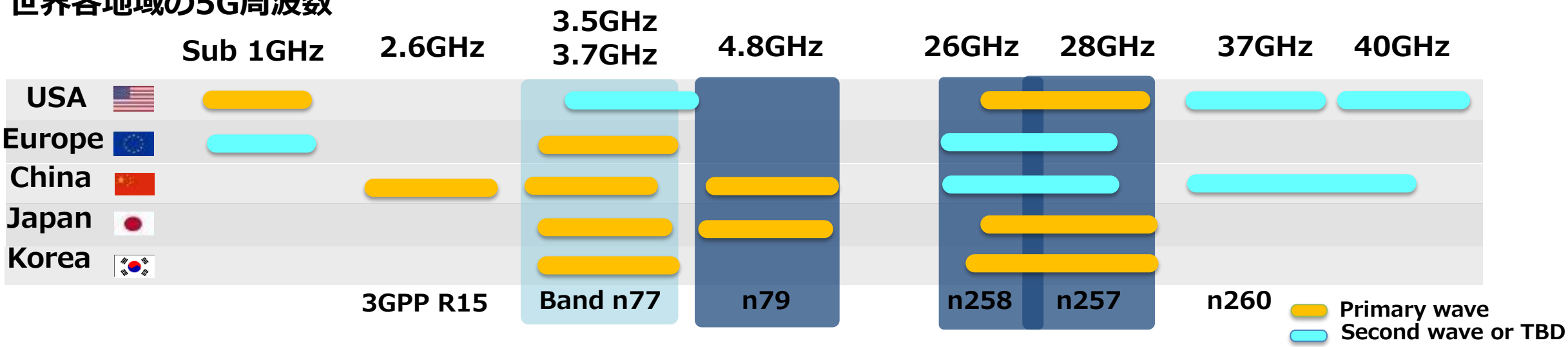
SA (Standalone)

LTE無しでも動作
eMBB/uRLLC/mMTCフルサポート
5Gコア（5GC）



5G周波数　グローバル共通化

世界各地域の5G周波数



Sub 1GHz
広域カバレッジ

- Deep and wide coverage
- Narrow bandwidth (<20MHz 80% operators)
- URLLC / mMTC

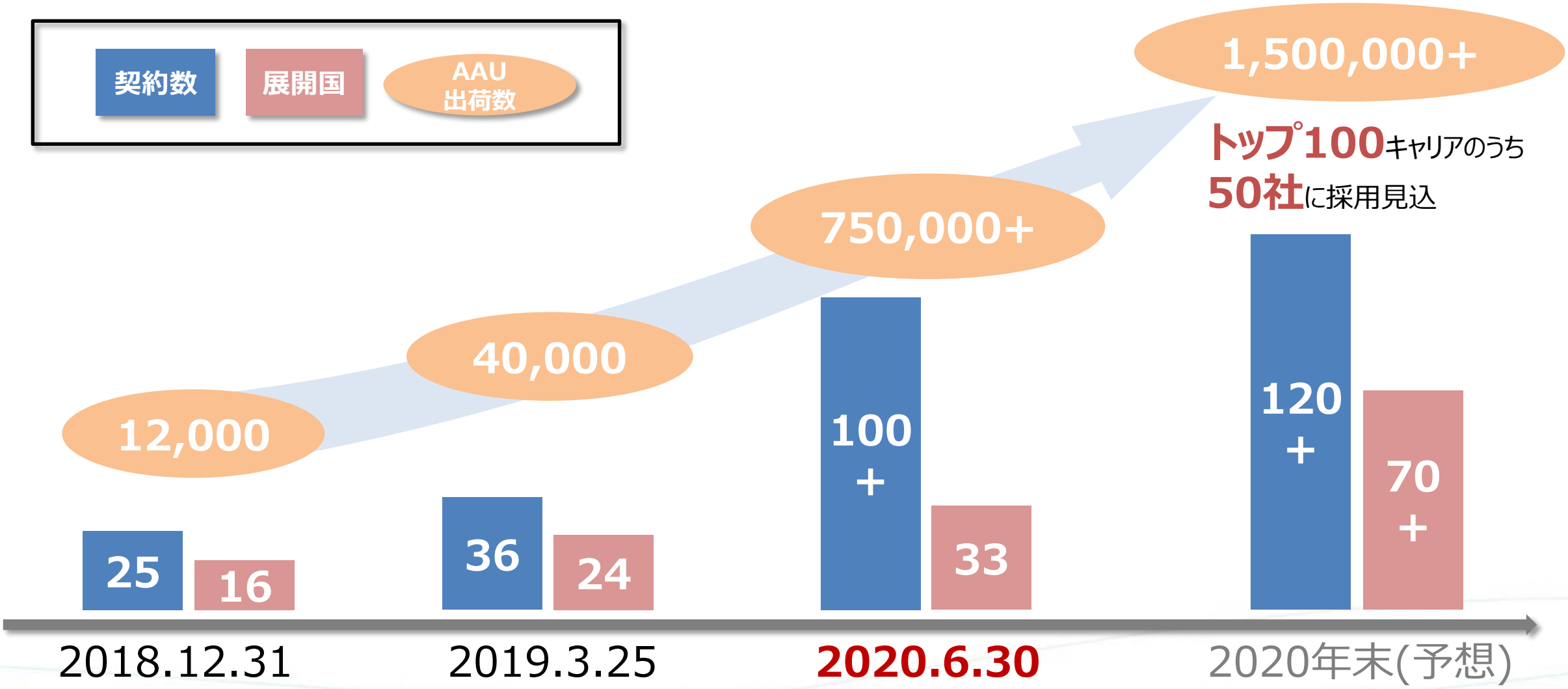
C-BAND（Below 6）
主流

- Global Harmonization
- 100MHz / Operator
- First priority 3.5GHz

mmWave（ミリ波）
容量補完

- Wide bandwidth available, >2GHz per country
- High penetration loss
- FWA (Outdoor CPE) / Hotspot

ファーウェイ　5G基地局　グローバル市場展開状況



韓国ソウル市内　5G基地局

3.5GHz AAU: Active Antenna Unit
4Gアンテナとコロケーション

韓国LGU+　エンタメ系5G付加サービス →高速大容量

韓国では1990年代より放送番組のネット配信が可能
通信事業者もコンテンツで加入者獲得競争

U+골프 5G　5G付加サービス “ゴルフ”

U+프로야구 5G　5G付加サービス “プロ野球”

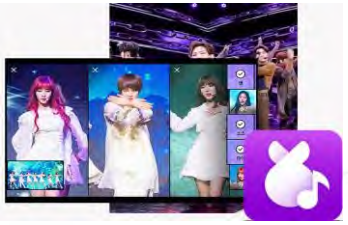
体験イベント（LTEベース）

AR、VRコンテンツ数　約1500（2019/6/27時点）

U+AR 5G
5G付加サービス
“AR”

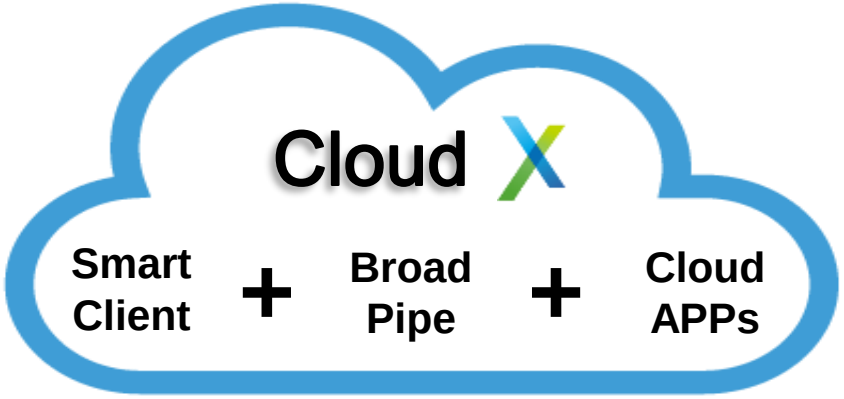
U+VR 5G
5G付加サービス
“VR”

U+아이돌Live 5G
5G付加サービス
“アイドルLive”



<Source>
https://www.uplus.co.kr/ent/fiveg/5GInfo.hpi?mid=12975

5Gによる”Cloud X”の実現→　高速大容量＋低遅延



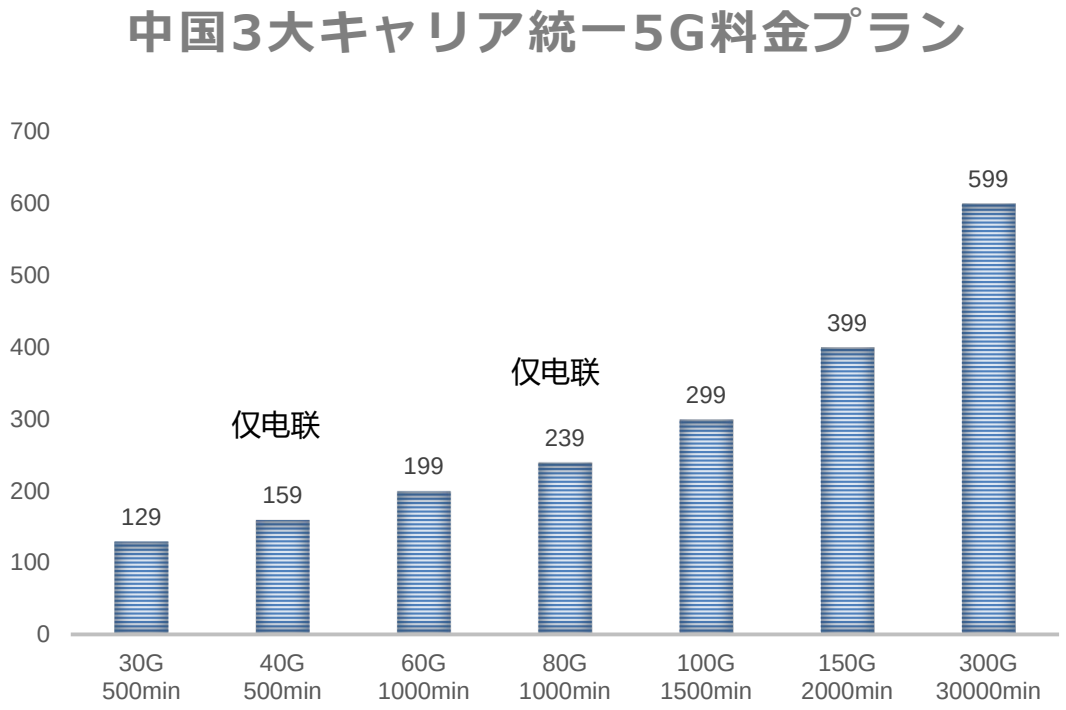
例えば、
X=PC
X=ゲーム
X=VR

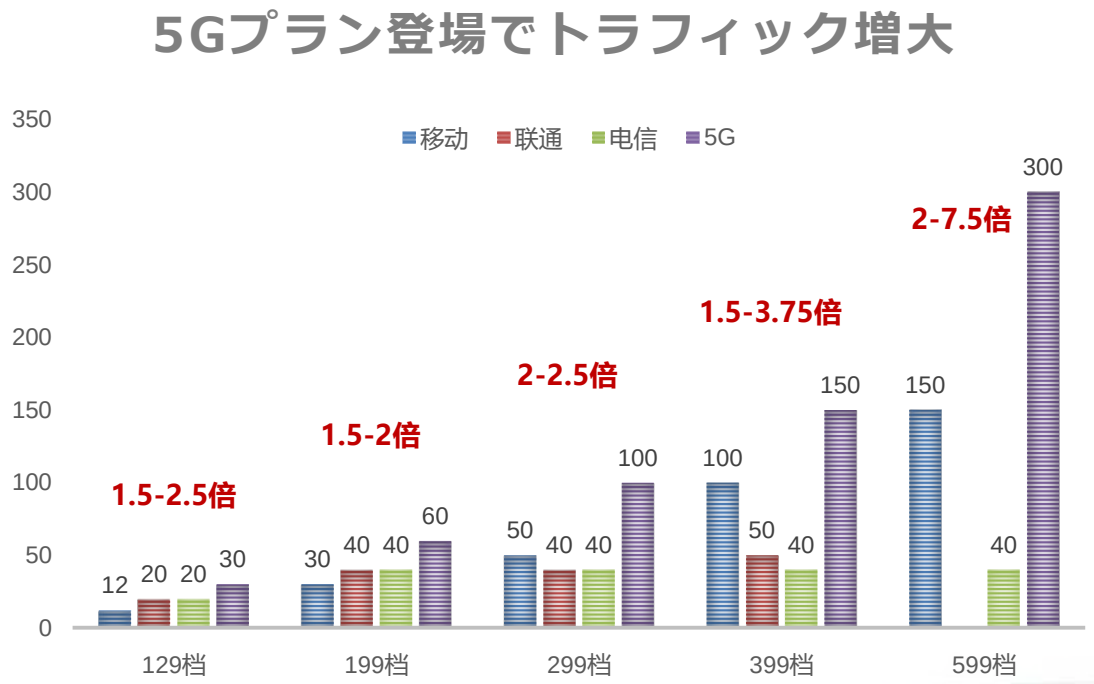
Mobile Edge Computing (MEC)
韓国KTの例　（https://www.zdnet.com/article/kt-completes-mobile-edge-computing-centers-for-5g/‘）

4G：ソウルにデータセンターを集中配置
5G：全国8都市にMECデータセンターを配置し遅延低減

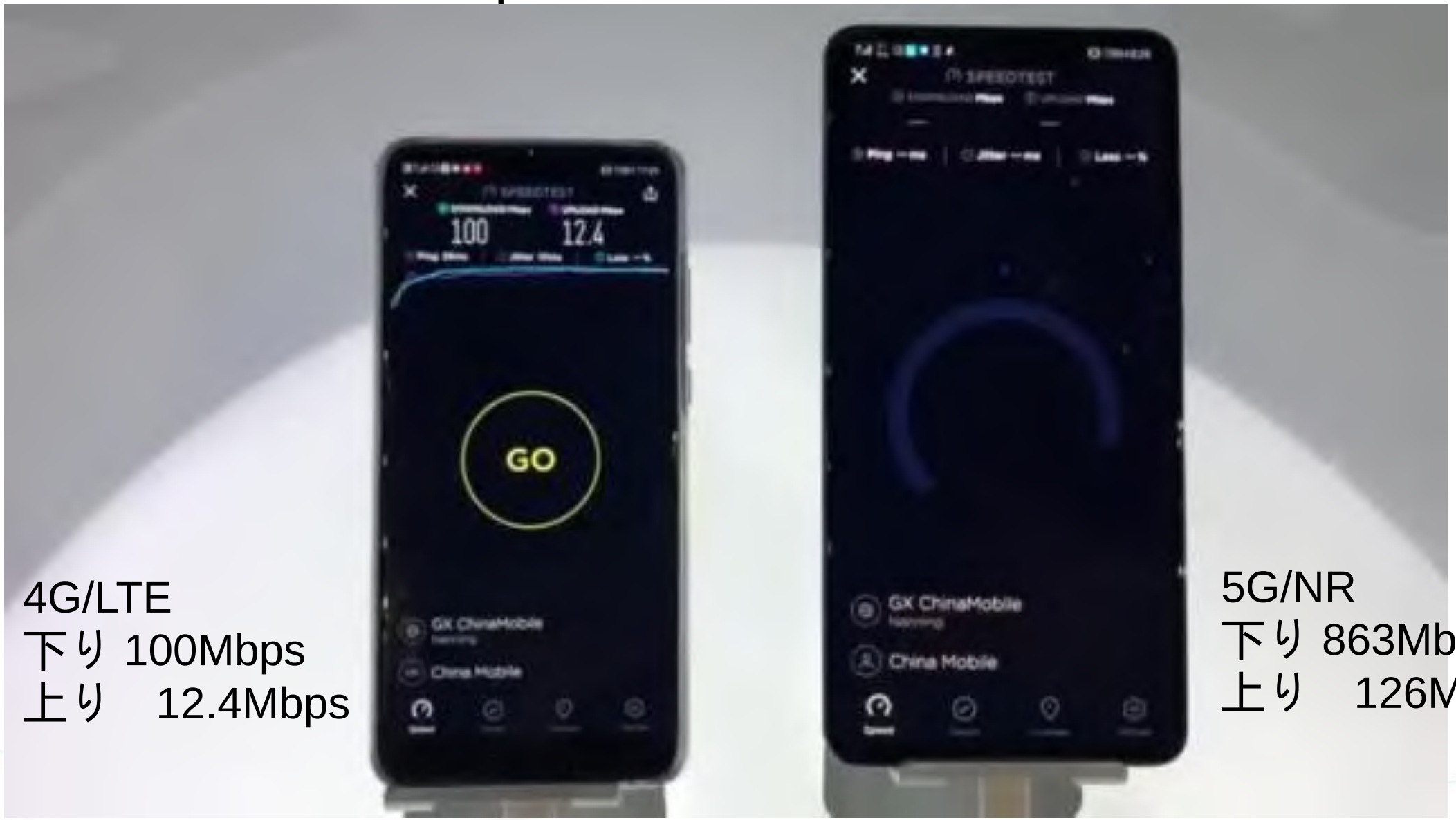
中国通信3社　5G統一料金プラン

月額128元から。5Gプランでトラフィックは4Gプランの1.5倍以上。





中国　深圳市　Speed test 4G（左）5G （右）比較



4G/LTE
下り 100Mbps
上り　12.4Mbps

5G/NR
下り 863Mbps
上り　126Mbps

中国・洛陽　5G遠隔操縦車両が導入された無人鉱山
→高速、低遅延通信

鉱山に専用の
5G基地局を設置し
危険作業（車両運転）
を無人化

40台の無人車両
そのうち30台は
無人搬送車
→走行速度
15Km/hから30km/h
に高速化

生産効率
30%向上

モバイル通信システムのセキュリティと技術標準

“セキュリティ“の定義

Cyber Security　（サイバーセキュリティ）
Information Security　（情報セキュリティ）

➡ 本資料のスコープ

情報セキュリティの3要素　<出展> 日本ネットワークセキュリティ協会　https://www.jnsa.org/ikusei/01/02-01.html

Confidentiality（機密性）
▶情報資産を正当な権利を持った人だけが使用できる状態にしておくこと
情報漏洩防止、アクセス権の設定、暗号の利用などの対策

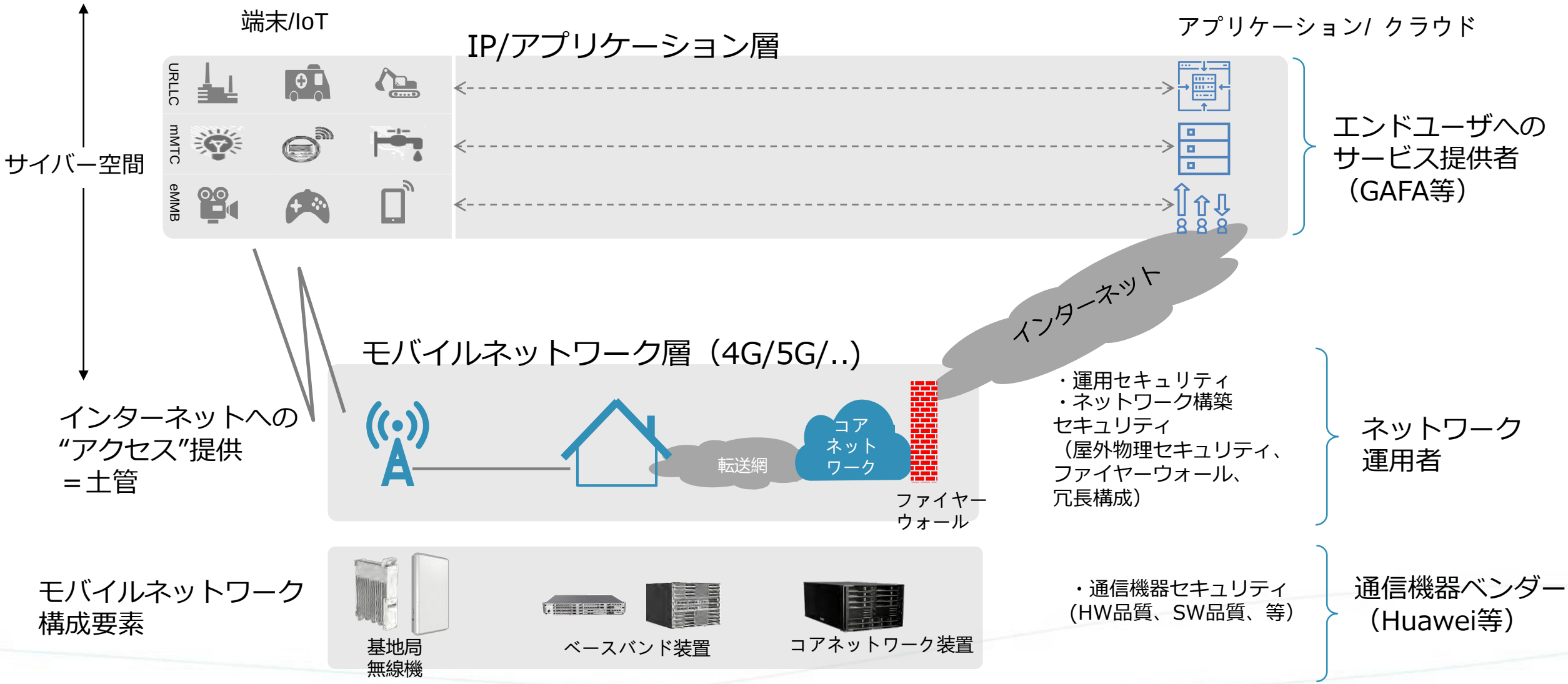
Integrity（完全性）
▶情報資産が正当な権利を持たない人により変更されていないこと
改ざん防止、検出などの対策

Availability（可用性）
▶情報資産を必要なときに使用できること
電源対策、システムの二重化、バックアップ、災害復旧計画などの対策

National Security （国家安全保障）　　鉄鋼貿易、アルミ貿易、自動車貿易、材料貿易、、
Job Security　（雇用保障）
等

➡ 本資料のスコープ外

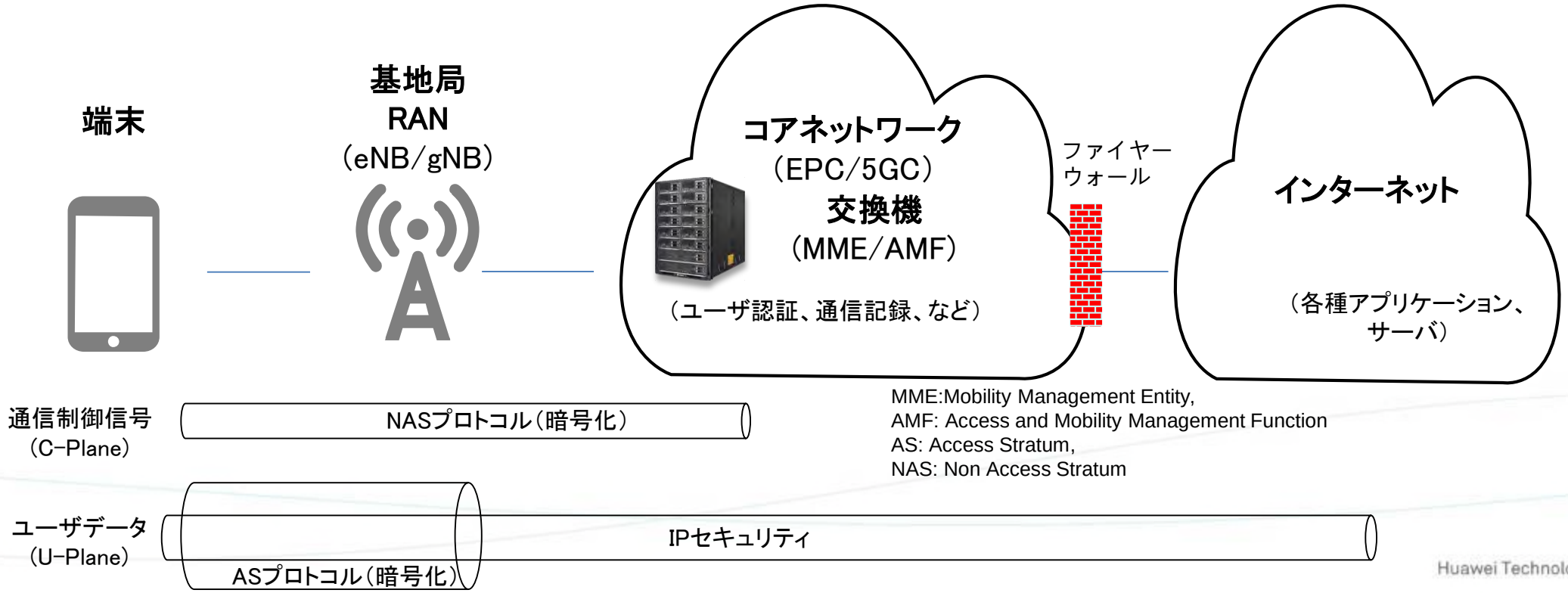
4G/5Gモバイルシステム　セキュリティ・階層構造



モバイルネットワークにおける無線・基地局のセキュリティ（機密性）
（後続2ページでより平易に解説）

＃１）無線、屋外設置機器（基地局）を含めた通信区間を暗号化による保護（機密性）
　暗号鍵は通信事業者により管理
→SIMカード内の共通鍵情報を元に、通信に用いる鍵を動的に生成（通信用共通鍵の再利用無し）

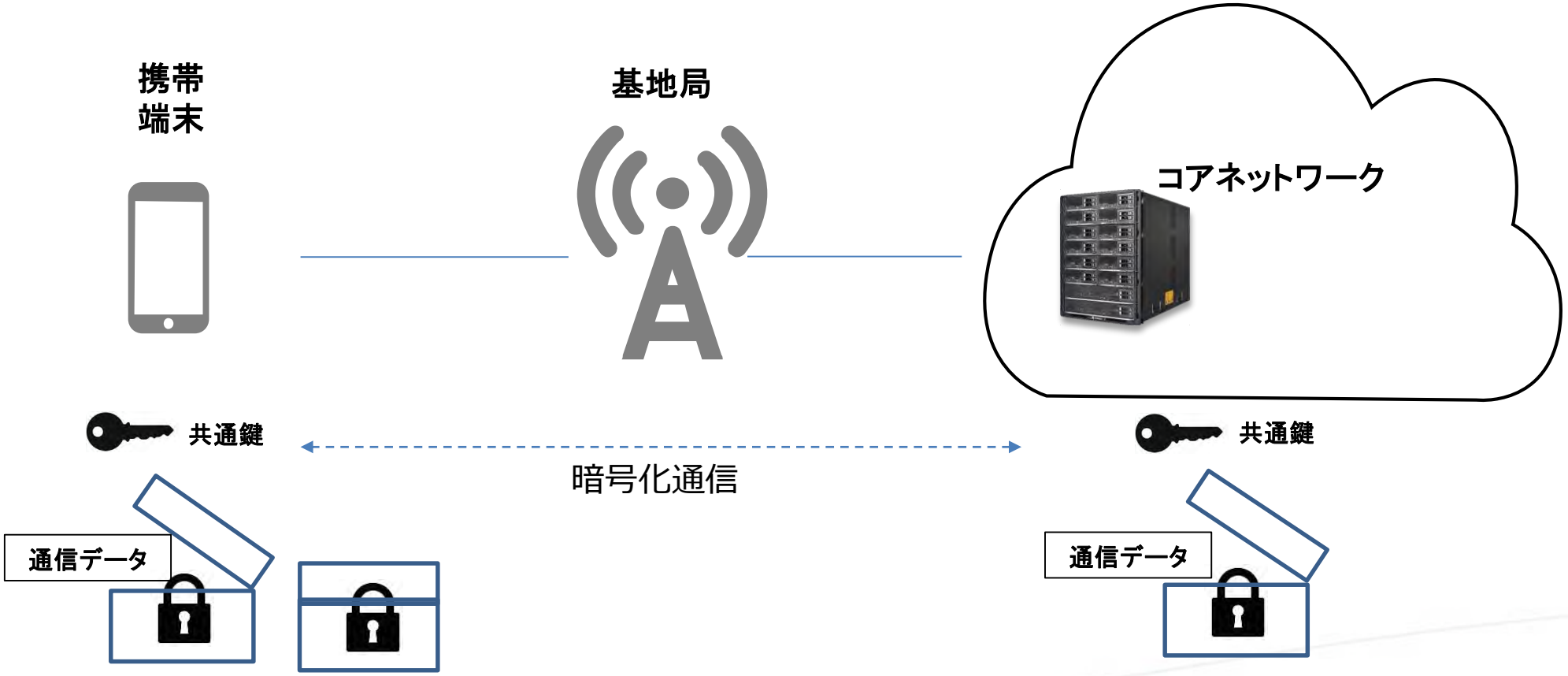
＃２）4G/5Gモバイルネットワークはインターネットから見ると「土管」
→トンネリングにより基地局にはインターネット・アクセスのIPアドレスがアサインされない



MME:Mobility Management Entity,
AMF: Access and Mobility Management Function
AS: Access Stratum,
NAS: Non Access Stratum

無線、屋外設置機器（基地局）通信データ暗号化

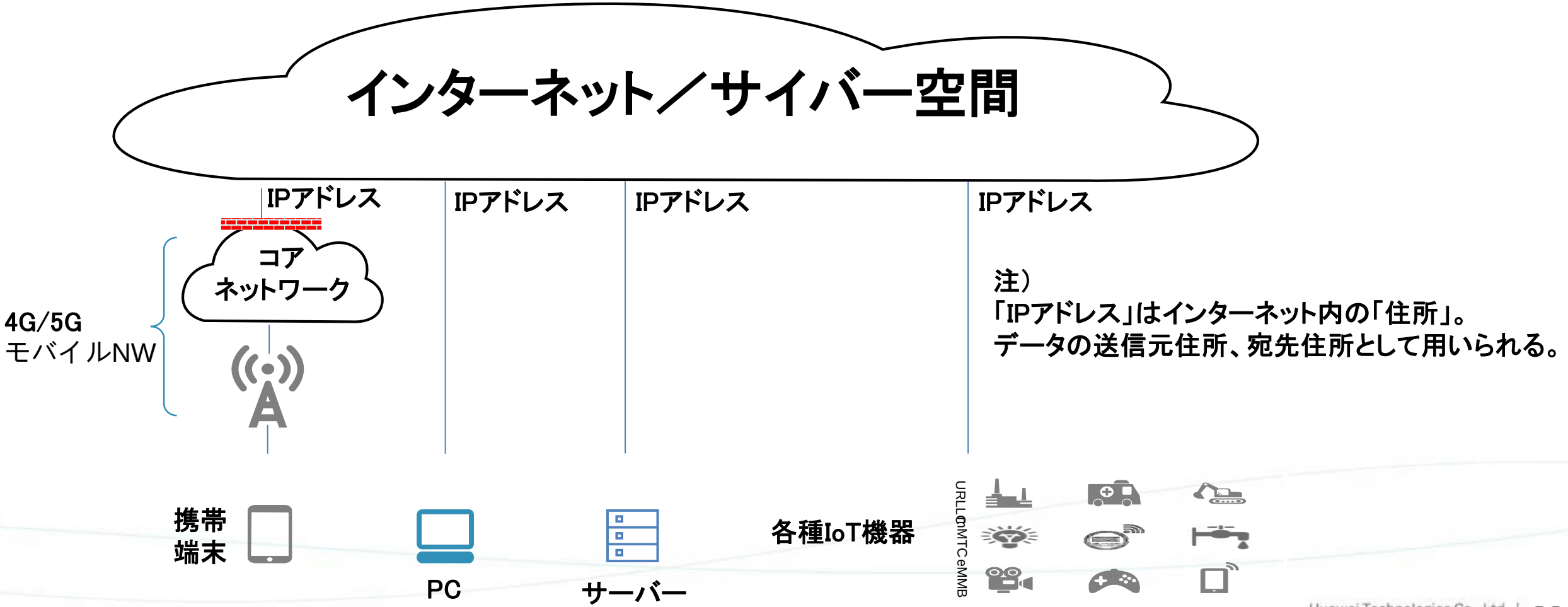
無線、屋外設置機器（基地局）を含めた通信区間を暗号化
暗号鍵は通信事業者により管理
→SIMカード内の共通鍵情報を元に、通信に用いる鍵を動的に生成（通信用共通鍵の再利用無し）



参考)「いちばんやさしい5Gの教本」　藤岡雅宣著　インプレス社
「5G 次世代移動通信規格の可能性」　森川博之著　岩波新書

＃２）インターネットから見たモバイルネットワーク＝「土管」

4G/5Gモバイルネットワークは、インターネットからは携帯端末を繋ぐ線と同等に見える
　インターネット上では、基地局を「宛先」にも「送信元」にもできない
　インターネットから基地局を操作したり、データを受信することはできない



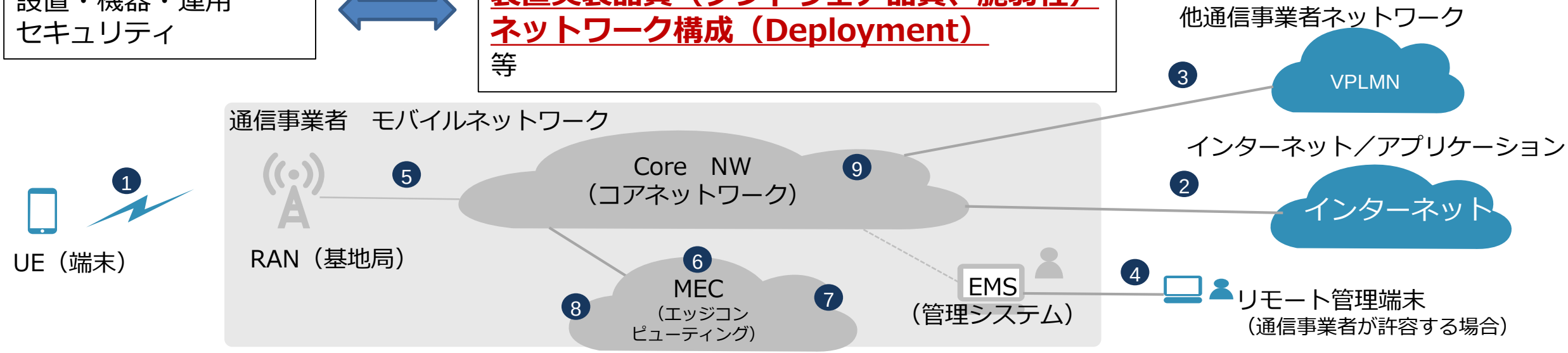
モバイルネットワーク層のセキュリティ・リスクと対策

リスク

設置・機器・運用
セキュリティ

対策

技術標準（3GPP/NESAS/SCAS/etc）
装置実装品質（ソフトウェア品質、脆弱性）
ネットワーク構成（Deployment）
等



モバイルネットワーク外部セキュリティ・リスク例

1 無線区間
- ユーザデータ不正取得
- 盗聴
- アクセス妨害・妨害電波
- 不正端末・違法アクセス
- 偽基地局

2 インターネット
- ユーザデータ不正取得
- なりすましアプリ
- なりすましサーバー
- DDOSアタック
- 不正・違法アクセス

3 ローミング

SS7共通線信号網
- ユーザデータ不正取得
- 偽通信事業者
- サービス拒否

4 リモート管理端末
- ユーザ情報流出
- 非適格者による不正操作
- 適格者による悪意操作
- 運用妨害

モバイルネットワーク内部・実装上のセキュリティリスク例

5 装置間インタフェース
- 盗聴
- なりすまし
- 不正アクセス

MEC内部
- ❻不正アプリ
- ❼アプリ間リソース競合
- ❽サードパーティアプリ

9 コア内部
- 仮想化/NFV

3GPP標準　5Gセキュリティ技術仕様

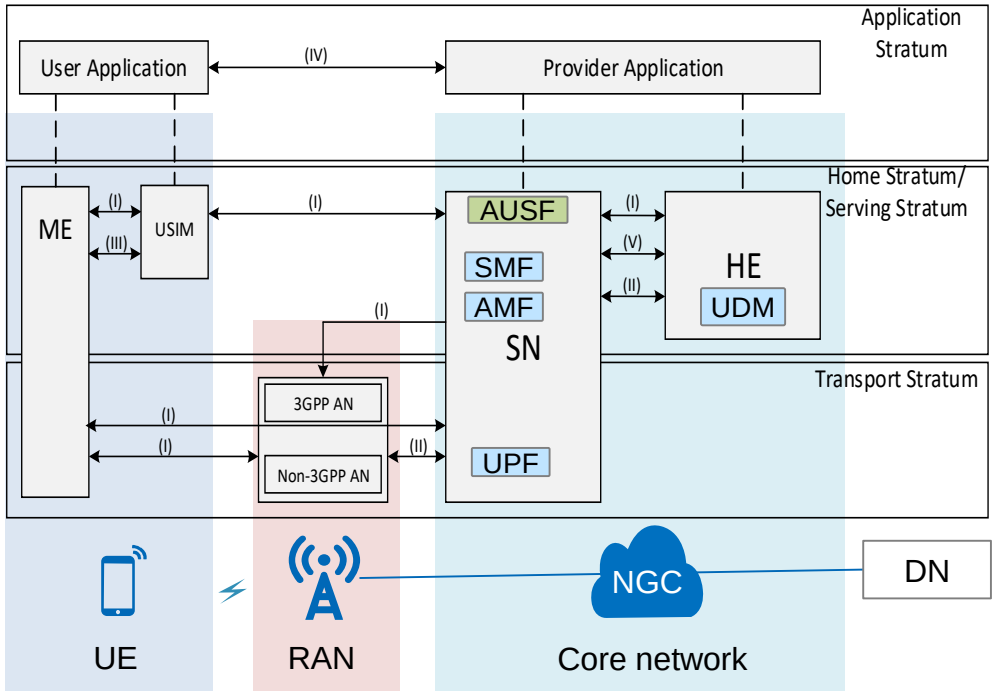
TS33シリーズ
　Security Aspect
TS 33.501
　5Gセキュリティのアーキテクチャ、プロトコル等の規定
TS 33.511 – 33.519
　5Gネットワーク機器のセキュリティ検証仕様　SCAS（Security Assurance Specification）

TS 33.501	Security architecture and procedures for 5G System
TS 33.511	Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class
TS 33.512	5G Security Assurance Specification (SCAS); Access and Mobility management Function (AMF)
TS 33.513	5G Security Assurance Specification (SCAS); User Plane Function (UPF)
TS 33.514	5G Security Assurance Specification (SCAS) for the Unified Data Management (UDM) network product class
TS 33.515	5G Security Assurance Specification (SCAS); Session Management Function (SMF)
TS 33.516	5G Security Assurance Specification (SCAS); Authentication Server Function (AUSF)
TS 33.517	5G Security Assurance Specification (SCAS) for the Security Edge Protection Proxy (SEPP) network product class
TS 33.518	5G Security Assurance Specification (SCAS) for the Network Repository Function (NRF) network product class
TS 33.519	5G Security Assurance Specification (SCAS) for the Network Exposure Function (NEF) network product class

<Source> https://www.3gpp.org/DynaReport/33-series.htm

3GPP標準　5Gセキュリティ・アーキテクチャ（TS 33.501）

3GPP Security Architecture



(I) Network access security, (II) network domain security, (III) user domain security, (IV) application domain security, (V) service domain security

Source: 3GPP TS 33.501

- Core network authenticates users and protects user subscription information
- RAN is unaware of user data and uses PDCP encryption and IPSec to ensure transmission security

3GPP Security Mechanisms

- UE access control
  - ✓ Bidirectional authentication is performed between the UE and the network to prevent fake base stations
  - ✓ The UE falls back from a high-RAT network to a low-RAT network
- Confidentiality and integrity of air interface
  - ✓ The encryption algorithm uses up to 256bit keys
  - ✓ IMSI encryption is added to protect user privacy
  - ✓ Integrity protection is added to the user plane
  - ✓ Flexible security protection policies are added
- Transmission security between 3GPP NEs
  - ✓ IPSec is used between 3GPP NEs to ensure information security
  - ✓ Use SEEP between HPLMN and VPLMN
  - ✓ HTTPS is used between 5GC service functions

3GPP標準　モバイルネットワークの鍵階層

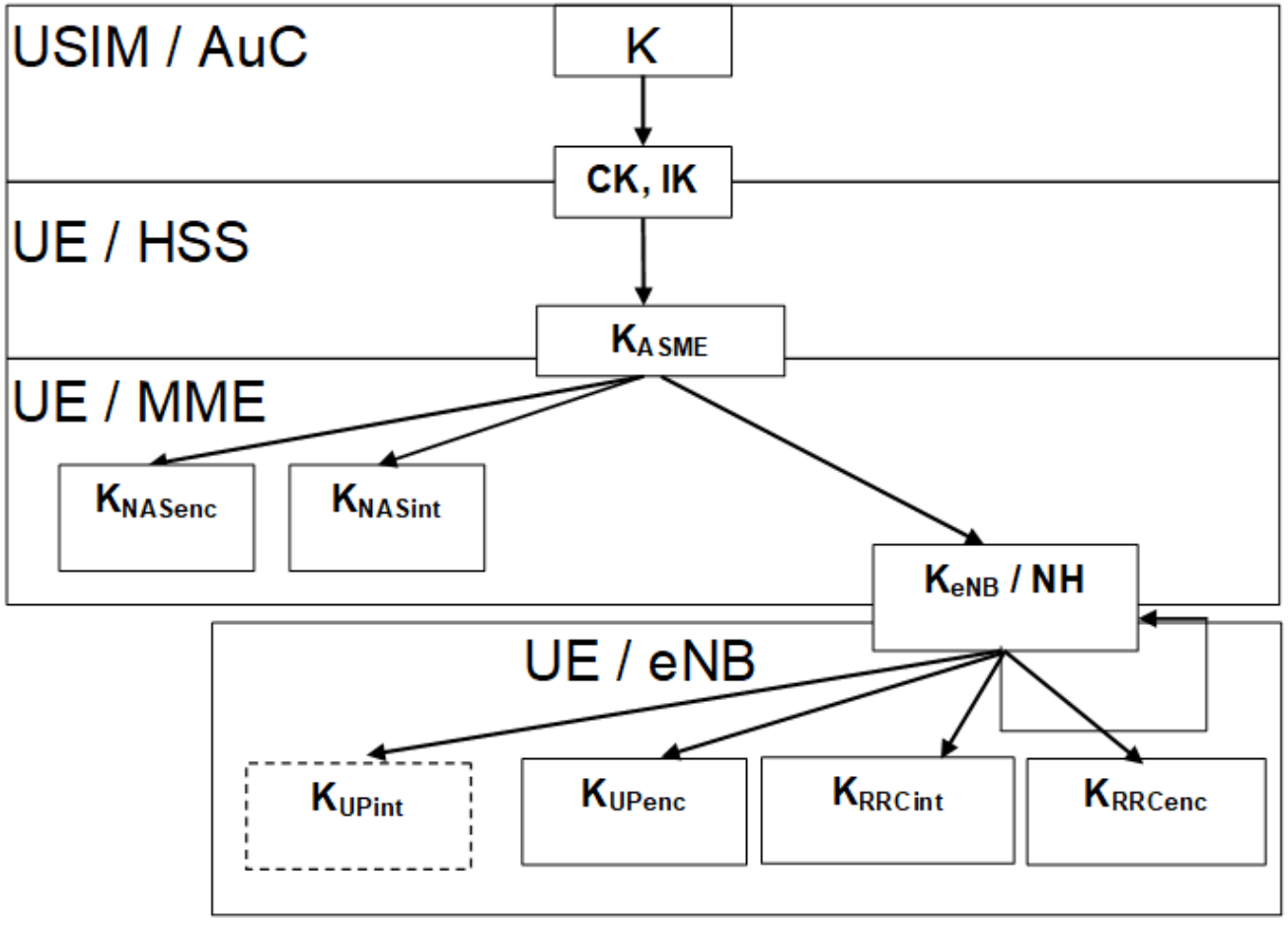


Figure 6.2-1: Key hierarchy in E-UTRAN

<Source> 3GPP TS 33.401

共通の秘密情報（鍵）K をUSIM（SIMカード）とAuC（コアネットワーク内データベース）で保持

ネットワークとユーザの相互認証の度に暗号化鍵CKと完全性保証鍵IKを生成

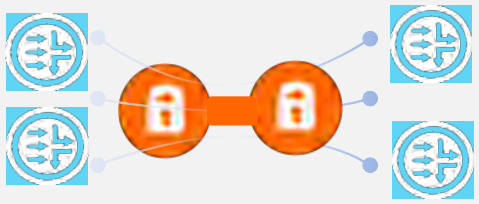
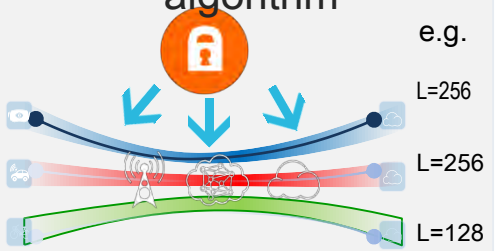
在圏ネットワークで使用するK_{ASME}を生成

NAS（制御信号）に使われる鍵を生成

ネットワーク接続時に鍵を生成

Uプレーン、無線制御用の鍵を生成

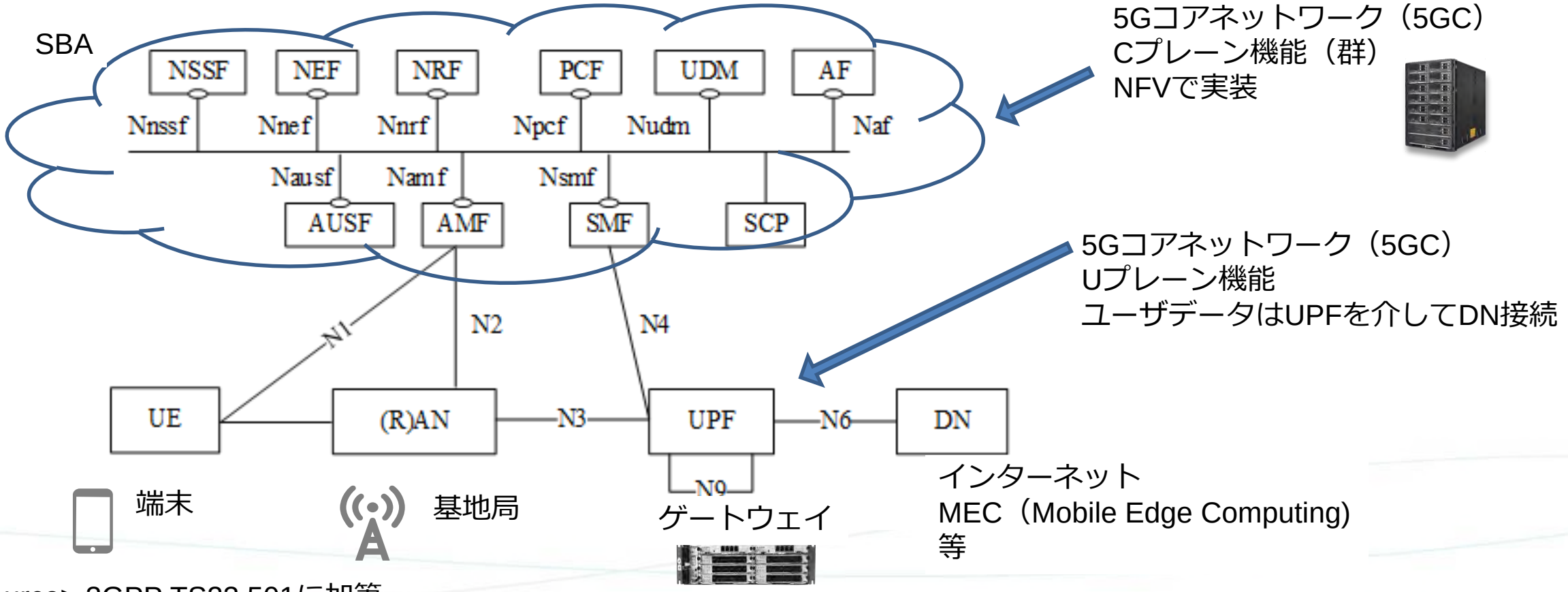
3GPP標準　4G→5G　セキュリティ機能強化点

4G	User Plane Encryption only	Hop-by-bop Protection Between PLMNs	Pseudonymization of users' permanent IDs	128-bit cryptographic algorithm
5G	User Plane Integrity Protection  Anti-alter	E2E Protection between PLMNs 	Encryption of users' permanent IDs 	256-bit cryptographic algorithm 
	Stronger Air Interface Security	**Enhanced** Interconnection security	**Better** user privacy protection	**Enhanced** cryptographic algorithm (256 bit algorithm evaluation in 3GPP)

3GPP標準 5Gコアネットワーク（5GC）

C/U分離：コアネットワーク機能をCプレーンとUプレーンで分離

CプレーンはHTTPベースのプロトコルで統一（Service Based Architecture：SBA）
→“仮想化” NFV（Network Function Virtualization）による実装を想定



<Source> 3GPP TS23.501に加筆

（参考）NFV=通信装置ソフトウェア化の歴史

NFV：Network Function Virtualization
　　“ネットワーク機能の仮想化”

１．通信装置向けに専用プロセッサを開発
通信装置は昔からソフトウェアで制御されている（ D70交換機等々）
専用のプロセッサ、プラットフォームを開発（他に手段が無かった）

２．汎用CPUチップの活用
PCの普及により低コストのCPUチップ(68020等）が市場に登場し、通信装置でも部品レベルで活用へ

３．汎用ITプラットフォームの活用
ITの進展に伴い、ITプラットフォーム（汎用サーバー）を制御装置にそのまま活用
Uプレーン（後述）処理には、組み込みソフトウェア（ファームウェア）用として部品レベルで継続活用

４．NFVの登場
さらなるITの進化により、ネットワーク機能（4Gコアネットワーク（EPC））も汎用サーバーで実現へ
主な動機は専用ハード開発・維持負担の軽減
5Gでは、NFVを前提としたコアネットワーク機能の標準化

NESAS (Network Equipment Security Assurance Scheme)

3GPP（標準化団体）とGSMA（通信事業者業界団体）で定義
3GPPのSCAS（Security Assurance Specification)に基づくネットワーク機器のセキュリティ認証

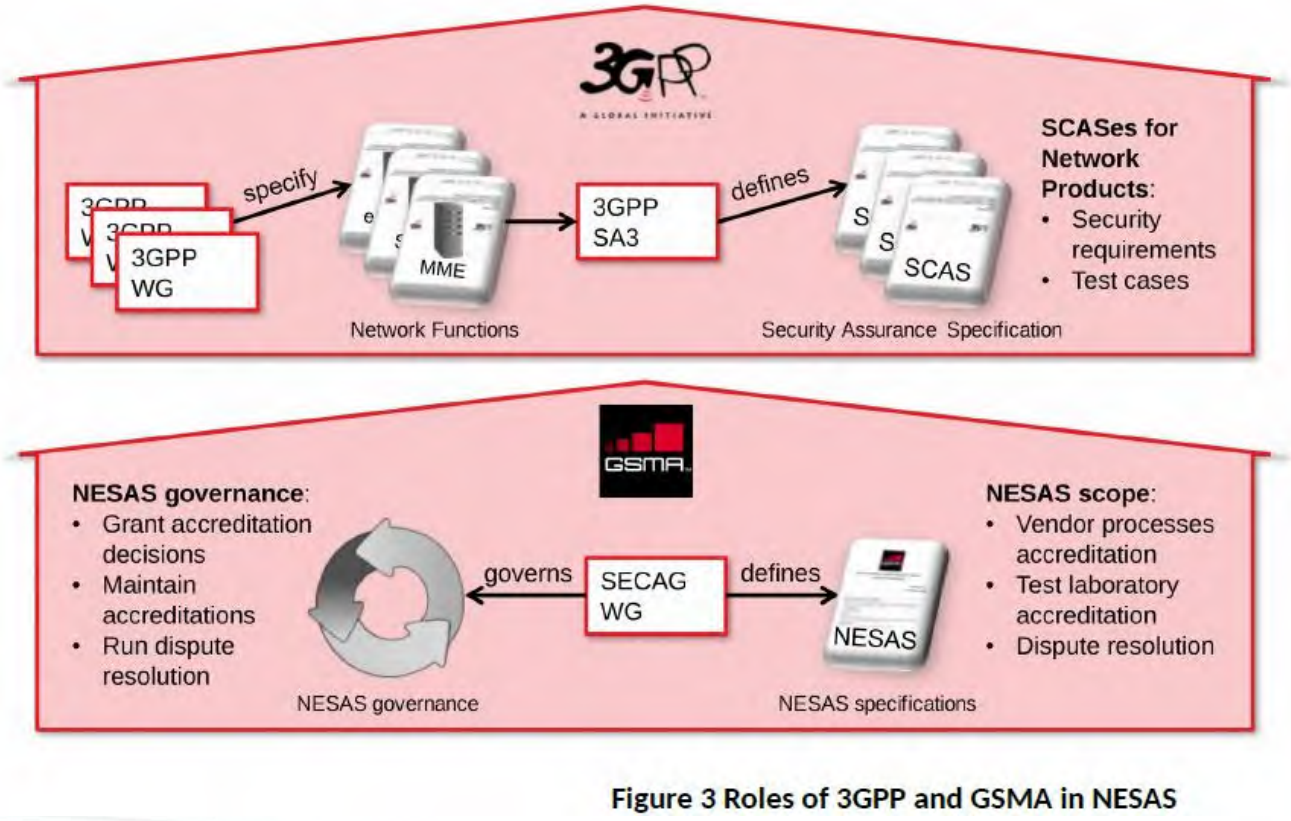


Figure 3 Roles of 3GPP and GSMA in NESAS

3GPP標準
SCAS（Security Assurance Specification）
TS33.xxx

GSMA標準

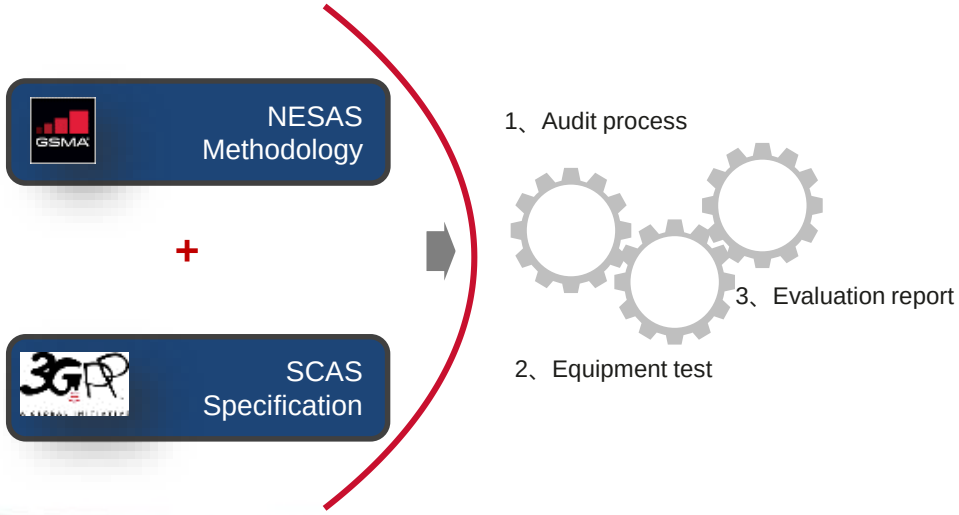
Network Equipment Security Assurance Scheme
FS.13 Overview FS.13
FS.14 Security Test Laboratory Accreditation FS.14
FS.15 Vendor Development and Product Lifecycle Requirements and Accreditation Process FS.15
FS.16 Dispute Resolution Process FS.16
FS 17 Consolidated Security Requirements FS.17

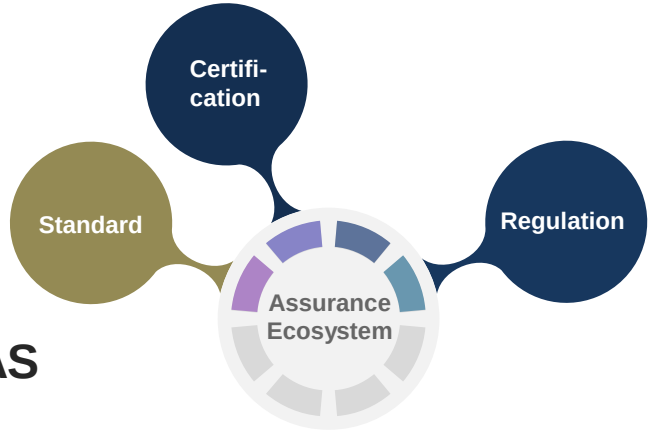
<Source> https://www.gsma.com/aboutus/wp-content/uploads/2017/03/FS.13-NESAS-Overview-Pilot-Release_0.3.pdf

NESAS Is Defined to Address Fragmentation of Regulations and Security Demands

NESAS Introduction

- ✓ In 2012, Ericsson took the lead in promoting the establishment of a telecom equipment security evaluation mechanism based on 3GPP.
- ✓ In 2014, 3GPP selected GSMA to develop process evaluation criteria, compared to Common Criteria (CC) in IT area.
- ✓ In October 2019, GSMA/3GPP released the 5G NESAS/SCAS standard.





Benefits of NESAS

- ✓ **Fragment avoidance:** Unified security evaluation standards are used to avoid the potential for fragmentation and for extra overhead introduced by different national regulations and different security demands from MNOs.
- ✓ **Technology-based:** Provide technical baselines for regulators based on authoritative processes and product evaluation specifications in industry.
- ✓ **Continuous evolution:** Continuous evolution based on industry requirements ensures telecom equipment security.
- ✓ **European certification:** Currently, 2 European audit companies and 10+ European labs on the way.

NESASによるネットワーク製品セキュリティ検証の流れ

GSMAの監査チームがベンダーの開発プロセス・製品管理プロセスを認定（Accredits）
認定を受けた試験ラボがベンダーのネットワーク製品をSCASに基づき評価（Evaluate）
評価リポートの通信事業者への提供

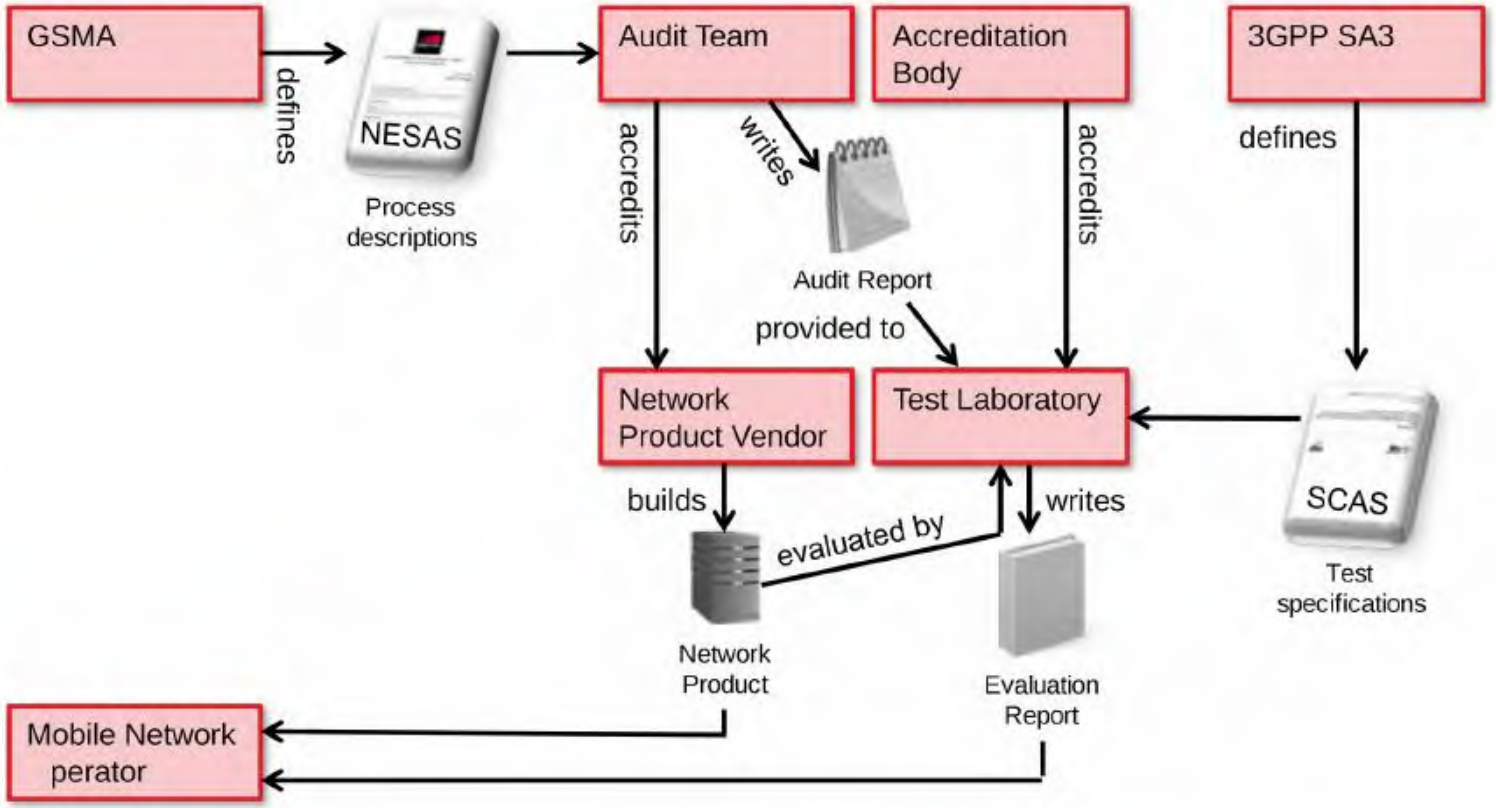


Figure 4 NESAS High Level Overview

<Source> https://www.gsma.com/aboutus/wp-content/uploads/2017/03/FS.13-NESAS-Overview-Pilot-Release_0.3.pdf

NESAS　ベンダー開発プロセス・製品管理プロセス認定

GSMAの監査チームによるベンダーの開発プロセス・開発工程の監査・認定
GSMAの監査チームによるベンダーの製品管理プロセスの監査・認定
（変更管理、構成管理、更新管理、パッチ管理）

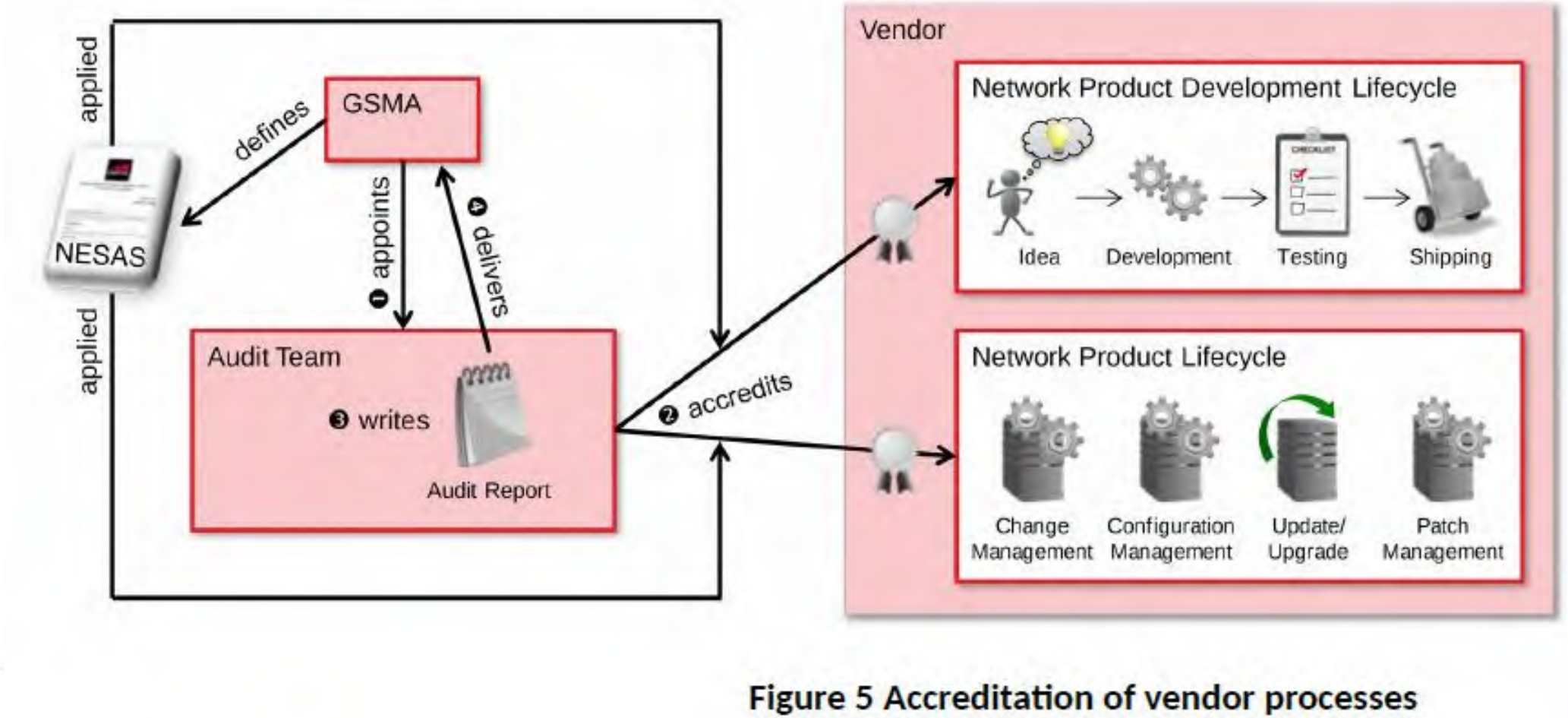


Figure 5 Accreditation of vendor processes

<Source> https://www.gsma.com/aboutus/wp-content/uploads/2017/03/FS.13-NESAS-Overview-Pilot-Release_0.3.pdf

NESAS　試験ラボの認定

ISO17025、NESAS、SCAS（試験仕様）に基づく試験ラボの監査・認定
（試験手順、試験機器、試験能力、専門性、等）

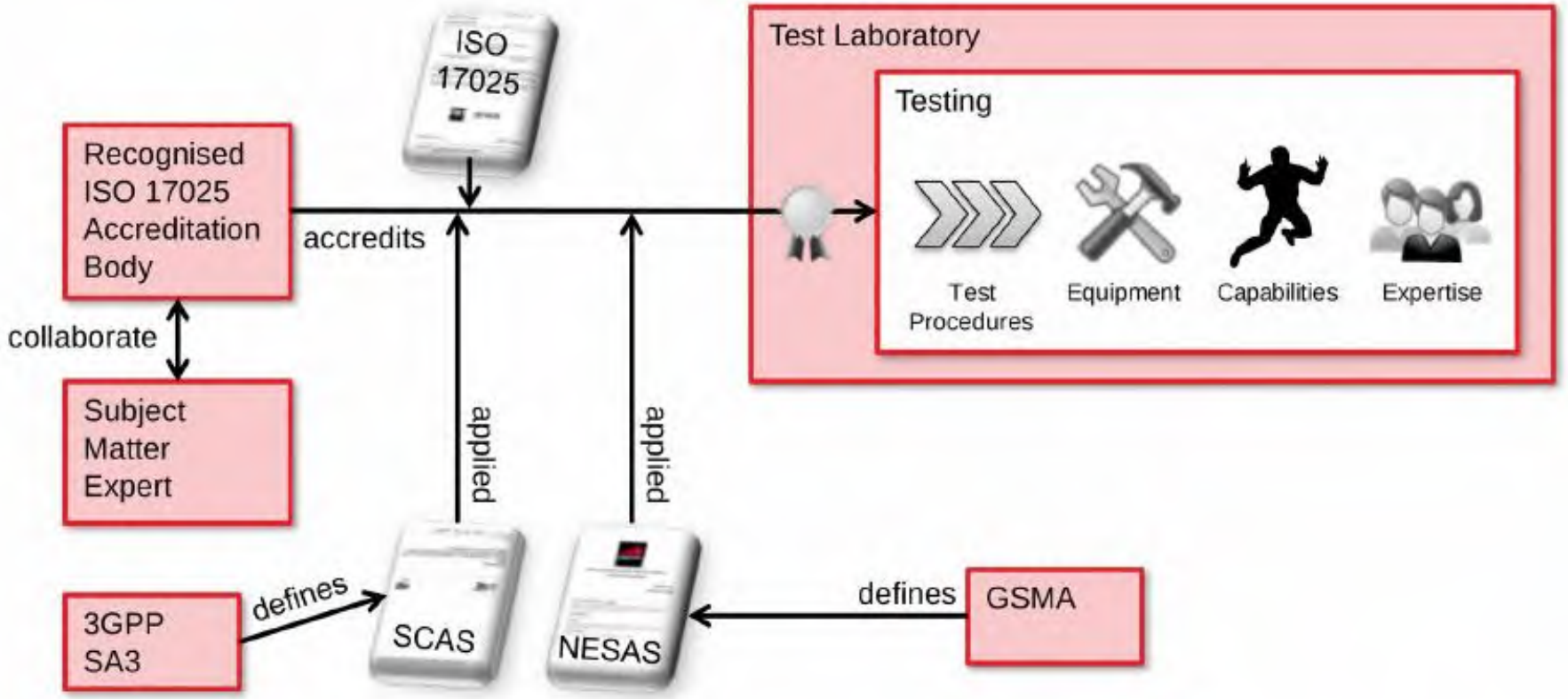


Figure 6 Accreditation of Test Laboratories

<Source> https://www.gsma.com/aboutus/wp-content/uploads/2017/03/FS.13-NESAS-Overview-Pilot-Release_0.3.pdf

NESAS　ネットワーク製品の評価

NESAS、SCAS（試験仕様）に基づく認定試験ラボによるネットワーク製品の試験評価

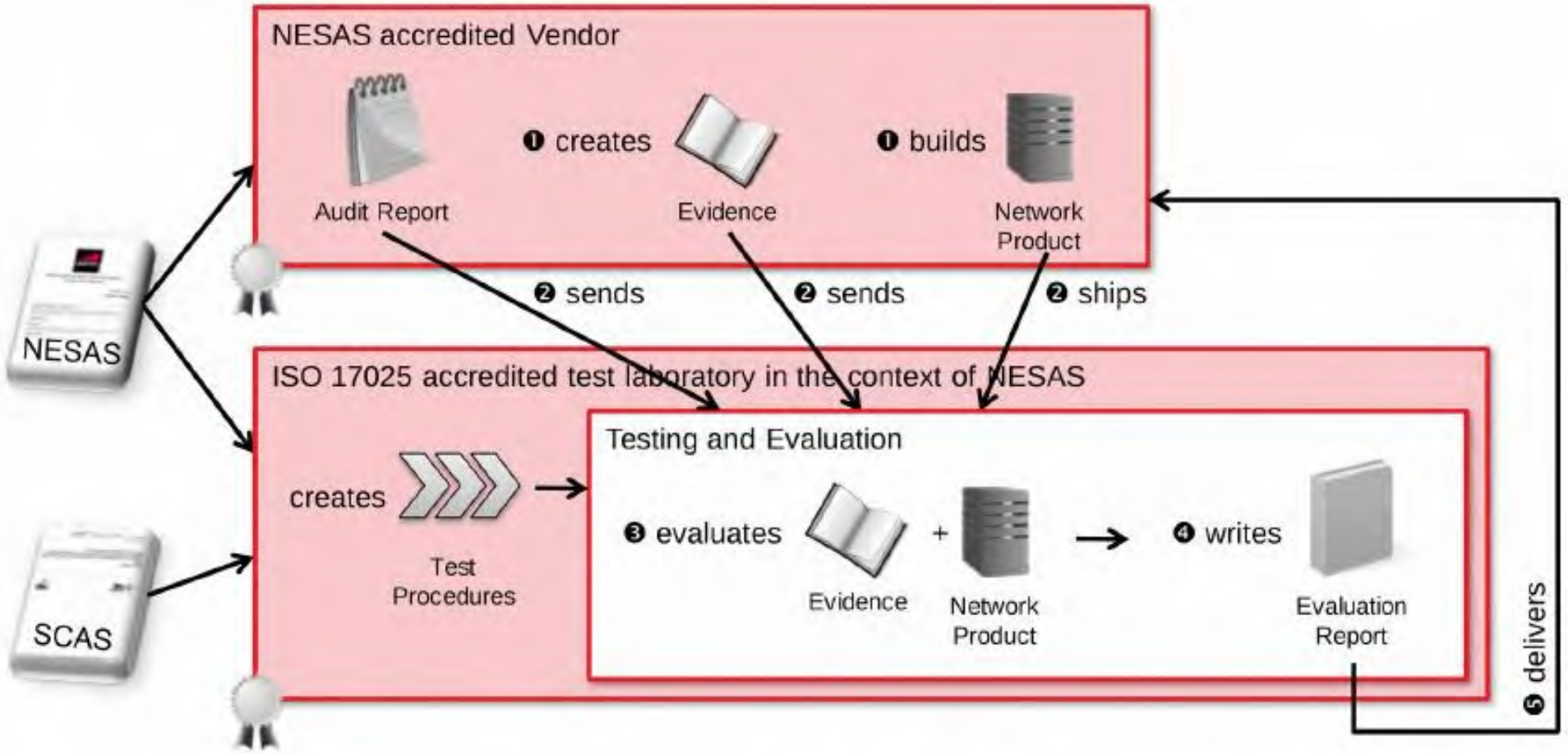


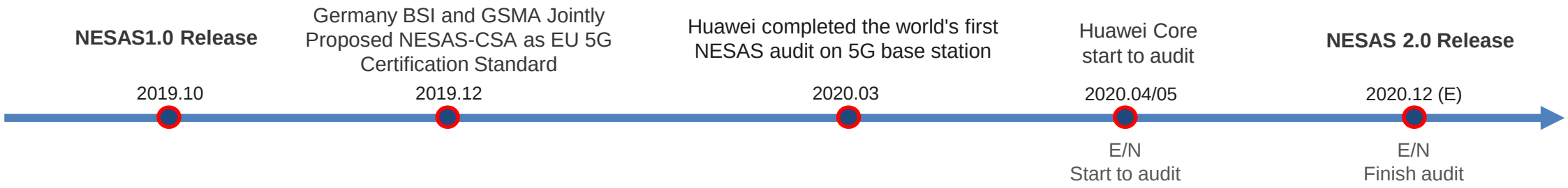
Figure 7 Evaluation of a Network Product

<Source> https://www.gsma.com/aboutus/wp-content/uploads/2017/03/FS.13-NESAS-Overview-Pilot-Release_0.3.pdf

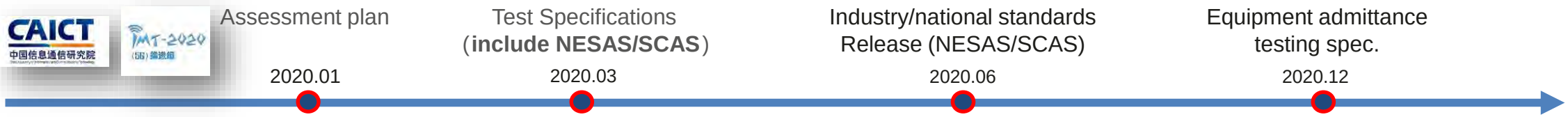
NESAS認証　進捗状況

Global

- In 2019, NESAS 1.0 was released. At the end of 2020, NESAS 2.0 is planned to be released.
- March 2020, Huawei completed the world's first NESAS audit on 5G base station, followed by A and B.



China



CAICT: China Academy of Information and Communication Technology

Huawei complete testing of RAN

Huawei complete testing of Core

CAICT Security Research Institute

Labs in China applying accreditation by GSMA

NESASと欧州5Gセキュリティ Toolbox

Such as **device security** assurance requirements, that NESAS can successfully support.

But NESAS is not designed for deployment, business continuity, non-5G devices, etc. (TM5,6,10,11)

NESAS

Support:

5G devices security and certification

- TM 2: Ensuring and evaluating the implementation of **security measures in existing 5G standards**
- TM 4: Increasing the **security of virtualized** network functions
- TM 7: Reinforcing software **integrity, update and patch management**
- TM 8: Raising the **security standards** in suppliers' processes through robust procurement conditions
- TM 9: Using **EU certification for 5G network components**, customer equipment and/or suppliers' processes
- TM 1: Ensuring the application of baseline security requirements (secure network **design and architecture**)
- TM 3: Ensuring **strict access controls**

For example:

TM09	**Using EU certification for 5G network components, customer equipment and/or suppliers' processes**	The Commission should consider including into the Union Rolling Work Programme[39] relevant EU-wide scheme(s) for critical network components used in the 5G networks and/or for 5G customer equipment (for example, for eSIMs and related cryptographic material) under the EU certification framework. It should also be examined at a later stage whether the certification or supplier's process could also be added to the Union Rolling Work Programme.	R3 R6 R7	▪ Relevant authorities ▪ EC ▪ ENISA ▪ Stakeholders

Not Related:

- O&M security
- Non-5G
- Deployment security
- Resilience and continuity

- TM 5: Ensuring secure 5G network **management, operation and monitoring**
- TM 6: Reinforcing **physical security**
- TM 10: Using EU certification for other **non 5G-specific ICT products** and services (connected devices, cloud services)
- TM 11: Reinforcing **resilience and continuity** plans

NESAS 1.0 vs. CC (EAL4) : Technical Comparison

NESAS Product Development & Lifecycle Audit		CC Product Development & Lifecycle Audit	
1	Security by design	ADV_ARC/FSP/HLD/LLD/ST	√
2	Version control system	ALC_CMC (on-site audit)	√
3	Change tracking	ALC_CMC (on-site audit)	√
4	Source code review	-	×
5	Security testing	ATE_COV/DPT/FUN	√
6	Staff education	-	×
7	Vulnerability remedy process	ALC_FLR (Flaw Remediation)	√
8	Vulnerability remedy independence	-	×
9	Information security management	ALC_DVS (Developer Security)	√
10	Automated build process	ALC_CMC (on-site audit)	√
11	Build environment control	ALC_CMC (on-site audit)	√
12	Vulnerability information management	-	×
13	Software integrity protection	ALC_DEL (Delivery with DS)	√
14	Unique software release identifier	ALC_CMC (CI Identification)	√
15	Security fix communication	-	×
16	Documentation accuracy	ALC_CMC (on-site audit)	√
17	Security point of contact	-	×
18	Source code governance	ALC_CMC (on-site audit)	√
19	Continuous improvement	ALC_CMC (on-site audit)	√
20	Security documentation	AGD_OPE/PRE	√

For Development Audit, NESAS > CC

Test	Contents of equipment evaluation test	SCAS	CC
SCT (security compliance test)	Sensitive info. storage, transfer, protection during access to system, privacy protection (FDP/FCS/FPR)	√	√
	System overflow, secure start-up, robustness of data input, software integrity (FRU/FPT)	√	√
	Authentication (credential/pwassword), token policy, account lock, principle of least authority (FIA)	√	√
	Log out, overtime auto protection (FTA)	√	√
	Security log, logrotate, log access authorization (FAU)	√	√
	Admin account, user account, IP/ICMP Process (FIA)	√	√
	https, web server log, session ID, input examination	√	√
	Message filtering, robustness of protocol, GTP-C/U filtering	√	√
	Security enhancement of baseline requirement	√	×
	OS Security enhancement	√	×
	Webserver Security enhancement	√	×
	Management/User plane separation (FDP/FPT)	√	√
	FCS (cryptographic algorithm implementation check, random number generator, etc.)	×	√
BVT (basic vulnerability test)	Port scan	√	√
	Known vulnerability scan	√	√
	Robust test for interface protocol	√	√
EVA (enhanced vulnerability analysis)	Penetration test	×	√
	Source code scan	×	√

For evaluation test method, NESAS < CC
however, CC not focused on 5G

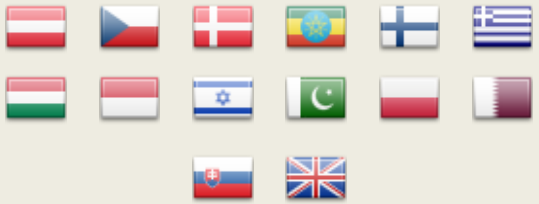
Common Criteria(CC) gNodeB EAL4+ Certificate

CCRA(Common Criteria Recognition Arrangement), the widest available mutual recognition of secure IT products. The certificate is recognized by 31 countries

17 authorizing members

US, Australia, New Zealand, Canada, ***France, Germany, Spain, Italy, the Netherlands, Sweden, Norway****, Japan, South Korea, Singapore, India, Malaysia, and Turkey*

14 consuming members, can only accept and recognize certificates issued by the authorizing countries.



UK, Austria, Czech Republic, Denmark, Finland, Greece, Hungary, Poland, Slovakia*, Ethiopia, Indonesia, Israel, Pakistan, and Qatar.*

On May 20, 2020, CCN, the Spanish certification authority, officially issued the Common Criteria (CC) Evaluation Assurance Level (EAL) 4+ certificate to Huawei 5G gNodeBs. This certificate is also the first CC certification for 5G products worldwide, indicating that Huawei 5G base station products (including source code) have reached the world-leading security level and can provide trusted security assurance for 5G wireless access.

The CC defines seven EALs. A higher EAL requires stricter evaluation and takes more time, meaning that the evaluated product is more secure. Generally, vendors apply for EAL4+ certification at most for general network devices. The CC EAL4+ certification covers **product development process audit, architecture evaluation, product testing,** and **source code review**. The CC EAL 4+ certification covers a wide range of contents and takes a long time (about two years). **Compared with CC EAL3+, CC EAL4+ security evaluation includes source code review.**

CCN
centro criptológico nacional

CERTIFICATE
CCN-CC-11/2020

Huawei 5900 Series 5G gNodeB Software V100R015C00SPC108

Type of product	Software
Conformance of functionality	Product specific Security Target – CC Part 2 conformant
Evaluation Facility	DEKRA Testing and Certification S.A.U.
Certification Report	CCN- CCN-CC/2018-60/INF-3128
Expiration Date	See Certification Report

Pursuant to the authority vested in me under Act 11/2002 regulating the National Intelligence Centre, and under Article 1 and Article 2.2.c of Royal Decree 421/2004 cf March 12th regulating the National Cryptologic Centre, I hereby:

Certify that the security of Huawei 5900 Series 5G gNodeB Software V100R015C00SPC108, developed by Huawei Technologies Co., Ltd., F4 F Area Administration Building, Headquarters of Huawei Technologies Co., Ltd. Bantian, Longgang District, Shenzhen, 518129, P.R.C., has been evaluated using Common Methodology for Information Technology Security Evaluation/Common Criteria for Information Technology Security Evaluation version 3.1 release 5, and it has met the requirements of its Security Target identified as "CC HUAWEI 5G gNodeB V100R015C00SPC108 Security Target v1.1 (25 March 2020)", for evaluation assurance level EAL4+ALC_FLR.2.

Madrid, 20 May 2020
Secretary of State Director

Paz Esteban López

This certificate, its scope and validity are subject to the terms, conditions and requirements specified in the "Reglamento de Evaluación y Certificación de la Seguridad de las T.I.C." at PRE/2740/2007, September 19th.

The above-mentioned Security Target and Certification Report are available at the National Cryptologic Centre.

5G gNodeB CC certificate

https://www.commoncriteriaportal.org/ccra/members/

5GC(UDG) ERNW Software Engineering Evaluation Report

Huawei Cloud Core Network product line proactively invited ERNW to evaluate UDG security software engineering. ERNW senior auditors reviewed the source code by using leading tools and methods as well as the industry's best practices, and released a review report. **The report showed that the source code quality is a good indicator that Huawei has established a mature and appropriate software engineering process for UDG. This is a convincing proof that Huawei 5G core networks are secure and reliable**.

The UDG is a converged network element that can process both 5G and traditional network services. On a 5G core network, it can function as a user plane function (UPF). On a traditional network, it can function as a serving gateway for the user plane and a packet data network gateway for the user plane. ERNW reviewed the source code for UDG components in the Huawei Cyber Security Transparency Center in Brussels, Belgium. *(*During Feb. and March, 2020)*

The review covered **source code quality**, **build processes**, and **open-source component lifecycle management**. The source code quality review showed that the complexity of the source code is below their threshold, duplicate code is rarely present only where appropriate, and unsafe functions seemed to be avoided wherever possible. The build process review indicated that all binaries are compiled with secure compilation options and are also built with an acceptable level of binary equivalence. The review of the lifecycle management of open-source components showed that the separation of open-source code, code handling, as well as documentation and patch management are all reasonable and meet modern standards. Considering all the results of the technical review, the source code quality is a good indicator that Huawei has established a mature and appropriate software engineering process.

* ERNW is an independent IT security service provider in Germany.

https://www.huawei.com/en/press-events/news/2020/5/huawei-5g-core-network-udg

欧州における通信機器セキュリティ検証

英国ファーウェイ サイバーセキュリティ評価センター

Huawei Cyber Security Evaluation Centre (HCSEC)　概要

2010年設立
DV認証（英国政府の機密情報を扱う最高レベルの資格）をもつ英国人による検証
英国通信インフラで使用するHuawei機器のサイバーセキュリティ検証、ソースコード検証を実施
英国政府、通信事業者に検証結果を報告

2014年よりOversight Board（英国GCHQ、通信事業者、Huaweiで構成）による管理・監査開始
GCHQは英国政府通信本部。国内外の情報収集・暗号解読業務を担当する機関
（2016年以降はGHCQ傘下に設置されたNCSC（英国家サイバーセキュリティ・センター）が担当部局）
毎年HCSECの活動結果、監査結果等をOBリポートとして発行

英国政府発行リポート（OBリポート）へのリンク

2019年　https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2019
2018年　https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2018
2017年　https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2017
2016年　https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2016
2015年　https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2015
2013年　https://www.gov.uk/government/publications/huawei-cyber-security-review
https://www.gov.uk/government/publications/foreign-involvement-in-the-critical-national-infrastructure-intelligence-and-security-committee-report

英国政府2019リポート（OBリポート） 概要（１）

1．HCSECが保証する安全性

英国政府は間違いなく世界で最も強硬かつ厳格な監督を実施

英国のネットワークが昨年よりも脆弱であることを示すものではない

英国重要ネットワークにおけるHuawei製品の国家安全リスクに関し、長期的解消を限定的に保証

計5回の第3者監査により、HCSECのHUAWEIからの独立性は問題なし

課題・脆弱性は中国に関係するものでは無い

2．検出されたHuawei機器の脆弱性

前年度と同程度（数100件）、過去の検証と同様の脆弱性
「スタック・オーバーフローに対する保護」
「プロトコルの準正常性に対する耐性」など

英国政府2019リポート（OBリポート） 概要（２）

3．ソフトウェアエンジニアリング（開発アプローチ）の主要課題

バイナリー一致性
　HCSEC環境で商用と同じバイナリーコードを作成することが困難

ソフトウェア・ビルド管理
　バイナリーコード作成環境（エンド・エンドの統一性、バージョン世代管理、ツール世代管理）

構成管理
　開発部署・製品で異なるコード管理、サードパーティで異なるコード・バージョン管理など

サードパーティ・汎用リアルタイムOS
　サードパーティ・汎用リアルタイムOSの脆弱性、サポート期間
　（ single memory space, single user）

ライブラリ世代管理
　異なるバージョンのOpen SSLを製品依存で使用

→抜本的対策として「ソフトウェアエンジニアリング能力の変革」を3年以上で全社的に過去の全てのコードに対して実施することをHuaweiが合意

Huaweiのソフトウェア・エンジニアリング改革

https://www.huawei.com/jp/press-events/news/jp/2019/hwjp20190213t

輪番会長　エリック・シュ―の記者会見より

“弊社と英国は外側から内側へと目を向けるようになりました、内側というのは、設備の堅牢さから、開発プロセスが高品質かどうか、信頼できるかどうかなどにまで及んでいます。結果のみならず、プロセスも問うようになったのです。”

“HCSECは弊社のソースコードが美しくないと言っています。弊社のソースコードは過去30年間にわたって構築してきたものですから、確かに美しくはないでしょう。コードの読みやすさや修正しやすさは改善すべきですし、コードの作成プロセスも改善が必要です。結果の品質と信頼性だけでなく、プロセスの信頼性も高めなければ、本当の信頼は得られません。このようにして、弊社はソフトウェア生産プロセス、すなわち我々がソフトウェアのエンジニアリング能力と実践と呼ぶものに注力するようになり、かつ、30年前からあったレガシーなコードを改善するために、将来を見据えた標準を適用することになったのです。”

“徹底的にソフトウェアエンジニアリング能力の向上、変革を行うことを決定しました。目標は信頼される製品を打ち立てることです。変革には3-5年の時間がかかります。将来を見据えた標準と要求に基づき、徹底的にソフトウェア生産のプロセス全体を変革します。同時に、過去のすべてのコードについても将来を見据えた標準にあわせてリファクタリングを行います。”

英国上院・科学技術委員会の結論　（2019/7/10）

要旨：

・英国の通信ネットワークからHuaweiを完全排除とする技術的証拠はない

・政府は（セキュリティだけではなく）あらゆるネットワーク障害においても、通信を活用する主要サービスを継続運用可能とする必要がある

・コアネットワーク
（コアと無線アクセスは5Gでも分離されているが）
政府はコア・ネットワークへのファーウェイの適用を（理由明確化の上で）制限すべき

・政府はファーウェイ サイバーセキュリティ評価センターからの報告書で指摘された課題への対応の進捗を注視すべき

・政府は同様の検証センターを他ベンダーにも設置することを検討すべき

＜出典＞
https://www.parliament.uk/business/committees/committees-a-z/commons-select/science-and-technology-committee/news-parliament-2017/chairs-comments-huawei-5g-network-17-19/

欧州委員会　5Gサイバーセキュリティへの共通アプローチ

2019/3/26:_5Gネットワーク・サイバーセキュリティへの欧州共通アプローチを勧告
“European Commission recommends common EU approach to the security of 5G networks”
　→リスクアセスメント、リスクマネージメント対策のマイルストーンを提示

2019/10/9：欧州全体のリスクアセスメント結果の報告書を発行
“EU coordinated risk assessment of the cybersecurity of 5G networks”

2020/1/29：リスク・マネージメント対策（EU Toolbox）を発行
”Cybersecurity of 5G networks EU Toolbox of risk mitigating measures”
　欧州各国に対策実施を勧告
　欧州共通の通信機器のセキュリティ認証システムの構築を勧告

2020/1/29： GSMA（通信事業者のグローバル業界団体）が、 UE Toolboxを補完する
セキュリティ検証システムNESAS（次頁参照）を提案。
https://www.gsma.com/gsmaeurope/safer-mobile-use/latest-news/the-gsma-will-work-with-enisa-to-secure-5g-networks/

2020/4/30（予定）：欧州各国が対策を実装・実施
2020/6（予定）　　：実施内容を報告
2020/10（予定）　:対策の効果のアセスメント

ドイツ　5Gセキュリティへの対応状況

2018.11.16:「ドイツにファーウェイ・セキュリティ検証センターを開設」
https://www.reuters.com/article/us-germany-telecoms-huawei-exclusive/exclusive-chinas-huawei-opens-up-to-german-scrutiny-ahead-of-5g-auctions-idUSKCN1MX1VB

・ソースコード（ソフトウェア設計情報）を開示し試験検証
・検証センターはファーウェイが運営するが、政府機関、オペレータによる検証のために使用

2019.10.14:　「ドイツの新セキュリティ要件　ファーウェイを排除せず」
https://www.reuters.com/article/us-germany-telecoms-5g/new-german-rules-leave-5g-telecoms-door-open-to-huawei-idUSKBN1WT110

・技術基準等に基づくセキュリティカタログを構築
・全てのベンダーに対して同等に適用

2019.10.15：ドイツ政府　セキュリティ・カタログ（要件）　改版案公開
https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2019/20191015_ITSicherheitskatalog.html?nn=404530

・技術基準等に基づくセキュリティカタログを構築
・全てのベンダーに対して同等に適用
・ドイツ政府がセキュリティ重点分野のリストを公開しその製品認証を行う
・製品認証は2021年1月1日以前の製品には猶予が与えられるが、2025年12月31日以降は必須となる

Thank You.