

# 情報セキュリティ技術

A Technique of Infomation Security

@umisama

とある電子の  
情報防衛

セキュリティ

@umisama

# ■ Agenda

- 自己紹介
- とある電子の情報防衛
- 楽しいを発見する

# ■ 自己紹介

- 茨木 隆彰(うみさま)
- 神戸高専卒業 12年入社
- 好きな街：秋葉原
- 好きな歌手：中島みゆき

# ■ 自己紹介(@OPTiM)

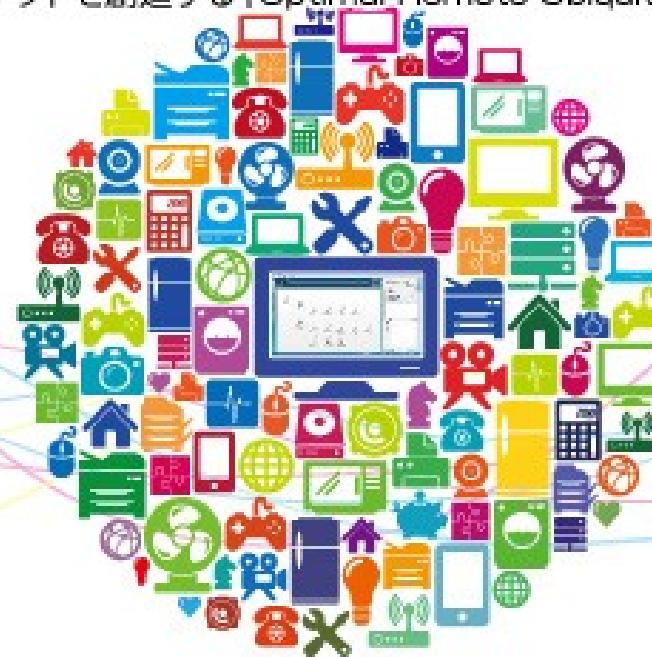


# ■ 自己紹介(@OPTiM)

国内最大1,200万人利用のOptimalRemoteに次世代バージョン誕生

## Optimal Remote Ubiquitous

日本で初めて有償サポートマーケットを創り出したオプティムが  
次のマーケットを創造する「Optimal Remote Ubiquitous」を発表



# ■ 自己紹介(@OPTiM)



フレッツ簡単セットアップツール  
無線設定/ネットワーク検出系



# ■ 自己紹介(@private)

# ■ 自己紹介(@private)



@umisama

うみさま

イケメン高専生

# イケメン高専生？

A large, empty rectangular input field for search queries. To its right is a small microphone icon, indicating the option to use voice search.

Google 検索

I'm Feeling Lucky



イケメン高専生



Google 検索

I'm Feeling Lucky

ウェブ

画像

地図

ショッピング

もっと見る ▾

検索ツール

約 61,900 件 (0.26 秒)

イケメン高専生 の画像検索結果 - 画像を報告うみさま (umisama) on Twitter<https://twitter.com/umisama> ▾

Takaaki IBARAKI / イケメン高専生からイケメンエンジニア(見習い)にジョブチェンジしました。

/ I'm lovin' touching keyboard. a computer engineer. / #kosenconf #spcamp #golang

#xperia. 神戸 - 品川 - fe2o3.jp · 42,198 Tweets · 376 Following · 1,071 ...

「あ、こいつ高専生だな」ってヤツの特徴 - 2ちゃんねる<engawa.2ch.net/test/read.cgi/senmon/1323245719/> ▾

2011/12/07 – 40 :名無し専門学校:2012/01/14(土) 23:04:36.82: 高専ではイケメンがぼっち

になる; 41 :名無し専門 ... 48 :名無し専門学校:2012/01/23(月) 04:10:51.52: バイク買いに

ウェブ

画像

地図

ショッピング

もっと見る ▾

検索ツール

約 61,900 件 (0.26 秒)

イケメン高専生 の画像検索結果 - 画像を報告うみさま (umisama) on Twitter<https://twitter.com/umisama> ▾

Takaaki IBARAKI / イケメン高専生からイケメンエンジニア(見習い)にジョブチェンジしました。

/ I'm lovin' touching keyboard. a computer engineer. / #kosenconf #spcamp #golang

#xperia. 神戸 - 品川 - fe2o3.jp · 42,198 Tweets · 376 Following · 1,071 ...

「あ、こいつ高専生だな」ってヤツの特徴 - 2ちゃんねる<engawa.2ch.net/test/read.cgi/senmon/1323245719/> ▾

2011/12/07 – 40 :名無し専門学校:2012/01/14(土) 23:04:36.82: 高専ではイケメンがぼっち

になる; 41 :名無し専門 ... 48 :名無し専門学校:2012/01/23(月) 04:10:51.52: バイク買いに

# イケメン高専生！

# ■ 自己紹介(@private)

- 遊びに行く
  - セキュリティ・キャンプ
  - 私立プログラミングキャンプ
  - 京都西陣町家スタジオ界隈
  - 高専カンファレンス



# とある電子の 情報が僕 セキュリティ

# とある電子の情報防衛

- Lv0 - Lv5まで
- ジャンルは広く
- 内容は浅めに
- 頑張ってキャラに絡めます

レベル 0





僕の個人的所感といたしましては、  
この女の子は常にお花の女の子の  
スカートを覗いている印象しか無いわけですが  
まあそこそこかわいいのでいいです。

# 覗かれる



物理セキュリティ

# ■ Physical Security

- 覗かれる
- 盜まる
- すり替えられる
- 直接の操作による脆弱性

チラッ

**Optimal  
Biz for Mobile**





あまりにしょうもない？

いえいえ、  
立派な  
セキュリティインシデント



ここで、レベルアップです。



# 橋下 大阪府知事





橋下徹



@t\_ishin



Follow

スマイルプリキュア



Reply



Retweet



Favorite



More

115,854  
RETWEETS

54,454  
FAVORITES



???



橋下徹



@t\_ishin



Follow

すみません。これ、小学校一年生のやんちゃ娘が  
勝手に打ちました。もうツイッター操作できるよう  
になつたんだと少し感動ですが。RT @t\_ishin:  
スマイルプリキュア

Reply Retweet Favorite More

34,006  
RETWEETS

12,864  
FAVORITES





橋下徹



@t\_ishin



Follow

娘が見ていないうちに、携帯のパスコードを変えました。僕の小1の時と比べたら、ほんと進歩しましたね。キーボードを打つことなんてなかったですから。変更後のパスコードは、もちろん妻には申告義務あります。

Reply



Retweet

Favorite

More

3,359

RETWEETS

2,026

FAVORITES





橋下徹



@t\_ishin



Follow

娘が見ていないうちに、携帯のパスコードを変えました。僕の小1の時と比べたら、ほんと進歩しましたね。キーボードを打つことなんてなかったですから。変更後のパスコードは、もちろん妻には申告義務あります。

Reply



Retweet

Favorite

More

3,359

RETWEETS

2,026

FAVORITES



# とある電子の情報防衛

- 後ろの人に注意
  - 覗き見の防止
- 適切なパスコードロック
- パスコードは人に教えない
  - 物理乗っ取りの防止

レベル 1



この人、コンピュータ得意らしいですね。

# ■ Buffer Overflow

- メモリの領域オーバーに  
による脆弱性
- PDFとかWindowsの脆弱  
性はだいたいコレ

# ■ Buffer Overflow

- Cのスタック

Code:

```
Int main() {  
    hoge();
```

前の関数のローカル変数

# ■ Buffer Overflow

## - Cのスタック

Code:

```
Int main() {  
    hoge();
```

ベースポインタ  
(まあ関数ポインタの補助みたいなもん)

呼び出し元関数ポインタ  
(例ではmain()へのポインタ)

前の関数のローカル変数

# ■ Buffer Overflow

## - Cのスタック

Code:

```
void hoge() {  
    int x;  
    int y;
```

ベースポインタ

(まぁ関数ポインタの補助みたいなもん)

呼び出し元関数ポインタ

(例ではmain()へのポインタ)

前の関数のローカル変数

# ■ Buffer Overflow

## - Cのスタック

ローカル変数

(ここでは x と y のこと)

ベースポインタ

(まぁ関数ポインタの補助みたいなもん)

呼び出し元関数ポインタ

(例ではmain()へのポインタ)

前の関数のローカル変数

Code:

```
void hoge() {  
    int x;  
    int y;
```

# ■ Buffer Overflow

## - Cのスタック

ローカル変数

(ここでは x と y のこと)

ベースポインタ

(まぁ関数ポインタの補助みたいなもん)

呼び出し元関数ポインタ

(例ではmain()へのポインタ)

前の関数のローカル変数

Code:

```
void hoge() {
```

~~

```
x++;
```

# ■ Buffer Overflow

## - Cのスタック

ローカル変数

(ここでは x と y のこと)

ベースポインタ

(まぁ関数ポインタの補助みたいなもん)

呼び出し元関数ポインタ

(例ではmain()へのポインタ)

前の関数のローカル変数

Code:

```
void hoge() {
```

~~

```
return;
```

```
}
```

# ■ Buffer Overflow

## - Cのスタック

Code:

```
Int main() {  
    hoge();
```

呼び出し元関数ポインタ  
(例ではmain()へのポインタ)

前の関数のローカル変数

# ■ Buffer Overflow

- Cのスタック

Code:

```
Int main() {  
    hoge();
```

呼び出し元関数ポインタ  
(例ではmain()へのポインタ)

前の関数のローカル変数

# ■ Buffer Overflow

- Cのスタック

Code:

```
Int main() {  
    Hoge();  
~ここから~
```

前の関数のローカル変数

# ■ Buffer Overflow

## - 実演します

- スタックの構造を見てみます。
- スタック破壊をやってみます。
- ココに任意のアドレスを仕込むと…

# とある電子の情報防衛

- 気をつけよう
  - Cで実装する事があれば
- どちらかと言えば
  - “こういう事がある”ことを  
知っておくことが重要

# レベル2



(そろそろキャラクター  
に引っ掛けるの疲れて  
きた)

# ■ Directory Traversal

- 意図しない所が見える
  - ディレクトリのバリデーションチェックが十分でないと発生する
  - サーバマシンの内容がイロイロ見えてしまうことがある。

# ■ Directory Traversal

- 実演します。
  - Directory Traversalが起こるサーバーを書いてきました。
  - コレは簡単なのでエクスプロイド成立まで見せられます。

# とある電子の情報防衛

- 気をつけよう
  - Webサーバを実装するときに
- どちらかと言えば
  - “こういう事がある”ことを  
知っておくことが重要

# レベル3

## (ry

ココですでに午前2時、僕はねむい。

レベル 4



ストーカーのイメージしかない

# ■ Social Hacking

- SNSなどの書き込みから  
情報を探定すること
- 住所や居場所、名前、  
趣向など

# 僕の家を特定します

# ■ ある日のつぶやき

6月11日 午後8時9分



うみさま

@umisama

帰ります。

View translation

Reply Delete Favorite More

# ■ ある日のつぶやき

## - 手持ちの情報

- うみさまはオプティムで働いている
- 8時9分に会社を出た

# ■ ある日のつぶやき

6月11日 午後8時43分



うみさま

@umisama

すた丼旨かったなー。

 View translation

 Reply  Delete  Favorite  More

8:43 PM - 11 Jun 13

# ■ ある日のつぶやき

## - 手持ちの情報

- うみさまはオプティムで働いている
- 8時9分に会社を出た
- それから34分ですた丼を食べ終わる

# Google Maps

# 「すた丼」



**食事10分**

**移動時間24分**







- 渋谷駅
- 秋葉原駅
- 御茶ノ水駅
- 品川駅

# ■ ある日のつぶやき

6月11日 午後8時48分



うみさま  
@umisama

すた丼、見ると食べたくなるんだよなあ。

View translation

Reply Delete Favorite More

8:48 PM - 11 Jun 13

「見ると食べたくなる」

→帰りに見かける所

→帰り道に店がある

# ■ ある日のつぶやき

## - 手持ちの情報

- うみさまはオプティムで働いている
- 8時9分に会社を出た
- それから34分ですた丼を食べ終わる
- すた丼は帰り道

# アキバ・御茶ノ水



# 渋谷駅周辺



# 品川駅周辺



# ■ ある日のつぶやき

## - 手持ちの情報

- うみさまはオプティムで働いている
- 8時9分に会社を出た
- それから34分ですた丼を食べ終わる
- すた丼は帰り道（最寄りは品川・渋谷？）

# ■ ある日のつぶやき

6月11日 午後8時54分



うみさま

@umisama

微妙に雨に当たりながらも、傘を差さずに帰宅で  
きた。

View translation

Reply Delete Favorite More

8:54 PM - 11 Jun 13

# ■ ある日のつぶやき

6月11日 午後8時54分



うみさま

@umisama

微妙に雨に当たりながらも、傘を差さずに帰宅できた。

View translation

Reply Delete Favorite More

8:54 PM - 11 Jun 13

雨は降っているが  
傘をささなくて良い程度  
0.5mm – 1.0mm





**最寄り駅は  
品川駅だ！！！**

# ■ ある日のつぶやき

## - 手持ちの情報

- うみさまはオプティムで働いている
- 8時9分に会社を出た
- それから34分ですた丼を食べ終わる
- すた丼は帰り道（最寄りは品川駅）

# ■ ある日のつぶやき

6月11日 午後8時54分



うみさま

@umisama

微妙に雨に当たりながらも、傘を差さずに帰宅できた。

View translation

Reply Delete Favorite More

8:54 PM - 11 Jun 13

# ■ ある日のつぶやき

6月11日 午後8時54分



うみさま

@umisama

微妙に雨に当たりながらも、傘を差さずに帰宅で  
きた。

View translation

Reply Delete Favorite More

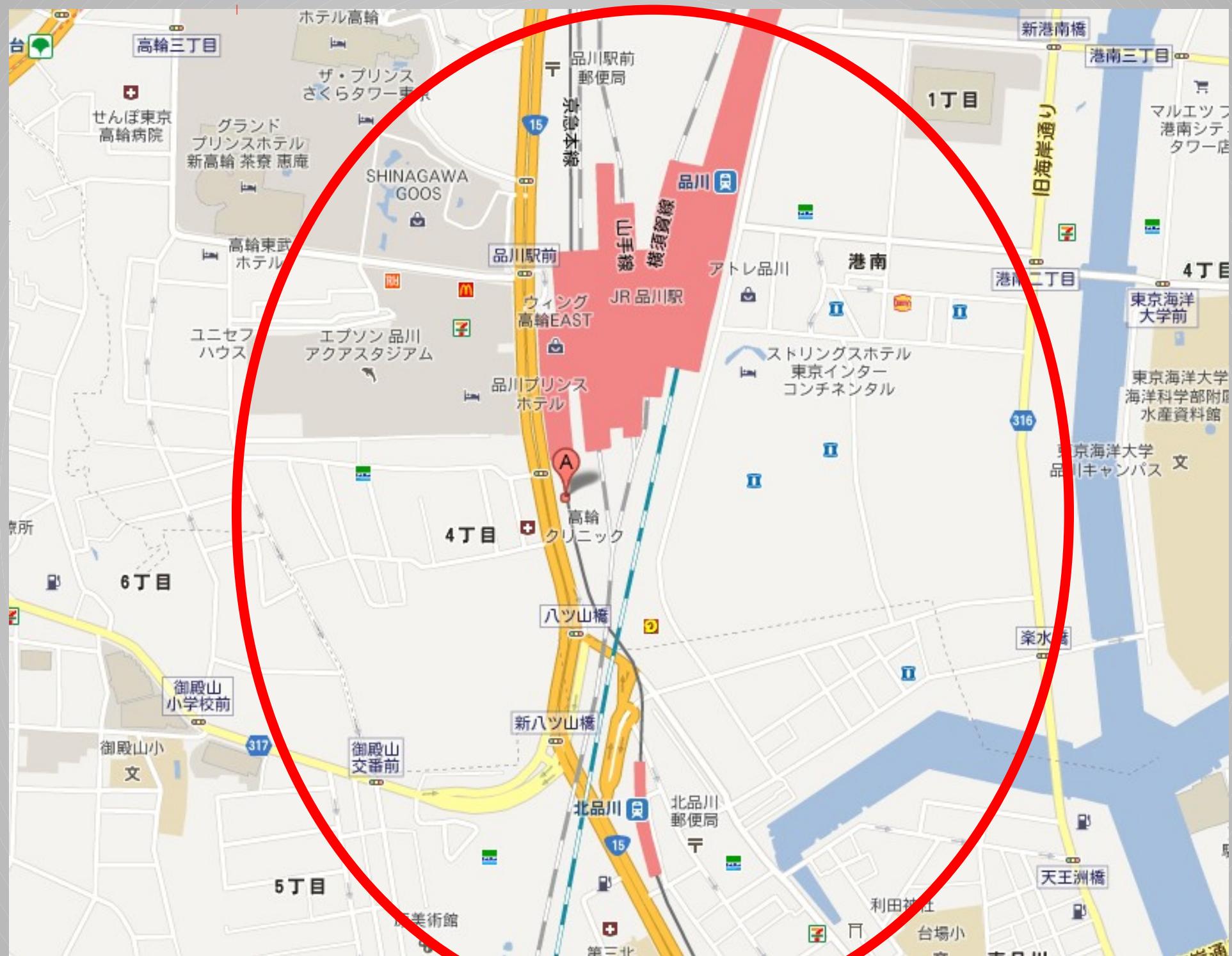
8:54 PM - 11 Jun 13

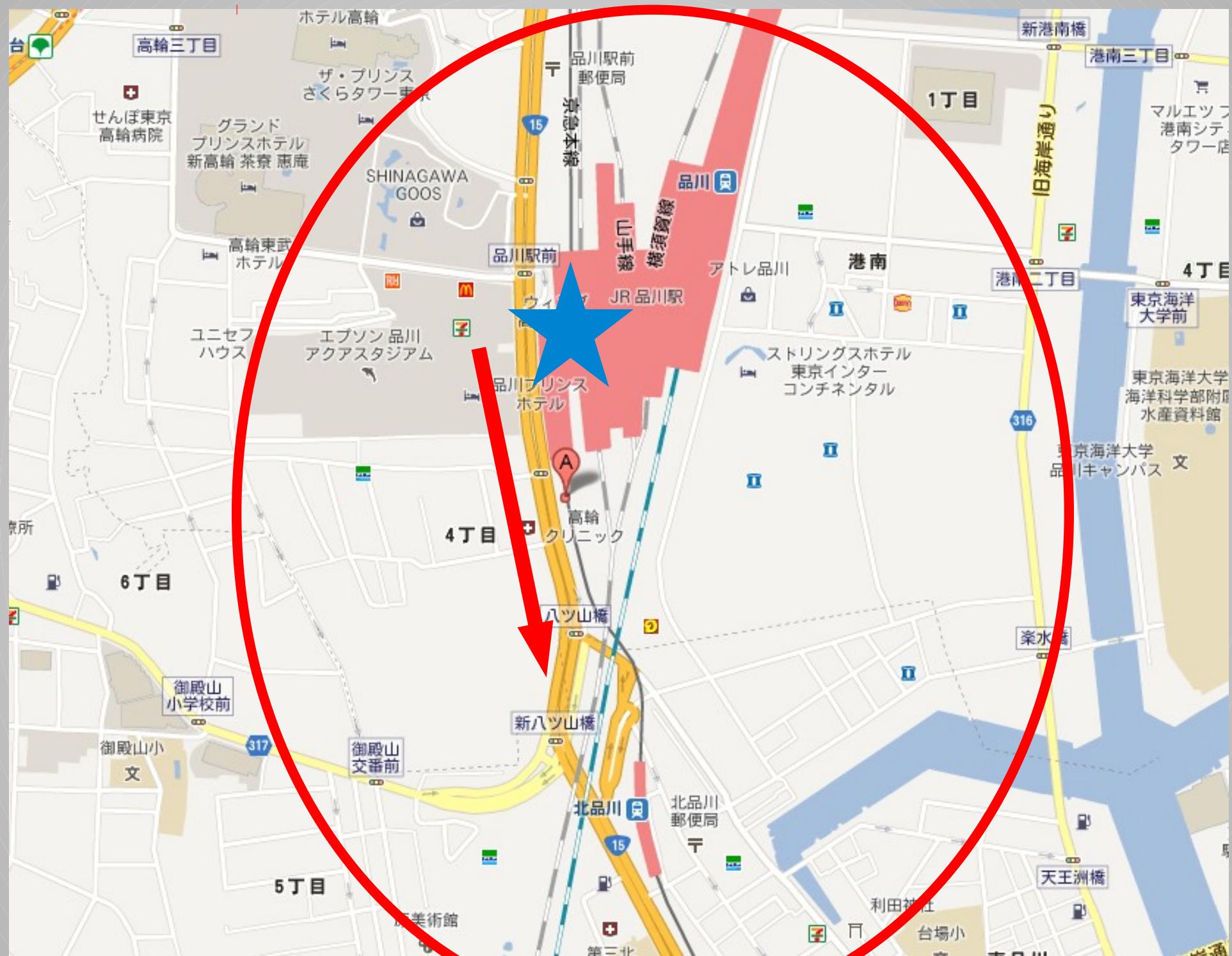
# ■ ある日のつぶやき

## - 手持ちの情報

- うみさまはオプティムで働いている
- 8時9分に会社を出た
- それから34分ですた丼を食べ終わる
- すた丼は帰り道（最寄りは品川駅）
- すた丼->家は11分







すた丼が  
通り道にならない



すた丼が  
通り道にならない

プリンスホテル  
と  
高級住宅街



# すた丼が 通り道にならない

プリンスホテル  
と  
高級住宅街

オフィス  
が中心

経路1 早 安 楽

定期券

22:13発 → 22:34着

所要時間 21分 乗車時間 8分 乗換 2回 総額 300円 距離 4.3km

印刷 テキスト

経路	乗車位置	運賃	指定席/料金	距離
■ 北品川	2番線発		<a href="#">路線図</a> <a href="#">時刻表</a> <a href="#">地図</a> <a href="#">グルメ</a> <a href="#">ホテル</a>	
22:13-22:15 2分	私 京急本線(品川行)		130円	0.7km
(5分)	品川		<a href="#">路線図</a> <a href="#">構内図</a> <a href="#">時刻表</a> <a href="#">地図</a> <a href="#">グルメ</a>	
22:20-22:22 2分	私 京急本線エアポート(印旛日本医大行)	前／8号車	↓	1.2km
(1分)	泉岳寺《直通》	4番線着	<a href="#">路線図</a> <a href="#">時刻表</a> <a href="#">地図</a> <a href="#">グルメ</a>	
22:23-22:24 1分	地 都営浅草線(印旛日本医大行)		170円	1.1km
(7分)	三田(東京)	2番線着 4番線発	<a href="#">路線図</a> <a href="#">構内図</a> <a href="#">時刻表</a> <a href="#">地図</a> <a href="#">グルメ</a>	
22:31-22:34 3分	地 都営三田線(西高島平行)	1・3・6号車	↓	1.3km
	■ 御成門	2番線着	<a href="#">路線図</a> <a href="#">地図</a> <a href="#">グルメ</a> <a href="#">ホテル</a>	

空路有効期間:2013年6月1日~2013年7月31日

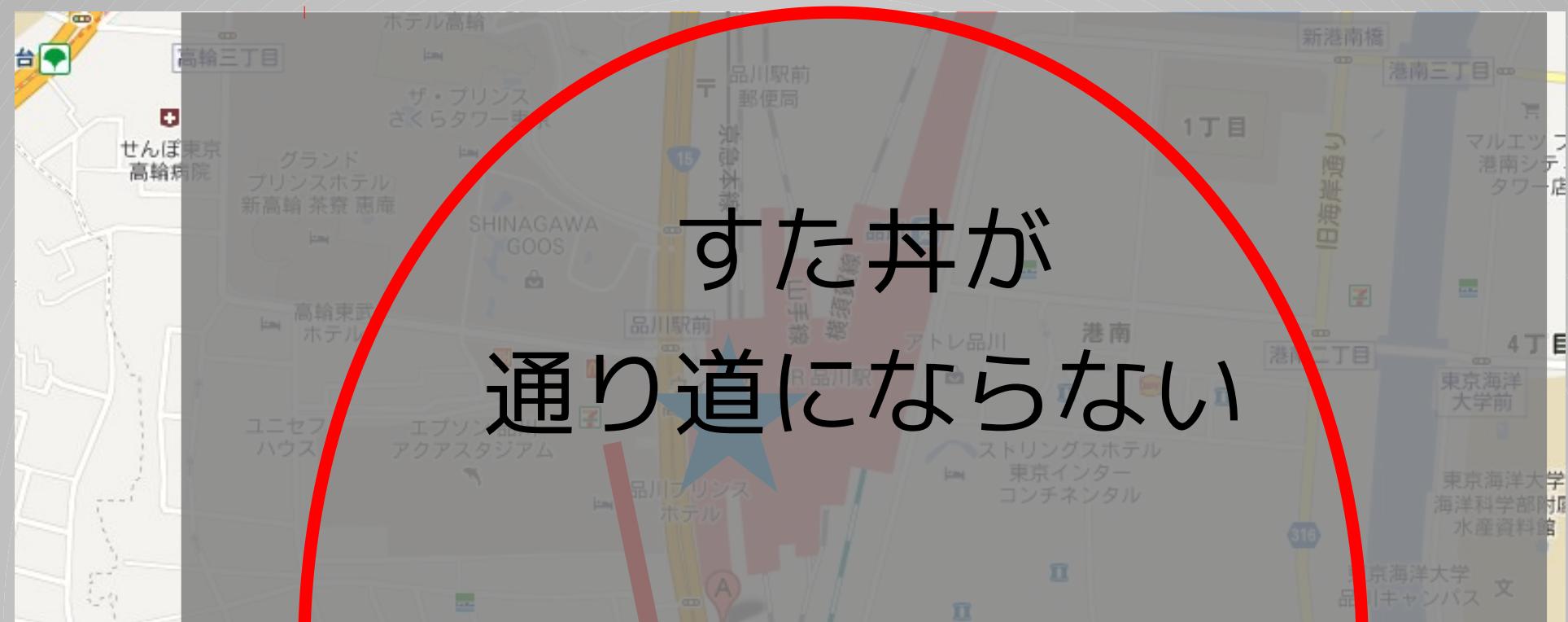
条件変更

すた丼が  
通り道にならない

プリンスホテル  
と  
高級住宅街

オフィス  
が中心

最寄りが  
品川にならない

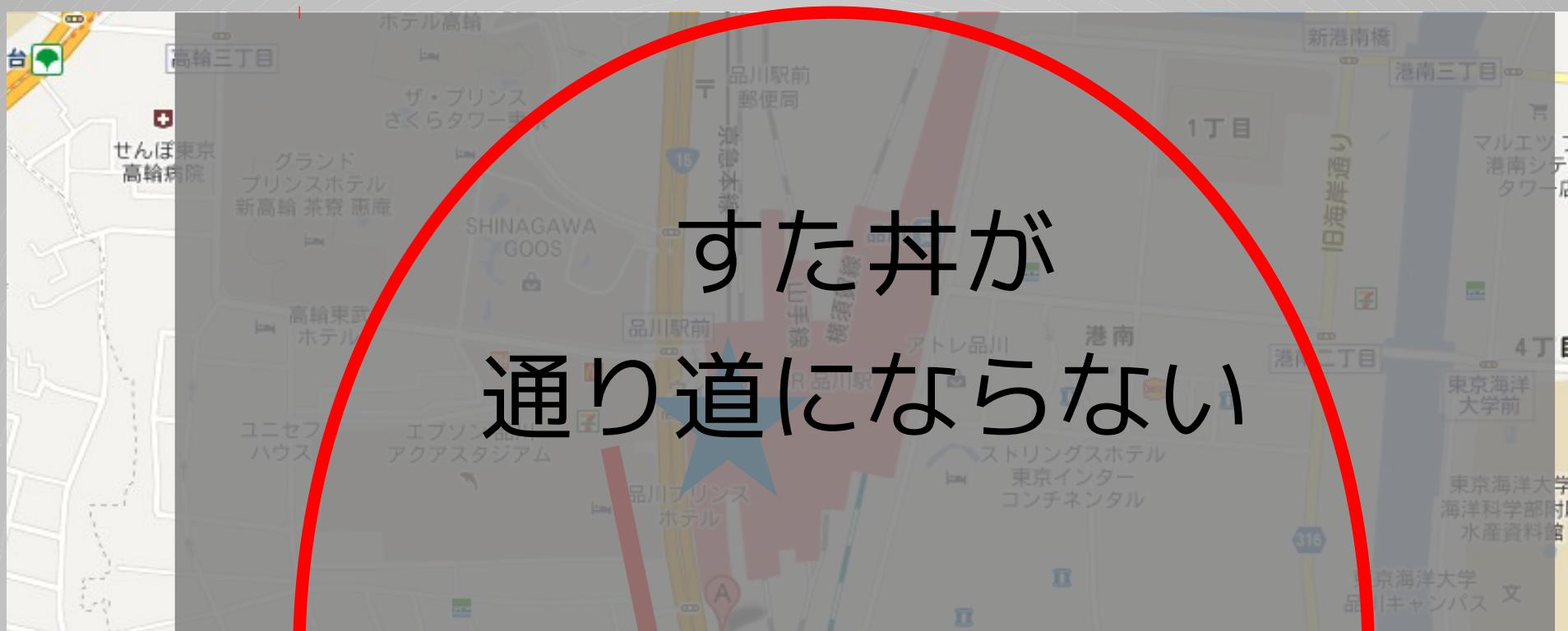


すた丼が  
通り道にならない

プリンスホテル  
と  
高級住宅街

オフィス  
が中心

最寄りが  
品川にならない



# 結構わかってしまう

# とある電子の情報防衛

- SNSの使い方
  - 発言から何が引き出せる？
  - しゃべりすぎてないか？
- 守る情報、守らない情報
  - 何がバレるとまずいのか？

# レベル 5



**最強っぽいやつにします。**

# Cross Site Scripting

- 任意のページで任意のスクリプトを実行
- 入力フォームに細工をする

# Cross Site Scripting

- 実演します。
  - なんかXSSが出来るサーバ作って来ました。
  - これでXSSがどう動くのか見ましょう。

# とある電子の情報防衛

- 気をつけよう
  - Webを実装することができれば
- どちらかというと
  - “こういう事があり得る”ことを知っておくと役立つ

(毎度これやな)

# ■ その他の技術

- CSRF
  - Cross Site Request Forgeries
  - あるリクエストを送信するように細工されたページ
  - 掲示板の書き込みが強制できるなど

# ■ その他の技術

## - 遠隔操作

- 多くのOSにはコマンドを実行する能力がある
- これを遠隔地から操作して対象を意図したように制御する

# Messages

僕だって高い所から言えた身分じゃないけれど  
やれって言われたからやります

# 楽しいを発見をしよう

こういう場で  
楽しく語れる  
「好き」を見つけよう

どんな  
エンジニアも  
多分「好き」を  
エネルギーに出来る

それは貴方の学科の

「情報工学」

じゃないかもしない

「楽しい」と「好き」  
を見つけて、従順に  
エンジニアをやろう

