アプリケーション解析技術と情報収集モジュール解析結果

JSSEC 技術部会 アプリケーションWG
アプリケーション解析G ／日本電信電話株式会社
リーダ　名雲 孝昭

目次

- 背景とグループ活動内容
- アプリケーション解析手法
- トライアル解析の事例
- 今後の取り組み

背景とグループ活動内容

背景

- アプリ・プライバシーポリシーの記載内容と、実際に送信される情報との整合が取れていない ⟶ 整合性確認には解析技術が必要
- 解析手法の多様化により、どのような場合にどの解析手法が適切か整理できていない

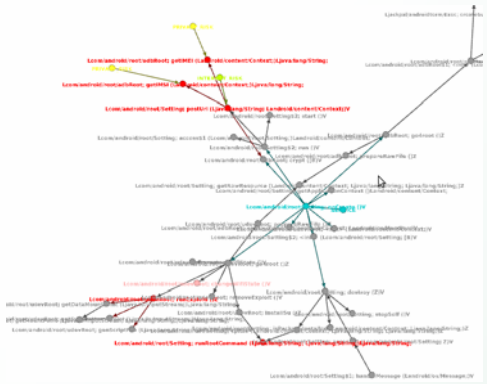
活動内容

- アプリケーション解析のハンズオン勉強会
  →解析エンジニアの技術レベル向上
- アプリケーション解析技術のマッピングとトライアル解析の実施
  →プライバシーポリシーと実際に送信される情報の検証
  →情報収集モジュールを解析した結果の一例を紹介

静的解析と動的解析

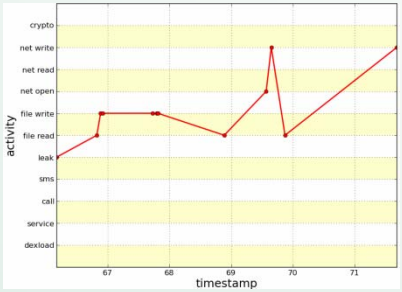
静的解析　アプリケーションを動作させずに解析する手法

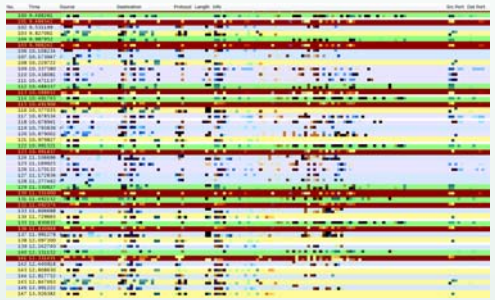
- 解析対象　　：実行コード/ソースコード



動的解析　アプリケーションを動作させて解析する手法

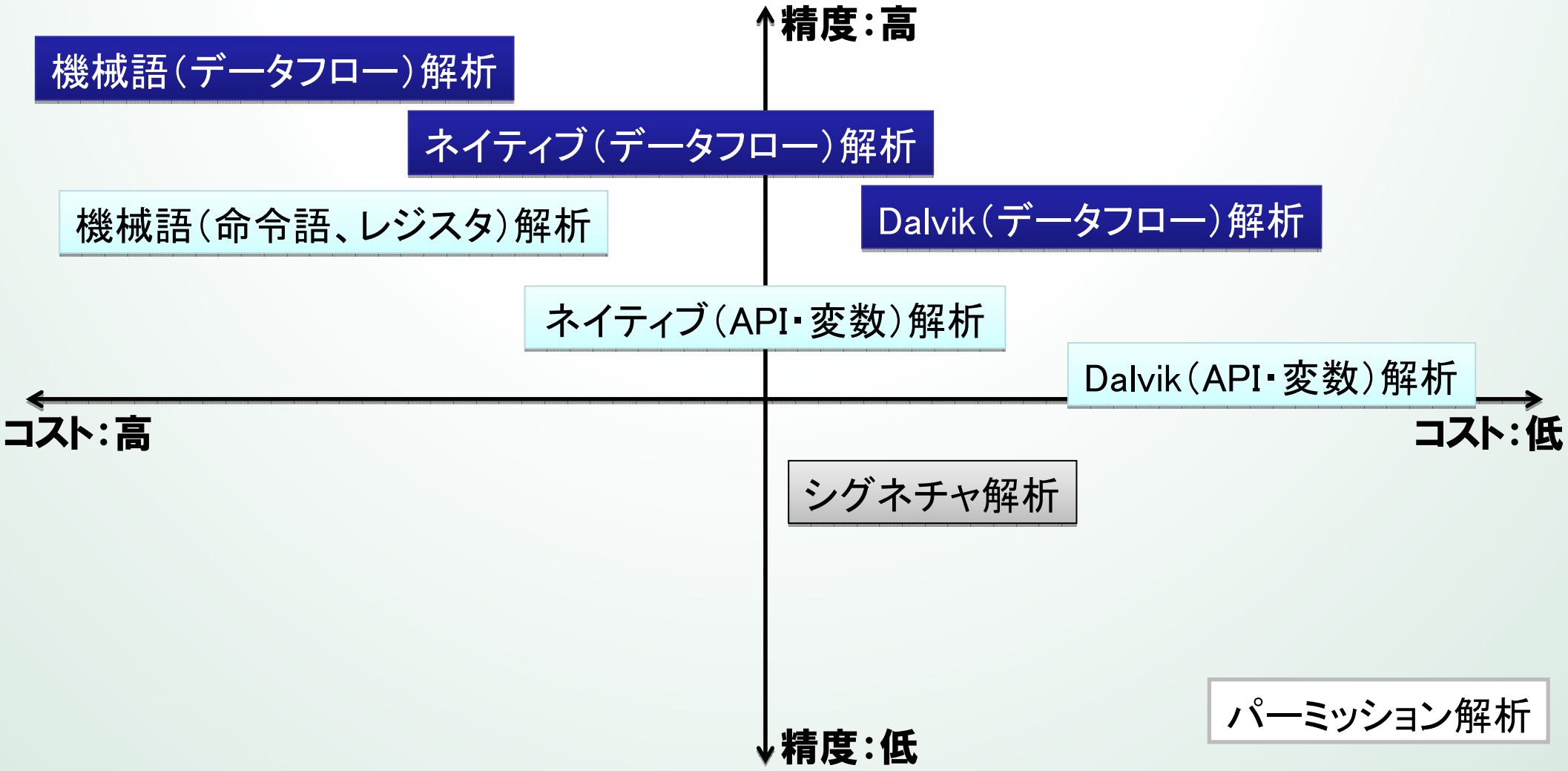
- 解析対象　　：メモリ、ストレージ、プロセス、パケットなど



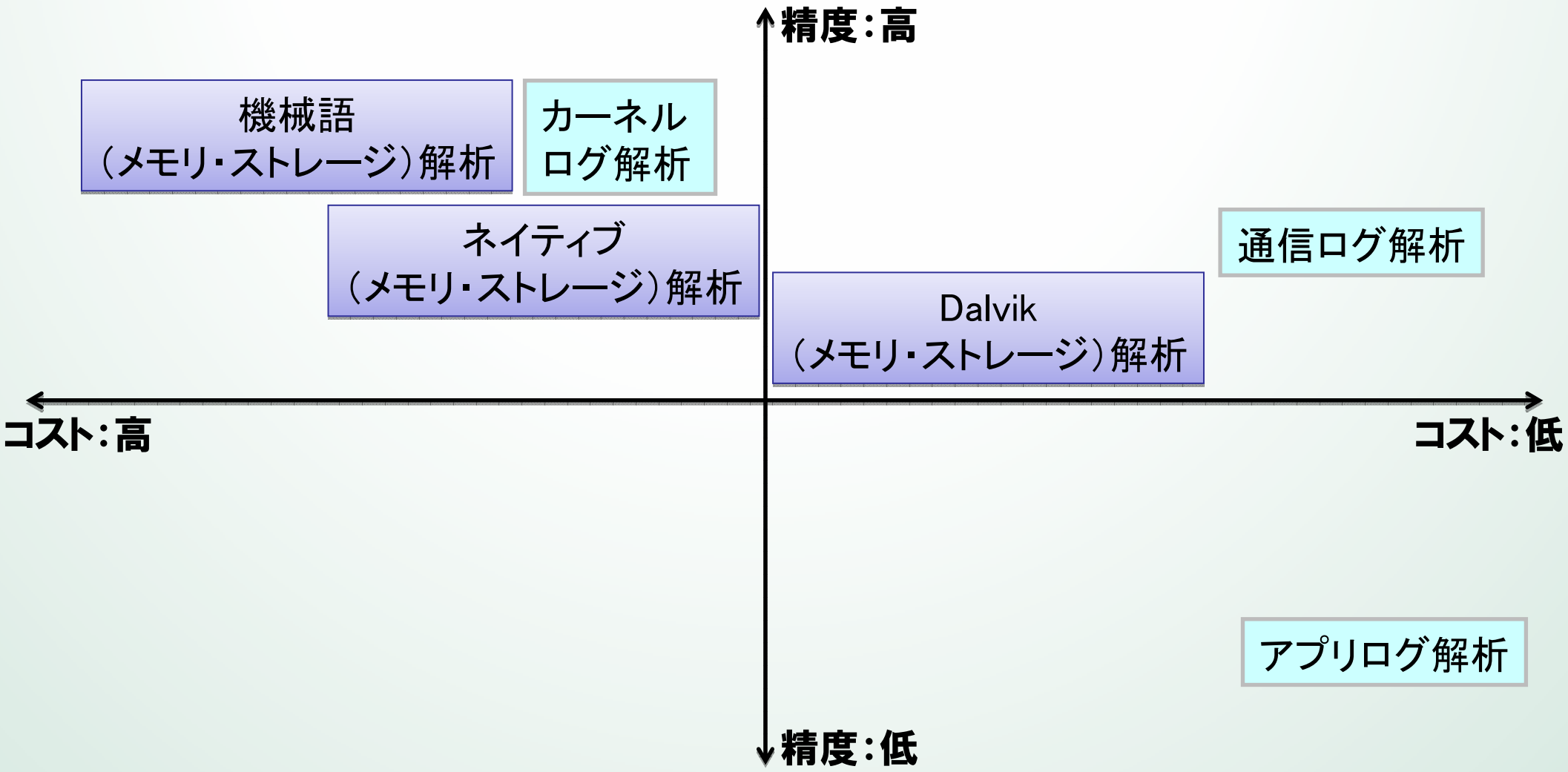


```
GNU gdb (Sourcery G++ Lite 2009q3-68) 6.8.50.20090630-cvs
Copyright (C) 2009 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "--host=i686-mingw32 --target=arm-none-eabi".
For bug reporting instructions, please see:
<https://support.codesourcery.com/GNUToolchain/>.
(gdb) # Load the symbol table
```

静的解析　解析技術の分類



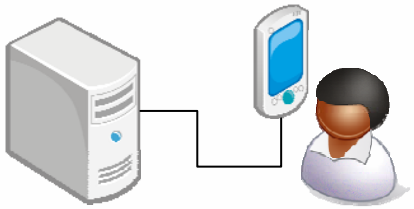
動的解析　解析技術の分類



手動解析と手動解析

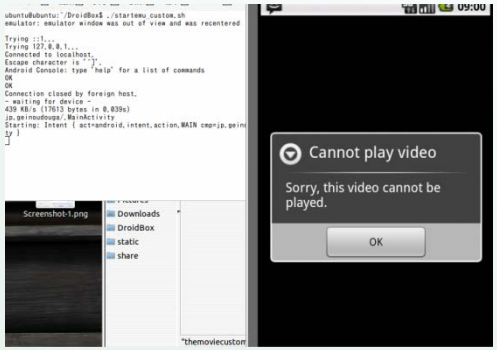
手動解析　人が操作して解析する手法

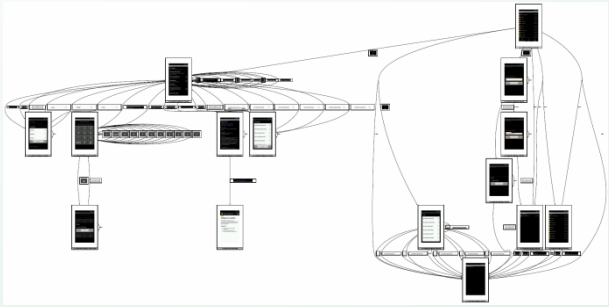
- 精度：高、コスト：高い



自動解析　ツールやロボットを用いて解析する手法

- 精度：低、コスト：低





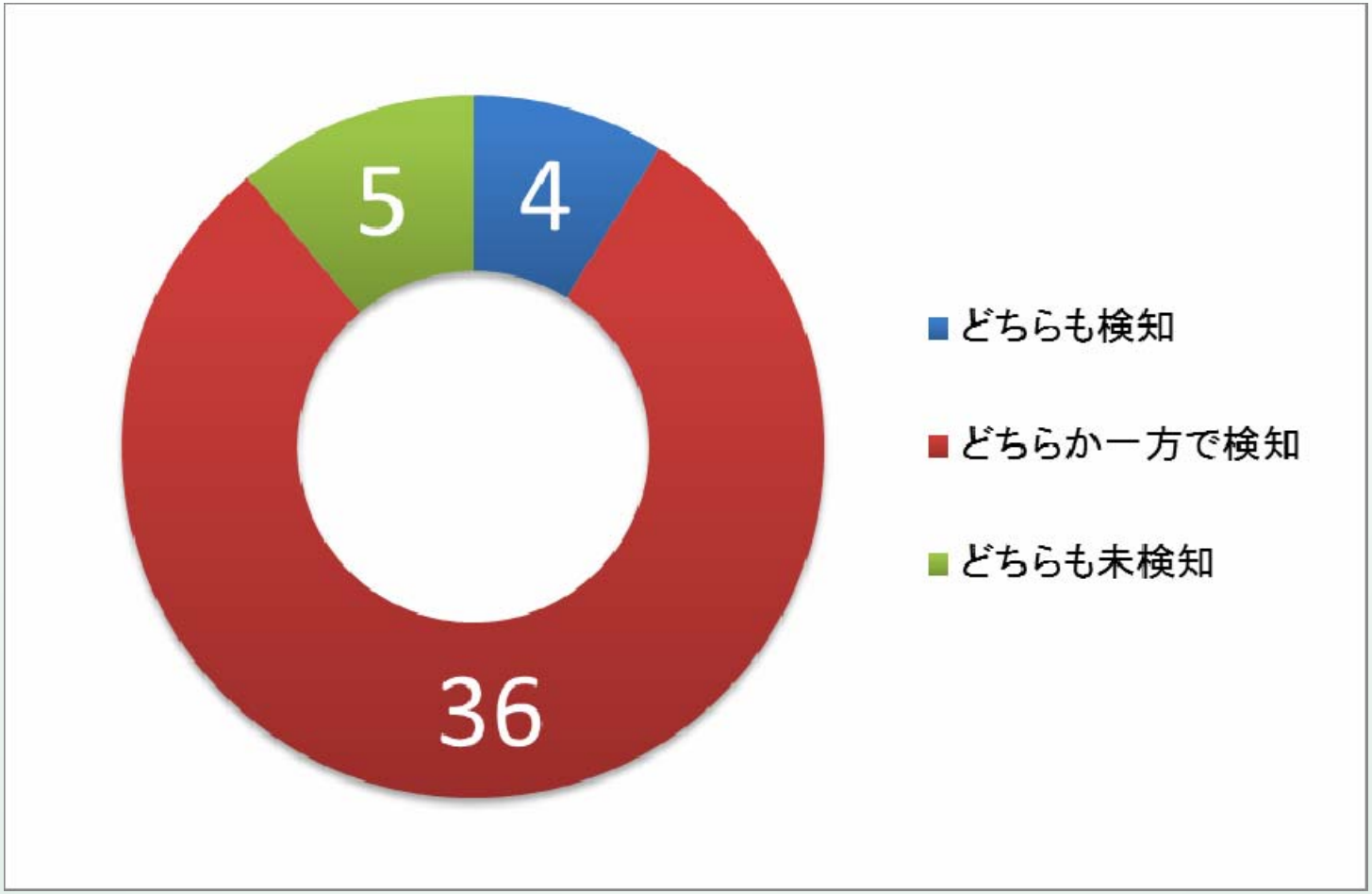
トライアル解析の事例(1/3)

- 解析手法と環境
  - 2種類の解析手法を用いた
    - A) 自動解析＋動的（テイント）解析
      （[動的解析]->[Dalvik（メモリ・ストレージ）解析]）
    - B） 手動解析＋動的（カーネル・通信ログ）解析

- 解析対象の選定
  - :情報収集モジュールG協力
    情報収集モジュールを含んだ127アプリケーションから、動作を確認できた45種類のモジュールを選定

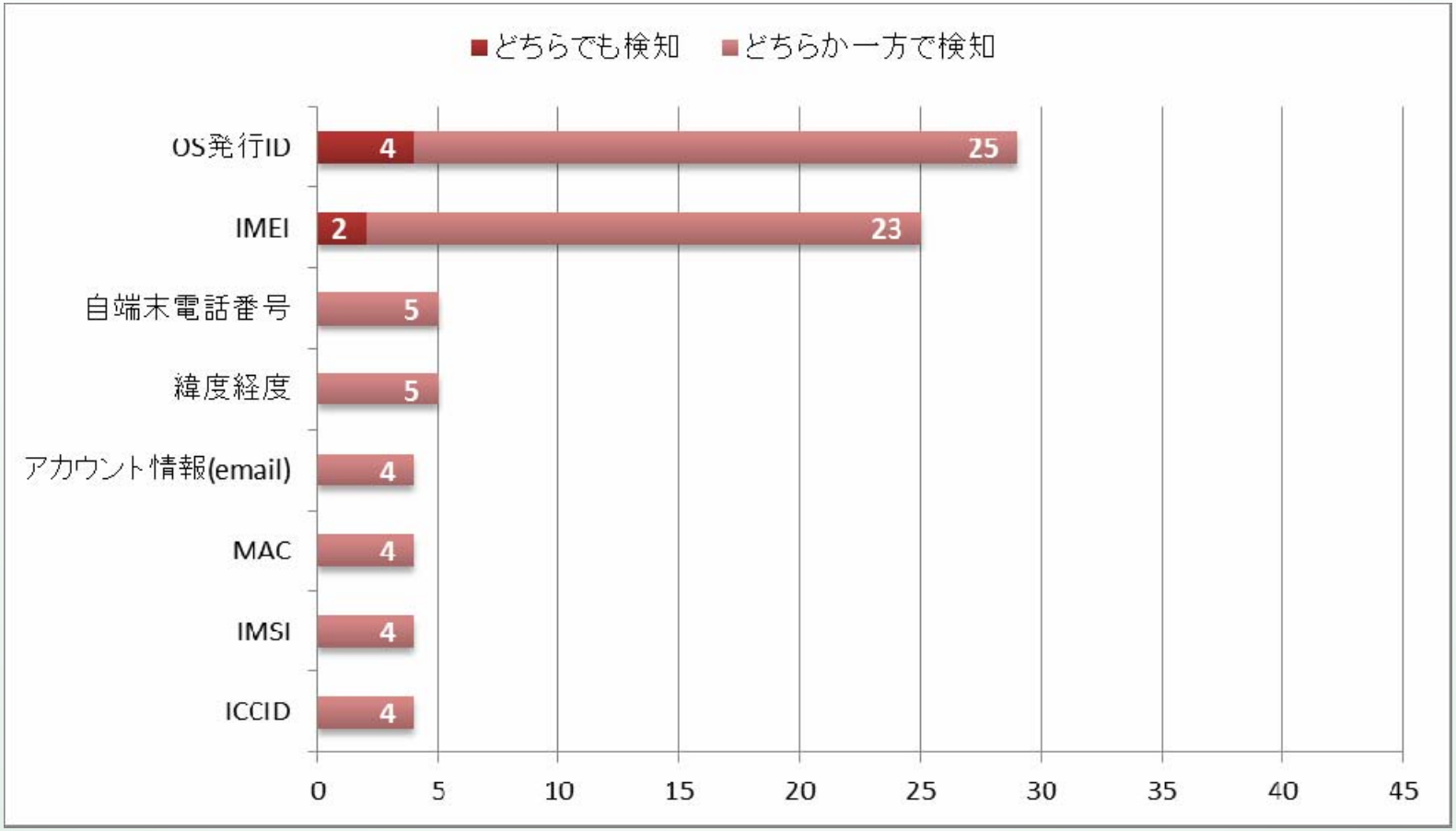
トライアル解析の事例(2/3)

- 利用者情報の送信検知結果
  - いずれかの解析手法で、利用者情報の送信を検知：40種類



トライアル解析の事例(3/3)

- 情報収集モジュールが送信する情報（全45モジュールのうち）



どちらでも検知できた項目は少なく、いくつかの解析手法の組み合わせが有効