334

琉球大学

豊美玲(B4)　津嘉山遼(B3)　山里昌一郎(B3)

テーマ

非接触型ICチップによる

ホームネットワークの

認証&制御

何故このテーマ？

- 今後，スマート家電やスマートホームは
  ホームネットワークを利用，活用することが
  考えられるのでホームネットワークの管理＆
  保護が重要になる

- しかし現状として，今の家のwi-fiは
  パスワードとSSIDだけわかれば誰でも利用
  することができる

事例

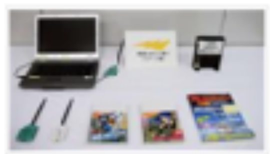
2016.6.30 06:00

【衝撃事件の核心】

狙われる自宅の無線ＬＡＮ　ただ乗り簡単、犯罪に巻き込まれる可能性

(1/3ページ) 【衝撃事件の核心】

お宅の無線ＬＡＮ、勝手に使われていませんか－。他人の無線ＬＡＮを"ただ乗り"したなどとして、警視庁と愛媛県警が6月、電波法違反容疑で、松山市和泉南の無職、藤田浩史被告（３０）＝不正アクセス禁止法違反罪などで公判中＝を再逮捕した。ただ乗りによる摘発は全国で初めて。企業や一般家庭にも普及している通信手段だが、セキュリティーが甘いと「便利な犯罪インフラ」になってしまう。



無線ＬＡＮの「ただ乗り」に使われたパソコンなどの機器＝警視庁赤坂署

パスワード解析ソフトを利用

藤田容疑者の逮捕容疑は昨年６月１１日、自宅で電波法が定める上限の９倍の電波を出力する無線ＬＡＮアダプターを設置。解析したパスワードで他人のＬＡＮに不正接続

無線ＬＡＮのメール丸見え　成田・関西・神戸の３空港

2014/8/26付

成田、関西、神戸の３空港が提供する無料の公衆無線ＬＡＮサービスでインターネットを利用した場合、送信したメールの宛先や中身、閲覧中のウェブサイトのＵＲＬを他人がのぞき見できる状態になることが26日、神戸大大学院の森井昌克教授（情報通信工学）の実地調査で確認された。

無線ＬＡＮを暗号化すればのぞき見を防止できるが、パスワードの入力などが必要となり、３空港は利便性を考慮し暗号化していないという。

現在、全国の公共施設やコンビニなど約90万カ所で公衆無線ＬＡＮが利用できるが、暗号化されていないものも多い。森井教授は「利用者はリスクがあることを理解し、クレジットカード番号など大事な情報のやりとりは避けるべきだ」と話している。

調査は７月下旬に実施し、無料で入手できるネットワーク解析ソフトとパソコン２台を用意した。２台とも無線ＬＡＮに接続し、１台目のパソコンから自分宛てにメールを送信、２台目のパソコンの解析ソフトでメールの内容などを確認できるかどうか調べた。

【ＩＴリポート】スマート家電が犯罪の道具に？　サイバー攻撃に悪用拡大　日本国内発生も「時間の問題」

2016.10.31 21:45

自分が使っている家電が犯罪の道具に使われていたら－。インターネット回線に接続した利便性の高い「スマート家電」が普及する中、家電をウイルス感染させて意のままに操り、標的に危害を加えるサイバー攻撃が拡大の兆しを見せている。米国では２１日に家電を使った大規模なサイバー攻撃が起きており、日本国内での発生も「時間の問題」（専門家）とされる。他者への攻撃の踏み台となるだけでなく、個人情報などを抜き取られる恐れもあり、パソコンと比べて遅れている家電のセキュリティー強化が急務となっている。（福田涼太郎）

■数十万の家電が一斉攻撃…「会社つぶれる」

米国で使われたのは、大量のデータを送りつけてシステムをまひさせる「ＤＤｏＳ（ディードス）攻撃」という手法。ＤＤｏＳ攻撃自体は珍しくないが、データを

Miraiボットネットとは

Miraiは、2016年9月13日夜、米国のセキュリティジャーナリストBrian Krebs氏のWebサイト「Krebs on Security」に対して行われた大規模なDDoS攻撃に使用されたとして話題になったボットネットです（関連記事）。Miraiは主にWebカメラやルーター、デジタルビデオレコーダーなどのIoTデバイスを踏み台としてDDoS攻撃を仕掛けます。

参考：セキュリティ用語事典：DDoS攻撃

攻撃を受けた後に投稿されたKrebs氏のブログ記事によれば、同サイトを保護していたAkamaiが、ピーク時にはそれまでに経験した最大規模の攻撃の2倍近いトラフィックを観測したそうです。

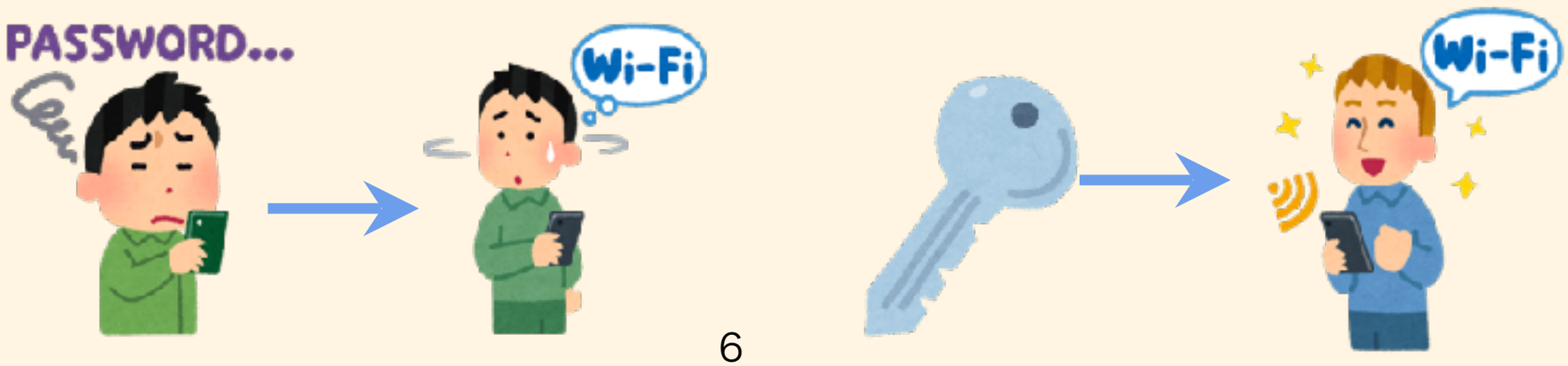
また、2016年10月21日にTwitterやNetflixなどが利用するDNSサービスへ行われたDDoS攻撃でも、Miraiボットネットが利用されていたのではないかと推定されています（関連記事）。

そしてKrebs氏のサイトへの攻撃後、ハッカーフォーラム上でMiraiのソースコードが公開されたことも大きな話題となりました。このソースコードは後にGitHub上に転載され、誰でも中身を見ることができるようになっています（注1）。

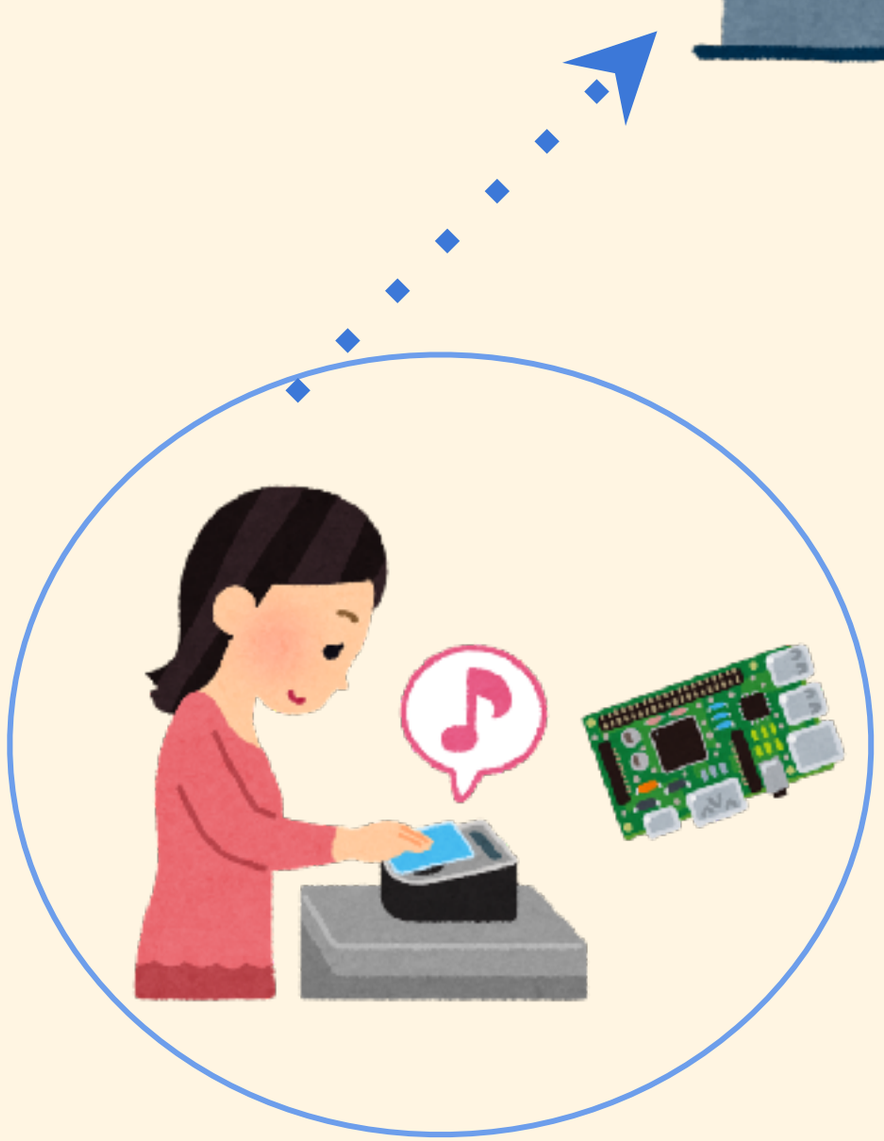
なら，今よりもその家の
住人だけが安全に快適に
家のwi-fiを使えるようにしたい！

つまり

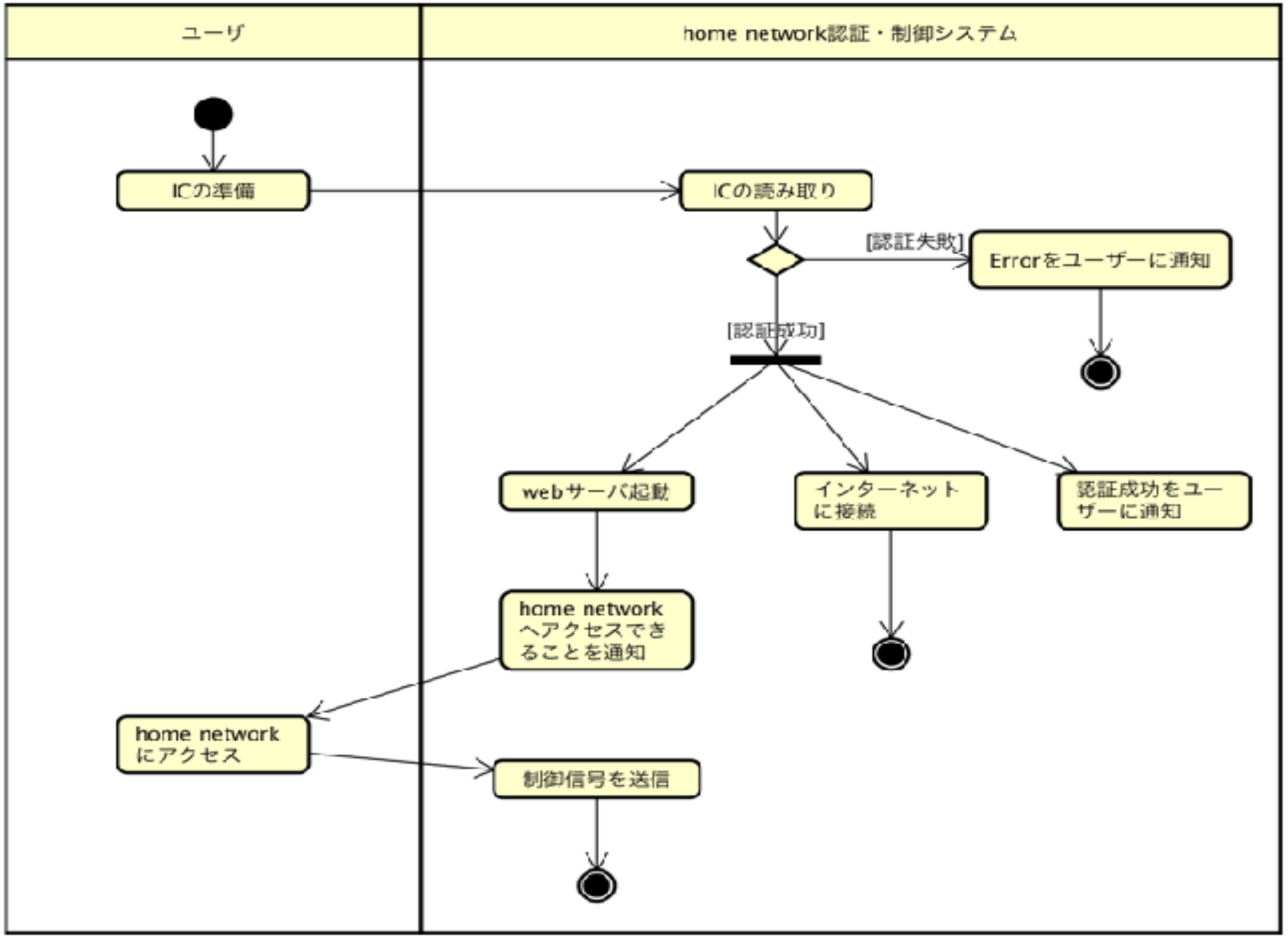
- 現在のwi-fiのパスワードとSSIDは知識認証なのでわかりにくい
- ならば，所有物認証にしてしまおう！
- 所有物認証にすることで皆がわかりやすい！



どのようなシステムにするか



どのようなシステムにするか



役割分担

- **豊**

LED工作・技術検証・統括

- **山里**

raspberryPiのAP化

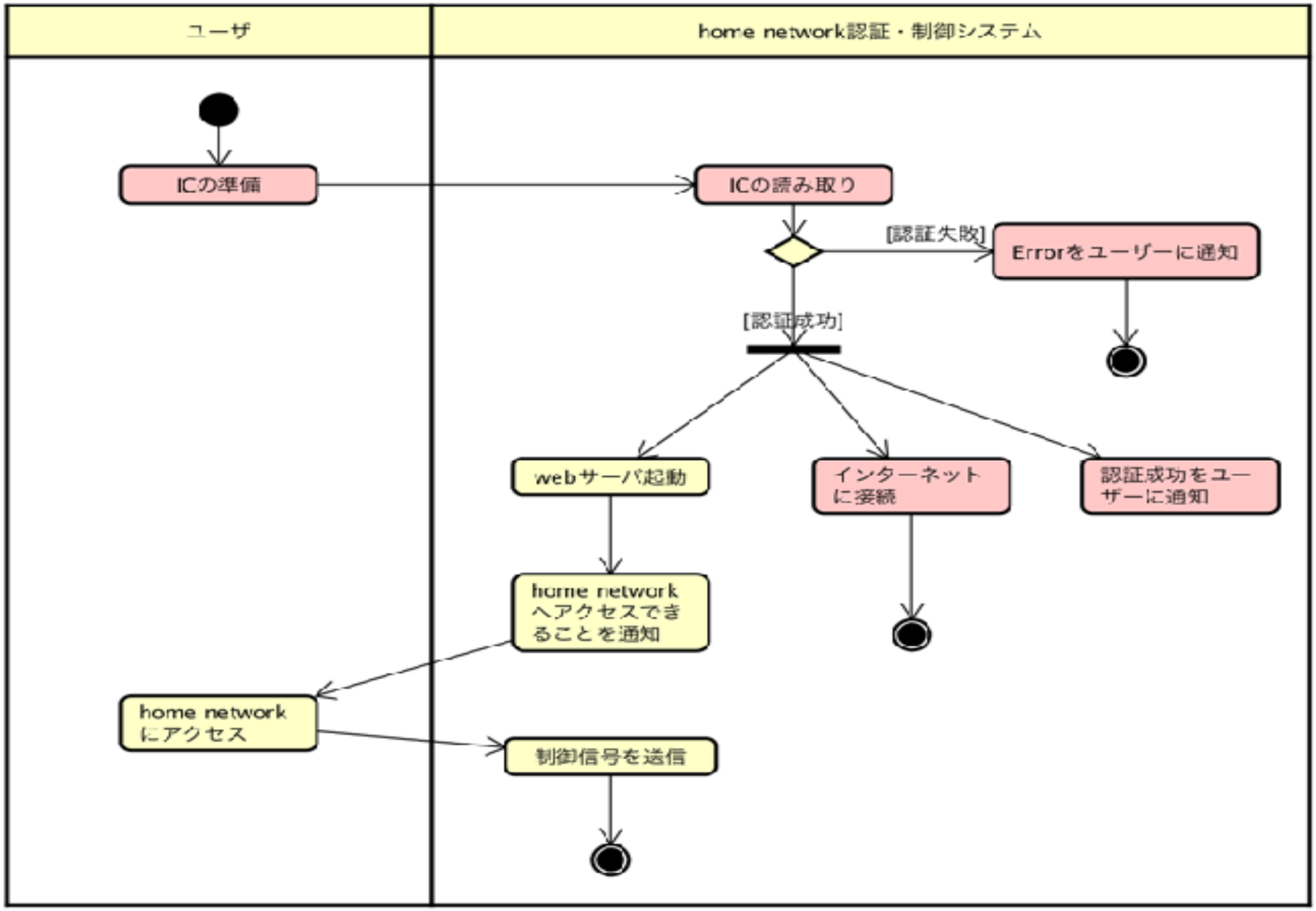
- **津嘉山**

ICカード認証・ログインユーザ照合

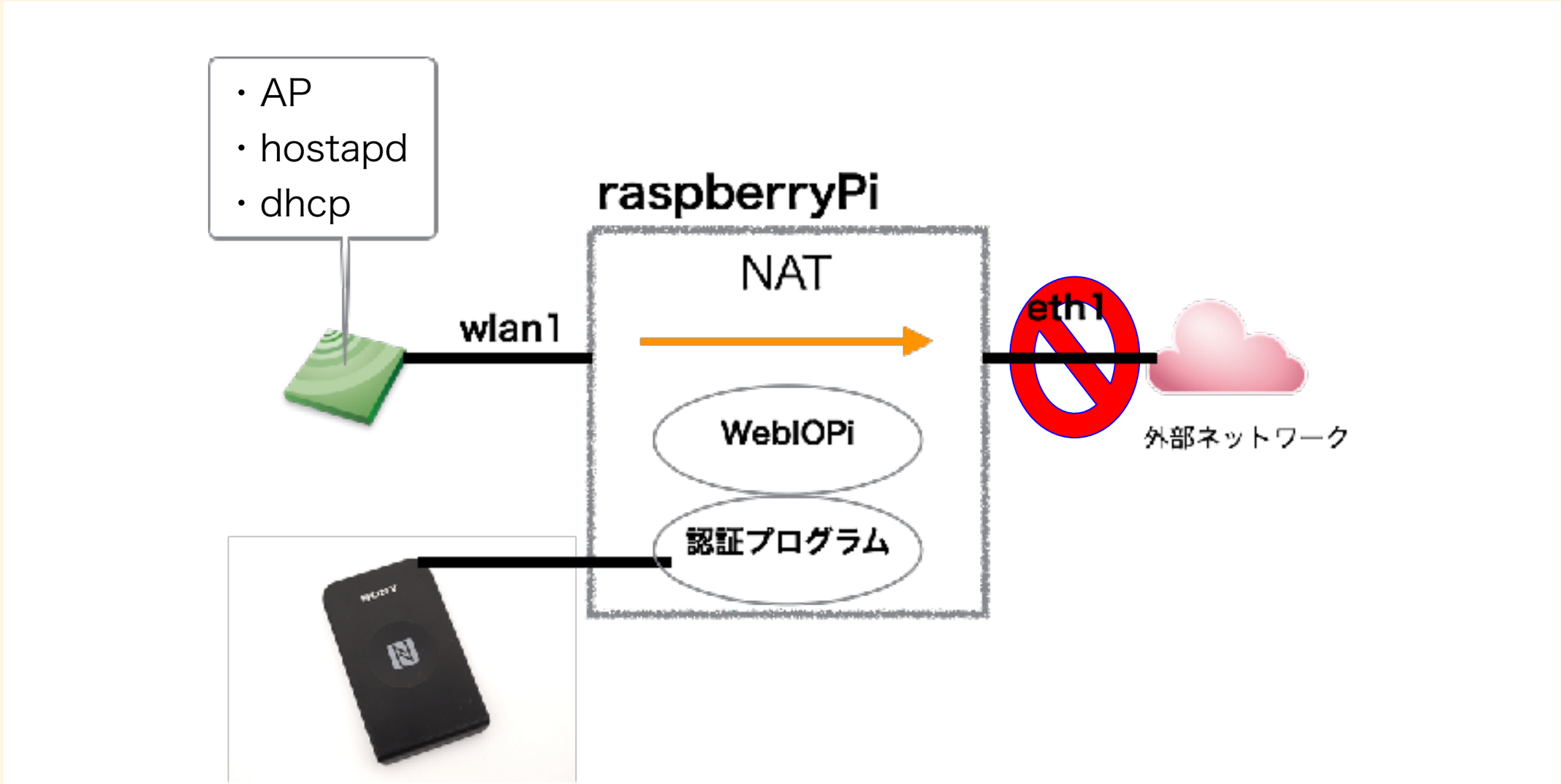
利用技術

- ハード
  - raspberry Pi
  - ICカード
  - PaSoRi
- ソフト
  - raspbian
  - nfcpy
  - WebIOPi
  - hostapd
  - dhcp

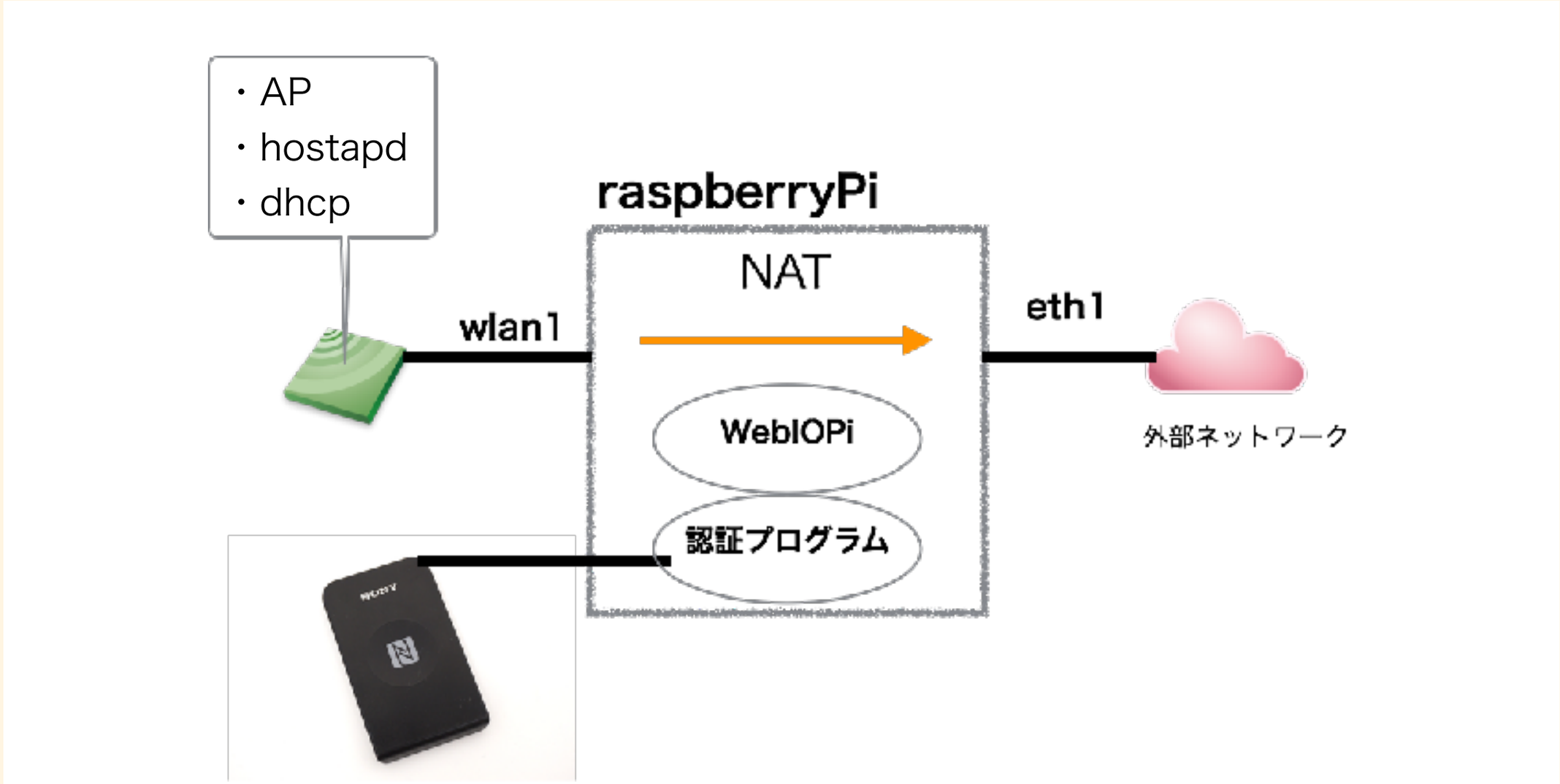
実装済システム


ユーザ
home network認証・制御システム
ICの準備
ICの読み取り
[認証失敗]
Errorをユーザーに通知
[認証成功]
webサーバ起動
インターネットに接続
認証成功をユーザーに通知
home networkへアクセスできることを通知
home networkにアクセス
制御信号を送信

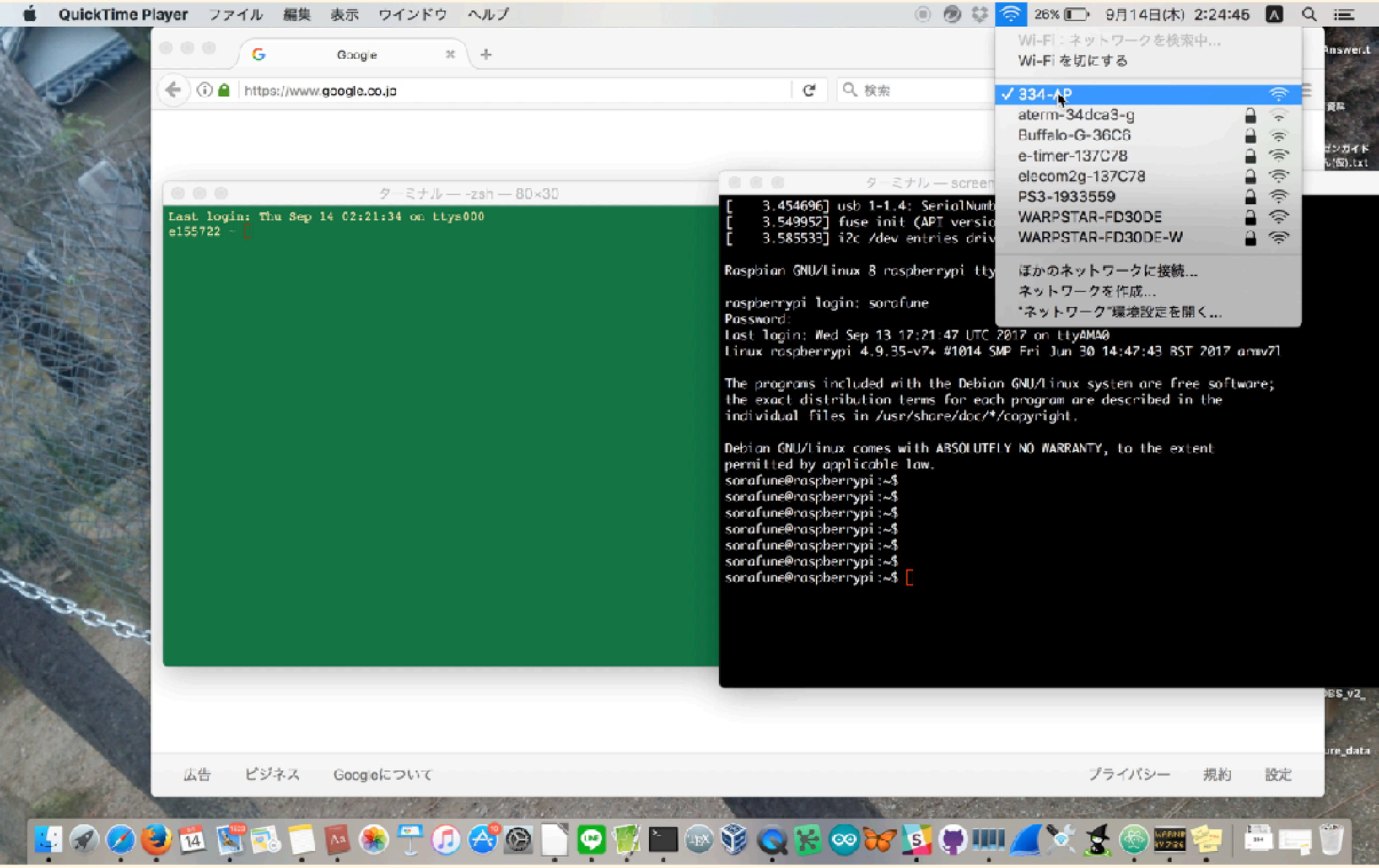
デモ環境


・AP
・hostapd
・dhcp
raspberryPi
NAT
wlan1
eth1
WebIOPi
認証プログラム
外部ネットワーク

デモ環境


・AP
・hostapd
・dhcp
raspberryPi
NAT
wlan1
eth1
WebIOPi
認証プログラム
外部ネットワーク

デモ


QuickTime Player ファイル 編集 表示 ウインドウ ヘルプ
26% 9月14日(木) 2:24:45
Wi-Fi：ネットワークを検索中...
Wi-Fi を切にする
✓ 334-AP
aterm-34dca3-g
Buffalo-G-36C6
e-timer-137C78
elecom2g-137C78
PS3-1933559
WARPSTAR-FD30DE
WARPSTAR-FD30DE-W
ほかのネットワークに接続...
ネットワークを作成...
"ネットワーク"環境設定を開く...
Google
https://www.google.co.jp
検索
ターミナル — -zsh — 80×30
Last login: Thu Sep 14 02:21:34 on ttys000
e155722 ~
ターミナル — screen
[3.454696] usb 1-1.4: SerialNumb
[3.549952] fuse init (API versio
[3.585533] i2c /dev entries driv
Raspbian GNU/Linux 8 raspberrypi tty
raspberrypi login: sorafune
Password:
Last login: Wed Sep 13 17:21:47 UTC 2017 on ttyAMA0
Linux raspberrypi 4.9.35-v7+ #1014 SMP Fri Jun 30 14:47:43 BST 2017 armv7l
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
sorafune@raspberrypi:~$
sorafune@raspberrypi:~$
sorafune@raspberrypi:~$
sorafune@raspberrypi:~$
sorafune@raspberrypi:~$
sorafune@raspberrypi:~$
sorafune@raspberrypi:~$
広告 ビジネス Googleについて
プライバシー 規約 設定

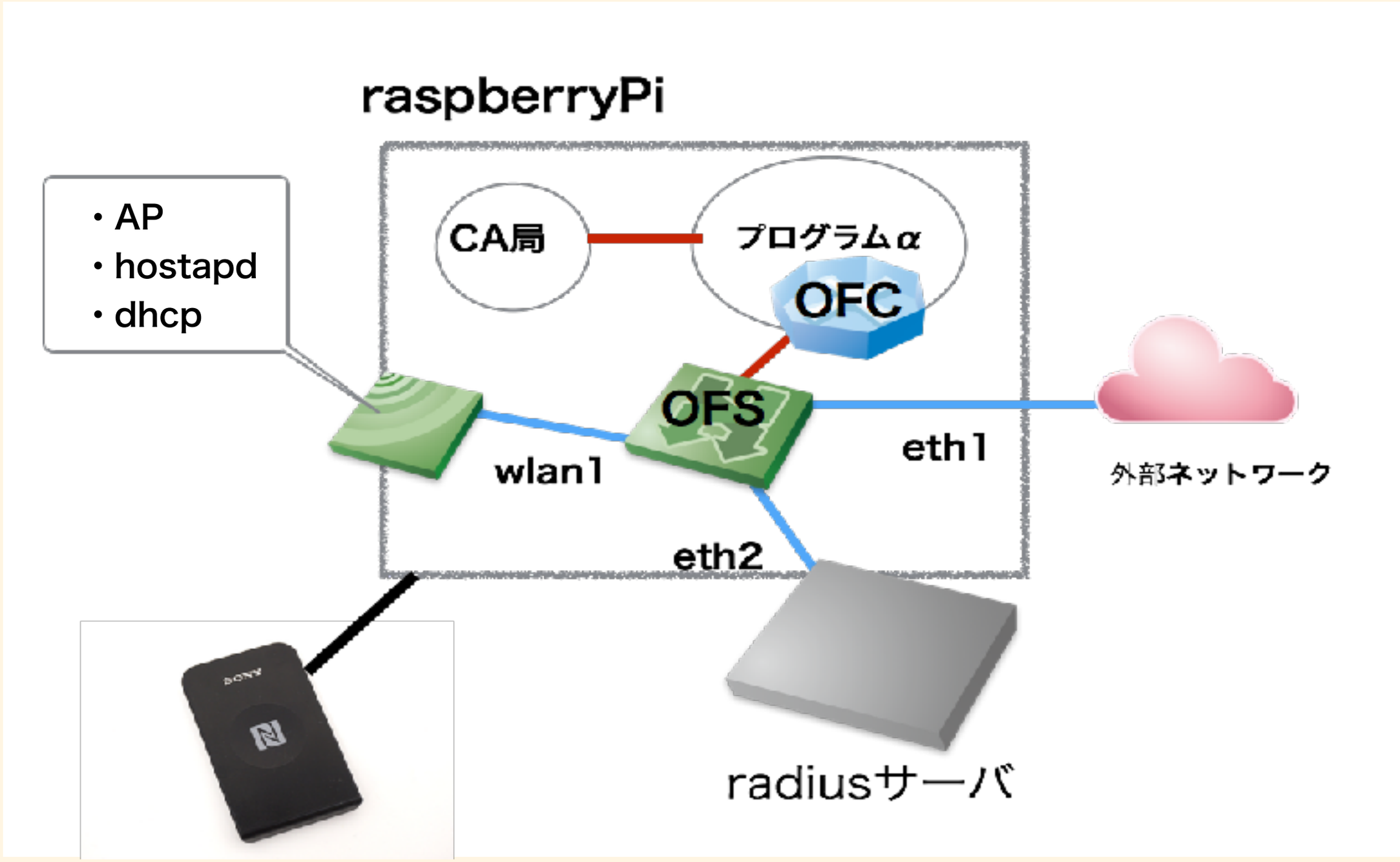
最終イメージ

- IC鍵による認証でホームネットワークを利用可能にする

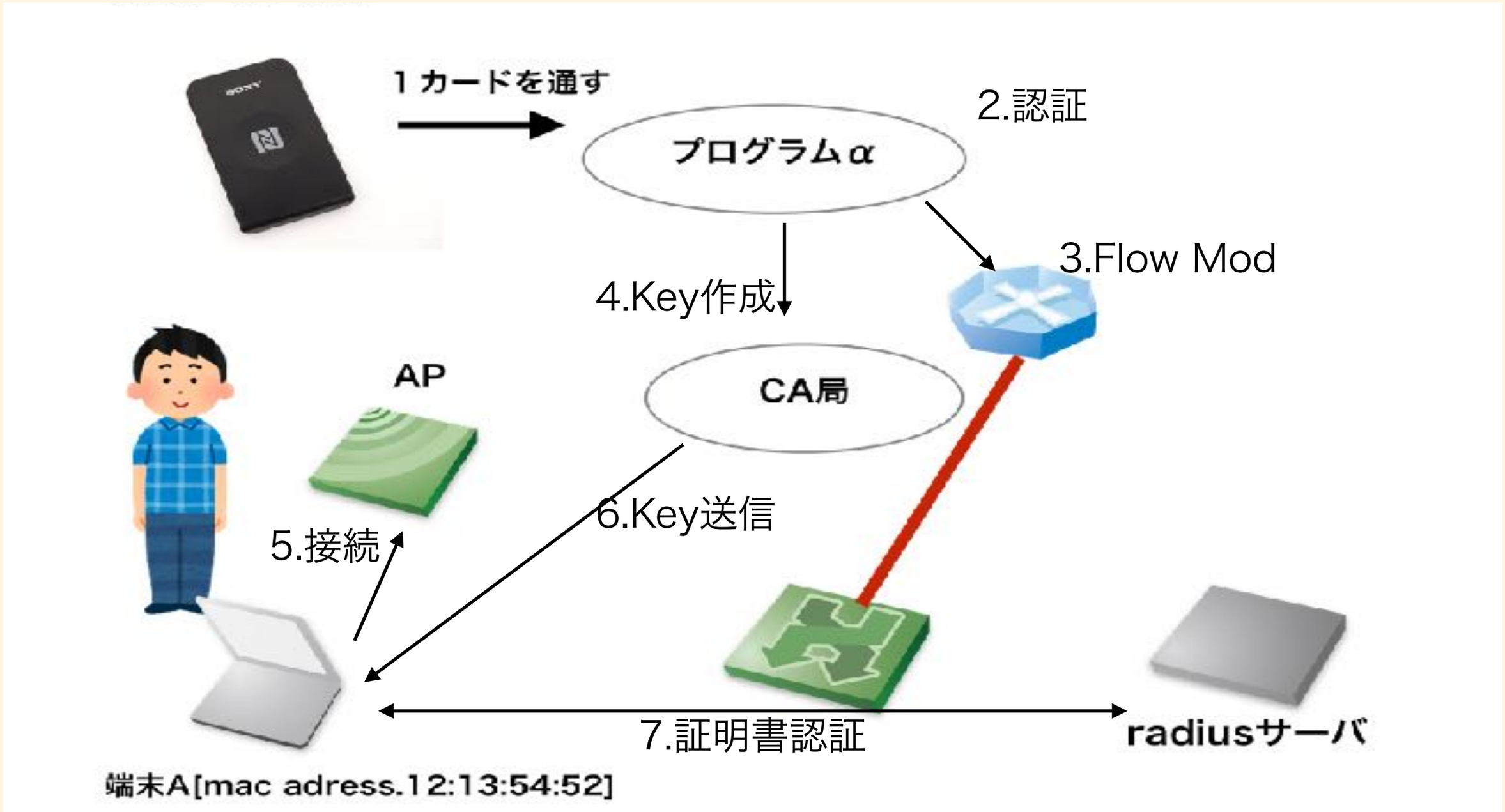
- スマート家電やスマートホーム自体の制御を認証されたデバイスのみからコントロールする

- 特定の認証されたユーザ以外はネットワークを利用できないようにする -> 安全性が確保できる

最終構想図(仮)


raspberryPi
・AP
・hostapd
・dhcp
CA局
プログラムα
OFC
OFS
wlan1
eth1
外部ネットワーク
eth2
radiusサーバ

ホームネットワーク認証手順



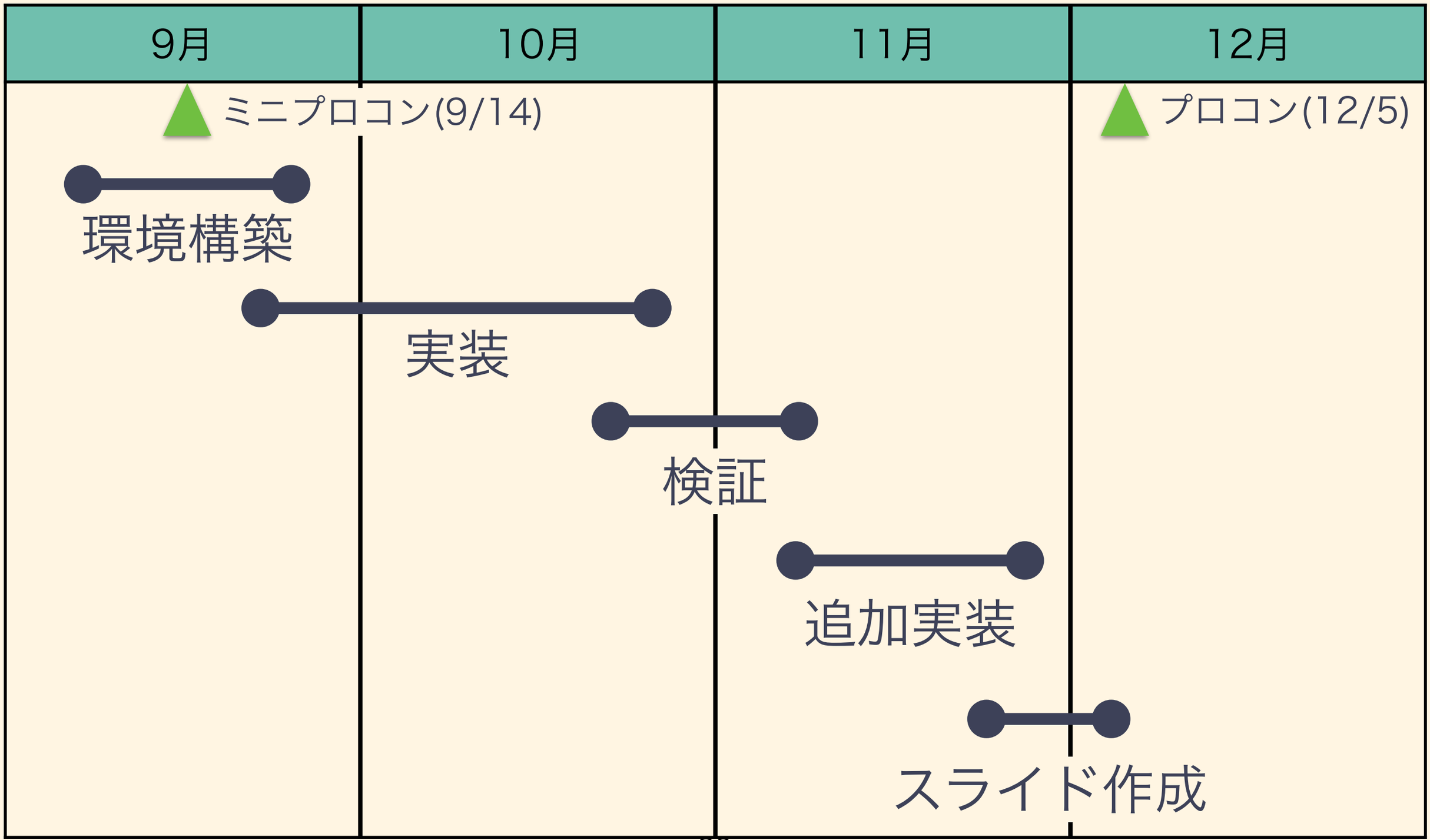
今後考えられるユースケース

- 会社などの社員証のICに導入することで，社員の私物端末によるセキュリティインシデントを低減できる！と考える

- 無料wi-fiスポットに導入することで，現在よりセキュリティが向上したり，怪しい動きをしているマシンをトラッキングできる！

- 学校などで導入することで，ICで出席をとったり，生徒の管理がしやすくなる！出席もICと端末情報をリンクさせることで代返なども防げる！

今後の日程



まとめ

- **今できていること**
  - ICの認証
  - ラズパイのAP化，ラズパイによるインターフェース制御
- **今後の課題**
  - ICカードへの書き込み
  - OpenFlowコントローラーの導入
  - 証明書を使った認証
  - DB等の実装