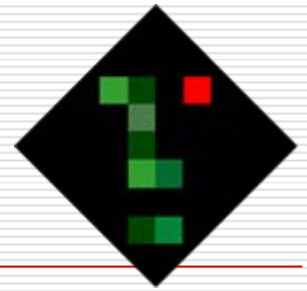
JPCERT CC®

脆弱性情報への対応業務を支援する KENGINEのご紹介



～ Knowledge ENGINEでサクサク判断 ～

有限責任中間法人 JPCERTコーディネーションセンター

水野 哲也、富樫 一哉

2007年7月12日

はじめに

- どんなツール？
  - 脆弱性対応業務における意思決定プロセスを主に支援
  - 一種のエキスパートシステム
- どんなことができる？
  - ノウハウの蓄積・共有、実業務への適用、一貫性の確保
  - 組織毎に柔軟にカスタマイズ、適切な脅威度の把握
- 誰に対してどんな効果が期待できる？
  - 組織、担当者、マネージャ

日常生活は判断の連続

- 今日傘を持って行く？
  - 予報、季節、空模様、荷物の量

  →「今日は折り畳み傘にしよう。」

- 今日のランチは何にする？
  - 天候、体調、メンバー

  →「今日は近くのウナギ屋に行こう。」

脆弱性情報の対応業務も判断の連続

- 脆弱性のアラートを公開する？
  - 利用状況、インパクト、対策・回避策の有無など

  → **注意喚起を出す**

- 脆弱性情報の公開日を調整する？
  - 国内の複数ベンダに影響、未知の脆弱性など

  → **関連ベンダへ通知する**

  → **公開日の調整を開始する**

脆弱性情報の対応業務における課題

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)
   - 増え続ける傾向(1Q, 2007 約2,200件)
   - 全てを詳細に調べる、優先順位付けするのも困難

   ニーズ：脆弱性対応業務を効果的に支援する仕組み

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、鵜呑みにするのは危険
   - 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

① 分析・評価結果を具体的な対策へマッピング
- 組織別に異なる脅威度にマッチした対策を提示

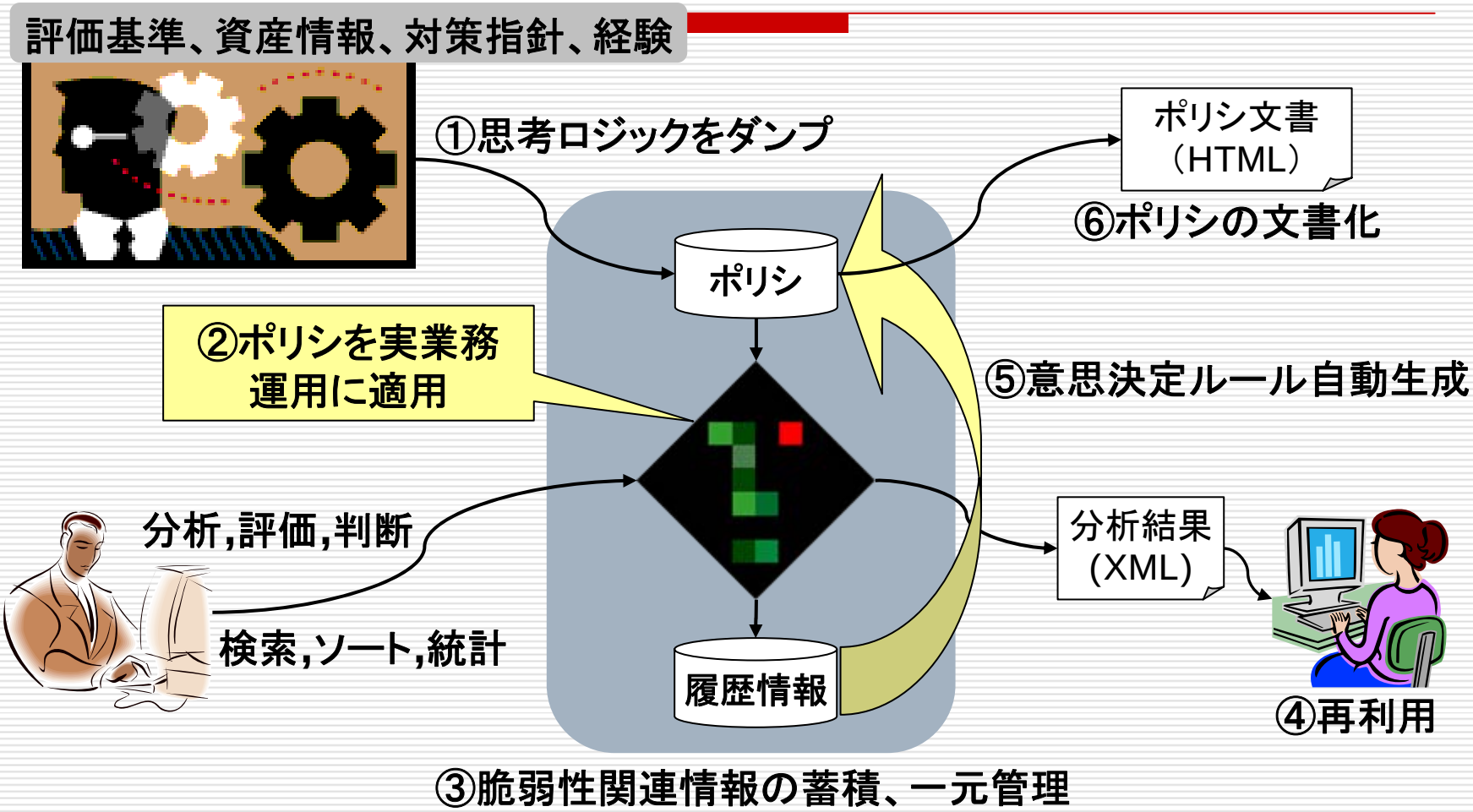
② 脆弱性情報への対応ポリシを動作パラメタとして定義
- 思考ロジック／脆弱性対応ルールをダンプ
- 評価基準、資産、対策アクション、意思決定ルールを定義

③ 組織的に脆弱性情報への対応ポリシを適用
- ポリシ適用と実業務運用の一体化を実現

④ 脆弱性情報を一元管理
- 多様な検索、優先度順位別の一覧表示、統計情報

⑤ 脆弱性の分析情報を定型フォーマットで蓄積
- XML形式でのインポート／エクスポート

絵で見るKENGINというソリューション



KENGINEの守備範囲

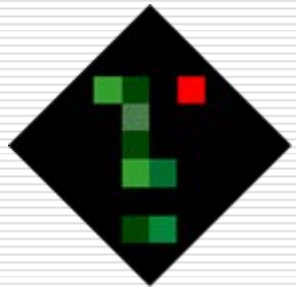
・情報入手		外部データソースからのインポート
・分析・評価		Q&A形式、製品分析テンプレート
・判断		ディシジョンツリーによる推論で支援
・対策実施		(守備範囲外)
・作業管理		対策アクション別進捗状況管理機能
・レビュー		統計情報、履歴検索・参照、ポリシ出力
・再利用		XML形式、データ抽出インタフェース

KENGINEで誰がどう嬉しいのか

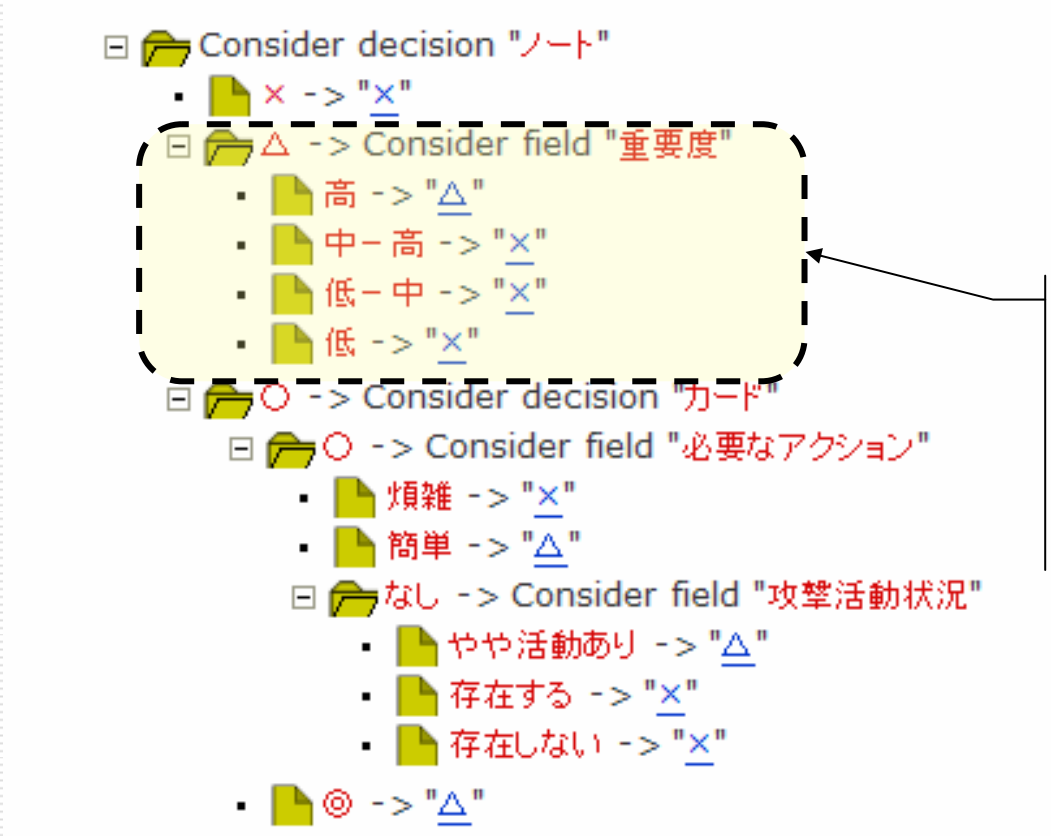
- 組織のメリット　→　**対応業務の品質向上に繋がる**
  - 組織別に異なる事情を考慮し、脅威を適切に把握
  - 分析と適切な対策アクションを一貫性を持って実施
  - 対応業務に関わるノウハウを蓄積・共有（組織への知識トランスファ）
  - ポリシを適宜見直し最適化
- 担当者のメリット　→　**迷うことが少なくなる**
  - 業務プロセスが定型化され迷わず業務に専念
  - 履歴情報から過去の対応を参考
  - 作業の進捗管理ができる
  - 長期休暇も多少安心、引き継ぎも楽
- マネージャのメリット　→　**状況の把握と管理が楽になる**
  - 全体あるいは担当者別の脆弱性情報への対応状況を容易に把握
  - 増員が楽
  - エスカレーションのための情報整理も容易
  - スキルレベルに合ったアカウント、ワークフロー設定が可能

KENGINEの機能概要

1. 脆弱性対応ポリシの定義、ドキュメント生成
   - 分析項目（質問と選択肢形式の回答）
   - 対策アクション
   - 意思決定ルール（ディシジョンツリー）
2. Q&A形式で定型化された分析フォーム
3. 意思決定ルールの自動生成（履歴データからの学習）
4. 簡易的な製品別分析テンプレート（製品DBの類）
5. 様々な視点での検索
6. 担当者別の作業進捗管理
7. 各種統計グラフ
8. ユーザ権限別アカウント管理
9. 多言語対応（日本語、英語）



意思決定ルール（ディシジョンツリー）



判断ロジックを
ディシジョンツリー
形式で管理

3つの要素をマッピング

1. **分析項目**
2. **分析結果**
3. **対策アクション**

Q&A形式で定型化された分析フォーム

アクセス必要性）

この脆弱性を利用し攻撃するために必要とされる、ネットワークや物理的なアクセスのタイプは？

○ インターネット経由　◉ 同一セグメント　○ システムログイン　○ 物理アクセス

ハードウェアに物理的にアクセスする必要がある

認証レベル）

この脆弱性を利用し攻撃するために必要とされる認証は、どの程度のレベルですか？

○ なし　◉ 低レベル　○ 標準レベル　○ 特権レベル

必要なアクション）

もし、この脆弱性を利用した攻撃を実施するためにユーザの関与が必要である場合、ユーザを関与させるのはどの程度難しいでしょうか？

○ なし　○ 簡単　◉ 煩雑

技術的困難さ）

脆弱性を利用するための、アクセス制限及び被害者ユーザの関与条件を除き、脆弱性自体を利用して攻撃を行うための技術的な難しさはどの程度ですか？

○ 低　○ 低−中　○ 中−高　◉ 高

OSに依存する有る特定の処理タイミングで割り込みアドレスを指定する必要がある

簡易的な製品別分析テンプレート（製品DBの類）

名称	関連レポート	FACT			最終確認
		利用規模	重要度	自組織使用製品	
Apache	1	少－中	中－高	はい	490日
Apache-HTTPD	0	中－多	高	はい	64日
Apache-Tomcat	0	少－中	高	はい	64日
Apple-MacOS-X	1	少	低	はい	348日
Apple-Safari	1	少－中	低－中	いいえ	348日
BIND	0	中－多	中－高	いいえ	64日
Chama-Cargo	0	少	低	いいえ	64日
Cicco-IOS-10	1	少	中－高	いいえ	348日
FSecure-SSHD	1	少	中－高	いいえ	427日
FreeBSD	4	少－中	中－高	いいえ	404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

様々な視点での検索

識別子

案件名

分析結果

関連製品名

その他メモなど

フィルタ: 意思決定可能

キーワード検索: Ruby 検索 リセット

FACT値で絞込み: 選択

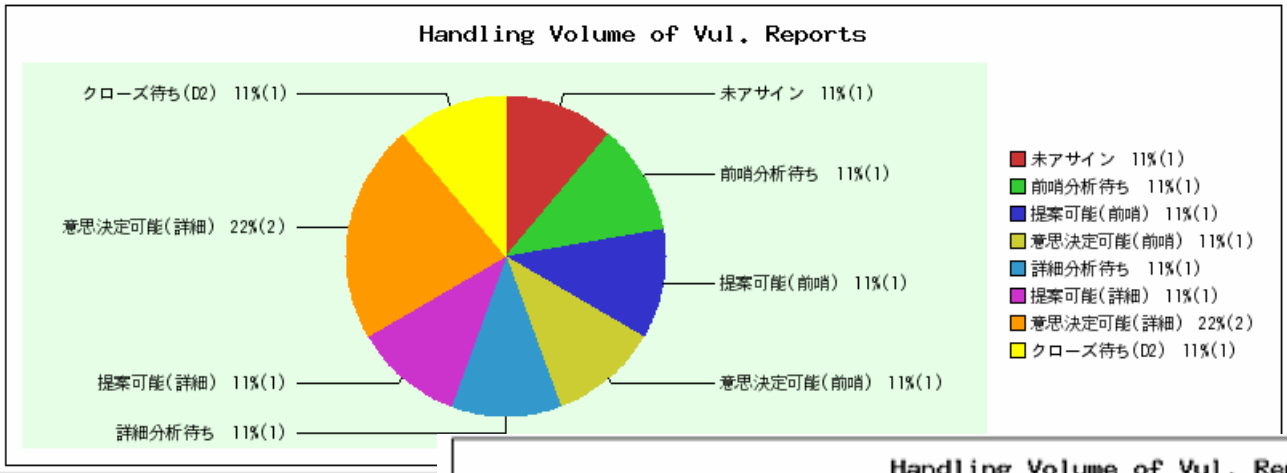
LAPT名称で絞込み: 選択

LAPTキーワードで絞込み: Http

1ページ当たりの件数: 10

レポート識別子	案件名	優先順[28]	状態	担当	タスク							作成日 更新日
					分析	通知	調整	カード	ノート	TA	SA	
JVN#11111111	RubyのAlias機能における脆弱性	1	意思決定可能(詳細)	test05 test06	◎ 決定	△ 決定	△ 決定	△ 決定	△ 承認待ち	× 推論	× 推論	'06/10/12 '06/11/17
JVN#44891144	X Window についての脆弱性(意思決定可能D2)	2	意思決定可能(詳細)	test05 test06	○ 承認待ち	◎ 承認待ち	◎ 承認待ち	◎ 承認待ち	◎ 承認待ち	◎ 承認待ち	◎ 承認待ち	'06/10/18 '07/06/06

各種統計グラフ

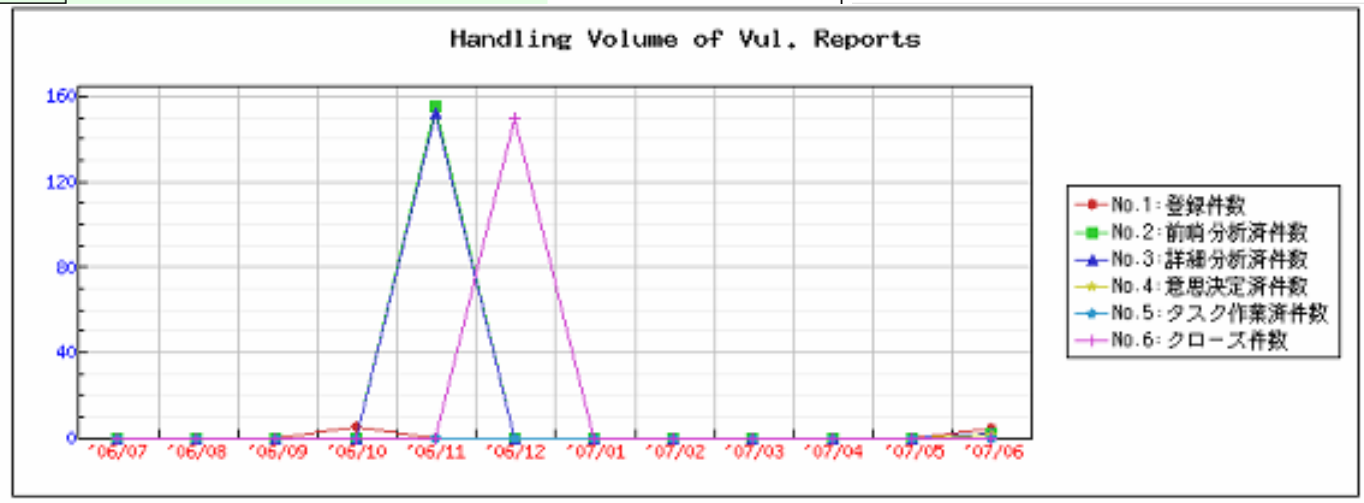


進捗状況

処理件数

関連製品

推論と判断のかい離



年別、月別

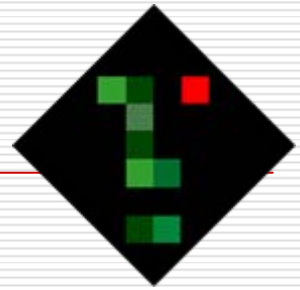
全体、担当者別

製品別

今後のKENGINE

- 2007年7月現在、公開に向けて準備中
  - JPCERT/CC内部で運用中
  - 追加機能の開発中
  - 数社に協力を得てβ版の評価運用中
- 年内に公開予定
  - 無償提供
  - 評価論文

おわりに



- 有限責任中間法人
  JPCERTコーディネーションセンター
  担当: 水野、富樫
  - Email: office@jpcert.or.jp
  - Tel :03-3518-4600
  - Web: http://www.jpcert.or.jp/