



# 大型物理実験装置の制御システムの 構築, 運用とセキュリティ

Design, operation and security issues  
of large experimental physics control systems

古川 和朗

Kazuro Furukawa

高エネルギー加速器研究機構 (KEK)

KEKB and Linac Control Groups, KEK

< kazuro.furukawa @ kek.jp >



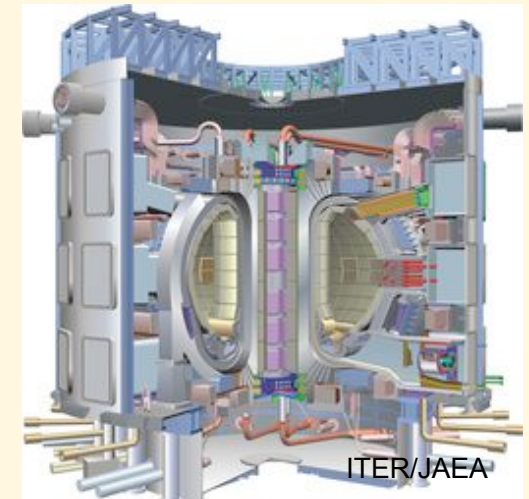
## 概要

- ◆ 大型物理実験装置と KEKB 粒子加速器
- ◆ KEKB 加速器と制御、ネットワーク
- ◆ KEKB 制御とセキュリティ、安全性

- ✧ セキュリティに対しては、都市インフラを支える制御システムなどに比べると、きわめて幼稚
- ✧ それであっても安全性は確保できるよう設計

# 大型物理実験装置

- ◆ 数十人から数千人規模の研究者が関わる物理実験装置
  - ❖ 素粒子物理学実験、光学・電波天文台、プラズマ核融合、など
  - ❖ ほとんどが国際協力で予算獲得、建設、運用
  - ❖ 例えば、素粒子のジュネーブ CERN/LHC、核融合のカダラッシュ ITER、天文のチリ ALMA などアジア、ヨーロッパ、アメリカの国際協力で実現しているものは多い
    - ✧ 関連した国際会議が開かれている、今年 10 月は国内 (神戸)



# KEK の粒子加速器



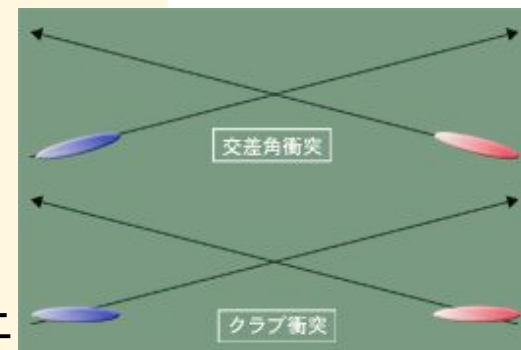
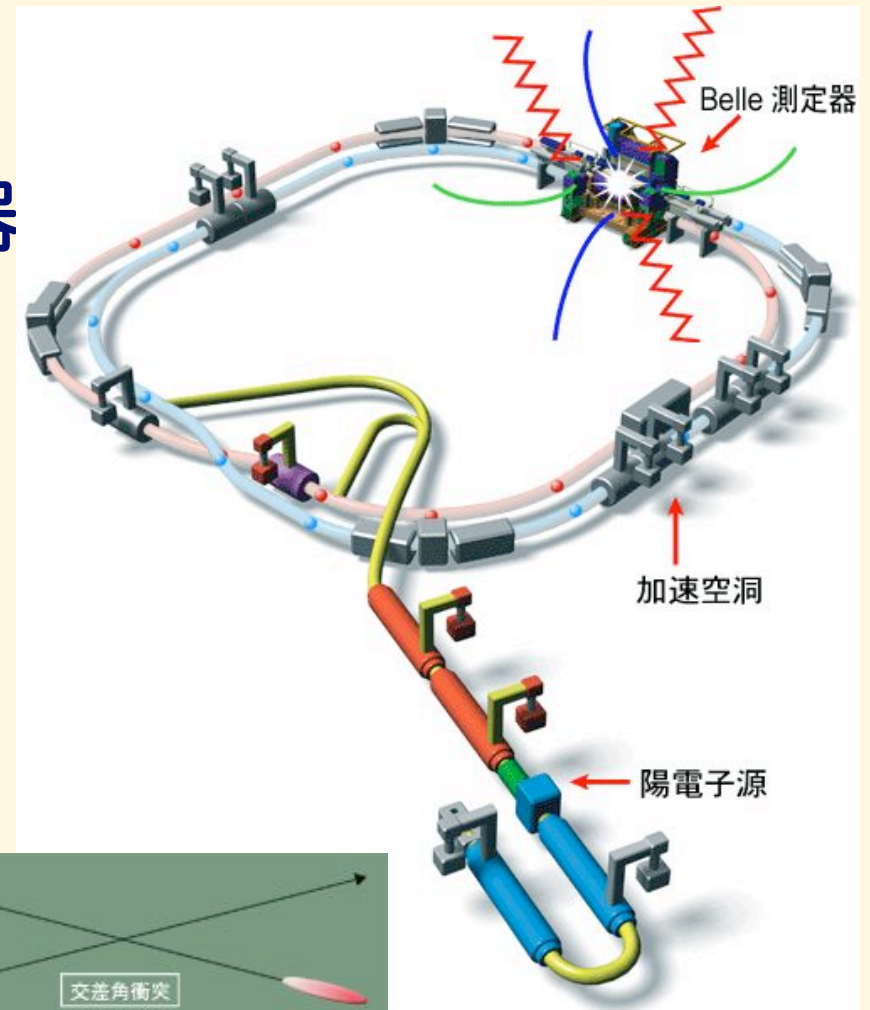
# KEKB リングと直線加速器

## ◆ KEKB B-ファクトリ:

電子陽電子非対称衝突型加速器  
主に CP 対称性の破れの研究

### ❖ ~3km 2重のリング:

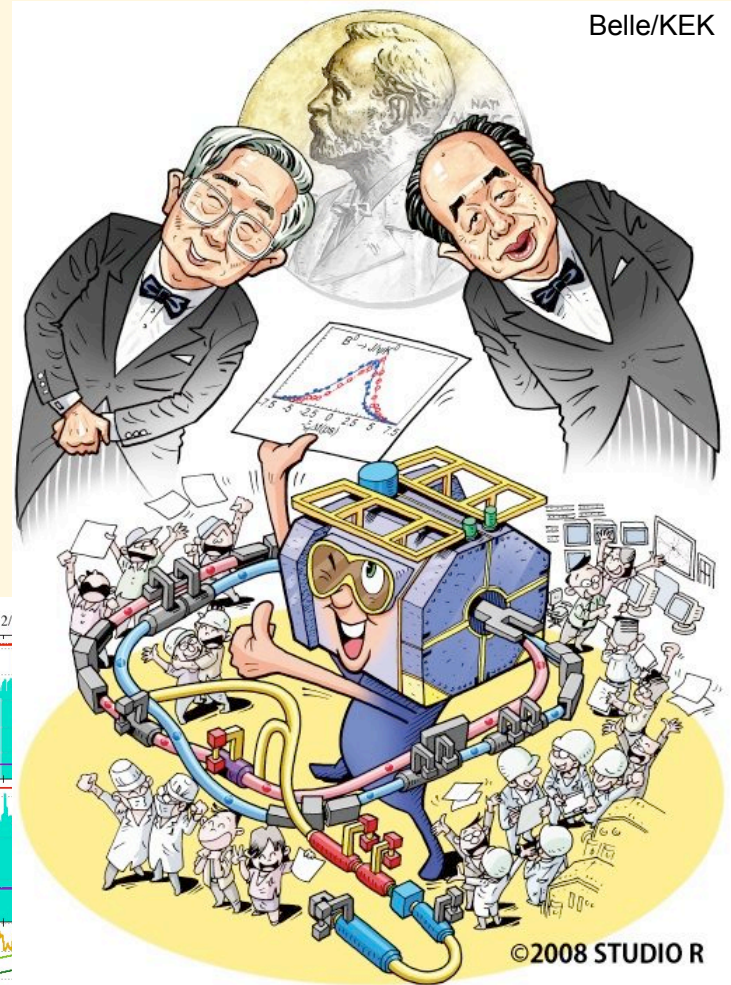
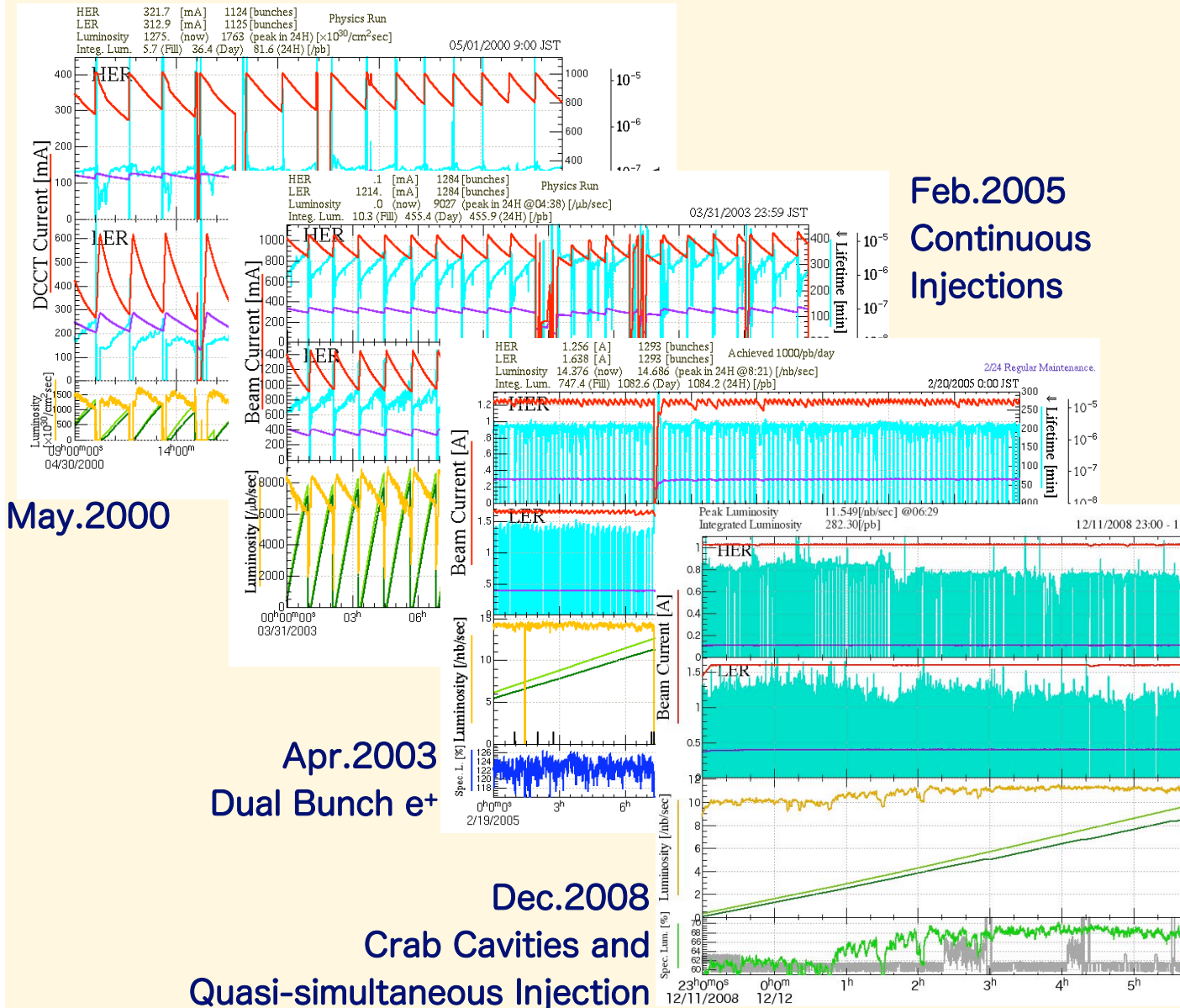
- ❖ 電子 (8GeV - 1.4A)
- ❖ 陽電子 (3.5GeV - 1.8A)
- ❖ 世界最高の衝突性能
- ❖ 放射光施設とも同時協調運用



世界初の Crab 空洞による性能の向上



# KEKB の性能の向上とノーベル賞



May.2000

Feb.2005  
Continuous  
Injections

Apr.2003  
Dual Bunch e<sup>+</sup>

Dec.2008  
Crab Cavities and  
Quasi-simultaneous Injection

# KEKB

## ◆多数の装置の複合体

- ❖ 数千の電磁石
- ❖ 数十の大電力マイクロ波生成装置
- ❖ 数千の真空装置
- ❖ 数千の診断装置
- ❖ 数百人の研究者
  - 現在では粒子加速器と測定器は分業している
  - 加速器も単なる電磁気学の応用では無く物理学の研究対象
  - また大規模超伝導利用や高真空などさまざまな分野と連携

## ◆制御

- ❖ 数千の組み込み小型コントローラ
- ❖ 数百の中間層の計算機
- ❖ 数十の取りまとめ用の計算機
- ❖ 主に IP を利用したネットワーク
  - IP アドレスで数千



# KEKB 加速器制御





# 過去のネットワーク

## ◆組み込み制御向け

### ❖光ファイバを多用した内製ネットワーク (1982~)

- ◆パルス高電圧 ( $\sim 50\text{kV}$ ,  $1\mu\text{s}$ ) を利用した機器からのノイズのため
- ❖数百台の機器が接続され、少しずつ計算機の利用範囲が広がる

### ❖IP ネットワークへ移行 (1989~)

- ◆内製をやめ、全ての通信を IP とすることにする
- ❖現在では当然の方向性と思われるが当時は意外とたいへん
- ◆しかし、機種依存性と保守の困難を避けるため無理かと思いつつ移行

### ❖媒体は何度か変遷したが、ソフトウェアは 15 年以上大きくは変わっていない

- ❖FDDI+10BaseFL ... 1000BaseLX+100BaseFx etc.
- ❖Redundant Tranceiver ... Rapid Spanning-tree + HSRP/VRRP

### ❖セキュリティは？

- ❖当初から研究用のネットワークとは分離されていた
- ◆しかし、研究所によっては...

## ◆研究向け

### ❖業界標準は DECnet であったが、徐々に IP へ (1992~)

## 過去のネットワークの脅威

### ◆過去にはさまざまな情報が原則公開（1990 年以前）

❖ドイツの中学生が国際 DECnet 経由で KEK や筑波大学に不正侵入 (1985)

❏さまざまないたずら、

❏その頃、加速器制御は特殊ネットワーク

❖その後も、主要制御計算機を国際 DECnet や Internet 上に置く研究所も多かった

❏研究者が国外研究所の File 取得したり Mail を読んだかなど容易に確認

❏その結果国外の研究所ではさまざまないたずらを受ける

◆一般公開日に研究者のタイプしたパスワードを覚え、後日侵入するなど

◆ログインメッセージを書き替えられるなど

❏当初から KEK の加速器制御は Firewall で分離

### ◆その後インターネットの普及とともにセキュリティの意識が高まる (1990 年以降)

❖現在では多重に Firewall で守られている

# KEKB 用コントローラと計算機

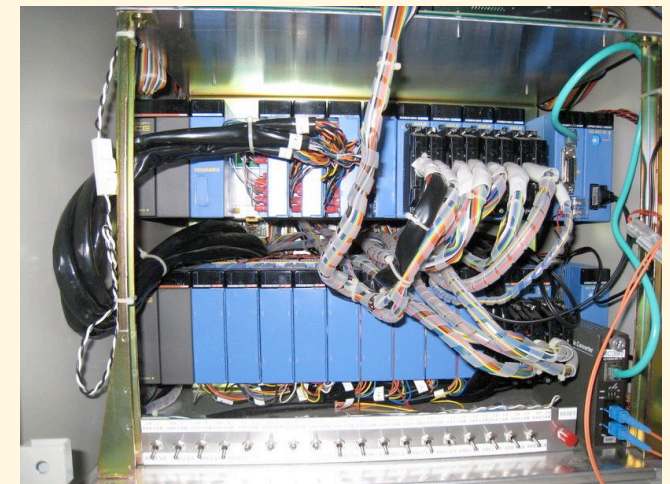
## ◆組み込み用

- ❖ VME - VxWorks, Linux, RTEMS, OS9, ...
- ❖ VXI - VxWorks, Unix, ...
- ❖ PLC - Ladder, Linux, ...
- ❖ Embedded Controllers - Linux, ITRON, ...
- ❖ FPGA-based Controllers - Linux, ...
- ❖ Measurement Tools - Proprietary, Windows, Linux, ...
- ❖ CAMAC - ...



## ◆全体制御用

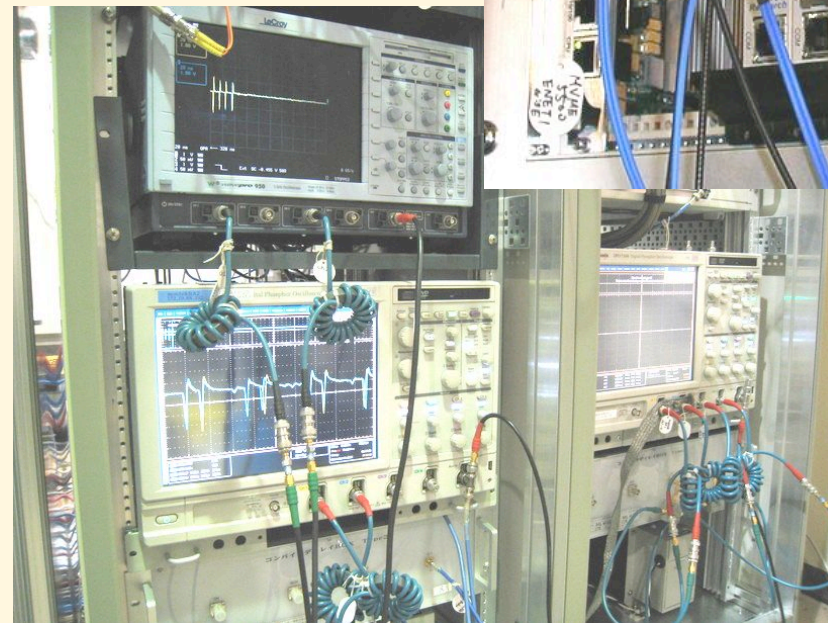
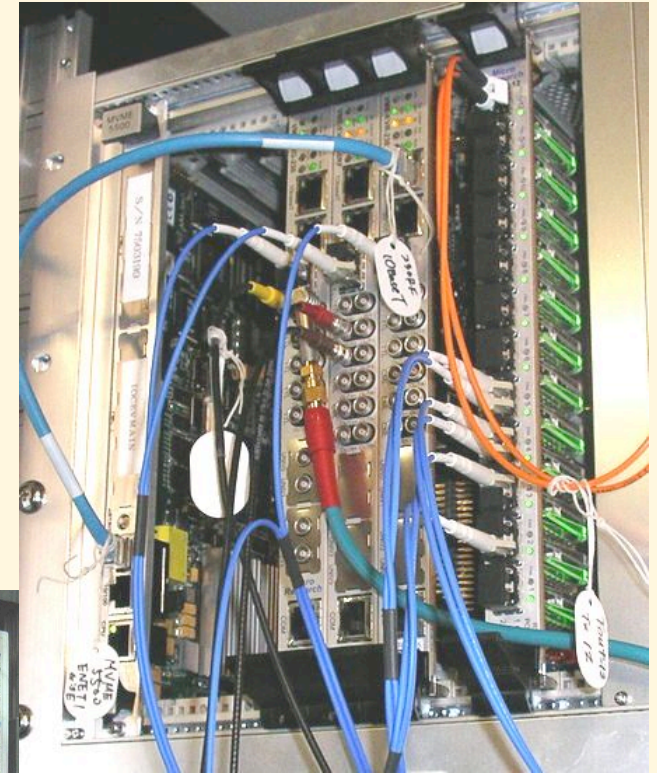
- ❖ Linux
- ❖ Macintosh
- ❖ Unix
- ❖ Windows
- ✧ 他の研究所でも大きくは変わらない



# コントローラ

## ◆最近 EPICS 組み込みのコントローラが増加

- ❖ VME - 高速処理
- ❖ PLC - 一般処理, EPICS 組み込みが増えそう
- ❖ 測定器 - 可能であれば EPICS 組み込み
- ❖ FPGA-コントローラ - EPICS 組み込み
- ❖ ATCA,  $\mu$ TCA - 高信頼性向け (ILC 等)



# 制御用ソフトウェア EPICS

- ◆ 以前はほとんどが内製ソフトウェアの組み合わせ
  - ❖ RPC, CORBA, ...
- ◆ 徐々に共通ソフトウェアに移行してきた
  - ❖ KEK では 1994 年から “EPICS” と呼ばれる国際共同開発のソフトウェアへ
    - ❏ BSD-like な Open-source、多数の研究所が採用
    - ❏ SCADA や Labview などとほぼ同等またはそれ以上の機能
    - ❏ 他に CORBA を基本としたものなどもある
  - ❖ 当初は中間層と全体制御の間で EPICS を利用していた
  - ❖ 現在は小型コントローラにも内蔵するようになってきている
    - ❏ 最近 ITER (プラズマ核融合) も採用を決める
- ◆ 上位ソフトウェアはスクリプト言語で書かれるものも多い
  - ❖ 粒子加速器の物理の記述が行えて Mathematica 文法に近い “SAD” というソフトウェアが多用される
  - ❖ 他に Python や Perl、Tcl など
- ◆ 下位ソフトウェアは C++ や C が多い

# IP ネットワーク

## ◆セキュリティ

- ❖ 1990 年頃 IP ネットワークの導入を決めた時点から、一般 IP ネットワークと同じセキュリティのリスクを持ち込んでしまった
  - ❏ もちろん当初はリスクの大きさの認識は無かった
  - ❏ 一般的でないネットワークを使用した方が人間の (放射線) 安全に強いだろうという議論はあった

## ◆保護対策

- ❖ 一般 IP ネットワークと同じ方法が取れる部分も多い
- ❖ 教育も一般研究用 IP ネットワーク向けに教育を受けているはず
- ❖ 制御向けの仕事はオフィス向けの仕事と異なることを認識してもらおう啓蒙
  - ❏ 機構内研究用ネットワーク及びインターネット接続のセキュリティ維持は、機構内計算科学センタ部門に依存
  - ❏ 制御用ネットワーク及び機構内研究用ネットワーク接続については制御部門の担当

# セキュリティに関連した特性 (1)

## ◆ KEKB 加速器は 100 人規模のグループ

- ❖ 頻繁にソフトウェアを変更するのは 20 人程度
  - ❏ 少なくはないが、管理できる範囲か
  - ❏ CERN/LHC などでは数千人規模

## ◆ 常に性能向上のための変更が行われている

- ❖ 実験施設建設時に性能の保証は無い
  - ❏ 施設を作ること自体も研究対象
- ❖ 安全性は運転制御ソフトウェアと独立に守られている
  - ❏ マシン (機器) 保護 (MPS)、研究員の保護 (PPS)、放射線防護 (Radiation Control)
- ❖ 上位ソフトウェアは毎日変わり得る
  - ❏ 毎朝の Meeting で提案される新しいアルゴリズムが午前中には試されることも多い
  - ❏ 1000 程度のアプリケーションソフトウェアが維持されている
- ❖ ハードウェアも保守機会に (例えば月 2 回) 変更になることがある
- ❖ ドキュメントは (KEKB の場合) 追いついていない、一部は研究者の頭の中

# セキュリティに関連した特性 (2)

- ◆ 研究室やユーザ施設において、少なくとも運転情報の読み出しは行いたい
  - ❖ ネットワークは別なので、ゲートウェイ/ファイアウォールを経由して利用
  - ❖ 通常、情報の秘密性は低い
- ◆ 国際共同研究の必要性
  - ❖ 現在のところ研究者が飛行機で現地に向かうことが普通
  - ❖ 将来は高価な機器の有効利用のため国際アクセスの必要性が高まるか
    - ❏ 例えば KEKB の Crab 加速空洞は世界に KEKB だけ
- ◆ 加速器によってはユーザが大きく異なる
  - ❖ KEKB では数百人規模の Belle 実験グループが一つの課題に取り組む
    - ❏ 比較的セキュリティに対する教育なども行き届いている
  - ❖ Spring8 や KEK-PF のような放射光利用加速器施設では年間数千人の研究者が 1000 を超える中小の実験を行う
    - ❏ 1 日しか滞在しないユーザも多い
    - ❏ ある程度のセキュリティの脅威を前提としてネットワークを構築する必要がある
- ◆ 場合によって秘密がある
  - ❖ 放射光加速器で製薬の研究を行う場合、直接その組織のネットワークを実験装置に接続して、セキュリティを確保する場合もある
  - ❖ 実験装置も厳重な施錠可能な部屋の中



# 安全システムの独立性

## ◆安全性は独立に確保する必要がある

- ✧ 研究員の保護 (PPS - Personnel Protection System)
- ✧ 放射線管理防護 (Radiation Control)
- ✧ マシン (機器) 保護 (MPS - Machine Protection System)
- ❖ PLC と独立ネットワークから構成されることが多い
- ❖ それぞれのシステムは二重化されている場合も多い
- ❖ さらにそれぞれが相互に補完し合っている

## ◆制御システムからは読み出しのみ

- ✧ できるだけ通信路ではなく、ハードワイヤ接続とする
- ✧ または制御が行うことのできない読み出しのみの通信路
- ✧ やむを得ない場合も IP の常時接続は行わず、保守時のみ
  - ◆ Windows update など必要なものは IDS を通して行うなど細心の注意
- ❖ 制御システムは得た情報の表示、警告、記録を行う

## ◆独立管理の必要性は徐々に認識されてきた

- ✧ 以前は3つの安全系の独立性が低く、混同されることもあった
- ✧ 少なくとも担当責任者を別にしている
- ✧ 人間を守ることが最優先

# EPICS のセキュリティ

## ◆ アクセス制限

- ❖ 資源名、資源グループ、相手計算機、相手ユーザ名、読み出し・書き込みの組み合わせによるルール
  - ◆ PLC にも同様の制限を課すことができるものがある
- ❖ プロトコル・ライブラリによる制限
  - ☐ 自分でライブラリを改変することはできてしまう…
- ❖ 動的にも変更可能
- ❖ 当面はあまり不満は無い

## ◆ 暗号化等は現在は無い

- ❖ SSL (または最近 ICE) で包もうという計画はある
  - ☐ 何年も前から原理的困難はない、利用者を待っている
    - ◆ UDP 部分は TCP に載せる
- ❖ 国際共同研究との関連から重要になる

## ◆ 危険性

- ❖ Root 特権や悪意を持つと運転を止めることはできる
- ❖ 安全は別に担保されているので、危険は無い、ということが前提

# IPブロードキャスト

## ◆名前解決に利用されることがある

### ❖EPICSも資源名の解決にブロードキャストを使用

- ❏研究所によっては名前のサーバを用意している
- ❏ユニキャストを使用することもできる

## ◆ブロードキャストと弱いIP機器

### ❖資源名を誤ったり、プログラムが約束に従わないと多量のブロードキャストを発生することになる

### ❖普通はハードウェア (NIC) で止められないので、IPスタック (ソフトウェア) に負荷がかかり、機能が停止する機器もある

- ❏例えば有名メーカーのスイッチの監視機能が、ブロードキャスト千万パケット程度で停止

## ◆以前はそのような弱い機器が多かった

### ❖現在でも生き残っているものもある

### ❖Ethernetにループを作れば簡単に停止させることができる

### ❖スイッチでのブロードキャスト頻度制限が少し有効

## ◆現在は改善しているが、名前のサーバも用意することを考えている

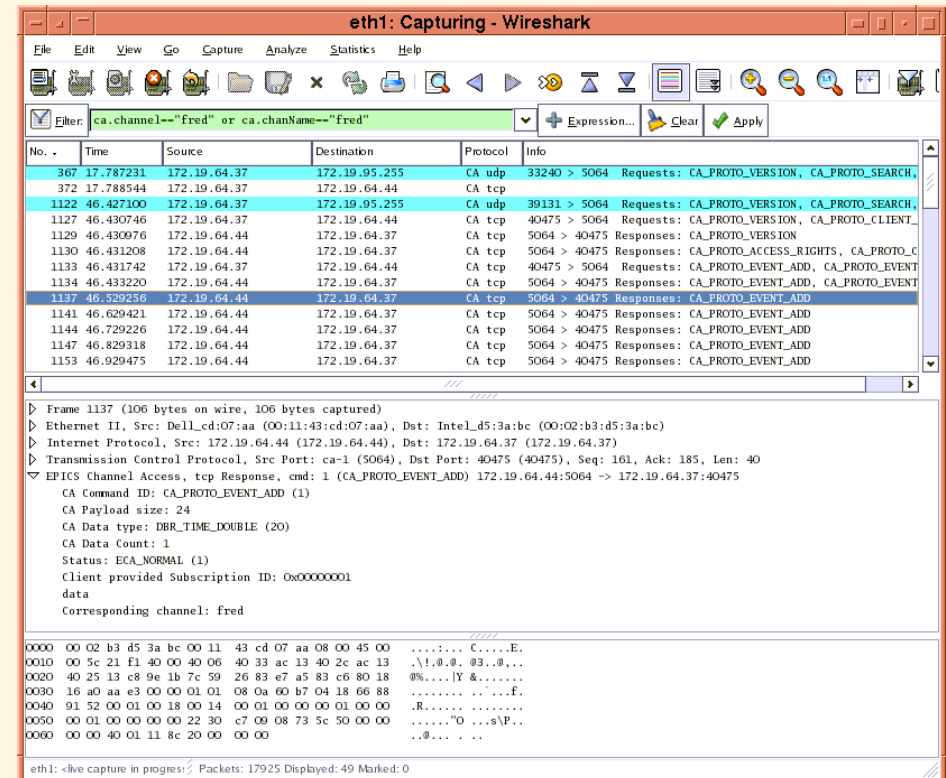
# プロトコル解析ツール

## ◆ EPICS のチャンネル・アクセス・プロトコル

- ❖ 実時間性を重視した制御プロトコル
- ❖ 比較的簡易でいくつか試験ツールも用意されている
- ❖ しかし、障害の早期発見のためにはプロトコル解析ツールが必要

## ◆ WireShark (Ethereal) のプラグインを開発

- ❖ スロベニア、米国、KEK の共同開発
- ❖ さまざまなフィルタを使用可能
  - ❏ 28 の全てのコマンドを認識
  - ❏ 数十の全てのフィールドを認識
- ❖ プロトコル・エラーを探すことで、セキュリティ対策となり得る



eth1: Capturing - Wireshark

Filter: ca.channel=="fred" or ca.chanName=="fred"

No.	Time	Source	Destination	Protocol	Info
367	17.787231	172.19.64.37	172.19.95.255	CA udp	33240 > 5064 Requests: CA_PROTO_VERSION, CA_PROTO_SEARCH,
372	17.788544	172.19.64.37	172.19.64.44	CA tcp	
1122	46.427100	172.19.64.37	172.19.95.255	CA udp	39131 > 5064 Requests: CA_PROTO_VERSION, CA_PROTO_SEARCH,
1127	46.430746	172.19.64.37	172.19.64.44	CA tcp	40475 > 5064 Requests: CA_PROTO_VERSION, CA_PROTO_CLIENT,
1129	46.430976	172.19.64.44	172.19.64.37	CA tcp	5064 > 40475 Responses: CA_PROTO_ACCESS_RIGHTS, CA_PROTO_C,
1130	46.431208	172.19.64.44	172.19.64.37	CA tcp	5064 > 40475 Requests: CA_PROTO_EVENT_ADD, CA_PROTO_EVENT
1133	46.431742	172.19.64.37	172.19.64.44	CA tcp	40475 > 5064 Requests: CA_PROTO_EVENT_ADD, CA_PROTO_EVENT
1134	46.433220	172.19.64.44	172.19.64.37	CA tcp	5064 > 40475 Responses: CA_PROTO_EVENT_ADD
1137	46.520250	172.19.64.44	172.19.64.37	CA tcp	5064 > 40475 Responses: CA_PROTO_EVENT_ADD
1141	46.629421	172.19.64.44	172.19.64.37	CA tcp	5064 > 40475 Responses: CA_PROTO_EVENT_ADD
1144	46.729226	172.19.64.44	172.19.64.37	CA tcp	5064 > 40475 Responses: CA_PROTO_EVENT_ADD
1147	46.829318	172.19.64.44	172.19.64.37	CA tcp	5064 > 40475 Responses: CA_PROTO_EVENT_ADD
1153	46.929475	172.19.64.44	172.19.64.37	CA tcp	5064 > 40475 Responses: CA_PROTO_EVENT_ADD

Frame 1137 (106 bytes on wire, 106 bytes captured)

Ethernet II, Src: Dell\_cd:07:aa (00:11:43:cd:07:aa), Dst: Intel\_d5:3a:bc (00:02:b3:d5:3a:bc)

Internet Protocol, Src: 172.19.64.44 (172.19.64.44), Dst: 172.19.64.37 (172.19.64.37)

Transmission Control Protocol, Src Port: ca-1 (5064), Dst Port: 40475 (40475), Seq: 161, Ack: 185, Len: 40

EPICS Channel Access, tcp Response, cmd: 1 (CA\_PROTO\_EVENT\_ADD) 172.19.64.44:5064 -> 172.19.64.37:40475

- CA Command ID: CA\_PROTO\_EVENT\_ADD (1)
- CA Payload size: 24
- CA Data type: DBR\_TIME\_DOUBLE (20)
- CA Data Count: 1
- Status: ECA\_NORMAL (1)
- Client provided Subscription ID: 0x00000001
- data
- Corresponding channel: fred

```
0000 00 02 b3 d5 3a bc 00 11 43 cd 07 aa 08 00 45 00 .....C.....E.
0010 00 5c 21 f1 40 00 40 06 40 33 ac 13 40 2c ac 13 ..\!.\0.\03.\0...
0020 40 25 13 c8 9e 1b 7c 59 26 83 e7 a5 83 c6 80 18 @%...|W&.....
0030 16 a0 aa e3 00 00 01 01 08 0a 60 b7 04 18 66 88 .....F.....
0040 01 52 00 01 00 18 00 14 00 01 00 00 00 01 00 00 .R.....
0050 00 01 00 00 00 22 30 c7 09 08 73 5c 50 00 00 .....O...sVP..
0060 00 00 40 01 11 8c 20 00 00 00 .....@.....
```

# 試験の重要性

## ◆さまざまな試験が有効な場合がある

- ❖新しい機器を導入する場合に行っている
- ❖ブロードキャスト
  - ❏インテリジェントでないスイッチをループさせてワイヤスピードのブロードキャストパケット列を作って負荷をかける
- ❖さまざまな長さのパケットでポートスキャンを行う
- ❖正しいパケットを数日間送り続け、応答が不安定にならないことを確認する
  - ❏応答時間のヒストグラムを作り、応答間隔に異常が無いか確認
- ❖などなど

## ◆標準的な試験手順を作成しようとする努力もなされている

- ❖“Cyber Security tools” in “Control Systems” は Internet 上で検索すると数十万のヒットがある

# 制御システムの中の Windows

## ◆もはや Windows も制御に参加している

- ❖ 通常の使い方では停止しなくなった、IP スタック等も意外と速い
  - ☞ 数年前まで使い物にならないと思っていたが…
- ❖ さまざまな電子測定器が Windows を内蔵している
  - ☞ 現在は主に Windows XP、EPICS も動作し、無駄なトラフィックを減らせる

## ◆ところが

- ❖ 速度の低下が問題になる場合にウィルス防護が困難
  - ☞ 実際かなり速度が低下する
- ❖ ベンダが Windows Update を行ったら性能を保証しないなどと言う

## ◆現在の対策

- ❖ 同じブロードキャスト・ドメインにウィルス検知ソフトウェアを実装した同様の Windows 計算機を置いておき監視する
- ❖ 測定用には Windows を使用するが、制御には使用しない
- ❖ 通常のセキュリティ規則にできるだけ従う
- ❖ 運用中常時のウィルス防護ではなく、保守時のウィルススキャン

# 内製のネットワーク機器

## ◆さまざまな試験

- ❖ブロードキャスト負荷
- ❖さまざまな長さ (100バイト毎) のパケットによるポートスキャン
- ❖通常と異なる間接契約でソースコードを入手できず

## ◆数年後、多数の機器が同時に停止する現象が 2 回発生

- ❖再度試験を行い、たまたま、ある長さのパケットをあるポートに送ると高い確率で機器が停止することを発見
- ❖ブロードキャストを使用すると同時に多数の機器を停止させられる
- ❖...

## ◆良い教訓になった

- ❖ソースコード
- ❖ブロードキャストドメインの縮小

# 情報の提供

- ◆ 情報が少ないと不必要な情報を取りに行く
  - ❖ その結果誤りを起こす可能性が高まる
  - ❖ 積極的な情報の提供が重要
- ◆ 例えば電子ログブック
  - ❖ 実験運転情報をできるだけ電子化し、Web で提供
    - ✧ 手入力、自動入力を合わせて1日1000件程度
      - ◆ あまり多いと読めない
- ◆ Web ブラウザへの情報供給
  - ❖ クライアント側にインテリジェンスを持たせない
    - ✧ 特に必要ない限り、書き込み (制御) 可能な領域に入ってこさせない



# インターネット経由の接続

- ◆ 制御室で行えることを海外から行いたいという希望
  - ❖ 研究室からゲートウェイ経由で行えること以上 (?)
- ◆ 国際共同研究の必要性
  - ❖ 現在のところ研究者が飛行機で現地に向かうことが普通
  - ❖ 一部の研究所で少なくとも診断目的で接続がされるようになっている
    - ❏ LHC の CMS グループは機器や情報の解析監視診断当番を海外から行う
  - ❖ 将来は高価な機器の有効利用のためインターネット経由の制御の必要性が高まるかも…
    - ❏ 将来の ILC などに向けて議論が続いている
  - ❖ おそらく航空運賃の方が安いのが共同費用分担の象徴？
  - ❖ ある意味このような要求から WWW が CERN で生まれた
- ◆ 技術的には大きな困難は無い？
  - ❏ Video 会議設備、SSH 経由の端末接続など
  - ❏ アジア、ヨーロッパ、アメリカで当番を分担できる
  - ❏ ドキュメント、図面、電子ログ等、詳細情報の翻訳が必要
  - ❏ 安全性の確保により多くの人員が必要となる
  - ❏ 国によって安全関連の法律が異なる



## まとめ

- ◆ 物理実験装置の運転制御では日々の性能向上、実験成果が優先されてしまう
- ◆ 人的な安全性は独立に確保を行う
- ◆ 将来さらに大きな実験装置が国際協力により計画されており、攻撃の対象になりやすいので、セキュリティの議論は重要になっている



**Thank you**