一般口演
一般口演12
ネットワーク・システム開発
2017年11月21日(火) 16:15 〜 17:45 B会場 (12F 会議室1202)

[2-B-3-OP12-3] 医療データを高性能計算機システムで利用するためのダイナミックセキュアなステージングシステム

伊達 進[1], 吉川 隆士[1], 野崎 一徳[2], 渡場 康弘[1], 木戸 善之[1], Lee Chonho[1], 下條 真司[1] （1.大阪大学サイバーメディアセンター, 2.大阪大学歯学部付属病院）

近年、あらゆる科学分野やデータ解析分野において、高性能計算機の必要性と重要性が急速に増大しています。しかしながら、セキュリティに敏感なデータを扱う医学者、歯科学者にとっては、データセキュリティの問題から計算機センターの高性能計算機を使用することは困難です。医学、歯学のデータの多くは個人情報に深く関わっているため、それぞれの病院からこれらのデータを計算機センターに持ち出すことが出来ないからです。そこで、我々はこのような秘匿性の高いデータをよりセキュアに計算機センターへ移動して高性能計算機を用いたデータ解析を実現するためのセキュアステージングシステムを提案します。
高性能計算機システムでは、複数のユーザが投入したそれぞれの計算処理（ジョブ）に対し、ジョブ管理スケジューラが計算機リソースの状態や実行時間を考慮することで、計算機センター全体としてのジョブ群の実行がスムーズに流れるように管理しています。ジョブで処理するデータ量が大きい場合、あらかじめ高性能計算機のストレージにデータを移行して速やかにジョブを実行する準備（ステージング）を行います。我々は、このステージングに着目し、秘匿性の高いデータの持ち出しから計算処理の実行までを物理的に他のユーザの実行環境から分離した状態で行えるようにしました。
そのための技術の一つは、ハードウェア分散仮想化技術 ExpEtherによる柔軟な計算機環境構築です。もう一つは、ジョブ管理スケジューラと SDNの連携による計算処理実行直前のデータ移動とデータ移動後のネットワークの分離です。
これらの技術により、従来の VPNを使ったネットワーク分離や暗号化を用いたデータ秘匿をさらに強化することができます。以上により、医学や歯学のデータを高性能計算機のストレージに安全に移動させて計算処理の実行を行うダイナミックでセキュアなステージングシステムを実現しました。

医療データを高性能計算機システムで利用するための ダイナミック・セキュア・ステージングシステム

伊達　進[*1]、吉川　隆士[*1]、野崎　一徳[*2]、渡場　康弘[*3]、
木戸　善之[*1]、Lee Chonho[*1]，下條　真司[*1]

*1 大阪大学サイバーメディアセンター、*2 大阪大学歯学部付属病院

Dynamic and Secure Staging for Medical Data Being Processed in The Computer Center

Susumu Date[*1], Takashi Yoshikawa[*1], Kazunori Nozaki[*2], Yasuhiro Watashiba[*1],
Yoshiyuki Kido[*1], Chonho Lee[*1], Sinji Shimojo[*1]

*1 Cybermedia Center, Osaka University, *2 Dental Hospital, Osaka University

Dynamic and secure staging mechanism is developed to process medical data by using high performance computers in the computer center. The system is composed of five secure partitioning technologies including time-based partitioning by a job scheduler, memory regional-partitioning by container, hardware-level attach/detach by PCI Express, encryption key pairing with container and hardware device, and SDN-based network connection control. With combination of those technologies, this system provides various enhanced security level appropriate for the medical data concealment of each data to realize approval of medical data usage out of the hospital location.

Keywords: Data Security, High Performance Data Analytics, SDN, JOB Scheduler, Container

1. 緒論

近年、あらゆる科学分野やデータ解析分野において、高性能計算機の必要性と重要性が急速に増大している。しかしながら、セキュリティに敏感なデータを扱う医学研究者、歯学研究者にとっては、データセキュリティの問題があり、計算機センターの高性能計算機を使用することは困難である。それは、医学、歯学のデータの多くは、個人情報に深く関わっているため、それぞれの病院からこれらのデータを計算機センターに持ち出すことが出来ないからである。そこで、我々はこのような秘匿性の高いデータを、よりセキュアに計算機センターへ移動して高性能計算機を用いたデータ解析を実現するためのセキュアステージングシステムを提案する。

2. 目的

医学、歯学のデータの多くは、個人情報に深く関わっているため、それぞれの病院からこれらのデータを計算機センターに持ち出すことが難しい。医療機関では、多くの場合、検査データ、カルテ、事務データを含めて、基本的に一切のデータが持ち出し禁止となっている。また、どうしても持ち出しが必要なケースが生じた場合には、患者の個人特定ができる可能性の低いデータや、匿名化の加工を行ったデータについて、患者の同意を得る、データ使用者を医師に限る、などの条件を付加したうえで、ケースごとに個別に倫理委員会で審議を行って、持ち出し承認を得る必要がある。

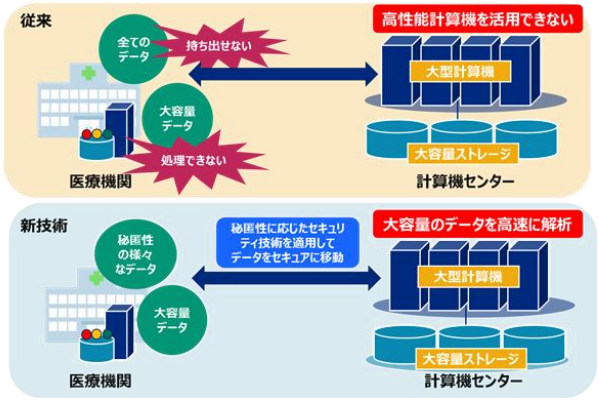

図1　医療系データの計算機センターでの処理

すなわち、図1に示す通り、今日、AI を含むデータ解析や、高性能計算機が急激に発展し、これらの医療データについても、大量、かつ高速に処理できる計算機センターを利用できることが望ましいが、持ち出し禁止という壁があり、実現が困難である。

これに対し、我々は、「医療データは持ち出し禁止」と言っても、実際にはその中に含まれるデータの秘匿度は多種多様であり、秘匿度に応じて、適切なセキュリティ技術を適用することで、計算機センターでの利用が可能になるデータが多く存在すると考えた。

一般にセキュア度を高める IT 技術としては、データ自体を加工する暗号化、匿名化や、データを送る経路をセキュアにする VPN などがある。

我々は、データ持ち出しの利用目的を、計算機センターでのデータ利用だけにフォーカスすると同時に、多重防御の考え方により、従来のセキュリティ技術に、新たに複数の仕組みを加えることでセキュア度を段階的に高める方式を検討した。

これにより、データ秘匿度と、それに応じたて適切なセキュア技術の組合せを用いることで、医療データを用いた高性能データ解析のうちの多くのケースで、計算機センターの高性能計算機を用いることを可能にすると同時に、ケースバイケースに倫理審議するだけでなく、ある程度、審議指針をメニュー化し簡便化きると考えている。

本論文では、前記の通り、医療データを、よりセキュアに計算機センターへ移動して高性能計算機を用いたデータ解析を実現するためのセキュアステージングシステムを提案する。

3. 方法

3.1 システムの概念

基本的な概念はセキュアな分離である。

本研究では計算機センターでの利用にフォーカスする。計算機センターでの計算処理は、JOBというくくりでスケジューラに投入される。スケジューラは複数のユーザから、複数のJOBを受け取り、ポリシーベースなどで優先順位をつけて、計算機リソースが空いたところへと JOB を投入して計算処理を実行していく。JOB が扱うデータが大きい場合などは、事前にデータ配置など、計算機リソースが空いた時に効率よく JOB を処理できるように準備を行う必要がある。これをステージインと呼ぶ。、逆に計算処理で発生した大量のデータなどをストレージへ退避させ次の処理に備えることをステージアウトと呼ぶ。

我々はこのステージングの概念を拡張して、計算処理を行う時だけ、計算処理を行う計算機を構成し、その時だけデータアクセスを可能にすることで、データの取り扱いを時間的、物理的、ネットワーク的に分離できると考えた。

これを実現するために、JOB スケジューラとネットワーク構成管理、並びに計算機構成管理などを連携して管理することが可能なダイナミック・セキュア・ステージングシステムを開発した。

3.2 構成要素

セキュアステージングシステムは、主に図2に示す通り、次に述べる五つの方式を用いて、それぞれにセキュアな分離を実現する。

セキュリティアタックは、アプリケーションや OS の脆弱性をつくなどのソフトウェアレイヤでの仕組みを用い、ネットワークを通して行われる。すなわち、攻撃を行う手段のほとんどが IP レイヤより上の層で行われる。そこで IP パケットより下のレイヤで、セキュアな分離を行う仕組みを導入することにより、IP Unreachable な、攻撃をされにくい世界で、セキュア度を向上することができると考えた。

この考えに基づいて、計算機の低位レイヤ、並びにネットワークにおける、以下のセキュアな分離方式を提案する。

3.2.1 スケジューラによる時間的分離

3.1 章に述べた通りスケジューラはもともと、異なるユーザの異なる JOB を時間的に分離する仕組みである。したがって、スケジューラに連携して、後にのべる仕組みを用いて、計算処理を実行する時だけ、データに到達することを可能にしたり、計算処理が実行できるようにしたりする事で、セキュア分離が実現される。[1)]

3.2.2 コンテナによるメモリ分離

計算処理を実行するソフトウェアプラットフォームをコンテナ上に実装することで、計算処理を行う時だけ、そのプラットフォームがメモリ上に用意され、処理の終了後にコンテナを消去することで、データも含めてメモリ上から消される。すなわちスケジューラに連携してコンテナを用いることで、ある種のメモリ分割が実現する。

3.2.3 データとコンテナの鍵分離

コンテナと、データストレージデバイスの間に秘密鍵を用いると、データストレージが鍵交換を行ったコンテナからしか読書きのアクセスができなくなる。次に述べるインターコネクションによるデバイスのつけ外しと連携すると、とあるストレージデバイスとコンテナの組が、ダイナミックに再構成可能になるため、秘密鍵を用いたハードウェアデバイスを単位としたアクセス制御が実現する。

3.2.4 PCI Express(PCIe)でのデバイス分離

ストレージデバイスやネットワークインターフェースカード(NIC)、SAN のホストバスアダプタ(HBA)などいわゆる IO デバイスは、PCI Express で接続されている。PCI Express は Hot Plug 機能を有しており、稼働中にデバイスの組込み・分離が可能である。本研究では PCI Express を拡張した ExpEther を用いる。[2)] ExpEther は PIC Express スイッチを Ethernet 上に仮想的に分散する PCI Express over Ethernet であり、管理ソフトエア、ExpEther Mnager により、リモートから Software Defined で PCI デバイスレベルの計算機ハードウェア再構成を実現する。すなわち、IP Unreachable な世界で、ハードウェアの再構成が行える。これと JOB スケジューラを連動することで、とある処理を行う時にだけ、データを保持しているストレージデバイスをハードウェア的に組み込んで、処理が終わると同時に切り離すことができる。逆に、データをネットワーク経由でロードする時だけネットワークカードを組込み、その後は切り離すことで、IP パケットだけでなく、ハードウェアレベルで一切のネットワーク的な reachability を無くす事ができる。

3.2.5 SDN によるネットワーク分離

SDN はネットワークのパスやアクセス制御などが、IP レイヤより下で実行できる。この制御はコントローラソフトエアで行える Software Defined な仕組みなので、JOB スケジューラと連携して、JOB を実行するためのデータ移動時だけネットワークを接続することで、ネットワークの分離が実現する。さらに3．2．4章で述べた ExpEther の Ethernet パスの接続・分離の制御も行うことができる。

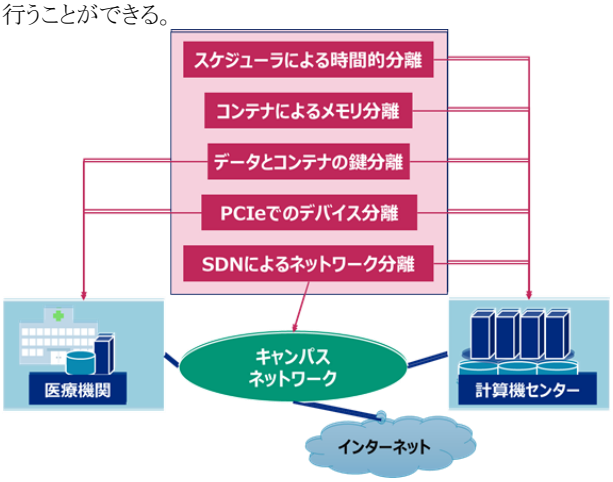

図2 システム概要と主要な機能

4. 実装と結果

4.1 実装

図3に示す JOB リソースマネージャーを実装した。そのうち3.2.4 に述べたExpEtherによるリソース再構成とJOBスケジューラとの連動部分について、実際に計算機ノード2台からなる最小構成のシステムを構築して、JOBの投入にあわせてリソースが再構成される事を確認した。[3)]

またトレードオフとして懸念される計算処理能力について、実際に 2 ノードの上にApach Spark 分散処理環境を構築して Logistic Regression の計算処理を行った。処理ノードが1

台と 2 台で性能を比較し、ノード数による処理能力の向上を確認した。

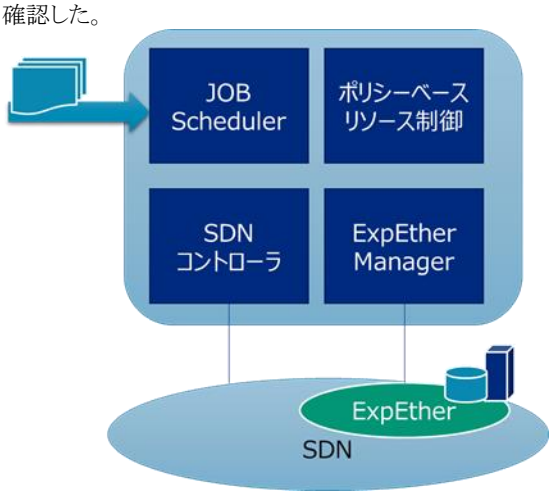

図3　JOB リソースマネージャの構成

4.2 ステージングシナリオ

このシステムを用いてダイナミックにセキュアなステージングを実行するシナリオ例を二つ、図4に示す。

シナリオ1は ExpEther を用いてデータの入ったストレージディスクのつけ外しの制御を行うものである。その特徴は、データの入ったストレージディスク、並びにデータは物理的、及び OS ソフトウェア的には医療機関の中から移動しないことである。計算処理を実行する直前に SDN で ExpEther のパスを医療機関側と接続し、HotPlug によりストレージデバイスを医療機関の計算機から論理的に取り外し、計算機センター側の計算機に論理的に接続する。PCI Express のレイヤで HotPlug されるため、計算機センター側の OS ソフトウェアは、このストレージデバイスが自身の内部にあるローカルディスクとして認識し、もともとの計算処理ソフトウェアがそのまま実行される。計算処理実行後は、データをストレージに格納し HotPlug で切離すと同時に、コンテナごとメモリを消去する。これにより、事実上、データは物理的には医療機関から出ていないのとほぼ等しい状態となる。ただしこの場合、計算実行中にストレージアクセスが発生すると、医療機関と計算機センターを介してデータアクセスが起きるためその遅延が100マイクロ秒のオーダーで起き、性能が若干落ちることになる。

	EE-DISK	EE-NIC	SDN-EE	SDC-IP	Scheduler	コンテナ
シナリオ1	✓		✓		✓	✓
シナリオ2		✓		✓	✓	✓

シナリオ1
1. NICを組み込む
2. パスを繋ぐ
3. 歯学部DISKを計算機センターへ接続
4. アプリコンテナOPEN
5. JOB投入
6. 処理
7. 歯学部のDISKへ書き込む
8. 歯学部のDISKを切り離し
9. パスを切り離す
10. NICを切り離す
11. コンテナごとメモリ消去

シナリオ2
1. パスを繋ぐ
2. 歯学部DISKのデータを計算機センターのDISKにコピー
3. アプリコンテナOPEN
4. JOB投入
5. 処理
6. 計算機センターDISKのデータを歯学部にDISKにコピー
7. パスを切り離す
8. コンテナごとメモリ消去

図4　ダイナミック・セキュア・ステージングのシナリオ

一方、シナリオ2は医療機関側から計算機センターへデータをコピーする。コピーする際に SDN によるパスの制御を行うと同時に、外界へのネットワークのインターフェースデバイスを ExpEther のしくみを用いてハードウェアレイヤで分離することで、外界からの分離度を増強することができる。

4. 考察

3章で述べた5つの方式はそれぞれ、その用い方も含めてセキュア分離度が異なる。これを表1に整理した。分離度は、定性的におおまかに3段階に評価した。これらを組み合わせたステージングシナリオにおいて、システムとしてのセキュア度がどれくらいになるのか、今後、定性的・定量的に評価していくことが重要である。それにより、5つの方式の組合せそれぞれのセキュア分離度と実現性能をメニュー化して、計算処理を実行したいケースに最適な組合せが、自動的に選択されるような、スマートな仕組みを実現していく。

表1　各方式の特徴とセキュア度の推定

方式	概要	分離度	
Scheduler	時間的に分離	△	他の方式と組合せ
コンテナ	メモリごと消去	△	メモリごと消去
EE DISK	ExpEtherでDISKを脱着	◎	ケーブルを抜くのと同じ
EE NIC	ExpEtherでNWへのNICを脱着	○	ケーブルを抜くのと同じ
SDN EE	ネットワークパスを分離	○	IPの下の層で分離
SDN IP	ネットワークパスを分離	○	IPの下の層で分離
鍵分離	コンテナ・デバイスの間で鍵交換	○	他の方式と組合せ

5. 結論

医療データを計算機センターの高性能計算機で処理を実行すること目的に、データの計算処理を実行する時だけ、計算機構成やネットワーク構成を変更してデータアクセス、処理が可能になるようなシステムと、それを用いた、ダイナミックなセキュアステージングのシナリオを検討した。

これにより、多くの場合一括して持ち出し不可とされてきたデータのうち、いくつかのデータについては、データの秘匿度にあわせて最適なセキュア技術を組合せて、セキュアなデータ移動を行い、計算機センタの計算機で処理を可能とすることができるスキームを提案した。

参考文献

1)渡場康弘, 木戸善之, 伊達進, 阿部洋丈, “計算資源とネットワーク資源を考慮した割当ポリシを配備可能とするジョブ管理フレームワーク, ” 電子情報通信学会論文誌 2014, vol.197-D, no.6, pp.1082-1093.

2) Suzuki J, Hidaka Y, Higuchi J, Yoshikawa T et. al, ExpressEther-Ethernet-Based Virtualization Technology for Reconfigurable Hardware Platform, Proceesings of the 14th Symposium on High-Performance Interconnects (HOTI) 2006, pp.45-51

3) Misawa A, Date S, Takahashi K, Shimojo S, et.al. Highly Reconfigurable Computing Platform for High Performance Computing Infrastructure as a Service: Hi-IaaS, 7th International Conference on Cloud Computing and Services Science 2017