

「脆弱性対策情報共有ツール MyJVN バージョン2の開発請負契約」

提案依頼書

1. 作業の概要

1. 1 業務の概要

本公募で求める業務は、公募要領「2. 応募要件（3）業務範囲」のとおりです。なお、業務内容の詳細については以下のとおりとします。

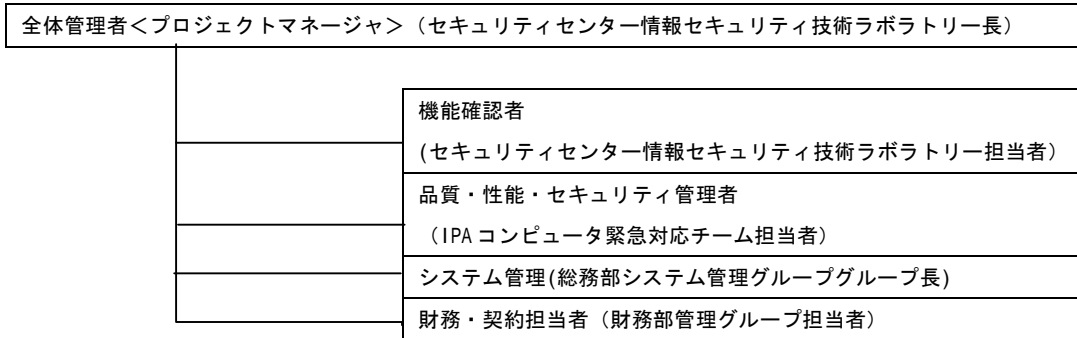
IPA セキュリティセンターでは、ウェブサイトやソフトウェア製品の脆弱性について適切な情報の流通および対策の促進を図るための仕組み「情報セキュリティ早期警戒パートナーシップ」制度を2004年7月から開始しております。さらに、「情報セキュリティ早期警戒パートナーシップ」において取り扱われた脆弱性、および国内で利用されているソフトウェア等の製品に関する脆弱性を対象として、その概要や対策情報を収集・蓄積する「脆弱性対策情報データベース（JVN iPedia）」を2007年4月から公開しております。また、特に世の中への影響が大きい場合は、IPA 注意喚起として公表し、脆弱性対策を呼びかけています。

また、社会全体として脆弱性を低減するためには、専門家が不足する中小規模組織においても実施できるように脆弱性対策の簡易化／自動化が望まれており、IPA では「脆弱性対策情報共有ツール MyJVN」を整備しました。

この「脆弱性対策情報共有ツール MyJVN」の成果を踏まえ、脆弱性対策パッチの簡易型バージョンチェック機能、クライアント PC の OS のセキュリティ設定チェック機能、JVN iPedia 最新版から MyJVN の DB サーバへの共通プラットフォーム一覧取り込み機能の開発業務を行っていただきます。

各機能の詳細については「2. 2 機能要件」を参照してください。

なお、本業務における IPA 側の体制は以下のとおりとします。



JVN iPedia は、1998 年に発見された脆弱性から収集を行い、2008 年 10 月公表時点で約 5,300 件の脆弱性対策情報を蓄積しています。

1. 2 納入成果物

本公募の納入成果物については以下のとおりとします。

また、公募要領「4. 契約条件（6）納入物件」及び「4. 契約条件（8）成果に係る知的財産権等の取扱い」についても注意してください。

- ◆ 電子媒体（CD-R等）をIPAに納入すること。
- ◆ 電子媒体の形式等についてはIPAが指定する様式とすること。
- ◆ 成果物の内容は以下のとおりとする。

機能設計書	1式
詳細設計書	1式
利用者マニュアル	1式
運用管理者マニュアル	1式
プログラム	1式
試験結果報告書	1式

1. 3 用語の定義

本提案依頼書における用語の定義は以下のとおりとします。

No	用語	定義	補足
01	SCAP	Security Content Automation Protocol: 情報セキュリティ管理の自動化と標準化を規定した仕様・規格。OVAL や CCE、CPE などがある。	下記 URL を参考 http://www.ipa.go.jp/security/fy19/reports/vuln_Framework/index.html
02	OVAL	Open Vulnerability Assessment Language: プログラム自身に内在する「プログラム上の脆弱性」や、「設定上のセキュリティ問題」などをチェックする項目を記述するため仕様。	下記 URL を参考 http://oval.mitre.org/index.html
03	CCE	Common Configuration Enumeration: プログラムが稼働するための「設定上のセキュリティ問題」を解決するための仕様で、セキュリティと関連する設定項目に一意的番号(設定項目識別子)を付与する。CCE の最新バージョンは 5 であり、9 つのプラットフォームグループと 3,000 以上の識別子で構成している。	下記 URL を参考 http://cce.mitre.org/
04	CPE	Common Platform Enumeration: 製品情報の標準化を規定した仕様・規定(共通プラットフォーム一覧)一つのデータは OS 名、バージョン名や対象言語など 7 項目で構成している。ソフトウェアなどに一意の名称を付与することで、CCE と製品との関連付けを可能にする。CPE の最新バージョンは 2.1 である。	下記 URL を参考 http://www.cpe.mitre.org/

2. 情報システムの要件

2. 1 システムの概要

脆弱性対策情報共有ツール MyJVN バージョン1は、図 2.1-1 に示すように IPA で運営している脆弱性対策情報 JVN iPedia から、情報セキュリティに対して専門的な知識を持っていない利用者（一般ユーザ、システム管理者）が必要な脆弱性対策情報のみを効率よく収集できるように開発しました。

利用者は MyJVN にウェブブラウザでアクセスし、利用しているソフトウェアのベンダ名や製品名を選択するだけで、JVN iPedia の中から該当する脆弱性対策情報を入手することができます。（フィルタリング）

機能として4つのAPI（ベンダー一覧取得機能、製品情報一覧取得機能、脆弱性概要情報一覧取得機能、脆弱性詳細情報取得機能）を実装しており、日本語、および英語での表示が可能となっています。また、API で取り出した情報を機械処理に適した XML フォーマットで提供することにより、他システムへの取り込みなど、加工・再利用を容易にしました。

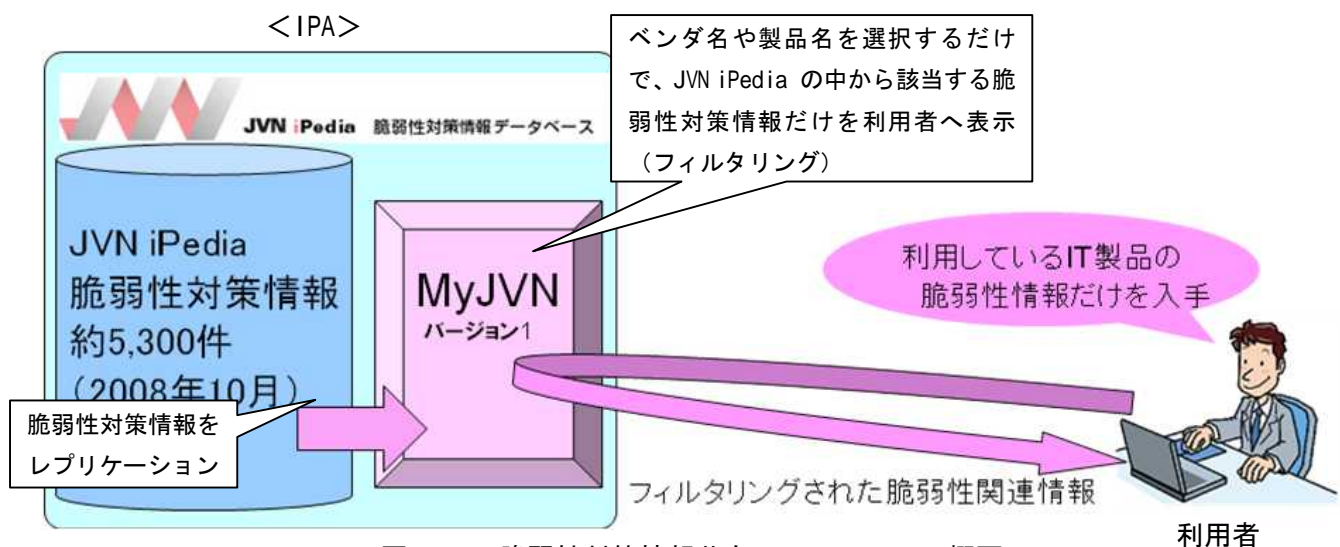


図 2.1-1 脆弱性対策情報共有ツール MyJVN の概要

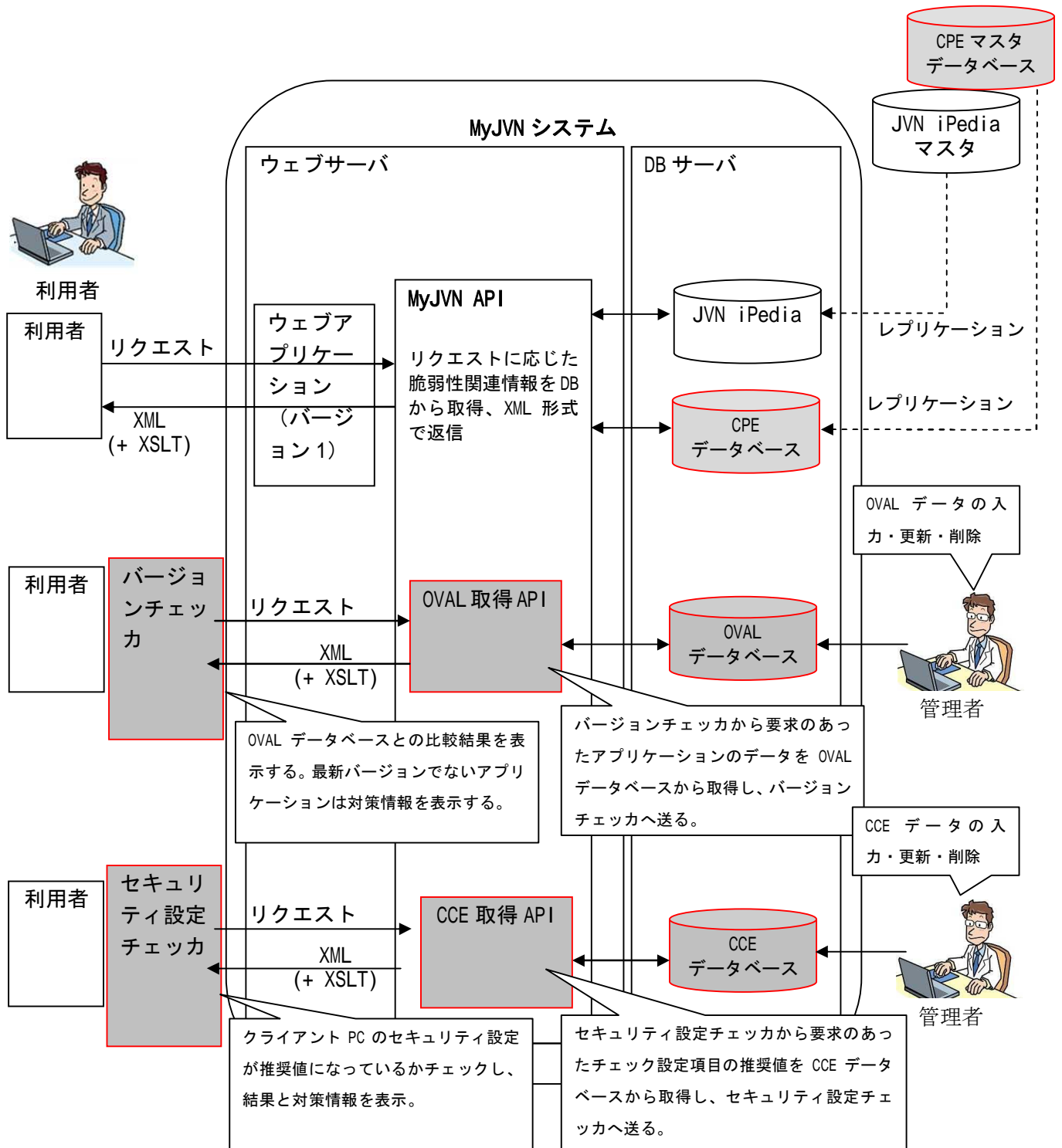
次に、本公募の開発概要は以下の通りである。図 2.1-2 の今回の開発範囲を参照。

脆弱性対策パッチの簡易型バージョンチェック機能（バージョンチェッカ）

クライアント PC の OS のセキュリティ設定チェック機能（セキュリティ設定チェッカ）

JVN iPedia 最新版から MyJVN の DB サーバへの共通プラットフォーム一覧受取り機能

なお、開発にあたっては、情報セキュリティ管理の技術面での自動化、標準化を規定した仕様群である SCAP(Security Content Automation Protocol)の OVAL(Open Vulnerability Assessment Language)と CCE(Common Configuration Enumeration)を採用します。



今回開発範囲：

図 2.1-2 システム構成図

2. 2 機能要件

本公募では以下の機能を求めています。

脆弱性対策パッチの簡易型バージョンチェック機能（バージョンチェッカ）

利用者（一般ユーザ、システム管理者）が IPA のウェブサイト（注意喚起のページなど）にアクセスし、クライアント PC にあるアプリケーションのバージョンをチェックできる機能（バー

ジョンチェッカ)を開発すること。

ソフトウェア製品の脆弱性対策として、最新バージョンにアップデートすることが一般的に推奨されている。しかしながら、利用者側では、アップデートの煩わしさや早急にアップデートする必要性を感じないなど、セキュリティ対策が浸透していないという現状がある。

そこで、MyJVN バージョン2では、情報セキュリティに対して専門的な知識を持っていない利用者が最新のアプリケーションを使っているかどうか簡単にチェックできる機能を開発する。複数のアプリケーションを一度にチェックすることで、セキュリティ対策の推進を期待する。

1) バージョンチェッカの画面遷移イメージを図 2.2-1 に示す。

利用者がバージョンチェッカの実行ファイルを起動するとバージョンチェッカの初期画面が表示され(①)、[START]ボタンをクリックすることにより、バージョンチェッカが、MyJVN の OVAL データベースから取得した当該アプリケーションのバージョンと、クライアント PC 内のアプリケーションのバージョンを比較し、同じかそれ以上の場合 ” ○ ”、異なる場合 ” × ” の比較結果を表示する(②)。比較結果の画面内の[詳細]ボタンを押すと、対策情報を表示する(③)。

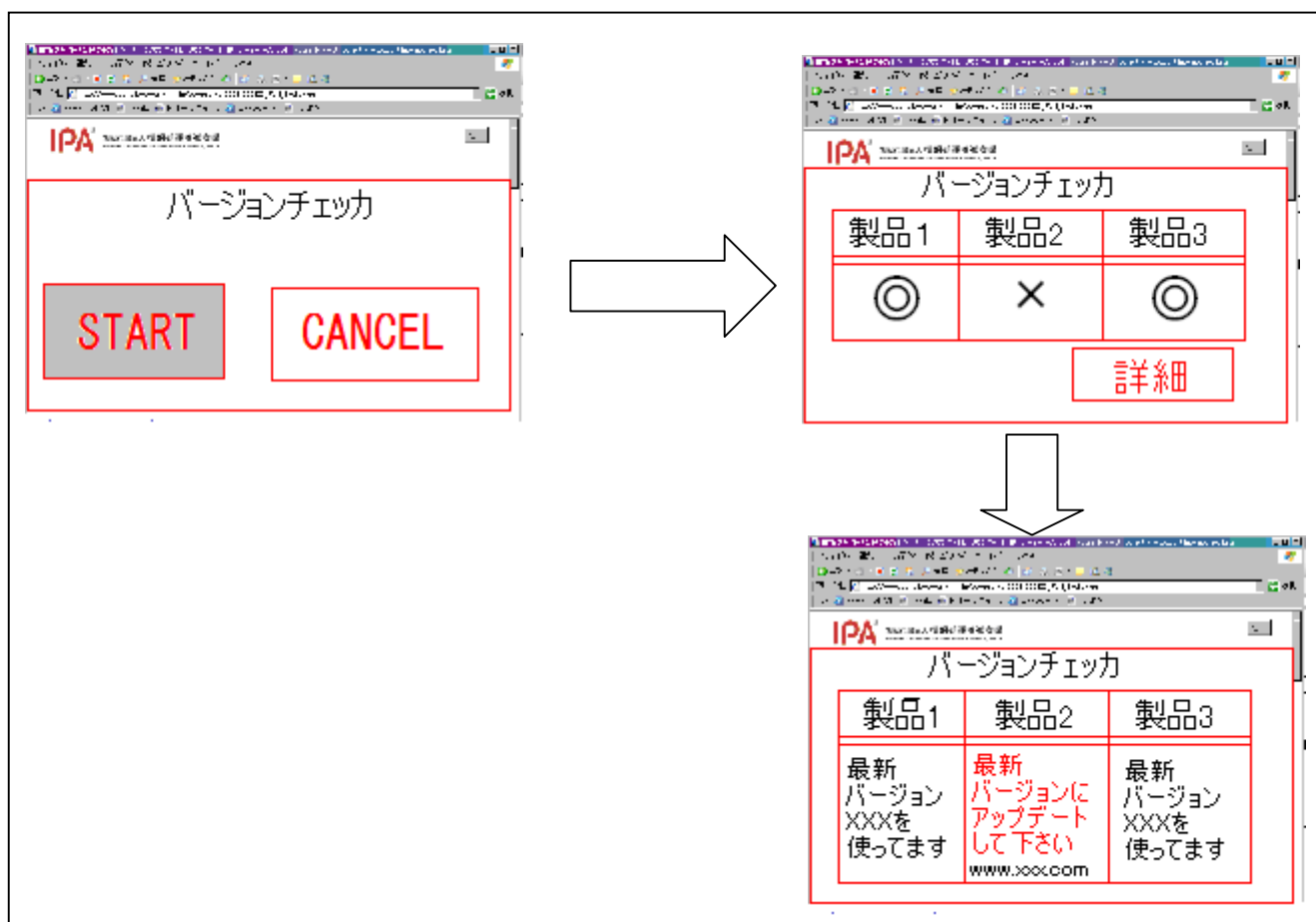


図 2.2-1 脆弱性対策パッチの簡易型バージョンチェック機能 利用画面イメージ

バージョンチェッカは、クライアント PC 環境へ一時的にダウンロードされた後、java アプレット等によって実行される形態とし、チェック対象のバージョン情報などが外部へ送信されることなくチェック処理が行われることとする。

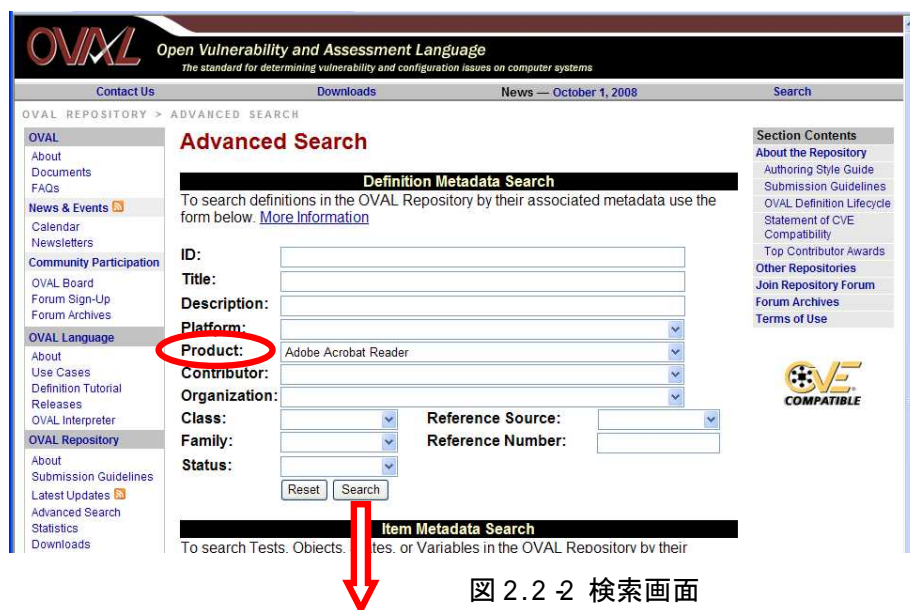
開発対象とするクライアント PC の OS は汎用的なものとし(今回の対象 OS は Windows とする)、対象アプリケーションについては、Adobe Reader、Adobe Flash Player、Java Runtime Environment (JRE)を含む 3 種類以上とすること。開発にあたり対象アプリケーションなどは IPA と協議の上決定すること。

- 2) バージョンチェッカでチェックするために利用する「OVAL ID」、「ベンダ名」、「アプリケーション製品名」、「チェックファイル名」の情報を蓄積するデータベース機能（OVAL データベース）を開発すること。
バージョンチェッカで用いる OVAL データベース項目を表 2.2-1 に示す。

表 2.2-1 OVAL データベース項目説明

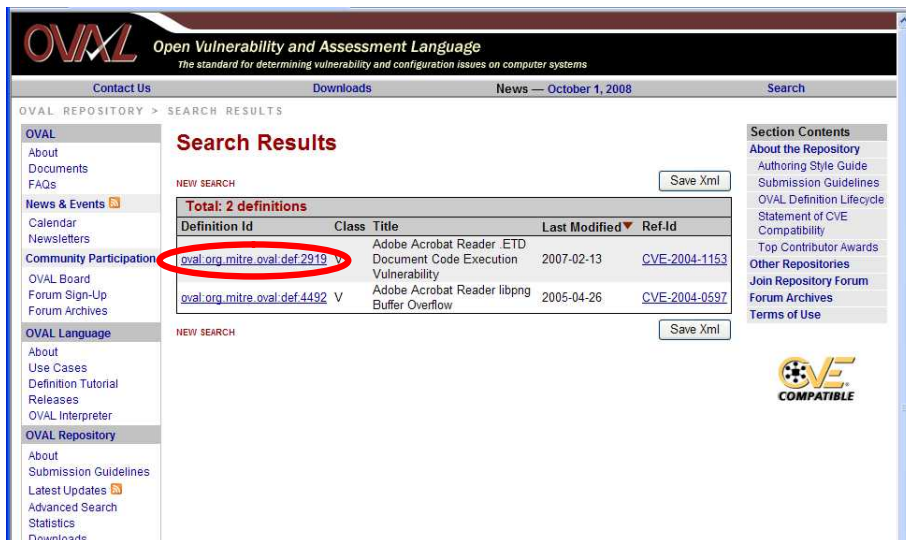
項目名	項目説明	タイプ(必要桁数)
OVAL ID	OVAL で採番された ID を格納する。	半角英数字 (10)
ベンダ名	製品開発・販売社名を格納する。	漢字 (20)
製品名	アプリケーション製品名を格納する。	漢字 (50)
チェックファイル名	OVAL より取得した情報を保管したファイル名を格納する。	半角英数字 (50)

各項目や技術的な仕様などは、規定が標準化されている OVAL を使うこと。
OVAL より取得する製品情報は MITRE 社の OVAL のウェブサイト
(<http://oval.mitre.org/repository/data/AdvancedSearch.jsp>)から、該当する製品情報を取得し、① 1)で IPA と協議の上決定した対象アプリケーションを格納する。
OVAL データベース項目の「OVAL ID」には、図 2.2-4 詳細画面、もしくは図 2.2-5 OVAL XML ファイルの definition id タグより取得し格納する。
OVAL データベース項目の「チェックファイル名」には、図 2.2-4 詳細画面で[Save Xml]をクリックすることにより取得し、ウェブサーバ上に保管したファイル名を格納する。



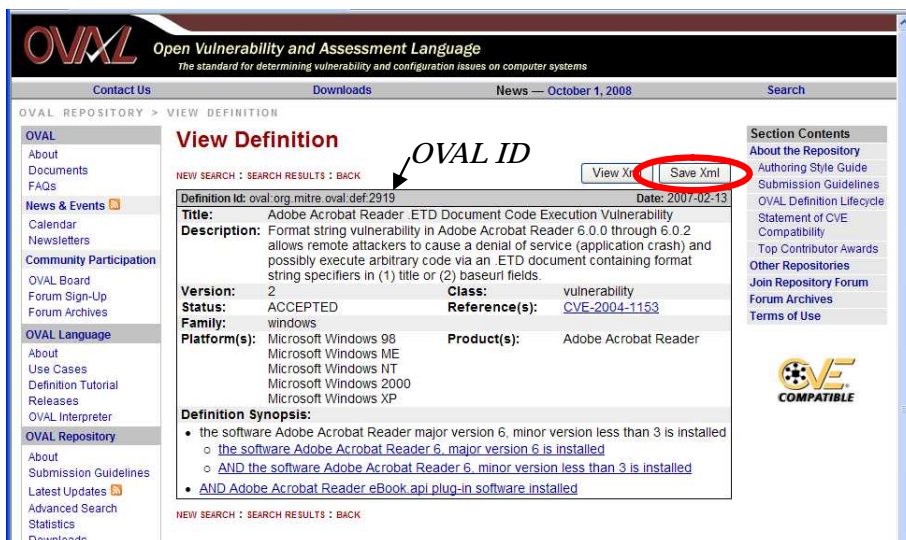
該当する製品を「Product」より選択し、[Search]ボタンをクリックする。

図 2.2-2 検索画面



検索結果より、最新の情報をクリックする。

図 2.2-3 検索結果画面



表示された詳細画面の上部にある[Save Xml]をクリックすることにより、該当製品の情報が保存できる。

図 2.2-4 詳細画面

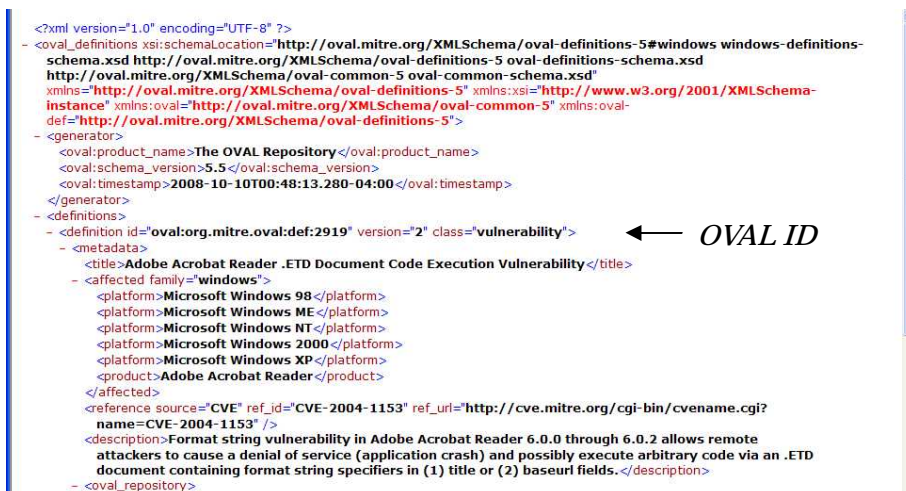


図 2.2-5 保存したチェックファイルの内容

- 3) 表 2.2-2 にバージョンチェッカがクライアント PC 内の情報と比較する際に用いる OVAL XML のタグ名を示す。

OVAL データベースに登録した当該製品のチェックファイル名が示すファイル内のタグに記載された情報と、クライアント PC 内の情報（Windows の場合、レジストリ情報）を比較することで、バージョンチェッカによるバージョンチェックが可能となる。

具体的には「レジストリの比較先」、且つ「製品情報」に記載されている内容をクライアント PC 内のレジストリファイルより探し、そのレジストリに格納されている値と、「バージョン情報」を比較する。比較した結果、クライアント PC 内の製品のバージョンが「バージョン情報」に満たない場合、クライアント PC にインストールされている当該製品は最新のバージョンではないと判断する。

チェック仕様の詳細は MITRE 社の OVAL のウェブサイト (<http://oval.mitre.org/language/download/schema/version5.5/index.html>) を参照すること。

表 2.2-2 タグ名比較表 (Windows の場合)

項目	OVAL XML のタグ名
レジストリの比較先	<objects><registry_object><hive>
製品情報	<objects><registry_object><key>
バージョン情報	<states><registry_state><value>

- 4) データベース管理者用に OVAL データベースのデータ入力・更新・削除ができる管理用ユーザインタフェースを開発すること。図 2.2-6 に OVAL データベース管理画面例を示す。

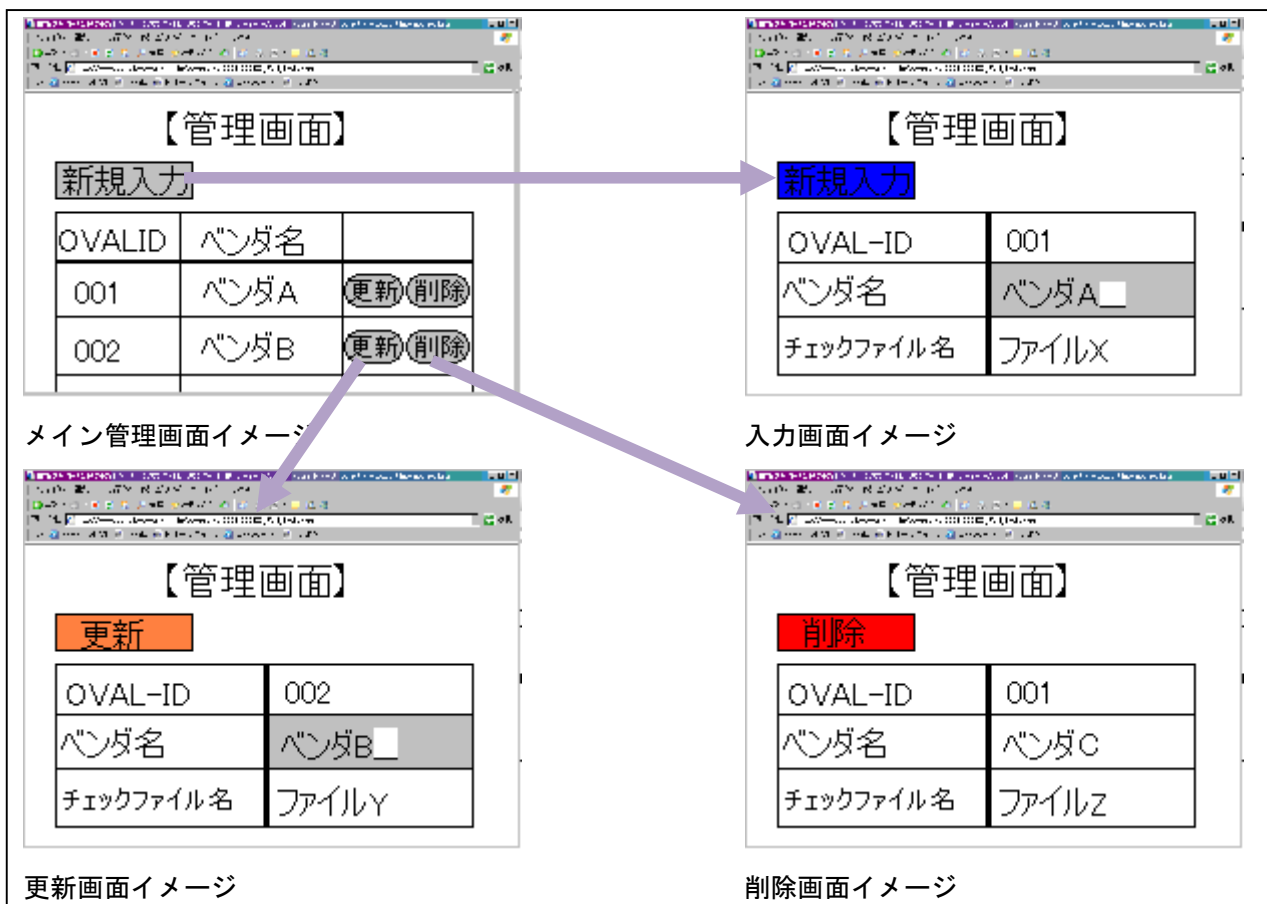


図 2.2-6 OVAL データベース管理画面例

- 5) バージョンチェッカからチェック対象とするアプリケーション情報の要求により、OVAL データベースから該当する最新バージョン情報を取得し、バージョンチェッカへ送信する OVAL 取得 API を開発すること。

図 2.2-7 に OVAL 取得 API の位置づけと処理の流れを示す。なお、OVAL 取得 API は公開できる仕様として作成し、他のウェブアプリケーションでも利用可能とする。

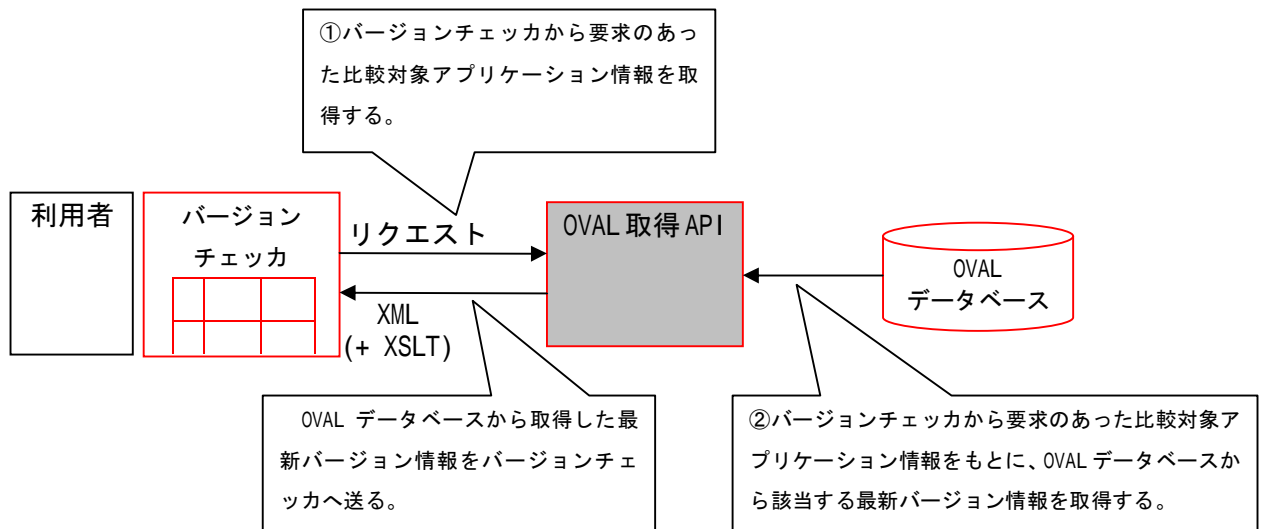


図 2.2-7 OVAL 取得 API の説明図

- 6) バージョンチェッカがチェック対象とするアプリケーション製品を増やしても容易に対応できるように、拡張を考慮した開発をすること。また、大量アクセス時のパフォーマンスについても考慮した開発をすること。

クライアント PC の OS のセキュリティ設定チェック機能（セキュリティ設定チェッカ）

利用者がウェブブラウザで MyJVN にアクセスした際に、クライアント PC の OS のセキュリティ設定項目が CCE データベースに格納されている IPA 推奨値となっているかどうかチェックする機能（セキュリティ設定チェッカ）を開発すること。

汎用的な OS (今回の OS は Windows とする) にはセキュリティ対策として、ログインパスワードの設定などがあるが、何文字で設定すれば安全か利用者自身が判断できない状態である。そこで、MyJVN バージョン 2 では、クライアント PC の OS 設定値と CCE データベースに格納されている IPA の推奨値を比較した結果と推奨対策を利用者に示すことでセキュリティを考慮した設定を推進する。

- 1) セキュリティ設定チェッカの画面遷移イメージを図 2.2-8 に示す。

利用者がセキュリティ設定チェッカの実行ファイルを起動すると、クライアント PC のログインパスワードの文字数や、一定時間操作しない場合の画面自動ロックの設定有無など、クライアント PC の OS でセキュリティ設定のチェックをする項目を選択する初期画面が表示される (①)。セキュリティ設定項目を選択し [START] ボタンをクリックすることにより、セキュリティ設定チェッカが、MyJVN の CCE データベースから取得した IPA の推奨値と、クライアント PC の OS 設定値 (Windows の場合、当該レジストリ値) を比較し、推奨値を満たしている場合 "OK"、推奨値に満たない場合 "NG" のチェック結果を表示する (②)。IPA 推奨値を満たしていない場合には、当該結果をクリックすることにより、セキュリティ設定を利用者に

促進する推奨対策を表示する (③)。

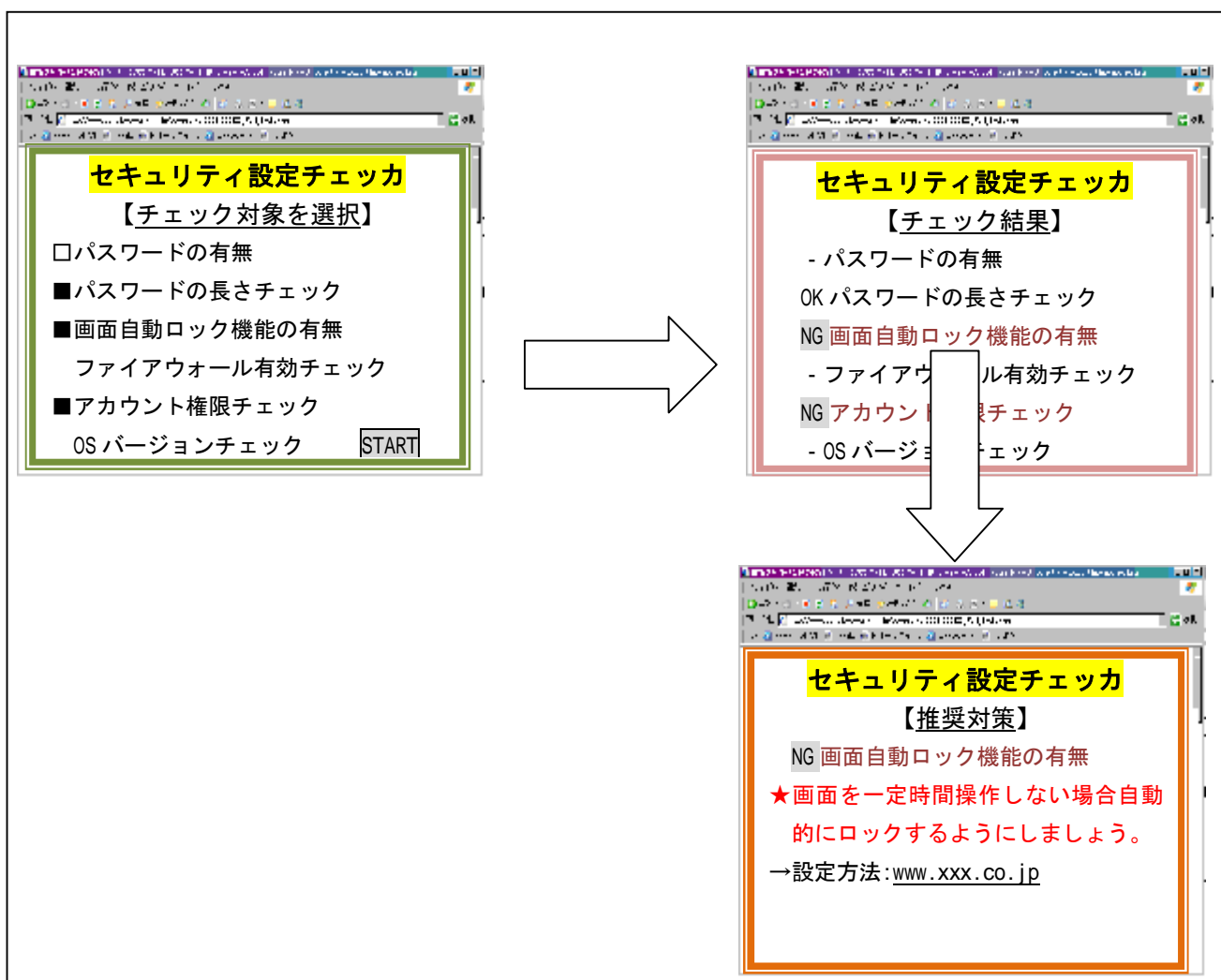


図 2.2-8 クライアント PC の OS のセキュリティ設定チェック機能 利用画面イメージ

セキュリティ設定チェッカは、クライアント PC 環境へ一時的にダウンロードされた後、java アプレット等によって実行される形態とし、チェック対象のバージョン情報などが外部へ送信されることなくチェック処理が行われることとする。

開発対象とするクライアント PC の OS は汎用的なものとし（今回の対象 OS は Windows とする）、セキュリティ設定項目はパスワード設定やログイン設定など実現可能なもの 7 項目以上とすること。開発にあたり対象となるセキュリティ設定項目などは IPA と協議の上決定すること。

- 2) セキュリティ設定チェッカでチェックするために利用する「CCE ID」、「表示種別」、「表示項目」、「チェック項目」、「推奨値」、「コメント」、「関連 URL」の情報を蓄積するデータベース機能（CCE データベース）を開発すること。

セキュリティ設定チェッカで用いる CCE データベース項目を表 2.2-3 に示す。

表 2.2-3 CCE データベース項目説明

項目名	項目説明	タイプ(必要桁数)
CCE ID	CCE で採番された ID を格納する	半角英数字 (15)
表示順	画面に表示する順番を格納する	半角英数字 (2)
OS 種別	確認する OS の種別を格納する。	半角英数字 (30)
表示項目	画面に表示するチェック項目名を格納する	漢字 (50)
チェック項目	セキュリティ設定確認を行う項目を格納する	半角英数字 (50)
推奨値	IPA 推奨値 (設定値) を入力する	半角英数字 (10)
コメント	推奨対策等の利用者へのメッセージを入力する	改行を含む漢字 (250)
関連 URL	コメントや設定方法等の補足説明用 URL を入力する	半角英数字 (50)

各項目や技術的な仕様などは、規定が標準化されている CCE を使うこと。

CCE より取得する各項目は、MITRE 社の CCE のウェブサイト

(http://cce.mitre.org/lists/cce_list.html)から、セキュリティ設定項目に関連する CCE のデータを取得し、② 1)で IPA と協議の上決定したセキュリティ設定項目を格納する。

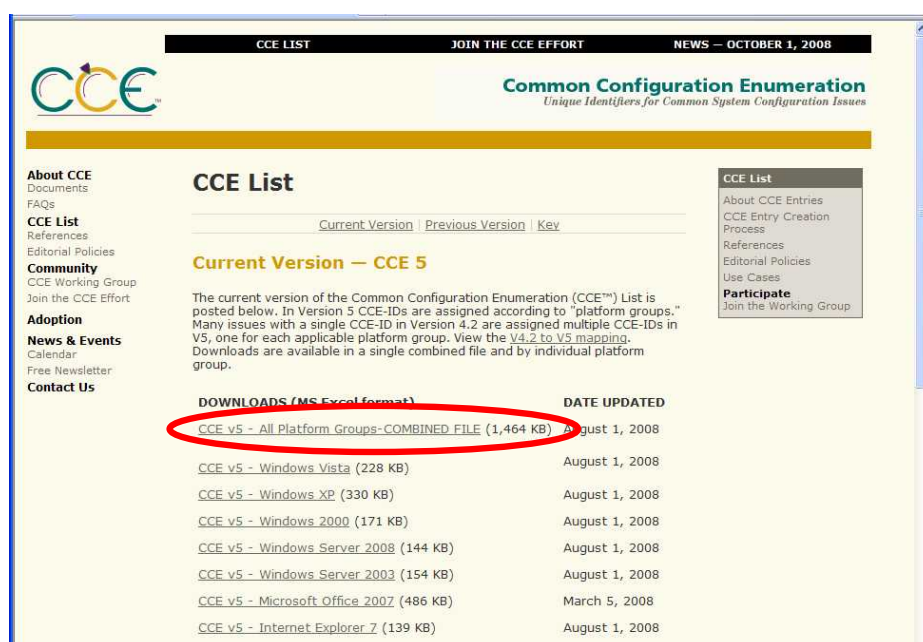
CCE データベース項目の「CCE ID」には、図 2.2-10 の CCE ID を格納する。

CCE データベース項目の「表示順」は、セキュリティ設定チェックが画面表示する順番 "01"、"02" ~ "99" を格納し、表示しない項目は空白 (" ")とする。

CCE データベース項目の「OS 種別」には、セキュリティ設定のチェックを行うプラットフォーム (クライアント PC の OS 種別) を格納する。

CCE データベース項目の「表示項目」には、図 2.2-10 ②の CCE Description の日本語訳を格納する。

CCE データベース項目の「チェック項目」には、図 2.2-10 の CCE Technical Mechanisms の(1)を格納する。



表示された CCE リスト画面の当該リンクをクリックすることにより、該当バージョンの情報が閲覧・保存できる。

図 2.2-9 CCE リスト画面

CCE ID	Old v4 CCE Id	CCE Description	CCE Parameters	CCE Technical Mechanisms
73	CCE-814	The "Users Prompted to Change Password Before Expiration" policy should be set correctly.	(1) number of days prior to expiration	(1) HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon>PasswordExpiryWarning (2) defined by Local or Group Policy
74	CCE-92	The "Shut Down system immediately if unable to log security audits" policy should be set correctly.	(1) enabled/disabled	(1) HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\CrashOnAuditFail (2) defined by Local or Group Policy
75	CCE-576	The "Digitally Sign Client Communication (Always)" policy should be set correctly.	(1) enabled/disabled	(1) HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\RequireSecuritySignature (2) defined by Local or Group Policy
76	CCE-519	The "Digitally Sign Client Communication (When Possible)" policy should be set correctly.	(1) enabled/disabled	(1) HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySignature (2) defined by Local or Group Policy
77	CCE-474	The "Digitally Sign Server Communication (Always)" policy should be set correctly.	(1) enabled/disabled	(1) HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignature (2) defined by Local or Group Policy

① : OVAL ID
 ② : CCE Description
 ③ : CCE Technical Mechanisms(1)

図 2.2-10 Excel ファイルの内容

- 3) セキュリティ設定チェックがクライアント PC 内の情報と比較する際に用いる手順を以下に示す。
 - ・ 図 2.2-8 ①の「チェック対象を選択」画面で、セキュリティ設定項目（表示項目）を、CCE データベース項目の「表示順」に従い昇順で表示する。「表示順」が空白(" ")の場合は非表示とする。
 - ・ 利用者により選択されたチェック対象のセキュリティ設定項目の情報をもとに、「チェック項目」に記載されている内容をクライアント PC 内のレジストリファイルより探し、そのレジストリに格納されている値（OS 設定値）と、CCE データベースの「推奨値」を比較する。
 - ・ 比較した結果、図 2.2-8 ②のようにクライアント PC 内の OS 設定値が CCE データベースの「推奨値」を満たしている場合は "OK" を表示し、「推奨値」を満たしていない場合は "NG" を表示する。
 - ・ CCE データベースの「推奨値」を満たしていない場合（"NG" のとき）、利用者により当該チェック設定項目（表示項目）をクリックした際に、図 2.2-8 ③のように推奨対策として CCE データベースの「コメント」と「関連 URL」を表示する。

- 4) データベース管理者用に CCE データベースのデータ入力・更新・削除ができる管理用ユーザインタフェースを開発すること。図 2.2-11 に CCE データベース管理画面例を示す。

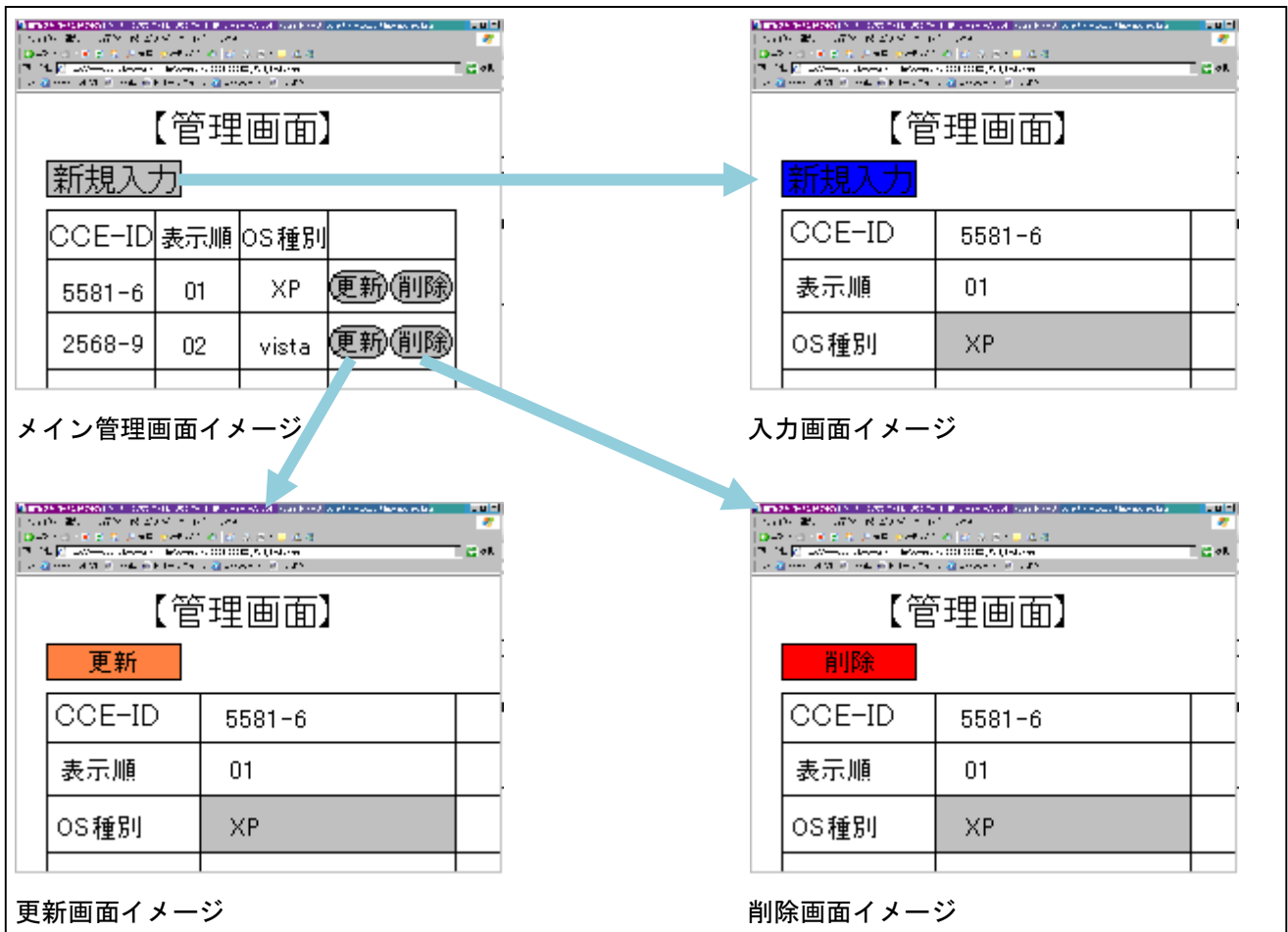


図 2.2-11 CCE データベース管理画面例

- 5) セキュリティ設定チェッカからチェック対象とするセキュリティ設定項目の要求により、CCE データベースより該当する IPA 推奨値、コメント、関連 URL を取得し、セキュリティ設定チェッカへ送信する CCE 取得 API を開発すること。

図 2.2-12 に CCE 取得 API の位置づけと処理の流れを示す。なお、CCE 取得 API は公開できる仕様として作成し、他のウェブアプリケーションでも利用可能とする。

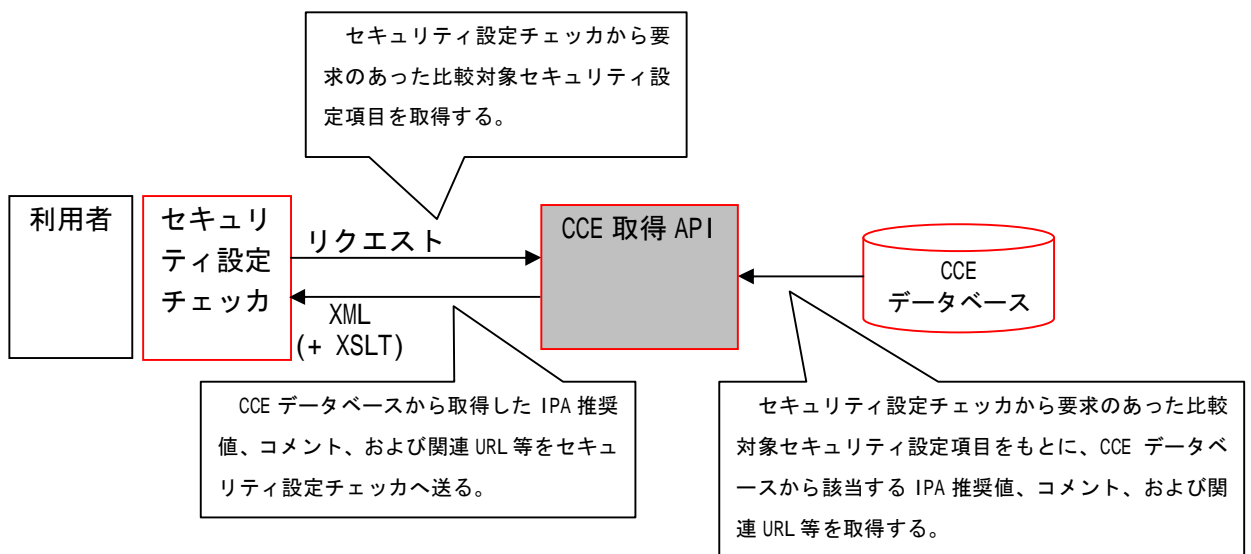


図 2.2-12 CCE 取得 API 説明図

- 6) セキュリティ設定チェックがチェック対象とするセキュリティ設定項目を増やしても容易に対応できるように、拡張を考慮した開発をすること。また、大量アクセス時のパフォーマンスについても考慮した開発をすること。

JVN iPedia 最新版から MyJVN の DB サーバへの共通プラットフォーム一覧受取り機能
JVN iPedia 最新版 の CPE マスターデータからレプリケーションされた CPE データを、MyJVN の DB サーバへ受取る機能を開発すること。

なお、これらの機能について、同等以上の機能があれば提案してください。

開発にあたり、すべての項目は IPA と協議の上決定すること。

また、MyJVN バージョン 1 の詳細を知りたい場合は、IPA セキュリティセンターまでお問い合わせください。

2. 3 作業環境等

本公募における作業環境等の要件は以下のとおりです。

- ◆ 開発（構築）、テスト等に係る作業については、提案者が用意する場所にて実施すること。
- ◆ 開発（構築）、テスト等に必要な機器等は、提案者が用意すること。
- ◆ 開発（構築）、テスト等に使用する機器等については、ウィルス対策、セキュリティホール対策等、十分なセキュリティ対策が実施されていること。

2. 4 基本設計及び詳細設計

上記「2. 2 機能要件」に記述されている要件を満たす機能の構築に向けた基本設計及び詳細設計を行います。設計にあたっては、OVAL や CCE を理解すること。OVAL、CCE は最新版に対応できるようにすること。開発にあたっては日本語環境に配慮すること。

2. 5 開発・構築

上記「2. 4 基本設計及び詳細設計」に基づく開発・構築を行います。

2. 6 システム試験

上記「2. 5 開発・構築」の作業中または作業後にシステム試験を行います。

- ◆ 試験計画を立案し、本番稼動前に適切な試験を実施すること。
- ◆ IPA の運用管理者によるユーザ試験を実施すること。
- ◆ セキュリティ問題に対する十分なテストを行い、発見された問題について対応し解消すること。
- ◆ 本番稼動環境と同等の利用環境下において、開発したシステムの操作作業を行い、操作性や品質、セキュリティ面を含めて、ユーザが目的の用途として利用可能な状態が保たれているか、十分な確認作業を行うこと。
- ◆ 開発したシステムによる既存の関係システム等の障害回復等に留意し、十分な信頼性が確保され

ているか確認作業を行うこと。

2. 7 移行・導入等支援

開発（構築）したシステムの本番稼働環境への移行・導入等作業についての要件は以下のとおりです。

- ◆ 本番稼働環境への移行・導入の支援を行うこと。

3. 規模・性能等要件

本公募で開発（構築）するシステムの規模や性能等についての要件は以下のとおりです。

- ◆ 本番稼働環境と同等の利用環境下において、「1. 1 業務の概要」または「2. 2 機能要件」で示した基準以上での操作等が可能であること。

4. 信頼性等要件

4. 1 信頼性・事業継続性要件

本公募で開発（構築）するシステムの信頼性や事業継続性等についての要件は以下のとおりです。

- ◆ 24 時間 365 日稼働可能であること。
- ◆ 障害時における復旧手順書などを作成すること。
- ◆ IPA で登録したデータを定期的にバックアップすること。
- ◆ 品質を保証するための品質検査を実施、および品質検査報告書を提出すること。

5. 情報セキュリティ要件

本公募における情報セキュリティに関する要件は以下のとおりです。

- ◆ 公募要領「2. 応募要件（5）その他 ①」に従って作業を行うこと。
- ◆ 設計・開発前にセキュリティ対策を IPA に提示し、承認を得てから作業を行うこと。

6. 稼働環境

6. 1 全体構成

本公募の納入成果物は以下の稼働環境で利用することを想定しています。

機器名称	主な機能
ウェブサーバ	MyJVN の機能を公開するサーバ
DB サーバ	MyJVN のデータが入るデータベース OVAL データベース(今回開発範囲) CCE データベース(今回開発範囲)

詳細なハードウェア・ソフトウェア構成の情報が必要である場合、IPA にお問い合わせください。

7. 保守要件

本公募の納入成果物についての保守に関する要件は以下のとおりです。

- ◆ 納入成果物の瑕疵に対して納入後 1 年間、無償保証のできる体制を用意すること。

8. 作業の体制及び方法

8. 1 プロジェクトの体制等

本公募における業務を行う場合のプロジェクト体制に関する要件は以下のとおりです。

- ◆ 公募要領「2. 応募要件（4）要員の要件」に従った体制とすること。
- ◆ ソフトウェア製品の脆弱性および、システムの開発作業について十分な知識を有するものが責任ある立場でプロジェクトにあたること。
- ◆ XML アプリケーション、Web アプリケーション、データベースの開発経験を有すること。

8. 2 プロジェクト管理等

本公募における業務を行う場合のプロジェクト管理に関する要件は以下のとおりです。

- ◆ 2009年2月27日(金)の中間納品、および2009年11月に本番環境での運用開始を目標とした計画を立てること。
- ◆ 原則としてIPAと合意したプロジェクト計画書に従って作業を実施すること。
- ◆ 必要に応じて適宜ミーティング等によりIPAと作業内容の調整及び報告を行うこと。
- ◆ 公募要領「2. 応募要件（5）その他 ②」及び「4. 契約条件（7）機密の保持」に従って作業を実施すること。また、そのために必要な措置を講ずること。

9. 条件等

本公募における業務を行う場合のIPA側が事前事後に負担する事項等があれば提示してください。

- ◆ 作業を実施するにあたり、前提条件等がある場合には提案時点でIPAに示すこと。
- ◆ 作業開始前・作業中にIPA側が負担する内容・物品等がある場合には、提案時点でIPAに示すこと。
- ◆ 作業完了後に、IPAが継続的に運用していくために必要な内容や条件等がある場合には提案時点でIPAに示すこと。
- ◆ 脆弱性対策パッチの簡易型バージョンチェック機能は中間納品とし、納入日は2009年2月27日(金)とする。中間納品物はIPAで公開する予定。なお、OVALやCCEの使用許諾等はIPAがあらかじめ了承を得ておく。

以上