セキュリティトレンドについて
予測とその結末

2010年のおさらいと2011年

http://dl.dropbox.com/u/7790765/shirahama20110526.pptx

株式会社ラック 最高技術責任者
西本 逸郎
itsuro@lac.co.jp
http://www.lac.co.jp/

株式会社ラック

蛇口をひねれば飲み水が出る当り前を、高度情報社会でも実現します。

株式会社ラックは1986年に設立されました。”Little eArth Corporation”という社名には、ICTの進展で地球が相対的に小さくなっていく中で、ITを基盤に国や企業の発展を支えていこうという理念がこめられています。**JSOC**（下記参照）、**サイバーセキュリティ研究所**、**サイバー救急センター**の配備が特徴です。

商 号	株式会社ラック LAC：Little eArth Corporation Co., Ltd.
設 立	1986年(昭和61年)9月
資本金	11億5,942万6,500円
株 主	ラックホールディングス株式会社(100%)
代 表	代表取締役社長 執行役員社長 齋藤 理
売上高	4,441百万円(25期：2010年03月期)
決算期	3月末日
認定資格	経済産業省情報セキュリティ監査企業登録 情報セキュリティマネジメントシステム (ISO/IEC 27001)認証取得(JSOC) プライバシーマーク認定取得

- ✓ http://www.lac.co.jp/
- ✓ sales@lac.co.jp
- ✓ Twitter @lac_security
- ✓ YouTube laccotv
- ✓ Facebook Little.eArth.Corp

・本社
〒102-0093 東京都千代田区平河町 2-16-1
平河町森タワー
03-6757-0111(代表)
03-6757-0113 (営業窓口)

・名古屋オフィス
〒460-0002 名古屋市中区丸の内2-18-11
46KTビル4F

・米国ニューヨークオフィス USLAC

・韓国ソウル 子会社 CSLAC
Cyber Security LAC Co.,Ltd.

・中国上海 子会社 LAC CHINA
上海楽客網絡技術有限公司

■ JSOC (Japan Security Operation Center)

JSOCは、ラックが運営する情報セキュリティに関するオペレーションセンターです。24時間365日運営。高度な分析官とインシデント対応技術者を配置しています。2000年の九州・沖縄サミットの運用・監視を皮切りに、日本の各分野でのトップ企業など高レベルのセキュリティが要求されるお客様に、高品質なサービスを提供しています。

わたし

にし　もと　　いつ　ろう
西本 逸郎　CISSP

昭和33年	福岡県北九州市生まれ
昭和59年3月	熊本大学工学部土木工学科中退
昭和59年4月	情報技術開発株式会社入社
昭和61年10月	株式会社ラック入社

通信系ソフトウェアやミドルウェアの開発に従事。1993年ドイツのシーメンスニックスドルフ社と提携し、オープンPOS（WindowsPOS）を世界に先駆け開発・実践投入。2000年よりセキュリティ事業に身を転じ、日本最大級のセキュリティセンターJSOCの構築と立ち上げを行う。
さらなるIT利活用を図る上での新たな脅威への研究や対策に邁進中。

情報セキュリティ対策をテーマに官庁、大学、その他公益法人、企業、各種ITイベント、セミナーなどでの講演、新聞・雑誌などへの寄稿等多数

株式会社ラック　取締役 最高技術責任者
サイバー救急センター
特定非営利活動法人 日本ネットワークセキュリティ協会 理事
データベースセキュリティコンソーシアム 理事、事務局長
日本スマートフォンセキュリティフォーラム 理事、事務局長

産業技術大学院大学 運営諮問委員（2009年～）
経済産業省 電子商取引等に関する法的問題検討会 委員（2007年～）
経済産業省　サイバーセキュリティと経済研究会　委員（2010年～）
IPA セキュリティ&プログラミングキャンプ実行委員（2007年～2009年）
（財）日本情報処理開発協会 リスク管理統制対応評価検討委員
2009年度情報化月間 総務省情報通信2008年～）国際戦略局長表彰

連載・コラム
西本逸郎のセキュリティー表ウラ
セキュリティー表ウラ　検索
http://it.nikkei.co.jp/security/column/nishimoto_security.aspx

ブログ　どらいつ　検索
@dry2

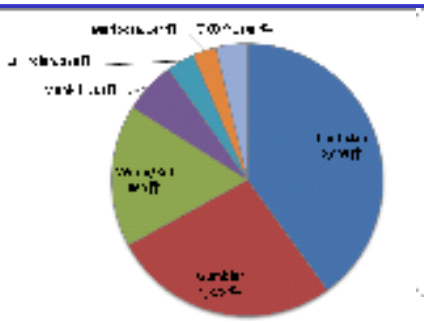
1. 昨年の予測とその結果

昨年の

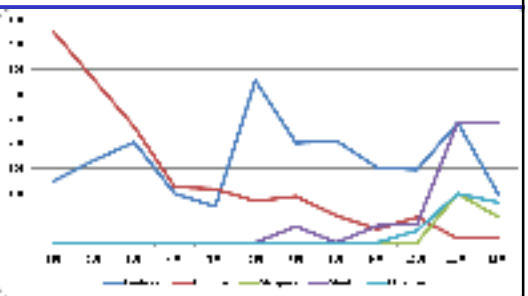
大胆予測

① ガンブラーの猛威はまだ続く。
Web改ざんの拡大
個人ブログなど

① ガンブラーの猛威はまだ続く。



内部ホストによるインシデントの内訳（2010年）



上半期においてはGumblarおよびConfickerのインシデントが全体の7割を占めておりましたが、下半期においては11月以降にMonkifやET Trojan（Taterf, Gammima）、Mariposaが検知されるようになりました。Monkifは、ダウンローダーウイルスの一種であり、日本でも10月ごろから大量感染が話題になっていたmstmpウイルスをダウンロードすることでも知られています。ET TrojanやMariposaは2010年以前から存在が知られていたものですが、監視機器へのシグネチャ追加によってこれらに関わる通信が検出可能になり、11月以降の検知が目立ちました。

2010年上半期において特にインシデント件数が多かったGumblarおよびConfickerの検知件数の推移および、下半期に検知が目立ったウイルスの検知推移を示します（グラフ 3）。2009年末より猛威を振るっていたGumblarの検知数は減少し続けており、2010年11月にはほとんど検知がなくなりました。5月前後から、攻撃対象として日本のホストを除外するといった動きも見られ、10月にはGumblar感染ホストが接続するボットネットの一つが停止した ことによる影響が現れています。
2010年のうちにGumblarの脅威は去ったように見えますが、年末にかけてはMonkifやET Trojanといった別のウイルスの検知が目立ってきています。これらのウイルスもGumblarと同様に、ドライブバイダウンロード攻撃によって感染するものであり、依然として無防備にウェブページを参照することによる脅威は継続しています。

② クラウドサービスの悪用

② クラウドサービスの悪用

Facebook
Twitter
AmazonEC2
などなど

③ クラウドとグレーゾーンの話題

③ クラウドとグレーゾーンの話題

どうせ、ブラックボックスだからね。
ブラックボックスだからこそ。

重要インフラになり得るのだろうか？

④ クラウドサービスでの事件

④ クラウドサービスでの事件

親ガメがこけると子ガメもこける。
どの親ガメに乗っているの？
それで、それは、どこにあるの？
ところで誰と契約しているの？

SaaS
PaaS
IaaS

⑤ ランサムウェア・スケアウェア（日本において）

⑤ ランサムウェア・スケアウェア

はずれ！

さて、
この1年何が？
おさらいオン！

昨年9月

関係者外秘

こんな事件が報道された。

FD改ざん事件が教えてくれたこと

改ざんFD

おい！ ドキュメントだけか？

現在、多くのところでデジタル写真やデジタル録音が、使用されている。
我々はすぐに、証明書が無いものはダメじゃん！と言ってしまいそうだ。

メタデータを変更することは可能。
費用対効果の考え方はないか？
完全に証拠を残すのか？
どっちが得？

そう言えば、こんなことも

関係者外秘

こんな報道も

そう言えば918

もともと節度のないピックアップ。

カモフラージュなのか？

日本国の見立てはどうだったのか？

最高機密で構わないけど、

どのレベルのインテリジェンスで

動いていたのだろうか？

そう言えば918　そうこうしてる間に

そう言えば918 そうこうしてる間に

こんなことも

そう言えば918 そうそう、当該期間に、、

これは？
チョイやばかも。

情報漏えい対応で分かること

個人情報漏えい事件で浮かび上がった事実

Webサーバのログを解析すると、、、リファラ(リンク元)の
フィールドに。

http://www.baidu.jp/s?lm=0&si=&rn=100&ie=utf-
8&ct=262144&wd=inurl%EF%BC%9A%20php+%C9%CF%20%D6%A7%B8%B6%20visa+jcb&
pn=200&cl=3&usm=0&ys=1”

①

犯人の行動 ①

① 百度で検索

→ JCB VISA 支

犯人の行動からわかること

正当な利用者も攻撃者も接点は検索エンジン

どういう検索キーワードで、自サイトを訪れたのか？ → 訪問目的 ？
SEO対策は、セキュリティの観点でも極めて重要。
利用者に興味を持たせ、攻撃者に興味を持たせない、SEO対策。

みんな、脆弱性をなくそうとかあらゆる脅威から防ごうとかいうけど、
その前に、

[redacted] ！

大量サイトの改ざん被害報道

広告サイトが改ざん

幕の内弁当サイト

広告、ブログツール、サイト統計など

利用者からみれば、当該サイト。
理屈としては背後にある
提供側サイトの問題だが、それで良いのか？

利用者への責任は誰に？

ある緊急対応

パソコンが不審な動作をしたということで119コール。
調査をしてみると。不審なファイルが。

大手量販店サイトのキャッシュ

悪性サイト接続時のクッキー

9月24日・25日で終結では？

jar_cache6353730857261419804.tmp	tmp	\Documents and Setti...	6.2 KB	2010/09/29 08:58:01
0.49385497375118415.swf	swf	\Documents and Setti...	24.5 KB	2010/09/29 08:58:03
mstmp		\Documents and Setti...	22.1 KB	2010/09/29 08:58:10

ウイルス関連ファイル

所謂、ボットタイプのコンピュータウイルス
パスワードの盗聴など

生成日時

大手量販店サイトへアクセス

スクリプトにより悪性サイトに誘導
恐らく、スクリプトは削除

JAVAの脆弱性をついて侵入
悪性プログラムのダウンロード

ボット感染

ある緊急対応

別の119コール。調査をしてみると。
やはり同様の不審なファイルが。

大手雑誌サイトの
クッキー

ma.b C:/Documents and Settings/XXXXXX/Cookies/XXXXXX@64.27.25[2].txt

Last Visit-	Prot.	Domain	Resource	Cache Filename	Size	Ext.
10/08/2010 10:08:51 4 +9	Cookie	imrworldwide.com	cgi-bin	@cgi-bin[2].txt		txt

同様の
悪性サイト
接続時の
クッキー！

？？？

大手雑誌
サイトへ
アクセス

スクリプトにより
悪性サイトに誘導
恐らく、
スクリプトは削除

JAVAの脆弱性を
ついて侵入
悪性プログラムの
ダウンロード

ボット感染

調査してみると

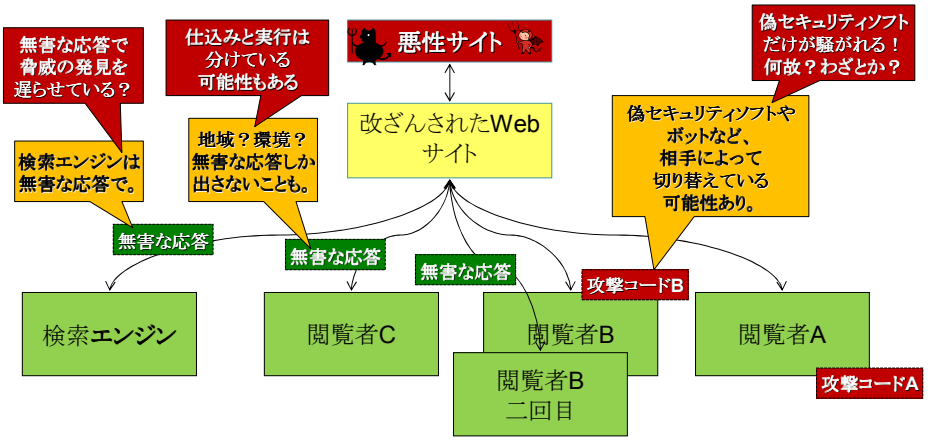
「ルパンを追っていたら、
とんでもないものを見つけてしまった。

どうしよう？」

銭形のとっつぁん in カリオストロの城

ある緊急対応

ある緊急対応要請あり。
サイト改ざんを受けたらしい。サイトオーナが確認するも見つからず。
同じようなケースが何件かあり、確認してみると、意外なことが。



あと大変気になること

この悪性プログラムが悪用する脆弱性 CVE-2008-5353

The Java Runtime Environment (JRE) for Sun JDK and JRE 6 Update 10 and earlier; JDK and JRE 5.0 Update 16 and earlier; and SDK and JRE 1.4.2_18 and earlier does not properly enforce context of ZoneInfo objects during deserialization, which allows remote attackers to run untrusted applets and applications in a privileged context, as demonstrated by "deserializing Calendar objects".

最新版
(6 Update 22)にアップデート

MyJVN バージョンチェッカ
http://jvndb.jvn.jp/apis/myjvn/vccheckhelp.html

バージョンチェッカがJREを使用している。JREのバージョンをチェックしたいのだから問題ないか？いやいや、もともと使用してなければ、わざわざ脆弱点を増やすことにもなるぞ。

JREは多くの組織の社内システムで使用されている。パッケージソフトにも使用しているものがある。JREの新版に対応してないケースもあり、JREを最新に出来ないことも。

参考:メディアの使用しているスクリプト

尖閣ビデオ流出事件

関係者外秘

※ http://www.youtube.com/watch?v=6VluqeyoyHc

尖閣ビデオ流出事件 ビデオ映像の管理を考えてみる

ビデオ映像の特徴

1. 大容量である。
2. 受け手により、受け取り方が異なる。
   → 文字とは違う
3. 様々な目的で使用される。
   → 記録、訓練、報道、証拠、外交

真正性担保と CIA(機密性・完全性・可用性)

動機として 興味、愉快

キャンペーン相手は事前に知りたい。メディアの競争。インサイダーは？

PR キャンペーン

強烈な動機がある
外部 無効化・PR
内部 内部告発・メディア 買収・内通

真正性は担保出来ていたのか？ 守りきれる自信があったのか？

プロセス・記録・根拠 内部・外部

私物のUSBメモリにコピーして持ち出し、インターネット喫茶から投稿。
→ 匿名性を担保し法律を抜けている。権限保持者の思想犯をどうするか？

警視庁公安部外事3課の内部資料流出

警視庁の公安情報流出、発信前に経路匿名化

ウェブサイトへの文書掲載や、イラク、中国の両在日大使館などへの掲載先を知らせるメールの送信などには、通信経路を見えにくくする匿名化のシステムが使われたことが捜査関係者への取材でわかった。

関係者によると、使われたのは「Tor」(The onion router)と呼ばれるシステム。

「オンラインストレージサービス」と呼ばれる、文書などを保存・閲覧できるサイト

なるほど、ばれないためにTORを使用したのか。また、人に告知するのにオンラインストレージか。ひょっとすると最初の持ち出しも？？？？

http://www.asahi.com/national/update/0103/TKY201101030295.html

話題のWikileaks

疑問点 日本でのミラーサイトは違法なのか？

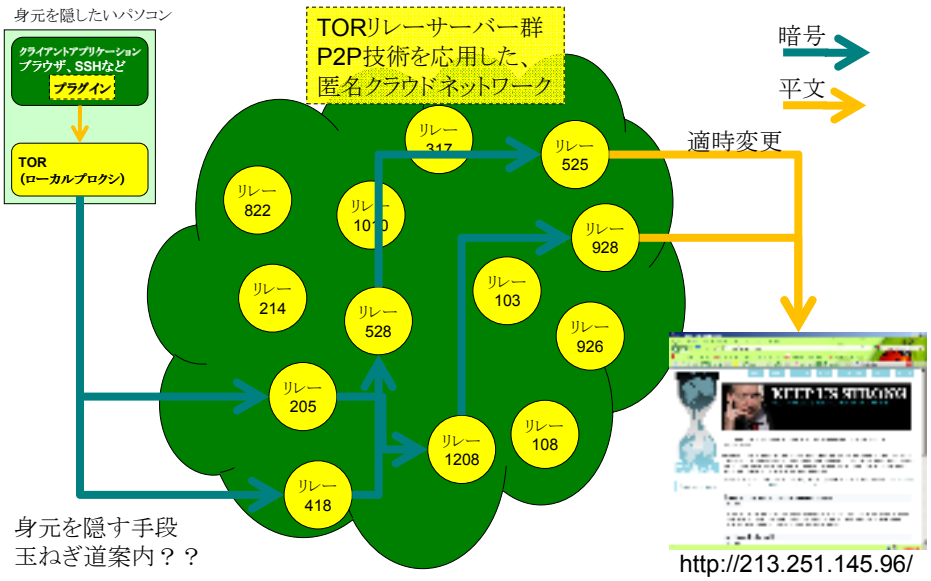
Wikileaksへの投稿はTORの使用が推奨されているらしい。

2010年4月
00点
年7月25日
米軍の機密文書約40万点
010年10月22日
告発内容
2010年11月29日～
テキストデータ
米国外交機密文書
251,287件
12/12現在 1295件公開
平均データ量 約13K
推定データ量 251287*13K 約3,3GB

25万件のデータって紙だと、100枚で1cmとすると25万ページは25m

高々、3.3GB 1cm²のUSBメモリで持ち出し可能。

TOR(The Onion Routing)



制御システムも

クローズな環境への侵入と制御を示し
データの持ち出しなどへの
可能性を示唆した。

また、国家関与の可能性示唆。

ソーシャルメディアの威力

中東諸国の情勢

ソーシャルメディアが民主化を後押ししている。

ソーシャルメディアインパクト。

一つの考察 サイバーテロ？？？？

一つの考察 サイバーテロ？？？？

標的型サイバー攻撃

弊社サイバー救急センターに寄せられた、
標的型と推測される、最近の相談

2008年　4件　**Web改ざん、USBメモリ、メール**
金融系、放送メディア、公益法人、情報通信

2009年　5件　**USBメモリ、メール**
製造、エンターテイメント、情報通信

2010年　6件　メール
製造、情報通信、エンターテイメント

2011年　4件 メール
製造、エンターテイメント

標的型メール … 狙いは政治家・官庁

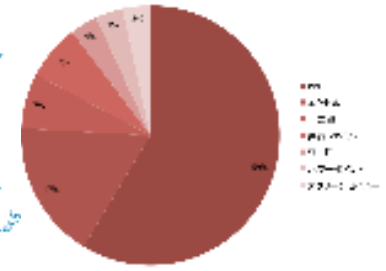
標的型メール … 狙いは一般企業

標的型メール … 狙いは一般企業

標的型メール … 狙いは一般企業

標的型メール 解析してみると

No.	内容	送信元（詐称）	備考
1	人事異動	総務部	公開情報であることが多い
2	業務執行体制の改正	総務部	公開情報であることが多い
3	IR 情報	広報	公開情報であることが多い
4	目標・評価表	総務部	
5	こども手当て	総務部	
6	イベント等の案内	公益法人	公開情報であることが多い
7	機密管理	総務部 / 役員	
8	海外ニュース	取引先	公開情報であることが多い
9	議事録	取引先 / 従業員	メールが盗聴されている可能性あり



標的型メール　ウイルス対策ソフトの反応

0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is goodware. 0 V
user(s) with a total of 0 reputation credit(s) say(s) this sample is malware.

File name:
Submission date: 2010-09- 04:59:59 (UTC)
Current status: finished
Result: 6 /42 (14.3%)

GData	21	2010.09.21	Dropped:Generic.Malware.S
Ikarus	T3.1.1.88.0	2010.09.21	-
Jiangmin	13.0.900	2010.09.20	-
K7AntiVirus	9.63.2561	2010.09.20	-
Kaspersky	7.0.0.125	2010.09.21	Heur.Trojan.Generic
McAfee	5.400.0.1158	2010.09.21	-
McAfee-GW-Edition	2010.1C	2010.09.21	-
Microsoft	1.6201	2010.09.20	-
NOD32	5465	2010.09.20	-
Norman	6.06.06	2010.09.20	-
nProtect	2010-09-21.01	2010.09.21	-
Panda	10.0.2.7	2010.09.20	-
PCTools	7.0.3.5	2010.09.21	-
Prevx	3.0	2010.09.21	-
Rising	22.66.00.03	2010.09.20	-
Sophos	4.57.0	2010.09.21	-
Sunbelt	6903	2010.09.21	BehavesLike.Win3
SUPERAntiSpyware	4.40.0.1006	2010.09.21	-
Symantec	20101.1.1.7	2010.09.21	-
TheHacker	6.7.0.0.025	2010.09.20	-
TrendMicro	9.120.0.1004	2010.09.20	-
TrendMicro-HouseCall	9.120.0.1004	2010.09.21	-
VBA32	3.12.14.0	2010.09.20	-

0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is goodware. 0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is malware.

File name:
Submission date: 2010-09- 02:22:35 (UTC)
Current status: finished
Result: 7 /43 (16.3%)

GData	21	2010.09.20	Gen:Trojan.Heur.FU.cq0aeWEAfdi
Ikarus	T3.1.1.88.0	2010.09.20	-
Jiangmin	13.0.900	2010.09.19	-
K7AntiVirus	9.63.2552	2010.09.18	-
Kaspersky	7.0.0.125	2010.09.20	Heur.Trojan.Generic
McAfee	5.400.0.1158	2010.09.20	-
McAfee-GW-Edition	2010.1C	2010.09.19	-
Microsoft	1.6201	2010.09.19	-
NOD32	5462	2010.09.19	-
Norman	6.06.06	2010.09.19	-
nProtect	2010-09-20.01	2010.09.20	-
Panda	10.0.2.7	2010.09.19	Suspicious file
PCTools	7.0.3.5	2010.09.20	-
Prevx	3.0	2010.09.20	-
Rising	22.65.05.00	2010.09.18	-

当該組織が使用している対策では、防御できないことを確認していると推測される。
（だから標的型）

標的型メール　ウイルス対策ソフトの反応

CVE-2010-3333（MS Office Word のセキュリティホール）
※ RTF のスタック バッファ オーバーフローの脆弱性

Virustotalのスキャン結果：　1/41（3月22日付）
Officeファイルの解析ツール：　未対応
※RTF（リッチテキストフォーマット）が利用

CVE-2009-3129（MS Office Excel のセキュリティホール）
CVE-2009-0927（アクロバットリーダー getIcon関数処理の脆弱性）
比較的検知率は高かったため、発見は早かった。

ウイルス対策ソフトは有効ではないのか？

ウイルス対策ソフト ＝ 有効

標的型攻撃での不正プラグラムを、
→ ウイルスと呼んではいけない。

ウイルス対策と 標的型攻撃の対策は
→ 根本的に異なる

経営者に対して
→ 異なった脅威であることの理解

標的型攻撃　メールだけなのか？

標的型攻撃＝メール は

メールは、内部に「入る為の手段」。

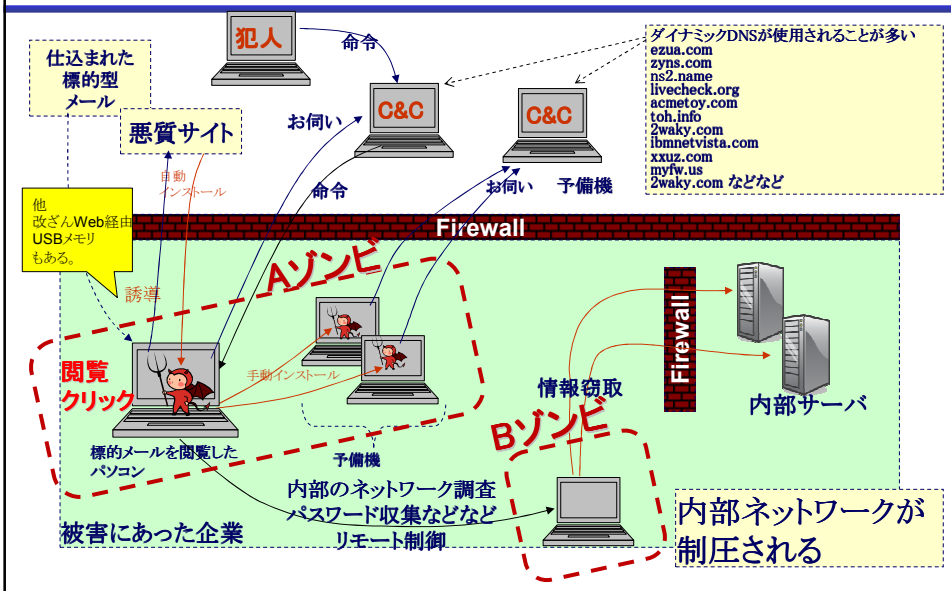
他の手段は、、、
パソコンに対して、、、
→ **USB**メモリ、改ざんサイト閲覧

サーバに対して
→ **SQL**インジェクション他　様々

標的型メール 手順（推測）

1. Webやネットでの公開情報 氏名・役職・メールアドレスなど取得する。
2. 公益法人などの外部文書や時事関連文章などを使用してメール送信する。
   →標的型メールは全て把握しているという妄信があり、安心している。
   →ウイルス対策ソフトへの過信もある。（標的型であることを意識できていない）
   →脆弱性管理、OS、ブラウザ、PDF、フラッシュ、JREなど
   → たかがウイルスと思っている。
3. 内部構成を調査し関連情報を手に入れる。
   ネットワーク構成、アカウント管理方法、サーバ配置など
4. アカウント情報・パスワード窃取。特に管理者権限の獲得を目指す。
   例えばアクティブディレクトリ（＋LM認証）、キーロガーの使用など
5. 渡っていくうちに、手に入れた本物の内部文書を使用した標的メール
   （役員などを名乗る）で、さらに侵入範囲を広げる。
6. 複数の予備経路を確保する。（利便性の確保と気付かれた時のためと推測される）
7. 当該組織専用プログラムも作成し使用している。
   （調査や情報窃取の生産性向上策と推測される。）
8. 内部ネットワークを制圧し、内部文書の窃取を行う。

標的型攻撃の本質 ＝ 内部システムが乗っ取られ操作される！



標的型メール 流出情報

標的型攻撃で狙われた情報

1. 技術情報

2. 大型投資情報

国家的？

標的型サイバー攻撃の課題　現場の実態

1. 脆弱性管理が出来ていない →「閉塞域だから大丈夫」が崩壊。

Windowsに関しては向上している。アドビーアクロバット、フラッシュ → 通達はしているものの守ってはいないことも多い。JREに関しては内部システムで使用されており、そもそもバージョンアップが困難である。

2. 緊急時に行動できる体制がない。 → 縦割り。事故未前提。

e-discovery対応などでアーカイブはされていることは多いが、調査の承認プロセスなどに、非常時のことが考慮されていない。役員クラスが部門を横断して指揮を執っていないことが多い。インシデント発生時のプロセスが適切ではない。（証拠の破壊）

3. 駆逐は困難を極める

行動解析（検体収集機の設置、IDS等、アーカイブ解析などなど）、接続先解析、ログ解析、外向き通信から、被弾PC特定、検体抽出、定義ファイル作成、駆除（可能ならば、不可の場合は再インストール）を行う。これを繰り返しを行いつつ、駆逐確認と残党狩りを実施する。重要なことは、これで全部かが分からない。そのため、他の情報もほしいがそのルートがない。単独の専門ベンダーでは対応に限界がある。しかも、ウイルスがいても、情報を取られているかもしれないけど、お仕事は止められない。

標的型サイバー攻撃の課題　現場の悩み

4. 従来のウイルス対策では対応が困難。

従来型脅威は防御（感染を止める）を行うことが出来る。万一感染しても、駆除を行えばよい。（実物を早期に入手できるし、局所的な被害が出にくい。）

一方、標的型の場合、徹底的な原因究明が必要となるが、一般的に侵入経路や窃取内容などの調査には被害企業も専門ベンダーも実施する動機が薄い。さらに、駆逐を行うためには不正プログラムの機能解析や目的調査も必要となるが、通常、費用も高額となり被害企業が費用を負担しない限り実施はしない。一般的に被害企業もそこそこで終わりにして業務継続を優先するため、情報も共有されずに、他の企業も被害にあってしまっている危険性も高く、その点検を行うこともできない。

全貌をつかむには一企業だけでは限界があるにもかかわらず、被害企業は決して公表しない。

ソニー事件で学ぶこと

1. [redacted]の経営
2. [redacted]セキュリティの崩壊
3. 境界防御は線から円へ
4. グローバルビジネスのローカル対応
5. これは一種の[redacted]かもしれない

「ソニーの情報漏えい事件で我々は何を学ぶか」
http://www.lac.co.jp/column/20110517.html

とはいえ、どうすればいいのか？

江戸時代のセキュリティ方針

1. 相互監視体制
   五人組、長屋など
2. 入り鉄砲に、[redacted]

境界防御の考え方を変化！

もうひとつ！

経営再建の神様
稲盛さんのお言葉

入るを図りて
を制す。

そうそうクラウドとスマホ

クラウドを
組織で活用している？
Yes?　　No?

スマートフォンを
組織で活用している？
Yes?　　No?

そうそうクラウドとスマホ

スマートフォンを
個人で活用している？
Yes?　　No?
クラウドを
個人で活用している？
Yes?　　No?

スマホの現状

日本におけるスマートフォン出荷予測（東京IT新聞）

2010年度	440万台 → 675万台	2.9倍 18.1%
2011年度	1,545万台	2.3倍 40.6%
2012年度	1,925万台	124% 50.1%
2015年度	2,410万台	63.1%

サムソン社

2009年	600万台
2010年	2,000万台
2011年	6,000万台

スマートフォンの位置づけ

組織とスマートフォン

二つの関係

1. 組織が利活用を図りたい。→ もろ刃の刃
   → 確実に、従来アプローチ
   Smartphone in Jail.（檻の中のスマートフォン）

2. 個人が利活用を図りたい。→ 生活技術
   → 圧倒的な普及速度。
   Smartphone into Jail.（檻に入るスマートフォン）

IT活用の「民主化要求」？

スマホで出会う、業務とプライベート
パソコンの将来像？？？

お付き合いの選択肢

1. 禁止する。
   → いたちごっこ。やっても一時的。
2. 黙認する。
   → あり得ない。　　← ここは多い

3. すべて許可する。（受け入れる）
   → 決断。

4. 安全なやり方を用意する。
   → 必然だけど、なかなか難しい。

5. 安全なやり方を学習していく。
   → ワークスタイル。リテラシー。生活を守る。

そう言えば、この会社！

ちなみに有名な「　　」

4つの行動原則って、ご存知でしょうか？

この1年の総括

IT事件の一般化

1. 朝ズバで
2. 多くの普通の事件にITが絡んだ
3. 取材メディアがストーリを持っている

この1年の総括

神話の崩壊

1. 物理的に隔離されているから大丈夫。
2. あり得ない組織であり得ないことが。

IT民主化の萌芽

1. ソーシャルメディア
2. スマホ＆クラウド
3. 告発
4. サイバー市民運動　穏健派・強硬派
   → 一種の戦争と言って良い。

これからの1年　予測

2011年　かのとう

辛卯

しんぼうの年

1. 辛い年。我慢の年。
2. 予期せぬ大事故・大災害が起きる年。
3. 草木が枯死して新しくなろうとする状態。

これからの1年　だから、、、

2011年

予測できません

1. びっくりすることが起きる。
2. あっという間に世代代わり。
   何が死滅するのだろうか？
   とって代ったものも、一時的。

どうすれば？

考えられているじゃないか！

2009年2月3日 内閣官房情報セキュリティセンター(NISC;National Information Security Center) から公開された「第二次情報セキュリティ基本計画」。

事故前提社会への対応力強化

これまで

100%の安全・安心の追求 → 消費者目線のつもり。
無謬性の追求　→ 実は提供者目線

それで

大人社会への変革が重要。
双方の責任を明示しリードしていくことが肝要。

具体的には

最悪の事態を共有し、
それが起きたらどうするのかを考える。

最後に

メガリークの時代

→ 流出は避けられない。

ステークホルダとの関係

→ 正直に。お互いに敬意を。
→ 社外秘を極力無くし、グレーなことを止め、満足度を高め、万一に備える。

3年から5年で考えよう！

→ ソーシャルメディアとスマホが第一歩。

もちろん最先端の低コスト防御技術も重要。個人やSOHOのセキュリティはただにしたい。

提言 情報管理八策

情報管理八策2011

一、情報管理とは、情報の「適切な利活用が目的」であり、組織や個人を守り社会に貢献するものである事。

二、電子化された情報に接する全ての者は、その劇的に変化する特徴や基本的なリスクを理解し、情報取り扱いの作法を身につけるよう努め、組織の長はその徹底を図る事。

三、情報の機密度や配布先、閲覧可能場所などは最初に決定すべきであり、途中で変更することは極めて難しいという心構えで臨む事。

四、あってはならぬことであっても、技術的欠陥、権限保持者の犯罪や告発、並びに詐欺などにより事故は発生するものである。100%の安全策は存在しないことを理解し、常に事故発生の備えをしておく事。

五、事故を起こした者や内部告発者への評価など、情報管理の有り様が世情により刻々として変化していくことを踏まえた上で、各組織の実情にあわせた公正妥当な管理策を制定する事。

六、電子機器の急速な進化により人々の生活や働き方が大きく変化しつづける中、情報が個人と組織の間を区別なく行き来することを前提に管理策を練る事。

七、全ての組織は、その情報への依存度にあわせ、制度制定、安全措置、教育や訓練の実施、監査、事故対応など、予防と抑止の両面で対策の高度化を推進する事。

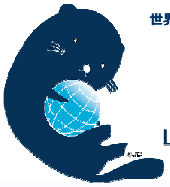
八、情報管理水準の向上に携わる全ての組織は、私たちが身に付ける情報管理の有り様が、来る高度情報社会における、わが国の成長と国際的な地位確立の礎となることと認識し、技術と意識レベルの向上に努める事。

※ http://www.lac.co.jp/hassaku/index.html

そうそう、
弊社の岩井が、
インターロップで、
クラウド環境での
フォレンジックに関して
なんかやるらしい。

ありがとうございました。

Any question ?



世界トップレベルのセキュリティノウハウで、
日本のスタイルを支える。

LAC
Little eArth Corporation

株式会社ラック
http://www.lac.co.jp/
sales@lac.co.jp