資料２－５

セキュリティ脅威の現状と対策の課題

～2006年　CSL・JSOCレポートから～

LAC
Little eArth Corporation

2007年1月26日

（株）ラック

目次

- セキュリティの脅威の現状
- 今後とりうる対策と課題

セキュリティの脅威の現状

ネットワークセキュリティ上の脅威(1)

脅威が様々な形で存在する。

- ✔ 不正アクセス
- ✔ 情報漏えい
- ✔ 踏み台
- ✔ 盗聴
- ✔ SPAM(迷惑メール)
- ✔ P2P(ファイル共有ソフトウェア)

ネットワークセキュリティ上の脅威(2)

ウイルスやボットはネットワークの●割！？

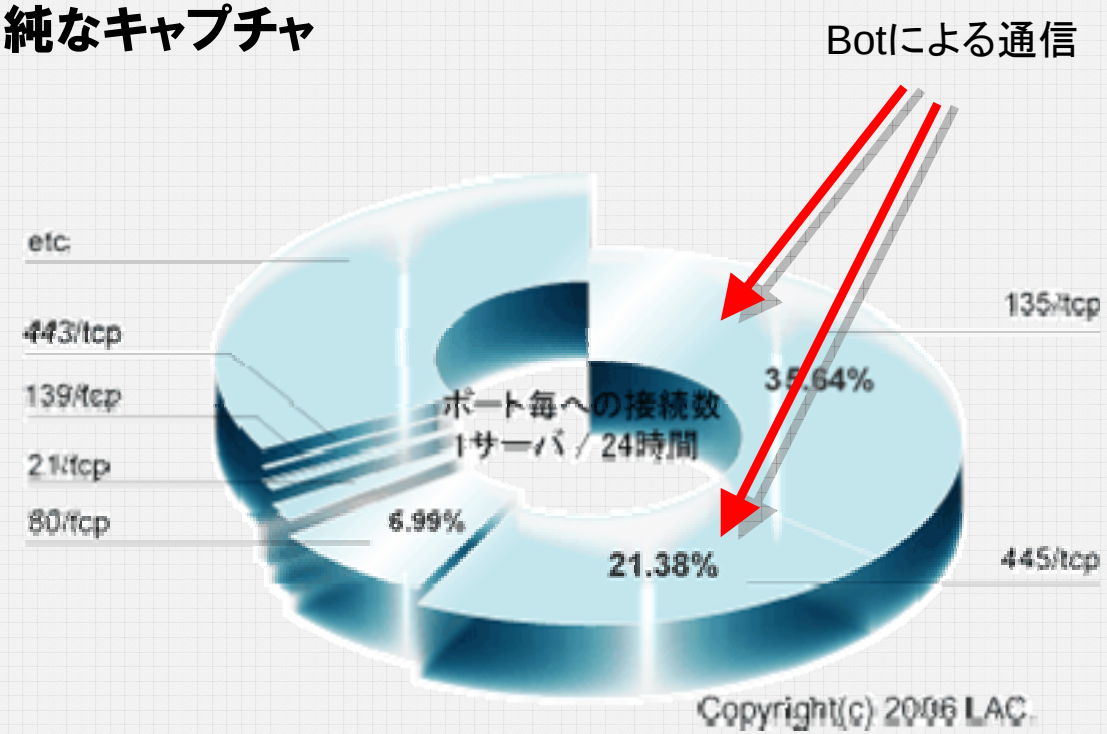
- ✔ 過剰通信
- ✔ ウイルス/ワーム
- ✔ ボット
- ✔ スパイウェア 
- ✔ Denial of Service（DoS）
- ✔ 詐欺・デマ 

- ✔ 恐喝

ネットワークには必要のない通信が多く流れています

CSLレポート（１）

- ADSL(フレッツ)
  - 神奈川県川崎市で観測
    - 観測時間　24時間
    - 観測方法　パケットモニタリング
      - Tcpdumpでの単純なキャプチャ
- 通信の概要
  - 約70%はワーム

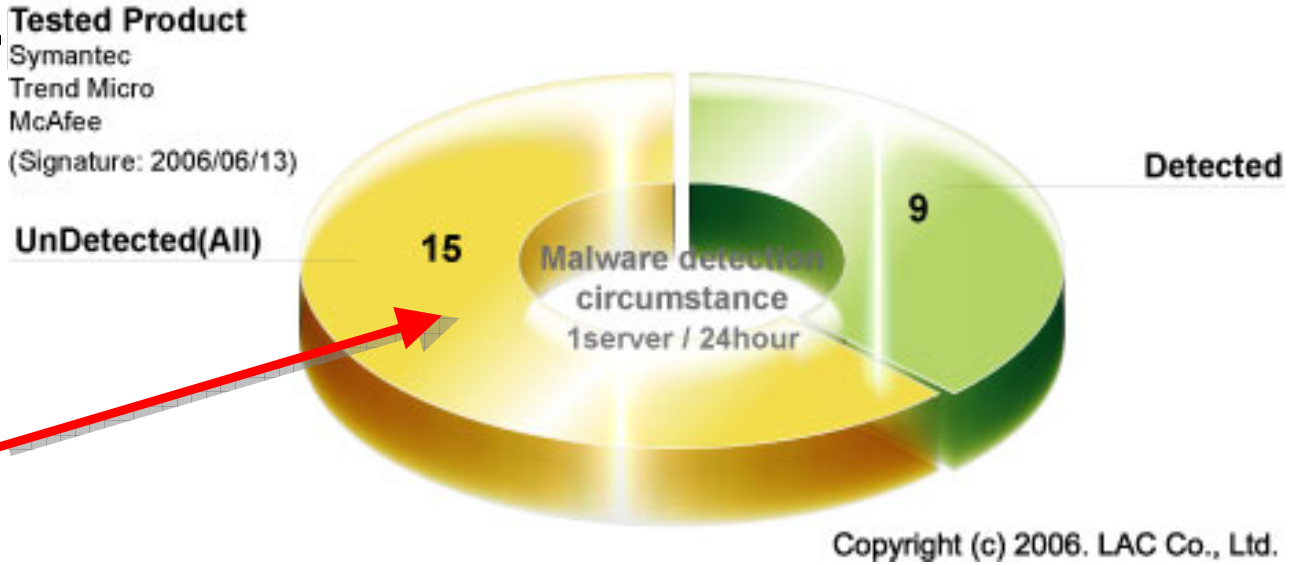


CSLレポート（１）

検出可能なマルウェアは37.5%　（6月）

- **捕獲したマルウェア（殆どBot）をウイルス対策ソフトウェアでスキャンを実施した結果、検出可能なマルウェアは全体の37.5%**
  - **捕獲したマルウェアの定義**
    - **NepenthesのShellcode Signatureに適合したバイナリを捕獲**

実際には、Virustotal.comも利用してます。
http://www.virustotal.com/



Nepenthes : http://nepenthes.mwcollect.org/

CSLレポート（３）攻撃傾向の変化

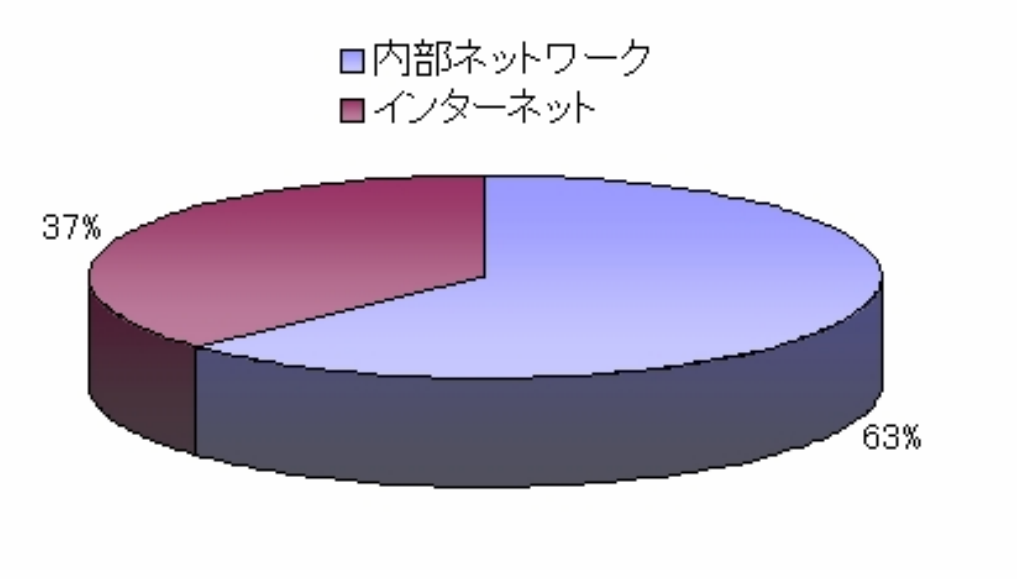
	攻撃の内容	攻撃の特徴	攻撃対象
～2005年	ウェブ改ざん 大規模に感染するワーム	目立ちやすい	・ベンダが公開しているアプリケーション ⇒脆弱性情報が広く公開される ⇒多くの企業が対応に慣れてきた
2006年	SQLインジェクション 攻撃者の命令で動くボット ⇒お金を目的としている	目立ちにくい	・企業が独自に作成したアプリケーション ・サーバの設定ミス、設定不備 ⇒脆弱性発見には診断を行う必要がある ⇒対応・対策が漏れやすい

JSOCレポートからの統計

http://www.lac.co.jp/business/sns/intelligence/report/20061030lac_report.pdf

JSOC（Japan Security Operation Center）レポート（１）

2006年上半期にJSOCで検出した、Critical以上の重要イベントの割合



分類	説明
Emergency	攻撃が成功し、侵入されたことを示します。侵入の根拠となるセッションデータもしくはパケットデータなどの侵入を証明する情報を元に判断しています。
Critical	攻撃が成功した可能性が著しく高い状況を示します。Emergencyとの違いは、決定的となる証拠が欠けている、もしくは攻撃は成功しているが侵入には至っていないなどがあります。
Warning	攻撃失敗および予備調査に成功し、サーバの設定情報など、後に攻撃を行う要素として考えられる情報が漏洩した場合などがあります。
Informational	攻撃であるかは不明ですが、悪意のあるコードは含まれていない通信。アプリケーションによる通信や日常通信である可能性が高く、情報通知レベルのものを示します。

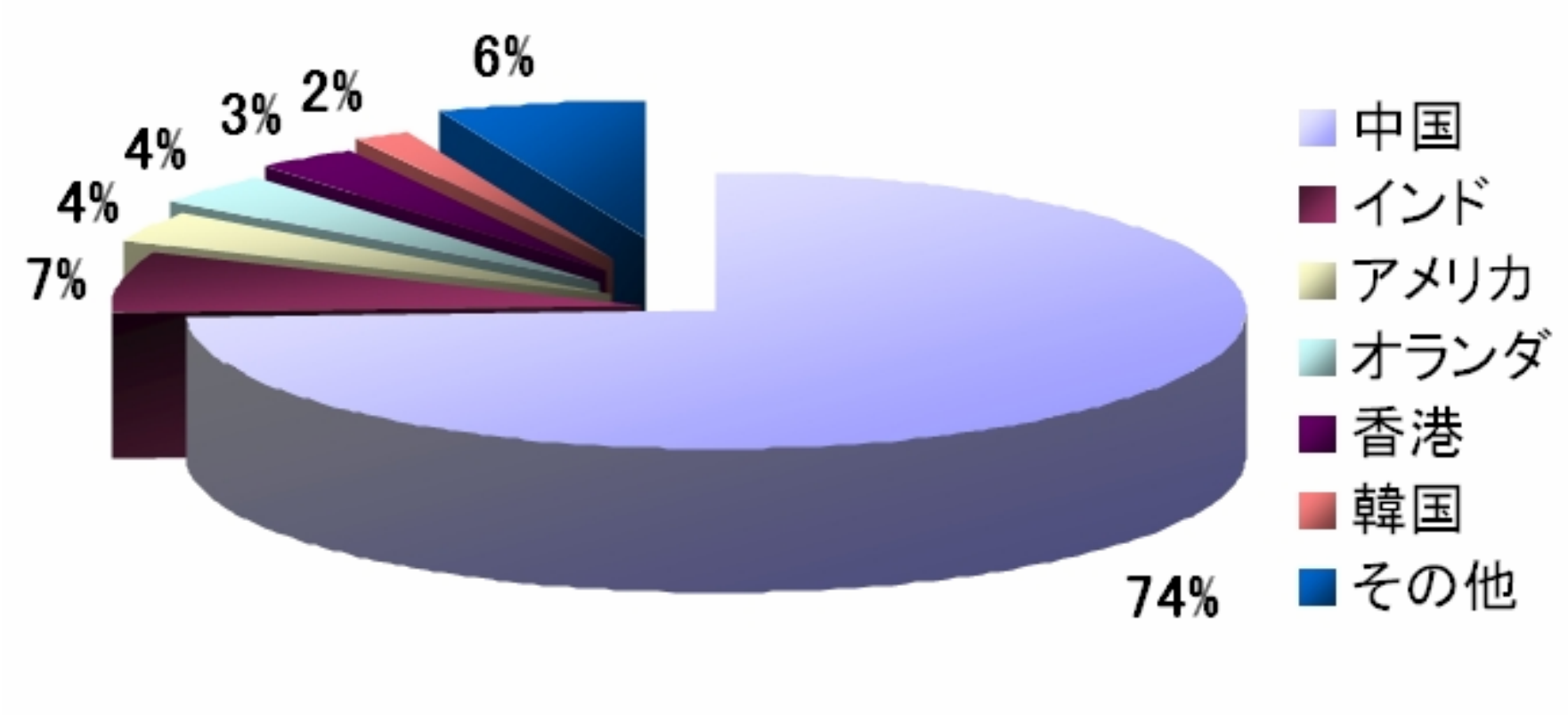
重要イベントの半数以上は内部ネットワークで発生。内部ネットワークにおいて、ボットやワームの感染通信を多く検出した。
なお、次々とワームやボットの亜種が発生するため、今後もこの傾向は続くと想定

JSOCレポートからの統計
http://www.lac.co.jp/business/sns/intelligence/report/20061030lac_report.pdf

JSOCレポート（２）SQLインジェクション攻撃

2006年1月1日～2006年6月30日

攻撃元ホスト（発信元IP）の分析をすると…



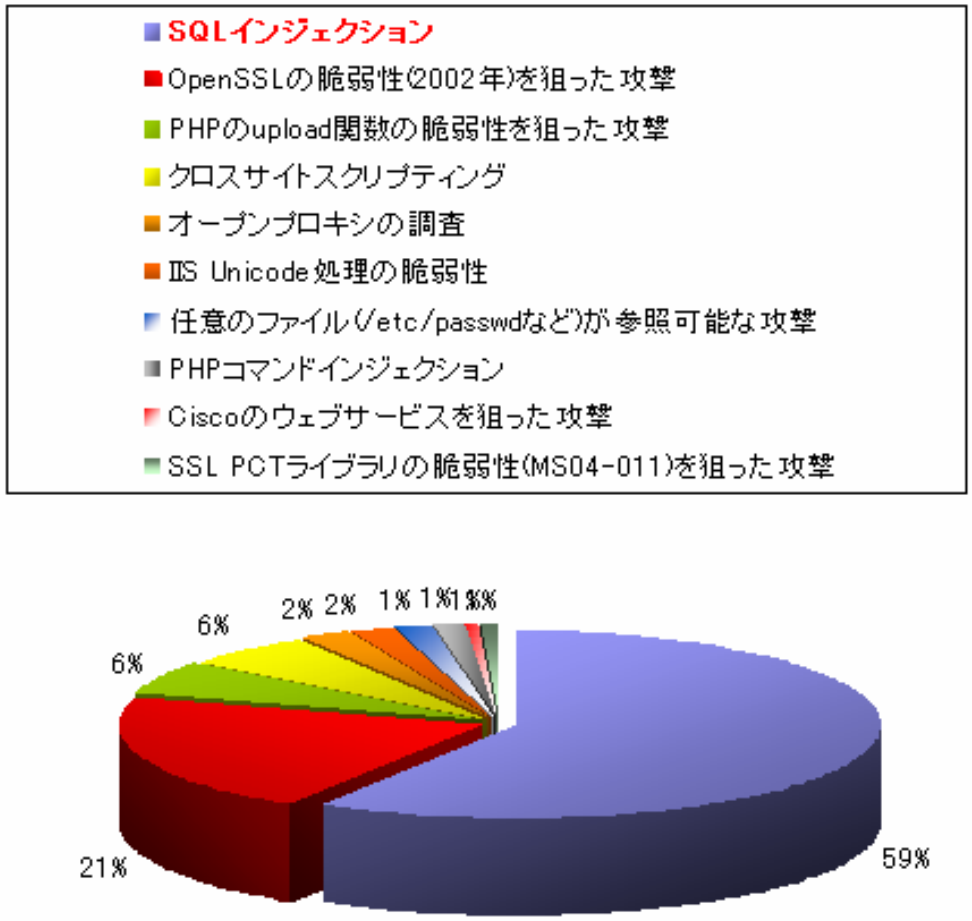
JSOCレポートからの統計

http://www.lac.co.jp/business/sns/intelligence/report/20061030lac_report.pdf

JSOCレポート（３）Webサーバへの攻撃傾向

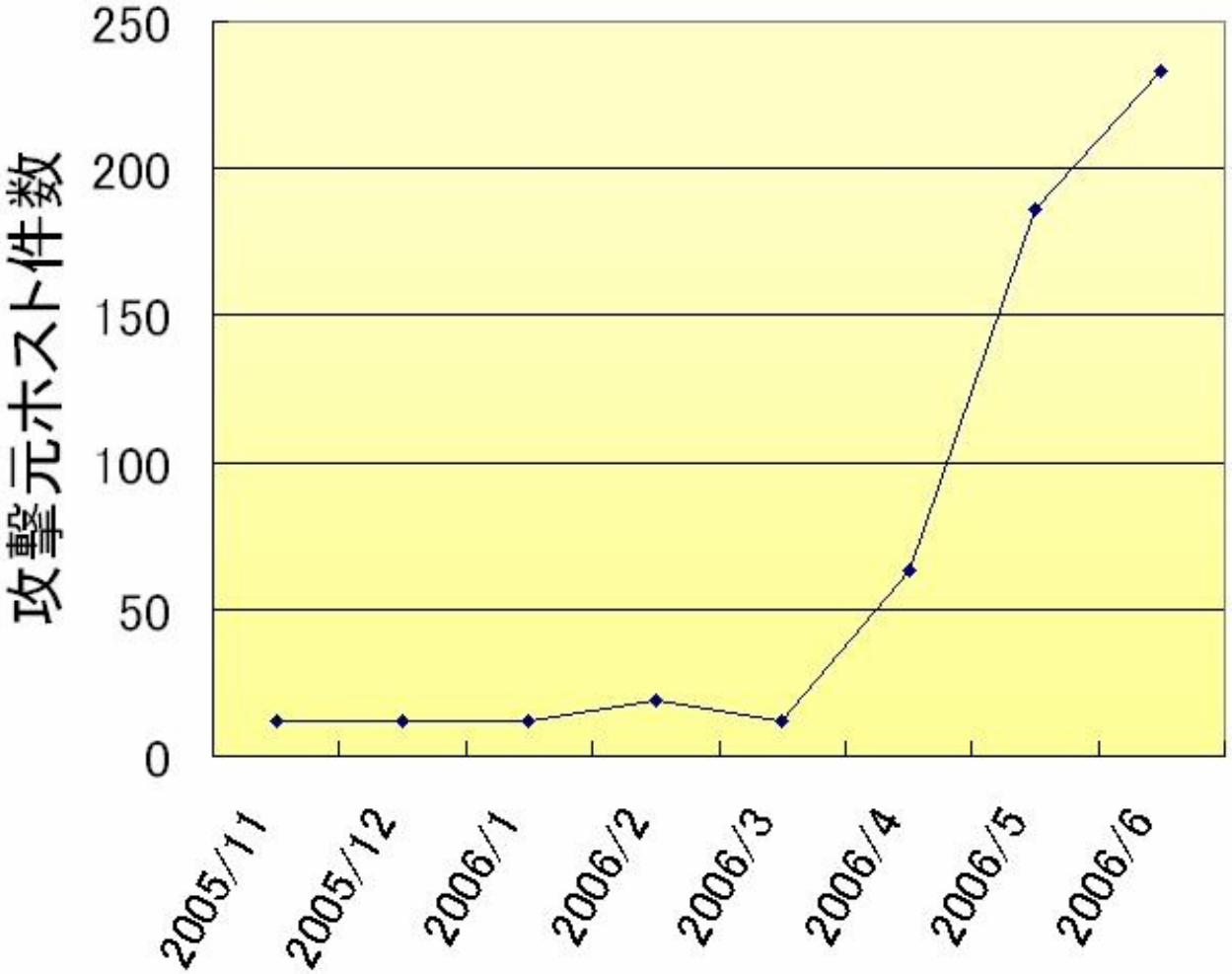
JSOCレポートからの統計

http://www.lac.co.jp/business/sns/intelligence/report/20061030lac_report.pdf



まだまだ対策が不十分のサイトがたくさんある…

JSOCレポート（４）FTPサーバーへの攻撃傾向



原因として考えられるものは・・

・ボットや著作権侵害の可能性のある不正なファイル交換サーバ

・フィッシングサイトを構築するための脆弱なサーバ

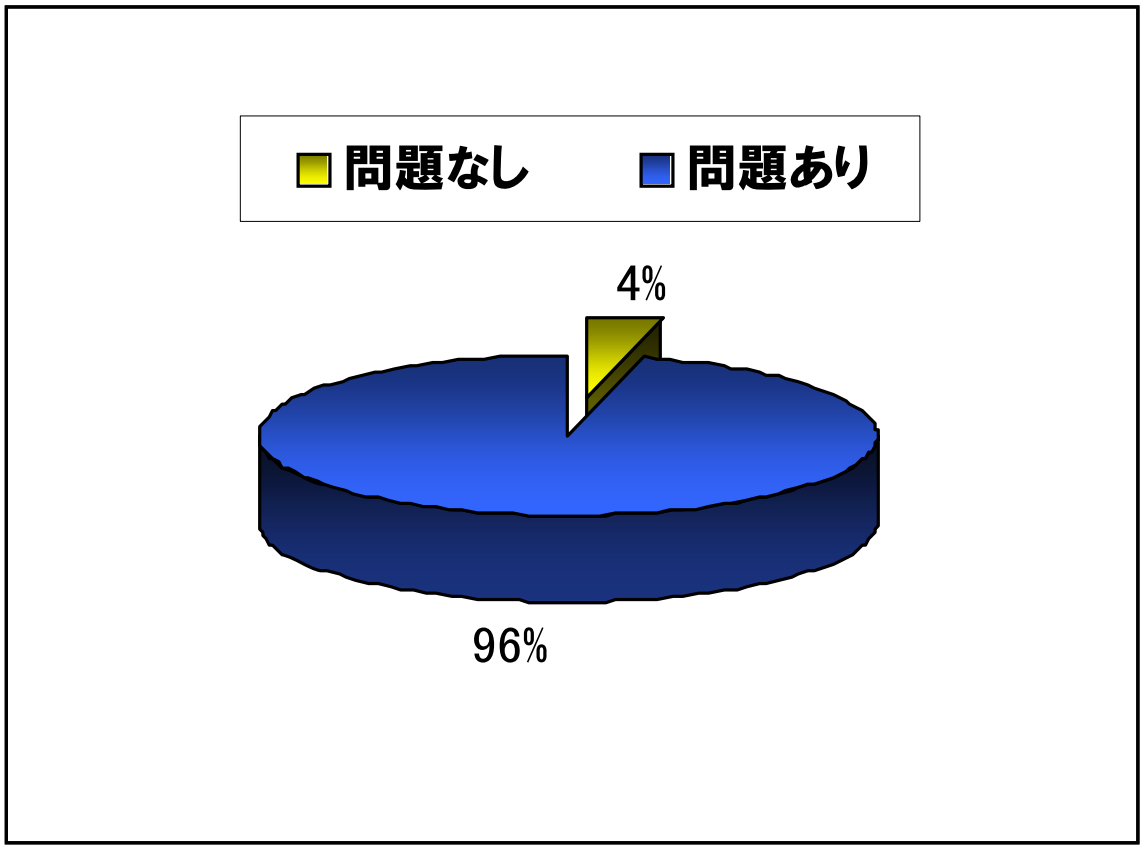
・FTPサービスで判別した脆弱なユーザを悪用し、SSHやTelnetサービスへ侵入

JSOCレポートからの統計

http://www.lac.co.jp/business/sns/intelligence/report/20061030lac_report.pdf

弊社の検査結果統計（１）Webサイトの脆弱性）

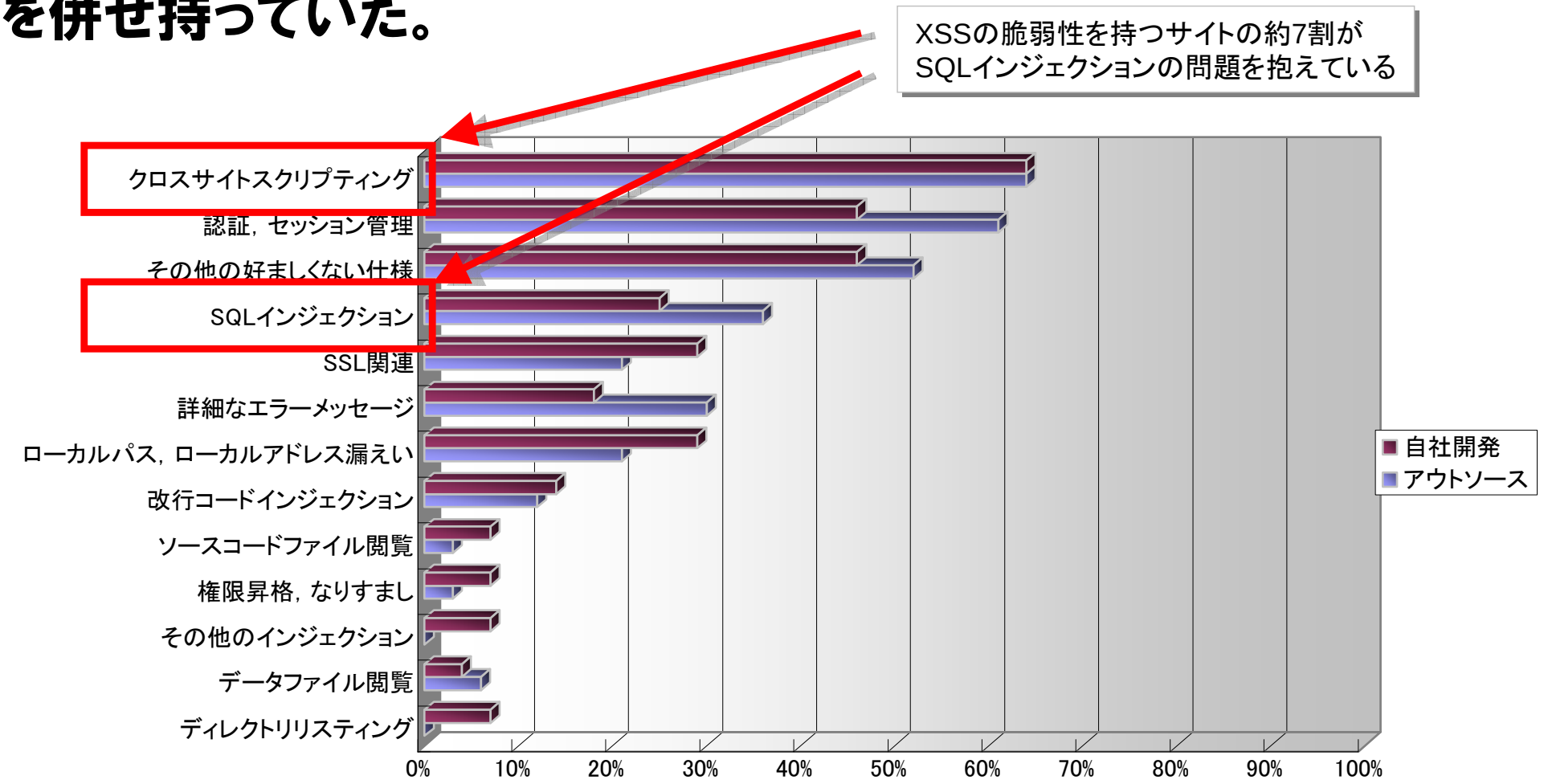
- 2006年1月～6月で、
  - 弊社脆弱性診断サービスの75サイトからのサンプリング統計結果



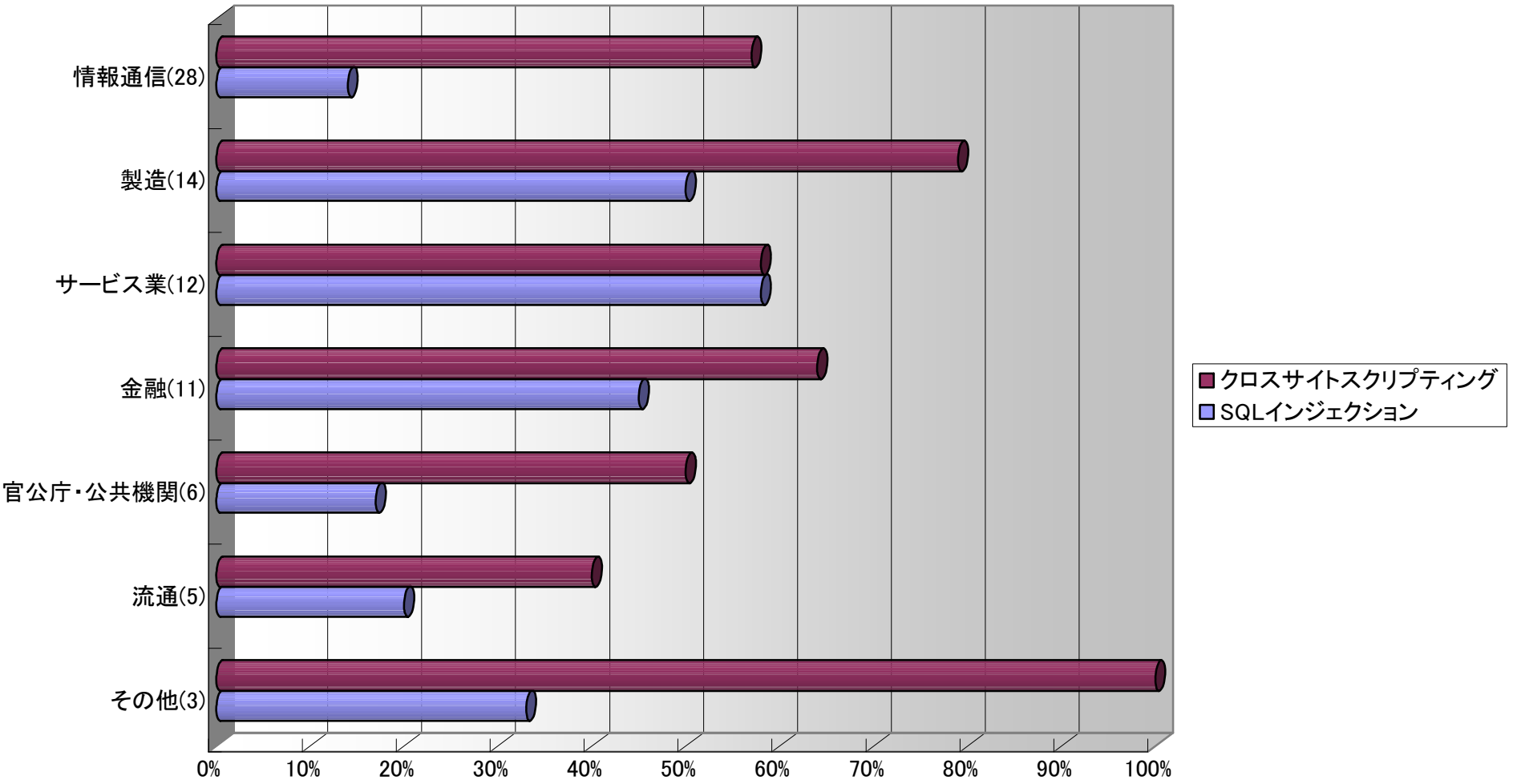
- 96％のサイトがWebアプリケーションに問題を抱えている。

弊社の検査結果統計（２）脆弱性診断の結果

クロスサイトスクリプテイングの脆弱性が存在する
アプリケーションのうち約７０％がSQLインジェクションの脆弱性
を併せ持っていた。



弊社の検査結果統計（業種別）



不正アクセスのインフラ（ボットネット）

ハニーポットによる検体収集によるボットネットの状況

JPCERT/CCのレポートから

	既知		未知		合計
	数	割合	数	割合	
検体数	35,741	90.30%	3,850	9.70%	39,591
種類	1,014	23.40%	3,324	76.60%	4,338

http://www.jpcert.or.jp/research/2006/Botnet_summary_0720.pdf

ボットネット対策

- 昨年１２月に　サイバークリーンセンターが発足
  - https://www.ccc.go.jp/

  経済産業省・総務省の連携プロジェクト
  （IPA,JPCERT/CC,T-ISAC　Japanによる相互連携
  https://www.ccc.go.jp/ccc/index.html）

- ボットネットに関する情報公開、ボット駆除ソフトの無償提供

問題の背景には・・・

なにが問題なのか？

- システムの欠陥（OS、アプリケーション）
- セキュリテ対策を実施する組織体制や制度の疲弊
- 監視体制の不備
- 従業員のセキュリティ意識の欠如
- 管理者側の認識不足　　etc

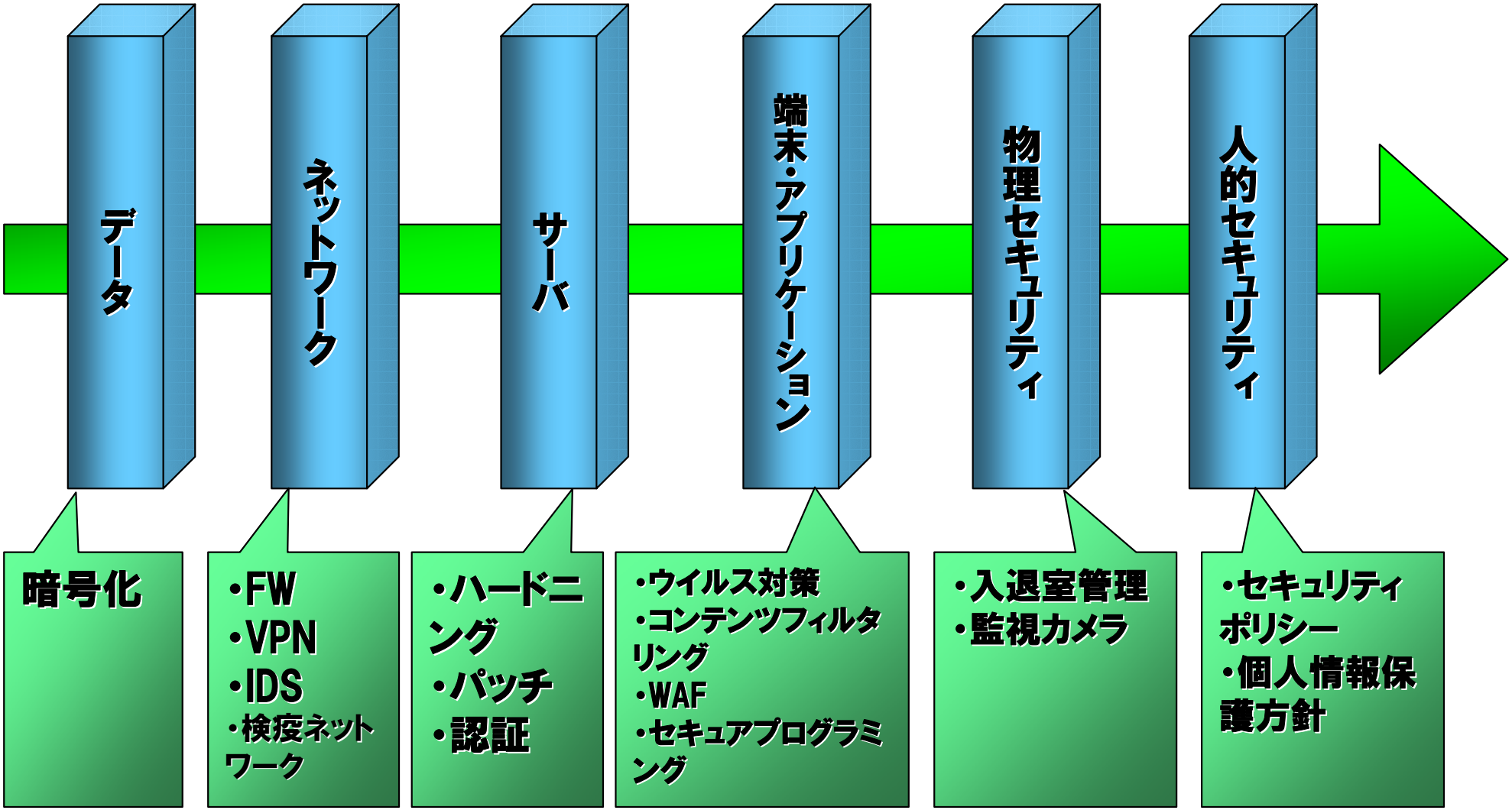
金銭目的化しつつある

今後とりうる対策と課題

多層防御とセキュリティの運用

- 多層防御 (Defense in Depth)

端末側とネットワーク側で相互連携した防御が必要になってくる。



可用性の維持(IT障害含む)

次世代IP端末を利用する場合、
サービス環境をいかに崩さず、安全に運用するか？


攻撃を止めなければサービスも止まる


攻撃を止めてもサービスは止まる

従来の妥協点


攻撃を受けてもサービスを止めない
端末や＆ネットワークの検討

現在の技術の限界点

侵入検知システムや防御システムを検討する場合

不正アクセスやDos/DDos・
ウィルス・ワーム等の検知の検知条件として・・・

- ✔ **定義可能な通信や現象など**
- ✔ **暗号化されていないもの**
- ✔ **実現可能な技術であること**

単一システムでの防御だけでの対処は難しいのが現状

対策としては（例）

道路がつまったら迂回路を作るイメージ？

セキュリティ環境を整えることは、環境維持に似ている。
利便性と安全性のバランスをとりつつ、安全サイドに
利用者をナビゲートするシステムと仕組みの検討

脆弱箇所のハンドリングを踏まえた堅牢なシステムの検討

利用者保護につながる

最低限の「見える化」を計ることも必要

1. 何が起こっているのか判る仕組み。
   例えば・・ 端末が利用者に危険性や、攻撃有無などを知らせる。
2. セキュリティ対策機器、端末、ネットワークなどの異なるレイヤが相互に連携できる仕組み。
   例えば・・ 端末がセキュリティ機能を柔軟に、且つ自動的に強化したり、機能を追加したりできる。
3. セキュリティ機能を選択できる端末やセキュリティサービス選択ができる端末の仕組み等の検討。
4. 利用者やサービス提供者納得できる課金方式の検討

安全・安心な次世代IP端末

ご清聴有り難うございました。