Internet Week 2003

インテリジェントレベルによる多段防御

Multi-Layer Protection by intelligent level of Analysis.

セキュリティ監視を主軸にした防御と インシデントレスポンス

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

スピーカ紹介

にし　もと　いつ　ろう
西 本 逸 郎

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実施

株式会社ラック JSOC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

1. 旬？な話題から、、、MS Blaster

1. 旬？な話題から、、、MS Blaster

JSOCセキュリティアナリストレポート※1発表後、大手企業を含め、一番多かった質問

「うちはファイアウォールがあるから大丈夫ですよね？」

⇒ 脅威はインターネットからやってくる

⇒ ファイアウォールで（135番を）防いでいるから安心

裏にあること、、、

だから、パッチはあてなくて良いよね！

⇒ PCの持ち込みで感染 ※2 JSOCセキュリティアナリストレポート参照

入らない事が前提だと被害甚大！

※1 、※2 JSOC セキュリティアナリストレポート

http://www.lac.co.jp/security/jsoc/report/

1. 旬？な話題から、、、MS Blaster

MS Blaster時の多くの組織での反省点
今回、分かってしまった事

1. 連絡体制	→	事件対応の根幹
2. 被害内容・原因・規模把握	→	コンピュータフォレンジックス
3. 局所化方法・再開手順	→	想定してない
4. 情報ライフラインが不明	→	事業継続計画
5. 事前の脅威予測の甘さ	→	リスク分析のフレームワーク
6. ウイルス定義ファイル	→	ウイルスに対する対策の勘違い
7. セキュリティポリシーの形骸化	→	大問題

1. 旬？な話題から、、、MS Blaster

特に、、

7. セキュリティポリシーの形骸化 は大問題！

運用する気がないのなら、無駄・邪魔・有害
まあ、対外的な言訳にはつかえるかも、、
言訳に使えるところはまだまし、、(☆o☆)

⇒ 責任者(経営者)のコミットメント
民間と公官庁系の大きな違い

ISMS2.0

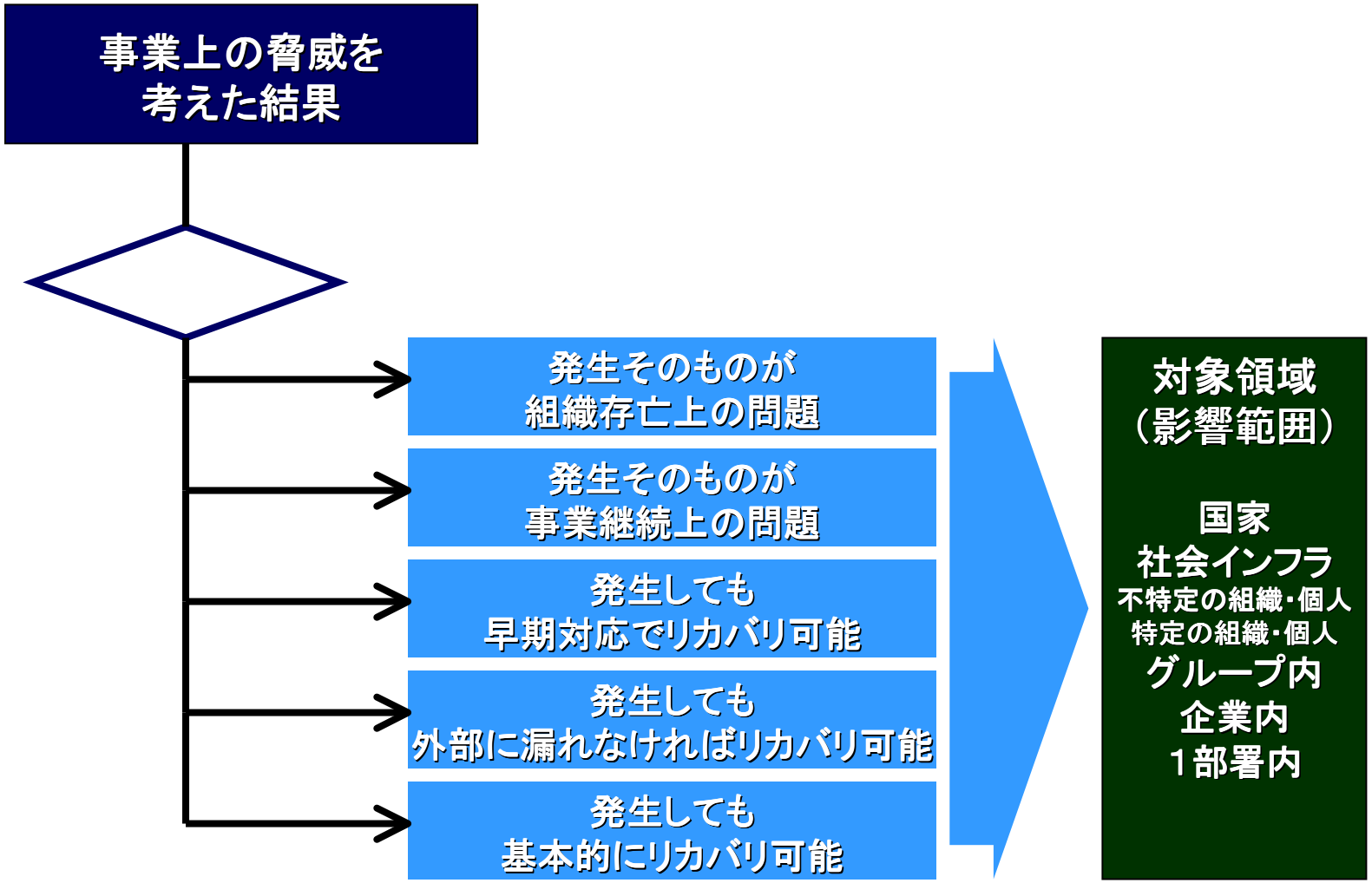
運用するつもりのない・出来ないポリシーは作らない事！！

⇒ 本気でリスク分析が必要と分かるはず

2. 事故を想定した対策の考え方

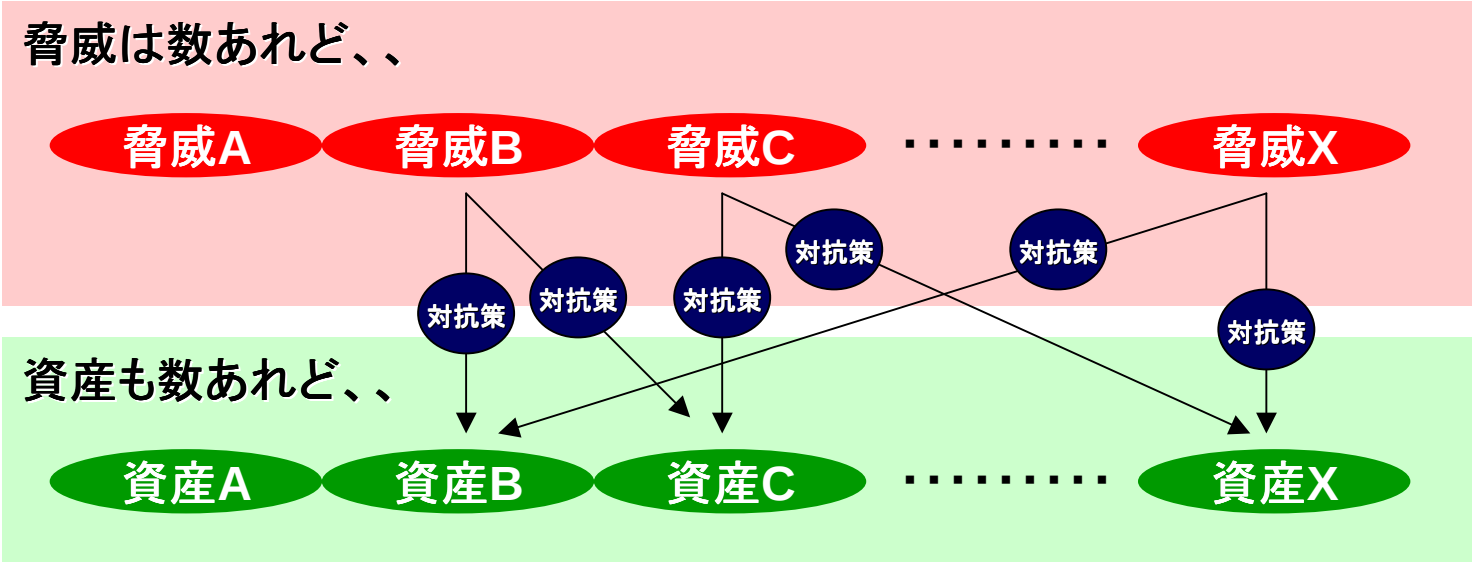
2. 事故を想定した対策の考え方

■セキュリティ対策の目的



2. 事故を想定した対策の考え方

■方針の考え方



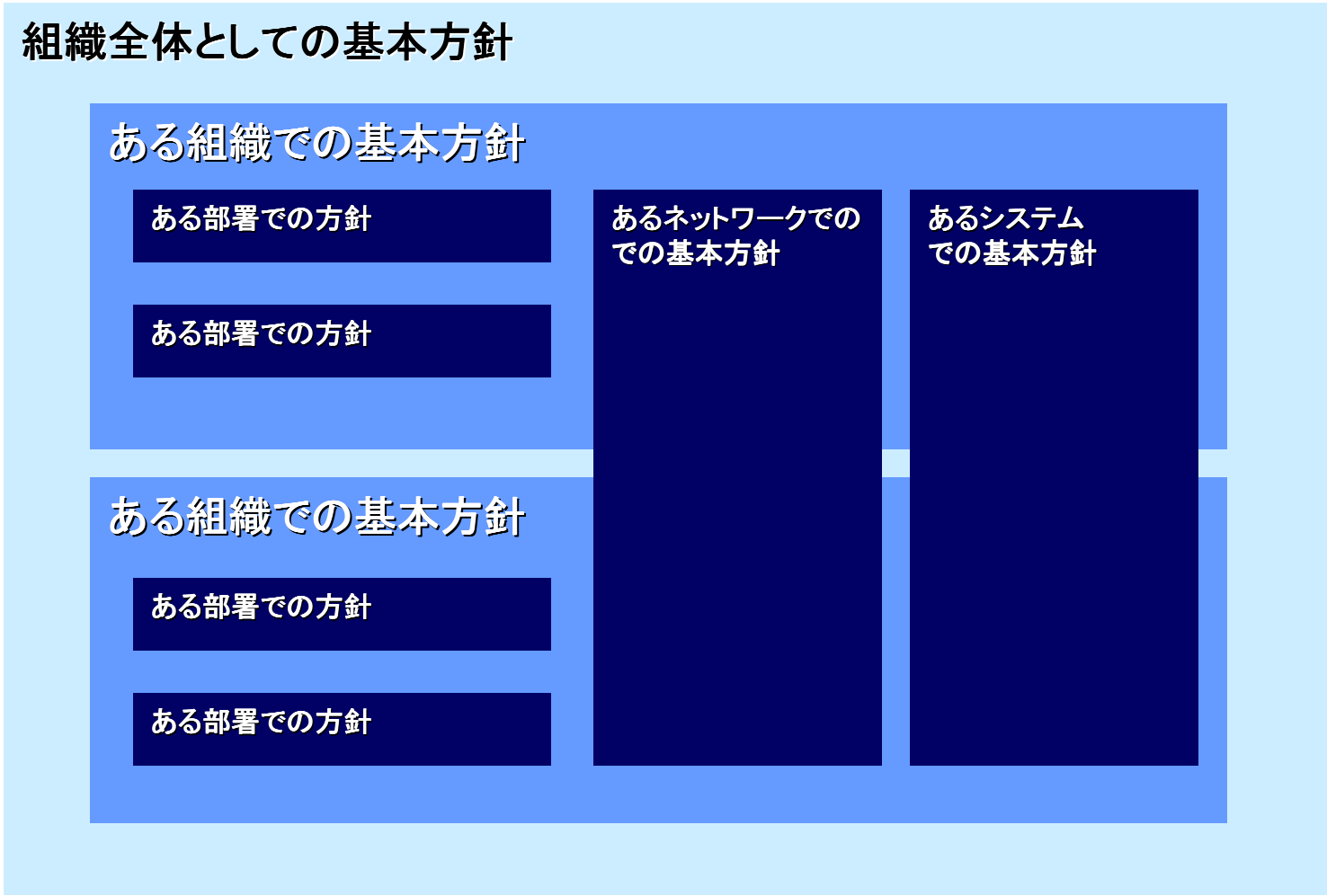
ポイントは、、

何が、どうなれば問題なのか？

対応の軸足をはっきり決めておくこと

2. 事故を想定した対策の考え方

■セキュリティ対策の目的



2. 事故を想定した対策の考え方

想定している事象は？

影響のカテゴリ	内容		リスクのカテゴリ
社会一般	人命に関わる事 プラント火災等物理的な被害に関わる事 国民の安全保障に関わる事 一般の社会生活や経済活動に関わる事 など	どの規模で どんな影響が	社会的責任
特定の第三者	個人情報・プライバシーに関わる事 犯罪に関わる事 第三者の犯罪の荷担・助長に関わる事 第三者に迷惑をかける事 など	だれに どの程度の 法的には？ 何に違反？	法的責任 コンプライアンス 不祥事
自組織	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 WEB改竄 等	どの規模で どんな影響が	自己責任

⇒ リアルタイムでのリスク分析が重要！

初動対応に大きな違い！

2. 事件・事故処理から考えるリスク分析

前述の「影響のカテゴリ」を判断するには、、

脅威のレイヤ		直接脅威	副次脅威
技術上の脅威	一般的な脅威	攻撃を受けることにより 懸念される一般的な脅威 Ex. ファイル改ざんが可能 情報が漏洩可能	対抗策により新たに発生する 一般的な脅威 Ex.パッチによりデグレード 機能制限
	個別に考慮すべき脅威	上記により個別に 考慮すべきの脅威 Ex. WWW改ざん 踏台になる DBが破壊される	実施する対抗策により 個別のシステムとして 懸念される脅威 Ex. サービス停止 バックアップが取れなくなる
事業上の脅威		上記により事業分野として 懸念される固有の脅威 前述の「影響のカテゴリ」 とその程度や影響範囲	対抗策により事業分野として 懸念される固有の脅威 Ex. 予定外の支出 営業損失

3. 事件/事故処理プロセスのポイント

3. 事件/事故プロセスのポイント

事件/事故処理のプロセスの肝は、リスクの理解にあります。

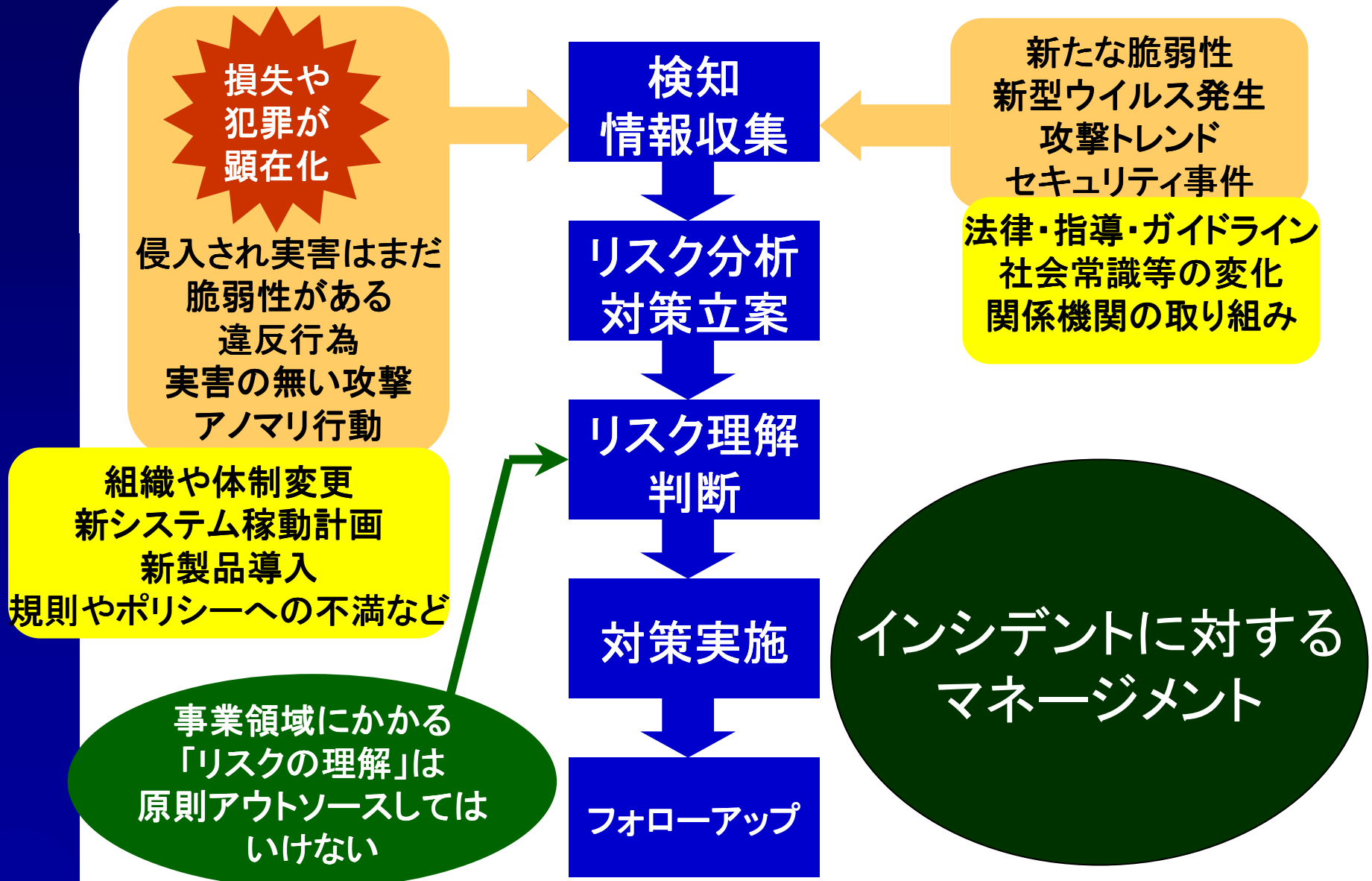
なぜならば、気が付かない事には誰も動けないからです。

リスクを理解するためには、事件発生を待っているのではだめです、普段からの訓練が重要です。

では、どういったことが訓練になるのでしょうか？

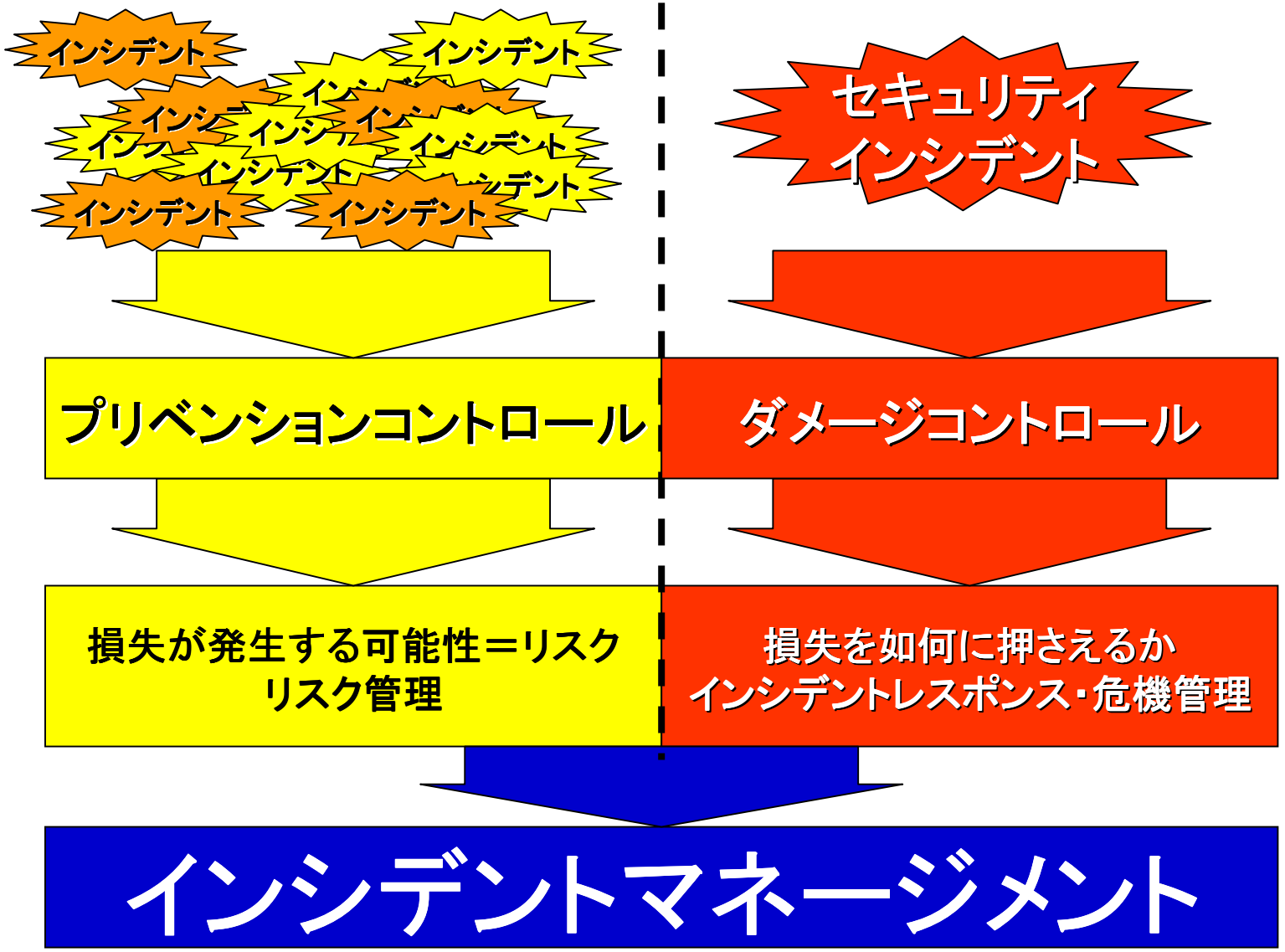
また、全て自分たちでやらなければならないのでしょうか？

3. 事件/事故プロセスのポイント



3. 事件/事故プロセスのポイント

■インシデントマネージメント



3. 事件/事故プロセスのポイント

1. 想定しておく事=危機意識
2. 極力アウトソースする
   アウトソース出来ない事の理解
3. いつでも訓練は出来る
   セキュリティバランスを崩す可能性のある事象は日常茶飯事
4. インシデントマネージメント

4. 知恵のレベルによる多段防衛

4. 知恵のレベルによる多段防御

これまでの成功しているセキュリティ製品は？

1. ファイアウォール
2. アンチウイルスソフト

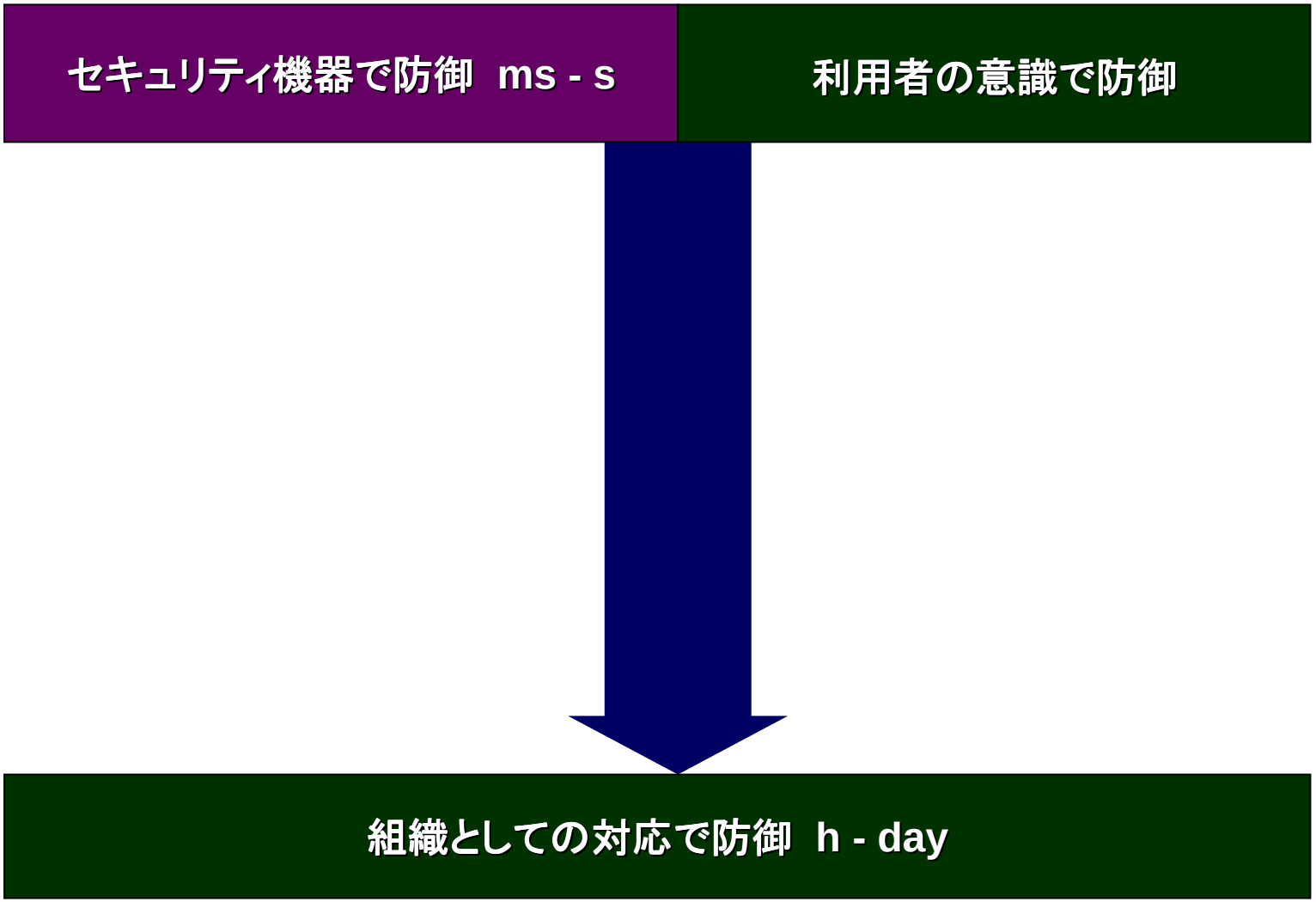
その他は？・・・・・・・・・ IDS、検査ツール、、、、

⇒ セキュリティソリューションは守る事が条件

各種のセキュリティ製品が
何をどうやって守るかを考えてみよう！

4. 知恵のレベルによる多段防御

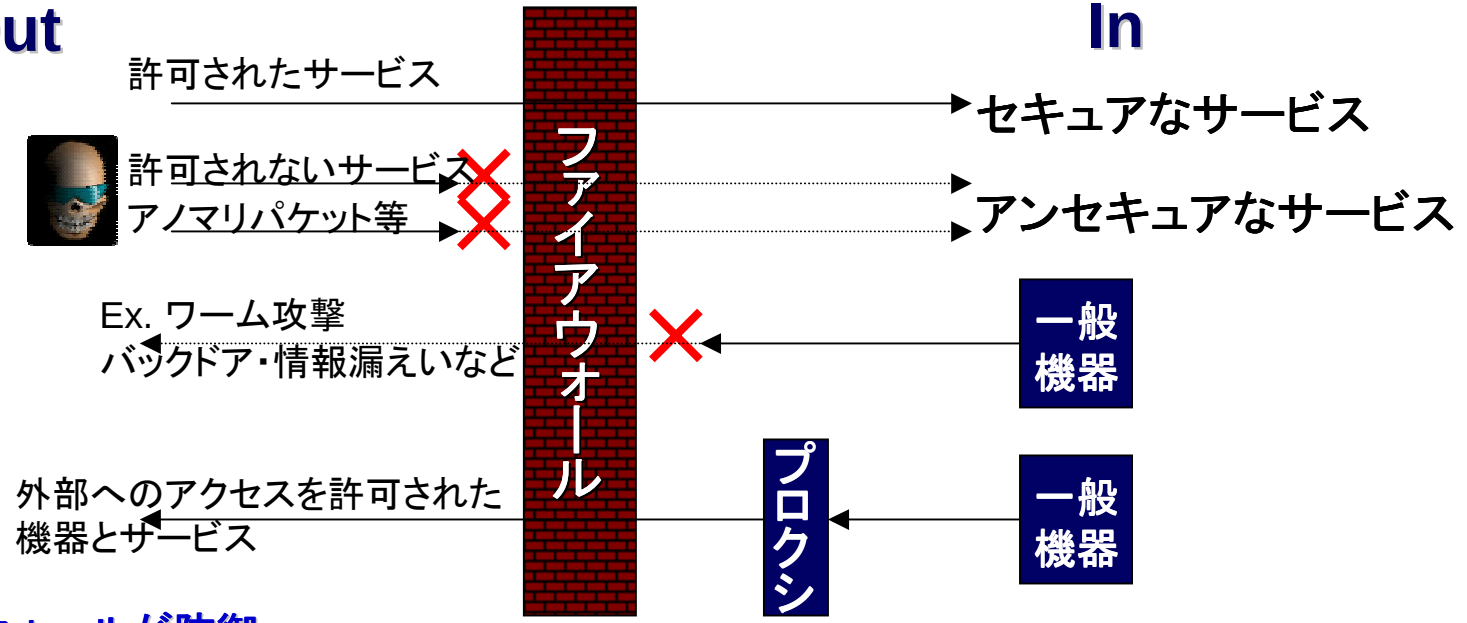
一般的な防衛の現状



4. 知恵のレベルによる多段防衛

■セキュリティ機器による防御

1. ファイアウォールは何を守るか？



ファイアウォールが防御

1. 外部に公開できない脆弱なサービスを外部脅威から防御
2. 外部に対するバックドアや情報漏えい・外部への攻撃の脅威から防御
3. Synfloodやアノマリパケットを使用した攻撃から防御

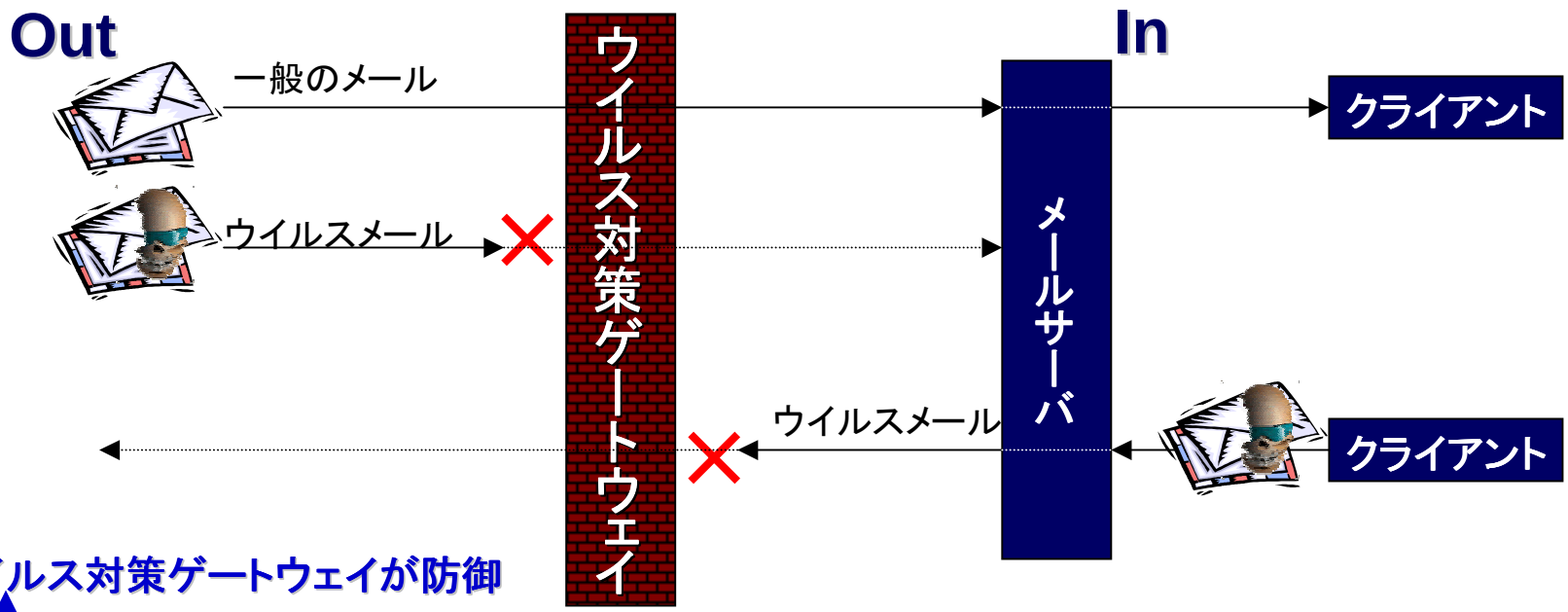
4. 許可されたサービスに対するブルートフォースを検出し他リスク分析実施し手を打つ
5. 上記2. 発生時にログなどを調査・他リスク分析実施し手を打つ

ファイアウォールがヒントをくれる

4. 知恵のレベルによる多段防衛

■セキュリティ機器による防御

2. ウイルス対策ソフトは何を守るか？　ゲートウェイ



ウイルス対策ゲートウェイが防御

1. 外部からウイルス侵入を防御
2. 外部へのウイルスばら撒きの脅威から防御

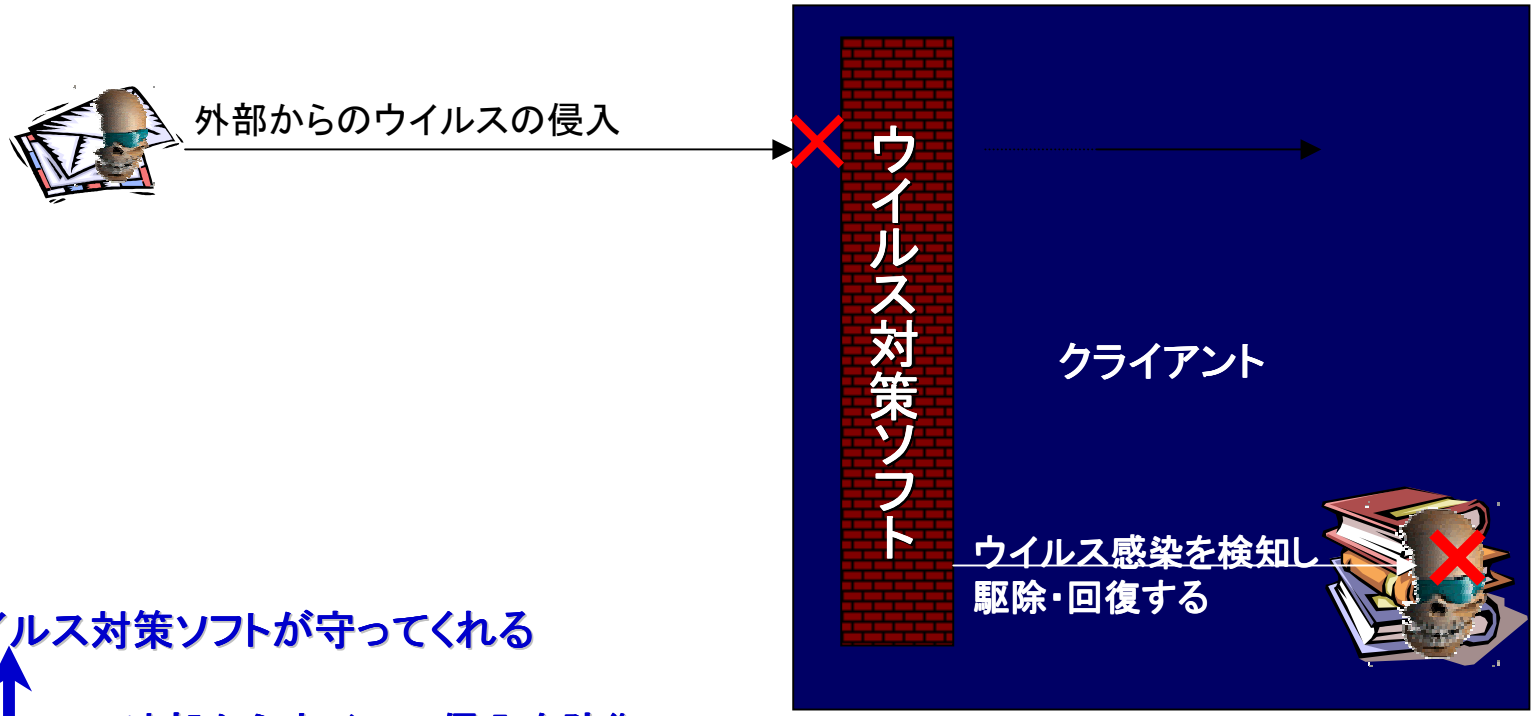
3. 上記2. 発生時にログなどを調査・他リスク分析実施し手を打つ

ウイルス対策ゲートウェイがヒントをくれる

4. 知恵のレベルによる多段防衛

■セキュリティ機器による防御

2. ウイルス対策ソフトは何を守るか？　クライアント対策



ウイルス対策ソフトが守ってくれる

1. 外部からウイルス侵入を防御
2. 感染したファイルなどを検知し駆除・回復させる

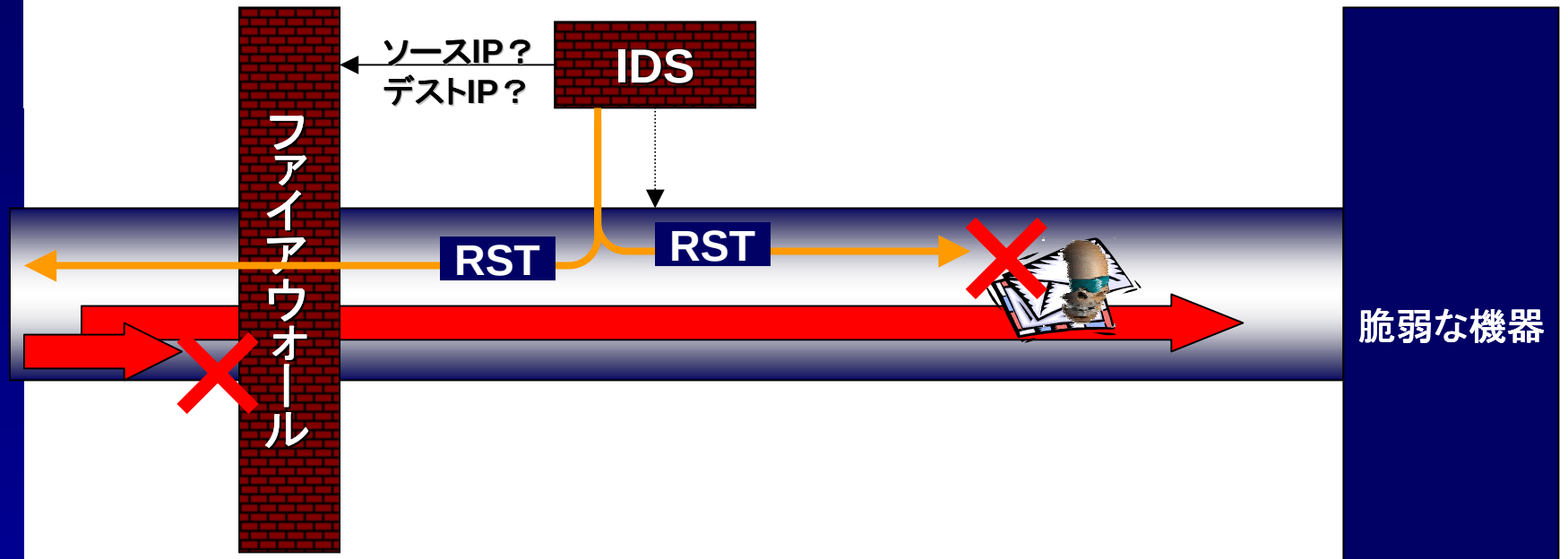
3. 上記2. 発生時にログなどを調査・他リスク分析実施し手を打つ

ウイルス対策ソフトがヒントをくれる

4. 知恵のレベルによる多段防衛

■セキュリティ機器による防御

3. IDSは何を守るか？



IDSが守ってくれる

1. 攻撃を検知しRSTパケット送出でセッションを中断させ防御する
2. 攻撃を検知しFWに指令を与え以降のアクセスを止める事で防御する

3. 検知した攻撃の内容・対象機器の状態・応答などを分析し手を打つ

IDSがヒントをくれる

4. 知恵のレベルによる多段防衛

■セキュリティ機器による防御

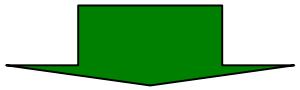
3. IDSは何を守るか？

1. 攻撃を検知しRSTパケット送出でセッションを中断させ防御する
2. 攻撃を検知しFWに指令を与え以降のアクセスを止める事で防御する

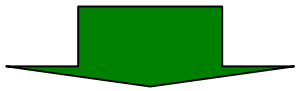
- □ 間に合うか？
- □ UDP、ICMPは？
- □ ワーム発生時は？

⇒ ポイント

1）ワームは対象外
2）TCPを使用しての攻撃
3）一撃で終わらない攻撃



元々フォールスポジティブが多い世界



運用管理

対象が保有している脆弱性に特化したシグネチャ
⇒ 攻撃ツールをある程度限定など
いずれにせよ、限定的なため守る機能はIPSへ移行

4. 知恵のレベルによる多段防衛

■セキュリティ機器による防御

3. IDSは何を守るか？

3. 検知した攻撃の内容・対象機器の状態・応答などを分析し手を打つ

- □ 本当に攻撃か？攻撃は効いたのか？
- □ 攻撃者のかく乱に引っかからないか？
- □ ワーム発生時は？ ⇒ ポイント

分析に適したIDS

↓

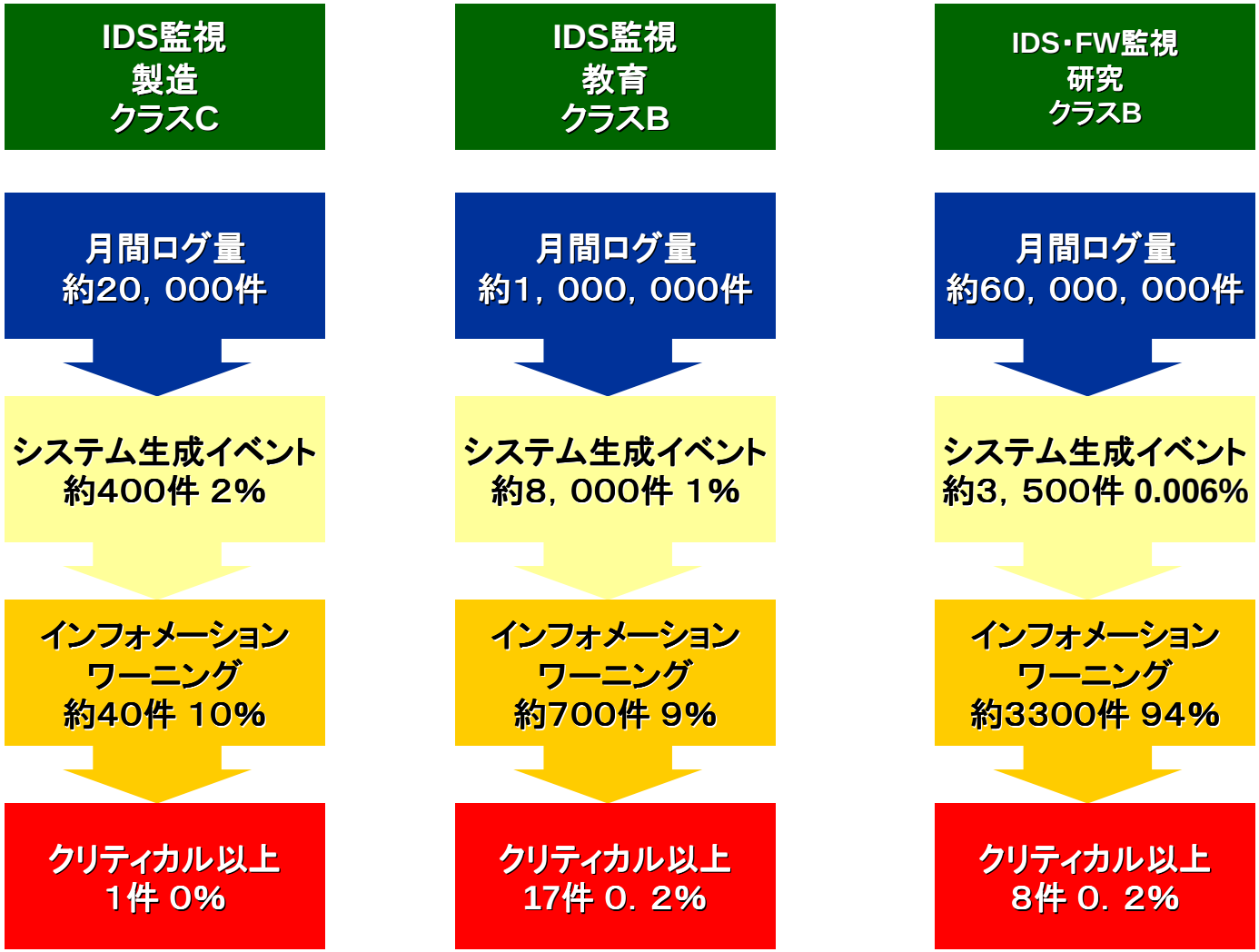
セッション情報の分析が可能である事

↓

大量のアラートを整理できる事

4. 知恵のレベルによる多段防衛

大量のアラートを如何に整理するか（実例）

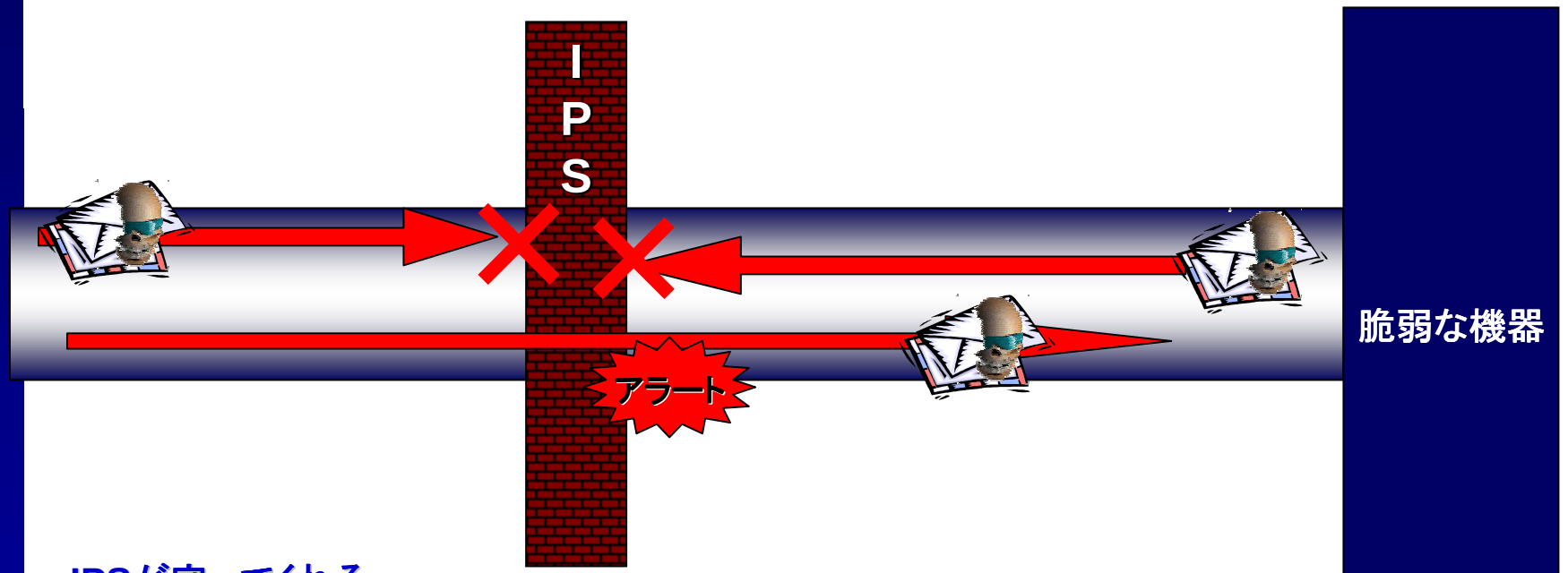


※ 実際に生成されるログ量や生成イベントなどの数量は実際の環境に依存します。あくまでも目安です。

4. 知恵のレベルによる多段防衛

■セキュリティ機器による防御

4. IPS（Inline型）は何を守るか？



IPSが守ってくれる

1. 攻撃を検知し防御する
2. 攻撃を検知し防御後、さらにアクセスを止める事で防御する など

3. 検知した攻撃の内容・対象機器の状態・応答などを分析し手を打つ

IPSがヒントをくれる

4. 知恵のレベルによる多段防衛

■セキュリティ機器による防御

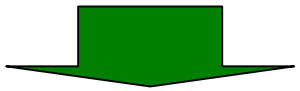
4. IPS（Inline型）は何を守るか？

1. 攻撃を検知し防御する
2. 攻撃を検知し防御後、さらにアクセスを止める事で防御する など

□ フォールスポジティブ？
□ 可用性？

⇒ ポイント

1）ワームは対象
2）保有している脆弱性に特化したシグネチャ
　攻撃ツールなどを限定
3）冗長構成・保守・テクニカルサポート



1. シグネチャのカスタマイズ性
   防御へのフォールスポジティブの回避
2. 可用性への考慮　フェイルオープン等
3. 保守・テクニカルサポート体制

4. 知恵のレベルによる多段防衛

■セキュリティ機器による防御

4. IPS（Inline型）は何を守るか？

3. 検知した攻撃の内容・対象機器の状態・応答などを分析し手を打つ
   - □ 本当に攻撃か？攻撃は効いたのか？
   - □ 攻撃者のかく乱に引っかからないか？

⇒ ポイント

分析に適した機能

セッション情報の分析が可能である事

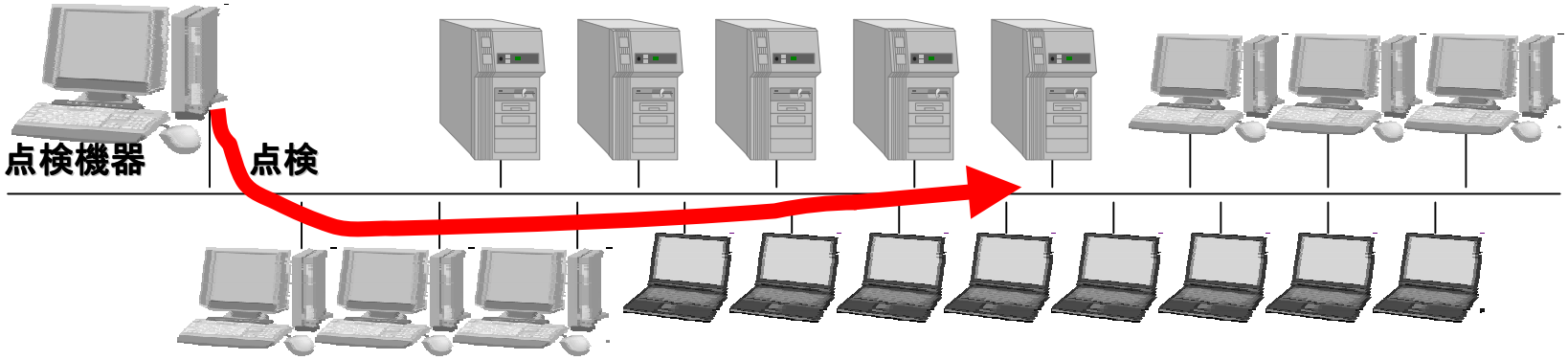
大量のアラートを整理できる事

シグネチャを防御用と分析用に分離

4. 知恵のレベルによる多段防衛

■セキュリティ機器による防御

5. セキュリティ点検ツールは何を守るか？



セキュリティ点検ツールが守ってくれる

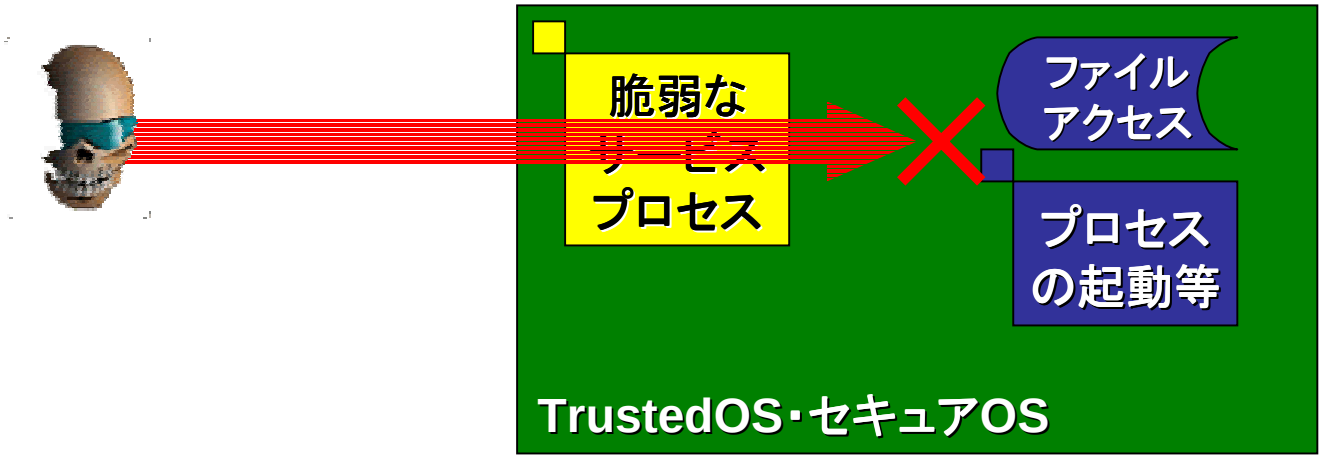
1. 点検結果を分析し手を打つ

セキュリティ点検ツールがヒントをくれる

4. 知恵のレベルによる多段防衛

■セキュリティ機器による防御

6. セキュアOS・TrustedOSは何を守るか？



セキュアOS・TrustedOSが守ってくれる

1. 侵入者の無認可での権限行使を防御する
2. 管理者の権限乱用抑止　など

3. ログを分析し手を打つ

セキュアOS・TrustedOSがヒントをくれる

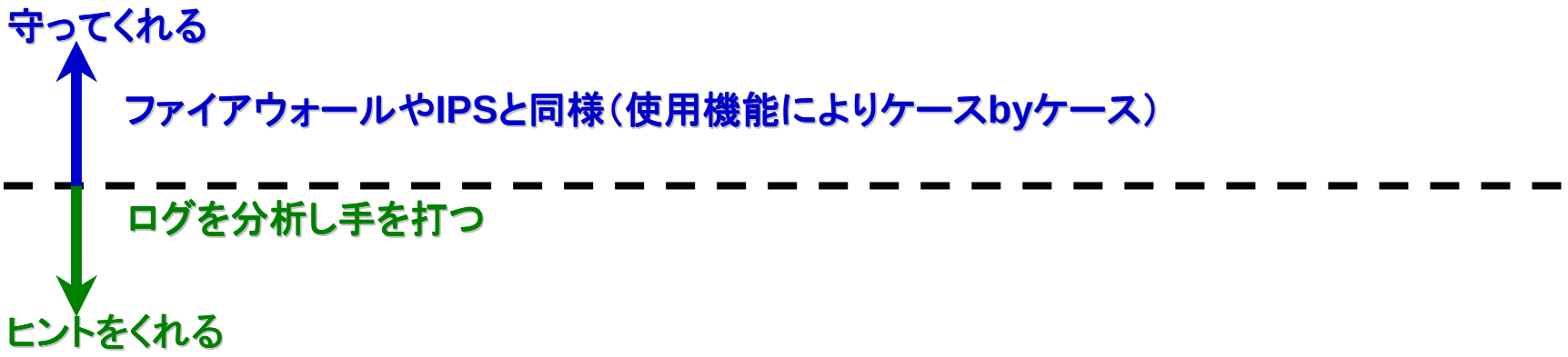
4. 知恵のレベルによる多段防衛

■セキュリティ機器による防御

7. その他

1）ルータ・スイッチ等
アクセス制御や高レイヤスイッチの場合は、FWやIPSと概ね同様の防御
使用帯域の変化

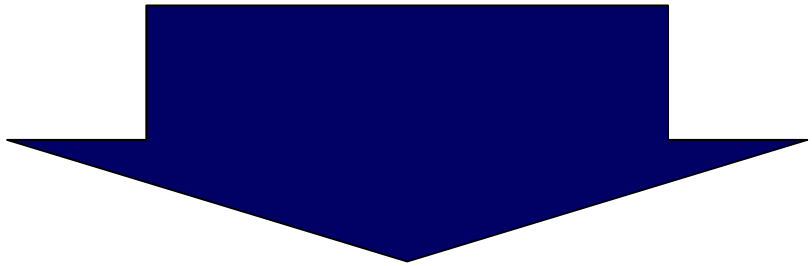
2）サーバ等
各種ログ



4. 知恵のレベルによる多段防衛

■セキュリティ機器による防御

1. 守る機器
   ⇒ 守って終わりではない
   ⇒ 分析する事でより重要なリスクを見つけることが可能
2. ヒントをくれる機器
   ⇒ そもそも分析が前提

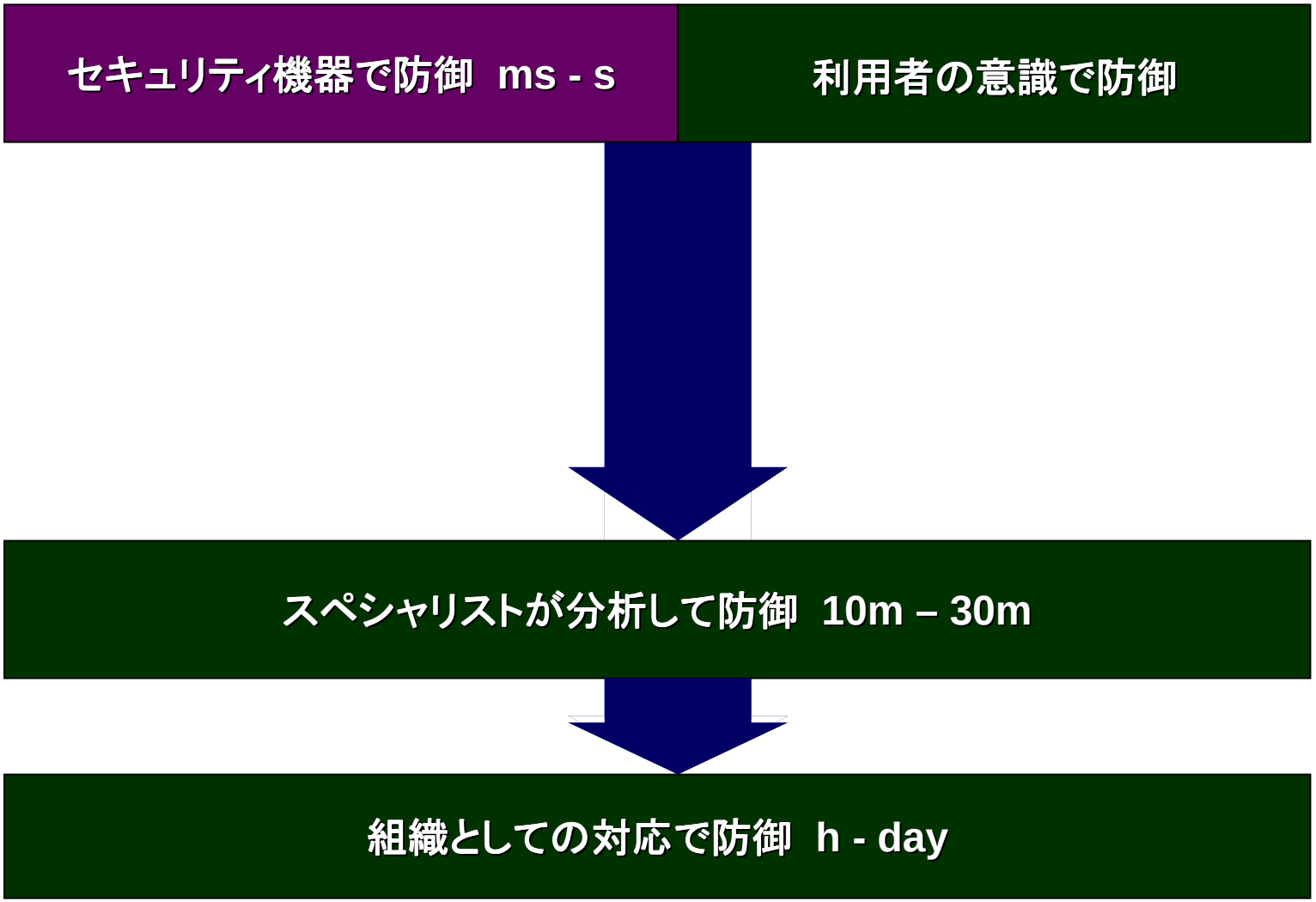


当たり前の事だが、、

分析を人間（スペシャリスト）が実施し、
リスクを分析し対策を講じる

4. 知恵のレベルによる多段防御

知恵のレベルの防衛の概念（スペシャリストによる防御）



4. 知恵のレベルによる多段防衛

■スペシャリストによる防御

1. インターネットセキュリティ

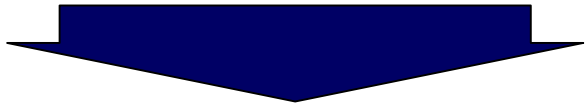
特にIDS（IPS）を駆使し、フォールスポジティブを含めよく分析し、

① そもそも攻撃（調査）が行われているのか？

②突破される可能性はあるのか？

③ どんな脆弱性をどんなツールなどを使用してどの程度のレベルの人間が狙っているのか？

④どんな目的を持っているのか　等



分析を人間（スペシャリスト）が実施し、リスクを分析し対策を講じる。

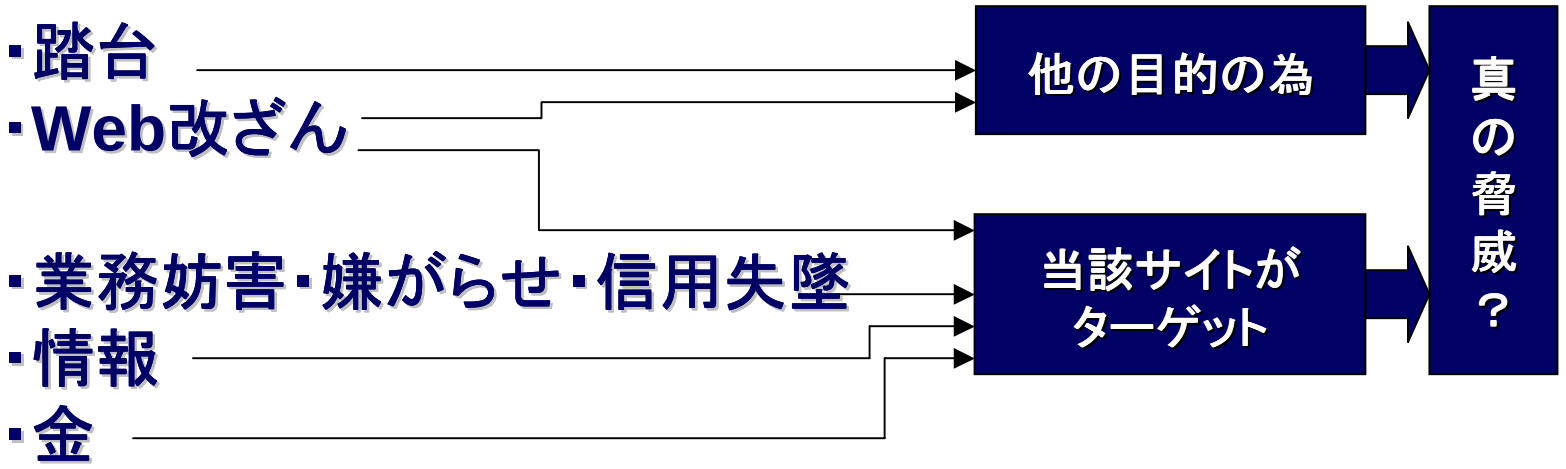
脆弱性に対する管理をしっかり実施出来ている組織の場合、念のために、実施する事が多い。

4. 知恵のレベルによる多段防衛

■スペシャリストによる防御

1. インターネットセキュリティ

侵入者の目的は？



4. 知恵のレベルによる多段防衛

■スペシャリストによる防御

1. インターネットセキュリティ

一発の攻撃で何が出来る？

WWWの改ざん
踏み台
ワーム・エージェント

真の脅威は？
ばれなければ良い？
やられても、外に出て行かなければ良い？

一発の攻撃が本当の脅威に
なるのならば
デバイスレベルでの防衛を！

4. 知恵のレベルによる多段防衛

■スペシャリストによる防御

1. インターネットセキュリティ

侵入調査～侵入、侵入して何をやる？

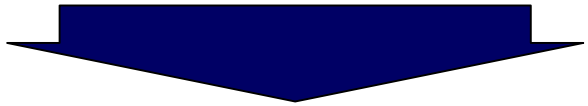
① ターゲット調査・脆弱性の推測、狙い付け
② 侵入トライ～侵入
③ 侵入マシンの調査
④ 攻撃ツール・ルートキットなどダウンロード
⑤ 侵入マシン周辺の調査
⑥ 侵入マシンでの情報収集の仕掛け作り
⑦ 侵入マシンでのルートキット・バックドアなど
・（他の足がかりへのレベルアップ）
・目的への行動開始 など

事前知識の有無
15～30分がリアルタイムの範囲か？

4. 知恵のレベルによる多段防衛

■スペシャリストによる防御

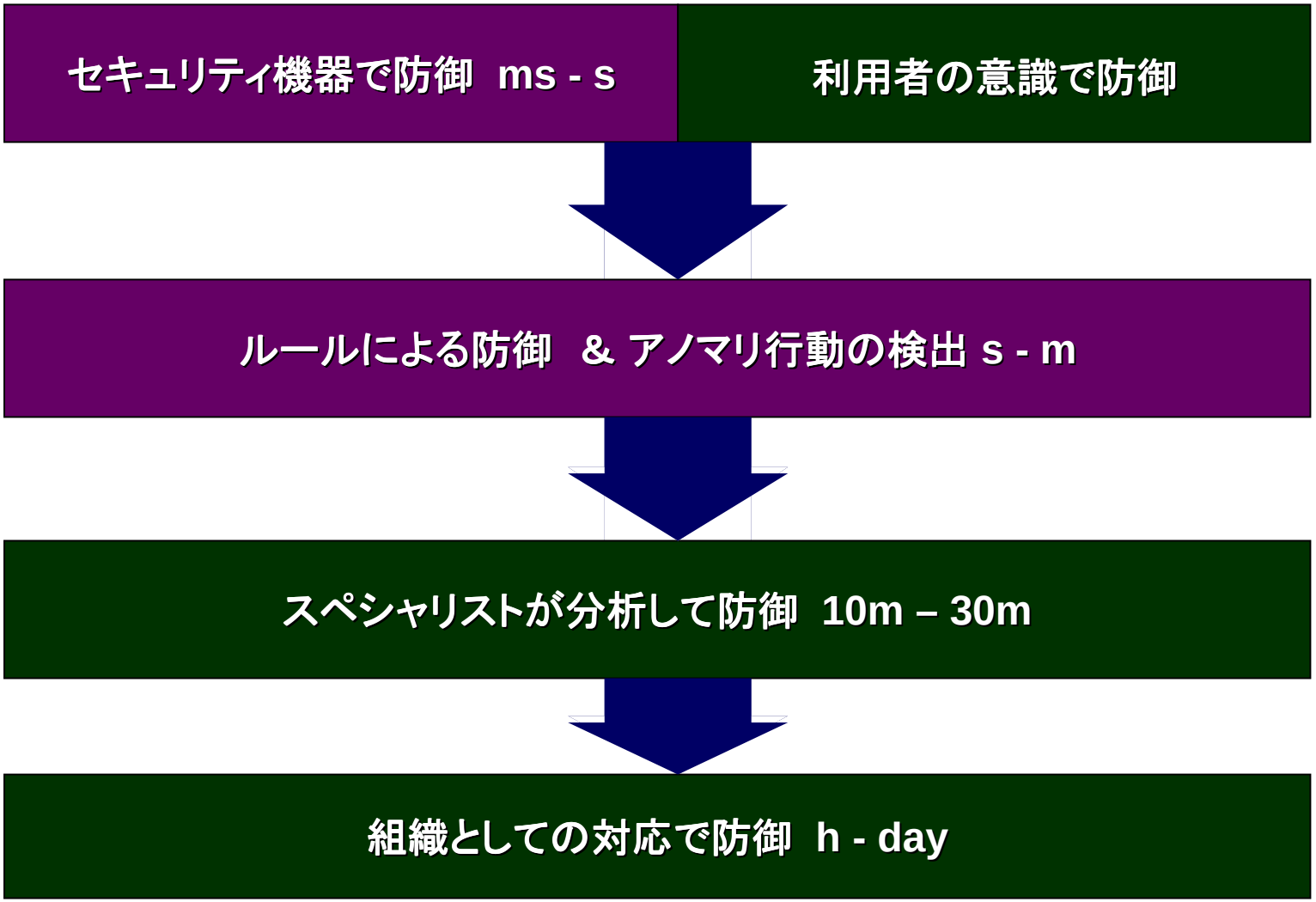
2. イントラネットセキュリティ
特にFWや内部の機器、点検ツール、IDS（IPS）を駆使し、分析し、
① 今現在どんなリスクを抱えているのか？緊急なのか？
② セキュリティポリシーへの違反行為はないか？
③ 異常が発生していないか？
④ それはセキュリティインシデントか？
⑤ 大規模なのか？



分析を人間（スペシャリスト）が実施し、リスクを分析し対策を講じる。大半の組織で実施する必要がある。
また、③、④、⑤に関しては、スピード勝負のところもあり、
人間の分析前に、自動分析と対応可能なものは実施

4. 知恵のレベルによる多段防御

知恵のレベルの防衛の概念（ルールによる防御）



4. 知恵のレベルによる多段防衛

■ルールによる防御

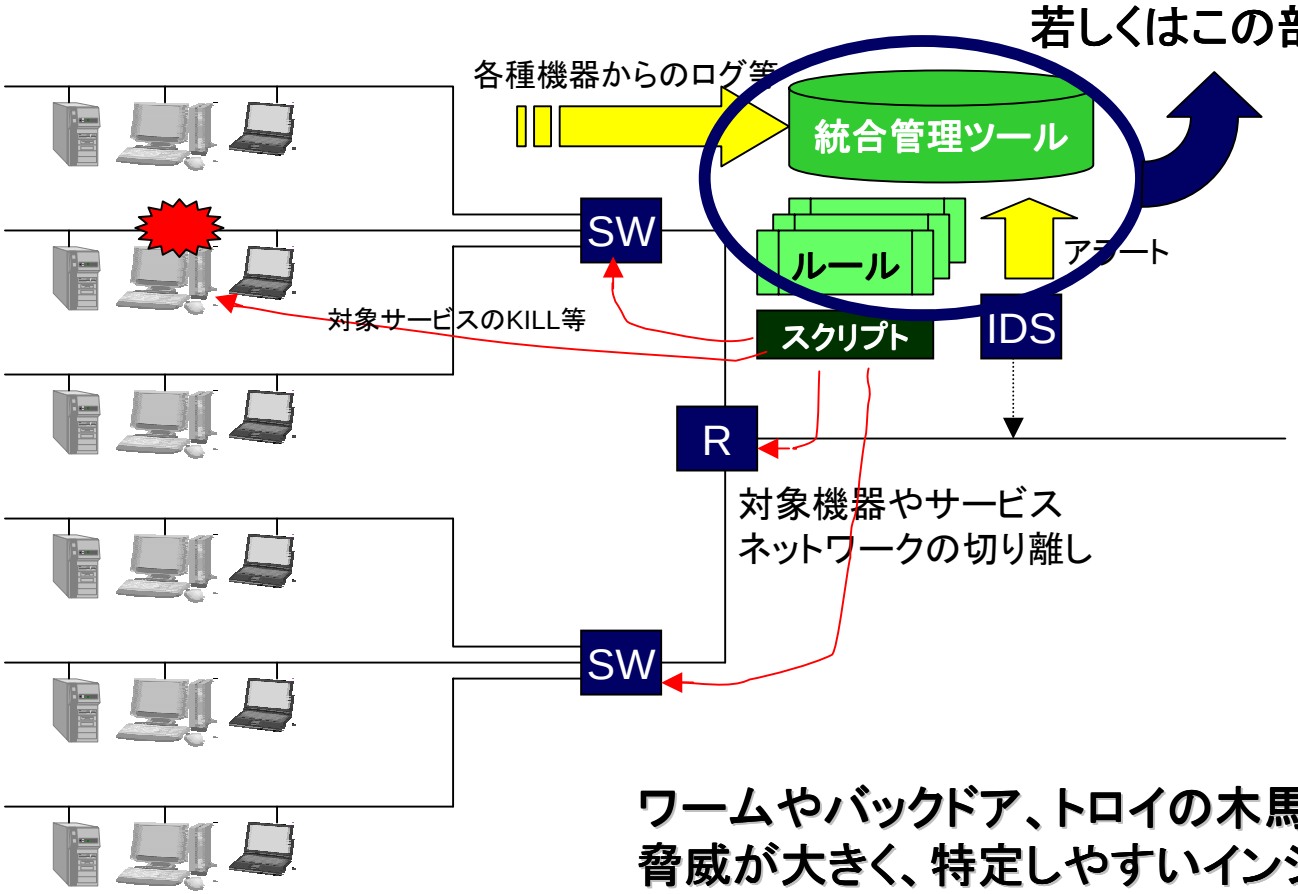
セキュリティ機器などが発する情報（ヒント：ログやアラート、レポートなど）を元に分析を実施し、対応を行うわけだが、この中で分析にスピードを要し自動分析化が可能なものはルール化を行い、対応を実施する。

これまでならば、所謂マニュアル化や手順化が可能なものであり、人にやらせるより自動化していこうという試みである。

また、MS Blasterの反省によりスピードを持った分析と対応が求められるようになったことも背景としては大きい。

4. 知恵のレベルによる多段防衛

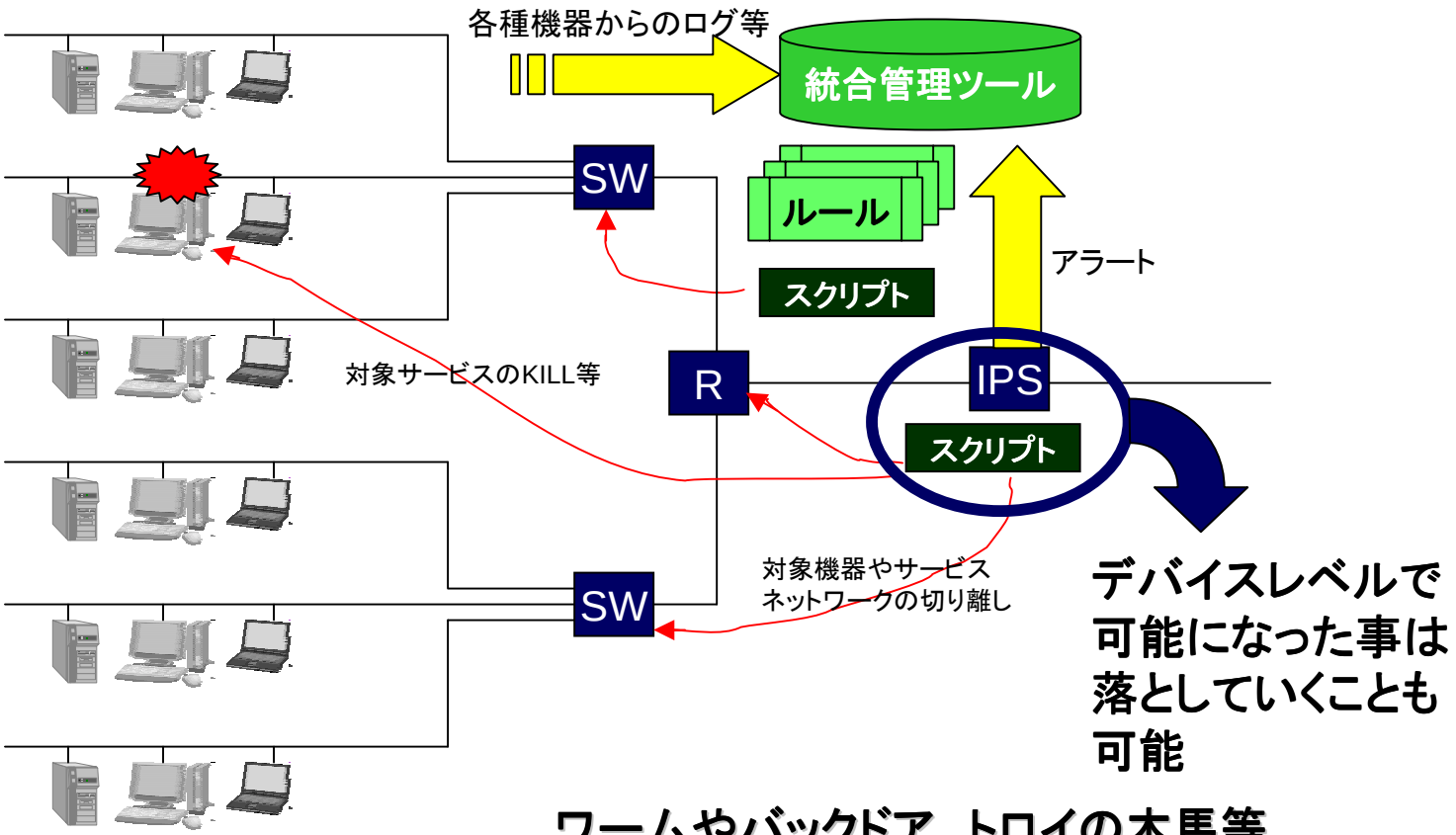
■ルールによる防御　イメージ＃１



ワームやバックドア、トロイの木馬等
脅威が大きく、特定しやすいインシデントに
に限定する。

4. 知恵のレベルによる多段防衛

■ルールによる防御 イメージ＃2

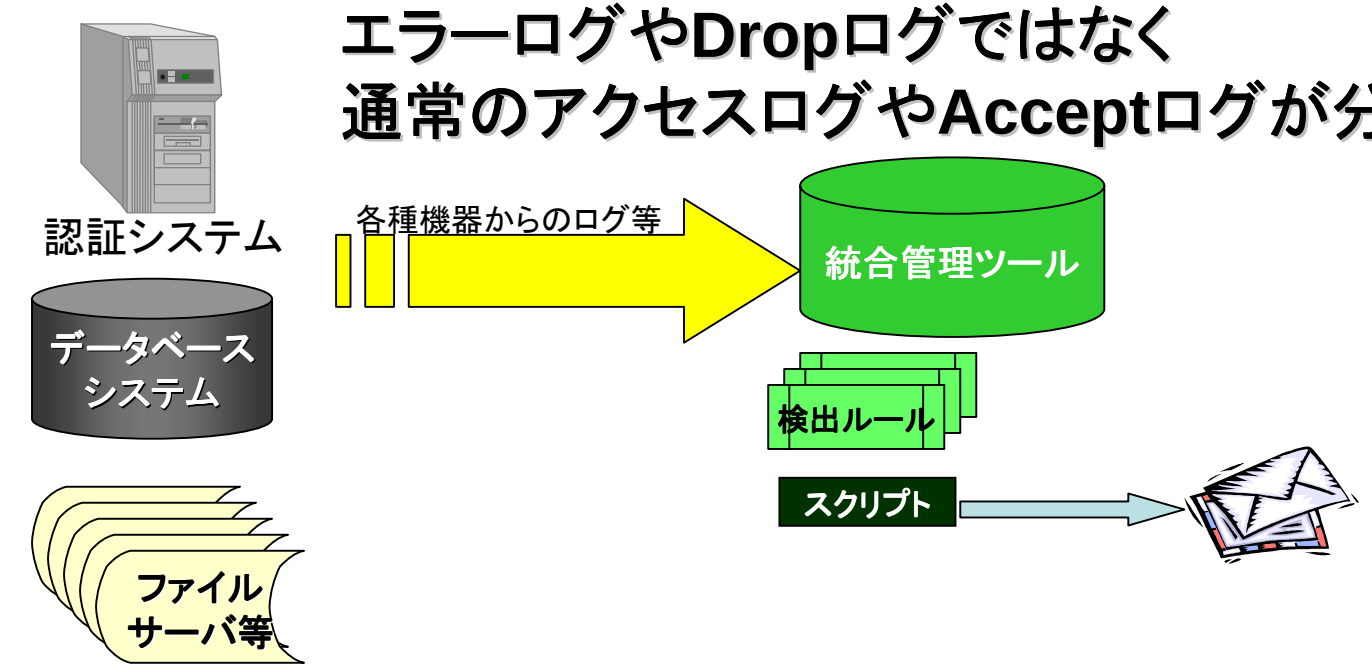


デバイスレベルで
可能になった事は
落としていくことも
可能

ワームやバックドア、トロイの木馬等
脅威が大きく、特定しやすいインシデントに
に限定する。

4. 知恵のレベルによる多段防衛

■ルールによる防御 イメージ#3
アノマリ行動の検出



エラーログやDropログではなく
通常のアクセスログやAcceptログが分析対象

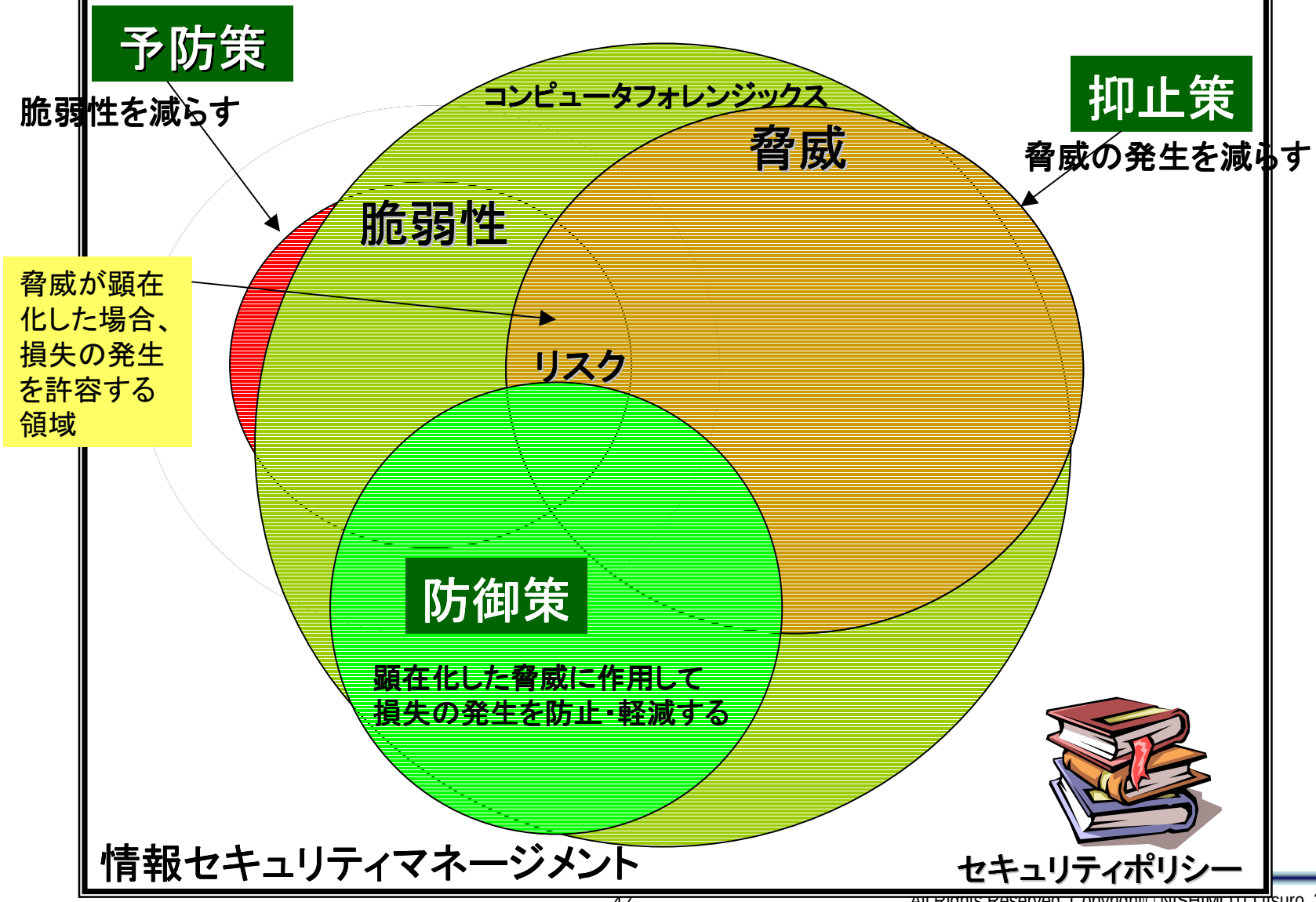
各種サーバアクセスログ

検出ルール作成には事前の行動分析が必要
組織ごとで検出ルールはまったく異なる

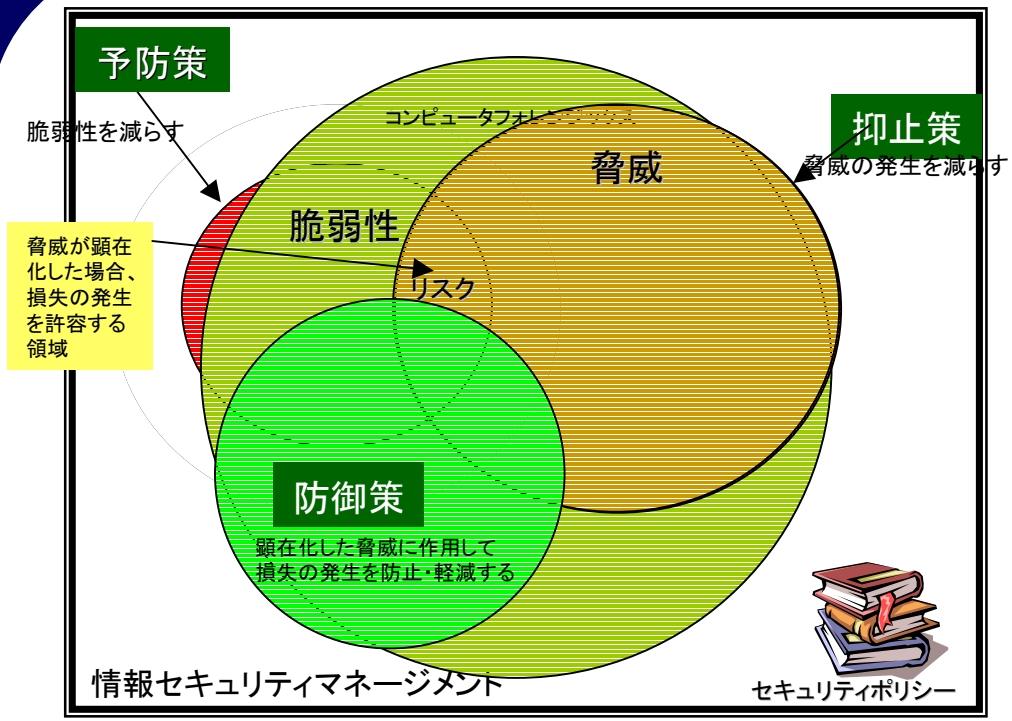
5. インシデントマネージメント

5. インシデントマネージメント

おさらいから、、



5. インシデントマネージメント



左記の、マネージメントシステムにて、、、

① 自動化・マニュアル化されていないもの

② 損失の発生を許容していた事象が発生

③ やっていたつもりが漏れていた等の人間の分析や判断と対応により損失の発生を抑えたり軽減する方策がインシデントハンドリング（インシデントレスポンス）となる。

上記の、マネージメントシステムのバランスを崩す（リスクが変化）事象に対して

、

原則リアルタイムに分析を実施し対応を図るフレームワーク＝

インシデントマネージメントが重要となる。

5. インシデントマネージメント

災害に対するマネージメントは？

	火事	台風	地震
抑止	放火の警備・整頓・村八分		
予防	火の用心・難燃性の材料等	護岸・土壌改善・補強	免震・耐震・補強
防御	スプリンクラ・防火壁等	ダム、排水等	つっぱり棒？・堤防等
検知	警備/見回り・火災報知器	ひまわり・アメダス・水位センサ	気象庁監視システム等
対応・回復	消防署・自衛消防隊・保険	防災体制・自衛隊・保険	防災体制・自衛隊・国家
基本スタンス	用心	耐える	諦める

セキュリティに当てはまるのか？

5. インシデントマネージメント

災害に対するマネージメントは？

	火事	台風	地震
抑止	放火の警備・整頓・村八分		
予防	火の用心・難燃性の材料等	護岸・土壌改善・補強	免震・耐震・補強
防御	スプリンクラ・防火壁等	ダム、排水等	つっぱり棒？堤防等
検知	警備/見回り・火災報知器	ひまわり・アメダス・水位センサ	気象庁監視システムなど
対応・回復	消防署・自衛消防隊・保険	防災体制・自衛隊・保険	防災体制・自衛隊・国家
基本スタンス	用心	耐える	諦める

セキュリティに当てはまるのか？

管理システム・防衛システム構築

危機意識から
左記の体制を整備

防止だけでは
怖いので情報収集

状況にあわせ
警戒や対応を実施

いざ、実害が出れば
復旧
（緊急対応）

インシデントレスポンス

インシデントマネージメント

5. インシデントマネージメント

損失や
犯罪が
顕在化

侵入され実害はまだ
脆弱性がある
違反行為
実害の無い攻撃
アノマリ行動

検知
情報収集

新たな脆弱性
新型ウイルス発生
攻撃トレンド
セキュリティ事件

法律・指導・ガイドライン
社会常識等の変化
関係機関の取り組み

リスク分析
対策立案

リスク理解
判断

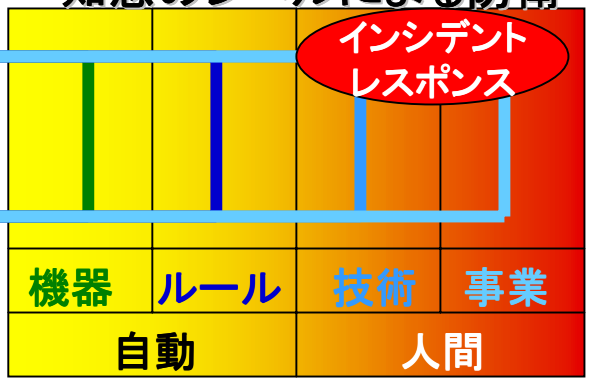
対策実施

フォローアップ

組織や体制変更
新システム稼動計画
新製品導入
規則やポリシーへの不満など

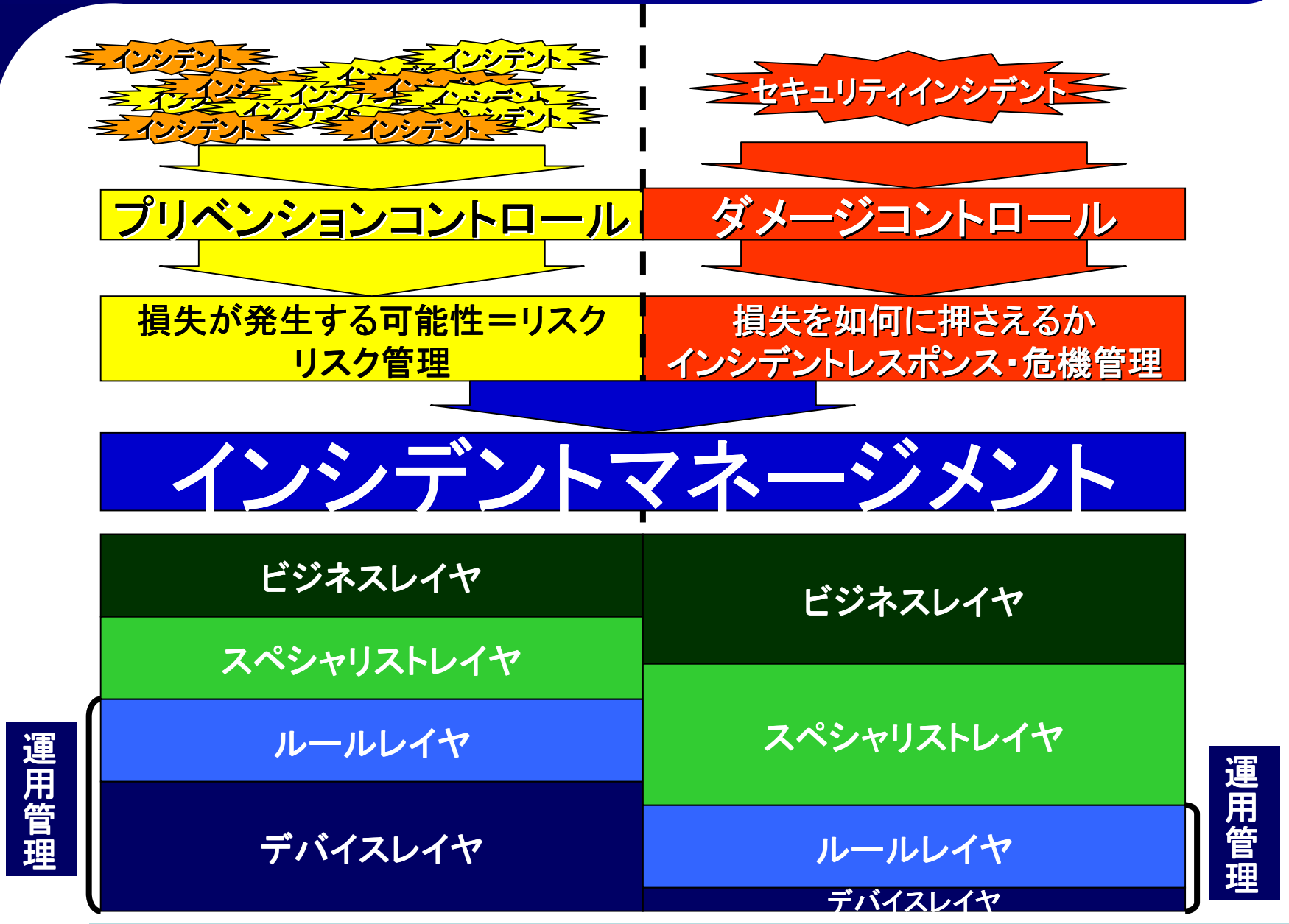
事業領域にかかる
「リスクの理解」は
原則アウトソースしては
いけない

知恵のレベルによる防衛



全体が
インシデントマネージメント

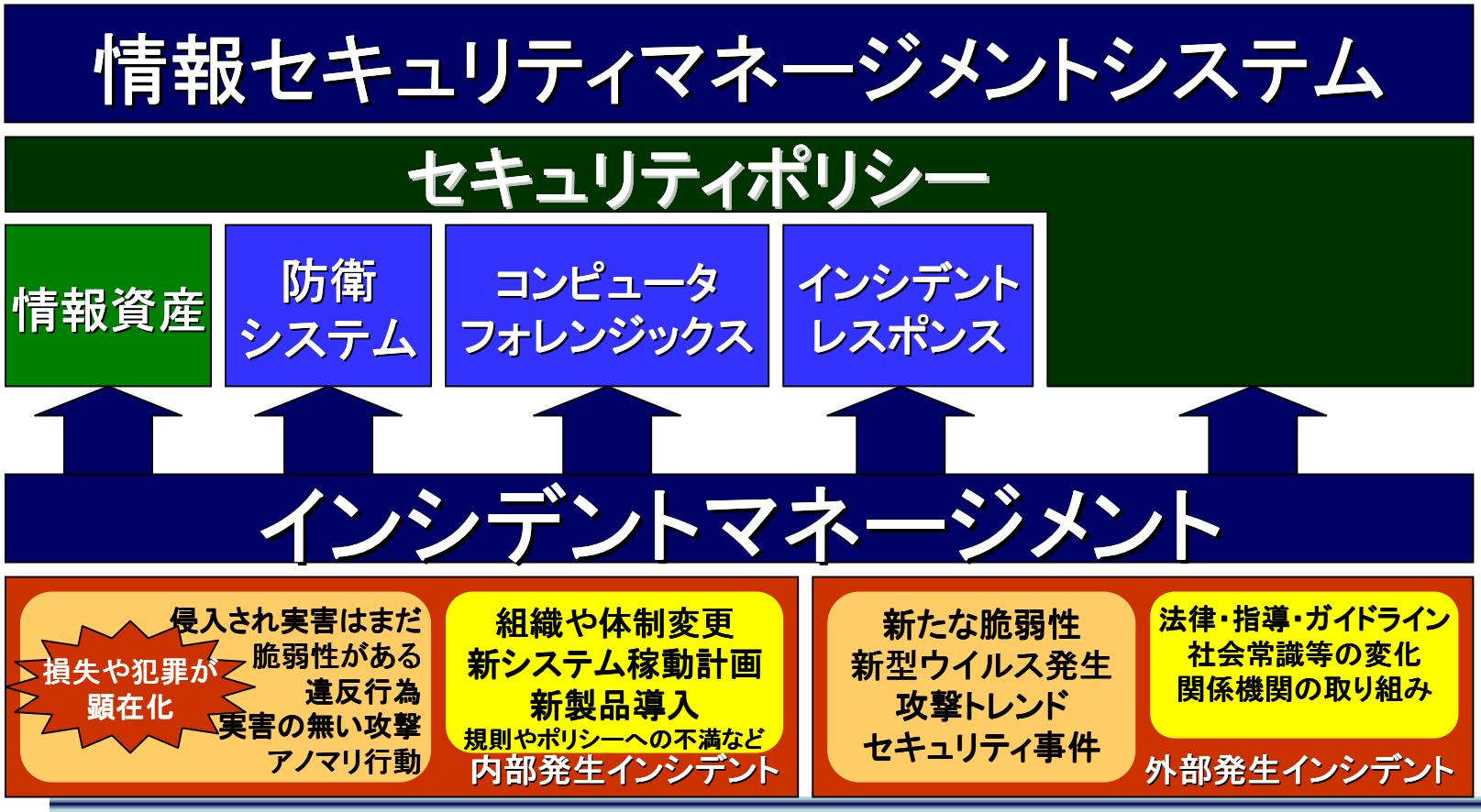
5. インシデントマネージメント



5. インシデントマネージメント

インシデントマネージメントの位置づけ

情報セキュリティマネージメントの中で特にリスクの変化を及ぼす事象（インシデント）に対してリスク分析～対応～フォローアップを行うフレームワークである。また、いざ事象が発生した場合に、損失見込みを判断しミニマム化を図るインシデントレスポンスを実施する。



5. インシデントマネージメント

インシデントの種類	例
被害や犯罪が 顕在化している	情報改ざん・破壊・搾取・漏洩 成りすまし、否認 機能停止、遅延、誤動作、踏み台、他への攻撃 など
侵入されているが 被害には至っていない	侵入し、内部調査を行っている状態 実害を出すため、犯罪、次の侵入等の準備を行っている状態 組織的な脆弱性スキャンが かかっている 、脆弱性に対する攻撃など
実害の無い調査行動 や攻撃	ポートスキャン・プローブ、定常的なウイルス・ワーム 単発的なブルートフォース（パスワードクラック、Exploitでの戻りアドレス探査） など
規則やセキュリティポリシー の 違反行為	禁止されているP2Pやチャットツール・攻撃ツールなどのアプリ使用 禁止されている外部BBSへの書き込み 禁止されている暗号の使用 など
アノマリ行動	クライアントごとの 機器（サーバなど）や情報（データベースやファイル等）への 変則（アノマリ）なアクセス状況 など
脆弱性がある	セキュリティパッチが適用されていない セキュアな設定になっていない セキュリティ上問題のある、サンプルなどが放置されている など
新システム稼動 新製品導入 組織や体制変更	基幹システムに分析系システムが追加され全社で利用できるようになる。 無線LANやモバイル、VPNなどが導入される 情報取り扱いや参照部署が変更、分断される など
規則やポリシーへの 不満や意見など	そもそも、守れない規則やポリシーを作成していないか？ ある条件下では守れないことがある など

5. インシデントマネージメント

インシデントの種類	例
脆弱性情報	OS、サービスアプリケーション、業務パッケージ、市販パッケージで脆弱性が見つかる フリーモジュールで脆弱性が見つかり、使用している市販パッケージなどで影響が出る 使用している技術仕様上の脆弱性が発表される など
新型ウイルスの流行	Codered、Nimda、SQLSlammer、MS Blaster 等の 大規模に発生したウイルス Sircam、BugBear.B Sobigなど 個別のウイルス など
攻撃トレンド	WEBサービス、SSH、SSLなどが狙われやすい など、、
世間で起こった セキュリティ事故	情報改ざん・破壊・搾取・漏洩、成りすまし、否認 機能停止、遅延、誤動作、踏み台、他への攻撃 など 世間で発生した事件 Zero day Exploit（公開されていない脆弱性を使用しての攻撃） など
法律・指導・ガイドライン 社会情勢・常識等の変化	法律の施行、判例、省庁や業界団体などからのガイドラインや指針 条約批准、マスメディアの論調や事件報道への取り組み 顧客や取引先などの関係機関のセキュリティへの取り組み など

5. インシデントマネージメント

■ インシデント検知の方法

インシデント検知方法	説明
自己の監視で検知	自組織の監視で検知
情報収集	情報収集で既知となる
内部通報・連絡	自組織の人間が（たまたま）検知 自組織の人間が連絡
外部通報・連絡（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・連絡（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

5. インシデントマネージメント

インシデント：どうやって見つけるか？

インシデントの種類		検知方法				
		セキュリティ監視	情報収集	内部通報・連絡	外部通報・連絡	報道
内部で発生	被害や犯罪が顕在化	○		○	○	○
	侵入され実害はまだ	○		△		
	実害の無い攻撃	○				
	違反行為	○		○		
	アノマリ行動	○		○		
	脆弱性がある	○		○	○	○
	新システム稼動 組織や体制変更			○		
	規則やポリシーへの 不満や意見			○		
外部で発生	新たな脆弱性		○	○	○	○
	新型ウイルス発生	△	○	○	○	○
	攻撃トレンド	△	○	○	○	○
	世間で起こった セキュリティ事故		○	○	○	○
	法律などの変化		○	○	○	○

5. インシデントマネージメント

参考：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
無認可のアクセス	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 これまでの一般的なウィルス等	△	○	◎	◎	
	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	◎	×	×	◎	

完璧なセキュリティは何故無いのか？

5. インシデントマネージメント

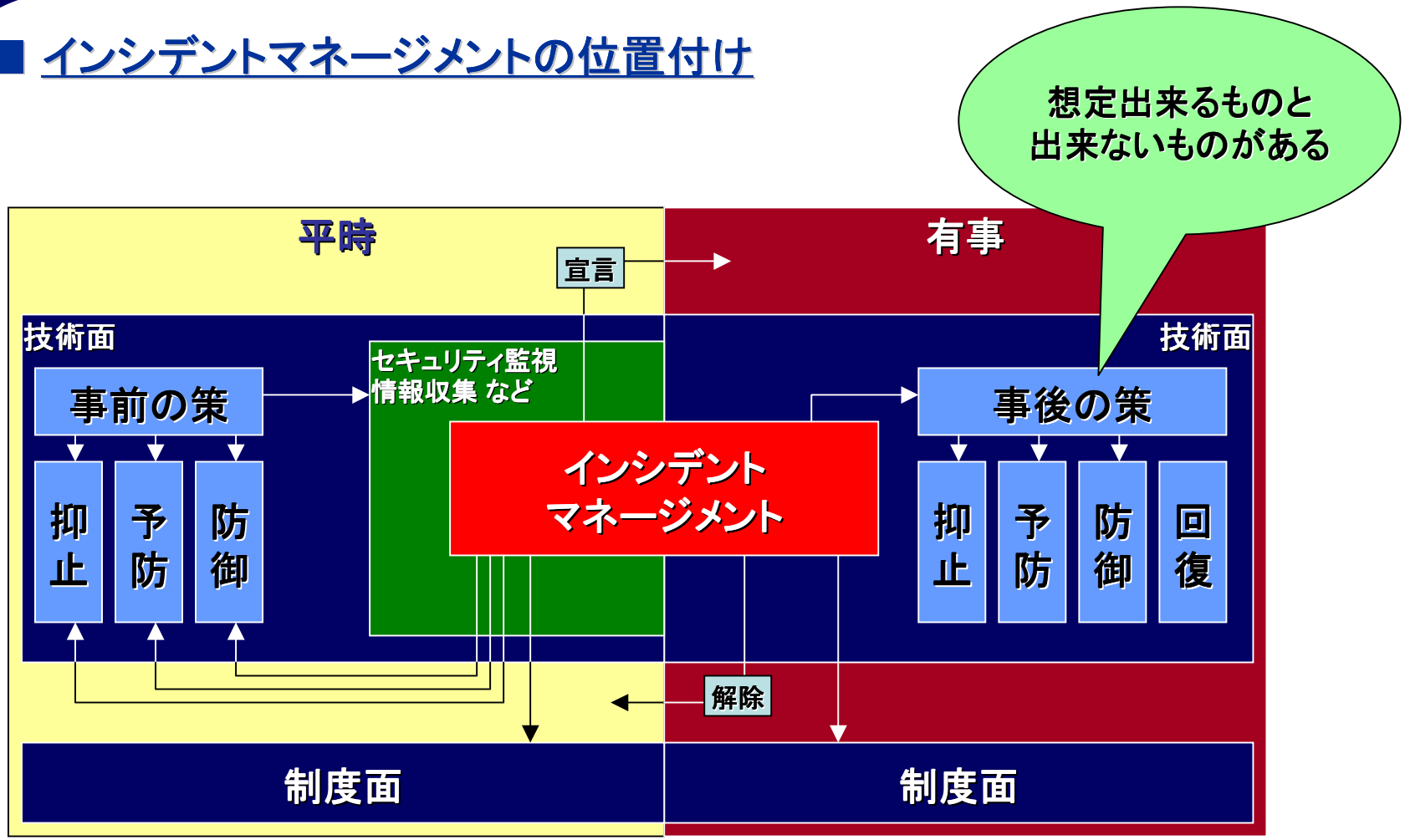
参考：セキュリティ５大機能

機能	概要	
抑止	脅威の発生そのものを押さえ込む EX.内部犯罪防止のため定期監査の実施など	防止策
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おく EX.セキュリティパッチ、ウイルス定義ファイル更新など	
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 EX.ファイアウォール、IDS、ウィルス対策ソフト等	
検知	脅威の発生若しくはその予兆を検知する EX.IDS監視、ファイアウォールやサーバのログ監視など	インシデント レスポンス
回復	ダメージから回復する	

コンピュータ フォレンジックス
証拠確保の機構と発生事象の分析

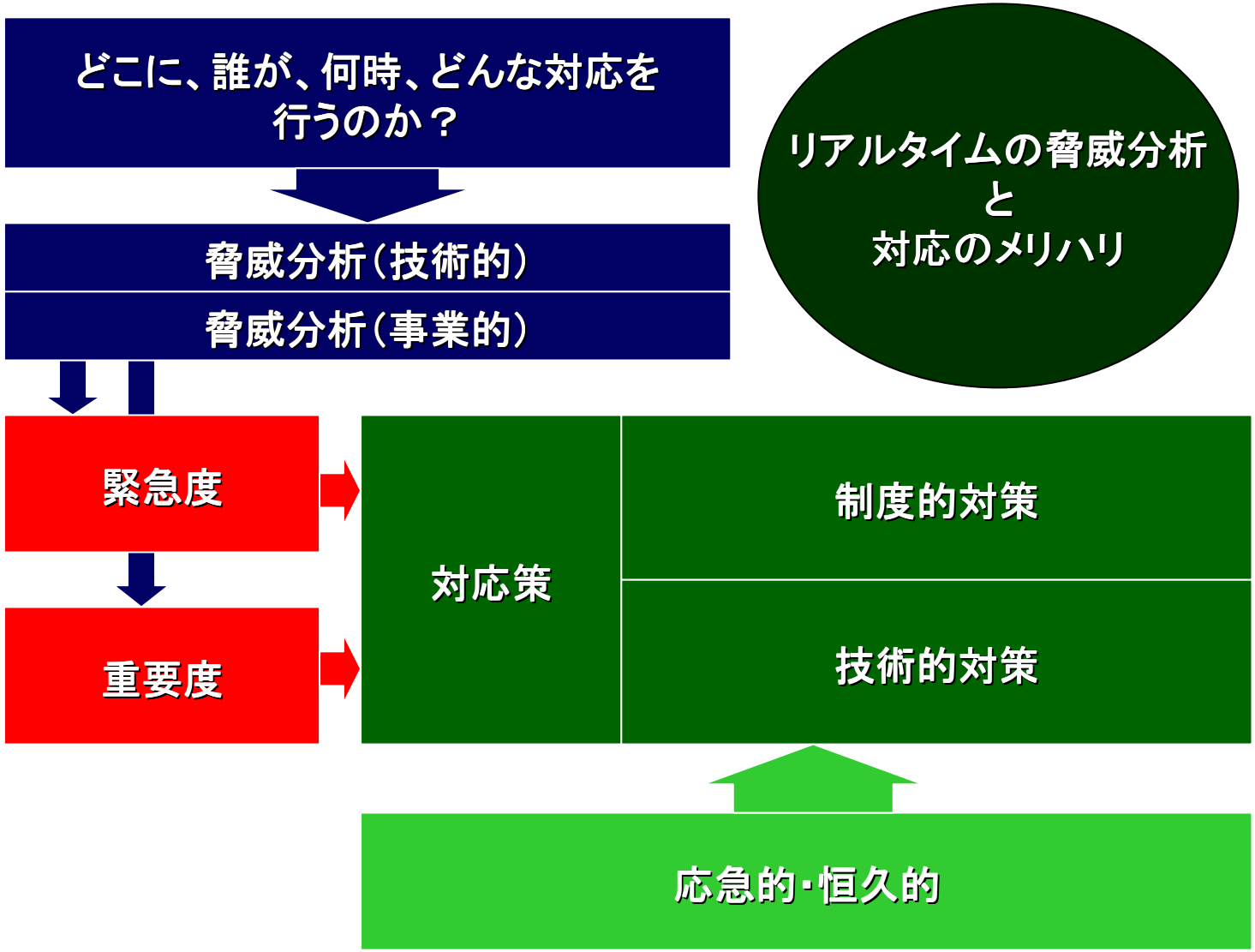
5. インシデントマネージメント

■ インシデントマネージメントの位置付け



5. インシデントマネージメント

■マネージメントのポイント



5. インシデントマネージメント

■インシデントに対する対応例－内部

インシデントの種類	対応例
被害や犯罪が顕在化している	応急処置：被害拡大防止、被害の封じ込め、証拠保全 緊急対応：原因・手法・侵入ルートの特定、被害範囲の特定、再開案策定 再発防止策策定、フォローアップ
侵入されているが被害には至っていない	応急処置：即時防御（リアルタイムプロテクション） 緊急対応：原因・手法・侵入ルートの特定、被害範囲の特定、再開案策定 再発防止策策定、フォローアップ
実害の無い調査行動や攻撃	統計分析により、防止策へ反映
規則やセキュリティポリシーの違反行為	規則やポリシーに照らし合わせ、注意などの抑止策 或いは、セキュリティポリシーの見直し、教育など
アノマリ行動	規則やポリシーに照らし合わせ、注意などの抑止策 或いは、教育など
脆弱性がある	脅威を分析し、防止策へ反映 検知策へ反映（対応策決定）
新システム稼動 組織や体制変更	脅威を分析し、セキュリティポリシーの見直し 検知策、防止策の見直し
規則やポリシーへの不満や意見	形骸化しないか・利便性を著しく阻害していないかなどを 分析し、当該規則やポリシー見直し或いは教育など

5. インシデントマネージメント

■インシデントに対する対応例－外部

インシデントの種類	レスポンス例
脆弱性情報	自組織への影響や脅威を分析し、防止策へ反映 内部点検 検知策へ反映（対応策決定）
新型ウイルスの流行	脅威・仕組みを分析し、防止策へ反映 内部点検 検知策へ反映（対応策決定）
攻撃トレンド	自組織への発生可能性や脅威を分析し、防止策へ反映 検知策へ反映（対応策決定）
世間で起こった セキュリティ事故	自組織への発生可能性や脅威を分析し、防止策へ反映 検知策へ反映（対応策決定）
法律・指導・ガイドライン 社会情勢・常識等の変化	自組織への影響を鑑みて脅威を分析し、防止策へ反映 検知策へ反映（対応策決定）

5. インシデントマネージメント

■ PIRTの体制（プライベート インシデント レスポンス チーム）

①目的
インシデントマネージメントを実施するチームと考えた方が早い

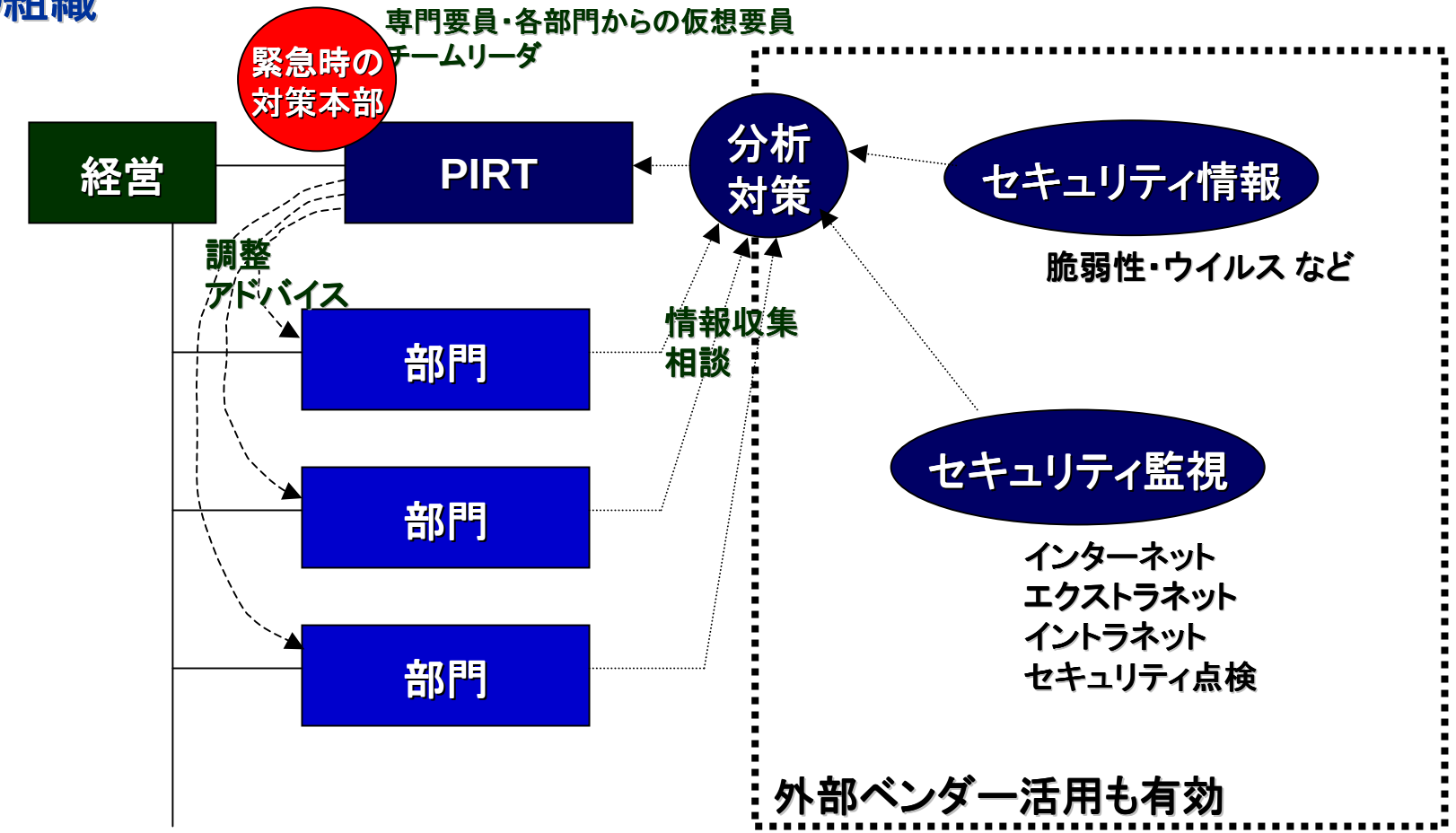
（1）平時
各種インシデントに関するマネージメント
教育、監査をつかさどっても良い

（2）有事
有事に対する対策本部的な役割

5. インシデントマネージメント

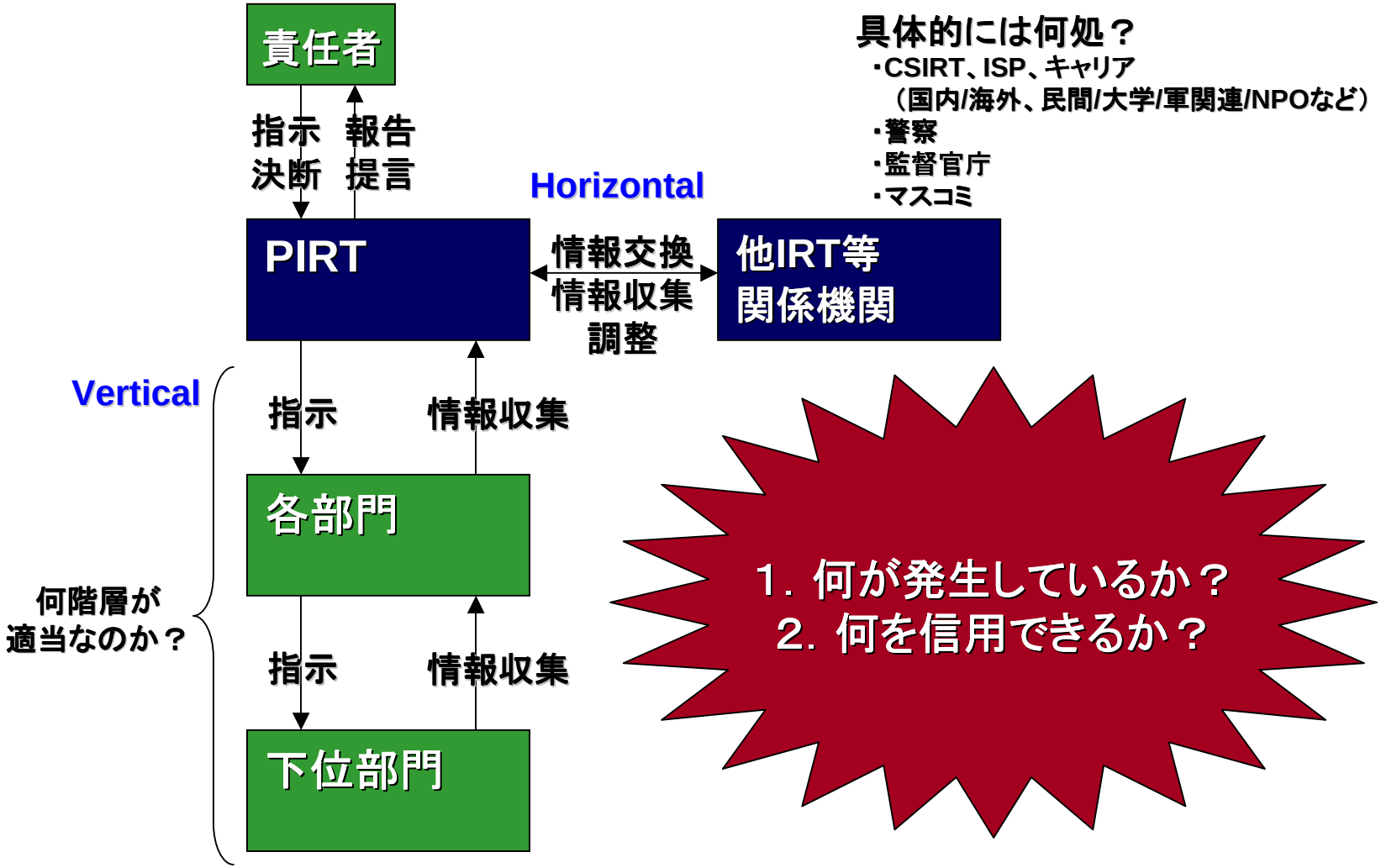
■ PIRTの体制（プライベート インシデント レスポンス チーム）

②組織



5. インシデントマネージメント

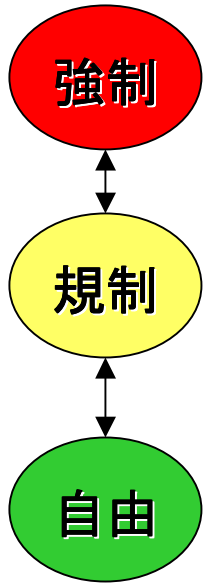
■ 神経系統



5. インシデントマネージメント

■ 適用事態 例

状態	意 味	適 用
Red	有事	非常事態宣言 権限行使
Orange	有事が想定される 有事からの回復期	準非常事態宣言 協力依頼・体制準備
Yellow	準警戒態勢	警戒警報 協力依頼
Green	平時	マニュアル



5. インシデントマネージメント

■ カテゴリ 分類例 例

基本的にBox毎に体制や手順を整備・訓練

カテゴリ	概要	Red	Orange	Yellow	Green
A	主要業務を支える事業インフラに対するもの	発生している状態 CIAが阻害されている	発生可能性が高い 収束時 警戒状態	可能性あり 注意状態	
B	クライアント環境に対するもの	発生している状態 CIAが阻害されている	発生可能性が高い 収束時 警戒状態	可能性あり 注意状態	
C	組織の基幹に対するもの	発生している状態 CIAが阻害されている	発生可能性が高い 収束時 警戒状態	可能性あり 注意状態	
D	不祥事	発生している状態 報道・クレーム	発生 クレーム可能性あり 外部へは未公開	可能性あり 注意状態	

6. インシデントレスポンス

6. インシデントレスポンス

■ レスポンス（対応）のカテゴリ（制度面）

①内部
- （1）脅威の把握と適用事態選択
- （2）エスカレーション・フロー
- （3）Verticalラインでの情報収集とIRTを中心とした指揮

②外部
- （1）CSIRT、ISP、キャリア など
  - ・情報交換
  - ・協力要請
- （2）マスメディア
- （3）取引先
- （4）株主
- （5）警察
- （6）監督官庁・業界団体・親会社など
- （7）通報者

6. インシデントレスポンス

■ レスポンス（対応）のカテゴリ（技術面）

有事対応

（1）応急処置（分～時間：例 30分以内）
　　→ 被害拡大防止、被害封じ込め、証拠保全
（2）緊急対応（時間～日：例 2日間以内）
　　→手法特定、脅威の推測（技術面）、被害範囲の特定
　　目的推測（社会面）、攻撃元への一次対応
　　本格対応までの対抗策
（3）本格対応（日～週～月）
　　→ 原因などから、再度事前策を策定し、実施
　　→ 残存被害がないか、再度被害が出ないか、点検・監視
　　→ 攻撃元への根絶対応

6. インシデントレスポンス

■ 応急処置

①「被害や犯罪が顕著化しているケース」
（1）被害が拡大しないように、他に影響しないように隔離
→ 対象機器を切り離す。（物理的、論理的）
→ 場合によってはシステム全体を切り離す
（2）証拠保全
→ 基本的に、シャットダウン、余計な操作は厳禁
調査の為、届出の為（被害者としての証拠）
②「侵入されているが被害はまだ」
（1）被害が発生しないように、攻撃者から隔離（緊急防御）
→ 対象機器を切り離す。（物理的、論理的）
→ 場合によってはシステム全体を切り離す
（2）証拠保全
→ 基本的に、シャットダウン、余計な操作は厳禁
調査の為、届出の為（被害者としての証拠）

⇒ 通常は、応急処置として電話などで指示する。

6. インシデントレスポンス

■ 応急処置

③ 責任者へ第一報
顕在化している被害等から判断し、先の①、②に並行し実施。
（1）可能性のある宣言レベル
（2）晒されている脅威の可能性
→社会面を中心に

④ 関係部署などへ連絡
責任者から実施するのか、IRTで実施するのかは、役割分担を含め、
事前取り決めだが、その取り決めに従い、実施。
連絡系はVerticalとHorizontalがある。
→ 何（開示内容）を何処に誰がどのように（確実・信頼）連絡するのか？

⑤ 外部からの通報であった場合
通報者へ対応状況の連絡 → 何を連絡するのか？事前検討項目
※ 場合により通報者への初期動作のまずさで、風評被害など別の脅威
へ発展可能性あり。慎重に対処。

6. インシデントレスポンス

■ 緊急対応

①手法特定
　顕在化している被害や稼動サービスや構成及び痕跡などから
　侵入ルート、侵入手法を特定・推測、可能なら一次攻撃元特定
　→ 何が信用できるか？、複数を想定
②脅威の推測（技術面）
　起こしえる技術的脅威を推測
　→ 顕在化している機器のみ？情報？稼動？
③目的推測（社会面）
　顕在化している被害や行動痕跡から、目的を推測
　→ 自己顕示レベル、確信犯（経済的、思想的、）

⇒ この時点で、責任者に一次報告が妥当
（1）提言する宣言レベル
（2）社会面での脅威
（3）証拠データ、論拠
並行して、関係部署などへ連絡
　→ 何（開示内容）を何処に誰がどのように（確実・信頼）連絡するのか？

6. インシデントレスポンス

■ 緊急対応

④被害範囲の特定
　被害範囲を特定或いは推測する
　→ 技術面
　　現実に発生している内容
　→ 社会面
　　現実に発生している内容
　　今後、発展する可能性

この時点で、責任者に二次報告が妥当
（1）提言する宣言レベル（変更）
（2）社会面での脅威（変更）と技術面の脅威
（3）証拠データ、論拠

並行して、関係部署などへ連絡
　→ 何（開示内容）を何処に誰がどのように（確実・信頼）連絡するのか？

6. インシデントレスポンス

■ 緊急対応

⑤本格対応までの対抗策
　暫定対応は可能か？ 技術面・社会面
　自組織だけで実施可能か？（ISP、キャリア、CSIRT）

⑥攻撃元への一次対応
　攻撃元への連絡など

⑦緊急対応フェーズのクローズ
　基本的に、危機状態を脱したと責任者の判断でクローズ
　通常は、Yellowモードで警戒態勢を引く
　→ 警戒態勢の定義・範囲

6. インシデントレスポンス

■ 本格対応

①制度的対応

（1）プロジェクト編成

（2）渉外担当

（3）セキュリティポリシー等

（4）教育・訓練

②技術的対応

（1）対抗策 策定・実施（抑止、予防、防御、検知、回復）

（2）点検・監査

※ 過剰・過敏 過小・鈍感

7. コンピュータフォレンジックス

7. コンピュータフォレンジックス

デジタルの世界に於ける証拠確保の機構と発生事象の分析であり、
目的は組織防衛にあり、基本的に以下の項目を意識して通常は考える。
事故処理時に必ず意識すべき事であり、（法的にどこまで有効かどうかを含め）
事故発生前に考慮しておかなくてはならない。

① リスク顕在化後の調査

②リスク顕在化の検知

③リスク顕在化時に適切な管理を実施していた
事を第三者へ証明

④リスク顕在化の加害者へ証明

⑤リスク未顕在化を第三者へ証明

① リスク顕在化後の調査

リスクが顕在化した時、速やかに回復や再発防止を図るために、侵入ルートや手法の特定、被害範囲の確認等の分析を行うために必要なログ等の確保と分析の実施である。

一般的に意識しやすい分野

② リスク顕在化の検知

リアルタイムフォレンジックスと言っても良いが、所謂セキュリティ監視であり、必要なログやアラートの確保とリアルタイム分析がこれにあたる。

リスクが顕在化していないか、リスクが顕在化する危険性はないかを分析・判断し、インシデントレスポンスにつないでいく。

通常はファイアウォールやIDSのログやアラートを分析することが多い。

③ リスク顕在化時に適切な管理を実施していた事を第三者へ証明

リスクが顕在化した場合、組織として法規違反などの明確なペナルティを負う事が無いように、管理内容とその監査証跡等の適切な確保である。

④ リスク顕在化の加害者へ証明

リスクが顕在化した場合、加害者（場合よっては警察や裁判所など）に対して、その行為と被害内容などを証明する為に、必要なログ等の証拠と分析結果などの確保である。

⑤ リスク未顕在化を第三者へ証明

リスクはあったが、顕在化していないことを特に潜在被害者に対して証明するために必要なログ等の証拠と分析結果などの確保である。

例えば、運用しているWEBサーバでクロスサイトスクリプティングの問題が発見されたり、データベースサーバにウイルスが侵入されたりしたが、情報漏えいの事実はないと分析と証明できるために必要な証拠を準備しておく事である。

7. コンピュータフォレンジックス

フォレンジックスの目的 / リスクのカテゴリ	① リスク顕在化後の調査	②リスク顕在化の検知	③リスク顕在化時の適正管理証明	④リスク顕在化の加害者へ証明	⑤リスク未顕在化を第三者へ証明
社会的責任	◎	◎	○	○	○
法的責任 コンプライアンス 不祥事	○	○	◎	◎	◎
自己責任	○	◎	△	◎	△

8. リアルリスクメータ(おまけ)

セキュリティ対策実施効果の把握

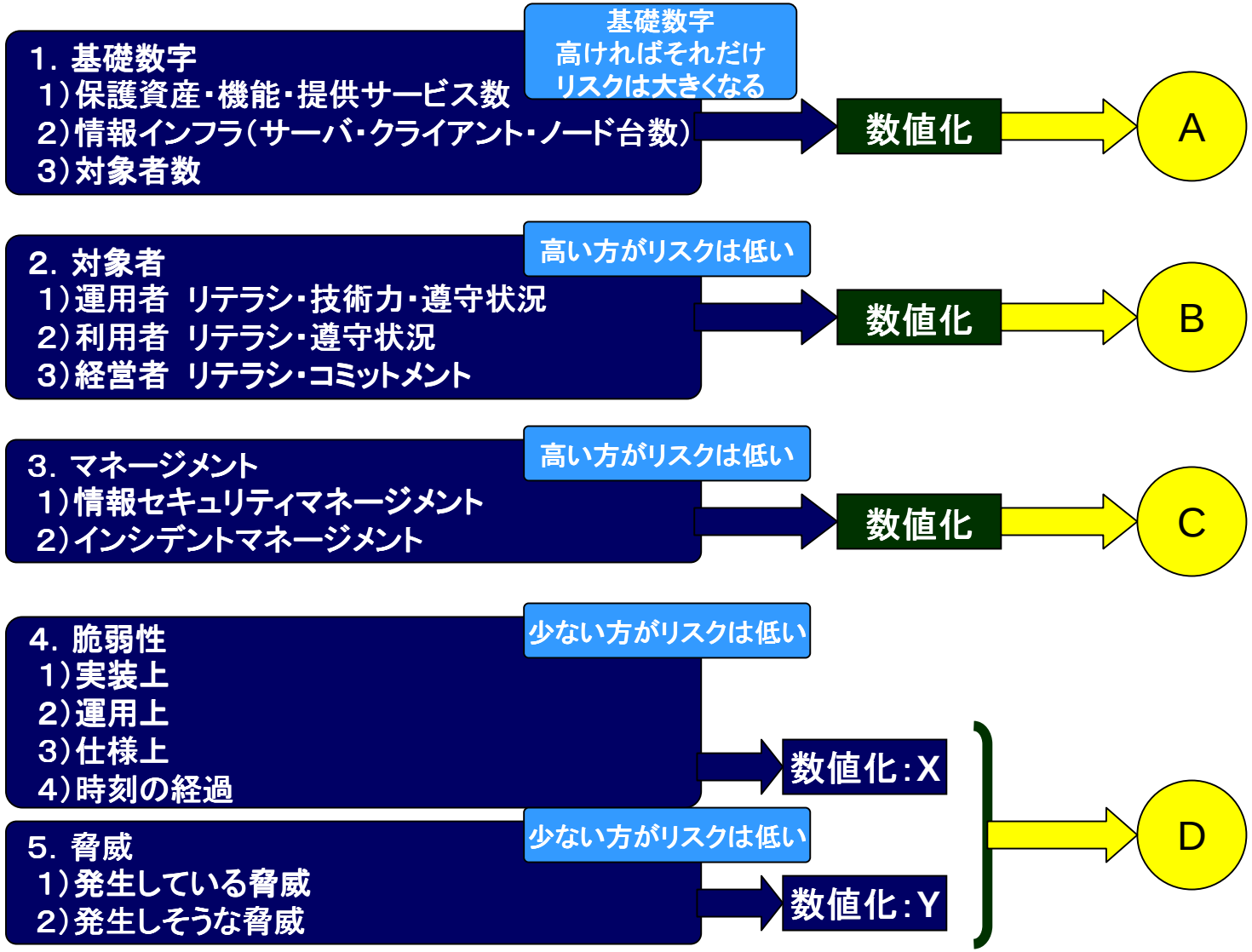
ISMSを構築して、どれだけリスクが減ったのか？
自動パッチ配布システムを導入してどれだけ効果が出たのか？
ファイアウォールを導入してどれだけ効果が出たのか？
緊急に点検を行い、脆弱性のある機器に対して対応してもらって、、、など

何らかの指針があると、目標になりやすい、、

一人歩きは怖いが、、、

8. リアルリスクメータ(おまけ)

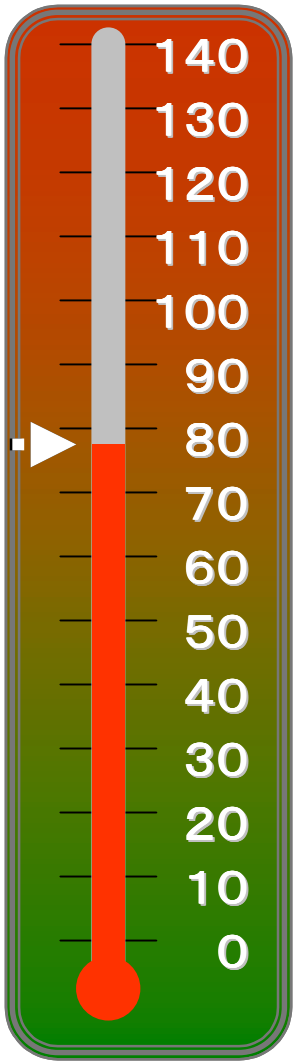
入力パラメータ 例



8. リアルリスクメータ(おまけ)

例えば、、、

A ＋ [A × 100-B × 100-C × D] ……▶



インシデント発生とその対応時に
リアルタイムで共有できれば、、、

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