SuperKEKB 加速器制御ネットワークのセキュリティ向上

IMPROVEMENT OF THE SUPERKEKB ACCELERATOR CONTROL NETWORK SECURITY

中村卓也 *A)、岩崎昌子 B)、大西幸喜 B)、帯名崇 B)、草野史郎 A)、
佐藤政則 B)、中村達郎 B)、古川和朗 B)、三増俊広 B)、森田昭夫 B)
Takuya Nakamura* A), Masako Iwasaki B), Yukiyoshi Onishi B), Takashi Obina B), Shiro Kusano A),
Masanori Satoh B), Tatsuro Nakamura B), Kazuro Furukawa B), Toshihiro Mimashi B), Akio Morita B)
A)Mitsubishi Electric System and Service Co.,Ltd.,
B)High Energy Accelerator Research Organization (KEK),

Abstract

We have improved the network security of the SuperKEKB accelerator control network system. In the KEKB project, the main server computers for the accelerator control were connected to both the KEKB-accelerator-control and the KEK-laboratory networks. For SuperKEKB, the network configuration has been improved to enhance the network security, by separating the accelerator control network from the KEK laboratory network. In this improvement, we construct the new account system, install the firewall between the networks, and set up the new login server to access the accelerator control network. Various network services are also reconstructed. In this paper, we report these improvements of the SuperKEKB accelerator control network.

1. はじめに

高エネルギー加速器研究機構では、KEKB 加速器の高輝度化計画として、SuperKEKB 加速器の建設を進めている [1]。この高輝度化に対応すべく、我々は SuperKEKB 加速器制御ネットワークの改良を行った [2]。

2010 年まで運転した KEKB では、主要な加速器制御用サーバー計算機は、加速器制御ネットワークと KEK 機構内ネットワークの双方に接続されていた。ネットワークセキュリティ対策の観点から、ネットワークの接続構成を見直し、加速器制御ネットワークと KEK 機構内ネットワークの分離を行った。この改良を行うために、新規に、2 つのネットワークシステムで運用するためのアカウントシステムの構築、2 つのネットワークを分離するためのファイアーウォールの設置・設定、加速器制御ネットワークへアクセスするためのログインサーバーの設定等を行った。また、このネットワーク分離に伴い、加速器運用のために必要な、種々のネットワークサービスの構築も行った。

本稿では、これら SuperKEKB 加速器制御ネットワーク構成の改良について報告する。

2. ネットワーク構成

2.1 従来の構成

2010 年まで運転していた KEKB では、加速器制御用サーバー計算機や SAD 計算機の多くが、加速器制御ネットワークと機構内ネットワークの双方に接続されていた (図 1)。これらの加速器制御用サーバー計算機や SAD 計算機では、加速器制御ネットワークを通じて現場の機器と通信を行い、加速器の運転制御を行っていた。また SAD 計算機は、加速器の運転制御だけでなく、SAD プログラム [3] と呼ばれるビーム光学計算プログラムの実行環境としても運用されており、KEKB 及び他のプロジェクトのユーザーによっても利用されている。SAD プログラムを利用するユーザーは、機構内ネットワークを通じて SAD 計算機にログインし、計算処理を行っていた。

また、加速器制御用サーバー計算機と SAD 計算機は、同一のアカウント管理システムによりユーザーの管理を行っていた。KEKB 関係者のユーザーと他のプロジェクトのユーザーとは、特に区別や制限を設けず同等に扱っていたため、ユーザーは加速器制御用サーバー計算機と SAD 計算機のどちらにもログイン可能な状況となっていた。このような環境であるため、例えば、他のプロジェクトのユーザーがビーム光学計算の処理で計算機やネットワークのリソースを多く消費した場合、KEKB 加速器の運転制御プログラムの処理が滞るなど、加速器の運転に影響を及ぼす可能性が考えられる。また、ユーザーの思い違いや操作ミスといったヒューマンエラーなどにより、シミュレーション計算のみを行うつもりであったとしても、実際の加速器のパラメータを変更してしまうことも起こりうる。

このような加速器の運転上のリスクを軽減させるため、今回、加速器制御ネットワークと機構内ネットワークとを明確に分離する構成を検討した。

2.2 新たなネットワーク構成

新たなネットワークの構成として、加速器制御用サーバー計算機や SAD 計算機、さらにはユーザーの PC に至るまで、加速器制御ネットワークと機構内ネットワークの双方に同時に接続しない構成を検討する。加速器制御用サーバー計算機や SAD 計算機は、必要に応じて加速器制御ネットワークと機構内ネットワークのそれぞれに用意し、各種サービスを提供する。加速器制御ネットワークに接続された計算機では、主として加速器の運転制御を行い、機構内ネットワークに接続された計算機では、各プロジェクトのユーザーに SAD プログラムの実行環境を提供する。

* nakataku@post.kek.jp

ここで、加速器制御ネットワークと機構内ネットワークとの分離を行うが、完全に切り離した構成とはしない。実際の運用では、それぞれのネットワークにあるサービスを利用する状況が考えられるため、双方のネットワーク間で通信できるような経路を用意する必要がある。ただし、ネットワーク間の通信は基本的には遮断しておき 、必要最低限の決められた通信のみを許可する構成としたい。そこで、双方のネットワークの間にファイアーウォールを設置し、決められた通信のみを許可する構成とする (図 2)。

今回の、加速器制御ネットワークと機構内ネットワークを分離した、新たなネットワーク構成の主要な構成要素について説明する。

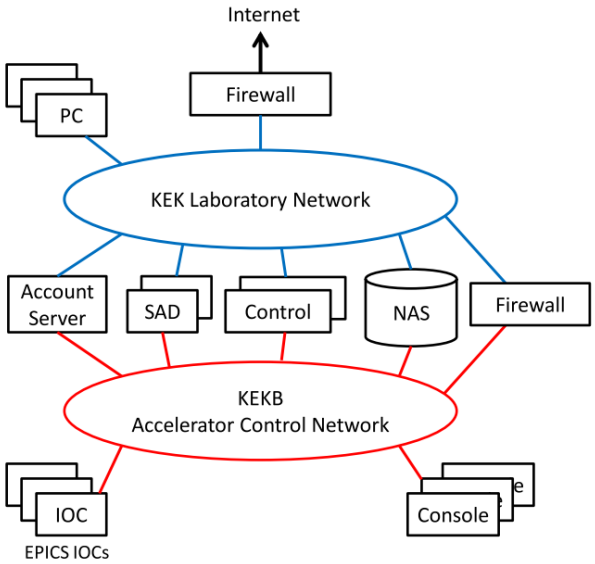

Figure 1: Former network configuration.

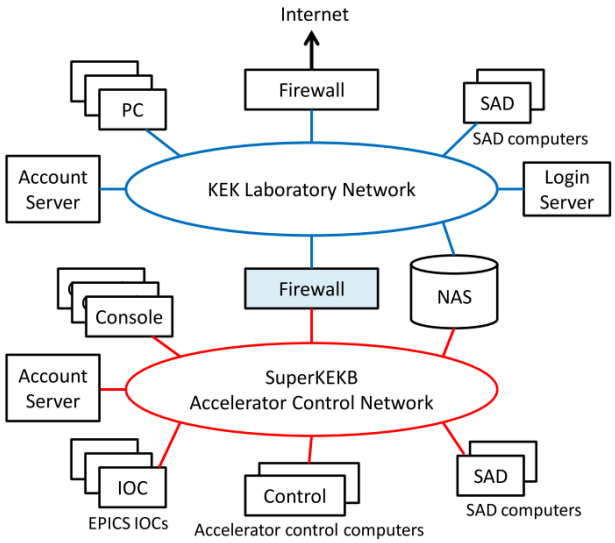

Figure 2: New network configuration.

3. ネットワークの構成要素

3.1 ファイアーウォール

加速器制御ネットワークと機構内ネットワークとの間にファイアーウォールを設置し、決められたホストやサービス、プロトコルのみを通過させるよう整備する。ファイアーウォールは、機能や通信帯域などの面から機種の選定を行い、Cisco 社の ASA5545-X を導入した。加速器制御ネットワーク、機構内ネットワークのスイッチとは Ether Channel を用いて接続し、4Gbps の通信帯域を確保している。

ファイアーウォールでは、必要に応じてそれぞれのネットワーク間の通信を許可している。後述するアカウント管理システムの通信、Web サービス、メール転送サービス、その他の主要なサービスなど、KEKB 制御グループが運用するサービスを提供できるよう整備している。また、KEKB 制御グループが運用する主要なサービス以外に、各ユーザーからのネットワークをまたいだ通信要求についても、必要に応じて許可している。例えば、機構内ネットワークの PC から制御ネットワークの測定器を直接操作したい場合には、その端末と測定器の間に限って通信を許可するよう設定している。

また、ファイアーウォールを経由した通信は全てログに記録しており、トラブルが発生した際にはログを遡って調査できるよう整備している。ファイアーウォールの機器本体が持つログの保存領域が少ないため、外部に syslog サーバーを用意してログの転送と保存を行っており、現在は 3ヶ月間のログを保存する設定としている。

3.2 アカウント管理システム

従来のアカウント管理システムでは、KEKB 加速器の関係者のユーザーと、他のプロジェクトのユーザーとは特に区別しておらず、一つのアカウント管理システムで管理していた。また、アカウント管理システムを運用している計算機は、双方のネットワークに接続してサービスを提供していたが、今回のネットワーク分離のために新たなアカウント管理システムの構築が必要となった。そこで、加速器制御ネットワークと機構内ネットワークのそれぞれに、アカウント管理システムを運用する計算機を用意する構成を検討した。

今回、アカウント管理の新たな方針として、KEKB 関係者のユーザーと、他のプロジェクトのユーザーとを区別し、ユーザーごとにログイン可能な計算機を分ける仕組みを導入したい。KEKB 関係者のユーザーは、加速器制御ネットワークと機構内ネットワークにある、全ての計算機へのログインを可能とし、他のプロジェクトのユーザーは、機構内ネットワークの計算機のみにログインできるよう調整する。このような方針を実現する為に、加速器制御ネットワーク側のアカウント管理システムでは、他のプロジェクトのユーザーが無効となるよう、アカウント情報を調整する必要がある。

また、加速器制御ネットワークと機構内ネットワークとで、それぞれにアカウント管理システムのサーバーを用意するが、管理や運用の面から、なるべく情報を共有したい。そこで、情報を共有しながらユーザーの区別が行えるよう、アカウント情報の調整を行うスクリプトを作成した。

3.3 アカウント情報調整スクリプト

今回検討したアカウント管理システムでは、KEKB 関係者のユーザーと他のプロジェクトのユーザーとを区別して管理する。従来より、KEKB ではアカウント管理システムとして LDAP を利用している。LDAP には、レプリケーションと呼ばれるサーバー間で情報を同期する機能があるが、今回の構成ではユーザーの無効化処理を行うなど、情報の一部を変更する必要があるため、利用することができない。そこで今回、アカウント情報の共有と変更を行うスクリプトを作成した。

今回検討したアカウントの管理方針から、機構内ネットワークでは全てのユーザーを有効とし、加速器制御ネットワークでは KEKB 関係者のユーザーのみを有効とするよう調整する。そのため、機構内ネットワーク側の情報をマスターとし、加速器制御ネットワーク側はマスターからの情報を編集して利用する構成とする。LDAP で管理するユーザーアカウントの情報には description という項目があり、この項目を利用してアカウントを区別する仕組みを整備する。加速器制御ネットワークの計算機でスクリプトを実行すると、機構内ネットワークの LDAP サーバーに問い合わせを行い、アカウント情報を取得する (図 3)。取得したアカウント情報の description の項目をチェックし、KEKB 関係者を示す情報が含まれていれば、加速器制御ネットワーク側の LDAP サーバーにそのまま登録する。また逆に、KEKB 関係者を示す情報が含まれていなければ、無効なアカウントとして情報を書き換えて LDAP サーバーに登録する。アカウントを無効にする方法としては、アカウント情報のパスワード、ログインシェル、ホームディレクトリの項目を、無効な値へと書き換える事で実現する (図 4)。

今回作成したスクリプトは毎分実行しており、LDAP サーバー間の情報の共有と調整を常時行っている。

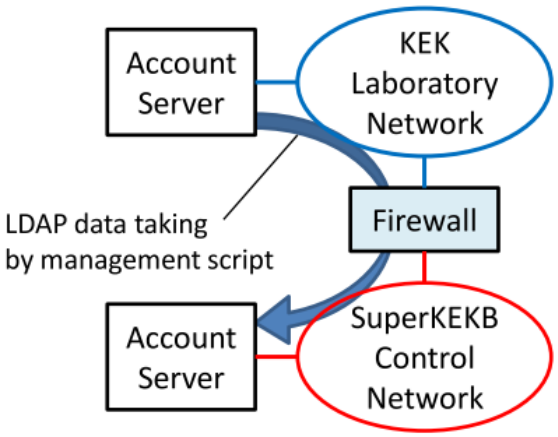

Figure 3: LDAP server layout, and LDAP data management script.

3.4 ファイルサーバー

ファイルサーバーは、ユーザーがログインして利用するサーバー計算機とは異なるため、双方のネットワークに接続して運用する方針とする。ファイルサーバーは加速器制御ネットワークと機構内ネットワークの双方に接続し、両ネットワークのサーバー計算機は、同一のファイルシステムを共用する構成とする。このファイルサーバーには、ユーザーのホームディレクトリや加速器のデータが納められており、どちらのネットワークの計算機からも同じ環境でアクセスできるよう整備されている。そのため、ユーザーはどちらのネットワークの計算機にログインしても、同じ環境でファイルを扱う事ができる。これにより SAD プログラムを利用するユーザーは、これまでと同様に機構内ネットワーク側の計算機での作業が可能となる。

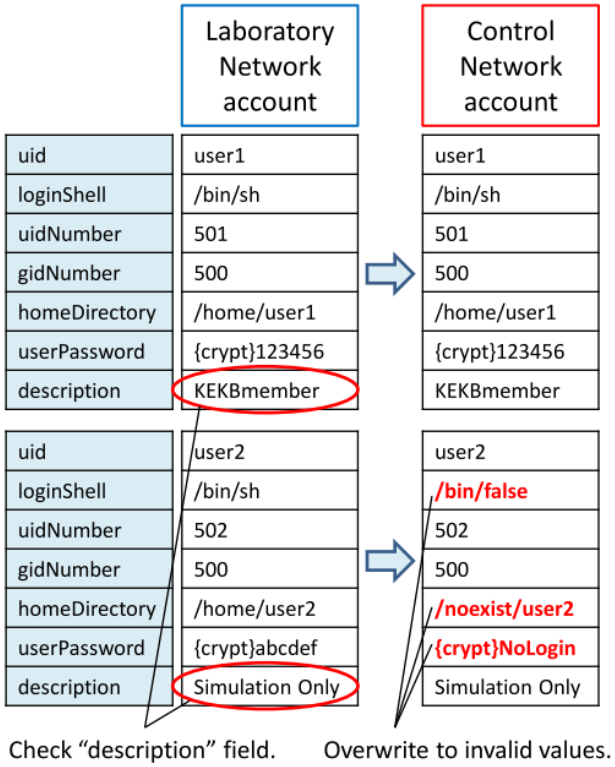

Figure 4: User account check by LDAP data management script.

3.5 ログインサーバー

機構内ネットワークの端末から、加速器制御ネットワークの計算機へとログインするために、ログインを中継するログインサーバーを用意した。機構内ネットワークの端末からログインサーバーにログインし、さらにそこから加速器制御ネットワークへの計算機へとログインする。ログインサーバーは機構内ネットワークに接続する計算機ではあるが、加速器制御ネットワークのアカウント管理システムを参照し、KEKB 関係者以外はログインできない構成としている。また、ログインサーバーでは、加速器制御ネットワークの計算機へのログインを中継することのみを想定している。そのためファイルサーバーにあるユーザーのホームディレクトリは参照せず、空のホームディレクトリを用意し、ログインサーバーでの作業ができないよう調整した。

3.6 その他のサービス

これまでに説明した以外にも、様々なサービスについて、加速器制御ネットワークや機構内ネットワークで利用できるよう整備した。運転ログシステムや、その他の制御グループで提供する Web サービスは、加速器制御ネットワークの計算機で運用している。それらの Web サーバーに機構内ネットワークの端末からもアクセスできるよう、Web アクセスの中継用のサーバーを用意した。機構内ネットワークの端末は、中継用のサーバーを通じて制御ネットワークの Web サービスを利用する事が出来る。また逆に、加速器制御ネットワークの端末から外部の Web サーバーへアクセスできるよう、プロキシサーバーの整備も行った。その他にも、メール中継サーバー、DNS サーバー、NTP サーバーなど、計算機の運用で必要となる様々なサービスについて、加速器制御ネットワーク内で利用できるよう整備した。

4. 運用実績とまとめ

2013 年 8 月、加速器制御ネットワークと機構内ネットワークとを分離した、新たなネットワーク構成の運用を開始した。今回構築した、アカウント管理システムやその他の各種サービス、ファイアーウォールを経由した通信は順調に動作しており、正常な運用を実現できている。今後は、アカウント管理システムやその他主要なサービスについて、サーバーの冗長構成などを構築するなどして、より安定なシステムを運用できるよう進めていきたい。

参考文献

[1] K.Akai, et al., “Design Progress and Construction Status of SuperKEKB”, Proc. of IPAC12, pp. 1822-1824 (2012); http://accelconf.web.cern.ch/AccelConf/IPAC2012/papers/tuppr006.pdf

[2] 岩崎昌子, 他, “SuperKEKB 加速器制御ネットワークシステムの構築”, in these proceedings.

[3] SAD program http://acc-physics.kek.jp/SAD/