# 企業の情報セキュリティ対策と実践

徳島県情報産業協会
平成17年11月29日（火）13：00～16：00
WEB110代表　吉川誠司

## 目次

1. サイバー犯罪の動向
2. 平成17年上半期の主なサイバー犯罪の事例
3. 情報セキュリティに係る政府の動向
4. 政府が予定する、企業の情報セキュリティ対策強化の為の具体的方策
5. 情報セキュリティを取り巻く各種制度
6. 企業で発生する情報漏えいの分類
7. 個人情報漏洩事件の分析
8. システム管理者が抱える課題
9. セキュリティ・ユニバーサル・デザインへの道
10. ウェブサイトからの個人情報の漏洩
11. スパイウェア
12. フィッシング

## （1）サイバー犯罪の動向

**1　サイバー犯罪の検挙件数**

サイバー犯罪（情報技術を利用する犯罪）の検挙件数は1，612件で、前年同期（1，063件）と比べて549件、約52％増加。［1頁］

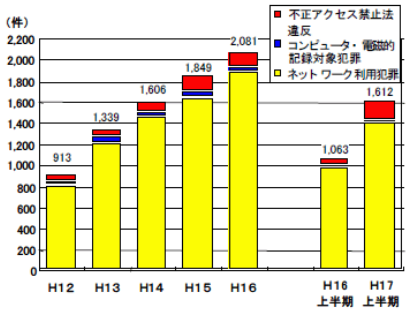
（主な特徴）

○ 不正アクセス禁止法違反が、198件で前年同期の3倍に増加し、昨年一年間の検挙件数を上回る。

○ネットワーク利用犯罪では、

・ 詐欺が約2．7倍に増加。インターネット・オークションを利用したものが多い。

・ 児童ポルノ事案が約２倍、青少年保護育成条例違反が約1．4倍に増加。




## （1）サイバー犯罪の動向

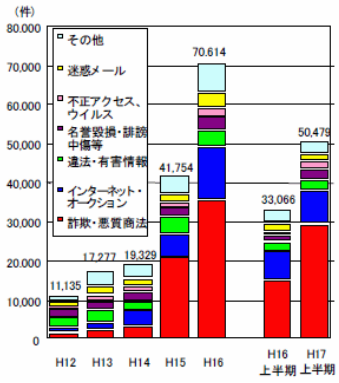
**2　サイバー犯罪等に関する相談受理件数**

都道府県警察のサイバー犯罪相談窓口等が受理した相談受理件数は、50，479件で、前年同期（33，066件）と比べて約1．5倍に増加。［5頁］

（主な特徴）

○ 詐欺、悪質商法に関する相談が約２倍に増加。有料サイトの料金請求に関する相談が多い。

○ 不正アクセス、ウィルスに関する相談が約1．8倍に増加。オンラインゲームやオークションでの不正アクセスに関する相談が多い。



## （1）サイバー犯罪の動向

（平成17年上半期の不正アクセス行為の発生状況からの帰結）

1. 認知件数
   317件（海外から31件、国内から265件、不明21件）＋119件
2. 被害に係るコンピュータのアクセス管理者
   主にプロバイダと一般企業
3. 認知の端緒
   利用権者からの通報が大部分を占める
4. 不正アクセス行為の手口
   検挙件数のうち、識別符号窃用型が大部分（193件）で、セキュリティホール攻撃型はわずか3件
5. 不正アクセス行為の後に利用されたサービス
   ネットオークション120件、オンラインゲーム193件、が圧倒的多数。
6. 識別符号の入手方法
   利用権者の設定の甘さにつけこんだものが大部分

## （2）平成17年上半期 主なサイバー犯罪検挙事例

（不正アクセス禁止法違反）

**●ハッキングツールを使用して不正取得した識別符号を他の学校に送りつけた事案**

被疑者（無職・男・19歳）は、以前在学していた学校のサーバに対して、自分のハッキングの力量を試す目的でハッキングツールを使用して不正アクセスを行い、同校生徒約500人分の識別符号を不正に取得した。これが原因で退学処分となったため、同校の信用を毀損する目的で、取得した識別符号を別の専門学校の統括責任者宛に電子メールで送信し、当該識別符号を利用権者以外の者に提供することで不正アクセス行為を助長した。（5月・京都）

**●元社員によるメールサーバーへの不正アクセス事案**

被疑者（会社員・男・39歳）は、以前コンピュータの管理を行っていた会社を退職させられたのを不満に思い、同社の業務を妨害する目的で、在職時に自ら設定していたID・パスワードを用いて当時の勤務先から同社のメールサーバーに不正アクセスを行い、約1千通のメールを閲覧したほか、数十通のメールを削除した。（4月・愛知）

## （2）平成17年上半期
## 主なサイバー犯罪検挙事例

（不正アクセス禁止法違反）

**●サーバのセキュリティ脆弱性をついて顧客情報を不正に取得した事案**

被疑者（大学生・男・27歳）は、旅行会社が管理運営するサーバに対し、セキュリティの脆弱性を付く手法により不正アクセスを行い、サーバに蔵置されていた同社会員の氏名、住所、会員ID、パスワードなどの個人情報を不正に入手した。（6月・警視庁）

（有線電気通信法違反）

**●他人の無線LANを踏み台にして迷惑メールを大量送信した事案**

被疑者（会社員・男・37歳）は、自ら経営する出会い系サイトに係る広告宣伝メールを、実在の電気通信事業者のごとく送信者名・返信先メールアドレスを偽った上で、他人の無線LANを利用して不特定多数に大量メールを送信し、その間、同送信によって発生した約41万件のエラーメールが同事業者に返送されたことにより、同事業者のコンピュータの正常な働きが妨げられ、同事業者が提供するメール転送サービスを妨害した。（4月・京都）

## （2）平成17年上半期
## 主なサイバー犯罪検挙事例

（不正アクセス禁止法違反・有線電気通信法違反）

**●楽天からの顧客情報漏えい事案**

輸入雑貨販売会社「センターロード」の元社員は、楽天が「利用権者」としてセンターロード社に与えたユーザー名とパスワードを使って27回にわたり不正アクセスし、3万6239件の顧客情報を入手した。 元社員は発信元を隠すため、自宅から離れた台東区のJR上野駅周辺の商店街などにパソコンを持ち出して無関係の会社や商店の無線LANに侵入し、サーバーの接続履歴に痕跡が残らないようにしていたという。
また、ビッターズでもセンターロード社の顧客情報約8500人分が流出しており、関連を調べる。（10月・警視庁）

## （3）情報セキュリティに係る政府の動向

2004年7月にIT戦略本部情報セキュリティ専門調査会の下に情報セキュリティ基本問題委員会を設置

→情報セキュリティに対する我が国の新たな取り組みについての検討を開始

2005年4月に内閣官房情報セキュリティセンター設置

→政府における情報セキュリティ確保の取組みについて中心的役割を果たす

2005年5月にIT戦略本部の下に情報セキュリティ政策会議を設置（さらにこの下に2つの専門委員会を設置）

→政府の情報システムにおける情報セキュリティ確保についての取組み、重要インフラにおける情報セキュリティ確保のためのフレームワーク作りを行う

## （4）政府が予定する、企業の情報セキュリティ対策強化のための具体的方策

**①企業における情報セキュリティリスク明確化のための取組み**

情報セキュリティ関係の事故事例を踏まえつつ、企業における情報セキュリティをめぐるリスクに対する定量的評価手法の研究を推進する。

## （4）政府が予定する、企業の情報セキュリティ対策強化のための具体的方策

### ②企業の情報セキュリティ対策が市場評価に繋がる環境の整備

a.企業における各種制度活用の推進

「情報セキュリティ対策ベンチマークの利用」、「ISMS認証の取得」、「情報セキュリティ監査」、「事業継続計画の策定」に向けて、自主的な取組みが行われるよう環境整備に努める。また、それらの実施状況に関する「情報セキュリティ報告書」の自主的な開示を推進する。

ISMS認証：（情報セキュリティマネジメントシステム：Information Security Management Systemという第三者適合性評価制度）

## （4）政府が予定する、企業の情報セキュリティ対策強化のための具体的方策

### ②企業の情報セキュリティ対策が市場評価に繋がる環境の整備

b.政府調達・自治体調達への各種制度の活用

各種政府調達においては十分な広報活動を行いつつ、受注候補先企業の情報セキュリティ対策レベルの評価（「情報セキュリティ対策ベンチマーク」「ISMS認証の取得」「情報セキュリティ監査」「事業継続計画」の活用）を入札条件の一つとして実施するための環境整備を行う。

## （4）政府が予定する、企業の情報セキュリティ対策強化のための具体的方策

### ②企業の情報セキュリティ対策が市場評価に繋がる環境の整備

c.表彰制度の整備
情報セキュリティ対策に積極的に取組む企業に対する表彰制度を整備する。

## （4）政府が予定する、企業の情報セキュリティ対策強化のための具体的方策

### ③企業における情報セキュリティ人材の確保・育成

①②を通じて経営トップの情報セキュリティへの理解を普及させるとともに、企業の情報システム担当者等に対する全国規模での広報啓発・普及活動を実施する。各企業において情報セキュリティ対策を行っている担当者のモチベーション維持のための取組みを推進する。

情報セキュリティアドミニストレーター（独立行政法人　情報処理推進機構）
http://www.jitec.jp/1_11seido/h13/ss.html
情報セキュリティ検定試験（財団法人　全日本情報学習振興協会）
http://www.joho-security.jp/license.html
個人情報保護士認定試験（財団法人　全日本情報学習振興協会）
http://www.joho-gakushu.or.jp/piip/piip.html

## （5）情報セキュリティを取り巻く各種制度

### 個人情報保護関連

- プライバシーマーク制度

http://privacymark.jp/

プライバシーマークは日本情報処理開発協会(JIPDEC)が管理する、個人情報取り扱いに関する認定制度。 個人情報保護JISに適合したコンプライアンス・プログラムを整備し、個人情報の取扱いを適切に行っている事業者を、評価・認定し、その証としてプライバシーマークと称するロゴの使用を許諾する。

- TRUSTeシール制度

http://www.truste-jp.org

個人情報保護の取扱に関して適正な取組みを実施している事業者に付与しているシール。TRUSTeは国際的なプライバシー保護組織として知られているため、シールを取得しているということは個人情報管理について世界的に安全性を認められたことだと言える。シールの有効期間は1年間。

## （5）情報セキュリティを取り巻く各種制度

### 情報セキュリティ関連

- ISMS適合性評価制度

http://www.isms.jipdec.jp/

企業の情報セキュリティマネジメントシステム(ISMS)が、国際標準規格である「ISO/IEC 17799」に準拠していることを認定する、財団法人 日本情報処理開発協会(JIPDEC)の評価制度。

- インターネット接続サービス安全・安心マーク制度

http://www.isp-ss.jp/

一般利用者が、インターネット接続サービスを選定するにあたり、その事業者が安全に、且つ、安心して利用できるかどうかについての目安としてマークによる情報を提供し、もってインターネットの利用の促進に資することを目的とする制度。

## （5）情報セキュリティを取り巻く各種制度

### セキュリティ関連の監査

- Trustサービス

Trustサービスは、米国公認会計士協会とカナダ勅許会計士協会が開発したシステムに関する保証サービスであり、公認会計士による第三者評価を提供します。

- WebTrust for CA認定

米国公認会計士協会によって定められた、認証局のシステムの信頼性又は安全性等に関する内部統制についての基準。WebTrust for CA基準を満たしているか審査し問題なしと判断された場合に取得されます。ウェブブラウザに「信頼された証明機関」として登録されているデジタル証明書の発行サービスを行う認証局を運用するためには、WebTrust for CA認定を取得する必要があります。

## （5）情報セキュリティを取り巻く各種制度

### セキュリティ関連の監査

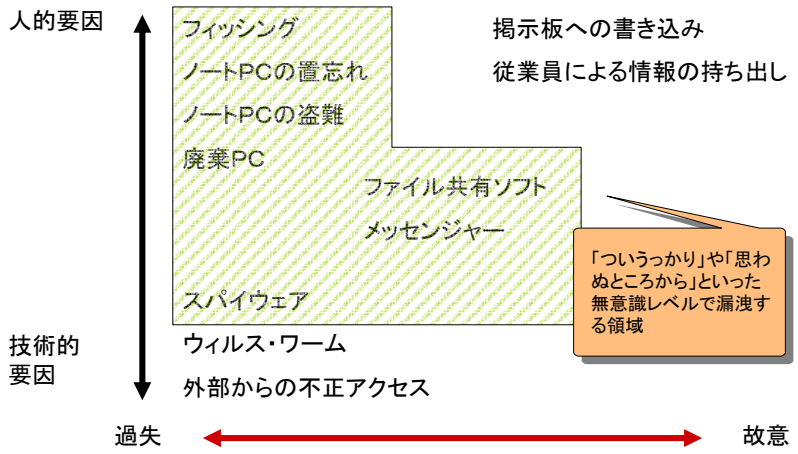
- 情報セキュリティ監査制度

情報セキュリティ監査制度は、組織やシステムが情報セキュリティ管理基準等の判断基準に準拠しているかを監査する「保証型監査」、それとのギャップは何かについて監査する「助言型監査」の2種類がある。いずれも、情報セキュリティ監査人が監査を実施し報告する制度。

- システム監査制度

システム監査制度は、「組織体の情報システムにまつわるリスクに対するコントロールがリスクアセスメントに基づいて適切に整備・運用されているかを、独立かつ専門的な立場のシステム監査人が検証又は評価することによって、保証を与えあるいは助言を行い、もってITガバナンスの実現に寄与すること」（システム監査基準/NPOシステム監査人協会）を目的とした制度 。

## （6）企業で発生する情報漏えいの分類




## 個人情報漏えい事件の分析

訴訟費用などの事故対応費用も発生する。さらには、企業イメージの低下による悪影響も発生。

| | 2002年 | 2003年 | 2004年 |
|---|---|---|---|
| 漏えい事件数 | 62件（55件） | 57件（51件） | 366件（336件） |
| 損害賠償総額 | 189億2201万円 | 280億6936万円 | 4666億9250万円 |
| 最大損害賠償額 | 90億円 | 71億1990万円 | 542億円 |
| 平均損害賠償額 | 3億4403万円 | 5億5038万円 | 13億8897万円 |
| 総被害者数 | 41万8716人 | 155万4592人 | 1435万61人 |
| 最大被害者数 | 10万人 | 56万人 | 451万人 |
| 平均被害者数 | 7613人 | 3万482人 | 3万1056人 |

出展：2004年度情報セキュリティインシデントに関する調査報告書 日本ネットワークセキュリティ協会

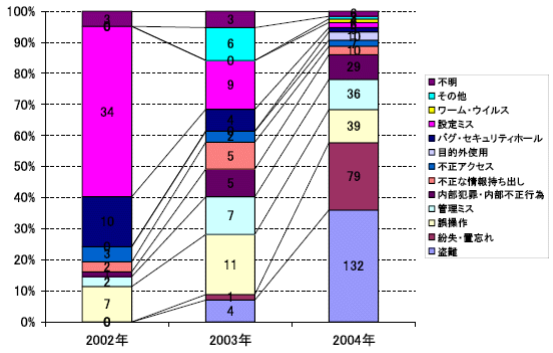
## 個人情報漏えい原因

| 情報漏えい原因 | 比率 | 情報漏えい原因 | 比率 |
|---|---|---|---|
| 盗難 | 36.15% | 目的外使用 | 2.7% |
| 紛失・置忘れ | 21.6% | 不正アクセス | 1.9% |
| 誤操作 | 10.7% | バグ・セキュリティホール | 1.4% |
| 管理ミス | 9.8% | 設定ミス | 1.6% |
| 内部犯罪・内部不正行為 | 7.9% | ウィルス・ワーム | 1.1% |
| 不正な情報持ち出し | 2.7% | その他・不明 | 2.4% |

盗難・紛失・置忘れだけで57.81%を占めている

出展：2004年度情報セキュリティインシデントに関する調査報告書 日本ネットワークセキュリティ協会

## 情報漏えい原因の経年変化




「盗難」「紛失・置忘れ」が大幅に増加しているのは、それらのが個人情報漏洩事件として報道されたから。逆に、「設定ミス」「バグ・セキュリティーホール」の比率が下がっていることから、システム的な対策が浸透してきたことが伺える。

出展：2004年度情報セキュリティインシデントに関する調査報告書 日本ネットワークセキュリティ協会

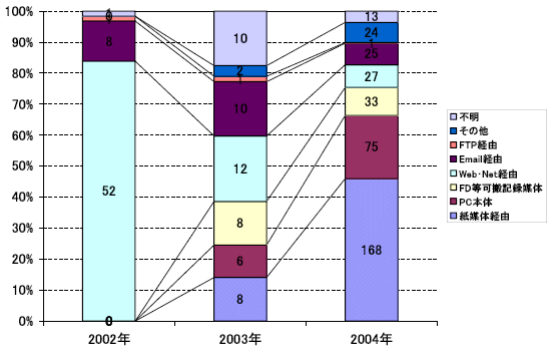
## 個人情報漏えい経路

| 情報漏えい経路 | 比率 | 情報漏えい経路 | 比率 |
|---|---|---|---|
| 紙媒体経由 | 45.9% | E-mail経由 | 6.8% |
| PC本体 | 20.5% | FTP経由 | 0.3% |
| FD等可搬記録媒体 | 9.0% | その他 | 6.6% |
| Web/net経由 | 7.4% | 不明 | 3.6% |

「紙媒体」「PC本体」「FD等可搬記録媒体」で75.4%を占めるのは、資料の入った鞄の盗難や車上荒らし、搬送中の紛失の発生率と連動しているため。

出展：2004年度情報セキュリティインシデントに関する調査報告書 日本ネットワークセキュリティ協会

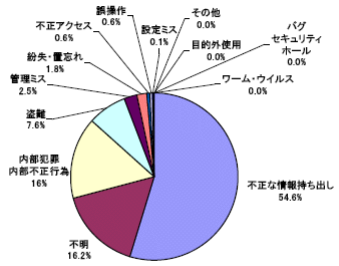
## 情報漏えい経路の経年変化




情報漏えい原因として「盗難や紛失」が増加したことに連動して「紙媒体」「PC本体」の比率が増加している。一方、システム的な対策が進んだことにより「web・net経由」での漏洩は減っている。

出展：2004年度情報セキュリティインシデントに関する調査報告書 日本ネットワークセキュリティ協会

## 情報漏えい原因別　被害者数の比率




原因別の被害者数の比率

情報漏えい原因の比率としては「内部犯行・内部不正行為」「不正な情報持ち出し」が合わせて10.6%であったのに対し、被害者数の比率では70.6%を占める。

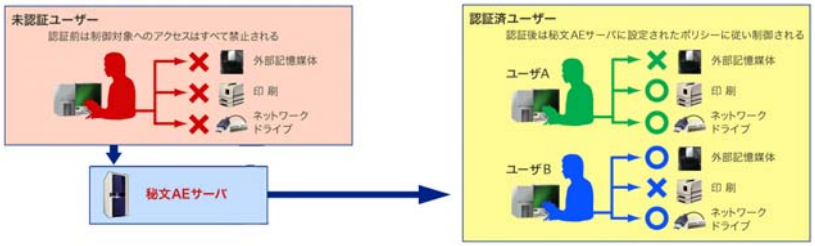
出展：2004年度情報セキュリティインシデントに関する調査報告書 日本ネットワークセキュリティ協会

## 情報漏えい対策ソリューションに求められる機能

| | |
|---|---|
| ファイル操作制御 | ファイル操作（コピーやリネーム）履歴の記録だけでなく、操作を詳細に制限する機能があるか。 |
| デバイス利用制御 | 外部記録媒体（FD、CD、USBメモリ、フラッシュメモリ、外付けHDDなど）の利用制御を端末単位で設定できるか。 |
| アプリケーション操作制御 | WordやExcelを始めとしたアプリケーションソフトでファイルを編集する際などに、ユーザ単位でコピーや保存、印刷、メール添付等の制御が可能か。 |
| 暗号化機能 | 暗号アルゴリズムにはAES（128ビット）か。クライアントPCのドライブ全体または外部記憶媒体に対して、自動的に暗号化／複合化の処理を行えるか。 |
| モバイル利用時の操作制御 | モバイル端末を社外で利用する際の挙動について、社内環境での利用時と同様の制御が行われるのか、ログは採取されるのか。 |
| ログの採取、統計機能 | ファイル操作ログ、印刷ログの他にどのようなログ取得が可能か。記録したログに対してどのような操作（抽出や統計）が行えるのか。 |

## 分散管理型の内部情報漏洩対策ソリューション

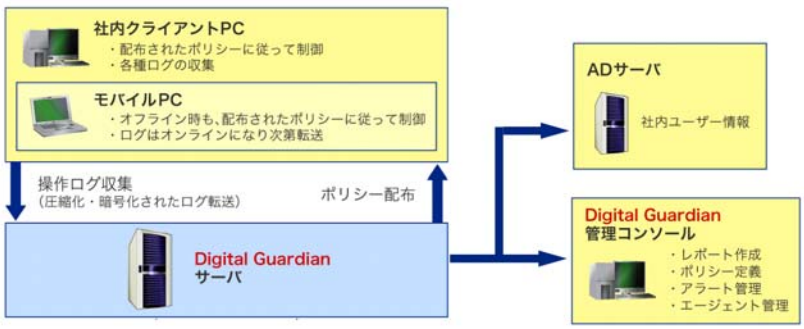
「秘文Advanced Edition（秘文AE）」シリーズ




この製品の導入を検討する場合には、自社の望む内部情報漏えい対策がどのようなものか正確に把握したうえで、システムインテグレーターと入念に相談してシリーズ製品を選択する必要がある。

## 分散管理型の内部情報漏洩対策ソリューション

Digital Guardian（米Verdasys）




この製品は「多岐にわたる社内ユーザーの行動を柔軟に制御すること」「社内ユーザーの行動を（ログの暗号化などの対策によって）確実にログに残すこと」「ログを有効に活用すること」について特に配慮した、完成度の高い内部情報漏えい対策製品

## （8）システム管理者が抱える課題

### 脆弱性情報収集に対する管理者の作業負荷

大量の情報から関連するものを抽出しなければならない

管理者主導型の情報収集・・・収集漏れ、対応の遅れ

重要性の判断が困難・・・対策漏れ

プッシュ型の脆弱性情報提供ソリューションが必要

## （8）システム管理者が抱える課題

### 脆弱性を解決するためのパッチが適用できない

- 脆弱性公開から脅威発生までの期間が短い
- 稼働中の重要なアプリケーションに対して即座にパッチを適用出来ない
- 全てのクライアントに対してパッチを適用することが出来ない
- かといってクライアントPCに管理者権限を与えると不要なアプリケーションをインストールされるおそれもあり、しかも管理者権限で動作させられることが別の重大なセキュリティホールになる可能性がある。

## （8）システム管理者が抱える課題

**感染経路の把握が困難**

ユビキタス・ネットワークにより社外での感染の危険性増大

社員が勝手に個人のノートPCやPDAなどをイントラネットに接続する

社員が勝手にイントラネットの中に無線LANのアクセスポイントを立てる

セキュリティパッチが適用されていない場合は接続を許可させない「検疫ネットワーク」ソリューション の必要性

## （8）システム管理者が抱える課題

- システム利用者全員のセキュリティ意識をどうやって高めるか
- 利用者の意識向上だけでは「ついうっかり」や「思わぬところから」の情報漏えいを防ぐことは不可能

利用者の意識に依存しないセキュリティ・ユニバーサルデザインが重要

## （9）セキュリティ・ユニバーサルデザインへの道

①ゲートウェイレイヤーでのメールセキュリティソリューション

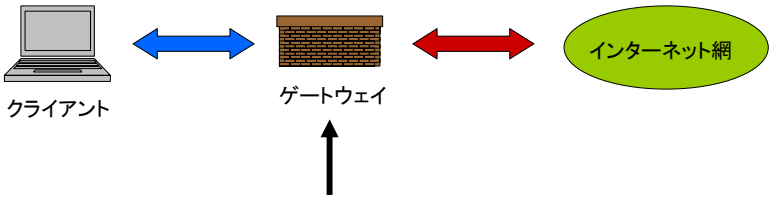
②許可しないアプリケーションの通信を遮断

③検疫ソリューション

④モバイルPCからの情報漏えい対策



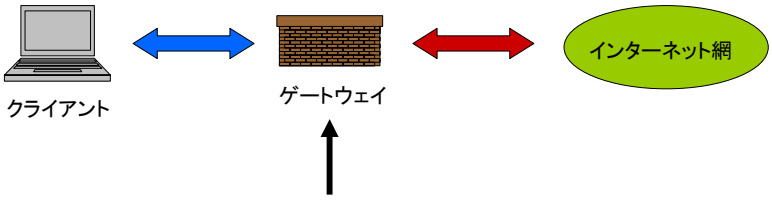
## ①ゲートウェイレイヤーでのメールセキュリティソリューション




- メールファイアーウォール・・DHA攻攻撃防御、SPF認証、コンテンツスキャニング
- ウィルスフィルタ・・・ヒューリスティックフィルタ、マスメーラークリーンアップ
- スパムフィルタ・・・URLフィルタ、ヒューリステック、シグネチャ、言語識別
- コンテンツフィルタ・・・キーワード辞書フィルタ、添付ファイルフィルタ、カスタムフィルタ

例：シマンテック　メールセキュリティ8160、8200シリーズ

## ②許可しないアプリケーションの通信を遮断




- ネットワークゲーム、ファイル共有ソフト、チャットプログラムの通信遮断
- メールソフトに依存しない、ウィルス自身のSMTPエンジンによる送信を禁止
- クライアントがDDos攻撃の発信源として利用されることを防止
- スパイウェア対策（リアルタイム監視、自動削除、除外設定）

例：シマンテック　クライアント・セキュリティ3．0

（9）セキュリティ・ユニバーサルデザインへの道

## ③検疫ソリューション

- PCサーバーのセットアップのためのシステムイメージの作成
- windowsとLinuxプラットフォームにおけるOSアップデート
- 新しいPCへの移行時における、ユーザー環境やアプリケーション設定の保持
- HDDの完全消去
- インベントリ情報とセキュリティパッチの適用

収集したインベントリ情報に基づいて、ポリシーに違反したPCを検知し、リモートパッチを適用する

例：シマンテック　ゴースト・ソリューション・スイート

## ④モバイルPCからの情報漏えい対策

- ハードディスクレスPCの導入


参考：日立　FLORA Se210シリーズ

（9）セキュリティ・ユニバーサルデザインへの道

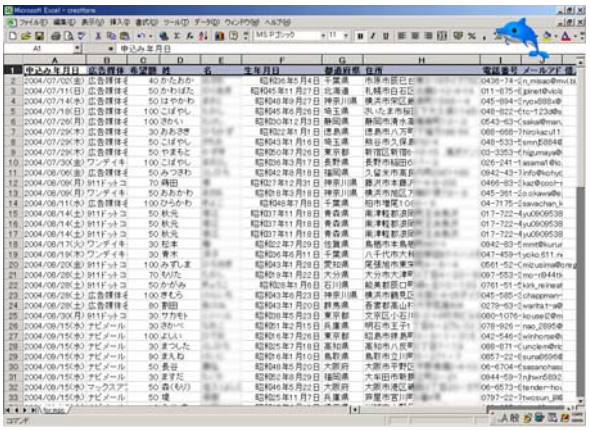
## ④モバイルPCからの情報漏えい対策

- USBメモリと、それに付属している暗号ソフトの併用による
  ノートPCのデータ保護

暗号化されたファイルはノートPCとUSBに2分割して保管する。移動する時には、ノートPCを鞄に入れ、USBメモリはキーホルダーに取り付け身につける。これならノートPCだけ盗まれても、個人情報をノートPCだけで復元することは難しい。

## 10. ウェブサイトからの個人情報漏洩

消費者金融サイトの顧客ファイルがブラウザで閲覧可能だった例





## （1）検索ロボット対策

### ①METAタグによるロボット対策

インデックスさせたくないHTMLファイルの<head>と</head>の間にMETAタグを挿入する

10. ウェブサイトからの個人情報漏洩

## （1）検索ロボット対策

### METAタグの挿入例（途中改行は入れない）

- 当該ページと、そこからリンクしている全てを検索対象からはずす

```
<meta name="ROBOTS" content="NOINDEX, NOFOLLOW">
```

- 当該ページのみを検索対象とし、その先のリンクを辿らないようにする

```
<meta name="ROBOTS" content="INDEX,NOFOLLOW">
```

- 当該ページは検索対象に載せず、そこからのリンクだけをたどるようにする

```
<meta name="ROBOTS" content="NOINDEX,FOLLOW">
```

- 当該ページをキャッシュをさせない

```
<META NAME="ROBOTS" CONTENT="NOARCHIVE">
```

10. ウェブサイトからの個人情報漏洩

## （1）検索ロボット対策

### googleキャッシュデータの削除

Google でのみ "キャッシュ" リンクが表示されないようにし、他の検索エンジンで表示されるようにするには、次のタグを使用します。
**<META NAME="GOOGLEBOT" CONTENT="NOARCHIVE">**

緊急を要し、Google で次回サイトをクロールするまで待てない場合や古くなった無効なリンクを削除するには、URL 自動削除システムを利用する。そのためにはまず上記のメタ タグをページの HTML コードに挿入しておくこと。

URL 自動削除システム

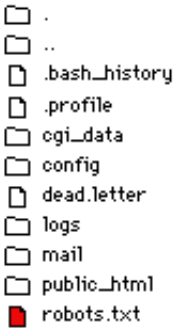
http://services.google.com/urlconsole/controller

10. ウェブサイトからの個人情報漏洩

## （1）検索ロボット対策

### ②Robot.txtの設置による対策

制限内容を書いたテキストファイルをrobots.txtという名前で作成し、ルート・ディレクトリへアスキーモードでアップロードしておく。




10. ウェブサイトからの個人情報漏洩

## （1）検索ロボット対策

全てのロボットに対して全てのディレクトリのクロールを拒否するには、robots.txt のエントリを次のように記述します。

```
User-agent: *
Disallow: /
（空白行）
```

10. ウェブサイトからの個人情報漏洩

## （1）検索ロボット対策

全てのロボットに対して当該ディレクトリ以下をクロール対象から外す場合

```
User-agent: *
Disallow: /cgi-bin/
Disallow: /tmp/
Disallow: /private/
（空白行）
```

10. ウェブサイトからの個人情報漏洩

## （1）検索ロボット対策

全てのロボットを排除しつつ、グーグルボットに対してのみ全てのディレクトリのクロールを許可する場合

```
User-agent:*
Disallow:/
（空白行）
User-agent: googlebot
Disallow:
（空白行）
```

10. ウェブサイトからの個人情報漏洩

## （1）検索ロボット対策

特定の種類のすべてのファイル（例: .gif ファイル）を削除するには、robots.txt のエントリを次のように記述します。

```
User-agent: Googlebot
Disallow: /*.gif$
（空白行）
```

10. ウェブサイトからの個人情報漏洩

## （1）検索ロボット対策

動的に生成されるページを削除するには、robots.txt のエントリを次のように記述します。

```
User-agent: Googlebot
Disallow: /*?
（空白行）
```

10. ウェブサイトからの個人情報漏洩

## （1）検索ロボット対策

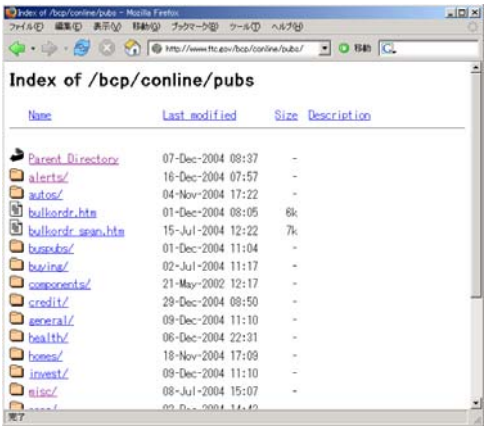
「robot.txt」を読まない、読んでも無視するロボットに対しては、
「.htaccess」でアクセス制限をする。

```
<Files *>
order allow,deny
allow from all
deny from 61.115.195.180
</Files>
```

10. ウェブサイトからの個人情報漏洩

## （2）ディレクトリ保護

ディレクトリ構造が丸見えの状態



## （2）ディレクトリ保護

対策その１：パーミッションの設定と拡張子による方法

```
./cgi/          ← ディレクトリ(701)
  |
  ├ form.cgi    ← CGIファイル(700)または(705)
  |
  └ formdata.cgi ← データ格納ファイル(600)
```

データ格納ファイルの拡張子は
csvやdatではなくcgiにしておくこと



## （2）ディレクトリ保護

対策その２：「.htaccess」による設定

①エラーメッセージファイルを作成し「errmsg.html」として保存しておく

```
<HTML>
<HEAD>
<TITLE>Forbidden - ページを表示できません -
</TITLE>
</HEAD>
<BODY>
<H2>Forbidden - ページを表示できません -</H2>

ファイル名を指定して接続してください。

</BODY>
</HTML>
```

## （2）ディレクトリ保護

対策その２ :「.htaccess」による設定

②下記の記述をした設定ファイルを作成し、「htaccess.txt」というファイル名で保存しておく

```
DirectoryIndex index.html errmsg.html
（空白行）
```

「index.html」が無いときは「errmsg.html」を表示する

10. ウェブサイトからの個人情報漏洩

## （2）ディレクトリ保護

②ファイルをドキュメントルートディレクトリに転送した後に、ファイル名を「.htaccess」に変更


**注意:「htaccess」の転送はアスキーモードで**

## スパイウェアの主な活動

- スクリーンキャプチャ・・・パソコンのデスクトップのスナップショットを撮る
- 特定のキーロギング・・・キーボードの打鍵内容をファイルに記録
- 行動分析・・・クリップボードのモニタリング、ブラウザの訪問履歴、クッキーファイルに保存された情報、キャッシュに保存されたパスワードを列挙して捕捉
- 特定の単語の認識・・・例えばクレジットカード番号やネットバンキングのURL、メールアドレスなど、一定の規則性を持った文字列が入力された場合にその内容を記録。
- ターゲットのIMウィンドーからメッセージを送信
- ウェブカメラのコントロール



## 進化するスパイウェア

「ホステージ・テイカー」

駆除するとPCのシステムを破壊する

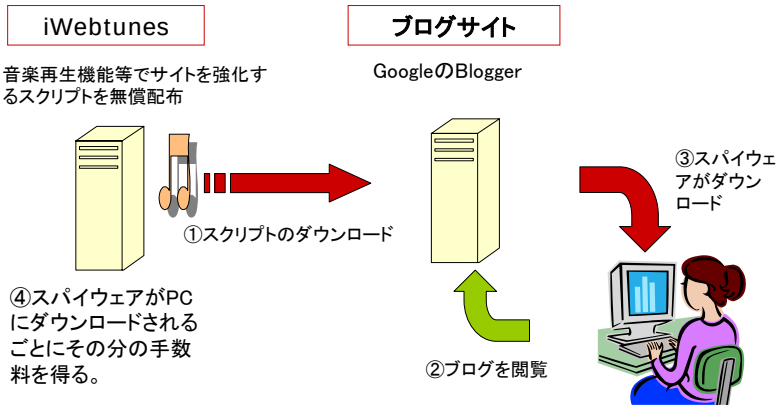
「ルートキット」と呼ばれる技術で作成されたスパイウェアは、OS内部に入り込み、システムレベルで権限を不正に取得して、一般的なユーザーでは検出・駆除ができなくなる。

「ウォッチャー」

2つ1組の形でPCに侵入して、互いに監視し合い、一方が削除されるともう一方が復活させる。このタイプも完全に駆除するのが難しい。

## ブログがスパイウェアの配布に悪用される

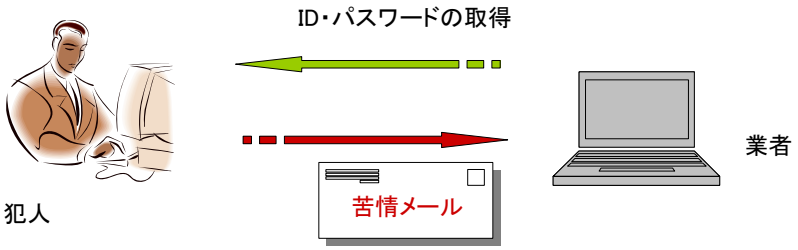
脆弱なウェブブラウザでブログにアクセスしてきたユーザーのPCに、JavaScriptやActiveXを使って自動的にスパイウェアを送りつける手口。





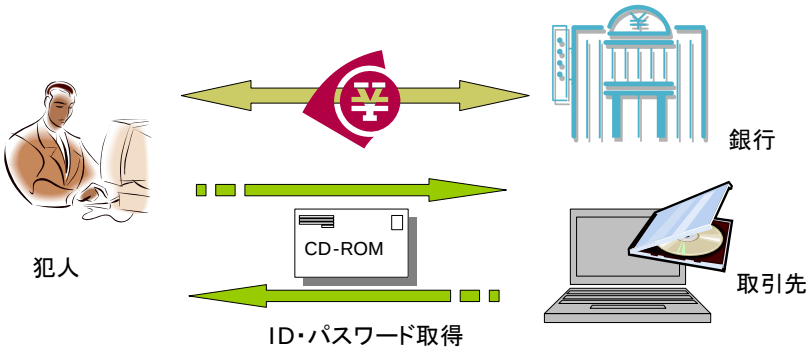

## メールでスパイウェアを感染させる手口

- 容疑者はスパイウエアを自ら作り、楽天市場などの出店業者に客を装って約600通のスパイウェア添付メールを送付。10業者からネットバンキングの IDとパスワードを入手していた。業者がメールを開かざるを得ないようにするため、件名を「苦情」などとし「不良品だった。添付ファイルの写真を見て」と書き込んでいた。不正に入手した出店業者のIDとパスワードを利用し、業者の10口座から約1140万円を、自分たちが管理する口座に移していた。（2005年11月11日 ）



## CD－ROMでスパイウエアを感染させる手口

- 2005年10月から11月にかけ、千葉銀行、北陸銀行、城北信用金庫の3金融機関を送り主と偽ったCD－ROMが顧客や取引先に郵送され、インストールした取引先の一部が不正送金の被害に遭う事件があった。






## スパイウェア専用対策ソフト

Spy Sweeper 4.5J（ウェブルート・ソフトウェア）

http://webroot.com/jp/

- 高度化して検出・駆除ができないスパイウェアを1回のスキャンで完全に駆除できるという優位性があるという。
- 11月下旬からベクターなどのウェブサイトから3990円でダウンロード販売予定。

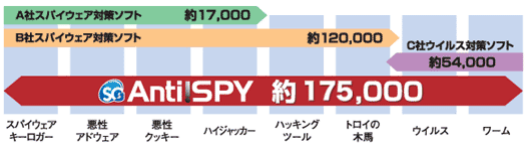
## スパイウェア専用対策ソフト

### スパイウェアの除去とインストール防止

SG AntiSPY

株式会社アークン

http://www.junglejapan.com/products/sec/aspy/index.html





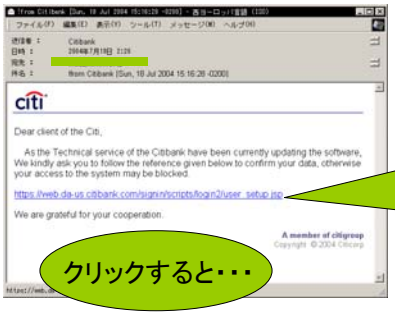
## 12. フィッシング

- ユーザーに偽の電子メールを送りつけ、相手の銀行口座のパスワードやクレジットカード情報などの個人情報をだましとろうとする行為。

■平成17年3月「UFJダイレクト」と「みずほ銀行」を騙るフィッシングメールが送信された。

# 国内フィッシング事案

一見、CITIバンクからのメール・・・



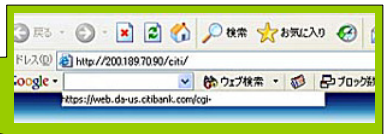

クリックすると・・・


偽のページへ誘導！



# 国内フィッシング事案

でもURLがずれてる・・

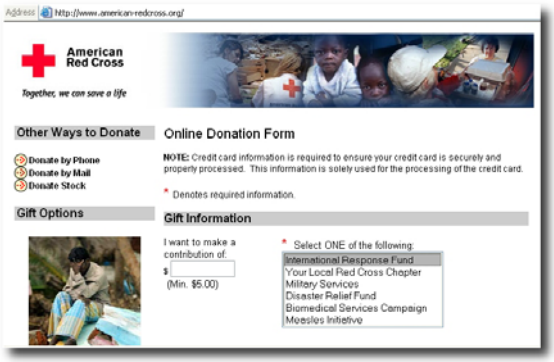




グーグルツールバーを使用していると正規のURLが欄外に表示されてしまっている

## 海外のフィッシング事案

- 最近は戦争や災害の義援金を名目としたフィッシングが主流

スマトラ沖津波に便乗して詐欺をしかける不正なWebサイトは133にも上った






## フィッシングのバリエーション

- HOSTSファイルの書き換えによるリダイレクト
- 小規模なファーミング詐欺。電子メールを通じて拡がり、感染した個々のパソコンのローカルホスト・ファイルを書き換えるウイルス――たとえば、主にインターネット・バンキング利用者を狙ったトロイの木馬『バンカー』(Banker)など――を使って行なわれてきた。ホストファイルが書き換えられていると、ユーザーが正しいURLを入力しても、不正なウェブサイトにつながってしまう。

## フィッシングのバリエーション

- DNS Poisoningによるリダイレクト=Pharming
- DNSサーバに保存された人気の高いウェブサイトのIPアドレスが、悪質なサイトのアドレスに置き換えられてしまう。このため、正規のウェブサイトにアクセスしようとしたユーザーが偽のサイトへリダイレクトされてしまい、そこで機密性の高い情報の入力を求められたり、有害なソフトウェアをPCへインストールするように指示されることになる。
- 脆弱性を抱えたサーバでは、BINDソフトウェアが安全でない状態で稼働しており、forwarder設定が有効になっているすべてDNSサーバは、BIND 9にアップグレードされなければならない。
- セキュリティ研究者のDan Kaminskyが、250万台のDNSサーバをスキャンしたところ、そのうちの約23万台が「DNSキャッシュ汚染」の脅威に対して脆弱であることがわかった。

12. フィッシング

## フィッシングのバリエーション

- Google.comを誤って入力した人へのトロイの木馬のダウンロード
- 米シマンテック社のファイアーウォールに存在する既知の脆弱性を悪用して、『イーベイ』、『Google』、『ウェザー・コム』の利用者を、訪問者のコンピューターにスパイウェアのインストールを試みる3つのサイトへとリダイレクトしようとしたケースがある。

## フィッシングのバリエーション

- DNSワイルドカードによるフィッシング
- 一部誤って入力された電子メールアドレスを正しいアドレスに変換するためDNSレコードで使用するのが、いわゆるワイルドカード機能。最近スパム業者がこれを悪用するようになり、現在ではフィッシング詐欺で使われている。
- イギリスのバークレイズ銀行が標的となったフィッシング詐欺では、送信された電子メールのメッセージに含まれていたリンクは、前半の文字列こそ「barclays.co.uk」と正しいURLのものだったが、これに続く文字列がユーザーを同銀行とは別のサイトへ導くものだった。



## フィッシング詐欺対策ツールバー

**セキュアブレイン の「PhishWall」（無償）**
ブラウザのプラグインとして動作する。アクセスしたサイトごとに正式なドメイン名、IPアドレス、IPアドレスが割り当てられている国名を表示する。想定外の国名が表 示された場合は，フィッシング・サイトの可能性がある。
http://www.securebrain.co.jp/download/index.html

**シンセキュアの「SecureVM for AntiPhishing」（無償）**
Webアクセス前にあらかじめ起動しておく。するとブラウザのやりとりを監視し、ブラウザがフィッシング・サイトにアクセスすると警告メッセージを出す。
http://www.synsecure.co.jp/japan/antiphishing/download.html