JAEA-Technology
2011-030

J-PARCにおける情報セキュリティ脆弱性リスク管理システムの開発

Development of Information Security and Vulnerability Risk Management System for J-PARC

石川 弘之　舘 明宏　村上 直

Hiroyuki ISHIKAWA, Akihiro TATE and Tadashi MURAKAMI

J-PARC センター
情報システムセクション

Information System Section
J-PARC Center

February 2012

Japan Atomic Energy Agency　日本原子力研究開発機構

JAEA-Technology

本レポートは独立行政法人日本原子力研究開発機構が不定期に発行する成果報告書です。
本レポートの入手並びに著作権利用に関するお問い合わせは、下記あてにお問い合わせ下さい。
なお、本レポートの全文は日本原子力研究開発機構ホームページ（http://www.jaea.go.jp）
より発信されています。

独立行政法人日本原子力研究開発機構　研究技術情報部　研究技術情報課
〒319-1195　茨城県那珂郡東海村白方白根 2 番地 4
電話 029-282-6387, Fax 029-282-5920, E-mail:ird-support@jaea.go.jp

This report is issued irregularly by Japan Atomic Energy Agency
Inquiries about availability and/or copyright of this report should be addressed to
Intellectual Resources Section, Intellectual Resources Department,
Japan Atomic Energy Agency
2-4 Shirakata Shirane, Tokai-mura, Naka-gun, Ibaraki-ken 319-1195 Japan
Tel +81-29-282-6387, Fax +81-29-282-5920, E-mail:ird-support@jaea.go.jp

© Japan Atomic Energy Agency, 2012

JAEA-Technology 2011-030

J-PARC における情報セキュリティ脆弱性リスク管理システムの開発

日本原子力研究開発機構
J-PARC センター 情報システムセクション
石川 弘之*[1]・舘 明宏※・村上 直*[2]

（2011 年 10 月 14 日受理）

大強度加速器研究施設（J-PARC: Japan Proton Accelerator Research Complex）では、利用者の研究活動やコミュニケーションの利便性向上を図るため、イントラネットワーク（以下、JLAN と略す）を設置している。JLAN では、各種情報セキュリティ機器を配置することでセキュリティ維持に努めている。情報セキュリティ機器により JLAN は守られているが、外部に対して情報公開やサービスを提供しているサーバは、悪意を持った人から不正アクセスを受ける危険性が高い。

万一不正アクセスされた場合、データの改ざんや情報漏えいの被害に遭うことが考えられる。さらには、攻撃を受けたサーバが悪意を持った者により操作され、外部の情報機器を攻撃してしまう危険性がある。不正アクセスは、概ねターゲットとなるサーバの脆弱性を突いて行われるため、サーバへ十分な情報セキュリティ対策を施すことが求められる。脆弱性検査ツールを用いたサーバへの検査は、脆弱性対策に極めて有効な手段の一つであるが、単に脆弱性検査を実施するだけでは不十分である。脆弱性検査結果を元に脆弱性対策が実施され、かつこれらが継続的に実施されることが重要である。

このような点に着目し、単に脆弱性検査を実施するツールではなく、実際の脆弱性対策を実施する人自らが脆弱性に対するリスク管理を行い、脆弱性対策の PDCA(Plan-Do-Check-Action)サイクルを回すことが可能なセキュリティ脆弱性検査システムを開発した。本書では、この開発における技術や創意工夫について報告する。

J-PARC センター：〒319-1195　茨城県那珂郡東海村白方白根 2-4
※技術開発協力員
＊1 富士通株式会社（2011 年 9 月 30 日まで情報システムセクションに所属）
＊2 高エネルギー加速器研究機構　計算科学センター

JAEA-Technology 2011-030

Development of Information Security and Vulnerability Risk Management System for J-PARC

Hiroyuki ISHIKAWA*[1], Akihiro TATE※ and Tadashi MURAKAMI*[2]

Information System Section, J-PARC Center
Japan Atomic Energy Agency
Tokai-mura,Naka-gun,Ibaraki-ken

(Received October 14,2011)

In J-PARC (Japan Proton Accelerator Research Complex) we have set up intra-network (internal network, we will abbreviate it as JLAN, below) to support research activity and communication among users. In JLAN, we set up various kinds of security devices to keep JLAN secure. However, the servers which provide information or service to public are still in danger of being accessed illegally.

If there is an illegal access, that may cause defacement of data or information leak. furthermore, the victim servers are manipulated by the malicious attackers, and they themselves attack the external information equipments. Vulnerability of servers enables unauthorized access. So, vulnerability test with use of a vulnerability tool is one of the most effective ways to take measures for vulnerability of the equipments. However, it is not enough to just conduct a vulnerability test. It is also essential for information security to take measures to cover constantly for the vulnerability of servers.

We focused on the points above, and developed the vulnerability testing system for security. It is not only a testing tool for the vulnerability of servers, but also management system which enables the server administrators in charge of taking measures for vulnerabilities to manage risks and handles PDCA (Plan-Do-Check-Action) cycles as countermeasure for vulnerability. In this paper, we report the technologies and ingenuities for the development of the above system.

Keywords: Information System, Vulnerability, Risk Management

※Collaborating Engineer

＊1 Fujitsu Ltd. (Information System Section until September 30, 2011)

＊2 High Energy Accelerator Research Organization Computing Research Center

目次

1. 序論 1
2. 課題と目標設定 2
2.1 これまでの課題 2
2.2 目標設定 3
3. 情報セキュリティ脆弱性リスク管理システム 5
3.1 システム概要 5
3.2 システムで提供される機能 6
3.3 J-PARC 版ポータル 7
3.4 Add-On サブシステム 8
3.5 他システムとの連携機能 16
3.6 開発における創意工夫 17
4. システムの評価 28
4.1. 要求定義の評価 28
4.2. 出力の評価 29
5. 今後の展開 34
6. まとめ 34
謝辞 34
参考文献 35
付録 1.「情報セキュリティ脆弱性リスク管理システム」の利用者画面イメージ 36

Contents

1. Introduction 1

2. Challenges and target settings 2

2.1 Challenges 2

2.2 Target settings 3

3. Information Security and Vulnerability Risk Management System 5

3.1 Brief overview of the system 5

3.2 Functions provided with the system 6

3.3 J-PARC portal 7

3.4 Add-on subsystem 8

3.5 Functions to cooperate with other systems 16

3.6 Ingenuities in development of the system 17

4. System evaluation 28

4.1. Evaluation by requirement definition 28

4.2. Evaluation by output 29

5. Future plans 34

6. Conclusion 34

Acknowledgment 34

References 35

Appendix 1 Screen captures of Information Security and Vulnerability Risk Management System 36

図一覧

図 1. 情報セキュリティ脆弱性リスク管理システム全体構成（概要） 5
図 2. ポータルシステムの主要な提供機能 6
図 3. Add-On サブシステム部及び外部連携システム全体構成 8
図 4. ホストごとの脆弱性検査結果時系列表示 [1] 9
図 5. ホスト毎の脆弱性検査結果詳細表示 [1] 10
図 6. 脆弱性 ID 毎の詳細情報表示 [1] 10
図 7. 管理対象ホストヒストグラム表示 [1] 11
図 8. 管理対象ホストチャートグラフ表示 [1] 11
図 9. 管理対象ホスト一覧表示 12
図 10. 管理対象ホスト統計情報 [1] 12
図 11. CVSS 分析グラフ [1] 13
図 12. ソーシャルグラフを用いた脆弱性検査結果表示例 [2] 14
図 13. CVE 及び脆弱性検査用シグネチャ登録状況表示 14
図 14. 死活確認及び脆弱性検査結果履歴の一覧表示画面 15
図 15. 公開前脆弱性検査事前案内メール送信画面 15
図 16. アクセス履歴及びリアルタイム表示 [1 3] 16
図 17. CVE 番号による脆弱性検知数 [1] 22
図 18. 不正アクセス履歴の可視化例 [1] 25
図 19. リアルタイムによる不正アクセスの可視化例 [3] 25
図 20. 検査対象機器のスコア分布図 [1] 29
図 21. 異なる指標による脆弱性検査結果比較 [1] 30
図 22. CVSS 指標による脆弱性の基本評価基準の可視化例 [1] 31
図 23. 機器管理者が管理する全機器の脆弱性情報 [2] 32
図 24. 脆弱性情報の保有関係 33

[1] 図 4,5,6,7,8,10,11,16,17,18,20,21,22 については AmChart[10]を利用してグラフ化を行った。

[2] 図 12,23 については Flash Force Directed Layout Graph[8]を利用して可視化を行った。

[3] 図 16,19 については Hummingbird[9]を利用して可視化を行った。

表一覧

表 1. 具体的な課題 2
表 2. 目標設定 3
表 3. 「情報セキュリティ脆弱性リスク管理システム」のシステム要件 4
表 4. J-PARC 版ポータルの機器管理者向け機能 7
表 5. Add-On サブシステム及び外部連携システムによって出力可能なグラフ一覧 19
表 6. CVSS による情報セキュリティ基準の特徴 20
表 7. 「情報セキュリティ脆弱性リスク管理システム」で採用している評価指標 21
表 8. 情報提供元による RSS 情報提供一覧 24
表 9. ポータルと Add-On サブシステムの機能比較 28
表 10. 脆弱性情報の保有状況 33

1. 序論

インターネットの普及やITの技術向上により、年々取扱う情報量が増加している。これにより多種多様な情報を扱う機会が増え、ほしい情報に簡単に手が届くようになり多くの恩恵を受けられるようになった。その反面、情報の取扱いを間違えると不正アクセスによる情報漏えいや情報の改ざんといった情報セキュリティインシデント[4]を引き起こしかねない。

情報セキュリティインシデントを起こした場合、いかに迅速に対応し収束させて問題解決できるかが重要であるが、根本的な原因が解決されなければ、情報セキュリティインシデントの発生数を減らすことができない。情報セキュリティインシデント自体を起こさないためにも、根本原因を除去して再発予防できるようにする必要がある。

外部に情報を公開する WEB サーバシステム構築手順の例を考える。システム構築者は業務サービスに合わせ、OS 及びソフトウェアを選択し、その上で動作する業務アプリケーションを作成する。このとき、システム構築者は情報セキュリティインシデントを起さないように、より脆弱性対策が施された版数のソフトウェアを採用する。さらに脆弱性対策を行うため、ベンダから提供される OS やソフトウェアの修正パッチを適用する。このような定石により健全で安全なシステムを構築することができる。

しかし、一度健全なシステムを構築してしまうと健全な環境が継続していると錯覚してしまい、脆弱性が指摘されるまでは、脆弱性対策が行われなくなる可能性がある。

J-PARC では、システム構築時の公開前情報セキュリティ脆弱性検査と、運用開始後の定期的な情報セキュリティ脆弱性検査を実施できるようにした。定期的に実施する情報セキュリティ脆弱性検査により、システム構築時～運用終了までのライフサイクル期間中、常に脆弱性の指摘を受けることができる。また、脆弱性情報の見せ方を工夫することで、システム構築者やシステム運用管理者自身の脆弱性への意識を高揚させ、脆弱性対策が実施されるシステムを提供できた。

[4] セキュリティインシデント: 情報管理やシステム運用に関して管理上の脅威となる現象や事案

2. 課題と目標設定

2.1 これまでの課題

J-PARC では、平成 19 年から情報セキュリティ脆弱性検査を実施している。当時は、J-PARC 計画の建設期であったこともあり、外部に対してサービスを提供している機器は 10 台程度であった。また、情報セキュリティ脆弱性検査の実施回数頻度が低かったこともあり、脆弱性検査は JLAN 管理者が実施していた。

当時採用した脆弱性検査ツールは、脆弱性検査対象機器の設置場所に持込んでも検査が可能なように、ノート PC 上にソフトウェアタイプの商用ツールをインストールしていた。このソフトウェアは、クライアント系の Microsoft Windows OS で動作するため、比較的容易に操作を行うことができた。しかしこの商用ツールは、使用 OS のバージョン制限（Windows XP Service pack 1a までサポート）があったため、OS アップデート（Windows Update）が適用できず、OS 自身のセキュリティ維持ができない状況であった。そのため、ノート PC の情報セキュリティを維持しつつ、情報セキュリティ脆弱性検査を実施するには、ノート PC に F/W 機器を接続して不正アクセス対策を行う必要が出てきた。また、脆弱性検査を実施しているうち、さらに機能面や運用面で課題がでてきた。表 1に具体的例を示す。

表 1. 具体的な課題

カテゴリ	課題
機能	① 脆弱性は“Low”、“Medium”、“High”の３つのレベルに分類されている。分類が少ないため、同一レベル内の脆弱性でぞれぞれの危険度の差がわからない。 ② 一般に脆弱性リスクは時間とともに変化するが、使用している脆弱性検査ツールは固定指標のため、時間が経過するとリスクの差異が生じてくる。 ③ 保有している脆弱性情報に対する検索機能が提供されていない。このため、どのような脆弱性情報がどの程度登録されているか確認できない。 ④ 脆弱性検査対象者が自身で脆弱性検査を実施できない。 ⑤ 脆弱性検査対象者に対して、メール（Push 型）による脆弱性検査結果を通知できない。 ⑥ 脆弱性検査対象者が自身で脆弱性検査結果を取り出せない。 ⑦ 脆弱性検査結果データを元に統計情報の可視化ができない。
運用	⑧ 脆弱性検査ツールがサポートする OS 制限（Microsoft Windows XP SP1a までが製品組み合わせ条件となる。）ただし、Microsoft 社のサポートが終了しているため、OS のアップデートが実施できない。このため、結果的に OS のメーカーサポートが受けられない。 ⑨ 脆弱性検査は概ね DMZ に設置された機器に対して実施している。一方、脆弱性シグネチャの更新は、外部に公開されていないネットワークセグメントから実施している。JLAN では、JLAN 接続機器がどのネットワークセグメントに属しているかを管理しているため、その都度ネットワーク接続先変更申請手続きを行わなければならず附帯作業で手間や時間がかかる。 ⑩ 同時並列による脆弱性検査ができないため、複数機器に対して脆弱性検査を実施すると検査に時間がかかる。 ⑪ 脆弱性検査実施する際の運用側の作業負荷が高く、検査対象機器の脆弱性状況を継続的に把握できていない。同様に脆弱性情報を把握できていないため、利用者に対しても情報提供できていない。

2.2 目標設定

2.1 に示すように平成 19 年から実施してきた情報セキュリティ脆弱性検査に、機能面と運用面で課題がでてきた。

平成 20 年 12 月の J-PARC 供用開始後、J-PARC 利用者が一気に増加することが予想されていたこともあり、後継の情報セキュリティ脆弱性検査システムに更新する必要がでてきた。そこで、平成 20 年 6 月 後継の脆弱性検査システム検討に着手した。

当時使用していた商用ツールの脆弱性検査結果レポート機能は脆弱性危険度を表す分類が少ないものの、脆弱性情報（危険度、放置した際の影響度、対処方法）を通知することができることから、既存ツールとフリーウエアの情報セキュリティツールを組合せて検討を進めていた。

一方、J-PARC の共同運営を行っている高エネルギー加速器研究機構（KEK）では、自前で開発した DMZ User's Portal[1][2][3]を用いて、機器管理者自らが脆弱性診断する運用が既に行われていた。機能、システム運用性に加えこれまでの運用実績から、DMZ User's Portal をベースに脆弱性検査システムを整備することにした。ただし、J-PARC と KEK は別組織であるため情報セキュリティポリシーも異なる。このことから、J-PARC 情報セキュリティポリシーに沿ったカスタマイズを施す必要があった。

また、序論でも記述しているが、一度セキュアな環境を構築した後は脆弱性対策が疎かになりがちである。この状況では情報セキュリティインシデントがいつ発生してもおかしくない。重要なことは、脆弱性対策を継続して実施すること、さらには情報セキュリティインシデントが発生する前に未然防止策をどうとるかである。このためには、機器管理者に対して脆弱性検査結果を効果的に見せる方法、さらには、提供された情報を元に機器管理者が自らの情報セキュリティレベルを認識してもらう施策が必要である。そして、高い情報セキュリティの確保に結びつくプロセス改善の仕組みを提供していくことである。

これらと表 1を踏まえ、表 2の目標設定を行った。さらに、目標から今回開発した情報セキュリティ脆弱性リスク管理システムのシステム要件として整理した。表 3にシステム要件を示す。

表 2. 目標設定

カテゴリ	目標設定	課題[5]
機能	a. 脆弱性に対して複数のリスク指標を用いて情報提供を行う。	①②
	b. 検出できる脆弱性、検出できない脆弱性の情報提供を行う。	③
	c. 定期的に自動で実施する脆弱性検査に加え、利用者がいつでも実施できる手動検査を提供する。	④
	d. PUSH 型で脆弱性検査結果を情報提供する。	⑤⑥
	e. 脆弱性検査結果を元にデータマイニングを行い、新たな情報提供を行う。	⑦
運用	f. オペレーションが複雑にならない環境を提供する。	②③⑤
	g. システム運用者側の運用負荷がかからないシステムを提供する。	⑧⑨⑩⑪

[5] 表 2、課題欄は表 1と対応している。

表 3. 「情報セキュリティ脆弱性リスク管理システム」のシステム要件

具体的なシステム要件
a. 脆弱性に対して複数のリスク指標を用いて情報提供を行う。 ・ リスク指標として時間の経過とともにリスクが変化する可変指標を採用する。ただし、可変指標のみであると、そもそもの脆弱性発生時点のリスクが把握できなくなるため固定指標（CVSS 基本値[6]）によるリスク評価も行えるようにする。これらの指標は、リスクの危険度差が判別できるように、数値による定量的な指標を採用する。 ・ 定量的指標だけだと数字だけで判断することになるが、実際のリスクは個々のネットワーク環境により異なるため、リスク（数値）が低い場合でも、その環境配下では高い脆弱性であると判定できるようにする。また、JLAN の個別環境を考慮した定性的な指標による判定ができるようにする。 b. 検出できる脆弱性、検出できない脆弱性の情報提供を行う。 ・ 検出できる脆弱性は、脆弱性 DB に登録されている脆弱性に依存する。脆弱性 DB で検出できる脆弱性及び検出できない脆弱性を明確化し情報提供する。 c. 定期的に自動で実施する脆弱性検査に加え、利用者がいつでも実施できる手動検査を提供する。 ・ 脆弱性は日々発見されている。また、検査対象システムの環境変更作業により、脆弱性保有状況が変わる。よって、脆弱性検査は継続的に実施することに意義がある。定期的（毎週）に自動で脆弱性検査を行うとともに、機器の環境変更後に利用者自身が手動で脆弱性検査を実施できるようにする。 d. PUSH 型で脆弱性検査結果を情報提供する。 ・ 検査対象システムの環境変更作業がなく、同じ脆弱性情報による検査を行っている限り、新規の脆弱性が検出されることは少ない。同じ情報しか得られないと、利用者は脆弱性検査結果を確認する手間が煩わしくなり脆弱性検査結果を取得しなくなる。このようなことを防止するため、必要最小限の情報に絞って脆弱性検査結果をメール通知できるようにする。 e. 脆弱性検査結果を元にデータマイニングを行い、新たな情報提供する。 ・ 脆弱性検査では脆弱性結果を得られるだけでなく、データを積上げることで傾向が見えてくる。利用者への啓蒙としてデータマイニング結果を可視化して、情報提供を行う。 f. オペレーションが複雑にならない環境を提供する。 ・ アプライアンス製品は専用製品のため、豊富な機能を提供するとともに、脆弱性機能ひとつ見てもきめ細かな設定項目が用意されている。これらの機能を用いて脆弱性検査を実施するには、オペレーションが複雑で利用者向けになっていない。また、JLAN の情報セキュリティ脆弱性検査の運用では必要としない機能も存在する。このような状況で、アプライアンス製品に直接ログインして使用することはとても難しい。よって、利用しない機能やオペレーションを簡素化するため、KEK 版ツールをベースに構築する。 g. システム運用者側の運用負荷がかからないシステムを提供する。 ・ システム運用負荷がかからないように、運用実績のある KEK 版ツールをベースに構築する。 ・ モジュール保守性を確保するため、コア部分は J-PARC/KEK 同一プログラムとし、最小限の変更でどちらの環境でも対応が可能な事とする。

[6] CVSS 基本値:　脆弱性そのものの特性を評価する基準。この基準による評価結果は固定していて、時間の経過や利用環境の異なりによって変化しない。

3. 情報セキュリティ脆弱性リスク管理システム

3.1 システム概要

「情報セキュリティ脆弱性リスク管理システム」は、2006 年度より KEK で運用されている「DMZ User's Portal」（以下、KEK 版ポータルと略す）をベースに構築した。KEK 版ポータルは、商用ツールの脆弱性検査装置と連携し、KEK で実施される脆弱性検査で必要となる機能を提供する。機器管理者が自ら脆弱性検査を実施できるほか、脆弱性検査装置を使ってレポートを作成し、提出することができる。また、脆弱性検査装置が危険と判断する脆弱性について、機器管理者に定期的にメールで情報配信することができる。

J-PARC で実施する脆弱性検査で必要となる機能を KEK 版ポータルに組込み、J-PARC 向けにカスタマイズしたものを J-PARC 版ポータルとして提供する。また、J-PARC 版ポータルに組込めなかった機能は、J-PARC の独自拡張機能として同サブシステム（以下、Add-On サブシステムと略す）として提供する。さらに、この Add-On サブシステムは、情報セキュリティ関連の他システムと連携する機能を備えてリスク管理に重点をおいている。

これにより、「情報セキュリティ脆弱性リスク管理システム」は、リスク管理機能を大幅に強化し、脆弱性情報等の可視化を行い、機器管理者へわかりやすく提示する事が可能となった。

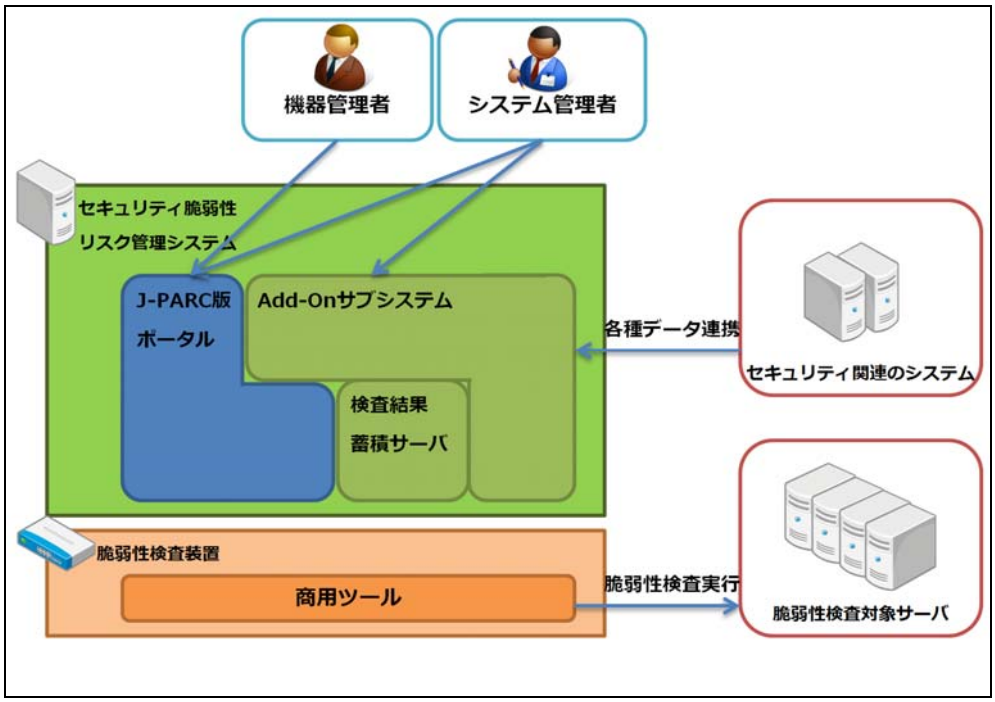


図 1. 情報セキュリティ脆弱性リスク管理システム全体構成（概要）

図 1にシステム全体の構成を示す。図 1で示したシステムは KEK 版ポータルと同じ位置づけにある J-PARC 版ポータル、J-PARC 独自拡張機能を提供する Add-On サブシステム及び検査結果蓄積サーバ、商用ツールの脆弱性検査装置から構成される。個々の機能については、3.3 項からくわしく説明する。

3.2 システムで提供される機能

「情報セキュリティ脆弱性リスク管理システム」は 4 つのシステムで構成されており、図 2で示す機能を主として提供している。

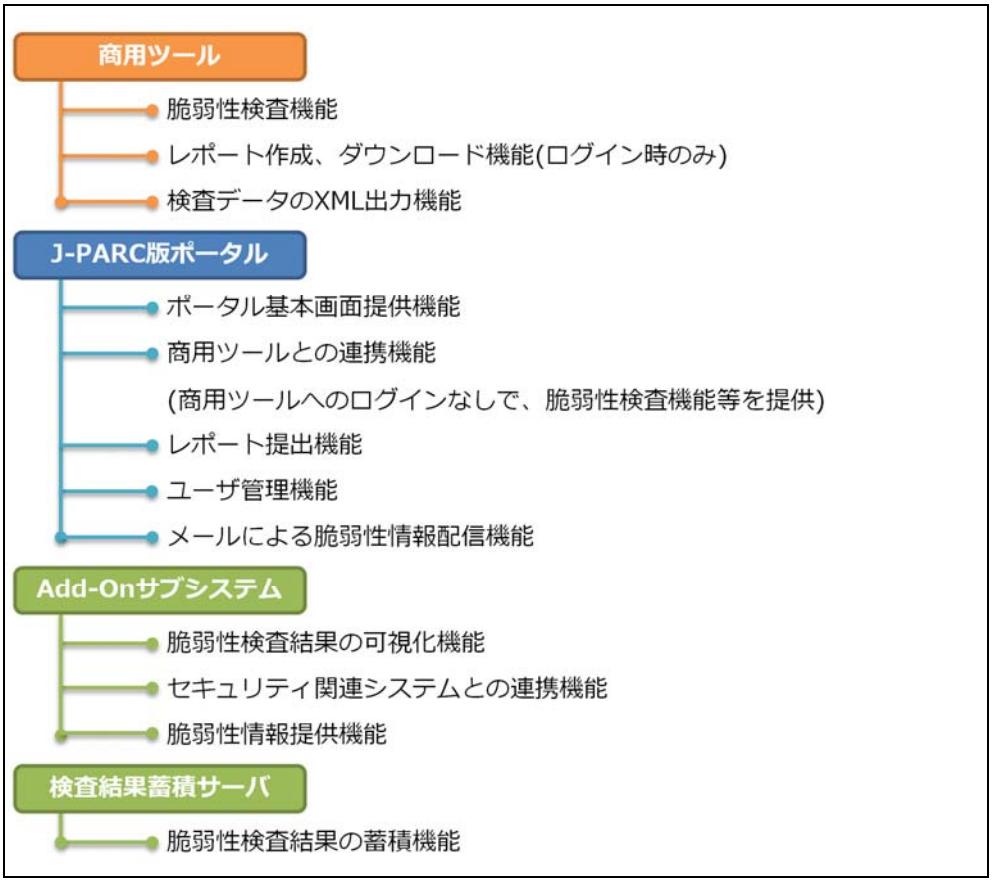


図 2. ポータルシステムの主要な提供機能

商用ツールは主として、脆弱性検査機能、検査データの出力機能、脆弱性検査結果レポートの作成機能、ダウンロード機能、検査データの XML[7]による出力機能を持っている。しかし、レポートの作成機能、ダウンロード機能については通常、商用ツールに直接ログインし操作する事が必要となってしまう。J-PARC 版ポータルはこれらの機能を商用ツールの画面上でなく、ポータルの画面上で提供するために商用ツールとの密な連携機能を持っている。その他、基本画面や、ユーザ管理機能、レポート提出機能等は J-PARC 版ポータルが提供している。Add-On サブシステムは商用ツールから出力された XML データを利用し、詳細な脆弱性検査結果、脆弱性分析結果の提供、また既に J-PARC で運用されている外部連携可能な他システムとの連携を行い、J-PARC 版ポータルでは提供しきれない情報をサーバ管理者へ提供している。検査結果蓄積サーバは Add-On サブシステムのデータソースとなる XML ファイルを格納し Add-On サブシステムへ提供している。

[7] XML Extensible Markup Language 文書やデータの意味や構造を記述するためのマークアップ言語の一つ

3.3 J-PARC 版ポータル

J-PARC 版ポータルは、KEK 版ポータルを元にして開発したものであり、「情報セキュリティ脆弱性リスク管理システム」の基本機能を提供する。J-PARC 版ポータルは機器管理者に対して、商用ツールや Add-On サブシステムが示す情報を統一的に提供するフロントエンドを担う（図 1, 図 2）。J-PARC 版ポータルはシステム管理者に対して、ユーザ管理機能を提供する。

J-PARC 版ポータルの機器管理者向け機能は表 4に示す通りである。各機能の内容とそれぞれの連携については、付録 1 に記した。

表 4. J-PARC 版ポータルの機器管理者向け機能

a) J-PARC 脆弱性リスク管理ポータルへのログイン （付録 1 Fig.2）
b) 機器管理者へのお知らせ （付録 1 Fig.3）
c) 脆弱性一覧の表示 （付録 1 Fig.4）
d) 管理する機器の一覧表示 （付録 1 Fig.5）
e) Add-On サブシステムへのリンク （付録 1 Fig.5）
f) 管理する機器の脆弱性検査実施 （付録 1 Fig.5）
g) 脆弱性検査結果の pdf レポートダウンロード （付録 1 Fig.6）
h) pdf レポートの提出 （付録 1 Fig.7）
i) パスワード変更 （付録 1 Fig.8）
j) 機器管理者へのメールによる脆弱性情報配信

a), f), g), i) は、商用ツールの機能を機器管理者に分かりやすい形で提供するものである。g) でダウンロードした pdf レポートは、h) により提出することができる。これらは、KEK 版ポータルの機能をそのまま利用している。

b), c), d), e), j) は、J-PARC と KEK の運用の違いが大きく出る箇所である。J-PARC 版ポータルではこれらについても KEK 版ポータルに基づいた機能を提供するが、モジュール保守性を確保するための工夫がなされている。これについては 3.6 - 4） で改めて述べる。

J-PARC 版ポータルはシステム管理者向けに、ユーザ管理機能を提供する。機器管理者と管理する機器の一覧を列挙したテキストファイルを用意し、これを読み込むことで、「情報セキュリティ脆弱性リスク管理システム」にユーザやホストを追加・変更・削除できる。この追加・変更・削除は、商用ツールへも同時に登録されるため、「情報セキュリティ脆弱性リスク管理システム」が管理するユーザやホストは、商用ツールにも同様に登録されている。この機能は、KEK 版ポータルの機能をそのまま利用している。

3.4 Add-On サブシステム

Add-On サブシステム部は大きく分けると、XML 解析システム、Add-On ツール群、検査結果蓄積サーバ、外部連携可能な他システムの 4 つのシステムで構成されている。図 3に全体のシステム構成を示す。

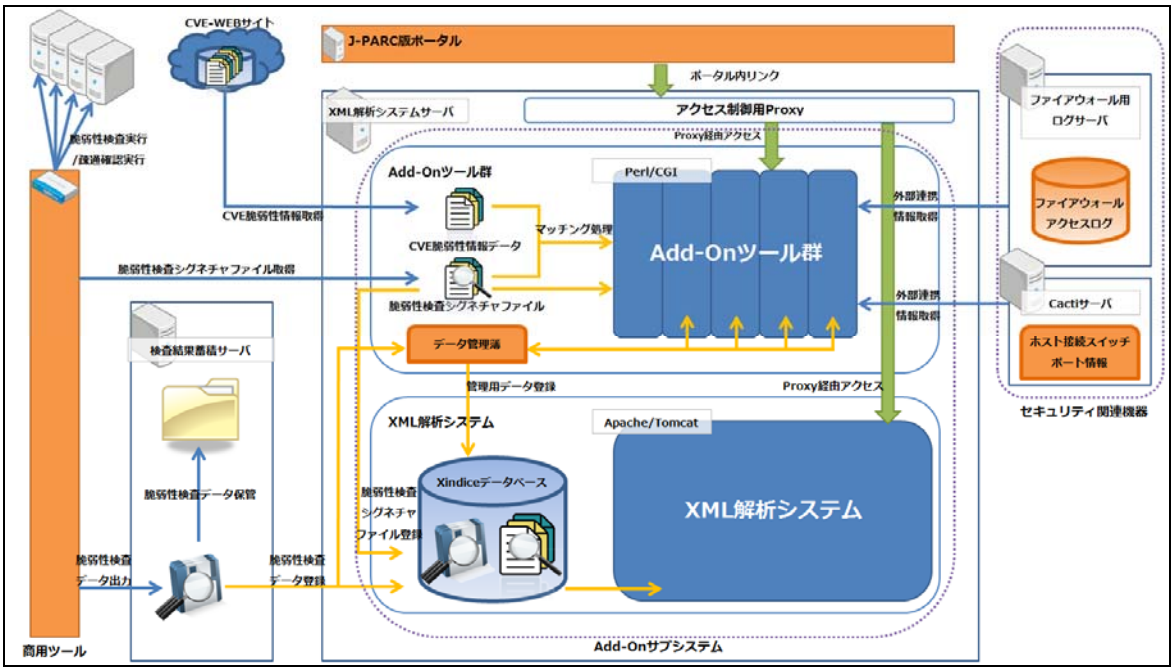


図 3. Add-On サブシステム部及び外部連携システム全体構成

Add-On サブシステムは検査結果蓄積サーバと XML 解析システム用サーバの２台のサーバで構成されている。商用ツールからの脆弱性検査データは全て検査結果蓄積サーバへ取り込まれ保存される。保存されたデータは同期プログラムによって一定時間ごとに XML 解析システムサーバへ転送され、XML 解析システムで使用している Xindice[12][8]データベースへ登録される。一部の情報については Add-On ツール群で使用しているデータ管理簿にも格納され、格納されたデータと WEB 上の画面から入力された情報を元に管理情報を作成し、それらも Xindice データベースへ登録する。

XML 解析システムではこれらの情報を元に、機器管理者/ホストごとに詳細な脆弱性検査結果や可視化した情報を提供し、Add-On ツール側でも、外部連携可能な他システムと連携した情報を利用することで、XML 解析システムを補完する形で情報を提供している。

[8] Xindice: Apache Software Foundation プロジェクトで開発されている XML データベース

3.4.1. XML 解析システム

XML 解析システムは Apache/Tomcat[13][9]を使用し構築されている。データベースは商用ツールが出力する脆弱性検査結果データ、脆弱性検査用シグネチャファイルが XML ファイルで出力されるため、XML データベースである Xindice を利用している。XML データベースの特徴は、XML ファイルをそのままの状態で取り込むことができ、それらに対して、Xpath 式[10]による柔軟な検索を行う事が出来る。取り込まれた XML ファイルを最大限活用して、J-PARC 版ポータルだけでは提供できていない詳細な検査情報や、検査結果のグラフ化等を行う。XML 解析システムは以下のような機能を提供している。なおユーザ向け提供画面については付録 1.にまとめて掲載した。

1） ユーザ向けの画面提供

a) 管理ホスト一覧表示

対象のユーザが管理しているホストの一覧を表示する。表示内容は最新の検査日時、ホスト名、IP アドレスに加えて、その際の検査スコア、J-PARC 固有脆弱性の保有状況、機器管理者情報が提供される。ホスト名、検査スコア欄にはリンクが用意されており、ホスト名を選択すると脆弱性検査結果時系列表示画面を表形式で、検査スコアを選択すると脆弱性検査結果時系列表示をグラフ形式で表示する。

b) ホスト毎の脆弱性検査結果時系列表示

対象のホストの脆弱性検査結果を時系列で表示する。表示方法は 2 種類あり表形式とグラフ形式が用意されている。表形式では対象ホストの脆弱性検査結果を時系列で表示しており、内容はその際の検査スコア、J-PARC 固有脆弱性の保有状況、機器管理者情報が表示される。また、スコア欄にはリンクが用意されており、選択された日時の詳細な脆弱性検査結果を表示する事が出来る。また、XML ファイルダウンロード用のリンクが提供されており、商用ツールから出力された XML ファイルを保存する事が可能になっている。グラフ形式では、対象ホストの脆弱性検査スコアを折れ線グラフで表示でき、スコアの増減が視覚的に分かるようになっている。

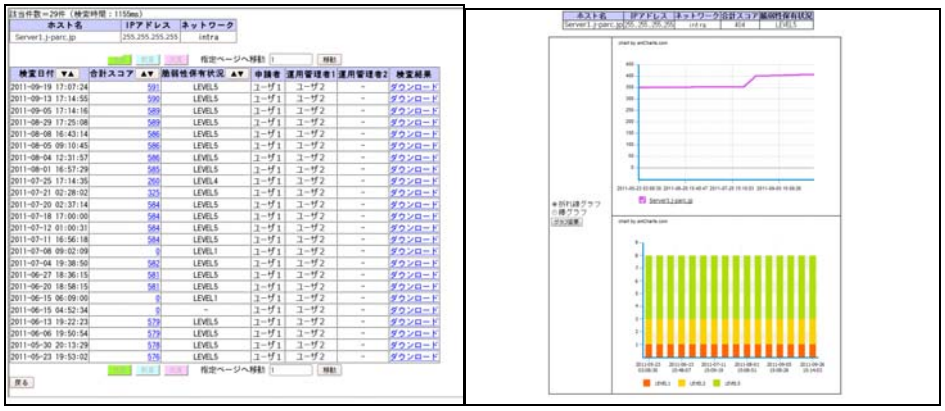


図 4. ホストごとの脆弱性検査結果時系列表示

[9] Apache/Tomcat: Java サーブレット・JSP を処理するアプリケーションサーバ
[10] Xpath: XML Path LanguageXML に準拠した文書の特定の部分を指定する言語構文

c) ホスト毎の脆弱性検査結果詳細表示

選択されたホストの脆弱性検査結果の詳細情報を表示する。表示内容は脆弱性検査の開始、終了日時、使用された脆弱性検査用シグネチャファイルのバージョン、ホスト情報、脆弱性検査スコア、CVSS 基本値、J-PARC 固有脆弱性保有情報、検出されたそれぞれの脆弱性の概要が表示される。それぞれの脆弱性 ID にはリンクが用意されており、脆弱性 ID 毎の詳細情報表示へリンクしている。

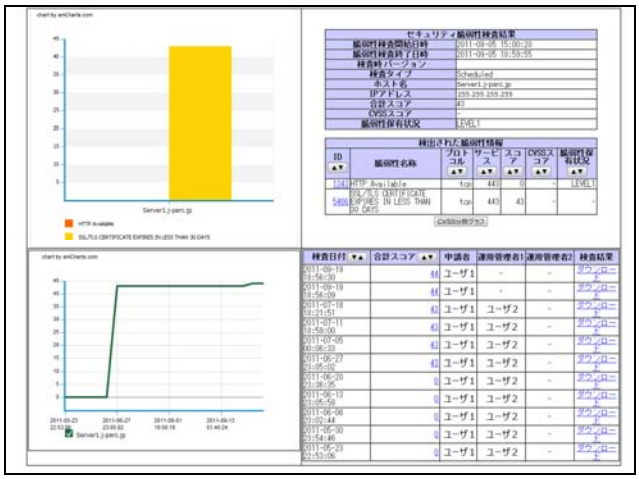


図 5. ホスト毎の脆弱性検査結果詳細表示

d) 脆弱性 ID 毎の詳細情報表示

選択された脆弱性の詳細な情報を表示する。表示される内容は脆弱性名称、スコア、J-PARC 固有脆弱性に該当しているかどうか、脆弱性の解説、保有している CVE[6][11]の情報等の関連情報、また、CVSS[12]基本値を持っている場合は、CVSS 基本値の内訳を表形式及びグラフで表示する。

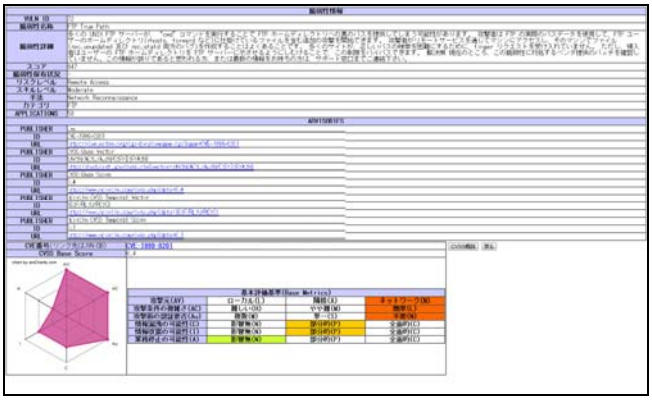


図 6. 脆弱性 ID 毎の詳細情報表示

[11] CVE:脆弱性情報データベース他の脆弱性情報データベースと異なり、内容がベンダ依存でないことが利点として挙げられる。
[12] CVSS:情報システムの脆弱性に対するオープンで汎用的な評価手法で、ベンダに依存しない共通の評価方法を提供している。

2） システム管理者向け（利用者向けと重複する機能を省いて記載）

a) 管理対象ホストのスコアによるヒストグラム表示

登録されている全てのホストの最新の脆弱性検査結果を利用して、スコア分布ヒストグラムを表示する。これにより、どのスコアレンジに何台のホストが存在しているかを視覚的に表現できる。

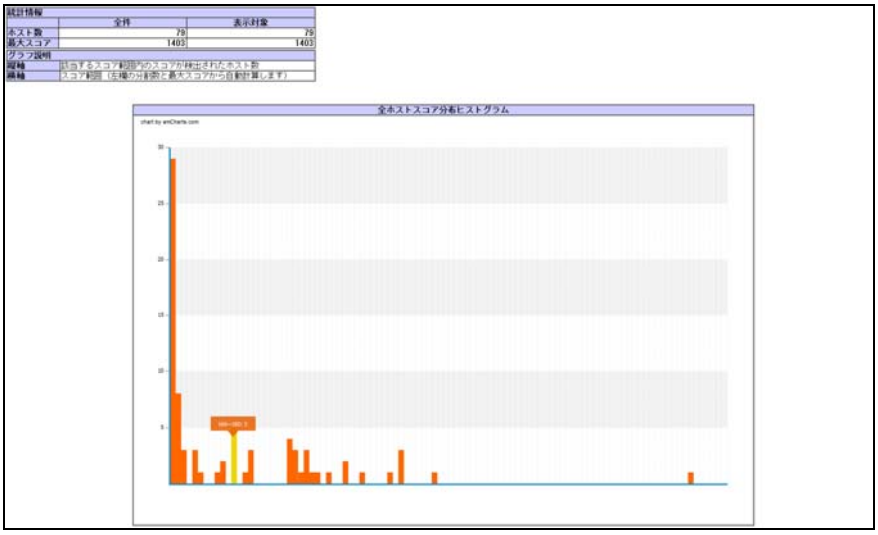


図 7. 管理対象ホストヒストグラム表示.

b) 管理対象ホストの所有している脆弱性スコアによるグラフ一覧表示

登録されている全てのホストの最新の脆弱性検査結果を利用して、それぞれのホストの脆弱性検査結果を一覧にしてグラフで表示する。表示するホストは、脆弱性検査結果スコア、J-PARC 固有脆弱性の保有状況で絞り込みができるようになっており、それぞれホスト名、IP アドレス、検査日時、検査スコア、J-PARC 固有脆弱性の保有状況、検出された脆弱性のグラフが表示される。脆弱性のグラフ形式は棒グラフ、円グラフがありサイズは通常/サムネイルで切り替えて表示する事が出来る。

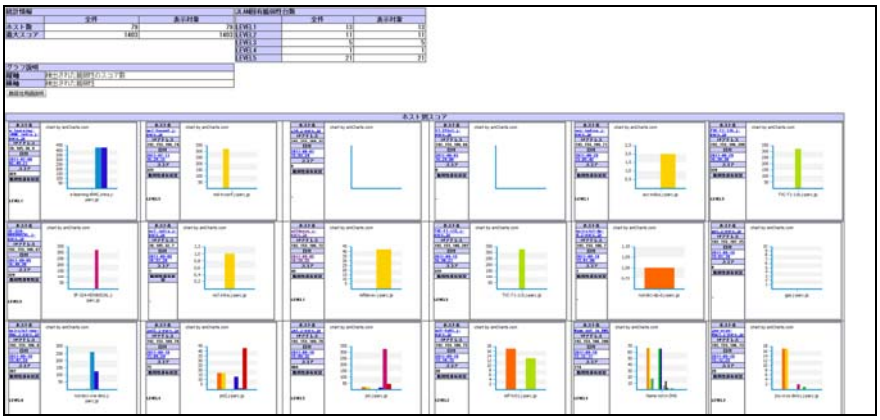


図 8. 管理対象ホストチャートグラフ表示

c) 管理しているホストの一覧表示

登録されている全てのホストの一覧を表示する。表示内容は最新の検査日時、ホスト名、IP アドレスに加えて、その際の検査スコア、J-PARC 固有脆弱性の保有状況、機器管理者情報が提供される。ホスト名、検査スコア欄にはリンクが用意されており、ホスト名を選択するとホスト毎の脆弱性検査結果時系列表示を表形式で、検査スコアを選択するとグラフ形式で表示する。システム管理者用の機能として、機器管理者情報による絞り込みが可能になっている。

図 9. 管理対象ホスト一覧表示

d) 脆弱性検査結果の統計情報表示

登録されている全てのホストの情報を利用した統計情報を提供する。

統計情報は脆弱性スコア分布グラフ及び脆弱性検査結果、脆弱性レベル分布グラフ、利用アプリケーション別利用数グラフ、アプリケーション別脆弱性数グラフ、CVE 番号別検出件数、CVSS 基本値、別検出件数グラフ、JLAN 固有脆弱性検出件数グラフ、申請者別グラフをそれぞれ対になる表とセットで表示する。

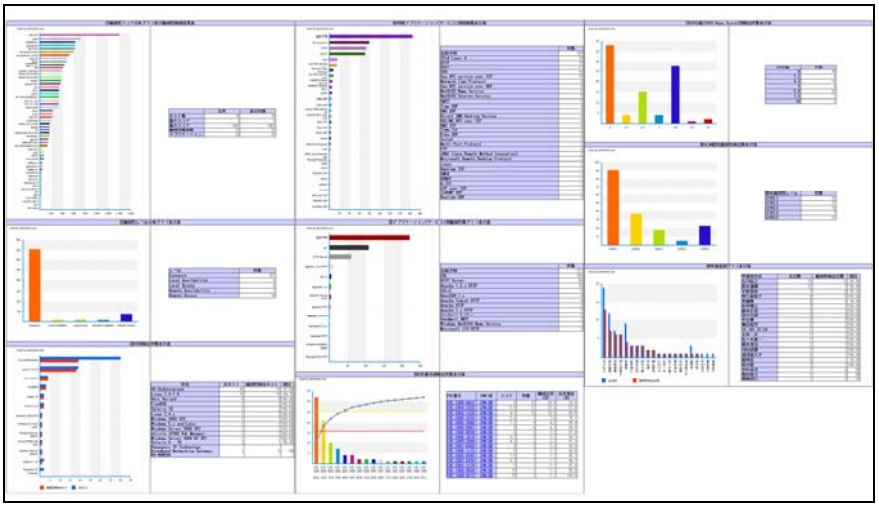


図 10. 管理対象ホスト統計情報

3.4.2. Add-On ツール群

Add-On ツール群は細かな修正なども容易に行えるように Perl/CGI で作成されている。管理簿へ登録されたデータを利用し、J-PARC 版ポータル、XML 解析システムでは用意されていない画面の提供、また対象ホストとの疎通確認等の実行、外部連携等を行う事で、商用ツールから出力される XML データ以外のデータソースも活用し、利用者へ有意義な情報を提供できるようにしている。Add-On ツール群は以下のような機能を提供している。

1） ユーザ向け提供画面

a) 疎通/脆弱性検査結果履歴表示画面

過去の脆弱性検査結果スコアと、商用ツールからの疎通履歴を表示する。ユーザがポータル内でホストごとに用意されているリンクを開くとその対象ホストへの脆弱性検査スコアの履歴と、商用ツールからの疎通の履歴をカレンダー形式で表示する。

b) ユーザ、ホストごとの CVSS 分析グラフ

脆弱性検査結果内に含まれている CVE 情報から、CVSS 基本値を取り出しスコアごとに積み上げ棒グラフで表示する。棒グラフの内訳は脆弱性検査 DB の Strategy（攻撃種別）、skill（攻撃に必要な技能）、risk（攻撃の危険性）、score（脆弱性検査スコア）で集計する事ができ、CVSS と脆弱性検査 DB 内の情報を比較して表示する事が出来る。

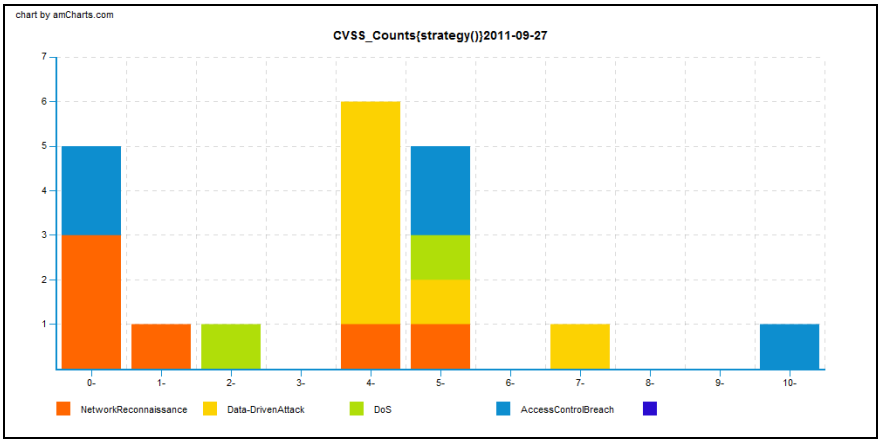


図 11. CVSS 分析グラフ

c)　ユーザ、ホストごとのスコアのソーシャルグラフ表示画面

ユーザが管理しているホストの一覧とホストが持っている脆弱性検査スコア、脆弱性情報を一覧にしてグラフィカルに表示する。また、ホストを選択する事で、ホストの持っている脆弱性 ID とそれに関連している CVE 情報を表示する。脆弱性 ID と CVE 情報を選択するとそれぞれの詳細情報が表示されるようになっている。

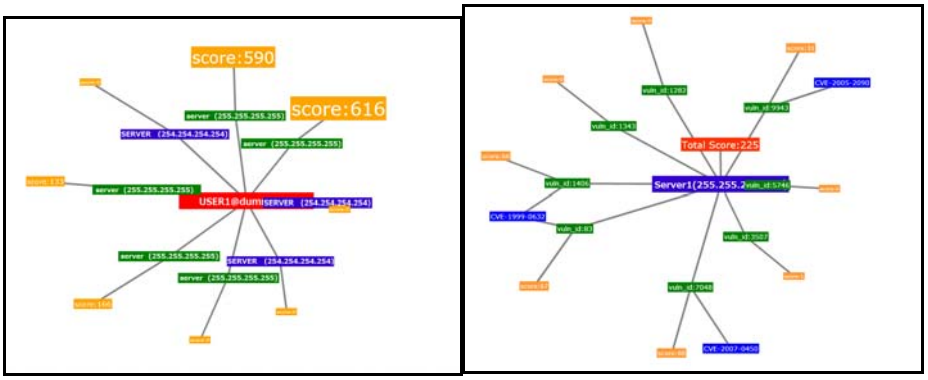


図 12. ソーシャルグラフを用いた脆弱性検査結果表示例

d)　CVE 及び脆弱性検査用シグネチャ登録状況表示画面

脆弱性検査用 DB と CVE の関連について表示する。

脆弱性検査用 DB 内でどの程度の CVE 脆弱性情報を含んでいるか、また CVE だけにしか含まれていない情報がどの程度あるかを表示する。

図 13. CVE 及び脆弱性検査用シグネチャ登録状況表示
（便宜上、値を判断できないようにしている）

e)　脆弱性検査結果についてのメール送信

商用ツールから、一定時間毎に管理されている全てのホストへ死活確認を行っている、疎通が全く取れない機器については電源が入っていない可能性があり、正常な脆弱性検査が出来ていない場合がある。J-PARC ポータルからのメール出力では、正常な脆弱性検査が行われなかったホストに対してのフォローは出来ていない為、本機能で疎通が取れないホストの機器管理者へ対応を促すメールを送信する。

2） システム管理者向け（ユーザ向けと重複する機能を省いて記載）

a) 商用ツールからの疎通及び検査点履歴の一覧表示

管理されている全てのホストの商用ツールからの死活確認、及び脆弱性検査結果の検査スコアを表示する。また、ホストごとのアクセスグラフ、疎通/脆弱性検査結果履歴、商用ツールからの死活確認、システム管理者からのメッセージ表示へリンクする事が出来る。

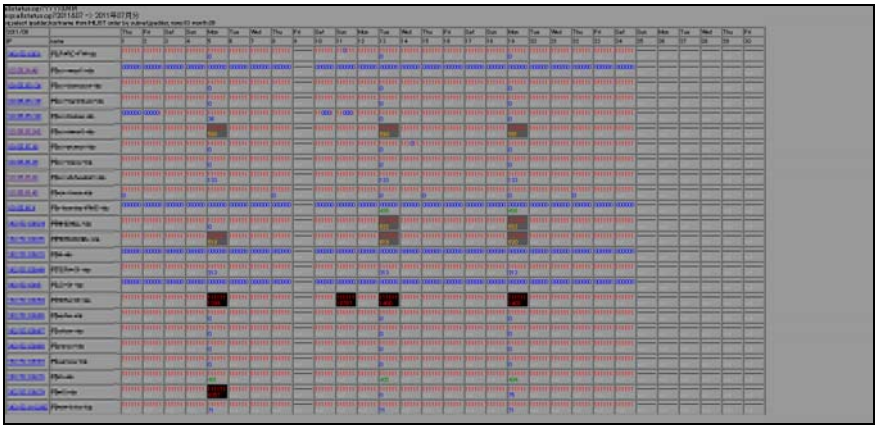


図 14. 死活確認及び脆弱性検査結果履歴の一覧表示画面

b) 公開前脆弱性検査事前案内メール送付

公開前脆弱性検査実行時に送信する案内メールを送信する。

宛先メールアドレス、対象ホストの IP アドレス、公開前脆弱性検査実施予定日時を入力する事で、事前に用意されているテンプレートを利用して機器管理者への通知メールを送信する事が出来る。

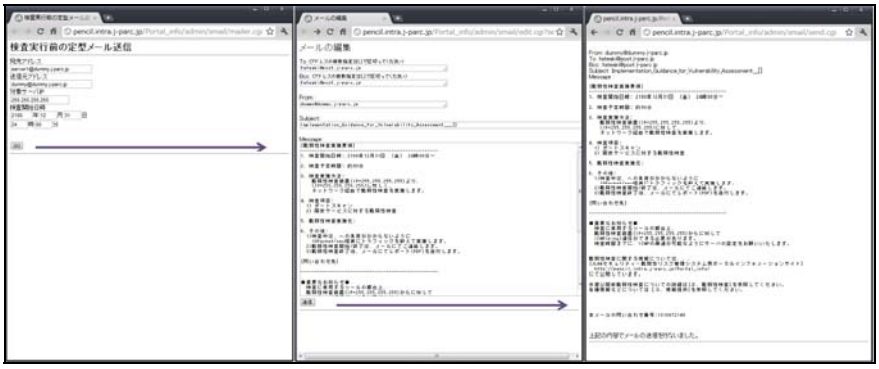


図 15. 公開前脆弱性検査事前案内メール送信画面

3.4.3. 検査結果蓄積サーバ

本システムは機器管理者やシステム管理者へ機能を提供する物ではないが、商用ツールから出力された XML ファイルデータが蓄積されており、XML 解析システム、Add-On ツール群のデータソースとなっている。

3.5 他システムとの連携機能

1） ファイアウォールアクセスログ表示画面[4]

ユーザが管理しているホストと JLAN 上へ設置されているファイアウォールを経由した通信のログを利用し、サービス/IP 等で集計しグラフ化を行い機器管理者へ提供する。

また、ネットワークセグメント毎のリアルタイムのトラフィック流量と IP を元にしたアクセス元地域の表示画面を閲覧できるようにしている。

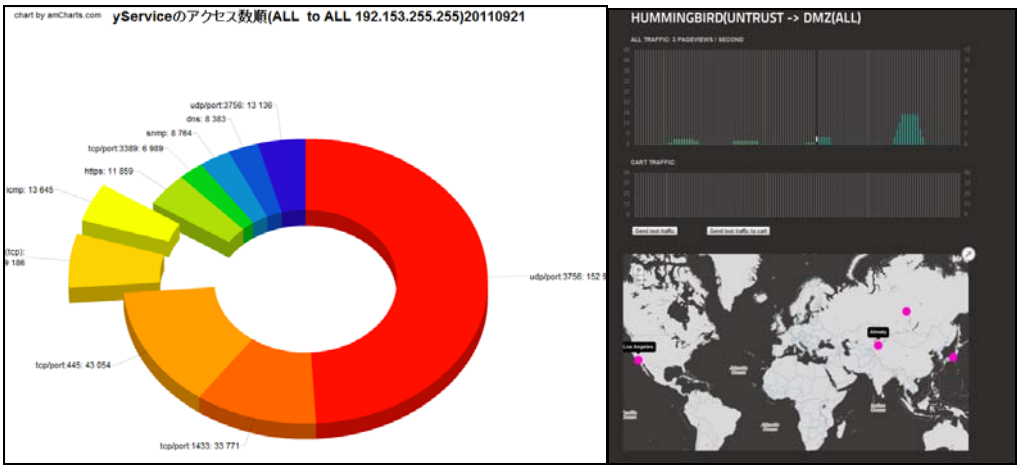


図 16. アクセス履歴及びリアルタイム表示

2） 対象ホスト接続済みスイッチ接続ポート情報表示画面

ユーザが管理しているホストの接続先ポートの情報を提供する。JLAN 上へ設置しているネットワーク監視サーバ（Cacti[11]）の情報を活用し管理しているホストが接続されているスイッチのポート情報に限って提供する。

3.6 開発における創意工夫

1） 提供機能の工夫

a) 使いやすい GUI[13]の提供

「情報セキュリティ脆弱性リスク管理システム」では、脆弱性検査を行う部分に商用ツールを使用している。この商用ツールは、GUI 機能を利用して脆弱性検査を実施できる。商用ツールは多機能である一方、脆弱性検査に熟知した人向けの GUI 機能となっており、素人には扱いづらい。また、一部の機能は J-PARC で使用する予定はないため、商用ツールをそのまま利用者に提供するには不向きであった。

商用ツールの GUI 機能を直接利用者に操作させない仕組みは KEK 版ポータルですでに実現され運用されていた。J-PARC 版ポータルでも同様のシステム要件により、KEK 版ポータルに J-PARC の要望を反映しカスタマイズしたものを J-PARC 版ポータルとして提供している。これにより、利用者が直接商用ツールにアクセスさせない環境を提供することができた。

さらに、ポータルの機能拡張として動作する Add-On サブシステムを開発した。この Add-On サブシステムでは、脆弱性検査結果をデータマイニングすることにより、利用者に新たな情報を提供することができた

b) 提供するグラフの種別

Add-On ツールで出力されるグラフは軸によってカテゴライズされており、以下の 4 つに分けられる。

① 時間/傾向分析

時間を軸にしたグラフは、時間の経過とともに変化していく情報を追う事に適している。Add-On サブシステムでは脆弱性検査のスコア、CVSS のスコアの時系列グラフ、アクセスログを作成しており、これらの情報の時間の経過、または設定変更等による影響を分かりやすく示すことができる。たとえば脆弱性点数が急上昇した、等のイベントが発生した際にそれがいつなのか、どの程度の影響があったのかを素早く理解できる。

② 内訳/情報提供

そのグラフの詳細な項目を軸としたグラフはその時に何が起きていたのか/どんな内容だったかを表すことが出来る。Add-On サブシステムでは脆弱性検査スコア内訳、CVSS 分析グラフ、アクセスログ、脆弱性詳細情報 CVSS 分布グラフ、ソーシャルグラフを用意している。それぞれ見つかった脆弱性のスコア内訳、CVSS 基本値の内訳をグラフ化し、ソーシャルグラフでは形は違うもののその検査で見つかった脆弱性とそのスコアを線で結ぶ事で表現している。

[13] Graphical User Interface

③　分布/統計による概観分析

　このグラフ群は全体の分布やばらつきの状態を把握するために用意されているため、機器管理綾へは提供されていない。Add-On サブシステムでは、脆弱性検査スコア、CVSS スコア以外にも OS による統計、検出されたアプリケーションの統計等を用意しており、システム管理者が全体の傾向を掴むため、突出しているホストを見つける為に用意される。

④　その他

　その他、利用者へ実際に脅威を認識してもらうために、リアルタイムでのアクセスログ表示が用意されている。これは脆弱性対策に利用するというより、啓蒙活動用に用意されている。このグラフはリアルタイムに外部から DMZ へのアクセスを表示する事が出来、どの程度のアクセスが常に発生し、許可、拒否されているかを表示している。

表 5に Add-On ツール及び外部連携で出力可能なグラフを表としてまとめた。

表 5. Add-On サブシステム及び外部連携システムによって出力可能なグラフ一覧

	名称	機能概要	参照画面	分類
管理者限定機能	脆弱性グラフスコア分布	全体の脆弱性検査結果スコアを使い、ホストを点数順で表示する。	図 10	③
	脆弱性グラフレベル分布	全体の脆弱性検査結果内の攻撃のレベルの記載毎の分布を表示する。	図 10	③
	OS 別検出件数分布グラフ	全体の脆弱性検査結果内で判別された OS 別、そのうちの何台で脆弱性が検出されているか分布を表示する	図 10	③
	アプリケーション別利用分布グラフ	全体の脆弱性検査結果内で識別されたアプリケーションの分布を表示する。	図 10	③
	アプリケーション別脆弱性分布グラフ	全体の脆弱性検査結果内で識別されたアプリケーションの内、脆弱性の見つかったアプリケーションの分布を表示する。	図 10	③
	CVE 番号別脆弱性検出数	全体の脆弱性検査結果内の CVE 番号別に分布を表示する。	図 10	③
	CVSS 別検出件数	全体の脆弱性検査結果より CVSS スコア別に検出件数の分布を表示する。	図 10	③
	JLAN 固有脆弱性検出表	全体の脆弱性検査結果より JLAN 固有脆弱性の分布を表示する。	図 10	③
	申請者別グラフ表示	申請者が持っているホストの台数の分布を表示する。	図 10	③
利用者向け機能	CVSS 分析グラフ	ホストの脆弱性検査結果より分類項目を抜き出し、CVSS 基本値で積み上げ棒グラフを表示する。	付録-図 17	②
	ソーシャルグラフ	機器管理者とホスト、ホストが持つ脆弱性等を関係に注目して表示する。	付録-図 18	②
	アクセスロググラフ	FW アクセスログを利用し、検索条件に応じてグラフを表示する。	付録-図 19	①②
	アクセスログリアルタイム表示	FW アクセスログを利用し、リアルタイムに通信の状態を表示する。	付録-図 20	④
	脆弱性検査スコアグラフ	ホストの脆弱性検査結果より脆弱性種別ごとのスコア分布を表示する。	付録-図 13	②
	脆弱性検査 CVSS 合計スコア時系列表示	脆弱性検査結果のスコアを利用して CVSS スコアの時系列を表示する。	付録-図 14 付録-図 13	①
	脆弱性検査合計スコア時系列表示	脆弱性検査結果のスコアを利用して脆弱性検査スコアの時系列を表示する。	付録-図 14	①

c) 複数指標による情報セキュリティ脆弱性分析

情報セキュリティ脆弱性リスク管理システムでは、商用ツールを用いて情報セキュリティ脆弱性検査を実施している関係で、必ず商用ツールの指標により判定される。この指標は、時間・リスク・スキルの３要素を用いて数値化（スコア）して、脆弱性の脅威度を定量化している。

同様に、ベンダに依存しない共通の評価方法で脆弱性を定量化する指標として CVSS がある。この CVSS では３つの情報セキュリティ基準（表 6）がある。

表 6. CVSS による情報セキュリティ基準の特徴(出典元: IPA 共通脆弱性評価システム CVSS 概説[5])

カテゴリ	概要
基本評価基準（Base Metric）	・ 脆弱性そのものの特性を評価する基準。情報システムに求められる３つの情報セキュリティ特性である「機密性（Confidentiality Impact）」「完全性（Integrity Impact）」「可用性（Availability Impact）」に対する影響を、ネットワークから攻撃可能かどうかといった基準で評価し、CVSS 基本値（Base Score）を算出する。 ・ この基準による評価結果は固定していて、時間の経過や利用環境の異なりによって変化しない。ベンダや脆弱性を公開する組織などが、脆弱性の固有の深刻度を表すために評価する基準
現場評価基準（Temporal Metrics）	・ 脆弱性の現在の深刻度を評価する基準。攻撃コードの出現有無や対策情報が利用可能であるかといった基準で評価し、CVSS 現状値（Temporal Score）を算出する。 ・ この基準による評価結果は脆弱性への対応状況に応じ、時間が経過すると変化する。脆弱性の現状を表すために評価する基準。
環境評価基準（Environmental Metrics）	・ 製品利用者の利用環境も含め、最終的な脆弱性の深刻度を評価する基準。攻撃を受けた場合の二次的な被害の大きさや、組織での対象製品の使用状況といった基準で評価し、CVSS 環境値（Environmental Score）を算出する。 ・ この基準による評価結果は、脆弱性に対して想定される脅威に応じ、製品利用者毎に変化する。製品利用者が脆弱性への対応を決めるために評価する基準。

表 6のうち、基本評価基準（Base Metric）は、脆弱性そのものの特性を評価する基準で、時間の経過や利用環境によって変化しない固定の指標である。この２つの指標を利用することで、商用ツールの可変スコアと固定スコアの異なる視点から定量的な評価を行えるようにしている。しかし本来の脆弱性の脅威は、組織環境により変わるはずある。そこで定量的評価に加え、JLAN 固有の指標として定性的な指標でも評価を行えるようにした。

本システムでは、最終的に定量的指標及び定性的指標を組合せ、３つの異なる指標で評価できるようにした（表 7）。

表 7. 「情報セキュリティ脆弱性リスク管理システム」で採用している評価指標

区分	評価指標	分類	脆弱性の脅威度
定量指標	商用ツール	可変指標	時間・リスク・スキルの３要素を用いて計算し数値化（スコア）している。 1. 時間 脆弱性が情報セキュリティ関連サイトで公開されてから検査を実施した日までの経過日数。脆弱性スコアが時間の経過と共に穏やかな伸び率となうように扱われている。 2. リスク 脆弱性が攻撃された時からシステム被害を７段階で表現する。 3. スキル 脆弱性の難易度を６段階のレベルで表現する。
	CVSS 基本値	固定指標	情報セキュリティ特性である機密性（Confidentiality Impact）、完全性（Integrity Impact）、可用性（Availability Impact）に対する影響を、ネットワークから攻撃可能かといった基準で数値化（スコア）している。 1. 機密性 脆弱性を攻撃された際に、対象システム内の機密情報が漏えいする可能性を 3 段階で評価する。 2. 完全性 脆弱性を攻撃された際に、対象システム内の情報が改ざんされる可能性を 3 段階で評価する。 3. 可用性 脆弱性を攻撃された際に、対象システム内の業務が遅延・停止する可能性を 3 段階で評価する
定性指標	JLAN 固有脆弱性	可変指標	JLAN 固有の環境でネットワーク攻撃や情報漏えい等のリスクがあるかを、不定期に JLAN 情報セキュリティ責任者が判断しレベル設定（非スコア）を行っている。 1. レベル 概ね”要注意”，”危険”で評価を行う。JLAN 環境の変化によりレベルを追加することがある。

d)　脆弱性識別子を基準とした脆弱性分析

検出された脆弱性を出現頻度順にヒストグラム化することにより、JLAN における未対処の脆弱性分布を確認することができるようになった。(図 17)　検出数の多い上位 4 つの棒グラフで、JLAN 全体の脆弱性の約 84%ある。CVE 番号について脆弱性対策がとられると、未対処の脆弱性件数が大幅に減らすことができる。

ただし、この方法は脆弱性指標のスコアを一切参照していないので、注意が必要である。

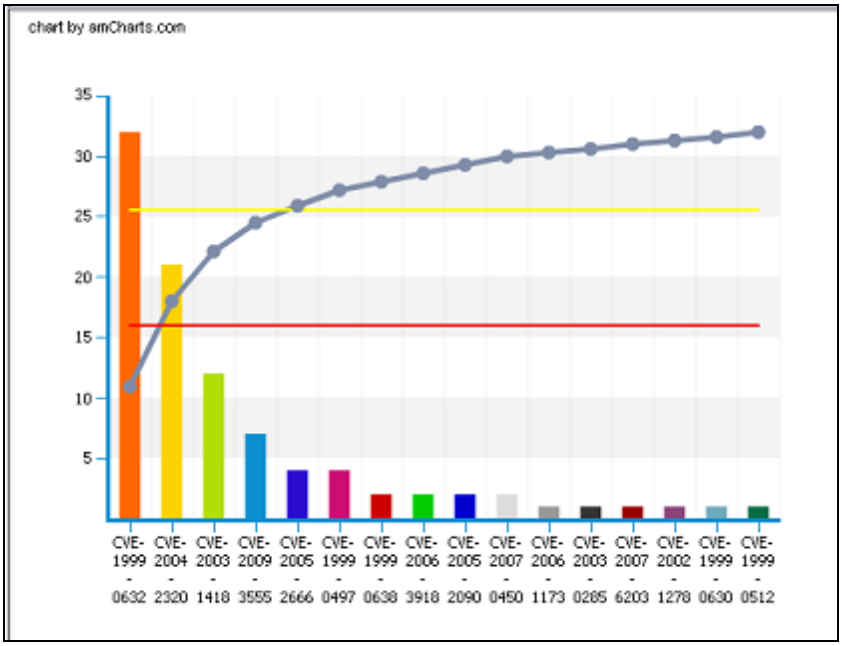


図 17. CVE 番号による脆弱性検知数

e)　直感的インタフェースの提供

機器管理者は通常複数の機器を管理している。目的のホストの脆弱性情報を取得するには、まず自身の管理する全機器の脆弱性検査結果（定量的指標（スコア）や定性的指標）を確認し、次に、高スコアの機器や前回の検査結果からスコアが高くなった機器について詳細な脆弱性情報を確認するのが定石である。

脆弱性対策レベルは機器管理者の保有スキルによりまちまちであるが、同一人物が実施する脆弱性対策には共通性がみられる。すなわち、同一人物が管理する機器は、共通の脆弱性を検知している可能性が考えられる。このような場合、サーバ毎に脆弱性検査結果を確認していては、作業効率が非常に悪い。そこでソーシャルグラフ（図 12）を用いて可視化をおこない、一度にかつ直感的に共通の脆弱性が検出されているかを確認できるようにした。

f) 脆弱性情報の検索

脆弱性検査では検査対象機器に対して多くの脆弱性チェックが行われるため、脆弱性DB には多くの脆弱性情報が蓄えられている。しかし、商用ツールで提供されている機能では脆弱性検査で検出されたものしか確認することができず、他にどのような脆弱性情報が登録されているのか判らない。そこで、脆弱性 DB を XML 形式で取り出して活用することとした。

脆弱性情報を XML 形式のデータとして取出した後、XML データベース（Apache XML Project Xindice）を用いて Add-On サブシステム上に脆弱性 DB として登録した。さらに、この脆弱性 db への検索機能を提供することで、商用ツールが保有している脆弱性の情報を確認できるようになった。

g) 検出できる脆弱性及び検出できない脆弱性情報の提供

商用ツールの脆弱性情報は、概ね 2～3 週間で更新され提供される。このため情報のリリース後に新規に発見された脆弱性は検出することができない。そこで、商用ツールの脆弱性 DB と CVE-DB の差分を作成し、商用ツールが検出できないと思われる CVE-ID を一覧で確認できるようにした。これによって利用者へ商用ツールの脆弱性 DB であっても全ての脆弱性が網羅されているわけではない事を直感的に理解させることが出来るようになった。

2） 情報セキュリティ啓蒙の相乗効果

a) RSS を利用した最新の脆弱性情報の提供

情報セキュリティ情報や脆弱性情報は、RSS を用いて情報セキュリティや脆弱性情報を発信するサイトから配信されている。Push 型の情報提供方式は、情報提供者側が一方的に情報を提供するため利用側は運用の手間がかからない。このため情報提供元の情報が信頼されるものであれば、有用情報を機器管理者に提供することができる。本システムでは情報セキュリティ及び脆弱性に対する目的に、表 8のサイトより RSS[14]を受信し、情報セキュリティ啓蒙の一環として機器管理者に情報発信を行っている。

表 8. 情報提供元による RSS 情報提供一覧

	RSS	発信情報
1	IPA 情報セキュリティ　緊急対策情報 .	放置しておくと不正アクセスを受ける危険が高い情報セキュリティ上の弱点を情報発信
2	.JVN（JapanVulnerabilityNotes） 脆弱性レポート[7]	脆弱性関連情報とその対策、製品開発者の対応状況を情報提供
3	JP-CERT コーディネーションセンター 注意喚起 ＆ Weekly Report[7]	注意喚起: 深刻かつ影響範囲の広い脆弱性などに関する情報を提供 Weekly Report: JPCERT/CC が得た関連情報のうち、JPCERT/CC が重要と判断したものの抜粋版を情報提供

[14] RSS: RDF Site Summary

b) F/W ログを用いたアクセス情報の提供

機器管理者にとって脆弱性対策に対するモチベーションが上がらない要因のひとつに、JLAN で導入している F/W 等のセキュリティ機器で安全が確保されているとの過信から、外部からの不正アクセスや DoS 攻撃に対して実感がないことが挙げられる。

脆弱性対策へのモチベーションを上げるため、自身の管理する機器が外部からどのようなアクセス（不正アクセス（ポートスキャンやアタック））が行われているか、あえて脅威を認識してもらうために、以下の２つのツールを提供することとした。

- 不正アクセス履歴の提供

  F/W アクセスログを送信元/送信先 IP アドレスやサービス種類を集計し可視化することで、ポートスキャン攻撃や DoS 攻撃を確認することができる。実際の可視化した例を図 18 に示す。

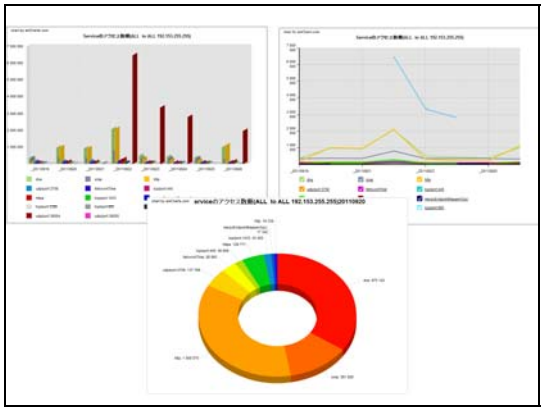


図 18. 不正アクセス履歴の可視化例

- リアルタイムによる不正アクセス状況の提供

  F/W アクセスログをリアルタイムに処理し可視化することで、どの地域から不正アクセスが行われているかを確認することができる。実際に可視化した例を図 19に示す。

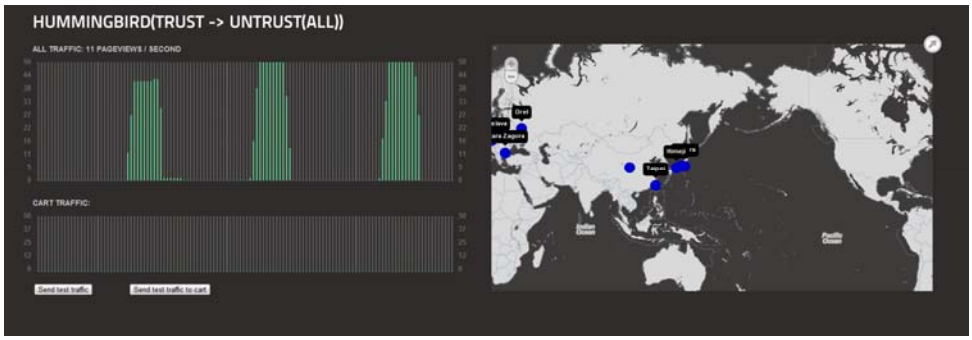


図 19. リアルタイムによる不正アクセスの可視化例

3） PDCA サイクル実行環境の提供

脆弱性検査は自動で定期的（毎週）に実施されており、検査結果は機器管理者にメール通知される。システム環境を変更した時には、機器管理者自身が直ちに脆弱性検査できるようにしている。

これにより、機器管理者は脆弱性に対して「対策計画（Plan）」－「対策の実行（Do）」－「実行結果の確認（Check）」－「対策の評価（Action）」を継続的に実行できる環境を提供することができた。

4） KEK 版ポータルとのソースコード統一による、開発効率やモジュール保守性への配慮

J-PARC 版ポータルは KEK 版ポータルを元にして開発したが、商用ツールの構成や要求仕様の差異があるため、当初は J-PARC 版と KEK 版を別々のソフトウェアとすることを考えた。しかしその場合、以下のような問題が発生する。

- バグが判明した場合、2 つのソフトウェアに対応する必要がある
- 片方の版で機能拡張しても、他方の版がその恩恵を受けられない

いずれの問題も、J-PARC 版と KEK 版のソースコードの乖離が大きくなれば、より困難な問題となることが予想された。そこで本開発では、KEK 版ポータルからのソースコードの乖離を極力避け、統一した管理を可能とするための工夫を行った。ポイントを下記に示す。

a) ネットワーク環境に応じた、J-PARC 版と KEK 版の自動判別

J-PARC 版ポータルのソフトウェアは、稼働中のネットワークのドメインを調べ、その値が j-parc.jp か kek.jp かによって、動作させるべき版を自動的に判別する。モジュール内では必要に応じてこの判別値を参照し、ソフトウェアとしての振る舞いを切り替える。このような設計は、以下の利点をもたらす。

- デプロイ作業の負荷軽減
- 共通機能の二重化を避けつつそれぞれの版の差異に着目した、効率的な開発や保守

b) J-PARC 版と KEK 版の、リソースの細やかな分離

複数の版を統一すると、一般的には機能の柔軟性が下がる。これを極力避けるために、J-PARC 版と KEK 版のリソースの細やかな分離を行った。特に Web 画面やメールのリソースについて、以下の工夫を行った

- 機器管理者の状況などによって可変となる文言をリソース内で変数化し、文言の内部で自由に配置できるようにした。
- 特に、所有機器一覧表内でカスタマイズを要する箇所については、項目ひとつをリソース化した。これにより、KEK 版では提供されない Add-On サブシステムについて、J-PARC 版の運用者が自由にカスタマイズ可能となった。

c) ソースコードリポジトリの使用 （Subversion[14]）

本工夫では J-PARC 版と KEK 版の統一したソースコード管理を実現したが、ソフトウェアとしての振る舞いやリソースが同じではない以上、ソースコードの修正の際には双方の版でのテストが必要となる。また、J-PARC と KEK では別々の運用をしているので、新版ソフトウェアをデプロイして良いタイミングも異なる。そこでソースコードリポジトリ Subversion を使用し、リポジトリが管理可能な程度の小さな開発ブランチの発生については、許容することにした。

4. システムの評価

4.1. 要求定義の評価

表 2及び表 3で設定したシステム要件に対する、J-PARC 版ポータルの改良元となった KEK 版旧ポータル及び、今回開発した J-PARC 版ポータルと Add-On サブシステムの機能の対応を表 9に示す。

J-PARC 版ポータルでは c, f, g の要件を満たすことが出来たが、a, b, d, e の要件を満たしていない。不足している機能については、Add-On サブシステムを追加し機能を補う事により、当初の計画通りの全ての要件を満たすことができ、これにより、表 1で述べた、機能面、運用面での課題を解消する事が出来た。

表 9. ポータルと Add-On サブシステムの機能比較

機能	Add-On サブシステム	J-PARC 版ポータル	KEK 版旧ポータル
a. 脆弱性に対して複数のリスク指標を用いて情報提供を行う			
商用ツールの脆弱性情報を利用した情報の提供	○	○	○
CVE 脆弱性情報を用いた脆弱性情報の提供	○	△[15]	△[15]
b. 検出できる脆弱性、検出できない脆弱性の情報提供を行う			
CVE 脆弱性情報と商用ツール脆弱性情報の対応情報の提供	○	－	－
CVE 脆弱性情報でしか管理されてない脆弱性情報の提供	○	－	－
c. 定期的に自動で実施する脆弱性検査に加え、利用者がいつでも実施できる手動検査を提供する。			
定期的な脆弱性検査の実施	－	○	○
手動による脆弱性検査の実施	－	○	○
d. PUSH 型で脆弱性査結果を情報提供する			
定期的な脆弱性検査結果のメール通知が可能	－	○	○
定期的な脆弱性検査が正常に行われなかったホストへのメール通知	○	－	－
e. 脆弱性検査結果を元にデータマイニングを行い、新たな情報提供を行う			
脆弱性検査結果と CVE 脆弱性情報を用いた統計情報の提供	○	－	－
f. システム運用側の負荷がかからないシステムを提供する			
定期的な脆弱性検査の実施が可能な事	－	○	○
手動による脆弱性検査の実施が可能な事	－	○	○
J-PARC/KEK どちらの環境でも最小限のプログラム変更で対応が出来る事	－	○	－
g. オペレーションが複雑にならない環境を提供する			
商用ツールにログインせずに脆弱性検査の実行及びレポートの取り出しが可能な事	－	○	○

○:提供有　△:制限付きで提供　－:提供無

[15] CVEID を利用したリンクが用意されている。

4.2. 出力の評価

1） スコアを基準とした出力の評価

図 20は 3.4-1　2)　a)の機能を使ったシステム管理者用の画面となる。各機器の脆弱性危険度（スコア）を横軸に、縦軸に台数をとり、スコア範囲に含まれる機器の台数をヒストグラム化した。商用ツールにおける脆弱性危険度は、脆弱性毎に与えられているスコアの大小によって判断が可能になっており、スコアが大きいほど危険度が高く、スコアが 0 に近いほど危険度は低いとしている。

システム管理者はヒストグラム表示を確認する事で、全体のスコア分布を把握できるようになり、システム管理者が注視するべき機器がどの程度あるかを視覚的に把握出来るようになった。その結果として、管理されている機器に対して脆弱性危険度に応じて適切な労力で対応できるようになった。

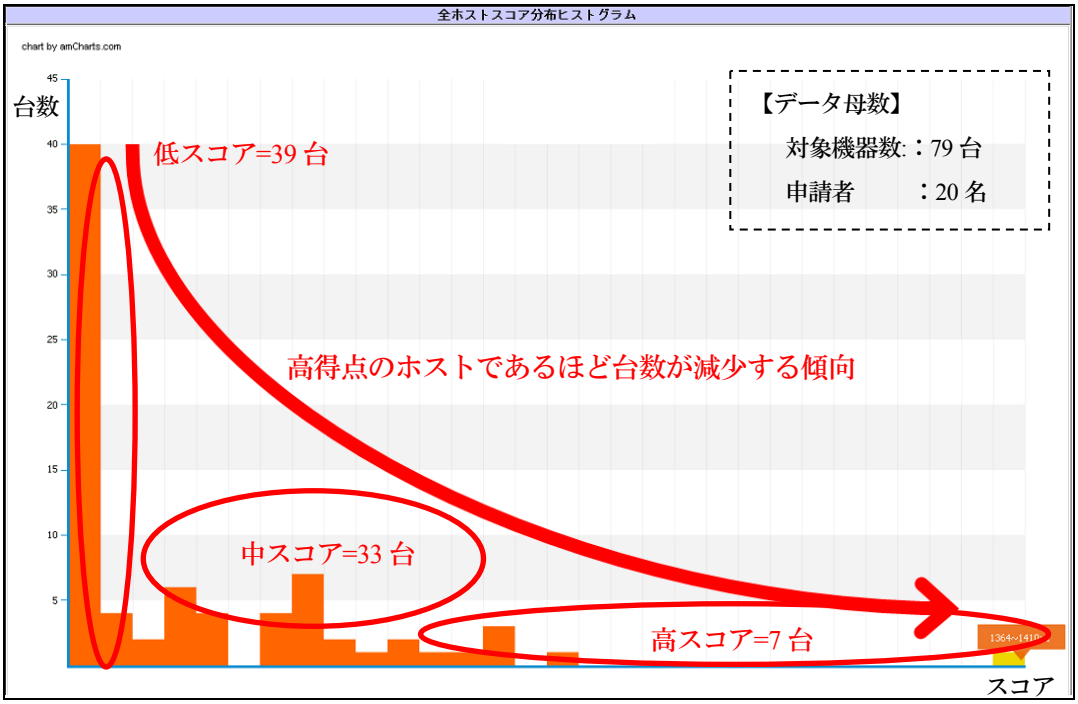


図 20. 検査対象機器のスコア分布図

2） 脆弱性指標別による出力の評価

図 21上段は 3.4.1　c)、下段は 3.4.2　b)の機能を使用した機器管理者、システム管理者用の画面である。図 21上段は横軸に検出された脆弱性項目、縦軸をスコアとして、検出された脆弱性に対するスコアを表した。下段は横軸に CVSS 基本値、縦軸を件数とし、検出された脆弱性に対する CVSS 基本値を表した。

商用ツールの指標では、脆弱性一件当たり最大スコアが 29 である。一件当たりスコア 29 というのは、商用ツールが持つその他の脆弱性のスコアと比較しても十分に低い値であり、対処が必要な脆弱性とは機器管理者に認識されない。これに対し、CVSS による指標（図 21下段）では、CVSS 基本値が 7 以上の深刻な危険性を示すものは検出されていないものの、CVSS 基本値が 4.0～5.9（中程度の危険性）を持つ脆弱性が確認できる。

システム管理者は、このような 2 つの異なる視点で脆弱性の危険度を評価する事で、商用ツールのスコアが必ずしも万能な物ではなく、スコアが低いからと言って、対策を怠ってしまう事は危険な場合がある事を機器管理者へ提示できるようになった。

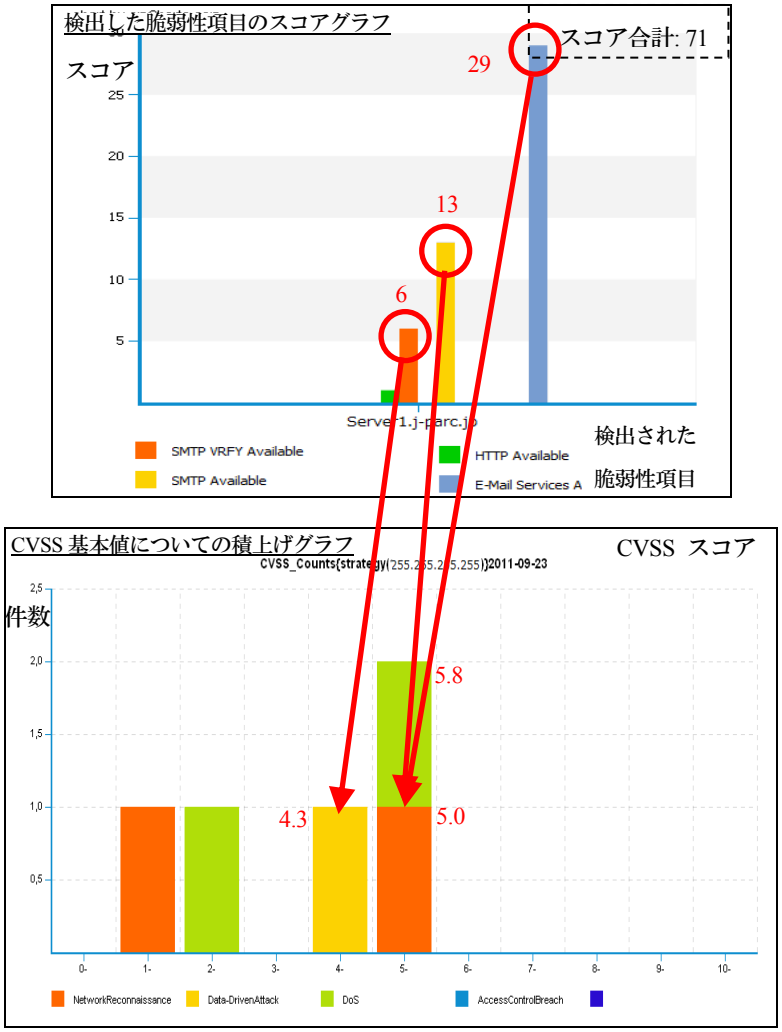


図 21. 異なる指標による脆弱性検査結果比較

3） CVSS 情報の出力の評価

図 22は機器管理者、システム管理者用の画面で、各脆弱性が持っている CVSS 基本値をグラフ化した画面となる。2)では、評価指標として、商用ツールの情報だけでなく CVSS 基本値も利用した。CVSS 基本値は 0.0 ～ 10.0 の範囲で表され、脆弱性が持つ影響度等を元に計算式により求められる。

CVSS 基本値は脆弱性の危険度を定量的に判断することはできるが、具体的にどのような影響があるのかまでは判断が難しい。また、CVSS を構成する 6 項目は数値等で指標があるわけではなく、文字で表現されているため、なおのこと理解が難しいものとなっている。

これを一般の機器管理者にも理解し、活用してもらうために図 22のようにそれぞれの項目をグラフ化し、また日本語での表を追加した。

これによって、システム管理者は、機器管理者にとって分かりにくく活用しづらい情報を機器管理者がわかりやすい形にする事ができ、商用ツールとは違う指標を利用しやすい形で提供出来るようになった。

図 21.上段 スコア=29 に割付けられている CVE 番号

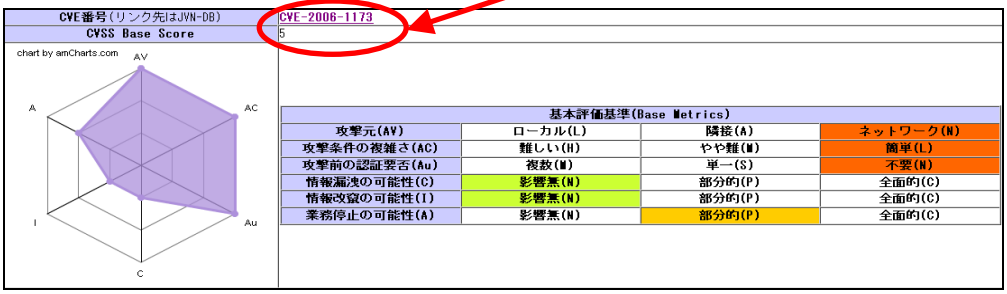


図 22. CVSS 指標による脆弱性の基本評価基準の可視化例

例として、図 21下段の CVSS スコア=5.0 の脆弱性について確認する。この脆弱性は CVE-2009-1173 が付与されている。CVSS のスコア算出時に使用される基準評価基準（Base Metrics）を可視化することで、その脆弱性が持つ影響度（情報漏えい、情報改ざん、業務停止への影響等）を機器管理者が確認できるようになった。

4） 機器管理者の管理する機器の一覧出力

図 23は機器管理者、システム管理者用の画面で、管理している機器、機器の脆弱性合計スコアと脆弱性識別子をそれぞれの関連性を持たせて一画面上に表示する、ソーシャルグラフとして提供している。このグラフは機器管理者、サーバ、検出されている脆弱性 ID、脆弱性スコア、CVE-ID をそれぞれの関係に従ってマッピングし、それぞれの関連性が一目でわかるようになっている。

たとえば、図 23で異なるサーバから同一の脆弱性 ID へ集約されている箇所がある。これは異なるサーバ間で同一の脆弱性情報を共有しているという事であり、同様の脆弱性対処で対応可能な場合が多い。機器管理者は共通している脆弱性については、サーバが異なっても同時に対応する事で効率的な脆弱性対応をとる事が出来る。また、システム管理者はその機器管理者の脆弱性対策におけるムラやクセを把握する事ができ、それぞれの機器管理者へ適した助言をすることが可能となった。

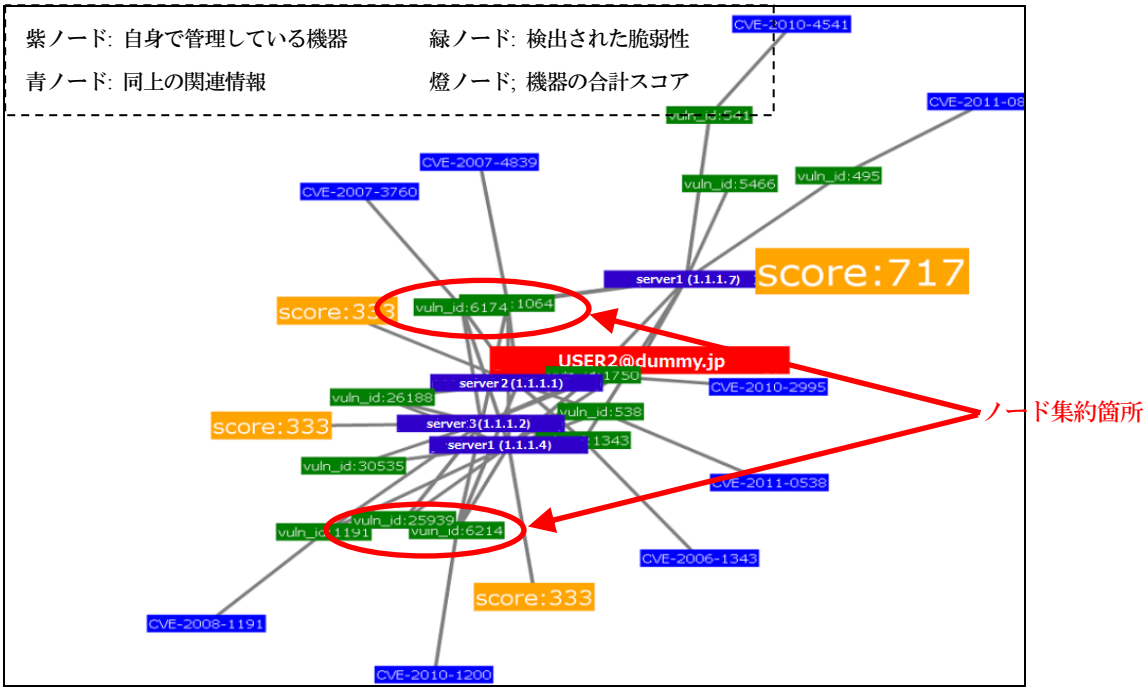


図 23. 機器管理者が管理する全機器の脆弱性情報

5） 脆弱性 DB の脆弱性網羅状況の出力の評価

商用ツールで使用している脆弱性 DB の脆弱性情報の網羅状況を確認した。商用ツールの脆弱性 DB（ASPL）と CVE-DB との脆弱性保有関係は、図 24.の様になる。

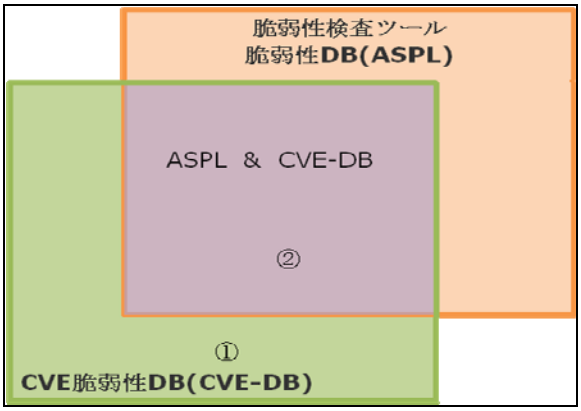
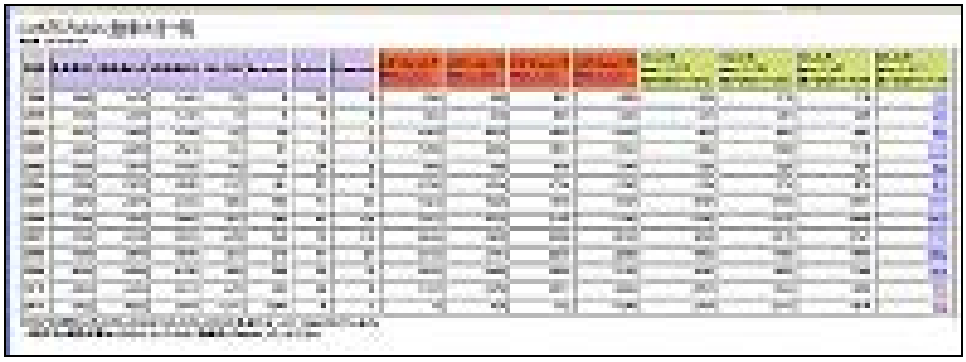


図 24. 脆弱性情報の保有関係

表 10は機器管理者、システム管理者用の画面で、3.4.1 d)の機能を使い、商用ツールの脆弱性 DB と CVE DB との対応を表示したものになる。CVE-DB に登録されている脆弱性のうち、商用ツールの脆弱性 DB に登録されていない脆弱性は図 24 ①となる。図 24 ①は商用ツールの脆弱性検査では検出できないため、どの程度の数の CVE-DB の脆弱性が収録されていないのか、年度毎に表として、②の部分についても商用ツールの脆弱性 DB 毎に表として提供できるようにした。

システム管理者はこれらの表を確認する事で新しい脆弱性が出た際にも商用ツールで対応が可能なものか、判断しやすくなり、新たに危険な脆弱性が見つかった際にも、既存の脆弱性 DB のアップデートが必要なのか、対応するまで時間がかかるためユーザへのアナウンスが必要なのかを素早く判断する事が可能になった。

表 10. 脆弱性情報の保有状況



（注意: 表 10は、便宜上①②の値が判別できないようにしている）

5. 今後の展開

「情報セキュリティ脆弱性リスク管理システム」は、商用ツール、KEK ポータルに J-PARC 要望を組込んだ J-PARC 版ポータル及び J-PARC 独自機能を提供する Add-On サブシステムにより構成されている。J-PARC 独自に組込んだ機能のうち、いくつかの機能はその有用性から、今後 KEK ポータルに取り込む検討がなされている。

また今後は、ネットワーク監視機器の情報や、ファイアウォール機器のログ以外にも機器管理者に有用な情報であれば、機器管理者に利用しやすい形にした上で積極的に情報を提供していく予定である。

6. まとめ

「情報セキュリティ脆弱性リスク管理システム」の開発をしたことで、これまで実現できていなかった定期的な情報セキュリティ脆弱性検査及び機器管理者自身による手動検査が、実施できるようになった。また、以前から実施していたシステム構築時の公開前脆弱性検査及び運用開始後からの定期脆弱性検査により、システム構築時～運用終了までのライフサイクル期間中、常に脆弱性検査する運用環境を整備できた。

また、セキュリティ関係の他システムとの連携では、情報の見せ方を工夫することで、脆弱性に対する啓蒙活動を進めることができた。これは機器管理者へ PDCA サイクルの Plan、Check を促す事に繋がり、PDCA サイクル全体を後押しする事が出来た。今後は PDCA サイクルが継続するために、機器管理者にとって有益な情報はなにかを常に考え、アイディアを提供していく必要があると考える。

謝辞

「情報セキュリティ脆弱性リスク管理システム」は、商用ツール、J-PARC 版ポータル及び同ポータル Add-On サブシステムより構成されています。

J-PARC 版ポータルは、高エネルギー加速器研究機構（KEK）で運用中の DMZ User's Portal を元に開発しました。DMZ User’s Portal の関係者の皆様（KEK 金子敏明氏、湯浅富久子氏、川端節彌氏、セキュリティグループの諸氏、セキュリティ管理部会の諸氏）に感謝の意を表します。Add-On サブシステムは、J-PARC 版ポータルの Add-On 機能として J-PARC センターで新規に開発しました。Add-On サブシステム開発に当たっては、Web アプリケーションフレームワーク全般の技術的助言及び協力をいただきました（株）ケーシーエス 田邉 豪信氏に感謝の意を表します。

また、同システムの開発にあたって有益な助言いただきました、J-PARC センター 情報システムセクションの関係者各位に感謝を表します。さらに、本報告書をまとめるに当たって適切な助言をいただいた J-PARC センター 情報システムセクション セクションリーダー 真鍋篤氏、同サブセクションリーダー五來一夫氏に厚く御礼申し上げます。

参考文献

[1] Tadashi Murakami, Fukuko Yuasa, Toshiaki Kaneko, "Vulnerability Management by the Integration of Security Resources and Devices with DBPowder, " Grid Camp and HEPiX Fall 2008, Oct. 2008

[2] 村上 直, “DBPowder-mdl: EoD と記述力を兼備した O/R マッピング言語,” 情報処理学会論文誌：データベース, Vol.3, No.3（TOD47）, pp.46-67, Sep. 2010.

[3] 高エネルギー加速器研究機構,“Activity Report 2009, Computing Research Center,” KEK Progress Report 2010-1，Oct. 2010

[4] 石川弘之, "平成 22 年度 熊本大学 綜合技術研究会 報告集", Mar 2011, 05 情報・ネットワーク技術分野 05B II-2 , "J-PARC センター基幹 LAN におけるセキュリティ対策について"

[5] 独立行政法人 情報処理推進機構, "共通脆弱性評価システム CVSS 概説" http://www.ipa.go.jp/security/vuln/CVSS.html, Sep. 2011

[6] 独立行政法人 情報処理推進機構, "共通脆弱性識別子 CVE 概説 http://www.ipa.go.jp/security/vuln/CVE.html, Sep.2011

[7] JPCERT コーディネーションセンター及び独立行政法人 情報処理推進機構, "JVN 脆弱性レポートの読み方" http://jvn.jp/nav/jvnhelp.html, Sep. 2011

[8] Flash Force Directed Layout Graph http://www.intsysr.com/force.htm

[9] Hummingbird http://hummingbirdstats.com/

[10] AmChart http://www.amcharts.com/

[11] Cacti http://www.cacti.net/

[12] Apache/Xindice http://xml.apache.org/xindice/

[13] Apache/Tomcat http://tomcat.apache.org/

[14] Subversion http://subversion.apache.org/

付録 1.「情報セキュリティ脆弱性リスク管理システム」の利用者画面イメージ

掲載画面一覧

1.J-PARC 版ポータル

画面1-1. J-PARC 版ポータルログイン画面
画面1-2. お知らせ画面
画面1-3. 脆弱性一覧画面
画面1-4. 診断レポート画面
画面1-5. レポートダウンロード画面
画面1-6. レポート提出画面
画面1-7. 診断不能証明提出画面
画面1-8. パスワード変更画面
画面1-9. 商用ツールからの疎通確認画面

2.Add-On サブシステム

画面2-1. 管理ホスト一覧表示画面
画面2-2. 脆弱性検査結果時系列表示画面
画面2-3. 脆弱性検査結果詳細及び時系列表示画面
画面2-4. 脆弱性検査スコア時系列グラフ表示画面
画面2-5. 脆弱性検査結果詳細画面
画面2-6. 脆弱性 ID の詳細表示画面
画面2-7. CVSS 分析グラフ表示画面
画面2-8. ソーシャルグラフ表示画面
画面2-9. ファイアウォールアクセスログ表示画面
画面2-10. ファイアウォールアクセスログリアルタイム流量及びアクセス元地域表示
画面2-11. スイッチ接続ポート情報表示画面
画面2-12. 管理者からのメッセージ表示画面
画面2-13. 疎通/脆弱性検査結果履歴表示画面
画面2-14. CVE 及び脆弱性検査用シグネチャ登録状況表示画面
画面2-15. 脆弱性検査用シグネチャと CVE 情報の対応表示画面
画面2-16. 脆弱性検査用シグネチャに収録されていない CVEID の一覧表示画面

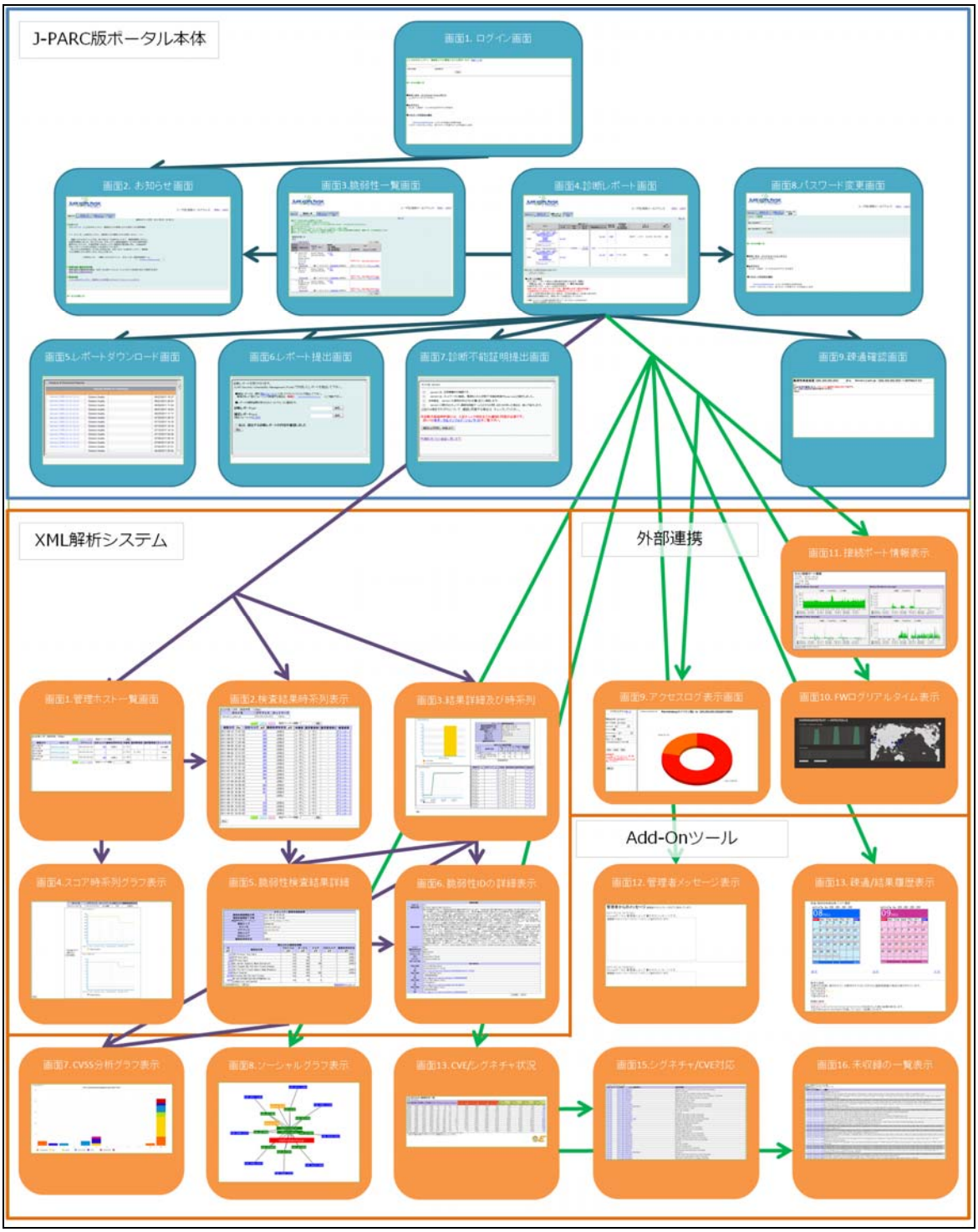


Fig.1.J-PARC 版ポータル及び Add-On サブシステムを含んだ画面遷移図

1.J-PARC 版ポータル

画面 1-1.J-PARC 版ポータルログイン画面

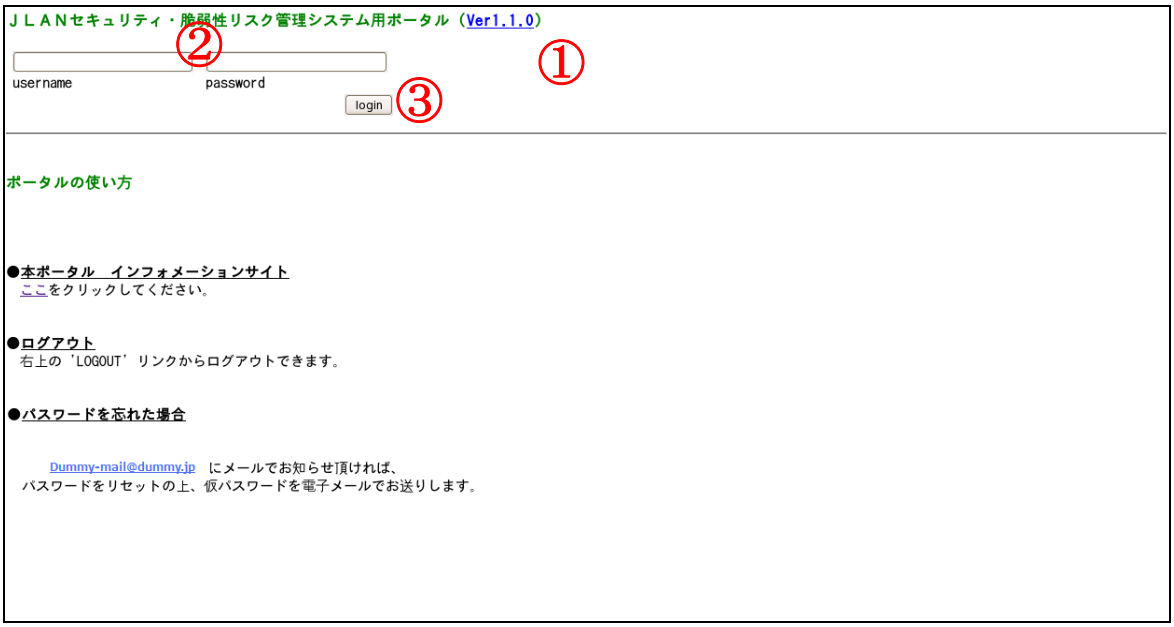


Fig.2.ポータルログイン画面

画面内容

①ポータル更新履歴情報

②ログイン ID 及びパスワード入力欄

③ログインボタン

画面 1-2.お知らせ画面

Fig.3.ポータルお知らせ画面

画面内容

①ユーザ名及び登録メールアドレス表示

②再読込及びログアウトリンク

③他画面リンクタブ

④管理者からのメッセージ表示

⑤インフォメーションサイトへのリンク

画面 1-3.脆弱性一覧画面

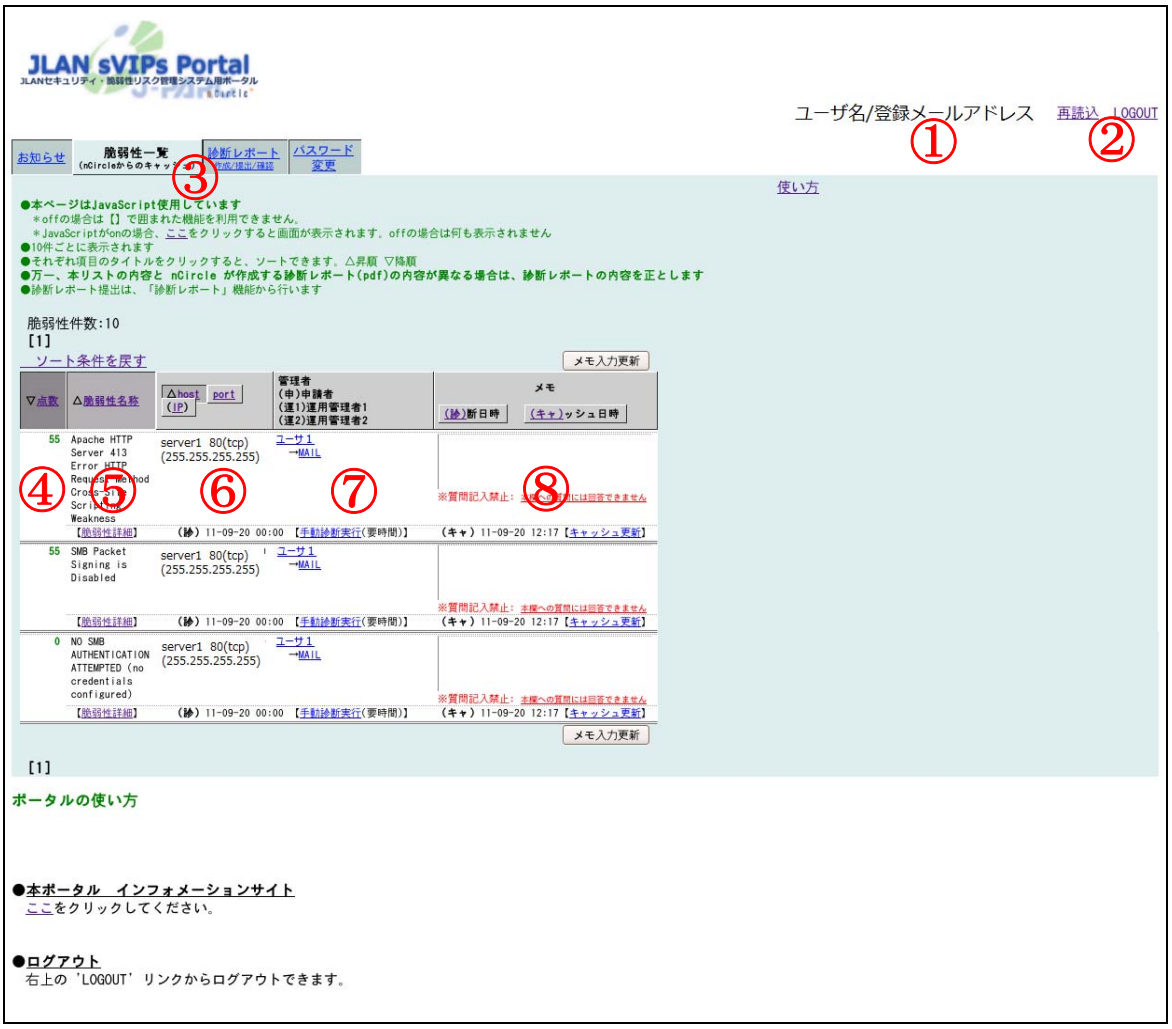


Fig.4.脆弱性一覧画面

画面内容

①ユーザ名及び登録メールアドレス表示

②再読込及びログアウトリンク

③他画面リンクタブ

④脆弱性スコア表示

⑤脆弱性名称表示及び脆弱性詳細情報表示リンク

⑥脆弱性対象サーバ及び検出プロトコル表示

⑦脆弱性対象サーバ管理者表示及び手動脆弱性検査実行リンク

⑧メモ入力欄及び表示内容更新リンク

画面 1-4.診断レポート画面

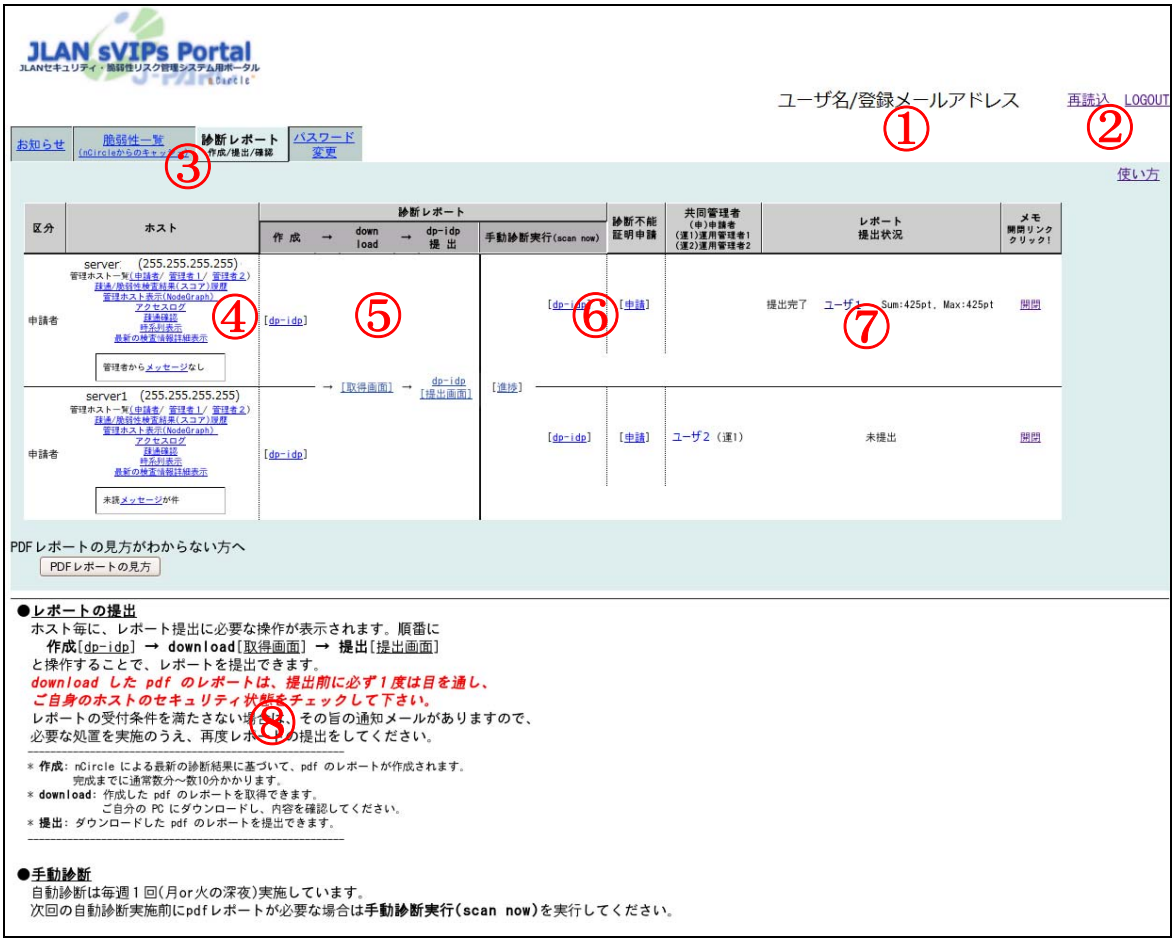


Fig.5.診断レポート画面

画面内容

①ユーザ名及び登録メールアドレス表示

②再読込及びログアウトリンク

③他画面リンクタブ

④管理サーバ名及び Add-On サブシステム用リンク

⑤脆弱性検査レポートの作成及びダウンロード及びレポート提出用リンク

⑥手動脆弱性検査実行リンク及び進捗状況確認及び診断不能証明提出用リンク

⑦脆弱性対象サーバ管理者表示及びレポートの提出状況表示

⑧レポート提出時の説明文表示

画面 1-5.レポートダウンロード画面

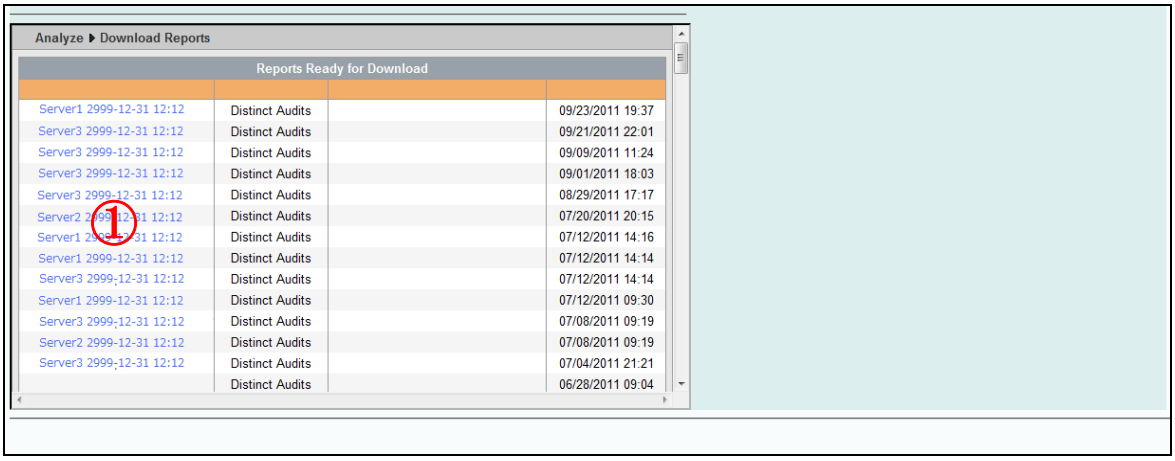


Fig.6.レポートダウンロード画面

画面内容

①レポートダウンロード用リンク

画面 1-6.レポート提出画面

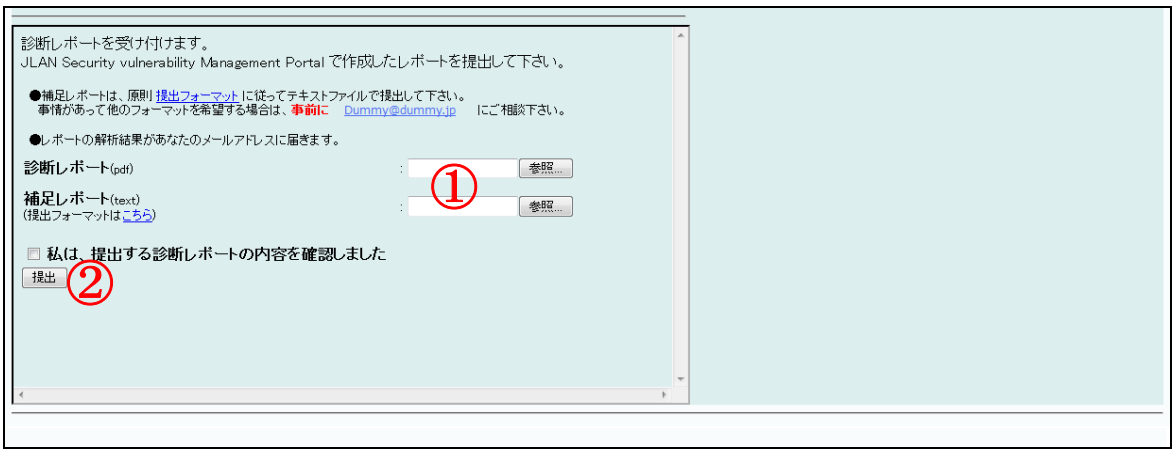


Fig.7.レポート提出画面

画面内容
①提出レポート選択用ボタン
②提出ボタン

画面 1-7.診断不能証明提出画面

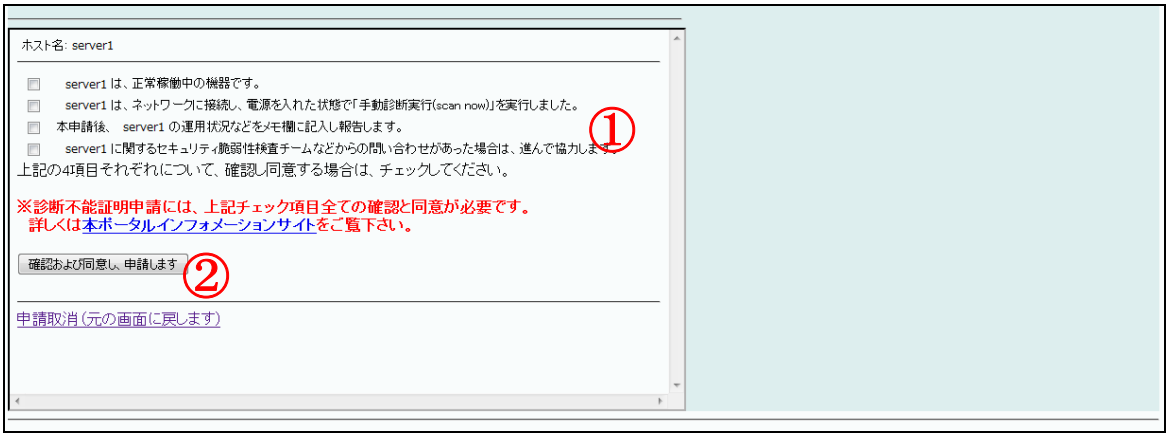


Fig.8.診断不能証明提出画面

画面内容

①同意事項チェックボックス

②提出ボタン

画面 1-8.パスワード変更画面

Fig.9.パスワード変更画面

画面内容

①ユーザ名及び登録メールアドレス表示

②再読込及びログアウトリンク

③他画面リンクタブ

④新パスワード入力欄

⑤パスワード変更ボタン

画面 1-9.商用ツールからの疎通確認画面

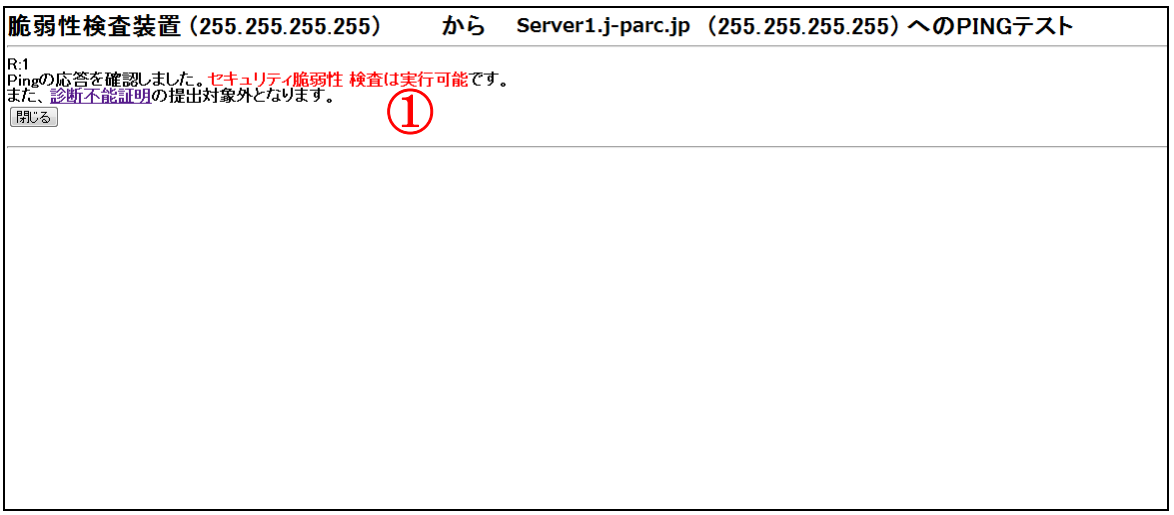


Fig.10.商用ツールからの疎通確認画面

画面内容

①商用ツールから対象ホストへの疎通確認結果表示

Add-On サブシステム

画面 2-1.管理ホスト一覧表示画面

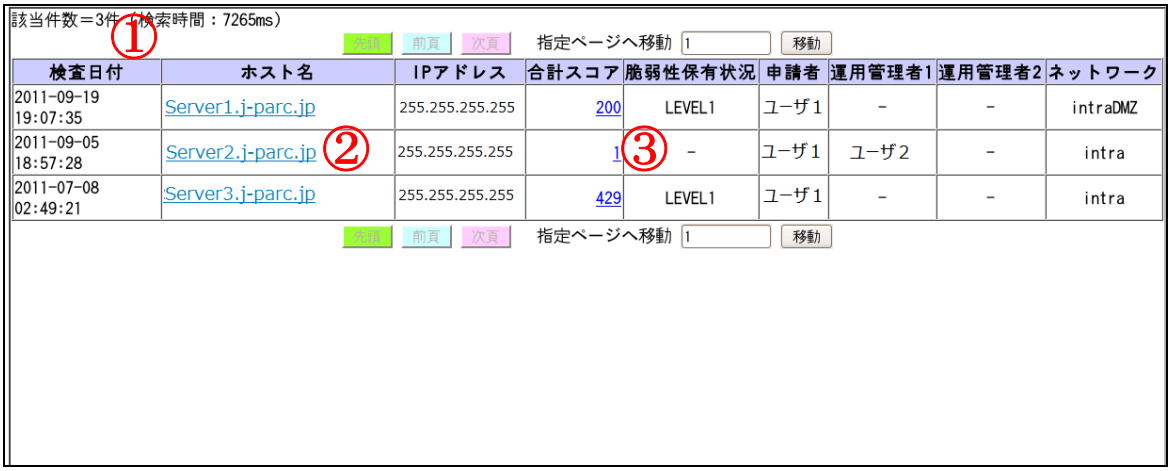


Fig.11.管理ホスト一覧

画面内容

①条件に該当した件数の表示

②ホスト名表示及びホストごとの脆弱性検査結果時系列表示画面へのリンク

③最新の脆弱性検査結果合計スコア表示及び選択したホストの脆弱性検査スコア時系列グラフ表示画面へのリンク

画面 2-2.脆弱性検査結果時系列表示画面

該当件数＝29件（検索時間：1155ms）

ホスト名	IPアドレス	ネットワーク
Server1.j-parc.jp	255.255.255.255	intra

先頭 前頁 次頁 指定ページへ移動 1 移動

検査日付 ▼▲	合計スコア ▲▼	脆弱性保有状況 ▲▼	申請者	運用管理者1	運用管理者2	検査結果
2011-09-19 17:07:24	591	LEVEL5	ユーザ1	ユーザ2	-	ダウンロード
2011-09-13 17:14:55	590	LEVEL5	ユーザ1	ユーザ2	-	ダウンロード
2011-09-05 17:14:16	589	LEVEL5	ユーザ1	ユーザ2	-	ダウンロード
2011-08-29 17:25:08	589	LEVEL5	ユーザ1	ユーザ2	-	ダウンロード
2011-08-08 16:43:14	586	LEVEL5	ユーザ1	ユーザ2	-	ダウンロード
2011-08-05 09:10:45	586	LEVEL5	ユーザ1	ユーザ2	-	ダウンロード
2011-08-04 12:31:57	586	LEVEL5	ユーザ1	ユーザ2	-	ダウンロード
2011-08-01 16:57:29	585	LEVEL5	ユーザ1	ユーザ2	-	ダウンロード
2011-07-25 17:14:35	260	LEVEL4	ユーザ1	ユーザ2	-	ダウンロード
2011-07-21 02:28:02	325	LEVEL5	ユーザ1	ユーザ2	-	ダウンロード
2011-07-20 02:37:14	584	LEVEL5	ユーザ1	ユーザ2	-	ダウンロード
2011-07-18 17:00:00	584	LEVEL5	ユーザ1	ユーザ2	-	ダウンロード
2011-07-12 01:00:31	584	LEVEL5	ユーザ1	ユーザ2	-	ダウンロード
2011-07-11 16:56:18	584	LEVEL5	ユーザ1	ユーザ2	-	ダウンロード
2011-07-08 09:02:09	0	LEVEL1	ユーザ1	ユーザ2	-	ダウンロード
2011-07-04 19:38:50	582	LEVEL5	ユーザ1	ユーザ2	-	ダウンロード
2011-06-27 18:36:15	581	LEVEL5	ユーザ1	ユーザ2	-	ダウンロード
2011-06-20 18:58:15	581	LEVEL5	ユーザ1	ユーザ2	-	ダウンロード
2011-06-15 06:09:00	0	LEVEL1	ユーザ1	ユーザ2	-	ダウンロード
2011-06-15 04:52:34	0	-	ユーザ1	ユーザ2	-	ダウンロード
2011-06-13 19:22:23	579	LEVEL5	ユーザ1	ユーザ2	-	ダウンロード
2011-06-06 19:50:54	579	LEVEL5	ユーザ1	ユーザ2	-	ダウンロード
2011-05-30 20:13:29	578	LEVEL5	ユーザ1	ユーザ2	-	ダウンロード
2011-05-23 19:53:02	576	LEVEL5	ユーザ1	ユーザ2	-	ダウンロード

先頭 前頁 次頁 指定ページへ移動 1 移動

戻る

Fig.12. 脆弱性検査結果時系列表示画面

画面内容

①該当件数及びホスト名 IP アドレス及び登録ネットワーク表示

②該当する検査日付の脆弱性検査合計スコア表示及び脆弱性検査結果詳細及び時系列表示画面へのリンク

③該当する検査日付の脆弱性検査結果 XML データのダウンロードリンク

画面 2-3.脆弱性検査結果詳細及び時系列表示画面

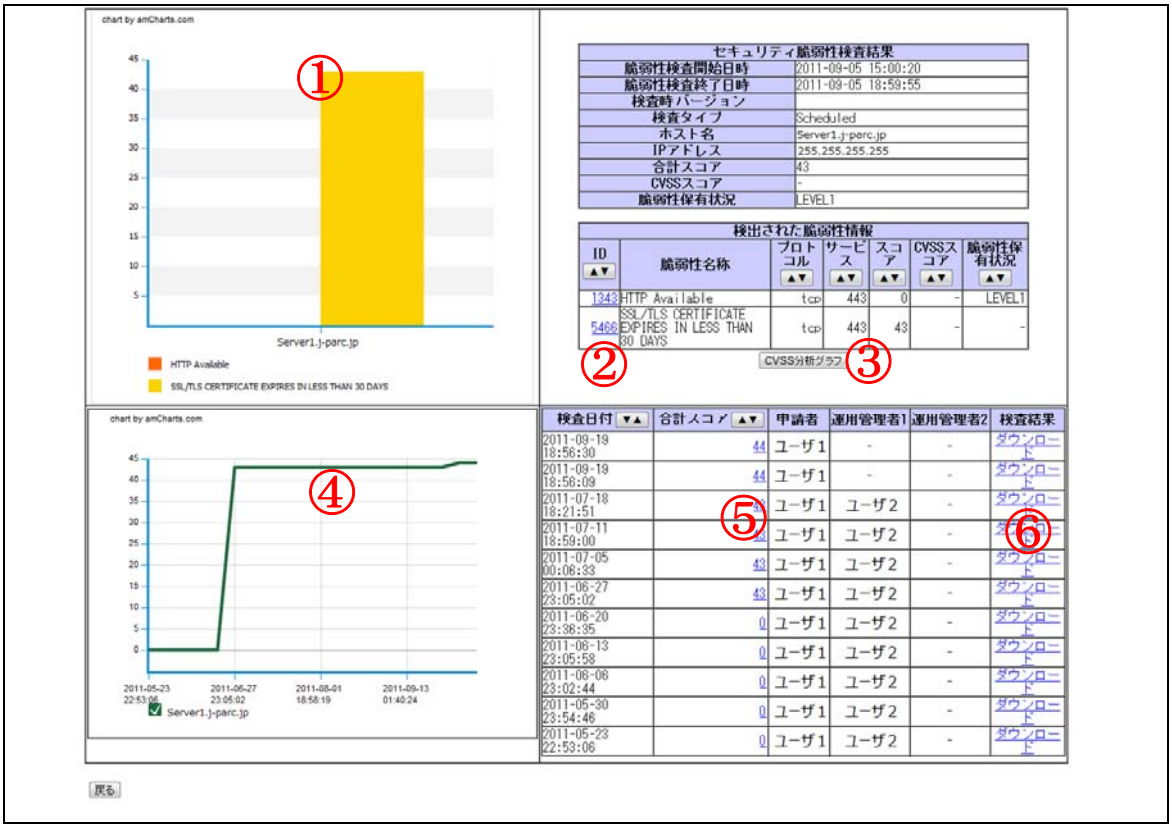


Fig.13. 脆弱性検査結果詳細及び時系列表示画面

画面内容

①検出された脆弱性毎のスコアグラフ表示

②該当する脆弱性の詳細情報表示リンク

③該当する検査結果の CVSS 分析グラフ表示へのリンク

④脆弱性検査スコア時系列グラフ表示

⑤該当する検査日時の脆弱性検査結果詳細へのリンク

⑥該当する検査日付の脆弱性検査結果 XML データのダウンロードリンク

画面 2-4. 脆弱性検査スコア時系列グラフ表示画面

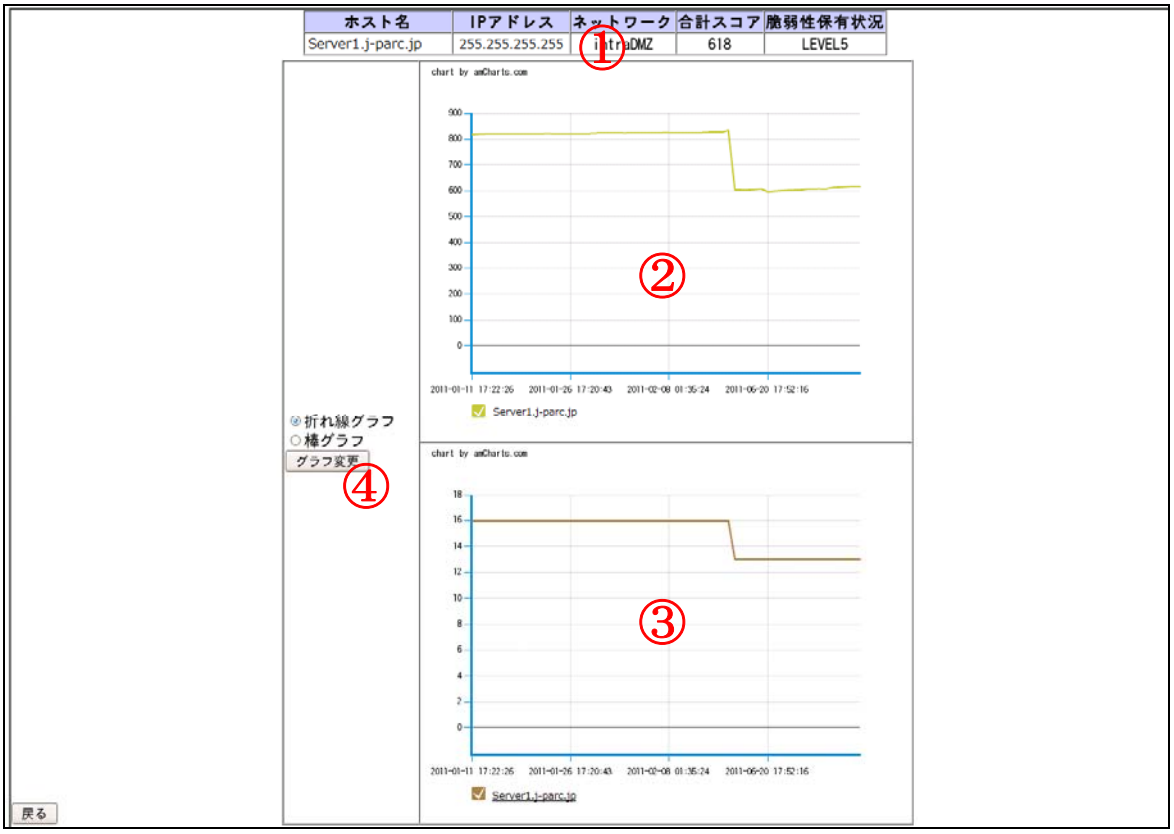


Fig.14. 脆弱性検査スコア時系列グラフ表示画面

画面内容

①ホスト情報の表示

②脆弱性検査合計スコアの時系列表示

③脆弱性検査 CVSS 合計スコアの時系列表示

④グラフ種別切り替えボタン

画面 2-5. 脆弱性検査結果詳細画面

セキュリティ脆弱性検査結果	
脆弱性検査開始日時	2011-09-19 15:00:30
脆弱性検査終了日時	2011-09-19 17:07:24
検査時 バージョン	
検査タイプ	Scheduled
ホスト名	Server1.j-parc.jp ①
IPアドレス	255.255.255.255
合計スコア	591
CVSSスコア	-
脆弱性保有状況	LEVEL5

検出された脆弱性情報

ID ▲▼	脆弱性名称	プロトコル ▲▼	サービス ▲▼	スコア ▲▼	CVSSスコア ▲▼	脆弱性保有状況 ▲▼
1191	SSH Protocol Available	tcp	22	0	-	LEVEL1
1343	HTTP Available	tcp	80	0	-	LEVEL1
1343	HTTP Available	tcp	443	0	-	LEVEL1
6174	SSL Server Supports Weak Encryption	tcp	443	330	-	LEVEL5
62	Self-Signed SSL/TLS Certificate Present	tcp	443	0	-	-
6214	SSL/TLS Certificate Domain Name Mismatch	tcp	443	1	-	LEVEL3
6766	SSLv2 Enabled	tcp	443	260	-	LEVEL4
26188	Untrusted SSL/TLS Certificate	tcp	443	0	-	-
30535	NO SSH AUTHENTICATION ATTEMPTED (no credentials configured)	tcp	22	0	-	-

CVSS分析グラフ ③ 閉じる　　検査結果ダウンロード ④

Fig.15. 脆弱性検査結果詳細画面

画面内容

①ホスト情報及び脆弱性検査時の環境情報表示

②該当する脆弱性の詳細情報表示リンク

③脆弱性検査結果の CVSS 分析グラフ表示へのリンク

④脆弱性検査結果 XML データのダウンロードリンク

画面 2-6. 脆弱性 ID の詳細表示画面

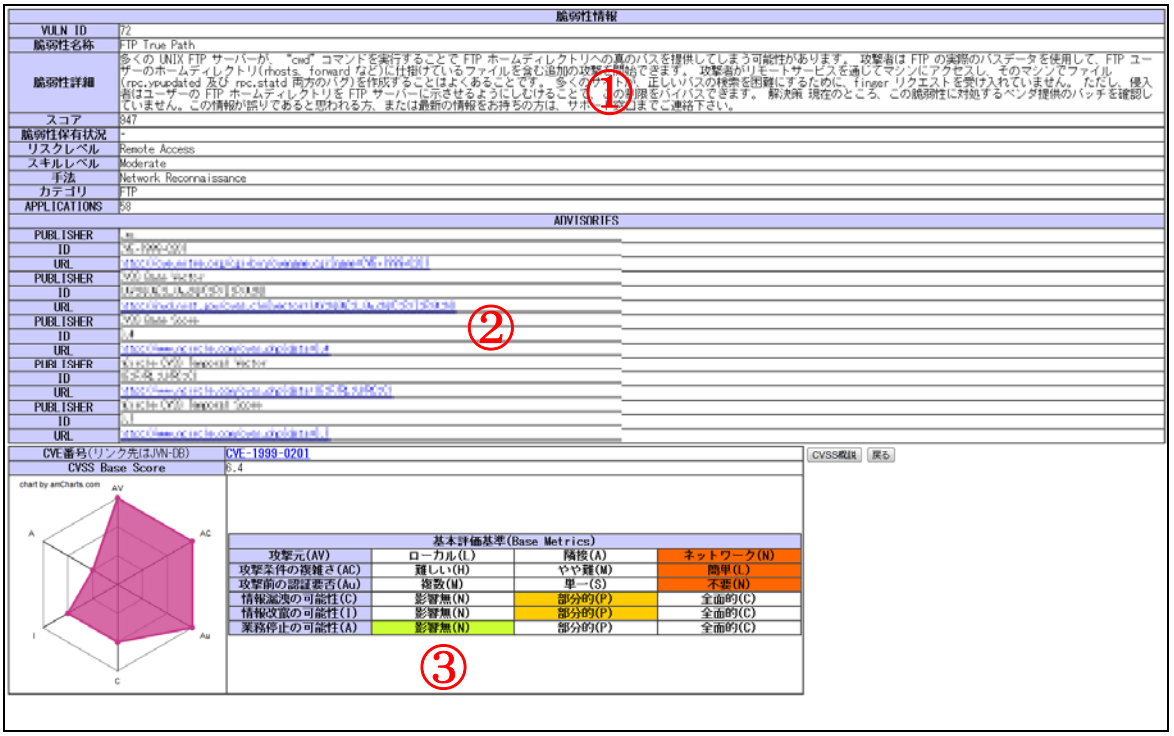


Fig.16. 脆弱性 ID の詳細表示画面

画面内容

①脆弱性情報の表示

②脆弱性情報の外部解説サイトへのリンク

③CVSS スコア概要グラフ表示

画面 2-7. CVSS 分析グラフ表示画面

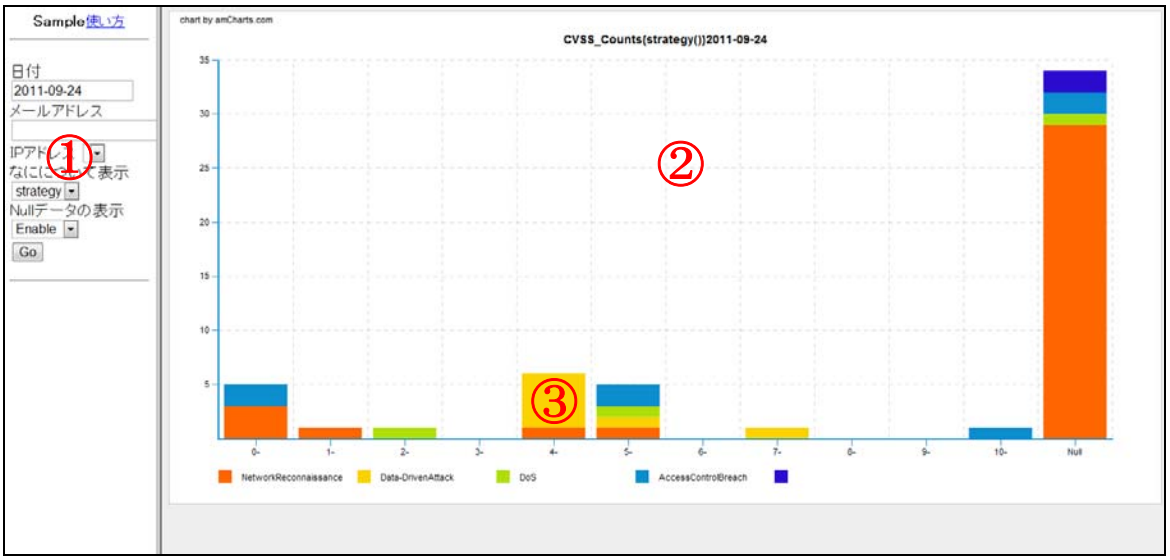


Fig.17. CVSS 分析グラフ表示画面

画面内容

①表示内容の選択及び切り替えボタン

②CVSS 分析グラフ表示

③該当する脆弱性 ID 毎の詳細表示へのリンク(画面 2-6)

画面 2-8. ソーシャルグラフ表示画面

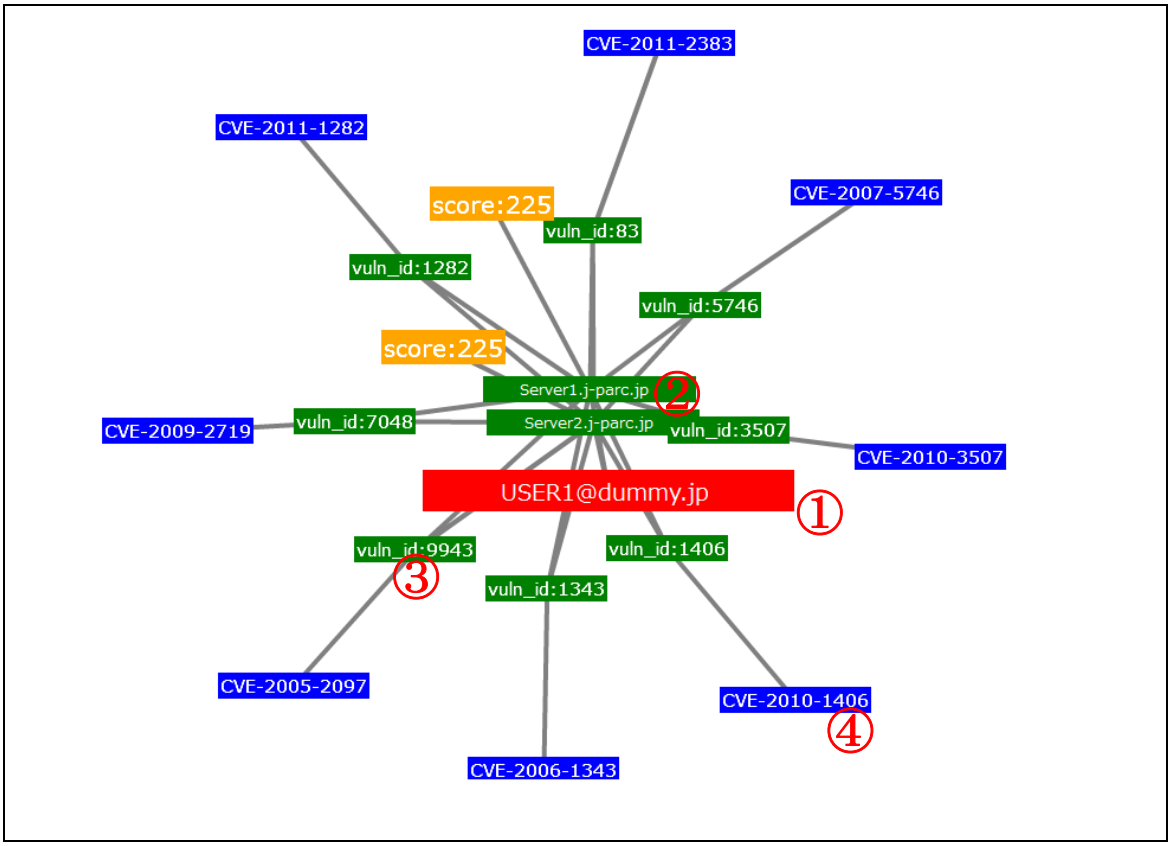


Fig.18. ソーシャルグラフ表示画面

画面内容
①管理者メールアドレス表示
②選択されたホストのソーシャルグラフ表示へのリンク
②選択された脆弱性 ID の詳細表示へのリンク
③選択された CVEID の詳細情報への外部リンク

画面 2-9. ファイアウォールアクセスログ表示画面

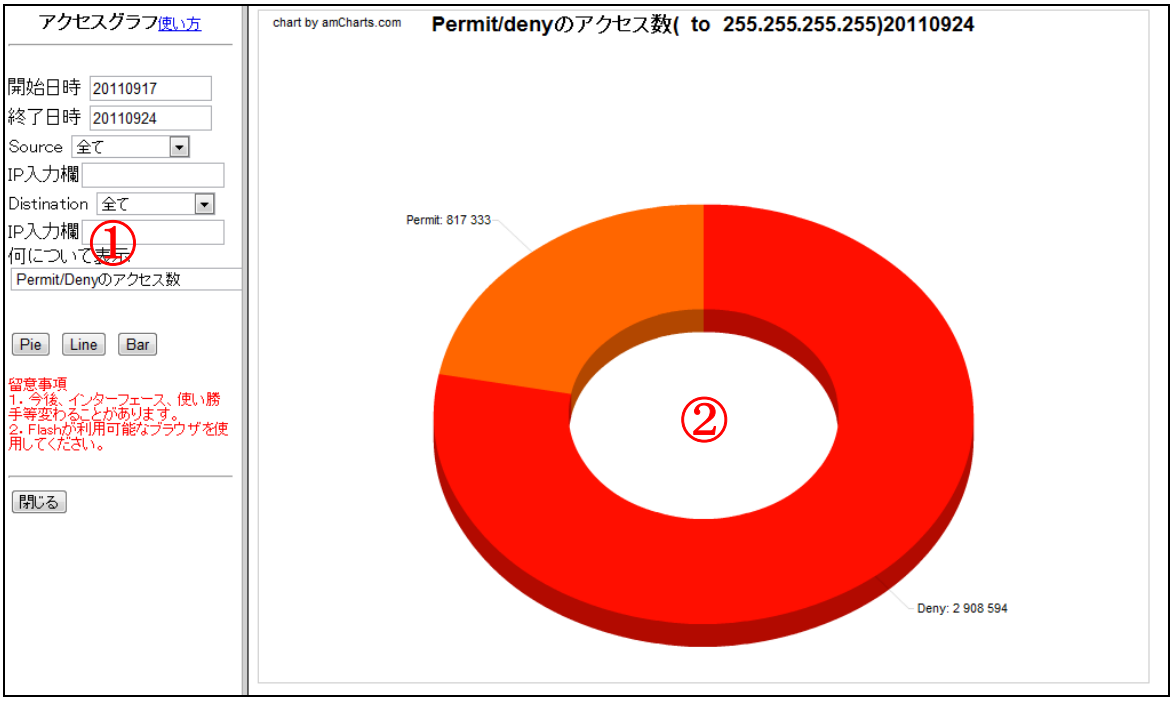


Fig.19. ファイアウォールアクセスログ表示画面

画面内容

①表示する条件及びグラフ形式切り替えボタン

②選択された条件に合致するグラフ表示

画面 2-10. ファイアウォールアクセスログリアルタイム流量及びアクセス元地域表示

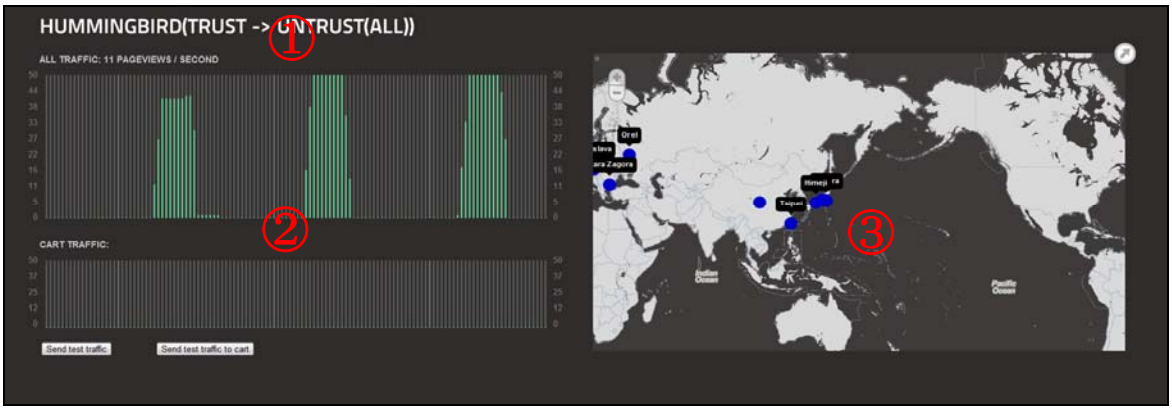


Fig.20. ファイアウォールアクセスログリアルタイム流量及びアクセス元地域表示

画面内容
①表示している内容の表示
②現在の流量を表示
③アクセス元地域を表示

画面 2-11. スイッチ接続ポート情報表示画面

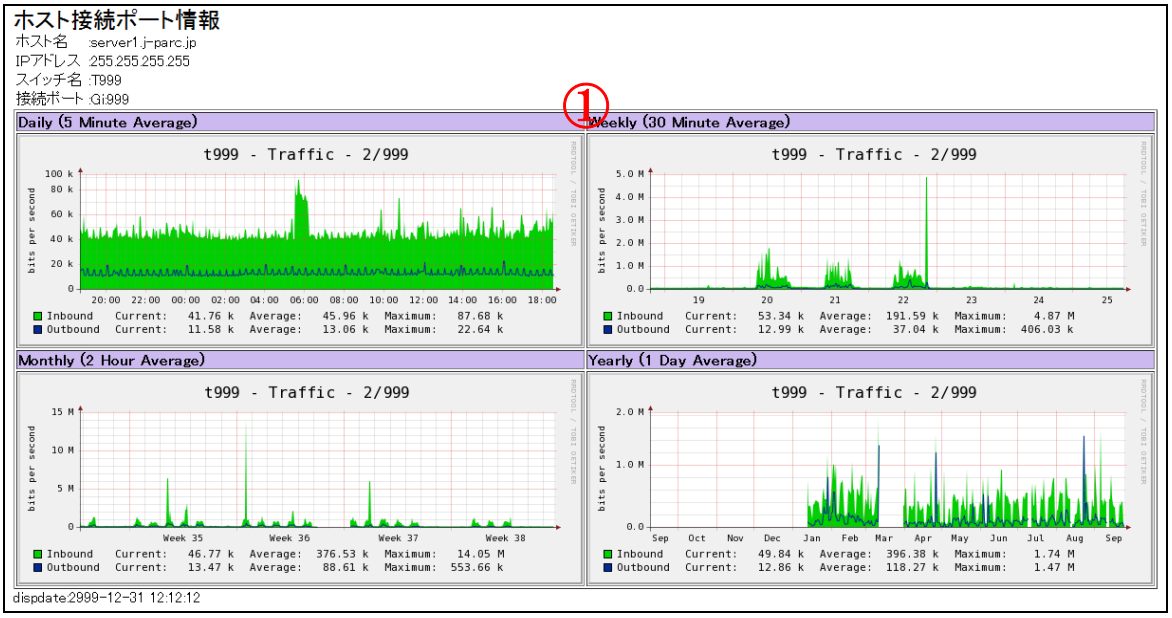


Fig.21. スイッチ接続ポート情報表示画面

画面内容

①該当するホストが接続されているスイッチのポート情報の表示

画面 2-12. 管理者からのメッセージ表示画面

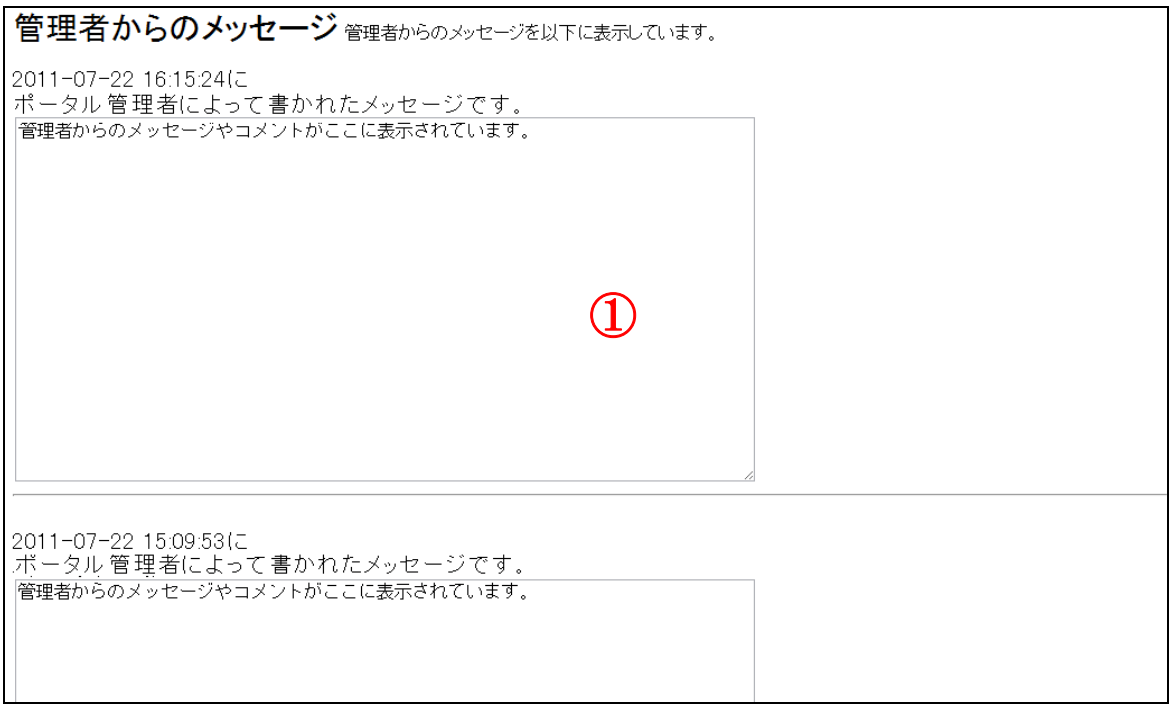


Fig.22. 管理者からのメッセージ表示画面

画面内容

①選択されたホストへの管理者からのメッセージ表示

画面 2-13. 疎通/脆弱性検査結果履歴表示画面

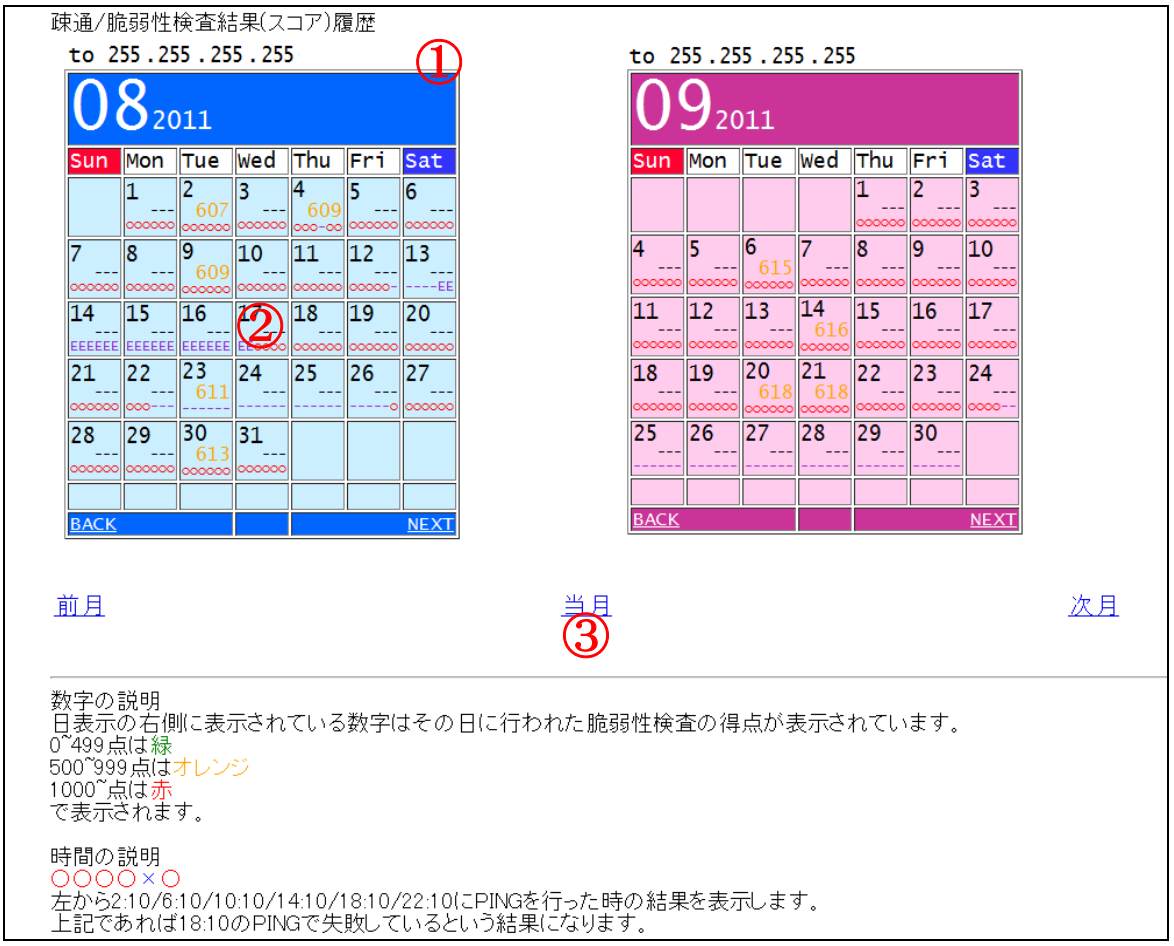


Fig.23. 疎通/脆弱性検査結果履歴表示画面

画面内容

①表示対象 IP アドレス表示

②カレンダー形式による商用ツールからの疎通確認結果及び脆弱性検査合計スコアの表示

③表示月切り替えリンク

画面 2-14. CVE 及び脆弱性検査用シグネチャ登録状況表示画面

CVE及び脆弱性登録状況一覧

作成日 2011/09/24

年度	最終番号	登録数(A)	有効数(B)	(A)-(B)	Reserve	Reject	Disputed								
1999	1593	1573	1540	33	0	33	0	834	830	821	822	706	710	719	718
2000	1246	1235	1235	0	0	0	0	854	854	846	846	381	381	389	389
2001	1587	1566	1534	32	28	2	2	1053	1053	1053	1053	481	481	481	481
2002	2434	2422	2341	81	57	19	5	1235	1235	1231	1231	1106	1106	1110	1110
2003	1596	1591	1493	98	76	20	2	968	968	966	970	525	525	527	523
2004	2769	2767	[illegible]	137	101	27	9	1756	[illegible]	1754	1760	874	870	876	870
2005	4889	4887	[illegible]	306	203	71	32	1943	[illegible]	1960	1982	2638	2630	2621	2599
2006	7245	7245	[illegible]	397	205	63	129	2072	[illegible]	2168	2198	4776	4776	4680	4650
2007	6743	6743	6315	428	243	73	112	2499	2505	2568	2612	3816	3810	3747	3703
2008	7299	7299	6950	349	275	47	27	2148	2161	2255	2288	4802	4789	4695	4662
2009	5095	5095	4786	309	266	30	13	2976	2986	3020	3132	1810	1800	1766	1654
2010	4833	4833	4413	420	386	28	6	1722	2569	3017	3848	2691	1844	1396	565
2011	3422	3422	2151	1271	1265	5	1	0	134	772	1379	2151	2017	1379	772

*2004年は更にCVE-2004-9998とCVE-2004-9999が存在(ステータス: Reject)しています。
上記2件は集計対象から外されているため、登録数とRejectに+2してください

Fig.24. CVE 及び脆弱性検査用シグネチャ登録状況表示画面

画面内容

①CVE 登録状況表示

②脆弱性検査用シグネチャ内で CVE 情報と対応が取れる物の個数を表示

③CVE 情報内でしか管理されていない脆弱性情報の個数を表示

④選択したバージョンの脆弱性検査用シグネチャと CVE 情報の対応表へのリンク

⑤選択した年度の脆弱性検査用シグネチャに収録されていない CVEID の一覧へのリンク

画面 2-15. 脆弱性検査用シグネチャと CVE 情報の対応表示画面

ver:

JVNへのリンク	CVE番号	脆弱性ID	脆弱性概要
JVN-DB	CVE-1999-0003	2079/	Multiple Vendor ToolTalk RPC Service Overflow Vulnerability
JVN-DB	CVE-1999-0005	808/	IMAP/POP buffer
JVN-DB	CVE-1999-0006	813/	Qualcomm POP Server Buffer Overflow Vulnerability
JVN-DB	CVE-1999-0007	9443/	MS98-002- Microsoft IIS 3.0 and 4.0 SSL "Error Message" Vulnerability
JVN-DB	CVE-1999-0008	2122/	Multiple Vendor NIS+ Buffer Overflow Vulnerability
JVN-DB	CVE-1999-0009	400/	BIND Inverse Query Overflow
JVN-DB	CVE-1999-0010	24/	BIND Malformed Query DoS
JVN-DB	CVE-1999-0012	2443/	Microsoft IIS And PWS 8.3 Directory Name Vulnerability
JVN-DB	CVE-1999-0016	7216/5416/3153/	FreeBSD loopback (land) Denial of Service Vulnerability
JVN-DB	CVE-1999-0017	1526/	FTP Bounce (ports >= 1024)
JVN-DB	CVE-1999-0018	1418/	RPC statd Available
JVN-DB	CVE-1999-0021	946/	Count.cgi
JVN-DB	CVE-1999-0022	7226/	FreeBSD rdist Buffer Overflow Vulnerability
JVN-DB	CVE-1999-0023	7226/	FreeBSD rdist Buffer Overflow Vulnerability
JVN-DB	CVE-1999-0024	1829/1830/	Multiple Vendor BIND Cache Poisoning Vulnerability
JVN-DB	CVE-1999-0032	7225/	FreeBSD lpr Buffer Overflow Vulnerability
JVN-DB	CVE-1999-0039	957/	IRIX cgi-bin webdist.cgi Vulnerabilty
JVN-DB	CVE-1999-0042	395/	IMAP/POP LOGIN buffer
JVN-DB	CVE-1999-0043	3099/	Multiple Vendor INN remote Vulnerability
JVN-DB	CVE-1999-0045	672/	Multiple Vendor nph-test-cgi Vulnerability
JVN-DB	CVE-1999-0047	412/	Sendmail MIME Overflow
JVN-DB	CVE-1999-0048	7222/	FreeBSD talkd Buffer Overrun Vulnerability
JVN-DB	CVE-1999-0050	6885/	HP-UX newgrp Buffer Overflow Vulnerability
JVN-DB	CVE-1999-0052	7209/	FreeBSD TCP/IP Implementations Vulnerability
JVN-DB	CVE-1999-0053	7210/	FreeBSD TCP RST Denial of Service Vulnerability
JVN-DB	CVE-1999-0058	1383/	PHP.cgi
JVN-DB	CVE-1999-0059	1413/	RPC fam Available
JVN-DB	CVE-1999-0063	6265/	Cisco IOS Syslog Crash
JVN-DB	CVE-1999-0066	1388/	Anyform CGI Semicolon Vulnerability
JVN-DB	CVE-1999-0067	670/	phf Remote Command Execution Vulnerability
JVN-DB	CVE-1999-0068	1381/1383/5185/	Mylog.html
JVN-DB	CVE-1999-0070	1380/	Multiple Vendor test-cgi Directory Listing Vulnerability
JVN-DB	CVE-1999-0071	1221/	Apache mod_cookies Buffer Overflow Vulnerability
JVN-DB	CVE-1999-0075	9534/	ftpd PASV Crash Information Leakage Vulnerability

Fig.25. 脆弱性検査用シグネチャと CVE 情報の対応表示画面

画面内容

①CVEID を利用した JVN 脆弱性情報データベースの外部検索リンク

②選択された CVEID の詳細情報への外部リンク

③選択された脆弱性 ID の詳細表示へのリンク

④脆弱性の概要表示

画面 2-16 脆弱性検査用シグネチャに収録されていない CVEID の一覧表示画面

脆弱性検査用シグネチャに収録されていないCVE一覧
CVE発行年:2011
更新日:2011/09/24

JVNリンク	CVE番号	概要
JVN-DB	CVE-2011-0003	MediaWiki before 1.16.1
JVN-DB	CVE-2011-0004	Multiple cross-site scripting (XSS) vulnerabilities in Piwik before 1.1 allow remote attackers to inject arbitrary web script or HTML via unspecified vectors
JVN-DB	CVE-2011-0005	Cross-site scripting (XSS) vulnerability in the com_search module for Joomla! 1.0.x through 1.0.15 allows remote attackers to inject arbitrary web script or HTML via the ordering parameter to index.php
JVN-DB	CVE-2011-0006	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized
JVN-DB	CVE-2011-0007	pimd 2.1.5 and possibly earlier versions allows user-assisted local users to overwrite arbitrary files via a symlink attack on (1) pimd.dump when a USR1 signal is sent
JVN-DB	CVE-2011-0008	A certain Fedora patch for parse.c in sudo before 1.7.4p5-1.fc14 on Fedora 14 does not properly interpret a system group (aka %group) in the sudoers file during authorization decisions for a user who belongs to that group
JVN-DB	CVE-2011-0009	Best Practical Solutions RT 3.x before 3.8.9rc2 and 4.x before 4.0.0rc4 uses the MD5 algorithm for password hashes
JVN-DB	CVE-2011-0011	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized
JVN-DB	CVE-2011-0015	Tor before 0.2.1.29 and 0.2.2.x before 0.2.2.21-alpha does not properly check the amount of compression in zlib-compressed data
JVN-DB	CVE-2011-0016	Tor before 0.2.1.29 and 0.2.2.x before 0.2.2.21-alpha does not properly manage key data in memory
JVN-DB	CVE-2011-0017	The open_log function in log.c in Exim 4.72 and earlier does not check the return value from (1) setuid or (2) setgid system calls
JVN-DB	CVE-2011-0018	The email function in manage_sql.c in OpenVAS Manager 1.0.x through 1.0.3 and 2.0.x through 2.0.rc2 allows remote authenticated users to execute arbitrary commands via the (1) To or (2) From e-mail address in an OMP request to the Greenbone Security Assistant (GSA).
JVN-DB	CVE-2011-0019	slapd (aka ns-slapd) in 389 Directory Server 1.2.7.5 (aka Red Hat Directory Server 8.2.x or dirsrv) does not properly handle simple paged result searches
JVN-DB	CVE-2011-0022	The setup scripts in 389 Directory Server 1.2.x (aka Red Hat Directory Server 8.2.x)
JVN-DB	CVE-2011-0023	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized
JVN-DB	CVE-2011-0025	IcedTea 1.7 before 1.7.8
JVN-DB	CVE-2011-0044	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized
JVN-DB	CVE-2011-0046	Multiple cross-site request forgery (CSRF) vulnerabilities in Bugzilla before 3.2.10
JVN-DB	CVE-2011-0047	Cross-site scripting (XSS) vulnerability in MediaWiki before 1.16.2 allows remote attackers to inject arbitrary web script or HTML via crafted Cascading Style Sheets (CSS) comments
JVN-DB	CVE-2011-0048	Bugzilla before 3.2.10
JVN-DB	CVE-2011-0049	Directory traversal vulnerability in the _list_file_get function in lib/Majordomo.pm in Majordomo 2 before 20110131 allows remote attackers to read arbitrary files via .. (dot dot) sequences in the help command
JVN-DB	CVE-2011-0050	Cross-site scripting (XSS) vulnerability in the nonjs interface (interfaces/nonjs.pm) in CGI:IRC before 0.5.10 allows remote attackers to inject arbitrary web script or HTML via the R parameter
JVN-DB	CVE-2011-0052	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized
JVN-DB	CVE-2011-0060	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized
JVN-DB	CVE-2011-0063	The _list_file_get function in lib/Majordomo.pm in Majordomo 2 20110203 and earlier allows remote attackers to conduct directory traversal attacks and read arbitrary files via a ../../ sequence in the extra parameter to the help command
JVN-DB	CVE-2011-0068	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized
JVN-DB	CVE-2011-0078	Unspecified vulnerability in the Java Embedding Plugin (JEP) in Mozilla Firefox before 3.5.19 and 3.6.x before 3.6.17
JVN-DB	CVE-2011-0082	The X.509 certificate validation functionality in Mozilla Firefox 4.0.x through 4.0.1 does not properly implement single-session security exceptions

Fig.26. 脆弱性検査用シグネチャに収録されていない CVEID の一覧表示画面

画面内容

①CVEID を利用した JVN 脆弱性情報データベースの外部検索リンク

②選択された CVEID の詳細情報への外部リンク

③脆弱性の概要表示

国際単位系（SI）

表１．SI 基本単位

基本量	SI 基本単位	
	名称	記号
長さ	メートル	m
質量	キログラム	kg
時間	秒	s
電流	アンペア	A
熱力学温度	ケルビン	K
物質量	モル	mol
光度	カンデラ	cd

表２．基本単位を用いて表されるSI組立単位の例

組立量	SI 基本単位	
	名称	記号
面積	平方メートル	m^2
体積	立法メートル	m^3
速さ，速度	メートル毎秒	m/s
加速度	メートル毎秒毎秒	m/s^2
波数	毎メートル	m^{-1}
密度，質量密度	キログラム毎立方メートル	kg/m^3
面積密度	キログラム毎平方メートル	kg/m^2
比体積	立方メートル毎キログラム	m^3/kg
電流密度	アンペア毎平方メートル	A/m^2
磁界の強さ	アンペア毎メートル	A/m
量濃度[a]，濃度	モル毎立方メートル	mol/m^3
質量濃度	キログラム毎立法メートル	kg/m^3
輝度	カンデラ毎平方メートル	cd/m^2
屈折率[b]	（数字の）　1	1
比透磁率[b]	（数字の）　1	1

(a) 量濃度（amount concentration）は臨床化学の分野では物質濃度（substance concentration）ともよばれる。
(b) これらは無次元量あるいは次元１をもつ量であるが、そのことを表す単位記号である数字の１は通常は表記しない。

表３．固有の名称と記号で表されるSI組立単位

組立量	SI 組立単位			
	名称	記号	他のSI単位による表し方	SI基本単位による表し方
平面角	ラジアン[b]	rad	1 [b]	m/m
立体角	ステラジアン[b]	sr[c]	1 [b]	m^2/m^2
周波数	ヘルツ[d]	Hz		s^{-1}
力	ニュートン	N		$m\ kg\ s^{-2}$
圧力，応力	パスカル	Pa	N/m^2	$m^{-1}\ kg\ s^{-2}$
エネルギー，仕事，熱量	ジュール	J	N m	$m^2\ kg\ s^{-2}$
仕事率，工率，放射束	ワット	W	J/s	$m^2\ kg\ s^{-3}$
電荷，電気量	クーロン	C		s A
電位差（電圧），起電力	ボルト	V	W/A	$m^2\ kg\ s^{-3}\ A^{-1}$
静電容量	ファラド	F	C/V	$m^{-2}\ kg^{-1}\ s^4\ A^2$
電気抵抗	オーム	Ω	V/A	$m^2\ kg\ s^{-3}\ A^{-2}$
コンダクタンス	ジーメンス	S	A/V	$m^{-2}\ kg^{-1}\ s^3\ A^2$
磁束	ウエーバ	Wb	Vs	$m^2\ kg\ s^{-2}\ A^{-1}$
磁束密度	テスラ	T	Wb/m^2	$kg\ s^{-2}\ A^{-1}$
インダクタンス	ヘンリー	H	Wb/A	$m^2\ kg\ s^{-2}\ A^{-2}$
セルシウス温度	セルシウス度[e]	℃		K
光束	ルーメン	lm	cd sr[c]	cd
照度	ルクス	lx	lm/m^2	$m^{-2}\ cd$
放射性核種の放射能[f]	ベクレル[d]	Bq		s^{-1}
吸収線量, 比エネルギー分与, カーマ	グレイ	Gy	J/kg	$m^2\ s^{-2}$
線量当量, 周辺線量当量, 方向性線量当量, 個人線量当量	シーベルト[g]	Sv	J/kg	$m^2\ s^{-2}$
酸素活性	カタール	kat		$s^{-1}\ mol$

(a)SI接頭語は固有の名称と記号を持つ組立単位と組み合わせても使用できる。しかし接頭語を付した単位はもはやコヒーレントではない。
(b)ラジアンとステラジアンは数字の１に対する単位の特別な名称で、量についての情報をつたえるために使われる。実際には、使用する時には記号rad及びsrが用いられるが、習慣として組立単位としての記号である数字の１は明示されない。
(c)測光学ではステラジアンという名称と記号srを単位の表し方の中に、そのまま維持している。
(d)ヘルツは周期現象についてのみ、ベクレルは放射性核種の統計的過程についてのみ使用される。
(e)セルシウス度はケルビンの特別な名称で、セルシウス温度を表すために使用される。セルシウス度とケルビンの単位の大きさは同一である。したがって、温度差や温度間隔を表す数値はどちらの単位で表しても同じである。
(f)放射性核種の放射能（activity referred to a radionuclide）は、しばしば誤った用語で"radioactivity"と記される。
(g)単位シーベルト（PV,2002,70,205）についてはCIPM勧告2（CI-2002）を参照。

表４．単位の中に固有の名称と記号を含むSI組立単位の例

組立量	SI 組立単位		
	名称	記号	SI 基本単位による表し方
粘度	パスカル秒	Pa s	$m^{-1}\ kg\ s^{-1}$
力のモーメント	ニュートンメートル	N m	$m^2\ kg\ s^{-2}$
表面張力	ニュートン毎メートル	N/m	$kg\ s^{-2}$
角速度	ラジアン毎秒	rad/s	$m\ m^{-1}\ s^{-1}=s^{-1}$
角加速度	ラジアン毎秒毎秒	rad/s^2	$m\ m^{-1}\ s^{-2}=s^{-2}$
熱流密度，放射照度	ワット毎平方メートル	W/m^2	$kg\ s^{-3}$
熱容量，エントロピー	ジュール毎ケルビン	J/K	$m^2\ kg\ s^{-2}\ K^{-1}$
比熱容量，比エントロピー	ジュール毎キログラム毎ケルビン	J/(kg K)	$m^2\ s^{-2}\ K^{-1}$
比エネルギー	ジュール毎キログラム	J/kg	$m^2\ s^{-2}$
熱伝導率	ワット毎メートル毎ケルビン	W/(m K)	$m\ kg\ s^{-3}\ K^{-1}$
体積エネルギー	ジュール毎立方メートル	J/m^3	$m^{-1}\ kg\ s^{-2}$
電界の強さ	ボルト毎メートル	V/m	$m\ kg\ s^{-3}\ A^{-1}$
電荷密度	クーロン毎立方メートル	C/m^3	$m^{-3}\ sA$
表面電荷	クーロン毎平方メートル	C/m^2	$m^{-2}\ sA$
電束密度，電気変位	クーロン毎平方メートル	C/m^2	$m^{-2}\ sA$
誘電率	ファラド毎メートル	F/m	$m^{-3}\ kg^{-1}\ s^4\ A^2$
透磁率	ヘンリー毎メートル	H/m	$m\ kg\ s^{-2}\ A^{-2}$
モルエネルギー	ジュール毎モル	J/mol	$m^2\ kg\ s^{-2}\ mol^{-1}$
モルエントロピー, モル熱容量	ジュール毎モル毎ケルビン	J/(mol K)	$m^2\ kg\ s^{-2}\ K^{-1}\ mol^{-1}$
照射線量（X 線及びγ線）	クーロン毎キログラム	C/kg	$kg^{-1}\ sA$
吸収線量率	グレイ毎秒	Gy/s	$m^2\ s^{-3}$
放射強度	ワット毎ステラジアン	W/sr	$m^4\ m^{-2}\ kg\ s^{-3}=m^2\ kg\ s^{-3}$
放射輝度	ワット毎平方メートル毎ステラジアン	$W/(m^2\ sr)$	$m^2\ m^{-2}\ kg\ s^{-3}=kg\ s^{-3}$
酵素活性濃度	カタール毎立方メートル	kat/m^3	$m^{-3}\ s^{-1}\ mol$

表５．SI 接頭語

乗数	接頭語	記号	乗数	接頭語	記号
10^{24}	ヨタ	Y	10^{-1}	デシ	d
10^{21}	ゼタ	Z	10^{-2}	センチ	c
10^{18}	エクサ	E	10^{-3}	ミリ	m
10^{15}	ペタ	P	10^{-6}	マイクロ	μ
10^{12}	テラ	T	10^{-9}	ナノ	n
10^{9}	ギガ	G	10^{-12}	ピコ	p
10^{6}	メガ	M	10^{-15}	フェムト	f
10^{3}	キロ	k	10^{-18}	アト	a
10^{2}	ヘクト	h	10^{-21}	ゼプト	z
10^{1}	デカ	da	10^{-24}	ヨクト	y

表６．SIに属さないが、SIと併用される単位

名称	記号	SI 単位による値
分	min	1 min=60s
時	h	1h =60 min=3600 s
日	d	1 d=24 h=86 400 s
度	°	1°=(π/180) rad
分	’	1’=(1/60)°=(π/10800) rad
秒	”	1”=(1/60)’=(π/648000) rad
ヘクタール	ha	$1ha=1hm^2=10^4m^2$
リットル	L, l	$1L=11=1dm^3=10^3cm^3=10^{-3}m^3$
トン	t	$1t=10^3$ kg

表７．SIに属さないが、SIと併用される単位で、SI単位で表される数値が実験的に得られるもの

名称	記号	SI 単位で表される数値
電子ボルト	eV	$1eV=1.602\ 176\ 53(14)\times10^{-19}J$
ダルトン	Da	$1Da=1.660\ 538\ 86(28)\times10^{-27}kg$
統一原子質量単位	u	1u=1 Da
天文単位	ua	$1ua=1.495\ 978\ 706\ 91(6)\times10^{11}m$

表８．SIに属さないが、SIと併用されるその他の単位

名称	記号	SI 単位で表される数値
バール	bar	$1\ bar=0.1MPa=100kPa=10^5Pa$
水銀柱ミリメートル	mmHg	1mmHg=133.322Pa
オングストローム	Å	$1\ Å=0.1nm=100pm=10^{-10}m$
海里	M	1 M=1852m
バーン	b	$1\ b=100fm^2=(10^{-12}cm)2=10^{-28}m^2$
ノット	kn	1 kn=(1852/3600)m/s
ネーパ	Np	SI単位との数値的な関係は、対数量の定義に依存。
ベル	B	
デジベル	dB	

表９．固有の名称をもつCGS組立単位

名称	記号	SI 単位で表される数値
エルグ	erg	$1\ erg=10^{-7}\ J$
ダイン	dyn	$1\ dyn=10^{-5}N$
ポアズ	P	$1\ P=1\ dyn\ s\ cm^{-2}=0.1Pa\ s$
ストークス	St	$1\ St\ =1cm^2\ s^{-1}=10^{-4}m^2\ s^{-1}$
スチルブ	sb	$1\ sb\ =1cd\ cm^{-2}=10^4cd\ m^{-2}$
フォト	ph	$1\ ph=1cd\ sr\ cm^{-2}\ 10^4lx$
ガル	Gal	$1\ Gal\ =1cm\ s^{-2}=10^{-2}ms^{-2}$
マクスウェル	Mx	$1\ Mx = 1G\ cm^2=10^{-8}Wb$
ガウス	G	$1\ G\ =1Mx\ cm^{-2}\ =10^{-4}T$
エルステッド[c]	Oe	$1\ Oe \triangleq (10^3/4\pi)A\ m^{-1}$

(c) ３元系のCGS単位系とSIでは直接比較できないため、等号「 ≙ 」は対応関係を示すものである。

表10．SIに属さないその他の単位の例

名称	記号	SI 単位で表される数値
キュリー	Ci	$1\ Ci=3.7\times10^{10}Bq$
レントゲン	R	$1\ R = 2.58\times10^{-4}C/kg$
ラド	rad	$1\ rad=1cGy=10^{-2}Gy$
レム	rem	$1\ rem=1\ cSv=10^{-2}Sv$
ガンマ	γ	1 γ =1 nT=10-9T
フェルミ		1フェルミ=1 fm=10-15m
メートル系カラット		1メートル系カラット = 200 mg = 2×10-4kg
トル	Torr	1 Torr = (101 325/760) Pa
標準大気圧	atm	1 atm = 101 325 Pa
カロリー	cal	1cal=4.1858J（「15℃」カロリー），4.1868J（「IT」カロリー）4.184J（「熱化学」カロリー）
ミクロン	μ	$1\ \mu\ =1\mu m=10^{-6}m$

（第8版，2006年改訂）

この印刷物は再生紙を使用しています