Android（ARM）＋TPMによる セキュアブート

KDDI研究所　竹森敬祐（Ph.D）

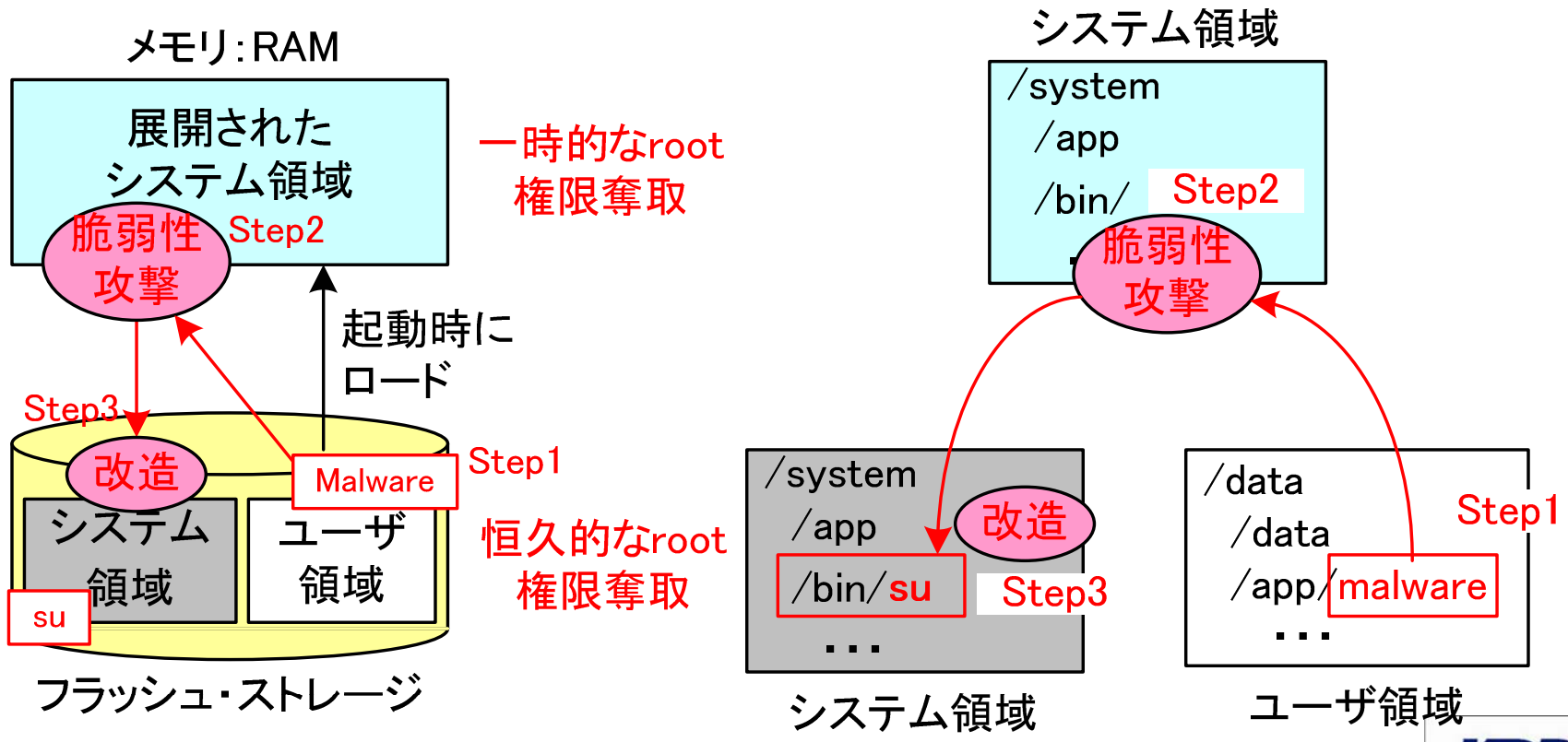
Android OSは、通常利用においてシステム領域の完全性が維持されている。
組み込みOSとしても利用されるAndroid OSのセキュアブートの意義を考察する。

KDDI R&D LABS

背景：root権限奪取とシステム改造の流れ

■ 攻撃のシナリオ

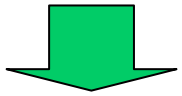
Step1: root権限奪取アプリをユーザ領域にインストールし、実行する。
Step2: OS等の脆弱性を突いてメモリ上でroot権限を奪う。
Step3: システム領域に恒久的にroot権限を利用できるようsuを置く（改造）。



背景：root権限奪取とシステム改造の脅威

■ 直接的な脅威
- su、busybox、botコードを埋め込まれる。
- スクリーンキャプチャ、キーロガーを仕掛けられる。⇒遠隔制御
- 他のアプリの挙動やhttpsなどの通信パケットもモニタ・盗聴される。
- MACアドレス、IMEI、IMSIなどを詐称される。
- 著作権保護サービスが影響を受ける。

■ 副次的な脅威
- 社内LANに持ち込まれた場合、スパイ端末にされる。
- 端末が正しいことを前提にした認証サービスが騙される。



セキュアブートによる端末状態の検疫が重要！

KDDI R&D LABS

TPMによる認証・セキュアブート

■ TPMの主な効果
- ◆ 秘密鍵を内部に持ち、リモートから端末を確実に「認証」できる。
- ◆ システム領域が完全であることを測定・検証しながら起動させる「セキュアブート」が可能になる。

■ PC向けOS（x86）＋TPMのセキュアブート
- ◆ システム領域がユーザに開放されたPCの場合、完全な状態の基準を策定しきれない難しさがあり、広範囲の普及に至っていない。

■ スマホ向けOS（ARM）＋TPMのセキュアブート
- ◆ システム領域は、原則、利用者に開放されていないが故に、完全な状態についての基準の策定は容易である。
- ★ 認証時に、端末の状態とアプリが完全な状態であることをリモートから検証できる意義は大きい。

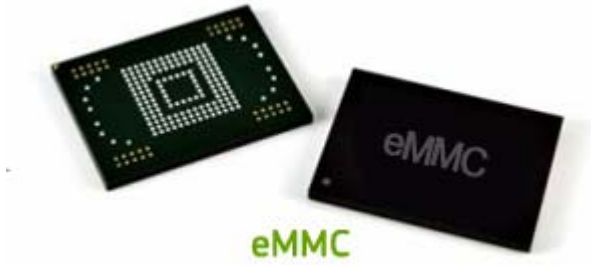
KDDI R&D LABS

2つのポイント

- ハッシュ測定にARM上のCPUをフル活用
  - TPMによるハッシュ測定は、大きな時間を要する。
  - eMMCフラッシュメモリ搭載のARM端末は、Boot Loader 1＊をROM焼きすることができ、Root of Trustとして利用できる。

（Windows 8のTrusted Bootでは、セキュリティH/W（UEFI）をroot of trustにする。）

＊ スマホ端末には、PC端末と違って、BIOSが無い。⇒Boot Loaderから起動スタート。



- 最小構成のLinuxから大きなAndroidシステムを測定
  - ARMボードのCPUをフル活用するために、File I/Oを効率的に行える最小構成のLinuxを切り出し・起動させ、そこから大きなAndroidシステムを測定する。

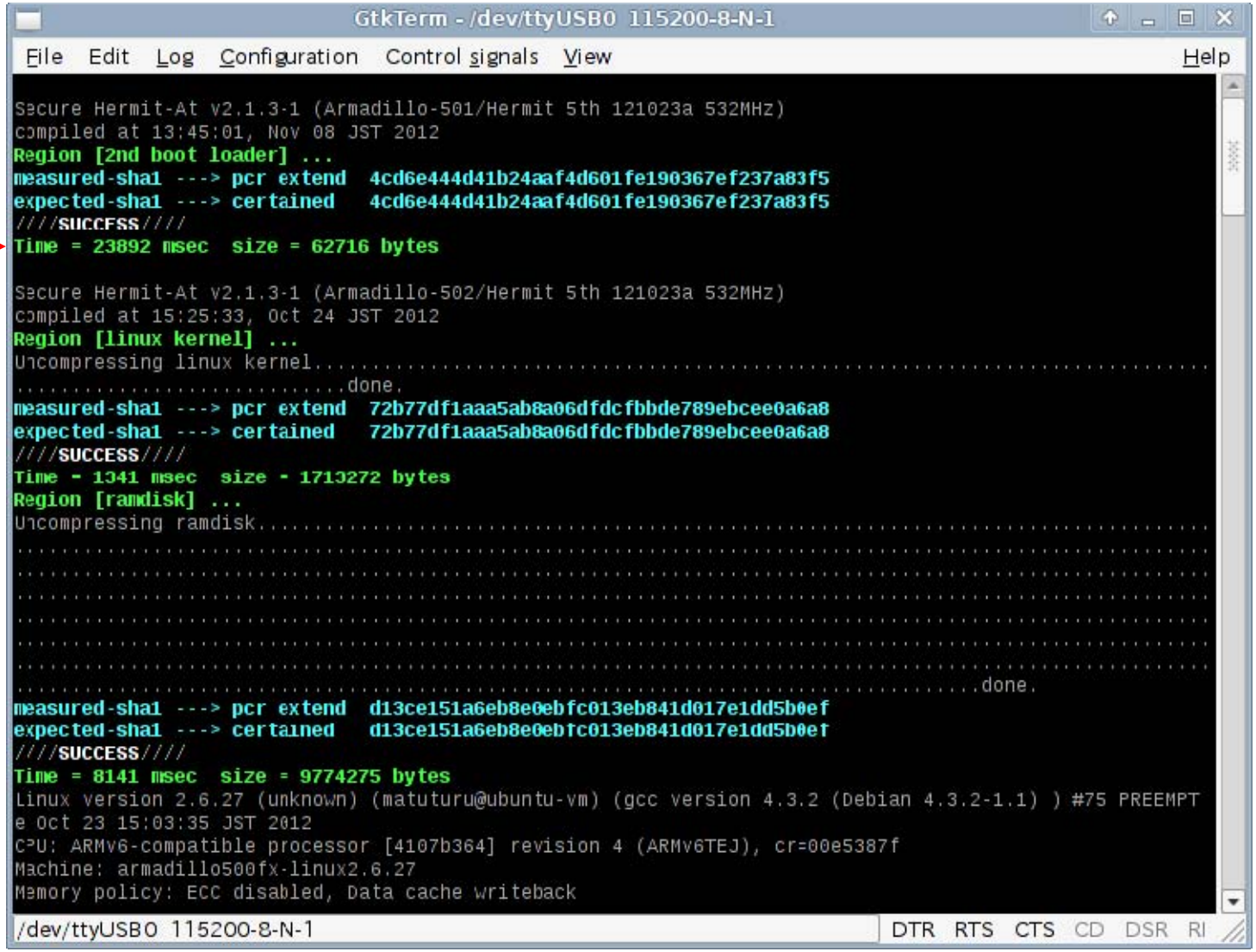
KDDI R&D LABS

研究途中の苦労：Boot Loader 2の測定 by TPM

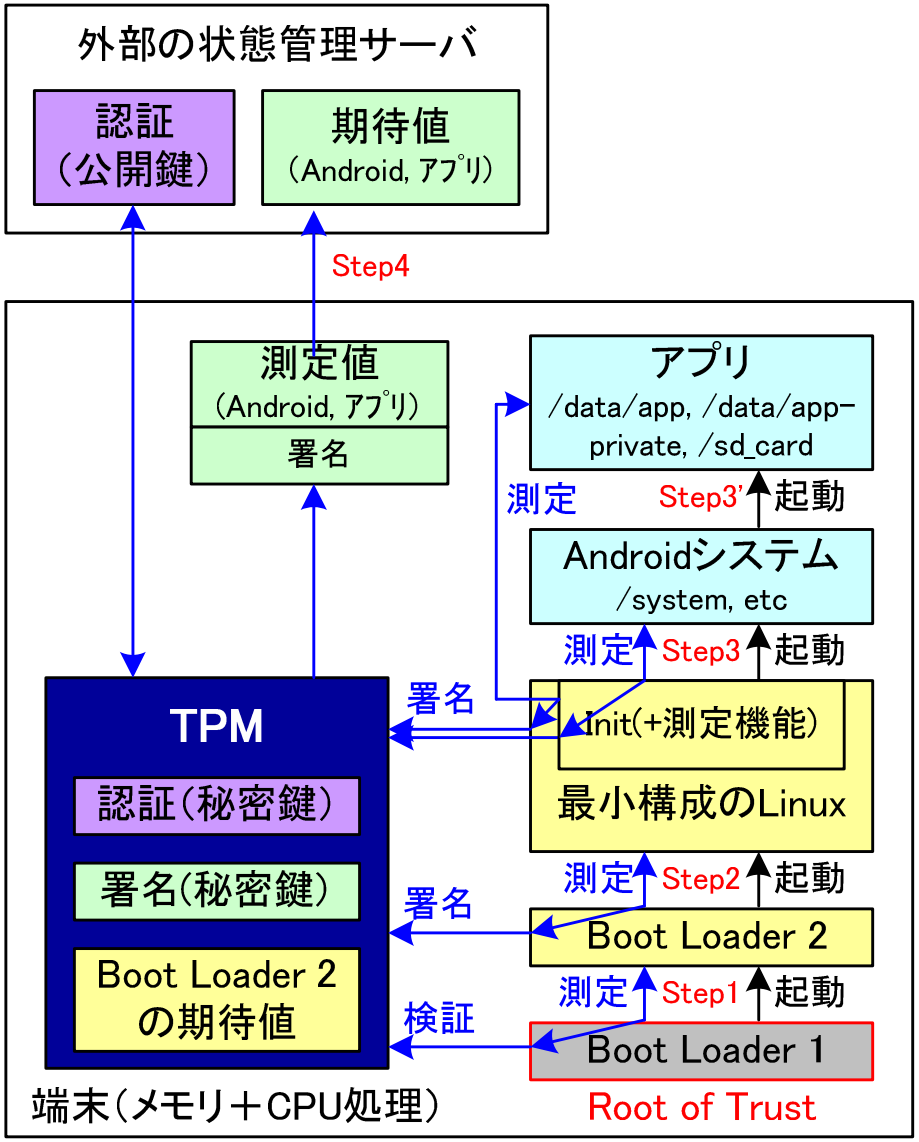
TPMによる
Boot Loader 2の
測定
24秒／61KByte

通信も100Kbps

ARM上のCPUを
活用することに。



設計：Android（ARM）＋TPMのセキュアブート



Step4. 状態管理サーバに測定結果を送付し、完全性をリモート検証する。

Step3. 起動プログラム（init）に組み込んだ測定機能で、Androidのシステム領域とアプリ領域を測定。Androidのシステム・アプリを起動。

Linuxカーネルのinitから大きなAndroid領域を測定

Step2. フラッシュメモリにある、システム起動のための最小構成のLinuxと起動プログラム（init）を測定。RAMに展開し、Linuxを起動。

Boot Loader2から最小構成のLinuxを測定

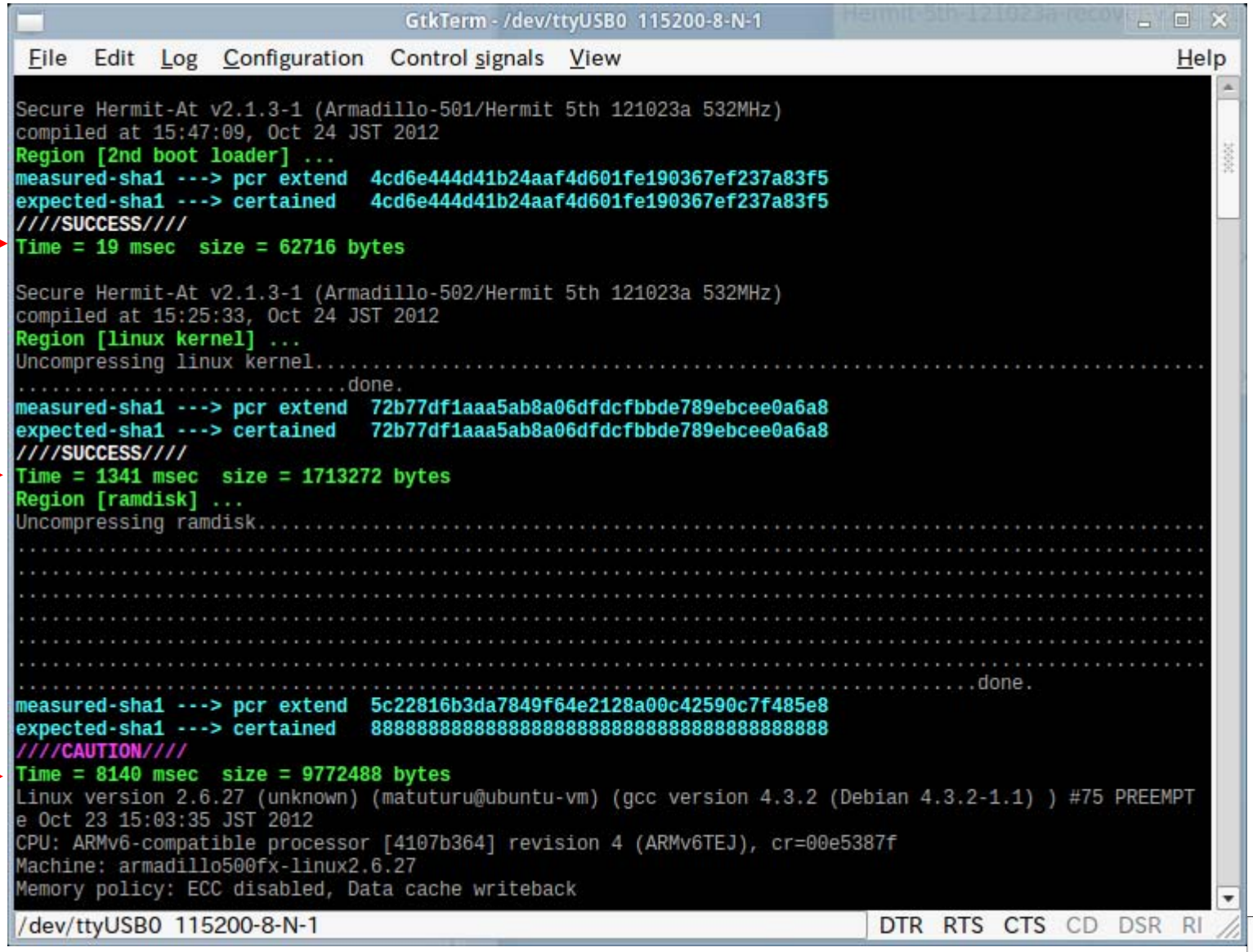
Step1. Boot Loader 2を測定。
Boot Loader2を起動。

Boot Loader1からBoot Loader2を測定

実装: 測定箇所

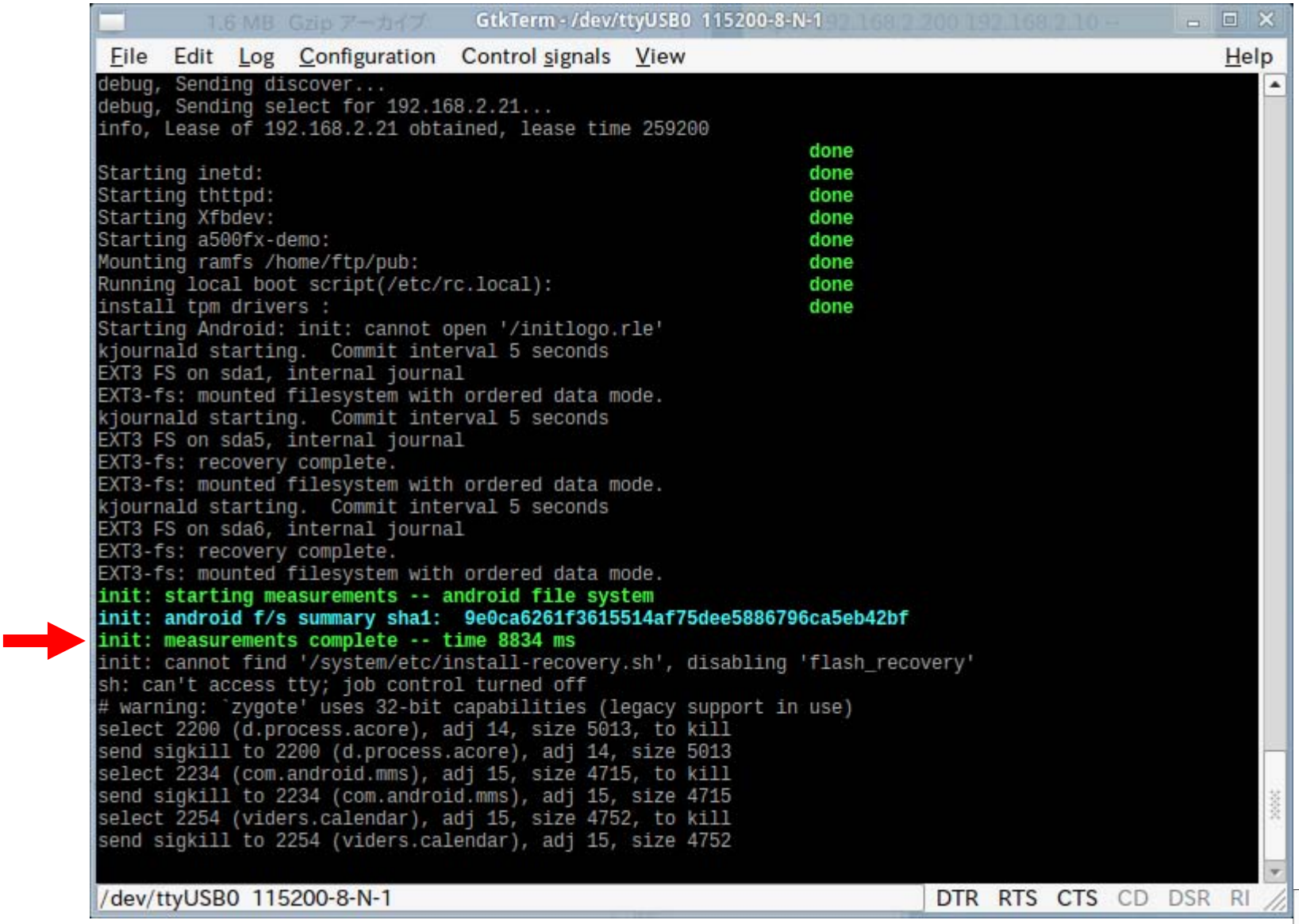
- 最小構成のLinuxの測定 by Boot Loader 2
  - /(ルート)下のファイルをBoot Loader2で測定
    - ⇒ init : システム起動処理＋Androidシステム領域測定機能
- Androidシステム領域の測定 by Linux init
  - initから以下の/system領域を測定
    - ⇒ app : システムアプリ＋一般アプリ測定機能
    - ⇒ bin : コマンド
    - ⇒ etc、lib : 設定ファイル、ライブラリ
    - ⇒ fonts : フォント
    - ⇒ framework:フレームワーク
    - ⇒ usr : 設定ファイルなど
    - ⇒ xbin : 拡張コマンド(TPMアプリ)
    - ⇒ 上記以外に/vendor/binがあれば追加
- アプリ領域の測定 by Linux init
  - アプリ領域測定用のシステムアプリからアプリ領域を測定
    - ⇒ /data/app にある所望のアプリ
    - ⇒ /data/app-private にある所望のアプリ

測定：Boot Loader 2、Linux＋init



KDDI R&D LABS

測定：Androidシステム・一般のアプリ層



KDDI R&D LABS

評価：起動＋測定に要する時間

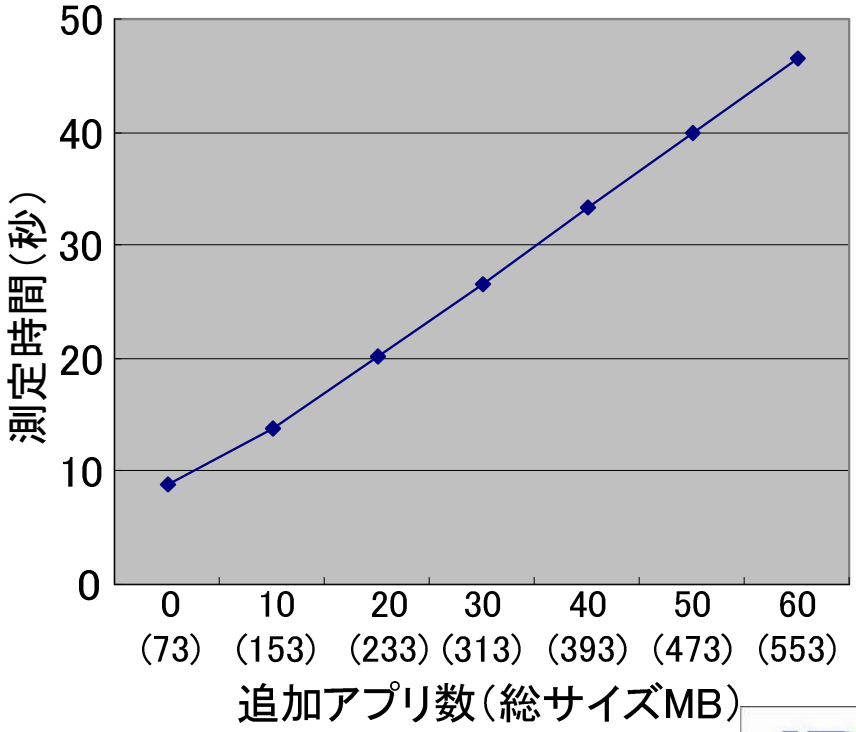
		イメージ展開	イメージ展開＋測定	サイズ
	ブートローダ1	0.0sec	ー	21 Kbyte
Step1	ブートローダ2	0.0sec	0.02 sec (差 0.02sec)	61 Kbyte
Step2	最小構成のLinuxイメージ	1.1 sec	1.3 sec (差 0.2sec)	1.6 Mbyte
Step2	起動用ファイルシステム（＋init）	6.7 sec	8.1 sec (差 1.4sec)	9.3 MByte
Step3	Android OS＋システムアプリ システムアプリ層 (42件)	0.0 sec	8.2 sec (差 8.2sec)	71.2 MByte
Step4	一般アプリ層（18件）	0.0 sec	0.6 sec (差 0.6sec)	1.4 MB
	LinuxとAndroidの起動	30.2 sec	40.6 sec (総差10.4sec)	
	操作を行えるまでの合計時間	48.4 sec	58.8 sec	

KDDI R&D LABS

評価: Androidシステム・一般アプリ数と測定時間

- アプリ数を変化させたときの測定時間
  - 2012年4月入手の無料アプリの平均サイズは約8MBであった。
  - 測定時間と合計サイズはシステム＋一般アプリの合計とする。
    （initからシステムアプリの測定と、システムアプリから一般アプリの測定は、同じFile I/OとSHA-1処理である。）

追加アプリ数	サイズ（MB）	測時間（秒）
0	72.6	8.8
10	152.6	13.8
20	232.6	20.2
30	312.6	26.6
40	392.6	33.3
50	472.6	39.9
60	552.6	46.6



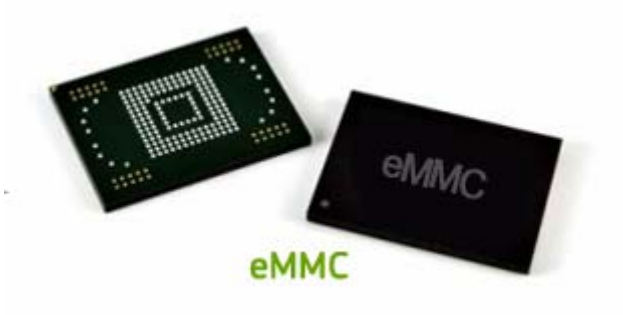
KDDI R&D LABS

今後の課題：最新OS,ボードへの移植

- CPU能力の向上 vs システムコードの増大
  - CPUの処理能力は、クロックの高速化とマルチコア化が進む。
  - Android 4.xのシステム領域は、1400ファイル、400MBを超える 。

- フラッシュメモリ（e-MMC）を使用したRoot of Trustの実現
  - Boot Loader1を書込み禁止に設定できる。
  - 50～140 Mbpsの転送速度を達成できる。
  - さらに未来には、より高速なフラッシュストレージが普及する。

10秒前後（現状と変わらず）と見込む。



- その他
  - メジャーなブートローダ（x-loader, U-boot）への対応

KDDI R&D LABS

効果・適用分野

- Bring Your Own Device（BYOD）
  - 法人LANに接続させる際に、システム領域が完全であって社員による不正改造や、root権限奪取マルウェアの影響を受けていない安全な端末であることを検疫する。

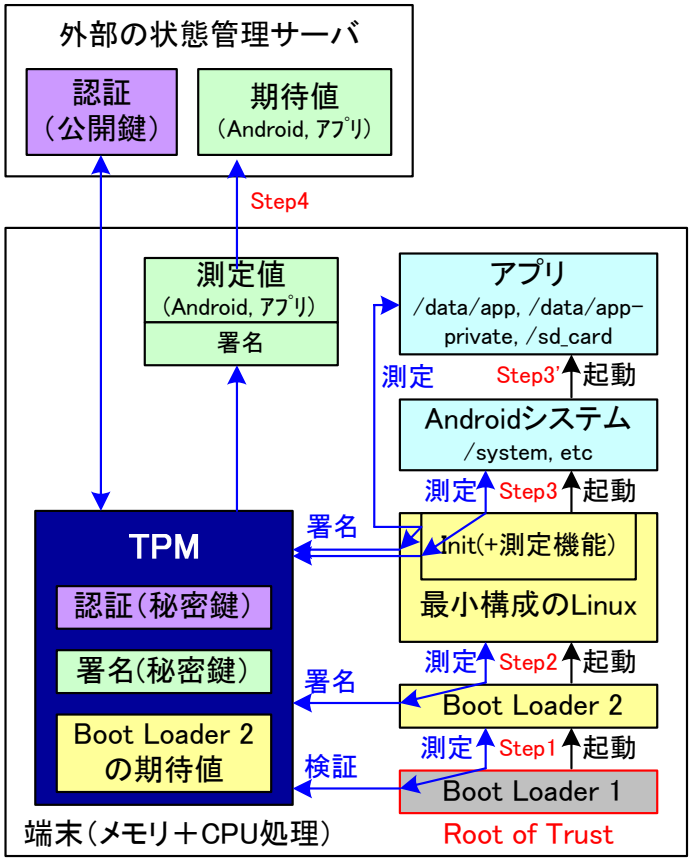
- 専用端末
  - 医療、カーナビなどの重要な処理を担う専用端末への組み込みにおいて、完全な状態であることを検証した後に、起動させる。

- 重要処理アプリ
  - 音楽・映像再生アプリ、銀行決済アプリなど、重要処理の前に端末・アプリが完全な状態であることを検証した後に、サービスを提供する。

デモ概要：Android（ARM）＋TPMのセキュアブート

■ セキュアブート

- ◆ Android搭載のARMボードにTPMを接続して、完全性検証を試作。
- ◆ 端末起動時に、ブートローダ、Android OS、アプリの状態を測定。
- ◆ 測定結果を、遠隔の状態管理局に送付し、完全性をリモート検証する。



デモ構成