SPring-8 および SACLA における遠隔制御システム WARCS のアップグレード

UPGRADE OF WIDE AREA REMOTE CONTROL SYSTEM (WARCS) AT SPRING-8 AND SACLA

坂本達亮 A)、杉本崇 A)
Tatsuaki Sakamoto A)*, Takashi Sugimoto A)
A) Japan Synchrotron Radiation Research Institute (JASRI/SPring-8)

Abstract

The accelerator control system of SPring-8 and SACLA are isolated from any other network for security reasons. When a malfunction occurs at the accelerator, operator calls machine experts for assistance, even if who are absent by holiday or official trip. WARCS (Wide Area Remote Control System) was developed and have been operated to provide secure network access from remote sites at urgent maintenance. Since the WARCS needs some non-standard applications, experts are required to bring dedicate lap-top PCs. Tunneling technology is another considerable issue, because the tunneling protocol of the WARCS are often disapproved under the recent security policy of universities, institutes, nor accommodations. To resolve these issues, we developed new WARCS. For the first issue, we consider the client platforms to be run under standard Windows or Mac PCs. For the second issue, the new WARCS consists of standard network technologies to pass the network security/access controls. The new WARCS are installed and in operation at both SPring-8 and SACLA from 2012.

1．背景

SPring-8 および SACLA の制御システムは、データベースを中心とした制御フレームワーク MADOCA [1] により構築されている。MADOCA はサーバー・ワークステーション計算機、データベース、ローカル・エリア・ネットワークをはじめとした計算機技術により大規模制御システムを実現している。

加速器は放射線発生装置の一種であるため、その計算機システムのセキュリティは重要である。例えば、ジェファーソン国立研究所では 2011 年 6 月、インターネットからのアクセスが可能な状態となっていた加速器制御システムに対する不正アクセスを受け、約 1ヶ月もの間システム停止に至った。加速器制御システムのセキュリティを確保するため、SPring-8 および SACLA では外部からのアクセスを厳格に禁止している。

運転中の SPring-8 における不具合が発生した場合、加速器運転責任者および運転員による一次対応が行われる。不具合の原因によっては、機器を深く理解している専門研究員による二次対応が必要となる。しかし、機器担当者が休日・夜間や出張などによる所内不在時は迅速な対応が困難であり、所外から緊急メンテナンスを実施する手段が求められていた。上記の問題を解決するため、仮想プライベートネットワーク (Virtual Private Network, VPN) を利用したリモートアクセスによる緊急メンテナンス作業が可能となる “WARCS” [2] （WARCS Version 1、以下 WARCSv1）が構築され、運用されてきた。

しかしながら、近年のネットワークセキュリティ動向およびシステム構成により、WARCSv1 の運用における様々な課題が浮かび上がってきた。上記課題を解消するため、新たな WARCS（WARCS Version 2、以下 WARCSv2）の構築を行った。

本稿では、はじめに WARCSv1 の概要および について解消すべき課題について述べ、その後、新たに構築した WARCSv2 の設計および構築について触れる。最後に WARCSv2 の導入と運用について述べる。

2．既存 WARCS の概要と課題

機器担当者によるリモートメンテナンスを実現する上で、特に以下 3 点の情報セキュリティを考慮し、WARCSv1 は設計された。（Figure 1 参照）

- 暗号通信による秘匿化
- 二要素認証（個人認証およびログイン認証）
- 加速器運転責任者による通信制御

上記に挙げた要求項目を満たすため、WARCSv1 では VPN 通信環境を構築する専用ソフトウェアである “Zebedee” [3] を中心的な構成要素として採用し、構築を行っている。

しかしながら、WARCSv1 によるリモートメンテナンス環境において、解決すべき課題が発生している。一点目は、緊急メンテナンス作業を実施するために接続用プログラムがインストールされた専用端末（ノート型 PC）が必須となっていることである。加速器の緊急メンテナンス作業に備えるため、休日・出張時も専用端末の携行を機器担当者へ要求しており、負担となっている。二点目は、近年のネットワークセキュリティ動向により、Zebedee で使用している暗号通信を許可していないネットワーク環境（大学、研究所、ビジネスホテル等）が増加していることである。機器担当者が WARCS 専用端末を携行していない状況もしくはネットワークセキュリティ上 WARCSv1 の通信制限が生じている状況において、緊急時のリモートメンテナンス作業を実施できない事態が発生している。

* Department of Information Engineering, Graduate school of Science and Technology, Shinshu University.

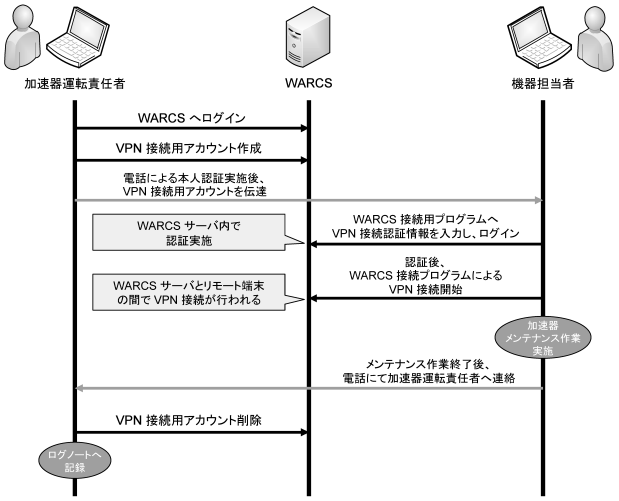

Figure 1: Operation flow of the WARCS version 1.

3． 新 WARCS の設計と構築

前章で述べた課題を解消するため、新規に設計する WARCSv2 ではクライアントとして一般的な PC を利用可能とし、近年のネットワーク接続環境へ適合した通信技術の採用を目指した。また、WARCSv2 の操作を行う者が直感的に理解できる画面デザインおよびユーザーインターフェイスの実装を目標とした。

VPN 構築技術は IETF (Internet Engineering Task Force) [4] による技術規格へ準拠した暗号通信プロトコルである SSL (Secure Socket Layer) [5] を使用している SSL-VPN を採用した。特にオンデマンド型 SSL-VPN の導入により、一般的なオペレーティングシステム (Microsoft Windows, Apple MacOS X) を搭載した PC における VPN 接続を行うことが可能となり、専用端末が手元に無い状況でも緊急メンテナンス作業が実施可能となった。また、緊急メンテナンス作業を実施する他研究所等のネットワーク環境において一般的に通信が許可されている SSL を使用することにより、WARCSv2 における VPN 接続の可用性が向上した。更に、専用の SSL-VPN 装置を用いることにより、悪意のある攻撃者によるセキュリティ問題が発生した場合に、加速器運転責任者あるいは運転員がネットワークケーブルを VPN 装置から物理的に切り離すという明快な操作で緊急対処が可能な構成にした。(Figure 2 参照)

VPN 装置と連携して動作する WARCS サーバの操作画面は一般的な Web ブラウザを用いてアクセスおよび全ての操作が可能となる Web アプリケーションとして構築した。WARCSv2 におけるアカウント追加および削除の操作を行う者は加速器の制御・運転を行う研究者および運転員であり、一般的にアカウントサーバーの管理技能を有していない。WARCSv2 では上記に留意し、操作する者が直感的に理解できるユーザーインターフェイスを設計した。また、操作において画面遷移が発生せず、全ての情報が 1 つの画面中に収まるような画面レイアウトを設計した。(Figure 3 参照)

Figure 2: Components of the WARCS version 2. These components are installed at the control room.

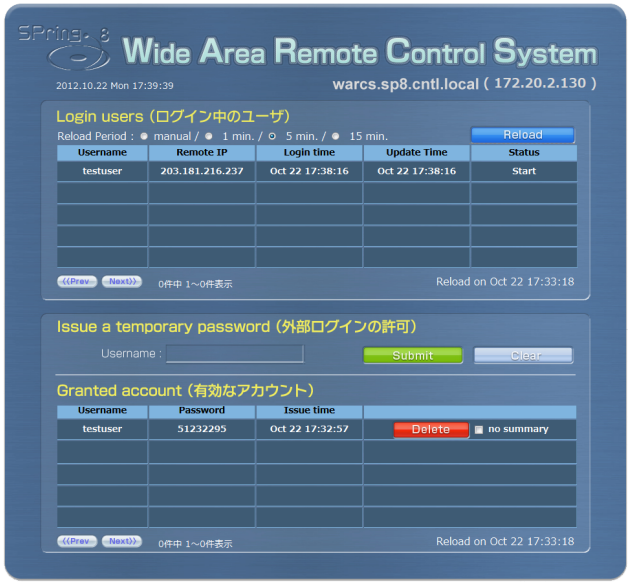

Figure 3: Account-control screen of the WARCS version 2.

4． 新 WARCS の導入と運用

WARCSv2 導入にあたり、システムの概要および操作手順についての説明会をあらかじめ複数回実施した。WARCSv2 は、WARCSv1 と操作が異なる部分があり、WARCS 利用者（加速器運転責任者、加速器運転員、および機器担当者）に十分な周知が必要と判断したためである。(Figure 4 参照) 説明会では WARCSv2 と同様な設定を施したトレーニング用システム一式を用意した。トレーニング用システムは実際の加速器制御系ネットワークとは接続されていないため、WARCSv2 の操作習熟および VPN 接続に使用する PC の接続テストを安全に行うことができる。

WARCSv2 は平成 24 年度より SPring-8 および SACLA へ導入し、運用中である。

5． まとめ

WARCSv1 における課題を解決するため、WARCSv2 では標準的なネットワーク関連技術を導入し、利便性および可用性の高いリモートメンテナンスシステムを実現した。また、Web アプリケーションの実装および視認性に優れた画面デザインの導入により、操作者にとっ

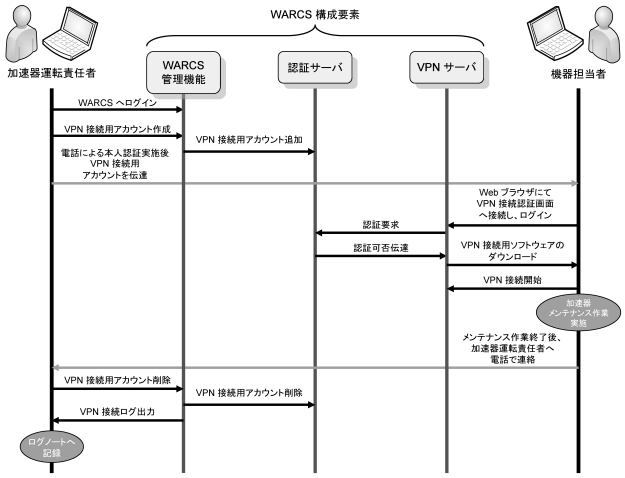

Figure 4: Operation flow of the WARCS version 2.

て使いやすい操作環境を提供している。

現在、WARCS によるリモートメンテナンス作業では、コマンドライン・インターフェイス (Command Line Interface, CLI) あるいは VNC (Virtual Network Computing) を用いた加速器操作端末の画面転送によるメンテナンス作業が行われている。今後、WebSocket や HTML5 を用いた操作インターフェイス [6] を組み合わせることにより、リモート端末側においても安全かつ快適なメンテナンス作業の実現が期待される。

参考文献

[1] R. Tanaka, et al., “Control System of the SPring-8 Storage Ring” In Proceedings of ICALEPCS ’95, page 201, Chicago, USA, 1995.

[2] A. Yamashita and Y. Furukawa, “WARCS: WIDE AREA REMOTE CONTROL SYSTEM IN SPRING-8.” In Proceedings of ICALEPCS 2005, Geneva, Switzerland, 2005.

[3] Zebedee: Secure IP tunnel., http://www.winton.org.uk/zebedee/.

[4] The Internet Engineering Task Force (IETF)., http://www.ietf.org/.

[5] A. Freier, P. Karlton, and P. Kocher., “The Secure Sockets Layer (SSL) Protocol Version 3.0”, RFC 6101 (Historic), August 2011.

[6] A. Uchiyama, et al., “Development and Implementation of EPICS Channel Access Client with Real-time Web using WebSocket” In Proceedings of PASJ 2012.