

9. 地対地通信と情報共有手法の実装に関する考察

機上等技術領域 ※金田 直樹、塩見 格一
通信・航法・監視領域 板野 賢

1. はじめに

航空機に搭載される、安全に関わるシステムは二重、三重構成を取ることにより高い可用性とフェールセーフ性を実現している。同様に、航空交通管制のための地上システムには、安全のために高い可用性とフェールセーフ性が求められる。このようなシステムとしては、単一の巨大システムより、複数の部分システムが協調して動作することができ、かつ、各々の部分システムが単独でも動作可能なシステムであることが望ましい。なぜなら、単一の巨大なシステムは、しばしば1箇所の障害がシステム全体に波及し、システム全体をダウンさせてしまうことがあり得るからである。このような、システム全体に影響を及ぼす可能性のある点は単一障害点 (single point of failure) と呼ばれる。単一障害点は冗長構成により除去することができる。例えば、航空路監視レーダの二重覆域化は各々のレーダが単独でも動作可能であることから、監視システム全体に可用性向上とフェールセーフ性をもたらしている。同様に、多数設置された VOR/DME や VORTAC も航法システム全体の可用性を向上させ、かつフェールセーフ性をもたらしている。

一方、我が国の航空交通管制に係る情報共有システムの冗長性はあまり大きくない。具体的には、航空管制や運航管理に必要な情報の共有は2地点間の回線を末端まで張り巡らせ、中央の大型コンピュータに情報を集約し、集約した情報を再度配信することにより情報の共有を行っている。例えば飛行情報管理システム (FDMS) は、管制情報処理部 (FDPS)、運航情報処理部 (FIMS) とともに、大型コンピュータに全国の官署等から送られてきた情報を集約し、処理し、配信するシステムとなっている。航空路レーダー情報処理システム (RDP) も同様に、システムの構造として多くのレーダからの情報を集約・処理し、各管制卓に情報の表示 (配信) を行っている。

このようなシステムはスター型と呼ばれ、中央に

情報を集約するため効率が良く、配信情報に一貫性があり、相互矛盾がないという利点がある。しかし、中央の情報集配信装置はシステム全体に対する単一障害点となり得るといった問題点がある。この問題はシステムが統合され巨大になるほど顕著になる。単一障害点を除去するには冗長構成が有効であるが、情報を集約する場所、すなわちデータベースの二重化はハードウェア障害に対する冗長構成であり、ソフトウェア障害に対する二重化とはならない。なぜなら、冗長化データベース (レプリケーション) ソフトウェアは、ひとつのデータベースを複数の場所に保持するものであり、ハードウェアが冗長構成であってもソフトウェアは同一であるため、ソフトウェアを原因とする障害が発生した場合は全てのシステムに影響が及ぶ。すなわち単一障害点が存在する。

このような問題は、情報集約装置をなくすこと、すなわち分散型情報共有システムによって解決可能と考えられる。しかしながら分散型情報共有システムには集中型情報共有システムにない、いくつかの問題もある。本発表ではそれらの諸問題について検討する。

2. 情報共有手法の分析

2.1 一般論

1対1の情報共有は通常の通信として考えられるため、まずは、Aさん、Bさん、Cさんの3者による情報共有について考える。情報理論では慣習的に頭文字からAさんのことをAlice、BさんのことをBob、CさんのことをCharlieと呼ぶことが多いので、ここでもその流儀に従うことにする。Alice、Bob、及びCharlieによる情報共有の最も簡単な形はAliceとBob、BobとCharlie、CharlieとAliceの間にそれぞれ通信路を用意し、全員が自分の持つ情報全てを通信路に送出することである。この方法では明らかに、 n 人で情報を共有するために、 $n(n-1)/2$ 本の通信路が必要で

あり、効率的とは言えない。情報共有を効率的に行うことが可能かどうかについての理論は理論計算機科学における計算量理論の一分野である、通信計算量理論として知られている。情報量がビットで測定できることから、3者での情報共有は Alice, Bob, 及び Charlie が共同でビットを決めることであると言える。通信計算量理論では、共有すべき Alice, Bob, 及び Charlie の持つビット全てを送る必要がある場合が存在することが知られている。しかしながら、通信複雑性の教えるところによると、Alice, Bob, 及び Charlie の全員が観測可能なビットが存在する「黒板モデル」は、1対1の通信路しかない場合に比べ、真に通信量を削減可能であることが知られている。これは1対1の通信網を多数引くことによる情報共有が非効率である場合があることを意味し、効率の良い情報共有の実現には、全員が参照可能な何かを必要とする。集中型情報共有システムはこの事実に基づいて構想された。なお、通信計算量について興味のある読者は、通信計算量に関する標準的な教科書 [1] を参照されたい。

2.2 現状の航空用情報共有システム

航空用システムが他のシステムと異なることは、第一安全に貢献するシステムが求められることである。安全の定義は「危害または損傷・損害を受ける恐れのないこと」であり、安全の実現のためにシステムには信頼性、可用性、連続性、保守性、管理性、完全性、検証可能性、弾力性、及び無矛盾性の確保等が要請される。

以上のような前提を踏まえた、現状の（計算機によらない方法も含め）航空用情報共有システムは以下のようなものがあると考えられる。

2.2.1 情報周知システム

情報共有システムの目的の一つとして、周知を行うためのシステムがある。この方法では、単独の管理責任を持つ人または組織が情報を集約し、各所に周知を行う。現在実装されている情報共有システムの目的の多くは周知である。計算機によらない情報共有システムも含めると、AIPの配布、NOTAMの発出、気象情報の参照(TAF/METAR、レーダ画像や天気図の配信)、ATIS、等が代表的な例である。管理責任は1箇所に集中しているため、データベースによる

運用が便利であると考えられ、実際そのようにシステムが設計されていると考えられる。

2.2.2 複数の関係者による情報の更新を行うシステム

情報共有システムには、2者以上が情報の更新を行う必要がある場合もある。CDMに必要な情報共有システムはこれに該当すると考えられる。例えば飛行(計画)情報が挙げられる。飛行(計画)情報は以下のように複数の関係者が情報を更新したい場合があることがわかる。

- 管制指示による飛行(計画)情報更新
- パイロットによる飛行(計画)情報更新
- FMSの計算結果に基づく飛行(計画)情報更新
- 運航管理者による飛行(計画)情報の更新

この場合の当事者はパイロット、運航管理者、管制官等に分散している。航空機の最終的な意思決定はパイロットが行うという意味で、各航空機に関する情報は航空機それ自身が持っているのが自然な設計であり、フライトオブジェクトはそのような思想の元に提案されたと考えられるが、ネットワーク的には各航空機が独立に情報を持つべき、という意味で分散型情報共有システムとして位置づけられると考えられる。

3. 集中型管理と分散型管理

情報共有システムとして集中型と分散型の手法があるが、本節では、集中型システムと分散型システムの利点と欠点についてそれぞれもう少し検討する。

3.1 分散型システムの利点

分散型システムは、冗長化されたフェールセーフシステムであるとも言える。これにより、単一障害点がなくなり、問題が発生した場合に影響範囲を局所にとどめることができる。世界最大の分散システムはインターネットであるといえるが、インターネットは自律システム(Autonomous System)の相互接続により構成され、また一つの自律システムは複数の部分システムに分割されており、インターネットは他のシステムで発生した障害が自システムの障害とならないように設計されていると言える。

拡張可能性も重要な長所である。システムとしての処理能力を向上させるためには、集中型システムでは中央処理装置をより大きな処理能力を持つものに更新する必要がある。しかし、分散システムでは部分システムの追加により処理容量増大に対して対応可能となる。そのため将来の処理容量増大への対応は分散型システムの方が有利である。

3.2 集中型システムの利点

分散型システムはデータの一貫性が問題となりうる。各部分システムで動作するアルゴリズムが同じでないと、部分システム間における情報の矛盾が発生してしまう。同じアルゴリズムにならない場合は例えば、複数バージョンの混在、意図的な動作変更を行う部分システムの存在などが考えられる。ただし、意図的な場合はセキュリティの問題であるためここでは考えない。異なるバージョンの混在について言えば、分散システムにおいては互換性のないプロトコルへの変更は困難を伴う。例えば、インターネットにおいて IPv4 から IPv6 への変更がなかなか進まない理由は IPv4 と IPv6 の非互換性が主な理由と考えられている。航空機搭載無線機器に後方互換性が要求されるため更新が進まない問題と本質的に似ている。

データベースの形式、すなわちデータ構造の変更が容易であることも集中型システムの利点である。分散型システムを設計する際は、データ構造がアルゴリズムを規定してしまうため、部分的なシステムの更新を繰り返した後も各システムで協調動作を実施できるように、データ構造の設計は将来必要になる要件も見据えて設計する必要がある。これは非常に難しい。

また、情報が相手に届くまでの時間、すなわちレイテンシも問題である。レイテンシの低いシステムが必要となるのは例えば航空管制通信である。管制通信では、航空機が高速で移動しており、管制間隔設定のためには通信遅延であるレイテンシを見込んで管制指示を発出する必要がある。そのため、レイテンシの低いシステムが必要とされる場合がある。集中型システムにおけるレイテンシについては中央での情報集約装置を適切に設計すれば小さくすることができるが、分散システムの多くはレイテンシが大きい。この問題点の一部を解決する方法として、分散ハッシュテーブルを利用して低レイテンシ分散型

システムが設計できると考えられる。これは将来の課題である。Chord[2, 3], CAN[4] のような分散ハッシュテーブル型 P2P システムによる管理は、分散型システムの欠点のうち他にもいくつかを補うことができる。分散ハッシュテーブルのアルゴリズムについてはいくつかの方法が提案されているが、詳細な調査が RFC 4981 として公開されているのでそちらを参照されたい [5]。

4. NNTP による分散情報共有システム

上記のような検討から、情報周知システムには中央集約型システムが適していると考えられる。典型的な実装方法としては、クライアント・サーバ方式による実装である。例えば Web サーバ + Web ブラウザのような実装形態が考えられる。しかしながら、複数の関係者による情報の更新を行うシステムにおいてクライアント・サーバ方式が適しているかは自明ではない。そこで、そのような場合に利用できる分散システムによる情報共有方式を以下提案する。

本発表では、時間的要件があまり厳しくない（1分程度でよい）情報共有システムとして、NNTP (Net News Transfer Protocol) による情報共有方式を提案する。NNTP は World Wide Web ができる前に、世界的な電子掲示板として利用されていた、NetNews の転送を行うためのプロトコルである。NNTP において、サーバ間の情報共有は分散型システム (Peer-to-Peer: P2P)、サーバから読み出しを行うクライアントとの接続はクライアント・サーバ方式として実装されている。これらが一つのプロトコルである NNTP によって実現されており、集中型かつ分散型のシステムを1種類のプロトコルで実現しているのが特徴である。サーバ間の情報共有としては、各サーバは識別子のないメッセージに識別子をつけ、隣のサーバに自分の持つメッセージをコピーし、同一の識別子を持つメッセージは捨てるという動作を行う。この単純な規則により、ネットワーク全域にメッセージが配送される。メッセージの形式は電子メールと同様である。

NNTP による NetNews の実際の運用として、組織毎にサーバが設置され、サーバ同士が P2P により通信を行うというネットワーク構成であることが多い。このようなネットワーク構成を採用した場合、どこかの組織でサーバが故障しても影響はそのサーバに

接続されるクライアントに限定され、他の組織に故障による問題は伝搬しない。また、サーバが復旧すれば、隣のサーバから自動的にメッセージが配送されてくるため、障害復旧も自動で実施される。

コピーを繰り返すことによる情報配信モデルのため、メッセージの同期が問題となる。しかし、メッセージの投稿時間を元に Expire Time を指定することができるので、複数ノード間での時刻同期が正しく行えていけば、全てのノードからある時刻に当該情報を一斉に消去することができる。一貫性の保持にとってこの性質は望ましい。なお、Effective Time / Expire Time による情報の同期を実施する方法は、AIP の配布方法である AIRAC (Aeronautical Information Regulation and Control) が全く同じ方法であることも指摘しておきたい。すなわち、メッセージのコピーによる配送と時刻による情報の同期は、航空業界では以前から行われている。

本実装提案の利点としては、十分な動作試験を積んだ既存の実装が存在することが挙げられる。クライアントとしては既存の、利用者にとってなじみ深い Mozilla Thunderbird, Microsoft Outlook Express 等が利用可能であり、またサーバとしてはオープンソースの INN 等が利用可能である。NNTP サーバの実装は複数種類存在しているためシステム全体がダウンすることもなく、INN による全世界的ネットワークが構築されていたという意味で、スケーラビリティについても申し分ない。また、NNTP は本質的に分散型電子掲示板システムであり、メッセージ形式が電子メールと類似しているため、添付ファイルを付けることができる。そのため、マルチメディア対応（画像や動画データを添付可能）や電子署名 (S/MIME) にも対応可能である。電子署名はメッセージに完全性を与えるため、メッセージ受信者が正当性を確認することに利用可能である。問題点としては、先に述べた分散型システムの問題点の殆どが当てはまることが挙げられる。

5. おわりに

今回は必要要件について述べたが、不要な要件についての検討もまた重要である。高信頼性システムはシステム全体の設計を単純にすることで高い信頼性を実現している場合が多いからである。また、必要機能のリストを並べて実装されたシステムの多くは

性能に問題を抱えることが多い。機能と性能の妥協点を何処に見いだすかは重要な設計のポイントである。長く使えるシステムの設計方針を調べると、インターネットに見られるように、Simple is the best の設計方針であることも多い。KISS: Keep It Simple, Stupid の設計方針を保つことは、将来の拡張性にとって重要であると思われる。

参考文献

- [1] Eyal Kushilevitz and Noam Nisan. *Communication Complexity*. Cambridge University Press, 1997.
- [2] Ion Stoica, Robert Morris, David Liben-Nowell, David Karger, M. Frans Kaashoek, Frank Dabek, and Hari Balakrishnan. Chord: A Scalable Peer-to-peer Lookup Service for Internet Applications. *IEEE Transactions on Networking*, Vol. 11, pp. 17–32, February 2003.
- [3] Ion Stoica, Robert Morris, David Karger, M. Frans Kaashoek, and Hari Balakrishnan. Chord: A Scalable Peer-to-peer Lookup Service for Internet Applications. In *Proceedings of the ACM SIGCOMM*, pp. 149–160. ACM Press, August 2001.
- [4] Sylvia Ratnasamy, Paul Francis, Mark Handley, Richard Karp, and Scott Schenker. A Scalable Content-Addressable Network. In *Proceedings of the ACM SIGCOMM*, pp. 161–172. ACM Press, August 2001.
- [5] J. Risson and T. Moors. Survey of Research towards Robust Peer-to-Peer Networks: Search Methods. IETF RFC4981, September 2007.
- [6] Jay Merkle (FAA). System Wide Information Management (SWIM). ENRI International Workshop, March 2009.
- [7] Vikram Prabhu and Duncan Thompson. SWIM Strawman Architecture. MITRE Technical Report, January 2007. MITRE CAASD.
- [8] A. S. Tanenbaum and M. V. Steen. 分散システム原理とパラダイム. ピアソン・エデュケーション, 2003. 水野, 宮西, 鈴木, 西山, 佐藤, 東野訳.