マルウエア対策の運用

Internet Week 2006　T13 (4)

住商情報システム株式会社
二木　真明 CISSP

マルウエアの変化と対策の変遷

- ウイルス対策ソフトウエア
  - パターンマッチによる検出が限界に
    - パターン提供が間に合わず感染するケースの増加
      - ウイルス感染拡大速度の圧倒的向上
      - 新種（亜種）登場頻度の激増（開発キット流通など）
    - 侵入経路、感染方法の多様化で対応が複雑化。（スパイウエア対応など）性能問題との格闘。
  - 未知ウイルス検出機能の本質的問題
    - ウイルス作者がウイルス対策ソフトを入手できること
  - 新種ウイルスのかなりの部分は、見落とすことを前提で利用する必要。（でも、既知ウイルス対策としては必須）

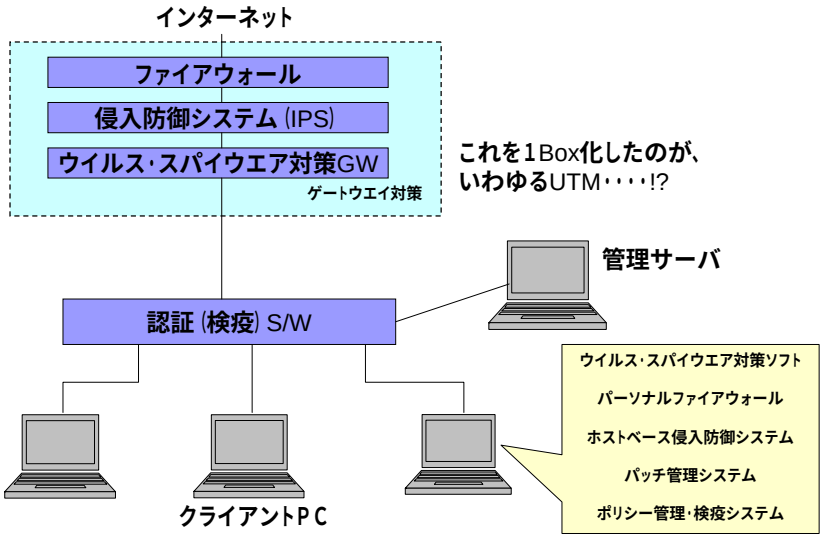
マルウエアの変化と対策の変遷

- クライアント対策の統合化（ソフトウエアのスイート化）
  - ウイルス／スパイウエア対策ソフトウエア
  - デスクトップファイアウォール
  - ホストベース侵入検知・防御システム
  - ソフトウエア起動、実行管理
- クライアント版UTMとでも言うべき流れ　UTM: Unified Threat Management
  - 既知マルウエア→ウイルス対策機能で対応
  - 未知マルウエア攻撃防御、不正通信の検知・阻止→デスクトップF/W HIPSで対応
  - マルウエア実行の検知・阻止→起動・実行管理で対応
- しかし、依然として回避の可能性は否定できない
  - これらはすべて「市販品」、しかも個人で入手可能な金額で手に入るもの。
  - 組織内のすべてのコンピュータに均一な対策を取ることができるのか・・・

階層的マルウエア対策

- クライアント（エンドポイント）での対策
  - セキュリティスイート製品の利用
  - 一般的な脆弱性対策の実施（パッチの適用、安全な設定の強制）
- ネットワークでの対策
  - メール、Webアクセスを経由したマルウエア流入阻止
  - ネットワーク上での侵入・攻撃検知と防御
  - （UTM製品の利用）
- 複数ベンダの組み合わせによるリスク分散
  - クライアント対策、サーバ対策、ネットワーク（G/W）対策
  - それぞれ違うベンダ製品を使うことも意味がある
  - 管理の手間とのトレードオフだが・・・・

最近のマルウエア対策のイメージ



さて、システムは導入したが・・・

- PC,サーバ
  - ウイルス対策ソフトウエア
  - デスクトップF/W・IPS
  - 検疫・ポリシー制御エージェント
- ゲートウエイ
  - ファイアウォール
  - ウイルス対策ゲートウエイ
  - IDS/IPS
  - UTM
- 入れただけ・・・・というのも多いのでは？

まずは、それぞれの集中管理を

- システムは導入しても管理できなければ無意味
  - 導入されたシステムが有効に機能しているかの確認
  - アラームの受信とチェック
  - 定期的な傾向掌握
  - エンドユーザに「適切な管理」を求めるだけではダメ！！
    - もちろん「ユーザ教育・啓発」はとても大切だが、その成果をきちんと評価できなければ意味がない
- 組織全体、もしくはグループ単位での一括管理を
  - 対策の組織レベルでの有効性の維持、検証
  - 組織全体での傾向の掌握＝次の対策への指針

基本的な管理と監視内容

- ウイルス対策システム
  - 稼働状況のチェック
    - すべてのエージェントが正常に動作しているか
    - ソフトウエア（エンジン）のバージョンは最新（or 許容されるレベル）か？
    - パターンファイルは最新か、また、それは適切な速さ（頻度）で更新されているか
    - 定期的にディスク全体のスキャンが行われているか
      - リアルタイム検知で見落としたものが後から検出できることもあるので重要
  - ウイルス検知状況の掌握
    - 全体的な傾向、組織単位での検知数の偏り、検知数の多い個人・・・など。＝未知ウイルス感染リスクの掌握につながる

基本的な管理と監視内容

- デスクトップファイアウォール・IPS
  - 稼働状況のチェック
    - ファイアウォール機能はポリシーどおりに正しく動作しているか
    - ソフトウエア及び各種データベースは最新か
  - 検知、防御状況の掌握
    - 拒否パケットの傾向、攻撃検知状況をネットワーク別に集計・掌握する＝全体としてネットワーク単位の傾向監視ができる
    - ソフトウエア起動、通信の発生状況の掌握（自動許可リストにないソフトウエア起動、通信状況の掌握）＝不審なソフトウエア起動の発見

基本的な管理と監視内容

- 検疫・ポリシー制御エージェント
  - 接続拒否状況の掌握（ポリシー違反の頻度）
    - 特にノートPCなどの接続拒否が頻発するユーザは、外部で感染してくる危険性が高い
    - 接続拒否が頻発する部署（ネットワーク）は、組織的にリスクが高い

基本的な管理と監視内容

- ゲートウエイ
  - 稼働状況のチェック（常時監視が望ましい）
  - 異常検知状況の掌握
    - 対応チームの警戒態勢レベル判定に利用
    - 特定の検知の極端な増加＝攻撃・マルウエアのアウトブレークが発生した可能性→ Orange Alert
    - 全般的な増加＝インターネット治安の悪化→Yellow Alert

日常的な通信傾向の掌握

- ファイアウォールの「ログ」は有用
  - 宛先ポート、プロトコル別、ネットワーク別などの集計を行って可視化しておく
  - 要注意ポートについて集中的に通信をチェック
    - ボットが頻繁に使うポートなど
      - （参考）インターネット治安情勢 by @Police
      - http://www.cyberpolice.go.jp/detect/index.html
  - Web (80,443/tcp) アクセス集計
    - 宛先アドレスランキングとランキング下位のアドレスリストの作成
    - ランキングアクセス下位リストのドメイン名から内容不明のドメインを抽出して要注意ドメインリストを作成
    - リスト中のドメインへのアクセス頻度が高い発信元＝不審サイトアクセスリスクの高いユーザである可能性＝要重点監視

残るリスクはどの程度か・・・・

- 既知マルウエア感染
  - ウイルス／スパイウエア対策ソフトの正しい運用でほぼ、ゼロにできる
- 未知マルウエア感染
  - 電子メール拡散型未知ウイルス・ワームへの感染リスク　は、「要注意者」の数で決まる
  - Webアクセスによる感染リスクは「不審なサイト」アクセス者の数で決まる
  - 既知脆弱性を利用するワームの感染は、パッチが適切に適用されていれば、ほぼゼロ（ゼロ・デイ・ワームの可能性は完全にゼロではないが・・・）
  - 「ねらい撃ち」された場合はより深刻なリスクが生じる
  - 未知マルウエアにRootkit技術を使われると、パターンが提供された後も検知できない可能性が生じる
  - ソフトウエア起動管理が可能なホストベースIPS（最近のパーソナルファイウォール製品の多くがこの機能を実装）ならば、かなりのものを検知できる可能性がある。但し、回避策を講じられる可能性もゼロではない。
  - **正しく管理されているという前提で、一般の会社、業務では受容可能なレベルのリスクではある（受容せざるを得ない・・・！？）**

万一の感染発生に備えて・・・

- 発見・対応のためのしくみと体制作りを
  - エンドユーザ啓発は基本
    - マルウエア感染を疑うべきケースの周知
      - 変なメールを開いてしまった
      - 変なサイトにアクセスしてしまった
      - その後でPCが急に重くなったり、不審な動作をするようになった・・・・・
      - タスクバーのネットワークアイコンがずっと点灯し続けている・・・・
    - 初期対応
      - ネットワークのコネクタを抜き、電源はいれたまま、独自の判断での操作を控えてIT部門やヘルプデスクなど担当部署に連絡を入れる

感染発見のための方策

- ネットワークから見た発見方法はマルウエアの種類によって異なる
- 電子メール大量送信型ウイルス、ワーム
  - 特定のPCから、短時間に複数の外部メールサーバに対して大量のメール送信が行われる
  - ファイアウォールログなどから、25/TCPの直接通信を検出する仕組みを（通信許可もしくは拒否ログ）
    - 原則として自社メールサーバを経ない通信は禁止しておいた方がよい。（万一の感染の際に外部への拡散を防ぐことができるし、外部サーバの利用制限でウイルス感染と誤認するケースを減らすことができる）
  - DNSサーバへの問い合わせ（MX参照）の異常増加からの検知も可能

感染発見のための方策

- 脆弱性攻撃型ネットワークワーム
  - ポートスキャン活動の検知
    - ファイアウォールの特徴的な一連のログもしくはIDS/IPSのポートスキャンアラーム
  - IDSによる内部から外部への脆弱性攻撃検知
    - 内部ネットワークにIDSが設置されていればなおよいが、インターネットに拡散するワームは出口のIDSやIPSでも検出可能
- バックドア（トロイの木馬）
  - 一般に自ら通信を発しないので検知は困難。
  - 脆弱性検査ツールなどを使用して、定期的にスキャンすることでバックドアのポートを検知することもできる
    - ツールによってはかなり副作用が出るので注意が必要
    - 副作用の少ないツールを使って、公開サーバや重要な情報を扱う部門について毎日、昼休みに自動的にスキャンする・・・といったことも有効な発見手段となる
    - パーソナルF/W,IPSから警告が出るので注意
      - 除外リスト登録が可能ならば回避できる

感染発見のための方策

- スパイウエア、ボット　(渡辺さんのプレゼンを参照)
  - IRCボットは通信監視で発見できる可能性
    - 6667/TCP 通信、IDSによるIRCプロトコル検知など (渡辺さんのお話参照)
  - 基本的に通信からの発見は非常に困難
    - 基本的には外向き通信といえども不要なポートはファイアウォールで閉じておくことが重要
    - 通常、あまり使用されないポート番号への通信を出しているホストを洗い出し、重点的に調査する
      - たとえば、8080/TCP 宛先が中国、韓国といったボットネットサーバが多数存在する国、といった条件で抽出してみる
      - 参考(9ページ を参照)
    - COVERT CHANNELを作られたらアウト・・・・(渡辺さんのお話)
      - アクセス先の傾向分析から見つけ出せる可能性もあるが・・・・
    - 地道な作業に疲れないことが重要

感染発見のための方策

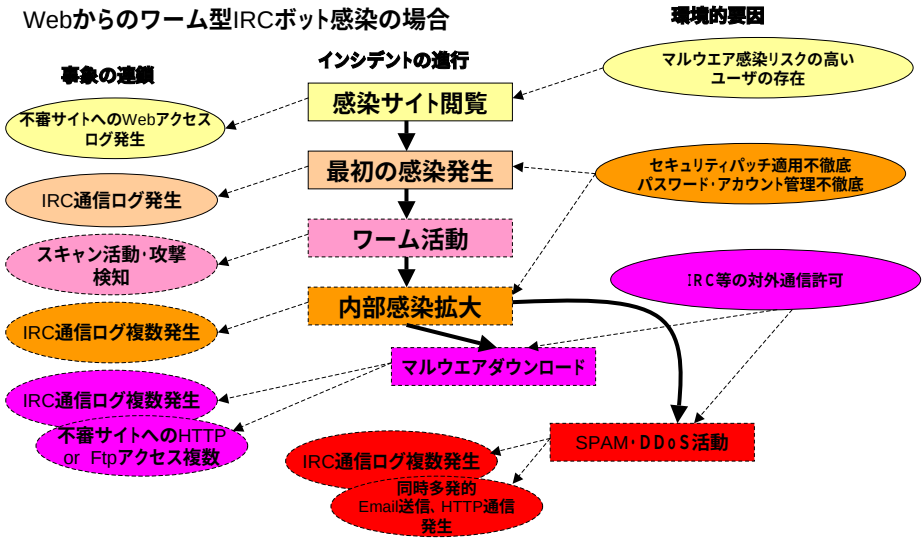
- 最後の砦はPC,サーバ本体での防御
  - 本当に重要な情報、業務を扱う部署はエンドポイントでの防御を
    - 起動可能なアプリケーションの限定、外部接続の限定などのポリシーをポリシー制御ツールを使用して強制する。検疫システムなどで、ポリシー違反PCを強制的に切断することも有効。
    - 許可外のプログラム起動、通信起動などについては強制的に停止し、監視システムで掌握可能にしておく。
  - 全部門への適用は困難な場合も
    - 特にIT系企業は、使うソフトウエア、通信が現場ごとに大きく異なる上、技術系の現場では現実に制限が困難なケースも多い
    - ただ、たとえば営業職、事務職、管理職などのPCは比較的対策が簡単な場合もあるので、それらに導入し、その部署のセンサー (警報装置) 代わりに使用する手もありそう。

総合的な監視

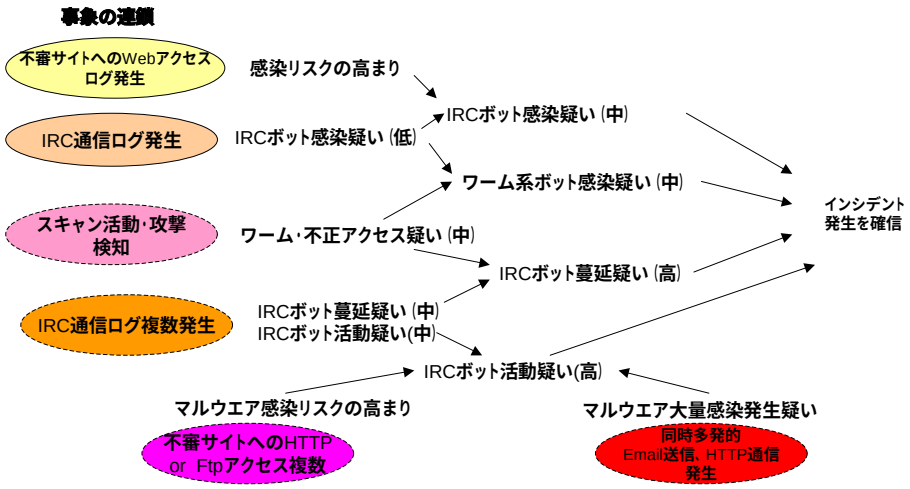
- 様々なシステム、それぞれの監視・管理機能
  - 個別の結果で判断するのではなく、複数のシステムからの情報を補完的に利用しよう
- インシデントの本質を理解する＝敵を知る
  - あるインシデントが、それぞれのシステムにどのように捉えられるかを考える
  - 各システムに同時または時系列的に発生した事象からインシデント像を推測する
- 自社の環境を理解する＝己を知る
  - ユーザの実態や管理状況から見た「リスク」への認識

事象の連鎖と環境要因

Webからのワーム型IRCボット感染の場合



事象からインシデントへ



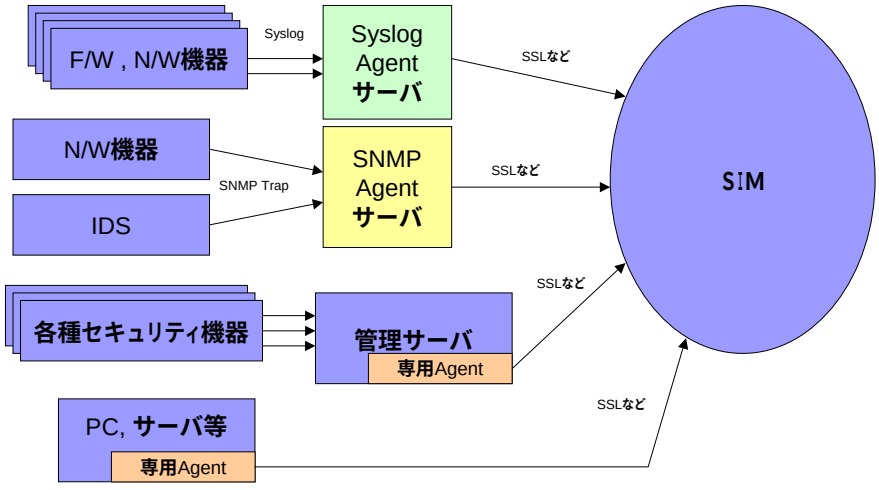
SIMまたはSEMという考え方

- **S**ecurity **I**nfor**m**ation **M**anage**m**ent
- **S**ecurity **E**vent **M**anagement
- 様々な情報を集中管理し、総合的に分析する
  - 様々な環境要因
  - 様々な機器からのリアルタイム情報
  - 分析、判断、レポーティングの自動化
  - 様々な角度からの分析と可視化
- 本当の意味でのUnified Threat Managementかも

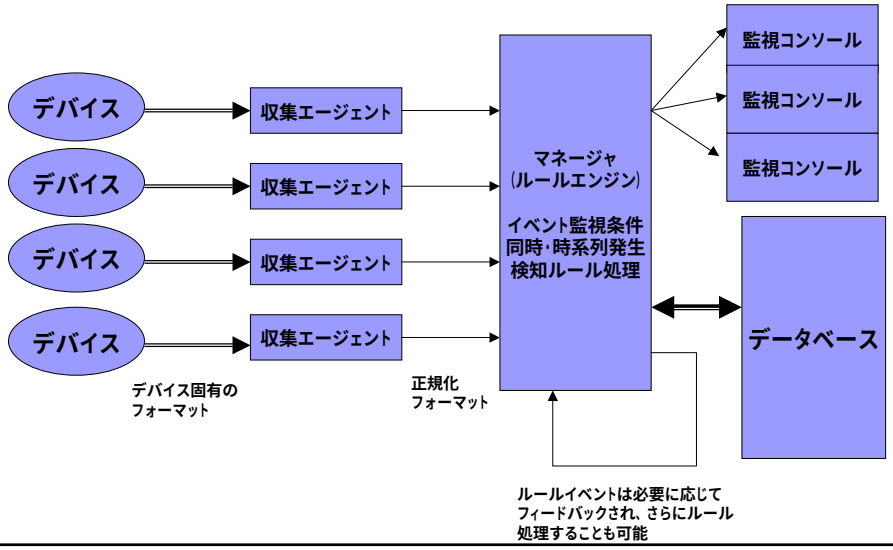
SIMのためのシステム

- セキュリティに関する様々な情報をリアルタイムに分析、管理するためのシステム
  - 様々なセキュリティ機器、コンピュータ、ネットワーク機器・・・からログなどの情報を収集
  - リアルタイムに分析
    - 関連づけされた事象（同時、時系列）の検出
    - 傾向分析と異常の発見
    - インシデントリスクの計算
  - 視覚化による監視とレポート
    - グラフィカルな形でのリアルタイム表示機能
    - 様々な角度からの分析レポート作成機能
  - インシデント対応マネジメント
    - トラブルチケット管理、ワークフローのサポート

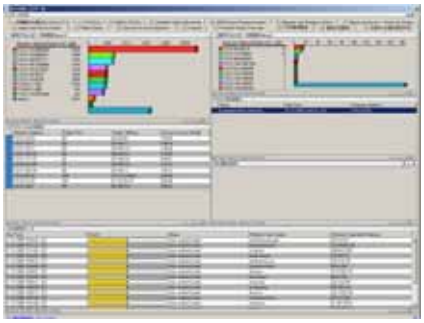
ログ、アラームの収集方法



SIMの構成

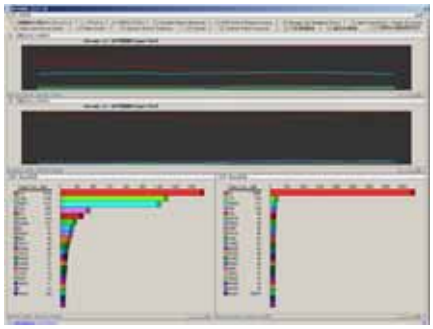


SIMのコンソール画面



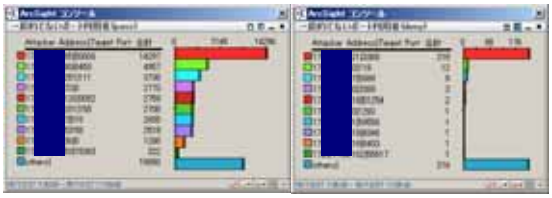
特定目的の監視パネルを並べた
ダッシュボード

通信状況の監視用ダッシュボード
(SIM版百葉箱？)



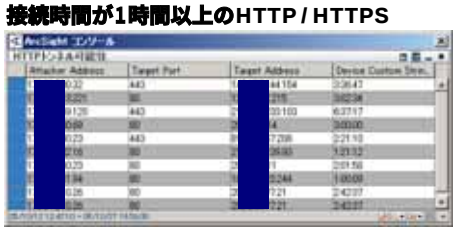
不正通信監視パネルの例

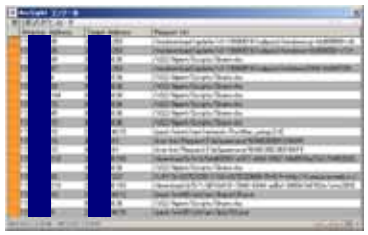
通常あまり使わないポート番号に対する通信監視



インターネットからの実行形式ファイルのダウンロード監視

接続時間が1時間以上のHTTP / HTTPS





深夜時間帯のHTTP(S)通信レポート

Target Address	Target Fqdn	Target Port	COUNT(sourceAddress)
[redacted]		80	1
		80	1
		80	1
		80	1
		80	1
		80	1
		80	1
		80	1
		443	1
		80	1
		80	1
		80	1
		80	1
		80	1
		80	1
		80	1
		80	1
		80	1
		80	1
		80	1
		80	1
		80	1
		80	1
		80	1
		80	1
		80	1
		443	1
		80	1
		80	1
		80	1
		80	1

深夜の1時から6時までの時間帯に、これだけの通信があると、ちょっとびっくりします

実際調査したら、キャッシュサーバの定時巡回がほとんどでしたが・・・ホッ

監視→インシデント対応へ

- インシデント対応を考えるポイント
  - インシデントの「緊急度」
  - インシデントの対象の「重要度」
  - インシデント発生の「確信度」
- たとえば、このような場合は？
  - 財務担当役員のＰＣから6667/TCP通信を検知
    - 緊急度 「中」～「高」 ボット感染疑い
    - 重要度 「最高」レベル
    - 確信度 「高」　業務状況から見てIRC以外の通信である可能性は低い
  - もし、これが営業部の一般社員のＰＣならば？
    - 緊急度 「中」～「高」 ボット感染疑い
    - 重要度 「中」～「高」レベル
    - 確信度 「中」　Ｓｋｙｐｅ等別の通信である可能性も‥‥

インシデント対応

- あらかじめ事態を想定して対応手順を決めておく
  - 複数インシデントの優先順位の考え方例
    - 「緊急度」を第一の判断材料に
    - 同一緊急度の場合「重要度」順に対処
  - 「確信度」の扱いは？
    - 確信度「高」→ 「まずコネクタを抜かせる」
    - 確信度「中」→ 「誤認の可能性を排除：直接調査もしくはヒアリングを最初に実施」
    - 確信度「低」→ 「過去の履歴、周辺環境などを調査して可能性を洗う。引き続き重点的に監視する‥など」

＊これはあくまで一つの考え方の例ですが、このような判断をロジカルに行えるような基準、マニュアルを整備しておくことが重要

外部との連携、アウトソース

- JPCERT/CC, IPAなどの公的団体への相談
  - 状況を正しく把握し、コミュニケーションをとっていくことが重要。
  - あくまで、自分たちが対応する前提で「アドバイス」を求めるスタンスで
  - 相談（情報提供）が対策情報の流通を促す（Give & Takeの関係）
- 専門企業のコンサルティング、緊急対応サービスの利用
  - 実行部隊としては非常に強力。（おカネもかかるけど・・・）
  - ただし、重要な判断は自分たちが行う必要有り。
    - たとえば、状況が悪いため、インターネット接続を一時的に停止するようにアドバイスされた場合に（ユーザ側が）短時間でその判断ができるかどうかが勝負。
    - 判断の遅れがすなわち対策の遅れに繋がるので、ユーザ側の責任も（・・のほうが）大きい点に注意

連絡体制は重要

- セキュリティに関する連絡体制は整備されているか
  - セキュリティポリシーと各種規程類、セキュリティ管理体制、統括部署などが定められているかどうかは重要。
  - 社内（ビジネス）に影響するような対策が必要になった場合の、判断、承認は誰が行うのかを決めておく
    - 一時的にインターネットとの接続を切る・・・
    - 重要なサーバをネットワークから切り離す・・・
    - ある部署のネットワークを切り離す・・・
    - ある担当者のＰＣを接収して調査する・・・
  - ビジネスに影響するような対策のためには部署間の連携と経営層の判断、指揮が必須

対応過程の記録

- インシデントの発見から対応完了までの記録
  - 時系列的な経過と、誰によってどのような対応が行われたかを記録しておくこと
    - ある時点までの対応内容の明確化（次の手を考えるための材料）
    - 同種のインシデントへの対応を迅速化（経験の蓄積）
    - インシデント対応経過の検証と考察→将来的改善
  - 作業承認過程の明確化（指示系統、責任の明示）
    - 誰がその作業を承認したか
    - 誰にその内容を報告したか
    - 誰から指示を受けて作業したか
    - ・・・・・

内部統制面からも重要

まとめ

- マルウエア対策
  - 予防的観点
    - ホスト側でのウイルス・スパイウエア対策、侵入防御、パッチ管理、プログラム起動管理などによる総合的防御
    - ゲートウエイにおけるウイルス・スパイウエア対策、侵入防御
    - ユーザへの啓発活動
  - 発見的観点
    - 感染リスクの掌握とリスクが高い部分の重点監視
    - 通信監視による異常の検知
  - 対応の観点
    - シナリオと（机上シミュレーション）と作業優先度判定基準の整備
    - 指揮・命令、連絡系統の明確化
    - 対外連携の検討（公的団体、他のIRTとの情報交換・共有）
    - 対応の記録

おまけ　（流行なので・・・・）

- 内部統制（IT全般統制）を意識したら・・・？
  - 対策導入過程の透明性
    - リスク評価、対策の妥当性、残存リスクとその許容理由などの検討資料と承認過程の記録を残す
  - 対策の有効性評価
    - 導入した対策が正しく稼働し、運用されていることの記録を残す。（定期的なウイルス発見・駆除状況、パターン、パッチの配布適用状況などのレポート・・・・・）
  - 運用・対応の有効性、効率性の評価
    - 対応記録をきちんと残す。
    - 対応記録のレビューと問題点の改善過程の記録などを残す。

Q＆A　ディスカッション

- ご質問・ご意見
- 経験談、失敗談など　（匿名で・・・(^^)）
- 情報

なんでもどうぞ！！

最新版資料は・・・

- http://www.kazamidori.jp/SECURITY/
  - 上記より各種資料がダウンロードできます。
  - メールによるご質問などは
    - futagi@kazamidori.jp までお願いします。