A1－6

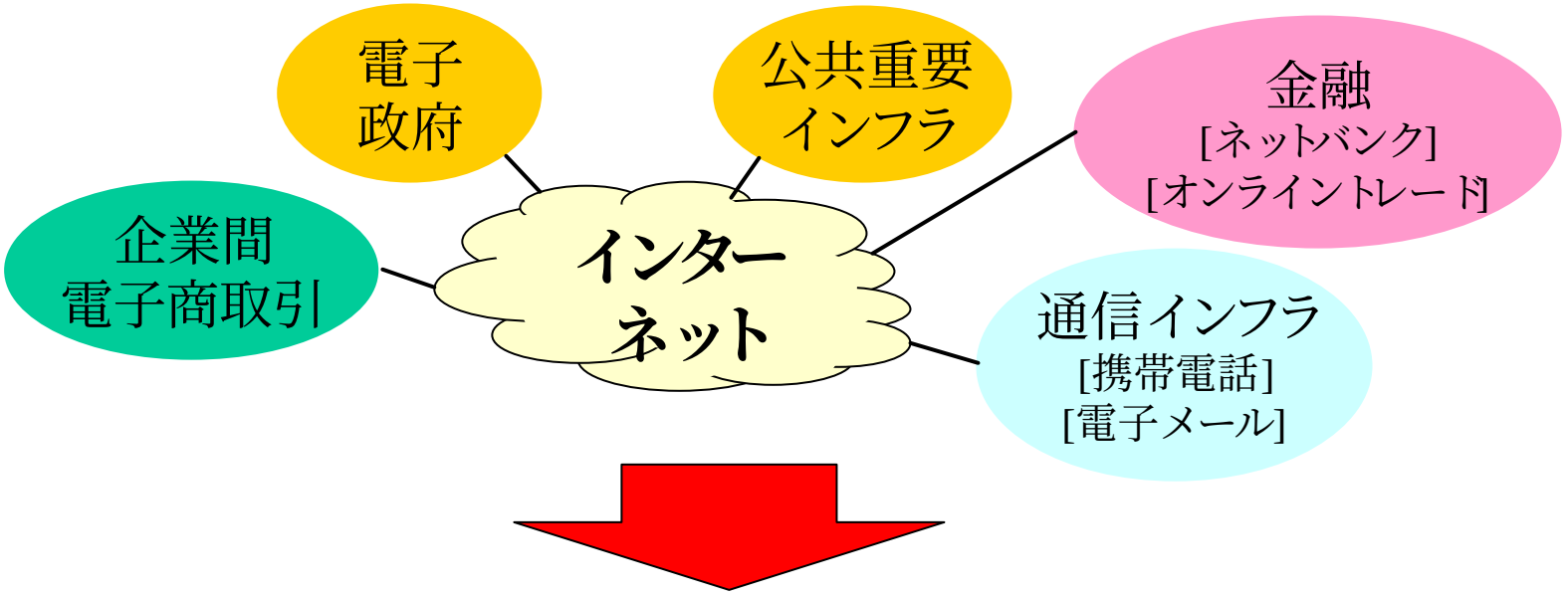
統合データベースを用いた
不正アクセス検出情報の分析
および
意思決定支援システム

平成14年3月4日

大谷尚通　桑田喜隆　小迫明徳　井上潮
㈱NTTデータ

1. はじめに

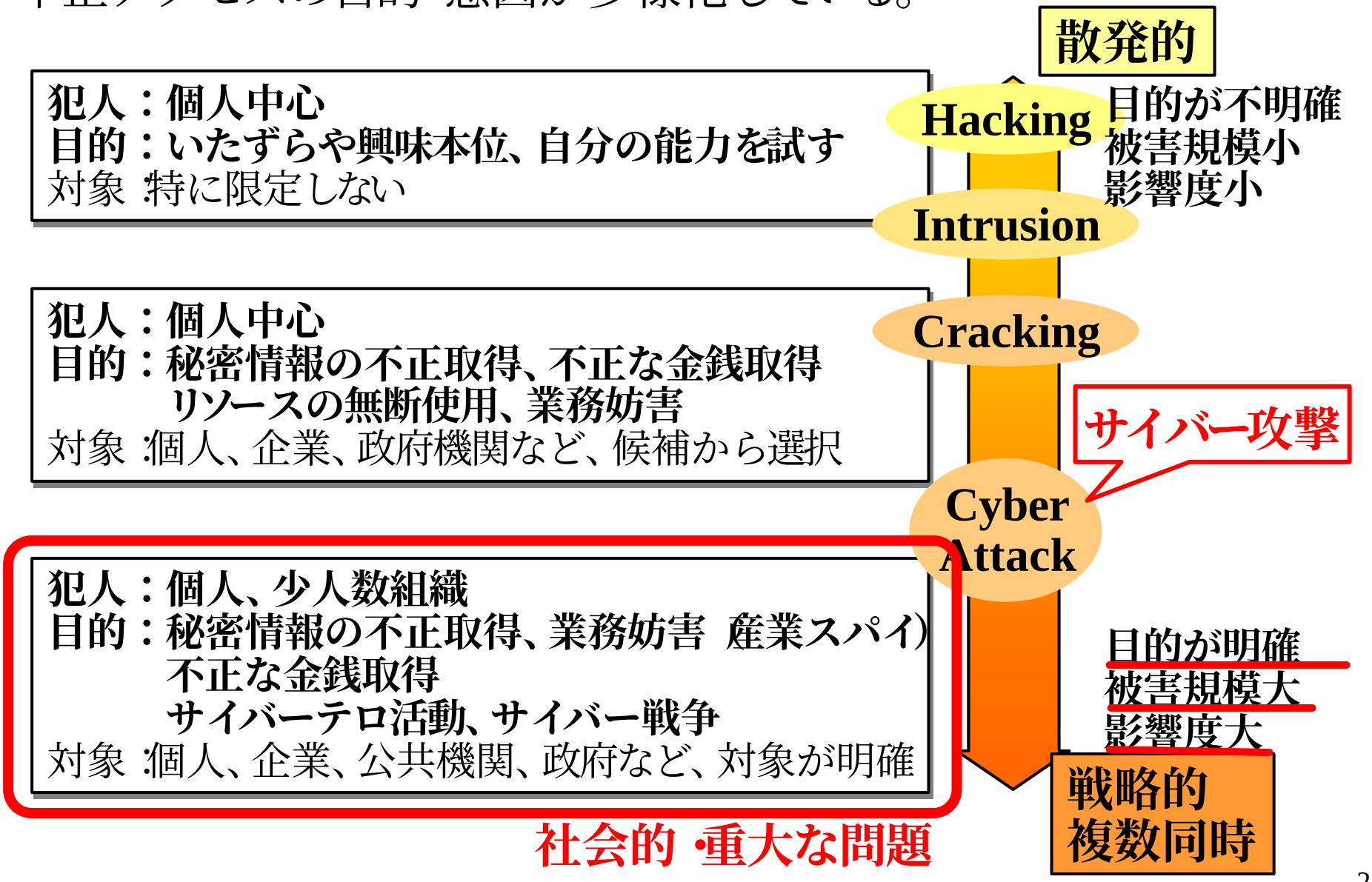
政府組織・企業・個人の多くのシステムがインターネットに接続し、利用している。＝インターネットに大きく依存しはじめた。



- 政府組織・企業・個人の区別なく、インターネットにつながっているすべての端末・システムが、不正アクセスの対象になる。
- 不正アクセス・サイバー攻撃による被害が、実世界に大きな影響を及ぼす。

2 不正アクセスの分類

- 不正アクセスの目的 ･意図が多様化している。

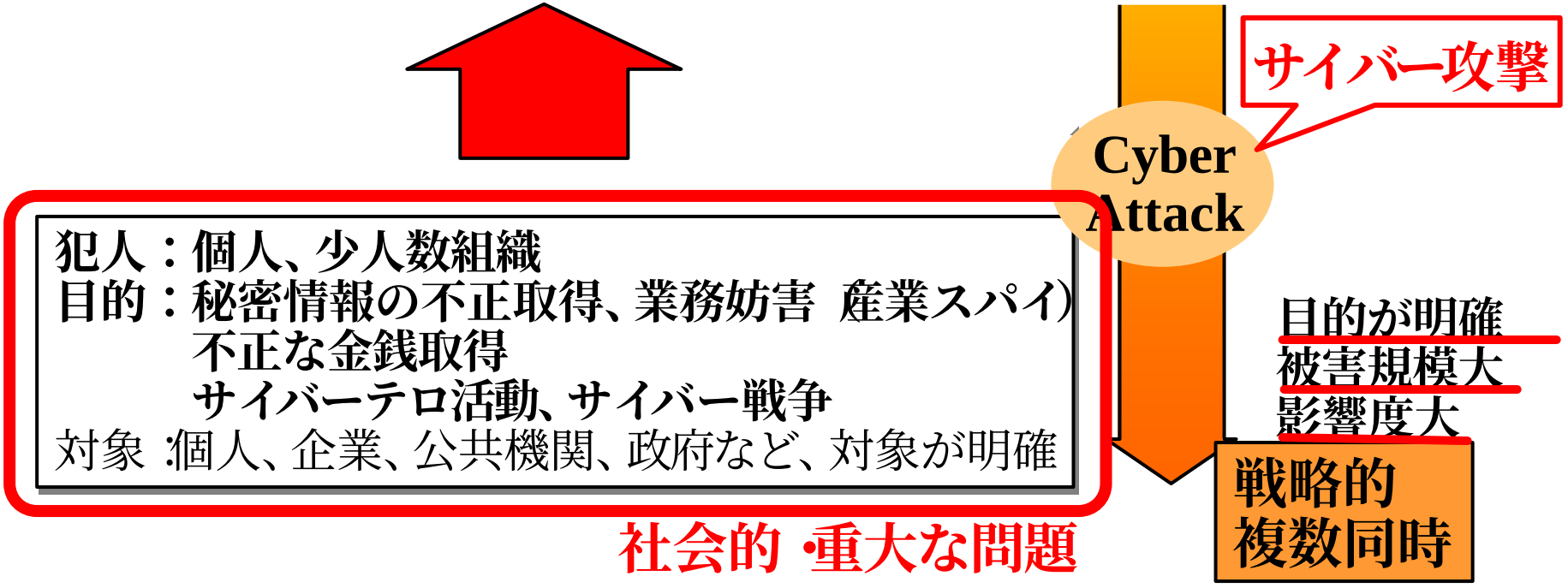


2 不正アクセスの分類

- 不正アクセスの目的・意図が多様化している。

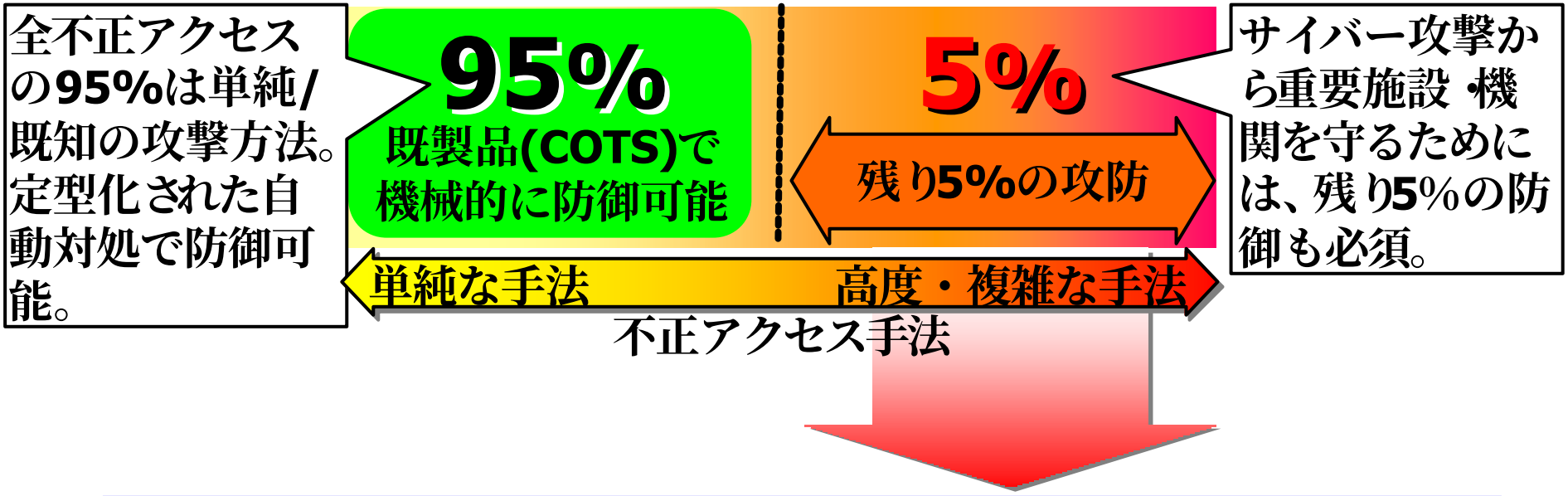
金融系、社会インフラ系、政府などの
重要施設・機関を攻撃目標とする場合が多い。

- 長期にわたる念入りな事前準備
- 高度な手法／内部犯によるサイバー攻撃



２１重要システムへの不正アクセスと対策方針

既存の製品・技術だけで不正アクセス・サイバー攻撃を100%防ぐことは不可能!



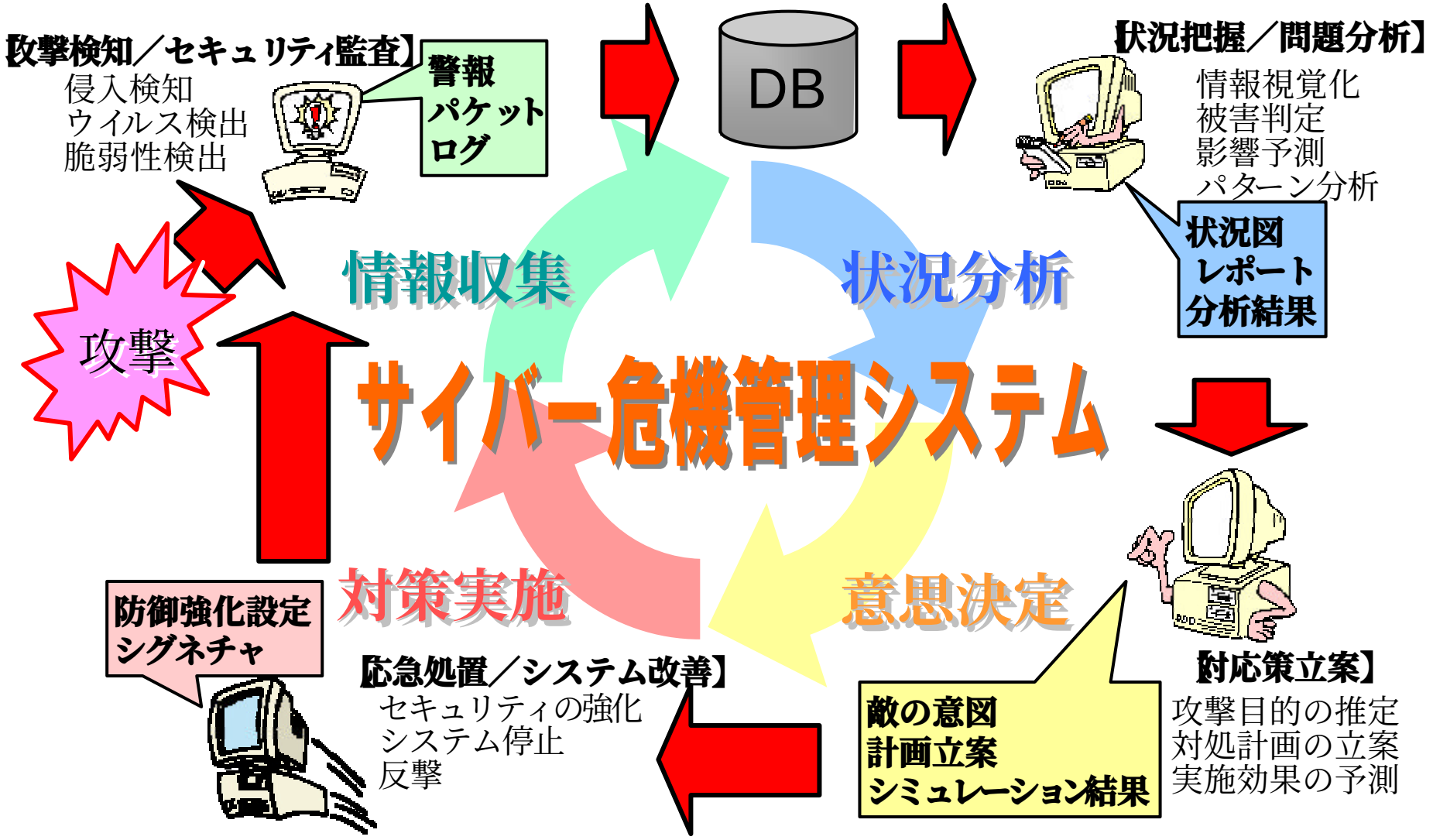
人間の手による高度な不正アクセス・サイバー攻撃に対して、

- 人間が状況把握・分析・判断等の対応を行なうべきである。
- 広範囲でより多くの情報を収集し、人間が把握・分析する。

～人間主体のシステム～

3. 不正アクセス対策システムのコンセプト提案

- 監視～分析～対応までトータルシステム
- 人間の状況把握・意思決定を含めた対応ワークフロー

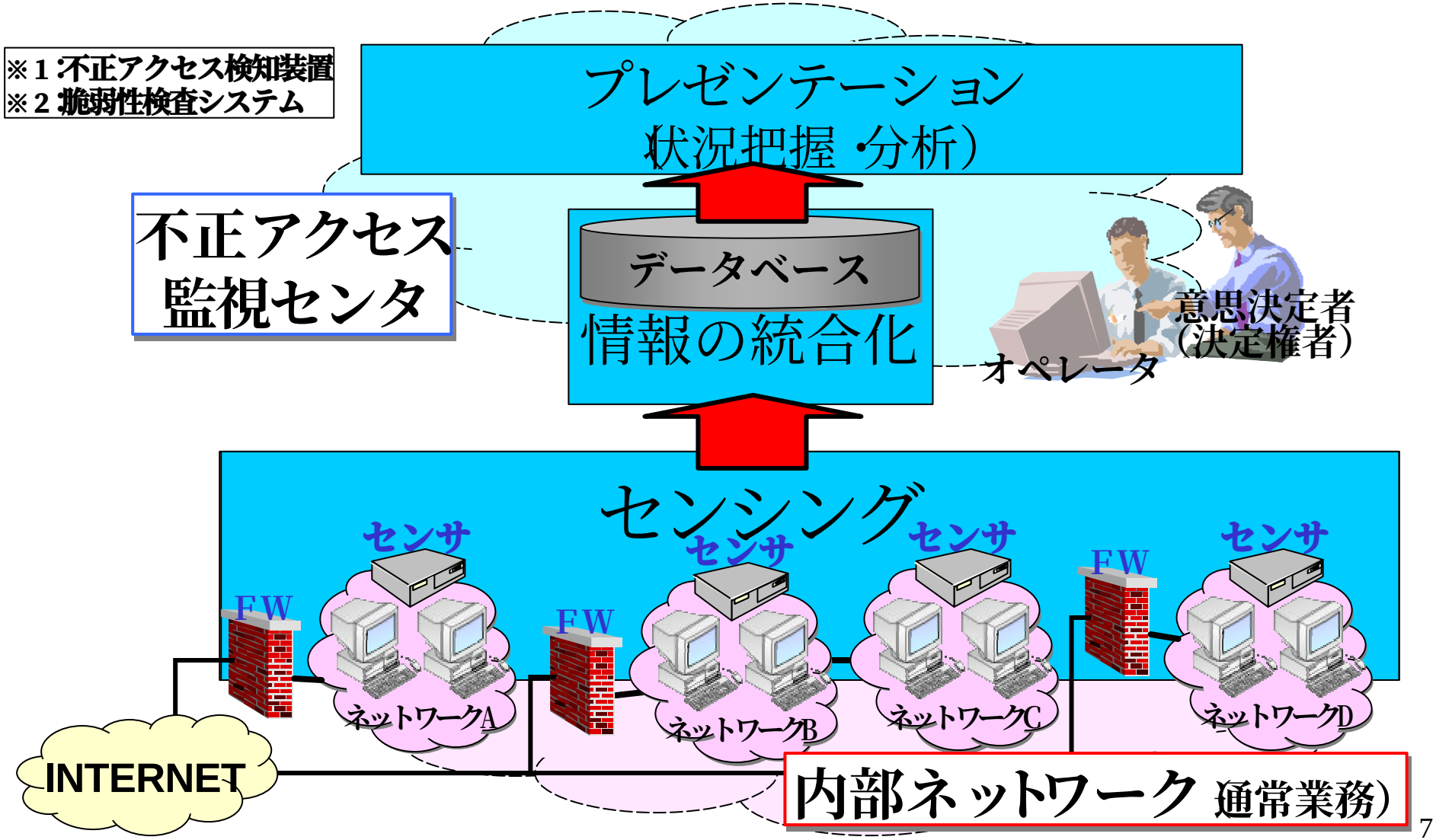


3. 不正アクセス対策システムのコンセプト提案

- 監視～分析～対応までトータルシステム
- 人間の状況把握・意思決定を含めた対応ワークフロー

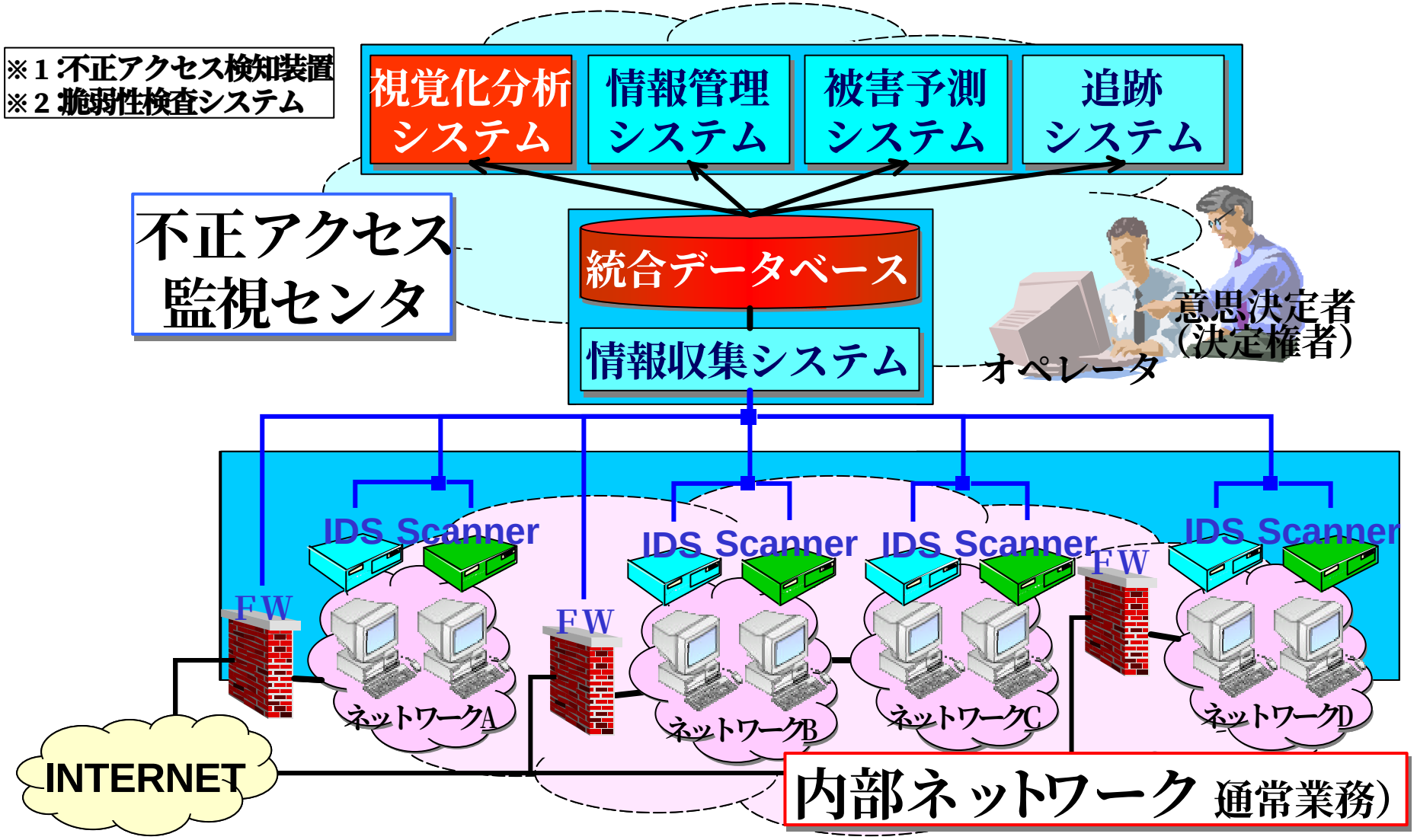
3.1開発システム全体構成

異種・複数センサ（IDS※1・Firewall・Scanner※2）からの情報を
統合データベースでまとめ、各分析システムにて、分析・意思決定を行う。



3.1開発システム全体構成

異種・複数センサ（IDS※1・Firewall・Scanner※2）からの情報を
統合データベースでまとめ、各分析システムにて、分析・意思決定を行う。

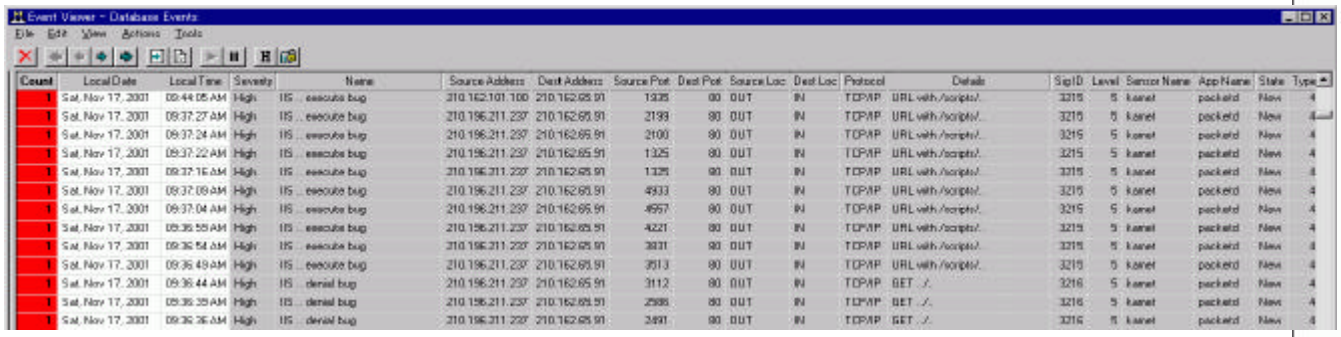


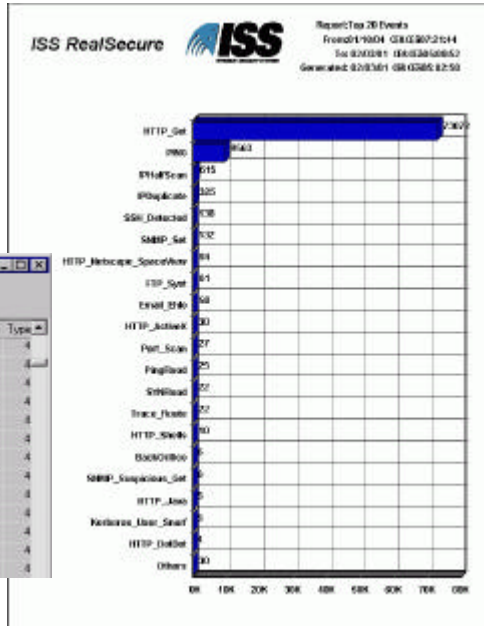
4. データベースの必要性

不正アクセス検知情報（≒警報）の分析・利用の現状：

- 1つ1つの警報のみに注目した分析が中心。
- 分析ツールは、統計計算をしてグラフ表現する程度。

＝ テキスト・ログ、リスト構造による警報の蓄積





- **各ベンダのフォーマットの異なる警報をまとめて扱いたい。**
- **大量の警報を使った分析がしたい。**
- **データマイニングをしたい。**
  - 検索性能
  - データの管理方法

4.1データベースの基本要求と設計の流れ

データベース設計における要求条件

- **管理の効率化**
  - –独立性を高めてデータの管理を容易にする
- **警報の網羅的な蓄積**
  - –オリジナル情報の保持、情報量の確保
  - –情報追加＝許可/変更＝不可
- **履歴管理**
  - –過去の情報との比較分析

データベース設計の流れ

1. **分析フレームワーク（手順）の定義**
2. **分析手法の決定**
3. **必要なデータの選定**
4. **DOAによる検討（OMT記法）**
5. **E-Rモデルによる設計**

4.2分析フレームワークと分析手法

「状況分析」のフェーズにおいて実施する分析フレームワークの各ステップと分析手法の対応

対応ステップ ＼ 分析手法	a	b	c	d	e
1. 緊急対応フェーズの開始判断	—	—	—	—	—
2. 監視対象全体の状況把握	○	◎		◎	
3. EOIの抽出		◎	○	○	○
4. EOIの内容分析					
i. 不正アクセス元の同定	○	○	◎	○	
ii. 不正アクセスの段階推定	◎	◎		○	
iii.犯人の意図、最終目標の推測	○	◎	○	○	◎
5. 被害推定					
i. 被害範囲、程度の推定		◎		○	◎
ii. 対処による効果推定		○		○	◎
6. 対策の立案／実施		○	○	○	◎

◎実施必須　○要実施　**[無印]**実施可　－実施不要

a 警報の時系列分析
b 不正アクセスの種類分析
c 不正アクセス元の分析
d 不正アクセス対象のロケーション分析
e 不正アクセス対象の属性分析

4.3分析手法とデータ項目

各分析手法にて用いるデータを選定し、オブジェクト毎にまとめる。

分析手法

a.警報の時系列分析
不正アクセスの発生時刻から、時間的な変化を追跡したり、時刻や曜日などに関係した周期性を捉える。

b.不正アクセスの種類分析
不正アクセスの段階や、その不正アクセス自身の攻撃の強さ(インパクト)を知る。

c.不正アクセス元の分析
送信元アドレスやドメイン名、ホスト名によって、不正アクセス元を分類する。

d.不正アクセス対象のロケーション分析
不正アクセス対象のロケーション（アドレスやドメイン名、ホスト名、所属組織、業務）を分類する。

e.不正アクセス対象の属性分析
不正アクセス監視対象ネットワークの多種の情報（セキュリティホール、脆弱箇所）を分析する。

要求データの選定

1.警報 (不正アクセスの情報)
- ➢不正アクセス発生日時
- ➢不正アクセスの種類・強さ
- ➢不正アクセス元／先のアドレス

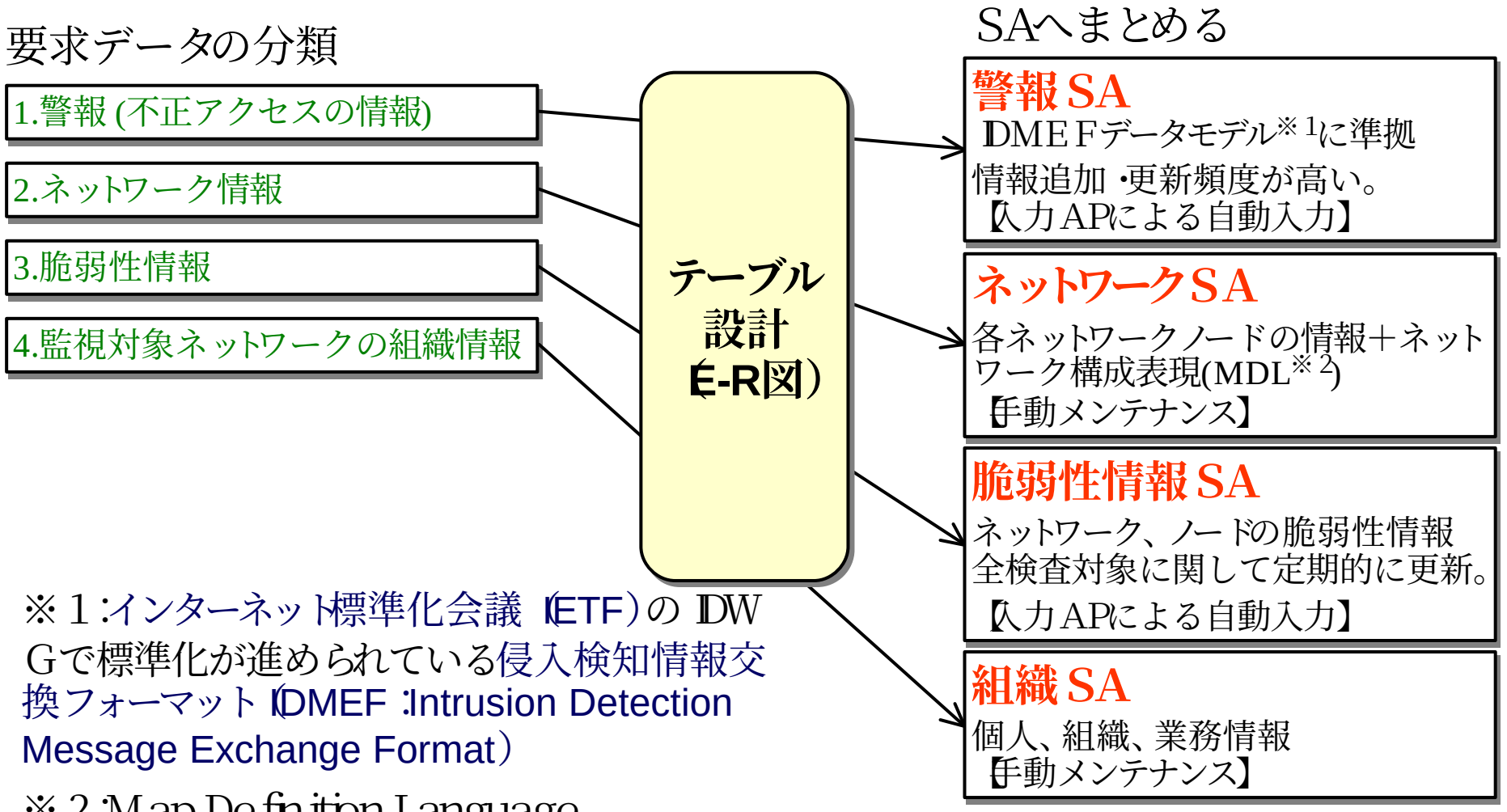
2.ネットワーク情報
- ➢ノード情報(ハードウェア)
- ➢ノード情報(ソフトウェア)
- ➢OS情報
- ➢利用者，管理者
- ➢ネットワーク構造

3.脆弱性情報
- ➢脆弱性検査結果

4.監視対象ネットワークの組織情報
- ➢所属組織
- ➢業務

4.4サイバー危機管理用データベース(C2MDB)の設計・実装

要求データを元にE-Rモデルを用いてテーブルを設計する。
テーブルをサブジェクトエリア(SA)へまとめ、テーブルスペースをあてはめた実装とする。

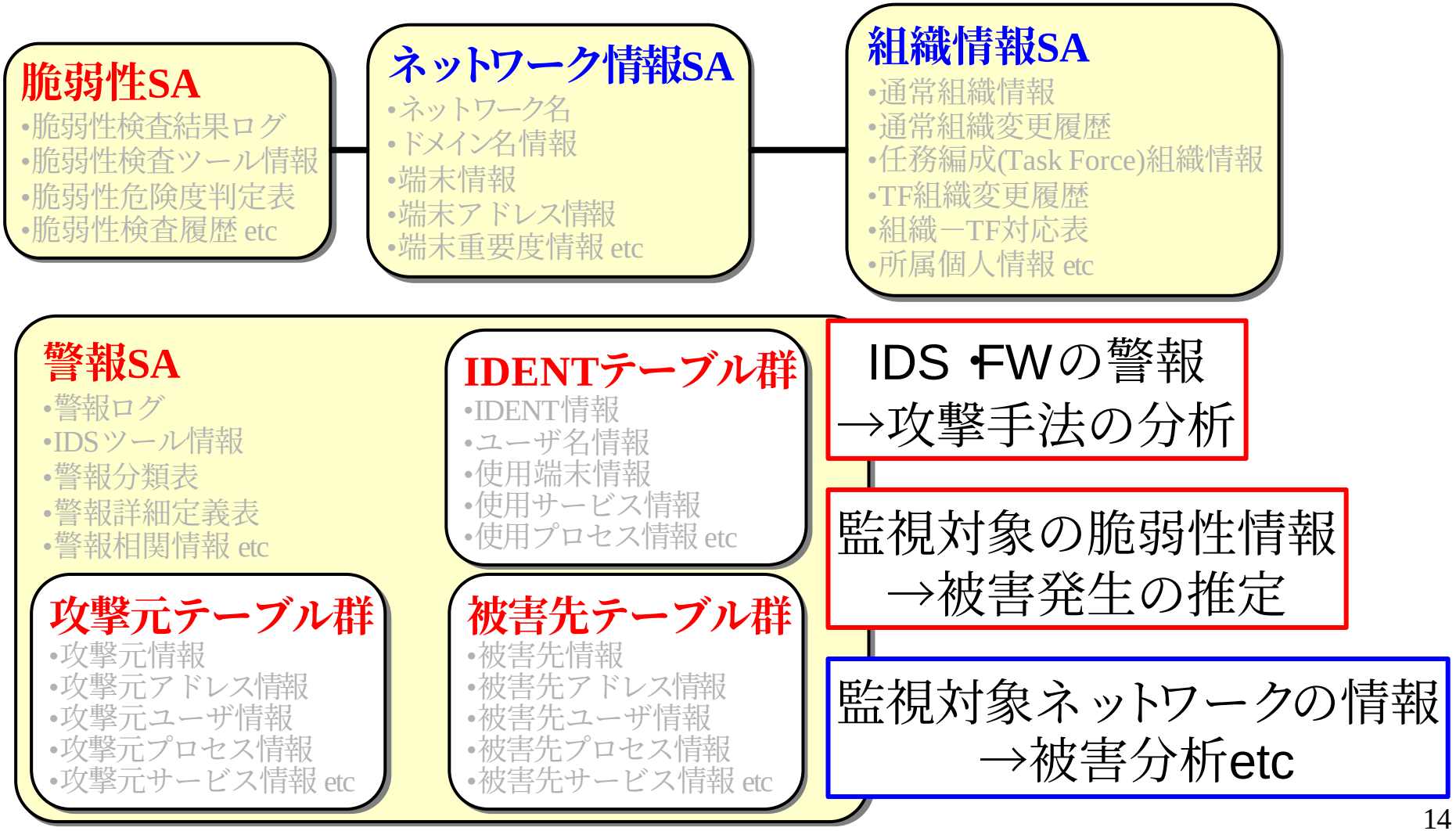


※1:インターネット標準化会議(IETF)のIDWGで標準化が進められている侵入検知情報交換フォーマット(IDMEF:Intrusion Detection Message Exchange Format)

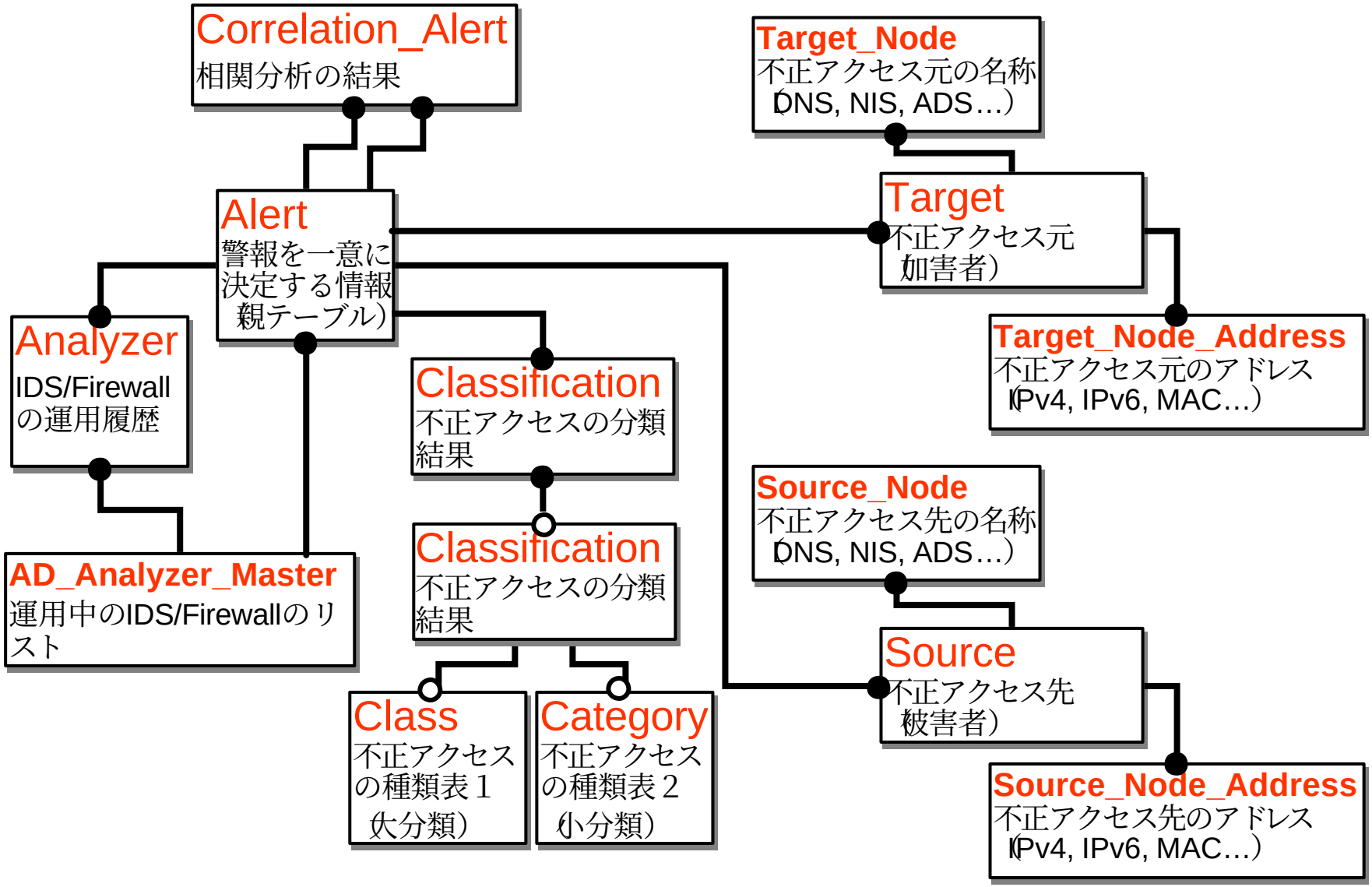
※2:Map Definition Language

4.5統合データベースC2MDBの構造（概略）

IDMEFに基づくアラート情報だけでなく、脆弱性情報、ネットワーク構成情報を持つことで、攻撃情報の分析だけでなく、総合的な分析も可能になる。



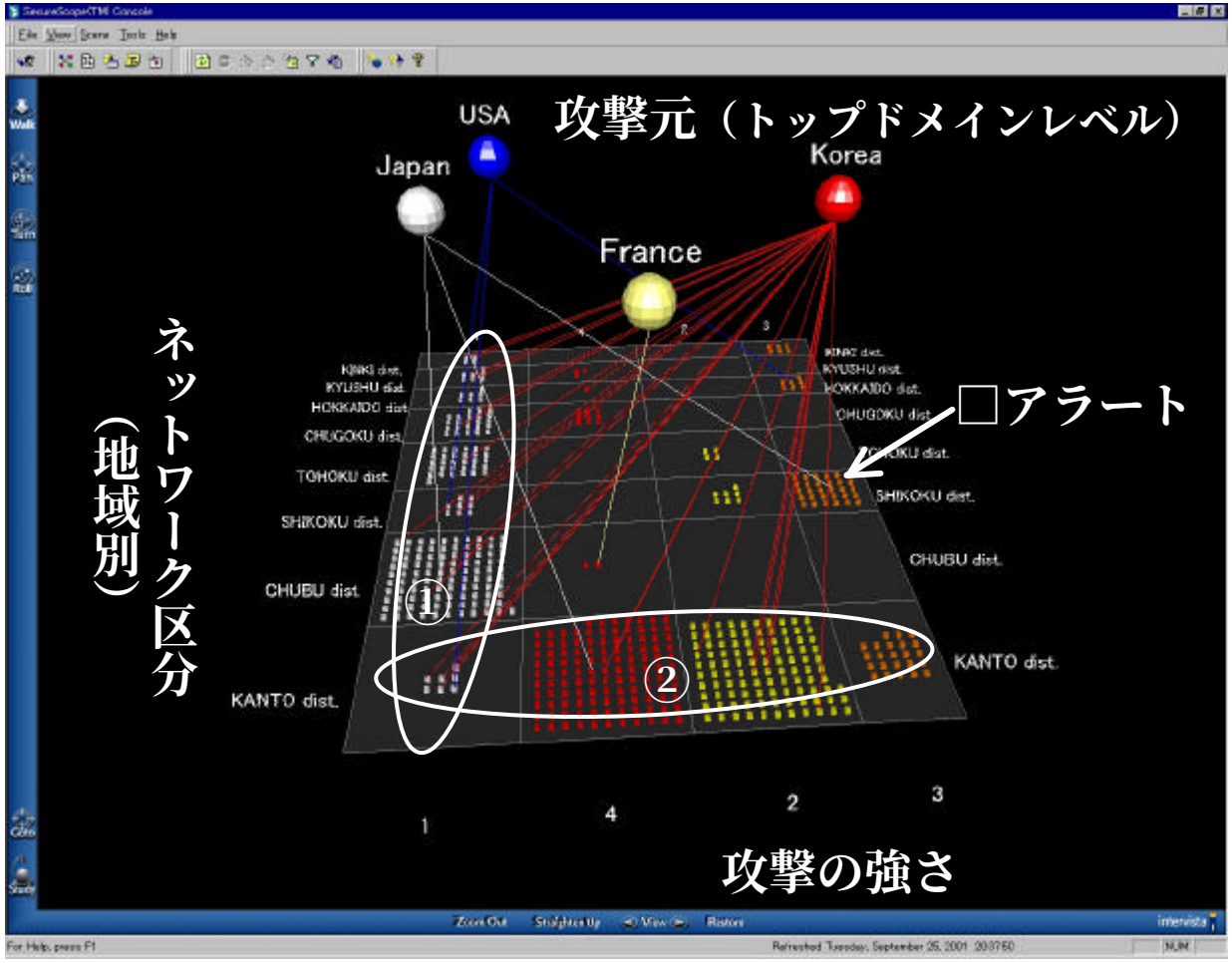
4.6 警報SA


Correlation_Alert
相関分析の結果
Alert
警報を一意に決定する情報（親テーブル）
Analyzer
IDS/Firewallの運用履歴
AD_Analyzer_Master
運用中のIDS/Firewallのリスト
Classification
不正アクセスの分類結果
Classification
不正アクセスの分類結果
Class
不正アクセスの種類表１（大分類）
Category
不正アクセスの種類表２（小分類）
Target_Node
不正アクセス元の名称（DNS, NIS, ADS…）
Target
不正アクセス元（加害者）
Target_Node_Address
不正アクセス元のアドレス（IPv4, IPv6, MAC…）
Source_Node
不正アクセス先の名称（DNS, NIS, ADS…）
Source
不正アクセス先（被害者）
Source_Node_Address
不正アクセス先のアドレス（IPv4, IPv6, MAC…）

5. 視覚化分析例 ―ステップ1―

オブジェクトの関係表示中心の視覚化

分析したい情報AをX,Y軸を用いて分類し、さらにZ軸方向にもう1種類の情報Bを配置し、AとBの関係を線で繋いで表現する。

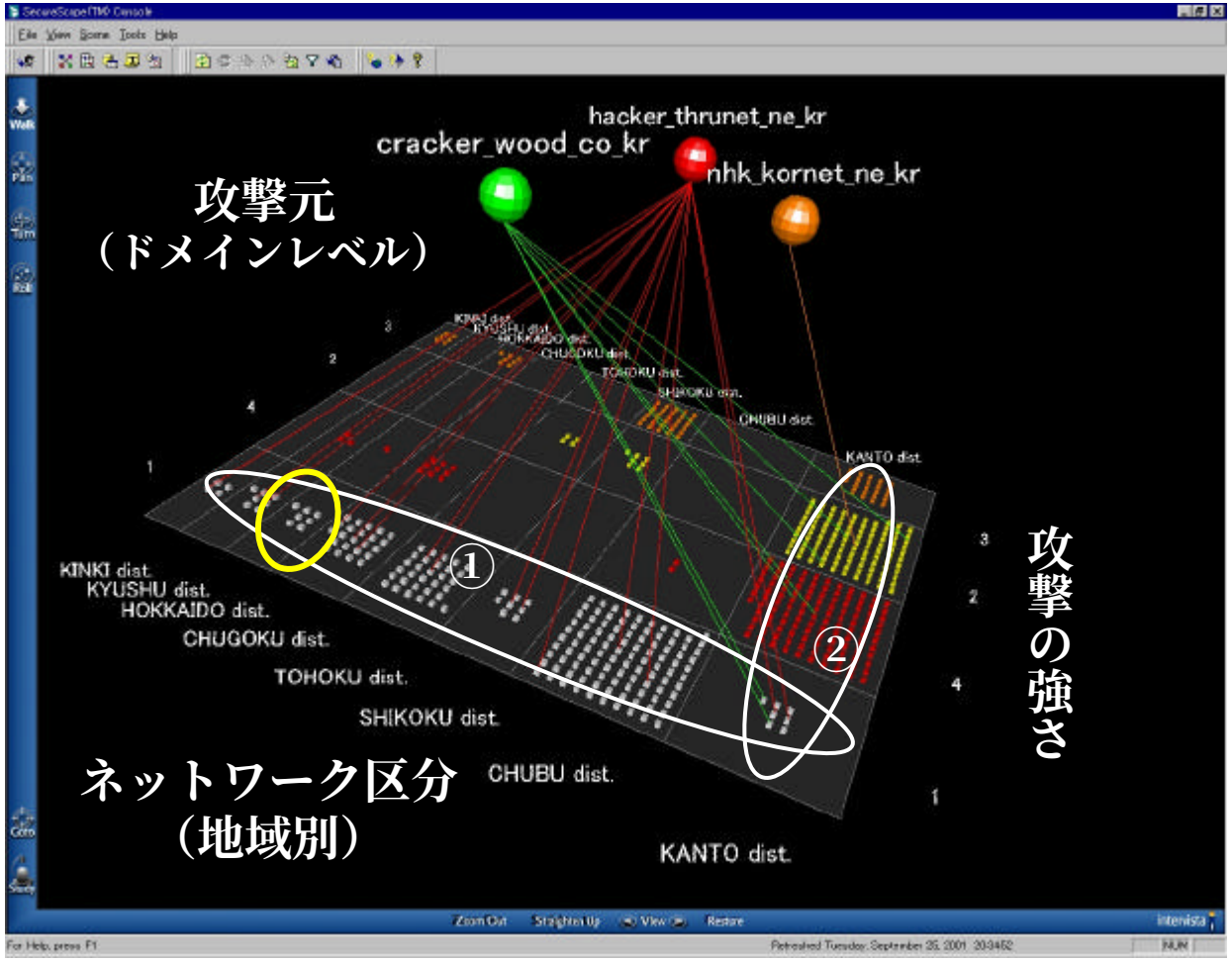


地域毎に独立したネットワークを持つ組織に対する攻撃元の傾向分析（想定）

- 韓国からの攻撃が多い。
- 韓国からの攻撃①は、関東から近畿まで全域に渡り、弱いレベルの攻撃（プローブ）を行なっている。
- 韓国からの攻撃②は、ターゲットを関東に絞って、集中的に攻撃を行なっている。

5.1視覚化分析例 ―ステップ2―

表示項目（上部の球）を変更



地域毎に独立したネットワークを持つ組織に対する攻撃元の傾向分析（想定）

- トップドメイン「韓国」を各ドメインレベルに詳細化して分析したところ、①と②は攻撃元が異なることが判明。
- ①の攻撃は、まだ北海道地区が行なわれていないことから、そこが次のターゲットになると予想される。

C2MDBから分析手法に応じて、さまざまな情報を取り出し、視覚化することが可能となった。

6. まとめと今後の課題

重要なシステムに対する高度な不正アクセス・サイバー攻撃に対処する方法として、定型化された自動対処システムに人間の高度な分析と的確な意思決定を加えた方法およびシステムを提案した。
このシステムに必要なC2MDBを構築し、それを用いた分析ワークフローおよび具体的な分析手法を示した。

今後の課題：

- 実データを用いた評価（C2MDBへの入力と視覚化分析）
- 警報収集～状況把握～分析～被害推定まで自動連携化
  - 警報－C2MDB入力システム
  - 被害推定システム
- 視覚化による状況把握・分析方式の有効性の検証
  （有効なデータマイニング手法の検討と検証）
- C2MDBの改良　（DMEF ver0.6対応）