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ワーキンググループ

金岡　晃

2007 年 6 月6日

Outline

- **ワーキンググループ概要**
- 2006**年度活動内容と成果物**
- **報告書概要**
- **報告書公開後の反応**

参加メンバー

氏名	会社名
郷間　佳市郎	京セラコミュニケーションシステム
小野　泰司	株式会社 IRIユビテック
鹿児島　健	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
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

(※ メンバーの所属は本WG活動中のものです)

活動目的と活動期間

WG発足時の状況と活動目的

ベンダ各々が独自の判断で脆弱性の危険度を報告

- 同じ「危険度高」であっても、A社とB社ではその判断基準が違う
- 判断基準そのものが公開されていない

ベンダの差に依存しない脆弱性の定量化が可能か？

WG活動期間

2004年11月-2007年3月：月2回のWGを開催

活動経過

2005年度以前

- 「脆弱性」の意味するところの合意
- 脆弱性の構成要素の検討
- 攻撃が発生するメカニズムのモデル化
- 数値化方法の決定

2006年度

- 数値化パラメータの決定
- 他組織との意見交換
- アンケートの実施・分析
- 報告書の作成・公開

報告書の概要

WG活動の時系列に沿った構成

1章	はじめに
2章	脆弱性
3章	攻撃発生のメカニズム
4章	トリアージ値の定量化
5章	トリアージ値の評価
6章	まとめ
付録A	アンケート結果分析
付録B	CVSS概要
付録C	TV算出ツール利用方法

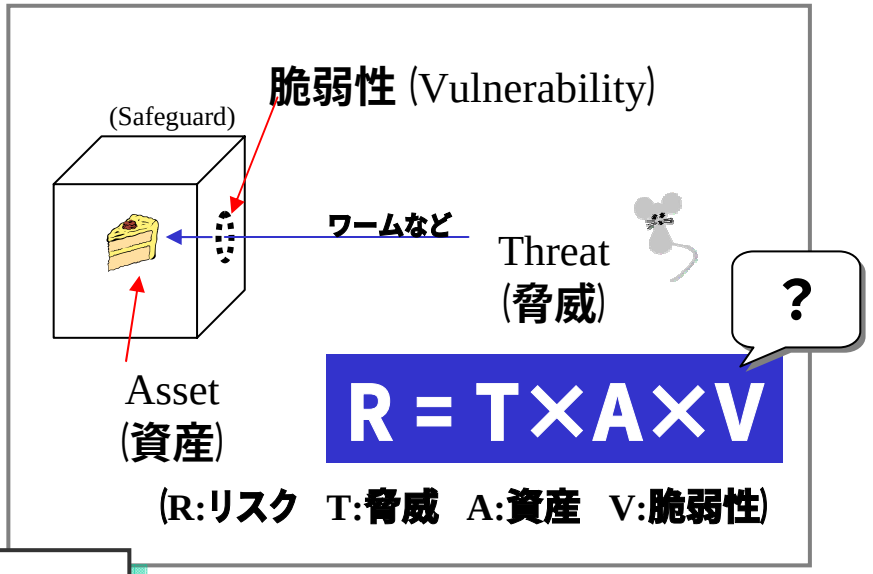
主に2005年度までの成果

2006年度の成果

「脆弱性とは何か？」のコンセンサス

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？

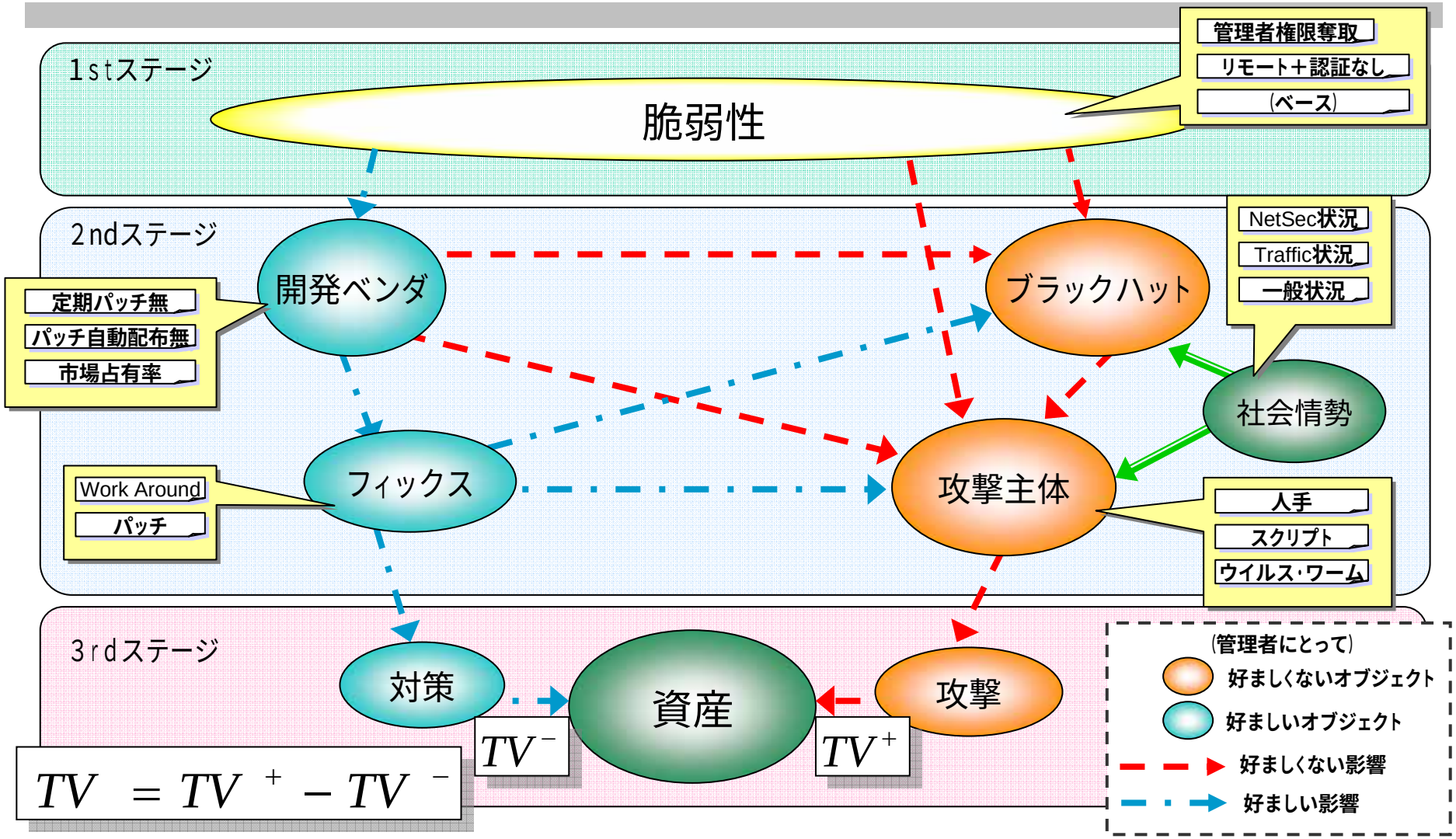
パッチがリリースされた時に、即座に適用するか、次の定期保守まで待つかという判断に使える指標

→ 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」

攻撃発生のメカニズム



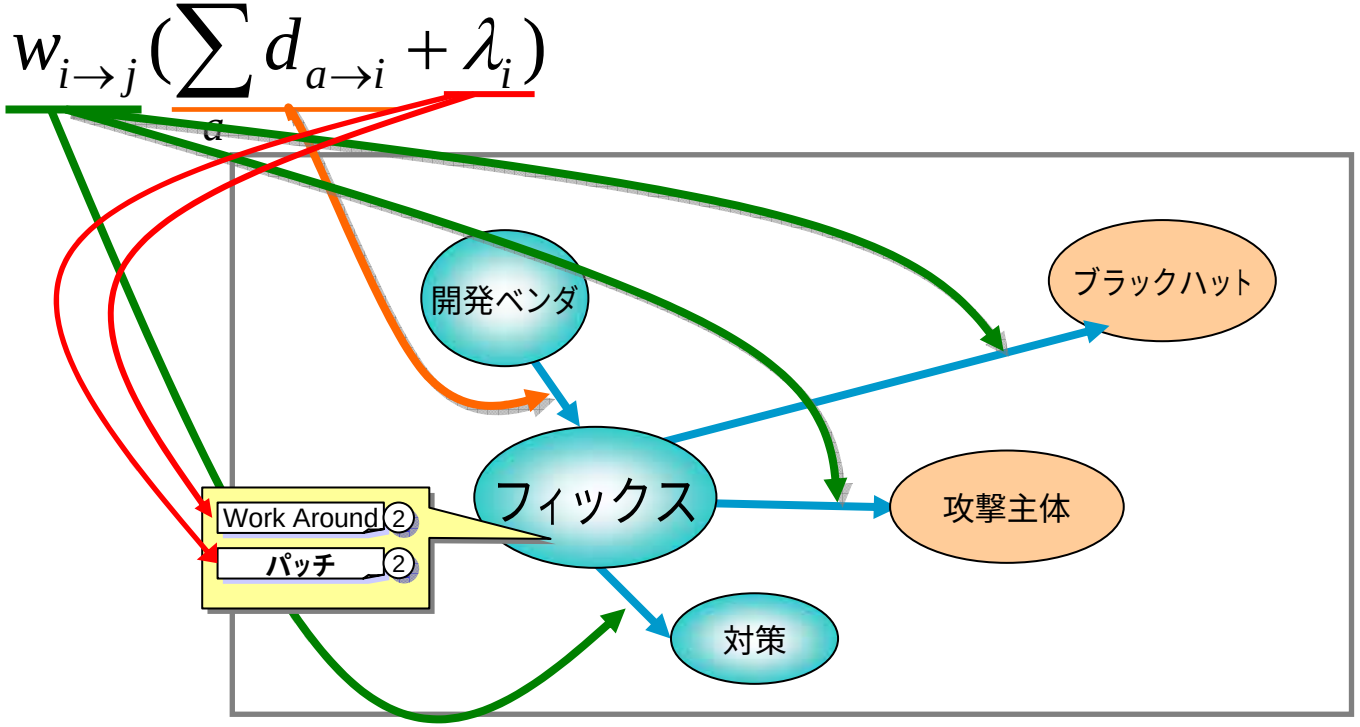
トリアージ値の定量化

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

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



トリアージ値の評価

アンケートの実施

ある脆弱性について、対象となるOSやソフトウェアの情報やそれらをめぐる状況･影響を詳細に記述した情報をもとに危険度を7段階で回答する形式

2006年
10月11日-11月20日
(41日間)
有効回答数：44

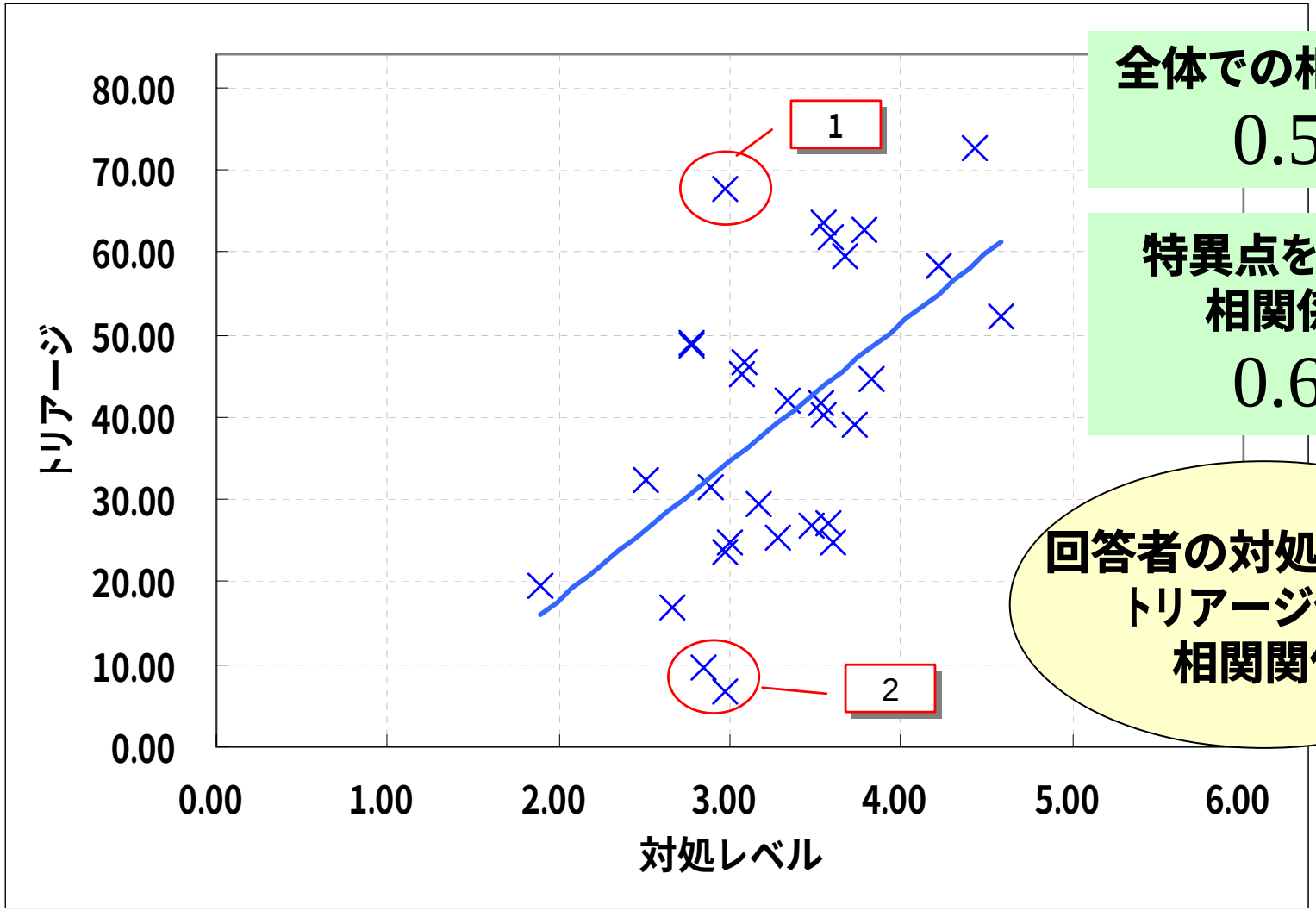
項目		特性情報
脆弱性	管理者権限の奪取が可能	○ or ×
	リモートから認証なしで利用が可能	○ or ×
攻撃状況		ウイルス・ワームが存在する/攻撃用ツールが存在する/ウイルス・ワーム、攻撃用ツール共に無し
対策状況		パッチあり/パッチ無し・回避策あり/パッチ・回避策共に無し
社会状況	ネット上の危険度	0～3
	ネットのトラフィック	0～2
	社会全体のセキュリティ	0～4

設問内容

レベル	
レベル6	今すぐ対処
レベル5	今日中に対処
レベル4	2～3日中に対処
レベル3	今週末に対処
レベル2	数ヶ月先に対処
レベル1	年内に対処
レベル0	対策しない

危険度（対処レベル）

アンケート結果とトリアージの関係



全体での相関係数

0.54

特異点を除いた相関係数

0.60

回答者の対処レベルとトリアージ値は相関関係

報告書公開後の反応

ネット上の記事・コラム

ITmedia	•「JNSA、脆弱性定量化手法の検討報告書を公開」 •「情報セキュリティあれこれ：脆弱性の切迫度の定量化モデル紹介」
マイコミジャーナル	•「システムの評価、できてますか？：トリアージ値、ご存知ですか？」
ソフトバンクビジネス+IT	•「【連載】3分セキュリティ講座 (25)：「広い視野」があってこそ意味がある「ゼロデイ攻撃対策」」

個人ブログなどでの言及も多数

好評価