2012年に起きたセキュリティ・インシデントの解説とイベント紹介

JSOC JAPAN SECURITY OPERATION CENTER

2012年11月22日

川口　洋, CISSP
株式会社ラック
チーフエバンジェリスト
hiroshi.kawaguchi @ lac.co.jp

自己紹介

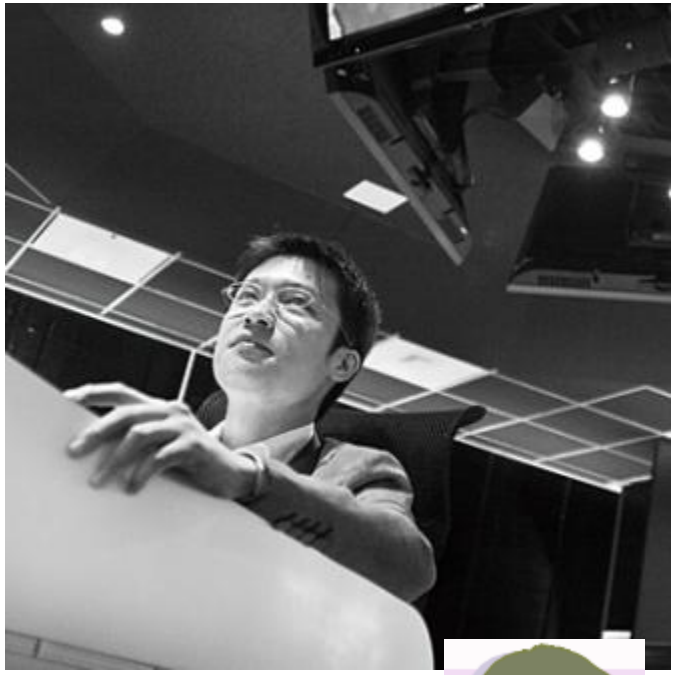
川口　洋(かわぐち　ひろし),CISSP

株式会社ラック

チーフエバンジェリスト 兼 担当部長

ISOG-J 技術WG リーダ

http://www.lac.co.jp/education/instructor/index.html



2002年　ラック入社
社内インフラシステムの維持、運用に従事する。その他、セキュアサーバの構築サービスや、サーバのセキュリティ検査業務なども行い、経験を積む。その後、IDS やFirewall などの運用・管理業務を経て、セキュリティアナリストとして、JSOC監視サービスに従事し、日々セキュリティインシデントに対応。2005年より、アナリストリーダとして、セキュリティイベントの分析とともに、IDS/IPSに適用するJSOCオリジナルシグネチャ(JSIG)の作成、チューニングを実施し、監視 サービスの技術面のコントロールを行う。

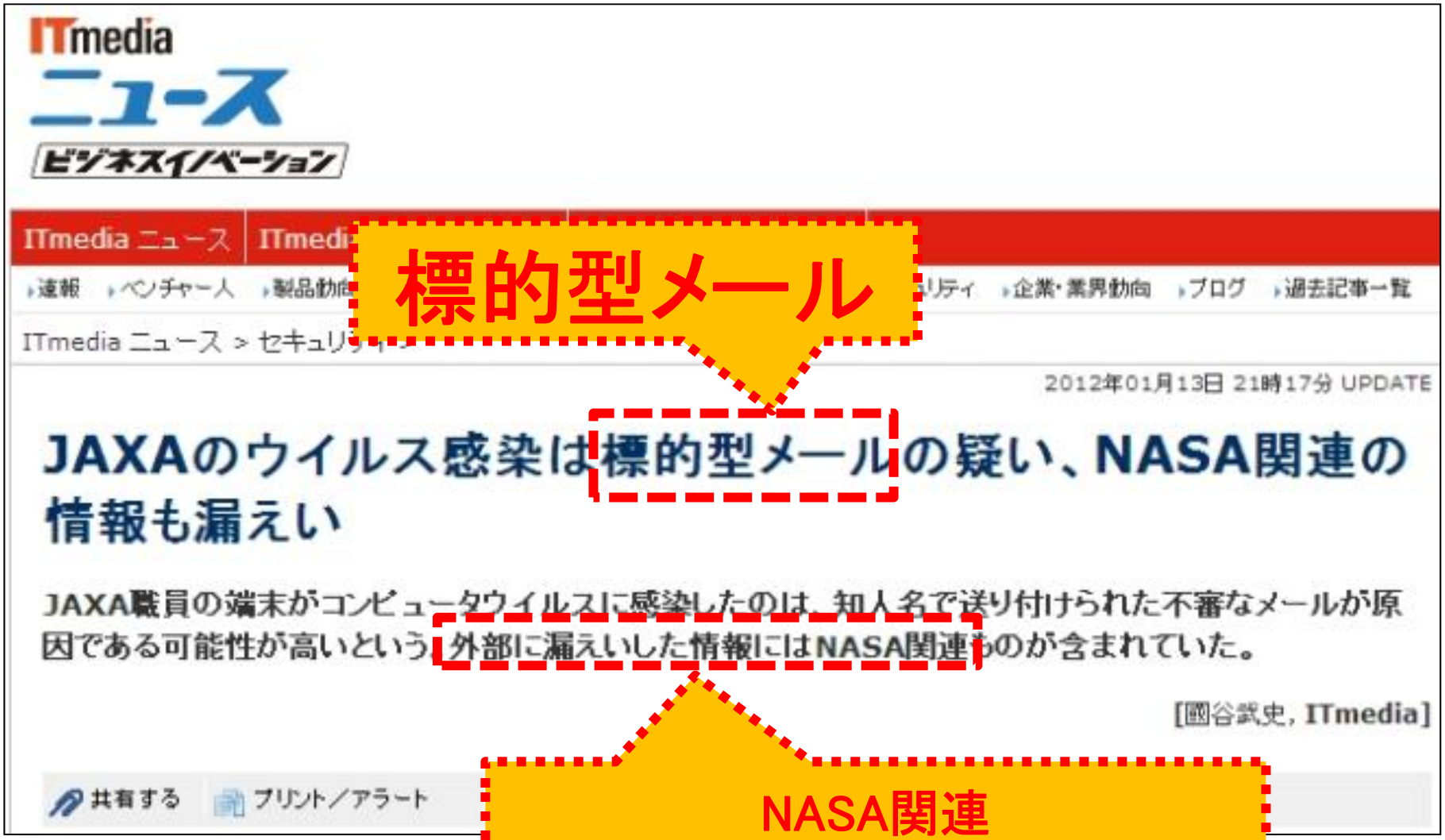
チーフエバンジェリストとして、セキュリティオペレーションに関する研究、ITインフラのリスクに関する情報提供、啓発活動を行っている。Black Hat Japan、PacSec、Internet Week、情報セキュリティEXPO、サイバーテロ対策協議会などで講演し、安全なITネットワークの実現を目指して日夜奮闘中。

2010年～2011年、セキュリティ＆プログラミングキャンプの講師として未来ある若者の指導にあたる。2012年、最高の「守る」技術を持つトップエンジニアを発掘・顕彰する技術競技会「Hardening」のスタッフとしても参加し、ITシステム運用に関わる全ての人の能力向上のための活動も行っている。

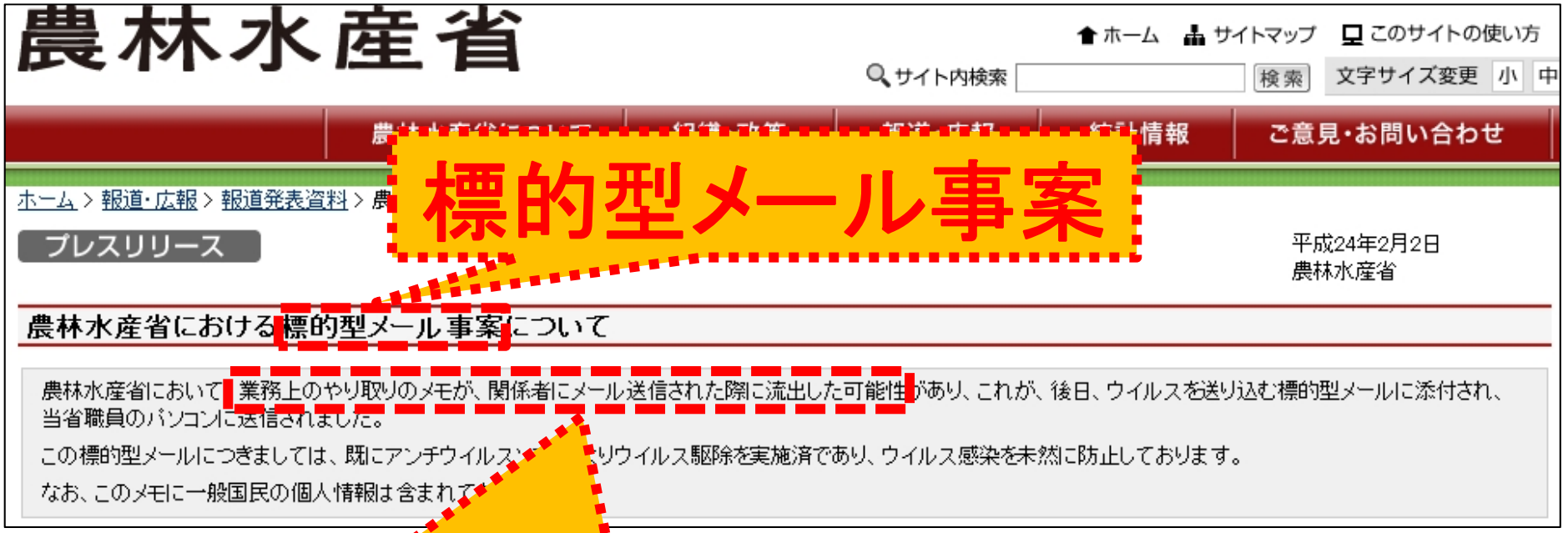
[川口洋のセキュリティ・プライベート・アイズ（@IT）連載中](http://www.atmarkit.co.jp/fsecurity/index/index_kawaguchi.html)
http://www.atmarkit.co.jp/fsecurity/index/index_kawaguchi.html

今年のニュースを振り返る

最近起きていた事件：1月



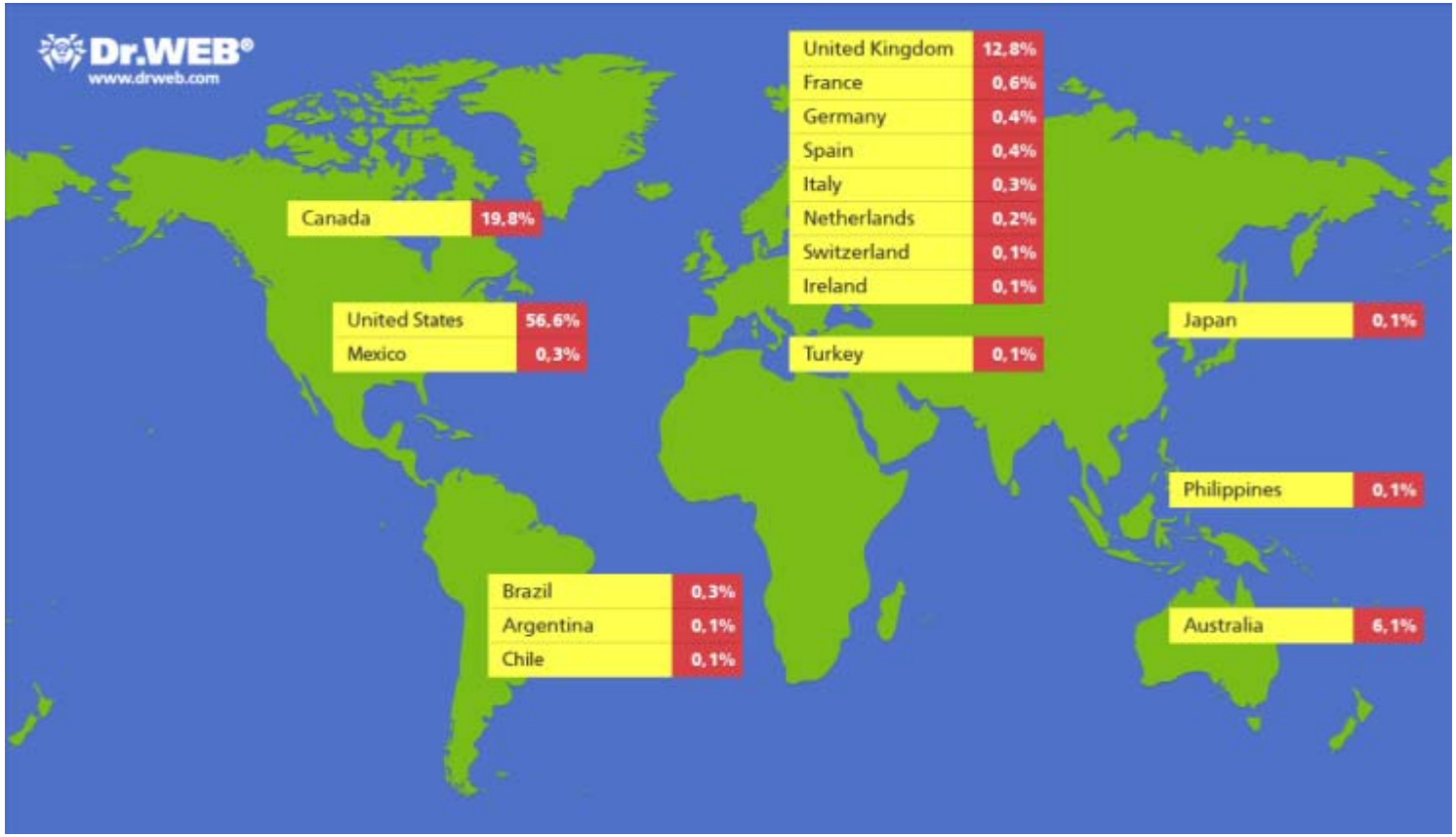
最近起きていた事件：2月



http://www.maff.go.jp/j/press/kanbo/hyoka/120202.html

最近起きていた事件：4月

Macを狙った「FlashBack」が流行 60万台が感染
Flash Playerの更新ファイルに偽装、Javaの脆弱性を悪用



http://news.drweb.com/show/?i=2341&lng=en&c=14

最近起きていた事件：4月

「the Movie」を名乗るAndroidアプリ、個人情報をレンタルサーバに不正転送か

「the Movie」というタイトルが付いた不審なAndroidアプリ
を国内のサーバに転送していた可能性がある。

個人情報を不正転送

[ITmedia]

Tweet　いいね！ 58　+1 0　共有する　プリント／アラート

「the Movie」というタイトルが付いた不審なAndroidアプリがGoogle Playストアで大量に見つかり、ダウンロードしたユーザーの端末から、個人情報を外部のサーバに送信していた可能性があると問題になっている。問題のアプリは既に削除されている。

http://www.itmedia.co.jp/enterprise/articles/1204/13/news113.html

最近起きていた事件：5月

Flame

Stuxnet級の高度なマルウェア出現、サイバー兵器に使用か

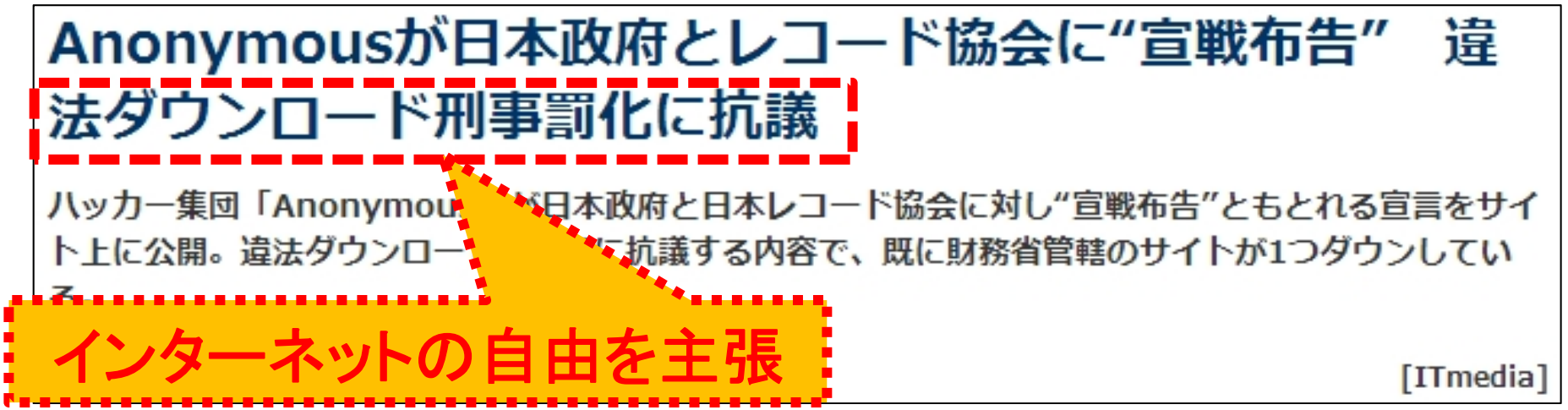
国家の施設を標的とする極めて高度なマルウェア「Flame」が見つかった。Kaspersky Labでは、DuquやStuxnetと同じ「スーパーサイバー兵器」の部類に属すると分析している。

[鈴木聖子，ITmedia]

このマルウェアは「Flame」と呼ばれ、国際電気通信連合（ITU）とKasperskyが別の破壊的なマルウェアを調べている過程で見つかったという。主にサイバースパイの機能を持ち、コンピュータ画面のスクリーンショット、標的とするシステムについての情報、保存されたファイル、連絡先情報、音声録音記録などの情報を盗み出してマルウェア制御用サーバのネットワークに送信。Stuxnetが悪用したのと同じプリンタの脆弱性やUSB経由の感染手段を使い、ローカルネットワークを介して増殖するワームの性質を持つ。

http://www.itmedia.co.jp/enterprise/articles/1205/29/news019.html

Operation Japan



Anonymousとは？

ハクティビスト

言論の自由、情報公開の自由」に対して、インターネット上で社会的な抗議活動を行う人

最近起きていた事件：7月

平成24年7月20日
財務省

財務省におけるウイルス感染事案について

財務省では、次期LANシステム導入に向け、昨今の政府機関への標的型メール攻撃などによるウイルス感染事案を踏まえ、現行LANシステムのセキュリティ対策の総点検を実施したところ、過去に複数の財務省職員用パソコンがウイルスに感染し、何らかの情報が外部に送信された可能性があることが判明しました。

なお、ウイルスの感染経路は不明ですが、既に、ソ…など必要な措置をとりました。

このような事態となりましたことを深くお詫び申し上げます。

今後、関係機関と協力し更なる調査を進めるとともに、この度の事案を重く受け止め、情報セキュリティ対策の一層の強化に取り組んでまいります。

総点検の際に発見

数か月以上

http://www.mof.go.jp/about_mof/other/other/press_20120720.html

財務省PC数か月情報流出か…トロイの木馬型

財務省の複数の職員用パソコンがコンピューターウイルスに感染し、海外などに内部情報が流出した可能性があることがわかった。

ウイルスは「トロイの木馬」型で、外部との不正通信が確認されたパソコンだけでも約120台に上るとみられる。数か月以上にわたって内部情報を抜き取られていた疑いがあるという。同省は、外部からサイバー攻撃を受けたとみて、感染経路とともに、流出した情報の特定を進めている。

http://www.yomiuri.co.jp/national/news/20120720-OYT1T00403.htm

最近起きていた事件：9月

裁判所HPが改ざん＝「釣魚島」に中国国旗

最高裁が管理する裁判所のホームページ（HP）が14日夜、尖閣諸島の中国の領有権を主張する内容の文言と中国国旗が書かれた画面に一時改ざんされたことが分かった。最高裁は原因を調べている。

改ざんされたのは裁判所のトップページ。尖閣諸島の中国名である「釣魚島」と書かれた島の画像の上に大きな中国国旗が置かれ、日本語と英語、中国語で「釣魚島は中国」などと書かれていた。国旗の絵の元になるデータは、中国のサーバーにあった。

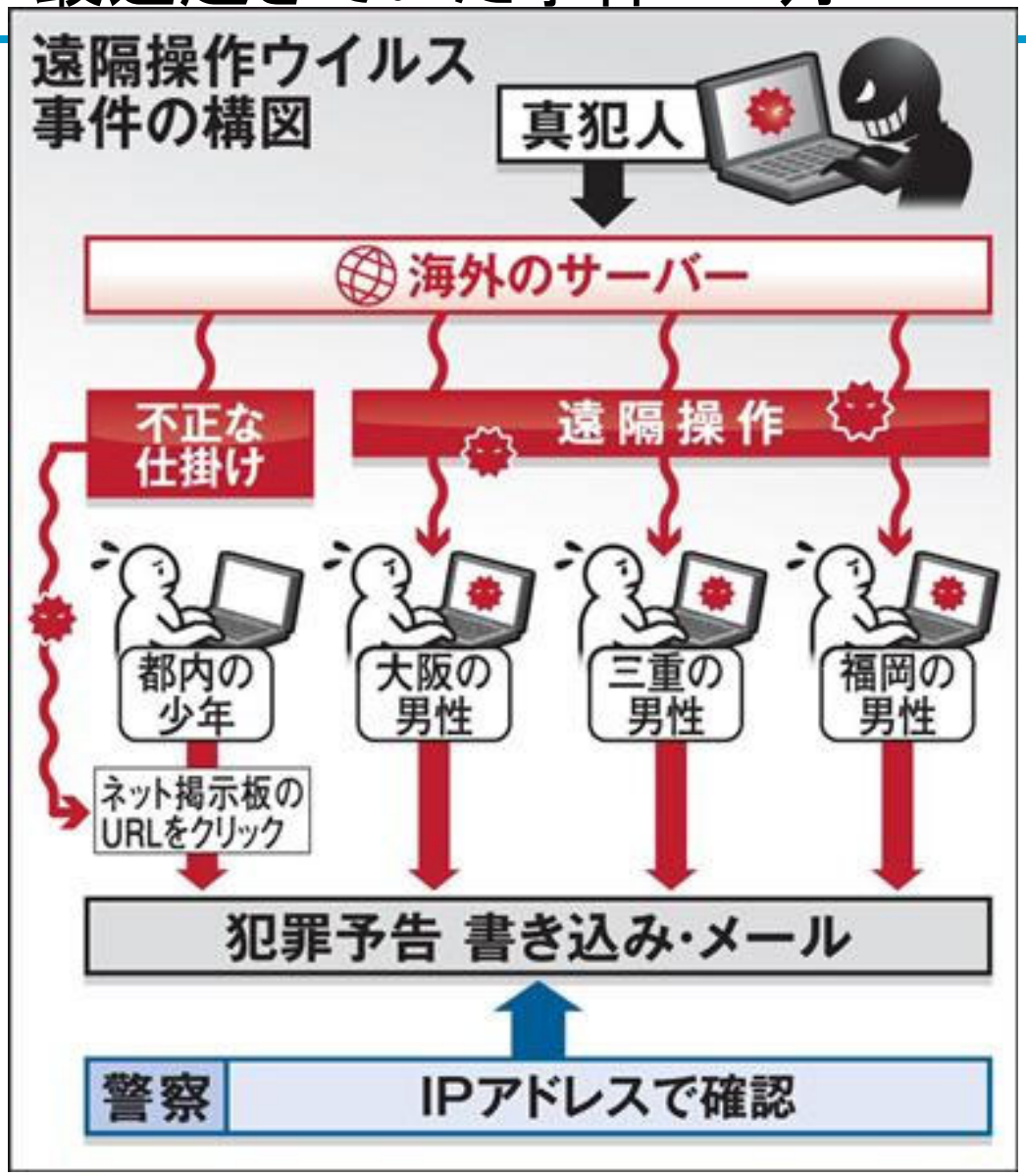
尖閣諸島をめぐっては、日本政府の国有化を受け中国各地で抗議運動が相次ぎ、14日には中国の海洋監視船6隻が尖閣諸島周辺の日本領海内に侵入した。（2012/09/14-22:13）

改ざんされた裁判所のホームページ。沖縄・尖閣諸島（中国名・釣魚島）の中国の領有権を主張する文言と、中国国旗がはためく画像が掲載されている

http://www.jiji.com/jc/zc?k=201209/2012091400980

復旧はしたが、詳細について記載なし

最近起きていた事件：10月



メールに記載されていた事件と
捜査当局の動き

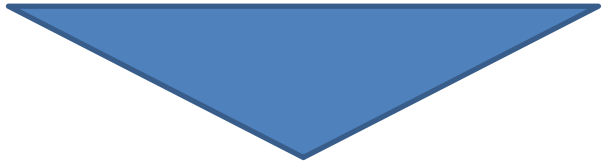
時期	事件	捜査当局の動き	パソコンの持ち主
6月29日	横浜市のサイトに小学校襲撃予告	神奈川県警が逮捕、保護観察処分	都内の私立大生
7月29日	大阪市のサイトに大量殺人予告	大阪府警が逮捕、釈放	大阪府吹田市の北村真咲さん
	首相官邸のホームページに殺人予告		
8月1日	日航への爆破予告	警視庁が捜査	
8月9日	同人誌の即売イベントの襲撃予告		愛知県内の企業の従業員
	天皇陛下の殺害予告		
8月27日	お茶の水女子大付属幼稚園に襲撃予告	警視庁が逮捕、釈放	福岡市の男性
	子役タレント脅迫	警視庁が再逮捕、釈放	
	学習院初等科に襲撃予告	警視庁が捜査	
	部落解放同盟に襲撃予告		
	アイドルグループイベントの襲撃予告		
9月10日	伊勢神宮を破壊予告	三重県警が逮捕、釈放	津市の男性
	任天堂に爆破予告	三重県警が捜査	

http://www.itmedia.co.jp/news/articles/1210/22/news037.html

http://www.itmedia.co.jp/news/articles/1210/17/news064.html

標的型攻撃対策の難しさ

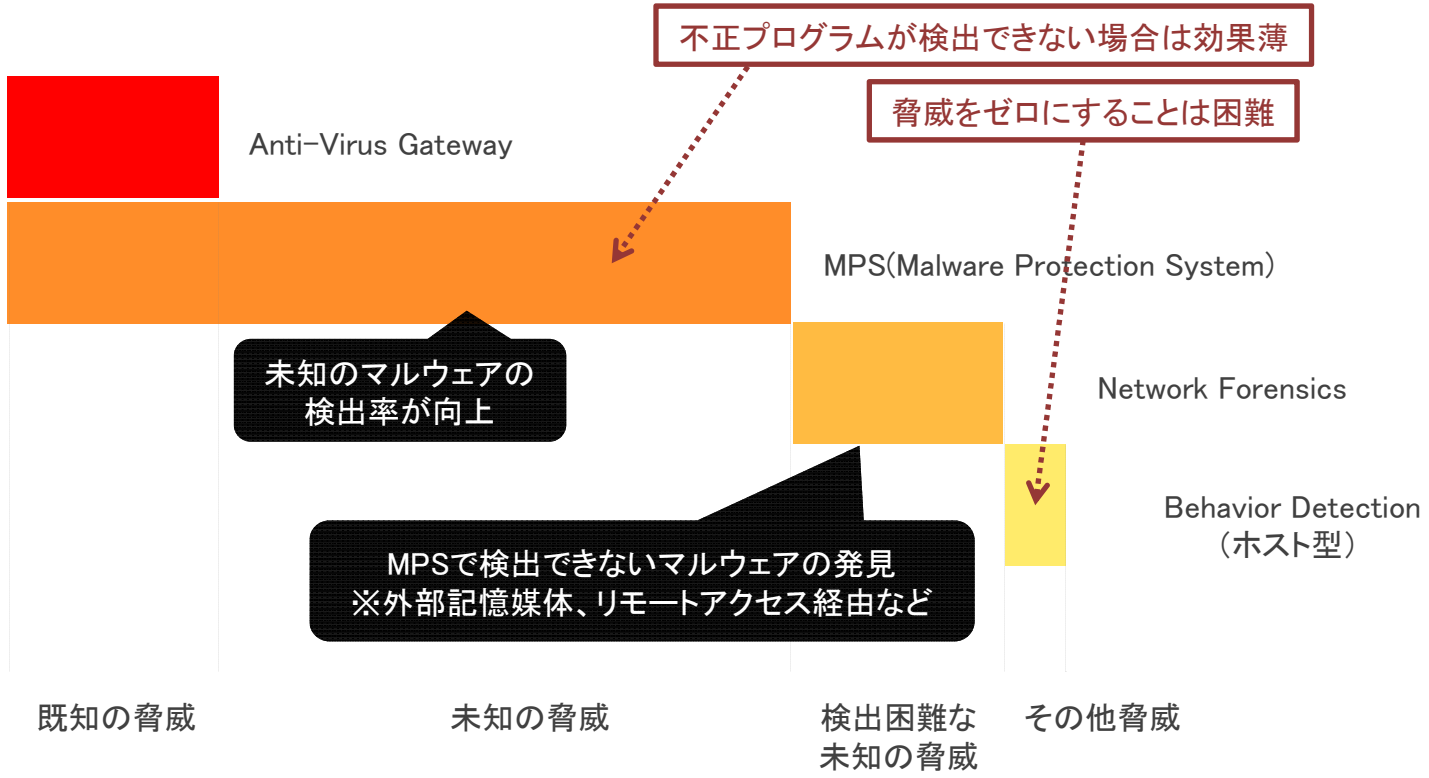
ハッカー vs IT専門家



ハッカー vs IT素人

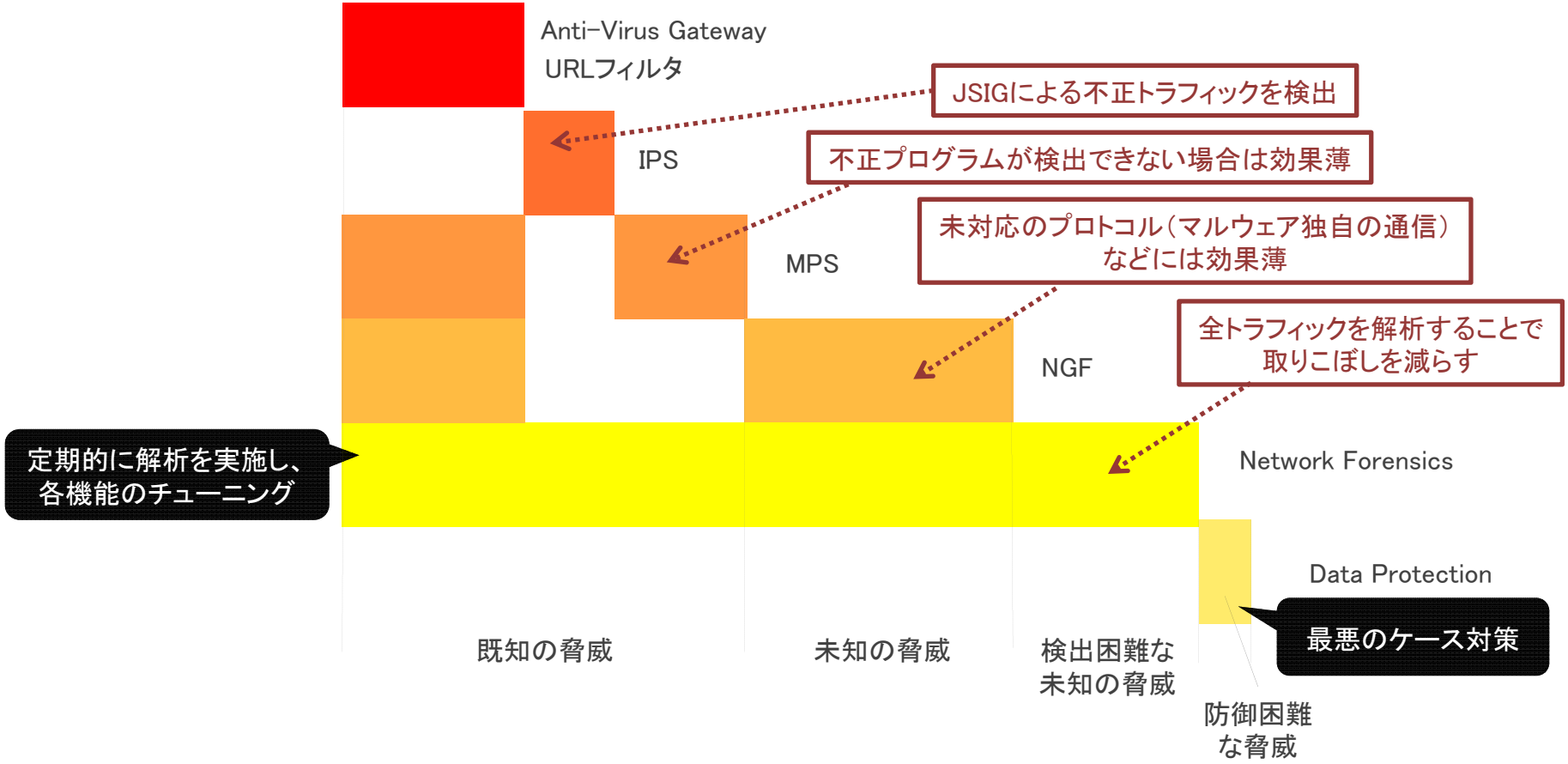
入口対策と脅威軽減の関係

多層防御により可能な限り脅威の検出率を挙げることが重要



出口対策と脅威軽減の関係

出口対策はダメージコントロールを目的とした対策が重要



ログ確認

- FW、Proxy、URLフィルタのログから以下のIPアドレスやドメインに対するアクセスがないか調べてください。
  - ezua.com
  - zyns.com
  - ns2.name
  - livecheck.org
  - acmetoy.com
  - toh.info
  - 2waky.com
  - ibmnetvista.com
  - xxuz.com
  - myfw.us
  - 2waky.com
  - www.microsoftoupdate.com
  - www.cloudsbit.com
  - nifty-login.com
  - nifty-user.com
  - nifty-japan.com
  - yahoo-user.com
  - yahoo-dns.com
  - google-login.com
  - 60.10.1.114
  - 60.10.1.118
  - 60.10.1.119
  - 60.10.1.120
  - 60.10.1.121
  - 112.213.118.31
  - 112.213.118.32
  - 112.213.118.33
  - 112.213.118.34
  - 112.213.118.43

対策の運用イメージ

機器運用と誤検知の問題

マルウェア対策は運用がキモ

専門知識を要し、非常に手間な作業

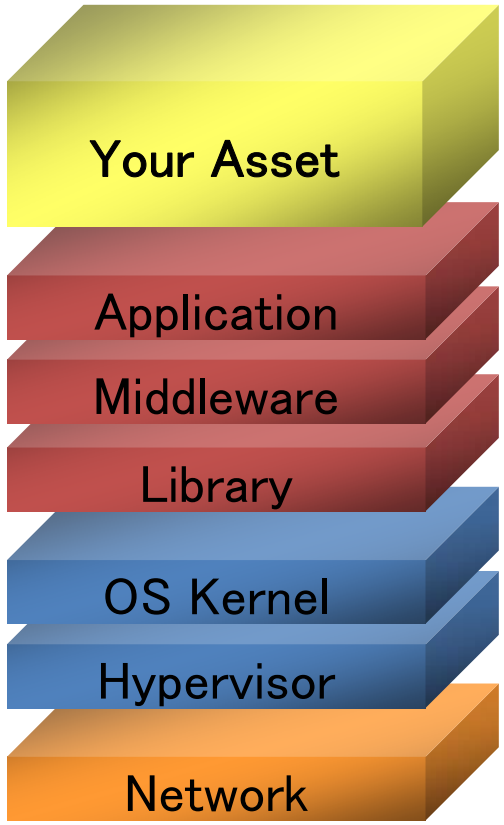
No	運用対象	説明
1	ウイルス対策ソフト	不審な添付ファイル発見 →メーカへ提供 →パターンファイル更新　のサイクル
2	IPS	ポリシーチューニング シグネチャを随時更新 誤検出の精査
3	MPS	検出したバイナリの即時解析 誤検出の精査
4	NGF	不明トラフィックの解析 ポリシーチューニング 誤検出の精査
5	Network Forensics	定期的な見えない脅威の検出
6	MPSによるマルウェア検出	検体解析による影響度判定
7	影響範囲の特定	マルウェア・フォレンジックス
8	修復・復旧	被害の修復・復旧

IT専門家のレベルアップ

- なくならない情報漏洩
- 億単位のユーザに影響

- 原因
  - サイトの脆弱性: アプリ、ミドルウェア
  - サーバの脆弱性: ライブラリ、カーネル
  - ネットワークレベルの脆弱性
  - 設計ミス
  - オペレーションミス

- 堅牢化（ハードニング）スキルの欠如



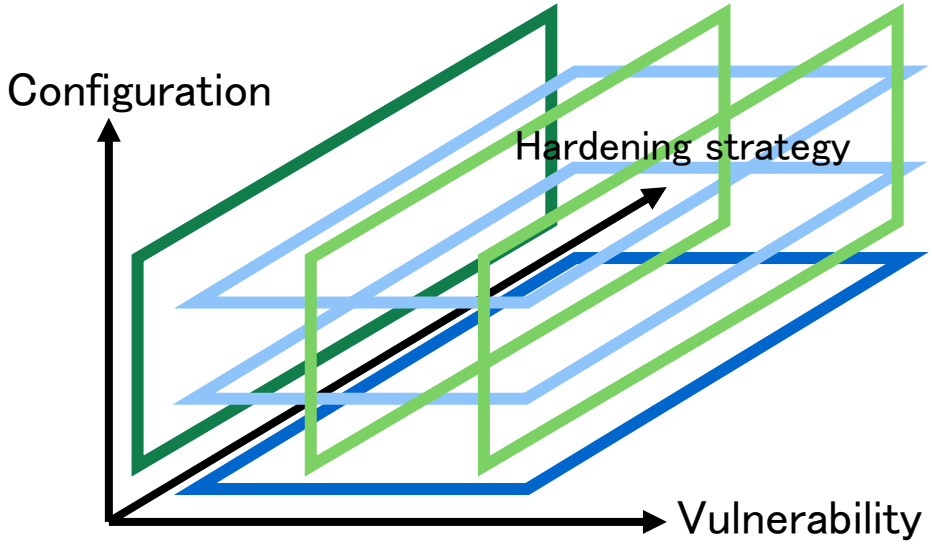
ハードニングはスキルだ

数万件の脆弱性情報

複雑なシステムの構成

守り方は数百通り

ハードニング戦略



ハードニングはビジネススキルだ

インシデント対応スキル
堅牢化スキル

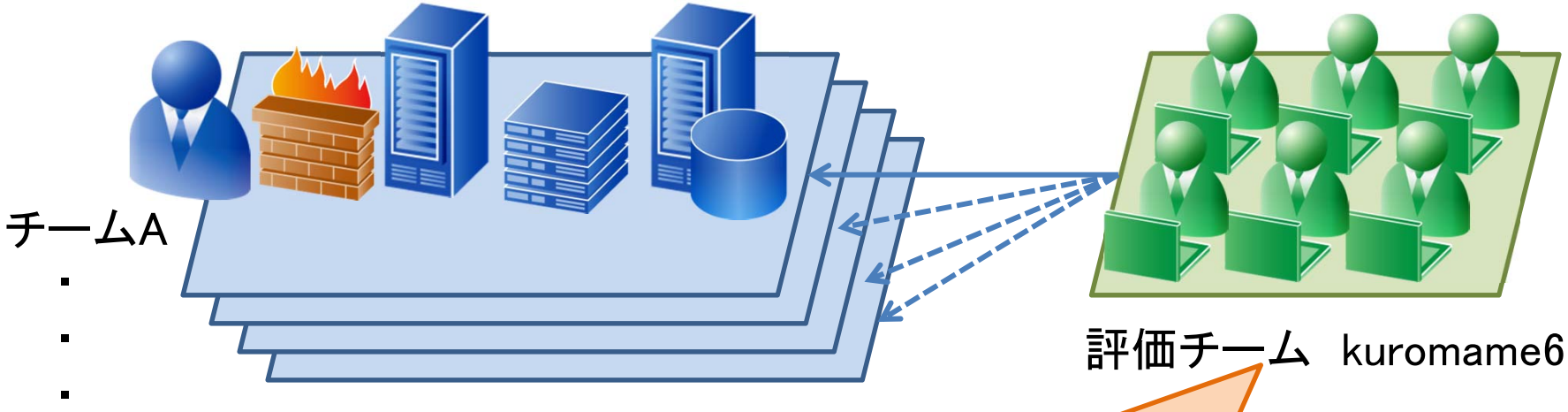
ダウンタイム最小化
メンテナンス戦略

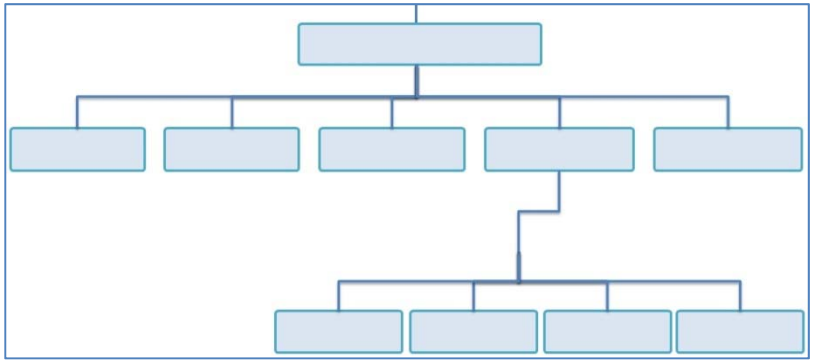
コミュニケーションスキル
アプローチの正当性

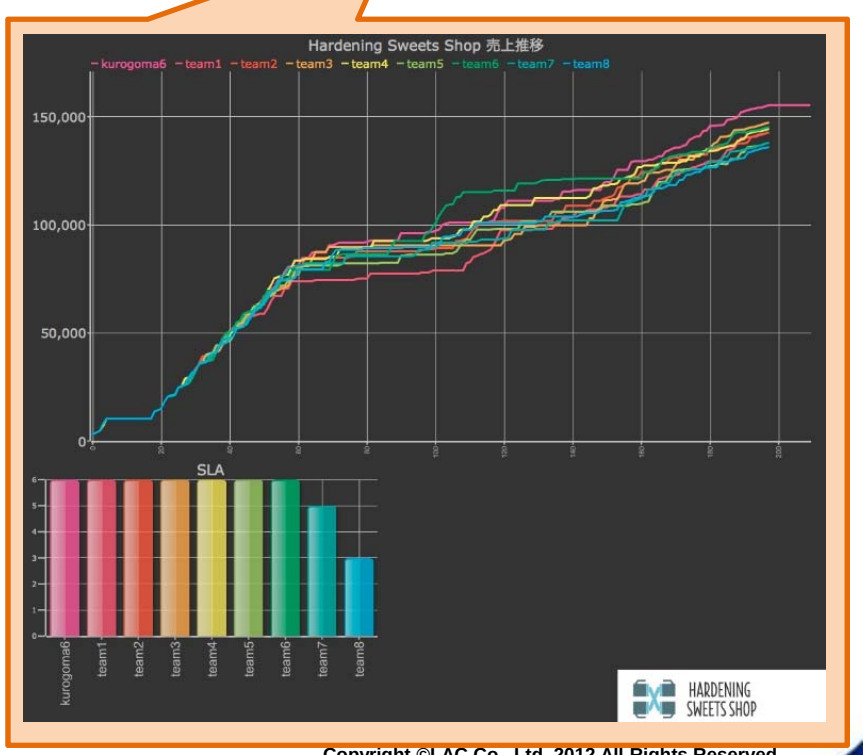
Hardening One 競技内容

- あらかじめ用意された、脆弱なeコマースサイトを8時間の間ハードニングしつつ**運営**
- 8チームがハードニングの強さを**総合的に競う**
- セキュリティ専門家によって構成されるペンテスト・チームがさまざまな手法と視点でハードニングの強さを**評価**
- 競技開始から終了までに、e コマースサイトのあちこちで発生するインシデントを乗り越えつつ、サイト運営を維持する総合力（堅牢性、売り上げ、ダウンタイム、コミュニケーションスキル）を評価

Hardening One 競技環境







8チームに同じ構成のECサイトを提供
8時間、ECサイトを守り続ける

Hardeningの狙い

- 堅牢化スキルの向上、経験知の共有
- 原則論からボキャブラリへ
- 現場で通用する頭脳筋肉力
- 矛盾や欠点をはらんだシステムを取り扱える精神力
- 他者と隔絶された「学び」から知的スポーツへの転換
- 最終的には.. 億単位の情報漏洩の撲滅！

Hardening 参加者の声

同じ環境、同じ商品、同じ攻撃が発生して運用の差で売上に三倍の差がでることがわかり、ITシステム運用の重要性を示すことができたのではないか

ITシステムの運用は"感じる"ことだ

あのバックドアはなんとなく見つけたので削除しておきました

限られた時間の中で対応するべき問題を取捨選択することが重要ですね

新入社員研修としてシステム運用の厳しさを味わわせるのが良い

今回のオペレーションミスを上司に報告したら怒られますね。精進します

インシデント対応時の情報共有の難しさがわかった

本番のシステムで障害を起こすわけにはいかないが、この環境で痛い目にあうことはいい経験になるはずだ

普段、めぐまれた環境で作業をしていたのでなかなか苦労しました

この参加者＆スタッフメンバーがこのイベントに集まったこと自体がすごいことだ

次回、リベンジしたい！！

日頃の業務で経験することのない「実務的な運用経験」を得ることができた

まとめ

敵の狙いを理解する
（狙われているところはどこか？弱いところはどこか？）

自分のシステムについて把握する
（できることとできないこと）

守る方は“運用”で勝負
（モノが同じならヒトとジョウホウで差がでる）

ありがとうございました。

ネット犯罪の多くは、
気づかなかったのではなく、
見えなかったのです。

株式会社ラック
http://www.lac.co.jp