Internet Week 2002 T13

不正アクセスの手法から考える監視技術

～雑音の除去と行動分析からリアルタイムプロテクションまで～

株式会社ラック
西本 逸郎
itsuro@lac.co.jp
http://www.lac.co.jp/security/

講師紹介

西本（にしもと） 逸郎（いつろう）

昭和33年	福岡県生まれ
昭和59年3月	熊本大学工学部土木工学科中退
昭和59年4月	情報技術開発株式会社入社
昭和61年10月	株式会社ラック入社　一貫して通信系ソフトウェアやミドルウェアの開発に従事。

その後、ドイツのシーメンスニックスドルフ社と提携し、オープンPOS（Windows POS）を世界に先駆け開発・実践投入。堅牢なシステムを如何に作って維持していくかをテーマにセキュリティ対策という観点で邁進中。

情報セキュリティ対策をテーマに展覧会などで講演会や専門雑誌への執筆を多数実施

株式会社ラック セキュアネットサービス事業本部 取締役本部長
特定非営利活動法人 日本ネットワークセキュリティ協会 理事

第一章 不正アクセス手法とセキュリティ監視

■手法のカテゴリとセキュリティ機能の関係

手法（脆弱性）	説明	抑止	予防	防御	検知	回復
実装上の弱点を利用	所謂、OS、サービスアプリ ユーザアプリの セキュリティホールや設定ミス等	△	◎	○	◎	※
運用上の弱点を利用	安易なパスワード パスワード等が漏れている ウィルス等	△	◎	○	◎	※
技術仕様上の弱点を利用	Flood系攻撃 ICMP、UDP等成りすまし SMTP成りすまし等	×	×	×	◎	※
権限を乱用	業務上の目的以外に権限を行使 顧客情報の横流しなど	◎	×	×	◎	※

セキュリティ対策5大機能

機能	概要	
抑止	脅威の発生そのものを押さえ込む	寄せ付けない
予防	脅威が発生しても ダメージとならないように脆弱性を無くして…	頑丈な扉 強固の鍵
防御	脅威が発生しても ダメージを受けないように防御する	電気ショック 応酬・撃退
検知	脅威の発生若しくはダメージの発生を検知	被害を見付ける 侵入者を見付ける
回復	ダメージから回復する	復旧 対処

■手法のカテゴリと検知方法

実装上の弱点を利用		
センサー	攻撃検知	侵入検知
ネットワーク型 IDS	攻撃パターン、異常パケット サービス、脆弱性 バナースキャン等	不審なコネクション
ホスト型 IDS		ファイル改竄、権限の行使、 ログイン、バックドア等
ホストログ	不審なログ	作業手順突合せ
ファイアウォール	異常パケット	不審なDrop

■手法のカテゴリと検知方法

運用上の弱点を利用		
センサー	攻撃検知	侵入検知
ネットワーク型 IDS	ブルートフォース	不審なコネクション
ホスト型 IDS	ログインエラー	ファイル改竄、権限の行使、ログイン、バックドア等
ホストログ	ログインエラー	作業手順突合せ
ファイアウォール	短時間での大量Accept	不審なDrop

■手法のカテゴリと検知方法

技術仕様上の弱点を利用		
センサー	攻撃検知	侵入検知
ネットワーク型 IDS	Flood系、Smarf系等	
ホスト型 IDS		※別途サービス稼動監視 応答監視
ホストログ	大量のエラーメール受信	
ファイアウォール	大量のDrop等	

■手法のカテゴリと検知方法

権限を乱用		
センサー	攻撃検知	侵入検知
ネットワーク型 IDS		
ホスト型 IDS		権限の行使のアノマリ検知
ホストログ		アクセスログから アノマリ検知
ファイアウォール		

第二章 セキュリティ監視の肝

■セキュリティ監視といえばIDS？

セキュリティ監視といえば、ネットワーク型IDS監視を想像するが？

既存のIDSだけでどこまでのことが出来るのだろうか？

基本的にネットワーク型IDSは誤報は免れない

となると、アプローチは、、、

1. 誤報の可能性のあるシグネチャーでは検知しないようにする
   ⇒ えっ！なに？

2. 対象ネットワークの特性に合わせチューニング（ポリシー設計）を行い監視する
   ⇒ シグネチャー（検知パターン）の頻繁な更新、構成の変更　大丈夫？

3. IDSで検知したイベントを都度誤報かどうか確認しながら監視する

■作戦

1. 意味のあるネットワーク分断（セグメンテーション）

2. セグメントの特性に合わせたログ設定
   特にファイアウォールやサーバのログ設定

■ファイアウォールの原点

1. ネットワークセグメント（部屋）を意味のあるものに分けること
   何故分ける必要があるのか？
   → セグメンテーション

2. アクセス制御を行うこと
   基本的なアクセス制御は？
   → 基本ネットワークポリシー

3. 記録をつけること
   なぜ？目的は？
   → ログ管理

■セグメンテーション

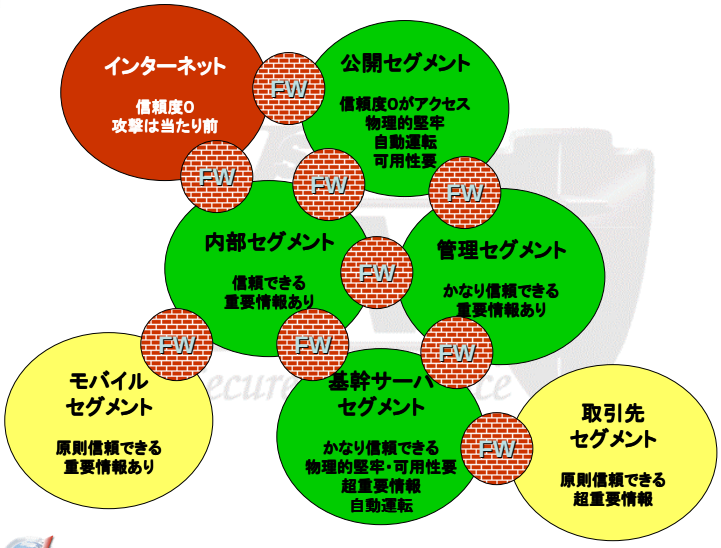
人
情報カテゴリ
機能（サービス）
適用できる規則
物理的条件
・・・・

お客様、社員、経営者、管理者、攻撃者、、、
関係者以外機密情報、社外秘情報、顧客情報、、、
一般向け、特定のお客様向け、社員向け、、、
就業規則・社内ポリシーが適用、評価基準、、、
物理的セキュリティ状態

鑑みてネットワークを分断する

ＣＩＡ（機密性、完全性、可用性）

■セグメンテーション 例



■アクセス制御 基本ネットワークポリシー

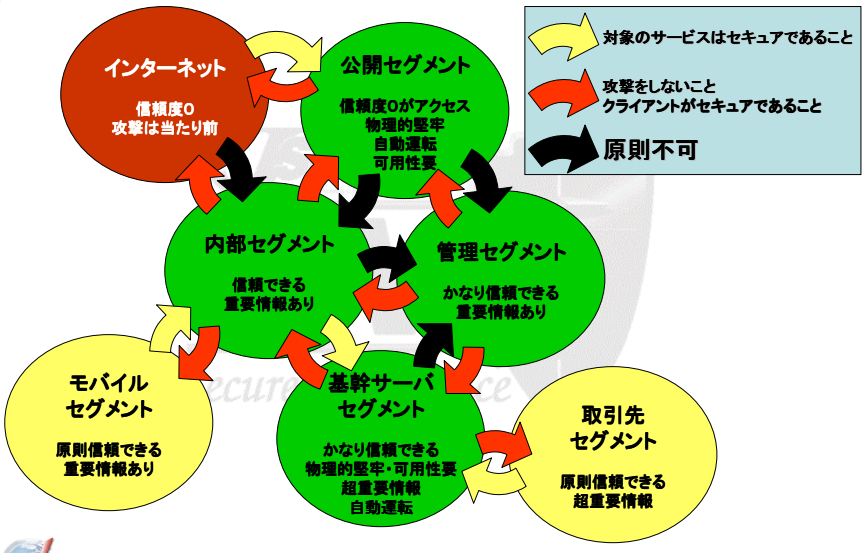
セグメント間でやり取りすることで想定される脅威（リスク分析）から、基本となるネットワークポリシー（セグメント間アクセス制御基準）を決める。

例：

1. 信頼度が低いセグメントへサービスを提供する場合は、脆弱性を排除しておく必要がある
2. セグメント外のサービスを利用する場合は攻撃しないようにする
3. セグメント外のサービスを利用する場合は受動攻撃を受けないようにクライアントをセキュアにしておく

→ 重要度に応じて、登録、変更手続きを決めると良い。

■基本ネットワークポリシー 例



■ログ管理

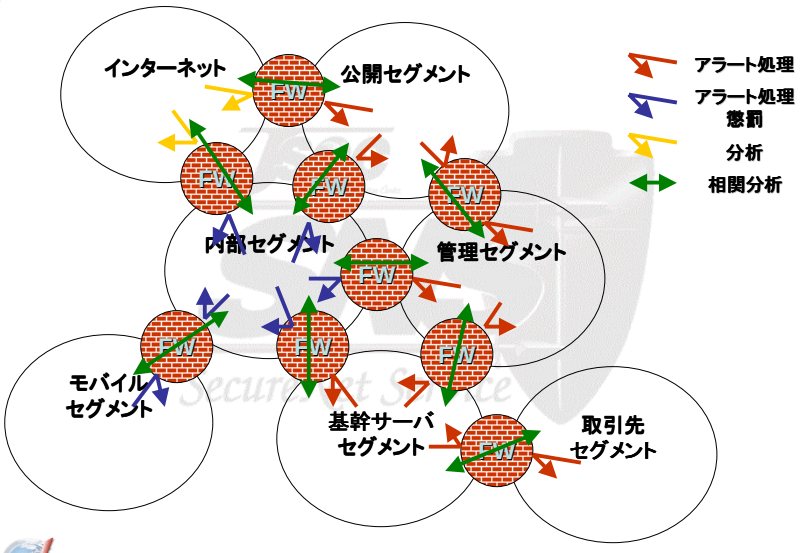
ログの種類
セグメンテーションし基本ポリシーを決めているのでログを分類できるようになる。

【例】
1. 自動運転しているセグメントで何故Dropが起きるのか？
   → アラート インシデントレスポンス
2. 規則を守るはずのところで何故Dropが起きるのか？
   → アラート インシデントレスポンス・懲罰
3. 攻撃があるのが当たり前のところでは、Dropは当然発生
   →データマイニングや相関分析が必要
4. 許可ログは、基本的にはストックして置けばよい。何か有ったときの調査用。
   →上記ログと併せて、分析

当然のことながら、ログは改竄されない仕組みが必要。

第二章 セキュリティ監視の肝

■ログ管理 例



第二章 セキュリティ監視の肝

ファイアウォールの基本的な機能は

⇨ **防御**

アクセス制御を行うことで脆弱性を持ったサービスが有っても防御する

セグメンテーションを行い基本ポリシーを持ちまた運用することで

⇨ **検知**

⇨ **回復**

アラート処理が出来るようになり、検知し回復を図り、

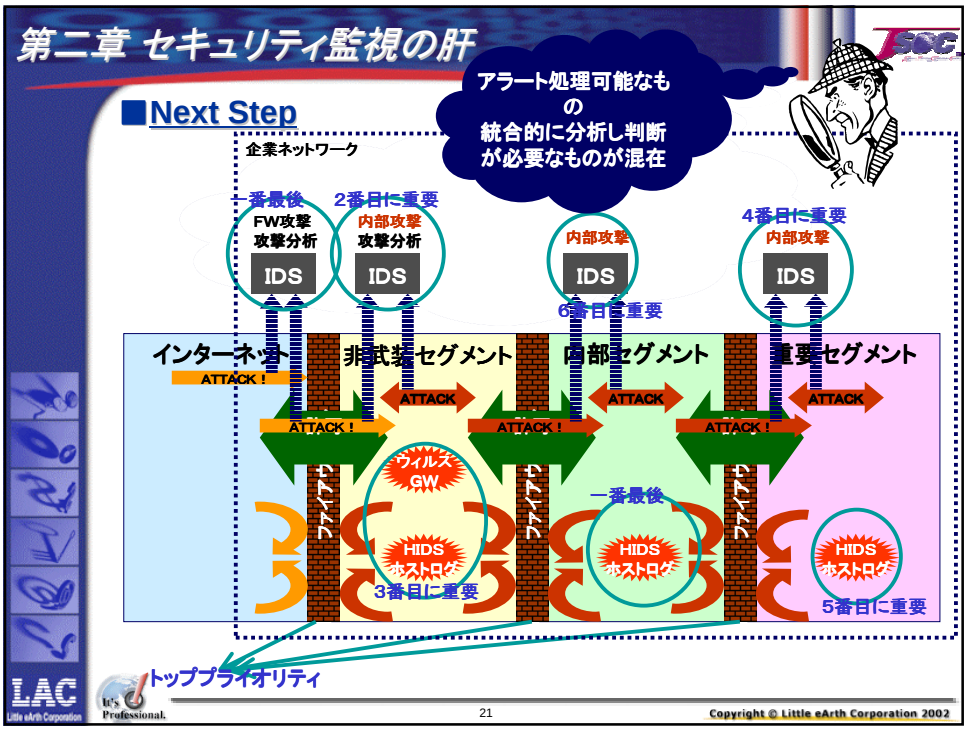
⇨ **予防**

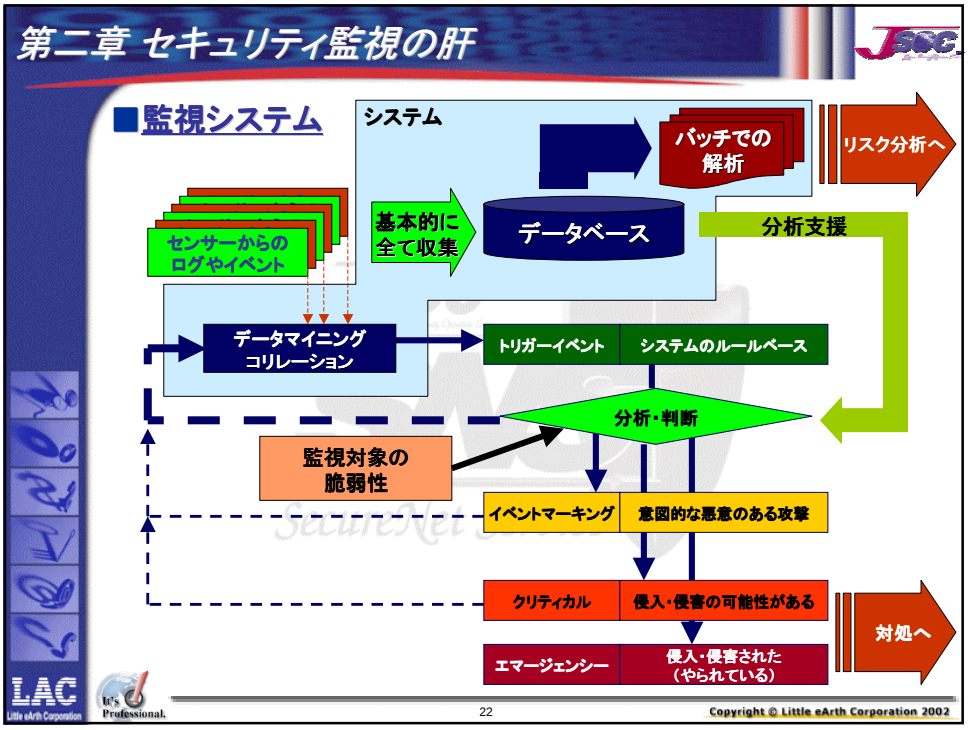
統合分析を行い傾向を分析することで、予防を図り、

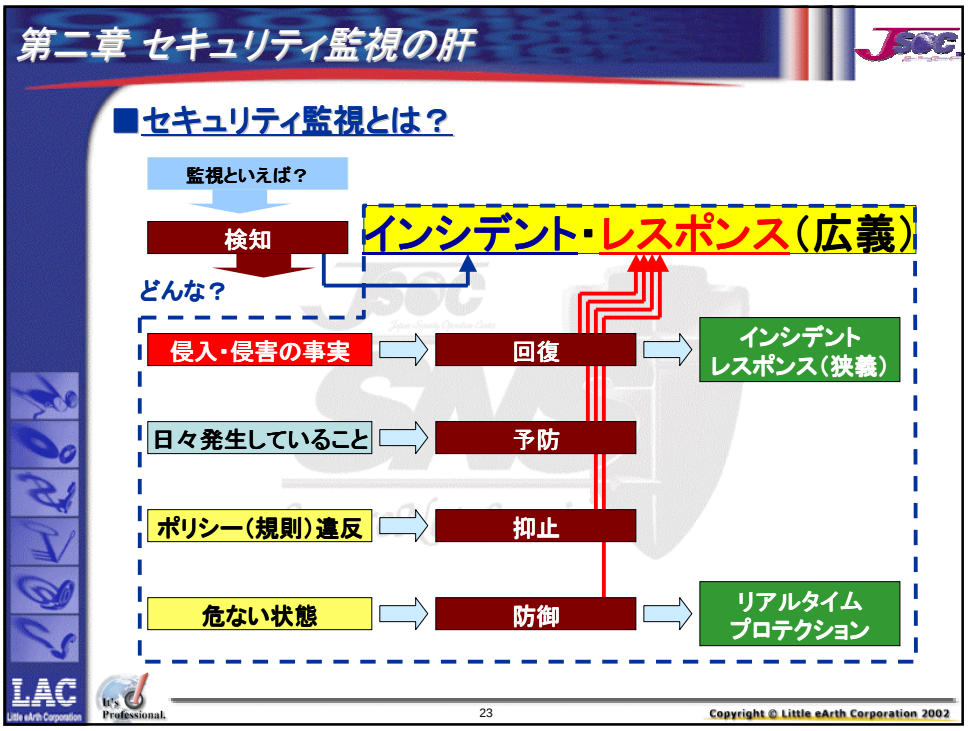
⇨ **抑止**

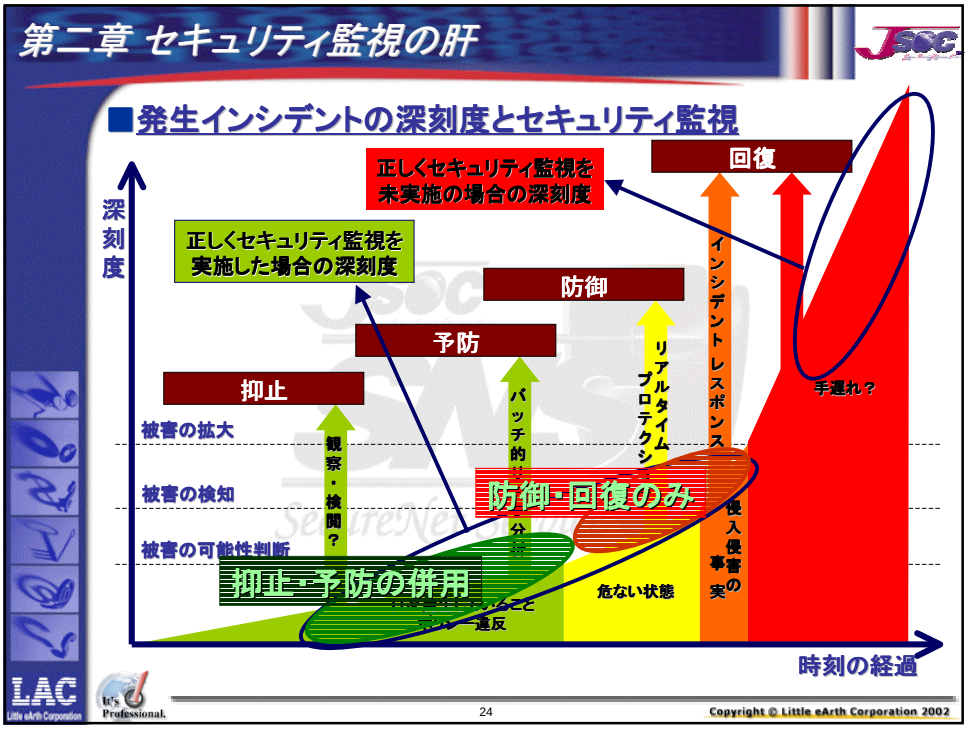
規則違反を発見し、またログを管理していることで、抑止を図る。

※ 各々の対策には仕様上限界がある。
適用場所によっては、これで十分である場合もあるが、他のセキュリティ機器を併用していくのが望ましい。


第二章 セキュリティ監視の肝
Next Step
アラート処理可能なもの
統合的に分析し判断が必要なものが混在
企業ネットワーク
一番最後
FW攻撃
攻撃分析
IDS
2番目に重要
内部攻撃
攻撃分析
IDS
内部攻撃
IDS
6番目に重要
4番目に重要
内部攻撃
IDS
インターネット
非武装セグメント
内部セグメント
重要セグメント
ATTACK！
ATTACK
ATTACK！
ATTACK
ATTACK！
ATTACK
ATTACK！
ファイアウォール
ファイアウォール
ファイアウォール
ウィルスGW
HIDS
ホストログ
3番目に重要
一番最後
HIDS
ホストログ
HIDS
ホストログ
5番目に重要
トッププライオリティ
LAC
Little eArth Corporation
It's Professional
21
Copyright © Little eArth Corporation 2002


第二章 セキュリティ監視の肝
監視システム
システム
バッチでの解析
リスク分析へ
センサーからのログやイベント
基本的に全て収集
データベース
分析支援
データマイニング
コリレーション
トリガーイベント
システムのルールベース
分析・判断
監視対象の脆弱性
イベントマーキング
意図的な悪意のある攻撃
クリティカル
侵入・侵害の可能性がある
対処へ
エマージェンシー
侵入・侵害された
（やられている）
LAC
Little eArth Corporation
It's Professional
22
Copyright © Little eArth Corporation 2002

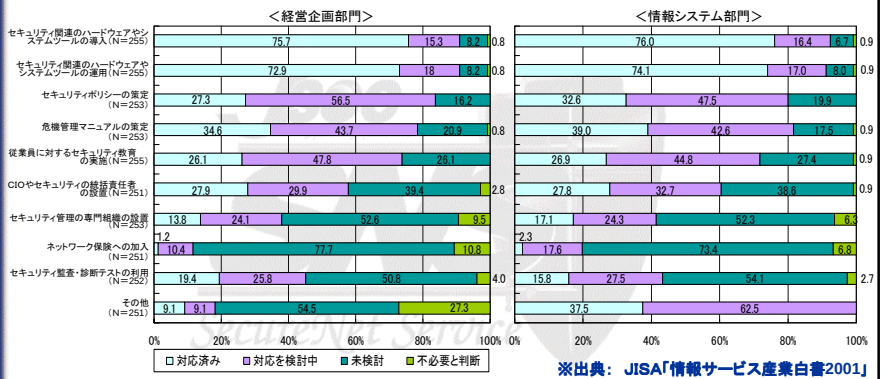

第二章 セキュリティ監視の肝
■セキュリティ監視とは？
監視といえば？
検知
インシデント・レスポンス（広義）
どんな？
侵入・侵害の事実
回復
インシデント
レスポンス（狭義）
日々発生していること
予防
ポリシー（規則）違反
抑止
危ない状態
防御
リアルタイム
プロテクション
23
Copyright © Little eArth Corporation 2002


第二章 セキュリティ監視の肝
■発生インシデントの深刻度とセキュリティ監視
深刻度
正しくセキュリティ監視を
未実施の場合の深刻度
回復
正しくセキュリティ監視を
実施した場合の深刻度
防御
予防
抑止
インシデントレスポンス
リアルタイムプロテクション
バッチ的な分析
観察・検閲？
手遅れ？
被害の拡大
被害の検知
被害の可能性判断
防御・回復のみ
抑止＋予防の併用
危ない状態
侵入侵害の事実
時刻の経過
24
Copyright © Little eArth Corporation 2002

第三章 セキュリティ監視の目的

■企業におけるセキュリティ対策状況アンケート（大企業の例）

■ 設問：自社のシステムについて、現在、行っている安全性・信頼性確保のための対策状況はいかがですか？
それぞれの対策について、あてはまるものを一つずつ○を付けてください。



※出典： JISA「情報サービス産業白書2001」

セキュリティ関連のハードウェアやシステムツールの導入・運用は7割超の企業が実施している

えっ！ セキュリティ監視の前にセキュリティ対策の目的？

■よく言われること

セキュリティ対策には際限が無い？？？
完璧なセキュリティはない？？？

セキュリティ対策 ＝ 守ること ？
事件事故が起こらないようにすること？

■セキュリティ対策実施の問題点

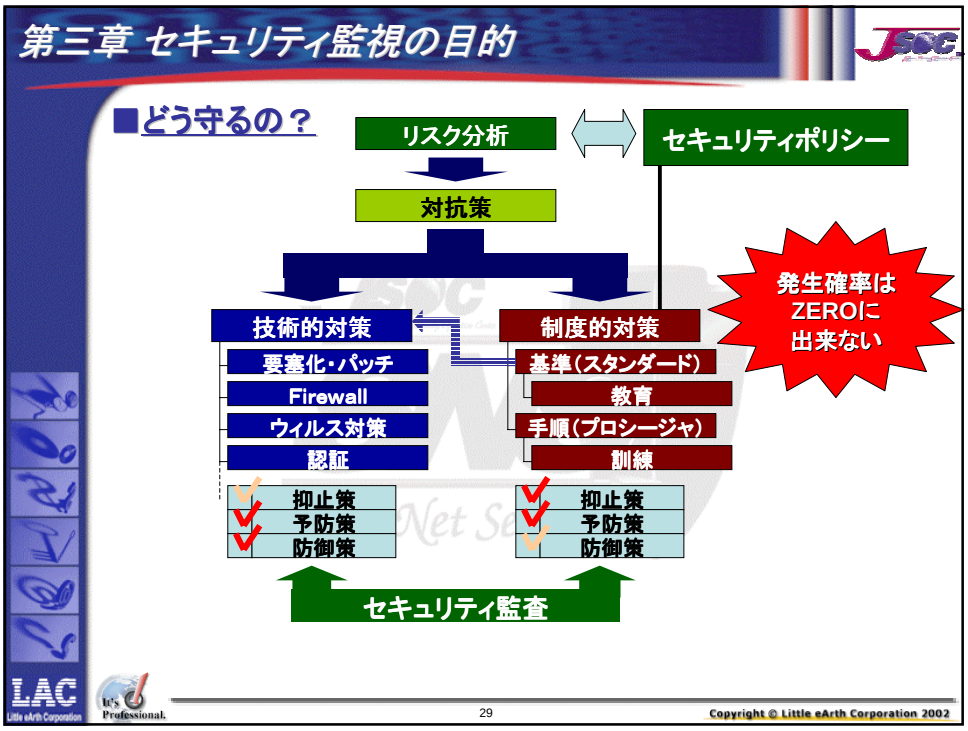
新しい事業モデルを支える為、合理化の為の情報システムは理解はされやすいが、、、

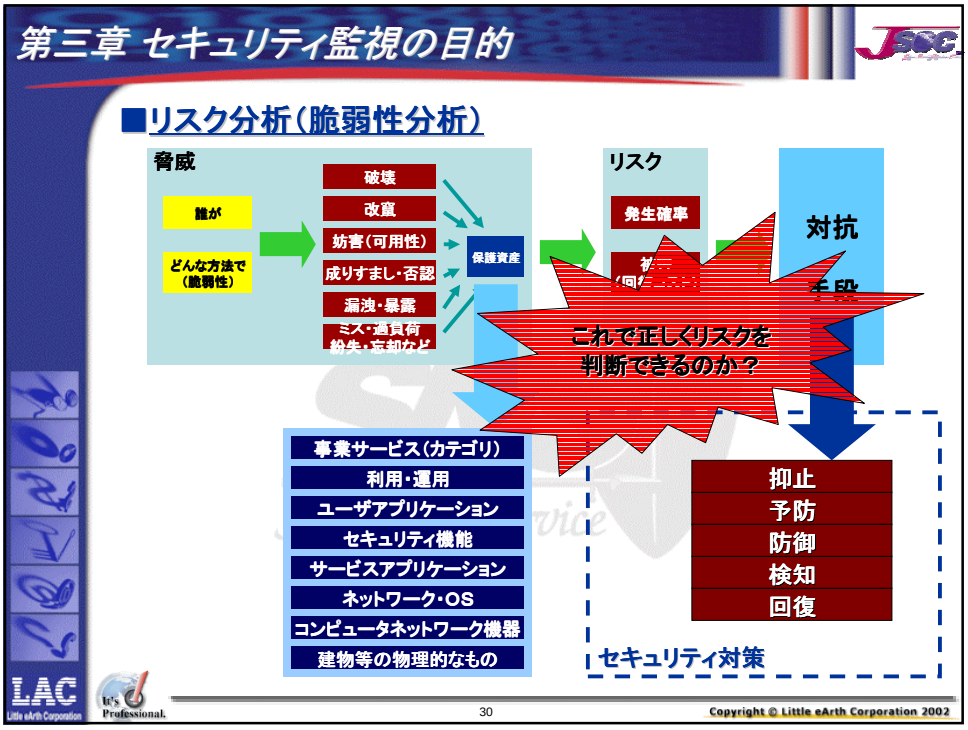
現場の判断・裁量でセキュリティ対策を実施するのは難しい

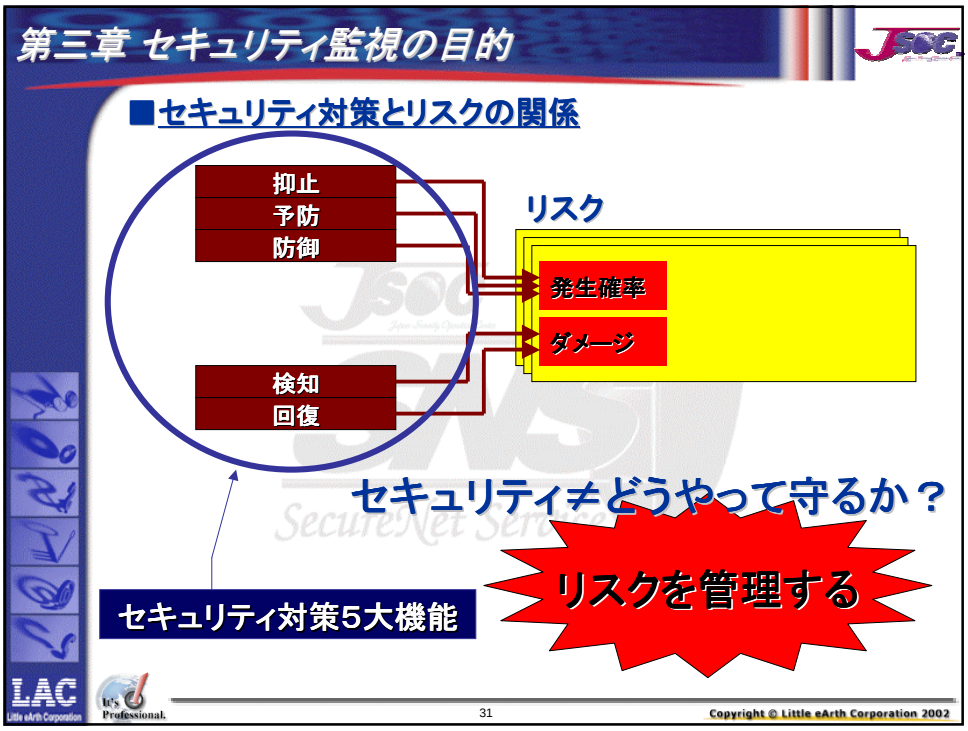
セキュリティ事故等

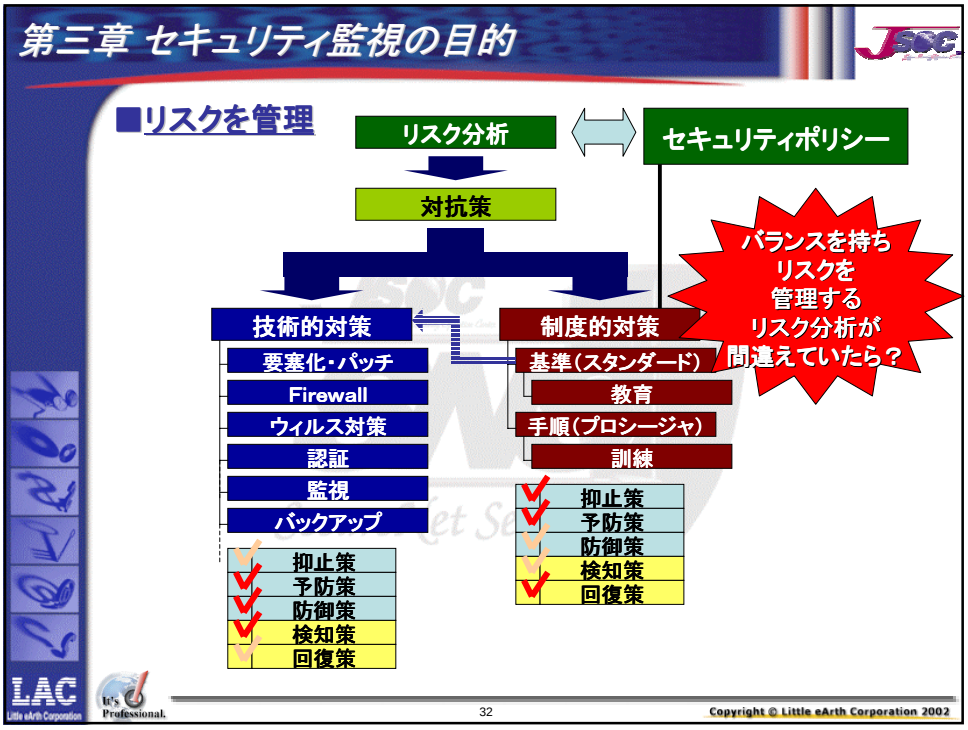
経営者・トップの方針

セキュリティ対策は
マイナスの要素なのか？


第三章 セキュリティ監視の目的
■どう守るの？
リスク分析
セキュリティポリシー
対抗策
発生確率は
ZEROに
出来ない
技術的対策
要塞化・パッチ
Firewall
ウィルス対策
認証
制度的対策
基準(スタンダード)
教育
手順(プロシージャ)
訓練
抑止策
予防策
防御策
抑止策
予防策
防御策
セキュリティ監査
29
Copyright © Little eArth Corporation 2002


第三章 セキュリティ監視の目的
■リスク分析(脆弱性分析)
脅威
誰が
どんな方法で
(脆弱性)
破壊
改竄
妨害(可用性)
成りすまし・否認
漏洩・暴露
保護資産
リスク
発生確率
対抗
これで正しくリスクを
判断できるのか？
事業サービス(カテゴリ)
利用・運用
ユーザアプリケーション
セキュリティ機能
サービスアプリケーション
ネットワーク・OS
コンピュータネットワーク機器
建物等の物理的なもの
抑止
予防
防御
検知
回復
セキュリティ対策
30
Copyright © Little eArth Corporation 2002


第三章 セキュリティ監視の目的
■セキュリティ対策とリスクの関係
抑止
予防
防御
検知
回復
リスク
発生確率
ダメージ
セキュリティ≠どうやって守るか？
リスクを管理する
セキュリティ対策5大機能
31
Copyright © Little eArth Corporation 2002


第三章 セキュリティ監視の目的
■リスクを管理
リスク分析
セキュリティポリシー
対抗策
バランスを持ち
リスクを
管理する
リスク分析が
間違えていたら？
技術的対策
要塞化・パッチ
Firewall
ウィルス対策
認証
監視
バックアップ
抑止策
予防策
防御策
検知策
回復策
制度的対策
基準（スタンダード）
教育
手順（プロシージャ）
訓練
抑止策
予防策
防御策
検知策
回復策
32
Copyright © Little eArth Corporation 2002

第三章 セキュリティ監視の目的

■これまでの一般的なセキュリティ対策

1. 脅威を分かって上で対策を行っていない
   本当に守らなければならないことは？
   → セキュリティ対策の目的が不明確

2. 守る策に終始している
   → 戦略が無い（各対策のバランシング）

第三章 セキュリティ監視の目的

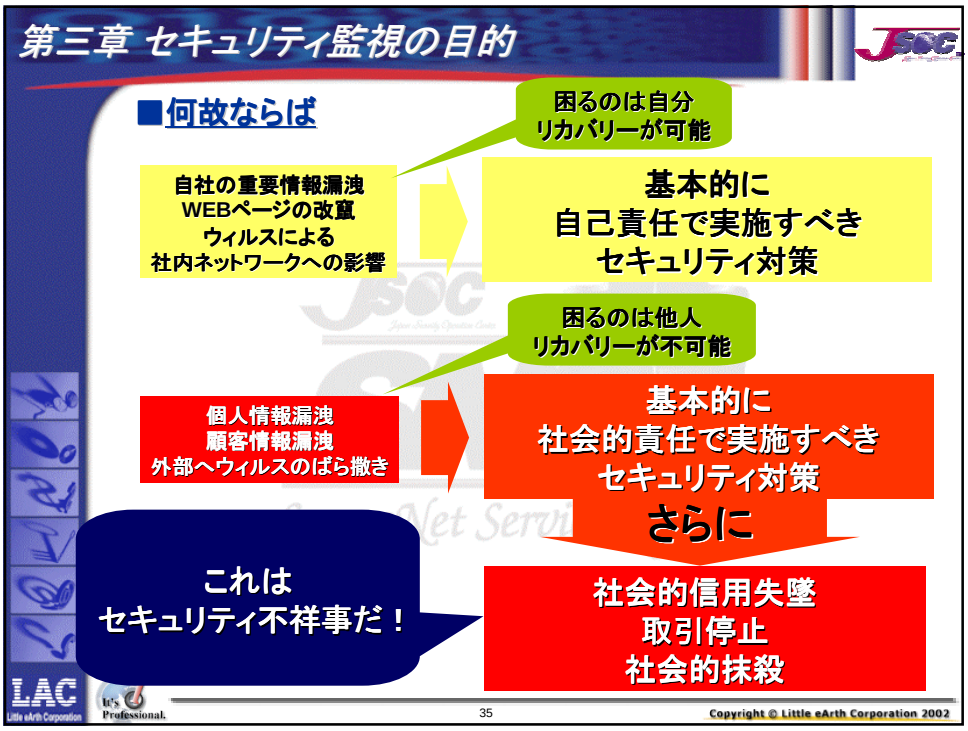
■経営レベルで考えると、何を気を付けなければならないか？

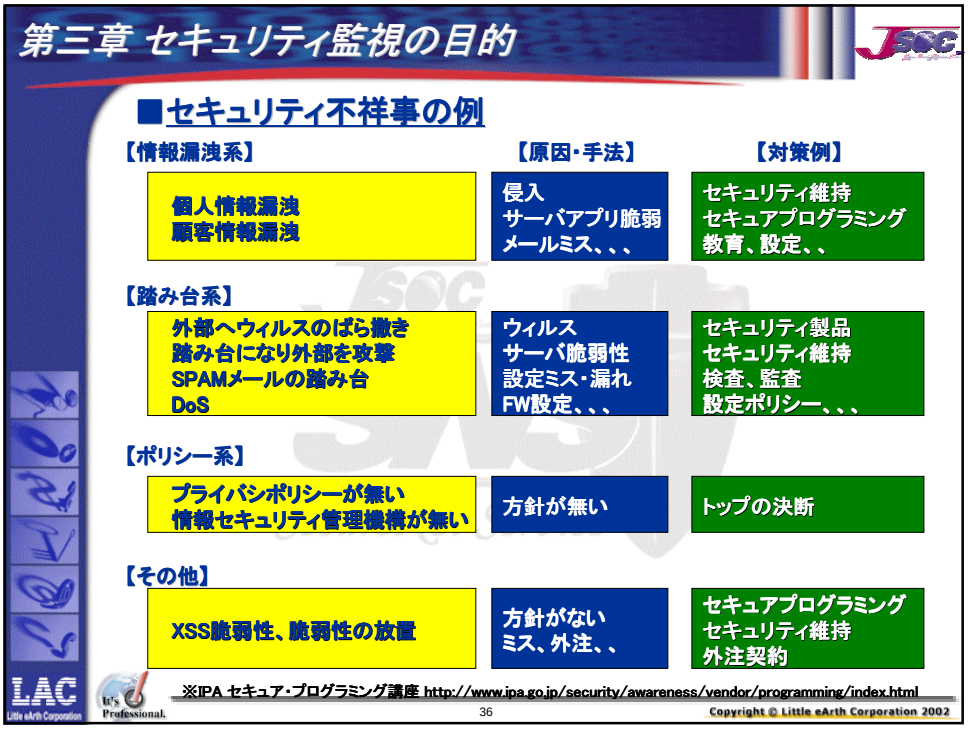
自社の重要情報漏洩
WEBページの改竄
ウィルスによる
社内ネットワークへの影響

よりも

個人情報漏洩
顧客情報漏洩
外部へウィルスのばら撒き

を、最優先で対処すべき。


第三章 セキュリティ監視の目的
■何故ならば
困るのは自分
リカバリーが可能
自社の重要情報漏洩
WEBページの改竄
ウィルスによる
社内ネットワークへの影響
基本的に
自己責任で実施すべき
セキュリティ対策
困るのは他人
リカバリーが不可能
個人情報漏洩
顧客情報漏洩
外部へウィルスのばら撒き
基本的に
社会的責任で実施すべき
セキュリティ対策
さらに
これは
セキュリティ不祥事だ！
社会的信用失墜
取引停止
社会的抹殺
35
Copyright © Little eArth Corporation 2002


第三章 セキュリティ監視の目的
■セキュリティ不祥事の例
【情報漏洩系】
【原因・手法】
【対策例】
個人情報漏洩
顧客情報漏洩
侵入
サーバアプリ脆弱
メールミス、、、
セキュリティ維持
セキュアプログラミング
教育、設定、、
【踏み台系】
外部へウィルスのばら撒き
踏み台になり外部を攻撃
SPAMメールの踏み台
DoS
ウィルス
サーバ脆弱性
設定ミス・漏れ
FW設定、、、
セキュリティ製品
セキュリティ維持
検査、監査
設定ポリシー、、、
【ポリシー系】
プライバシポリシーが無い
情報セキュリティ管理機構が無い
方針が無い
トップの決断
【その他】
XSS脆弱性、脆弱性の放置
方針がない
ミス、外注、、
セキュアプログラミング
セキュリティ維持
外注契約
※IPA セキュア・プログラミング講座 http://www.ipa.go.jp/security/awareness/vendor/programming/index.html
36
Copyright © Little eArth Corporation 2002

第三章 セキュリティ監視の目的

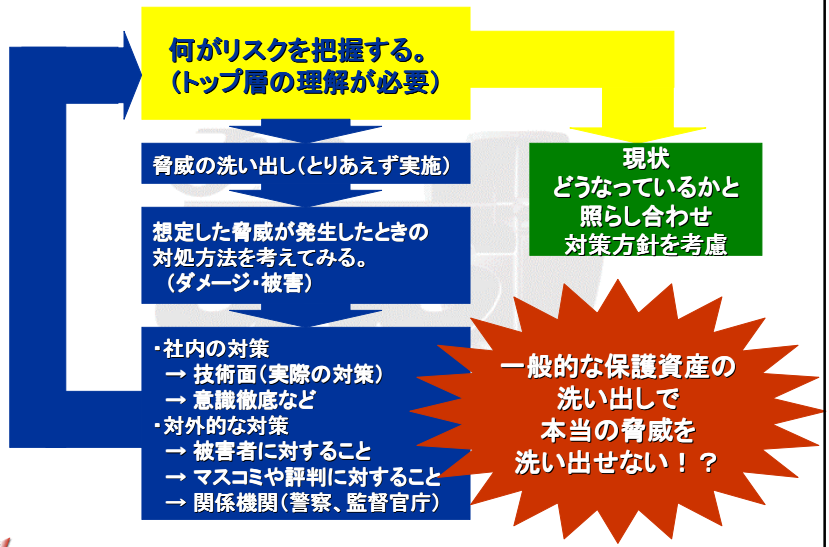
■セキュリティ対策の目的

セキュリティ不祥事	大半の組織
セキュリティ事故	セキュリティ事故が 事業継続上、重要なリスクと 認識される組織
サイバーテロ	重要インフラ

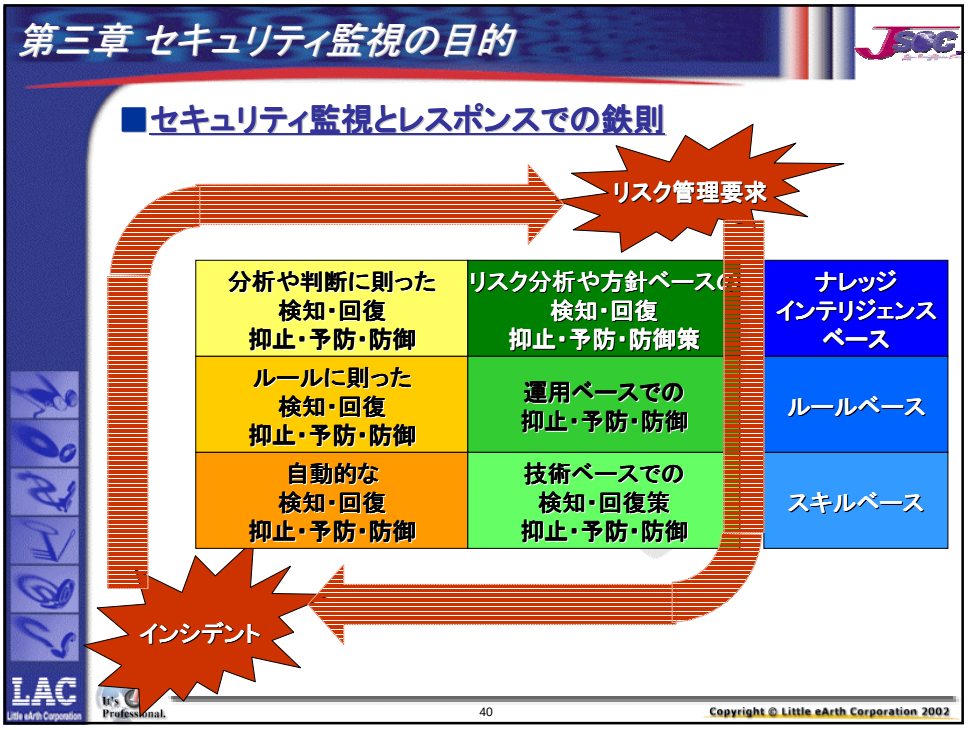
結局、何がリスクか責任かを明確に理解することが重要

第三章 セキュリティ監視の目的

■インシデント・レスポンスから考えるリスク分析




第三章 セキュリティ監視の目的
■基本アプローチ（提案）
インシデントレスポンスを考える
体制の整備、準備、訓練
インシデント検知策
発生確率・体力・ダメージ他（業界内などの常識法制など）を鑑みて、
リスク管理
守る為の対策の実施レベル等を適切に判断し、随時実施
インシデント検知
回復（レスポンスの実施）
39
Copyright © Little eArth Corporation 2002


第三章 セキュリティ監視の目的
■セキュリティ監視とレスポンスでの鉄則
リスク管理要求
分析や判断に則った検知・回復抑止・予防・防御
リスク分析や方針ベースの検知・回復抑止・予防・防御策
ナレッジインテリジェンスベース
ルールに則った検知・回復抑止・予防・防御
運用ベースでの抑止・予防・防御
ルールベース
自動的な検知・回復抑止・予防・防御
技術ベースでの検知・回復策抑止・予防・防御
スキルベース
インシデント
40
Copyright © Little eArth Corporation 2002

第三章 セキュリティ監視の目的

■目的と実施範囲

【目的】
1. セキュリティ不祥事を意識
2. セキュリティ事故を意識
3. サイバーテロを意識

【実施範囲】
1. インターネットサイド
2. DMZセグメント
3. イントラネット

第三章 セキュリティ監視の目的

■目的 セキュリティ不祥事を意識

【ポイント】
1. ウィルス・ワームの外部への発信
   ⇒ ウィルスゲートウェイ監視
   ⇒ ファイアウォールでウィルス感染活動を監視
2. 外部への攻撃
   ⇒ IDSで外向け攻撃を監視
   ⇒ メールサーバエラーログ監視
3. 個人情報漏洩若しくは漏洩の危険性
   ⇒ IDSでWEBサーバへの攻撃監視

レスポンスは対象組織のトップサイド（ナレッジベース）が優先、追って、ミドルサイド（ルールベース）と技術サイド（スキルベース）

第三章 セキュリティ監視の目的

■目的 セキュリティ事故を意識

【ポイント】

1. イントラへのウィルス・ワームの侵入や内部での攻撃
   ⇒ IDSでイントラネットを監視
   ⇒ 内部のファイアウォール監視
2. 公開サーバや重要サーバへの侵入行為
   ⇒ 作業手順チェック
   ⇒ ホスト型IDS
3. 外部への情報漏洩
   ⇒ メールサーバ監査、セッションのアノマリ検知
3. 成りすましや権限の乱用
   ⇒ アクセスログでのアノマリ検知
   ⇒ 作業手順チェック

レスポンスは対象組織のミドルサイドが優先、追って、トップサイド並びに技術サイド

第三章 セキュリティ監視の目的

■目的 サイバーテロを意識

【ポイント】

1. 基幹サービスへのDoS攻撃
   ⇒ ファイアウォールでの検知
   ⇒ ファイアウォールでのアクセスアノマリ検知
   ⇒ 基幹サービスの稼動監視（レスポンスアノマリ）など
2. セキュリティ監視へのDoS攻撃
   ⇒ 監視システム稼動監視（ログ量アノマリ）など
3. 内部侵入の監視
   ⇒ トラステッドOSレベルでのアクセス制御違反監視

レスポンスは技術サイドが優先、追って、トップサイド並びにミドルサイド

第三章 セキュリティ監視の目的

1. セキュリティ対策 ≠ 守ること
   → リスクを管理すること
2. 本当のリスクを把握する。
   → インシデントが起こったと想定し、
   レスポンスを考える。
3. セキュリティ監視は余裕があったら
   やるレベルではなく、最初に実施する
   ことを真面目に検討すべき。
4. レスポンス対策が出来ている組織は
   価値が高い。

第四章 セキュリティ監視の実際

■ログ分析 IDSのセッション確認例（誤報の確認）

基本的にこの文字列でIDSは検知

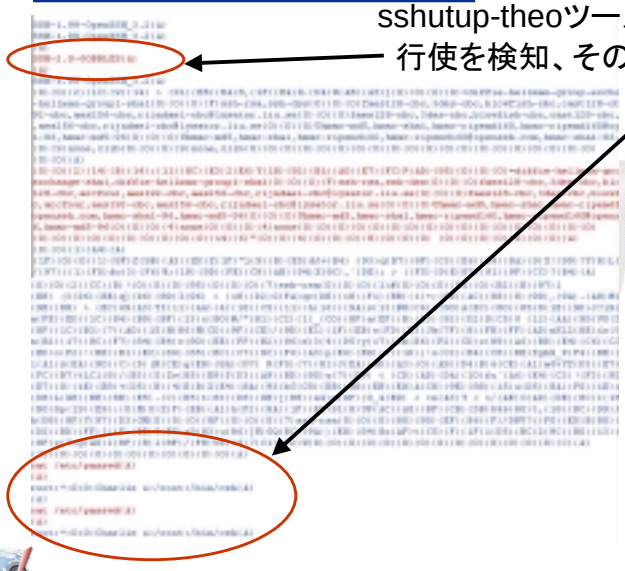
この場合、攻撃は不成功

■ログ分析 IDSのセッション確認例（行動の確認）

Anonymous ログインで検知
その後、行動をトレース

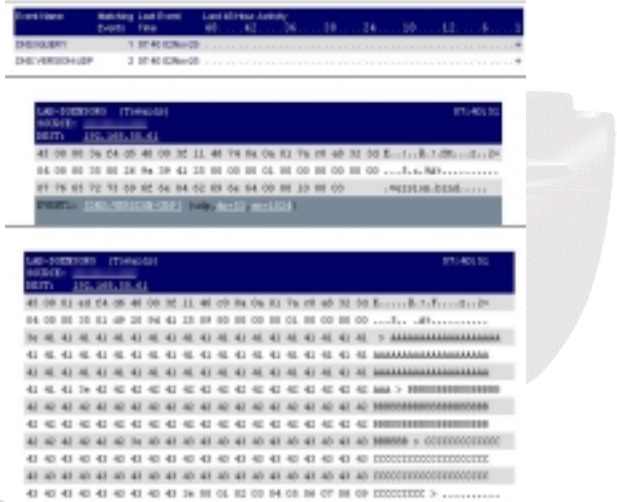
■ログ分析 IDSのセッション確認例

sshutup-theoツール（GOBBLES）
行使を検知、その後行動を確認

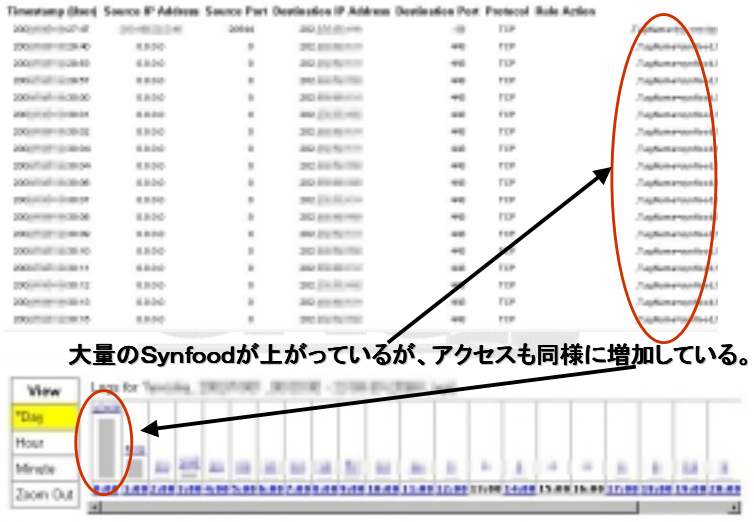


■ログ分析 IDSのセッション確認例（バイナリ）

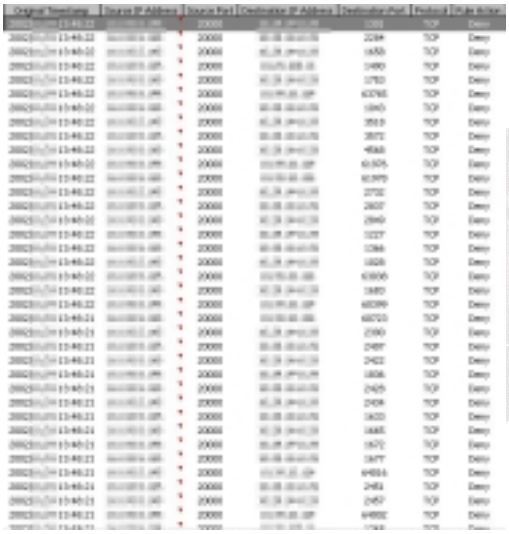
BINDにバッファオーバフロー攻撃



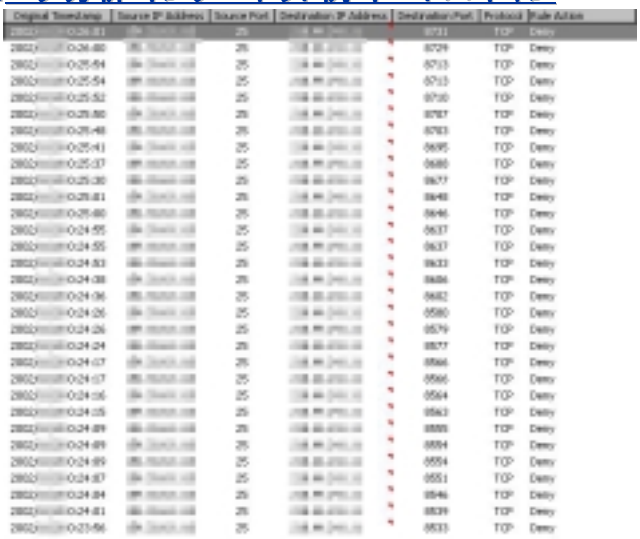
■ログ分析 IDSの誤報？



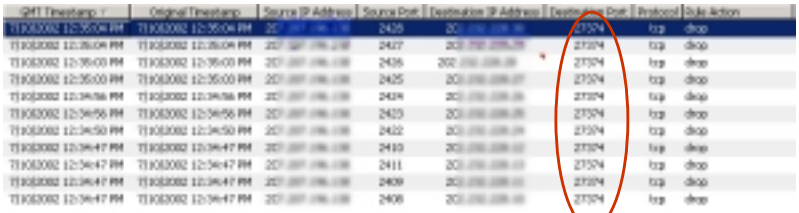
■ログ分析 インターネット例 ポートスキャン



■ログ分析 インターネット例 ポートスキャン

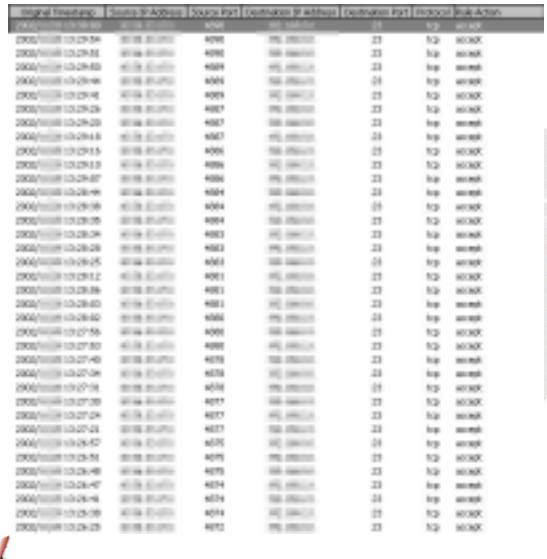


■ログ分析 インターネット例 SubSevenスキャン

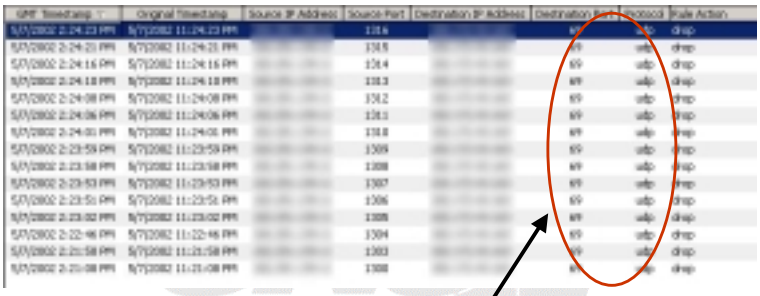


インターネットから特定のトロイの木馬を探している？

■ログ分析 インターネット例 ブルートフォース

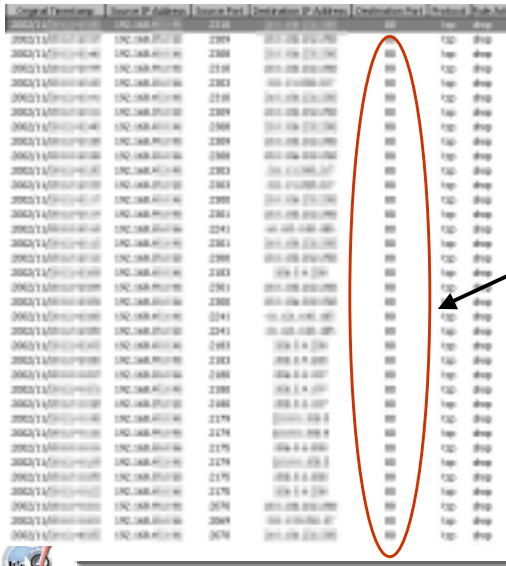


■ログ分析 イントラネット例 内部のNimda感染前



内部から外部にTFTP(UDP)で接続
Nimdaの本体をダウンロードする行為？

■ログ分析 イントラネット例 内部のCodeRed？



ここのサイトはプロキシ経由で
インターネットへアクセス

短時間にランダムIPに同一IPから
HTTP接続を試みている

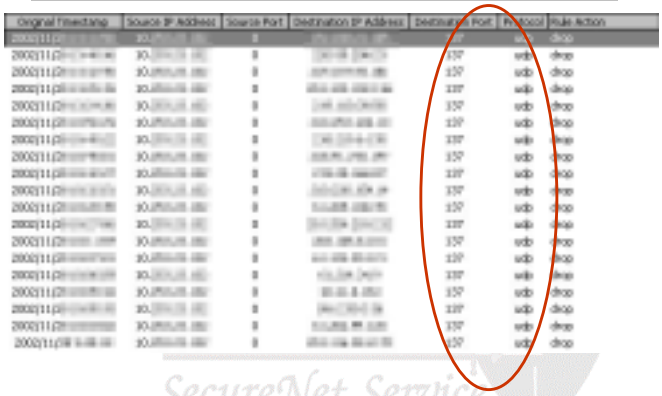
Coderedの感染活動？

■ログ分析 イントラネット例 内部のSircam感染活動？

短時間にランダムIPに同一IPから
SMTP接続を試みている

Sircam等の感染活動？

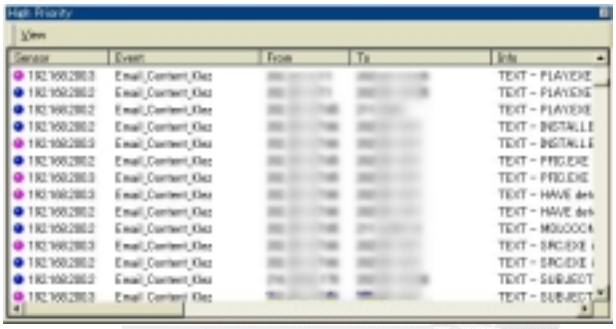
■ログ分析 イントラネット例 内部のウィルス？



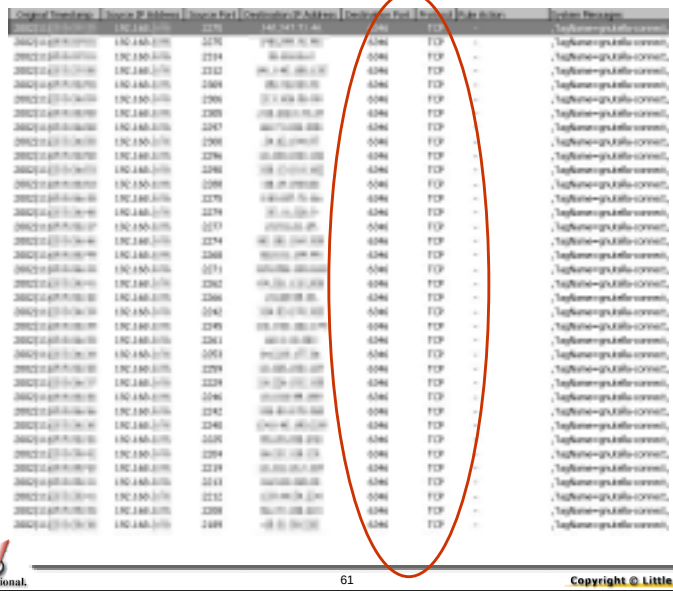
短時間にランダムIPに同一IPから
MS ファイル共有アクセスを試みている

ファイル共有を通じて感染するウィルス？

■ログ分析 イントラネット例 klezの感染活動



■ログ分析 イントラネット例（gnutella、limewire）ファイル交換ソフト？



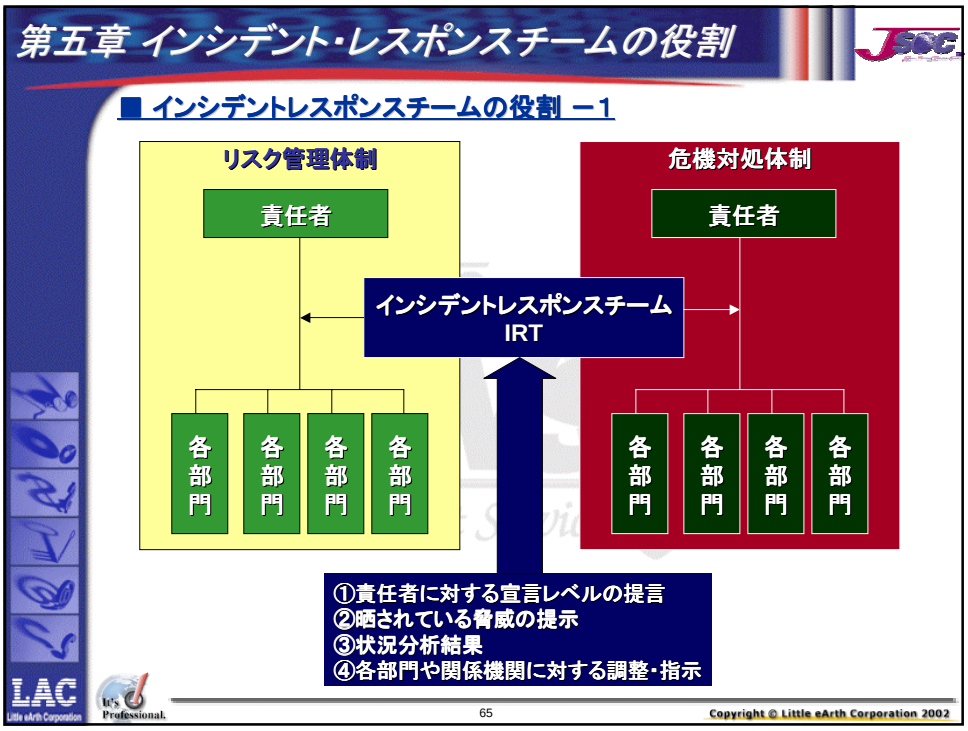
■ログ分析 イントラネット例 外部にセキュリティスキャン

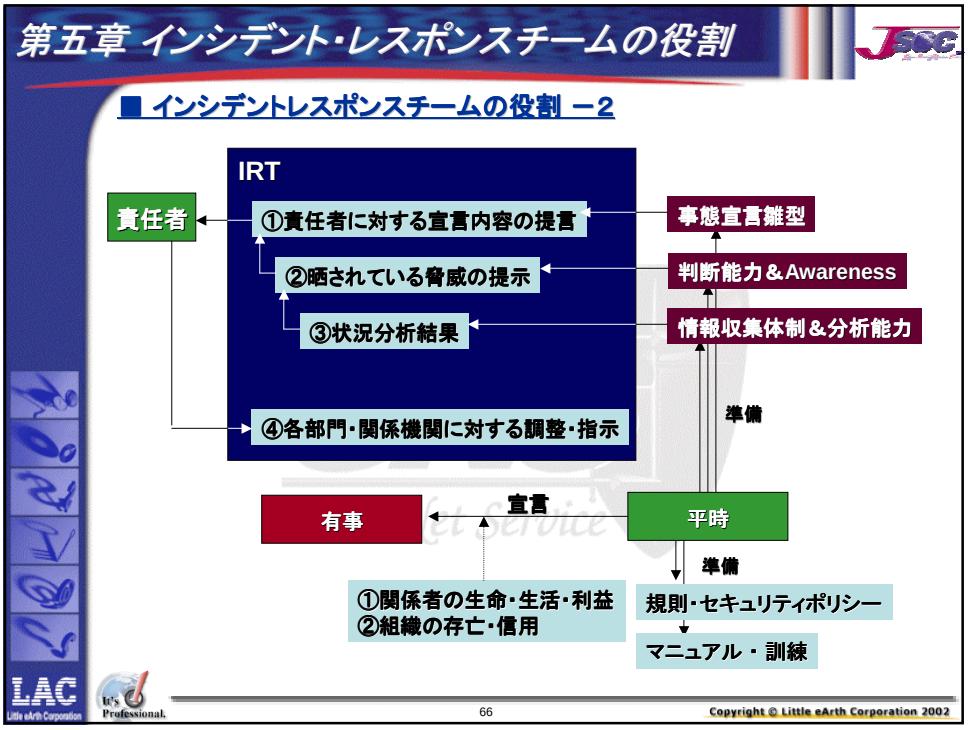
■IDSでの違い

**同じ脆弱性に対して、攻撃ツールA、B、Cを使用して
IDS A、B、C、Dで検知した結果**

IDS	Exploit A	Exploit B	Exploit C
IDS A	FTP Tilde FTP site exec	FTP Tilde Shellcode x86 FTP cwd overflow	FTP Passwd Overflow FTP cwd overflow
IDS B	FTP Site exec Shellcode x86	FTP cwd overflow Shellcode x86 Shellcode x86 stealth	FTP Passwd Overflow
IDS C	FTP Site exec FTP Tilde	FTP cwd overflow FTP Tilde	FTP Passwd Overflow FTP Tilde
IDS D	FTP site exec Shellcode x86	FTP cwd overflow FTP RNFR ./ attempt Shellcode x86	FTP cwd overflow Shellcode x86

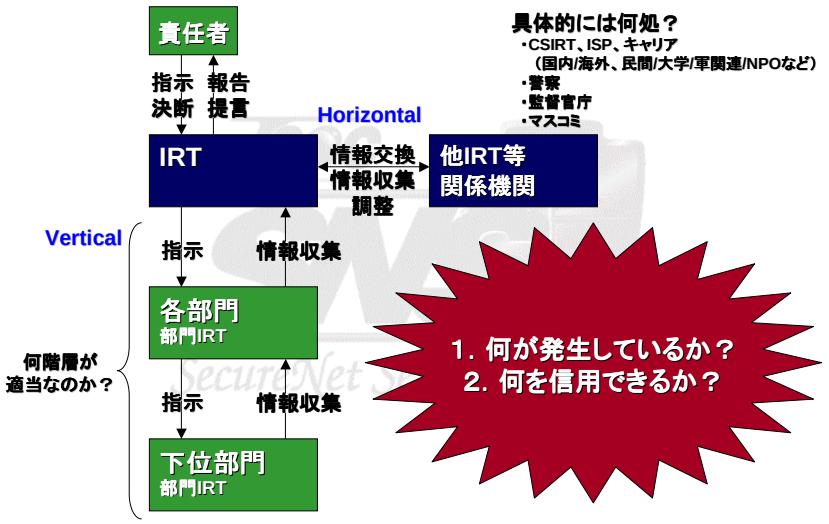
第五章 インシデントレスポンスチームの役割


第五章 インシデント・レスポンスチームの役割
■ インシデントレスポンスチームの役割 －1
リスク管理体制
危機対処体制
責任者
責任者
インシデントレスポンスチーム
IRT
各部門
各部門
各部門
各部門
各部門
各部門
各部門
各部門
①責任者に対する宣言レベルの提言
②晒されている脅威の提示
③状況分析結果
④各部門や関係機関に対する調整・指示
65
Copyright © Little eArth Corporation 2002


第五章 インシデント・レスポンスチームの役割
■ インシデントレスポンスチームの役割 －2
IRT
責任者
①責任者に対する宣言内容の提言
②晒されている脅威の提示
③状況分析結果
④各部門・関係機関に対する調整・指示
事態宣言雛型
判断能力＆Awareness
情報収集体制＆分析能力
準備
宣言
有事
平時
準備
①関係者の生命・生活・利益
②組織の存亡・信用
規則・セキュリティポリシー
マニュアル・訓練
66
Copyright © Little eArth Corporation 2002

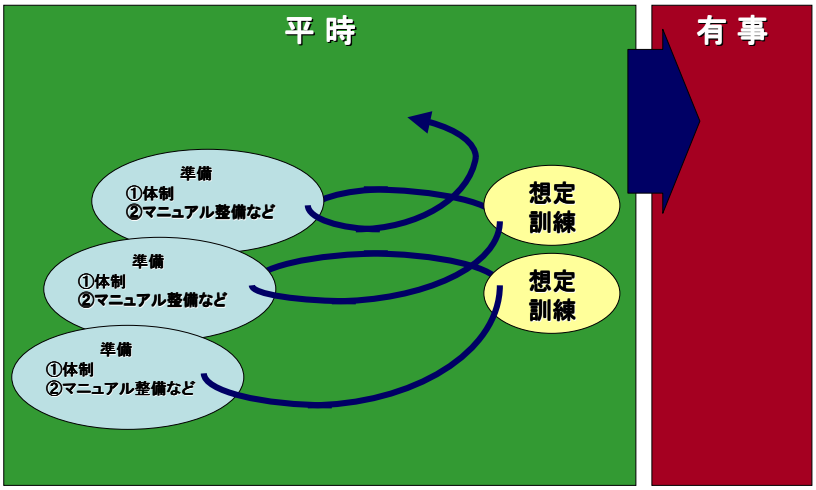
第五章 インシデント・レスポンスチームの役割

■ 神経系統



第五章 インシデント・レスポンスチームの役割

■ 準備と訓練



第五章 インシデント・レスポンスチームの役割

ここで取り扱うインシデントは所謂コンピュータセキュリティインシデント（ 以降、単純にインシデント）

■ インシデントの特徴

① サイバー空間にて操作され、顕著化はサイバー空間に限らない

② 捜査が困難

・攻撃者の匿名性が強い

・国境などの、境界が基本的に存在しない

・技術の脆弱性と急激な進歩

③脅威の把握が困難

・発生しているインシデントの影響度合いの判断を行なう為には、様々な観点と技術力が必要

→ 手法や侵入ルートの特定や推測

→ 被害範囲や影響範囲の特定や推測

第六章 インシデントレスポンス概要

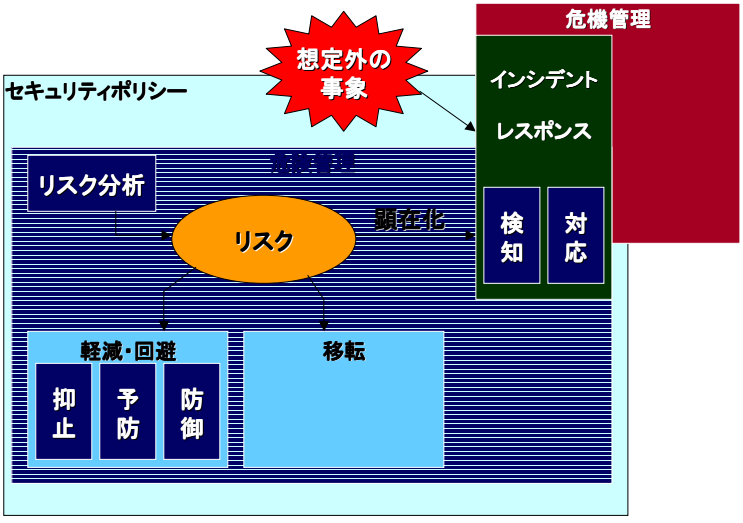
■ インシデントレスポンスの大原則

① どういう状態が危機（クライシス）であるか、明確であること。
危機管理体制の一環として明確に組み込まれ、責任者が明確であること
責任者が迅速に決断し宣言を行なえること

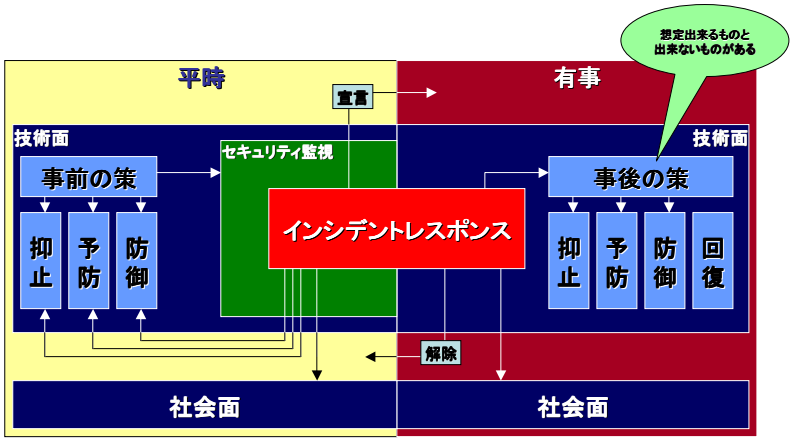
② どういう状態が危険（リスク）であるか、明確であること。
危険管理体制の一環として明確に組み込まれ、責任者が明確であること
想定しているリスクが顕在化した場合に、危機として対処すべきことが明確であること。

③ 教育と訓練
インシデントレスポンスは一部の関係者のみが実施するものではない
各レイヤにおける意識の向上と、対処能力養成が重要

■ インシデントレスポンスの位置付け －1



■ インシデントレスポンスの位置付け －2



■ 脅威のカテゴリ

脅威のカテゴリ	内容
セキュリティ不祥事	社会的に迷惑をかける 犯罪に荷担・助長 犯罪 Ex.個人情報漏洩、ウィルスばら撒き、踏台等
セキュリティ事故	自己責任で完結可能なもの EX.内部情報漏洩、内部システム破壊 等
サイバーテロ	国家や社会の転覆・混乱などを狙ったもの または、同様の影響があると判断されるもの EX.重要インフラ、マルチナショナル

■ インシデントのカテゴリ

インシデント・カテゴリ	説明
被害や犯罪が顕在化している	改竄、情報漏洩 他(内、外)を攻撃 停止、誤動作 など
侵入されているが被害はまだ	侵入されているが、 被害発生はまだ (まだ、間に合う)
侵入されてもおかしくない (被害が出てもおかしくない)	脆弱性がある状態で運用 強烈なウィルス発生情報・攻撃情報 ※風評・外部からの指摘に関して要注意
実害の無い 調査行動や攻撃	通常IDS等で検知する攻撃や調査
規則やポリシーの違反行為	業務上の目的以外に権限を行使 顧客情報の横流しなど
アノマリ行動	権限の行使状況のアノマリ

■ インシデント検知のカテゴリ

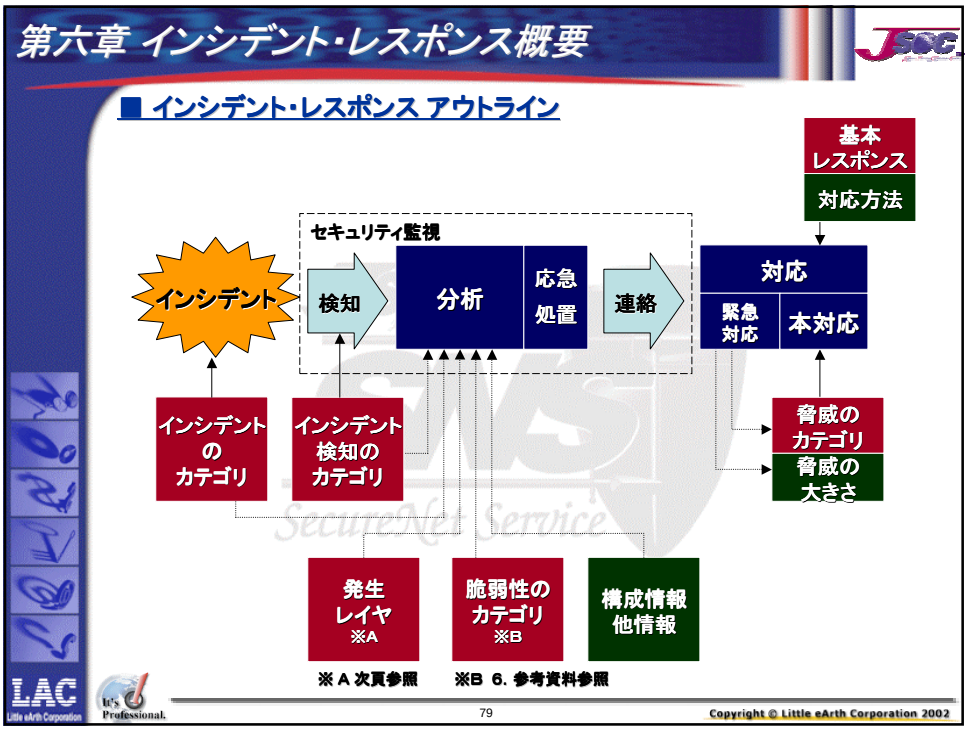
インシデント検知カテゴリ	説明
自己の監視で検知	自組織の監視で検知
内部通報	自組織の人間が(たまたま)検知
外部通報(一般非公開)	他組織の人間が検知し 個別に通知・連絡
外部通報(一般公開)	他組織の人間が検知し 公開しながら通知・連絡
報道	TV、新聞、ネットニュースなどの報道

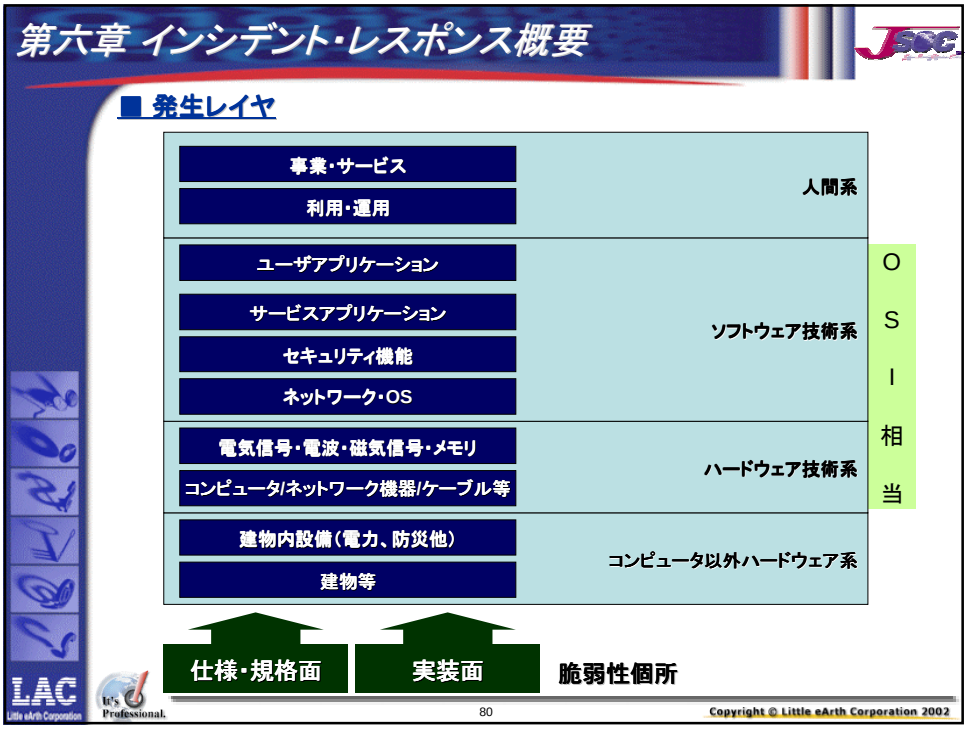
■ 検知可能なインシデントのカテゴリ

インシデント・カテゴリ	検知方法			
	自己監視	内部通報	外部通報	報道
被害や犯罪が顕在化している	○	○	○	○
侵入されているが被害はまだ	○	△	×	×
侵入されてもおかしくない	○	○	○	○
実害の無い 調査行動や攻撃	○	×	×	×
規則やポリシーの違反行為	○	○	×	×
アノマリ行動	○	○	×	×

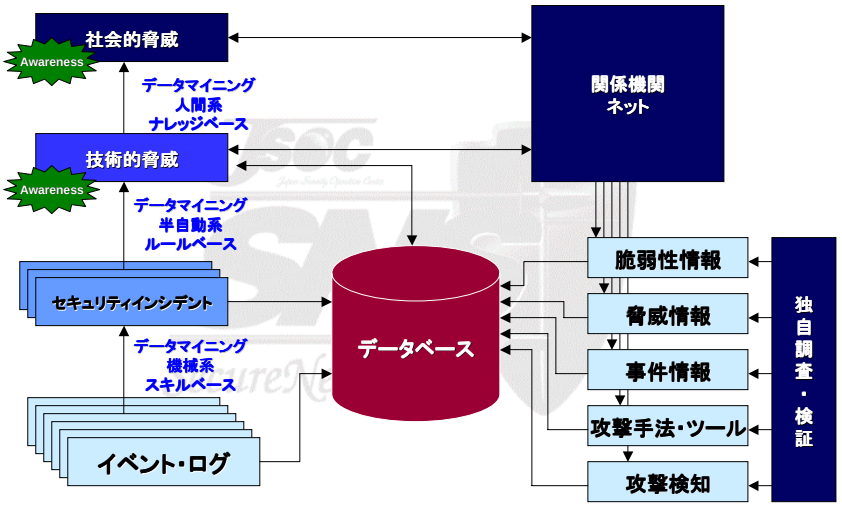
■ インシデントのカテゴリと基本レスポンス（基本対応方法）

インシデント・カテゴリ	基本レスポンス
被害や犯罪が顕在化している	応急処置→緊急対応→本格対応
侵入されているが被害はまだ	応急処置→緊急対応→本格対応
侵入されてもおかしくない	緊急対応→緊急予防対策若しくは警戒態勢
実害の無い 調査行動や攻撃	傾向分析→予防対策
規則やポリシーの違反行為	抑止対策
アノマリ行動	抑止或いは防御対策


第六章 インシデント・レスポンス概要
■ インシデント・レスポンス アウトライン
基本レスポンス
対応方法
セキュリティ監視
インシデント
検知
分析
応急処置
連絡
対応
緊急対応
本対応
インシデントのカテゴリ
インシデント検知のカテゴリ
脅威のカテゴリ
脅威の大きさ
発生レイヤ ※A
脆弱性のカテゴリ ※B
構成情報他情報
※A 次頁参照
※B 6. 参考資料参照
79
Copyright © Little eArth Corporation 2002


第六章 インシデント・レスポンス概要
■ 発生レイヤ
事業・サービス
利用・運用
人間系
ユーザアプリケーション
サービスアプリケーション
セキュリティ機能
ネットワーク・OS
ソフトウェア技術系
電気信号・電波・磁気信号・メモリ
コンピュータ/ネットワーク機器/ケーブル等
ハードウェア技術系
建物内設備（電力、防災他）
建物等
コンピュータ以外ハードウェア系
OSI相当
仕様・規格面
実装面
脆弱性個所
80
Copyright © Little eArth Corporation 2002

■分析概念



■分析階層

階層	分析分類	対応分類	ベース
社会面	社会ベースでの 脅威を判断 人間系	関係機関など 人間系での対応	ナレッジ インテリジェンス ベース
技術面	技術ベースでの 脅威を判断 半自動	技術面での ルールに則った対応	ルールベース
システム面	システムでの分析 自動化	自動的な対応 システム対応	スキルベース


ありがとうございました
http://www.lac.co.jp/security/
お問い合わせ　：　itsuro@lac.co.jp
LAC
Little eArth Corporation
It's Professional
83
Copyright © Little eArth Corporation 2002