資料6

クラウドサービスで発生している インシデントについて

LAC
Little eArth Corporation

2012年3月19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

平成23年度第3回学術情報基盤オープンフォーラム

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)

LAC
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。

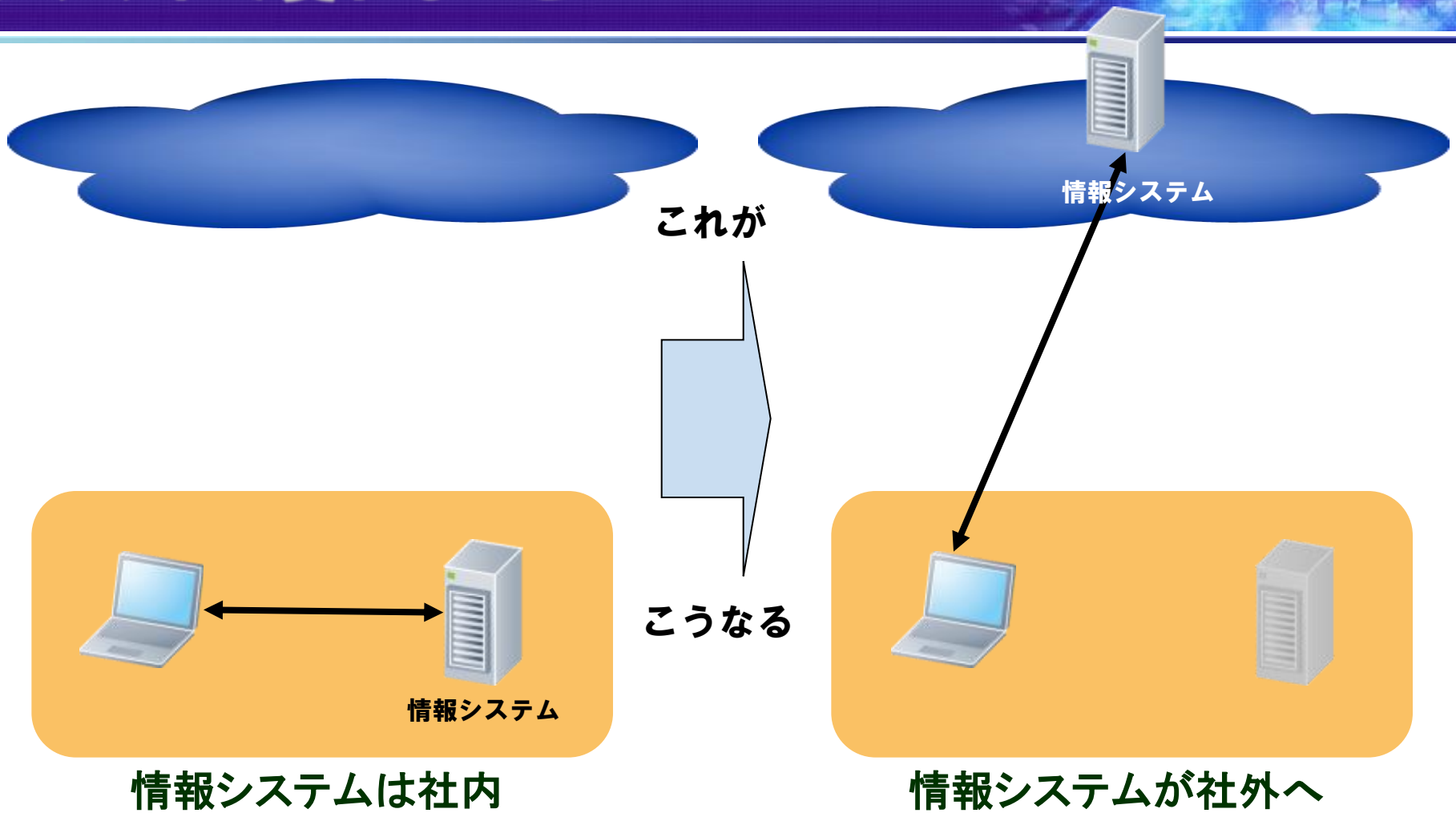
ー FW 監視サービス
ー IDS/IPS 監視サービス

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

クラウドで変わること

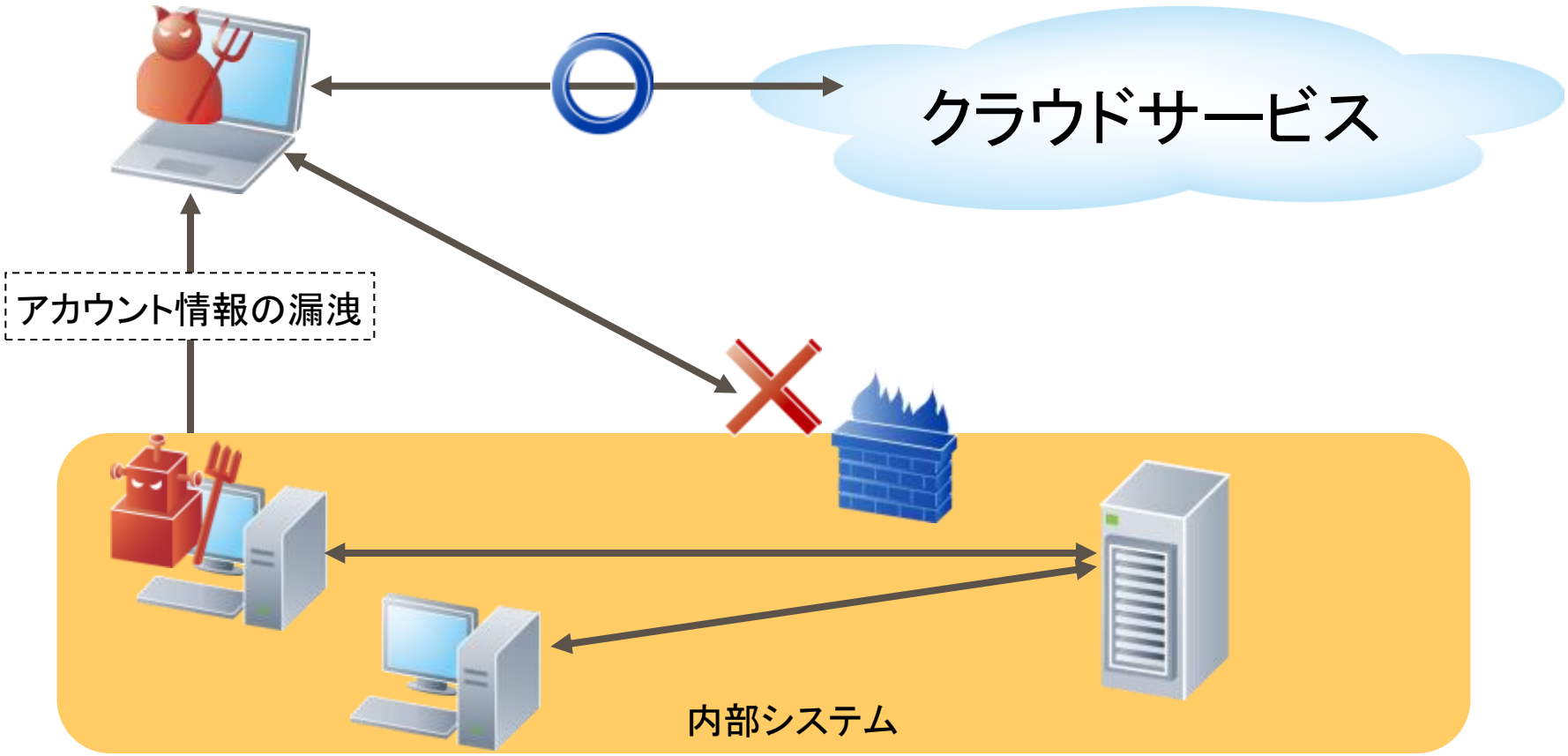


コンプライアンス対応

可用性・パフォーマンス

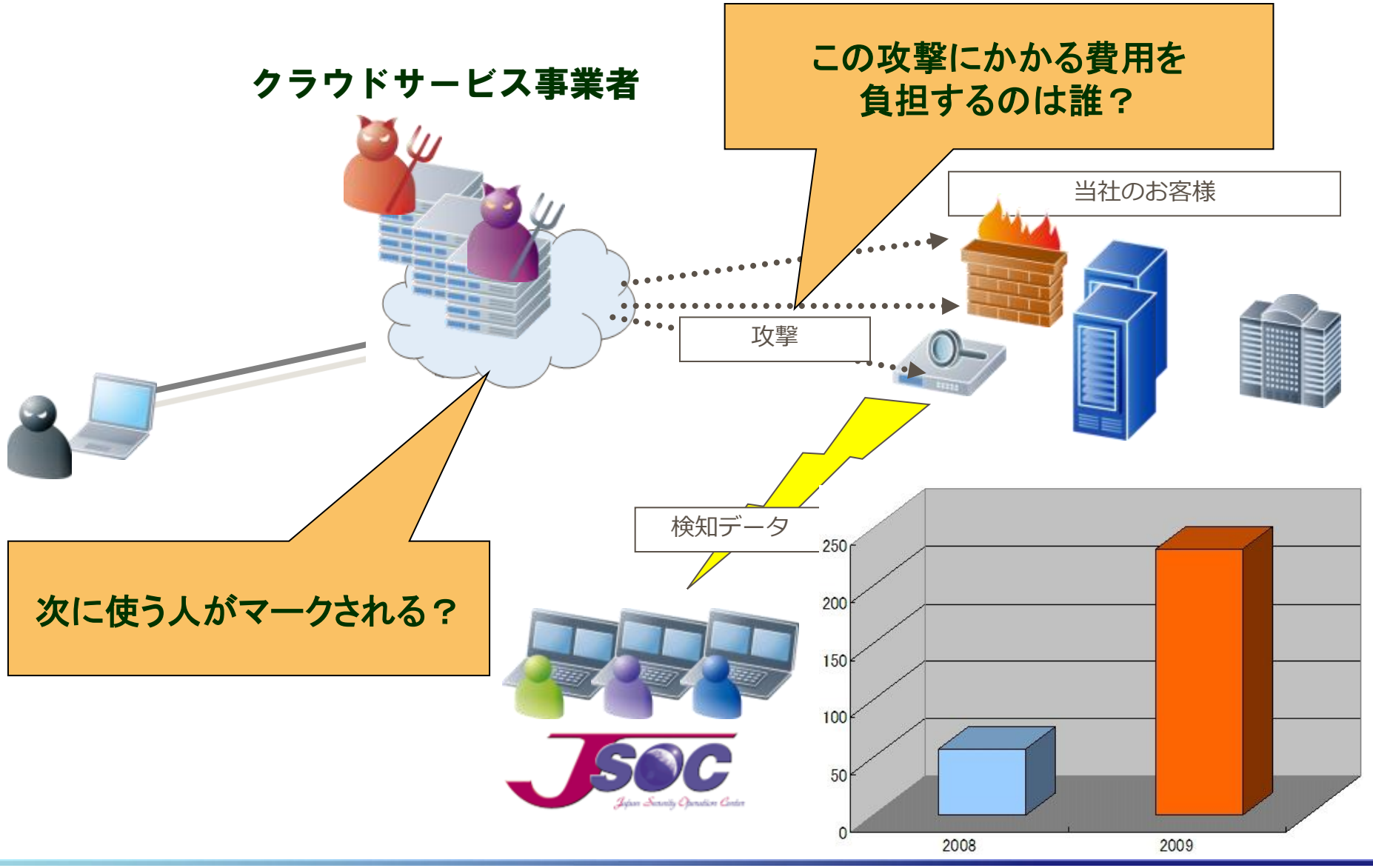
クラウドのアクセス制御

クラウドの利用による変化



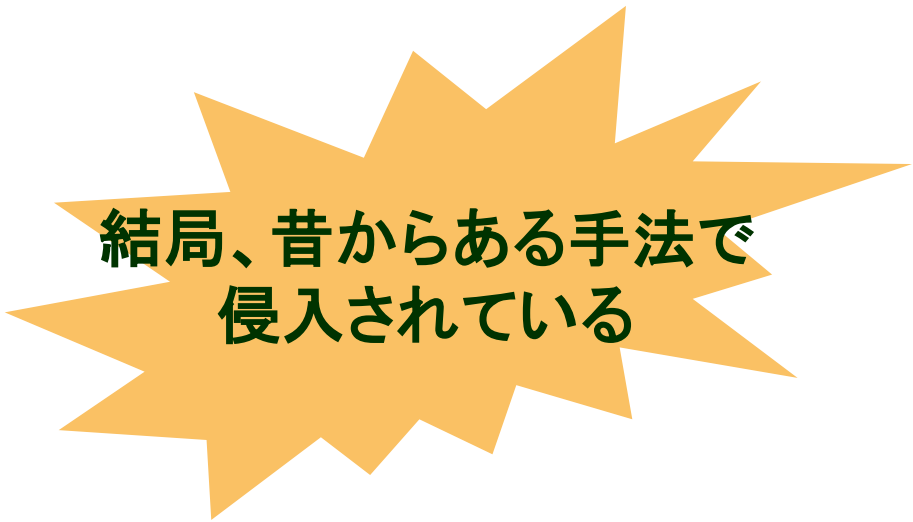
- 従来のシステムはIPアドレスによるアクセス制御が設定されている
- (パブリック)クラウドは誰でもアクセス可能(※アクセス制御は可能)
- 悪用された場合でも、課金請求は正規の利用者へ
- **アカウント情報を盗用**するボットが大きな脅威になる

クラウドからの攻撃



発生しているインシデント

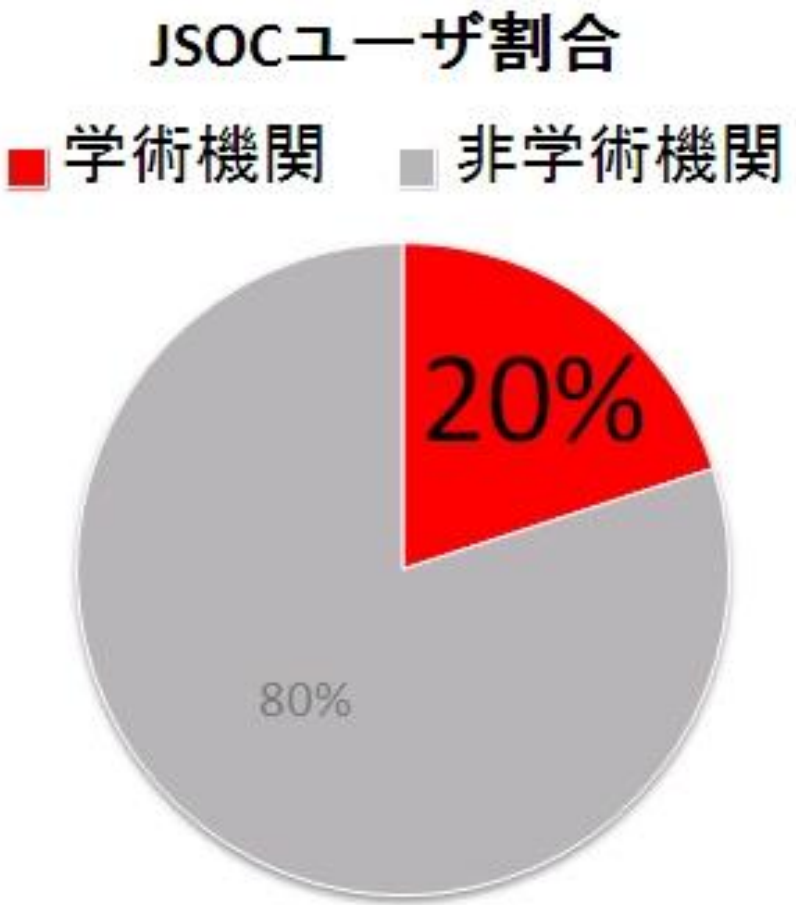
- SSHブルートフォース
  - 22/tcp
  - パスワード認証
  - 脆弱なパスワードを設定しているユーザ
- サーバ管理画面に対する侵入
  - Tomcat
  - JBoss
- CMSに対する侵入
  - phpMyAdmin
  - Plone/Zope
  - Joomla!
  - Xoops
  - phpBB
  - その他、聞いたことがないCMS

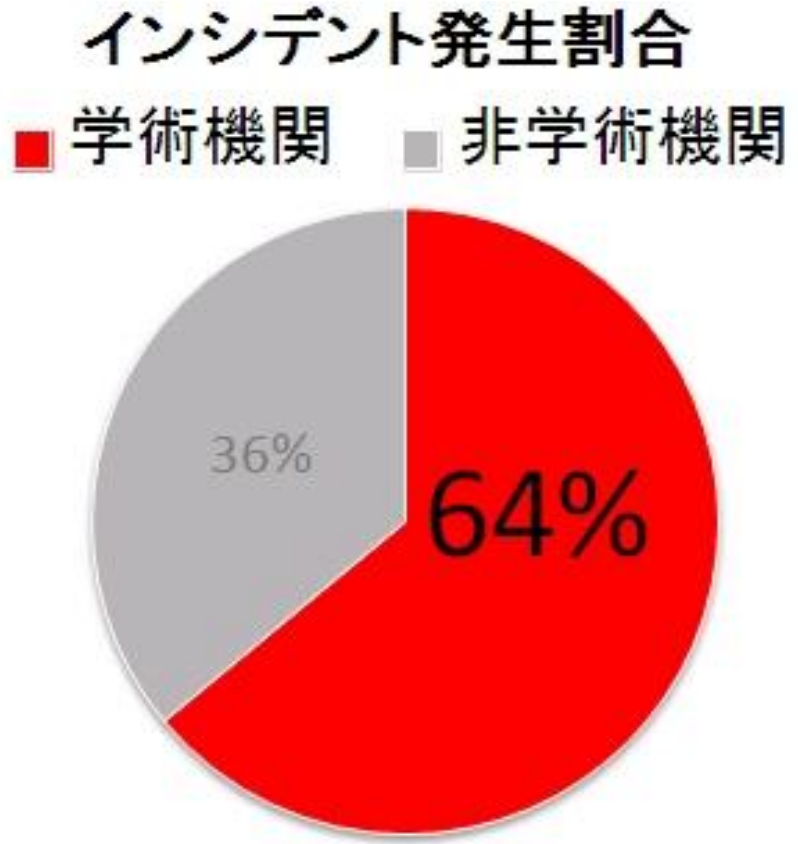


原因

- 脆弱なパスワード設定
  - ユーザ
  - 管理画面
- Firewallのアクセス制御不備
  - 設定したつもり
  - 一時的な設定
- アップデートしていないアプリケーション
  - 脆弱性情報に気づかない
  - 脆弱性情報より先に攻撃手法が公開される
  - アップデートできない環境

学術機関のインシデントの実態



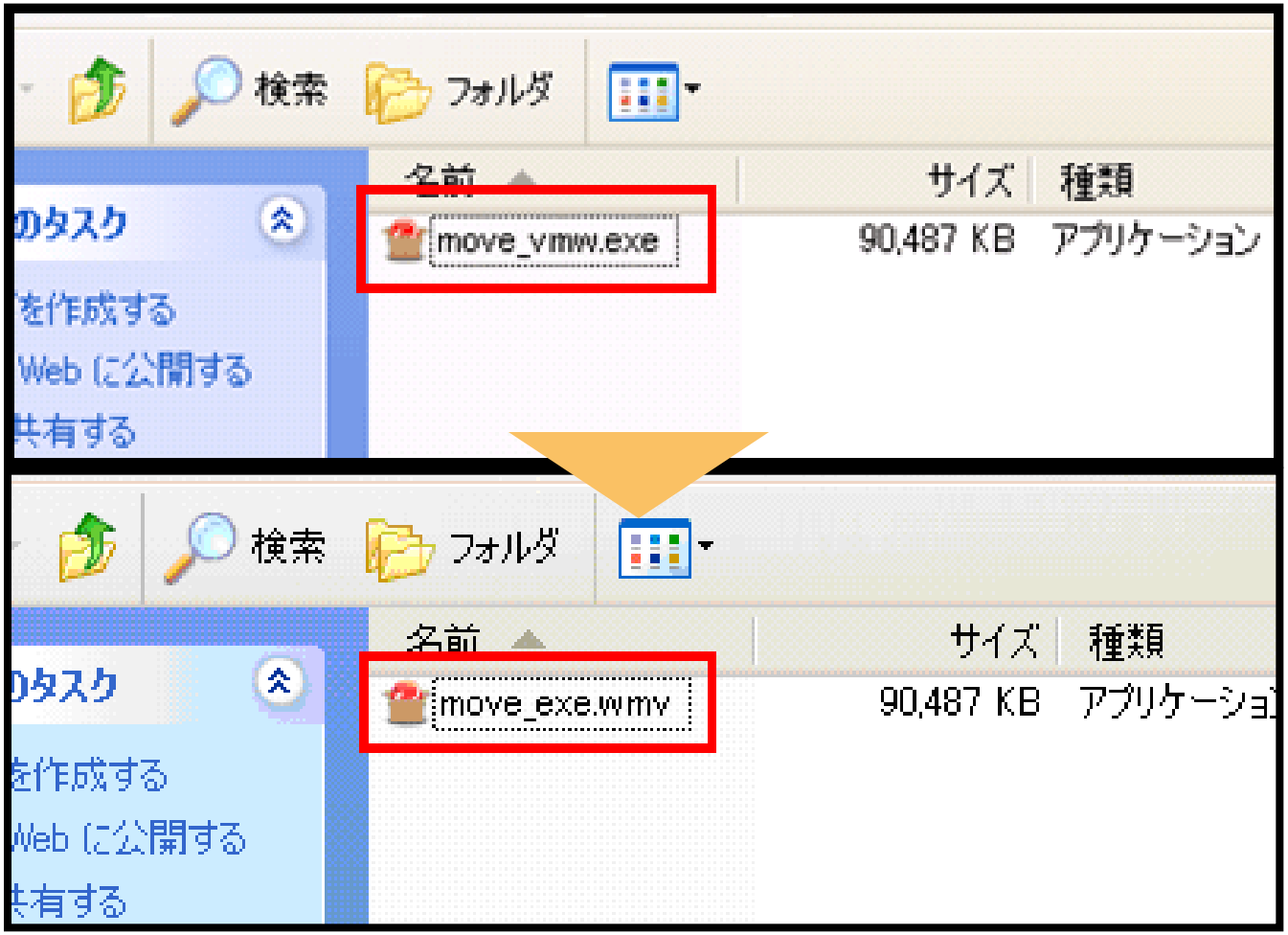


20%のユーザが64%のインシデントを占めている
特にウイルス感染事故が多い

学術機関で発生するインシデント

- ウイルス感染
  - ウイルス対策ソフトが未導入
  - ウイルス対策ソフトをアップデートしていない
  - 不用意に添付ファイルを開く
- P2Pファイル交換ソフト
  - 著作権侵害意識のないユーザ
  - 外国人留学生
- 不用意なサーバ公開
  - XAMPPの使用　→　開発用アプリ
  - アップデートしていない

ウィルス感染手口　ファイル名偽装



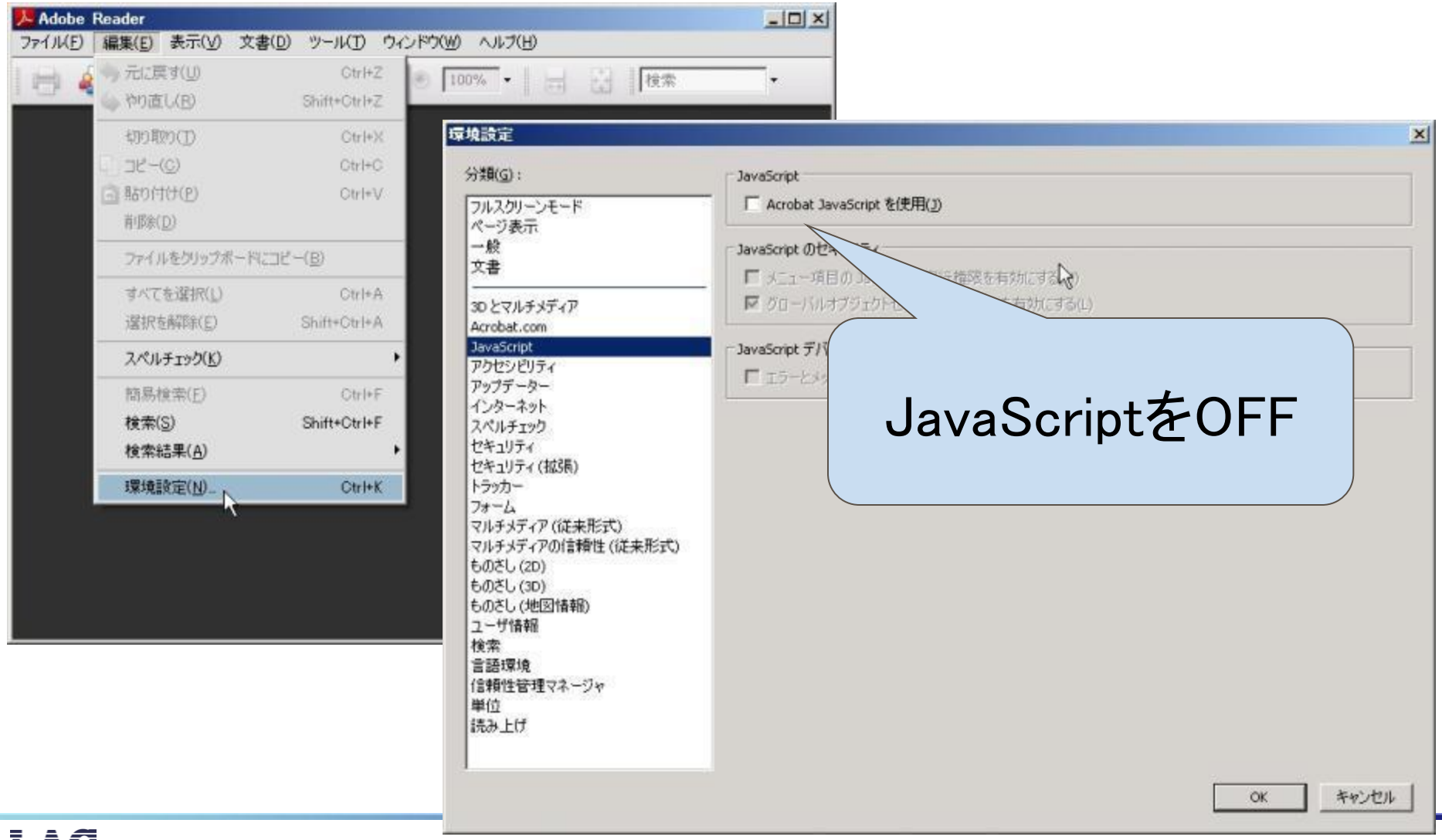
http://www.atmarkit.co.jp/fsecurity/rensai/tipstoday08/tips01.html より

ファイル名の向きを操作することが可能（RLO）

対策

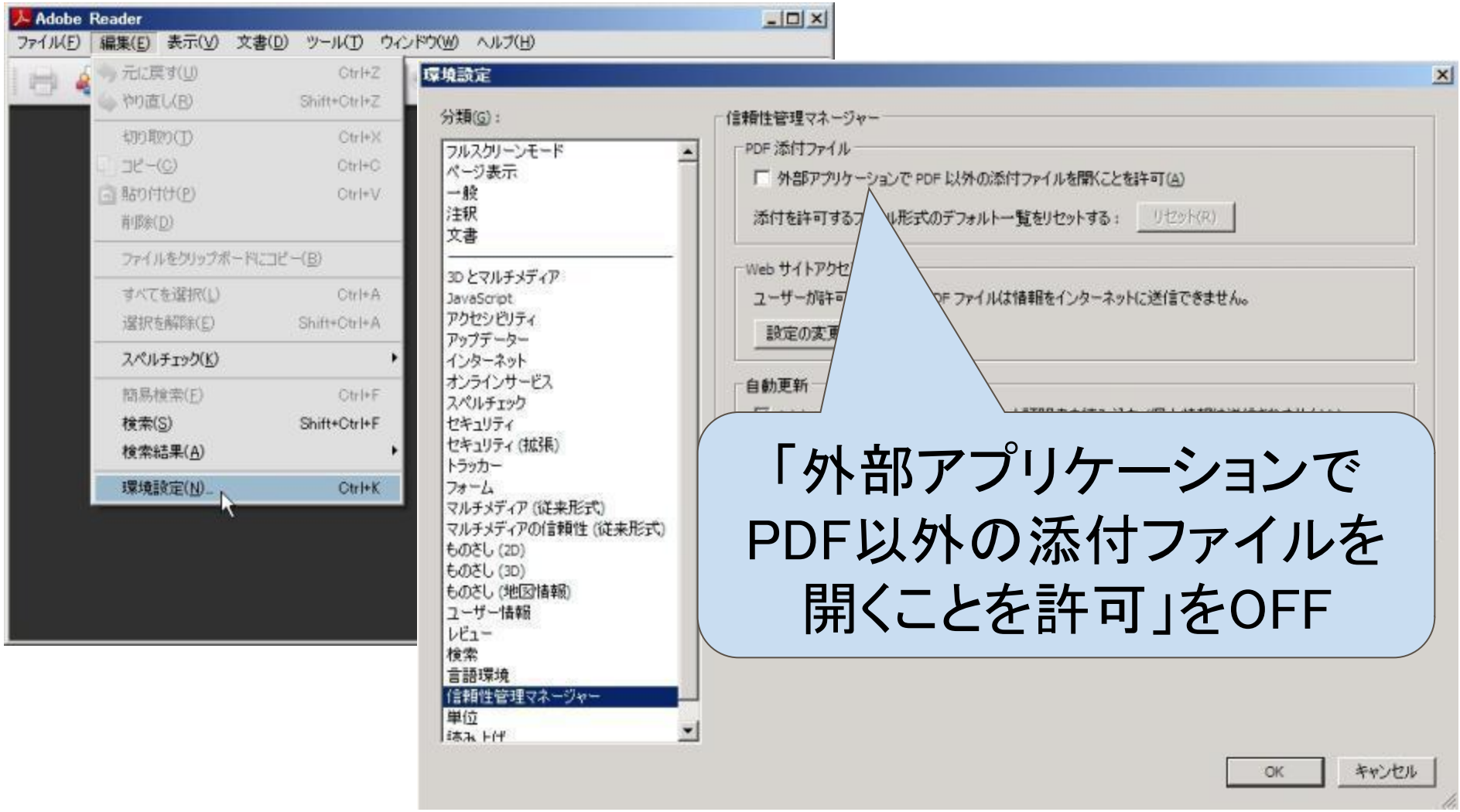
共通対策：Adobe Reader設定

Acrobat JavaScriptを無効化



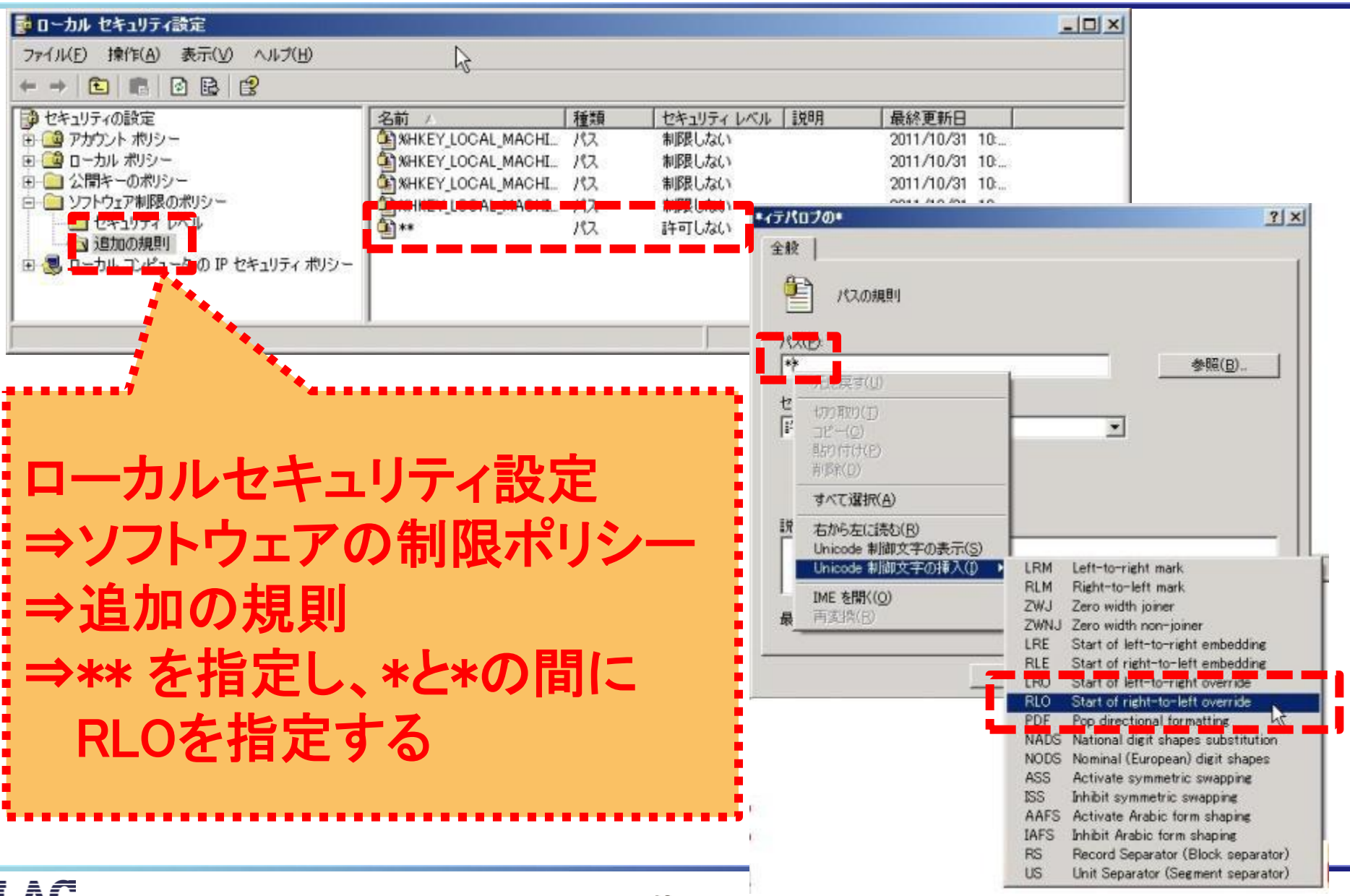
共通対策：Adobe Reader設定

外部アプリケーションの起動をさせない



「外部アプリケーションで
PDF以外の添付ファイルを
開くことを許可」をOFF

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

まとめ

クラウドも従来のシステム管理の基本が重要

基本的なウイルス対策を実施
ウイルスが仕込まれると内部からやられる

外国人留学生のオリエンテーションを手厚く

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