サイバーセキュリティ情報の利活用基盤

(独)情報通信研究機構
ネットワークセキュリティ研究所
セキュリティアーキテクチャ研究室

本提案の概略

目的

- サイバーセキュリティ情報の全世界規模での共有・流通
- それらの情報の効果的な活用

提案内容

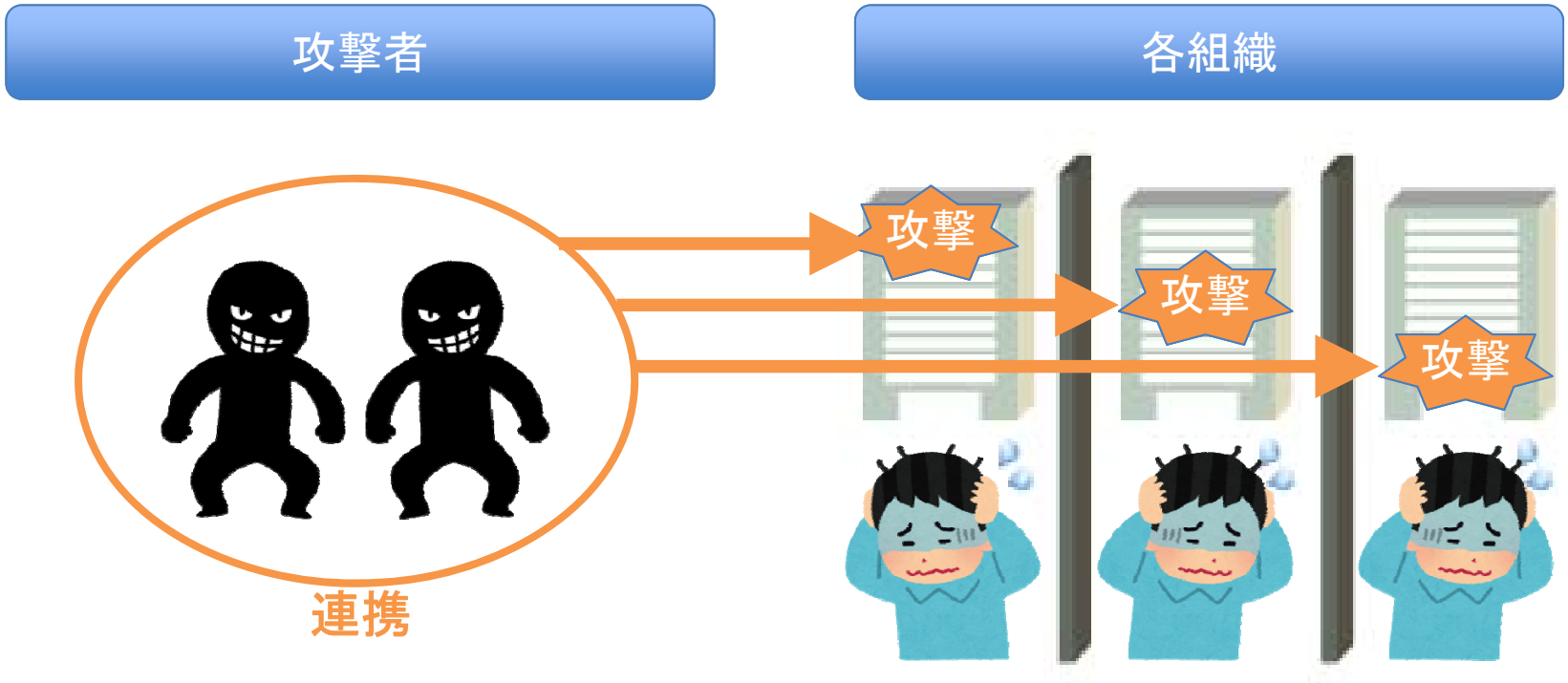
- Web上に散在する多様なサイバーセキュリティ情報に対して統一的な手段でアクセスすることができるアプリケーションを構築
- 本アプリケーションはRDFにて情報を管理し、SPARQLエンドポイントとしての機能を有するなど、二次利用を考慮
- これにより実際のセキュリティオペレーションの自動化を支援

期待する社会へのインパクト

- サイバーセキュリティ情報の共有・流通が加速し、より安心・安全なサイバー社会を構築
- 各組織におけるセキュリティオペレーションの自動化を支援

目次

セキュリティ情報の共有の現状は不十分



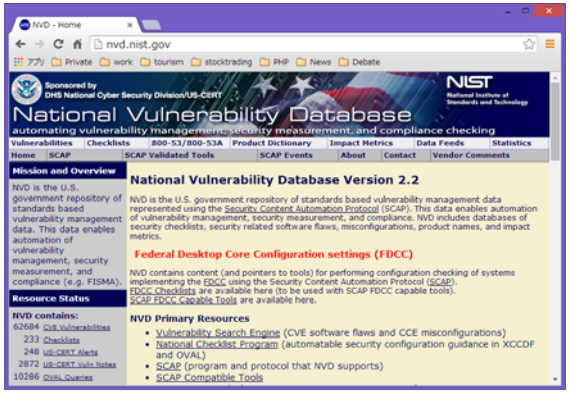
- 攻撃者は連携するが、各組織はバラバラに対応しており、情報共有すらできていない
- 情報共有時も、電話や電子メールなど、非効率な手段が主流であるのが現状

セキュリティ情報のLOD化に向けたアプリが必要

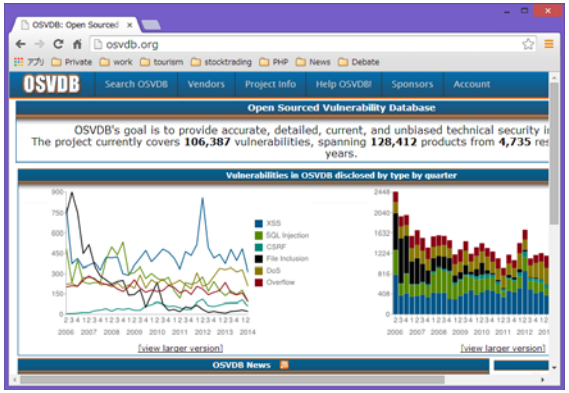
- LODは情報流通を促し、本問題解決の本命の一つ
- 昨今のOpen Dataの流れに従い、セキュリティ情報に関しても各種情報がWebで公開され始めているものの、LODには至らない
  - それらの情報はWeb上の各所に散在
  - RDFなどのLinked Open Dataに即した形で公開されている情報は限定的
- 有用なセキュリティ情報の交換・流通に向けて、それらの情報をLODとして扱うことができ、かつ統一的な手段で効率的にアクセスできるアプリケーションが求められている

【参考】各種セキュリティ情報の主なリポジトリ

National Vulnerability Database (NVD)

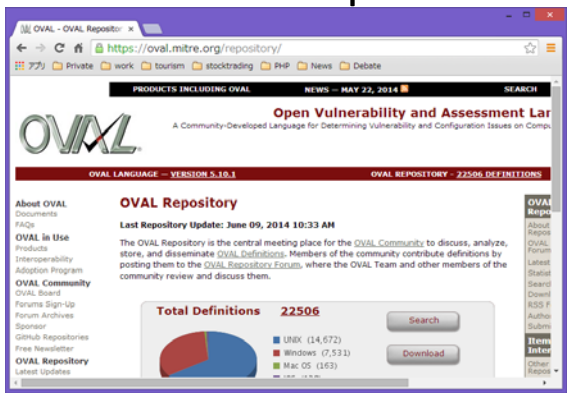


OpenSource Vulnerability Database (OSVDB)

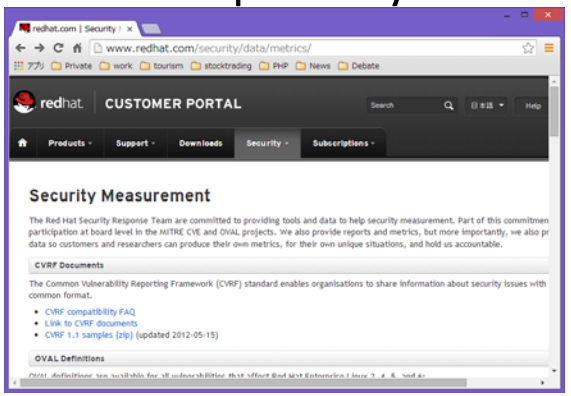


Japan Vulnerability Notes (JVN)

MITRE's OVAL repositories



Red Hat repository



- 情報はWeb上に散在し、データ保存形式も異なる
- これらの情報に対して統一的な手段で効率的にアクセス可能なアプリケーションが求められている

目次

- 背景
- 提案内容
- プロトタイプ

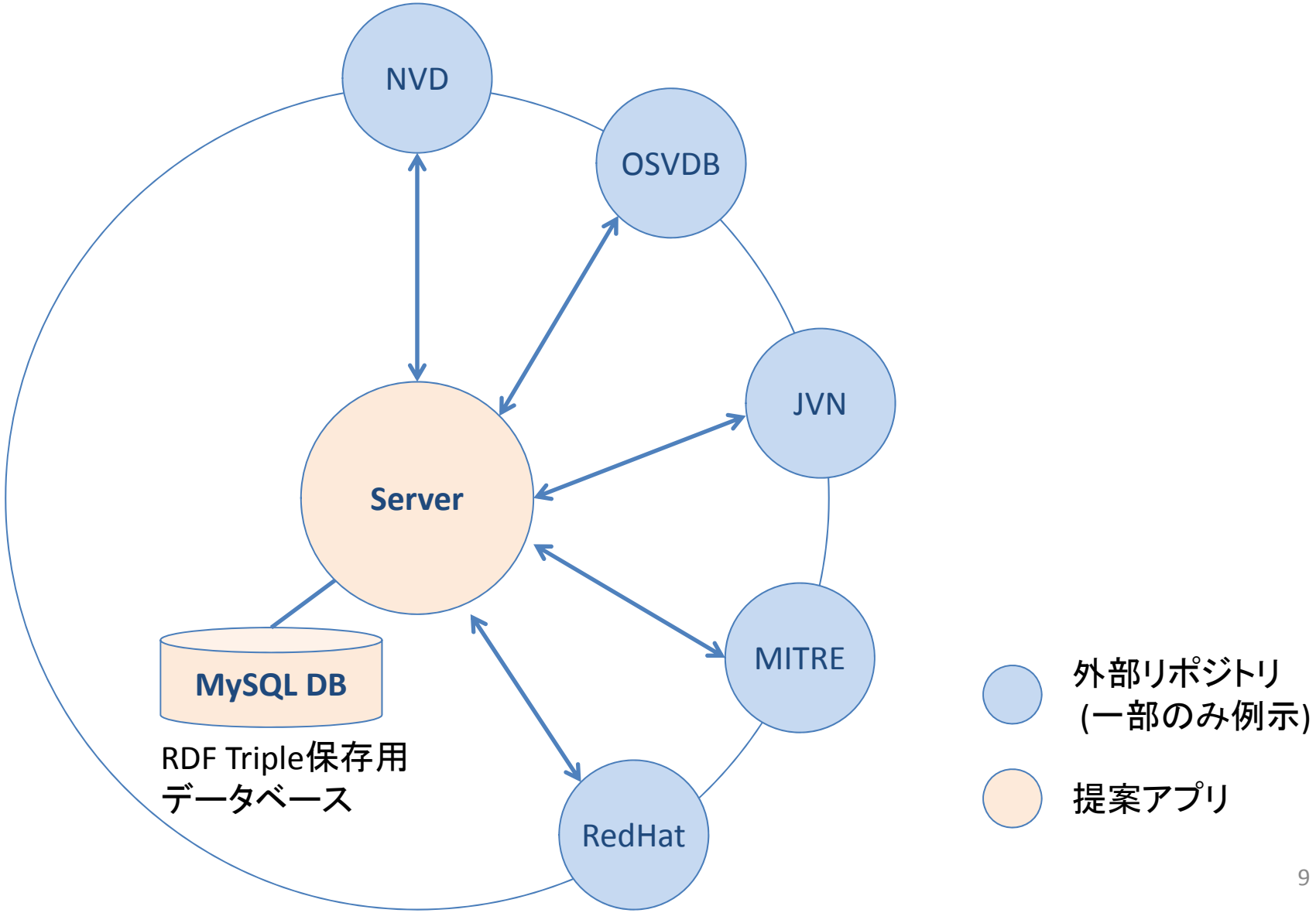
提案アプリケーションの概要

- 情報が利活用可能な形で公開され、またそれらを効率的に利用できるような利活用基盤アプリケーションを提案

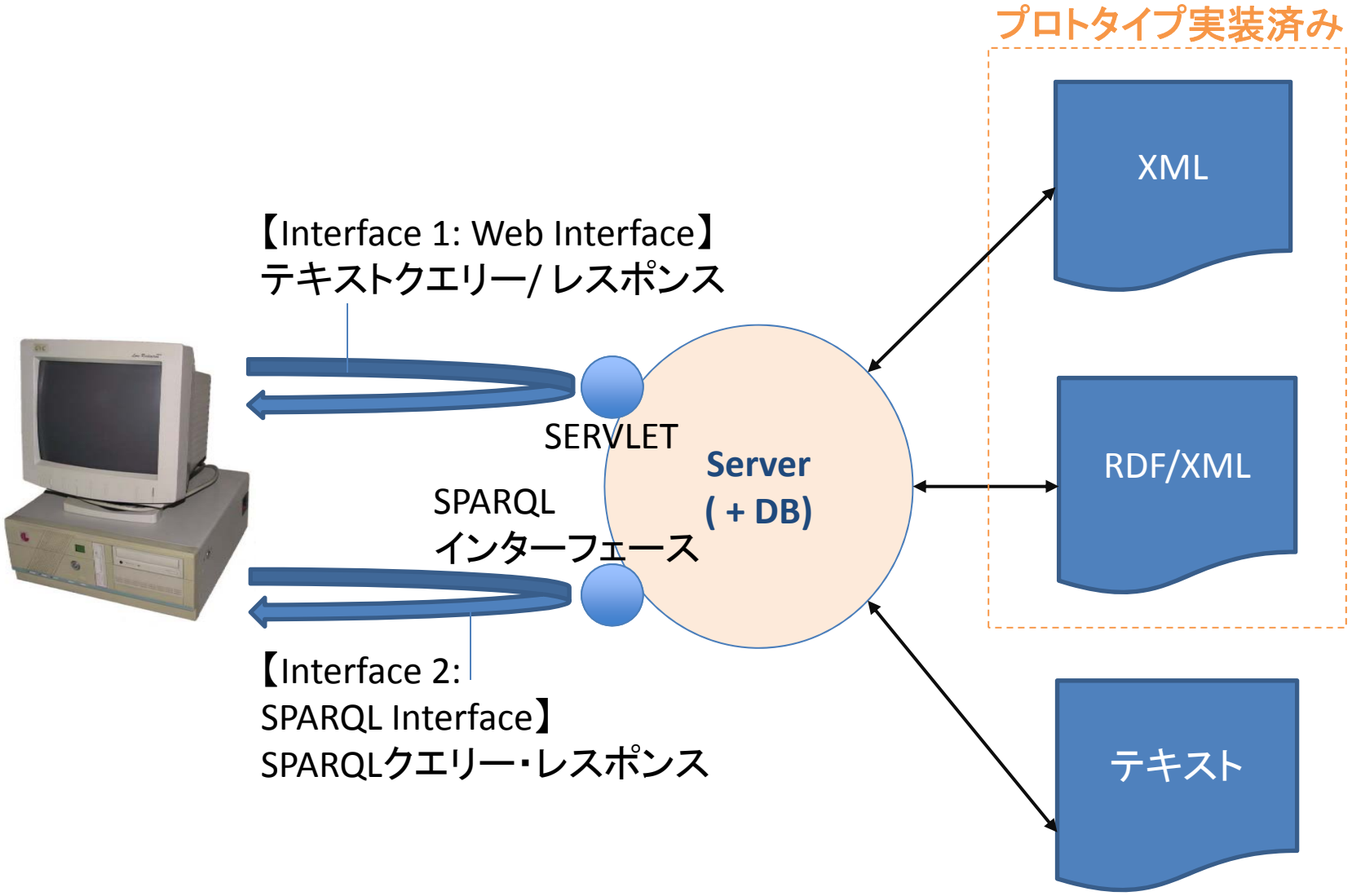
- Web上のサイバーセキュリティに関するRDF、XML、その他の情報をリンクし、ユーザのリクエストに応じて必要な情報のURIを返却
  - 情報提供者は、必ずしもRDFなどのOpen Linked Dataに適した形式で情報を提供する必要はない
  - 提案アプリケーション側で、メタデータをRDF化して保持

- 2つのユーザインターフェースを準備
  - ブラウザー上の検索インターフェース：クエリーにより引き当てられた情報のURI、またその内容をブラウザー上にて表示
  - SPARQLエンドポイント

提案アプリケーションは各種データをリンク



2つのインターフェースを持つ



目次

- 背景
- 提案内容
- プロトタイプ

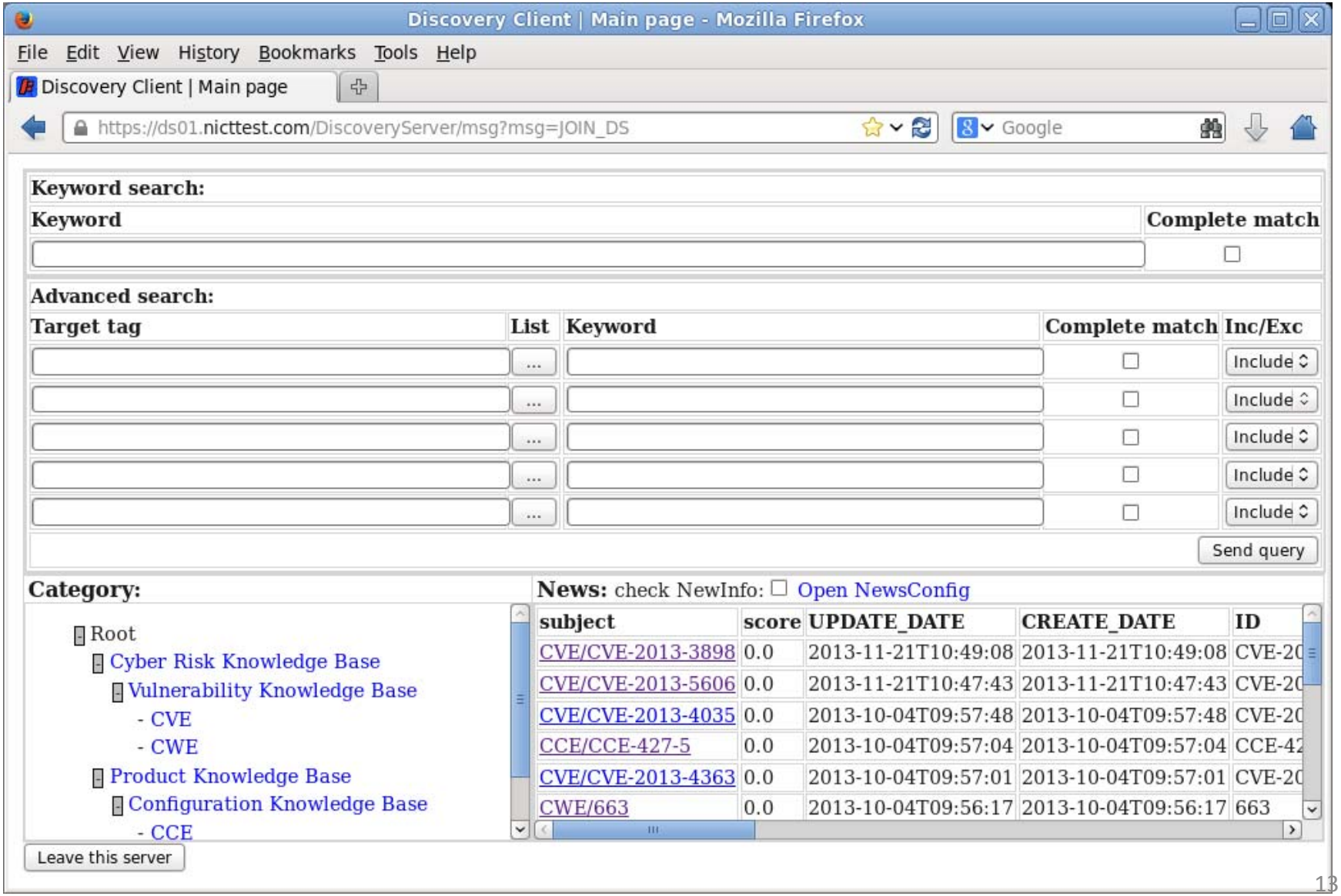
アイデア実現に向けたアプリケーションの実装状況

- Web上の各種セキュリティ情報リポジトリをリンクするアプリケーションを構築中
  - 各種リポジトリのスキーマギャップに対応
    - 各種リポジトリの用いるXML・RDFのスキーマ構造には統一性がない
    - これらの情報を汎用XSLTによりRDF化し、その情報を内部で保存することにより、ユーザからの検索クエリに対応
  - すでにNVD、JVN、OSVDBなど、各種リポジトリをリンク

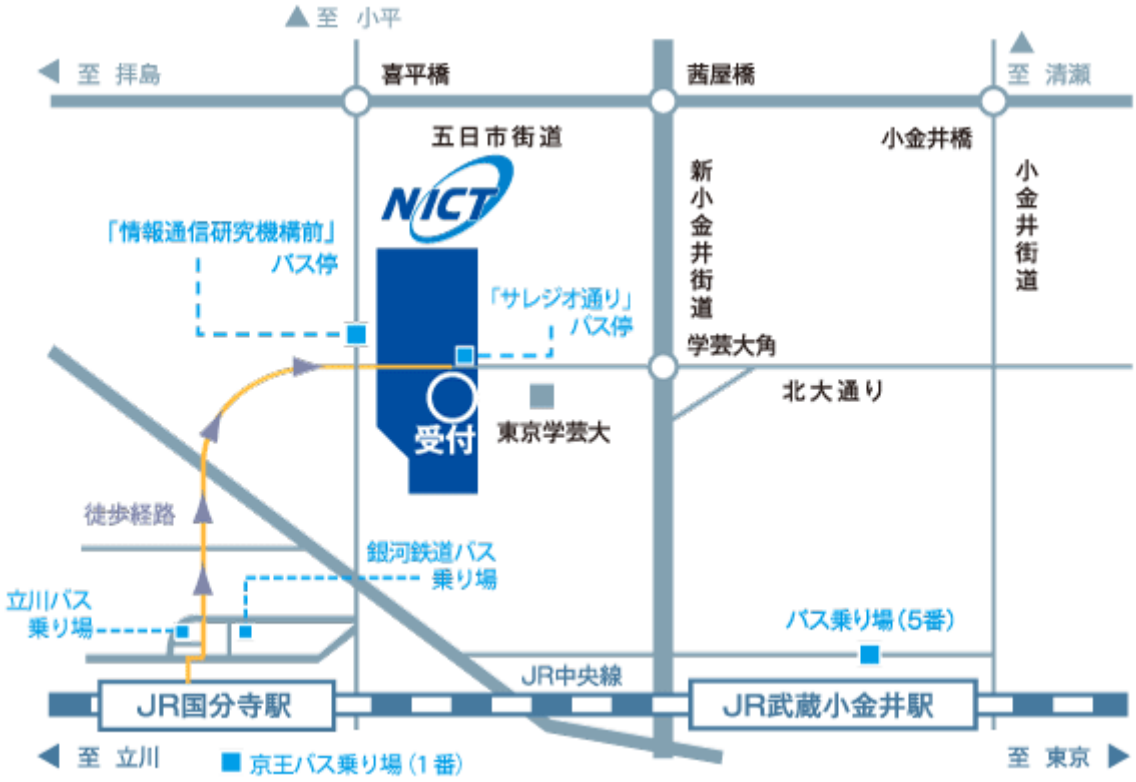
- ユーザがほしい情報のURIを返却する機能、その内容を表示する機能、またSPARQLインターフェースを実装済み

- 将来的には外部公開する方向で活動を進めている
  - 外部公開にはアプリケーションの悪用などの問題をクリアする必要有
  - そのため、現時点ではアイデア部門での投稿とさせて頂いている

プロトタイプ


Discovery Client | Main page - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Discovery Client | Main page
https://ds01.nicttest.com/DiscoveryServer/msg?msg=JOIN_DS
Google
Keyword search:
Keyword
Complete match
Advanced search:
Target tag
List
Keyword
Complete match
Inc/Exc
Include
Send query
Category:
Root
Cyber Risk Knowledge Base
Vulnerability Knowledge Base
- CVE
- CWE
Product Knowledge Base
Configuration Knowledge Base
- CCE
News: check NewInfo: Open NewsConfig
subject
score
UPDATE_DATE
CREATE_DATE
ID
CVE/CVE-2013-3898 0.0 2013-11-21T10:49:08 2013-11-21T10:49:08 CVE-20
CVE/CVE-2013-5606 0.0 2013-11-21T10:47:43 2013-11-21T10:47:43 CVE-20
CVE/CVE-2013-4035 0.0 2013-10-04T09:57:48 2013-10-04T09:57:48 CVE-20
CCE/CCE-427-5 0.0 2013-10-04T09:57:04 2013-10-04T09:57:04 CCE-42
CVE/CVE-2013-4363 0.0 2013-10-04T09:57:01 2013-10-04T09:57:01 CVE-20
CWE/663 0.0 2013-10-04T09:56:17 2013-10-04T09:56:17 663
Leave this server

Contact



(独)情報通信研究機構
ネットワークセキュリティ研究所セキュリティアーキテクチャ研究室
Address: 〒184-8795 東京都小金井市貫井北町4-2-1
Email: takeshi_takahashi@nict.go.jp
Members: 高橋健志, パンタ ボーラ、山口修平、中尾康二、平和昌