DMZネットワークのサーバ管理者自身による脆弱性診断

村上 直[1,a)]　湯浅 富久子[1,b)]　金子 敏明[1,c)]

概要：研究所のネットワークなどでは，大小さまざまなグループが個々の事情をもってサーバ機器を運用しているケースがみられる．特に，このような運用形態を公開サーバが設置される DMZ ネットワークでとる場合，各サーバの統一的な管理が困難であることと，サーバの管理者がかけられる負担やスキルが千差万別となることから，DMZ ネットワークセキュリティの把握や管理も容易ではなくなる．本研究では，DMZ ネットワークのセキュリティ維持管理を目的として，脆弱性診断を機器の管理者自身が実施して状態を把握できるポータルサイト DMZ User's Portal を構築導入し，各々の機器管理者が自主的かつ自走的にセキュリティを把握できる方式を提案し，実施してきた．脆弱性診断装置が示した 10 年間の診断結果の推移から，提案方式が機器管理者の情報セキュリティへの意識向上を促し，セキュリティ状態の維持や向上に成功していることを読み取ることができた．本稿では，このポータルサイトの内容や運用事例を含めたセキュリティの把握や管理への取り組みについて述べ，得られた効果について報告する．

Vulnerability Analysis Scheme for DMZ Network Performed by Server Administrators Themselves

Murakami Tadashi[1,a)]　Yuasa Fukuko[1,b)]　Kaneko Toshiaki[1,c)]

Abstract: In such as research institutes, there are cases where various kinds of servers are connected to DMZ network and it is difficult to manage the servers in a unified manner. In this situation, the degree of administration skill in each server may also vary and that causes difficulties to grasp or manage the network security in the DMZ network. In this paper, we report a proposal of the portal site DMZ User's Portal. Using the DMZ User's Portal, each server administrator can perform vulnerability scan for his/her own servers. Then the administrator can grasp and manage the network security. Each server administrator in KEK-DMZ grasp and manage the network security by himself/herself. And then, the 10 years results of vulnerability scans show that the status of security in KEK-DMZ has been kept in good conditions.

1. はじめに

近年，サイバー攻撃がますます高度化，悪意化，国際化，かつ苛烈化しており，公開サーバのネットワークセキュリティを維持するための運用コストは増大する一方である．セキュリティ把握の観点からは，一般的には各サーバが統一的な運用方針の下で管理されることが有効である．しかしながら，研究所のネットワークなどでは，大小さまざまなグループが個々の事情をもってサーバ機器を運用しているケースがみられ，これらを統一的な運用方針の下で管理するのは困難である．たとえば高エネルギー加速器研究機構（KEK）では，100 名以上の管理者が，300 台以上の DMZ 機器を各々の運用事情に合わせて多様性に富む運用をしており，自由度が高い．

このような運用形態では，機器管理者自身のセキュリティへの関わり方も様々である．機器管理者がかけられる手間やスキル，セキュリティへの意識，機器の重要度，注目度，運用形態などの事情は千差万別であり，それに伴い機器の攻撃の受けやすさも様々である．

深刻なセキュリティインシデントは，研究活動の停止や情報資産の流出などにつながるものであり，特に DMZ ネットワークにおいて良好なセキュリティ状態を維持することは重要である．近年のセキュリティ施策は，上意下達

[1] 高エネルギー加速器研究機構（KEK）
[a)] tadashi.murakami@kek.jp
[b)] fukuko.yuasa@kek.jp
[c)] toshiaki.kaneko@kek.jp

的な発想によって画一的な管理がなされることが多く，また，この手法が有効に作用する場合も多い．しかしながら，画一的な管理を研究所での各々の運用に強制すると，研究にとって重要な多様性を奪うことにつながる．研究所に与えられた社会的使命を考慮すると，多様性を重視し自由な発想に基づいた研究活動を推進するべきである．画一的な管理を避け多様性を確保しつつ良好なセキュリティ状態を維持するためには，各々の機器管理者が自身の運用にとってセキュリティがどう関わるかを自ら考え理解し，自身の責任のもとでセキュリティ維持管理を実践すること，すなわち自主的かつ自走的なセキュリティ維持管理の実践が重要である．このように機器管理者が自治的な意識でセキュリティを維持管理することは，機器の運用における多様性を保つには不可欠である．但しこの実現は容易ではない．

KEK では DMZ ネットワークにおいて，セキュリティが組織のガバナンスとして意識されるより以前から，各々の機器管理者が自主的かつ自走的にセキュリティ維持管理を実践できるよう，取り組みを進めてきた．本研究では，このような取り組みの柱として，DMZ ネットワークのセキュリティ維持管理のための脆弱性診断を，機器の管理者自身が実施して状態を把握できる，ポータルサイト DMZ User's Portal を提案し，実際に構築や運用を実施してきた．セキュリティ専門家向けの機能が豊富かつ複雑な脆弱性診断装置を，KEK のセキュリティモデルに沿った形で必要な機能のみを機器管理者に直接的に提供する仕組みを構築した．週一度の自動診断で各機器のセキュリティ状態を定期診断するほか，機器管理者が自ら脆弱性診断をワンクリックで実施できるようにし，必要なときに自ら何度でも診断の実施と確認をできるようにした．本研究では，機器管理者が自身の管理する機器の状態を容易に把握できるための仕組みを提供することで，上意下達的な画一的管理に頼らずにセキュリティ維持管理を実践できるよう，サポートした．

DMZ User's Portal を活用して，KEK では 2005 年度より毎年，機器管理者自身によるセキュリティ自己点検を実施している．脆弱性診断装置の評価をベースにし，そのうえでセキュリティに関する会議において要求すべき基準を決定し，組織全体の対策水準を明確化している．

このような方法により，KEK の DMZ ネットワークでは，機器運用の多様性とセキュリティ維持の双方を実現している．脆弱性診断装置が示した 10 年間の診断結果の推移から，提案方式が機器管理者の情報セキュリティへの意識向上を促し，セキュリティ状態の維持や向上に成功していることを読み取ることができた．

DMZ User's Portal では，脆弱性診断装置へのアクセスにラッパーモジュールを介すことを必須としている．また，DBPowder [1], [2] を導入することで，データベースの仕様変更に柔軟に対応できるようにしている．このようにシステム設計においても工夫を施している．その結果，KEK の連携組織ながら情報セキュリティポリシーが異なる大強度陽子加速器施設 J-PARC でも，DMZ User's Portal を 2011 年度より並行した運用が可能となった [3].

脆弱性診断ツールを各々の機器管理者が利用できる環境を構築して運用している取り組みとして，文献 [4], [5] では，脆弱性診断ツールへの設定を自動化して機器管理者に使いやすくする一方で，脆弱性が検出されたポートへの外部からのアクセス状況を確認できる手段を提供している．また文献 [6], [7] では，複数種類の脆弱性診断ツールを機器管理者が使いやすく利用できる環境を構築し，脆弱性診断ツールの運用状況を論じている．本研究の特徴は，個々のサーバ機器の脆弱性を複数の方法で継続的に機器管理者にフィードバックし，機器管理者が自主的かつ自走的にセキュリティを把握できる方式を示したことと，その効果を定量的に示したことにある．

以下，本論文の構成を示す．2 節で，本研究で対象とした KEK のネットワーク環境とセキュリティモデルについて述べ，それを踏まえて本研究で提案するポータルサイト DMZ User's Portal と，各々の機器管理者が自身でセキュリティ状態を把握できる方式について述べる．3 節で，2 節の提案内容を実現するための DMZ User's Portal のシステム設計を述べる．4 節で評価と議論を行う．5 節で本論文のまとめを示す．

2. DMZ 機器のセキュリティ確保のために

本節では，本研究が対象としている KEK ネットワークやそれに関連する環境について述べた後に，本研究で提案する，脆弱性診断を機器の管理者自身が実施して状態を把握できるポータルサイト DMZ User's Portal と，それによりもたらされる各々の機器管理者が自主的かつ自走的にセキュリティを把握できる方式について述べる．

2.1 KEK ネットワーク環境とセキュリティモデル

図 1 に，KEK ネットワークの概念図を示す．KEK ネットワークは，複数のスイッチを用いた VLAN から構成されており，中央ファイアウォールと中央スイッチを介してインターネットと接続している．KEK ネットワークの大部分は，中央ファイアウォールを境界として WAN, DMZ, LAN の 3 つの領域に分割されている [*1]．KEK ネットワーク内に機器を設置するためには，MAC アドレスの登録申請が必要である．申請が受理された機器について，KEK ネットワーク内からインターネットへの通信は，中央ファイアウォールで遮断された一部の宛先を除いて，原則接続を制限していない．

[*1] 本研究で対象とする DMZ ネットワークもこの VLAN の一部だが，インターネットからの通信を受け付ける運用をしていることから，図 1 では区別して示している．

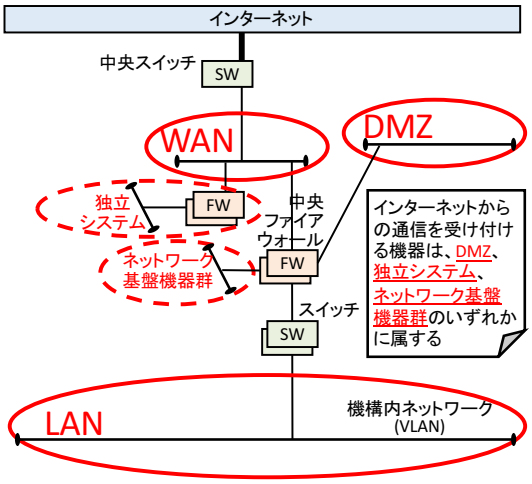

図 1　KEK ネットワークの概念図

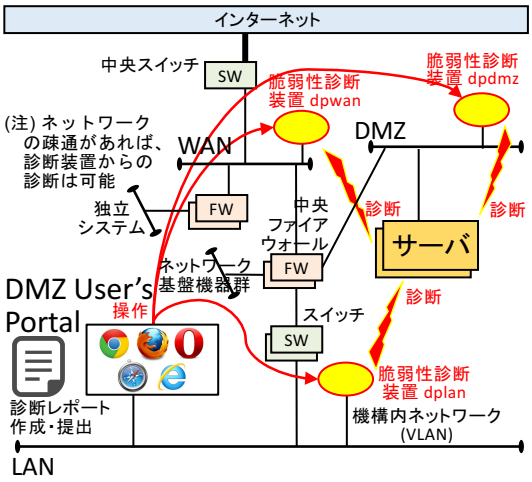

図 2　常時セキュリティ診断システムの概念図

大規模計算システムなど，中央ファイアウォールを介さずに個別のファイアウォールを用いた運用が認められたシステムが存在する．また，KEK ネットワークの運用に必要なネットワーク基盤機器群のなかには，中央ファイアウォールを介しつつ，接続元を限定して外部からのアクセスを受け付ける機器も存在する．図 1 では，このような機器群をそれぞれ，独立システム，ネットワーク基盤機器群として示している．

インターネットから KEK ネットワークへの通信は，図 1 に示した DMZ，独立システム，ネットワーク基盤機器群に限っている．本論文では，これらの機器をまとめて DMZ 機器とよぶ．DMZ 機器を運用するためには，KEK 職員である責任者が必須である．責任者のほかに，最大 2 名の共同管理者を加えることができる．これらの責任者と共同管理者をまとめて，機器管理者と呼ぶ．

インターネットから DMZ 機器への通信要求については，外部からのアクセスが必要なポートに限定した機器管理者からの申請にもとづき，接続が許可される．DMZ 機器からインターネットへの通信要求については，一部の宛先を除き通信を制限していないが，機器管理者からの申請にもとづき，中央ファイアウォールによる通信遮断もできる．

DMZ 機器の合計台数は，2005 年度で 177 台，2015 年度で 378 台であり，年を追うごとに増加している．KEK は大学共同利用機関法人であり，国内外の関連分野の研究者に対して研究の場を提供することを目的としている．このため，DMZ 機器は大小様々なグループが運用しており，利用者も国内外多岐にわたっている．また運用目的も，実験，広報，ログインシェル提供など多彩である．2016 年 1 月現在，登録された機器管理者の人数は 111 名である．

DMZ 機器に限らず，KEK におけるネットワークの使い方は多様である．研究所としての社会的使命を果たすためには，自主的なセキュリティ維持管理は重要である．KEK 内の各部門が部門に合った形でこれを実践できるよう，情報セキュリティ管理部会が組織されている．情報セキュリティ管理部会では，部門ごとにセキュリティマネージャが選出されて委員となり，KEK におけるコンピュータセキュリティについて定期的に議論が交わされている．

機器管理者は，年度ごとのセキュリティ自己点検（2.4 節）で，診断レポートの提出を義務付けられている．提出が求められる対象は，開始した 2005 年度当初は図 1 における DMZ ネットワーク上の機器のみであった．2007 年度には，独立システムの一部が対象に加わった．さらに 2014 年度には，独立システムとネットワーク基盤機器群のうち，インターネットからの通信要求を受け付ける全ての機器が対象に加わった．機器管理者が提出した診断レポートは，情報セキュリティ管理部会で審議される．

2.2　常時セキュリティ診断システム

常時セキュリティ診断システムは，脆弱性診断装置と DMZ User's Portal ポータルサイトから構成される．図 2 に概念図を示す． 脆弱性診断装置は，インターネットからの攻撃を想定した WAN のほか，KEK ネットワーク内部からの攻撃を想定した LAN に設置している．さらに，図 1 の DMZ 上の機器は，管理者の所属組織が様々であり，運用の背景も様々であるため，不正侵入されてしまった他の DMZ 機器からの攻撃にも備えて，DMZ 上にも脆弱性診断装置を設置している [*2]． WAN, DMZ, LAN の領域に 1 台ずつ設置した脆弱性診断装置のそれぞれを，dpwan, dpdmz, dplan[*3] とよぶことにする．

本研究では，Tripwire 社の nCircle IP360 [8] を脆弱性診断装置として採用した．この脆弱性診断装置は，診断対象の機器にネットワークを介してアクセスし，稼働しているネットワークサービスやシステム情報を調査し，PDF 形式

[*2] 独立システムやネットワーク基盤機器群については，システム毎に別々のサブネットが区切られており，また，各々の機器についても通信対象を極力絞った運用としていることから，脆弱性診断装置を各々のサブネット内に個別には設置していない．
[*3] dp は，Device Profiler の略．

のレポート（以下，pdf レポート）を作成する． KEK では，各々の機器管理者が任意のタイミングで実施する手動診断と，週次の自動診断を実施している． 検出された個々の脆弱性は，危険度に応じて以下のように点数付けされ，高い点数ほど危険とされる．

- サービスは検出されたが具体的な脆弱性を確認できない場合は，0 点と評価される．
- 点数に応じて緑→黄→赤のグラデーションで表現され，20 点前後が緑，500 点前後が黄，1000 点以上が赤色である．これに従い，1000 点を超える脆弱性を赤色脆弱性と呼ぶ [*4]．

実施済のセキュリティ対策を診断装置が判断できないなどにより，診断結果に誤診断が含まれる可能性がある．

また，脆弱性診断装置が発する診断パケットに対して一切の応答が無く，対象の DMZ 機器を検出できない場合がある．この原因は，ファイアウォールやホストの設定などにより通信を厳しく制限している場合と，電源断などによりネットワークに接続していない場合の 2 種類に大別できる．

個々の脆弱性点数は，nCircle IP360 が内蔵する Vulnerability Scoring System [9] により算出される．点数は時間の経過とともに増加する．これは，脆弱性が時間を経て一般的に広く知られるようになり，攻撃対象になりやすくなるという考え方に基づく．対象の脆弱性が世に知られてからの日数を t_n，対象の脆弱性について Vulnerability Scoring System が格付けするリスク度を $r_n (0 \leq r_n \leq 6)$，攻撃の容易度を $s_n (1 \leq s_n \leq 6)$ としたとき，脆弱性点数 V_n は，下記の式 (1) によって表される．

$$V_n = \sqrt{t_n} \cdot \frac{r_n!}{s_n{}^2} \qquad (1)$$

こうしてえられた脆弱性点数の KEK における評価は，年度ごとのセキュリティ自己点検において，情報セキュリティ管理部会で毎年議論している．

2.3 機器管理者自身による脆弱性診断

DMZ User's Portal は，機器管理者が自主的かつ自走的にセキュリティを把握し，維持管理できる環境の提供を目的としたポータルサイトであり，機器管理者は全員がアカウントを保持している．メイン画面のキャプチャを図 3 に示す．DMZ User's Portal は，KEK のセキュリティモデルに沿った形で，脆弱性診断装置がもつ豊富かつ複雑な機能のうち，必要な機能のみを機器管理者に提供し，不足している機能を補う．DMZ User's Portal を用いると，機器管理者は管理する DMZ 機器に対して下記のことを行える．

- 任意のタイミングでの手動診断の実行．
- 手動診断や自動診断の，結果閲覧．
- 脆弱性診断装置が作成した pdf レポートの取得．

[*4] たとえば CVE-2011-3192 Range header DoS vulnerability Apache HTTPD などが赤色脆弱性として検出されている．

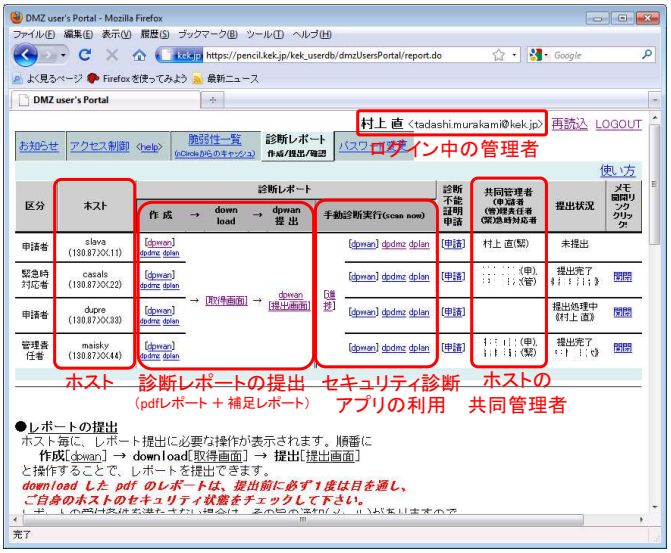

図 3 DMZ User's Portal メイン画面のキャプチャ

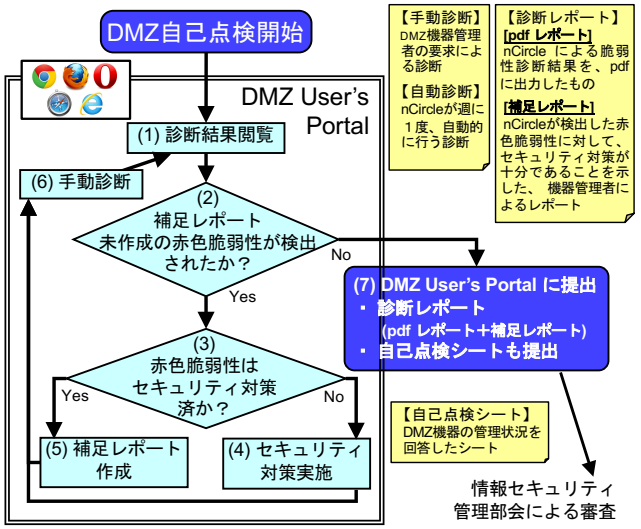

図 4 自己点検における診断レポートの提出フロー

- セキュリティ自己点検で要求される各種レポートの提出．pdf レポートと補足レポートから構成される診断レポートや，自己点検シートがある（2.4 節で後述）

DMZ User's Portal では，このほか，1000 点以上の赤色脆弱性が対策されていない場合に，機器管理者に対して週次でメール配信するサービスも行っている．

2.4 セキュリティ自己点検

KEK では情報セキュリティポリシーに基づき，年に一度機器管理者によるセキュリティ自己点検を実施している．DMZ User's Portal は，このセキュリティ自己点検で中心的な役割を果たしている．

図 4 に，自己点検における診断レポートの提出フローを示す．自己点検では，機器管理者がインターネットからの攻撃を想定した dpwan からの脆弱性診断と設定変更を何度も繰り返し，赤色脆弱性が除去された後の pdf レポート

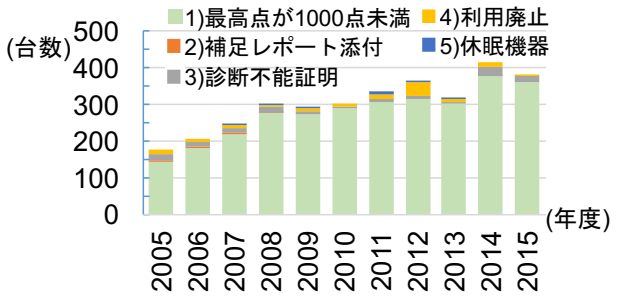

図 5 診断レポート提出状況の推移．4) は，レポート提出期間中に申請された利用廃止の件数であり，提出期間外にも DMZ 機器の利用廃止は発生している．

を報告結果として提出する．診断結果に誤診断が含まれていると機器管理者が判断した場合は，該当の脆弱性についてセキュリティ対策が十分であることを示した補足レポートを，追加資料として提出することができる．pdf レポートと必要に応じて加えた補足レポートをあわせて診断レポートとよぶ．くわえて，機械による診断結果のみではなく，稼働させているサービス，パスワードの管理状況，DMZ 機器からインターネットに対する通信の管理状況などを，機器管理者が自ら管理状況をまとめ，自己点検シートとして提出する．

提出された診断レポートは，情報セキュリティ管理部会で審査される．この審査では，脆弱性診断装置が検出した脆弱性とその点数についての議論を出発点とし，各々の DMZ 機器の運用状況について検討される．1000 点未満の脆弱性であっても，影響が大きく重要な脆弱性であり解消が望ましいと管理部会が判断した場合は，セキュリティマネージャから機器管理者に対処するよう要請が出される．

脆弱性診断装置が検出できない DMZ 機器のために，機器管理者は，DMZ User's Portal から診断不能証明申請を行うことができる．DMZ User's Portal は，過去の診断データ，dpwan 以外の診断装置 dpdmz と dplan の診断結果，および ARP 要求の応答をチェックする．いずれかに記録や応答があった場合は，該当の DMZ 機器はネットワークに接続されていると判断できる．この場合は，通信が厳しく制限されていると考えられるため，脆弱性点数 0 点とみなす．いずれも応答がなかった場合は，該当の DMZ 機器の運用状況が把握できないため，機器管理者による説明を求めている．機器の故障などにより自己点検期間中にネットワークに接続して脆弱性診断装置による診断を受けられない場合は，休眠機器申請を提出する必要がある．休眠機器は，ネットワーク再接続時に自己点検を実施することが求められる．

検出された個々の脆弱性のうち最高点が高い場合は，今後危険性がさらに高まっていくことが予想され，早めに対処しておくことが求められる．また，個々の点数は低いが足し合わせた合計点が高い場合は，具体的な危険性は指摘できないものの，OS が古かったりサービスを多数起動し

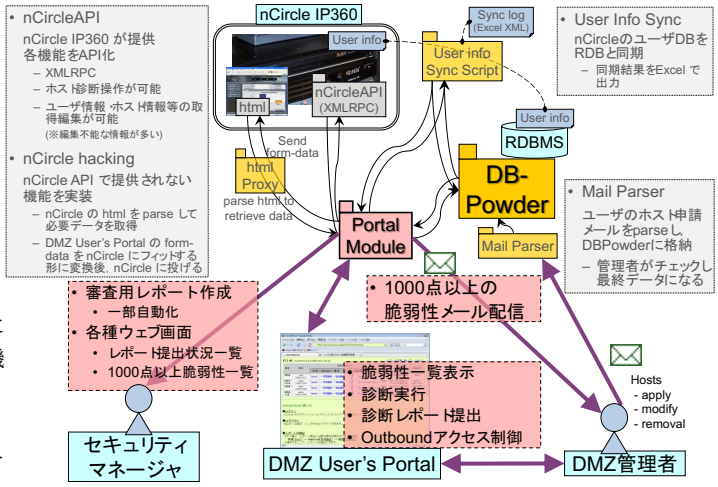

図 6 DMZ User's Portal のシステム設計

ていたりするケースが多く，注意が必要である．

2.5 セキュリティ自己点検での診断レポートの提出状況

図 5 に，2005 年度から 2015 年度までの各年度での自己点検における診断レポートの提出状況の推移を示す．自己点検の対象となる DMZ 機器の台数はゆるやかに上昇しているが，毎年度すべての機器が以下に述べる 1）から 5) に該当し，自己点検を終了している．1) は検知された個々の脆弱性の点数が, 全て 1000 点未満である場合に提出される pdf レポートの件数である．2) は脆弱性診断装置で 1000 点以上の赤色脆弱性が検知されているが，セキュリティ対策済みであることを説明する補足レポートの提出件数で, 3) は脆弱性診断装置が対象となる機器の存在を検出できない場合に提出される診断不能証明申請の提出件数である．4) は，自己点検期間中にネットワーク接続が廃止になった機器の件数である．5) は，脆弱性診断装置による診断を受けられない場合の休眠機器申請の件数である．

3. DMZ User's Portal のシステム設計

本節では，2 節に示した運用を可能にするために実装した，DMZ User's Portal ポータルサイトのシステム設計について述べる．図 6 にシステム設計を示す．

脆弱性診断装置である nCircle IP360 は XMLRPC による API (nCircle API) を用意しており，DMZ User's Portal は API を介してこの診断装置を操作する．但し，nCircle API は，pdf レポートのダウンロードなどユーザの利用に不可欠な重要機能の一部を提供していない．このような一部の機能を実現するために，html Proxy モジュールを開発した．html Proxy は，診断装置のウェブアプリケーションが描画する html を解釈し，必要な機能やデータを抽出する機能を担う．

nCircle IP360 は，利用者，登録機器の IP アドレス，および診断結果を，データベース内に保持している．DMZ User's Portal でも同様のデータを扱う必要があるが，DMZ

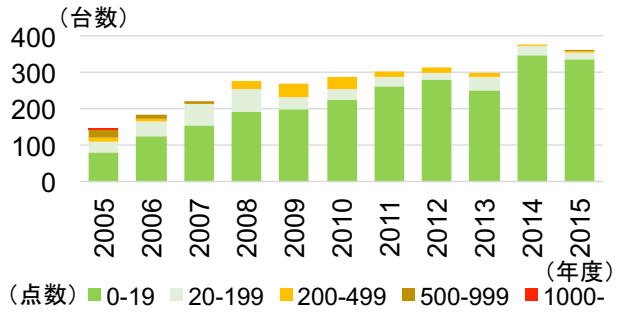

図 7 最高点について，機器管理者が自己点検で報告した脆弱性点数の推移（wan）

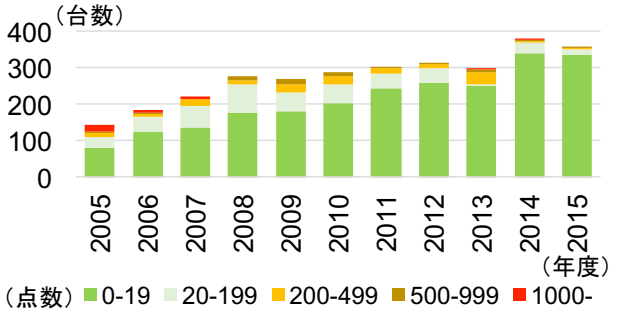

図 8 合計点について，機器管理者が自己点検で報告した脆弱性点数の推移（wan）

User's Portal ではこの診断装置が扱わないデータも同時に扱う必要がある．そこで，DMZ User's Portal では診断装置とは独立にデータベースを保持することとし，診断装置が保持するデータベースと必要に応じて同期をとる仕掛けとした．

DMZ User's Portal の特定の脆弱性診断製品へのモジュール依存性を下げるために，nCircle IP360 を操作するための XMLRPC および html Proxy は，必ずラッパーモジュールを介してアクセスするように設計している．これにより，診断装置側の仕様変更の影響をラッパーモジュール内にとどめることができている．また，DMZ User's Portal が保持するデータベースについても，DBPowder [1], [2] の導入により，仕様変更に柔軟に対応できる構成としている．

Portal Module は，ラッパーモジュールを介した nCircle IP360 の操作および，DBPowder を介した DMZ User's Portal のデータベースへのアクセスを司り，全体として DMZ User's Portal の機能を実現する．画面出力やメールの文章については，プログラムコードに埋め込まず，テンプレートを用いるようにしている．これにより，KEK とは運用ポリシーの違うサイトに DMZ User's Portal を導入することを可能としている．

4. 評価

本節では研究内容の評価を実施する．4.1 節では，年度ごとのセキュリティ自己点検（2.4 節，2.5 節）で機器管理者から報告のあった dpwan の脆弱性点数について，年度の推移を示す．4.2 節では，脆弱性診断装置が検出した dpwan, dpdmz, dplan の脆弱性点数について，年度の推移を示す．4.3 節では，4.1 節および 4.2 節の結果をふまえ，脆弱性点数の推移について考察することにより，本研究の有効性の評価をおこなう．また 4.4 節では，3 節で示したシステム設計により得られた効果を示す．

4.1 セキュリティ自己点検時の脆弱性点数推移

機器管理者がセキュリティ自己点検で報告した dpwan からの診断結果のうち，検出された脆弱性点数の最高点について，脆弱性点数の推移を集計したものを，図 7 に示す．

図 7 では，最高点を 5 つの区分に分けて集計した．自己点検では，最高点が 1000 点を越えないことが求められる．なお，補足レポート付きで報告された 1000 点以上の脆弱性は対策済み（図 4 参照）とみなし，図 7 では脆弱性 0 点として補正した．この補正により，自己点検で報告された dpwan からの診断結果で 1000 点を超えた脆弱性は 2005 年度の 1 件のみで，2006 年度以降では 0 件となった．

dpwan からの診断結果のうち，図 7 で示した最高点の代わりに検出された脆弱性点数を足し合わせた合計点について，脆弱性点数の推移を集計したものを，図 8 に示す．図 7 と異なり，ある 1 台の機器に脆弱性が複数件検出された場合，2006, 2007, 2013, 2014 年度では最高点が 1000 点未満でも合計点は 1000 点を上回ることがあった．例を挙げると，

- 2007 年度には，ある DMZ 機器は 987 点, 928 点, 267 点など 1 台で 21 件の脆弱性をかかえ，その合計点は 2900 点であった．
- 2013 年度には，ある DMZ 機器は古い SSL の使用が原因で，4 件の脆弱性（390 点が 3 件と，276 点）が検出された．ほか，SSL に関係する 0 点の脆弱性が 17 件検出された．この機器がかかえる脆弱性の件数は 27 件，合計点は 1482 点であった．

図 7 および 8 から，DMZ 機器の台数が年々増加しているにもかかわらず，2013 年度を除き点数の高い脆弱性が年を追うごとに減少していることがわかった．2013 年度の合計点数（図 8）では，200–499 点の区分が 2012 年度までと比べて増加し，点数の分布が悪化している．これは，脆弱性診断装置が OpenSSL や OpenSSH に関係する脆弱性診断を強化したタイミングと自己点検の実施期間が重なったことにより，100 点から 200 点程度の脆弱性を複数件抱えたままレポートを提出せざるを得なかった機器管理者が多数存在したためである．自己点検の期間中は点数が悪化したものの，その後には対応がなされ，OpenSSL や OpenSSH の脆弱性は解消に向かい，2014 年度の点数分布は大幅に改善した．

4.2 全脆弱性診断装置からの脆弱性点数推移

表 1 に，脆弱性診断装置が検出した各々の脆弱性について，総件数と 1 台あたりの平均検出件数を，点数を 3 区分（0 点，1–19 点，20 点以上）に分けて集計した結果を示す．集計対象は 2005, 2013, 2015 年度とし，図 2 に示した診断装置の全て（all: dpwan, dpdmz, dplan）について，件数を集計した．なお DMZ 機器の総台数は，2005, 2013, 2015 年度の順に，177 台，316 台，378 台である．

脆弱性の総件数（表 1 上）をみると，その合計は年度を追うごとに増加している．これは，0 点の脆弱性が 2005, 2013, 2015 年度の順番に 1499, 4435, 4848 件と大幅に増加していることが原因である．逆に 1–19 点と 20 点以上の脆弱性件数については，2005 年度から 2013 年度の推移はいずれも半数未満と大幅に減少している．2013 年度から 2015 年度の推移はいずれもほぼ横ばいである．さらに，1 台あたりの件数（表 1 下）をみると，2013 年や 2015 年度の 1 点以上の脆弱性の件数は，2005 年度から比べて 3 分の 1 未満と顕著に減少している．

図 9 に，2005, 2013, 2015 年度について，脆弱性診断装置が検出した脆弱性の点数分布を示す．ここでは，3 つの診断装置でみた結果（all）と，dpwan の診断結果（wan）を示している．表 1 に示したとおり，2013 年度と 2015 年度の脆弱性点数 0 点の件数が非常に多いため，図 9 では 1 点以上を表示した．このグラフから，2005 年度は 500 点以上の脆弱性も数多く見られたが，2013 年度と 2015 年度については，500 点以上の脆弱性はほぼ解消されていることがわかった．なお，2013 年度の 380 点–399 点区分には脆弱性が 100 件あり，そのうち 86 件は 4.1 節で述べた OpenSSL や OpenSSH の脆弱性である．この脆弱性の多くは 2014 年度の自己点検までに解消されたが，全てが解消されたわけではない．DMZ User's Portal で導入した脆弱性診断装置では，各々の脆弱性について点数が日々自動的に上昇することから，2015 年度には OpenSSL や OpenSSH の脆弱性は 420–439 点と 440–459 点の区分に移動している．また 2015 年度では，840–859 点の区分にも脆弱性が検出されている．これは 2014 年に発見された Apache に関係する脆弱性である．このような脆弱性が報告や発見された場合は，情報セキュリティ管理部会での議論を経て必要に応じて機器管理者に問い合わせるなどの対応をとっている．

表 1 all(wan,dmz,lan) の脆弱性診断装置が検出した脆弱性について，総件数と 1 台あたりの件数（2005，2013，2015 年度）．

all (wan,dmz,lan) 総件数 （年度）

	2005	2013	2015
0点	1499件	4435件	4848件
1–19点	829件	391件	366件
20点以上	831件	356件	387件
合計	3159件	5182件	5601件

all (wan,dmz,lan) 1台あたりの平均件数 （年度）

	2005	2013	2015
0点	8.47件/台	14.03件/台	12.83件/台
1–19点	4.68件/台	1.24件/台	0.97件/台
20点以上	4.69件/台	1.13件/台	1.02件/台
合計	17.85件/台	16.40件/台	14.82件/台

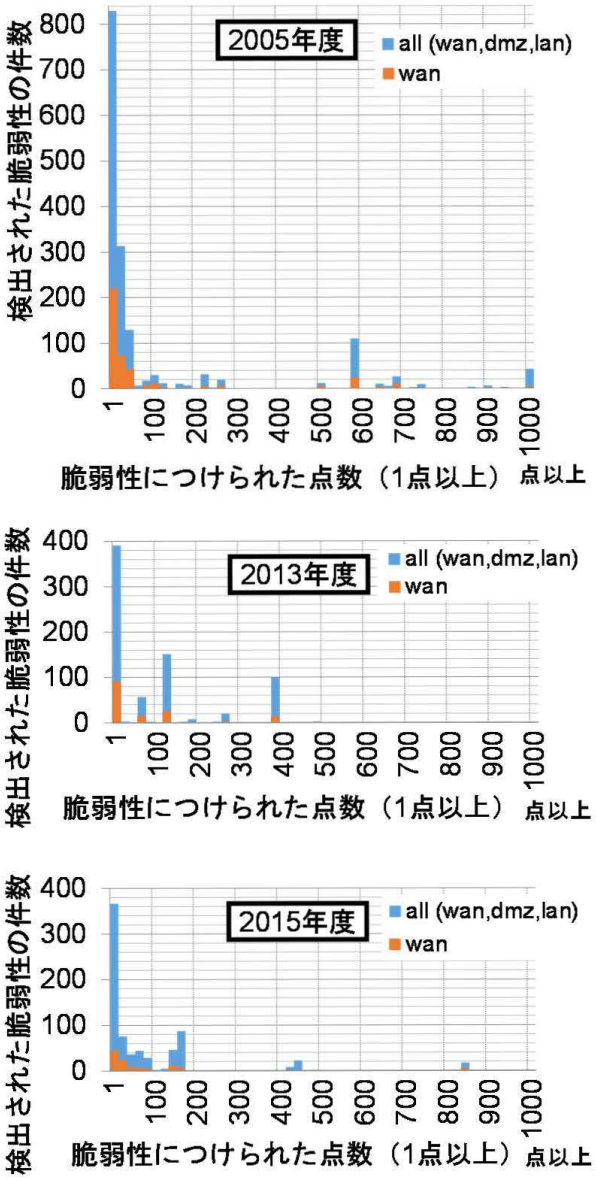

図 9 脆弱性診断装置が検出した脆弱性の点数分布（2005，2013，2015 年度）

4.3 脆弱性点数の推移について評価

DMZ User's Portal で導入した脆弱性診断装置は，下記の性質をもっている．

- 各々の脆弱性点数は，日々自動的に上昇する（2.2 節）
- サービスが検出されたが具体的な脆弱性がない場合は，0 点の脆弱性と評価される（2.2 節）
- 深刻な脆弱性は日々発見されている．これに対応して脆弱性診断装置が検出できる脆弱性の種類は増える．
- 脆弱性診断装置は改良が重ねられており，検出できるサービスの種類は年々増えると予想できる．

2005 年度から DMZ 機器の台数は年々増えている．さらに，自己点検の対象を拡大してきた．これらを考えると，有効なセキュリティ対策が打たれなければ，脆弱性診断装置が算出する点数は，年度を追うごとに大幅に上昇するはずである．それにもかかわらず，図 7, 8, 9，および表 1 の全てにおいて，点数が高い深刻な脆弱性の検出件数は年度を経るごとに大幅に減少している．これは，2005 年度時点では技術レベルやセキュリティ意識について多様性があったが，DMZ User's Portal の運用によって DMZ 機器の脆弱性情報を機器管理者自身が簡単に取得できるようにしたことと，毎年の自己点検でレポート提出を義務づけたことにより，年々機器管理者の情報セキュリティへの意識が向上していった結果であると考えることができる．また，自己点検では dpdmz や dplan が直接の点検対象ではないにもかかわらず，表 1 および図 9 にみられるように，dpdmz や dplan の 1 点以上の脆弱性の検出件数も，dpwan と同様に大幅に減少している．この結果は，各々の機器管理者がみずから外部に公開するサービスをコントロールし，必要なもののみに極力絞った成果であるとみなせる．

4.4 他組織への展開

DMZ User's Portal を，KEK の連携組織である大強度陽子加速器施設 J-PARC に，2011 年度より展開して運用している [3]．J-PARC の情報セキュリティポリシーは KEK と異なる．また，2 サイトでは運用条件も同じではなく，たとえば脆弱性診断装置のバージョンが異なる場合がある．図 6 に示した柔軟な構成を取ることで，処理内容は 2 サイトで同様ながら，画面への出力項目の切替やバージョンの差異の吸収を実現した．また J-PARC では，KEK と異なる J-PARC の独自運用部分を，AddOn サブシステム [3] として一体的に運用している．

5. まとめと課題

本研究では，DMZ ネットワークのセキュリティ維持管理のための脆弱性診断を，機器の管理者自身が実施して状態を把握できる，ポータルサイト DMZ User's Portal を構築導入し，各々の機器管理者が自主的かつ自走的にセキュリティを把握できる方式を提案し，実施した．セキュリティ専門家向けの機能が豊富かつ複雑な脆弱性診断装置を，KEK のセキュリティモデルに沿った形で必要な機能のみを機器管理者に直接的に提供する仕組みを構築し，機器管理者が必要なときに自ら何度でも診断の実施と確認をできるようにした．この仕組みと年度毎の全組織にわたるセキュリティ自己点検実施の組み合わせにより，KEK において公開サーバの台数が年々増加しているにもかかわらず，DMZ ネットワークのセキュリティが年々改善されていることが，脆弱性診断装置が示した 10 年間の診断結果の推移から確認された．また，システム構成をラッパーモジュールやテンプレートの活用などにより柔軟にすることで，KEK とは情報セキュリティポリシーが異なる J-PARC でも DMZ User's Portal を構築導入し，並行して運用できている．このように，本研究で掲げた各々の機器管理者が自主的かつ自走的にセキュリティを維持管理するという目標は，実現できたと考えられる．

今後の課題としては，脆弱性診断装置が検出できない脆弱性への取り組みがあげられる．パスワードの適切な管理，DMZ 機器からインターネットに対する通信の把握，ゼロデイ攻撃への備えなども重要だが，脆弱性診断装置では検出が難しい．そこで自己点検では，機器管理者自らが DMZ 機器の管理状況を自己点検シートとして提出している．しかし現状ではこの結果をセキュリティ維持管理に十分に活かしきれておらず，DMZ User's Portal による自主的かつ自走的な考え方を活用した解決方法を検討したい．また，DMZ User's Portal はラッパーモジュールなど柔軟なシステム構成にはなっているが，対象の脆弱性診断装置は特定の製品に依存している．DMZ User's Portal が使用する脆弱性診断装置の機能を API 化するなどシステムを改良して，特定の製品に依存しない構成にしたいと考えている．

参考文献

[1] Murakami, T., Amagasa, T. and Kitagawa, H.: DBPowder: A Flexible Object-Relational Mapping Framework Based on a Conceptual Model, *COMPSAC*, IEEE Computer Society, pp. 589–598 (2013).
[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 (TOD), Vol. 3, No. 3, pp. 46–67 (2010).
[3] 石川弘之， 舘明宏， 村上直：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，*JAEA-Technology 2011-030*, pp. 1–62 (2012).
[4] 毛利公美, 高橋秀郎, 広岡俊彦, 曽根直人, 森井昌克：ネットワーク資源に対する脆弱性自動監査システムの開発，電子情報通信学会技術研究報告 (OIS)，Vol. 104, No. 69, pp. 13–18 (20040514).
[5] 蓮井亮二，毛利公美，森井昌克：管理・運用を容易にするネットワーク資源脆弱性自動検査システムの開発，電子情報通信学会技術研究報告 (OIS)，Vol. 105, No. 529, pp. 17–22 (20060113).
[6] 田島浩一, 岸場清悟， 近堂徹, 西村浩二, 相原玲二：コンピュータセキュリティ脆弱性診断の実施方法についての運用評価，情報処理学会研究報告 (EVA)，Vol. 2008, No. 30, pp. 1–6 (2008).
[7] 田島浩一，岸場清悟， 近堂徹，大東俊博，岩田則和，西村浩二，相原玲二：脆弱性診断ツールの連携動作によるセキュリティ診断システムの構築，マルチメディア、分散協調とモバイルシンポジウム 2013 論文集，Vol. 2013, pp. 749–754 (2013).
[8] 京セラコミュニケーションシステム株式会社：脆弱性診断・管理システム 導入事例大学共同利用機関法人高エネルギー加速器研究機構，`http://www.kccs.co.jp/products/ncircle/case/case01.html` (Jul. 2010, accessed in Sep. 2016).
[9] Tripwire, Inc: Tripwire Vulnerability Scoring System, White paper, `http://www.tripwire.com/register/tripwire-vulnerability-scoring-system/` (2016).