J-PARC 加速器制御 LAN から所内 LAN へのリアルタイムかつ詳細な加速器運転情報の提供

REAL-TIME AND DETAILED PROVISION OF ACCELERATOR OPERATION INFORMATION FROM THE J-PARC ACCELERATOR CONTROL LAN TO THE J-PARC OFFICE LAN

山田秀衛 *
Shuei YAMADA*
High Energy Accelerator Research Organization (KEK) / J-PARC Center

Abstract

J-PARC Main Ring (MR) started its beam operation in 2008. As MR become more sophisticated in the past 10 years, yet more stable operation is required. Accordingly, demands to acquiring real-time and detailed status of the accelerators and its equipment are increasing from equipment experts and users, not only from the accelerator control network but also from the J-PARC office network. On the other hand, any kind of operation of the accelerator, whether intentional or not, shall be prohibited from the office LAN. This report describes construction of a gateway system, which relays real-time information of MR from the control network to the office network, while minimizing the influence from the office network to the control network.

1． はじめに

J-PARC のオフィス LAN は JLAN と呼ばれている。これまで JLAN に提供されていた J-PARC 加速器の運転情報は, Fig. 1 に示すような,

- 加速器シフトリーダーが随時入力する” 最新の器運転状況”
- 1 分に 1 回程度更新される画像による総合運転情報

の 2 つを 1 枚の web ページにまとめたものだけであった。

MR が 2008 年にビーム運転を開始して以来, 加速器の高性能化と高度化が進んでおり, より安定した運転が求められるようになっている。これに伴って, 従来は加速器制御 LAN からしか取得できなかった,

- MR 加速器の電磁石等の電源の状態
- ビームダクト内の真空の現在の圧力と過去の履歴
- 電源棟内の現在の気温と過去の履歴

といったより詳細な運転情報を, 居室からもリアルタイムに取得したいという機器担当者やユーザーからの要望が高まってきた。

2． EPICS と CA GATEWAY

J-PARC 加速器の制御システムは, 分散制御システムのフレームワークである EPICS [1] を用いて構築されている。EPICS は Channel Access (CA) と呼ばれるプロトコルを用いて, TCP と UDP の両方でポート 5064 と 5065 を通してクライアント・サーバ通信を行う。加速器のオペレータや機器の担当者が操作する上位制御系アプリケーションは OPI と呼ばれる。OPI は CA のクライアントで, CA のサーバにアクセスする。対象機器を制御するフロントエンドの計算機を I/O Controller (IOC) と呼ぶ。IOC は CA のサーバとなって, クライアントに制御点への I/O アクセスを提供する。

通常は, 同一のネットワーク内でのみ CA を用いた通信が可能である。クライアントは UDP のブロードキャストを用いてネットワーク上の制御点を検索する。PV を検索するブロードキャストに対して, 当該制御点を提供している IOC がクライアントに返答すると, クライアントは TCP で IOC への接続を確立する。

あるネットワークから別のネットワークへと CA を中継するためのユーティリティプログラムとして, CA Gateway [2] が提供されている。CA Gateway は, 一方のネットワーク上では CA のクライアントとして機能する。他方のネットワークではクライアントに CA のアクセスを提供するサーバとして IOC のように振舞う。CA Gateway を用いることで, 加速器制御 LAN と同じ加速器運転情報をリアルタイムに JLAN に中継することが可能となる。

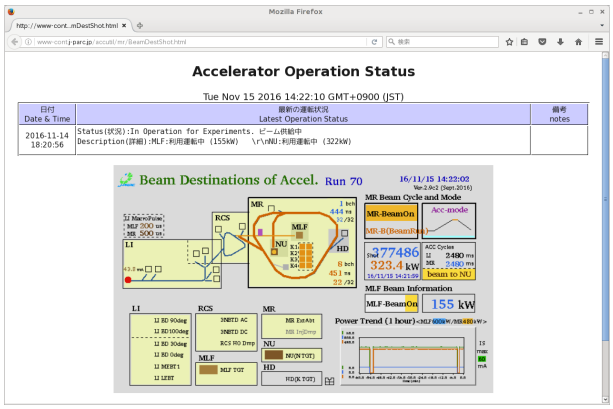
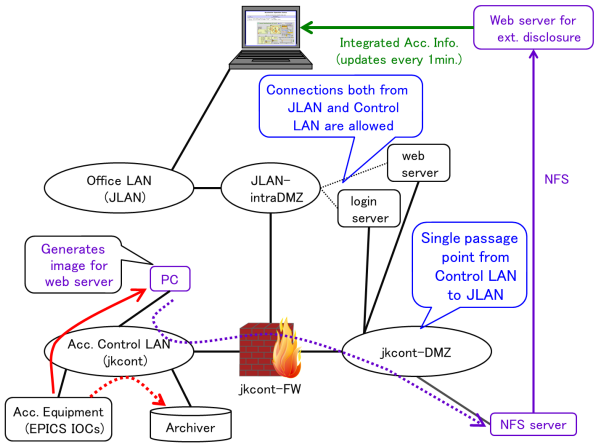
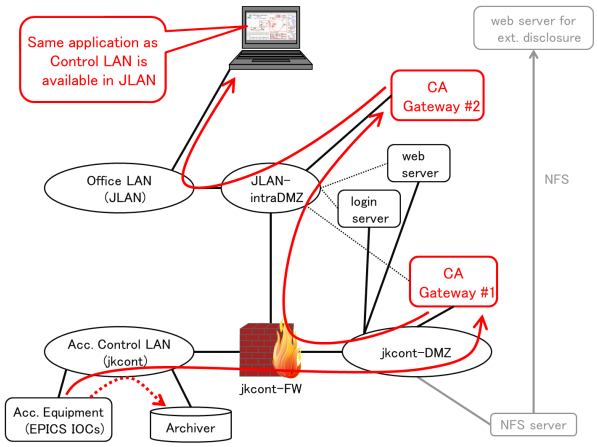


Figure 1: A web page which shows J-PARC accelerator status.

* shuei@post.kek.jp



(a) Before introduction of the gateway system.



(b) After introduction of the gateway system.

Figure 2: Transmission path of data from the accelerator control LAN to the JLAN.

3． 二段階の GA GATEWAY を用いた加速器制御 LAN への影響の緩和とアクセス制限

加速器制御 LAN はファイアウォール装置を介して JLAN に接続されている。制御 LAN と JLAN の間には，緩衝領域としてファイアウォール装置の機能を用いた非武装地帯 (DMZ) が設けられている。制御 LAN, 制御 DMZ, JLAN の三つのネットワーク間の通信は，

- これらのネットワーク間の通信は必ずファイアウォール装置を経由しなければならない。ファイアウォール装置以外の情報機器は，これらのネットワーク間をブリッジ接続してはならない。
- 制御 LAN に接続された機器と JLAN に接続された機器が直接通信することは一切禁止する。
- 制御 LAN と制御 DMZ は，特定のポート番号，送信元 IP アドレス，送信先 IP アドレスのパケットに限り通信可能とする。
- 制御 DMZ と JLAN も，特定のポート番号，送信元 IP アドレス，送信先 IP アドレスのパケットに限り通信可能とする。

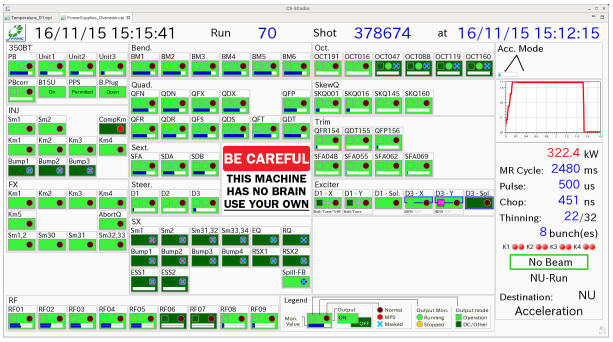
というポリシーで運用されている。

Figure 2a に，加速器運転情報が JLAN に提供されるまでの従来の情報の流れを示す。1 分間に 1 回，加速器制御 LAN に接続された PC で加速器総合運転情報の画像ファイルを作成し，制御 DMZ に接続されたファイルサーバにコピーする。JLAN に接続されている web サーバがファイルサーバにアクセスし，web ページとして画像を JLAN に提供する。制御 LAN から JLAN に提供するのは画像ファイルであること，web サーバは読み取り専用でファイルサーバにアクセスすることで，JLAN から制御 LAN に接続されている加速器の機器を操作することがないようにしている。

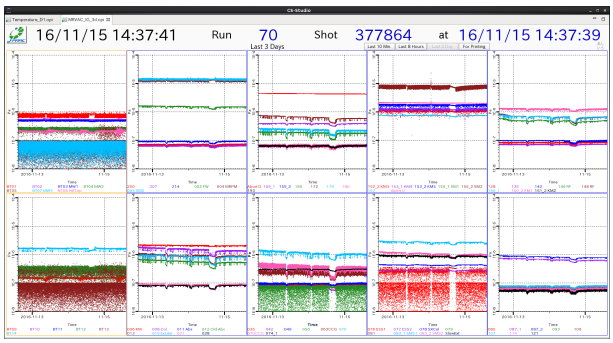
先に述べたように，CA Gateway を用いると制御システムが利用している CA プロトコルを JLAN に中継することが可能となる。Figure 2b に示す経路で加速器運転情報がリアルタイムに JLAN へと提供される。CA Gateway をそのまま用いると JLAN から加速器の機器を操作することも可能となってしまうが，本報告で構築するゲートウェイシステムは JLAN から加速器の運転情報を読み出すことだけを目的としている。意図的で有る無しにかかわらず，JLAN から加速器の機器を操作することは想定していない。そこで，JLAN から制御 LAN にある加速器の制御機器への書き込みを禁止し，アクセス制限を行うため，CA Gateway を次に述べるような二段構成とする。

- 制御 DMZ に置く CA Gateway #1
  加速器運転情報を制御 LAN から CA Gateway #2 だけに提供する。制御 LAN-JLAN 間の通信を可能にするために，CA Gateway #1 には制御 DMZ の IP アドレスのほかに，ファイアウォールの NAT 機能を用いて JLAN-intraDMZ にも IP アドレスを割り当てる。
  CA Gateway の設定で，制御 DMZ から制御 LAN への CA による書き込みを禁止する。また，ファイアウォールでアクセス制限と侵入検知を行う。CA の送信元は CA Gateway #2 からの接続だけに制限し，CA Gateway #2 との通信は CA が用いるポートだけに制限する。SSH によるログインは，制御 DMZ に接続されているログインサーバだけを許可する。
- JLAN-intraDMZ に置く CA Gateway #2
  JLAN に接続された各ユーザーのクライアント PC に CA の接続を提供する。CA Gateway の設定で，JLAN から制御 DMZ への CA による書き込みを禁止する。ファイアウォールでアクセス制限と侵入検知を行う。CA の送信元は JLAN からの接続だけに制限し，送信先は CA Gateway #1 だけに制限する。SSH によるログインは，制御 DMZ に接続されているログインサーバだけに許可する。

JLAN 側にある CA Gateway #2 からアクセス可能な制御 DMZ の機器は CA Gateway #1 だけである。従って，たとえ CA Gateway #2 に侵入されても，制御 LAN 内のその他の機器に直接アクセスされることはない。



(a) A screenshot of an OPI showing operation mode of MR and status of power supplies.



(b) A screenshot of an OPI showing time variation of pressure in MR beam pipe.

Figure 3: Example of OPIs actually used for MR operation.

4． JLAN での制御アプリケーションの利用

従来, MR で EPICS の上位制御系アプリケーションを開発する場合は, X Window System 上で動作する EDM [3] や MEDM [4] といった GUI ビルダを用いていた。これらのアプリケーションを JLAN で利用する場合は, 各利用者の PC に X Window System がインストールされていなければならない。また, 画面定義ファイルも別途配布し, 各利用者の PC にインストールする必要がある。MR の運転で用いている画面定義ファイルの数は 100 を超えている。開発者は画面定義ファイルが更新されるたびに最新版を配布しなければならず, 利用者は随時ダウンロードしてインストールしなければならない。EDM や MEDM を JLAN でも利用する場合は, 開発者と利用者の双方にとって煩雑となることが予想された。

MR では, 2015 年に加速器制御システムの GUI 開発に CSS を導入した [5, 6]。これにより, JLAN への最新版の画面定義ファイルの配布・インストールの問題と X Window System の問題が解決した。

CSS は EPICS で大規模な制御システムの GUI を構築するための統合環境で,

- BOY : GUI のビルダと実行環境
- Data Browser : リアルタイムデータとアーカイブからの取得した過去の時系列データのトレンドグラフの表示
- BEAST : アラームシステム
- 電子ログ
- アーカイブシステム

といった様々な機能を連携して運用することができる。また, マルチプラットフォームな統合開発環境である Eclipse をベースにしており, Linux, macOS, Windows 上で実行することができる。

MR 加速器では, JLAN から加速器の運転状況を閲覧したい機器担当者やビームのユーザー向けに, JLAN での利用に向けて設定した CSS のパッケージを zip ファイルで所内に配布している。CSS の画面定義ファイル群は実行時に web サーバから取得するように設定してある。CSS の利用者は画面定義ファイルが更新されるたびにこれをダウンロードして自分の PC にインストールする必要がない。加速器の運転に用いているのと同じ最新の画面定義ファイルを常に利用可能である。加速器の状態をモニタするために使用している CSS アプリケーションの例を Fig. 3 に示す。

Figure 4: Two server PCs running the gateway system.

Table 1: Specifications of PiNON Sabataro® Type-P

Processor	Celeron J1900 (2 – 2.42 GHz), 4 cores
RAM	8 GB (1333 MHz DDR3L SO-DIMM × 1)
Storage	128 GB (mSATA SSD × 1)
Network	GbE × 2
Display I/F	HDMI
USB ports	USB 2.0 × 2
Dimension	W80.6 mm × D110.6 mm × H34.4 mm
TDP	max 15 W
	Fan-less
Power Supply	DC 12 V (AC/DC Adapter)

5． ゲートウェイシステ運用の履歴とまとめ

本報告で提案したゲートウェイシステムは 2018 年 4 月から運用を開始した。Figure 4 はゲートウェイシステムのハードウェアで, 2 台のサバ太郎 ® Type-P で構成されている。サバ太郎は PiNON 製のファンレス小型サーバで, その仕様を Table 1 に示す。

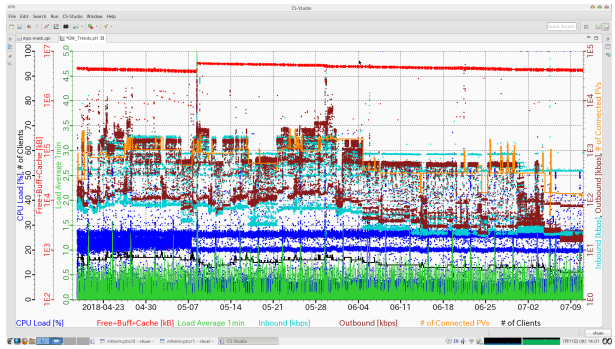


Figure 5: History of load of the gateway system for three months.

Figure 5 に示すのは, 2018 年 4 月の運用開始から 2018 年 7 月の加速器の夏季シャットダウンまでの CA Gateway #2 の運用状況の時系列グラフである。JLAN から CA Gateway #2 への CA のアクセス状況を見ると,

- 常時 10∼20 のクライアントからゲートウェイシステムへの接続があった。そのうち 8 クライアントは CA Gateway #2 を監視し, 時系列データを記録するための EPICS のアーカイブシステムである。
- アクセスがあった制御点の数は 100∼3000 個程度であった。
- ゲートウェイシステムを通過するデータ量は 1∼10 Mbps 程度であった。
- ゲートウェイの CPU, メモリともに余裕がある。ゲートウェイの CPU 負荷が 25% に達しているのは, アンチウィルスソフトが毎週 2 回フルスキャンをかけている最中に対応している。

となっている。約 3 ヶ月に亘って, ゲートウェイシステムは安定にサービスを継続できた。今後のゲートウェイシステムの利用者の増加と活用が期待される。

参考文献

[1] EPICS - Experimental Physics and Industrial Control System; `http://epics.anl.gov/`
[2] Channel Access Gateway; `http://epics.anl.gov/extensions/gateway`
[3] EDM - Extensible Display Manager; `http://ics-web.sns.ornl.gov/edm/edmUserManual/`
[4] MEDM - Motif Editor and Display Manager; `http://www.aps.anl.gov/epics/extensions/medm/index.php`
[5] CSS – Control System Studio; http://controlsystemstudio.org/
[6] S. Yamada *et al.*, “Deployment of Control System Studio at J-PARC Main Ring”, Proceedings of the 8th Annual Meeting of Particle Accelerator Society of Japan, WEP103, pp.543 (2011).