Semantic Webを利用したセキュリティ要件検討支援ツールSPATのご紹介

2008年03月07日

独立行政法人 情報処理推進機構

セキュリティセンター

（調達におけるセキュリティ要件研究会）

Copyright © 2008 独立行政法人 情報処理推進機構

1. 背景

◆ セキュリティに関する情報の問題

● 情報の分散性

セキュリティに関する情報はインターネット上に大量に存在する。

● 関連情報の収集

必要なセキュリティを検討するためには、関連するセキュリティに関する情報を入手する必要がある。

● 最新情報の収集

セキュリティを検討するためには、最新のセキュリティに関する情報を入手する必要がある。

● タイムリーな情報の収集

セキュリティ事故、対策の情報は、タイムリー（最短）に入手する必要がある。

● 情報の活用

セキュリティを確保するためには、関係するセキュリティに関する情報を関連づけて、適切な対策を行う必要がある。

Copyright © 2008 独立行政法人 情報処理推進機構

2. SPAT開発の背景

【セキュア・ジャパン2007（案）】

第3章　第1節　ア　キ）　情報セキュリティに配慮したシステム選定・調達の支援

各政府機関が情報セキュリティに配慮したITシステムの調達を実効的かつ効率的に行えるようにするため、**2007年度に、独立行政法人情報処理推進機構（以下、「IPA」という。）において、ITセキュリティ要件、ITセキュリティ評価及び認証制度の認証製品活用の可否を確認する際の支援ツールを開発する**とともに、政府機関統一基準の関連マニュアル等に反映することを通じて、政府機関等における当該ツールの活用を促進する。

【SPAT開発および研究会の趣旨】

IPAでは、「情報システムに必要なセキュリティ要件とセキュリティ機器調査および情報セキュリティ機器調達支援ツール（SPAT:　Security Procurement Aid Tool）の開発」を実施しています。
また、開発業務を円滑に進めるために、**政府機関、地方公共団体の関係者と関係ベンダーの参加**による研究会をIPA内に設置し「情報システムに必要なセキュリティ要件とセキュリティ機器調査および情報セキュリティ機器調達支援ツール」開発に関する取組みを支援しています。

Copyright © 2008 独立行政法人 情報処理推進機構

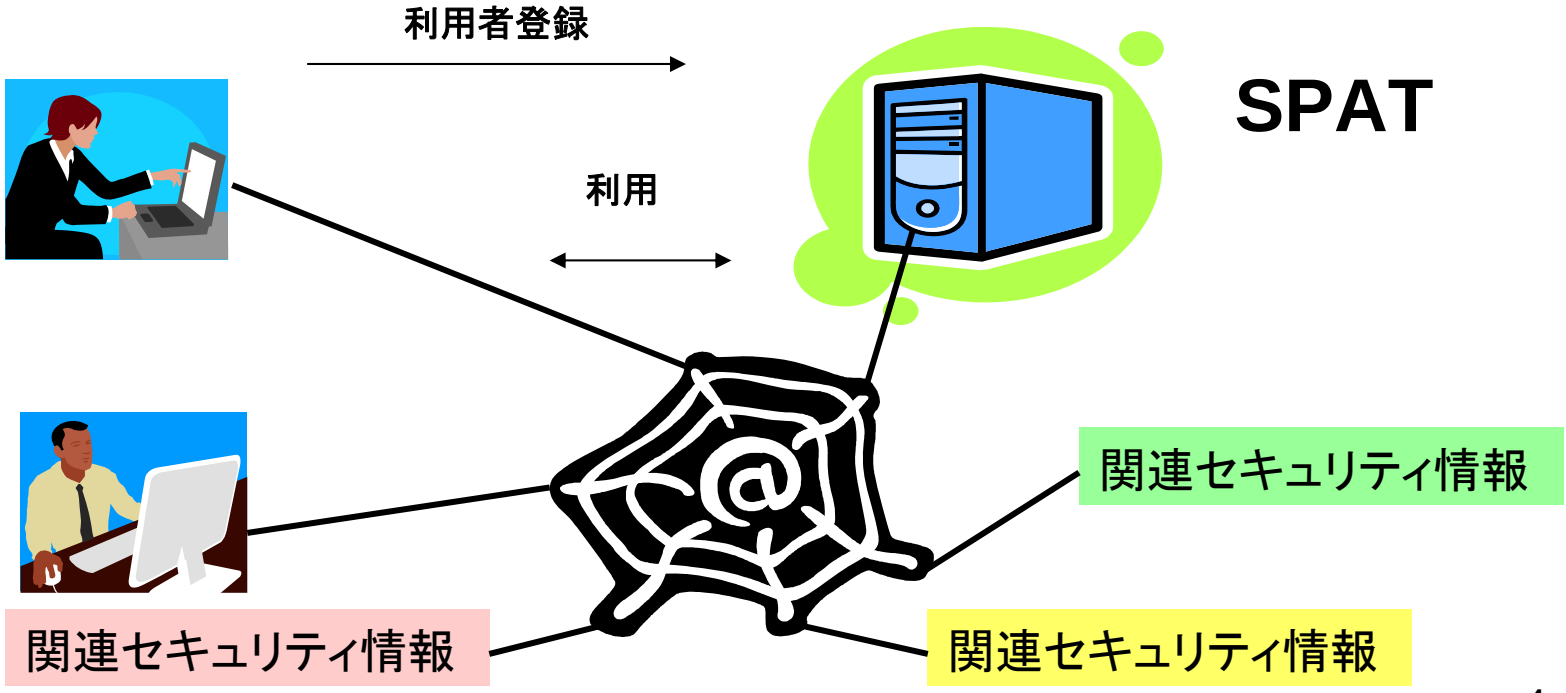
開発の概要：SPATの基本仕様について

システムの概要

・セキュリティの専門家が関係づけたセキュリティ要件などの必要なセキュリティ情報を提供できる環境を構築します。

・主要関係先のWebサイトより発信される関連するセキュリティ情報、適宜参照して統合的なセキュリティ要件検討環境を提供します。（RSS情報、関連サイト情報を参照）

・SPATは、登録されたユーザがインターネット経由でセキュリティ要件の検討が出来る環境を提供します。

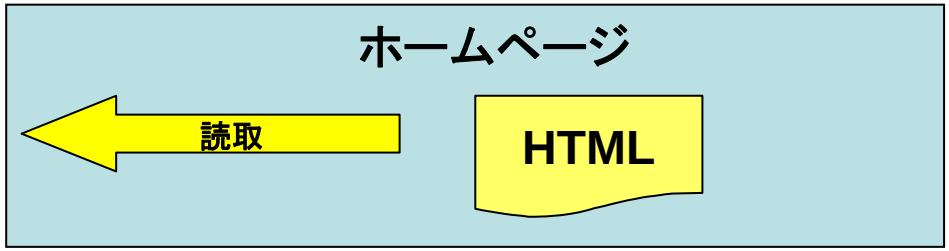


Copyright © 2008 独立行政法人 情報処理推進機構

開発の概要：インターネット上の情報の性質と活用について

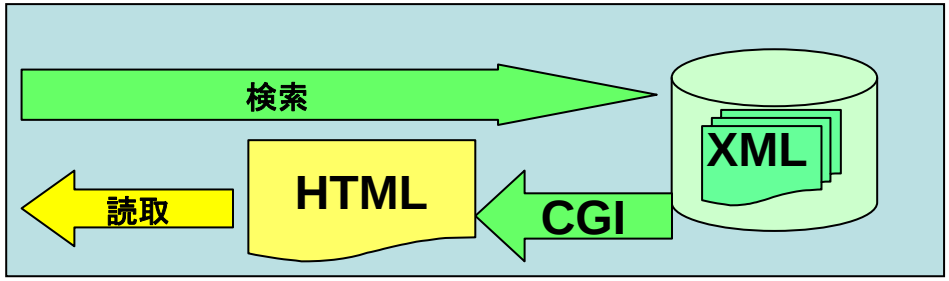
IPA

情報の読取



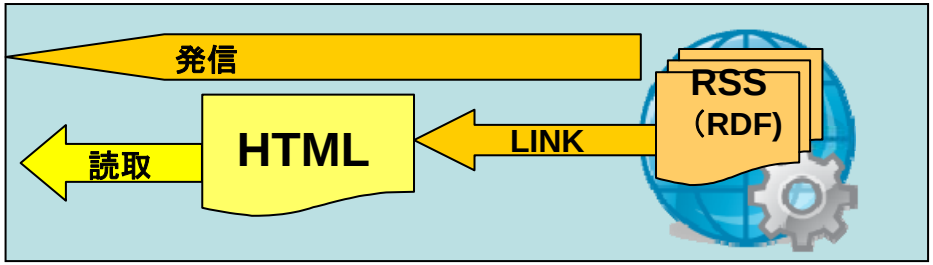
利用者に情報を表示する。

情報の検索



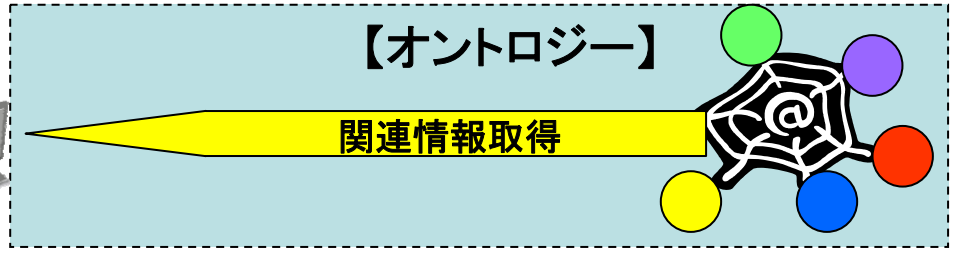
利用者が必要な情報をまとめて表示する。

情報の発信



サイトが発信したい情報をまとめて発信する。

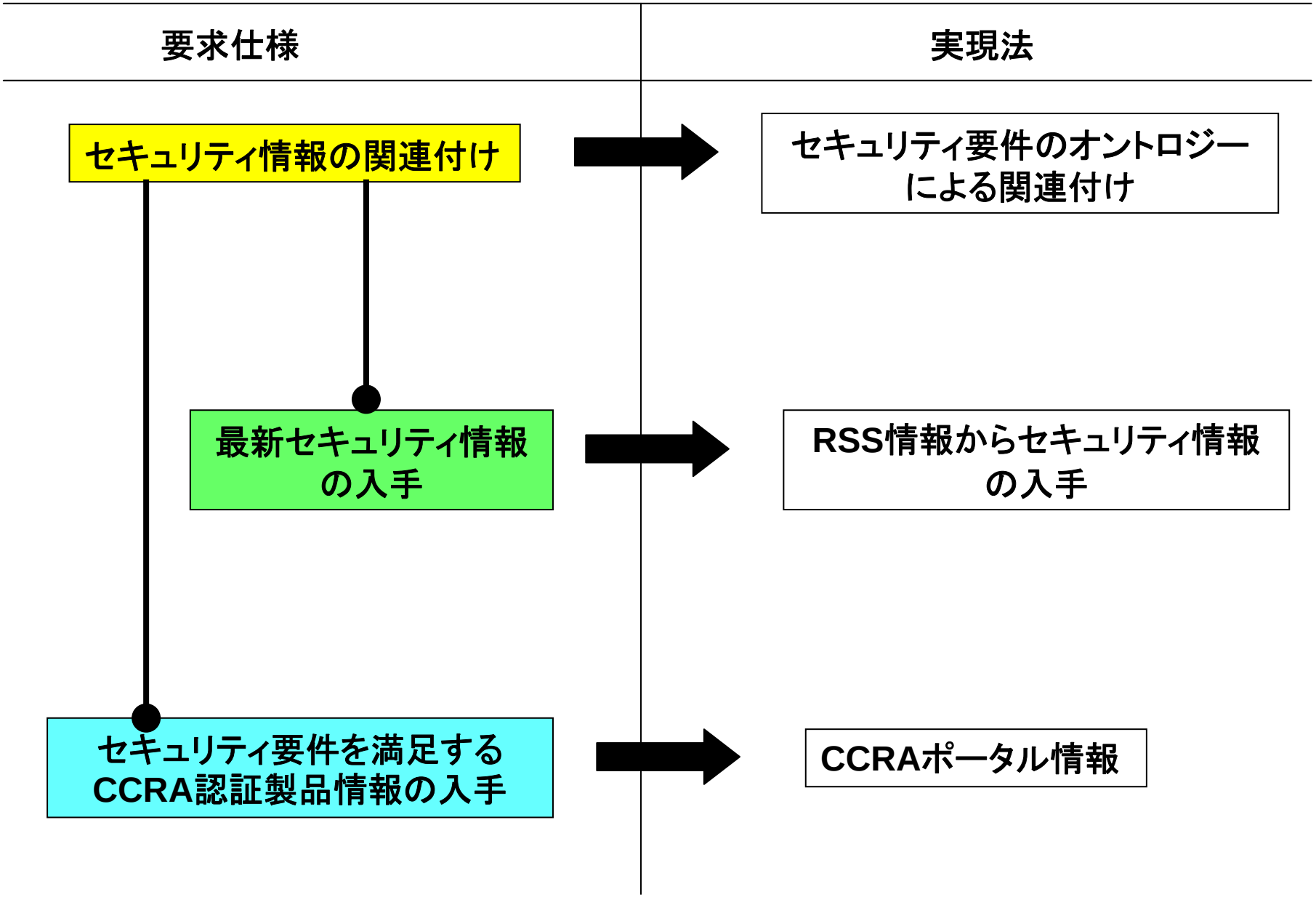
関連情報取得



メタファイルの関係を有機的に、関連付け再構成することが出来る。

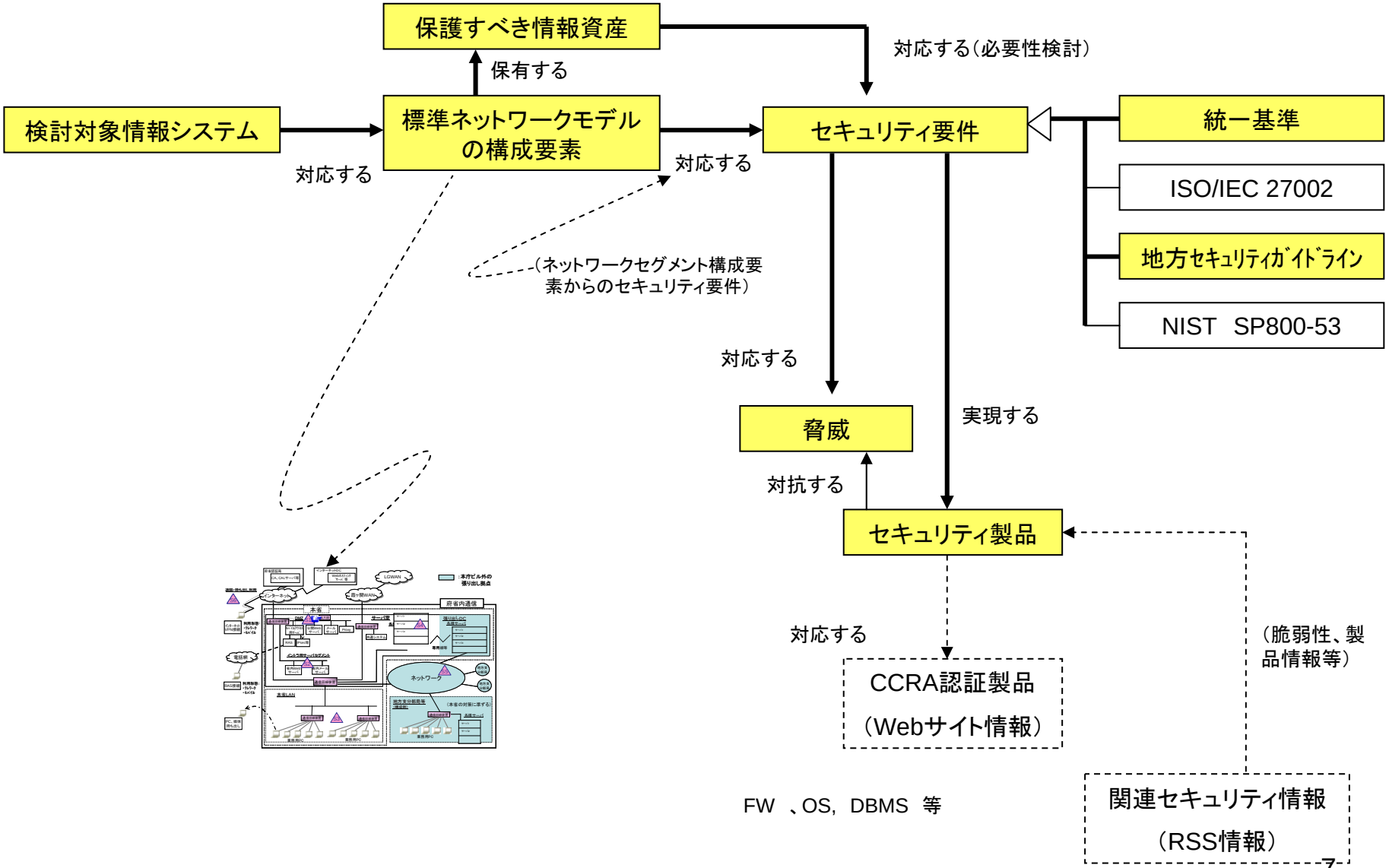
Copyright © 2008 独立行政法人 情報処理推進機構

開発の概要：SPATの要求仕様とインターネット上の情報活用



Copyright © 2008 独立行政法人 情報処理推進機構

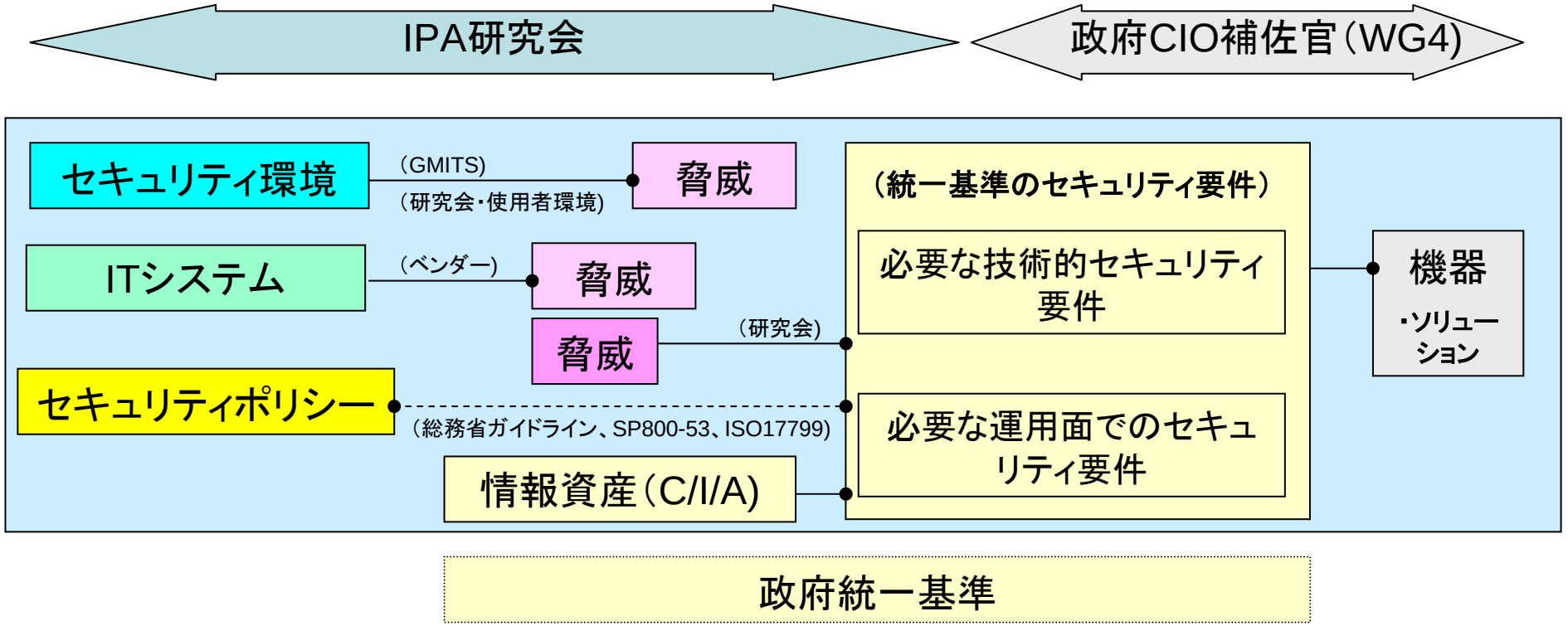
開発の概要：SPATのセキュリティ要件の関係について



Copyright © 2008 独立行政法人 情報処理推進機構

開発の概要：セキュリティ要件の関係について

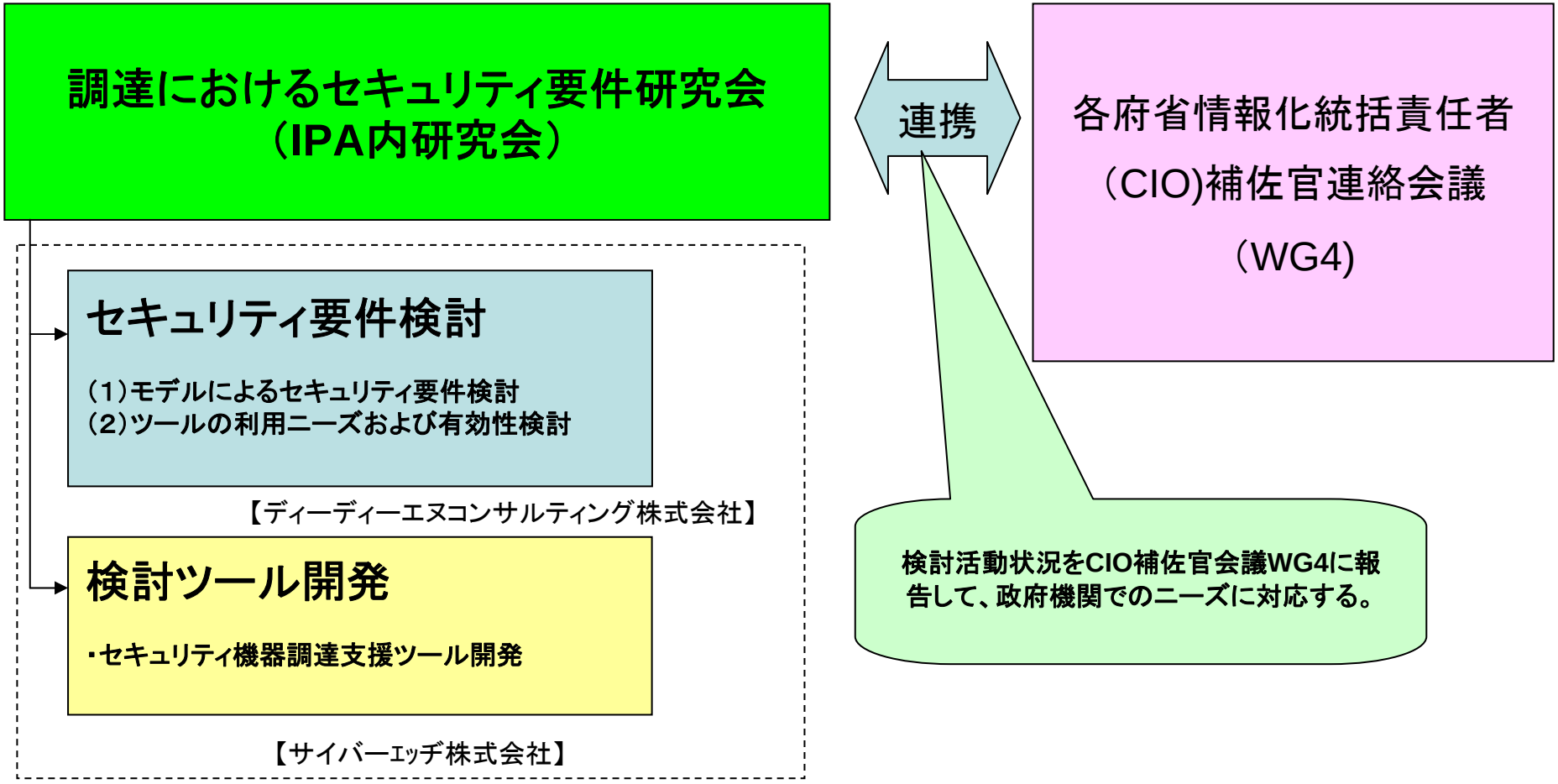
セキュリティ要件の関係は、統一基準、GIMITS等の規格を参照したり、セキュリティの専門家の経験と知識より整理する。



セキュリティ環境、脅威、必要なセキュリティ要件と関係する情報機器の関係が導かれる。

Copyright © 2008 独立行政法人 情報処理推進機構

調達におけるセキュリティ要件研究会と開発体制に関して



Copyright © 2008 独立行政法人 情報処理推進機構

調達におけるセキュリティ要件研究会委員（2007年度）

氏名	所属会社・団体等	所属部署等
苗村憲司	情報セキュリティ大学院大学	セキュア社会システム研究所教授
井堀幹夫	市川市役所	ＣＩＯ情報政策監
三科清高	神奈川県庁	企画部参事（ＩＴ担当）
伊藤博明	高知県庁	政策企画部情報政策課　課長
森口聖	滋賀県庁	県民文化生活部IT統括監
石川家継	（財）地方自治情報センター	自治体セキュリティ支援室　室長
満塩尚之	ディーディーエヌコンサルティング㈱	（環境省情報化統括責任者（CIO）補佐官）
野村邦彦		（経済産業省情報化統括責任者（CIO）補佐官）　（オブザーバ）
平林元明		（内閣府情報化統括責任者（CIO）補佐官）
山岸行弘	サイバーネットシステム株式会社	
沢田寛治	沖電気株式会社	社会情報ソリューション本部　担当部長
篠原郁二	日本電気株式会社	政策調査部担当部長
織茂昌之	株式会社日立製作所	セキュリティソリューション推進本部　主幹
西見俊彦	富士通株式会社	アウトソーシング事業部 情報セキュリティセンターセキュリティ監査部　部長
則包真一	NTTコミュニュケーションズ株式会社	第2法人営業本部　U-Japan推進部（課長）
白杉武志	新日鉄ソリューションズ株式会社	ITエンジニアリング事業部
金子浩之	みずほ情報総研株式会社	情報コミュニュケーション部情報セキュリティ評価室　室長

Copyright © 2008 独立行政法人 情報処理推進機構

開発の概要：最新セキュリティ情報の入手（セキュリティ情報RSSポータル）

（1）目的

セキュリティに関係する最新情報を利用者に提供するセキュリティ情報サービス機能

（2）機能目標

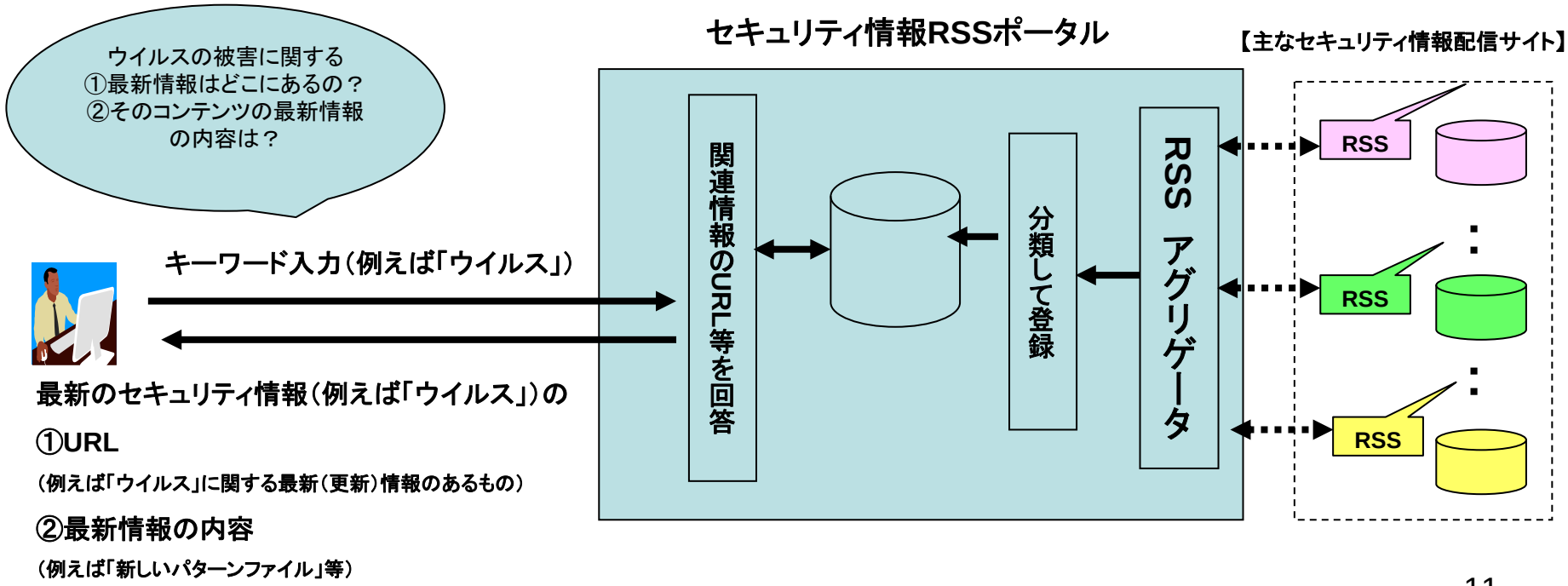
1）利用者に最新のセキュリティ情報の内容と場所（URL）を示す：

代表的なWebサイトのRSS情報を収集して、利用者に最新情報提供する。

RSS(RDF Site Summary)は、サイトの情報、およびサイトから発信されたコンテンツの内容を、見出し、要約情報、発信日時の情報としてまとめて提供することが出来る。（通常のキーワード検索では、コンテンツの内容、更新情報を知ることは出来ない。）

（1）代表的Webサイトの情報最新情報の存在
（2）カテゴリー別の最新情報の存在

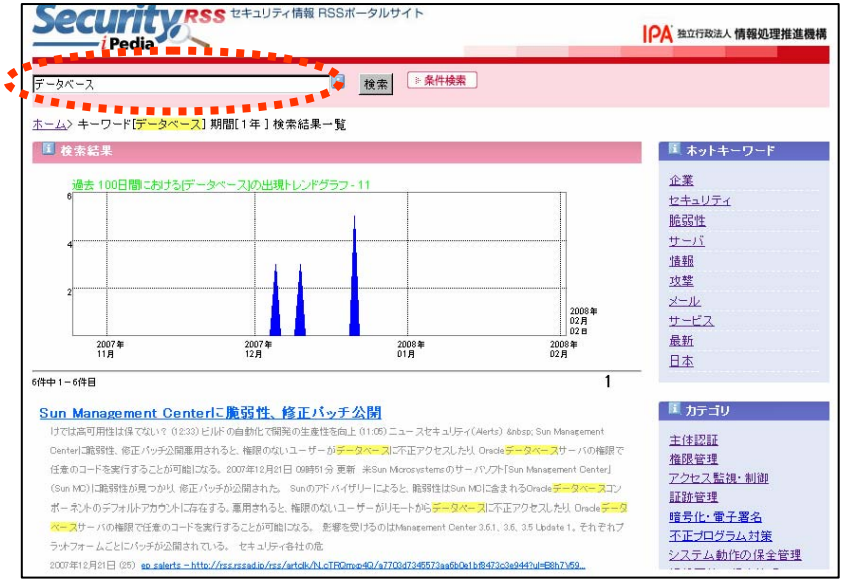
⇐ 最新の情報入手



Copyright © 2008 独立行政法人 情報処理推進機構

【条件検索】

【キーワード検索】



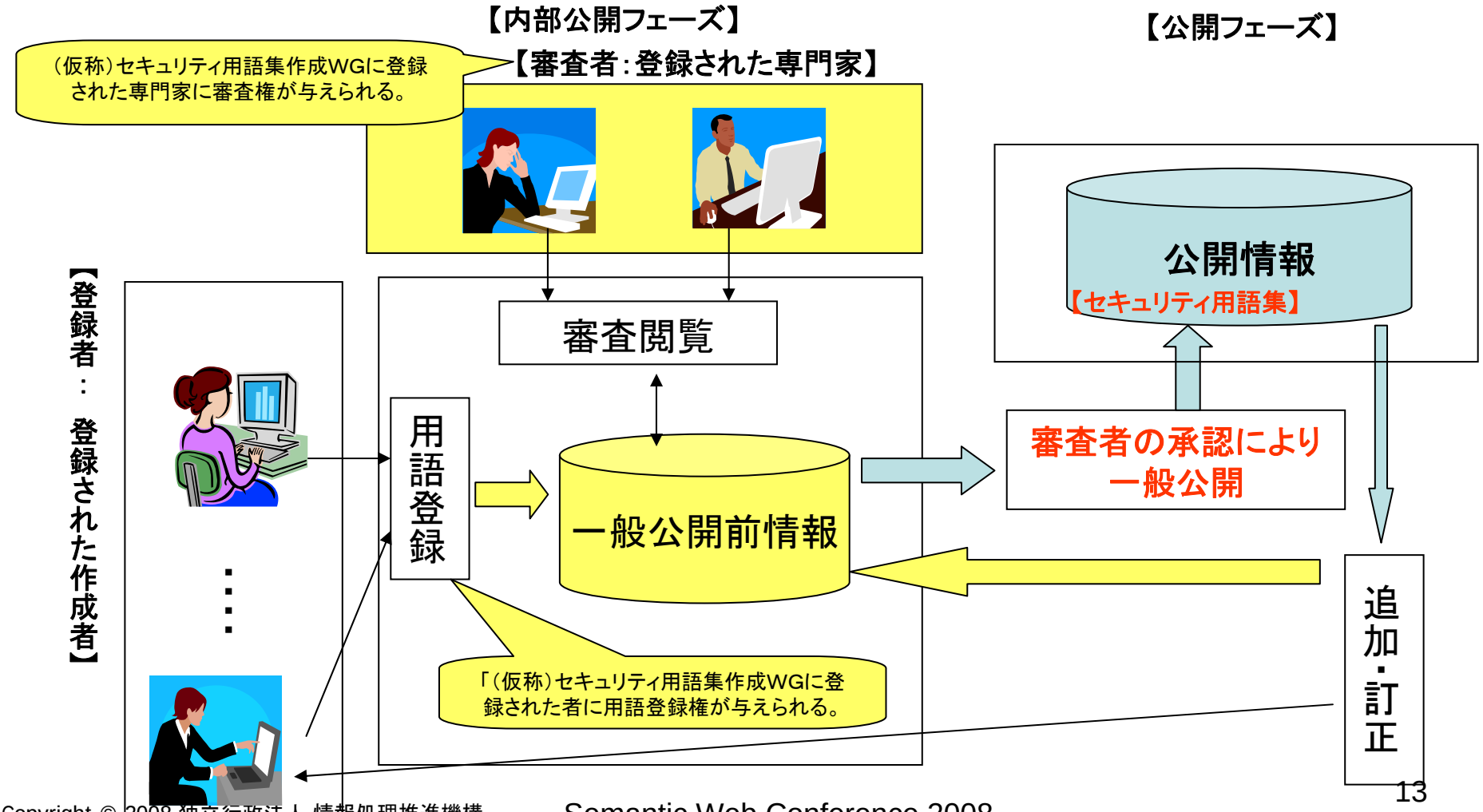
【カテゴリー検索】

Copyright © 2008 独立行政法人 情報処理推進機構

開発の概要：最新セキュリティ情報の入手（セキュリティ用語集構築環境）

（1）目的

ITセキュリティに関係する用語集をIPAの（仮称）セキュリティ用語集WGに登録された者が、インターネット上で協調して、セキュリティ用語集のセキュリティキーワードを登録、説明の登録して、セキュリティ分野の標準辞書を効率的に作成する環境を作る。

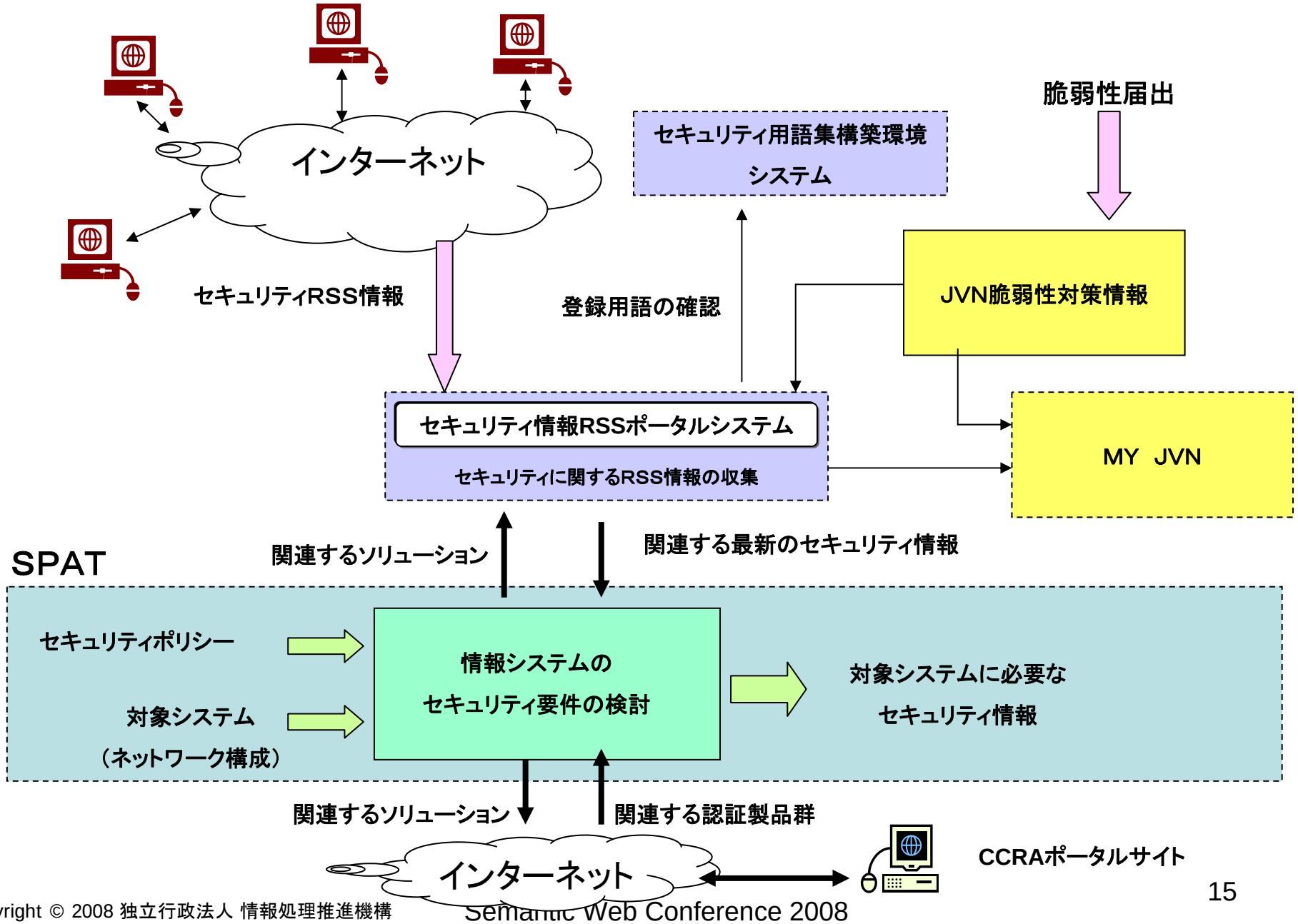


【カテゴリー検索】

【トレンドキーワード検索】

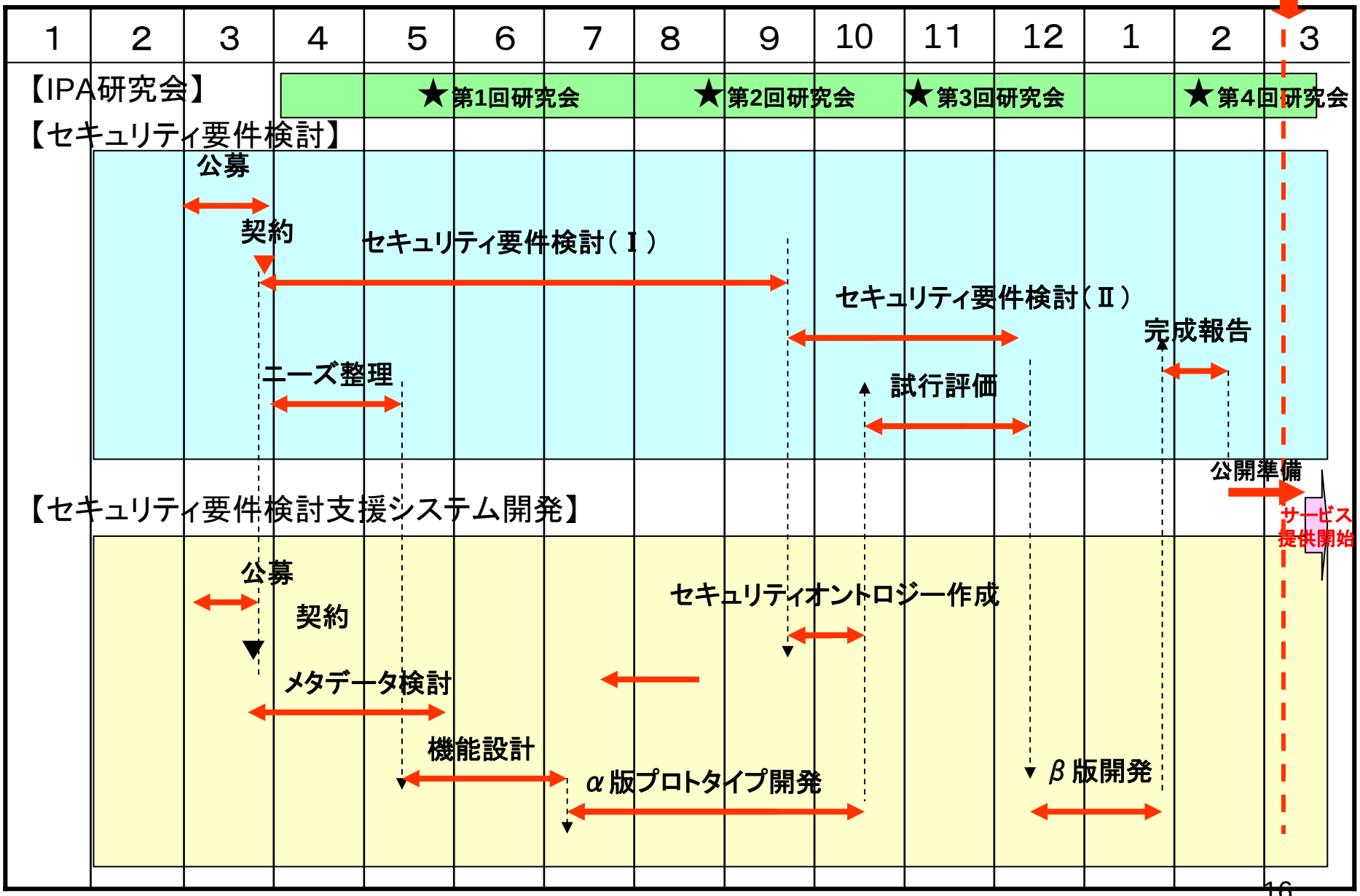
Copyright © 2008 独立行政法人 情報処理推進機構

開発の概要：セキュリティに関するSemanticネットワーク



Copyright © 2008 独立行政法人 情報処理推進機構

開発スケジュール



Copyright © 2008 独立行政法人 情報処理推進機構

開発の効果：セキュリティに関するSemanticWebシステム（SPAT）の開発の効果

効果

- **関係付けされた情報は、利用価値が高まる。**

検討対象の情報システム関係するセキュリティ要件、ソリューション情報、脆弱性、セキュリティ事故を様々な視点で検討することが可能。

- **Web上の膨大な知識を体系的に利用可能となる。**

今まで、見落とされていた重要な情報を収集して、選択して利用者に提示できるようになる。

必要な情報を手短に活用できるようになる。

Copyright © 2008 独立行政法人 情報処理推進機構

開発の総括：セキュリティに関するSemanticWebシステム（SPAT）の開発法について

開発法

● 情報の関連付けが最も重要。

意味ある情報とするために、情報の関連付けが最重要。

・情報の関連、冗長性を少なくするために、全体から個別の関連付けの整理が効果的。

● Web上の情報を活用するための工夫が必要。

現在は、インターネット上で活用できる膨大な非SemanticWebデータ（非オントロジーデータ）情報を活用するためのインターフェースを設計、構築することが重要である。

Copyright © 2008 独立行政法人 情報処理推進機構

期待：Semantic　Webへの要求（期待）

期待

1.　Semantic　Web開発のためのツールの充実。

・開発ツール、管理ツール等現時点で不充分。

・Semantic　Webの専門知識が無くとも開発できる環境の実現。

2.　開発事例、方法論の蓄積が不充分。

・開発に当たり、参考となる方法論が見当たらなかったので、試行錯誤を繰り返した。

・参考となる事例が不充分。

3.　オントロジデータの充実を期待。

・情報の連携で、利用する情報の価値が高まるが、現在利用可能なオントロジーデータは少ない。（Semantic　Webの更なる普及で相乗効果期待できる。）

Copyright © 2008 独立行政法人 情報処理推進機構

独立行政法人　情報処理推進機構
セキュリティセンター（IPA/ISEC）

〒113-6591
東京都文京区本駒込２－２８－８
文京グリーンコートセンターオフィス１６階
電子メール　isec-info@ipa.go.jp
URL　http://www.ipa.go.jp/security/

Copyright © 2008 独立行政法人 情報処理推進機構