VRDA
Vulnerability Response Decision Assistance

アート・マニオン
（Art Manion）
CERT/CC

伊藤 友里恵
（Yurie Ito）
JPCERT/CC

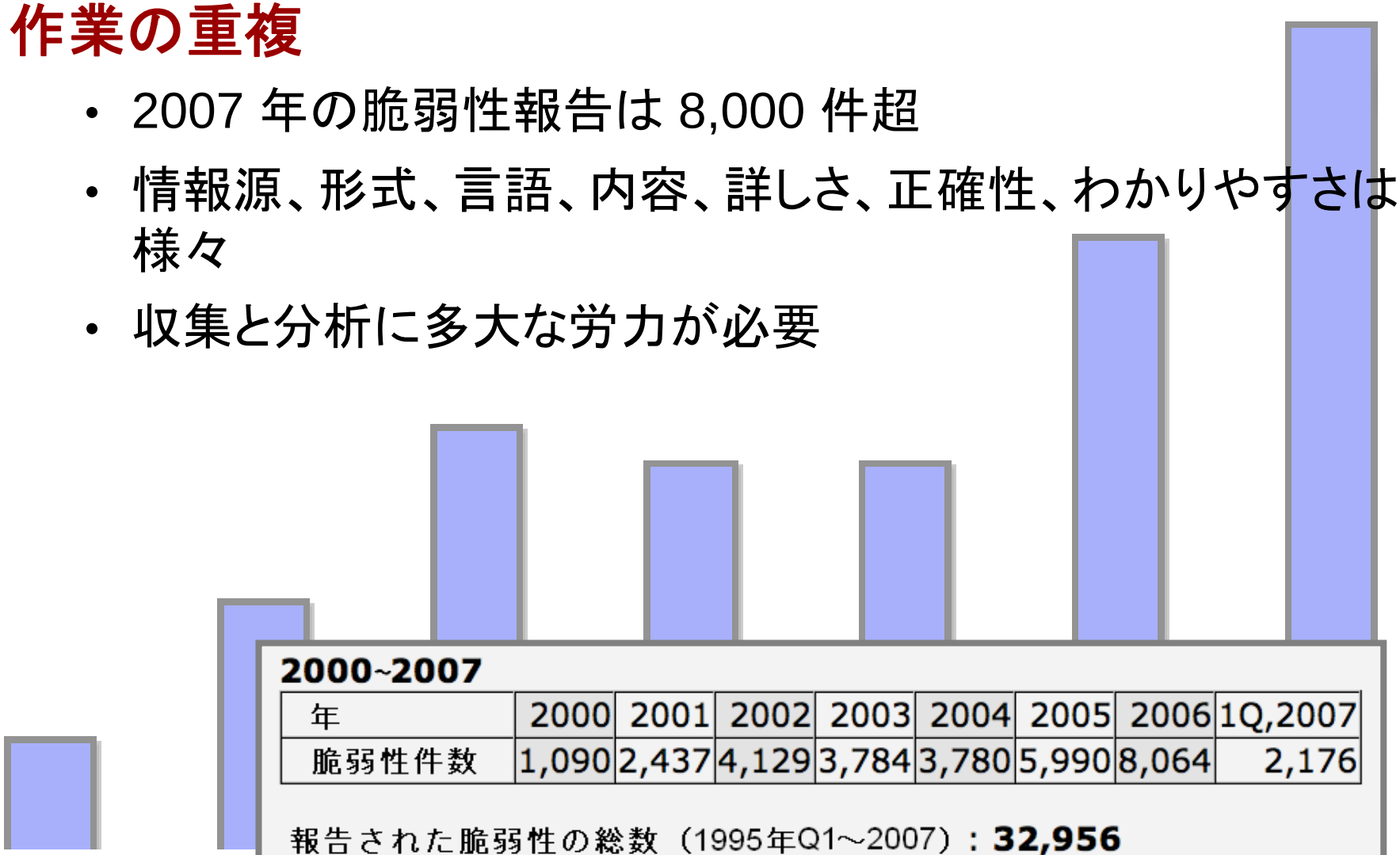
EC2ND 2007

VRDA の原理と設計

課題

作業の重複

- 2007 年の脆弱性報告は 8,000 件超
- 情報源、形式、言語、内容、詳しさ、正確性、わかりやすさは様々
- 収集と分析に多大な労力が必要



2000~2007

年	2000	2001	2002	2003	2004	2005	2006	1Q,2007
脆弱性件数	1,090	2,437	4,129	3,784	3,780	5,990	8,064	2,176

報告された脆弱性の総数（1995年Q1～2007）：**32,956**

課題(2)

対応の決定に一貫性がない

- 分析担当者の意見が一致しない
- 分析担当者が個人的な先入観を適用する
- 決定に組織の価値観が反映されないことがある

課題（3）

既存の評価基準が不十分

- ほとんどの評価基準は一般化された深刻度を示す
  - すべての組織に適しているわけではない
- CVSS（Common Vulnerability Scoring System）
  - 環境にかかわる評価基準が含まれる
  - 基本スコアに重点
- 組織によって価値観が異なる
  - 同じ脆弱性への対応が異なる場合がある
  - 異なるソフトウェアを使用する
  - 同じソフトウェアを異なる方法で使用する
  - 情報資産の価値評価が異なる

解決策

VRDA が答えようとしている問い:

脆弱性報告に対してどのように対応するのが最善か？

ゴール

- 脆弱性データを構造化された形式で記録する
- 個人による対応の意思決定を支援する
- 組織としての知を分析担当者から VRDA に移転する
- 対応の正確性と一貫性を改善する
- 作業の重複を減らす

対象者

システム管理者

- システムの修正にかかわる運用責任者

CSIRT

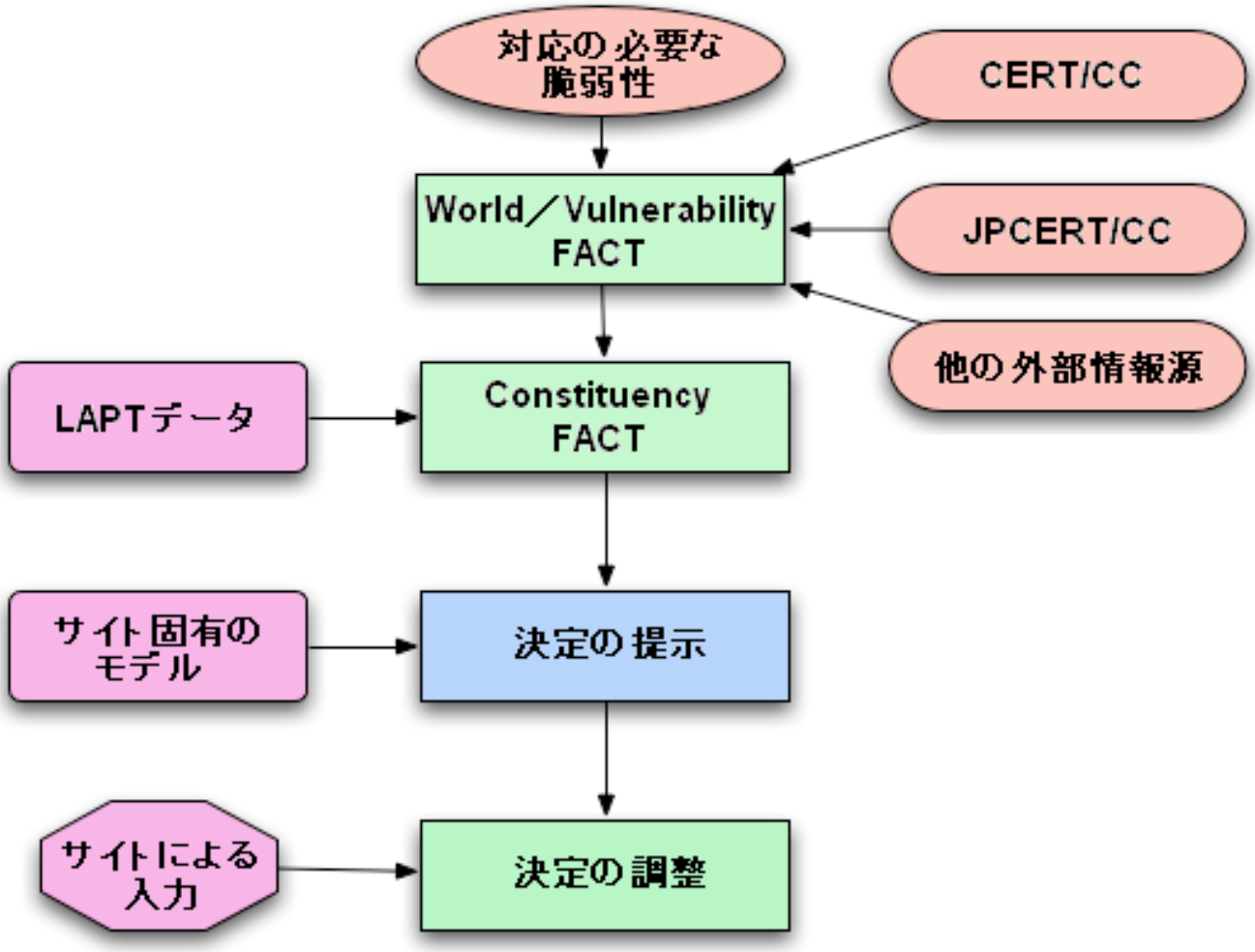
- システム管理者やユーザにアドバイスを提供する

ベンダ

- 製品にかかわるセキュリティ対応チーム

脆弱性報告への対応を日常的に実施している人

運用コンセプト


対応の必要な
脆弱性
CERT/CC
World／Vulnerability
FACT
JPCERT/CC
他の外部情報源
LAPTデータ
Constituency
FACT
サイト固有の
モデル
決定の提示
サイトによる
入力
決定の調整

構成要素

意思決定の内容： タスク

脆弱性の記述： FACT（事実関係）

製品の利用： LAPT

意思決定のコード化： 意思決定モデル

タスク

組織が行わなければならないことの意思決定

VRDA ユーザごとに固有

タスクの例

- 勧告の公開
- パッチプロセスの開始
- 回避策の実施
- 無視（優先度の低い脆弱性に労力を割かない）

FACT

脆弱性およびその環境の特性

入手可能な情報に基づく主張

- Vulnerability（脆弱性）FACT–固有の技術的な属性
- World（ワールド）FACT–環境について
- Constituency（サービス対象）FACT–VRDA ユーザの組織に固有

正確性、完全性、粒度、コストのバランス

LAPT

Lightweight Affected Product Tags

課題：Constituency FACT は他から与えられるものではない

LAPT は、脆弱性の影響を受ける製品を明らかにする

Constituency FACT の参照を円滑化

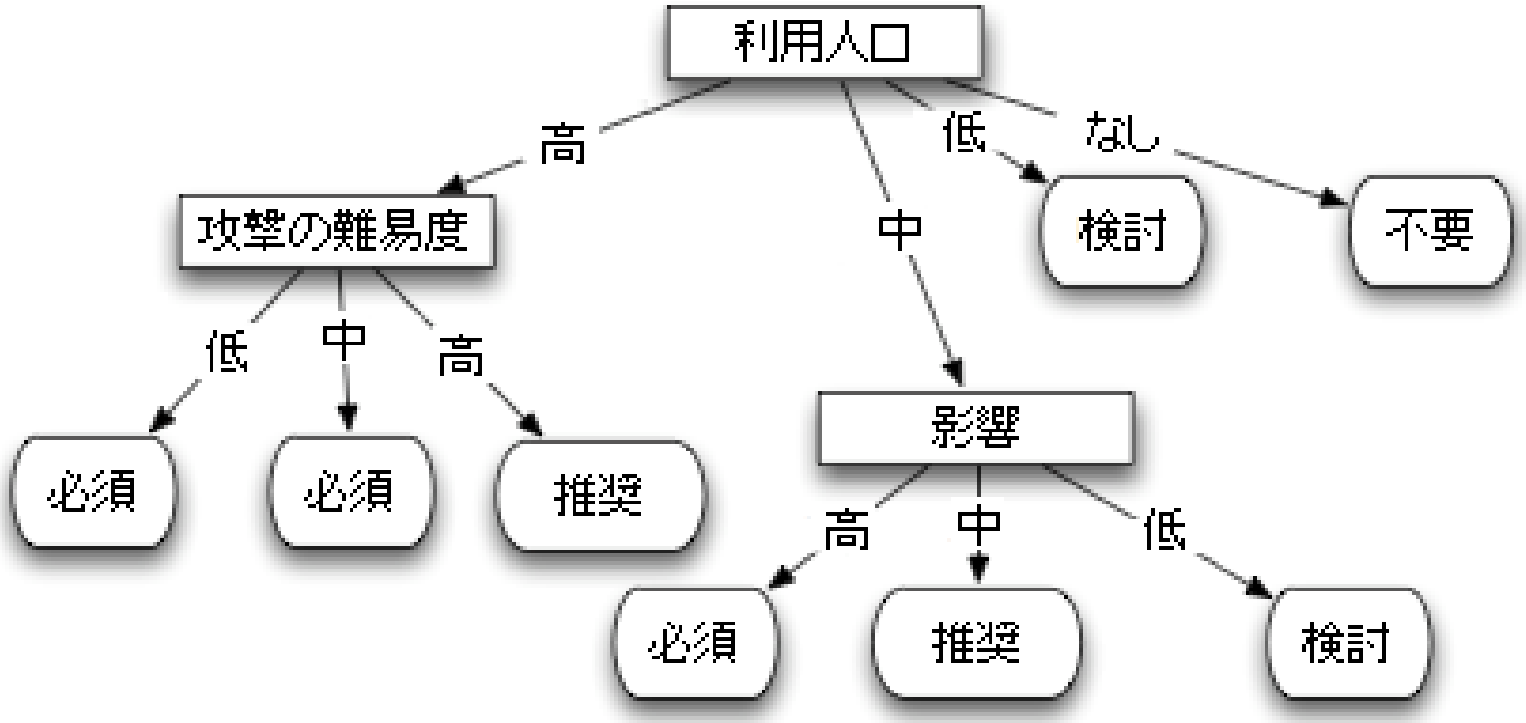
- 外部フィードが各脆弱性の LAPT を提供
- 自組織のデータベースと照合

意思決定モデル

個人の意思決定行為を表現する

組織の価値観を反映するエキスパートシステム

ディシジョンツリー



意思決定モデル(2)

ディシジョンツリーを選ぶ理由

- 確認しやすい、理解しやすい
- 手作業で作成と調整が可能

モデルの作成

- 経験に基づいて最初のモデルを設計
- 記録されたデータに基づいて経験的モデルを作成

関連研究

構造化された脆弱性記述

- CVSS（Common Vulnerability Scoring System）
- OSVDB（Open Source Vulnerability Database）
- OVAL（Open Vulnerability and Assessment Language）

アドバイザリ交換形式

- CAIF（Common Announcement Interchange Format）
- EISPP Common Advisory Format Description
- DAF（Deutsches Advisory Format）
- VULDEF（VULnerability Data publication and Exchange Format）

システム情報

- CMSI（Common Model of System Information）
- CPE（Common Product Enumeration）

関連研究(2)

深刻度の評価基準

- CVSS(Common Vulnerability Scoring System)

SCAP(Security Content Automation Protocol)

- NIST(米国国立標準技術研究所)、MITRE
- 脆弱性管理標準およびコンプライアンス標準のセット(CVE、CCE、CPE、CVSS、XCCDF、OVAL)

KENGINE における VRDA の使用

KENGINE

VRDA の実装は、JPCERT/CC が開発

- オープンソースとする予定

KENGINE は、一貫性のある分析と推論処理を提供

KENGINE のその他の機能

- タスク 管理
- LAPT 管理
- ディシジョンツリー管理
- レポート

KENGINE

最小限のリソースで最大限の数の脆弱性を取り扱う

導入

ユーザ組織からの聞き取り

- 考えられるすべてのタスクを特定する
  - タスクの依存関係を明らかにする
  - 選択肢のない必須または条件付きの活動はタスクではない
- FACT を明らかにする
  - タスクに関する意思決定に必要な事実関係のみを選択する

意思決定モデルを作成する

- サンプリングした VRDA データを使用し、適切なタスクを選択することでシステムに学習/鍛錬させる
- ディシジョンツリーを手作業で作成または修正する

使用法

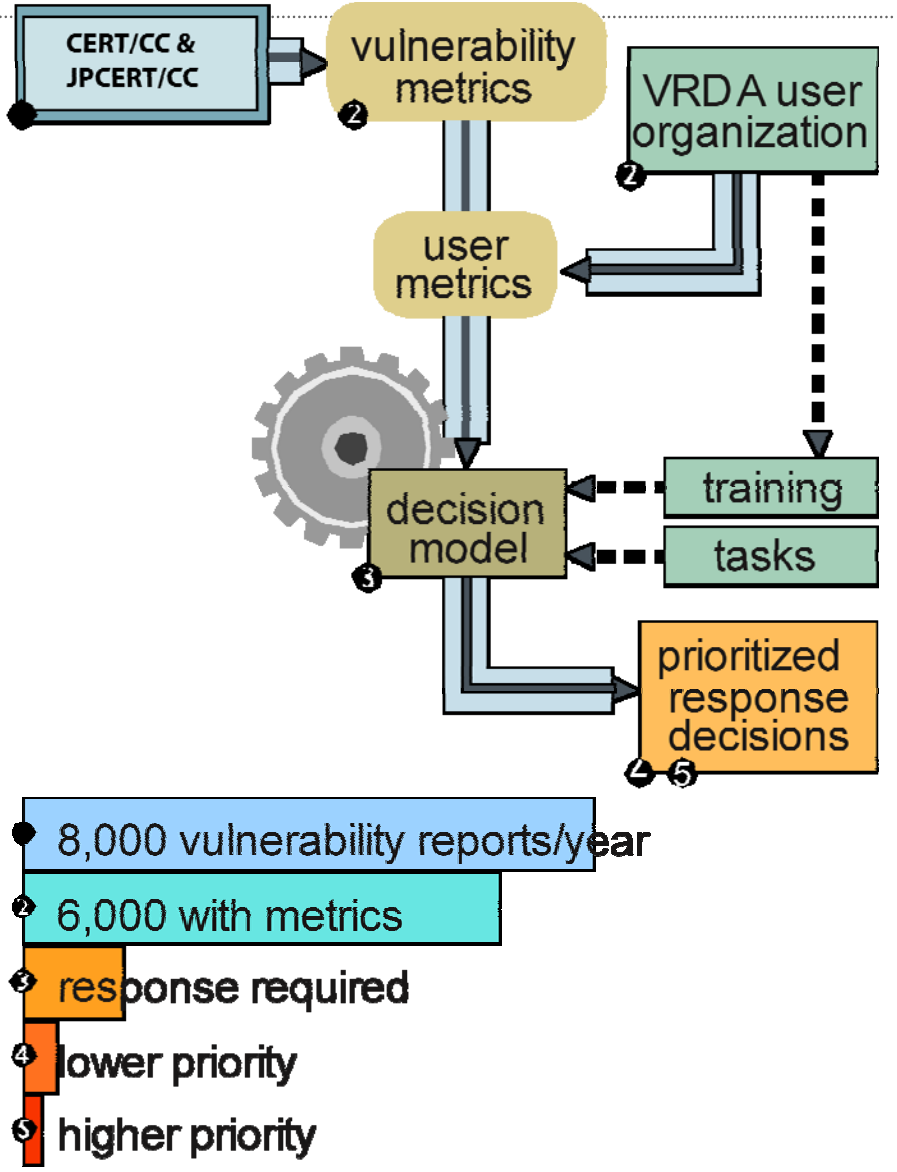
CERT/CC、JPCERT/CC は、Vulnerability FACT を公開（評価基準）

ユーザはタスクを明らかにし、意思決定モデルを作成し、ユーザ固有の事実関係を提供（評価基準）

KENGINE は、優先順位付けされた対応を提示

VRDA の判断を実際の対応と比較し、必要に応じて意思決定モデルを調整

3 つのスライドに示す図において各部を強調



使用法

VRDA データの入手または作成

- CERT/CC および JPCERT/CC は、FACT のフィードを公開

組織固有の FACT のスコア設定

脆弱性報告の処理

- 意思決定モデルを使用する
- 実際の決定を記録する

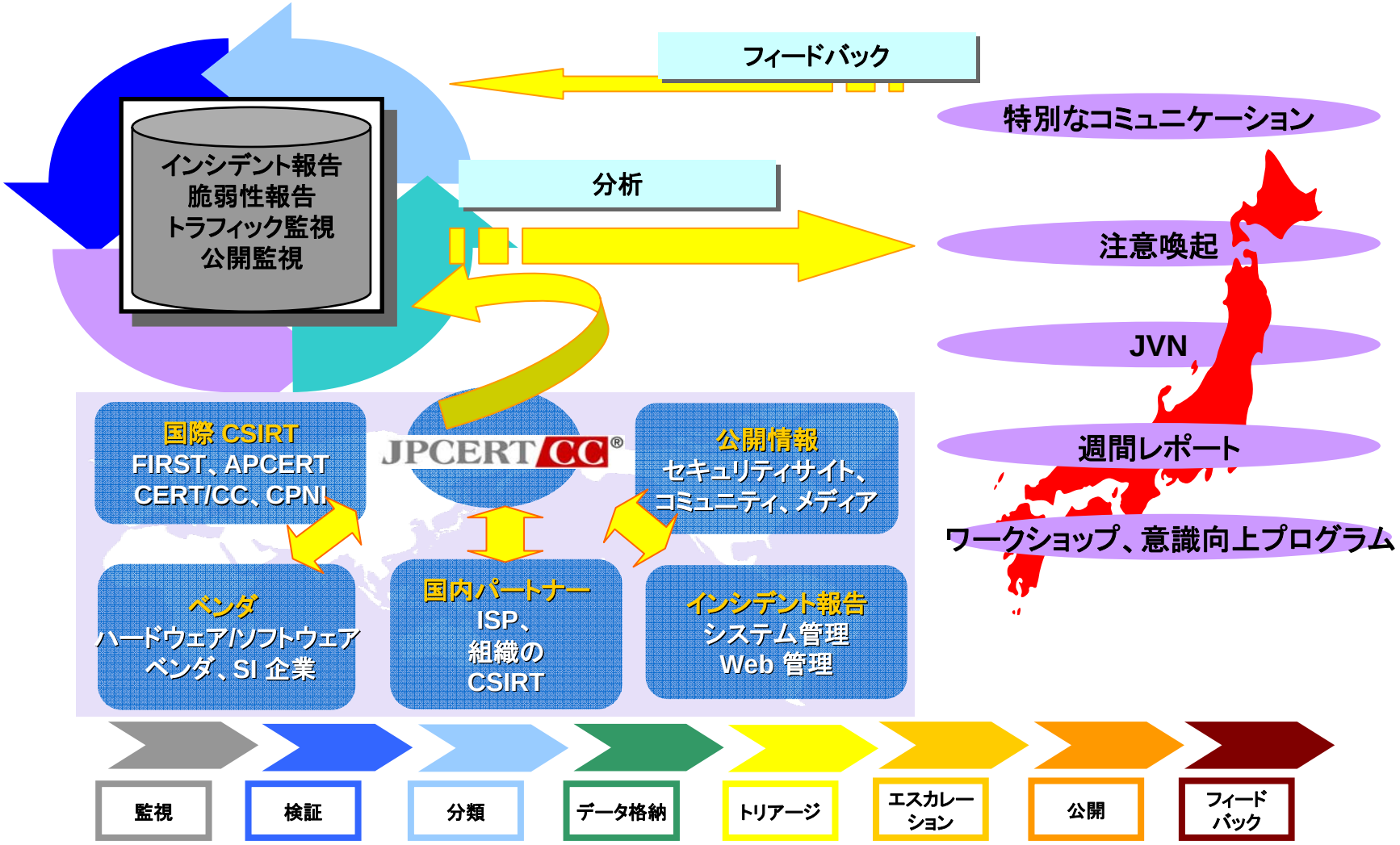
フィードバック

提示された決定と実際の決定を比較する

意思決定のプロセスを調整する

- 意思決定モデルを更新する
- FACT が欠落していたり不正確である可能性
- タスクが欠落している可能性

JPCERT/CC の運営

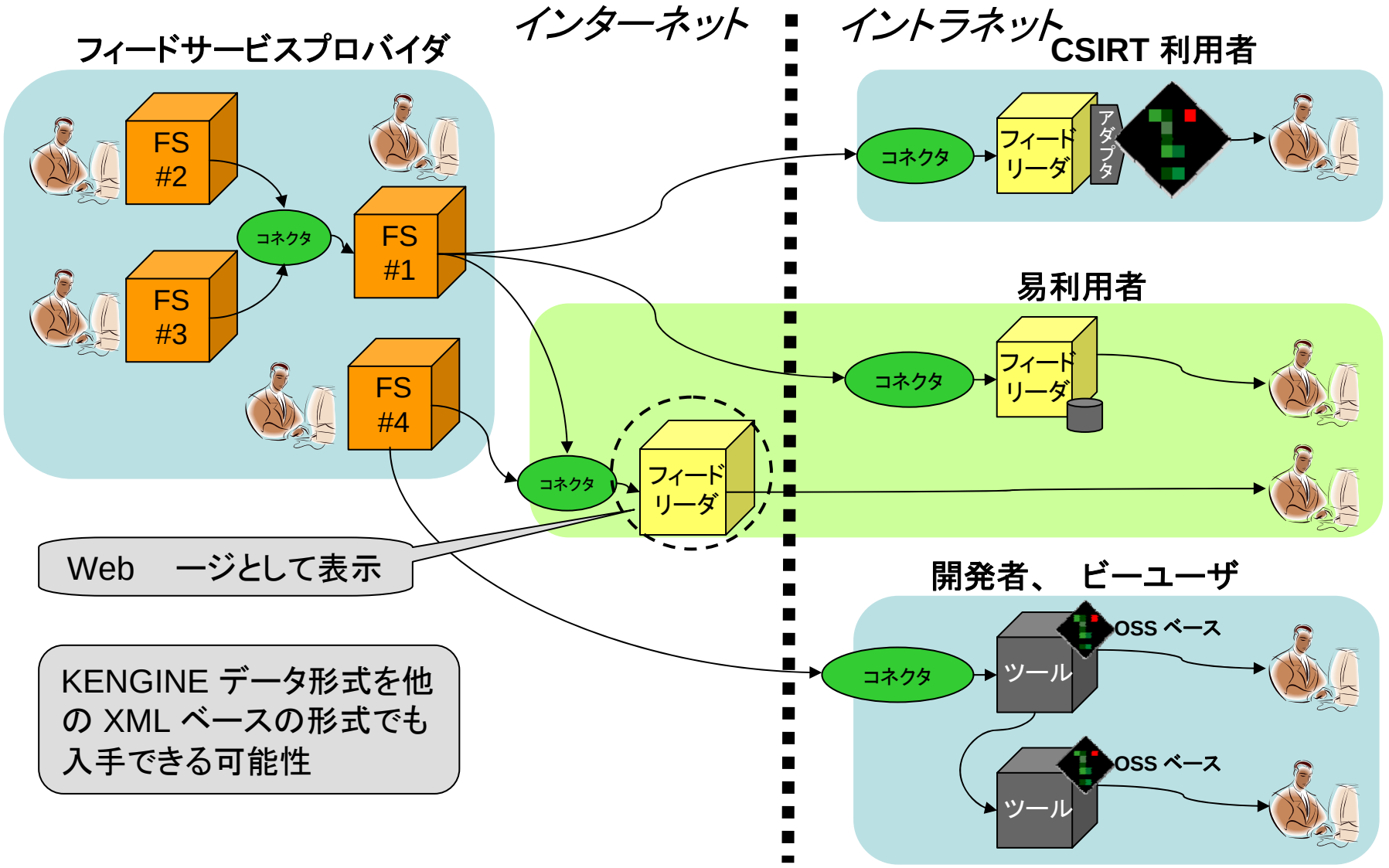


JPCERT/CC 提供の FACT

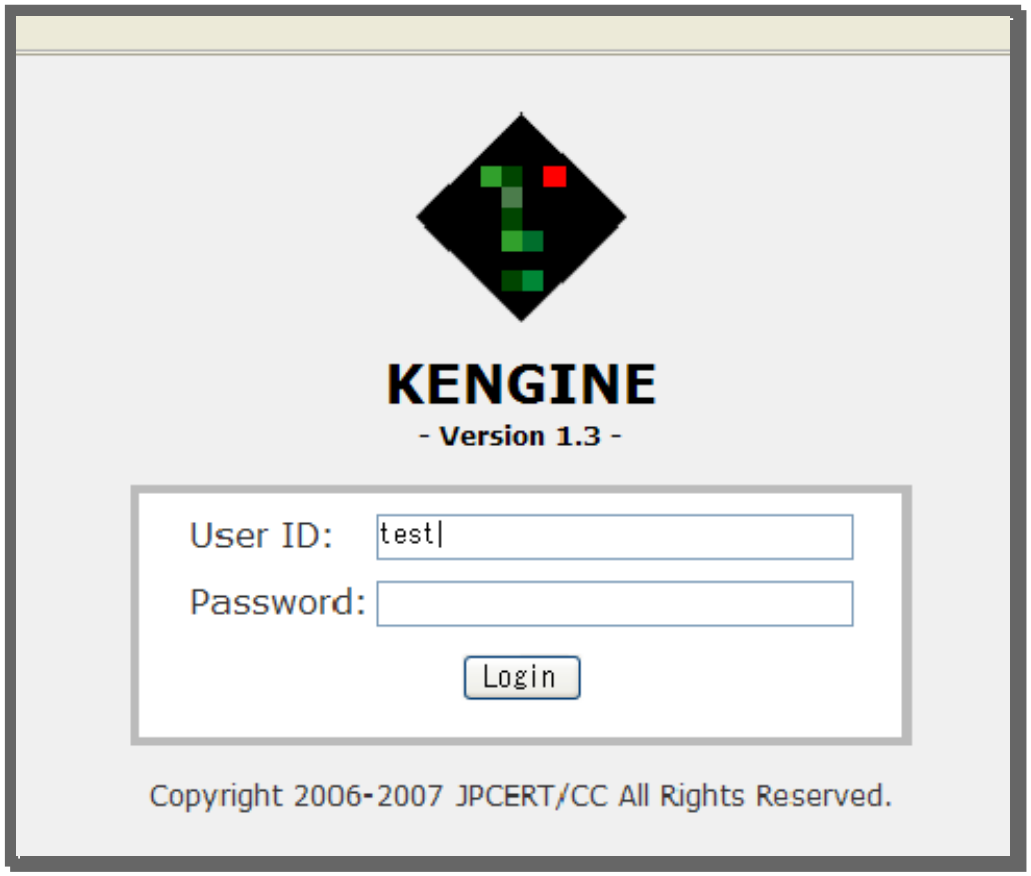
影響
日本におけるシステムの重要性
日本におけるシステムの利用人口数
重要インフラストラクチャでの利用
インターネットインフラストラクチャに対する影響
アクセスの要件
攻撃の難易度
インシデント/攻撃活動
情報の入手のしやすさ（公開または非公開の報告）
情報源の信頼性
対策の有無（パッチ/対応策）
JPCERT での利用

Constituency FACT
Vulnerability FACT
World FACT

フィードの運営


インターネット
イントラネット
フィードサービスプロバイダ
CSIRT 利用者
FS #2
FS #3
FS #1
FS #4
コネクタ
フィード リーダ
アダプタ
易利用者
開発者、 ビーユーザ
ツール
OSS ベース
Web ージとして表示
KENGINE データ形式を他の XML ベースの形式でも入手できる可能性

KENGINE


KENGINE
- Version 1.3 -
User ID:
test
Password:
Login
Copyright 2006-2007 JPCERT/CC All Rights Reserved.

脆弱性報告

Report ID	Title	Priority [8]	Status	Assign	Task			Created Updated
					Analyze	Security_Alert	Sharing	
JVN#00000023	MS Updates for Multiple Vuls	1	Pending Close (D2)	admin admin	Yes Final	Notify Final	Yes Final	'07/08/14 '07/08/14
JVN#00000029	MS Updates for Multiple Vuls	1	Proposal Req'd (Detailed)	admin admin	Yes Computed	Notify Computed	No Computed	'07/08/14 '07/08/14
JVN#00000013	Sourcefire Snort DCE/RPC Preproce...	1	Pending Close (D2)	admin admin	Yes Final	Refer Final	No Final	'07/06/14 '07/08/14
JVN#00000028	MS SQL Vulnerability	1	Proposal Req'd (Surface)	admin None	Yes Computed	Alert Computed	No Data Computed	'07/08/14 '07/08/14
JVN#00000021	Abobe Acrobat reader	1	Decision Req'd (Surface)	None None	Yes Computed	Refer Proposed	No Data Computed	'07/07/14 '07/08/14
JVN#00000025	GnuPG Vulnerability	1	Detailed Analysis Req'd	admin admin	Yes Computed	Notify Computed	No Data Computed	'07/08/14 '07/08/14

脆弱性報告の詳

** General Information ** Edit

Report ID	: JVN#00000023		
Title	: MS Updates for Multiple Vuls		
Memo	:		
Status	: Pending Close (D2)		
Created	: 2007/08/14 23:11	**Last Updated**	: 2007/08/14 23:28
Created By	: admin		
Tri Handler	: admin	**Vul Handler**	: admin
Surface Completed	: 2007/08/14 23:12		
Detailed Completed	: 2007/08/14 23:28		
Decision Finalized	: 2007/08/14 23:28		
Report Closed	:		

Hide ** Analysis Information **

- LAPT - Edit

Selected LAPTs

[Microsoft-Excel][Microsoft-InternetExplorer][Microsoft-Windows-Vista][Microsoft-Windows-XP][Microsoft-Word]

- FACT - Edit

Impact)

The impct of the vulnerability is:

None Low ✔ Medium High Unknown

Access_Required)

The type of network and/or physical access required to exploit this vulnerability is:

Routed ✔ Non-routed Local Physical Unknown

Authentication_Required)

What level of authentication does exploiting this vulnerability require?

None Limited ✔ Standard Privileged Unknown

LAPT 管理

Search | Reset

Items per page: 50

Name	Related Reports	FACT		Last Checked	Action
		Organization_Used	Importance		
Adobe-Acrobat	0	Yes	Low	61days	Edit Delete
Adobe-Acrobat-Reader	1	Yes	Medium	61days	Edit Delete
Apache	1	Yes	High	61days	Edit Delete
Apple-MacOS-X	2	Yes	Low	61days	Edit Delete
Apple-QuickTime	2	No	None	61days	Edit Delete
Apple-Safari	1	Yes	Low	61days	Edit Delete
Bind	1	Yes	High	61days	Edit Delete
Cisco-IOS-10	1	Yes	High	61days	Edit Delete
Debian	1	No	None	61days	Edit Delete

タスクワークフロー

Report ID	Task	Decision	Priority [8]	Task Status Not Started | In Progress | Completed	Update	Memo	Details	Last Updated Report Closed	Action
JVN#00000005	Analyze	Yes Final	1	○ ◉ ○					Details Memo
JVN#00000003	Analyze	Yes Final	1	○ ○ ◉					Details Memo
JVN#00000010	Analyze	Yes Final	1	○ ○ ◉					Details Memo
JVN#00000023	Analyze	Yes Final	1	○ ◉ ○					Details Memo
JVN#00000020	Analyze	Yes Computed	1	◉ ○ ○					Details Memo
JVN#00000002	Analyze	Yes Final	1	○ ◉ ○					Details Memo
JVN#00000012	Analyze	Yes Final	1	○ ○ ◉					Details Memo

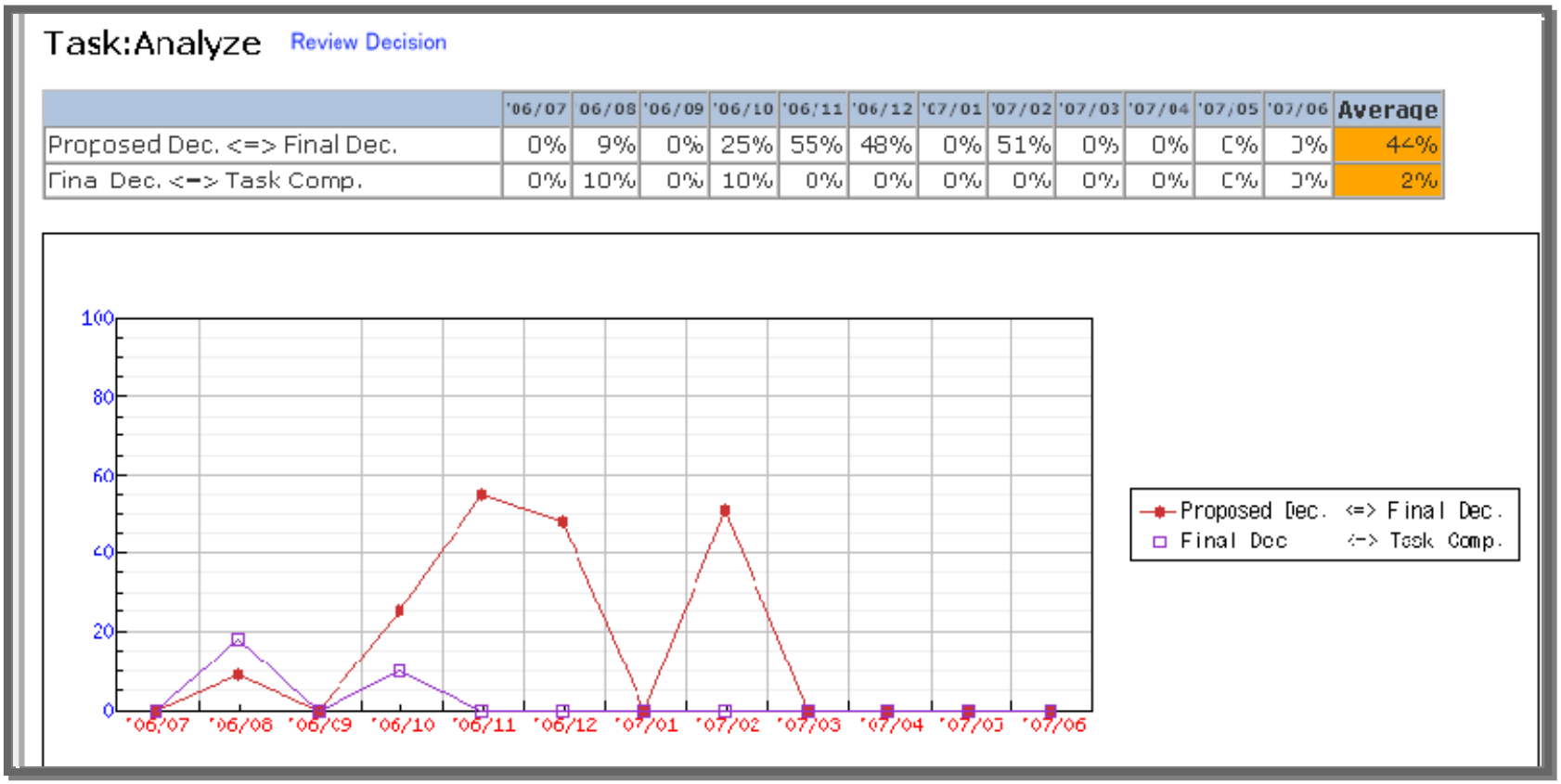
ディシジョンツリー


Name:
Security_Alert
Back
Master :
Tree Tag Name : MASTER-Generated
Comment :
Consider field "Importance"
Unknown -> Consider field "Impact"
Unknown -> Consider field "Required_Actions"
Unknown -> Consider field "Authentication_Required"
Unknown -> "No_Act"
Privileged -> "No_Act"
Standard -> "No_Act"
Limited -> "Refer"
None -> "Notify"
Complex -> "No_Act"
Simple -> "Notify"
High -> "Alert"
Medium -> "Notify"
Low -> "Refer"
None -> "No_Act"
High -> Consider field "Impact"
Unknown -> Consider field "Activity"
Uknown -> "No_Act"

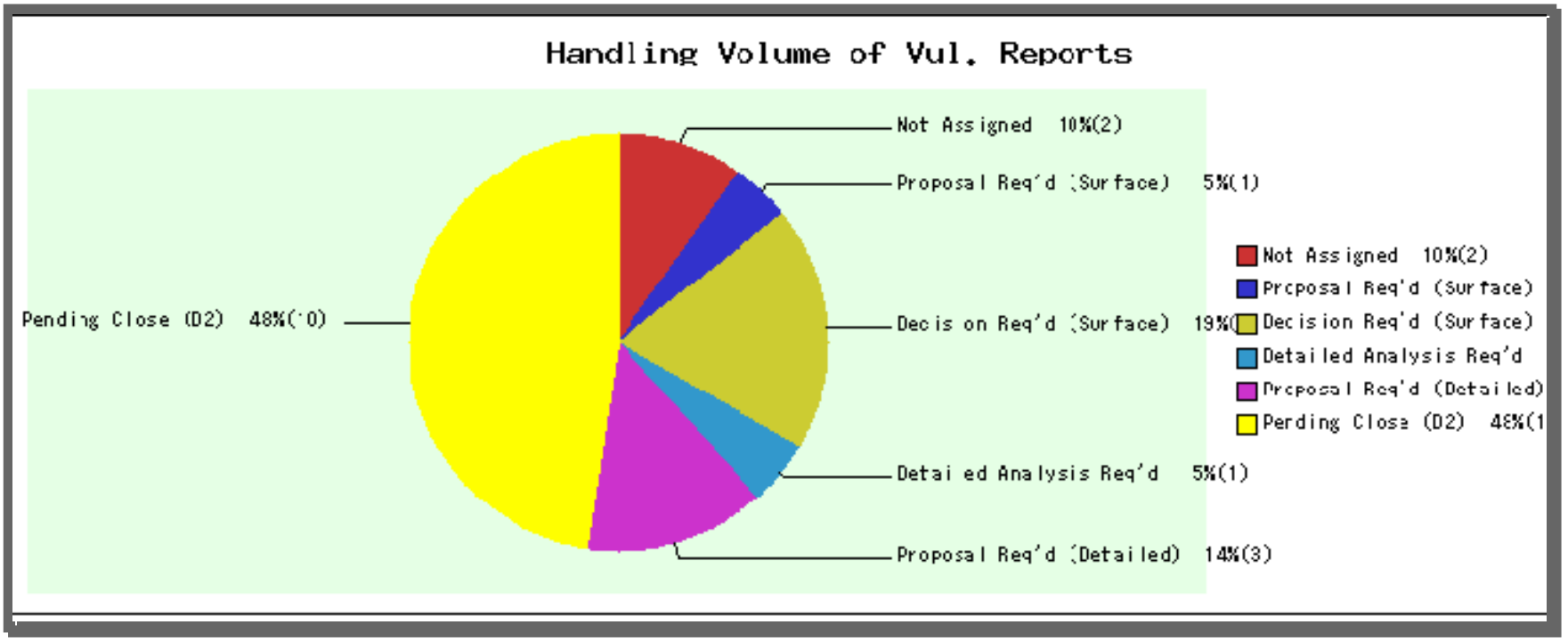
タスク　異レポート

Task:Analyze Review Decision

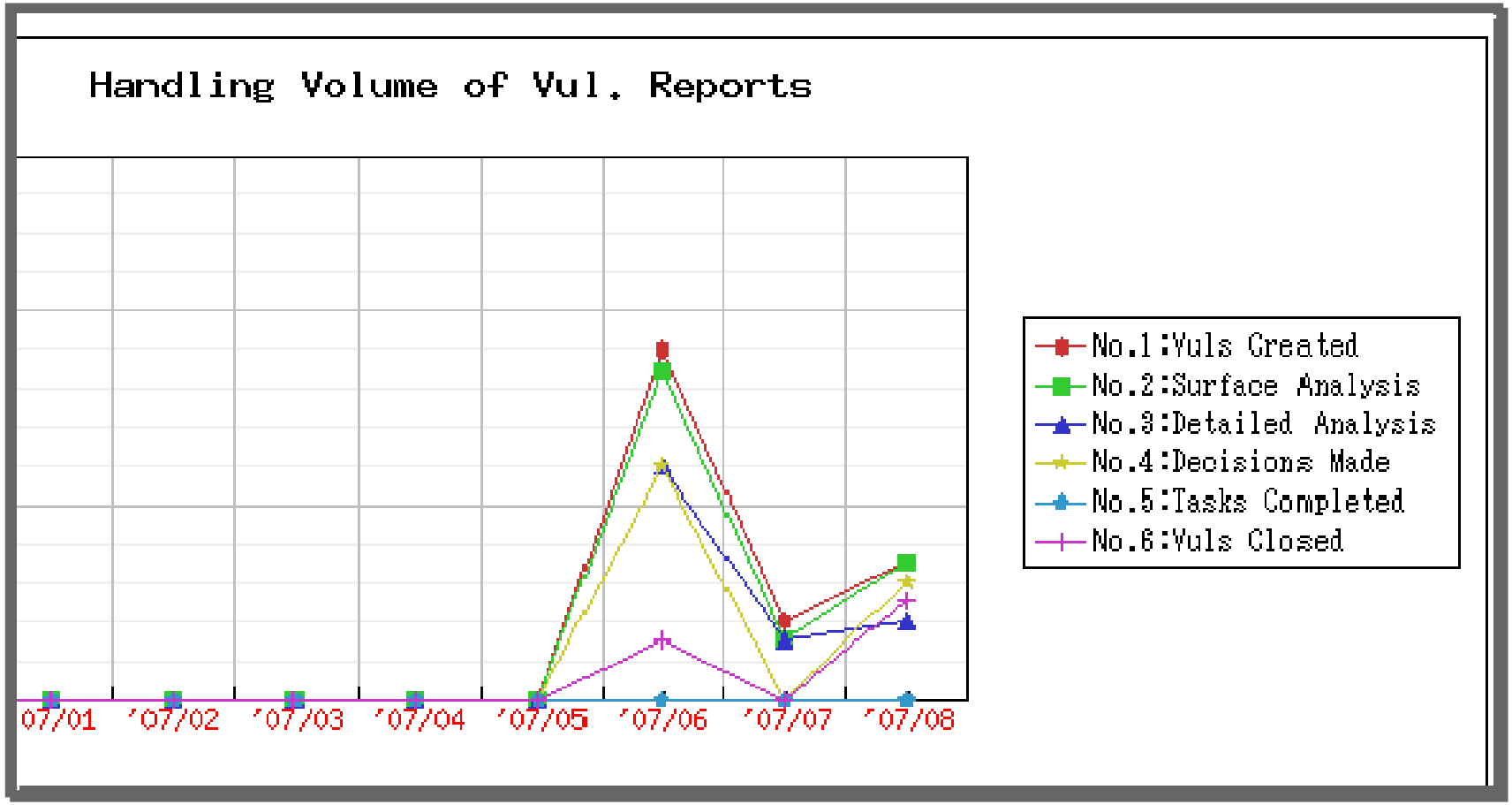
	'06/07	06/08	'06/09	'06/10	'06/11	'06/12	'07/01	'07/02	'07/03	'07/04	'07/05	'07/06	Average
Proposed Dec. <=> Final Dec.	0%	9%	0%	25%	55%	48%	0%	51%	0%	0%	0%	0%	4%
Fina Dec. <-> Task Comp.	0%	10%	0%	10%	0%	0%	0%	0%	0%	0%	0%	0%	2%



レポート


Handling Volume of Vul. Reports
Not Assigned 10%(2)
Proposal Req'd (Surface) 5%(1)
Decision Req'd (Surface) 19%(
Detailed Analysis Req'd 5%(1)
Proposal Req'd (Detailed) 14%(3)
Pending Close (D2) 48%(10)
Not Assigned 10%(2)
Proposal Req'd (Surface)
Decision Req'd (Surface)
Detailed Analysis Req'd
Proposal Req'd (Detailed)
Perding Close (D2) 48%(1

取扱　レポート


Handling Volume of Vul. Reports
07/01
'07/02
'07/03
'07/04
'07/05
'07/06
'07/07
'07/08
No.1:Vuls Created
No.2:Surface Analysis
No.3:Detailed Analysis
No.4:Decisions Made
No.5:Tasks Completed
No.6:Vuls Closed

KENGINE の入手

- JPCERT/CC は、オープンソースとして提供する予定
- 日本語および　語で　　化

JPCERT/CC

- Vulnerability FACT、World FACT を含ん　VRDA データフィードを提供
- パイロットプログラムが　行
- 導入のコンサルティング

CERT/CC

- パイロットプログラムの策定
- ワークフローおよび製品への組み　みを検

お問い合わせはこ　らへ

Art Manion <amanion@cert.org>

Yurie Ito <yito@jpcert.or.jp>