RSA CONFERENCE 2007

ログとセキュリティイベントの管理と活用

～膨大なログを腐らせないために～

二木真明（ふたぎ　まさあき） CISSP
住商情報システム株式会社
2007年4月25日 – C3-5

最終版：ノート付き

講師自己紹介

- 住商情報システム株式会社
  - 情報セキュリティ・IT統括部　担当部長
    - 情報セキュリティ技術、IT全般統制担当
  - （兼）ITプロダクト＆サービス事業部　担当部長
    - 海外ベンチャー製品の技術評価、各種の技術調査・企画を担当
- NPO　日本ネットワークセキュリティ協会（JNSA）
  - 幹事・技術部会長
- 略歴
  - C, C++, JAVA等のプログラマー・SEとして制御システム、デバイスドライバからビジネスアプリケーションまで幅広い開発に従事
  - FreeBSDをベースとしたファイアウォール製品の開発に従事
  - 2000年より住友商事グループのセキュリティビジネス立ち上げに参加
    - ファイアウォール、SIM製品、Web アプリケーションファイアウォール等の製品立ち上げ
  - 2005年より現職
  - CISSP，　情報セキュリティアドミニストレータ

RSACONFERENCE2007

問題意識

- 「ログをとりましょう」・・・・というけれど
  - いったい何をどこまでとればいいの？
  - どれくらい保存しておく必要があるの？
  - どう使えばいいの？
- 「監視しましょう」というけれど
  - 何をどう監視すればいいの？
  - 監視の精度は結局、担当者のスキルに依存してしまう？
- で、何かあったらどうしよう？

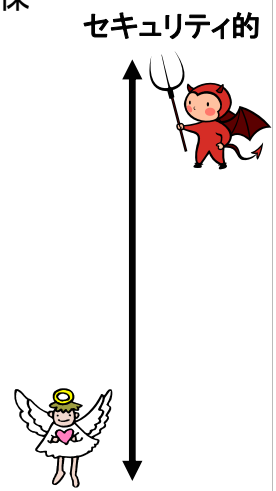
RSACONFERENCE2007

言うのは簡単だけれど、その中身はまったくのケース・バイ・ケース。

目的があって、方法論があるという点をきちんと認識しておくことが重要。

なぜログをとるのか

- セキュリティインシデントに関するトレーサビリティの確保
- セキュリティインシデントとその予兆の察知
- 情報システムの利用状況（傾向・推移）の掌握
- システム障害とその予兆の察知
- システム障害発生時の問題解決



RSACONFERENCE2007

運用管理とセキュリティは表裏一体。しかし、とるべきログの性格は異なる。システムの動きに重きを置くのが「運用管理的」なログ、人や外的要因の動きに重きをおくのが「セキュリティ的」なログというような考え方もできる。

何をログとして記録するのか

たとえば

- 通信や操作の内容、参照、記録した情報の内容
- 不正と思われる行為へのアラーム
- 通信や操作の履歴、許可、拒否情報
- 認証における成功、失敗情報
- システム・サービスの稼働状況（起動、停止など）
- システム上のエラー、アラーム
- システム、通信の負荷状況・推移

RSACONFERENCE2007

セキュリティ・運用、いずれも目的によってログの情報量も異なる。一般に、より情報量の多いログほど、多くの事象（傾向）が読み取れる。ただし、ログから読み取れるすべての事象が、単純にログの中に書き込まれているわけではない。なんらかの解析を行うことで、はじめて浮かび上がる事象も多い。

ログには正常系と異常系がある。異常系ログは障害や不正発見に直結するが、どうしても情報量は限られる。正常系ログは傾向分析によって、より多くの情報が得られる可能性が高い。

ログの種類

- システム利用者／管理者認証のログ（成功、失敗）
  - 管理者認証のログは内部統制上、特に重要
- アクセス（操作）ログ（ネットワーク、システム（アプリ）、データ、施設）
  - システムの設定や構成変更操作に伴うログは内部統制上、特に重要
- ポリシー違反ログ（通信拒否、アクセス拒否、操作拒否・・・）
- アラームログ（攻撃や不正の検知、好ましくない状況発生の警告）
- エラーログ（システム上の不具合等の警告）

RSACONFERENCE2007

これはセキュリティ目的で考えた場合のもの。アクセスログは一般に膨大になるが、情報量も多い。傾向分析によって多くの情報が得られる。

ログのデータ量についての考察

- （例）ファイアウォールのログ（セッションログを含む）
  - 3000人規模のある企業の例を単純計算すると
    - 平均100イベント／秒
    - ＝6000イベント／分　＝360000イベント／時
    - ＝8,640,000イベント／日　＝3,153,600,000イベント／年
    - 1イベント平均256バイトとして、約800GB／年
- （例）ファイルサーバのアクセスログ（Read/Write含む）
  - 1500人規模のある企業の例
    - １日50MB程度（約400,000アクセス）　年20～30GB程度
    - ファイル保存場所としての利用なら意外と少ない
    - PCの作業領域の一部としてマウントしているとログは激増する

RSACONFERENCE2007

実際のデータ量の目安。なかなか難しいが、考え方の目安として。

実際の利用状況を当てはめて考えてみよう。

ログのデータ量についての考察

- （例）メールサーバのログ
  - 3000人規模のある企業
    - 1人平均20通／日として60,000イベント／日　約2100万イベント／年　1イベント256バイトとして、約5．3GB／年
    - 但し、SPAMは考慮していない。激しい場合、1日平均1日数十通以上の可能性有り。（人によってばらつきが大）
    - スパムはフィルタするのが理想だが、していない場合はログは保存しておくべき。（ウイルス感染などの原因究明の際に必要になる）
- （例）Webサーバのログ
  - サイトの性格、外部向けか内部向けかによってログの量は大きく異なる
    - あるSI・製品ベンダ企業（一部上場）の公開Webサイト、平均400,000PV／月のアクセス
    - 1イベント 320バイトとして、約128MB／月、約1.5GB／年
  - イントラネットのポータルサイトなどは、多くなりがち

RSACONFERENCE2007

これも目安として・・・・

ログの保存期間についての考察

- ログ取得の目的と保存期間の考え方
  - セキュリティインシデントやシステム障害、その予兆の発見、傾向掌握
    - 定期的な解析を行う間隔が最短保存期間
  - トレーサビリティの確保（インシデント発覚時の追跡）
    - 一般論として、最低90日程度は必要。保存期間は長期化の傾向
    - 内部統制（IT統制）がらみのログは最低1年以上保存したほうがよい
      - 内部統制テスト時に必要になる場合もある。
      - 監査時に当該年度についての確証を求められることも。
      - どこまで残すかは、監査法人とも相談を
    - 場合によっては数年・・・という可能性も

RSACONFERENCE2007

予防、発見が主体か、事後調査が主体かで、保存期間の考え方は大きく異なる。事後調査主体の場合は、一般に長いほどいいが、ストレージ容量（コスト）とのバランスが重要。

ログの正確性・完全性の保証

- 特に監査対象となりうるログは、欠落、改竄がないことを証明できることが重要
  - たとえば、ログを保存するファイルの単位でハッシュ値を取得して別途保存しておく
    - 安全なハッシュ方式へ移行を（SHA-2 224,256,384,512など）
      - MD5はもうだめ？SHA-1も・・・。実用レベルではまだ使えそうだが
  - ログ管理権限の分離
    - ログ取得対象のシステム（機器）管理者と、ログ（サーバ）管理者を同一にしない
      - ログは原則として別の管理サーバへ転送して管理する
    - ハッシュ値はログとは別に（別の管理者のもとで）保存しておく
      - たとえばログファイルローテーション時に自動生成して複数の管理者にメール送信するなど
  - ログ欠落防止
    - 必要なログが確実に取れるかどうかの検証を（場合によっては負荷試験なども行ってみる）
    - UDPによるsyslog転送はパケット紛失によるログ欠落の可能性に留意。
      - ネットワーク負荷が高い場合は要注意。DoS攻撃による意図的なログ転送妨害も考え得る。
      - 監査用ログは転送するならば、少なくともTCPベースの方法を推奨
        - Syslog-ngなどを利用

RSACONFERENCE2007

ハッシュはMustではないが、ログの完全性を担保するには良い方法。基本原則は管理権限の分離による不正からの保護になる。（ハッシュはある単位でしか付与できないから、リアルタイムログを改ざんされるようなケースは防げない）

ちなみに、MD5ハッシュは、既に十分脆弱として、SHA-1は現実的にはまだ、しばらくは使えそう。（コンピュータの計算能力に依存するので、一般企業や個人のレベルを考えれば・・・）ただ、簡単に、より強力なハッシュをとるツールが手に入るので、これから考えるのであれば、SHA2ファミリーなどを使うのがおすすめ。

ログが欠落しない保証も重要。特にトレーサビリティという意味では不可欠。転送や保存の方法に一考が必要。

ログの収集と保存方法

- 一般的なログ出力先
  - Syslogファシリティ （UNIX系OS、ネットワーク機器など）
    - Syslogサーバに転送して集中管理
  - Windows イベントログ
    - 個別に管理（VISTAでは転送が可能になっている）
    - Syslogに転送するツールもいくつか流通している
  - テキストファイル
    - 個別に管理、もしくはファイルサーバへ転送
    - ちょっとしたツールでSyslogへの転送も可能
  - データベース
    - 個別に管理
- 汎用ログサーバ製品の利用
  - 各種のログを収集して一括管理できるような製品がいくつか流通

RSACONFERENCE2007

個別管理の場合、どうしてもそのシステムの特権に対するガードは甘くなる。集中管理を前提に、ログ管理者をログ取得対象となるアプリケーション操作者やシステム特権保有者と分けることで保全することが重要。

市販の汎用ログサーバ製品を選ぶならば、レポート機能にも着目。また、どうしても出来合いのレポートでは不十分な場合が出てくるので、カスタムレポートを柔軟に作れるような仕組みや、データ構造を持っているものがよいだろう。

取得したログをどう使うか（セキュリティ視点）

- 傾向の掌握
  - 全体的な傾向
  - 部分的な傾向
  - 時系列的な変化
- 違反の検出
  - 規則やセキュリティポリシーに（明確に）違反した行為の発見
- 異常（な傾向）の検出
  - エラー、アラーム
  - 異常や不正が類推される単独または一連の事象
  - （一般の傾向と異なる）特異な傾向＝アノマリー

RSACONFERENCE2007

異常系ログからではなく、正常系ログから異常な事象（アノマリー）を発見するためには、日常的な傾向把握が必須。こうした傾向から外れるような事態を発見することで、異常を見つけ出すことができる。

たとえばファイアウォールの通信ログ（内部→外部）

- 傾向分析
  - アクセス先の集計、アクセス元（ユーザ）の集計
  - 部署別のアクセス先集計、時間帯別のアクセス先集計など
    - Top N だけではなく、Bottom N もとっておくと役に立つことも
  - プロトコル（ポート）別集計
  - アクセス数の24時間変化、一週間の変化などの傾向
  - 特定サイトへのアクセス傾向の集計
- 異常発見の例
  - 特定クライアントから複数の宛先への大量SMTP通信 （ウイルス感染疑い）
  - 特定クライアントから複数の宛先へのping、特定ポート宛通信（ポートスキャン、ワーム感染疑い）
  - 不明なポートや要注意のポート番号を使った通信、深夜、早朝の通信、業務に関係なさそうな海外IPアドレスへの通信など・・・（特定目的のマルウエア感染疑い、トンネル、許可外アプリケーションの使用など利用者の不正利用疑い）
  - 持続時間が数分間以上のHTTP通信（トンネル、Web以外の目的での利用疑い）

RSACONFERENCE2007

ファイアウォールの通信（セッション）ログはまさに宝の山。解析ソフトなどをうまく使うことで、日常的な傾向を把握し、異常を見つけ出すことが可能。

運用面からはアクセスランキング集計はTop Nだが、セキュリティ面を考えると、普段まったくアクセスしないようなサイトへのアクセスは要注意。従って、ランキング下位にあるサイトへのアクセスレポートも役に立つことがある。

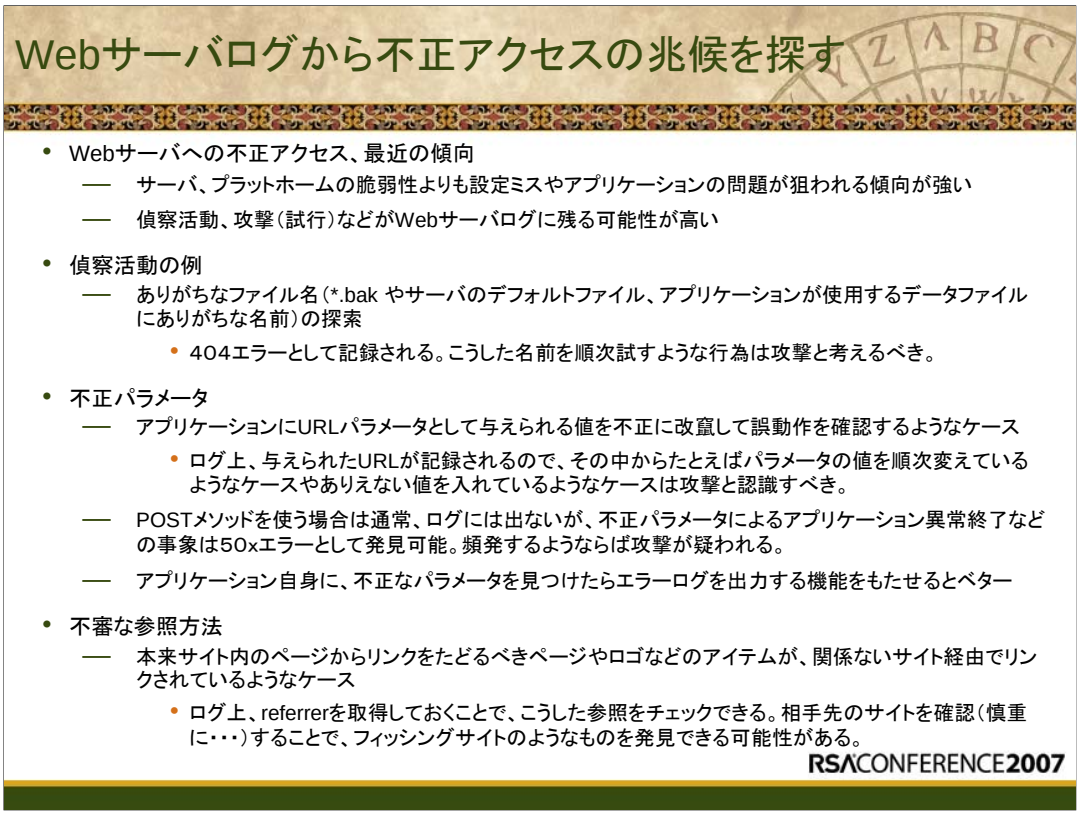
ファイアウォールログからボット感染を探す・・・

- IRCボットの特性
  - IRCサーバを介してハーダー（指令者）と通信
    - ファイアウォール内部からサーバに接続
    - 但し、一般のIRCポート（6667/tcp）が使われるとは限らない
    - よく使われるポート番号 （警察庁資料参照）
      - http://www.cyberpolice.go.jp/detect/pdf/20060316_botnet.pdf
  - ハーダーから指令を受けるまでは、派手な活動はしない
- 見つけ方
  - 6667/tcp, 8080/tcp, 5555/tcp, …. など、よく使われるポートで、米国、韓国、中国などの割り当て範囲のIPアドレス（DNSドメイン逆引き、Whoisなどで調査）宛の通信ログを抽出、利用者に心当たりがあるかどうかのヒアリングを実施（80/tcpが使われるケースもあるので、不審な宛先を持った通信はチェックしておこう）
  - SKYPEのような、P2P的動作をするアプリ、VoIP, ストリーミング系の一部のアプリや、Passive modeのftpなどで、こうした番号がダイナミックに使用される可能性があるので要注意。よく見ると前後の通信から判断できることが多い。
  - ログの定時ローテーションにあわせてログを検索する簡単なスクリプトをsyslogサーバで起動、結果を管理者に送付する、などのしくみは簡単に作れる。

RSACONFERENCE2007

かつて経験したBot系ワーム感染インシデント対応の経験上、ファイアウォールログが問題のトレースに役に立つことがわかった。

一般にあまり使われないポート番号の利用者をチェックしておくことは重要。ただし、一部のアプリケーションはそうしたポートを使ったり、ダイナミックにポートを割り当てるので、紛らわしい。最近のぼっとはもはや6667を使わないので、発見には地道な努力が必要。



Webサーバログのなかでも、referrerはおもしろい情報を提供してくれる。アクセス元のリンク情報はマーケティングにも利用できるが、たとえばフィッシングサイトのように、本物サイトの一部を使いながら不正なコンテンツを組み込むようなものは、参照元から発見できる可能性が高い。

最近、Webアプリケーションへの攻撃が主流になっているが、こうした攻撃は、その前に、ほとんどの場合、ログに偵察活動の記録が特徴的な形で残るので、こまめにチェックしていれば攻撃を予測することもできる。

そういう意味で、Webサーバのログは取得できるものはできるだけ多く取得しておくほうがいいだろう。（エラーログはもちろん、リクエストの内容（URL）、参照元リンク情報（referrer）など）

ファイルサーバのアクセスログから不審な兆候をみつける

- ファイルアクセスログ
  - 個人情報保護法以来、様々なツールが売られているが、その機能は千差万別。
    - トレーサビリティの確保を目的としたものが多い
    - 異常をうまく発見できるものは少ない（目視だより）
  - たとえば、フォルダ内のファイルへの短時間での同一PCからの大量アクセスは、一括コピーなどの操作に起因することが多い。それが個人情報や機密情報などを格納したフォルダであれば、確認しておいたほうがいい場合もある。特に夜間、休日、休憩時間などでの発生は要注意
  - 重要情報を扱う部門に属する社員のアクセス履歴は、定期的に監査する制度があってもいい

RSACONFERENCE2007

ファイルアクセスログを取得するツールは数多く市販されているが、選ぶ場合は、やはり解析、レポート機能を重視すべき。事後トレースの機能だけでなく、むしろ、異常なアクセスを見つけ出すための手段として活用できることが重要なので。

重要になる社内システムのログ

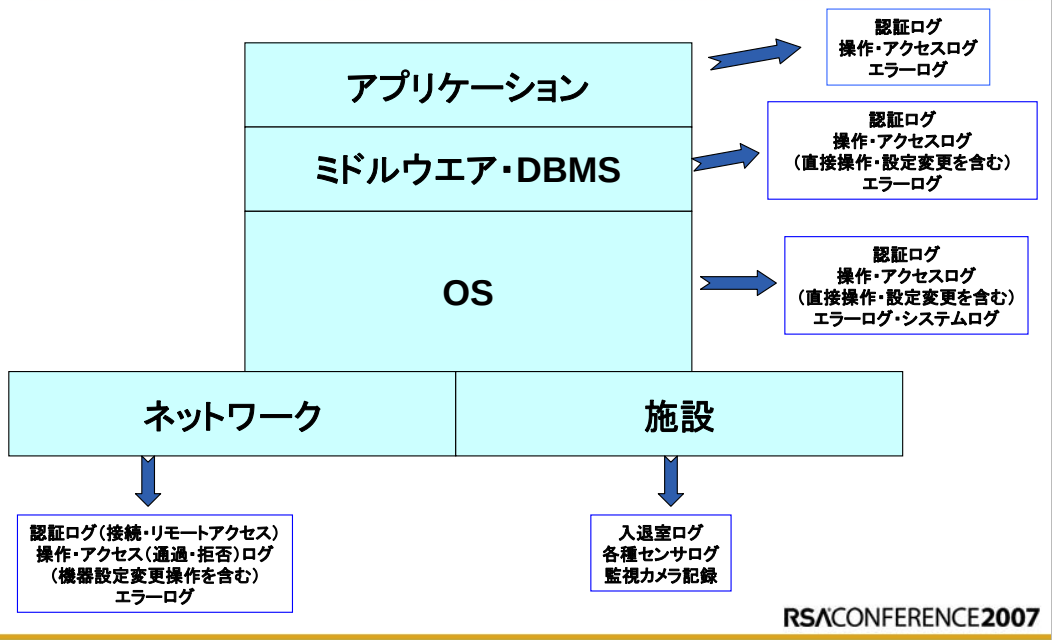
- ERP、CRM・・・・などの社内システムでは財務情報や個人情報を含めた重要な情報を扱う。
- 個人情報保護、内部統制上、重要な情報を扱うシステムに対してユーザが行った操作についてのトレーサビリティ確保は重要事項
  - 認証ログだけでは不十分
  - 入力、出力、データの追加、変更、削除などの操作（成功、失敗）の履歴（少なくとも操作を行った事実と操作対象は記録）
  - アクセス制御違反（エラー）の履歴
- システムやデータに対するリスクアセスメント結果（特に有権限者についてのリスク）に対する統制としてのログ取得と定期的なチェック（牽制）は重要な課題
- アプリケーションと同時にデータベースの安全も担保する必要がある
  - データの直接操作、とりわけ、DBA権限での操作に対する牽制・保護を考慮する必要有り（ログ取得と別管理者による管理など）

RSACONFERENCE2007

なかなか、これまで開発アプリケーションでログをとる、という概念は一般的ではなかったが、今後は重要になってくる。そういう意味で、開発者は意識を変える必要があるだろう。

取り扱うデータ、システムの機能として、そのトレーサビリティをどこまで確保すべきかを十分検討すれば、何をログとして残すべきかは、おのずと明らかになる。

社内システムにおけるログ管理



RSACONFERENCE2007

一つのヒント：EUC（End User Computing）管理とログ

- ユーザ部門が独自に作ったプログラム
  - 表計算やPC用データベースソフトなどのファイル
  - 管理上の課題
    - 処理の正確性の保証
    - 確実な変更管理
    - 正しい利用の保証、不正なもしくは誤っての改変防止
- 変更、利用管理のひとつのアイデア
  - ファイルを共有サーバ上で管理し、アクセスを制限
  - ファイルサーバ側でアクセス履歴を取得
  - 完全ではないが、少なくともアクセスに関するトレーサビリティは確保できる

RSACONFERENCE2007

これは、ある意味でこじつけに近いが、ログ、という切り口から、こういうことも考えられる・・・とう例。

ログ解析の手段

- 市販のログ解析ツール
  - セキュリティ機器用（たとえばファイアウォール用）のツールは、ほぼ必要事項が網羅されている。
  - ファイルアクセスログ取得ツールに付属するレポート機能は、ツールによってまちまち・・・
  - Webサーバ用ツールはどちらかといえば、アクセス解析が中心
  - 総じて、「及第点」でも、かゆいところには手が届かない
- 自作する
  - Perl等のスクリプトを使用して、まずログを整形
    - 必要な要素を抽出してCSV化
  - 表計算ソフト、データベース等に読み込んで検索、レポート化
  - かなり柔軟な処理ができるが、形ができるまでは手間暇がかかる

RSACONFERENCE2007

ちょっとして解析ツールを自作できれば、意外に重要な情報が簡単に得られることも多いので、是非、挑戦してみていただきたい。

例）ファイアウォール（NetScreen）ログの整形

ログの例

```
Apr 25 00:02:14 galaxy galaxy: NetScreen device_id=galaxy  [Root]system-notifica
tion-00257(traffic): start_time="2007-04-25 00:31:34" duration=0 policy_id=7 ser
vice=udp/port:1027 proto=17 src zone=Untrust dst zone=Home action=Deny sent=0 rc
vd=0 src=204.xxx.xxx.235 dst=61.197.xxx.x src_port=50722 dst_port=1027 session_id
=0
```

awk スクリプトの例

```
/action¥=Deny/ {i1=index($0,"start_time="); i2=index($0,"proto"); i3=index($0,"s
rc="); i4=index($0,"dst="); i5=index($0,"src_port="); i6=index($0,"dst_port=");
i7=index($0,"session_id");
if (i5!= 0)
printf "%s %s, %s, %s, %s, %s, %s¥n", substr($0,i1+12,10),substr($0,i1+23,8), su
bstr($0,i2+6,2), substr($0,i3+4, i4-i3-5), substr($0, i4+4, i5-i4-5), substr($0,
 i5+9, i6-i5-10), substr($0,i6+9, i7-i6-10);
        }
```

整形後

```
2007-03-24 00:29:00, 6 , 204.xxx.xxx.x, 61.197.xxx.x, 50722, 135
```

RSACONFERENCE2007

NetScreenファイアウォールの通信ログは、このような複雑な書式で、機械的な処理には向かない。これを、UNIX系に標準のawkで加工して特定の条件にあてはまるログをCSV化するためのスクリプトの例。（ただし、この例はあまり実用向きではないので念のため）

ログのリアルタイム監視

- 定期的なログチェックの意味
  - 表面化していないインシデントの発見
  - ポリシーどおりにものごとが進んでいるかどうかの監査
  - チェックしている・・・という事実を周知することによる牽制効果
  - しかし、発見できた時にはすでに遅い・・・・ということも
    - 大量の情報が流出してしまっていた・・・・・・
    - すでにマルウエアが全社に蔓延・・・・・
- リアルタイム監視の必要性
  - 初動対応がその被害の大きさを決めるようなインシデントも少なくない

RSACONFERENCE2007

何日もたったあとから見つけても、遅かった・・・・という事故の増加。

予知・予防は困難としても、できるだけ早期に発見して被害の拡大を阻止したい・・・。これがリアルタイム監視の主目的。（あまり、予防に重きを置きすぎず、早期発見を重視したほうが現実的かもしれない）

心理的にはリアルタイムで監視しているということ自体が大きな牽制効果を持つ。

ログ監視の手段

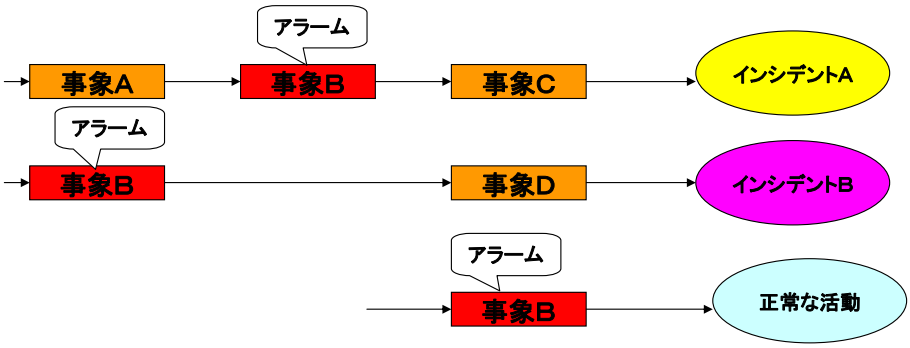
- ログのストリームから特定のパターンを発見する方法
  - Syslogは手段が豊富
    - Swatch を使う
    - Syslog-ngを使う（同時にTCPによる転送を利用可能）
      - 管理者あての警告メール送信などによる異常の通知
  - 汎用ログサーバ製品でも、この種の機能はサポートされていることが多い
  - たとえば
    - ログの中から特定の種類のエラーメッセージを見つける
    - 一定時間内に決められた数以上のエラーや特定のイベントの発生
  - 誤報は覚悟する必要あり
    - 単純なパターン検索では正確なインシデント発見は困難
    - あくまで「注意喚起」としてとらえ、「オオカミ少年」を見捨てない粘り強さが、管理者には必要

RSACONFERENCE2007

ログに対するパターンマッチは単純で簡単だが、初期のIDSなどと同じように誤報、誤認が大量に発生することを覚悟しておいたほうがよさそう。誤報かどうかの判断を毎回、地道に行っていく辛抱強さも必要になる。

アラーム発生時、異常発見時の調査

- インシデントなのか、誤報なのか・・・
  - インシデント発生のメカニズムをモデル化しておく（インシデントシナリオ）
  - インシデント発生過程においてログに記録される「一連の」事象を推定
  - アラームから推測される事象（インシデント）に関連したログを確認

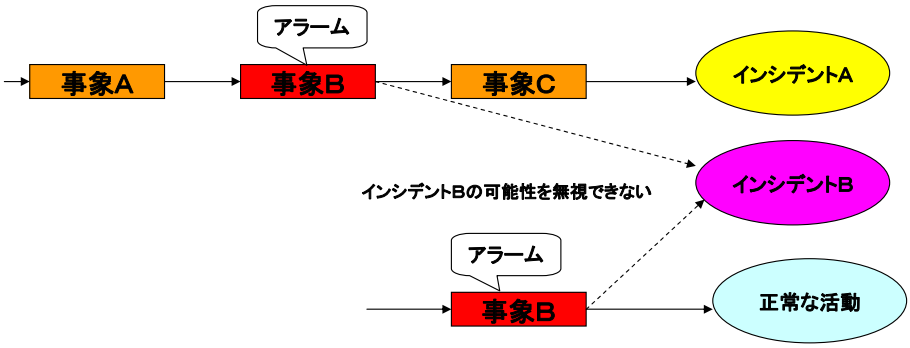


RSACONFERENCE2007

誤報か実際のインシデントかの判断をスムーズにおこなうためには、想定されるインシデントを熟考して、そのシナリオを明らかにしておく必要がある。それに基づいて、前後で発生すべきイベントを探すことが早道。

でも実際は・・・・

- 経験とカンが必要になる場合が多い・・・・のだが・・
  - ―「経験値」を頼りすぎると危険 （判断が個人に依存、説明不能・・・）
  - ― 判断過程と判断のための情報をできるだけ「見える化」すること



RSACONFERENCE2007

ただ、これは経験値に大きく左右されがち。熟練者が必要。

ただし、熟練者に頼りきるのではなく、少しずつ、そのノウハウや実際に処理した手順を文書化（シナリオ化）するなどして残していくことは重要。

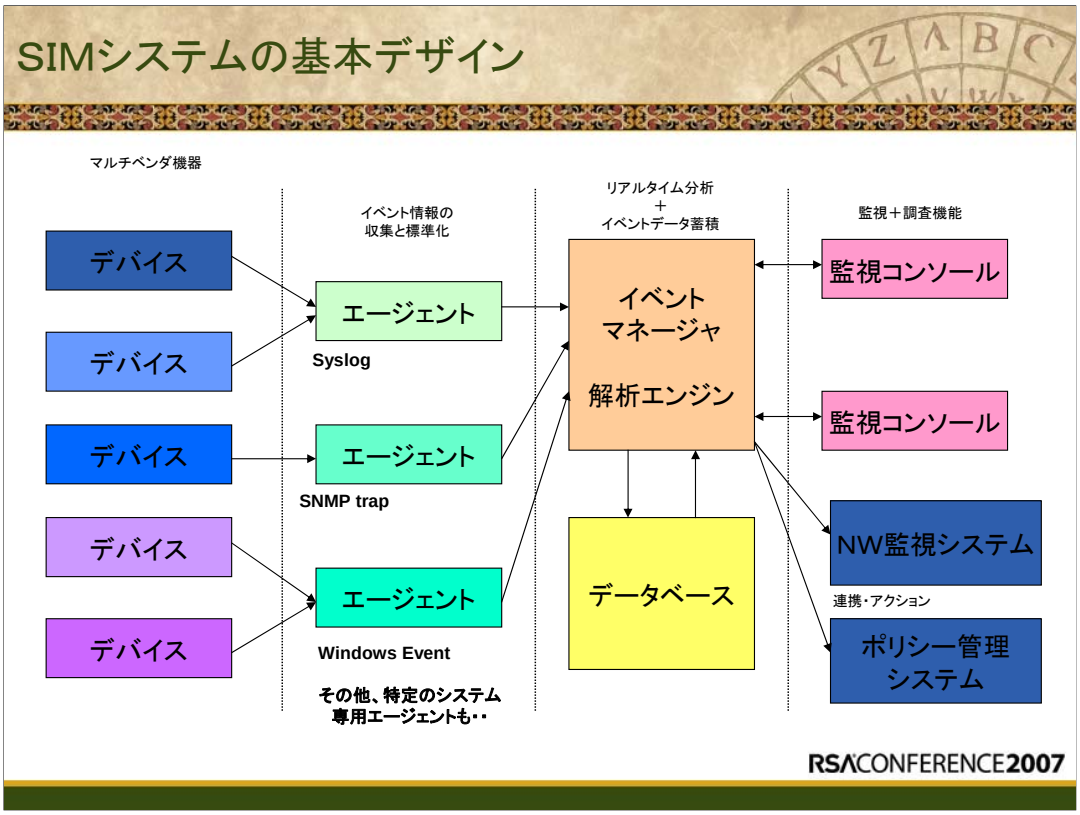
SIM製品を使う

- **SIM**（Security Information Management）製品の主な機能
  - 汎用ログ・アラームサーバとしての機能
    - 各種のログ・セキュリティイベントをリアルタイムで収集、標準フォーマットに変換（正規化）してデータベースに格納
  - イベント処理ルールによる監視機能
    - 一連のイベント連鎖を発見するルールを作成可能
    - 発見したイベント連鎖に対し各種のアクションを実行可能
      - アラームの発生、プログラムの実行、他システムとの連携・・・
  - 汎用的なログ・イベント解析・集計エンジン
    - リアルタイムに統計処理を行いながらダッシュボードに状況を表示
    - 過去のイベントに対する検索、解析、統計処理機能
    - 各種の条件でのレポート自動生成

RSACONFERENCE2007

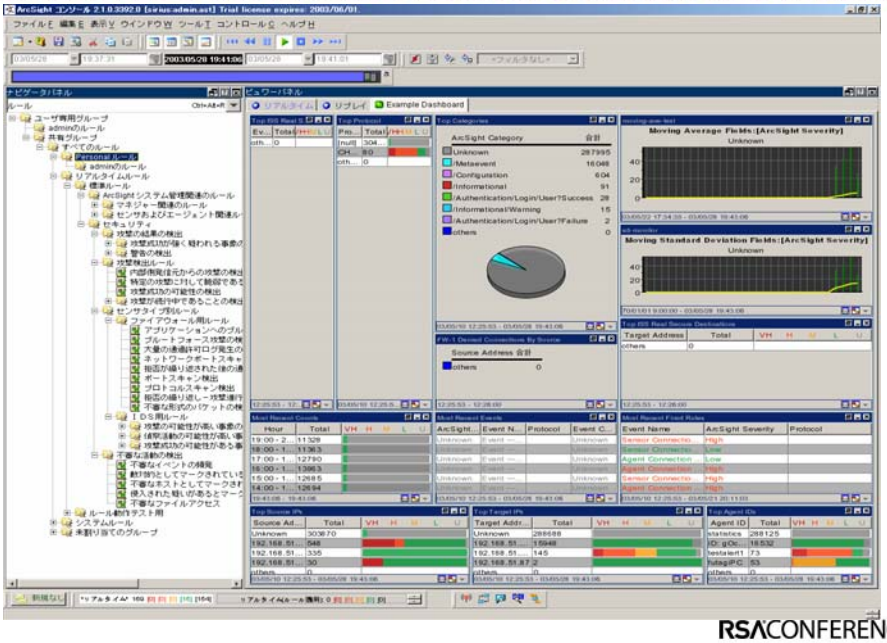
ある程度シナリオができ、解析過程をパターンかできるならば、それを自動化する方法もある。それが、SIMである。

SIMを使うためには、インシデントシナリオの蓄積が不可欠であることに注意する必要がある。あるインシデントにおける、セキュリティイベントの種類や時系列的な発生順序が明確でなければ、自動化は難しい。



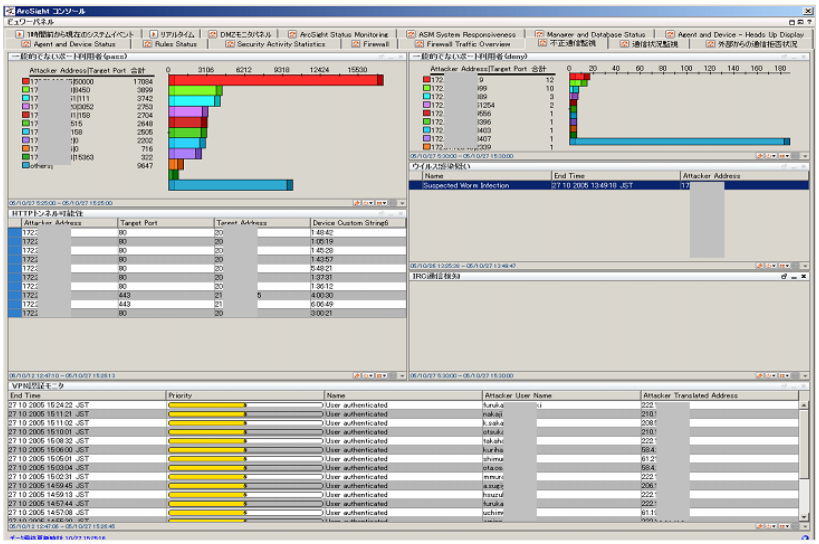
エージェントによるログの正規化（マルチベンダのログを専用フォーマットに変換して統一的に管理する方法）が大きなポイント

SIM監視コンソールの例 （ArcSight Enterprise Security Manager）



ArcSight社製 ESM のコンソール画面例（これはデモ画面。実際の使用では、監視対象に応じてカスタマイズされる）

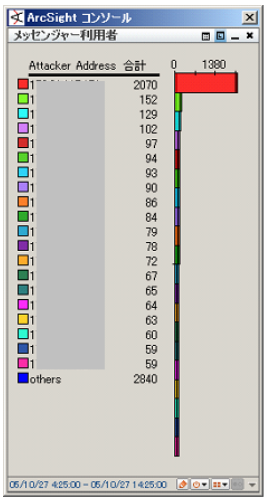
SIMによる可視化の例

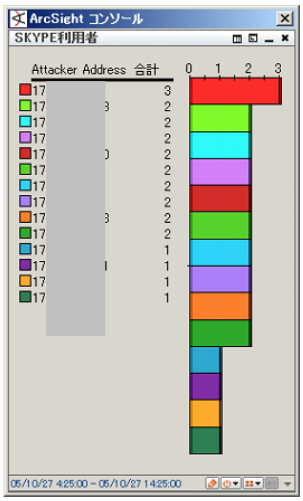


RSACONFERENCE2007

カスタマイズされた監視パネルの例

特定アプリの検出パネルの例





IM検出

特定のIMプロバイダサイトに対する通信をIPアドレスごとに集計して表示

SKYPE検出

Proxyのログから、URLにSKYPE固有のパターンを含む通信を検出して集計

または、IDSを使って検知

RSACONFERENCE2007

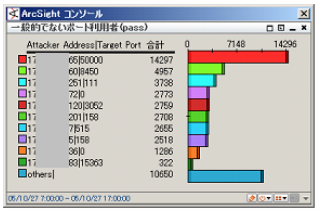
特定のアプリケーション利用者検出。

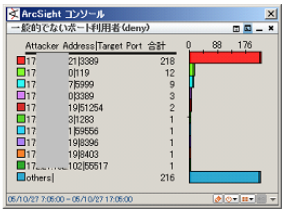
外部通信ツールの利用者は他の利用者に比べて情報漏洩、流出のリスクが高いので、重要な情報を扱う組織では、こうした掌握が必要になるかもしれない。

SKYPEやIM利用者を特定しておくことはボット、スパイウエア発見（特殊なポート番号使用者検出）における誤認可能性が高いユーザの洗い出しにも役に立つ。

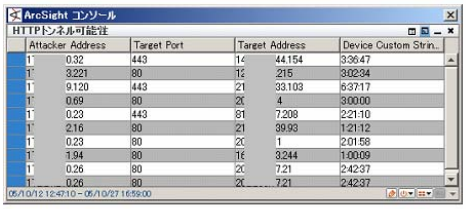
不正通信監視パネルの例

通常あまり使わないポート番号に対する通信監視

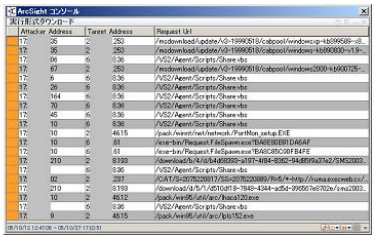




接続時間が1時間以上のHTTP / HTTPS



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



RSACONFERENCE2007

異常やリスクが高い操作のモニタリング例

（不正通信の探索例）深夜、休日時間帯のHTTP通信

- 人がいない時間帯のHTTPは機械的に行われているケースが多い
  - ―キャッシュサーバもしくは類似ソフトウエアの自動巡回
  - ―市販常駐ソフトウエアなどの自動更新
  - ―宛先からまず判断し、次に、利用者調査（ホストの種別や利用ソフトウエアなど）

RSACONFERENCE2007

たとえば、HTTPの通信異常を見つけるという意味での、ひとつの例

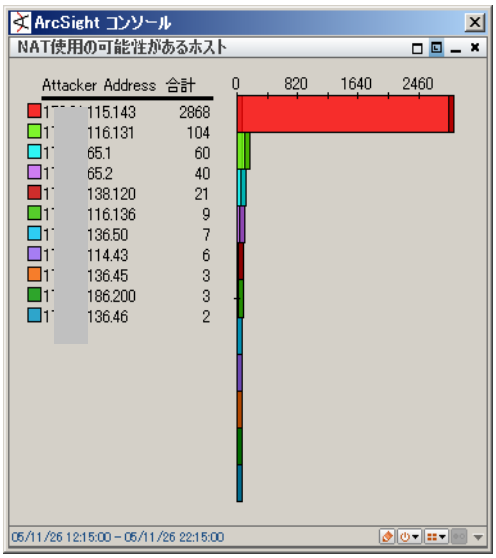
深夜時間帯のHTTP(S)通信レポート

Target Address		Target Fqdn	Target Port	COUNT(sourceAddress)
2	37	.	80	1
2	56	.	80	1
2	03	.	80	1
2	68	.	80	1
2	183	.	80	1
2	.41	.	80	1
2	.216	.	80	1
2	.21	.	80	1
2	.162	.	443	1
2	.216	.	80	1
2	.254	.	80	1
2	113	.	80	1
2	.182	.	80	1
2	3	.	80	1
2	5	.	80	1
2	.138	.	80	1
2	.32	.	80	1
2		.	80	1
2		.	80	1
2	0	.	80	1
2	190	.	80	1
2	60	.	80	1
2	25	.	80	1
2	253	.	80	1
2	253	.	443	1
2	177	.	80	1
2	.144	.	80	1
2	.7	.	80	1
2	.230	.	80	1
2	.114	.	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

隠し（NAT，Proxy）の発見



＊社内ネットワークに接続されたNATデバイスは、ユーザの挙動を隠蔽して、インシデント対応を難しくする。

＊NAT（NAPT）デバイスの多くが発信元ポートの初期値として大きな値を取ることに着目。また、初期値が小さくても、多数のホストを隠蔽しているNATデバイスでは、ポート番号の消費が大きく、結果的に高い値が使われる。

＊この例では発信元ポート番号に32768以上の値を使った通信の発信元を調べている

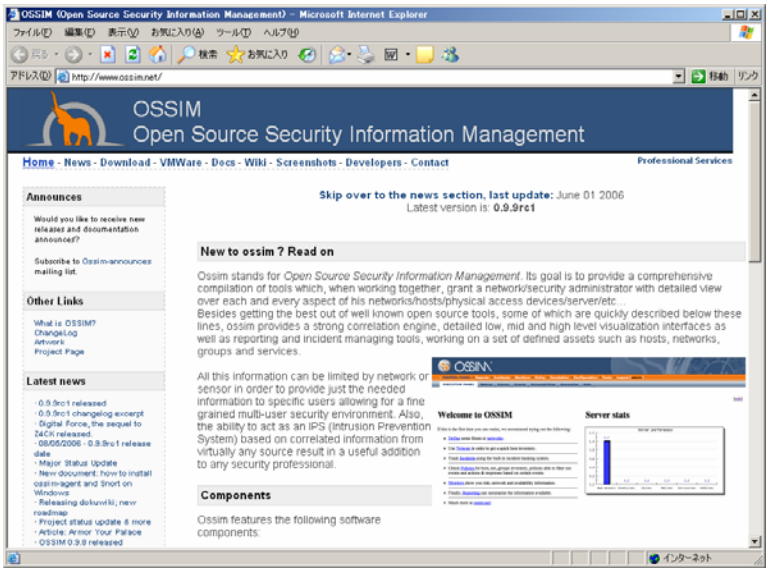
RSACONFERENCE2007

NAT（NAPT/IP Masquerade)やProxy　で処理された通信はその特性上、どうしても大きな値を持つ発信元ポート番号を持つことが多くなる。

これは、単純にそうした通信を発生させているホストを洗い出すもの。通信発生頻度が高いほど、こうした共用デバイスである可能性が高くなる。

オープンソースのSIM

http://www.ossim.net/



RSACONFERENCE2007

SIM製品は一般には、導入・構築を含めて、かなり費用がかかるので、なかなか中小規模の企業での導入は難しい。パワーユーザ向けにはこうしたオープンソースのSIMもあるので、小規模な導入にはいいかもしれない。

SIM製品の発展方向

- リアルタイムのリスク評価と可視化を重視する方向
  - IT資産管理との融合による資産別の状況掌握
    - 重要度、脆弱性、依存関係など
  - 発生した事象（脅威）と各資産との関連づけ、リスク指標値の算出
  - 人的リスクの取り込み
    - チェックリストやアンケート評価等の結果をもとにしたリスク評価のデータベース化と従来の監視機構によるリスク評価との結合
  - ダッシュボード機能の強化
    - サマリを表示できるマネジメントダッシュボードの機能
- SIMからESM（Enterprise Security Management）へ

＊入れてすぐ使う・・・というわけにはいかない。まず、自分たちの管理のためのシナリオを明確にし、その上で使い方を考える

RSACONFERENCE2007

最近は、リスクマネジメントをリアルタイムにやろう、という傾向が米国で強まっており、SIMもそうした傾向に乗せられている感じがする。さらに、セキュリティリスクと内部統制リスク管理の融合もはかられつつあり、こうした昨日はどんどん複雑化しているのが実情だ。

そういう意味では、いきなりSIMを導入しても使い切れないことも多くなりがち。まず、どのような管理（リスク管理を含めて）をするのかを明確にしてから、それを実現できる製品を選ぶことが重要だろう。

インシデント対応体制の重要性

- 監視はできても、発見したインシデントに対応できなければ意味がない
  - 最低限のインシデント対応体制（IRT/CSIRT）は必要
    - IRT（Incident Response Team）リーダーの要件
      - セキュリティ技術とマネジメントの ”Generalist” であること
        - 特定の技術のみに強くてもダメ。むしろ、そういう人たちと、きちんと「お話し」ができ、判断できる幅広いスキルが必要
        - たとえば、米国ではCISSP™ホルダーであることを要求されることも多い
      - 交渉上手であること
        - インシデント対応の過程で、様々なコミュニケーションが必要になる
        - 場合によっては、「社内政治」を理解することも要求されるかもしれない。（本来はCISOの仕事なのだが・・・）

RSACONFERENCE2007

最後に、ここは重要なポイント。

ログの監視から問題が発見できても、それに対処できる体制がないとだめ、というお話。

一般企業が、必要な専門技術者をすべて抱えるのは難しいが、少なくともセキュリティ全般（技術面を含め）にある程度の深みで広い知識をもった専門家を1～2名は雇っておくべきだ。

こうした専門家は、社内のセキュリティ管理を技術面で企画するだけでなく、インシデント対応においては、たとえば専門業者や関係者をとりまとめて調整する役割もはたす。そのためには、ある分野の専門技術者とも会話ができ、マネジメントもある程度できる人材が不可欠となる。

インシデント対応のありかた

- インシデントシナリオと対応マニュアルの整備を
  - インシデント対応は時間との競争。シナリオ化できるインシデントはできるだけ洗い出して、対応方法をマニュアル化しておく
  - 対応に他部署を巻き込む必要があれば、あらかじめ対応方法を協議しておく
  - たまには「防災訓練」も
- 内部ですべてできる組織は少ない
  - 専門性の高い作業レベルでは専門企業へのアウトソースを
    - シナリオのない特殊なインシデントへの対応についてのコンサルティング
    - マルウエア感染や、不正アクセスへの技術的対応
    - コンピュータフォレンジック
  - 但し、対応の「指揮」「判断」は必ず、組織のIRTとその管理者が行わないとダメ

RSACONFERENCE2007

インシデント対応を迅速に行うためには、かなりの経験を要する。すべてを経験にゆだねてしまう危険を避けるには,少なくとも可能性がある重大なインシデントを洗い出し、シナリオ化して、対応手順を決めておくことが必要だろう。

必要な技術的対応が社内で困難ならば専門業者を巻き込めばいい。ただし、専門業者は「決断」は一切しない。選択枝を専門業者から提示されたときに、タイムリーに決断できる人材、体制が不可欠である。

監視を含めたアウトソースの場合

- アウトソース先の監視対象、内容などについて十分に精査を
  - まず、自分たちのニーズ（要求事項）ありきで考える
  - インシデントシナリオを考え、その監視方法について、アウトソース先と協議を
  - 最終的に、ニーズを満たせるアウトソース先を選定する
- 連絡と対応のための体制の整備
  - アウトソース先との連絡、通知窓口の設定
  - インシデント対応体制の整備
    - 監視の精度がどれだけよくても、自分の組織に対応できる体制がなければ「宝の持ち腐れ」になりかねない
    - アウトソース先は、選択肢を提示することはできるが、判断はできない（対応についての最終責任は持てない）ことに留意。（自組織の管理責任までは移転できない！！）

RSACONFERENCE2007

これはアウトソース先選びの鉄則。

まとめ

- ログを「なぜ」とるのかを考えよう
- ログを「どう」使うのかを考えよう
- 「何」を「どのように」ログにとるかを考えよう
- 「いつ」ログをとって「いつまで」保存するのかを考えよう

- とったログは、きちんと「チェック」しよう
  - そのための道具も用意して・・・・（人頼みでは辛い・・・）
- インシデントへ対応のための体制作りも忘れずに！！

RSACONFERENCE2007

ご清聴ありがとうございました

- ご質問

- SIM関連記事サイト
  - http://www.atmarkit.co.jp/fsecurity/special/71sim/sim01.html

- 資料庫： http://www.kazamidori.jp/SECURITY/

RSACONFERENCE2007