JNSA

NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

# 脆弱性定量化に向けての検討WG活動報告

金岡 晃
セコム株式会社

2006 年 5 月 30日

# 参加メンバー

| 氏名 | 会社名 |
|---|---|
| 鹿児島　健 | 株式会社インフォセック |
| 小野　泰司 | 株式会社インフォセック |
| 齊藤　伸雄 | ウチダインフォメーションテクノロジー株式会社 |
| 北島　健治 | エス･アンド･アイ株式会社 |
| 郷間　佳市郎 | 京セラコミュニケーションシステム |
| 中嶋　一樹 | 住商エレクトロニクス株式会社 |
| 金岡　晃 | セコム株式会社 |
| 小野　潤 | 大日本印刷株式会社 |
| 川又　祥正 | 大日本印刷株式会社 |
| 坂本　慶 | 株式会社ディアイティ |
| 松井　康宏 | 日本アイ･ビー･エム株式会社 |
| 宮永　直樹 | 日本電気株式会社 |
| 世良田　照治 | 日本電気株式会社 |
| 奥原　雅之 | 富士通株式会社 |

| 氏名 | 会社名 |
|---|---|
| 長谷川 喜也 | 富士通株式会社 |
| 倉持　慎一郎 | 富士通サポート＆サービス株式会社 |
| 鶴田　章浩 | 富士通サポート＆サービス株式会社 |
| 能見　真也 | 富士通サポート＆サービス株式会社 |
| 伊勢　俊介 | 富士通サポート＆サービス株式会社 |
| 伊澤　誠 | マイクロ総合研究所 |
| 中山　和郎 | みずほ情報総研株式会社 |
| 伊藤　良孝 | 三井物産セキュアディレクション株式会社 |
| 後沢　忍 | 三菱電機株式会社　情報技術総合研究所 |
| 原田　道明 | 三菱電機株式会社　情報技術総合研究所 |
| 横山　哲也 | 横河電機株式会社 |
| 横地　裕 | 横河電機株式会社 |
| 岩井　博樹 | 株式会社ラック |

# 「攻撃が発生するメカニズム」を モデル化するというアプローチ

JNSA

- CVSSやMSの脆弱性に関する評価の違い
  → なぜ違うのか？
- 「検証可能」なものが必要なのではないか？
  → モデルを使ったアプローチ

結果的に、「なぜ攻撃が発生するのか」という メカニズムをモデル化することになった。

# なぜ、数値化のために「モデル」を示す必要があるのか？

- なぜ、その数値になるのかという、実社会に投射したモデルの必要性
- モデルが提示されていないものは説得力がない
  (説得力＝合意)
  → ブラックボックスでは合意が取れない。
  (私意が入る)
- 検証が可能であるかどうかも重要

※他の数値化アプローチは、なぜそのスコアになるのかというモデルの提示が不十分なのではないのか？

# モデル化に至るまでに検討されたこと

1. 「脆弱性とは何か？」のコンセンサスが、まず必要だった

2. 脆弱性の構成要素の検討

3. 攻撃が発生するまでの「参加者（主体）」（エンティティ）の設定し、これを「オブジェクト」とした

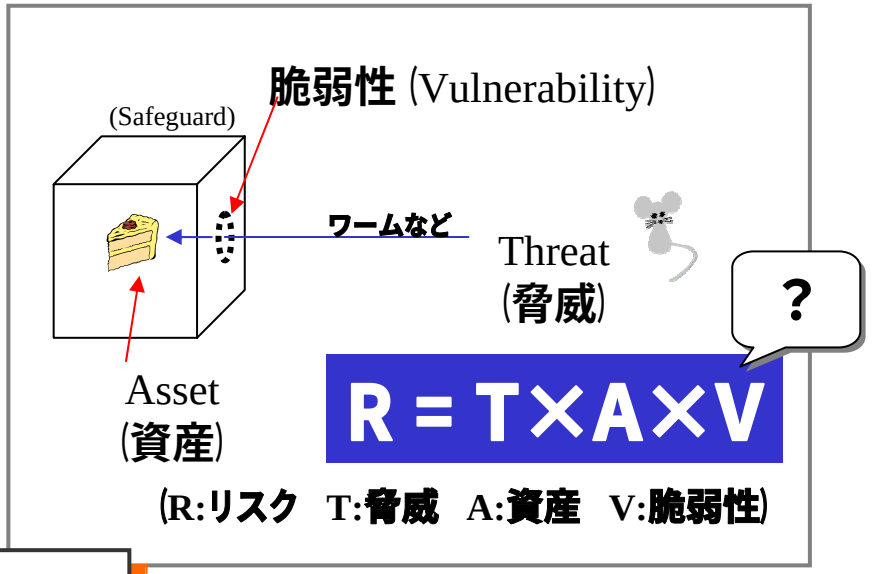
4. それぞれのオブジェクト間の関連（リレーション）の検討を行った
   それぞれのオブジェクトに対して、
   ・良い影響を与えるもの
   ・悪い影響を与えるもの
   を検討した

# 「脆弱性とは何か？」のコンセンサス

JNSA

## 脆弱性って何だ？

- 「脆弱性」というものの共通した意識がない
- 「脆弱性」と「リスク」の混同




## ゴール設定

どんな指標？

パッチがリリースされた時に、即座に適用するか、次の定期保守まで待つかという判断に使える指標

→ 純粋な「脆弱性」よりも、脅威をある程度含んだ、リスクに近い危険度を求める

→ 仮に「Z (Zeijakusei)」と呼ぶことにした

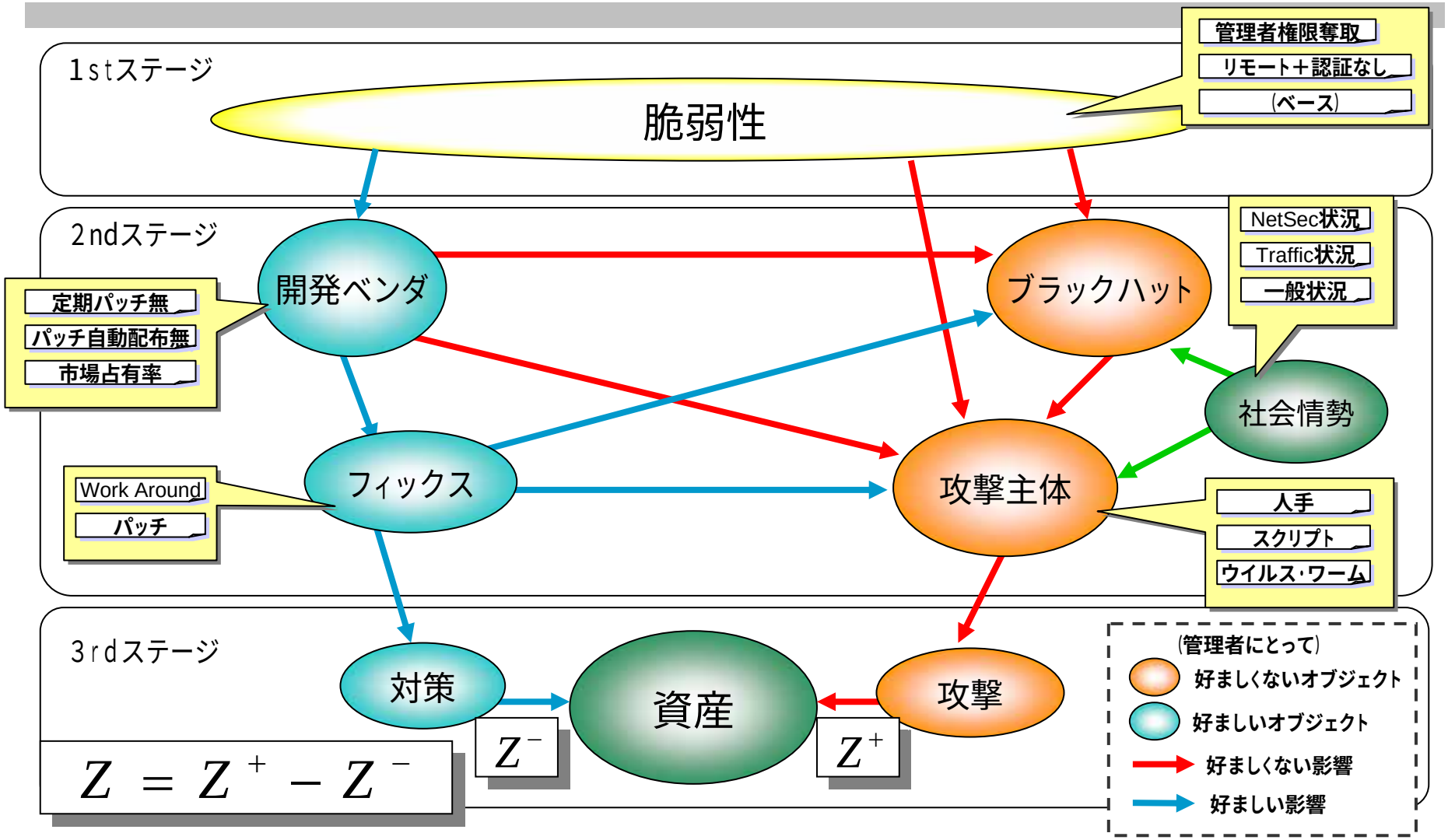
**「意思決定者が、対応する／しないの決定、あるいは、対応の緊急性を判断するための指標となる数値」**

# Z (Zeijyakusei) の構成要素

| 要素名 | 内容 |
|---|---|
| 手法 | Exploitの存在、レースコンディション |
| 影響 | CIAの要素 v.s. 権限＋ブランド |
| 環境 | プロトコルのリモート/ローカル、認証 |
| 対策 | 対策をとれるか否か、それが一時的なものか<br>正式な対策が出ている・一時的 (Workaround) ・ない<br>副作用の話 |

| 要素名 | 内容 |
|---|---|
| 原因 | 仕様・コーディング・設定<br>パッチの作り易さ |
| ターゲット属性 | 誘引性 |
| ソフトウェア特性 | ソフトウェアのシェア、ベンダー |
| 社会情勢 | 定期的、テンポラリ⇒イベント、カレンダー |

# 攻撃発生のメカニズム



# 用語定義

- 脆弱性
  - ソフトウェア及びハードウェアに存在するものであり通常期待されている安全性を損なっている要因
- フィックス
  - 脆弱性を除去するもの／こと
- パッチ
  - ソフトウェアでフィックスするもの
- ワークアラウンド
  - 副作用のあるフィックス
- 開発ベンダー
  - 対象となるハードウェア、ソフトウェアを開発した人または組織
- ブラックハット
  - 攻撃者に手段や手段に関する情報を提供する人または組織（ウイルス作成者も含む）
- 社会情勢
  - 攻撃行為の動機に影響を与える事象一般
- ウイルス・ワーム
  - 攻撃者のうち自己の意思をもたないもの（ボットなども含む）

# モデル化から数式化へ

- 数値化方法の検討
- 一般的な式と、最も単純な式
  - モデル間の重み付け
- ユーザが入力可能なツールの作成
  - Excelシートによる計算

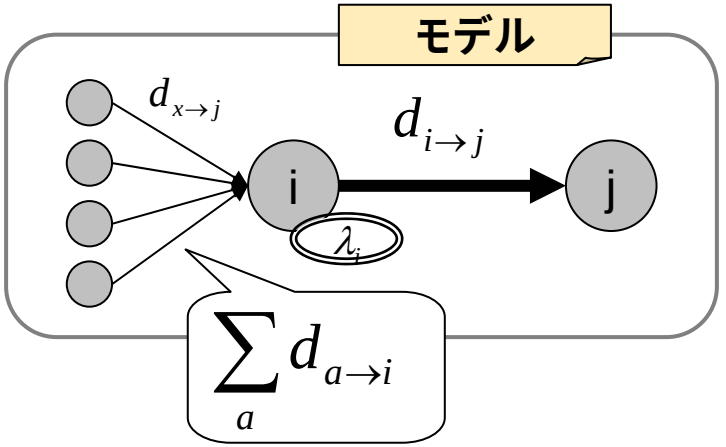
# 数式化に用いた数式とモデル

**一般式**

$$d_{i\to j} = f\left(\sum_a d_{a\to i} + \lambda_i\ ,\ j\right)$$

演算子は仮に和（＋）としてある

$d_{i\to j}$ ：オブジェクトi から オブジェクトj への矢印がもつ値




関数fや、演算をどうしましょうか？

**最も単純なものから考えよう**

・演算は和（＋）
・関数f は、総和に重みwで積（×）を取ったもの

$$d_{i\to j} = w_{i\to j}\left(\sum_a d_{a\to i} + \lambda_i\right)$$

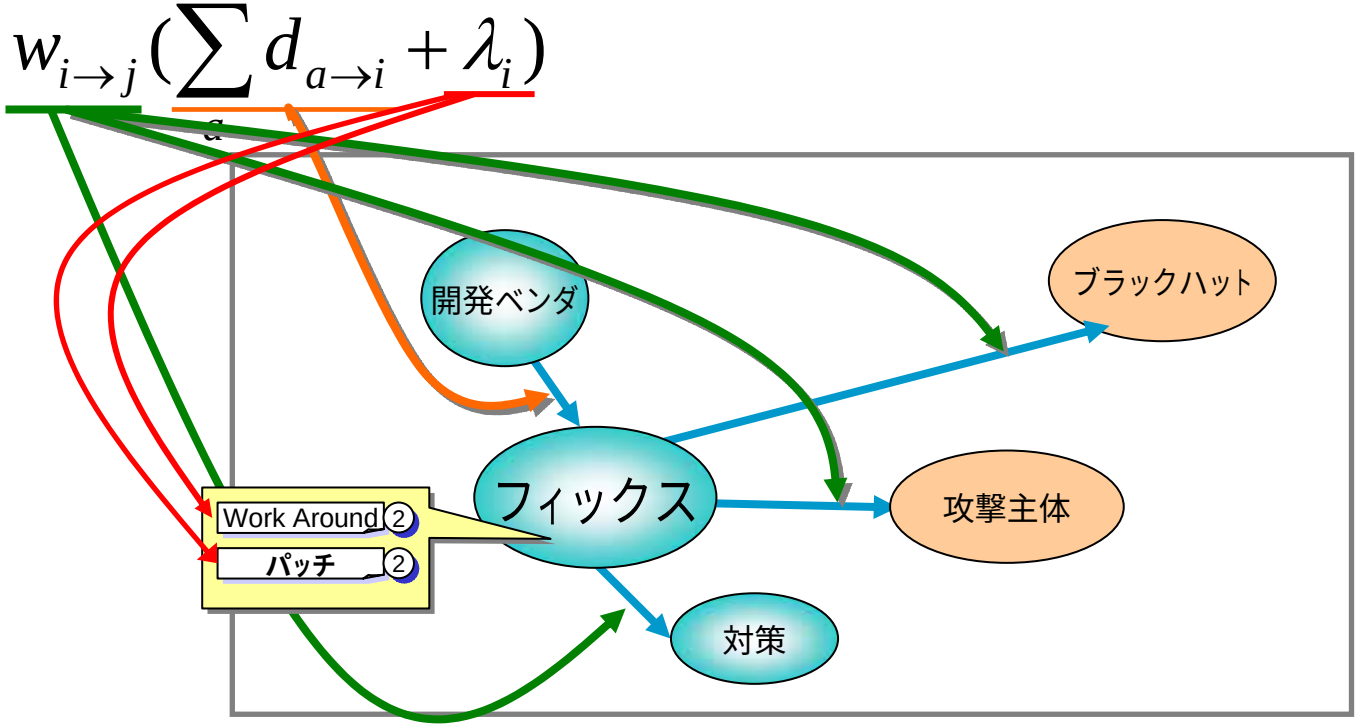
# WGで調整した値

**式のモデル図**

・演算は和（＋）
・関数f は、総和に重みwで積（×）を取ったもの

**我々が調整した値**

$$d_{i\to j} = w_{i\to j}\left(\sum_a d_{a\to i} + \lambda_i\right)$$



# 数値計算ツール（Excelシート）

固有値の計算部分

$\lambda_i$

オブジェクト名
（色はモデル図に従う）

$$d_{i\to j} = w_{i\to j}\left(\sum_a d_{a\to i} + \lambda_i\right)$$

オブジェクト
がもつ属性

| 脆弱性 | 有無 | 重み係数 |
|---|---|---|
| 管理者権限奪取可能 | 1 | 2 |
| リモートからの認証なし利用可能 | 1 | 2 |
| （ベース） | 1 | 1 |
| 固有値 | | 5 |

属性の有無（0/1）、あるいは
度合（0-3とか0-5とか）

属性に対する重み
（同オブジェクト内での
関連を考慮）

# 数値計算ツール（Excelシート）

**矢印の重み** $w_{i \to j}$

$$d_{i \to j} = w_{i \to j}\left(\sum_{a} d_{a \to i} + \lambda_i\right)$$

$j$

| | | Destination | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 固有値 | 脆弱性 | | 社会情勢 | | 開発ベンダ | | フィックス | | ブラックハット | | 資産 | | 攻撃主体 | | 対策 | | 攻撃 | |
| | 到達オブジェクトの特 | | 1 | | 1 | | -1 | | -1 | | 1 | | 1 | | 1 | | -1 | | 1 | |
| Source | 脆弱性 | 5 | 0 | 0 | 0 | 0 | 2.4 | -1 | 0 | 0 | 2.4 | 1 | 0 | 0 | 0.6 | 1 | 0 | 0 | 0 | 1 |
| | 社会情勢 | 1.25 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.8 | 1 | 0 | 0 | 0.6 | 1 | 0 | 0 | 0 | 0 |
| | 開発ベンダ | 5 | 0 | 0 | 0 | 0 | 0 | 0 | 1.2 | -1 | 2.4 | 1 | 0 | 0 | 1.8 | 1 | 0 | 0 | 0 | 0 |
| | フィックス | 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.8 | -1 | 0 | 0 | 0.6 | -1 | 0.4 | -1 | 0 | 0 |
| | ブラックハット | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1.2 | 1 | 0 | 0 | 0 | 0 |
| | 資産 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| | 攻撃主体 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.8 | 1 |
| | 対策 | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | -1 | 0 | 0 | 0 | 0 | 0 | 0 |
| | | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |

$i$

前表から
算出された固有値

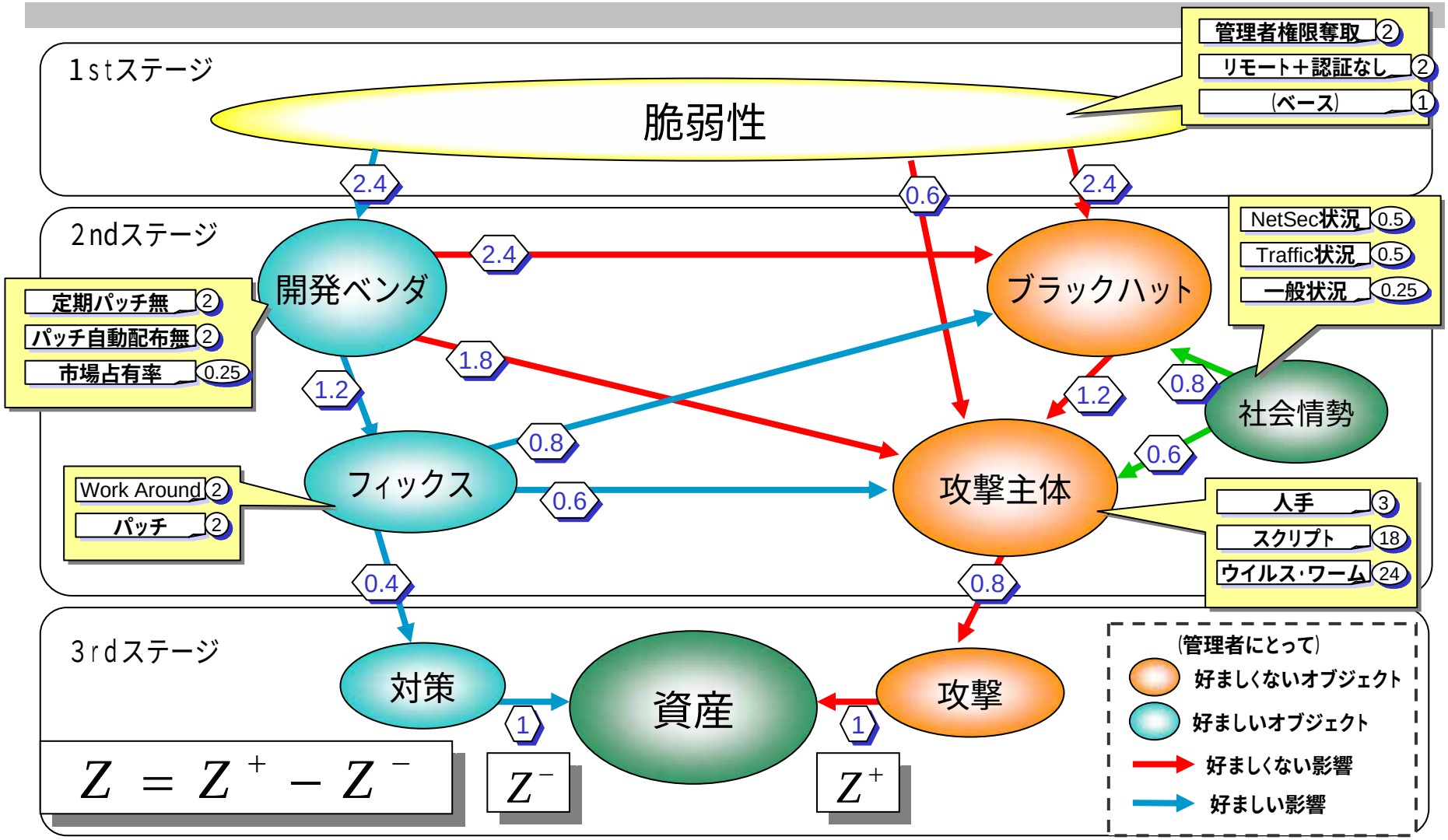
値の大きさは、
影響の度合

Sourceオブジェクトから
Destinationオブジェクト
に矢印があれば、
値をもつ

「好ましい」オブジェクトから
「好ましくない」影響（同類でない）
の矢印は　マイナスの値

「好ましい」オブジェクトから
「好ましい」影響　（同類）
の矢印は　プラスの値

# 攻撃発生のメカニズム



# 数値化の検証

- 実際に、ベンダから公表されている脆弱性情報を元に数値を算出

→ WGメンバ内でレビュー、重み値の修正

# 2006年度の計画

1. **数値化の確定、ツールの公開**
   - **公開後のコメント募集、改訂版**

2. **報告書の作成**
   - **攻撃発生モデルの詳細**
   - **数値化モデルの詳細**
   - **数値計算ツールの詳細**