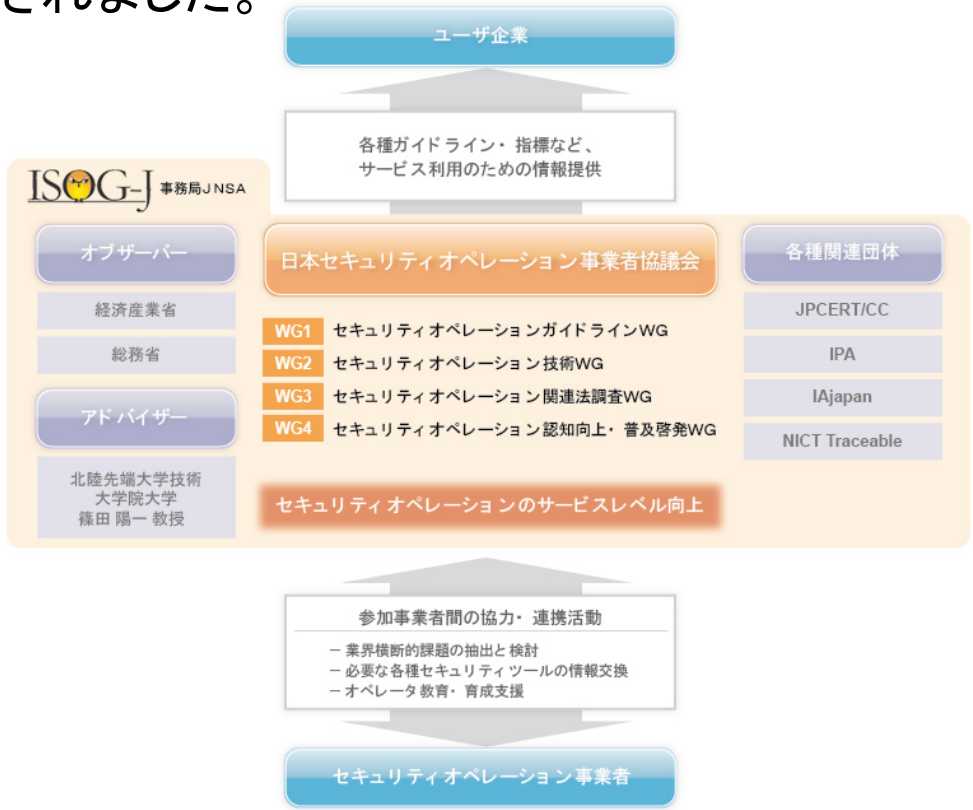
セキュリティオペレーション事業者間の新しい協力体制

2010年11月25日
ISOG-J WG2
株式会社 ラック
川口洋

ISOG-Jとは

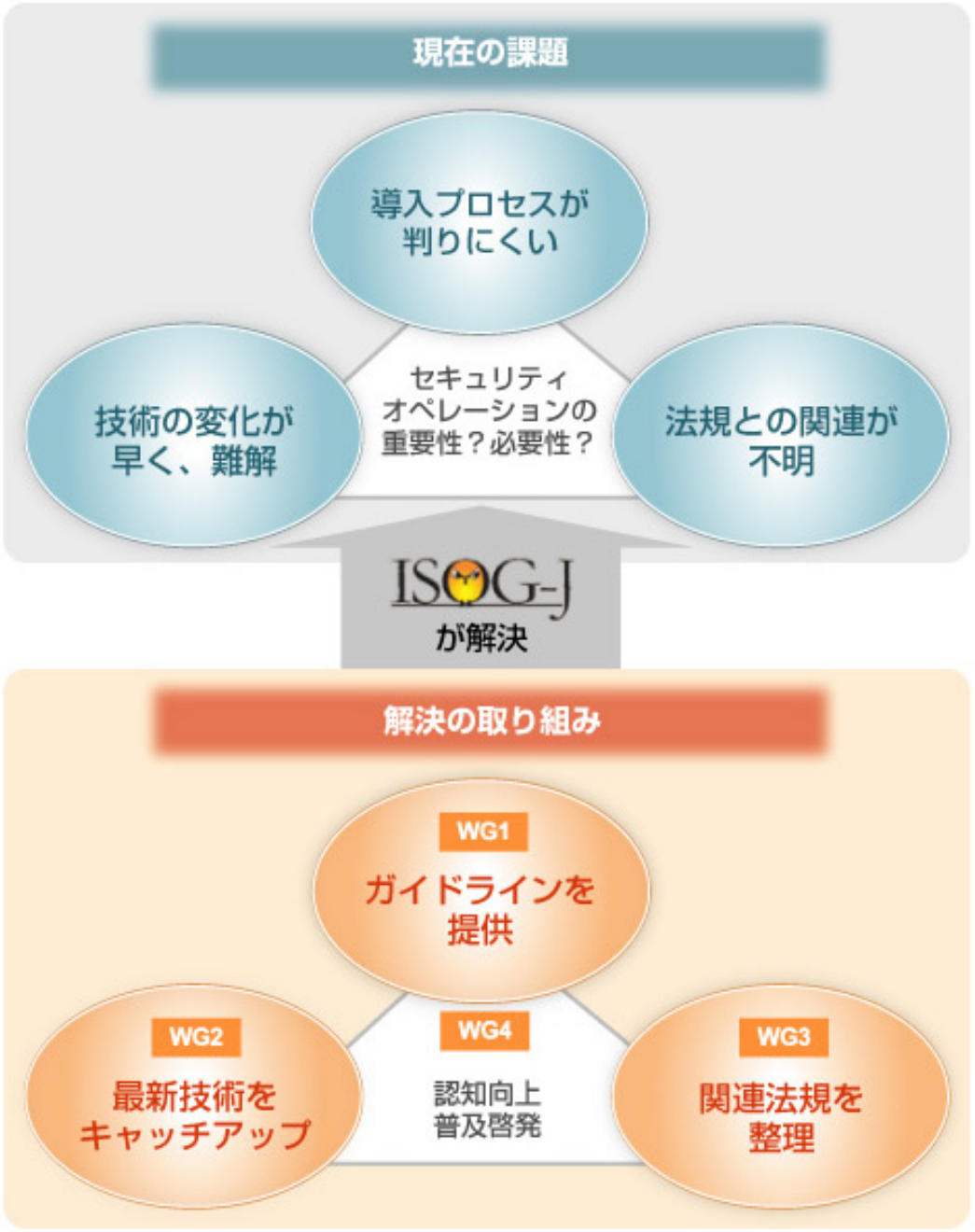
- 日本セキュリティオペレーション事業者協議会（Information Security Operation providers Group Japan 略称：ISOG-J）は、セキュリティオペレーション技術向上、オペレータ人材育成、および関係する組織・団体間の連携を推進することによって、セキュリティオペレーションサービスの普及とサービスレベルの向上を促し、安全で安心して利用できるIT環境実現に寄与することを目的として設立されました。



参加企業 17社 2010/10/22 時点

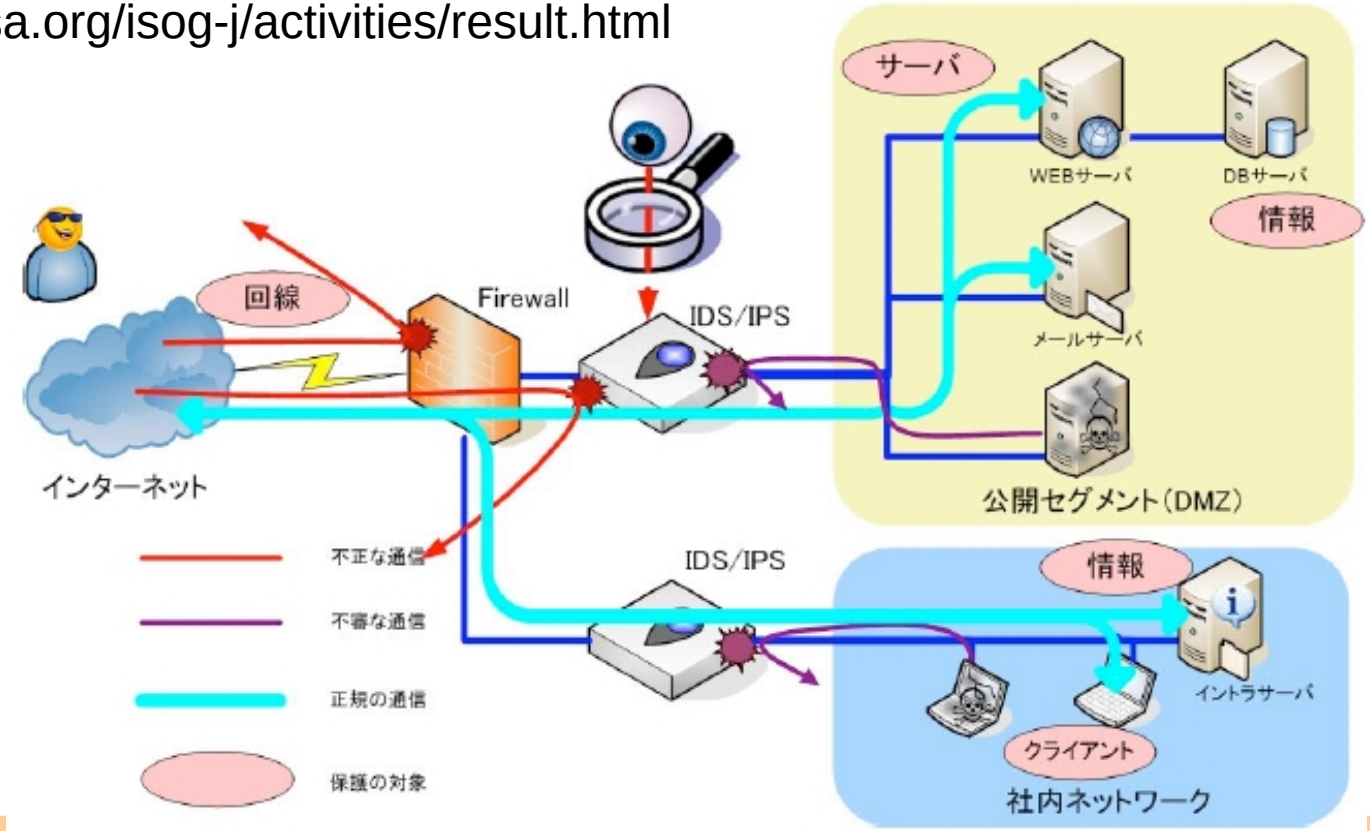
- 株式会社インターネットイニシアティブ
- NRIセキュアテクノロジーズ株式会社
- NECネクサソリューションズ株式会社
- エヌ・ティ・ティ・コミュニケーションズ株式会社
- NTTコムテクノロジー株式会社
- 株式会社NTTデータ
- NTTデータ・セキュリティ株式会社
- 株式会社 Kaspersky Labs Japan
- 日本アイ・ビー・エム株式会社
- 日本電気株式会社
- 日本電信電話株式会社
- 株式会社日立情報システムズ
- 富士通株式会社
- 株式会社富士通ソーシアルサイエンスラボラトリ
- 株式会社ブロードバンドセキュリティ
- 三井物産セキュアディレクション株式会社
- 株式会社ラック

WGの活動目的



WG1の活動

- セキュリティオペレーション事業者（MSSP）の提供するサービスを選別する際に利用できるガイドラインを策定する。
- セキュリティオペレーションガイドラインWGで2009年度に作成した、セキュリティオペレーション事業者を利用する人向けの「マネージドセキュリティサービス選定ガイドライン」
- http://www.jnsa.org/isog-j/activities/result.html



セキュリティサービスマップ

		企画	設計・構築	運用						その他
				定常			異常			
				運用・監視	分析	監査/評価	運用・監視	調査	対応	
組織		認証・資格取得支援 ポリシー・ガイドライン作成支援 経営者啓発	認証・資格取得支援 ポリシー・ガイドライン作成支援 プロジェクト管理支援	セキュリティ管理運用支援	セキュリティ管理運用支援	認証・資格審査 認証・資格監査支援 セキュリティ監査	セキュリティ管理運用支援 緊急対応	緊急対応 影響度分析 フォレンジック	対応支援	セキュリティ情報提供 セキュリティ教育・研修
アプリ	フロント (Web アプリ等)	要件定義支援	設計支援 レビュー支援 脆弱性診断	システム監視・運用 セキュリティ機器監視・運用	脆弱性診断 ログ分析	脆弱性診断	システム監視・運用 セキュリティ機器監視・運用 事後対応	対応策策定 脆弱性診断 原因調査 フォレンジック	対応確認検査	セキュリティ教育・研修
	バックエンド (DB 等)	要件定義支援	設計支援 レビュー支援 脆弱性診断	システム監視・運用 セキュリティ機器監視・運用	脆弱性診断 ログ分析	脆弱性診断	システム監視・運用 セキュリティ機器監視・運用 事後対応	対応策策定 脆弱性診断 原因調査 フォレンジック	対応確認検査	セキュリティ情報提供 セキュリティ教育・研修
インフラ	サーバ	要件定義支援	設計支援 レビュー支援 脆弱性診断	システム監視・運用 セキュリティ機器監視・運用	脆弱性診断 ログ分析	脆弱性診断	システム監視・運用 セキュリティ機器監視・運用 事後対応	対応策策定 脆弱性診断 原因調査 フォレンジック	対応確認検査	セキュリティ情報提供 セキュリティ教育・研修
	ネットワーク	要件定義支援	設計支援 レビュー支援 脆弱性診断	システム監視・運用 セキュリティ機器監視・運用	脆弱性診断 ログ分析	脆弱性診断	システム監視・運用 セキュリティ機器監視・運用 事後対応	対応策策定 脆弱性診断 原因調査 フォレンジック	対応確認検査	セキュリティ情報提供 セキュリティ教育・研修
クライアント		要件定義支援	シンクライアント パッチ管理 検疫ネットワーク	シンクライアント パッチ管理 検疫ネットワーク	端末挙動分析	端末検査	シンクライアント パッチ管理 検疫ネットワーク 端末検査 事後対応	対応策策定 端末検査 原因調査 フォレンジック	対応確認検査	セキュリティ情報提供 セキュリティ教育・研修
その他		物理セキュリティ関連	物理セキュリティ関連	物理セキュリティ関連 ログ保全			物理セキュリティ関連 ログ保全			セキュアメール セキュアファイル交換 PKI ソリューション データ破棄

WG2の活動

- 目的：最新の技術動向を調査し、最適なセキュリティオペレーション技術を探究し、技術者の交流を図る
- 毎月1回開催
- 各社持ち回り
- 開催場所、ホスト会社が毎回変わる

- 2010年の活動実績
  - SnortをつかったIDSハンズオン講座
  - ウイルス感染実験とインシデントレスポンス
  - WireSharkで遊びましょう
  - 内部犯行についての議論
  - SOC事業者とIPv6
  - ウェブサーバのログの解析に挑戦
  - サイバーセキュリティと肉食系

WG3 活動

- 目的：数多くの関連法規が散在する中、利用組織および事業者が特に認識すべき項目を分かりやすく整理する

- ISOG-J主催 特別内部セミナー
  - 2010年9月17日（金）16:00～19:00
  - クラウド時代のセキュリティと法律の関係

セミナーアジェンダより
http://www.jnsa.org/isog-j/event/index.html

WG4 活動

- 目的：セキュリティオペレーションの必要性について認知度向上を目的とした普及啓発活動を行う

- JNSA主催「Network Security Forum 2009（NSF2009）」
  - 2010年1月27日（水）10:30～18:00
  - パネルディスカッション：IPv6導入でセキュリティはどう変わるか
- JNSA 2009年度活動報告会
  - 2010年6月11日（金）9:30～15:30
- ISOG-J主催 特別内部セミナー
  - 2010年10月13日（水）16:00～19:00
  - 国際・日本でのセキュリティ組織間連携の取組みの最新状況
- Internet Week 2010
  - 2010年11月25日（木）16:00～18:30
  - セキュリティオペレーション2010～現場から見たインシデント対応 -ISOG-Jにおける連携の試み～

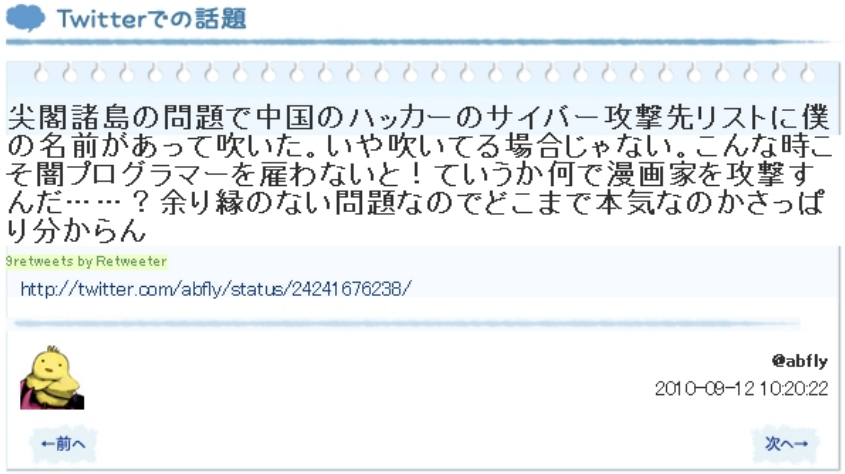
【NEW】セキュリティオペレーション情報共有・連携プロジェクト

- セキュリティオペレーション事業者間の情報共有・連携のあり方について検討し、情報発信に向けて活動を行います。

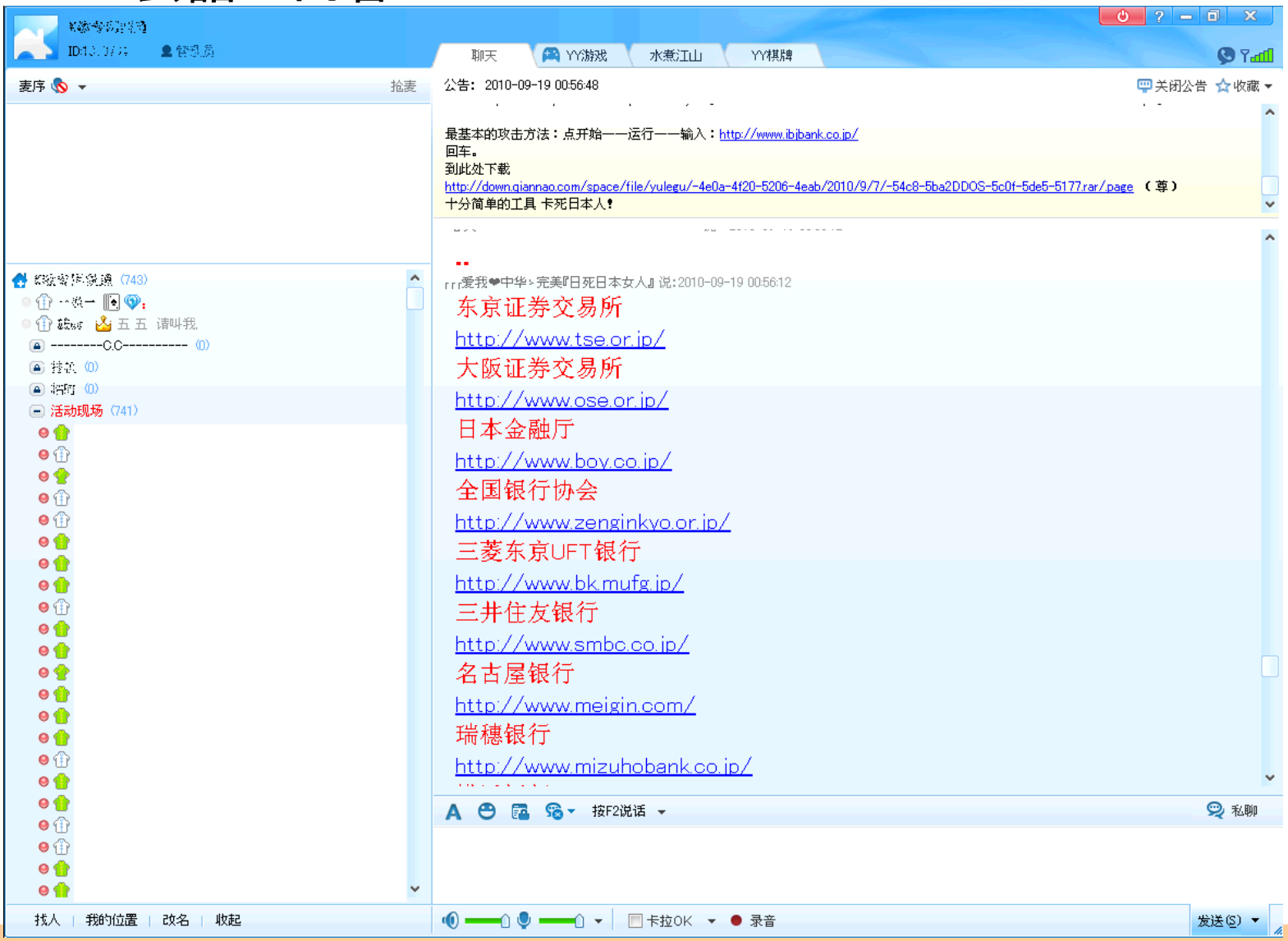
- この後のセッションに期待！！

尖閣諸島問題

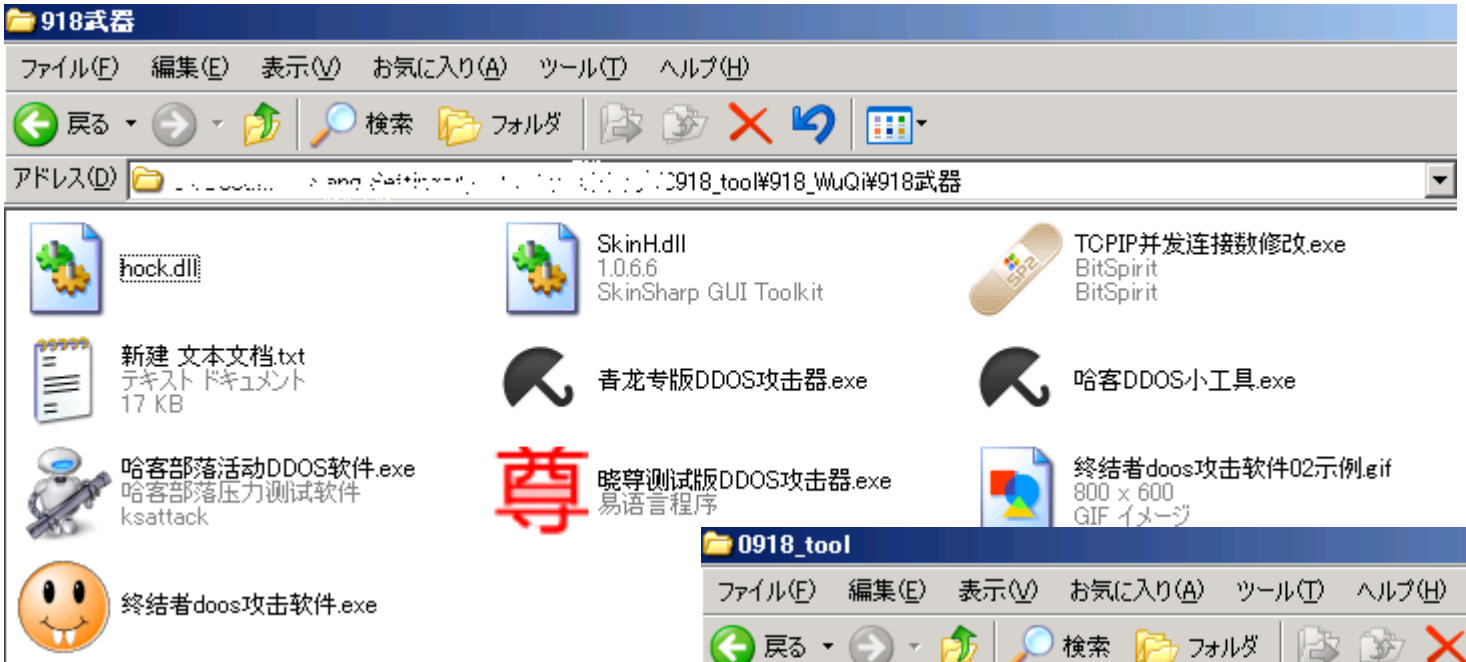
- 中国の漁船を尖閣諸島付近で確保
- それに呼応して9/18に日本に一斉攻撃宣言
- 攻撃対象となったサイトのリストを掲載
  - 中央省庁
  - 各都道府県
  - 公共系サービス
- 皆様のところは？

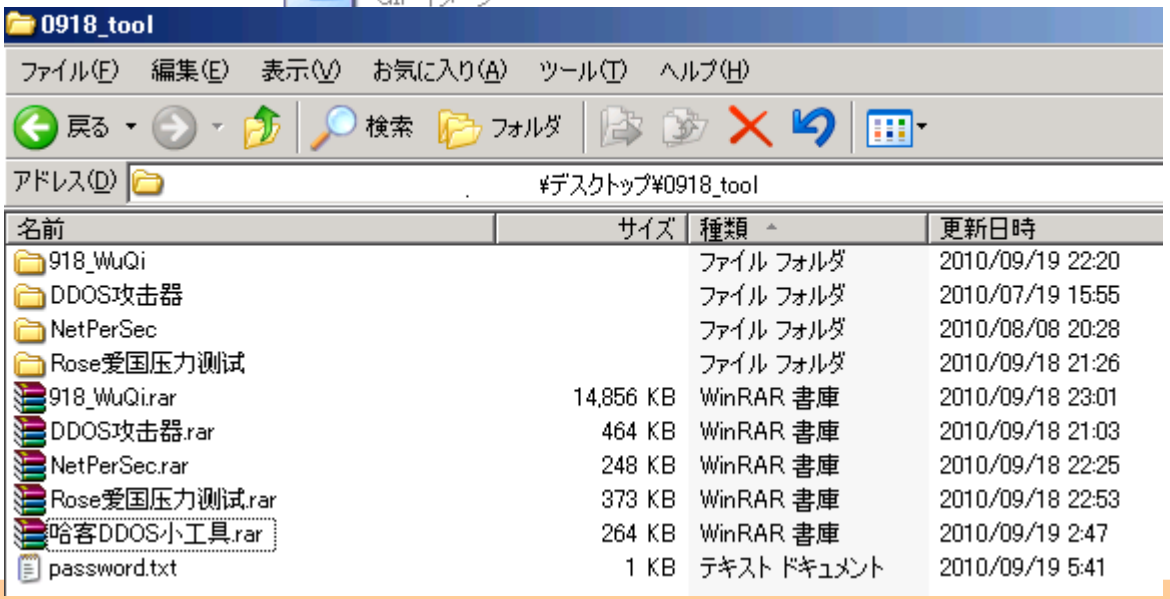


チャットでの会話の内容

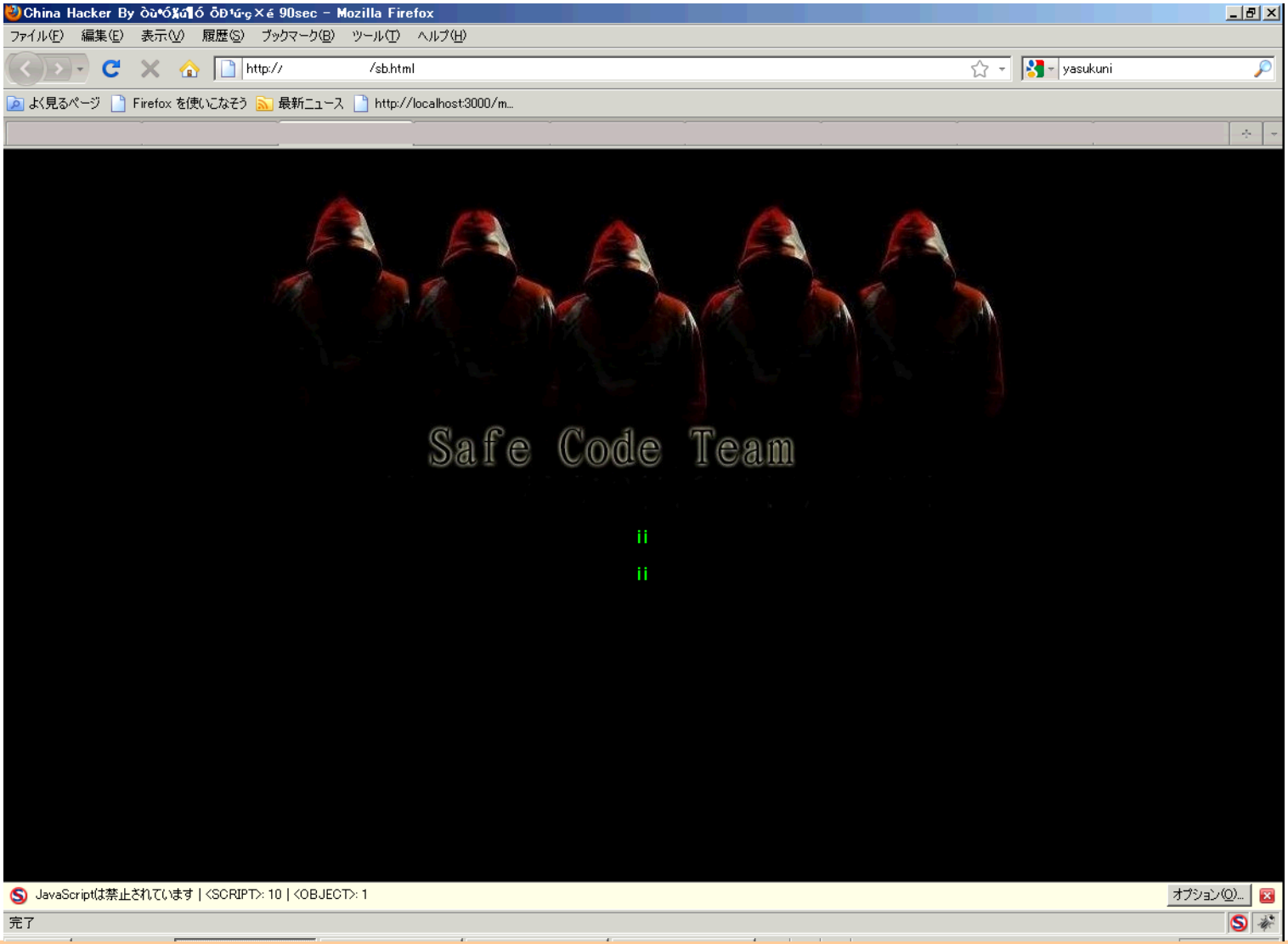


攻撃ツール

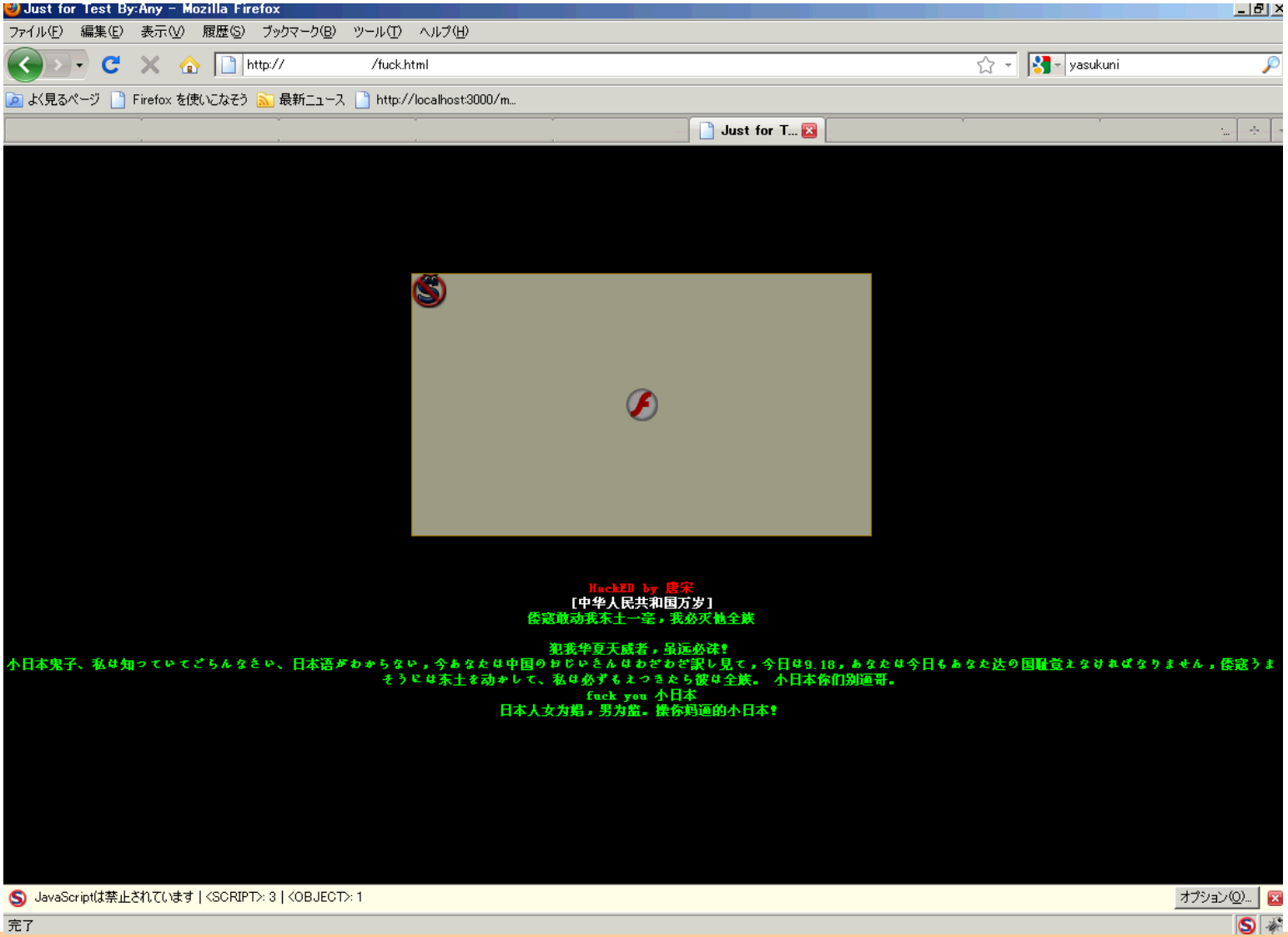




改ざんされたホームページ

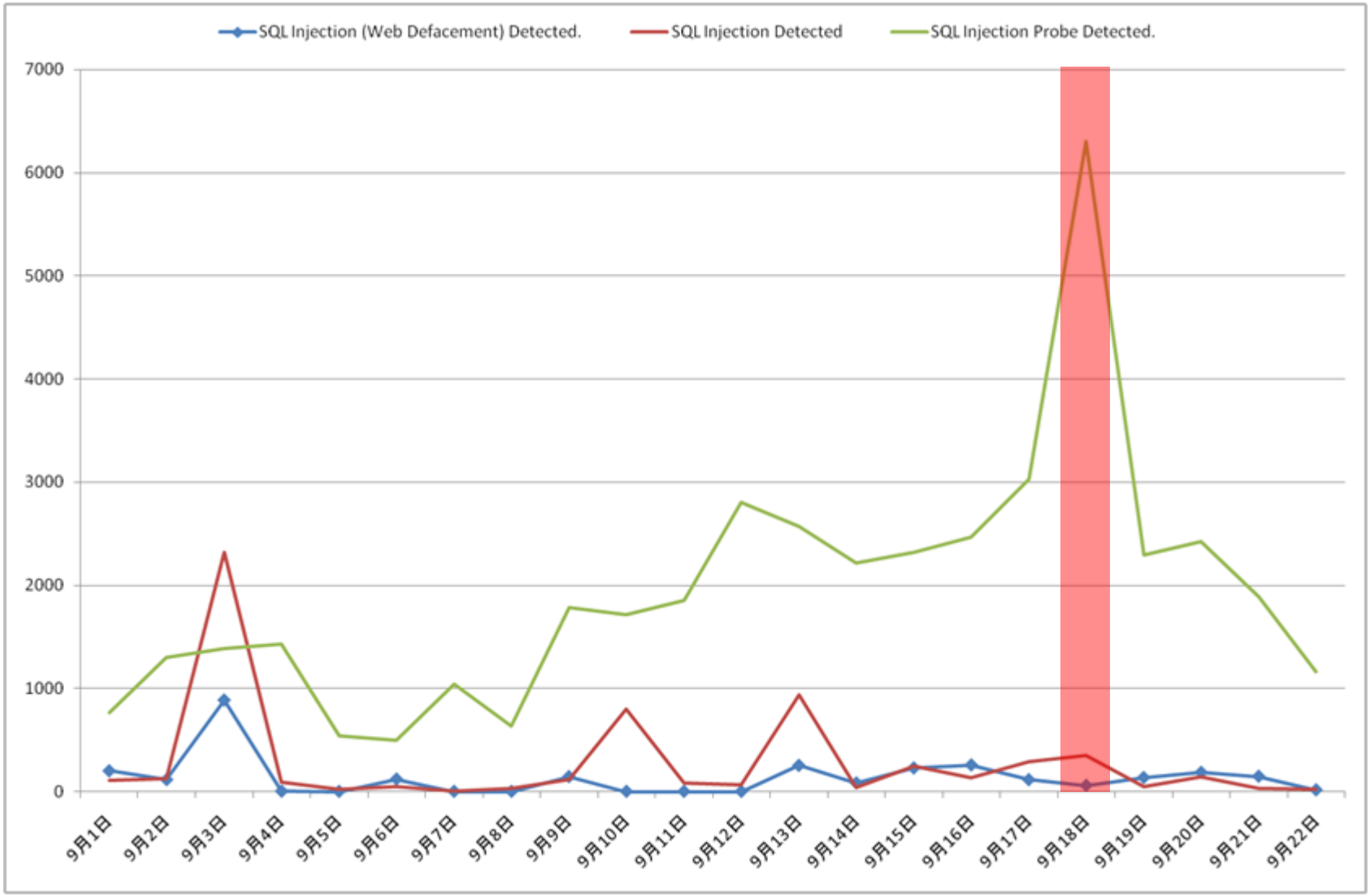


改ざんされたホームページ



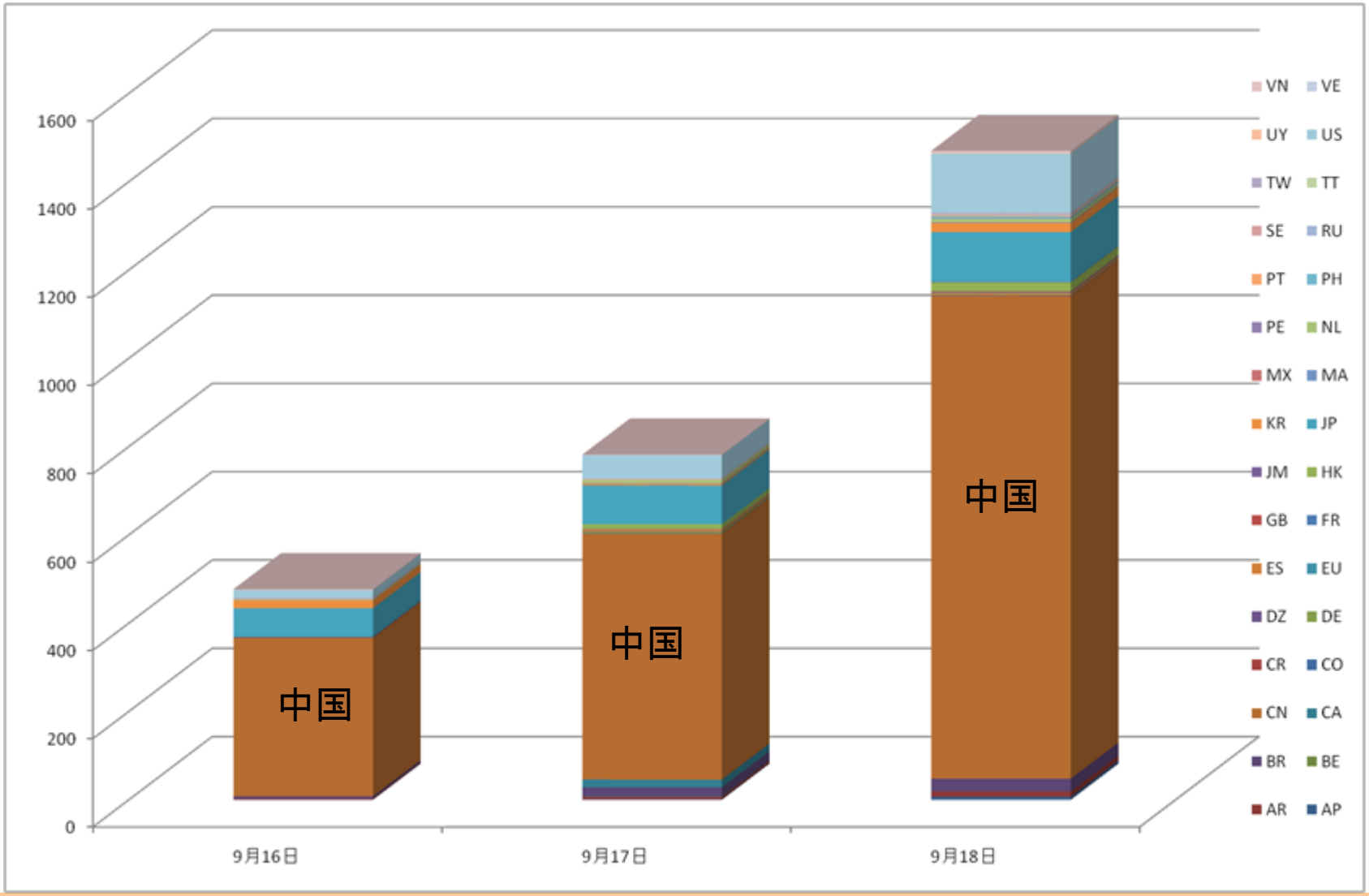
9/18 SQL インジェクション

株式会社ラック JSOC観測データより



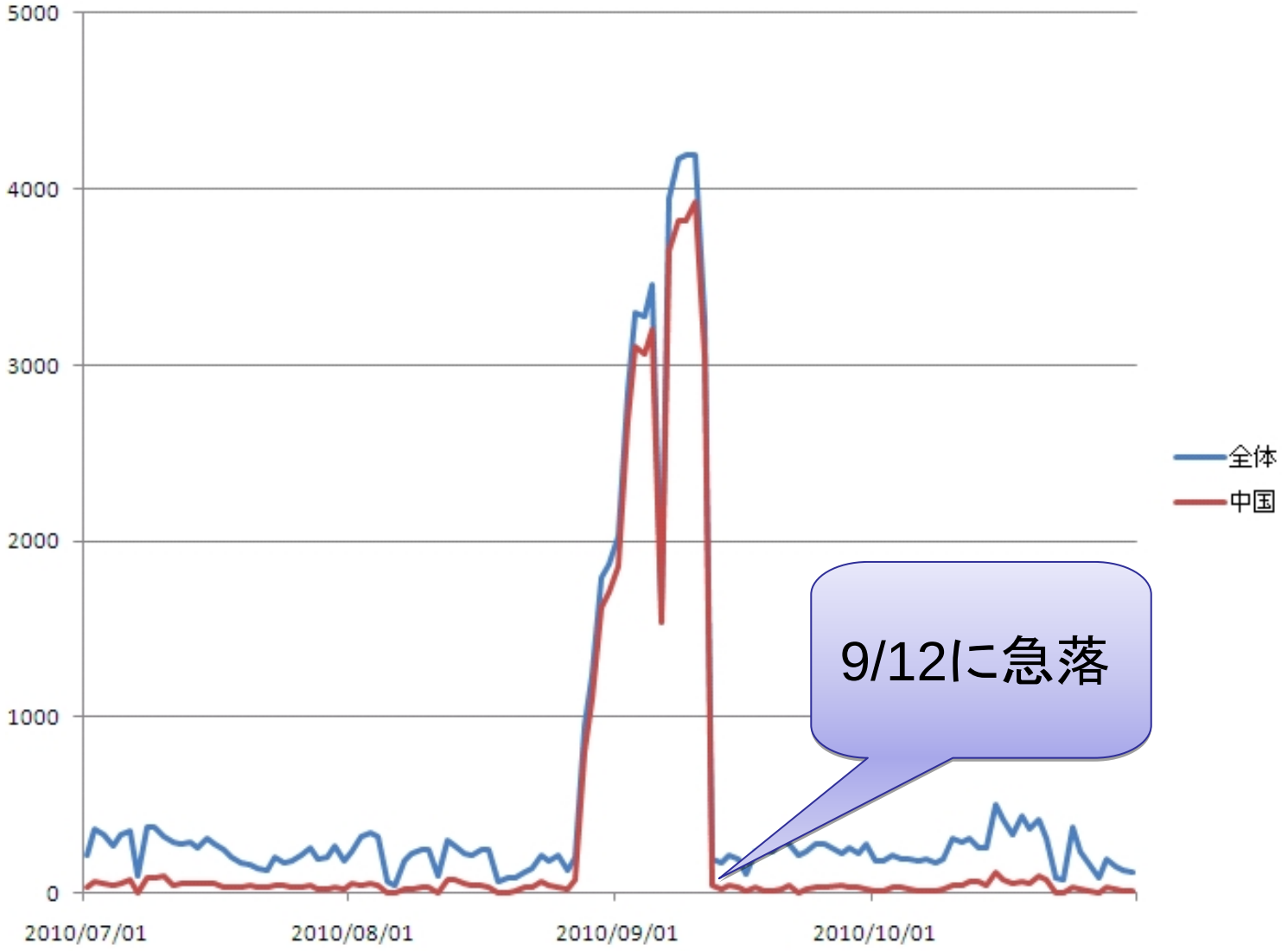
9/18 SQL インジェクションの攻撃元は？

株式会社ラック JSOC観測データより



Proxy調査

株式会社ラック JSOC観測データより



9/18 に関する悲鳴（匿名です）

- うちは特に何もなかった
- うちも何もなかった
- 一応待機していたけど平和だった
- いやいや、大変なところもあったのよ
- お客様から「本当に何もなかったの？」とよく聞かれた
- お客様からの問い合わせがDoSだった
- 「何かあったら連絡ください」と言われた
- 「当然、緊急配備ですよね？」と言われた
- 緊急呼び出しがかかった
- インシデント対応マニュアルの再整備ができたからちょうどよかった
- 某所でサーバが落ちないように祈りをささげていた
- 全国から情報を求めている人から電話が鳴りまくった
- いっそ計画訓練にしてくれた方がすっきりする
- 結婚式を挙げていた
- 嫁の機嫌が悪くなった

SOC事業者とIPv6

http://www.kokatsu.jp/blog/ipv4/ より

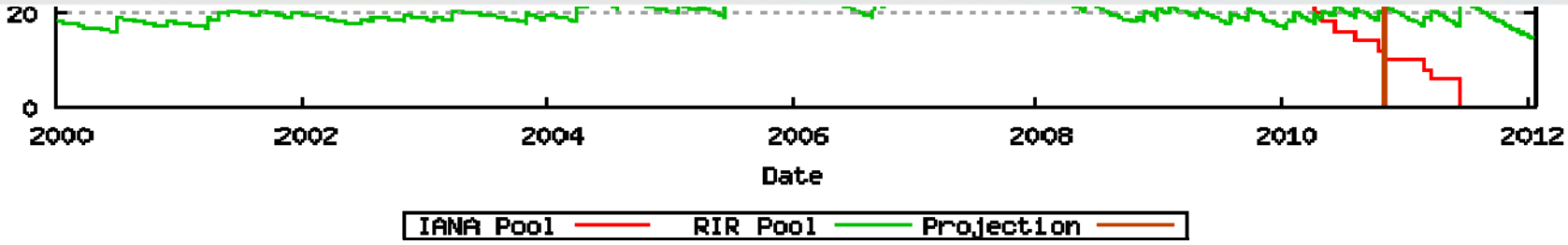
IPv4 EXHAUSTION IPv4アドレス枯渇対応タスクフォース

お問い合わせ RSS twitter 検索 日本語 ENGLISH

概要 ABOUT TF | ニュース NEWS | セミナー&イベント SEMINAR & EVENT | 活動報告等 ACHIEVEMENTS | 参加団体 MEMBER | よくある質問 FAQ

IPv4アドレス
枯渇対応タスクフォース

IPv4アドレスのIANA在庫、残り5%未満へ



SOC事業者とIPv6

- 一部の資料を抜粋

しばしばされる議論 -2-

- **IPv4アドレスを回収すればなんとかなる**
  - 小さなブロックを回収したとしても再利用は難しい
    - 経路情報が細かくなりすぎ、経路表が爆発する
    - 細かいアドレスをたくさんまとめて大組織に渡しても使いにくい
  - ほとんどのユーザーはアドレスを返さない
    - 返すことにインセンティブがない
    - アドレスは既得権益
  - 2007年には/8が４つ返却された
    - 枯渇予想に織り込み済みの事象であり、枯渇までの時間に影響を与える範囲ではない
- **NATでいいじゃん**
  - IPv4アドレスが枯渇した後NATで頑張るとすると、非常に厳しい制限が発生する（後述）

ISOG-J

問題点

- IPv6協議会では、IPv6の普及と啓蒙
- IPv4枯渇TaskForceでは、IPv4の枯渇に対応したアクション
  - IPv4/v6 Dual Stackの教育や、テストベッドの提供
- しかし、この活動で全てが網羅できているわけではない
  - し、できるわけもない。
- 特にThird Party運用者（MSP/MSSP等）関連に関しては全くと言っていいほど考慮されていない
  - MSPやMSSPがほとんど参加していないと言う状況もある
- 開発者に関してもほとんど考慮されていない
  - ほとんど参加していないから、声が届かないし、業者が多すぎて対応し切れない

ISOG-J

現状のMSSP

- 基本的に、MSSPの利用者は少ない
  - MSSPの知名度は低い
  - 「被害を受けなければ認識されない」ことが多い
  - MSSPが出来る範囲は限られている
    - MSSPは警察でも検察でもなく、捜査権はない
    - MSSPは本質的に運用（の一部）を委託されているに過ぎない
- Dual Stackへの移行といわれても
  - 顧客がいなければ動けない
  - サービスにできるだけの知見が足りない

ISOG-J

WG2メンバーのIPv6へのコメント

- 製品がまだまだ対応してきていない
- お客様が本気にならないとサービスを用意できない
- IPv6普及初期の時期にサービスを作るとユーザが少ないのでコスト増になる
- そろそろ本気でやらなければと思ってはいる
- 思ってはいるんだけど・・・
- IPv6スタックレベルの脆弱性がたくさん存在しそうで心配
- 勉強するモチベーションがあがらない
- 地デジ対応と同じでおしりに火がつかないとできない
- 機器のパフォーマンスが心配
- ハードやソフトは徐々に対応してきているが、オペレーションは何も考えられていない
- きっととばっちりがくるにちがいない
- サービスを受ける国ごとにIPv6対応のプライオリティが違うのでサービス提供が難しい
- 偉い人は「経験がないが権威のある人」の言葉より、「身近な現場のエンジニア」の言葉も聞いてほしい

Snortを使ったIDS講座

- 各自PCを持ち寄ってSnortを使いながらIDSについて学ぶ

1. ガイダンス：Snort の概要説明、起動確認
2. 動作確認：テストシグネチャによるSnortの動作確認
3. 演習（初級編）： Snortシグネチャの作成練習
   課題の条件に一致するシグネチャの作成とテスト。
4. 演習 (中級編)： 対象パケットの抽出
   時間の都合により割愛
5. 演習（上級編）： Exploitの特定
   パケットデータから特徴的な情報を抽出。各 Exploitとの比較。
   各社毎に演習課題を振り分けて個々に演習実施。
6. 演習（演習課題）： パケットに隠された答えを探せ！
   pcapファイル中にあるヒントを辿って設問の答えを見つける。

Snortを使ったIDS講座の資料

Snortの起動、設定

- Snortの起動方法

Snortを取得
$ wget http://xxxxxxxxxxxxxxxx

シグネチャ作成

- Snortシグネチャの見本

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP PORT bounce attempt";
flow:to_server,established; content:"PORT"; nocase; ftpbounce; pcre:"/^PORT/smi";
classtype:misc-attack; sid:3441; rev:1;)
```

alert	アラートを出力	必須
tcp	プロトコルを指定。通常はtcp,udp,icmpのみ	必須
any (ip)	IPアドレスを指定。$HOME_NETなどの変数も使用可能。CIDR指定も可	必須

演習 初級

- 以下の通信のシグネチャを個別に作成し、Snortにcamp2.pca

・送信元IPアドレスが172.17.0.7である通信
・送信先IPアドレスが172.17.0.14である通信
・送信先IPアドレスが172.17.0.24である通信
・送信元IPアドレスが172.17.0.0/24である通信
・172.17.0.7と172.17.0.25の通信
・送信先ポート番号が84/tcp～86/tcpの通信
・送信先ポート番号が3250/tcpである通信
・送信元ポート番号3241/tcpから送信先ポート番号8
・“ifconfig” という文字列を含む通信
・送信先IPアドレスが172.17.0.15で、“ipconfig” という
・User-AgentがFirefoxである通信
・送信元ポート80/tcpの中に“Highly program-depen
・データサイズが1000バイト以上の通信
・HTTPレスポンスコードが200である通信
・POSTリクエストの通信
・UDP通信

1-53 Copyright©2010 Little eArth Corporation Co.,Ltd

演習 上級編

- pcapファイルをWireSharkで参照し、該当するExploitを特定してください。

exploit1.pcap の通信を発生させたexploitは exploit1 ディレクトリのどれか？
exploit2.pcap の通信を発生させたexploitは exploit2 ディレクトリのどれか？
exploit3.pcap の通信を発生させたexploitは exploit3 ディレクトリのどれか？
exploit4.pcap の通信を発生させたexploitは exploit4 ディレクトリのどれか？
exploit5.pcap の通信を発生させたexploitは exploit5 ディレクトリのどれか？
exploit6-1.pcap の通信を発生させたexploitは exploit6 ディレクトリのどれか？
exploit6-2.pcap の通信を発生させたexploitは exploit6 ディレクトリのどれか？
exploit6-3.pcap の通信を発生させたexploitは exploit6 ディレクトリのどれか？
exploit6-4.pcap の通信を発生させたexploitは exploit6 ディレクトリのどれか？

1-61 Copyright©2010 Little eArth Corporation Co.,Ltd

Snortを使ったIDS講座の風景

Snortを使ったIDS講座 参加者の声

- 参加者の声
  - セキュリティオペレーションっぽいネタでとても面白かったです。
  - こんな課題ができるなんてイマドキの学生は幸せだと思いました。
  - configを手で書いたことがなかったので、新鮮な気持ちでsnortを使うことができた
  - いろいろパケットキャプチャして遊んでみようかなという気になった
  - 5, 6年前にSnortの記事を書いたきり、Snortにはご無沙汰だったので純粋に楽しかったです。
  - シグネチャの書き方とか起動時のオプションとかをほとんど忘れてしまっていたのが、個人的にショック
  - S木無双がすごかった。
  - やはり、S木無双は圧巻

研修用マルウェアを用いたインシデントレスポンス訓練

- 概要：インシデント対応力強化を目的とした社内研修および大学等の授業で使用している研修用マルウェアの解析を行う
- 解析ツールは指定されたものを使用。
- IDAPro等の使用は禁止。

- 設定
  - とある製造業のお客様システムにおいて、ウイルス感染事故が発生
  - お客様担当者から被害の状況を正しくヒヤリングする
  - 被害の状況を想定しながらパソコン、サーバの調査を行う
  - さまざまな情報が錯綜し、正しい情報でないケースもある

研修用マルウェアを用いたインシデントレスポンス訓練の風景

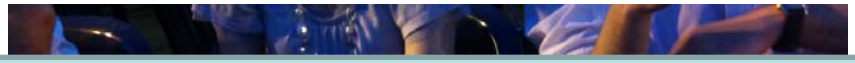
研修用マルウェアを用いたインシデントレスポンス訓練 参加者の声

- 面白かったです。真剣にやったので、かなり疲れました。
- コンテンツもシナリオも作りこまれていて、これを若手3年目に受けさせることができる環境はいいなぁ、と思いました。
- これが噂のS木無双…。始終置いてけぼり。
- ストーリーが整理されていて楽しかった。これは受けると思う。
- ウイルス感染事件をどうやって発見して終息させていくかをリアルに体験できる。
- 面白かった！毎年開催されているだけあって、とてもクオリティが高かった。
- 使用するツールを制限することで、逆に新たな使い方を発見できたりしてよかった。
- 人のやり方を見るのはとても参考になる。
- 現実にあり得そうなシナリオで感情移入？して課題に取り組めた。
- ツールを最近使ってなかったので情報の取り方がなかなかとれなくてもどかしかった
- シナリオとマルウェアとやられサーバが作りこまれていて大変素晴らしいと思いました。
- Process Explorerだとアンパックしなくてもメモリの中を覗けるんですね（当たり前？）。
- ふだんから使い慣れていないツールばかりだったので、使い方でアタフタしてました。
- 自分の業務担当外もガシガシやっていかないといけないってことですね。

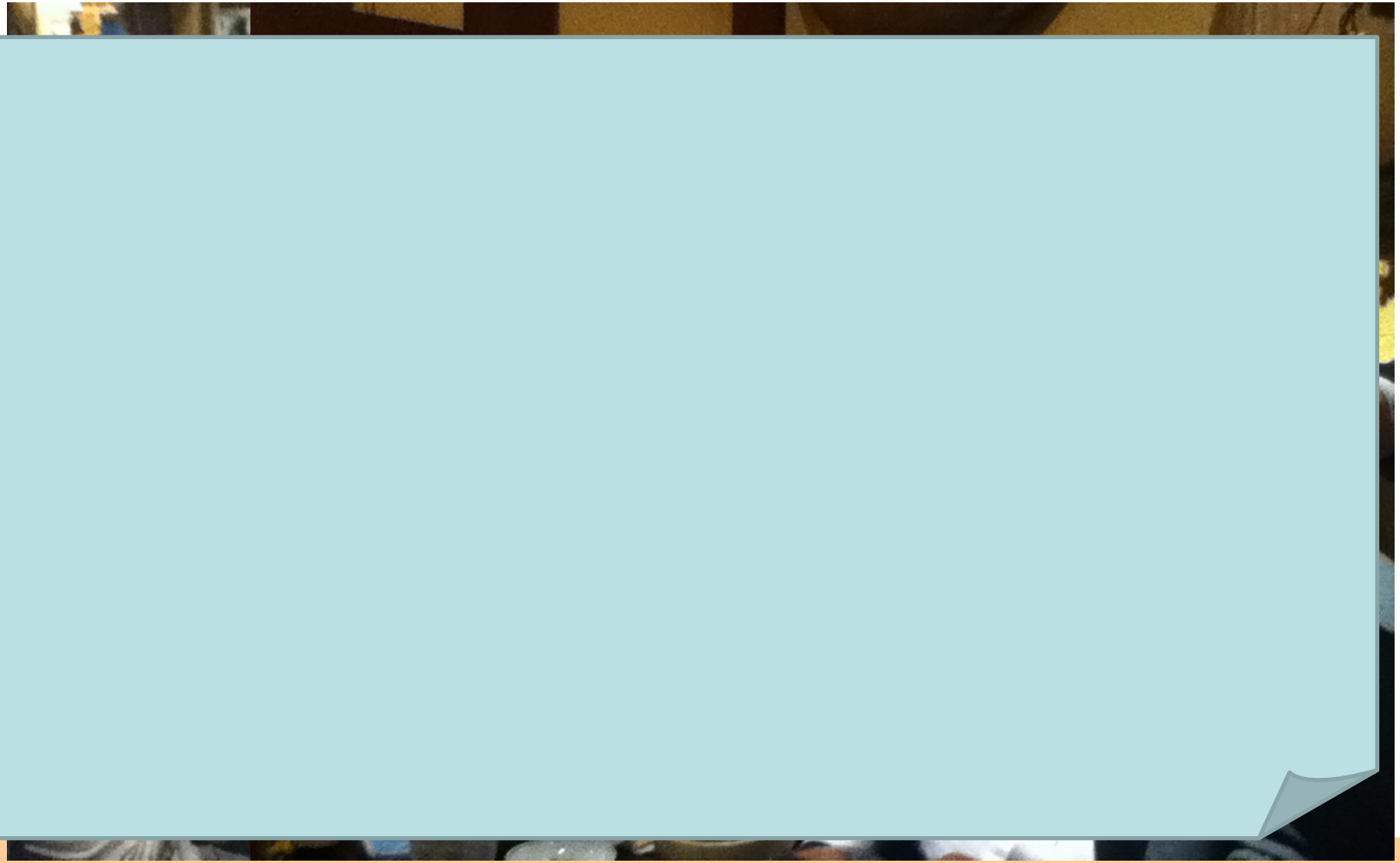
その他WG2メンバーのコメント

- 世界中で改ざん事件が多発
- Gumblarスキームが常態化
- auroraとかstuxnetとか、割と政治色の強い(と思われる)事件
- AdobeとJREの脆弱性が多い
- ウイルス対策ソフトはどう使うべきか
- 岡崎図書館事件 誤認逮捕と情報漏洩
- ソーシャルネットワークを使った情報拡散

交流も活発に（1）



交流も活発に（2）



こんな方はぜひWG2へ

- セキュリティオペレーションを何とかしたい
- 対応がグレーなところを相談したい
- 濃い話がしたい
- 色々鬱憤がたまっている
- お酒を飲みたい