ＩＴセキュリティ保護のコストについて

～住基ネット上での個人情報の安全性確保のためには～

長野県本人確認情報保護審議会

審議委員

吉田柳太郎

アジェンダ

以下のような流れでお話をしていきます

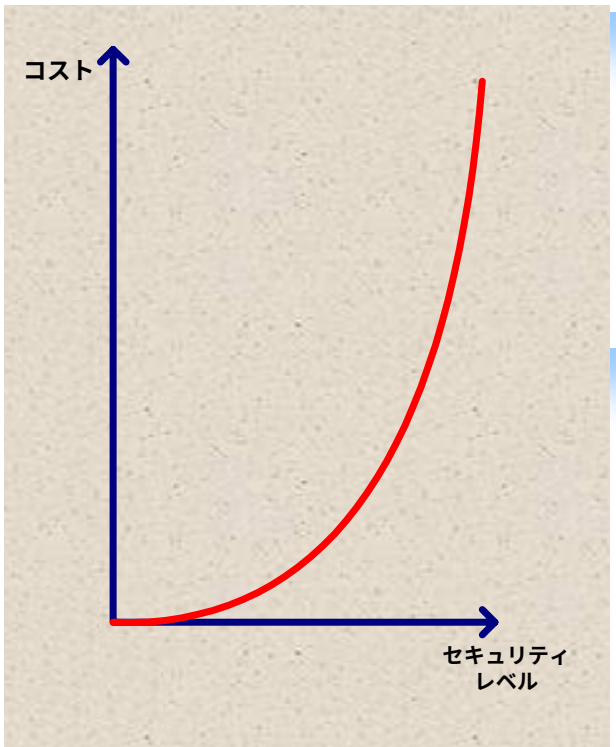
- 脅威のヘッジとコストについて
- 不正アクセスがもたらす損失を換算してみる
- 実際の具体的な進入について
- 最近議論されている不正アクセス対策
- とりあえず安全なネットワーク概要と最低限の具体的費用

ここで言葉をおさらい

Firewall 、VPNとIDS について

- Firewall
  - これは有名。いわゆる関所。ビルに例えると警備員のいる入退室警備。
- VPN
  - 暗号のトンネルをネットワーク上に張ることでベストエフォートのインターネット上に自社の専用線を敷設したような利用方法を提供する技術。
- IDS　（Intrusion Detection System:不正侵入検知システム）
  - NIDS（ネットワーク型IDS）　サポートするＯＳを限定しない性質
    - ネットワークを流れるデータを全部見て、異常と認識できるものがあった時
    - お知らせするシステム。廊下にある監視カメラ。
  - HIDS（ホスト型IDS）　　サポートするＯＳを限定する性質
    - 最後の砦と呼ばれるホストへの侵入を検知するシステム。侵入されると
    - 困ってしまうホストに直接インストールし、異常な方法でのアクセスが
    - あった場合にお知らせするシステム。大量の金塊の周りを囲む赤外線
    - のようなもの。

脅威のヘッジとコスト



100%のセキュリティ = 無限のコスト

- クラッカーとのイタチごっこ
- 技術の陳腐化の速度
- クラッカーのモチベーション

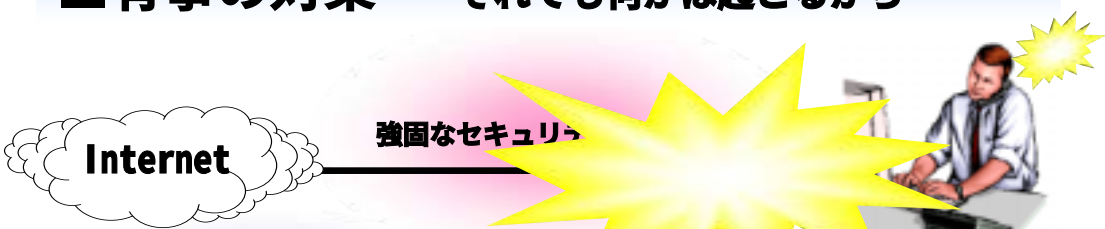
セキュリティレベルの限界

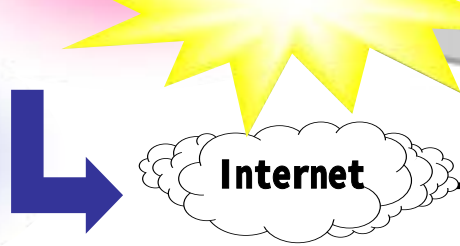
- ソーシャルエンジニアリング
- 未知のセキュリティホール
- 人的ミスによるセキュリティホール

理想的な危機管理対策の形とは

■論理的な対策　－有事の可能性を低くする設備－

■有事の対策　－それでも何かは起こるから－

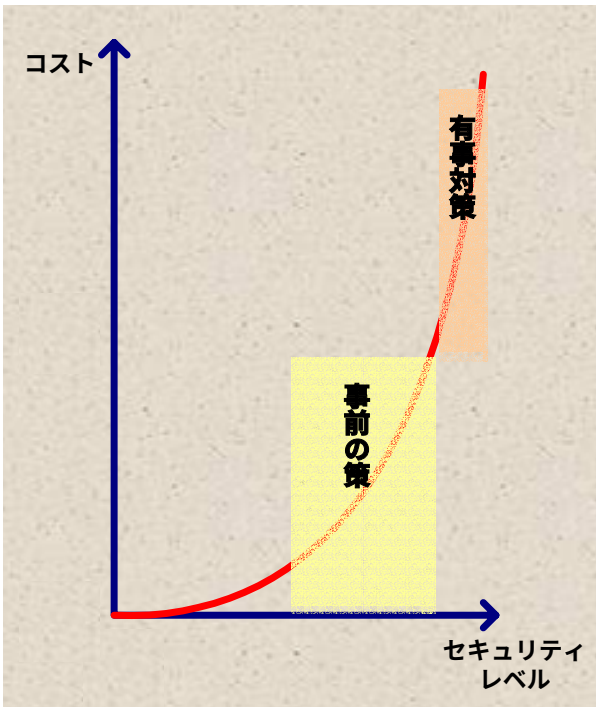




事前の策
＋
有事対策
＝
理想的な
セキュリティ対策の形

ではどのようにセキュリティ対策を考えればいいのでしょうか？

ＩＴセキュリティ対策の具体策



事前の策

・強固なセキュリティシステム

・24時間365日の不正侵入監視（IDS・Firewall）

・セキュリティ専門技術者によるアナライズとレポート

有事対策

・コンサルティングによって定める対応フォーメーション

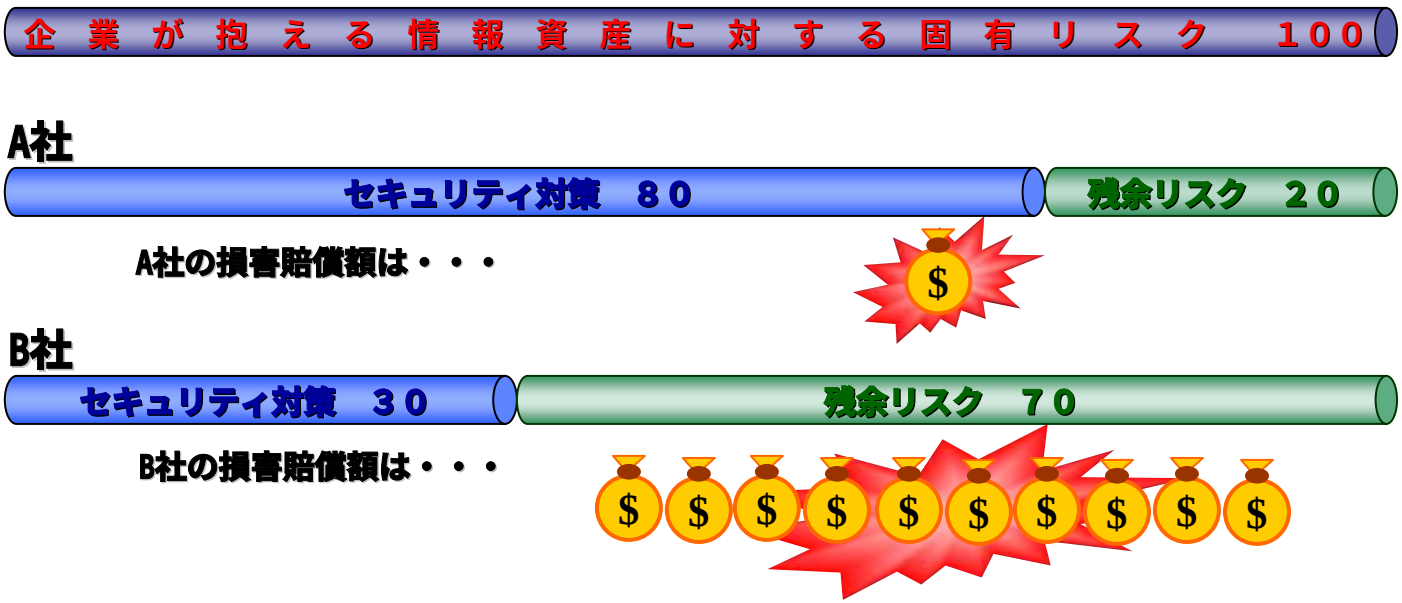
・有事の際の対応フロー策定

・証拠保全のオペレーション

・被害を最小限に抑える対応

セキュリティ対策のポイントは、「危機管理」の観点をもって運用することです。

セキュリティ対策のROIのイメージ



ある2つの会社がインターネットからアタックを受け、それぞれ10万人の顧客リストを盗まれその1万人が団体訴訟を起こしたとします。

企業が1人に支払う損害賠償額は1万円から10万円と言われており、全体で1億から10億の損失になります。そして、　**その金額はどのようなセキュリティ対策をおこなっていたのかに依って決まります。**インターネットに繋がれた環境の中で、情報資産の残余リスクを如何に減らしていたかが重要なポイントになるのです。

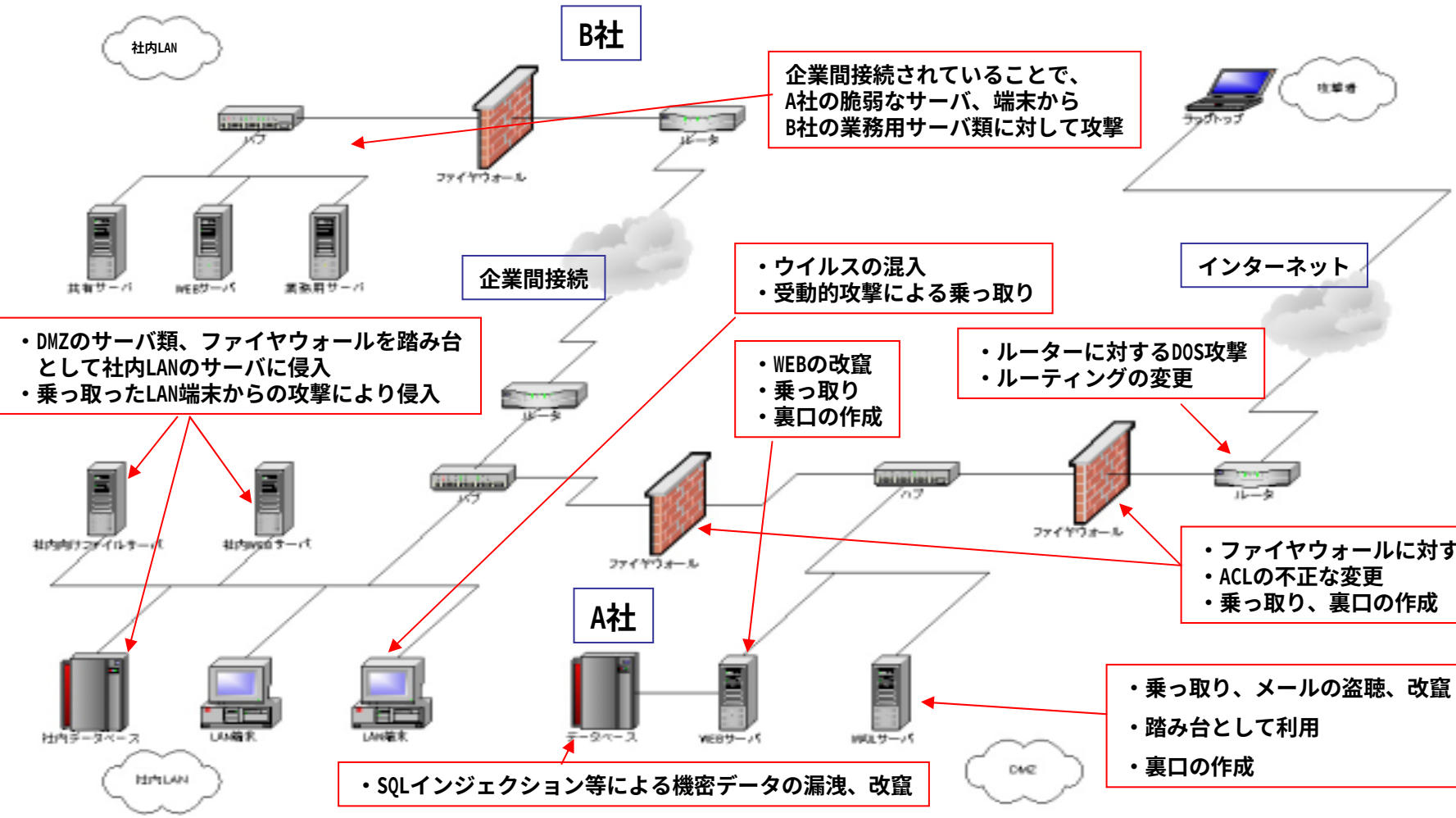
このケースでは９０億円の効果をもたらすのがセキュリティ対策です。対策への投資で直接のリターンはありませんが、損失を防ぐ投資と利益を生む投資は同じものであるという認識を持つことが大切なのです。

不正アクセスとは？

- 不正アクセスとは・・・
  - 他人のID・パスワードを無断で使用する行為
  - セキュリティホールを利用してコンピュータに侵入する行為
  - 上記の不正アクセス行為を助長する行為

- でも・・・不正アクセス以外の「攻撃」もある
  - 不正アクセス以外にも、威力業務妨害等の法律に触れる可能性のある攻撃がある。例えばポートスキャンやDoS攻撃などでネットワークに障害が生じた場合など。
  - ワームと呼ばれる進化したウイルス。自己増殖し能動的に情報を持ち出したり破壊したリ出来る。

一般的なネットワークでの攻撃の実態



一般的なＩＰネットワークの攻撃手順例

１）　対象ネットワークに対する情報収集（whois ,nslookup , search engine等）
２）　ネットワークに対するポートスキャン
３）　ファイヤウォールの検出
３）　ファイヤウォールのルールの推測
４）　DMZ内のサーバに対する攻撃
　　buffer overflow , formatstrings attack 等による
５）　DMZ内のサーバに侵入、裏口の設置
６）　web サーバ経由で、データベースに対してSQLインジェクション攻撃の実行による、不正な情報の搾取、書き換え
７）　侵入したサーバ経由で社内LANに対して情報収集、攻撃、侵入
８）　社内LAN経由で、企業間接続している他社ネットワークに対する情報収集攻撃、侵入、裏口の設置

そんなに不正アクセスがあるのか①

http://www.npa.go.jp/hightech/index.htm警察庁の統計資料から

◇ハイテク犯罪の検挙状況

（件）

罪種＼年	平成14年	増減	平成13年	平成12年
不正アクセス禁止法違反	51	＋16	35	31
コンピュータ、電磁的記録対象犯罪	30	－33	63	44
電子計算機使用詐欺	18	－30	48	33
電磁的記録不正作出・毀棄	8	－3	11	9
電子計算機損壊等業務妨害	4	0	4	2
ネットワーク利用犯罪	958	＋246	712	484
児童買春・児童ポルノ法違反 児童買春	268	＋151	117	8
児童ポルノ	140	＋12	128	113
詐欺	112	＋9	103	53
わいせつ物頒布等	109	＋6	103	154
青少年保護育成条例違反	70	＋60	10	2
脅迫	33	－7	40	17
著作権法違反	31	＋3	28	29
名誉毀損	27	－15	42	30
その他	168	＋27	141	78
合計	1,039	＋229	810	559

※　その他には、覚せい剤取締法違反等の薬物事犯、銃砲刀剣類所持等取締法違反、売春防止法違反、商標法違反等がある。

そんなに不正アクセスがあるのか②

http://www.npa.go.jp/hightech/index.htm警察庁の統計資料から

◇相談受理件数

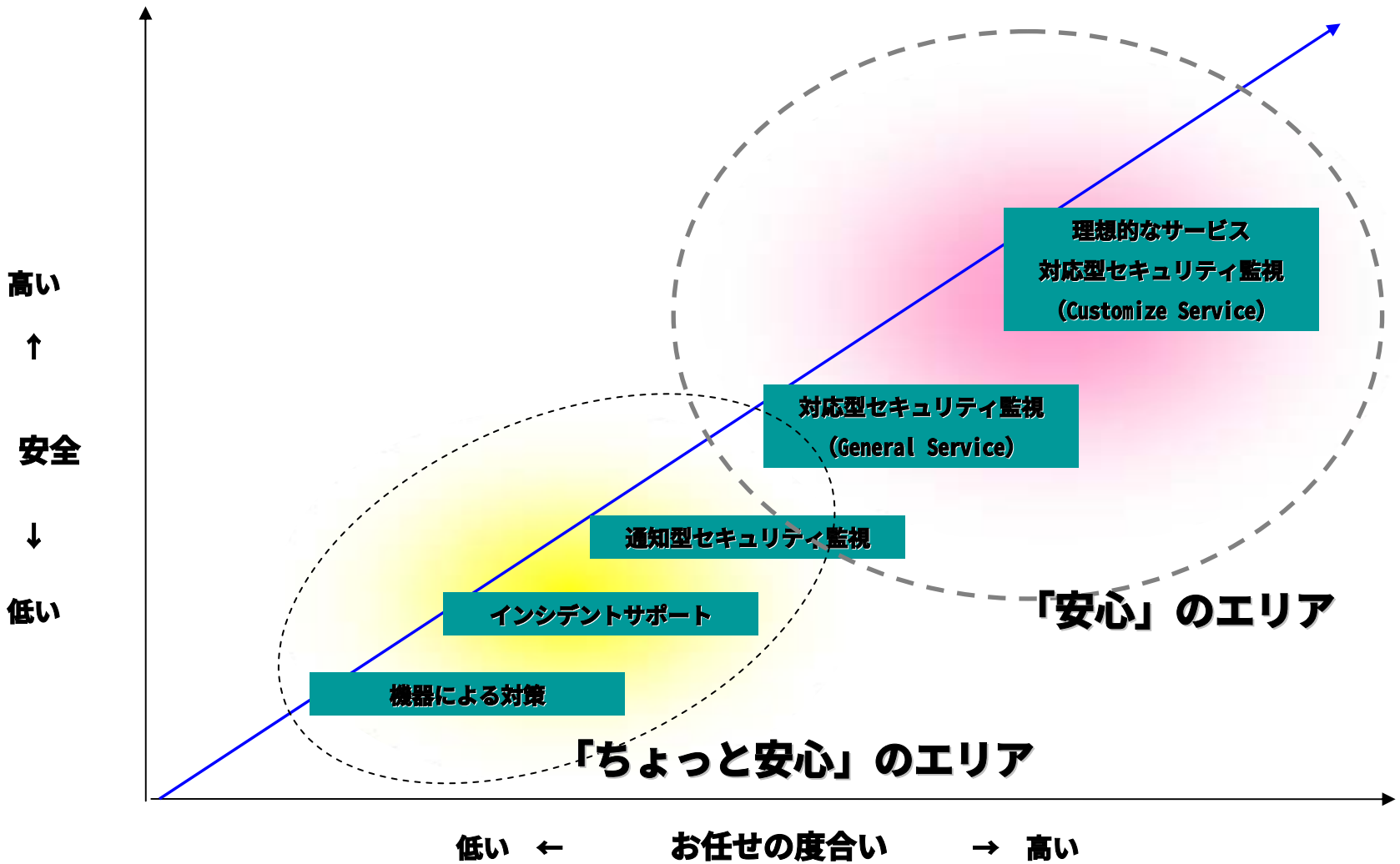
	平成14年	平成13年	平成12年
ｲﾝﾀｰﾈｯﾄ･ｵｰｸｼｮﾝに関する相談	3,978	2,099	1,301
詐欺・悪質商法に関する相談（ｲﾝﾀｰﾈｯﾄ・ｵｰｸｼｮﾝ関係を除く）	3,193	1,963	1,396
名誉毀損・誹謗中傷等に関する相談	2,566	2,267	1,884
違法・有害情報に関する相談	2,261	3,282	2,896
迷惑メールに関する相談	2,130	2,647	1,352
不正ｱｸｾｽ、ｺﾝﾋﾟｭｰﾀｳｲﾙｽに関する相談	1,246	1,335	505
その他	3,955	3,684	1,801
合　　計	19,329	17,277	11,135

※　その他の相談には、プロバイダや有料サービス会社とのトラブルやネットワークセキュリティ全般に関する相談が含まれる。

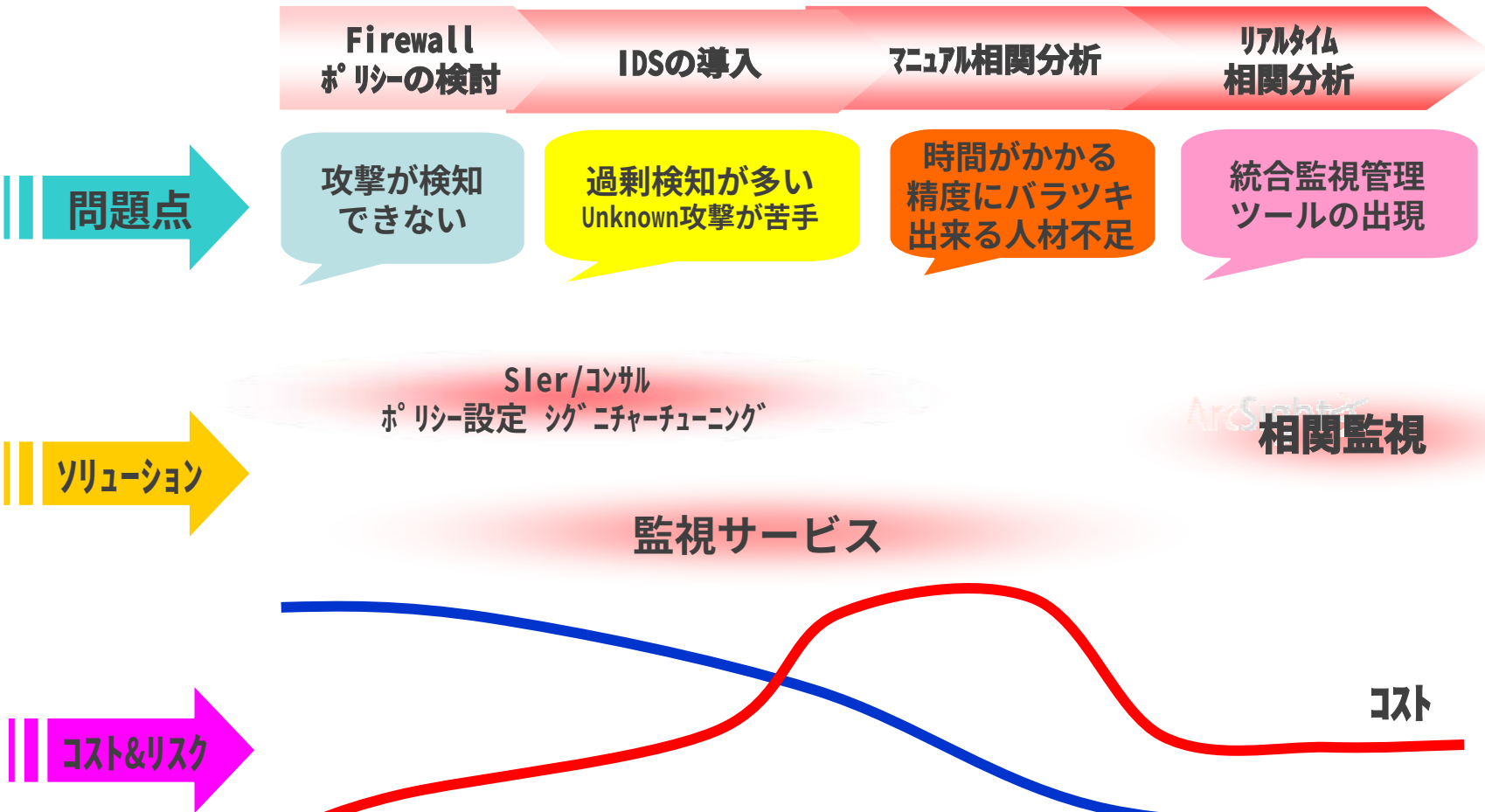
最近議論されている不正アクセス対策

不正アクセス対策の道筋

・　「お任せ」と「安全」の関係　→　「安心」のエリアへ



セキュリティ・インシデント対策動向



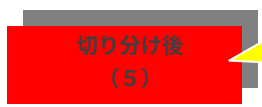
IDS運用上の問題点①

False Positive

－IDSは攻撃の可能性があると判断したとき、たとえ本当に攻撃があった場合ではなくてもアラートを発する。この様に実際には攻撃ではない行為を過剰に検出することを**false positive**という。⇒**切り分けが必要**

意味のあるアラートは

約５％程度



アナリストの**スキル**により

ばらつき有り

↳ 事後対応へ

IDS運用上の問題点②

- NIDSでアラート発生時に必要なAction

１）NIDSのアラートから想定される攻撃方法で関係すると思われる周辺機器の絞り込み

２）保存されている周辺Deviceのログの解析

－FW,HOST(WEB,DNS,Mail,DB etc.)

－長時間時間をかけると意味がない

３）攻撃が成功しているかどうかの切り分け

－あらゆるログの相関関係を見出すには相当の熟練したスキルが必要

IDS運用上の問題点③

➢HIDSでは対応OSが限定されておりWindowsNT4.0はHIDSも動作保証外が大半。

http://www.tripwire.co.jp/　**CSサーバーの動作OS自体の見直しを検討する必要がある。**（他社も同傾向）

Tripwire for Network Devices のインストール

Windows に Tripwire for Network Devices をインストールするには

1. インストール先のマシンが、次の必須要件を満たしていることを確認します。

0 ～ 200 ノードの場合	200 ノードを超える場合
Windows 2000 Professional、SP2 または Windows XP Professional 533MHz のプロセッサ 256MB の RAM 200MB の空きハードディスク領域 256 色ディスプレイ 静的 IP アドレス	Windows 2000 Server、SP2 1GHz 以上のプロセッサ 512MB の RAM 200MB の空きハードディスク領域 256 色ディスプレイ 静的 IP アドレス

2. 管理者権限でログインします。
3. コマンドプロンプトを開きます。
4. 次のコマンドを実行し、TFTP または HTTPS サーバーが動作していないことを確認します。

IDS運用上の問題点④

- HIDSをよしんば設置は出来てもＯＳのＮＴ４．０サーバー自体のサポートが打ち切られる。
- http://www.microsoft.com/japan/products/ntserver/ProductInfo/Availability/retiring.asp
- 今後はセキュリティパッチの配布も終了することが見えている。以下マイクロソフト社のサイトより抜粋

製品のサポートに関して
現在 Windows NT Server 4.0 (Standard Edition、Enterprise Edition、Terminal Server Edition) が動作しているシステムには、以下の有償サポート サービスが提供されています:

プレミア サポート ： 追加料金不要にて、新規ホットフィックス（修正プログラム）開発要求と、既存ホットフィックスの入手が可能です。
プロフェッショナル ： 追加料金不要にて、既存ホットフィックスの入手が可能です。

なお、上記に加え、オンライン サポートでも当該製品に関する技術情報を公開しています。
上記サービスに関して以下の通り変更されます。

2004 年 1 月 1 日
この日より、新規ホットフィックス（修正プログラム）のご提供については、セキュリティ関連のみとさせていただきます。

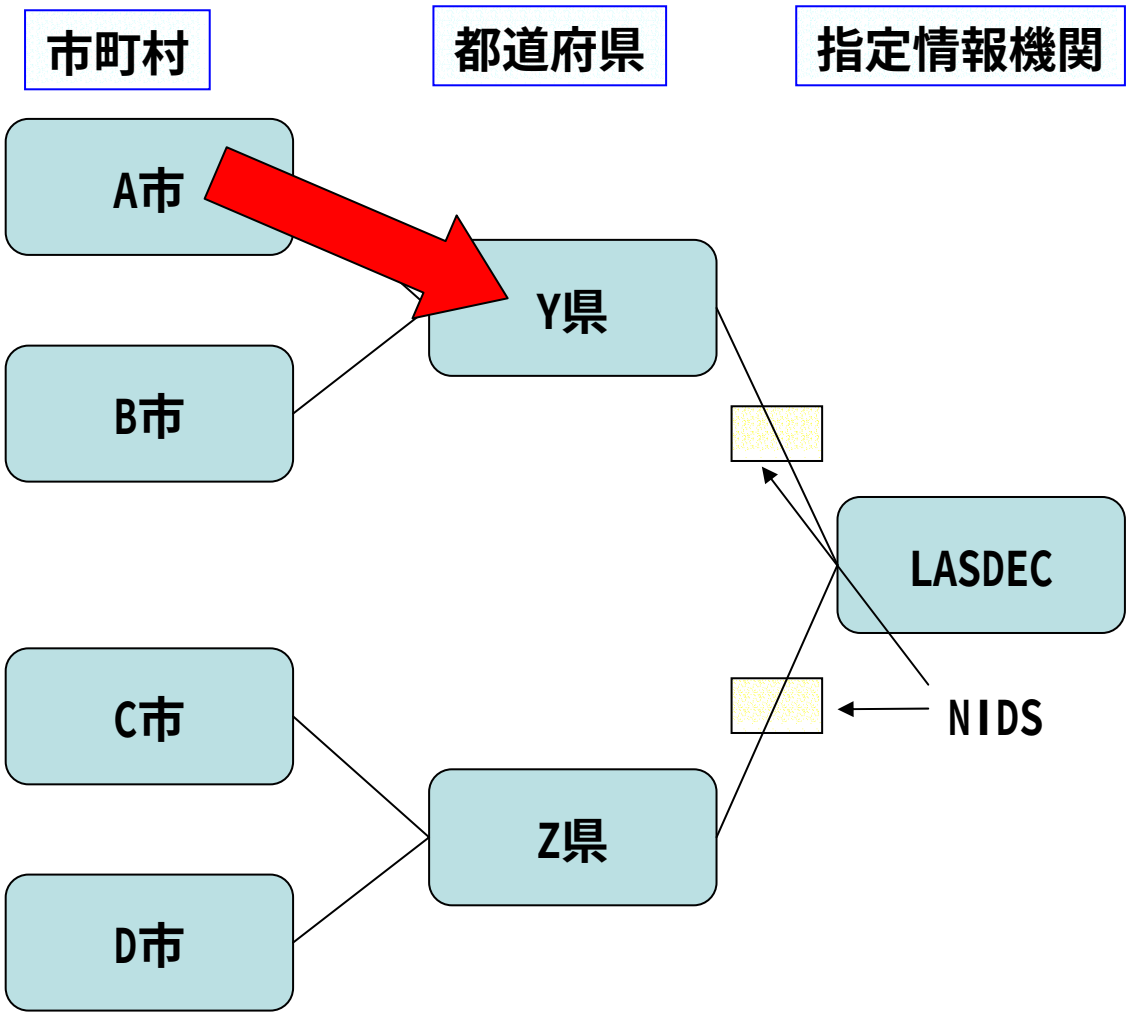
2005 年 1 月 1 日
この日より、プレミア サポートおよびプロフェッショナル サービスはサポート対象外となります。セキュリティ ホットフィックス（修正プログラム）も合わせて対象外となります。

2005 年 1 月 1 日以降
オンライン サポートもご利用いただけません。

LASDEC側の侵入検知装置（NIDS）では検知されない攻撃①

・市町村から都道府県に対する攻撃

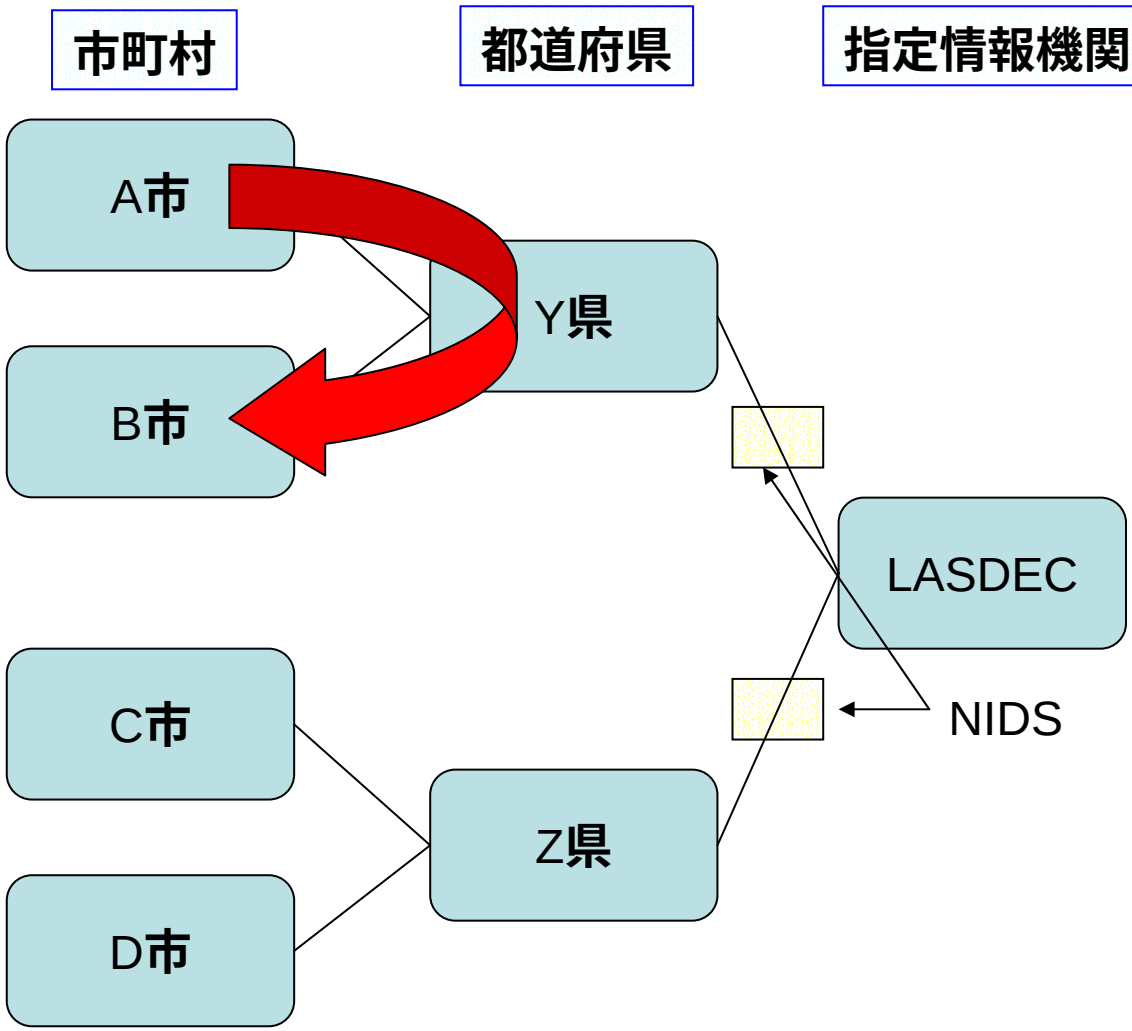
例　- A市の末端端末に物理的にアクセスし、Y県のネットワークに対して攻撃。
論理上は住基ネットワークとインターネットが分離の場合においても、物理的に接続されているならば、ルータ等の設定を変更することで、インターネット側から住基ネットに接続可能なバックドアを設置



LASDEC側の侵入検知装置（NIDS）では検知されない攻撃②

・市町村から市町村に対する攻撃

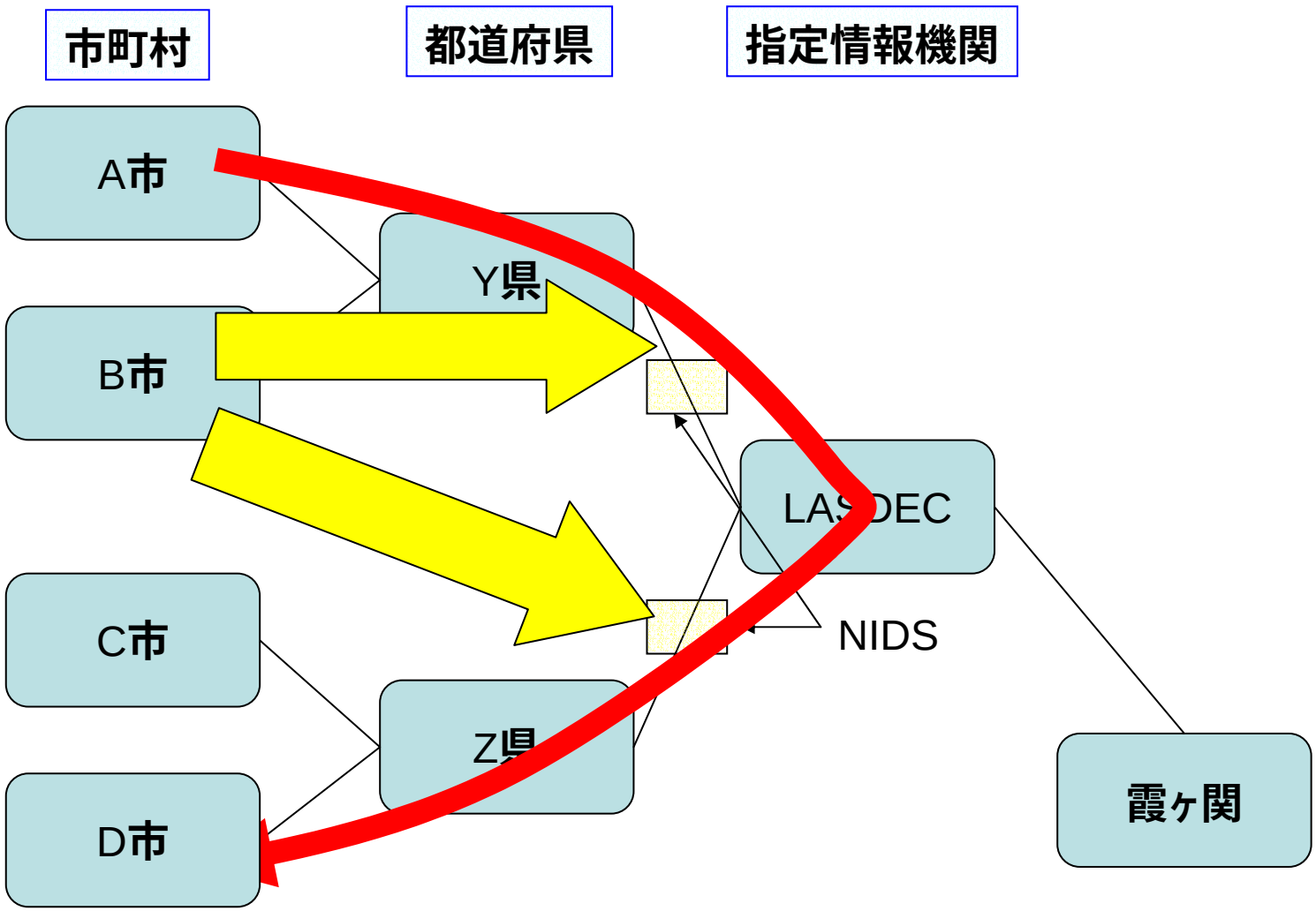
例　- A市の末端端末に物理的にアクセスし、B市のサーバに対して攻撃。
バックドア等を設置することでどこからでも、アクセス可能に。端末にモデム等が設置されている場合は設定変更により、そのモデムに対して外部から接続する可能性等。



LASDEC側の侵入検知装置（NIDS）が無効化される攻撃①

・IDSには検出されるが、大量のアラートを出すことで実質的にIDSを無効化する

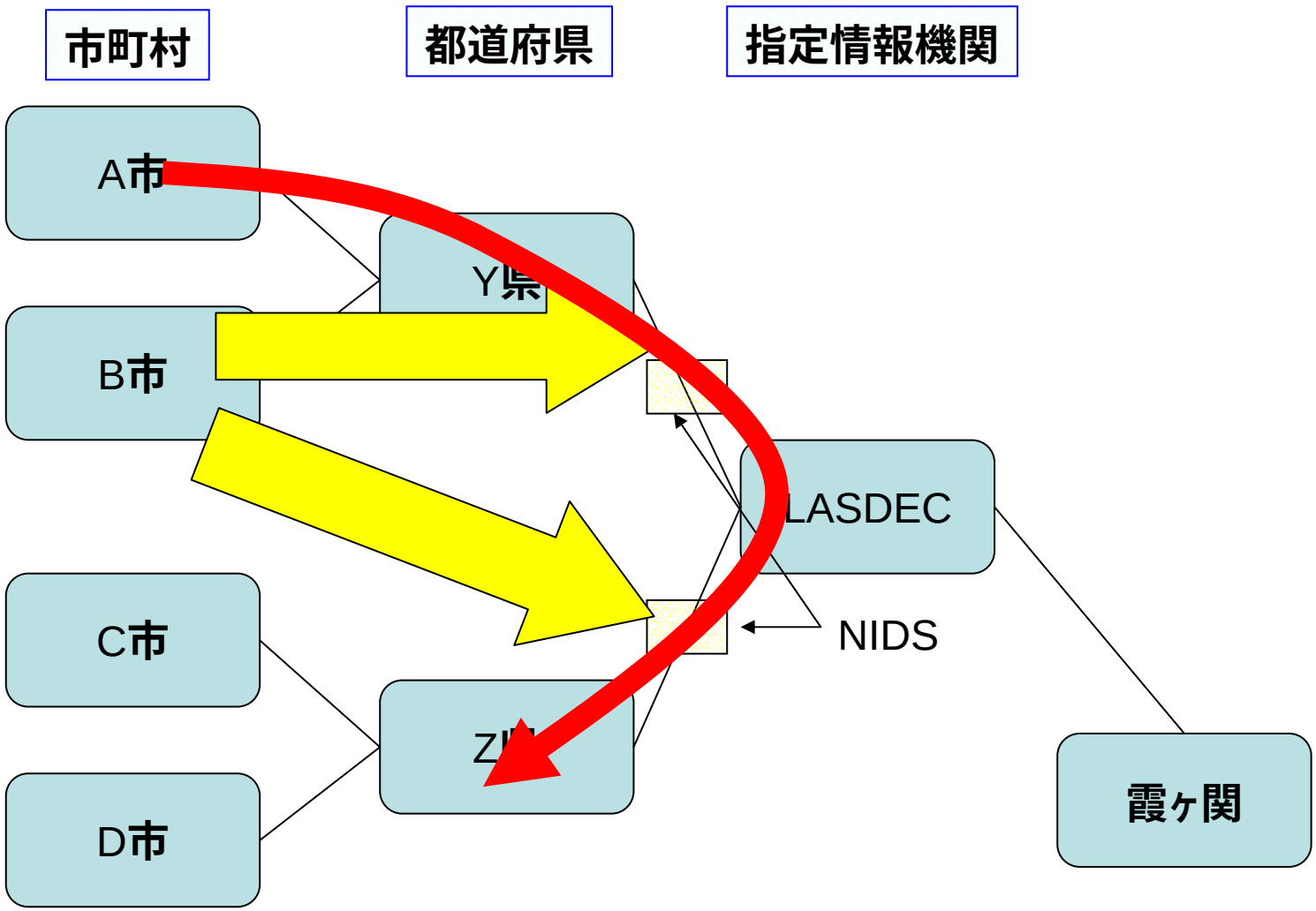
例 – B市からIDSに指定の時刻に大量のアラートが出るようセットし、大量のアラートを出すと同時にA市よりD市に対して攻撃
監視オペレータはB市から攻撃が来ていると思ってしまう。



LASDEC側の侵入検知装置（NIDS）が無効化される攻撃②

・IDSには検出されるが、大量のアラートを出すことで実質的にIDSを無効化する

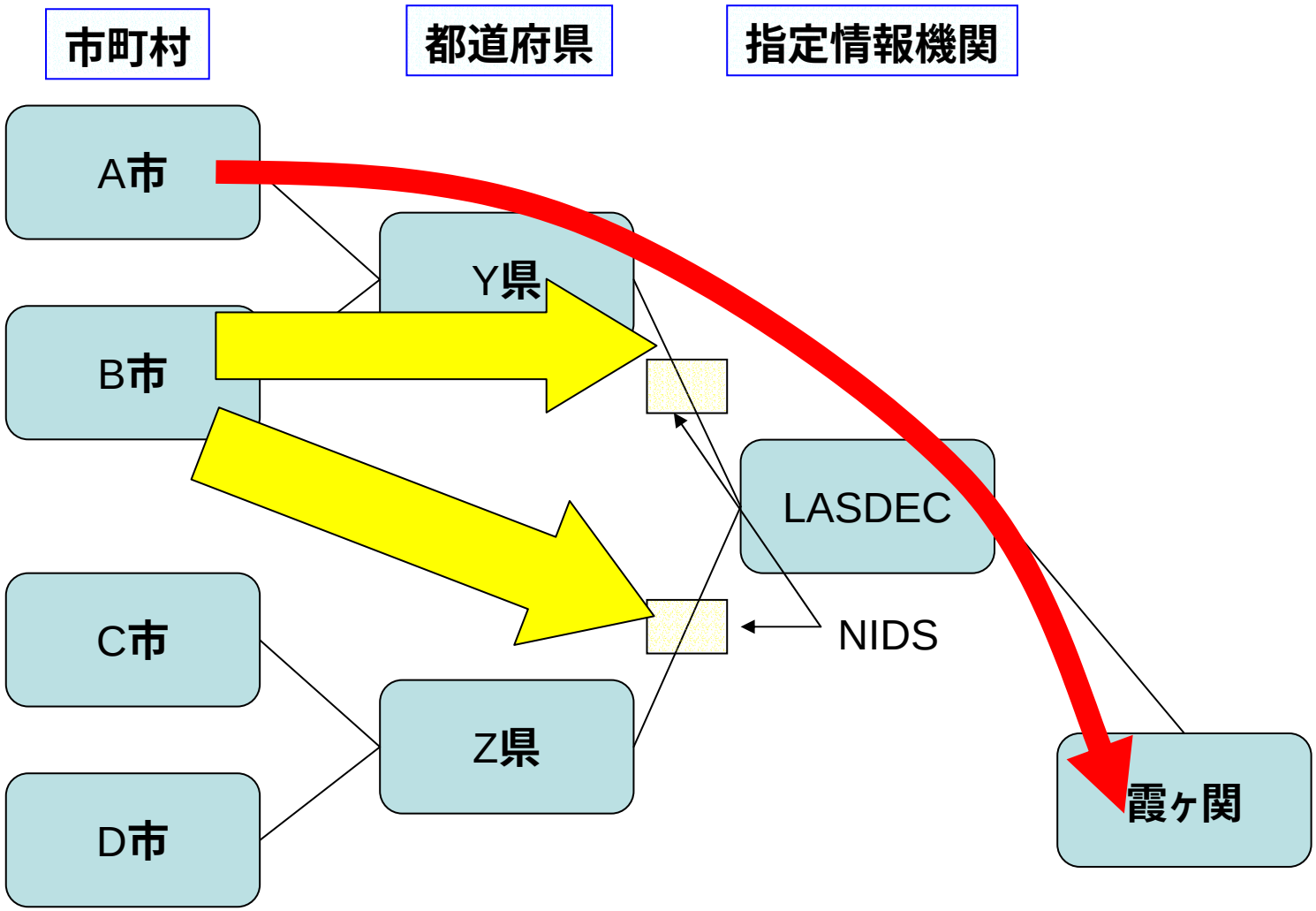
例 – B市からIDSに指定の時刻に大量のアラートが出るようセットし、大量のアラートを出すと同時にA市よりZ県に対して攻撃
監視オペレータはB市から攻撃が来ていると思ってしまう。



LASDEC側の侵入検知装置（NIDS）が無効化される攻撃③

・IDSには検出されるが、大量のアラートを出すことで実質的にIDSを無効化する

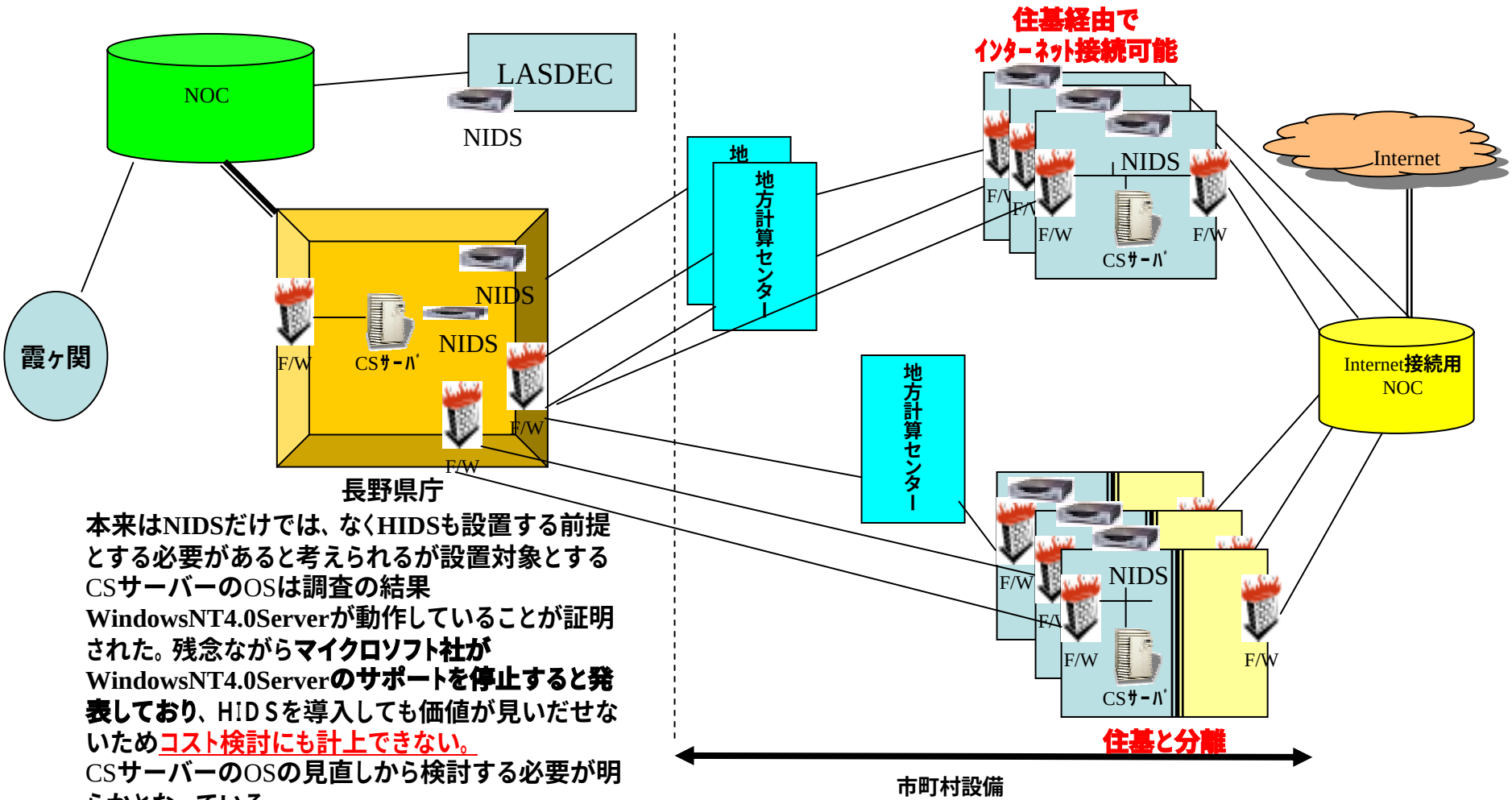
例 – B市からIDSに指定の時刻に大量のアラートが出るようセットし、大量のアラートを出すと同時にA市より霞ヶ関に対して攻撃。
監視オペレータはB市から攻撃が来ていると思ってしまう。



ネットワーク概要とコスト

住基ネットとインターネットはファイアーウォール経由でも分離することを前提とする。

ーファイアイーウォールは、必要なポート番号のみを通過させる関所機能であるので、通過させた中身は管理できない。よってファイアイーウォールは万全でなくインターネットからの脅威は拭えない。



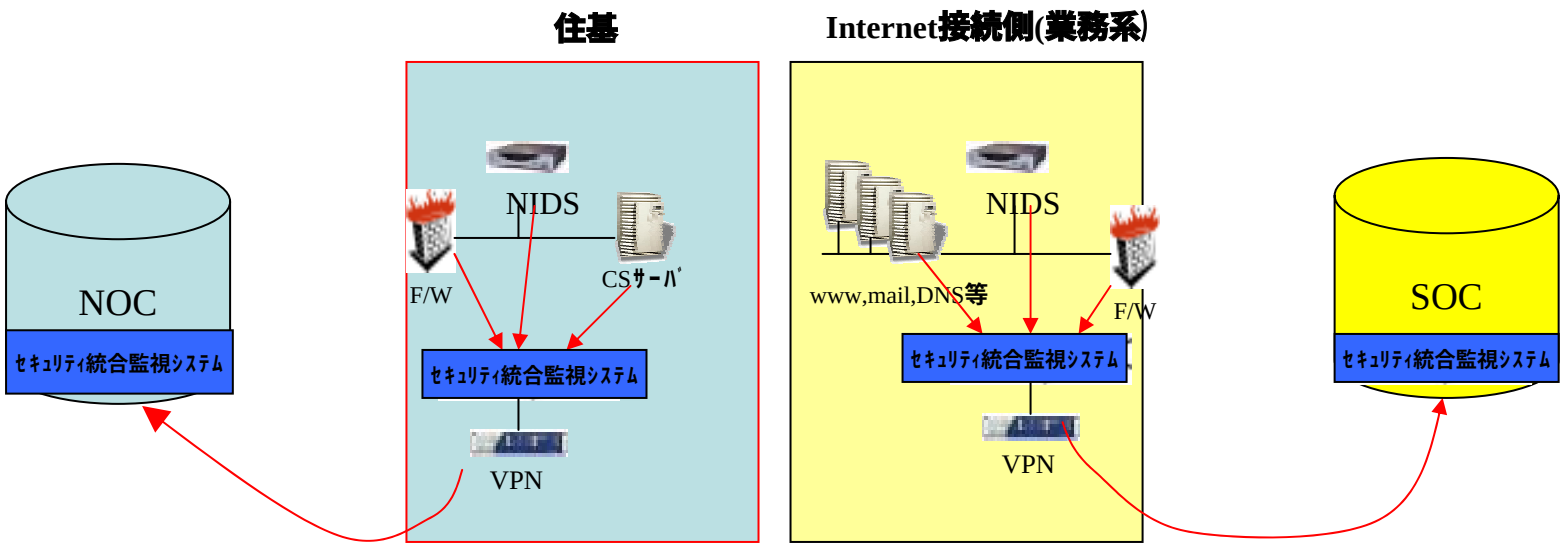
本来はNIDSだけでは、なくHIDSも設置する前提とする必要があると考えられるが設置対象とするCSサーバーのOSは調査の結果WindowsNT4.0Serverが動作していることが証明された。残念ながらマイクロソフト社がWindowsNT4.0Serverのサポートを停止すると発表しており、HIDSを導入しても価値が見いだせないためコスト検討にも計上できない。

CSサーバーのOSの見直しから検討する必要が明らかとなっている。

セキュリティ監視パターン①

大規模（5ヶ所想定）

A市



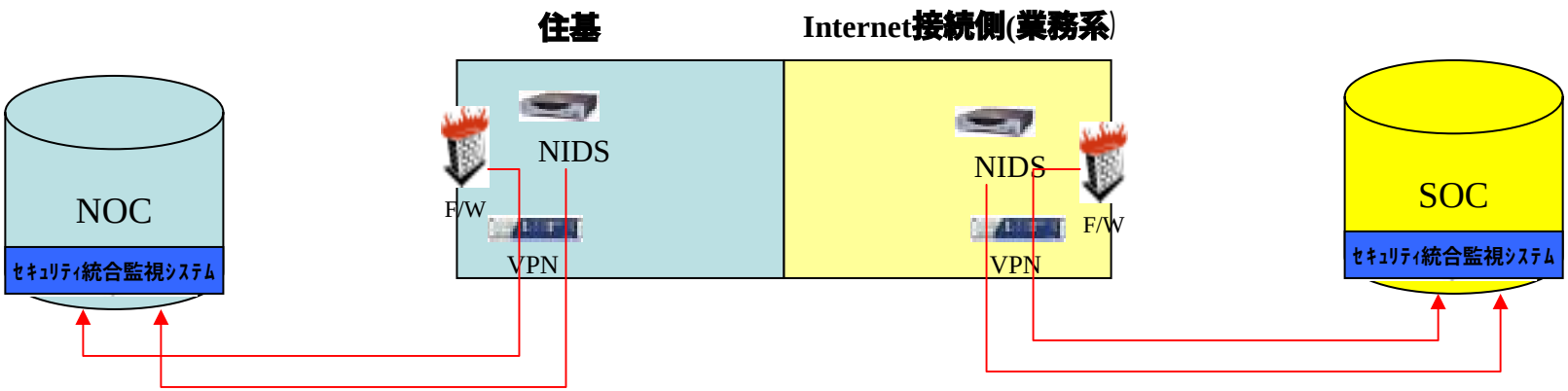
ログの収集経路

- ログの発生量が多い箇所に関しては、セキュリティ監視システムの階層構成を取る（NOC/SOC側が親機、自治体側が子機）
- ログはVPN経由にてNOC/SOCに送信
- FW+IDS＋HOSTの相関分析運用監視業務をNOC/SOCに委託

セキュリティ監視パターン②

中小規模（115ヶ所想定）

B市



ログの収集経路

- ログの発生量はそれ程ないものとし、直接NOC/SOC内のセキュリティ監視システムにログを送信
- 各セグメントに存在するFirewall,IDSのログをVPN経由にてNOC/SOCに送信
- FW+NIDSの相関分析運用監視業務をNOC/SOCに委託

コスト(監視サービス費用)

市町村が監視サービスに支払う費用想定	
	単位:百万円
初期	
ソフト・ハード	520
設計・構築	58
ランニング(年間)	
保守費	101
運用	900
合計	1579

- 規模別に大(5ヶ所)、中小(115ヶ所)に大別
- 規模大の場合、住基側の監視費用40万円／月、Internet接続側を80万円／月に設定
- 規模中小の場合、住基側の監視費用30万円／月、Internet接続側を30万円／月に設定
- 監視対象はFW+NIDS+(HOSTの生死)
- 監視サービス内容は全て相関分析することが前提

コスト(監視センター、平日9時-17時)

監視設備費用(平日9－17時対応)	
	単位:百万円
初期	
ソフト・ハード	131
設計・構築	15
ランニング(年間)	
保守費	24
運用	167
合計	337

- 監視時間平日9時－17時
- 住基側監視用(NOC)にシステム一式、Internet接続側監視用に(SOC)にシステム一式
- 監視Sensor数は480台で設計
- オペレータ8名、アナリスト1名での運用を想定
- 監視対象はFW+NIDS+(HOSTの生死)
- 監視サービス内容は全て相関分析することが前提

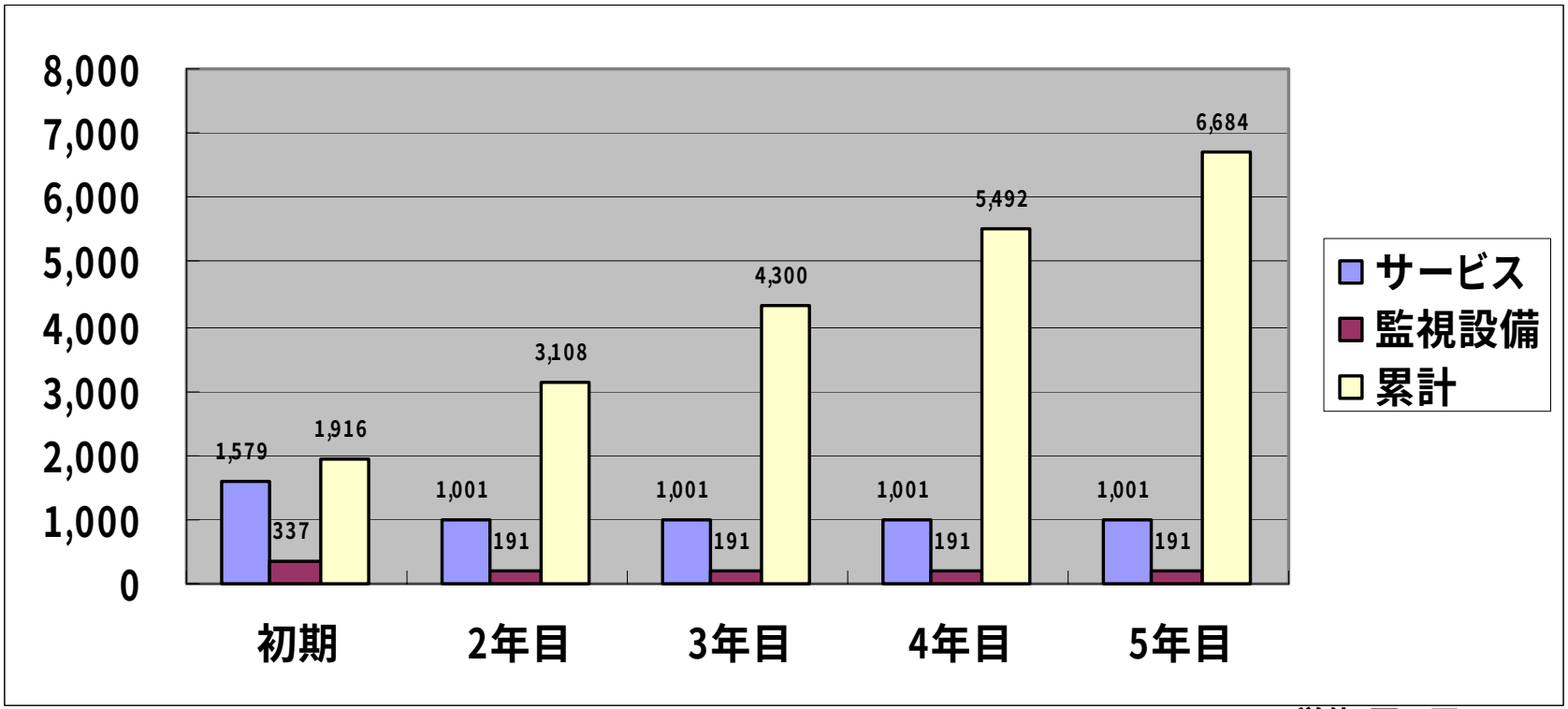
コスト（監視センター、24時間365日）

監視設備費用（24時間365日対応）	
	単位：百万円
初期	
ソフト・ハード	131
設計・構築	15
ランニング（年間）	
保守費	24
運用	500
合計	671

- 監視時間24時間365日
- 住基側監視用（NOC)にシステム一式、Internet接続側監視用に（SOC)にシステム一式
- 監視Sensor数は480台で設計
- オペレータ24名、アナリスト3名での運用を想定
- 監視対象はFW+NIDS+(HOSTの生死)
- 監視サービス内容は全て相関分析することが前提

総額コスト(平日9時-17時)

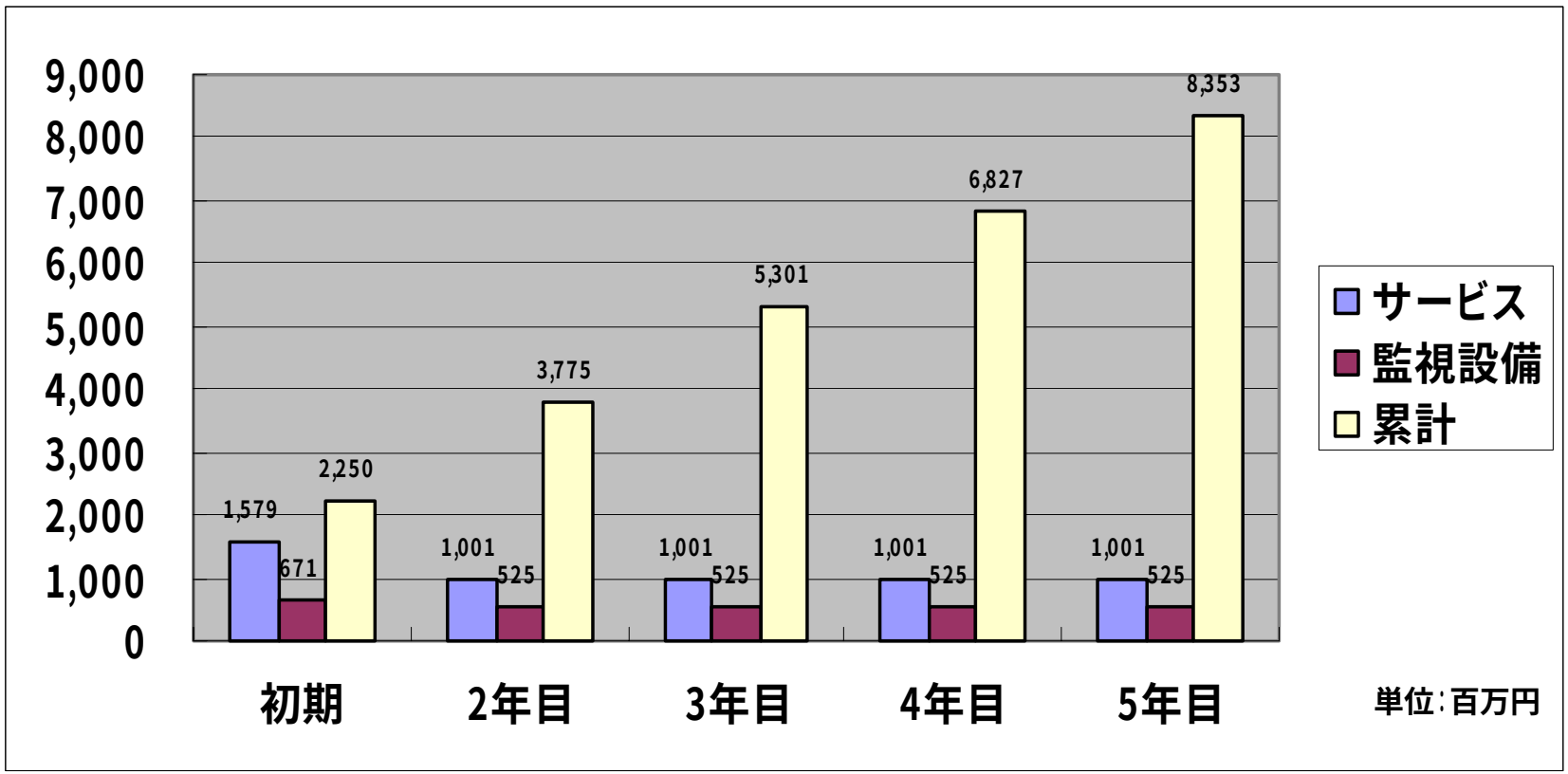
累計金額は5年間でおよそ70億円弱



単位:百万円

総額コスト（24時間365日監視）

5年間の累計はおよそ80億円強



結　論

費用対効果では算出出来ないコストが永続的に発生します。

1．いかなる手法を用いても万全な状態を確保することは不可能である。
2．安全性を高めるためにはリスクとする目的単位に
　リスクをコンポーネット化する。
3．コンポーネント化したリスクに対するセキュリティポリシーを作成する。
4．セキュリティポリシーにマッチした運用をおこなう。
5．運用の状況を管理する管理監視体制を整備する。
6．管理監視体制は客観的な第3者とし、県は審議会等によりその第3
　者を監査できる。
7．問題発生時に最大限の運用維持とリスクの最小化を行うべく
　対応フォーメーションをポリシーとは別にアクションルールを確立する。
8．上記項目を永遠に維持する。