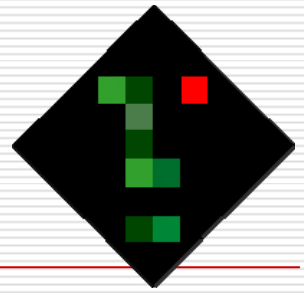
JPCERT CC®

脆弱性マネジメントの効率化を支援する KENGINE™ の紹介



JPCERTコーディネーションセンター

チーフシステムアーキテクト

富樫 一哉

2007年12月12日

アジェンダ

1. VRDAのコンセプト

   VRDA: Vulnerability Response Decision Assistance
2. 脆弱性マネジメントの課題
3. KENGINE™の概要
4. KENGINE™の適用範囲、機能、期待効果
5. KENGINE™の動作環境

はじめに

- どんなツール？
  - 米CERT/CCとJPCERT/CCが共同で開発した脆弱性マネジメントの新しいコンセプトである VRDA（Vulnerability Response Decision Assistance）を実装したWebアプリケーション
  - 一種のエキスパートシステム
  - 脆弱性対応業務における意思決定プロセスを主に支援
- 誰のために作られた？
  - 米CERT/CCやJPCERT/CCをはじめとする脆弱性情報の調整機関
  - IT資産を守るために脆弱性への対応業務を行う人たち
- ゴールは？
  - 組織毎に異なる事情を考慮した脅威分析に基づく適切な対策実施を支援
  - 組織として一貫性のある脆弱性への対応業務の実現とその効率化
  - 担当者の知識・ノウハウを組織へトランスファ

脆弱性への対応業務における意思決定プロセスの一例

- 脆弱性情報を入手、対応（対策アクション）を検討
  - 対応が不要か？
  - 脆弱性のアラートを公開すべきか？
- 考慮する点（判断要素）
  - 利用状況（IT資産の特性） → 数は多くないが組織内で重要な用途で利用
  - インパクト → 情報の改ざんと漏洩の可能性
  - 対策・回避策の有無 → ベンダ公式パッチあり
  - その他様々な判断要素
- 判断（ディシジョン）
  - 無視できない脆弱性である
  - 注意喚起を行いパッチ適用を促す

◆ 特定の「対策アクション」を実施するという「判断」は、「関連性」の強い幾つかの「判断要素」を基に行われる。

◆ また、脆弱性対応において、適切な「判断」を行うためには、組織個別の「IT資産の特性」を把握した上で脅威分析を行う必要がある。

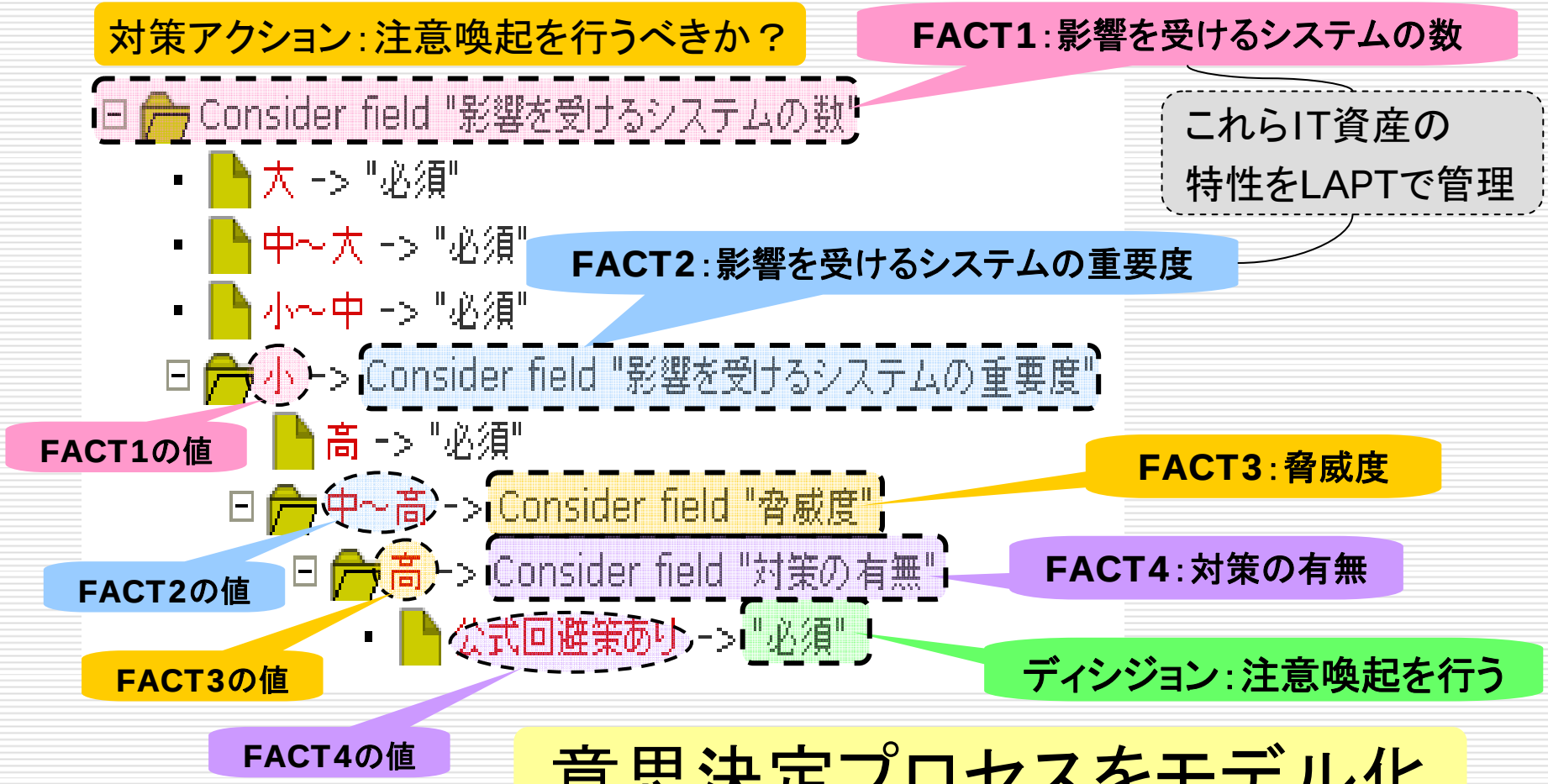
VRDAによる意思決定プロセスのモデル化アプローチ(1/2)

- **V**ulnerability **R**esponse **D**ecision **A**ssistance
- 意思決定プロセスに関係する要素を抽出し、要素間の関係をモデル化
- モデル化に必要な3つのコンポーネントと組織固有の脅威を適切に把握するためのLAPT(Lightweight Affected Product Tag)
  - タスク(対策アクション)
  - FACT(判断要素)
  - 意思決定モデル(対策アクションと判断要素の関連)
  - LAPT(IT資産の特性)

VRDAによる意思決定プロセスのモデル化アプローチ(2/2)

- VRDA意思決定モデルは、ディシジョンツリーで表現される。
- ディシジョンツリーは、確認・理解し易い。
- このディシジョンツリーは、一つのタスク(対策アクション)とFACT(判断要素)の関連である。
- LAPT(IT資産の特性)は、組織固有のFACT(判断要素)を適切に且つ一貫性を持って認識する、IT資産キーワードとIT資産に依存するFACTの関連である。
- LAPTにより脆弱性の対象となるIT資産を特定するだけで、幾つかの判断要素(FACT)が明らかになる。

注意喚起を行うという対策アクションの意思決定プロセスをVRDAのモデルで表現



意思決定プロセスをモデル化

脆弱性マネジメントにおける課題

1. 増え続ける脆弱性に対して迅速な対応が求められるが…
   - 8,000件以上(2006)、増加傾向(1Q, 2007 約2,200件)
   - 全てを調べ、優先順位付けするのも困難

   ニーズ：脆弱性対応業務の効率化を支援する仕組み

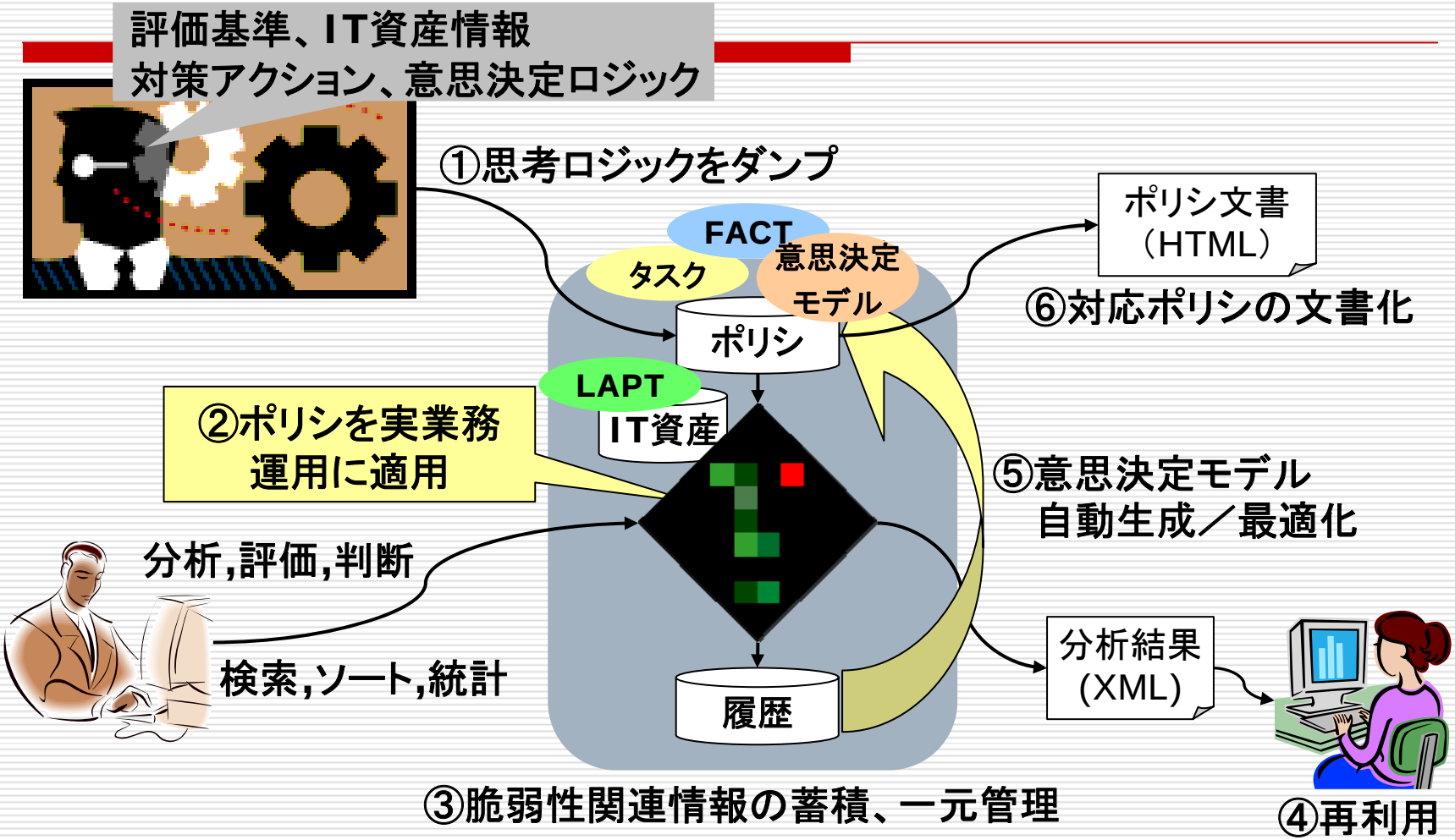
2. 組織的に一貫した分析・判断と適切な対策が求められるが…
   - 個人の経験、知識、偏見に依存するところが大きい現実
   - 個人の経験や知識を共有することが困難

   ニーズ：個人から組織へノウハウ移転、共有、実務へ反映

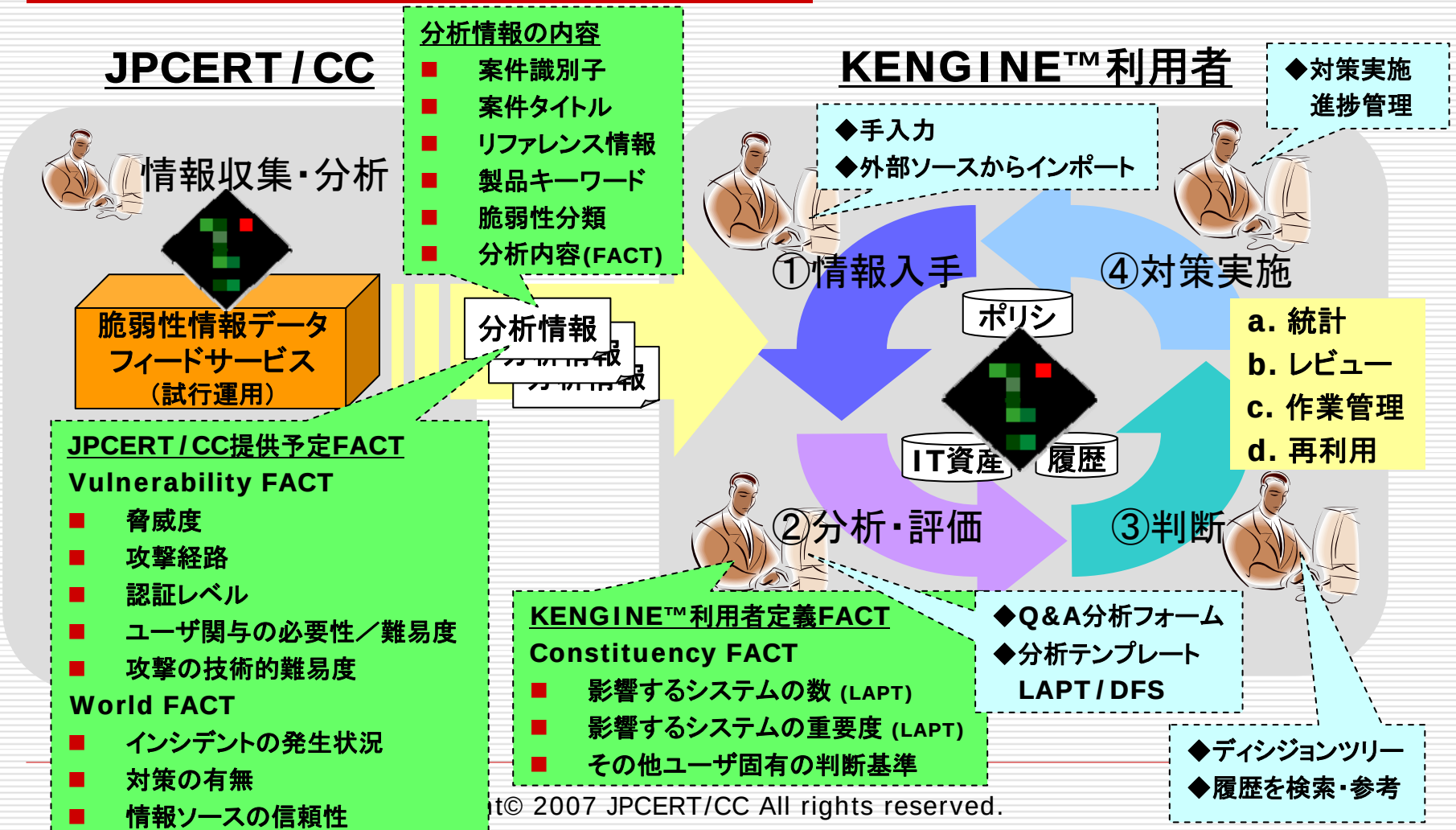
3. 脆弱性の脅威度を計るスコアリングシステムは存在するが…
   - 一般化された脅威度の指標であり、鵜呑みにはできない
   - 自組織にとっての脅威度を再度評価する必要有り

   ニーズ：組織別に異なる脅威度を適切に分析、評価、処置

KENGINE™というソリューション



脆弱性対応業務における KENGINE™の適用範囲と利用イメージ

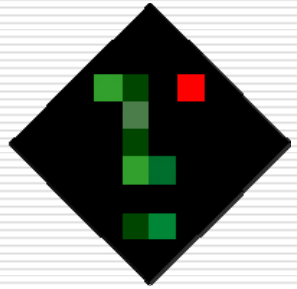


脆弱性対応業務の作業サイクルと KENGINE™の提供機能の対応

① 情報入手	JPCERT/CCが提供する脆弱性情報データフィードサービスなど外部データソースからのインポート、手入力も可能
② 分析・評価	Q&A形式分析フォーム、製品分析テンプレート(LAPT)、自由に定義可能な分析テンプレート(DFS)、脆弱性情報データフィードサービス利用
③ 判断	ディシジョンツリーによる推論、履歴検索・参照
④ 対策実施	対策アクション別進捗状況管理機能
a. 統計	脆弱性の傾向、対応作業状況やボリューム、推論と判断の乖離率などの統計情報
b. レビュー	履歴検索・参照、ポリシ修正、ポリシを文書として出力
c. 作業管理	作業上の役割分担別の権限管理
d. 再利用	XML形式によるデータ入出力インタフェース

KENGINE™機能一覧

1. 脆弱性対応ポリシの管理とドキュメント生成
   - 分析項目（FACT）と分析値（FACT値）の管理
   - 対策アクション（タスク）の管理
   - 意思決定モデル（ディシジョンツリー）の管理
   - 利用される用語（分析項目や分析値の意味など）の管理
2. 意思決定モデルの自動生成（履歴データからのフィードバックにて学習）
3. 外部データソースからの脆弱性分析情報取り込み
4. Q&A形式で定型化された分析フォーム（用語の定義情報も管理可能）
5. 分析支援テンプレート
   - LAPT：簡易的な製品別分析テンプレート
   - DFS：自由に定義可能な分析テンプレート
6. 様々な視点での検索
7. 担当者別の作業進捗管理
8. 各種統計グラフ
9. システム利用者の役割別アカウント管理
10. 他外部システムとの連携用Webサービスインタフェース
11. ユーザインタフェースは日本語と英語をサポート

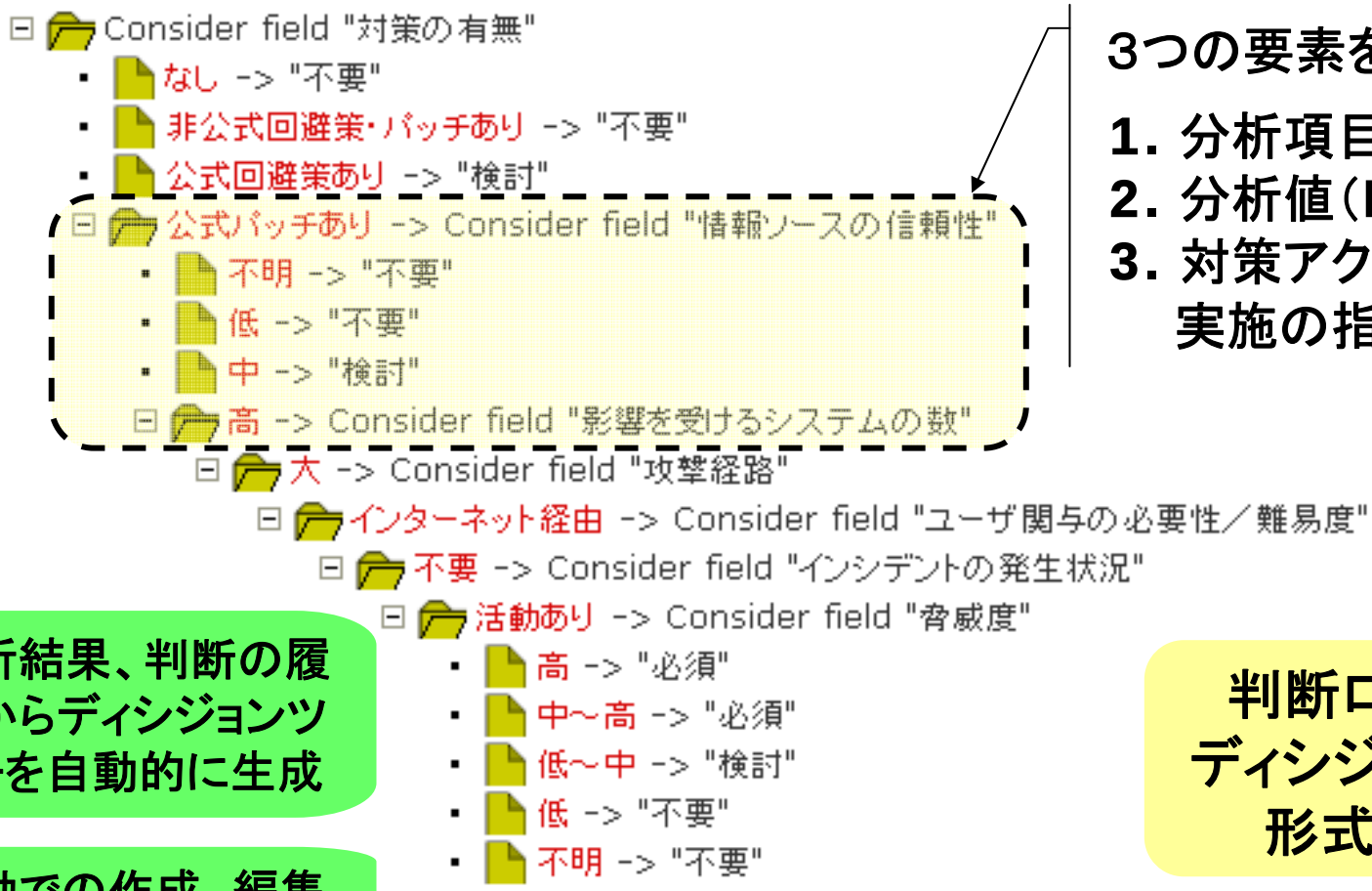


FACT（分析項目／判断要素）管理

FACT名称	グループ-オーダー		質問文	LAPT
	グループ	オーダー		
影響を受けるシステムの数	1	1	この脆弱性が影響するシステムの数は？	はい
影響を受けるシステムの重要度	1	2	この脆弱性が影響するシステムの重要度は？	はい
顧客向けサービスへの影響有無	1	3	この脆弱性は顧客向けサービスを提供するシステムへの影響はありますか？	はい
脅威度	2	1	この製品の脆弱性を狙う攻撃が成功した場合に受ける影響の大きさは？	いいえ
攻撃経路	2	2	この脆弱性を利用するためのアクセス要件（認証は考慮しない）は？	
認証レベル	2	3	この脆弱性を利用するために必要なアカウントの権限要件は？	
ユーザ関与の必要性／難易度	2	4	この脆弱性を利用するために付加的に必要な人的アクションの複雑さは？	
攻撃の技術的難易度	2	5	この脆弱性を利用した攻撃を遂行するために必要な技術的な難易度は？	いいえ
インシデントの発生状況	2	6	この脆弱性についてのPOC・エクスプロイトコードの有無も考慮したインシデントの発生状況は？	いいえ
対策の有無	2	7	この脆弱性についての対策は存在しますか？	いいえ
情報ソースの信頼性	2	8	この脆弱性についての情報ソースの信頼性は？	いいえ

自由にディシジョンを行うための判断要素（分析項目と分析値）を定義

意思決定モデル（ディシジョンツリー）



3つの要素をマッピング

1. 分析項目（FACT）
2. 分析値（FACT値）
3. 対策アクション（タスク）実施の指針

分析結果、判断の履歴からディシジョンツリーを自動的に生成

手動での作成、編集

判断ロジックをディシジョンツリー形式で管理

脆弱性対応ポリシドキュメント生成

JPCERT/CC 脆弱性情報ハンドリングポリシ Ver 1.0

組織名：有限責任中間法人 JPCERTコーディネーションセンター

INDEX

定義されたタスク、FACT、ディシジョンツリー、LAPT情報などの管理情報をまとめてHTML形式で出力

ポリシの履歴管理

ポリシの共有

ポリシの見直し

脆弱性情報データフィードサービス
分析情報の検索・一覧

脆弱性の分析情報の一覧を検索・取得、KENGINE™へ取り込みが可能

脆弱性情報データフィードサービス
特定脆弱性分析情報の表示

脆弱性識別子: JVNVU#433810
タイトル: Apple Mailに任意のコマンドが実行される脆弱性

製品タグ/DFSタグ (更新回数=1):
(黄色は製品タグ、緑色はDFSタグを表しています)

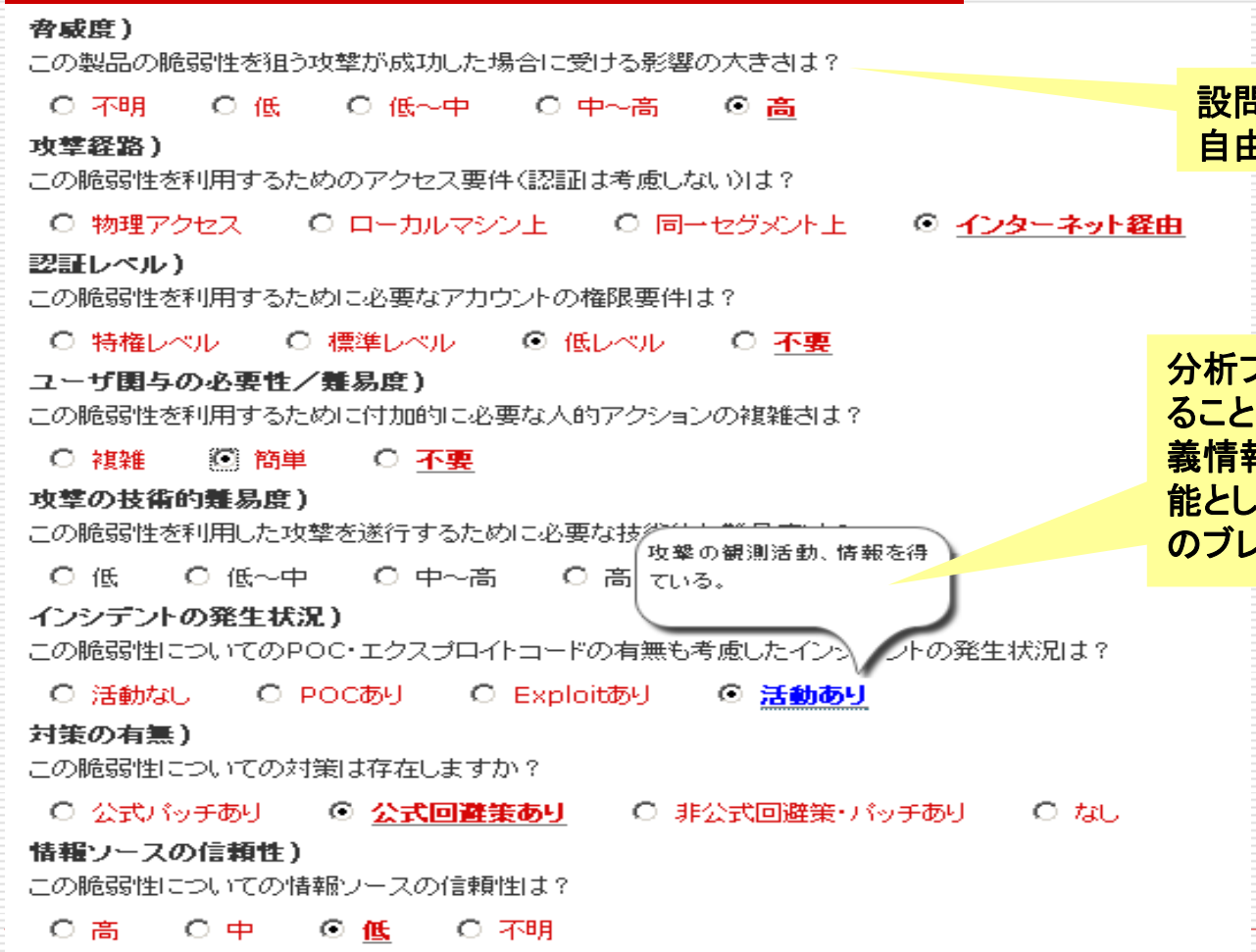
Apple-Mail

分析質問項目/回答 (更新回数=2):

脅威度)			
低	低～中	中～高	✔高
攻撃経路)			
物理アクセス	ローカルマシン上	同一セグメント上	✔インターネット経由
認証レベル)			
特権レベル	標準レベル	低レベル	✔不要
ユーザ関与の必要性／難易度)			
煩雑	簡単	✔不要	
攻撃の技術的難易度)			
低	低～中	中～高	高
インシデントの発生状況)			
活動なし	POCあり	Exploitあり	✔活動あり
対策の有無)			
公式パッチあり	✔公式回避策あり	非公式回避策・パッチあり	なし
情報ソースの信頼性)			
高	中	✔低	不明

分析内容が提供される

Q&A形式で定型化された分析フォーム



設問と回答選択肢を自由に定義可能

分析フォームを定型化することに加えて、用語の定義情報を分析時に参照可能とし、担当者間での分析のブレを最小限に

LAPT：簡易製品別分析テンプレート（簡易的な製品データベース）

組織固有のIT資産の特性を示す項目

Lightweight Affected Product Tag (LAPT)

名称	関連レポート	FACT			最終確認
		影響を受けるシステムの重要度	影響を受けるシステムの数	顧客向けサービスへの影響有無	
Microsoft-Windows	16	高	大	影響あり	0日
Microsoft-Word	8	低～中	大	影響なし	6日
Microsoft-Excel	7	低～中	大	影響なし	4日
CISCO-IOS	6	高	大	影響あり	6日
Microsoft-InternetExpl...	5	低～中	大	影響なし	6日
Justsystem-ichitaro	3	低～中	小	影響なし	32日
Microsoft-PowerPoint	3	低～中	中～大	影響なし	6日
Sendmail	3	高	小～中	影響あり	6日
Apple-Mail	2	低	小	影響なし	4日
Apple-QuickTime	2	低	中～大	影響なし	4日
Microsoft-DNSServer	2	中～高	小	影響あり	6日
Sun-Java_Runtime_Envir...	2	中～高	大	影響なし	6日
lhaplus	2	低～中	中～大	影響なし	6日
Adobe-Acrobat				なし	6日
Adobe-Flash-Player				なし	6日
Apache-HTTPD				あり	4日

製品キーワード別にデフォルトの分析値をアサインして共有

ベンダー情報の管理

キーワード検索: 検索 リセット

1 2 ▶ 1ページ当たりの件数: 50

ベンダー	正式名称	関連レポート	関連LAPT	メモ（ベンダーのポリシ）
Microsoft	Microsoft Corporation.	47	30	http://www.mi...
McAfee	McAfee, Inc.	0	11	http://www.mc...
Adobe	Adobe Systems Incorporated.	2	7	http://www.ad...
Apple	Apple Inc.	4	7	http://www.ap...
CISCO	Cisco Systems, Inc.	6	5	http://www.ci...
Sun	Sun Microsystems, Inc.	4	5	http://www.su...
CA	CA, Inc	0	4	http://ca.com/
IBM	IBM Corporation	1	4	http://www.ib...
GNU	GNU Project	0	3	http://www.gn...
Mozilla	Mozilla Corporation	1	3	http://www.mo...
Symantec	Symantec Corporation	0	3	http://www.sy...

- **LAPT名で利用されるベンダ名を管理**
- **特定のベンダに紐付くLAPT（製品情報）を一覧**

DFS:ユーザ定義分析テンプレート一覧表示

Default Fact Set (DFS)

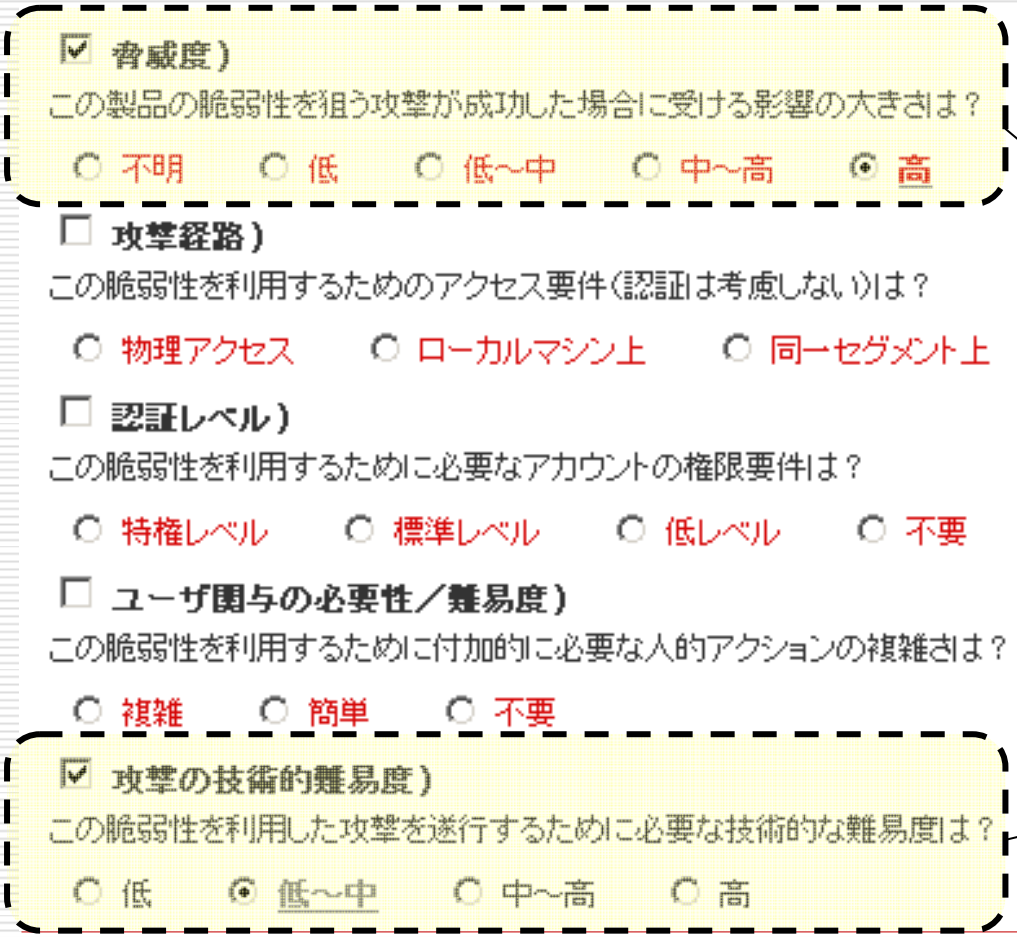
キーワード検索: 検索 リセット

1ページ当たりの件数:

名称	関連レポート	メモ (DFSのポリシ)	最終確認
BOF	2	バッファオーバーフロー	0日
CSRF	0	クロスサイトリクエストフォージェリ	0日
IOF	0	整数オーバーフロー(C/C++)	0日
SQLインジェクション	0		0日
XSS	0	クロスサイトスクリプティング	0日
コマンドインジェクション	1		4日
切り捨てエラー	0		0日
符号エラー	0	主にC/C++	0日

- **DFSはユーザが自由に定義可能な分析テンプレート**
- **この例では脆弱性の分類別に分析テンプレートを活用**
- **特定の分類に関連する脆弱性レポートを一覧可能**

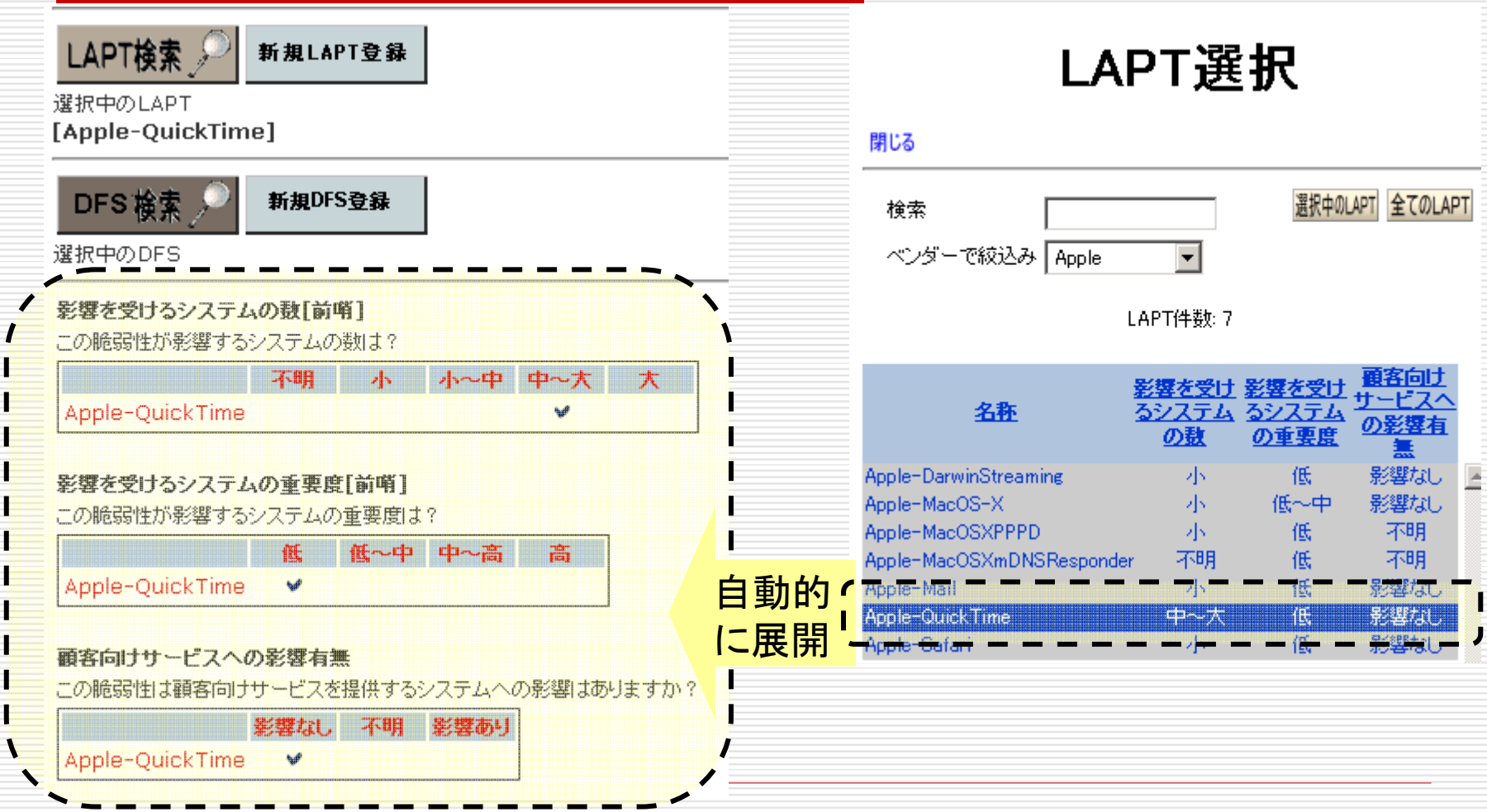
DFS:ユーザ定義分析テンプレート
分析テンプレートの作成



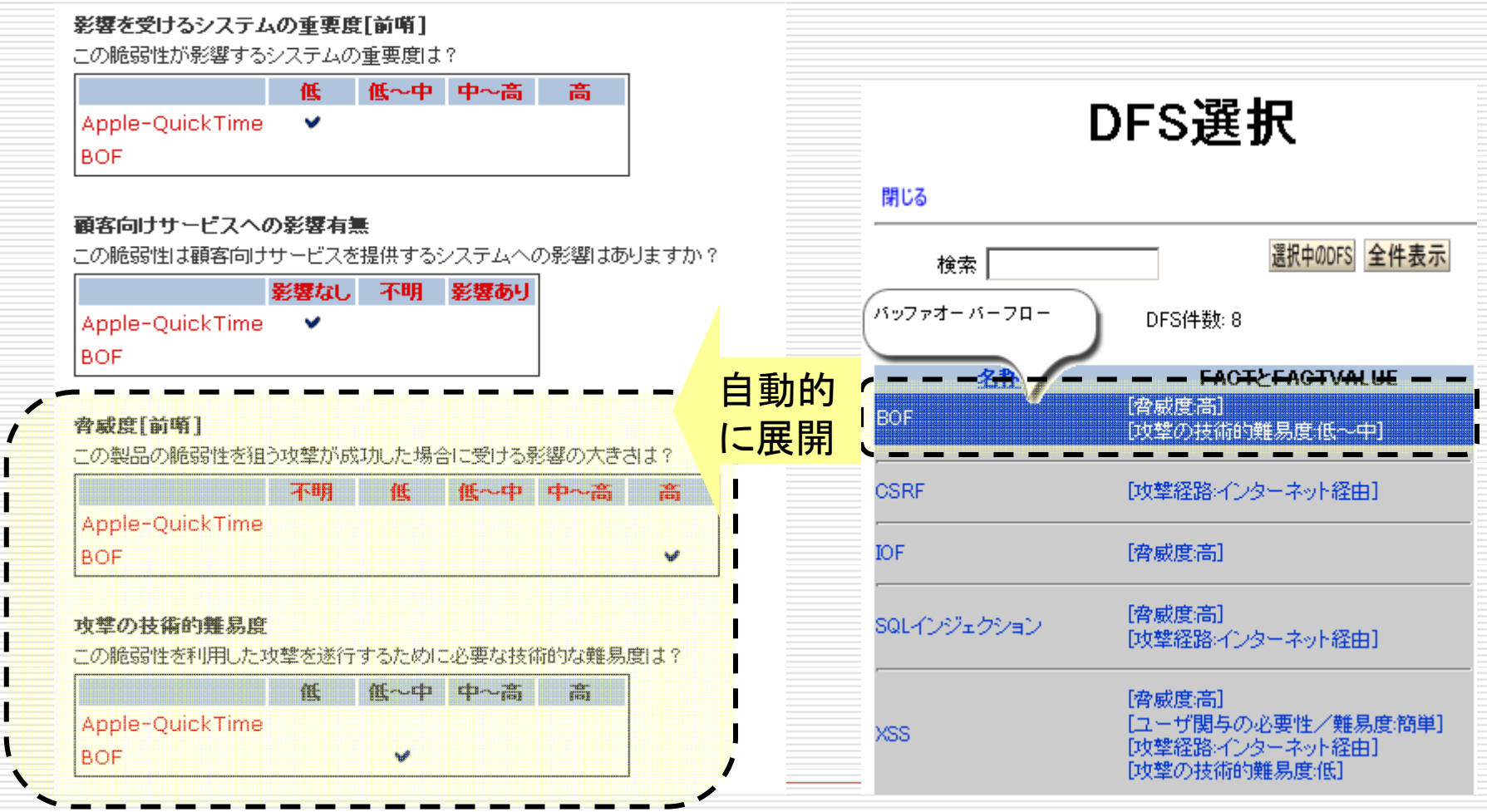
Default Fact Set (DFS)

ユーザが任意の分析項目に任意のデフォルト分析値をテンプレートとして定義可能

LAPTを利用して分析作業の効率化と一貫性確保



DFSを利用して分析作業の効率化と一貫性確保



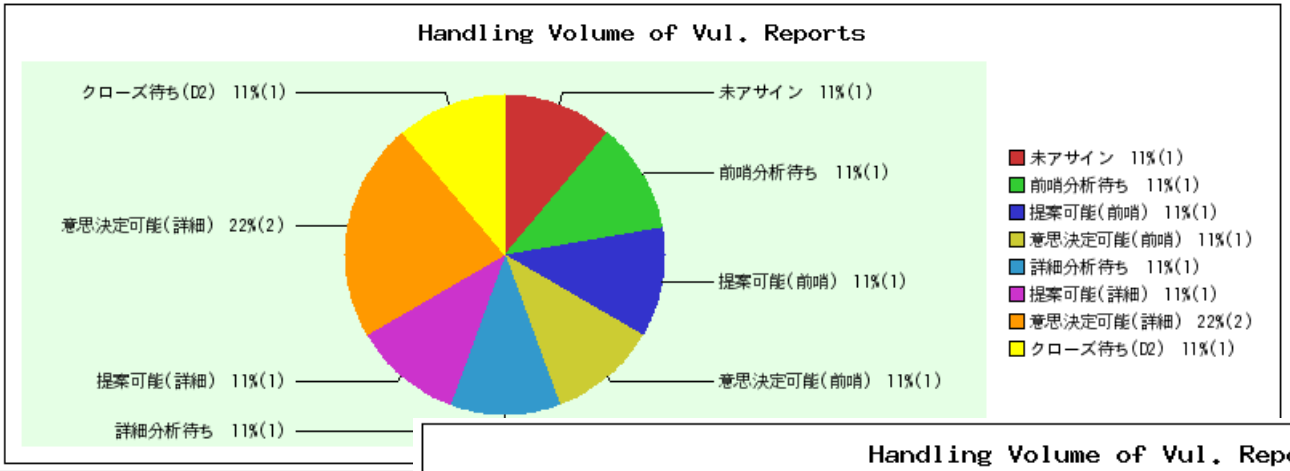
様々な視点での検索

影響を受けるシステムの重要度が高く Microsoft Windows に関するデータを検索

検索条件として、特定のFACT値（分析値）を指定

蓄積された脆弱性情報を、キーワード、LAPT名称、FACT値など様々な条件で検索可能

各種統計グラフ



進捗状況

処理件数

推論と判断のかい離

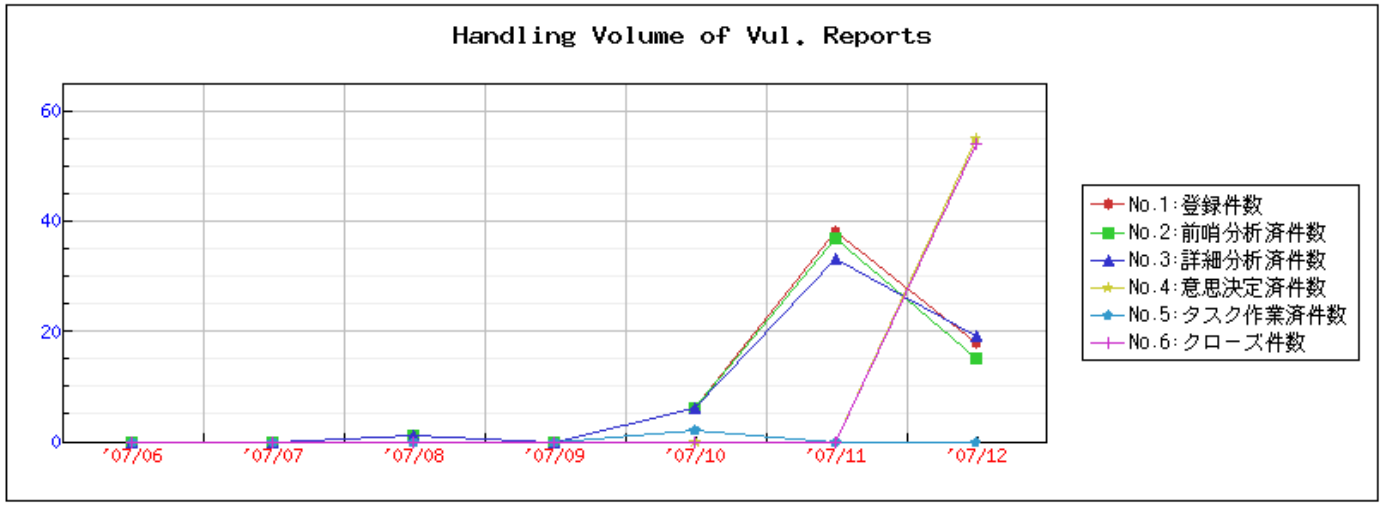
製品別

ベンダー別

脆弱性種類別

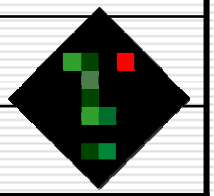
年別、月別

全体、担当者別



システム利用者の役割別アカウント管理

役割	作業内容
システム管理担当	全ての機能を利用可能で、タスク、FACT、ディシジョンツリーなど脆弱性対応ポリシ全体を管理する
LAPT管理担当	LAPT情報の登録・保守を行う
脆弱性情報登録担当	脆弱性情報の登録を行う
脆弱性情報分析担当	登録された脆弱性情報の分析を行う
対応判断担当	分析結果を基に対応を決定する
リソース管理担当	作業担当をアサインする
ビューア	データの参照のみ可能



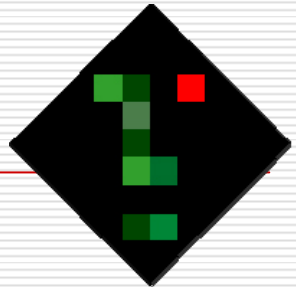
KENGINE™の機能と期待効果のまとめ

期待効果 ＼ KENGINE機能	ポリシ定義/適用	ポリシ文書生成	ツリー編集/生成	脆弱性情報データフィードサービス	Q&A形式分析フォーム	LAPT/DFS分析テンプレート	履歴検索	統計	権限管理
組織への知識トランスファ	✓		✓			✓			
業務の一貫性確保	✓		✓		✓	✓	✓		✓
業務の可視化/最適化	✓	✓	✓					✓	
業務の効率化	✓			✓		✓		✓	
脅威への対策意思決定を支援			✓				✓		
ユーザ個別の事情を考慮した脅威分析	✓		✓		✓	✓			

KENGINE™の動作環境など

- KENGINE™
  - Webアプリケーション
  - Ruby on Rails 1.2 を利用
  - PostgreSQL 8.1 を利用
  - Firefox 2.0、Internet Explore 7.0 など
  - Apache Web Server など
  - Debian Linux など
- 脆弱性情報データフィードサービス
  - Webサービスインタフェース（REST）
  - KENGINE™は同Webサービスのクライアントとして機能
  - データ交換フォーマットはVULDEFをベース

おわりに



- 目的は脆弱性マネジメントの効率化
- ユーザ視点での脅威分析にフォーカスした、VRDA/KENGINE™の新しいアプローチ
  - コンセプトの有効性の実証
  - ソフトウェアとサービスのチューニング
- JPCERT/CCとしても新しい取り組み
  - 新たな活動を推進する体制を整備
- KENGINE™についての問い合わせ・ご意見は
  - Email: kengine@jpcert.or.jp