

KEK における脆弱性診断装置の運用と活用

與那嶺 亮, 橋本 清治, 一井 信吾, 鈴木 聡, 中村 貞次, 前田 裕文

高エネルギー加速器研究機構 共通基盤研究施設 計算科学センター

ryo.yonamine@kek.jp

Utilization of Vulnerability scanner at KEK

Ryo Yonamine, Kiyoharu Hashimoto, Shingo Ichii,
Soh, Suzuki, Teiji Nakamura, Hirofumi, Maeda

High Energy Accelerator Research Organization (KEK),
Applied Research Laboratory, Computing Research Center

概要

KEK における DMZ 機器の脆弱性管理体制について報告する。脆弱性診断装置を中心に、それを補完する週次通知システム、自己点検システム、チケットシステムを連携させ運用している。

2024 年 6 月末には、脆弱性診断装置のシステム移行を我々自身の手で行い、知見と反省点が得られたので、情報共有も兼ねて報告する。

1 はじめに

高エネルギー加速器研究機構（以下、KEK）では、組織外からアクセス可能な機器（DMZ 機器）に対し、脆弱性診断装置を利用した常時脆弱性診断を行なっている。具体的には、

- 週次通知
- チケットによる対応管理
- オンデマンドスキャン
- 自己点検

から成る。ここで、「週次通知」とは、脆弱性診断を週一回の頻度で自動実行し、検知された脆弱性を機器管理者にメールで通知するサービス、「チケットによる対応管理」とは、週次通知で検知された脆弱性に対し、機器管理者による脆弱性対応が完了するまで追従・把握・適宜対応を行うこと、「オンデマンドスキャン」とは、管理者自身が任意のタイミングで脆弱性診断装置を自ら操作し、脆弱性診断を行うこと、「自己点検」とは、年一度の頻度で開催する、現状を把握と運用の見直しを行う、組織的なキャンペーンであり、脆弱性診断装置による脆弱性検知を補完することを目的としている。

2022 年度から 2023 年度にかけて、従来からの方法を見直し、脆弱性診断装置アプライアンスに備わっている機能をなるべく活かすようにシステム・ワークフ

ローの見直しを行った。その際に一新した週次通知システム、自己点検システムの詳細については [1]、[2] にて報告済みである。本報告では、我々の運用ワークフローにおいて脆弱性診断装置をどのように活用しているか、という観点から紹介する。また、2024 年 6 月末に行った脆弱性診断装置のシステム移行を通して得られた知見についても簡単に報告する。

2 脆弱性管理体制の構成

脆弱性診断装置を核とするシステムと、DMZ 機器管理者を中心に、セキュリティグループ（計算科学センターのセキュリティ担当の職員）、セキュリティ管理部会の関係を図 1 に示す。セキュリティ管理部会は、各部局に配置される情報セキュリティマネージャ（CSIRT との連携や各部局の機構職員等への情報セキュリティに関する支援を行う職員）から構成される。DMZ 機器の脆弱性管理は、DMZ 機器管理者が責任を持って行い、セキュリティグループとセキュリティ管理部会は、それを補佐、補完する、という位置付けとなっている。

以下、各システムについて補足する。

2.1 脆弱性診断装置

KEK では、2018 年度より、Tenable 社の Security Center[3] および、Nessus[4] を利用している。Nessus がターゲットの脆弱性のネットワークスキャンを行う脆弱性スキャナーであり、Security Center は Web UI

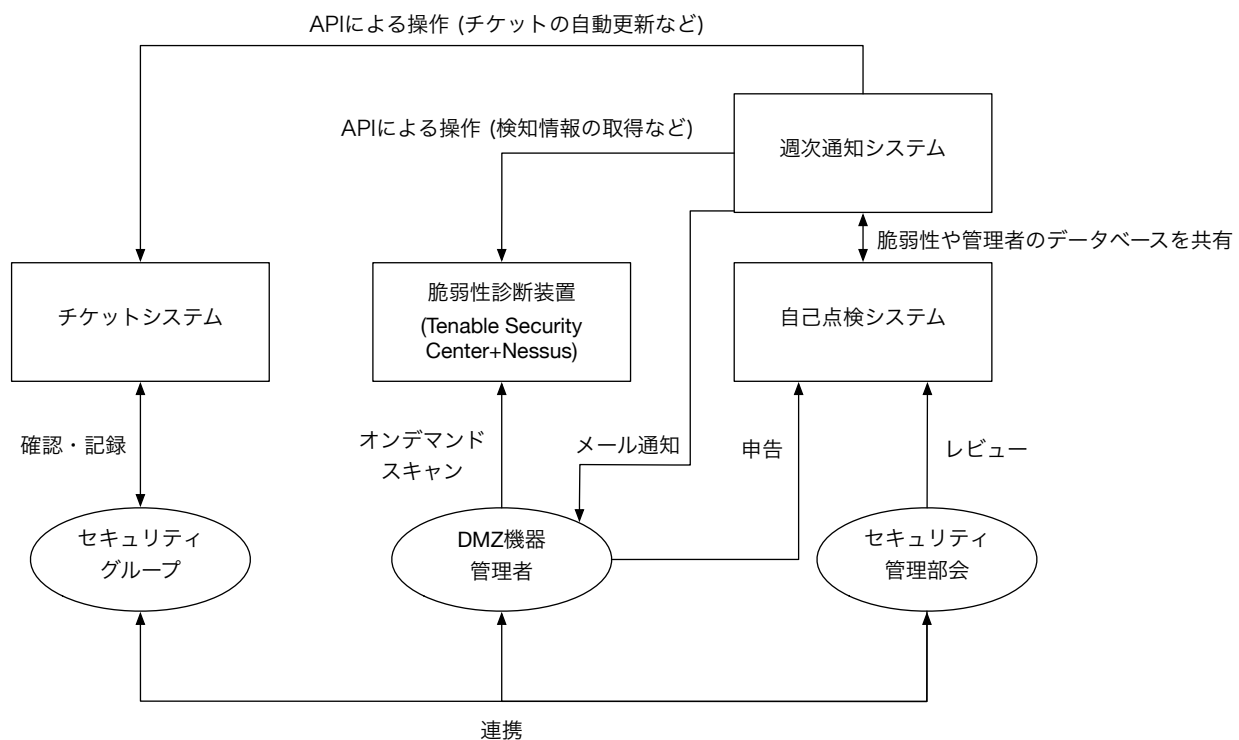


図1 DMZ 機器の脆弱性管理体制

を通して複数の Nessus を一元的に操作・管理するためのシステムである。Security Center では、脆弱性診断の定期的な自動実行が設定可能であり、KEK における週次通知ではこの機能を利用している。また、Security Center の Web UI は、アカウントさえ作っておけば、DMZ 機器管理者自身でログインし、好きなタイミングで脆弱性診断を実行し、結果を確認することが可能である。Security Center には Python などのスクリプトから種々の操作を可能にする Web API が用意されており、KEK では DMZ 機器管理者の負担軽減のため、あらかじめアカウント作成のほか、スキャンやレポート生成に必要なコンフィギュレーションファイルをスクリプトで一括作成し、配布している。つまり、DMZ 機器管理者が実際に行う操作は、ログインとスキャン・レポート作成実行ボタンの押下だけである。

KEK では3台の Nessus を利用しており、それぞれ機構内、DMZ、機構外に配置し、各領域から脆弱性スキャンを実行し、不正侵入によりファイアーウォールが突破された場合の横展開に備えている。

2.2 週次通知システム

脆弱性診断装置の定期診断実行機能を利用して、週に一度、自動的に登録されている DMZ 機器に対し、脆弱性スキャンを実行している。ここで、Medium 以

上に格付けされた脆弱性が検知された場合は、機器管理者自身へメールで迅速な対応が必要であることを通知する。この週次通知システムは、機器管理者情報と脆弱性診断装置で検知された脆弱性情報を格納するデータベースとスクリプトから構成される内製システム ([1]) で、脆弱性診断装置に備わっている Web API を使って情報の取得を行い、関連する管理者の情報と検知された情報を整理し、メールを送信・データベースの更新・チケットの発行・更新を行う。

2.3 チケットシステム

週次通知されるタイミングで、検知された機器や、その脆弱性の内容などが記載されたチケットが、週次通知システムにより自動的に発行される。前の週から継続して検知されている場合は、同じチケットに脆弱性検知が継続していることが追記される。前の週に検知された脆弱性が検知されなくなった場合は、チケットの状態を「確認要求」というステータスにし、チケットクローズが可能であることを明示する。最終的なチケットのクローズは、チケット管理者のレビュー後に手でクローズされる。

Critical, High に格付けされた緊急度の高い脆弱性に関しては2週、Medium に関しては4週以上連続で検知され続けるような場合は、対応状況などについて確認する為に連絡を取る。なお、機器管理者自身が脆

弱性が誤検知もしくは運用上リスクを受け入れなければならないと判断する場合、該当の脆弱性に関しては週次通知システムが更なる通知を行わないように設定する(非通知設定)。

2.4 自己点検システム

自己点検システムは、機器管理者ごとにログインして利用する内製ウェブフォームである([2])。機器管理者がログインすると、機器管理者情報のデータベースに基づいて、関連する機器に関する情報を自動選択し、IP アドレスやホスト名、共同管理者、非通知設定にした脆弱性一覧などを含めて動的に生成される。フォームには、年度ごとに決められた一連の点検項目が表示され、機器管理者は現在の運用に合わせて、ソフトウェアの名前やバージョン、SSH や CMS の公開サービス運用方法などについて申告を行う。

2.5 自己点検のレビュー

自己点検システムに集められた自己点検の結果は、セキュリティ管理部会でレビューが行われ、管理体制についてチェックを行なっている。レビューに使う自己点検の結果の資料は、自己点検システムにより定型フォーマットに出力される。必要に応じて機器管理者へフィードバックし、必要な対応を依頼する。

3 脆弱性管理システムの現状と今後の課題

本報告で紹介したシステムは順調に稼働しており、今のところメンテナンスに継続的に時間を割かなければならないという事態に陥っていないが、Security Center のメジャーバージョンアップデートにより、Web API や UI の仕様が一部変更されたため、それに追従するアップデートが必要になり、一時的にメンテナンスの時間を要することはあった。

一方、システムの属人化を防いで、如何に安定的な運用を行うかは継続中の課題である。ドキュメントの整備を進めているが、ドキュメントの陳腐化を防ぐ仕組みなど試行錯誤しながら検討している。

4 脆弱性診断装置の移行

2024 年の 6 月末で、CentOS 7 のサポートが終了し、それをベースにしていた KEK の脆弱性診断装置(Security Center + Nessus)は、別 OS へのシステム移行が必要になった。移行作業の金額が予算に見合わなかったため情報収集を行った上で我々自身で移行作業を行えるかどうかを慎重に吟味し、最終的に自前で移行作業を行う方向で進めることにした。

4.1 事前準備

4.1.1 情報収集と移行計画

システム移行に関する Tenable が公開しているドキュメントを読みながら、具体的な移行計画を立てた。旧システムから新システムへのデータ移行やライセンスに関する細かい問題などは、ドキュメントだけでは判断できなかったため、Tenable の KEK 担当者に問い合わせを行い、確認・打ち合わせを行いながらあいまいな点を明確にするように努めた。

Tenable Core[5] と呼ばれる Oracle Linux 8 をベースとしたカスタム OS 上に、あらかじめ Nessus や Security Center がインストールされた仮想アプライアンスも配布されており、今回はそれを利用することにした。Tenable Core ではサーバ証明書のインストールなど Web UI から行えるようなサービスも動作しており、各アプリケーションのインストールの手間が省けるだけでなく、運用上の利便性も向上している。

4.1.2 移行スケジュールと機器の手配

Security Center1 台と Nessus3 台のうち、Security Center と機構内に設置する Nessus は既存の仮想化基盤上に用意したが、残りの DMZ と機構外に設置する 2 台の Nessus は新規サーバを 2 台調達してデプロイすることにした。これは既存の仮想化基盤ハイパーバイザーのライセンス体系の変更に伴い、仮想化サーバの台数圧縮が急務であったこと、さらには近い将来別のハイパーバイザー等への移行が不可避となったからである。新規サーバの調達などにかかる待ち時間をなくし、作業時間を最大限確保できることを最優先にするべく、仮想化サーバへのデプロイを最初に実施した。これは、この時点では移行作業の経験が我々には皆無であったため、事前には想定できなかった問題が起これ、作業時間に遅れがでることを覚悟していた、という背景がある。

一方、DMZ と機構外に設置する Nessus に関しては、3 台の Nessus のうち 1 台でも動作すれば、多少停止期間が生じても影響は小さいと判断し、慌てずに新規のラックサーバを 2 台調達し、それぞれデプロイすることにした。

4.2 移行

具体的に必要になった移行作業は、

- 仮想基盤上のインスタンス・物理サーバのセットアップ
- 仮想アプライアンスのインストール
- Security Center と Nessus の連携

- ネットワークの登録
- ACL 設定の移行
- データ移行 (Security Center のみ)
- サーバ証明書のインストール

仮想アプライアンスのインストールで、hostname を新旧システムで揃えておくことで、旧システムで利用していたライセンスキーがそのまま利用できる (ライセンスキーを再作成しても良い)。なお、仮想アプライアンスの OVA イメージは閉鎖ネットワークに構築した vCenter からデプロイ出来ず、ESXi のコンソールから OVF としてデプロイする必要があった。

仮想アプライアンスにまとめられた Security Center や Nessus のインストールは、通常の OS をインストールと同じようにほぼ自動的に進み、完了した。Security Center と機構内に設置した Nessus に関しては、既存のシステム上に構築したこと、想定外の問題が生じなかったことにより、結果的に、旧システムの停止後、週次スキャンを途切らすことなく、新システムで再開することができた。

DMZ と機構外に設置する Nessus に関しては、サーバの納期の事情により 2 週間ほど遅れたが、大きな問題もなく、こちらも無事再開することができた。

4.3 移行後に発覚した問題への対処

Security Center と機構内 Nessus を動作させた時点で、DMZ 機器管理者にシステムを開放したが、実際には DMZ 機器管理者は LDAP 認証に常に失敗して Security Center にログインができない状態となってしまった。原因は 2 つあり、一つは、Tenable Core が NII が発行する UPKI サーバ証明書のルート証明書をデフォルトで信頼しておらず、ルート証明書を手で追加する必要があった。もう一つは、LDAP サーバ側の内部 ACL で新しい仮想アプライアンスの IP アドレスからのアクセスを遮断していたことであった。

4.4 作業を振り返って

サーバ納期、ネットワーク登録で想定よりも遅れが出ていたが、実際の移行作業においては、スムーズに事が進み、終わってみれば、あらかじめ余裕を持ってスケジュールを立てておいたこともあり、当初の計画より 1 日遅れるだけの遅延で移行が完了できた。事前調査・不具合調査・ネットワーク登録などの時間を除けば、実質的な作業時間は、未経験の場合で 1 日程度、一度経験すれば、半日程度で十分完了できる程度の工数であった。

今回は、新旧システムを同時にセットアップした状

態を作って、必要に応じて一時的に旧システムに戻れる状態を保ちながら、セットアップを別に用意した。そのため旧システムの IP アドレスを引き継がずに、新システムでは新しい IP アドレスを利用する必要があった。その結果として LDAP サーバの ACL 設定や機構全体のファイアーウォール設定など作業が余分に必要になってしまい、移行直後 LDAPS での通信できない問題の起源もここにあることを考えると、IP アドレスは新旧で引き継ぐように移行した方が良かったと反省している。一方、大きな収穫は、移行作業を通じて、Tenable システム自体への理解が深まったことである。

5 まとめと今後の課題

KEK では、DMZ 機器の脆弱性管理体制を、脆弱性診断装置を軸に構成しており、必要な機能を内製システムなどにより補完し、業務効率化を図っている。システムを如何に属人化させないかが今後の課題である。

また、脆弱性診断装置のシステム移行を自分たちの手で行った結果、改善すべき点はあったものの、大きな問題もなく移行が完了し、同時に脆弱性診断装置への理解が深めることができた。

脆弱性診断装置のさらなる活用として、脆弱性診断装置によって記録されるファイアーウォールログの活用を検討している。脆弱性診断装置による脆弱性スキャンは、実際のサイバー攻撃を模したものである。つまり、脆弱性診断によって残されるファイアーウォールログを調べることは、ファイアーウォールログ調査の良い教材であり、また、機械学習の学習データとしても役立つ可能性がある。

参考文献

- [1] 與那嶺 亮、鈴木 聡、一井 信吾、“KEK における脆弱性自己点検 PDCA サイクル高速化”、研究報告インターネットと運用技術 (IOT)、2022-IOT-57、15、1 - 6、2022-05-12.
- [2] 與那嶺 亮、鈴木 聡、一井 信吾、“KEK における DMZ 機器自己点検システムの再構築”、インターネットと運用技術シンポジウム論文集、2023、1 - 8、2023-11-30.
- [3] Tenable Security Center、<https://docs.tenable.com/security-center/Content/Welcome.htm>.
- [4] Tenable Nessus、<https://docs.tenable.com/>

nessus/Content/GettingStarted.htm.

[5] Tenable Core, <https://docs.tenable.com/tenable-core.htm>.