世界のセキュリティコミュニティ

その入り込み方と重要性について

日本電信電話株式会社
中島明日香

whoami

中島 明日香（なかじま あすか）

@AsuNa_jp　https://www.kun0ichi.net/

- サイバーセキュリティ研究者 @ NTT
  - 研究分野：脆弱性発見・対策、IoTセキュリテイ
- CTF for GIRLS 発起人&代表
  - 2014年設立 / 日本初の女性セキュリティコミュニティ

CTF for GIRLS

- 著書『サイバー攻撃 ネット世界の裏側で起きていること』
  - 講談社 ブルーバックス、2018年1月発売 / 発行部数約2万部

- 国際会議 BlackHatUSA/Asiaにてプログラム委員（査読）
  - 情報セキュリティ分野における世界トップレベル産業系国際会議（採択率10%前後）

本日のテーマ（再掲）

世界のセキュリティコミュニティの入り方

なぜ私がこのテーマを話すのか？（1/2）

過去5年位、国外で様々な研究活動やコミュニティ活動などしてきた

国際会議の委員や共同研究/発表

- ❖ 国際会議委員
  - ○ BlackHatUSA（米国）
  - ○ BlackHatAsia（シンガポール）
  - ○ IEEE WOOT（米国）
  - ○ Blue Hat Shanghai（中国）
- ❖ 海外での研究/発表/講義など
  - ○ 米カーネギーメロン大学
  - ○ 台湾/韓国の女性コミュニティ
  - ○ インドの女性コミュニティ
  - ○ 台湾政府主催の人材育成プログラム
  - ○ 国際会議で閉会時基調講演

なぜ私がこのテーマを話すのか？（2/2）

過去5年位、国外で様々な研究活動やコミュニティ活動などしてきた

発表などで訪れた国(都市) と回数

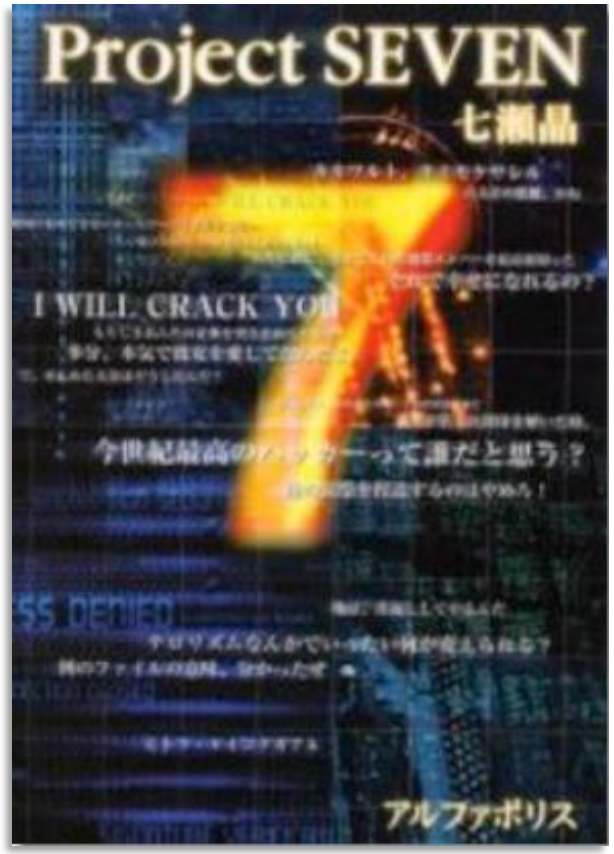
- 米国（ラスベガス/ピッツバーグ）5回
- シンガポール　3回
- 台湾（台北/台中/高雄）　2回
- ロシア（モスクワ）　1回
- ドイツ（ダグスツール）　1回
- イギリス（ロンドン）　1回
- フィリピン（タガイタイ）　1回
- ニュージーランド（オークランド）1回
- 中国（上海）　1回
- カナダ（バンクーバー）　1回

世界のセキュリティコミュニティの一員になる為の知見が提供出来るのでは？

ここに至るまでの背景と道のり

セキュリティ技術者/研究者を志した経緯

切っ掛けは14歳の時ハッカーが主人公の小説を読んだ事



女子高生ハッカーと天才プログラマーが
サイバーテロリストから世界を救う話 🕮

「パソコン一つで世界を転覆出来るし、
救う事も出来るんだ！すごいカッコいい！」

そんなカッコいい人に私もなりたい！
という漠然とした憧れからスタート

『Project SEVEN』七瀬晶著, アルファポリス, 2005年10月発売

学生時代

独学でスタート ＆ 大学でもセキュリティの研究/外部活動を

活動例

- ❖ 大学の研究室に入学4日目に入る
- ❖ セキュリティ・キャンプに参加
- ❖ 各種大会に参加（CTF/MWS/Hardening）
- ❖ 各種企業のインターン/アルバイトに参加

※ 具体的な活動内容に関しては2014年に江戸前セキュリティ勉強会にて発表
https://www.slideshare.net/asukanakajima9/10-48968684

社会人になってから何を成したいのか？

原点を思い起こすと‥

社会人になってから何を成したいのか？

原点を思い起こすと‥

ハッカーと呼ばれるような人になって、世界/社会を広く良い方向に変える

社会人になってから何を成したいのか？

原点を思い起こすと‥

目標①

目標②

ハッカーと呼ばれるような人になって、世界/社会を広く良い方向に変える

目標1: ハッカーと呼ばれるような人とは？

私自身が目標逆算型の人間のため、目標の具体化が必要であった

目標1: ハッカーと呼ばれるような人とは？

私自身が目標逆算型の人間のため、目標の具体化が必要であった

目標1: ハッカーと呼ばれるような人とは？

私自身が目標逆算型の人間のため、目標の具体化が必要であった

目標1: ハッカーと呼ばれるような人とは？

私自身が目標逆算型の人間のため、目標の具体化が必要であった

目標1: ハッカーと呼ばれるような人とは？

私自身が目標逆算型の人間のため、目標の具体化が必要であった

目標1: ハッカーと呼ばれるような人とは？

著名ハッカー系(産業系)国際会議

後はcccとかも有名

目標1: ハッカーと呼ばれるような人とは？

著名ハッカー系(産業系)国際会議

どちらに採択されてもカッコいい！
が、BlackHatを選択

後はcccとかも有名

BlackHatとは？

概要

特にUSAが

- 世界最高峰のセキュリティ分野での産業系国際会議
- 年に3回各地で開催
  - BlackHatUSA（米ラスベガス）/ 参加者は2万人
  - BlackHatEurope(英ロンドン)
  - BlackHatAsia(シンガポール)

採択率は10%台。特にUSAは10%切ることも。

BlackHatとは？

概要

特にUSAが

- 世界最高峰のセキュリティ分野での産業系国際会議
- 年に3回各地で開催
  - BlackHatUSA（米ラスベガス）/ 参加者は2万人
  - BlackHatEurope(英ロンドン)
  - BlackHatAsia(シンガポール)

どれかには通ればいいなぁ・・

目標2: 世界/社会を広く良い方向に変える

世界/社会を広く良い方向に変えられるもの(研究)とは？

ソフトウェアの脆弱性発見・対策

目標2: 世界/社会を広く良い方向に変える

世界/社会を広く良い方向に変えられるもの(研究)とは？

ソフトウェアの脆弱性発見・対策

何百万人/何億人が利用している著名ソフトウェアの
脆弱性を発見/対策することができれば目標と合致する

社会人になってから何を成したいのか？

原点を思い起こすと‥

目標①

目標②

ハッカーと呼ばれるような人になって、世界/社会を広く良い方向に変える

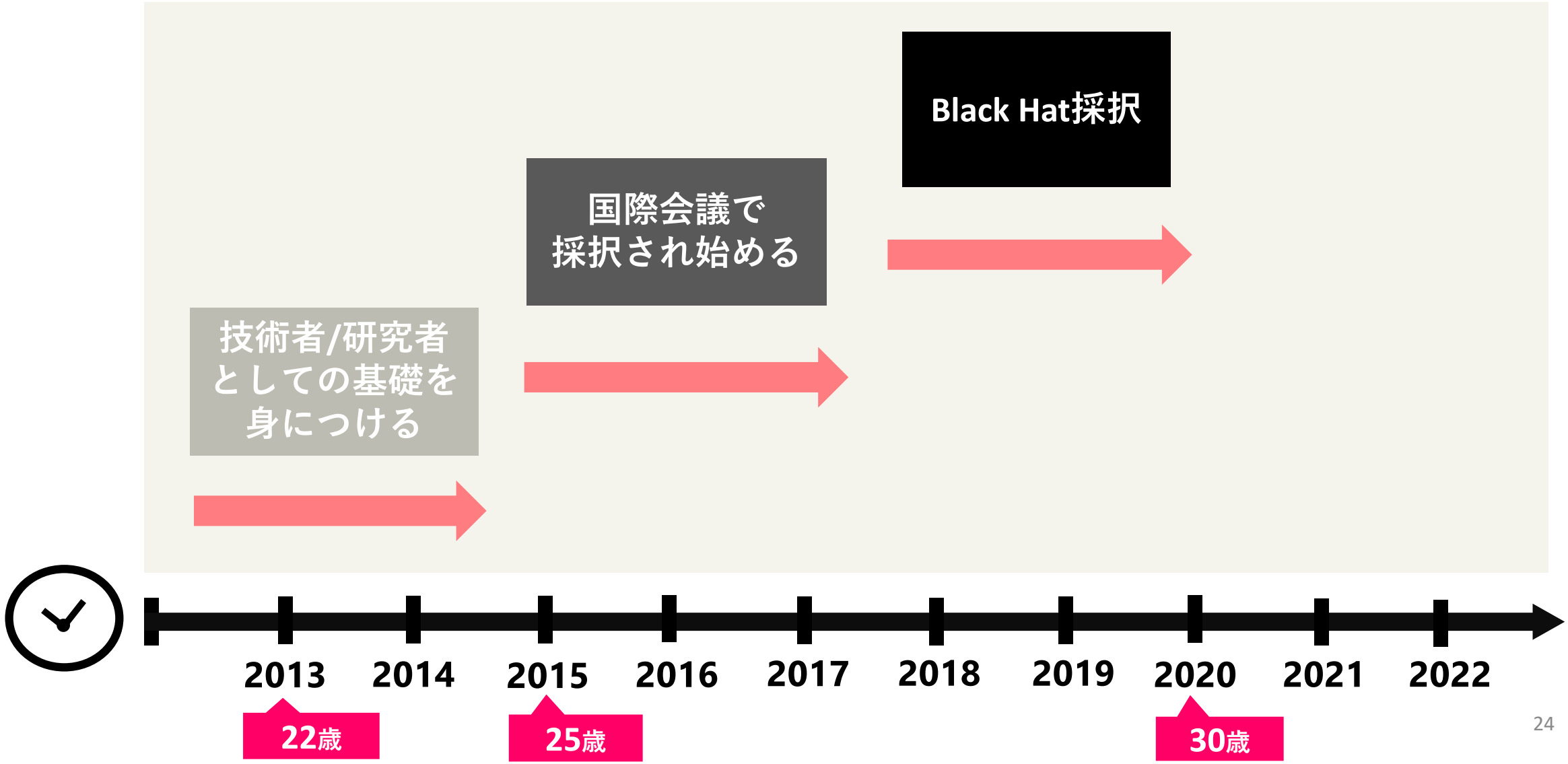
具体的な目標案

ハッカー系カンファレンスで著名な BlackHat に 30歳までに

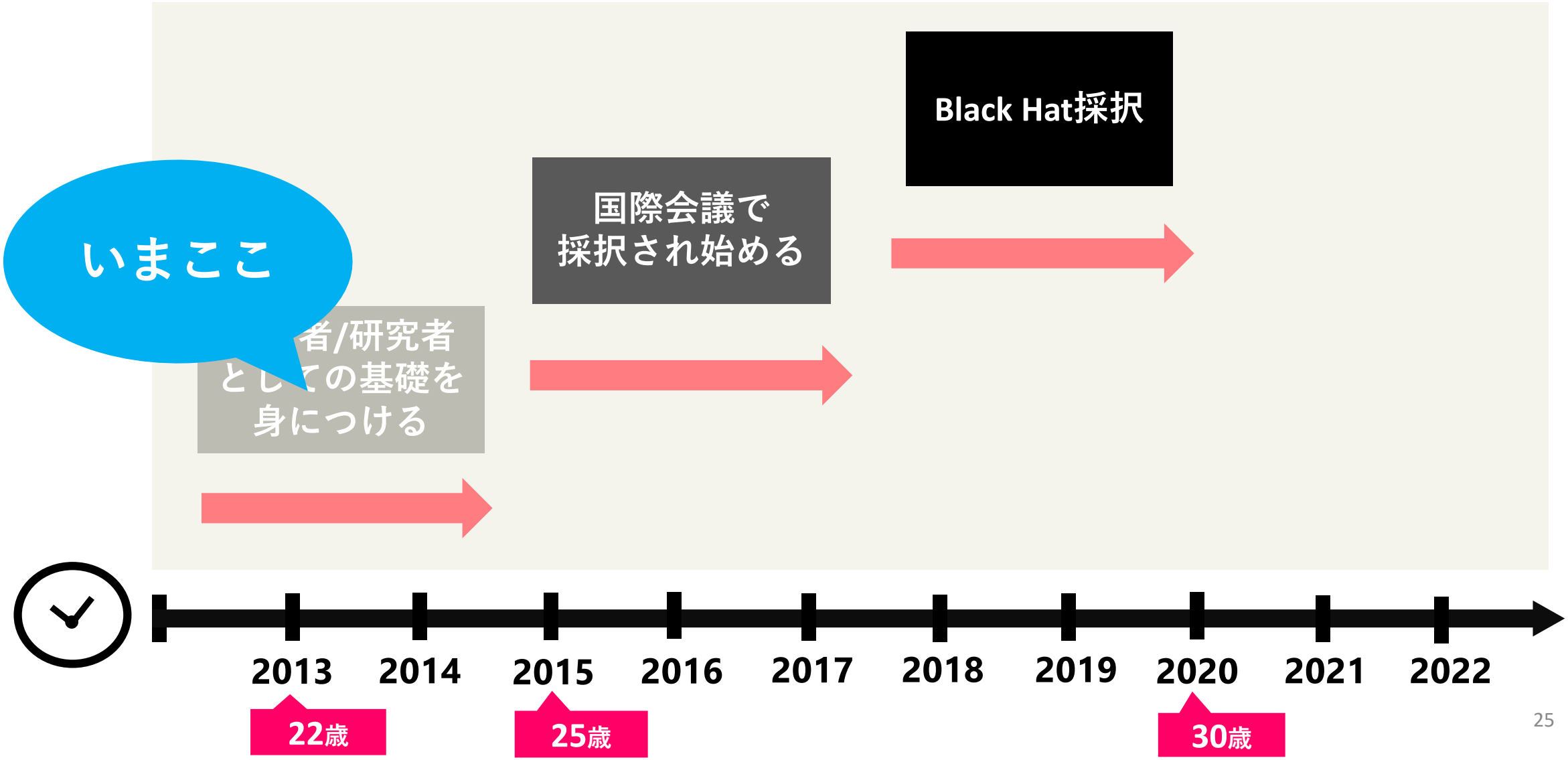
採択/発表(①) し、その研究 or それまでに得られた知見を通じて

社会を広く良い方向に変える(②)

社会人になりたての私の10年計画

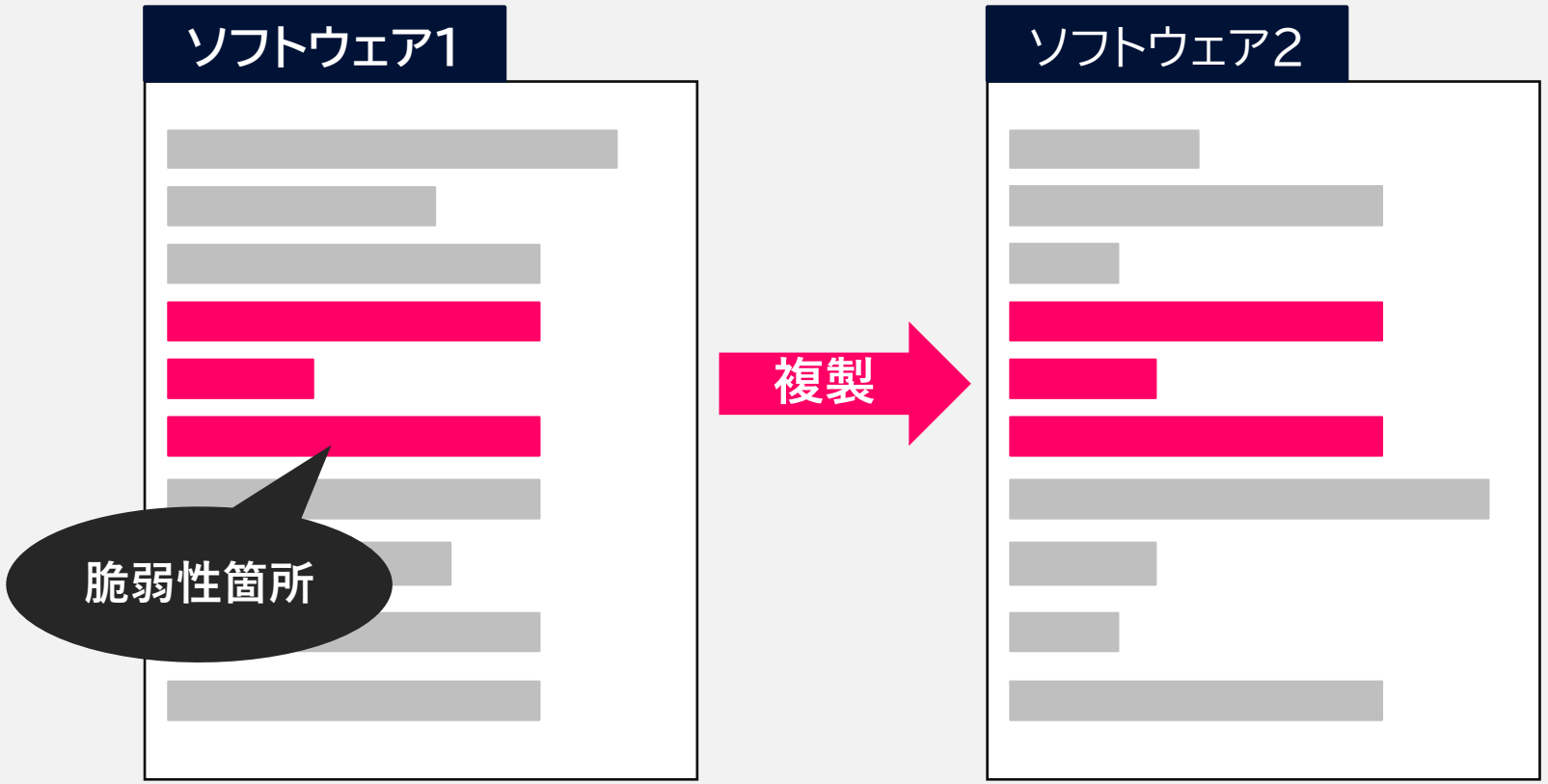


社会人になりたての私の10年計画



最初の研究テーマ: コードクローンの脆弱性発見

コードクローンの脆弱性とは



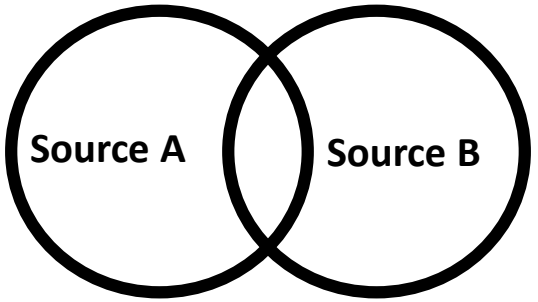
何らかの理由で他のソフトウェアに複製された脆弱性のこと

コードクローンの脆弱性が発生する理由

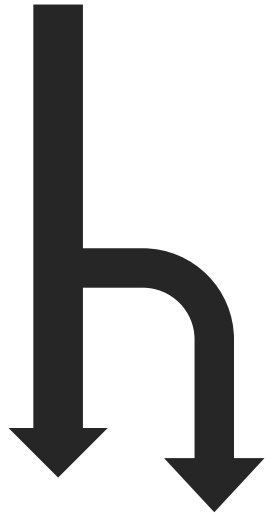
コピー & ペースト

Ctrl + C
Ctrl + V

ソースコード共有

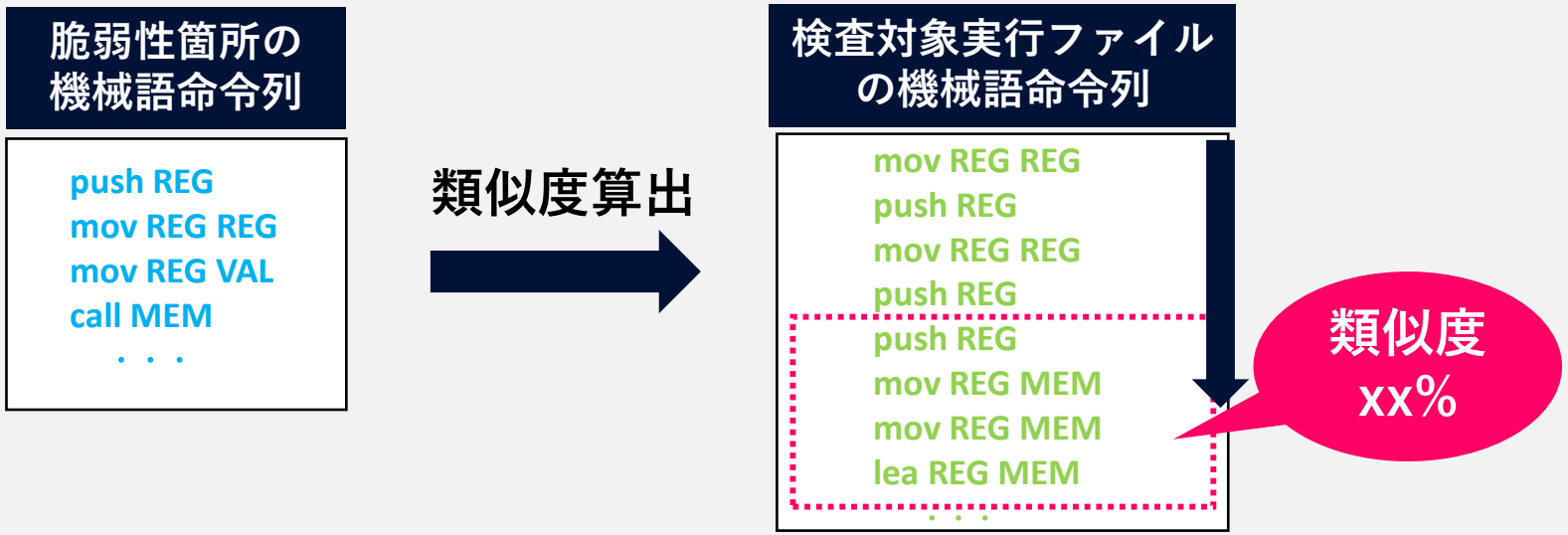


プロジェクトのフォーク



提案手法(概要)

機械語命令間の類似度を、類似文字列検索アルゴリズムを
用いて算出する事で複製された脆弱性を発見する手法を提案

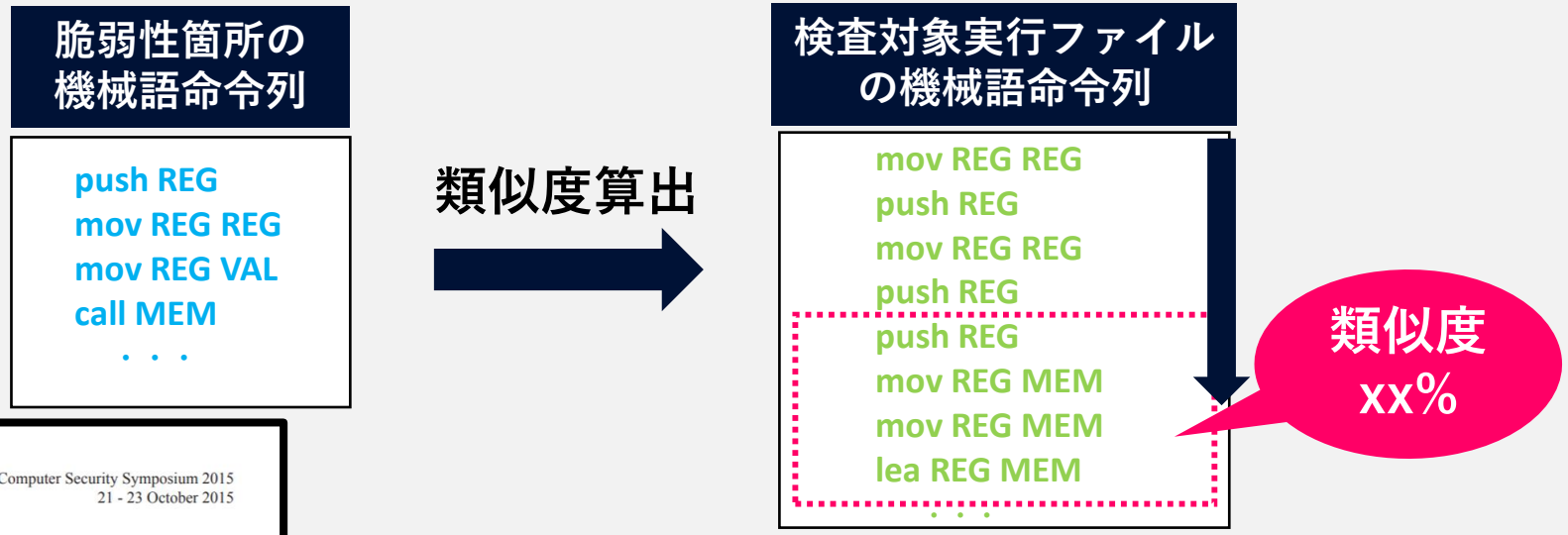


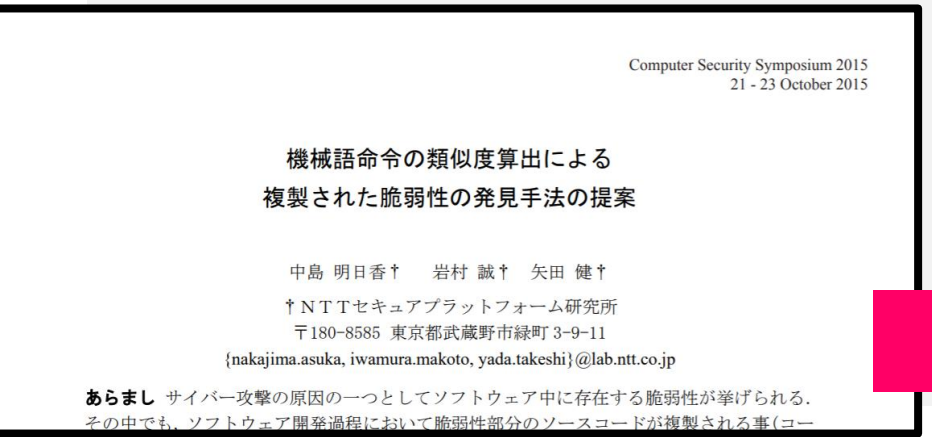
■ 提案手法の流れ

1.逆アセンブル・正規化 → 2.類似度算出 → 3.脆弱性有無の判定

提案手法(概要)

機械語命令間の類似度を、類似文字列検索アルゴリズムを
用いて算出する事で複製された脆弱性を発見する手法を提案





Computer Security Symposium 2015
21 - 23 October 2015

機械語命令の類似度算出による
複製された脆弱性の発見手法の提案

中島 明日香† 岩村 誠† 矢田 健†
†NTTセキュアプラットフォーム研究所
〒180-8585 東京都武蔵野市緑町 3-9-11
{nakajima.asuka, iwamura.makoto, yada.takeshi}@lab.ntt.co.jp

あらまし サイバー攻撃の原因の一つとしてソフトウェア中に存在する脆弱性が挙げられる．
その中でも，ソフトウェア開発過程において脆弱性部分のソースコードが複製される事(コー

手法の提案まではCSS2015でも発表

研究成果

実際にWindowsで未修正の脆弱性箇所を発見する！

- CVE-2015-1789（OpenSSLの脆弱性）
  - ［オリジナル］libeay32.dll ［複製先］JunosPulseVpnBg.dl
  - 元々PulseClientに存在していた脆弱性。それがWindowsにも組み込まれていた

“Windows In-Box Junos Pulse Client (VPN Client)”

※“Microsoft Windows 8.1 introduced Junos Pulse client as part of the Windows operating system. (Microsoft calls this an “in-box” application.)”

https://www.juniper.net/techpubs/software/pulse/guides/j-pulse-windows-inbox-client-qsg.pdf

CVE-2015-1789（OpenSSL）

複製元(オリジナル)

```
text:11071B40                   public X509_cmp_time
text:11071B40 X509_cmp_time     proc near               ; CODE XREF: sub_
text:11071B40                                           ; sub_11071E90+8A
text:11071B40
text:11071B40 var_44            = dword ptr -44h
text:11071B40 var_40            = dword ptr -40h
text:11071B40 var_3C            = dword ptr -3Ch
text:11071B40 var_34            = dword ptr -34h
text:11071B40 var_30            = dword ptr -30h
text:11071B40 var_2C            = dword ptr -2Ch
text:11071B40 var_28            = byte ptr -28h
text:11071B40 var_1C            = byte ptr -1Ch
text:11071B40 var_1B            = byte ptr -1Bh
text:11071B40 var_4             = dword ptr -4
text:11071B40 arg_0             = dword ptr  4
text:11071B40 arg_4             = dword ptr  8
text:11071B40
text:11071B40                   mov     eax, 44h
text:11071B45                   call    __alloca_probe
text:11071B4A                   mov     eax, ___security_cookie
text:11071B4F                   xor     eax, esp
text:11071B51                   mov     [esp+44h+var_4], eax
text:11071B55                   push    ebp
text:11071B56                   mov     ebp, [esp+48h+arg_4]
text:11071B5A                   push    esi
text:11071B5B                   mov     esi, [esp+4Ch+arg_0]
text:11071B5F                   mov     ecx, [esi]
text:11071B61                   mov     eax, [esi+8]
text:11071B64                   push    edi
text:11071B65                   mov     edi, [esi+4]
text:11071B68                   cmp     edi, 17h
text:11071B6B                   jnz     short loc_11071BA8
text:11071B6D                   add     ecx, 0FFFFFFF5h
text:11071B70                   cmp     ecx, 6
text:11071B73                   ja      short loc_11071B94
text:11071B75                   mov     ecx, [eax]
text:11071B77                   mov     edx, [eax+4]
text:11071B7A                   mov     [esp+50h+var_34], ecx
text:11071B7E                   mov     cx, [eax+8]
text:11071B82                   mov     word ptr [esp+50h+var_2C], cx
```

複製先

```
.text:1009D790
.text:1009D790 sub_1009D790     proc near               ; CODE XREF: sub_1
.text:1009D790                                          ; sub_1009E090+62↓
.text:1009D790
.text:1009D790 var_44           = dword ptr -44h
.text:1009D790 var_40           = dword ptr -40h
.text:1009D790 var_3C           = dword ptr -3Ch
.text:1009D790 var_38           = dword ptr -38h
.text:1009D790 var_34           = qword ptr -34h
.text:1009D790 var_2C           = dword ptr -2Ch
.text:1009D790 var_28           = byte ptr -28h
.text:1009D790 var_1C           = byte ptr -1Ch
.text:1009D790 var_1B           = byte ptr -1Bh
.text:1009D790 var_4            = dword ptr -4
.text:1009D790 arg_0            = dword ptr  4
.text:1009D790 arg_4            = dword ptr  8
.text:1009D790
.text:1009D790                  mov     eax, 44h
.text:1009D795                  call    __alloca_p
.text:1009D79A                  mov     eax, ___se
.text:1009D79F                  xor     eax, esp
.text:1009D7A1                  mov     [esp+44h+var_4], eax
.text:1009D7A5                  push    ebp
.text:1009D7A6                  mov     ebp, [esp+48h+arg_4]
.text:1009D7AA                  push    esi
.text:1009D7AB                  mov     esi, [esp+4Ch+arg_0]
.text:1009D7AF                  push    edi
.text:1009D7B0                  mov     edi, [esi+4]
.text:1009D7B3                  mov     ecx, [esi]
.text:1009D7B5                  mov     eax, [esi+8]
.text:1009D7B8                  cmp     edi, 17h
.text:1009D7BB                  jnz     short loc_1009D7EF
.text:1009D7BD                  add     ecx, 0FFFFFFF5h
.text:1009D7C0                  cmp     ecx, 6
.text:1009D7C3                  ja      short loc_1009D7DB
.text:1009D7C5                  mov     cx, [eax+8]
.text:1009D7C9                  lea     edx, [esp+50h+var_2C+2]
.text:1009D7CD                  movq    xmm0, qword ptr [eax]
```

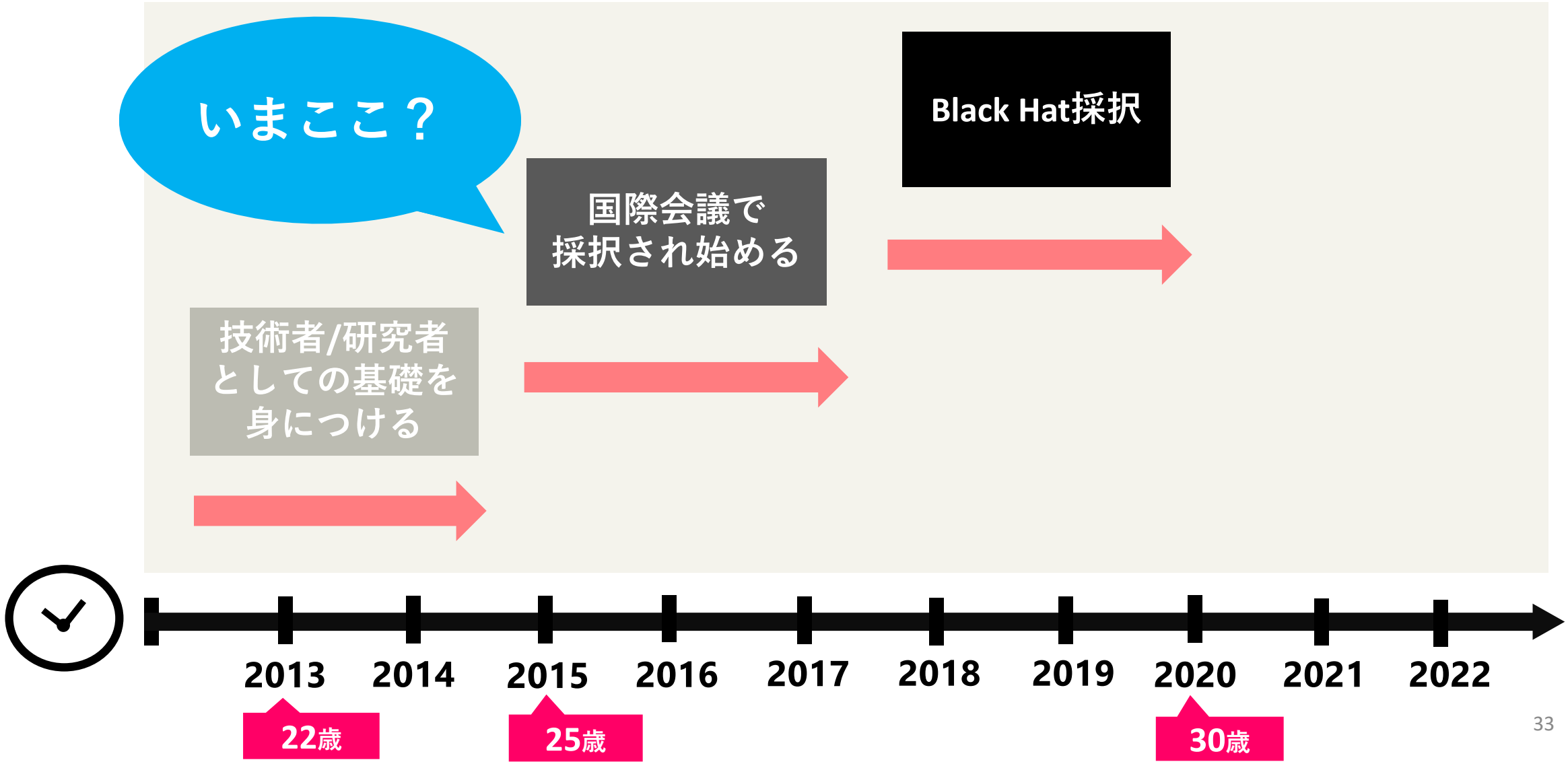
ほぼ同じ！！

CVE-2015-1789（OpenSSL）

- 脆弱性修正のタイムライン

複製先の脆弱性の修正までに２ヶ月が生じていた

社会人になりたての私の10年計画（再掲）



U25 Track

CODEBLUE 2015 投稿

日本国内の産業系国際会議

U25 Track

CODEBLUE 2015 投稿

Reject!!

日本国内の産業系国際会議

投稿は2015年10月頃

BlackHatAsia 2016 投稿

シンガポールの産業系国際会議

投稿は2015年10月頃

BlackHatAsia 2016 投稿

Reject!!

シンガポールの産業系国際会議

そのまま2016年に本格突入

こんなはずじゃ無かったのに・・・

自分にいったい何が足りないのか？

ハッカー系の会議（産業系会議）は査読コメントが返ってこない

ハッカー系の会議（産業系会議）は査読コメントが返ってこない

英語力？

ハッカー系の会議（産業系会議）は査読コメントが返ってこない

英語力？

さらに手法の有効性
を評価するべき？

ハッカー系の会議（産業系会議）は査読コメントが返ってこない

英語力？

研究テーマ？

さらに手法の有効性
を評価するべき？

ハッカー系の会議（産業系会議）は査読コメントが返ってこない

英語力？

研究テーマ？

さらに手法の有効性
を評価するべき？

当時日本で産業系会議に詳しい人は一握り
五里霧中状態になる

結論

わからない

個人的な戦略

行き詰った時は
自分の行動パターンを変える

（余談）キャリア形成論

- ❖ 目標逆算型
- ❖ 偶然活用形

計画的偶発理論

成功した人のキャリア形成の
きっかけの8割が偶然によるもの

↓

その偶然を計画的に設計するのが大事

基本的には計画的だが、
行き詰まった時は偶発性に任せる

最初の一歩

まずは何でも良いから海外との接点を作る

SECCON決勝大会が2016年1月末開催

- 海外からの参加
  - 米国
  - 韓国
  - 台湾
  - タイ
  - ベトナム
  - ロシア
  - ルーマニア

交流会に積極的に参加して観光ガイド役も引き受ける

交流会にて（一日観光ツアー）

ロシアチームのメンバと雑談にて

ロシア

中島

交流会にて（一日観光ツアー）

ロシアチームのメンバと雑談にて

ロシア

何の仕事しているの？

中島

交流会にて（一日観光ツアー）

ロシアチームのメンバと雑談にて

ロシア

何の仕事しているの？

中島

セキュリティの研究開発！
最近の研究は～

交流会にて（一日観光ツアー）

ロシアチームのメンバと雑談にて

ロシア

何の仕事しているの？

結構面白いことしてるね！

中島

セキュリティの研究開発！
最近の研究は～

交流会にて（一日観光ツアー）

ロシアチームのメンバと雑談にて

ロシア

何の仕事しているの？

結構面白いことしてるね！

中島

セキュリティの研究開発！
最近の研究は～

いやぁ、中々研究が採択されなくって

交流会にて（一日観光ツアー）

ロシアチームのメンバと雑談にて

ロシア

何の仕事しているの？

結構面白いことしてるね！

その研究、PHDaysだったら
採択されるよ！

中島

セキュリティの研究開発！
最近の研究は～

いやぁ、中々研究が採択されなくって

交流会にて（一日観光ツアー）

ロシアチームのメンバと雑談にて

ロシア

何の仕事しているの？

結構面白いことしてるね！

その研究、PHDaysだったら
採択されるよ！

中島

セキュリティの研究開発！
最近の研究は～

いやぁ、中々研究が採択されなくって

え？あのPositive Hack Daysに？？

Positive Hack Days とは

PHDaysの特徴

- ロシア最大級の産業系会議
  - 主催者: Positive Technologies
  - 開催地はモスクワ
- 2019年の参加者は8000人とのこと
- JPCERT/CCブログでもおすすめ会議として掲載
  - https://blogs.jpcert.or.jp/ja/2020/05/security_conference.html
- 名物は「2drunk2hack」
  - Web系コンテストで(たしか)ハッキングに失敗したら、強いお酒を飲む競技

PositiveHackDays
2016 投稿

PositiveHackDays

2016 投稿

Accept!!

PHDaysにて発表（2016年6月）

https://www.slideshare.net/phdays/ss-62579634

めでたし、めでたし

が、これだけでは
終わらなかった

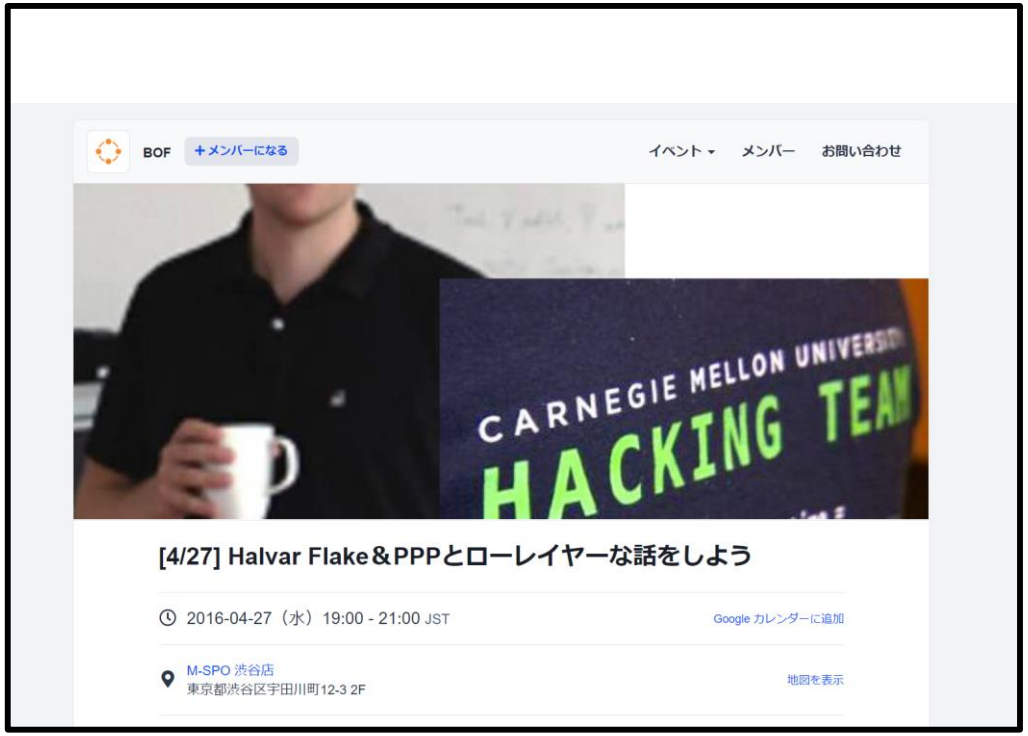
?!

最初の一歩（その2）

まずは何でも良いから海外との接点を作る

著名な海外エンジニアとの交流会が４月に

- PPP（米国のCTFチーム）
- Halver Flake
  - バイナリ差分解析ツールBinDiffの開発者



https://7bd76f3e7d0cf6c4962c0a8da8.doorkeeper.jp/events/43029

主催の篠田佳奈さんに感謝

飲み会にて(二次会？)

Halver Flakeさんと雑談にて(うろ覚え)

Halver Flake

中島

私もバイナリ間の類似度を算出するような研究してるんですよ！
今度PHDaysでも発表予定です！

飲み会にて(二次会？)

Halver Flakeさんと雑談にて(うろ覚え)

Halver Flake

へぇどんな？

中島

私もバイナリ間の類似度を算出するような研究してるんですよ！
今度PHDaysでも発表予定です！

飲み会にて(二次会？)

Halver Flakeさんと雑談にて(うろ覚え)

Halver Flake

へぇどんな？

中島

私もバイナリ間の類似度を算出するような研究してるんですよ！
今度PHDaysでも発表予定です！

(すかさずパソコンとスライドを取り出して説明)
ちなみにBinDiffよりも良い結果がでるケースもあります！

飲み会にて(二次会？)

Halver Flakeさんと雑談にて(うろ覚え)

Halver Flake

へぇどんな？

おぉー、中々面白いねー！

中島

私もバイナリ間の類似度を算出するような研究してるんですよ！
今度PHDaysでも発表予定です！

(すかさずパソコンとスライドを取り出して説明)
ちなみにBinDiffよりも良い結果がでるケースもあります！

飲み会にて(二次会？)

Halver Flakeさんと雑談にて(うろ覚え)

Halver Flake

へぇどんな？

おぉー、中々面白いねー！

後で考えたらHalver Flakeさんに
喧嘩売ってたような？と若干反省

中島

私もバイナリ間の類似度を算出するような研究してるんですよ！
今度PHDaysでも発表予定です！

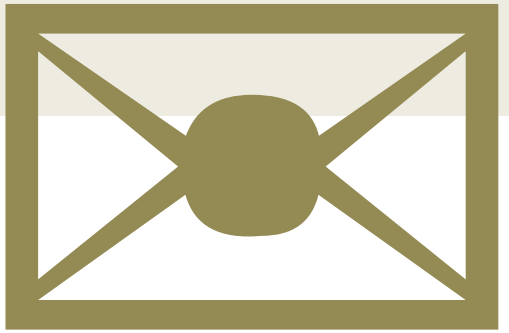
(すかさずパソコンとスライドを取り出して説明)
ちなみにBinDiffよりも良い結果がでるケースもあります！

1年後・・

2017年某日

奇妙な招待状が届く

Dagstuhl Seminarへの招待状



なにそれ・・？

Dagstuhl Seminarとは

国立情報学研究所(NII)広報誌から一部抜粋
https://www.nii.ac.jp/userdata/results/pr_data/NII_Today/47/2-3.pdf

特徴

- 1980年代からドイツのDagstuhlで毎週行われる国際集会
- 世界トップクラスの情報学者が参加し、Open Problem(未解決問題)について議論する、一週間の合宿形式セミナー
- あのdblpを管理している団体が主導

Halver Flakeさんが、マルウェア解析を
テーマにしたセミナーを主催
世界中から著名技術者/研究者約40名が招待

Dagstuhl Seminarにて

- バイナリ間の類似度算出の論文を30本以上読み、体系的に整理して発表。皆のディスカッションのネタに
- 休憩時間には交流しつつ研究議論
- ビリヤードで遊んだり、ピクニックも

この交流をきっかけに、
後々につながる様々な繋がりが持てた

さらなるチャンスも舞い込んだ

集合写真

段々ネットワーキングのコツを覚えていく

私自身のことを覚えてもらうためにした努力

- お土産を持っていく　（日本茶、お菓子）
- 自分の名刺など配る（ちなみに国内外で1000枚以上は配った）
- 自分の活動を宣伝する品を持っていく
  - ステッカー、自分の本（目の前でサインすると喜ばれる）
- 発表スライドを常にPCに入れておいて、機会があれば紹介する
- （特に同じアジア人は英語苦手な人が多いので交流がしやすい）

英語で自分の情報を発信していく

Facebook	2016~
Twitter	2018~
Website	2019~

Facebook

https://www.facebook.com/asuka.nakajima.9

Twitter

@AsuNa_jp

Website

https://www.kun0ichi.net

kun0ichi.net

About News Biography Media

Asuka Nakajima | Cyber Security Researcher

About me

Asuka Nakajima is a researcher at **NTT Secure Platform Laboratories**. Her research interests include reverse engineering, vulnerability discovery, and IoT security. Since 2014, she has been a member of the executive committee of SECCON, the largest CTF organizer in Japan. She is also a **founder and leader of "CTF for GIRLS"**, which is the first female infosec community in Japan.

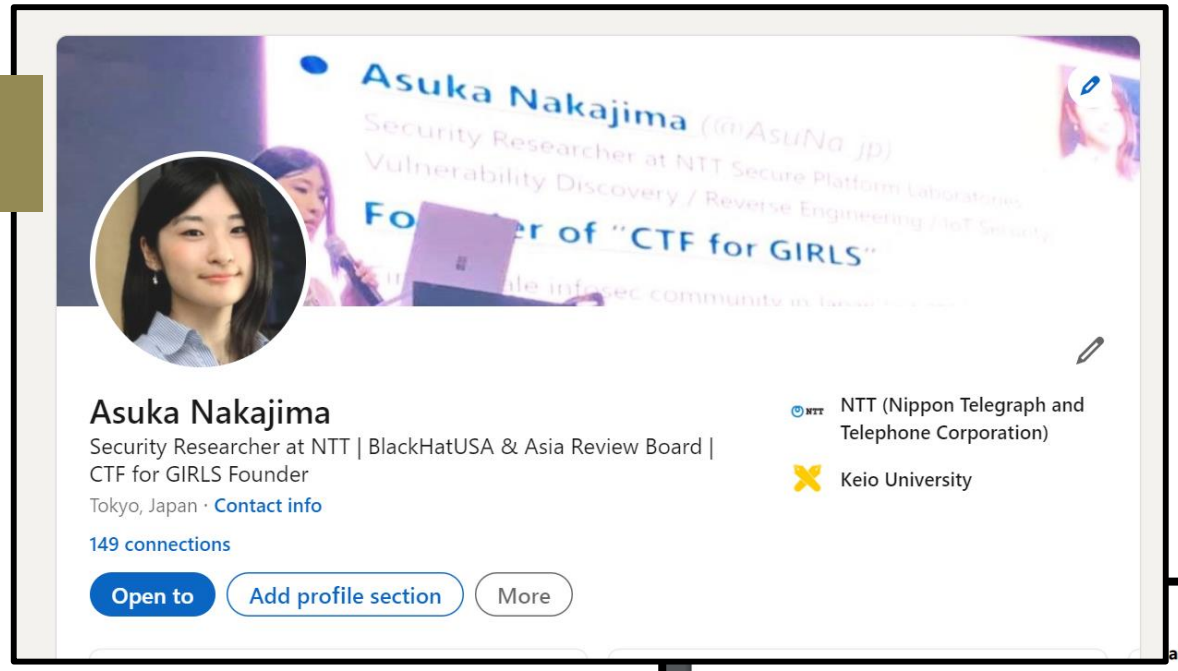
She has presented at various security conferences and events including **Black Hat USA 2019, Black Hat EU 2019, BlackHat Asia 2020**, Asia CCS 2019, ROOTCON 2019, AIS3 2018/2016, and PHDays IV. Asuka also serves as a **Review Board member for Black Hat Asia** from 2018, and BlueHat Shanghai 2019. She is also an author of the best seller book called "Cyber Attack" in Japan. (Bluebacks, 2018)

Recent Awards

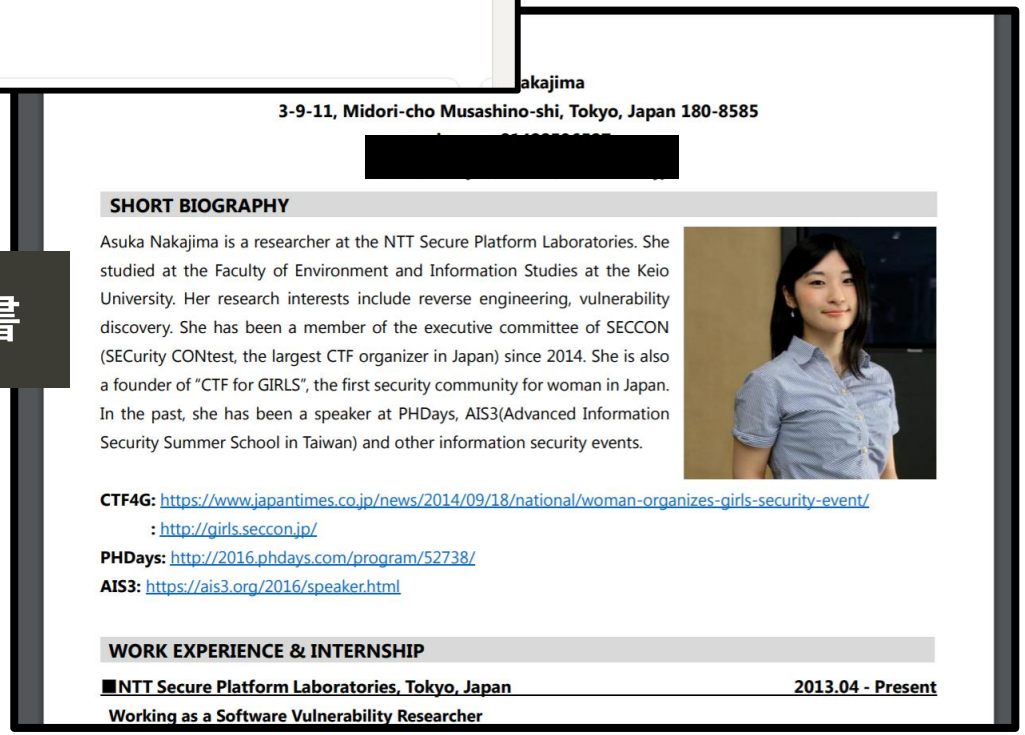
- (2019) 平成31年 サイバーセキュリティに関する総務大臣奨励賞 個人最年少受賞
- (2019) 第十五回 情報セキュリティ文化賞　個人最年少受賞

その他

LinkedIn



英語履歴書



話は戻って2016年

PHDays以降
海外での活動に拍車がかかる

PHDays以降の活動（2016年内）

- 台湾高度セキュリティ人材育成プログラムAIS3で招聘講師
  - 台北市/台中市/高尾市の大学を訪問
  - リバースエンジニアリングの講義を実施
- 米カーネギーメロン大学で訪問研究員として滞在
  - 10月末～11月末(帰国は12月)まで
  - 会社内で英語力など見込まれて/後は若手研究者育成目的など
  - 共同研究立ち上げの試行錯誤をしに(まず信頼関係構築など)

他にも幸運は続く

他にも幸運は続く

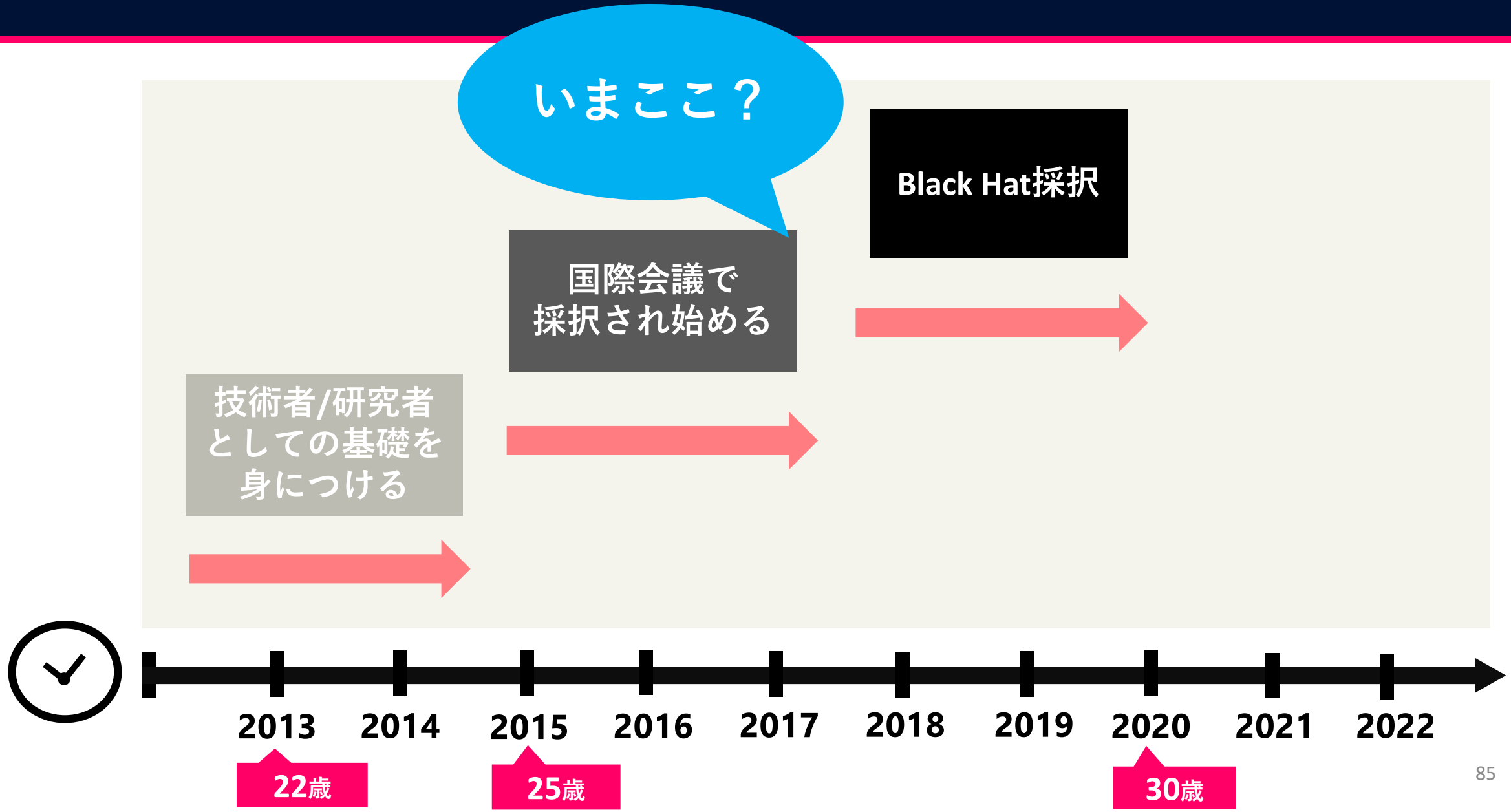
なんと2017年にBlackHatAsia(2018)の
レビューボードとして推薦・着任する

他にも幸運は続く

なんと2017年にBlackHatAsia(2018)の
レビューボードとして推薦・着任する

自分がBlackHatで発表するのも、もう目前のように思えた

社会人になりたての私の10年計画（再掲）



すごい順調のようにも見えるが・・

採択率約１０％

BlackHatレベルの研究成果が出せないという壁にぶち当たる

結論

しっかりした実力を身につける

個人的な戦略

実力があってもアピールしなければ
欲しい機会は得づらい

逆に自分の宣伝ばかりしても実力が身につかない

実力と宣伝力、両輪で回すのが大事

採択率約１０％

BlackHatレベルの研究成果が出せないという壁にぶち当たる

アピールばかりして
実力という車輪が回せてなかった

楽な道はない・・・

既に目指し始めて
４～５年・・

研究に専念する

基本的に未修正の脆弱性を探すようなテーマの研究

- ❖ 米カーネギーメロン大学との共同研究
  - ○ 高名な研究者のもと、世界レベルの研究成果の出し方を学ぶ
  - ○ 準トップの学術系難関国際会議であるAsiaCCSにて論文が採択
  - ○ 合計2000時間位かかった。議論も100回以上

- ❖ 自分自身でも単独で、IoT機器の脆弱性発見/対策の研究を
  - ○ 共同研究で鍛えた研究力で推進
  - ○ 研究名は「OEM Finder」
  - ○ これも数百時間とかかけた

OEM Finderの研究紹介

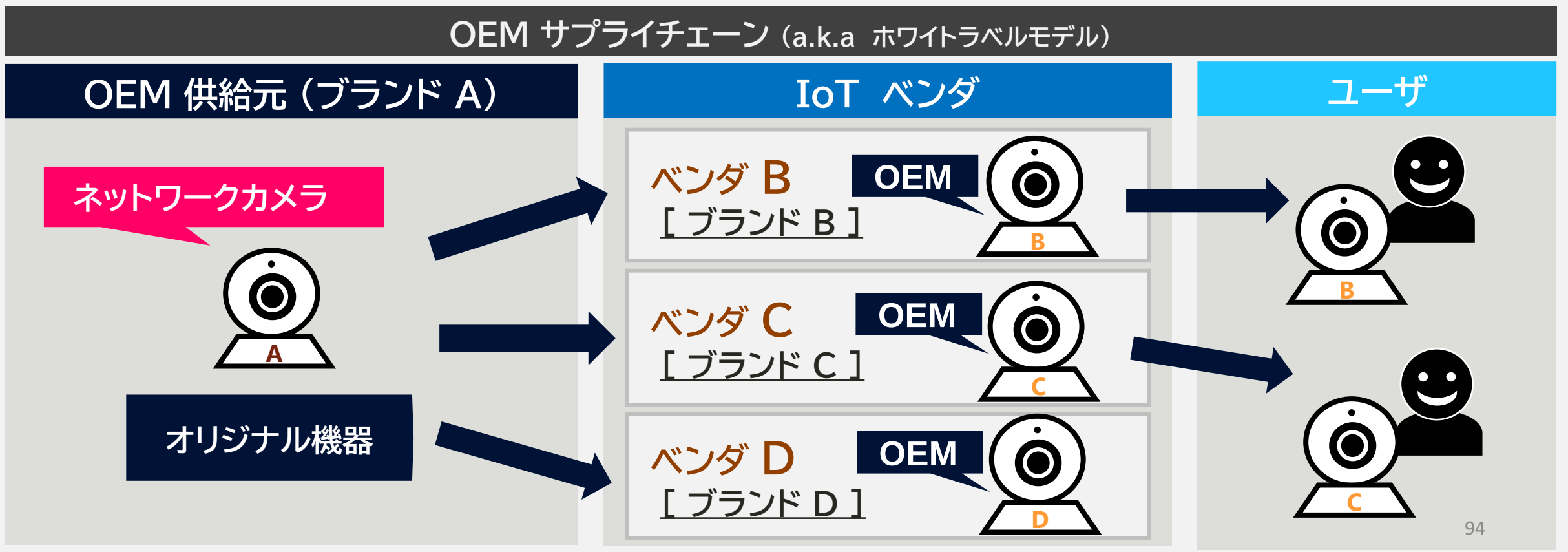
一言でいうと

OEM製造されたIoT機器が内包する脆弱性残存リスクを指摘する研究

未修正の脆弱性

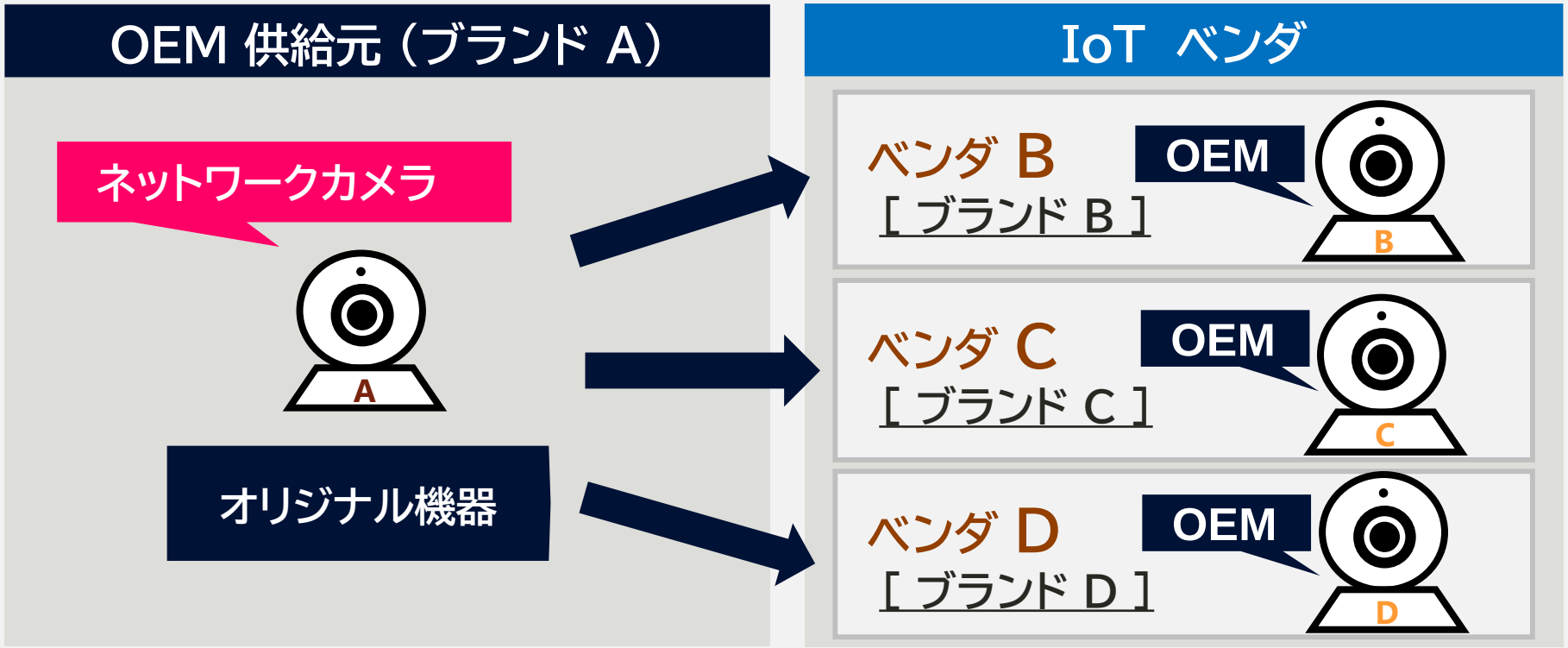
研究の背景［1/4］

一般消費者向けIoT機器を販売するベンダの多くは、
OEM（相手先ブランド名製造）生産モデルを採用している



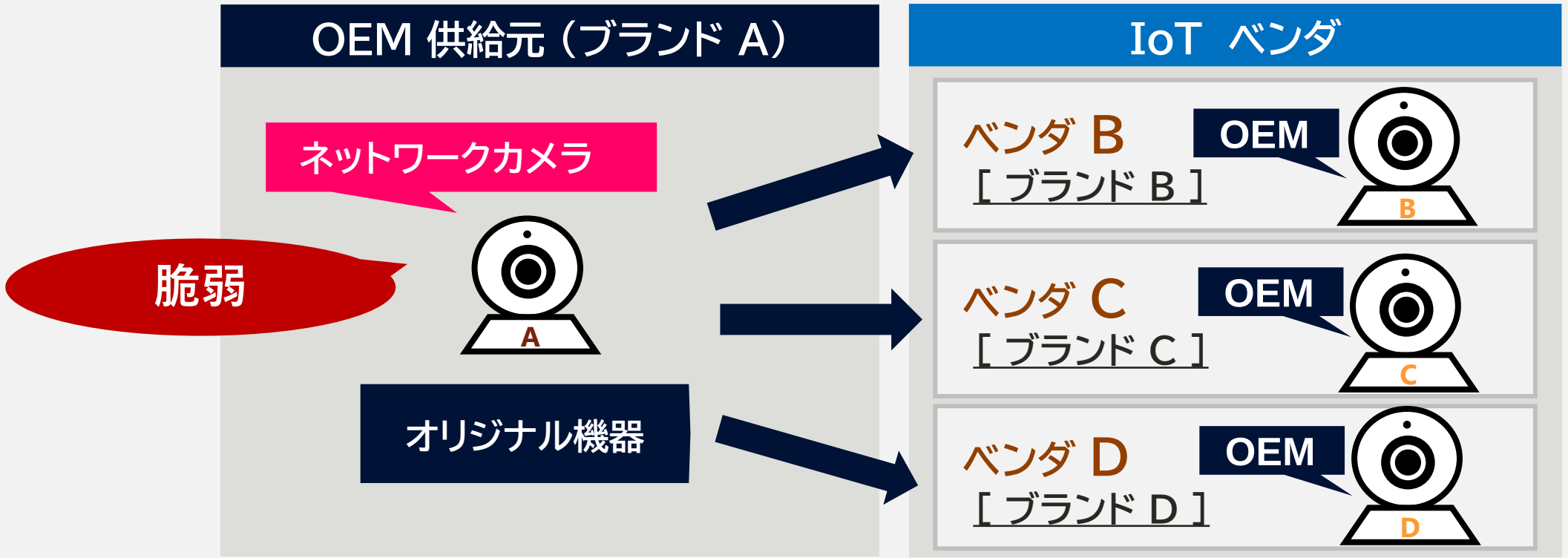
研究の背景［2/4］

OEM生産は機器製造コストを削減できる一方で、
セキュリティリスクに繋がる可能性がある



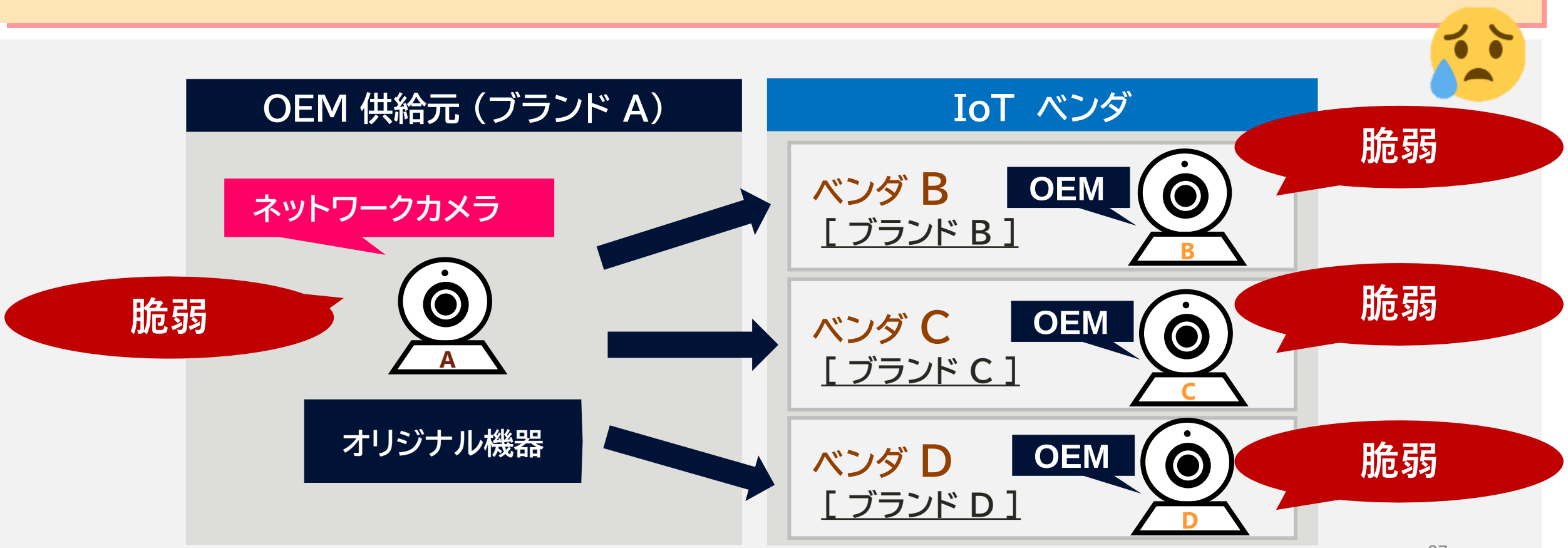
研究の背景［2/4］

OEM生産は機器製造コストを削減できる一方で、
セキュリティリスクに繋がる可能性がある



研究の背景［2/4］

OEM生産は機器製造コストを削減できる一方で、
セキュリティリスクに繋がる可能性がある



研究の背景［3/4］

2017年

CVE-2017-7921

Hikvision社（OEM供給元ベンダ）のネットワークカメラに発見された脆弱性は、80社以上のベンダから販売されているOEM品にも伝搬していた［※］

※ 80+ OEMs Verified Vulnerable To Hikvision Backdoor, IPVM, Sep 22, 2017, https://ipvm.com/reports/hik-oem-vuln

研究の背景 [3/4]

例) NVD, CVE

一般的に脆弱性情報データベースでは、発見された脆弱性の影響を受ける製品リストにOEM品を含まない

事前調査

- ✓ NVD data feedを用いて、2002年-2018年半ばまでのIoT機器に関連するCVEを調査.
  1. 製品・ソフトウェア名に「ファームウェア」、「カメラ」、「ルータ」、「モデム」、「ルータの名称※」が含まれるCVEを検索
  2. 単一のベンダのみ影響を与えるCVEを除外後, 全CVEを手動調査

2000 CVE 近く発見

- ✓ 影響を受ける製品の1つとしてOEM品をも含めて掲載したCVEはわずか6個

CVE-ID	影響を受けるベンダ	
	OEM供給元ベンダ	OEM品を販売するベンダ
CVE-2010-4230 CVE-2010-4231 CVE-2010-4232 CVE-2010-4233 CVE-2010-4234	Camtron	Tecvoz
CVE-2017-3216	Zyxel	Huawei, Zteo, Mada, Greenpacket,

NVD Data Feeds, https://nvd.nist.gov/vuln/data-feeds
※Router Check Support, http://support.routercheck.com/

研究の背景［4/4］

例) NVD, CVE

一般的に脆弱性情報データベースでは、発見された脆弱性の
影響を受ける製品リストにOEM品を含まない

考えられる原因の一つ

OEM品を自動的に探す手法がまだ存在しないため

現状ではOEM供給元に問い合わせるか、各機器を個別に手動調査する他無い

OEM品を探すには

OEM品とオリジナル製品は機器外観が類似している

CVE-2010-4230

オリジナル機器

ベンダ: Camtron
モデル: CMNC-200

OEM 品

ベンダ: Tecvoz
モデル: CMNC-200

CVE-2017-3216

オリジナル機器

ベンダ: ZyXEL
モデル: max308m

OEM 品

ベンダ: Greenpacket
モデル: ox350

OEM品を探すには

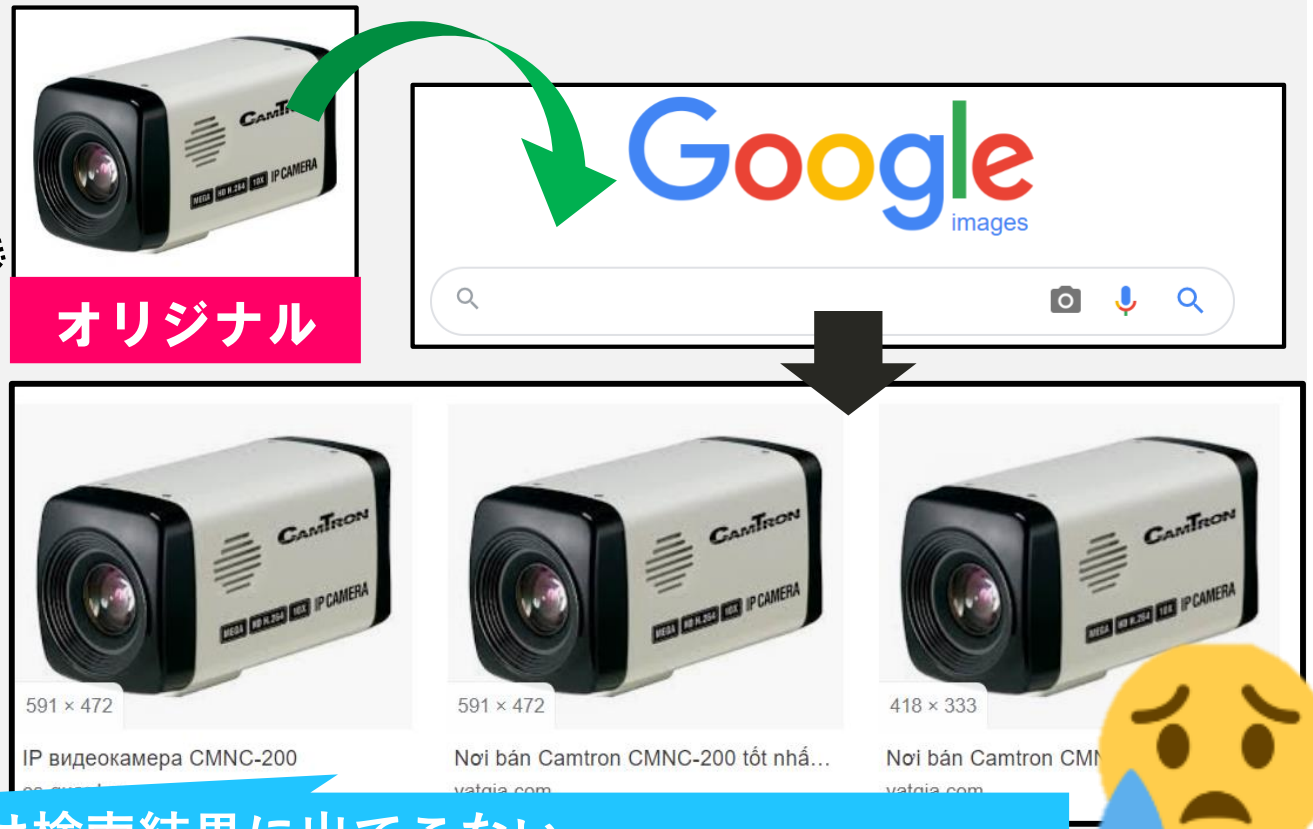
一般的な類似画像検索アルゴリズムでは、今回の目的に沿わない

主な課題

1. OEM品はカスタマイズされることがあり、オリジナル品と外観が完全一致とは限らない
   - 例）追加のアンテナ，異なるレンズ

2. オリジナル製品の場合と違う撮影方法/環境で、OEM品の写真が撮影されている場合がある
   - 例）異なるアングルからの撮影，異なる光源

Google 画像検索サービス



OEM品は検索結果に出てこない (Tecvoz CMNC-300)

提案手法

STEP1 | STEP 2 | STEP 3 | STEP 4

特定物体認識アルゴリズム（KAZE[※]）を用いて
画像から局所特徴量（キーポイント）を抽出

オリジナル機器の画像

Hikvision / DS-2CD2232-I5

検査対象機器(OEM機器)の画像

Trendnet / TV-IP312PI

※Alcantarilla, P.F., A. Bartoli, and A.J. Davison. ”KAZE Features.” *ECCV 2012, Part VI, LNCS 7577*. 2012, p. 214

提案手法

STEP1 | STEP 2 | STEP 3 | STEP 4

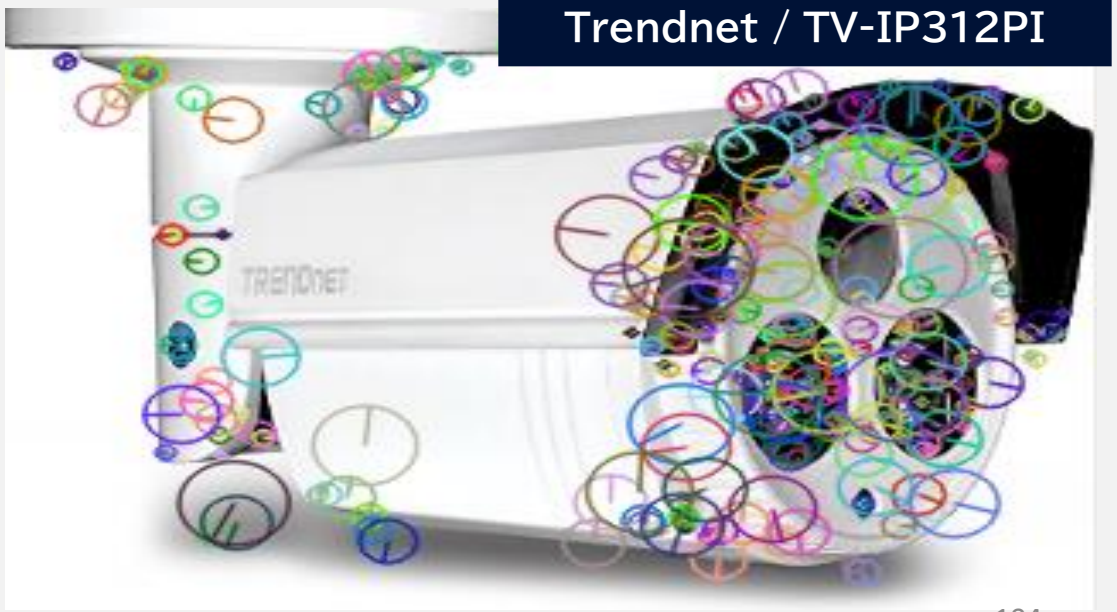
特定物体認識アルゴリズム（KAZE[※]）を用いて
画像から局所特徴量（キーポイント）を抽出

オリジナル機器の画像

Hikvision / DS-2CD2232-I5

検査対象機器(OEM機器)の画像

Trendnet / TV-IP312PI



※Alcantarilla, P.F., A. Bartoli, and A.J. Davison. ”KAZE Features.” *ECCV 2012, Part VI, LNCS 7577*. 2012, p. 214

提案手法

STEP1 | STEP 2 | STEP 3 | STEP 4

マンハッタン距離(L1ノルム)を用いて、
類似するキーポイント同士をマッチングする

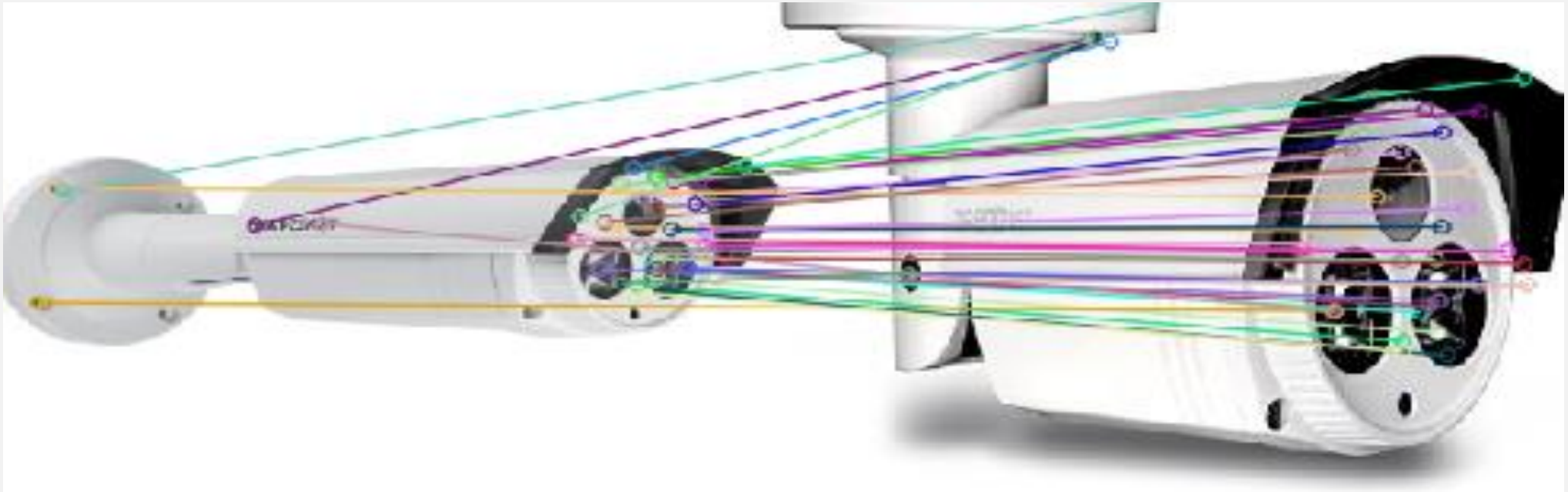
$$\text{類似度} = \frac{\text{マッチしたキーポイント数}}{\text{オリジナル機器のキーポイント数}}$$

もし 「類似度 < 閾値」 であった場合 次の画像の検査に移る

提案手法

STEP1 | STEP 2 | **STEP 3** | STEP 4

マッチしたキーポイントを利用して相対近傍グラフを構築

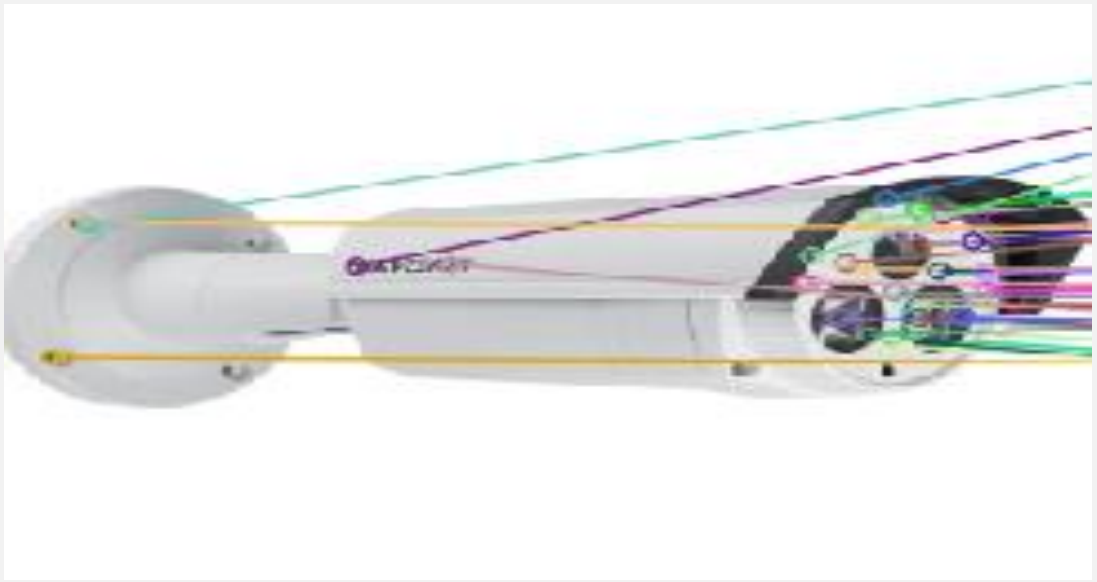


提案手法

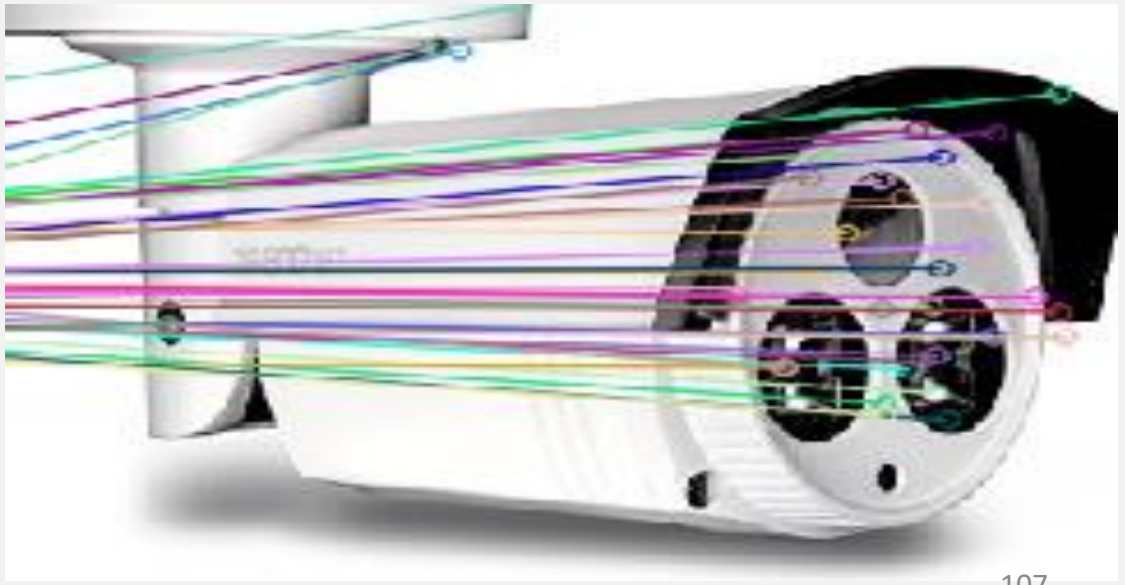
STEP1 | STEP 2 | STEP 3 | STEP 4

マッチしたキーポイントを利用して相対近傍グラフを構築

オリジナル機器の画像



検査対象機器(OEM機器)の画像

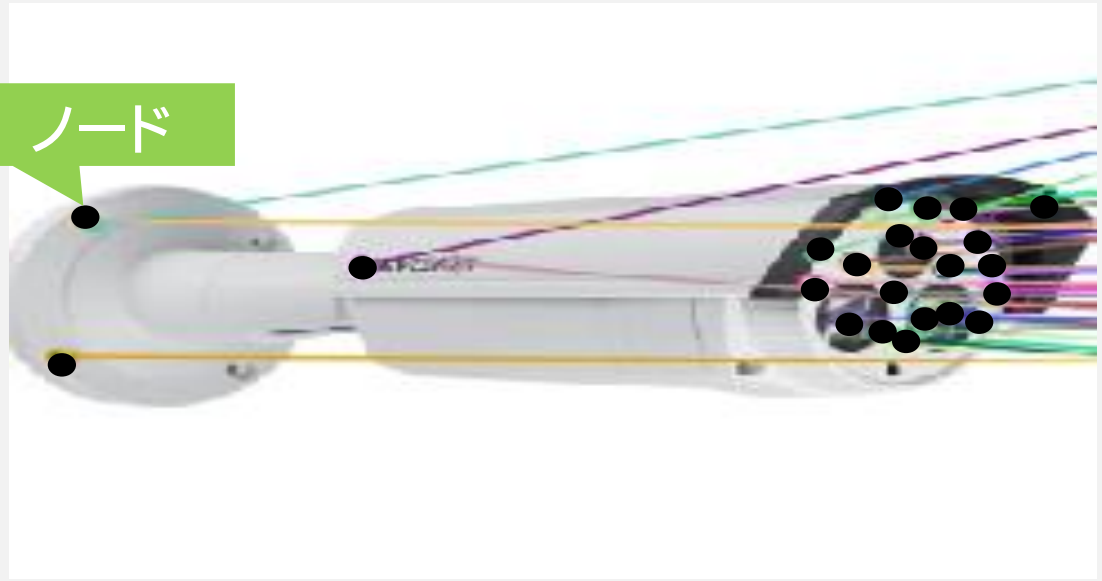


提案手法

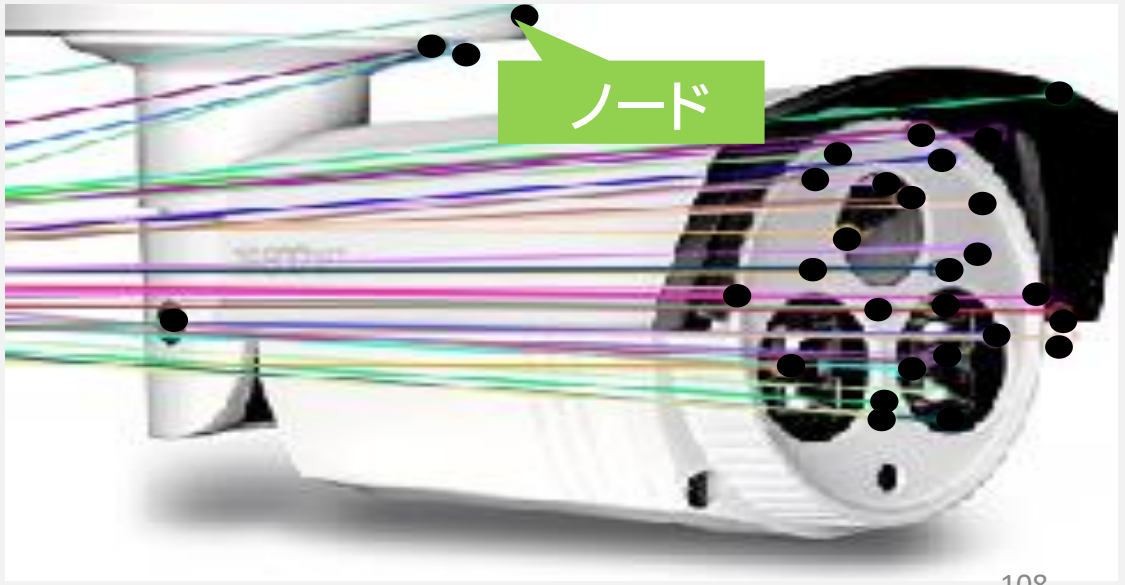
STEP1 | STEP 2 | STEP 3 | STEP 4

マッチしたキーポイントを利用して相対近傍グラフを構築

オリジナル機器の画像



検査対象機器(OEM機器)の画像



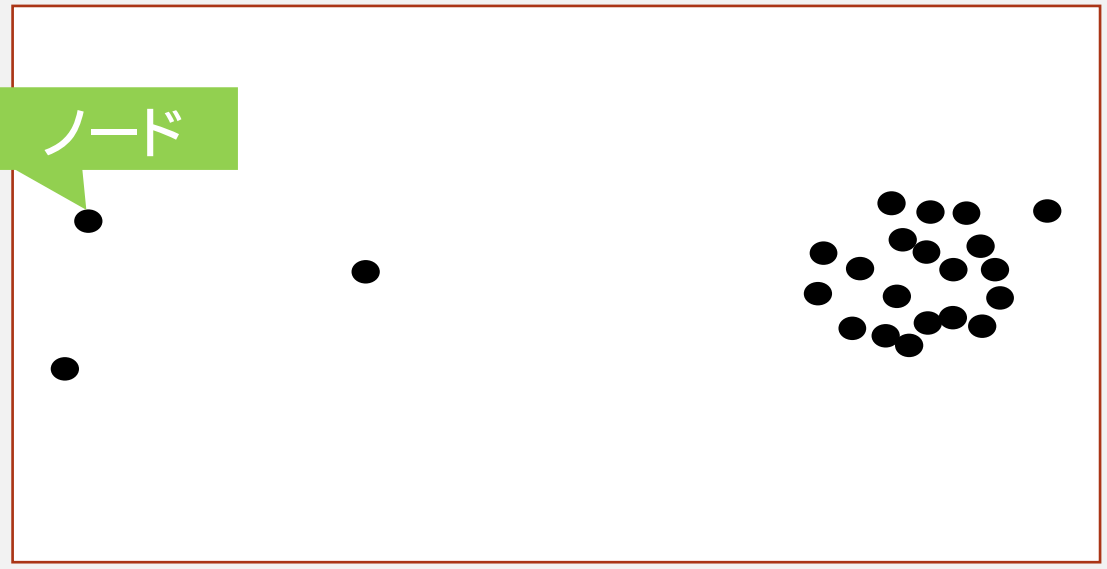
*マッチしたキーポイント同士に同じラベルを付与

提案手法

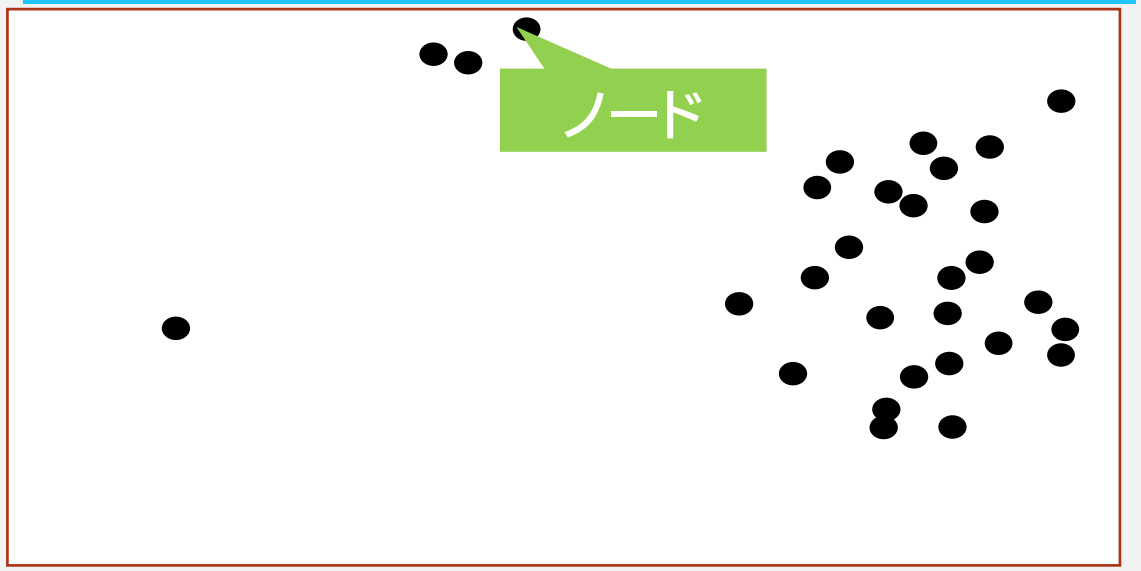
STEP1 | STEP 2 | STEP 3 | STEP 4

マッチしたキーポイントを利用して相対近傍グラフを構築

オリジナル機器の画像



検査対象機器(OEM機器)の画像



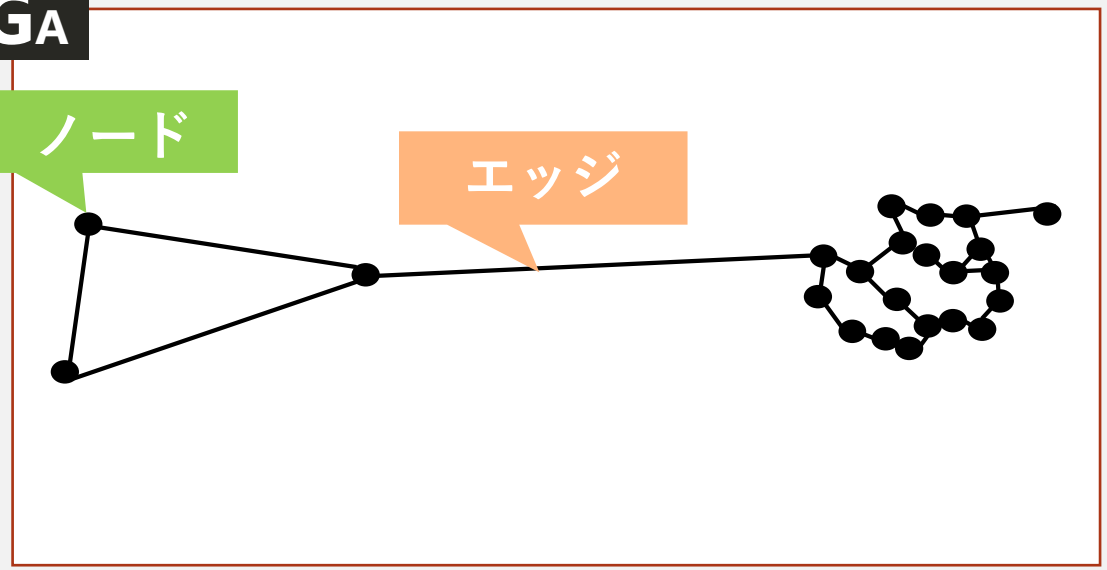
提案手法

STEP1 | STEP 2 | STEP 3 | STEP 4

マッチしたキーポイントを利用して相対近傍グラフを構築

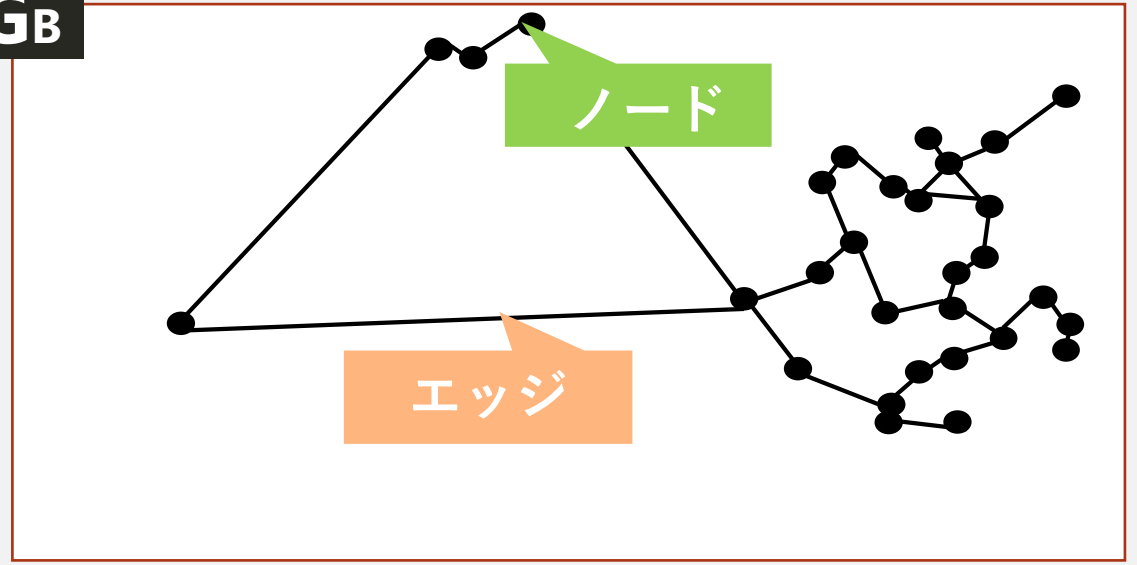
オリジナル機器の画像

G_A



検査対象機器(OEM機器)の画像

G_B

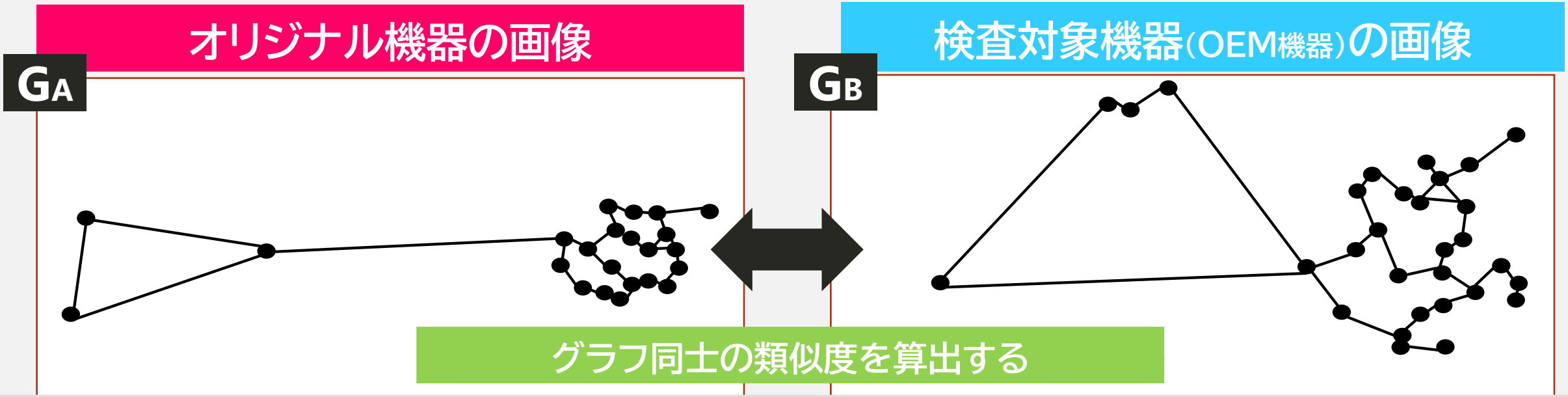


* 上記は相対近傍グラフのイメージ画像であり、実際の例ではありません

提案手法

STEP1 | STEP 2 | STEP 3 | STEP 4

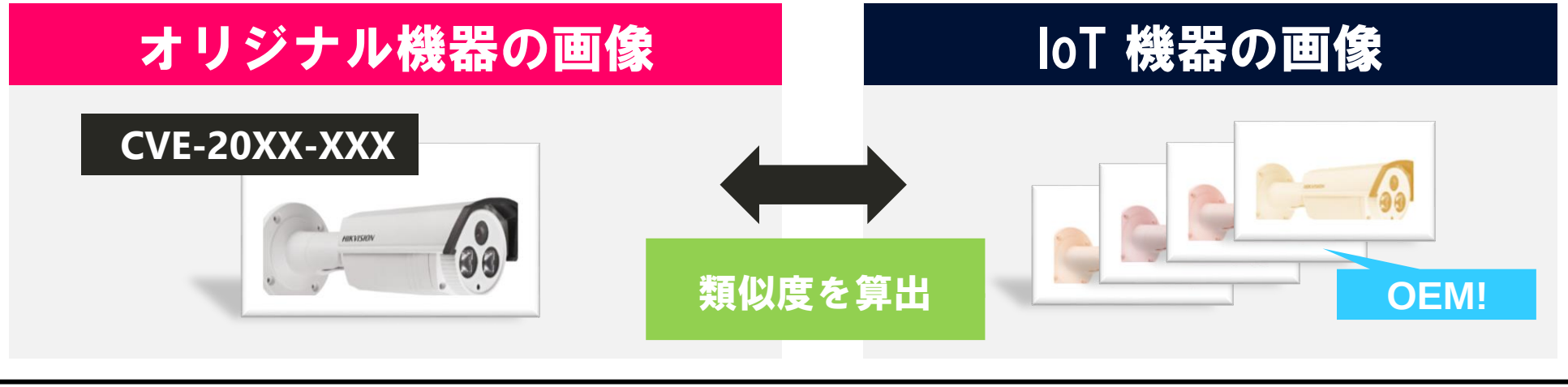
構造の類似性(大域的な類似性)を
最小パス距離グラフカーネルを用いて算出



$$sim(G_A, G_B) = \Sigma\ sim(\text{all-shortest-path}(G_A), \text{all-shortest-path}(G_B))$$

実際に脆弱な可能性の高い OEM IoT機器を探してみる

実施したこと



データセット 1/2

■ IoT機器画像のデータセット

Amazon & Walmart から合計54000枚以上ものネットワークカメラの画像を収集

EC サイト名	リージョン	API	対象カテゴリ	収集した画像数
Amazon	Amazon.com	Product Advertising API	Dome Camera	13433
			Bullet Camera	7410
			Web Camera	2114
	Amazon.jp	Product Advertising API	Dome Camera	541
			Bullet Camera*	1000
			Web Camera	3277
Walmart	walmart.com	Open API	Indoor Camera	23159
			Outdoor Camera	3651
			Wireless Camera	247
			Web Camera	3
合計				54835

*Bullet Camera のカテゴリは amazon.jpでは “Standard Camera”と呼ばれるがカテゴリIDはamazon.com のBullet Cameraと同一のため、表ではBulletCameraと表記

データセット 2/2

■ オリジナル機器画像のデータセット

代表的なOEM供給元ベンダ4社が販売しているネットワークカメラの内、過去2年間に脆弱性が発見された製品の画像を120枚以上収集（amazon.comより）

ベンダ名	CVE数(脆弱性数)	製品数	収集した画像数
Hikvision	3	20	21
Dahua	5	75	80
Foscam	24	21	21
Wanscam	1	1	3
合計	33	117	125

結果

まとめ

- ✓ **25社以上のベンダで販売されている、180種類以上もの脆弱性な可能性の高いOEM品候補を発見**

- ✓ **発見したOEM品候補の最新のファームウェアを数個程度解析**
  - 発見したOEM品候補の機器が**真にOEM品であることを確認**
  - OEMベンダから配布されているファームウェアが**未だに脆弱であることを確認**

ケーススタディ1：Hikvision

CVE-2017-7921 & CVE-2017-7923

オリジナル

モデル: ds-2cd2312-i

OEM品候補

ベンダ: KT & C
モデル:KNC-P3TR6XIR

ベンダ: PNET
モデル: PN-402EX

ベンダ: PWS Security
モデル: Unknonwn

ベンダ: LTS
モデル: CMIP3032-28

ベンダ:
Orange Sources
モデル: Unknown

ベンダ: P2P Security
モデル: Unknown

ベンダ: HDView
モデル: Unknown

ベンダ: AVUE
モデル:AV50HTWX

ベンダ: CMPLE
モデル:1287-N

ベンダ:
Securtiy Camera King
モデル:IPOD-PR2EXIRE28

ケーススタディ1：Hikvision

CVE-2017-7921 & CVE-2017-7923

オリジナル機器

モデル: ds-2cd4132fwd-i(z)

OEM品候補

ベンダ: Panasonic
(ブランド名: advidia)
モデル:A-44-IR-V2

ケーススタディ2：Dahua

CVE-2017-9317 & CVE-2917-9315

オリジナル機器	OEM品候補			
				
モデル **IPC-HDBW4831E-ASE**	ベンダ: **iMaxCamPro** モデル:WEC-IP9-WiFi	ベンダ:**PWS Security** モデル: Unknown	ベンダ: **Night King** モデル:NK-6030G-4K	ベンダ: **Urban Security Group** モデル: USGDK8W405GAHBB56A

ケーススタディ3：Foscam

CVE-2018-6830

オリジナル機器

モデル: FI9805W

OEM品 候補

ベンダ: Skyreo
モデル:
SR8905W-SLUS

オリジナル機器

モデル: FI9900EP

OEM品候補

ベンダ: Ambient Weather
モデル: AMBIENTCAMHDA

ケーススタディ3：Foscam

CVE-2018-6830

オリジナル機器	OEM品候補			
				
モデル: FI9816P	ベンダ: Vstarcam モデル: C37A	ベンダ: Escam モデル: QF001	ベンダ: Sricam モデル: Unknown	ベンダ: EVAKION モデル: EV130

詳細解析

CVE-2017-9315

オリジナル

ベンダ:Dahua
モデル:
SD52C430U-HNI

OEM 品候補

ベンダ: iMaxCamPro
モデル:
IMAX-CVI720P12X-PTZ-FM

ファームウェアをダウンロード（IMAX Cam Pro）

WEC-C12X-PTZ-F Camera　Build (2013-09-30)

https://www.worldeyecam.com/iMaxCamPro-Firmware-Download-Page.html

アンパック

A

Dahua ロゴ！

脆弱性箇所が！

B

```
"Group" : "admin",
"Memo" : "888888 's account",
"Name" : "888888",
"Password" : "888888",
```

まとめ

- ✓ 発見したOEM品候補の機器が真にOEM品であることを確認（A）
- ✓ OEMベンダから配布されているファームウェアが未だに脆弱である事を確認（B）

BlackHatUSA
2019 投稿

Black HatUSA

2019 投稿

Reject!!

ただし・・

CTF for GIRLSの活動の一貫として
2018年に新設されたCommunity Trackに投稿

注: 元々台湾や韓国の女性セキュリティコミュニティと何らか連携をしたいと考えていたが、
CTFを共同開催出来るほどの余力がなく、新設されたCommunity Trackの共同投稿が良い交流機会になるのでは思い提案

BlackHat USA

2019 投稿

Accept!!

BlackHatUSAでの発表（2019年8月）

Women in Security:
Building a Female InfoSec Community in Korea, Japan, and Taiwan

- アジアの女性セキュリティコミュニティの共同発表
  - 韓国 Power of XX
  - 台湾 HITCON GIRLS
  - 日本 CTF for GIRLS

https://www.youtube.com/watch?v=OsZ63tlxCQU

でもまだ研究がBlackHatで
採択されたわけではない

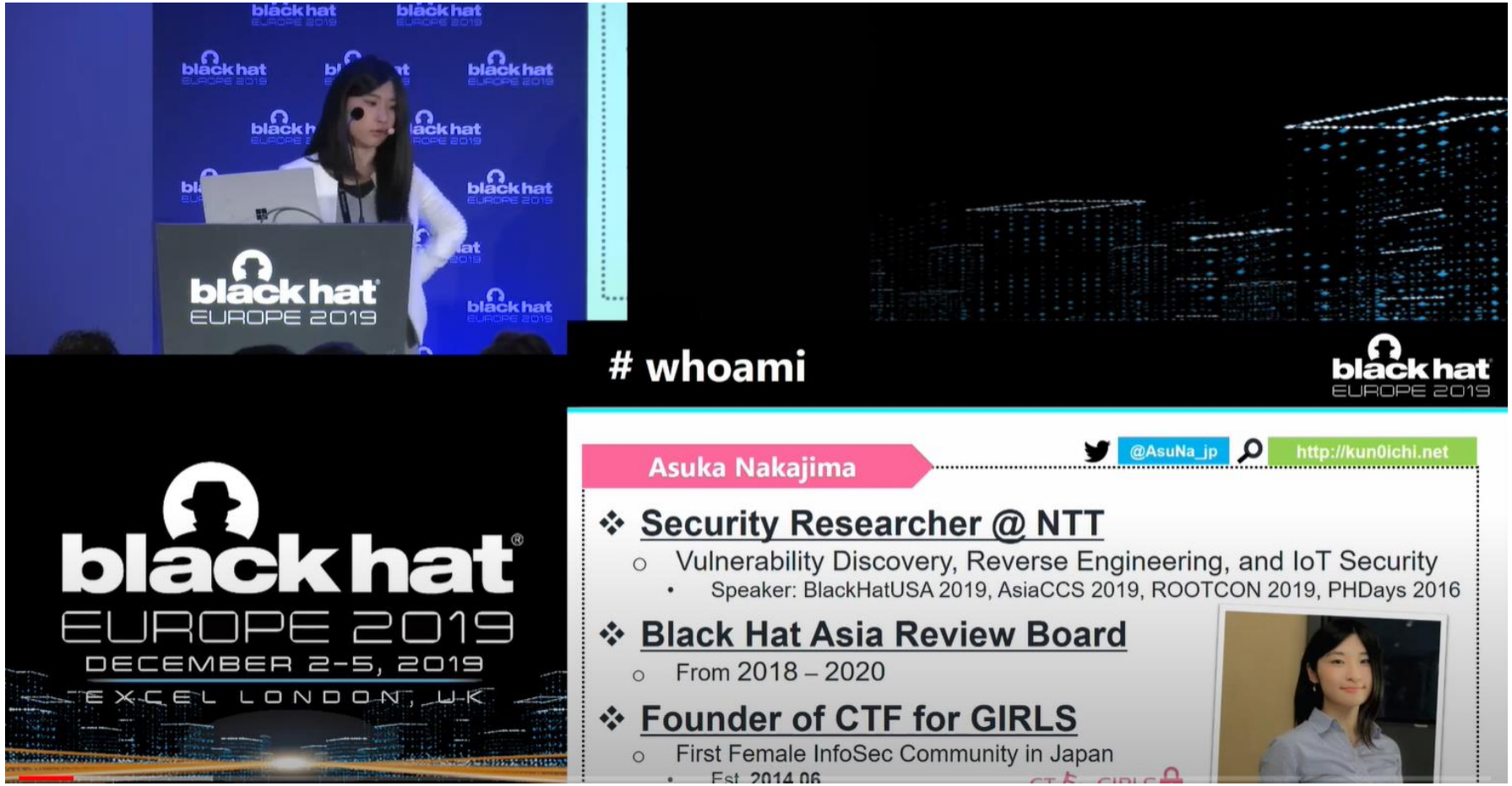
BlackHatEurope
2019 投稿

BlackHatEurope

2019 投稿

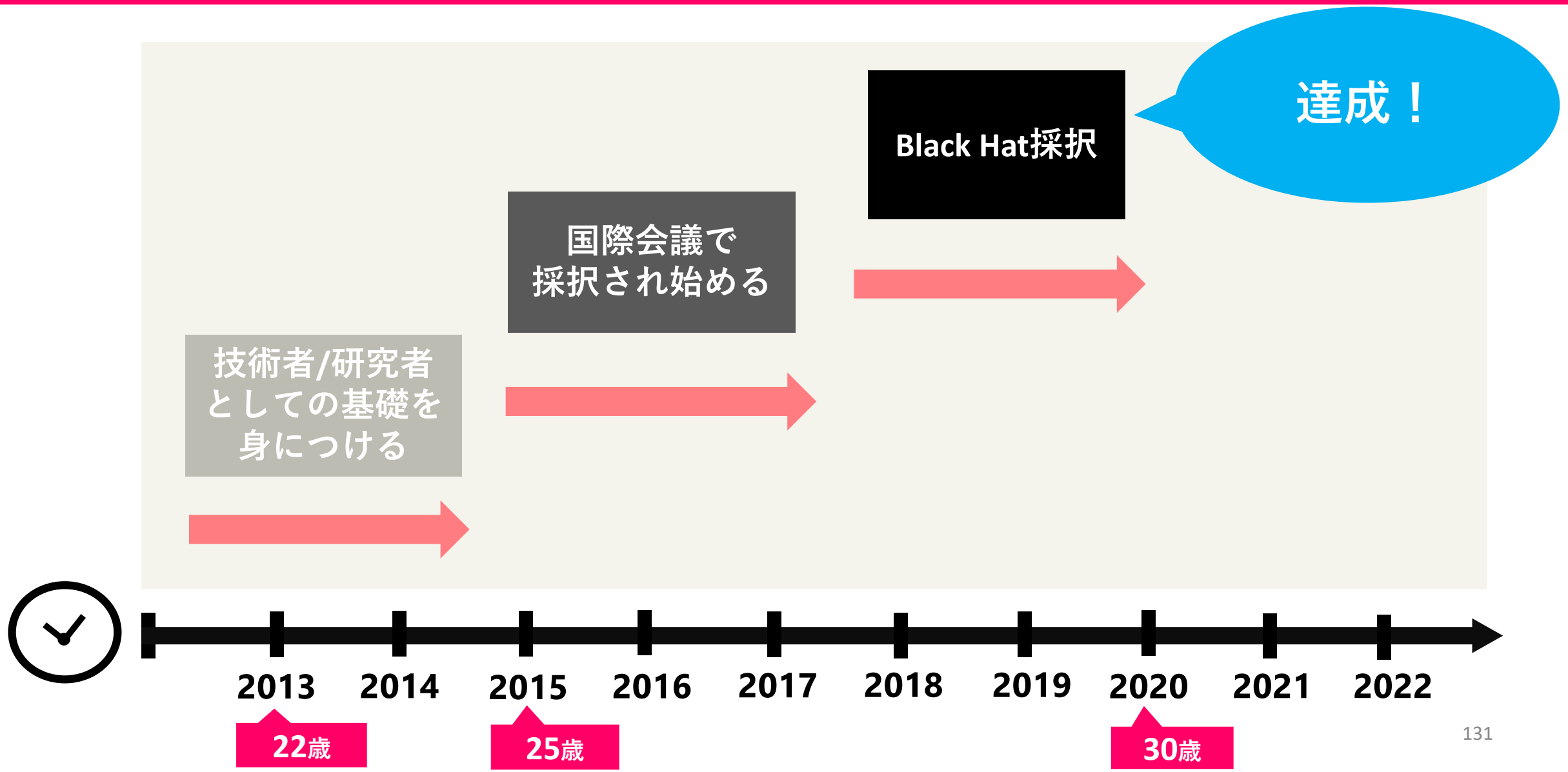
Accept!!

BlackHatEuropeでの発表（2019年12月）



https://www.youtube.com/watch?v=AgzfII4pHYE

社会人になりたての私の10年計画（再掲）



世界を広く良い方向に変えられたか？（1/2）

脆弱だと思われるOEM製品が市場に多数
出回っているのは、多くの人にとって衝撃的であった

- 海外メディアで複数回取り上げられ、多くの人の目に触れた
  - LinuxMagazineとか
  - BlackHat運営からも宣伝

多くの人に警鐘できた

Suchmaschine entdeckt Sicherheitslücken in Security-Kameras

Von *Kristian Kißling* - 05. Dezember 2019

Auf der Black Hat Europe 2019 haben japanische Security-Forscher von NTT eine Online-Suche vorgestellt, mit der sie Sicherheitslücken in No-Name-Security-Kameras leichter entdecken können.

Wer heute eine Netzwerk-basierte Sicherheitskamera kauft, erhält oft unter verschiedenen Namen das gleiche Gerät. Das ist so, weil ein OEM-Hersteller seine Kamera an verschiedene OEM-Anbieter verkauft, die dann ihre Sticker auf das Gerät pappen und es in den Handel bringen. Das aber bringt in puncto Sicherheit gleich mehrere Probleme mit sich.

Oft stecken in der ausgelieferten Firmware des Originalanbieters Sicherheitslücken. Stopft der OEM-Hersteller diese Sicherheitslücken, landen diese Fixes dennoch häufig nicht in den verkauften Geräten der OEM-Anbieter. Zugleich verraten die National Vulnerability Database (NVD) und die Datenbank der Common Vulnerabilities and Exposures (CVE) nicht, in welchen Geräten welcher weiteren Anbieter diese Sicherheitslücken stecken.

Zudem sind auch die OEM-Anbieter nicht wirklich daran interessiert, dass die Kunden erfahren, von dem die Kamera eigentlich stammt. Der OEM-Hersteller ist daher oft nicht offensichtlich. Kaufen Admins solche No-Name-Security-Kameras, müssen sie also selbst herausfinden, wie sicher diese sind. Sie können dazu die Firmware dumpen, den OEM-Hersteller herausfinden und dann die Firmware-Versionen der Modelle vergleichen.

https://www.linux-magazin.de/news/suchmaschine-entdeckt-sicherheitsluecken-in-security-kameras/

世界を広く良い方向に変えられたか？（2/2）

脆弱だと思われるOEM製品が市場に多数
出回っているのは、多くの人にとって衝撃的であった

- ❖ 米国の国家電気通信情報管理庁に研究が注目される
  - IoT機器のSBOM（Software Bill of Materials）の推進のための参考に
  - 著名な会議で何度も紹介（RSAC等）

その他にも・・

https://www.automotiveisac.com/wp-content/uploads/2020/05/2020_05_12_Friedman_AutoISAC_SBOM_CommunityCall.pdf

多少は、世界/社会を広く良い方向に変えることができた・・？

BlackHatEurope 2019後（1/2）

- **世界のコミュニティを先導する側にまわる**
  - BlackHatAsia2020で閉会時基調講演/セミナーを主催
  - BlackHatUSAのレビューボードで最先端の研究の査読/推進

- **得た知見や知名度を使って社会にさらに還元**
  - BS-TBS『身近なパソコン世の中を変える』に出演
  - セキュリティ啓発に貢献

BlackHatEurope 2019後（2/2）

❖ また新たな壁にぶつかる

- 技術力がまだまだ不足している感じ
- 研究の社会実装への壁（企業研究者の難しさ）
- 私自身の現場感覚の足りなさ（研究/外部活動ばかりだった為）
- 個人の幸せについてや価値観の変化（健康問題/30代女性という身）

- 目標２の世界/社会に広くより良くする方法を模索中
- しばらくは計画的偶発理論に乗っ取り偶然に身を任せ中

振り返ってみると(結果だけ見れば)

- BlackHatUSA 2019 発表　　28歳
- BlackHatEurope 2019 発表　29歳
- BlackHatAsia 2020 発表　　29歳(30歳直前)

BlackHatシリーズすべての会議に20代で登壇

(余談)コミュニティに入り込むコツ

私自身絶対的な実力を持ち合わせているわけでは無い

自分が相手に対してどのような価値提供が出来るのを常に念頭におく

- BlackHatAsiaレビューボード
  - アジアの会議のため、アジア人である私の意見は尊重(価値がある)
  - (やはりまだまだ欧米中心なので)特に英語が出来るアジア人は重宝される
  - 日本の状況など共有すると喜ばれたり
- カーネギーメロン大学共同研究
  - 高名で多忙な研究者が相手。とにかく私自身の労働力を提供
- この勉強会
  - 海外コミュニティに深く入り込んだ、私独自の知見の提供 (おそらく他では聞けない話)

さいごに

世界のコミュニティに入り込むことの重要性（1/2）

- **良い機会（依頼）を貰えるチャンスを増やすことができる**
  - コミュニティに入り込むことで「あの人なら会ったことあるし、任せられそう」というのが増える
- **ルール/トレンドを知ることができる**
  - どの国際会議では、どのようなテーマが採択されやすいのか？
  - 査読の際に、どこに重きが置かれているのか？
  - 皆から注目されて始めている研究テーマは何なのか？
- **（頑張れば）ルール/トレンドを作る側にまわれる**
- **（世界の中における）自分自身の相対的価値を知ることが出来る**
  - 例）アジア人（日本人）であることに意外にも価値があった。
  - 外国人であるというだけでも喜ばれるケースも（もちろん一定の実力は必要だが）

ずっと日本にいるから関係ない・・？

世界のコミュニティに入り込むことの重要性（2/2）

- **選択肢が広がる**
  - 日本に住みながら海外企業に就職する（しやすくなる）
  - 海外にこそやりたい仕事があった場合に、選択肢に入れられる

- **個人としてのリスクマネジメント**
  - この先も経済成長率の低迷が続くようならば・・？
  - 特に若い人は人生長い。この先私自身も50年はある。

ご清聴ありがとうございました！