# 情報セキュリティ実践セミナ

株式会社アークン
代表取締役　渡部　章

## はじめに

- セキュリティは諸刃の剣
  - ブラックハット　vs. ホワイトハット
- セキュリティ技術は広くて深い
  - スキルマップ
- あなたは何を目指す？
  - ユーザ／サービス提供者／製品開発者

## アジェンダ

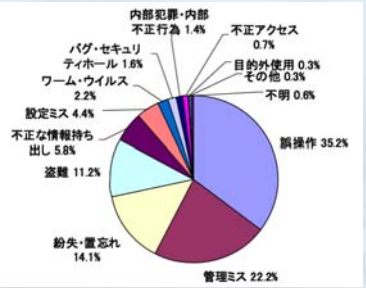
- 情報セキュリティの脅威の動向
  - 2009年度、情報漏えい事件
  - 2009年度、セキュリティ10大ニュース、セキュリティ10大脅威
- 情報セキュリティ対策
  - 情報セキュリティのためのスキルマップ
- 人的セキュリティ対策
  - リスク分析　情報資産の分類と管理手法
  - 事業継続計画（BCP）
  - IT管理者の管理
- 技術的セキュリティ対策
  - 不正アクセス対策（ファイアウォール）
  - ウイルス対策の実際
  - スパム対策の実際
  - フィッシング対策の実際
  - バックアップ体制

## 2009年度、情報漏えい事件

- 2009-01-26 神奈川県、中退／生活保護家庭情報11万人分流出、IBMが委託違反
- 2009-02-06 兵庫県加古川市、職員が納税者の情報を自宅PCよりメール誤送信
- 2009-02-20 会社サーバーに社員が不正アクセス、顧客情報18万人分を流出
- 2009-02-25 原子力機構のサーバに不正アクセス、研究者ら281人分漏えい
- 2009-03-31 三菱UFJ証券、元部長代理が顧客の個人情報4万9千人分を売却
- 2009-04-17 兵庫県明石市、中学教師がUSBメモリを紛失、466人の成績漏れる
- 2009-05-11 福島県郡山の2中学校、生徒ら1338人分の個人情報をWinnyで流出
- 2009-05-18 兵庫県の外郭団体、“婚活”男性の情報732人分を流出
- 2009-05-28 福岡県大牟田市消防署、個人情報含む文書2910件Winnyで流出
- 2009-06-15「ファミ通ドットコム」で顧客情報約7700人分が外部から閲覧可能に
- 2009-06-22 着メロ会社、会員メルアド30万人分を出会い系会社に売却
- 2009-07-22 りそな銀行、顧客情報を誤廃棄、33万件紛失
- 2009-07-23 アリコジャパン、委託先PCから1万8千件流出、カード不正使用2700件
- 2009-07-29 住友生命保険、従業員約1600人の個人情報がWinnyで流出
- 2009-08-08 アミューズ、顧客カード情報3万4千件が不正アクセスで流出
- 2009-08-28 大阪府、SDカード紛失　重度障害者1万1千人分の情報流出
- 2009-09-05 三菱商事系通販サイト、不正アクセスでカード情報5万件流出
- 2009-10-01 都立高校、USBメモリ紛失で1343人分を流出

## 情報セキュリティ・インシデントの原因

出典：JNSA 2008年情報セキュリティインシデントに関する調査報告書




技術的な情報漏えいは全体の4.5%

- 不正アクセス
- バグ・セキュリティホール
- ワーム・ウイルス

技術対策と共にポリシーの策定と運用が重要

## 情報セキュリティ脅威の動向

- JNSA 2009 セキュリティ10大ニュース
  - http://www.jnsa.org/result/2009/news10.html
  - ネットワークリスクマネジメント協会（NRA）から引継ぎ
- IPA 情報セキュリティ白書2009　10大脅威
  - http://www.ipa.go.jp/security/vuln/10threats2009.html

## JNSA 2009セキュリティ10大ニュース

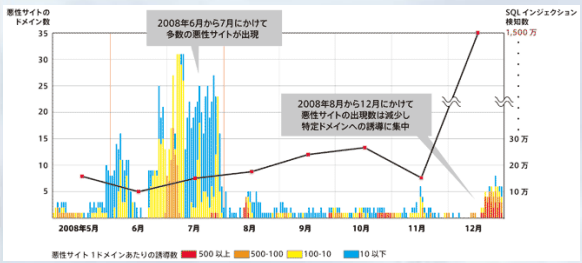
【第1位】 3月29日 クラウド台頭、セキュリティは雲の中
【第2位】 5月20日 長引く不況でセキュリティ投資低迷
【第3位】 10月 8日 台風18号、通勤客をもてあそぶ
【第4位】 10月 8日 Winny開発者に高裁で逆転無罪判決
【第5位】 3月30日 パンデミックが明らかにしたBCPの不備
BCP＝Business Continuity Plan（事業継続計画）
【第6位】 10月23日 IPv4アドレス枯渇、いよいよカウントダウンか！？
【第7位】 9月11日 政権交代で後退する？セキュリティ政策
【第8位】 7月23日 アリコジャパン、犯人特定に苦戦
【第9位】 7月29日 P2Pによる意図的な情報流出でついに逮捕者
【第10位】 5月19日 Gumblerウイルスによる改ざん被害

## IPA 情報セキュリティ白書2009 10大脅威

| | 2008年 | 2007年 | 2006年 |
|---|---|---|---|
| 【第1位】 | Kaminsky DNSキャッシュポイズニングの脅威 | なし | なし |
| 【第2位】 | Webサイトを狙った攻撃の広まり | 3位 | 8位 |
| 【第3位】 | 巧妙化する標的型攻撃 | 4位 | 1位 |
| 【第4位】 | 検知されにくいボット、潜在化するウイルス | 7位 | 2位 |
| 【第5位】 | 恒常化する情報漏洩 | 2位 | 3位 |
| 【第6位】 | WEPの衰退 | なし | なし |
| 【第7位】 | 高まる「誘導型」攻撃の脅威 | 1位 | なし |
| 【第8位】 | 信用できなくなった正規サイト | 5位 | なし |
| 【第9位】 | 検索エンジンからマルウェア配信サイトに誘導 | 8位 | なし |
| 【第10位】 | 減らないスパムメール | 11位 | 6位 |

## 増加するSQLインジェクション攻撃

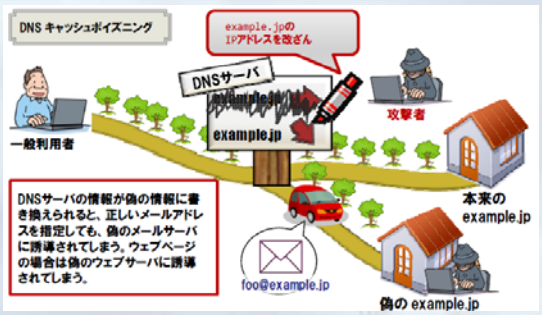
2008年通期のSQLインジェクション攻撃の検知状況




前年比61倍増に！

出典：ラック

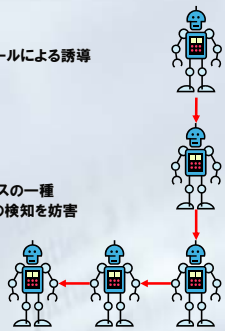
## DNS キャッシュ ポイズニング



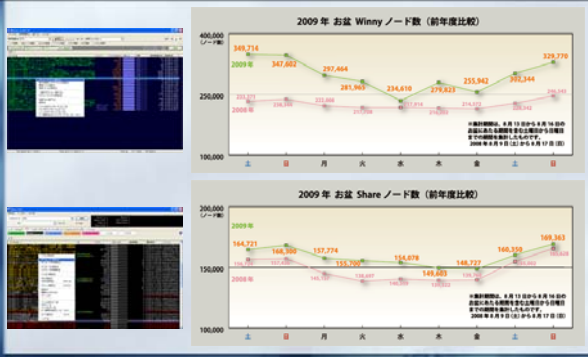

出典：情報セキュリティ白書2009

## ウイルスの多様化

- **感染**
  - Webサイトからのウイルス侵入の増加
    - SQLインジェクション、SEOポイズニング、メールによる誘導
  - USBメモリ感染型ウイルスの増加
  - ソフトの脆弱性を狙ったウイルスの増加
    - PDF、Word、画像・動画ファイルによる感染
- **潜伏**
  - ボットウイルスの増加
    - 作者の命令を伝達し合い不正を働くウイルスの一種
    - 自動更新で姿形を変化させワクチンソフトの検知を妨害
- **発病**
  - 無差別感染から標的型へ
    - ソーシャル・エンジニアリングの手口
  - 愉快犯から情報・金銭目的へ
  - 亜種多発、複合型の症状（Gumbler）



## ファイル交換ソフト（Winnyなど）の危険




出典：ネットエージェント

## 情報セキュリティ対策： 支える柱

- **人的対策**
  - セキュリティポリシーの策定、理解と履行
  - 情報モラル、ネチケット
  - 人権問題
- **技術的対策**
  - インターネットの入り口で（ゲートウェイ）
  - ネットワーク上で
  - サーバーで
  - PC上で（クライアント）
- **物理的対策**
- **セキュリティの基本**
  - セキュリティ3原則 :可用性、完全性、機密性
  - セキュリティサイクル（PDAC） :計画、実施、監視、改善
  - 実施の3原則 :予防(抑止・軽減)、検出、回復

**バランスが重要**

## 情報セキュリティ対策： バランス

- **セキュリティと利便性**
  - セキュリティと利便性はトレードオフの関係にある
- **権利と義務**
  - 社員の権利
    - 管理された安全なネットワーク環境を利用できる権利
    - ワクチンソフトなどセキュリティ技術を利用できる権利
  - 社員の義務
    - 社内システムとデータ、セキュリティ技術の適正な利用
    - ルール違反による事故は、個人の責任であり、処分の対象
      - 持ち込みPCによるウィルス感染
      - 自宅PCで会社情報が漏えい
- **費用対効果**
  - リスク分析による対策の絞込み
    - 頻度の高さと被害の大きさ

**リスク分析を実施しよう！**

## 人的セキュリティ： リスク分析

- **情報資産の洗出しと分類**
  - 組織の情報資産の適切な保護を維持するため、機密性、完全性、可用性等の観点から情報資産を重要度により分類する。
  - **機密性**:漏えいや不正アクセスを受けると困る情報やシステム
  - **完全性**:改ざんや間違いがおこると困る情報やシステム
  - **可用性**:情報の紛失・破損やシステム停止で困る情報

| | | 機密性 | 完全性 | 可用性 | 重要度 |
|---|---|---|---|---|---|
| 社内データ | 営業データ | 1 | 1 | 1 | 3 |
| | 経理データ | 2 | 5 | 5 | 12 |
| | 技術データ | 4 | 3 | 2 | 9 |
| 顧客データ | 個人情報 | 5 | 4 | 4 | 13 |
| 外部向けデータ | Webデータ | 3 | 2 | 3 | 8 |

## 人的セキュリティ： リスク分析

- **情報資産の管理**
  - 情報資産の管理方法、管理責任を規定し、重要度に応じた情報セキュリティ対策を行う。

| データ | 重要度 | 管理方法 | 責任者 |
|---|---|---|---|
| 個人情報 | 13 | | |
| 経理データ | 12 | | |
| 技術データ | 9 | | |
| Webデータ | 8 | | |
| 営業情報 | 3 | | |

| システム | 重要度 | 管理方法 | 責任者 |
|---|---|---|---|
| 個人情報格納データベース | | | |
| Webサーバ | | | |
| Mailサーバ | | | |
| ファイルサーバ | | | |
| クライアント | | | |

## 人的セキュリティ： リスク分析

- **リスク分析・評価**
  - 情報資産の重要性、情報資産に対する脅威、現状における対策の脆弱性からリスク(潜在する損害の大きさ)を評価し、その評価に基づく効果的な情報セキュリティ対策を行う。

| | 重要度 | 脅威 | リスク | | 評価 | 情報セキュリティ対策 |
|---|---|---|---|---|---|---|
| | | | 頻度 | 大きさ | | |
| 個人情報 | 13 | | | | | |
| 経理データ | 12 | | | | | |
| 技術データ | 9 | | | | | |
| Webデータ | 8 | | | | | |
| 営業情報 | 3 | | | | | |

## 事業継続計画(BCP)： 発見

- **外部からの連絡**
- **目視による発見**
- **ログの確認やセキュリティ対策機器による発見**

| No | 事故事例 | 発覚のきっかけ |
|---|---|---|
| 1 | Web での ID パスワードを不正利用され、情報を他のサイトに掲示された。 | ・自己申告／内部発見<br>・外部からの指摘<br>（風評を含む） |
| 2 | Web でのぜい弱性を悪用し不正アクセスされ、非公開情報を搾取された。 | |
| 3 | Web アプリケーションのぜい弱性を悪用され、データベースサーバの非公開情報を搾取された。 | |
| 4 | Web アプリケーションのぜい弱性を悪用され、Web サーバにウイルスを埋め込まれた。 | |

出典：IPA

## 事業継続計画(BCP): 報告

- 障害が明らかな場合は監督官庁に連絡
- 事実確認と情報の一元管理が重要
- 口頭ではなく情報共有シートを利用し正確な報告を行う

監督官庁への報告に含むべき項目(例)
- 事業者名
- 発覚日
- 事故原因
- 漏えいした情報の内容(情報漏えいがある場合)
- 事故の被害内容(二次被害の影響含む)
- 警察届出有無
- 個人への連絡
- 再発防止策

出典: IPA

## 事業継続計画(BCP): 初動対応

- 事実関係の掌握

| 事実関係を5W1Hで整理する | |
|---|---|
| (1) 不正アクセスした当事者は誰か? | a)誰の情報か? |
| (2) 何(物)を不正アクセスされたのか? | b)何の情報か? |
| (3) 不正アクセスされた情報は何か? | c)いつ頃の情報か? |
| (4) いつ不正アクセスが行われたのか? | d)情報の量(件数)はどのくらいか? |
| (5) どこで不正アクセスが行われたのか? | e)どのような形で保存されていたか? |
| (6) なぜ不正アクセスが発生したのか? | (暗号化/平文、HDD 保護、パスワード保護など) |
| (7) 不正アクセスが発覚した理由は何なのか? | |

- 応急処置

| No | 応急処置例 | 留意点 |
|---|---|---|
| 1 | 不正アクセスを受けた機器(サイト)のネットワークからの切り離し | ・不正アクセスされた原因、経路を特定せずに、代替サイトを立ち上げると、再び不正アクセスされる可能性が高い |
| 2 | 不正アクセスを受けた機器(サイト)の停止 | |
| 3 | 代替サイトの立ち上げ | |

出典: IPA

## 事業継続計画(BCP): 調査

- 証拠保全の措置
  - 機器に残された記録は重要な証拠
- 調査
  - 不正アクセス方法
  - アクセスされた情報
  - 予想される二次被害の確認

| 被害の重要度を判定する |
|---|
| (1) 漏えいした情報区分は? (個人情報/公共性の高い情報/一般情報) |
| (2) 漏えいした情報の保護策は、何を実施していたか? |
| (3) 影響はどこにあるか? (個人/公共インフラ/特定企業) |
| (4) 管理上の問題点は? |

出典: IPA

## 事業継続計画(BCP): 通知・公表等

- 個人情報にアクセスされた可能性がある場合
  - 範囲を特定し本人に通知し謝罪
- 規模が大きい場合
  - Webでの情報公開や記者発表を検討
- 警察への届出
  - 従業員の内部犯行によって情報が漏えいしてしまった場合
    - 背任、不正競争防止法違反等被疑事件
  - 外部からの侵入等によって情報が漏えいしてしまった場合
    - 不正アクセス禁止法違反被疑事件
  - 漏えい情報に関して不正な金銭等の要求を受けた場合
    - 恐喝・脅迫・強要等被疑事件
- JPCERT/コーディネーションセンターによる支援

出典: IPA

## 事業継続計画(BCP): 抑制措置と復旧

- 不正アクセスされたサーバ等の内容をバックアップ
- 再発防止措置後、サービス復旧
- アカウント再発行
- パスワード変更

| No | 二次被害防止策例 | 留意点 |
|---|---|---|
| 1 | 漏えいした情報の回収 | ・第三者からの情報回収該当情報を保持または掲載する第三者が情報回収に応じてくれない場合の対応 |
| 2 | Web サーバ設定の見直し | |
| 3 | ID パスワード、アクセス権限の見直し | |
| 4 | サーバ、Web アプリケーションのぜい弱性の除去 | |
| 5 | クレジットカード、銀行口座番号、ID パスワードが含まれていた場合、本人に通知し、カード停止、口座停止、ID 停止などを促す | |

出典: IPA

## 事業継続計画(BCP): 事後対応

- 違反や管理上のミスがあった場合必要な処分を実施
- 必要に応じて漏えい情報による被害の補償等救済処置を実施
- 各社のポリシーにあわせ、事故の再発防止策を実施

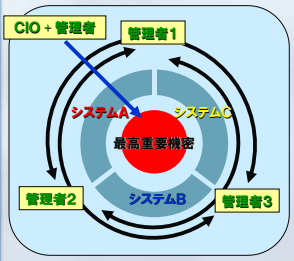
出典: IPA

## IT管理者の管理

- **体制作り**
  - 経営者の中から最高情報責任者(CIO)を任命
- **リスク分散**
  - 業務分担、パスワードの二分割、アクセス権の工夫
- **抑止効果の利用**
  - 監視機能の導入、IT担当者同士の監視
- **健康管理**
- **退職時の対応**
  - 退職決定前後の権限レベルとアカウントの管理
  - 主要パスワードの変更

## IT管理者のリスク分散

スーパーバイザー＝CIO




- **業務分担**
  - システムA
    - 正担当：管理者1
    - 副担当：管理者2
  - システムB
    - 正担当：管理者2
    - 副担当：管理者3
  - システムC
    - 正担当：管理者3
    - 副担当：管理者1
- **パスワードの分割**
  - 最高重要機密
    （権限設定、パスワードリスト等）
    - パスワード1：CIO、および、取締役
    - パスワード2：IT管理者
- **アクセス権の工夫**
  - システム　：システム管理者
  - データ　　：データ管理者

## 早期事業継続のための準備

- **障害時における行動指針の策定**
  - 職務別の行動指針（経営者、担当者、IT管理者、一般社員）
  - 連絡網（命令伝達経路、報告経路の確認）
- **監査体制の確立**
  - 定期的に実施　→　見直し
- **監視装置(サービス)の配備と運用**
  - 接続監視、ウイルス監視、IDP、WAF、帯域監視
- **バックアップ体制**
  - システム、電源、データー
- **通信の確保**
  - 無線
- **訓練・教育**
  - 障害時のシュミレーション

$$\text{稼働率} = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}}$$

MTBF = Mean Time Between Failure:平均故障間隔
= 稼動時間÷故障回数

MTTR = Mean Time To Repair:平均修復間隔
= 故障時間÷故障回数

## 情報セキュリティを支える技術：　スキルマップ

| | |
|---|---|
| 情報セキュリティマネジメント: | リスクアセスメント・リスク対応、ポリシー作成のポイント、情報セキュリティ監査 |
| インフラセキュリティ: | ネットワーク分割、アドレスとNAT、運用管理、パケットフィルタリング、ルーティング、LANスイッチ、VPN、無線LAN |
| アプリケーションセキュリティ: | アプリケーションサーバ全般、Web・メールサーバ、DNS |
| OSセキュリティ: | Windows、UNIX、セキュア OS |
| ファイアーウォール: | 役割、基本方式と特性、製品機能、導入設計、 運用・管理 |
| 侵入検知(IDS): | 機能、検知、運用、侵入防止システム、IDSの課題事項 |
| ウィルス: | 管理体制、感染後ポリシー、予防ポリシー、発病、検出方法と駆除、感染、種類 |
| セキュアプログラミング: | 人々の役割、脆弱性の拡散、開発工程と脆弱性対策、学習方法 |
| セキュリティ運用: | 基本設計、システム設計と運用、異常時の対応 |
| セキュリティプロトコル: | アプリケーション、トランスポート、ネットワーク、データリンク |
| 認証: | 認証、PKI(Public Key Infrastructure)、電子署名 |
| 暗号: | 開鍵・共通鍵暗号、ハッシュ関数、乱数、鍵管理、ゼロ知識証明、解読・強度評価 |
| 不正アクセス手法: | 予備調査、遠隔侵入、侵入後の行動、その他の手法 |
| 法令・規格: | 法制度・法律問題、基準・ガイドライン・規格など |

http://www.ipa.go.jp/security/fy15/reports/skillmap/index.html

## 不正アクセス対策：　ファイアウォール


← アプリケーションレベル・ゲートウェイ型

← サーキットレベル・ゲートウェイ型

← パケットフィルタ型

## パケットフィルタ型

- 主にネットワーク層(レイヤ3)でパケットをフィルタリング
- レイヤ3スイッチ(ルータ)などで利用

- 利点：高速
- 欠点：ルールの設定が煩雑になりやすい

- スタティック・パケット・フィルタリング
  - プロトコル
  - 始点アドレス・ポート
  - 終点アドレス・ポート
  - 動作(通過／遮断)
- ダイナミック・パケット・フィルタリング
  - 内部からの通信に関係する外部からの通信を自動的に許可
- ステートフル・パケット・インスペクション
  - ダイナミックの一種で不当な手順のパケットは自動的に遮断する

## アプリケーションレベル・ゲートウェイ型

- アプリケーション層（レイヤ7）でプロトコル毎に通信を中継
- プロキシサーバ
- サーバプログラム、または、アプライアンスで提供

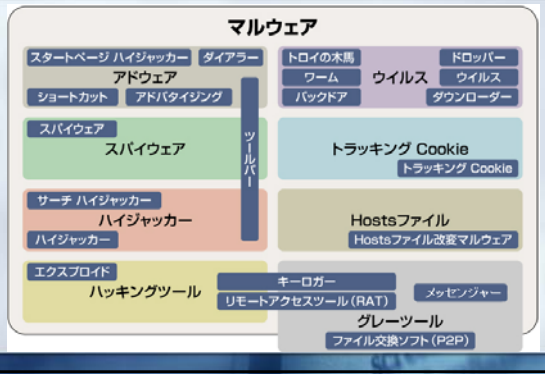
- 利点：
  - 社内からは外部と直接接続することなく安全にサービスを利用できる
  - サービスの内容毎にフィルタリングできる
- 欠点：
  - プロトコル別に個別のゲートウェイが必要になる
  - パケットフィルタ型よりやや遅い

## サーキットレベル・ゲートウェイ型

- トランスポート層（レイヤ4）でコネクション要求を中継
- レイヤ4スイッチ（ロードバランサなど）で利用

- 利点：
  - ルールの設定が簡単
- 欠点：
  - クライアントアプリケーションやユーザー操作の変更が必要な場合がある

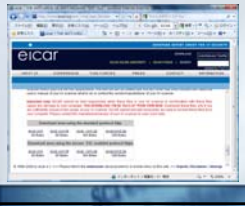
## ウイルス対策： マルウェアの実態




## ウイルス対策： 導入時のテクニック

- 製品選択・評価
  - http://www.virusbtn.com/index
- ウイルス・テスト・ファイルの利用
  - http://www.eicar.org/anti_virus_test_file.htm

X5O!P%@AP[4¥PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

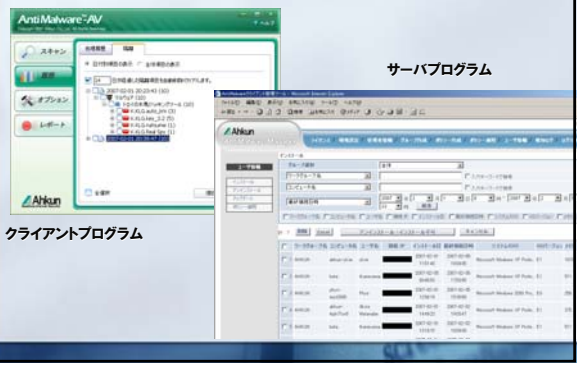


## ウイルス対策： 解析・調査・研究

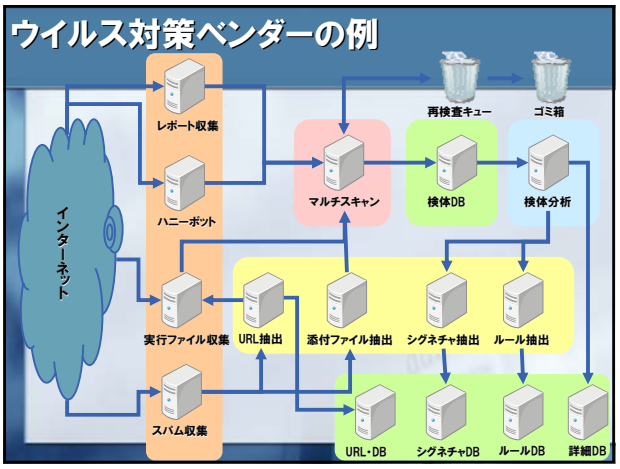
- 疑わしいファイル、駆除不能マルウェアの解析
  - http://www.virustotal.com/jp/
  - http://virusscan.jotti.org/en
  - http://anubis.iseclab.org/
  - http://www.virusbtn.com/resources/vgrep/index.xml
- マルウェア名からの詳細調査
  - 各社ワクチンベンダーのホームページ
  - https://isec.ipa.go.jp/zha-virusdb/web/Top.php
  - http://www.spywareguide.com/index.php
- ウイルス／ワクチン研究
  - http://vx.netlux.org/

## ウイルス対策： 製品事例

Ahkun社 AntiMalware



## ウイルス対策ベンダーの例




## スパム対策： スパム対策の技術

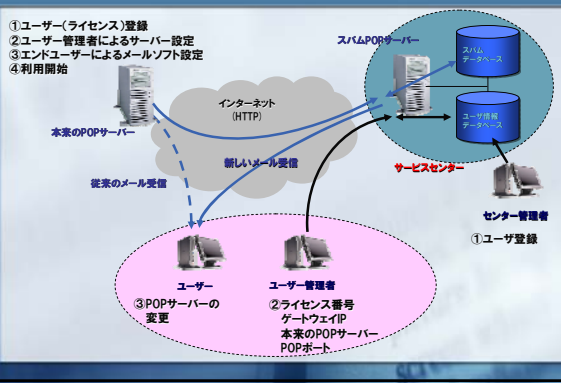
- **ホワイトリスト、ブラックリスト（BlackList/WhiteList）**
  - 許可するメールアドレスと拒否するメールアドレスを登録することでスパムを軽減する。
  - 一度、許可してしまうとリストから削除しない限りにそのアドレスからのメールを受信。
- **RBL（Real-timeBlockList）**
  - 第三者機関が作成するのブラックリストをリアルタイムに参照して判断。
  - 第三者機関のほとんどが海外にあり、主に海外産のスパムが対象である。
- **ペリメター検査（PerimeterCheck）**
  - IP、DHA、ゾンビ、スプーフィング、DoS攻撃の各検査、またRFC822基準と比較。
  - PCのモバイル使用時にIPが変更してしまうために、IP検査が正常にできなくなる。
- **コンテンツフィルタリング（ContentFiltering）**
  - メールのコンテンツ（本文など）に含まれるキーワードやフレーズを分析し判別。
  - 様々な言語やHTMLで送られるスパムへの対応が困難、画像スパムには対応できない。
- **ヒューリスティック検査（HeuristicCheck）**
  - スパムに利用される特徴（単語、表現など）にスコアをつけて判断。
  - スコアの高い単語がメールに使われると誤検知。
- **ベイジアンフィルタ （BayesianFilter）**
  - メールに含まれる単語の出現頻度と単語の関連性を数値化し、過去のスパムと比較判断。
  - 個人がスパムと判断することで効率が高くなる技術の為、管理とトレーニングが必要。
- **認証 （Authentication）**
  - 業界標準認証： DKIM（Yahoo!, Cisco）、 SPF/SIDF（Microsoft、AOL）
  - チャレンジ・レスポンス認証： 新しい差出人のメールに対して認証を求めることで判断。

BoxSentry社 RealMail

## スパム対策の実際（アプライアンス例）

Ahkun社 SpamInformer

## スパム対策の実際（POP対応例）




Ahkun社 AntiPhisher

## フィッシング対策の実際

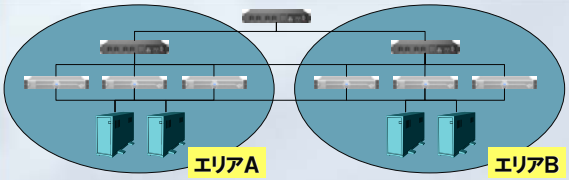
- いよ銀行
  - http://akira.0web.cib.net/phishing/0174iyo.htm
  - https://bb1.finemax.net/0174iyo/bob/BOB_90N90.htm
- 百五銀行
  - http://akira.0web.cib.net/phishing/105direct.mht
  - https://www.105direct.105bank.com/WBIG0000.html
- 百十四銀行
  - http://akira.0web.cib.net/phishing/114bank.mht
  - https://www.inb.114bank.chance.co.jp/int/banking?_TRANID=INBLGNLGN001_001
- ゆうちょ銀行
  - http://akira.0web.cib.net/phishing/direct.jp-bank.japanpost.htm
  - https://direct.jp-bank.japanpost.jp/tp1web/U010101SCK.do
- 北國銀行
  - http://akira.0web.cib.net/phishing/hokkokubank.mht
  - https://ib.hokkokubank.co.jp/HKIK/BankIK?xtr=aulogon01000&NLS=HKIKP
- 北陸銀行
  - http://akira.0web.cib.net/phishing/hokugin.direct.A.mht
  - https://www2.paweb.anser.or.jp/BS?CCT0080=0144
- 愛媛銀行
  - http://akira.0web.cib.net/phishing/ib-channel.mht
  - https://www.ib-channel.net/ehime/web/isp/B02-01.isp

## 最重要セキュリティ対策

- OSやワクチンソフトは自動更新に設定
- ファイル交換ソフトの使用禁止
- メッセンジャーの使用禁止
- ブラウザのセキュリティ設定を変更したら元に戻す
- HTMLメールの禁止
- スクリプトの自動実行の停止
- スパム対策の実施
- CDからの自動実行の停止
- USBメモリーの使用禁止
- 承認外ソフトの使用禁止
- ソフトの違法コピー禁止
- 文書・画像・映像などの著作権への配慮

**運用基準により例外あり！**

## バックアップ体制の例 （HA構成）




- **システム**
  - Webサーバ/APサーバ
  - バランシング
- **データ**
  - レプリケーション
    - マルチマスタ方式
    - マスタスレーブ方式
- **電源**
  - 電源系統の二重化
  - 自家発電、無停電電源（UPS）
- **その他**
  - 物理的不正侵入対策、雷対策、
  - 電波対策、地震対策、水害対策、
  - 火災対策、温度対策、湿度対策

## セキュリティに関する資格・認定制度の紹介

- **国家資格制度（情報処理技術者試験）**
  - 情報セキュリティアドミニストレータ
    - 情報システム利用者側の資格。情報セキュリティ管理の現場責任者として、情報セキュリティに関する企画・実施・運用・分析のすべての段階で、物理的観点、人的観点及び技術的観点から情報セキュリティを保つための施策を計画・実施し、その結果に関する評価を行う業務に従事し、次の役割を果たすことを目的にしている。http://www.jitec.jp/1_11seido/h13/ss.html
  - テクニカルエンジニア試験（情報セキュリティ）
    - 開発・運用側の資格。実施予定：平成18年4月
      http://www.jitec.jp/1_00topic/topic_20050901_ts.html
- **民間資格制度**
  - ネットワーク情報セキュリティマネージャー（略称：NISM）
    - ハッカーやサイバーテロの脅威に対処し、情報通信ネットワークの安全性・信頼性を確保するために、情報通信サービスを提供する事業者に配置する専門家を育成することを目的として創設。主催団体が実施する資格認定のための講習（認定講習）を受講し、一定のレベルに達すると、有資格者として認定される。http://www.nism.jp/
  - CISSP（CertifiedInformationSystemsSecurityProfessional）
    - (ISC) 2(InternationalInformationSystemsSecurityCertificationConsortium)が認定を行っている国際的に最も権威あるセキュリティ専門家認証資格。
      https://www.isc2.org/japan/

## その他の情報源

- 情報セキュリティマネジメントシステム（@IT基礎講座　全10回連載）
  - http://www.atmarkit.co.jp/fsecurity/rensai/guide01/guide01.html
- 情報セキュリティ理解度セルフチェック　ISHOT4a6
  - http://slb.insa.org/slbm/
- 中小企業情報セキュリティ対策促進事業
  - 情報セキュリティの基礎
  - http://www.insa.org/ikusei/
- 情報セキュリティに関するツール
  - http://www.ipa.go.jp/security/tools/index.html
- 情報セキュリティに関する調査研究・報告書
  - http://www.ipa.go.jp/security/products/products.html
- JNSA　WGによる成果物
  - http://www.insa.org/result/index.html
- 中小企業向け　5分でできる！自社診断シート
  - http://www.ipa.go.jp/security/manager/know/sme-guide/index.html

## お疲れ様でした！

株式会社アークン
代表取締役
渡部　章