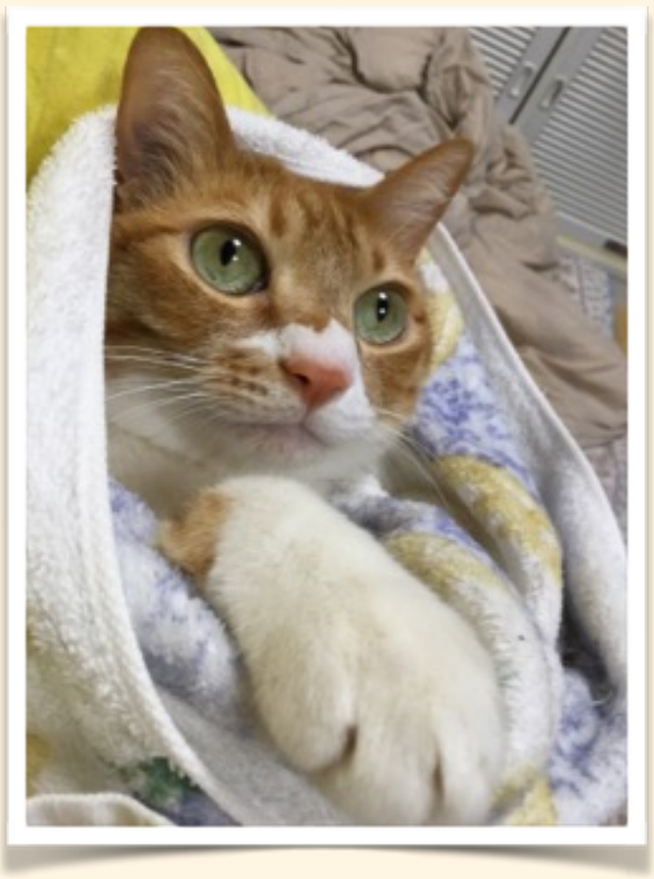
セキュリティオペレーション:
みんなどんなの使ってるの？

株式会社インターネットイニシアティブ
セキュリティ本部　セキュリティ情報統括室
ももい やすなり <momo@iij.ad.jp>

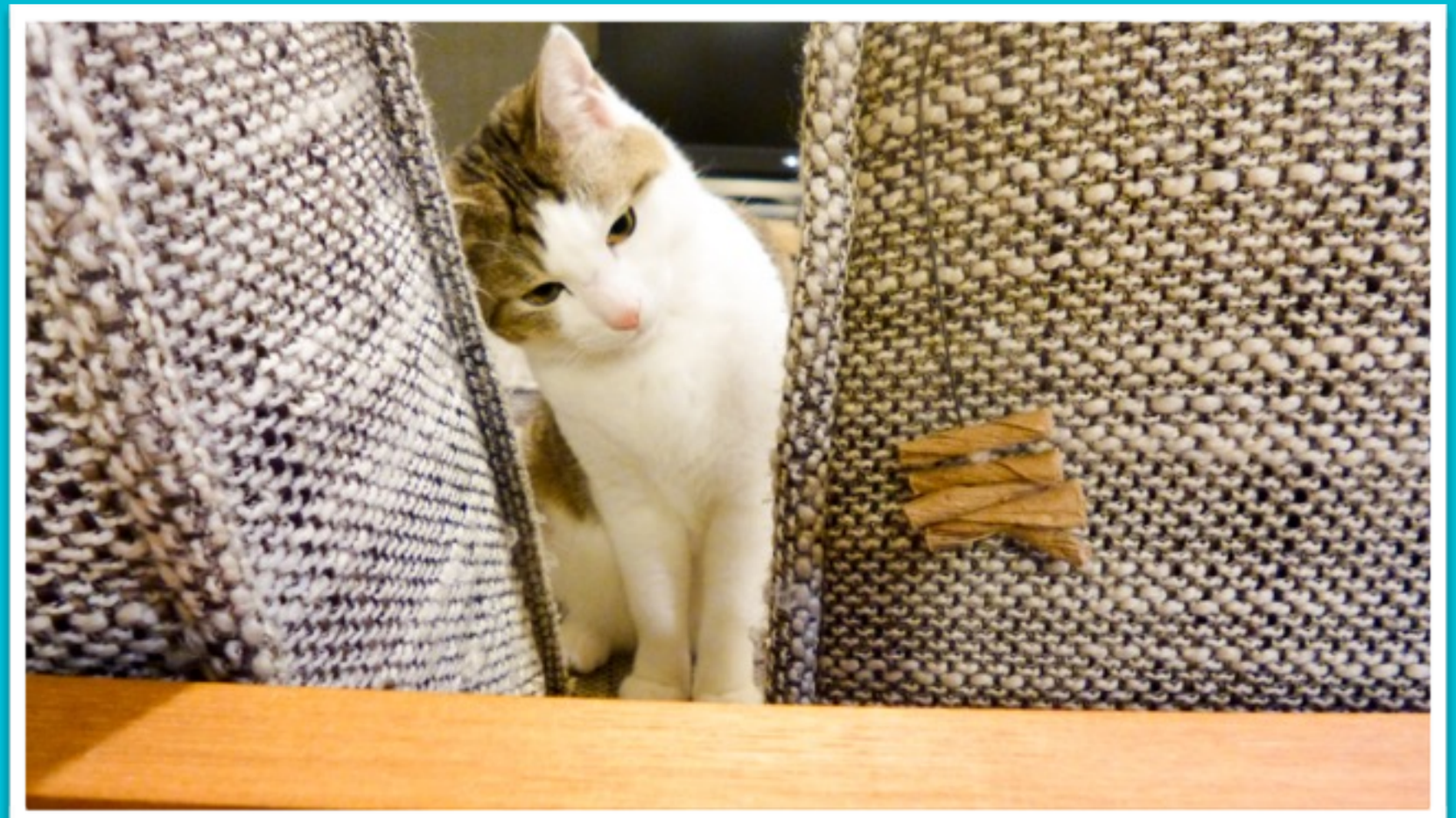
2016/07/06 JANOG38 @ 沖縄

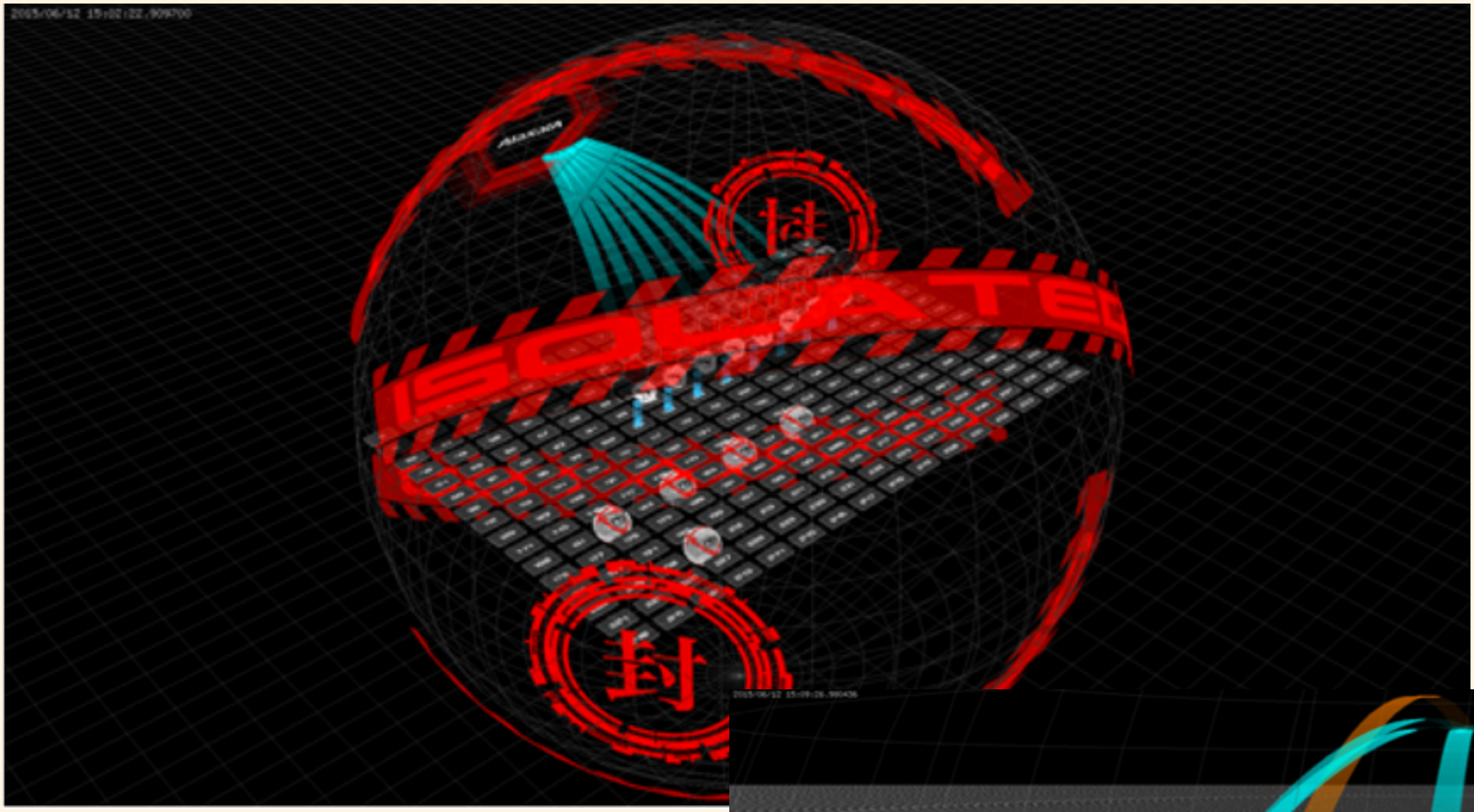
自己紹介

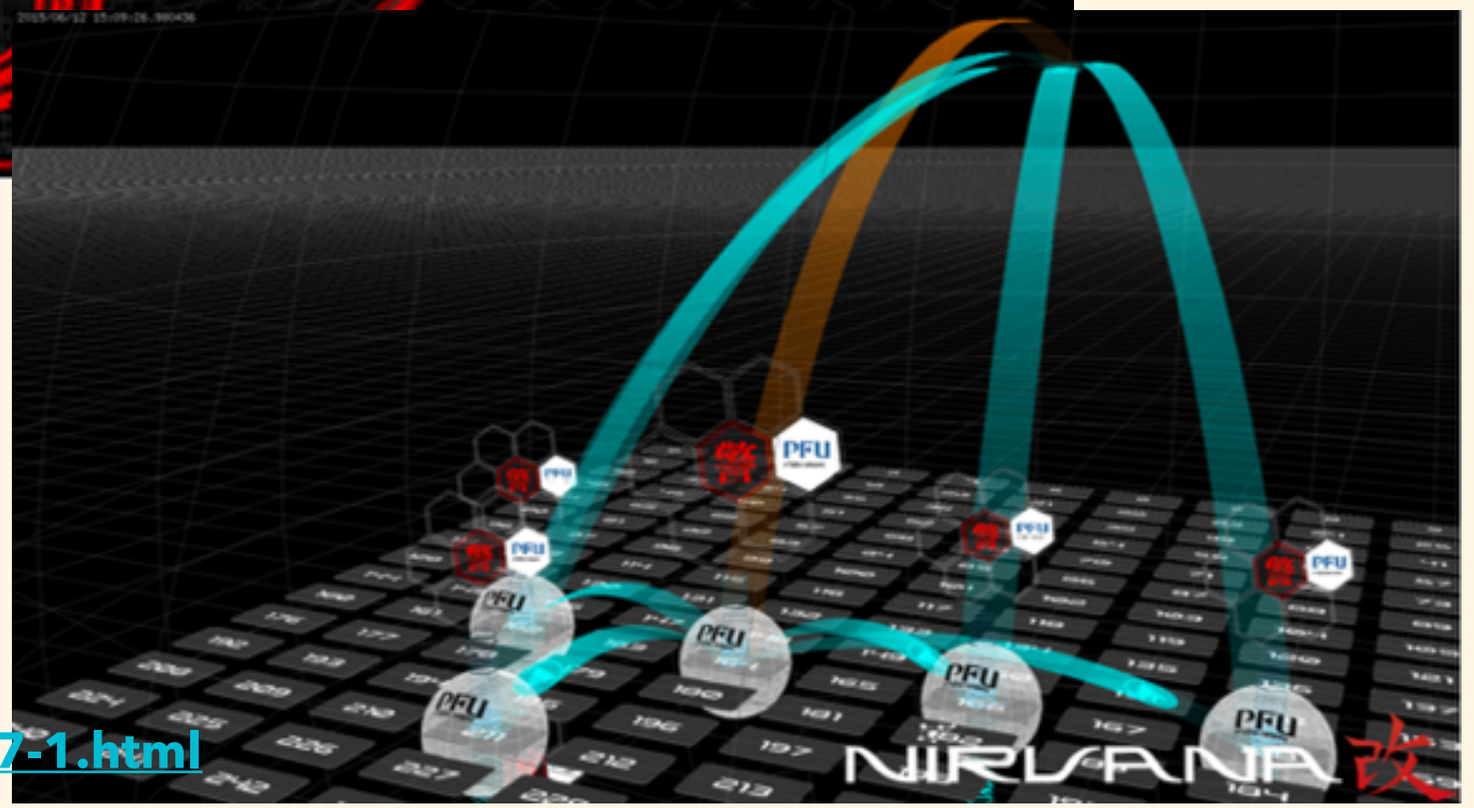
- ももい やすなり <momo@iij.ad.jp>
- システム開発、サービス開発やってます
- 勉強会、セキュリティ、食べ物担当
- Twitter @sbg　Facebook ymomoi
- ねこ、HR/HM



セキュリティ
オペレーションの
イメージは？





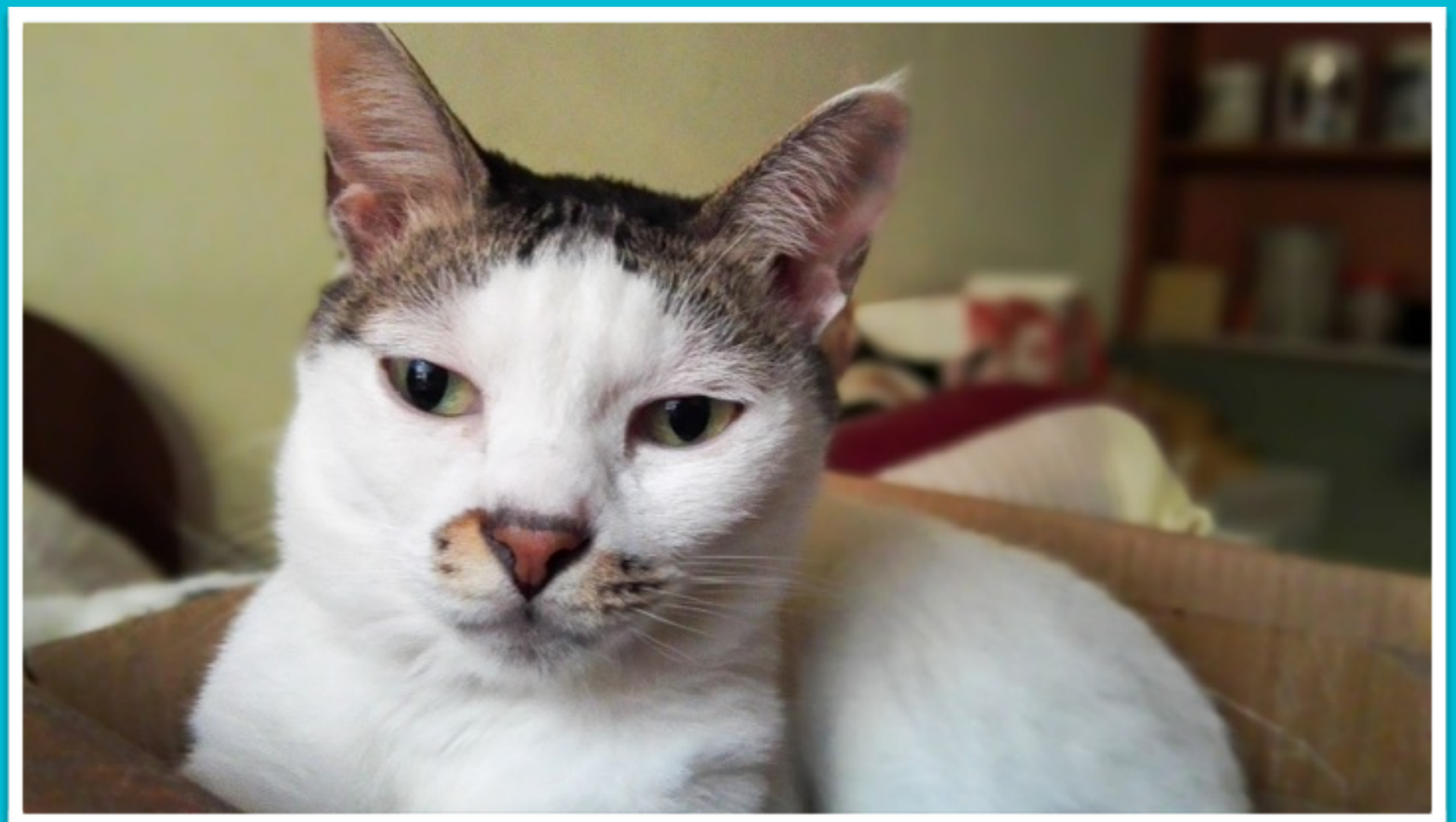


NIRVANA改が更にバージョンアップ！

https://www.nict.go.jp/press/2016/06/07-1.html

実態

ログ調査



ログ調査

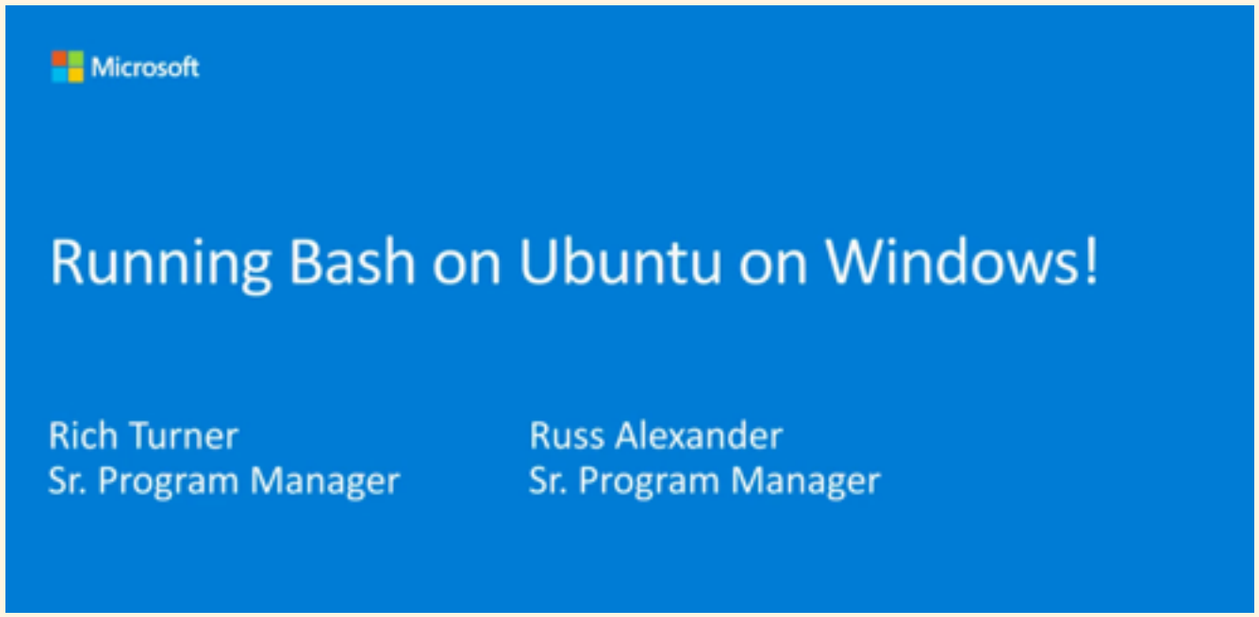
- すべてはログ調査から始まる (?)
- FW, IPS, Proxy, 各種サーバ, ...

ログ調査の定番

- なんといっても UNIX tools
  - 例: grep, awk, cut, sort, uniq...
- Q: Windows しかできない人がきたら？
- A: 覚えてもらいます

Windows 環境では...

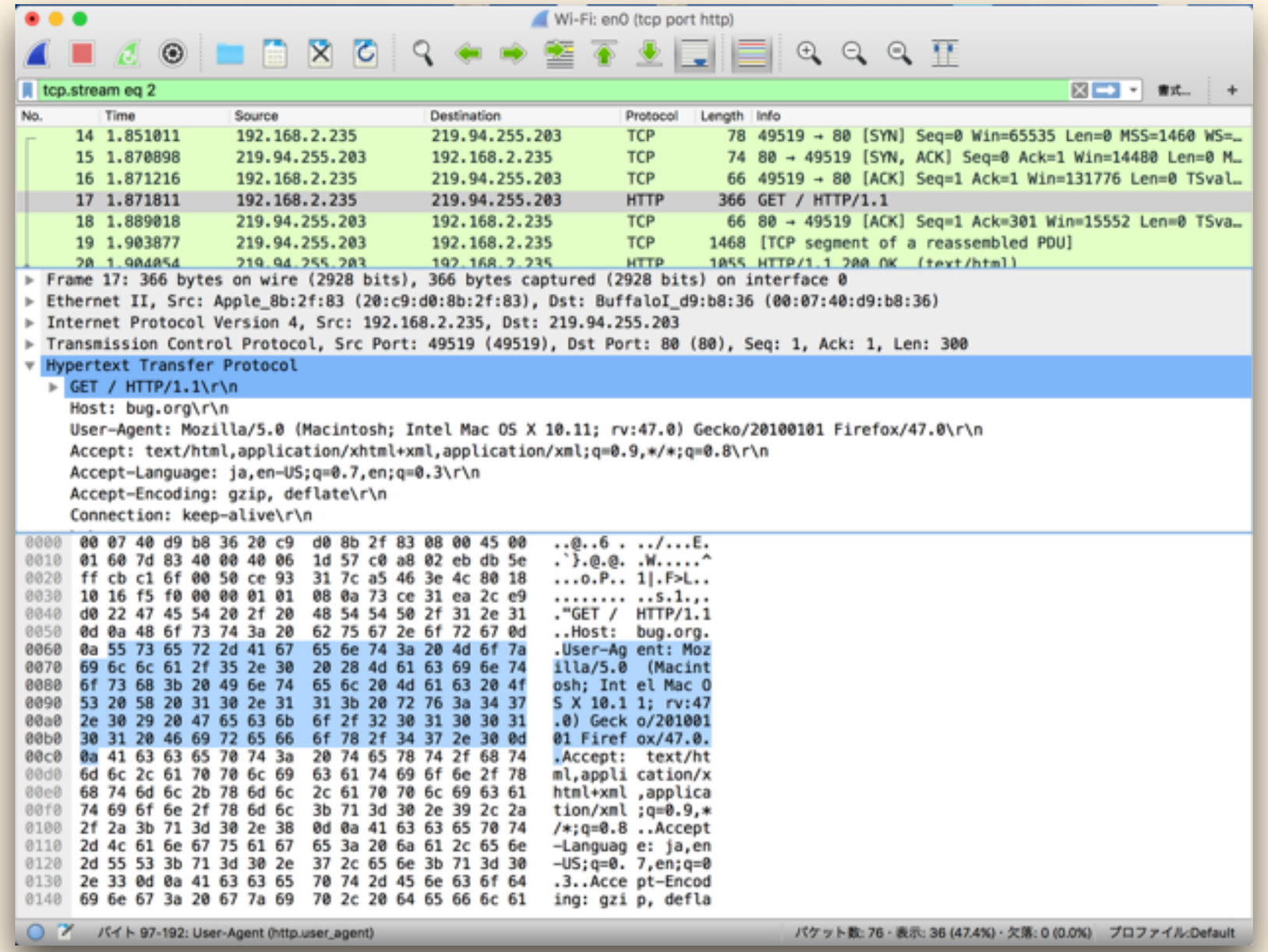
- Cygwin
- Babun
- Bash on Ubuntu on Windows
  - 結局 UNIX tools?



通信内容の調査

通信内容を見る

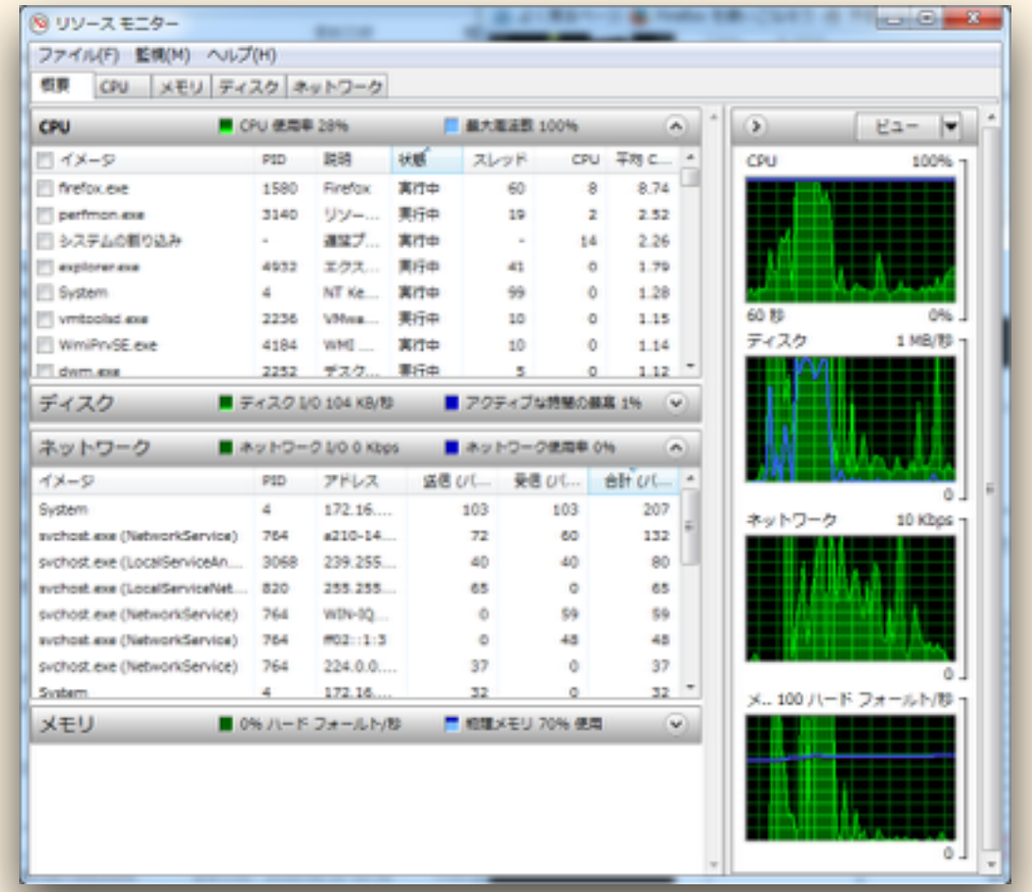
- Wireshark
- Fiddler
- 詳細ログ
- 見れたらラッキー？



システム状態の調査

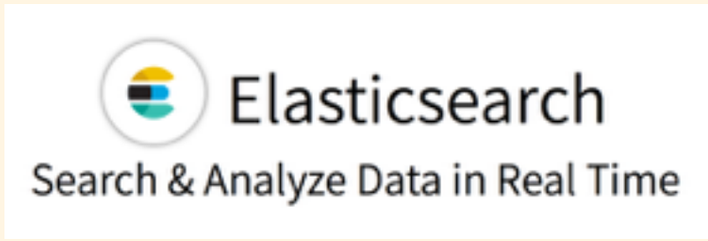
モニタリングツール

- top, stat 系, lsof など
- タスクマネージャー, リソースモニター
- Windows Sysinternals



ログやステータスを集めて監視

- MRTG, Nagios, Cacti, Munin
- Fluentd, Embulk
- nxlog
- Elasticsearch, Kibana, Logstash
- Beats (Winlogbeat, Packetbeat)



あれ？

ネットワーク／サーバオペレーションとそんなに変わらない？

セキュリティ
オペレーションの要素

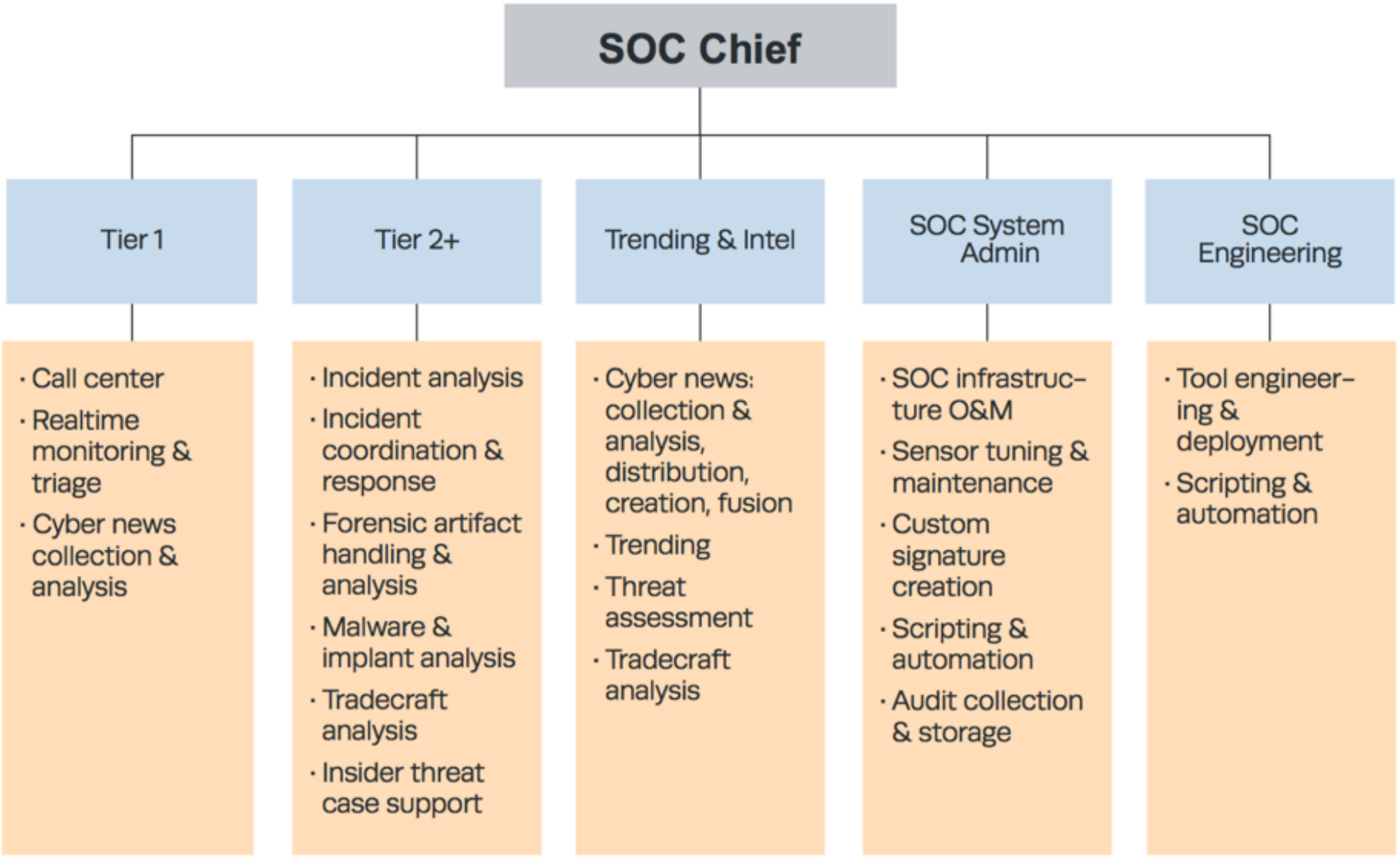


Figure 10. All Functions of CND in the SOC

Ten Strategies of a World-Class Cybersecurity Operations Center
https://www.mitre.org/publications/all/ten-strategies-of-a-world-class-cybersecurity-operations-center

SOC の構成要素

- リアルタイム監視、トリアージ
- 事件の調査、分析、対応
- 情報収集と分析
- 基盤システムの運用管理
- ツールなどの開発と展開

それにくわえて…

- 各セクションのマネジメント
- 関係者間のコーディネーション
- …広すぎない？

余談：Yahoo 知恵袋にて

セキュリティエンジニアを将来の夢にしている…

ID非公開さん　　2016/4/17 16:01:05

セキュリティエンジニアを将来の夢にしているのですが
現在高2なのですが現在大学選びに悩んでいて、
セキュリティエンジニアは自分が技術を持っていることをアピールさえできれば
学歴はそこまで気にする必要はないと聞いたのですが、
関西大学、総合情報学部の社会情報システム系かコンピューティング系もしくは専門学校（ECCコンピューター専門学校、ネットワークエンジニア専攻）

http://detail.chiebukuro.yahoo.co.jp/qa/question_detail/q12158290662
「知恵袋 セキュリティ」で検索

htokumarさん　　2016/4/19 11:37:52

業界のものです。
今高2ということは、大卒で就職するとしたら6年後ですね。6年後の就職しやすさの状況は正直誰も分からないと思います。現在セキュリティ業界は、（なぜか）東京オリンピック開催に向けて活況ですが、6年後だと東京オリンピックも終わっていますし。

htokumarさん　　2016/4/19 11:37:52

業界のものです。

今高

しや

は、

オ!

ベストアンサーに選ばれた回答

tetsu_talowさん　　2016/4/20 10:25:32

徳丸さんにご推薦を頂いて光栄です。立命館大学の上原です。

私からも補足を。

セキュリティの分野で今、最先端で活躍しておられる方の中には、少なからず「大学でも専門学校でもセキュリティのことを学ばなかった」方がお

htokumarさん

2016/4/19 11:37:52

業界のものです。

今高

しや

は

ベストアンサーに選ばれた回答

tetsu_talowさん

2016/4/20 10:25:32

sunakichiwideさん

2016/4/20 11:58:52

慶応の砂原です。

徳丸さんも上原先生も言っておられますが、まず学歴は関係無いというのは今の状況であって、将来もそうかと言われるとわからないでしょう。僕自身も学歴がすべてではないと思う方ですが、「学歴」という印は言葉を尽くして説明しないでもわかりやすい印の一つではあると思っています。ただ、ここでいう学歴は、どこで何を誰の元で学んだのかということです

上原です。

る方の中には、少なか

学ばなかった」方がお

htokumarさん

2016/4/19 11:37:52

業界のものです。

今高

しや

は

ベストアンサーに選ばれた回答

tetsu_talowさん

2016/4/20 10:25:32

sunakichiwideさん

2016/4/20 11:58:52

慶応の砂原です。

徳丸さんも上原先生も言っておられますが、まず学歴は関係無いというの

は今

自身

尽く

ただ

上原です。

る方の中には、少なか

お

ntsuji1337さん

2016/4/20 15:37:26

私は質問者様が候補に挙げている専門学校を14年ほど前に卒業しています

。

また、質問者様の年齢の頃に初めてコンピュータを触りました。

これも何かの縁かと思い回答します。

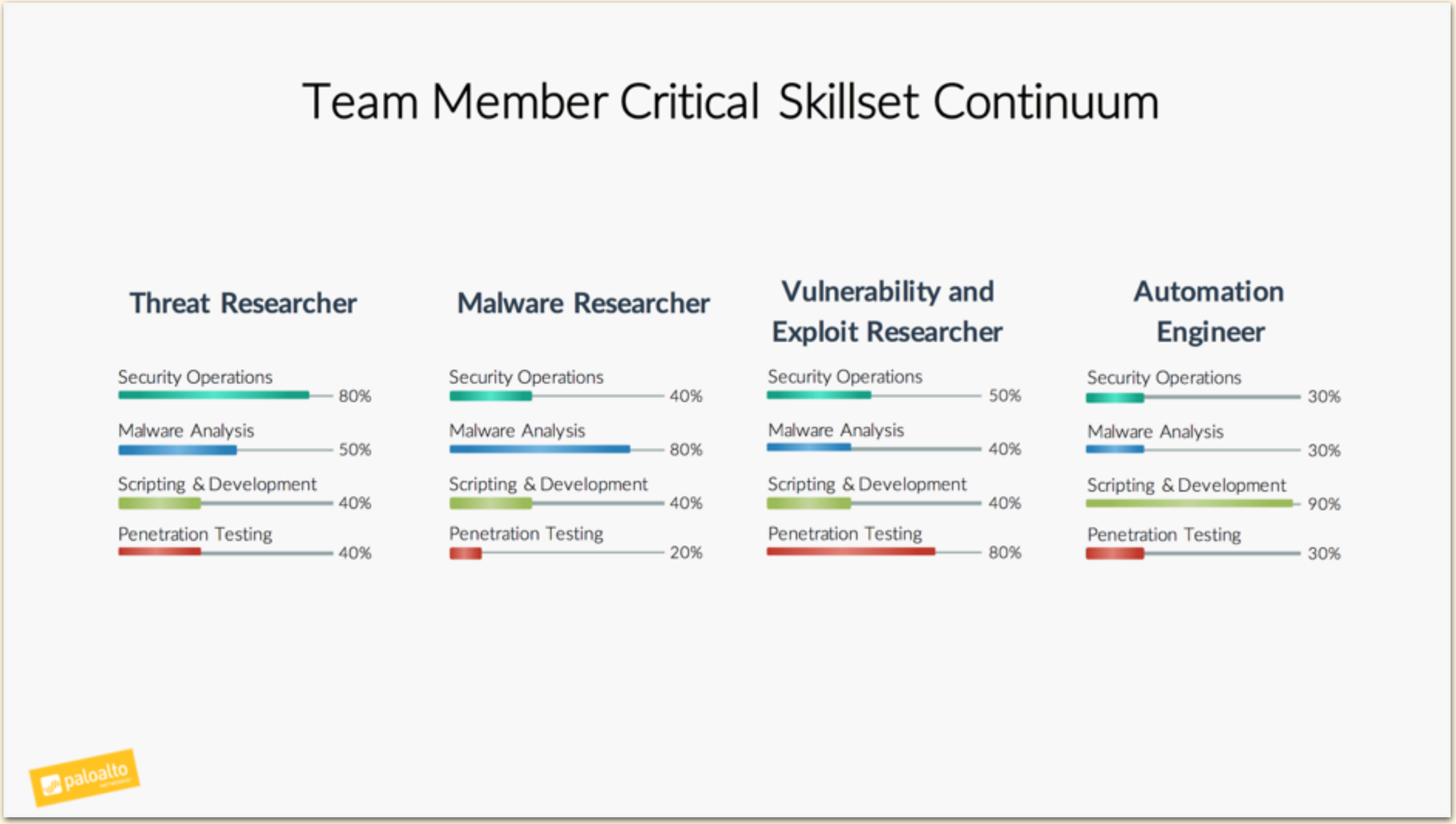
砂原先生の回答から

- セキュリティという分野は、総合芸術だと思っています
- 技術も重要ですが、マネジメント、法律、社会制度、倫理、政策といったことも学ばなければなりません
- 俯瞰して全体を見る力をつけることができたら、新しい問題が発生してもさまざまな知識を応用して問題に取り組むことができるでしょう

セキュリティオペレーション

- セキュリティという分野の一端を担っている
- 現状と、移り変わる現実に対応していく
- 幅広い人材による組織的な対応
- 組織をこえた連携の必要性

チームメンバーのスキルセット



Powering Prevention: Building a Global Security Response Team
https://speakerdeck.com/xen0ph0n/powering-prevention-building-a-global-security-response-team

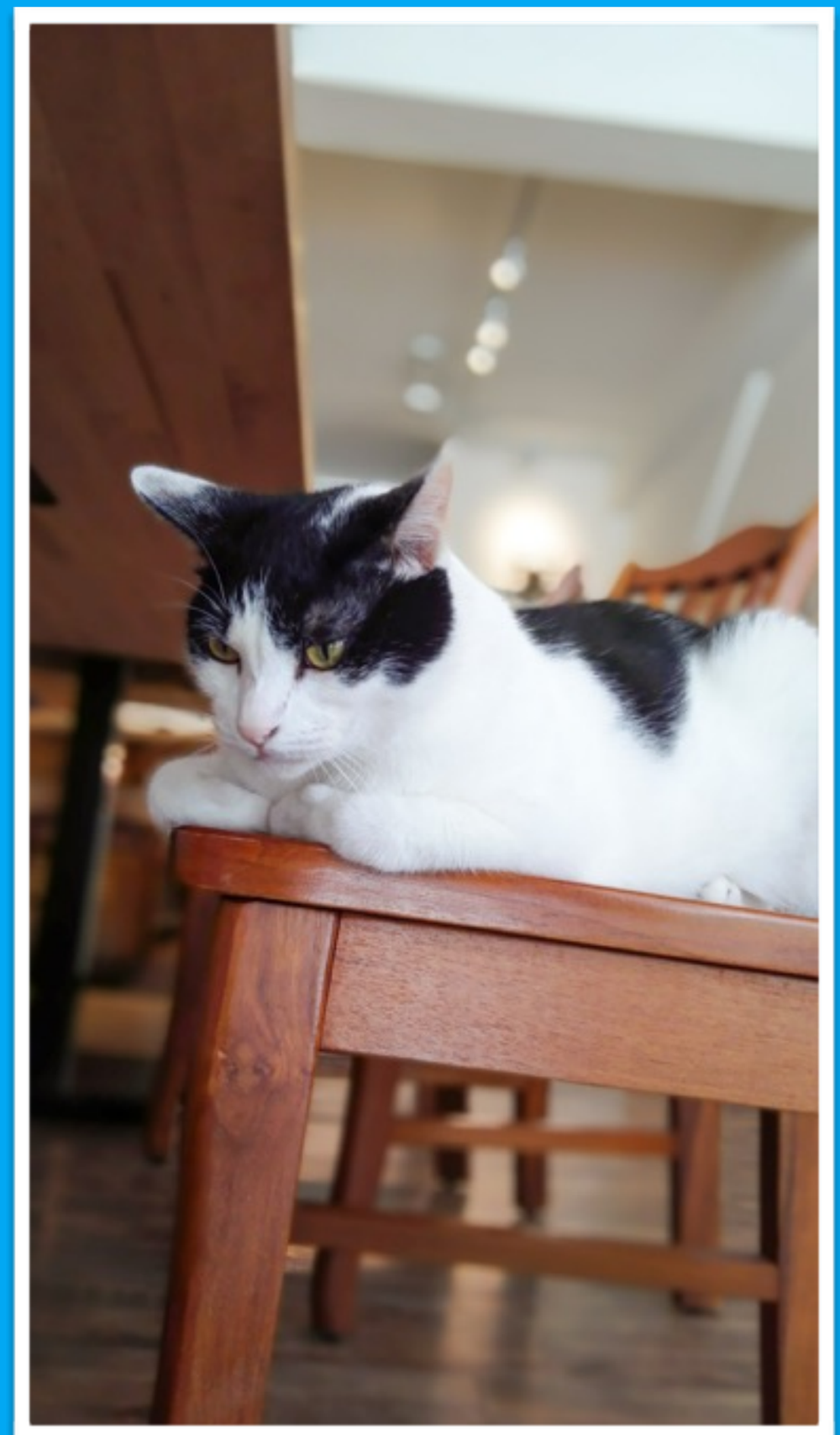
JANOG34 印象的なセッション

- 学生：何を勉強したらネットワーク屋になれますか？
- 企業側：何でもいいので、面白いと思ったことを全力でしてきてください
- セキュリティ人材育成
- セキュリティ人材を目指すには？

ネットワーク企業は高等教育に一体何を求めるか、あるいは何も求めないか
http://www.janog.gr.jp/meeting/janog34/program/nwedu.html

もっと
セキュリティっぽい
道具たち

隔離環境



隔離環境が必要

- 怪しいものを踏んでみるため
- 隔離実行
  - sandbox, fakenet, Honeypot
- 外部サンドボックスサービス
  - VirusTotal, Deepviz, Malwr

脆弱性スキャン
ペネトレーションテスト

脆弱性

- Vuls: VULnerability Scanner
  - この後の BoF をお楽しみに！

- Metasploit, Nessus, Nmap, OpenVAS

metasploit®

NMAP

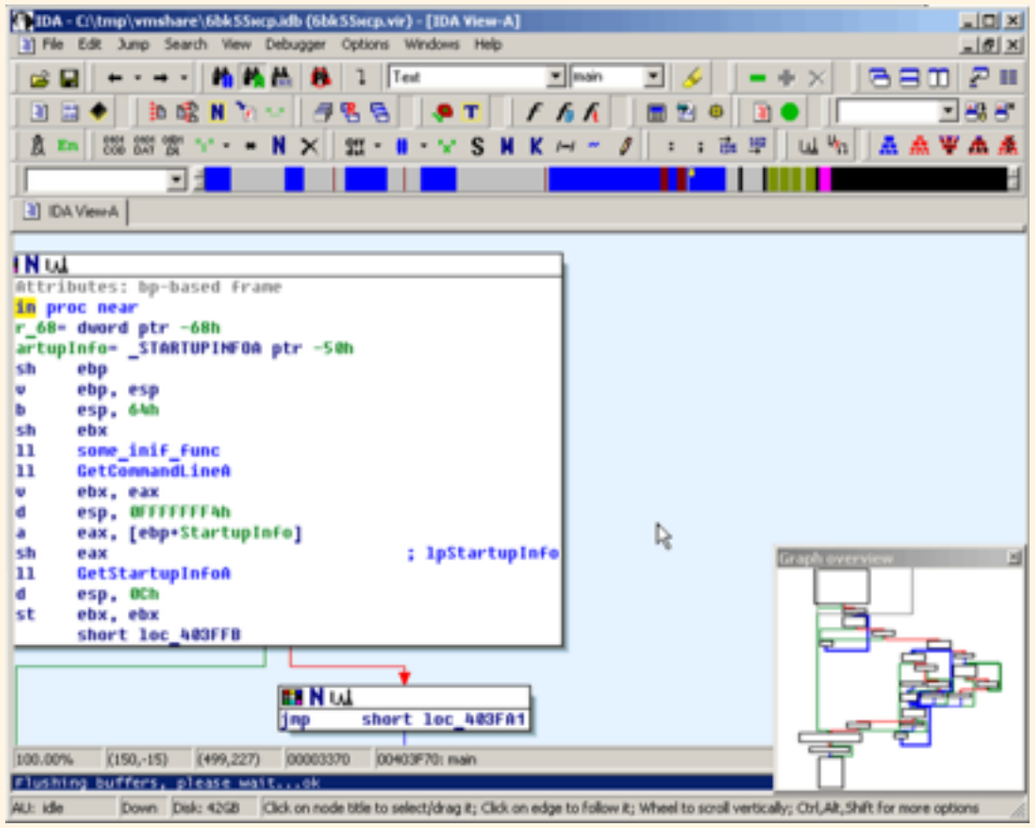
Nessus®
vulnerability scanner

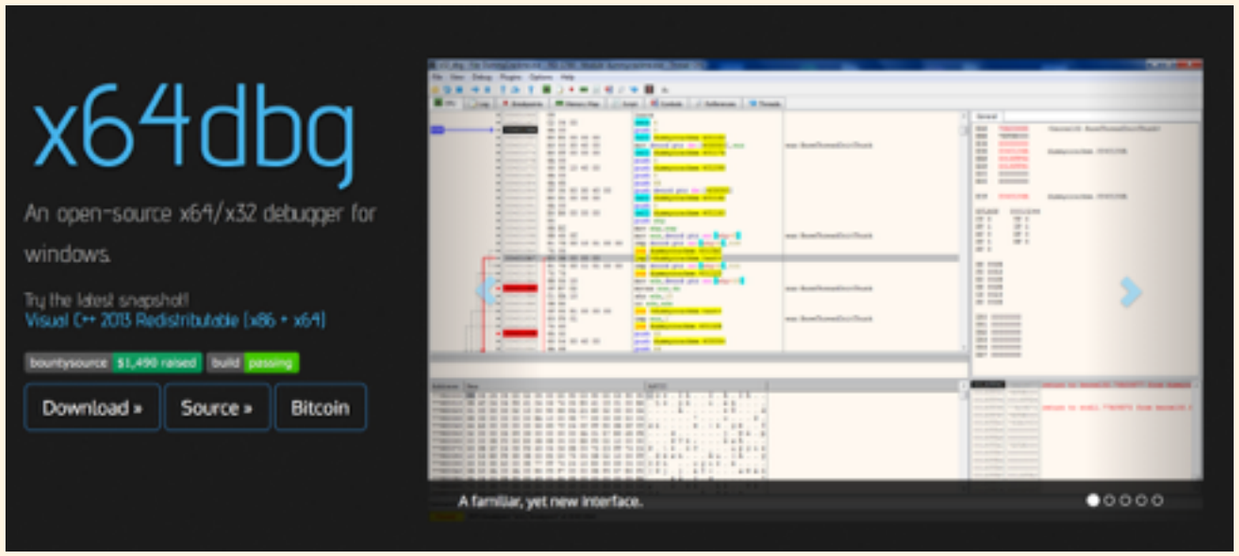
OpenVAS
Open Vulnerability Assessment System

マルウェア解析
フォレンジック

解析ツール

- リバースエンジニアリング
- IDA Pro, OllyDbg, x64dbg
- X-Ways forensics, EnCase
- 痕跡
- タイムライン





その他のツール

運用で人気のツールなど

- 差分表示：設定変更時の確認など
  - diff, winmerge, rekisa
- クリップボード管理：さまざまなコピペ
- スクリプト：shell, Python, Perl, awk
- Chrome拡張機能：チームで共有

IIJで使っているツール

ブラウザ脆弱性チェッカー

- 社員が日常的にアクセスするところに設置

ブラウザ脆弱性チェッカー

詳細版

ソフトウェア	脆弱性	バージョン	配布元リンク
Windows NT	無し	6.1	更新 削除
Firefox	無し	46.0.0.0	更新 削除
Java	無し	1.8.0.91	更新 削除
Flash	有り	21.0.0.213	更新 削除
Shockwave	無し	未検出	更新 削除
AdobeReader	有り	15.10.20056.36345	更新 削除
Silverlight	無し	5.1.41212.0	更新 削除
QuickTime	無し	未検出	更新 削除
RealPlayer	無し	未検出	更新 削除
Office	無し	14	更新 削除

<<判定結果>>
お使いのブラウザ、プラグイン等に脆弱性のあるバージョンが見つかりました。
速やかに該当ソフトウェアをアップデートしましょう。(アップデートが存在しない場合は無効化推奨)
うまくパッチが適用できない場合はこちら(BIRD-IS FAQ)

備考

- 頻出するOdayに備えて不要なプラグインの無効化
  Firefoxは「クリックして実行」の設定状態を検出不可能
- Java/Flash等は更新時に余計なソフトウェアを入れよ

セキュアな設定 (0day対策)

- プラグインの自動実行制限
  IE(ActiveX フィルター)、Firefox(クリックして実行)、
- Javaアプレットの無効化
- EMETの導入

FAQ

ブラウザ脆弱性チェッカー

ソフトウェア	脆弱性	バージョン	配布元リンク
Mac OS X	無し	10.11	更新 削除
Firefox	無し	47.0.0.0	更新 削除
Java	無し	未検出	更新 削除
Flash	有り	21.0.0.242	更新 削除
Shockwave	無し	未検出	更新 削除
AdobeReader	無し	未検出	更新 削除
Silverlight	無し	未検出	更新 削除
QuickTime	無し	未検出	更新 削除
RealPlayer	無し	未検出	更新 削除
Office	無し	未検出	更新 削除

<<判定結果>>
お使いのブラウザ、プラグイン等に脆弱性のあるバージョンが見つかりました。
速やかに該当ソフトウェアをアップデートしましょう。(アップデートが存在しない場合は無効化推奨)
うまくパッチが適用できない場合はこちら(BIRD-IS FAQ)

ブラウザ脆弱性チェッカー

詳細版

ソフトウェア	脆弱性	バージョン	配布元リンク
Windows NT	無し	6.1	更新 削除
Firefox	無し	46.0.0.0	更新 削除
Java	無し	1.8.0.91	更新 削除
Flash	無し	21.0.0.242	更新 削除
Shockwave	無し	未検出	更新 削除
AdobeReader	無し	15.16.20039.54196	更新 削除
Silverlight	無し	5.1.41212.0	更新 削除
QuickTime	無し	未検出	更新 削除
RealPlayer	無し	未検出	更新 削除
Office	無し	14	更新 削除

<<判定結果>>
お使いのブラウザ、プラグイン等に脆弱性のあるバージョンは見つかりませんでした。

パターンリビジョン:[redacted]

備考

- **頻出する0dayに備えて不要なプラグインの無効化、または後述のセキュアな設定にて対応しましょう。**
  Firefoxは「クリックして実行」の設定状態を検出不可能な為、設定しても0day時にはNG判定表示になる場合があります。
- Java/Flash等は更新時に余計なソフトウェアを入れようとします。必ず拒否しましょう。

[redacted]

セキュアな設定（0day対策）

- プラグインの自動実行制限
  IE(ActiveX フィルター)、Firefox(クリックして実行)、Chrome(プラグインコンテンツをいつ実行するかを選択する)
- Javaアプレットの無効化
- EMETの導入

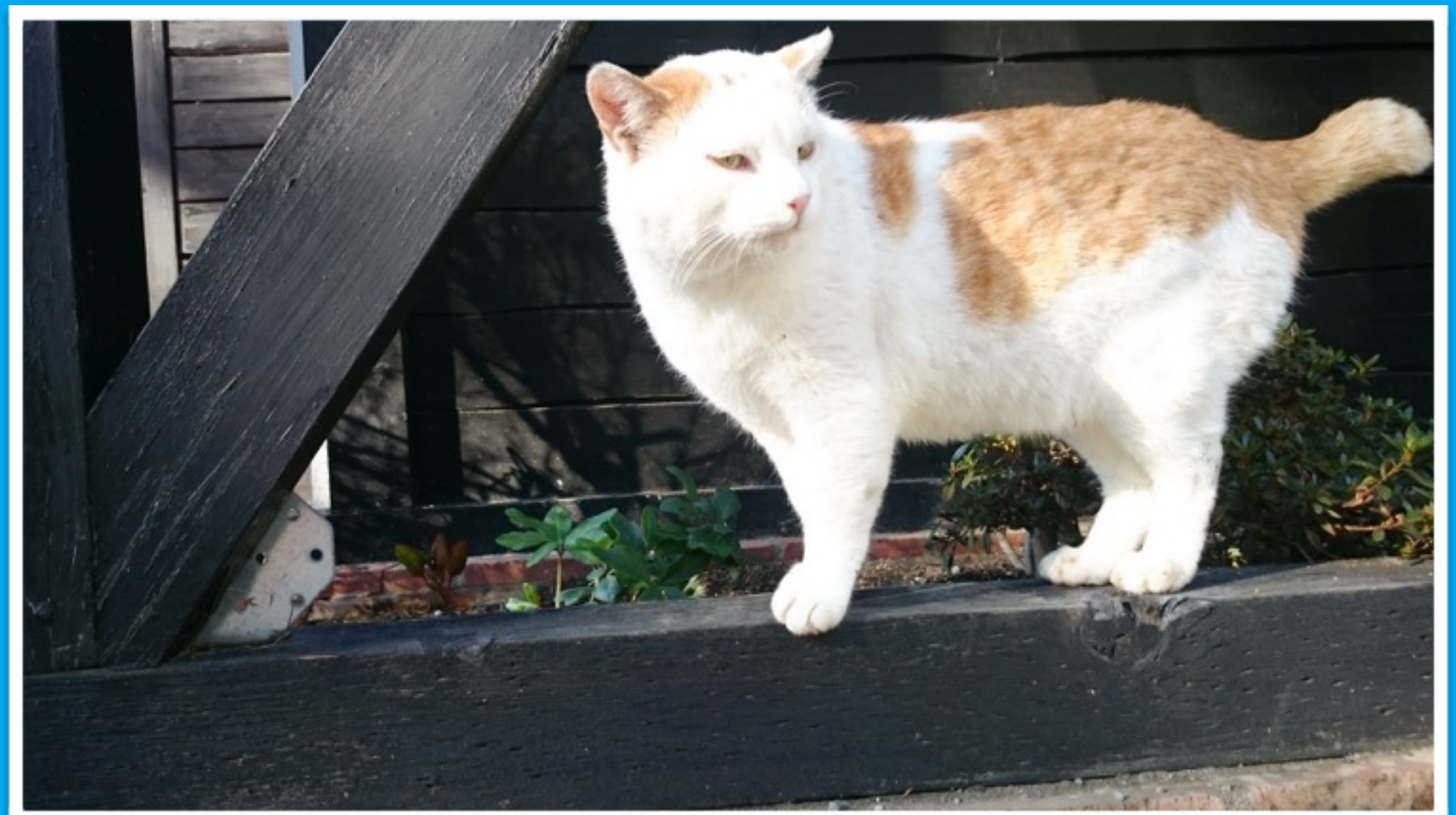
FAQ

ネットワークスキャン

- 定期スキャンして、おかしいものをレポート
  - 自社グローバルアドレス
  - 社内のサーバセグメント
- 情勢に応じてトピック的に観測

事案の分析と対応
インシデントレスポンス

事案対応



事案対応の状態管理

- チケットを使った管理、運用
  - Trac, Redmine
- 情報収集、作成、更新などは手作業
  - テンプレ的なものはある

状況調査
分析

調査で素性をあきらかにする

- DNS, whois
- Google
- aguse.jp
- DomainTools
- VirusTotal
- 各種ブラックリスト

分析

- 収集した情報を元に事案を分析
    - 人が考える
- 分析結果から対応を決定
    - 人が決断する

情報収集

一般的な情報

- Twitter
- RSS Feed
- Google Alerts
- はてぶ
- 検索

脆弱性情報

- 自動収集しやすい
    - サイト、形式などがある程度決まっている
    - 定期的に出る
- JPCERT, IPA, JVN, NVD, CVE

個人的なおすすめ

OWASP

- The Open Web Application Security Project
  - OSS のコミュニティ
  - Top10, ZAP Proxy, Cheat Sheet など
  - OWASP Japan も活発に活動してます
  - http://www.owasp.org/

Hardening Project

- 「守る」技術を競う
- チームで EC サイトを守り売り上げを上げる
  - 様々な役割の人が参加
- 結果発表が動画公開されてます
- MINI Hardening もやってます

Q&A

私が聞きたいこと

- Q: Netflow v9 使ってる？ Cisco NBAR 使えそう？
- Q: 外部サービスが便利すぎる問題
  - VirusTotal, ドメイン調査, 脆弱性検査
  - 魚拓, 共有ブックマーク
- Q: 情報をまとめるダッシュボード
  - 欲しい... 作るしかないか...

Webサービス図鑑／スタートページ：iGoogle
http://www.itmedia.co.jp/bizid/articles/0910/13/news074.html

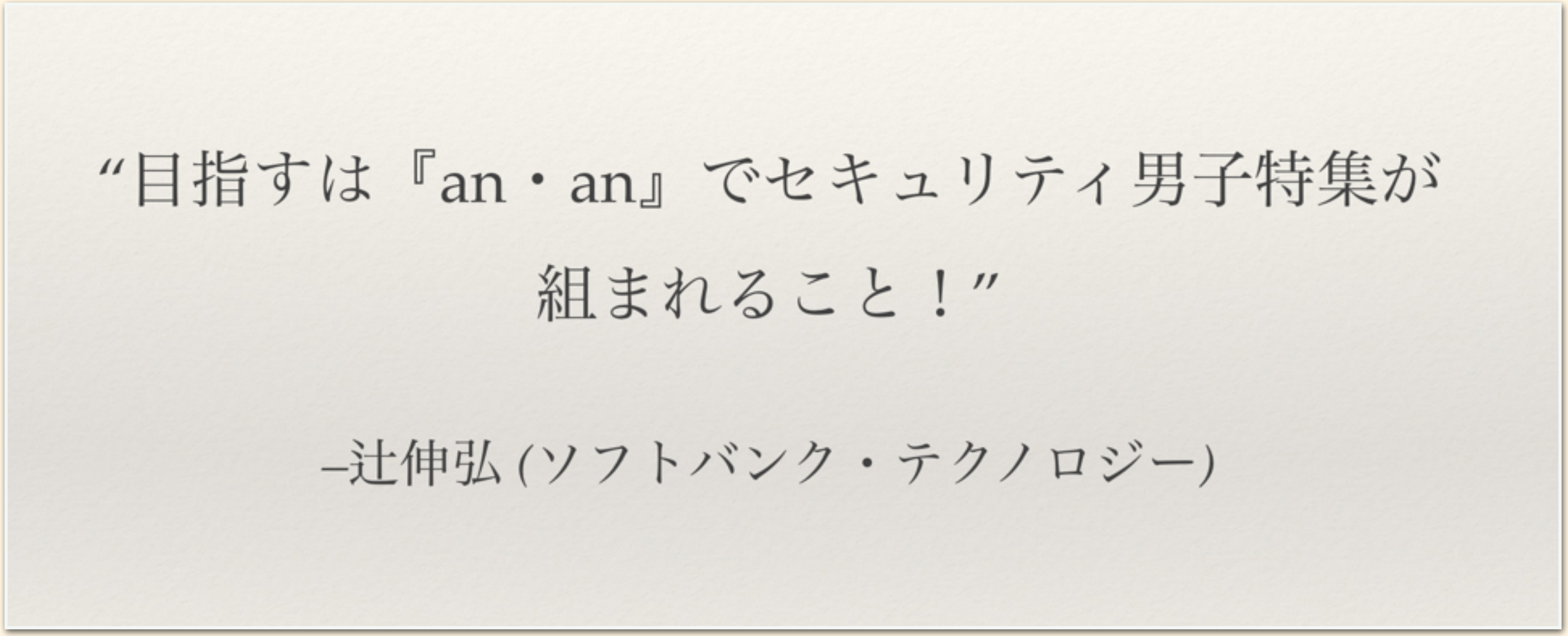
Q&A

- こんなものを探してるけど誰か知らない？
- もっといいのを知ってるぜ！
- こんなの作ったぜ！
    - ぜひ BoF で話してください

おまけ

余談：JANOG34 初心者LT

- みんなで高めるセキュリティ



みんなで高めるセキュリティ @ JANOG34 高松 (Light) LT

http://www.slideshare.net/ymomoi/201407-janogltsecurityop

ntsuji さん anan に出ちゃったよ！

X BRAND　人気雑誌の最新記事が読める

ログイン
IDでもっと便利に[新規取得]

HOME　FASHION　GOURMET　PRODUCT　VEHICLE　BEAUTY　TRAVEL　LIFESTYLE　ENTE

HOME > カテゴリー覧 > ライフスタイル > あなたのID ＆ パスワード、結構バレバレです！

anan

最新!!　No.2010
毎週水曜日発売
マガジンハウス

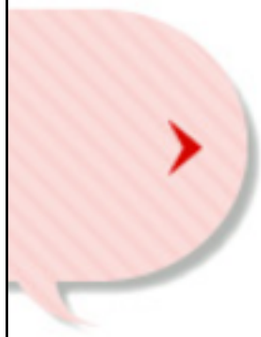
いいね！ 312　ツイート　B!

前へ　1/5　次へ

2016/04/07

**あなたのID＆パスワード、
結構バレバレです！**

近頃よく耳にするのは、アカウントの乗っ取りや、なりすましなど、ID＆パスワードを盗まれてしまう被害。本人は気をつけているつもりでも、じつは管理がかなりずさんな人が多いよう。あなたは本当に大丈夫？



ITセキュリティ騎士
辻 伸弘さん
ソフトバンク・テクノロジーに所属。情報セキュリティの第一人者として、講演や執筆活動など、情報発信を行う。セカオワの深瀬さんに似ているとの噂あり。

[anan No.1999 P46〜]

http://xbrand.yahoo.co.jp/category/lifestyle/19275/1.html