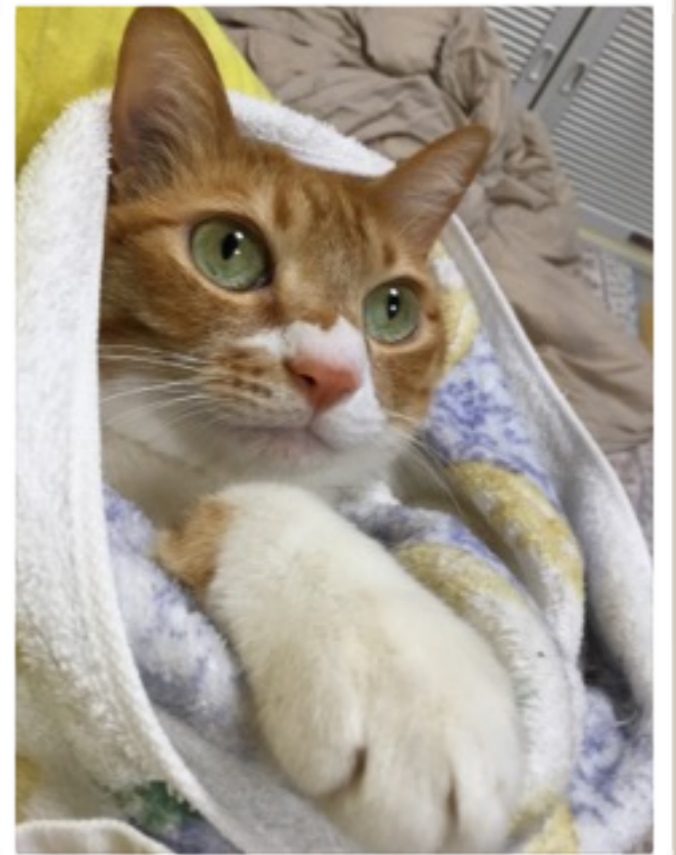


# セキュリティオペレーション： みんなどんなの使ってるの？

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](mailto:momo@iij.ad.jp)>

# 自己紹介

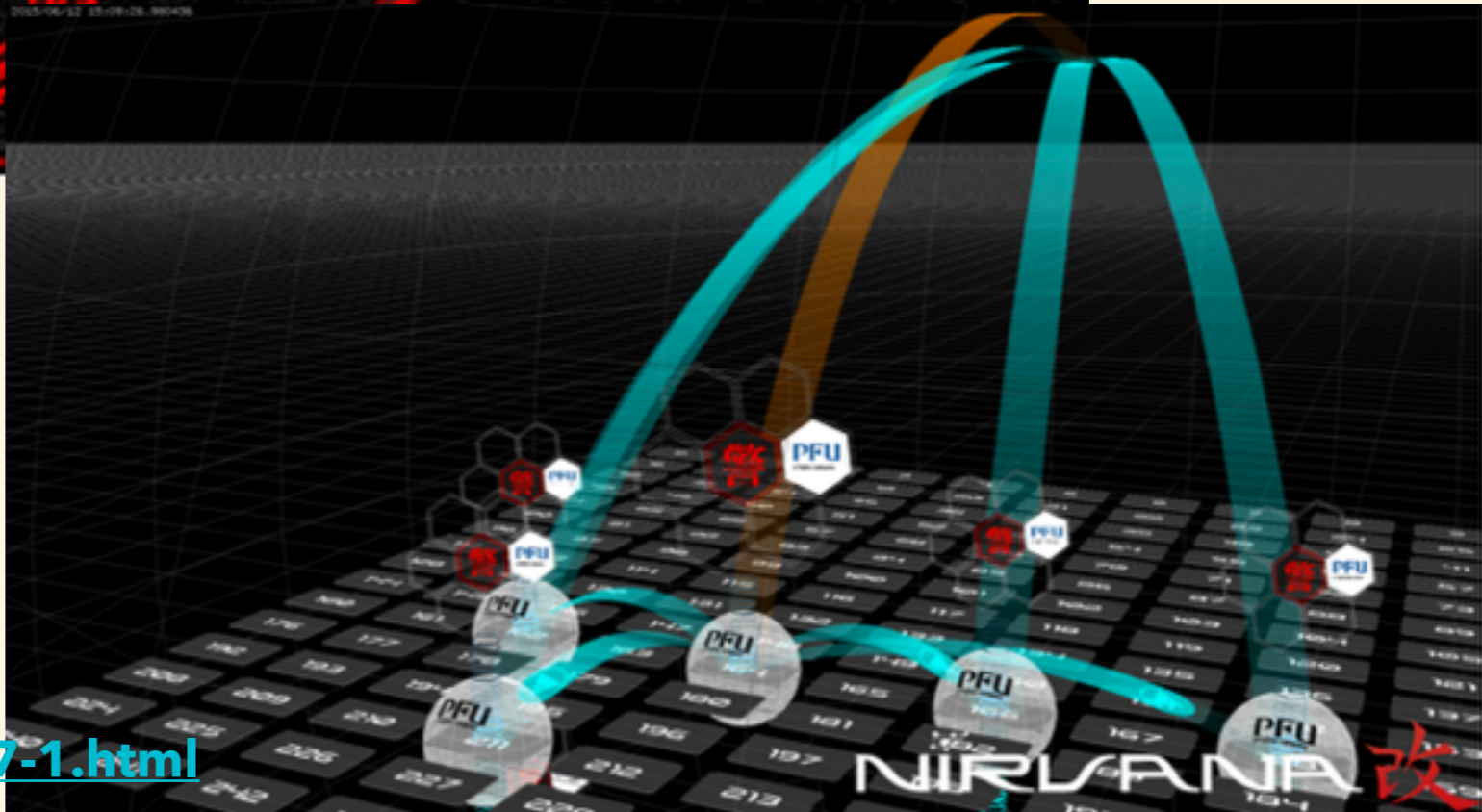
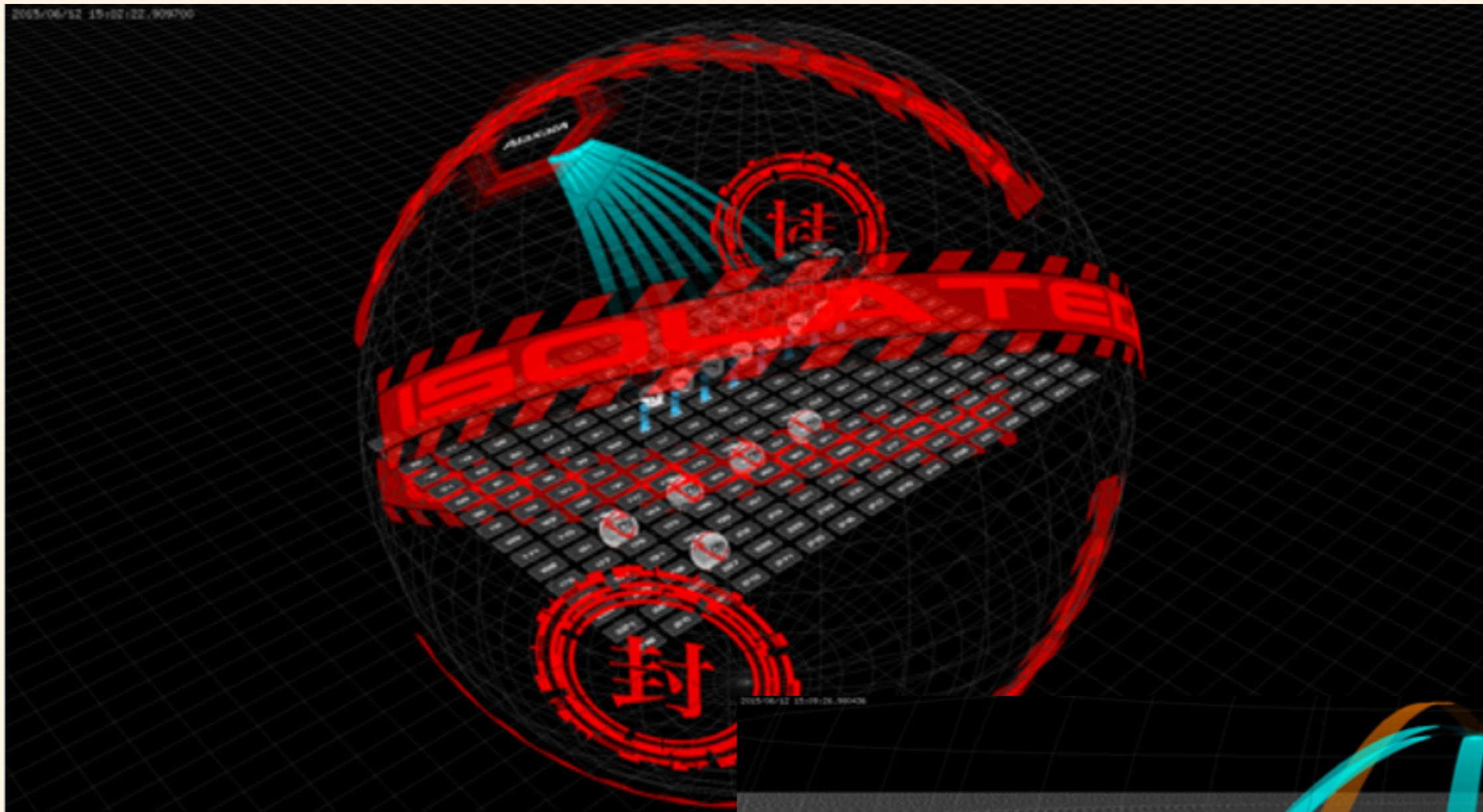
- ももい やすなり <[momo@iij.ad.jp](mailto:momo@iij.ad.jp)>
- システム開発、サービス開発やっています
- 勉強会、セキュリティ、食べ物担当
- Twitter @sbg Facebook ymomo
- ねこ、HR/HM



# 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?



Running Bash on Ubuntu on Windows!

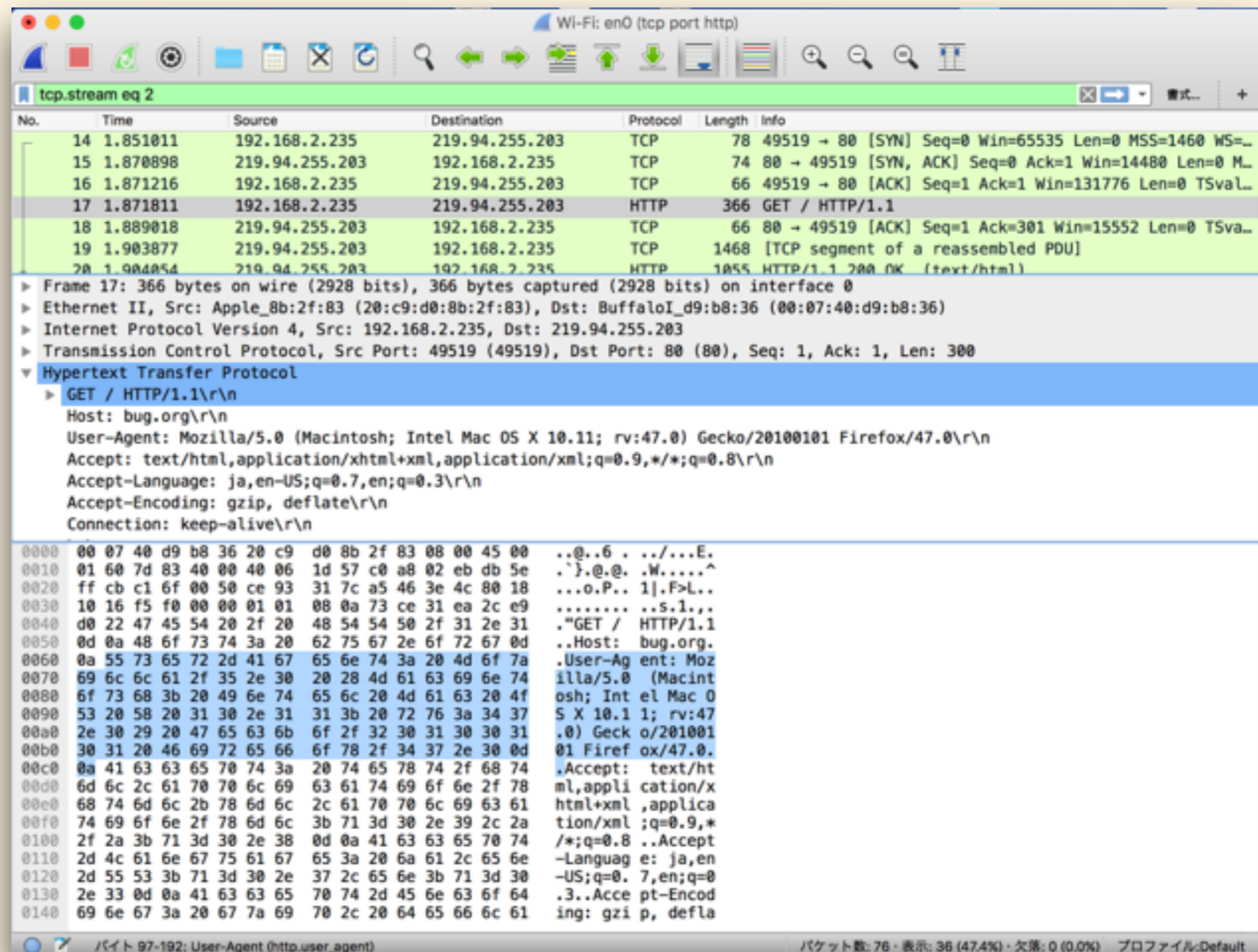
Rich Turner  
Sr. Program Manager

Russ Alexander  
Sr. Program Manager

# 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？



The screenshot shows the Wireshark interface with a network capture on the 'tcp.stream eq 2' filter. The packet list pane shows several packets, with packet 17 selected. The packet details pane shows the following information:

- Frame 17: 366 bytes on wire (2928 bits), 366 bytes captured (2928 bits) on interface 0
- Ethernet II, Src: Apple\_0b:2f:83 (20:c9:d0:8b:2f:83), Dst: BuffaloI\_d9:b8:36 (00:07:40:d9:b8:36)
- Internet Protocol Version 4, Src: 192.168.2.235, Dst: 219.94.255.203
- Transmission Control Protocol, Src Port: 49519 (49519), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 300
- Hypertext Transfer Protocol
  - GET / HTTP/1.1\r\n
  - Host: bug.org\r\n
  - User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:47.0) Gecko/20100101 Firefox/47.0\r\n
  - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8\r\n
  - Accept-Language: ja,en-US;q=0.7,en;q=0.3\r\n
  - Accept-Encoding: gzip, deflate\r\n
  - Connection: keep-alive\r\n

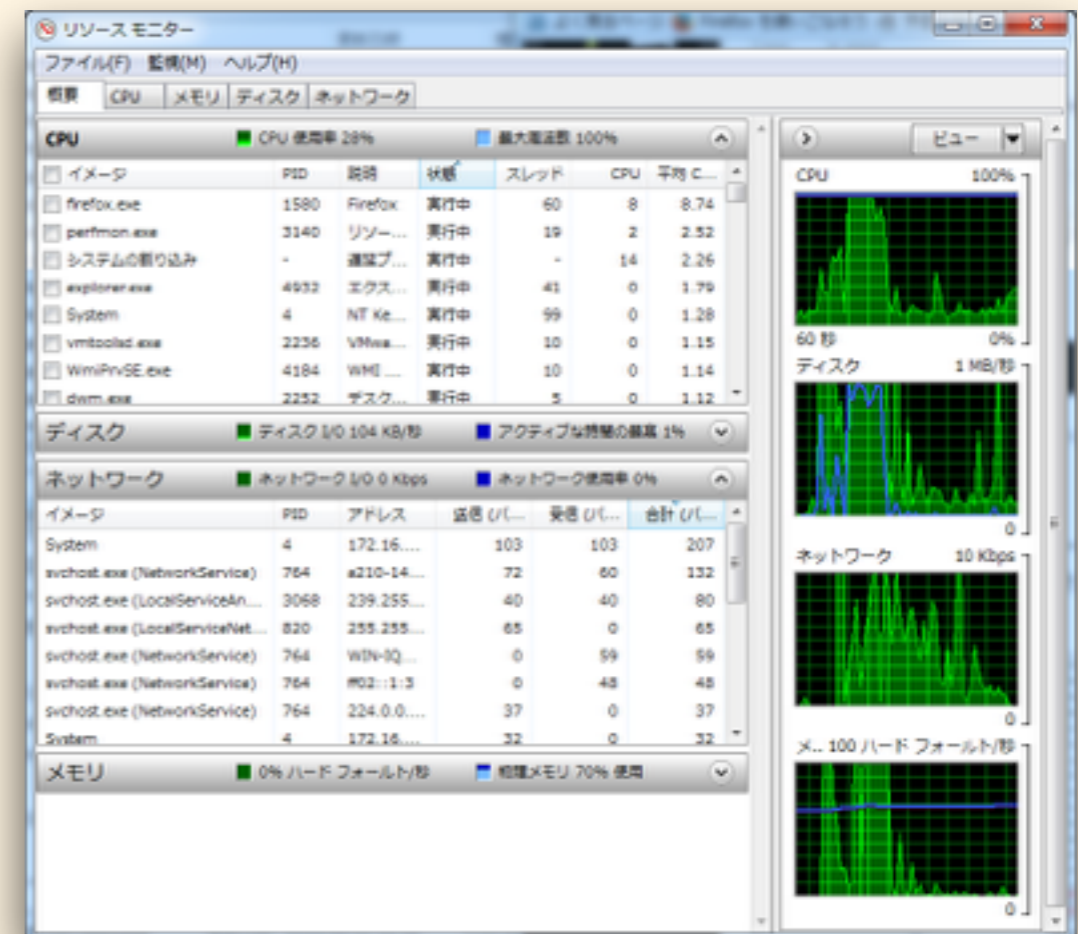
The packet bytes pane shows the raw data of the captured packet, including the Ethernet II header, IP header, TCP header, and the HTTP GET request body.

# 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



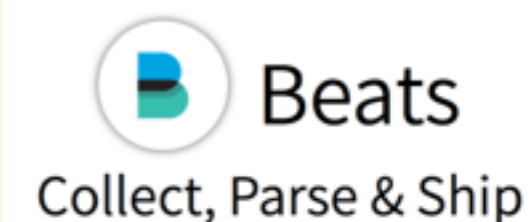
- nxlog



- 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



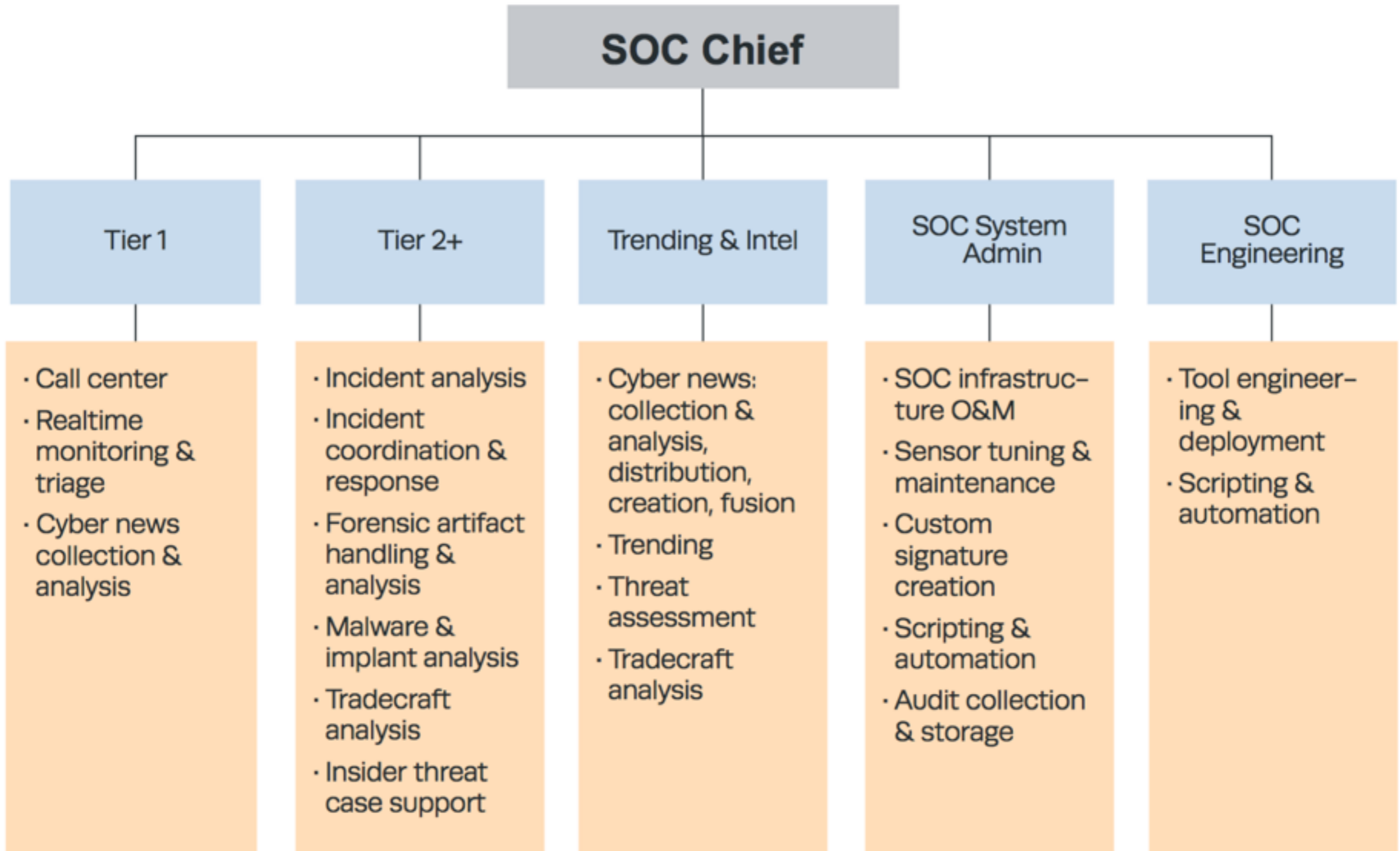


Figure 10. All Functions of CND in the SOC

# SOCの構成要素

- リアルタイム監視、トリアラージ
- 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…



シェア

5738



ツイート



はてブ

2206



知恵コレ



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](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  
し  
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  
し  
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  
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

上原です。

慶応の砂原です。

徳丸さん、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

る方の中には、少な

は今  
自身  
尽く  
ただ



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れば、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

## Team Member Critical Skillset Continuum

### Threat Researcher



### Malware Researcher



### Vulnerability and Exploit Researcher



### Automation Engineer



# JANOG34 印象的なセッション

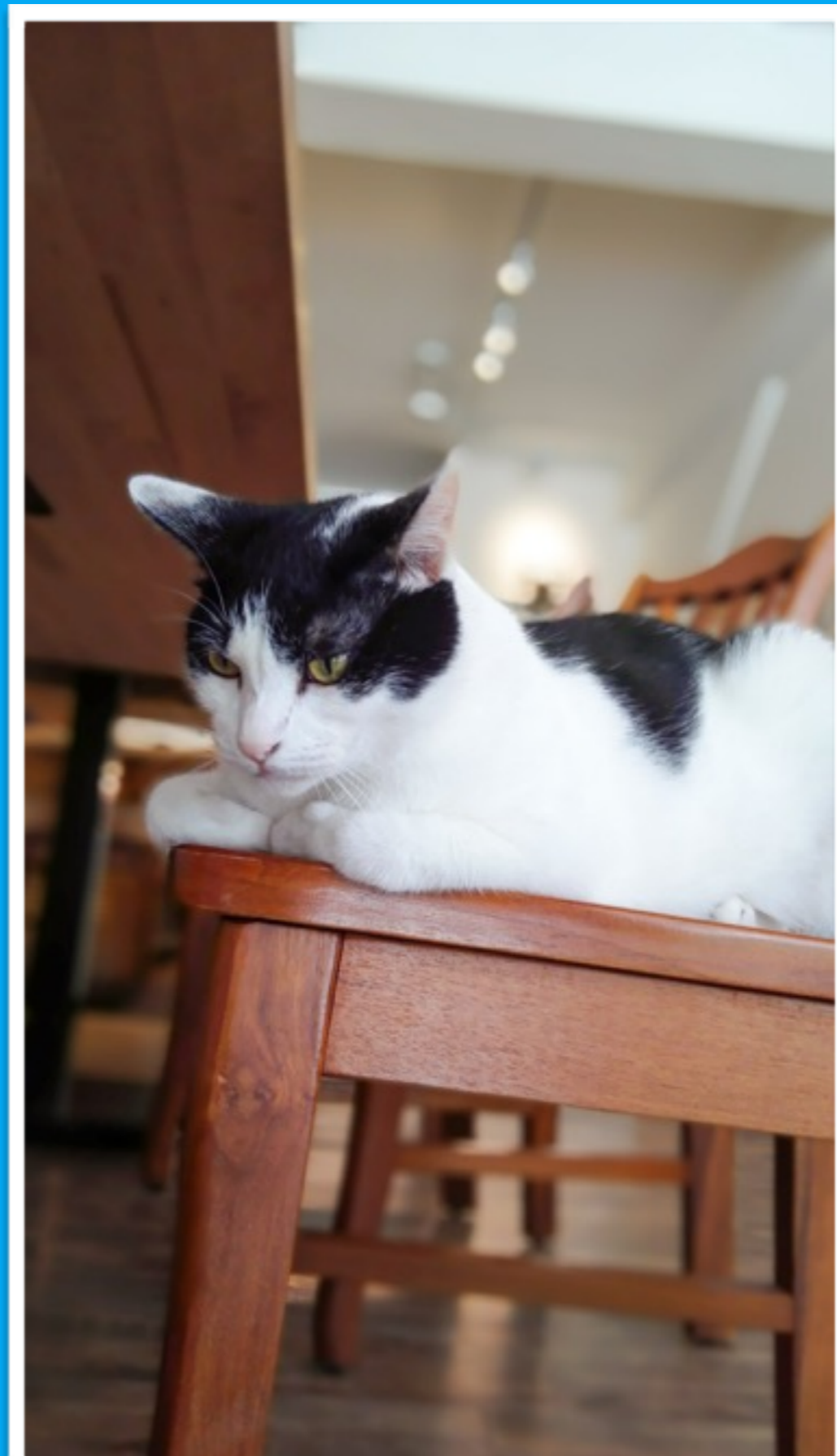
- 学生：何を勉強したらネットワーク屋になれますか？
- 企業側：何でもいいので、面白いと思ったことを全力でしてきてください
- セキュリティ人材育成
- セキュリティ人材を目指すには？

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, Honeyypot
- 外部サンドボックスサービス
  - VirusTotal, Deepviz, Malwr



VirusTotal は、疑わしいファイルや URL を分析する無料のサービスです。ウイルス、ワーム、トロイの木馬、あらゆる種類のマルウェアを素早く検出できます。

# 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

## Vuls: VULnerability Scanner

[slack join](#) [license](#) GNU General Public License v3.0

Vulnerability scanner for Linux/FreeBSD, agentless, written in golang.

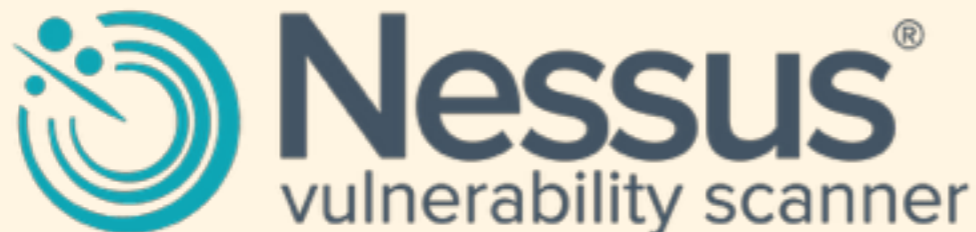
We have a slack team. [Join slack team](#)

[README in Japanese](#)

[README in French](#)

```
172.31.4.62 [ 1] CVE-2016-0799 | 10.0(High) The fmtstr function
[ 2] CVE-2016-0483 | 10.0(High) Unspecified vulnera
[ 3] CVE-2016-0494 | 10.0(High) Unspecified vulnera
[ 4] CVE-2016-0705 | 10.0(High) Double free vulnera
[ 5] CVE-2016-0720 | 7.2 (High) The join session ke
[ 6] CVE-2016-1950 | 6.8 (Medium) heap-based buffer o
[ 7] CVE-2016-0778 | 6.5 (Medium) The {1} roaming_re

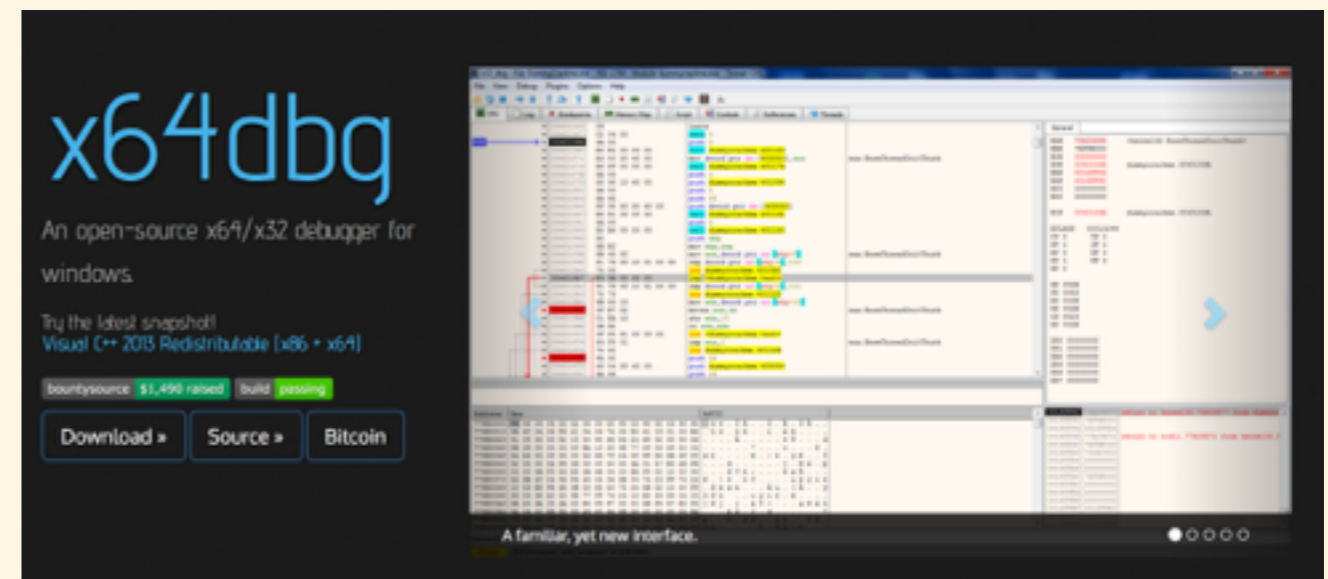
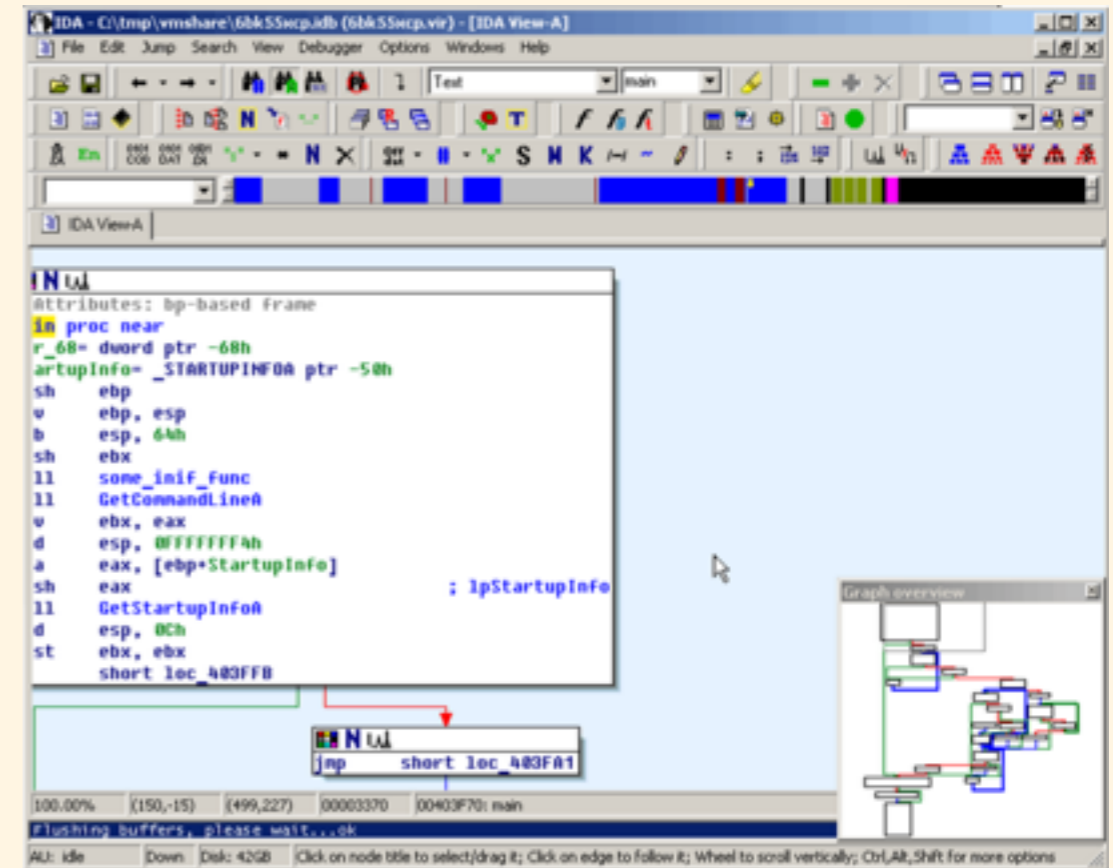
CVE-2016-1950
.....
CVSS Score
.....
6.8 (Medium) (AV:N/AC:M/Au:N/C:P/I:P/A:P)
```



# 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

The image shows a screenshot of a Confluence dashboard. The top navigation bar includes the Confluence logo, 'スペース', 'ユーザー', '作成', and 'サポート'. The main content area has a 'ダッシュボード' section with a yellow warning box that says '脆弱なブラウザです 詳細 (0日経過)'. Below this is a search bar for '社員検索' with a dropdown menu showing 'who's who' and a search button labeled '検索'. A second yellow warning box is overlaid on the page, pointing to the search bar area, with a callout box containing the text: 'ブラウザの脆弱性チェッカーサイト。使用中のブラウザが安全か確認可能。' Below the warning boxes, there are links for '各社情報一覧' and '一覧へ', and a 'New' button.

Confluence スペース ユーザー 作成 サポート

ダッシュボード 脆弱なブラウザです 詳細 (0日経過)

コラボレーション/情報共有のためのWiki、Confluenceでお使いください。

Confluence案内所：このサイトについての情報  
Confluence 事始め：初めてアクセスの方はこちら  
ブログや独り言や技術トピックなど、自由に書くことができます

社員検索  
who's who who's who検索キーワード 検索

各社情報一覧

脆弱なブラウザです 詳細 (0日経過)

ブラウザの脆弱性チェッカーサイト。使用中のブラウザが安全か確認可能。

一覧へ

開 New

■ IJグループ関連情報



## 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	<a href="#">更新</a> <a href="#">削除</a>
Firefox	無し	46.0.0.0	<a href="#">更新</a> <a href="#">削除</a>
Java	無し	1.8.0.91	<a href="#">更新</a> <a href="#">削除</a>
Flash	有り	21.0.0.213	<a href="#">更新</a> <a href="#">削除</a>
Shockwave	無し	未検出	<a href="#">更新</a> <a href="#">削除</a>
AdobeReader	有り	15.10.20056.36345	<a href="#">更新</a> <a href="#">削除</a>
Silverlight	無し	5.1.41212.0	<a href="#">更新</a> <a href="#">削除</a>
QuickTime	無し	未検出	<a href="#">更新</a> <a href="#">削除</a>
RealPlayer	無し	未検出	<a href="#">更新</a> <a href="#">削除</a>
Office	無し	14	<a href="#">更新</a> <a href="#">削除</a>

#### <<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

### 備考

- 頻出する0day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
- 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

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	<a href="#">更新</a> <a href="#">削除</a>
Firefox	無し	47.0.0.0	<a href="#">更新</a> <a href="#">削除</a>
Java	無し	未検出	<a href="#">更新</a> <a href="#">削除</a>
Flash	有り	21.0.0.242	<a href="#">更新</a> <a href="#">削除</a>
Shockwave	無し	未検出	<a href="#">更新</a> <a href="#">削除</a>
AdobeReader	無し	未検出	<a href="#">更新</a> <a href="#">削除</a>
Silverlight	無し	未検出	<a href="#">更新</a> <a href="#">削除</a>
QuickTime	無し	未検出	<a href="#">更新</a> <a href="#">削除</a>
RealPlayer	無し	未検出	<a href="#">更新</a> <a href="#">削除</a>
Office	無し	未検出	<a href="#">更新</a> <a href="#">削除</a>

#### <<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\(BIRD-IS FAQ\)](#)

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	<a href="#">更新</a> <a href="#">削除</a>
Firefox	無し	46.0.0	<a href="#">更新</a> <a href="#">削除</a>
Java	無し	1.8.0.91	<a href="#">更新</a> <a href="#">削除</a>
Flash	無し	21.0.0.242	<a href="#">更新</a> <a href="#">削除</a>
Shockwave	無し	未検出	<a href="#">更新</a> <a href="#">削除</a>
AdobeReader	無し	15.16.20039.54196	<a href="#">更新</a> <a href="#">削除</a>
Silverlight	無し	5.1.41212.0	<a href="#">更新</a> <a href="#">削除</a>
QuickTime	無し	未検出	<a href="#">更新</a> <a href="#">削除</a>
RealPlayer	無し	未検出	<a href="#">更新</a> <a href="#">削除</a>
Office	無し	14	<a href="#">更新</a> <a href="#">削除</a>

<<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。

パターンバージョン: [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て、必ず拒否しましょう。



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](#)

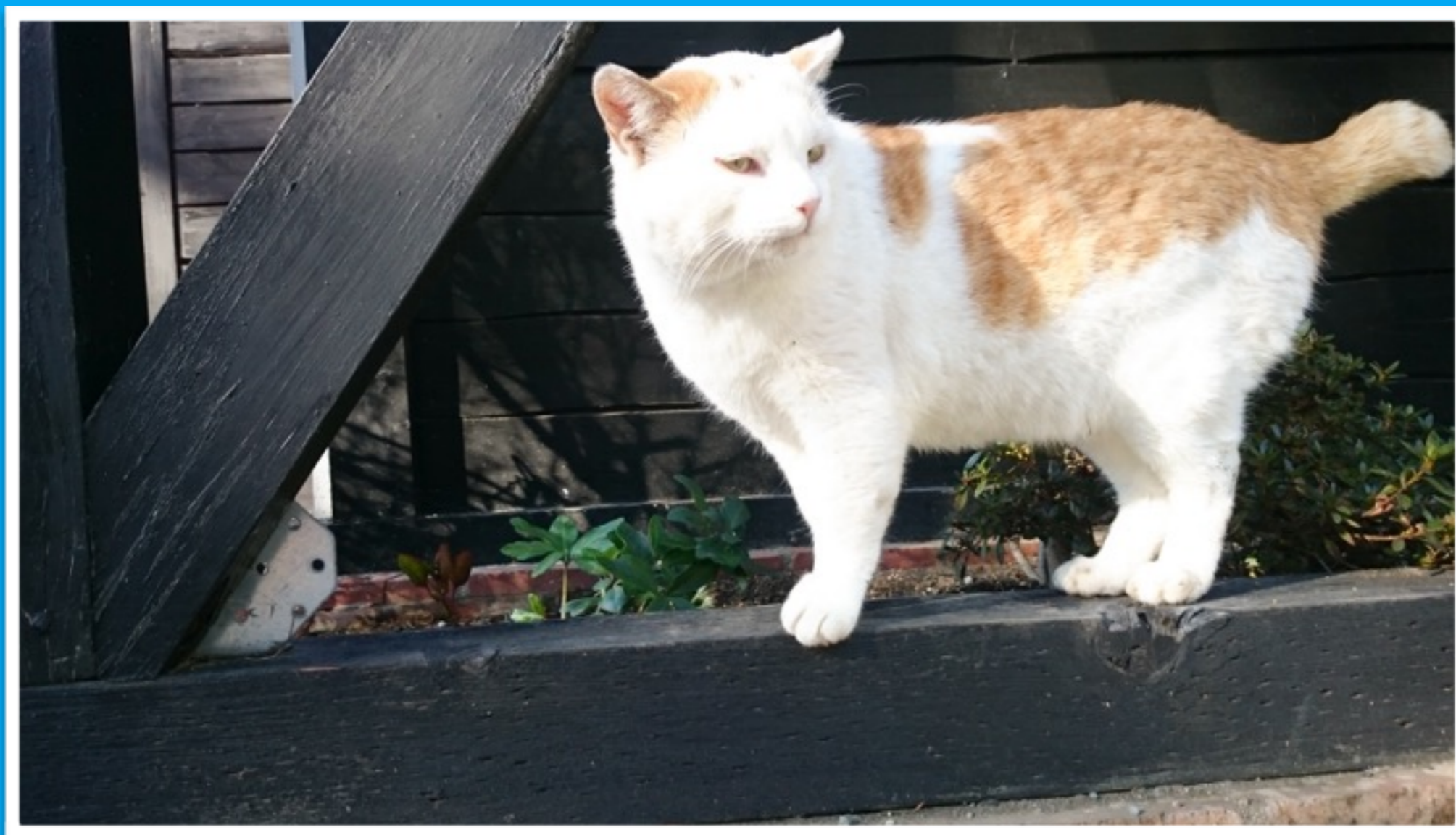
# ネットワークスキャン

- 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 も活発に活動しています
- <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います
- MINI Hardening もやっています



# 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！
- こんなのが作ったぜ！
- 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

“目指すは『an・an』でセキュリティ男子特集が  
組まれること！”

—辻伸弘 (ソフトバンク・テクノロジー)

# 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 > カテゴリー一覧 > 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！



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。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>





