特集論文

無停止型サーバftServerの公衆インターネット網を用いた遠隔監視システム

渡辺和也*
冨塚　潔*
尾崎勝広*

Remote Support System via Internet for Fault-tolerant Server "ftServer"

Kazuya Watanabe, Kiyoshi Tomizuka, Katsuhiro Ozaki

要　旨

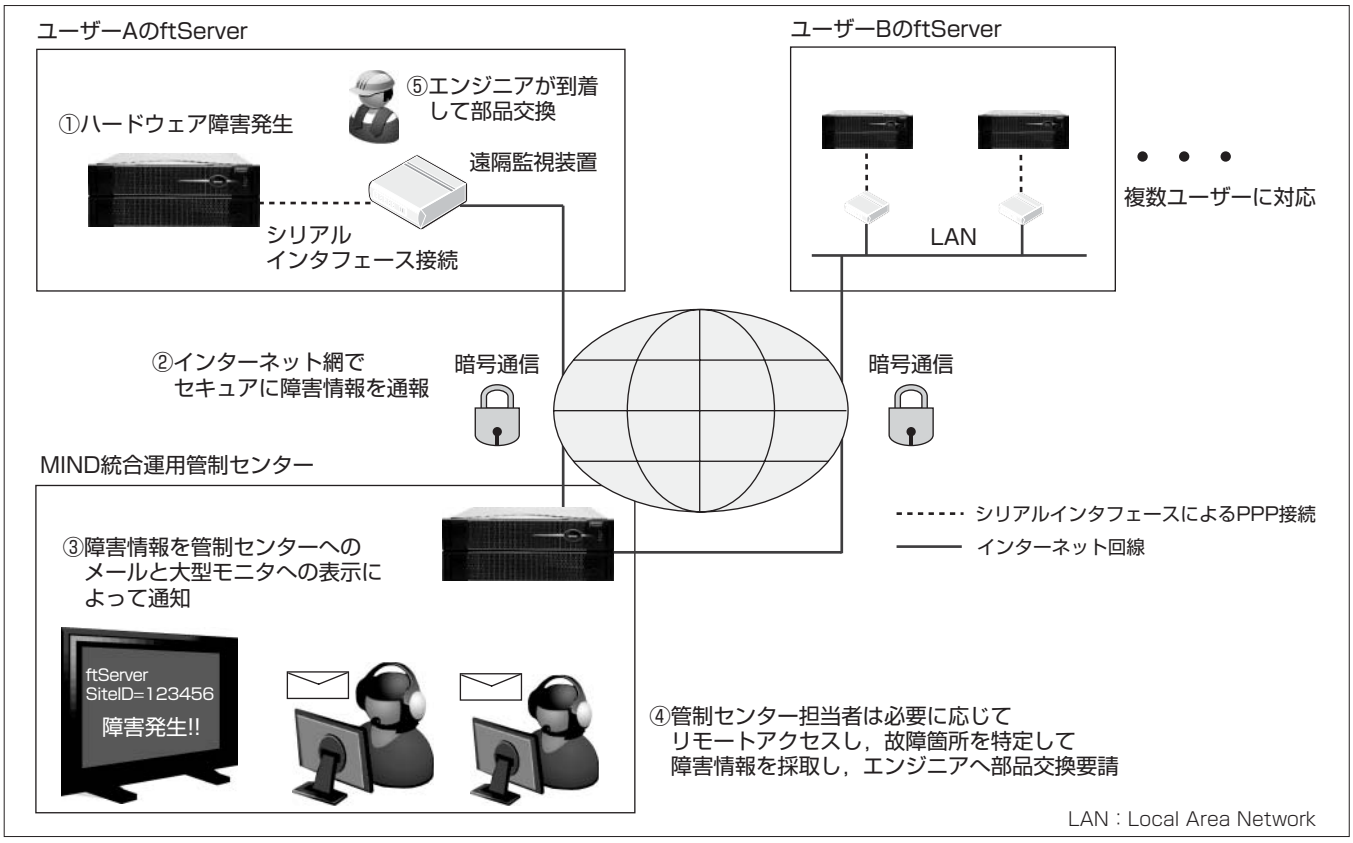
三菱電機インフォメーションネットワーク㈱(MIND)では，止められないシステムに対して無停止型サーバ“ftServer”(注1)の販売・保守を行っている。

ftServerは二重化したハードウェアが完全同期しながら動作するため，片方が故障しても動作し続けて無停止を実現している。しかし，二重故障によるシステムダウンを防ぐためには迅速なハードウェア障害の検知と故障部品の交換が重要である。MINDでは，ハードウェア障害が発生すると，電話回線を用いてMIND統合運用管制センター(以下“管制センター”という。)へ自動通報し，管制センターからリモートアクセスで診断して部品交換の手配をする仕組みを提供している。しかし専用の電話回線の敷設が必要なことや，PBX(Private Branch eXchange)を介さない回線に限られるなど，設置条件に合わない場合もあり，別の手段による仕組みを提供することが課題となっていた。

そこで公衆インターネット網を用いた遠隔監視システムを開発し，2015年2月から保守サービスを開始した。

ユーザー側にはftServerを監視するための遠隔監視装置を配置し，ftServerとシリアルインタフェースでPPP(Point-to-Point Protocol)接続することで既存のネットワーク構成に影響を与えない。また遠隔監視装置と管制センターを公衆インターネット網で接続するに当たり，公開鍵認証基盤(Public Key Infrastructure)を用いてセキュリティを担保した。ユーザー側に公衆インターネット環境さえ準備すれば，安価で容易にセキュアで高可用性を維持するための保守サービスを提供することが可能である。

(注1)　ftServerは，Stratus Technologies Bermuda Ltd.の登録商標である。



公衆インターネット網を用いた保守サービスの流れ

遠隔監視装置からftServerのハードウェア障害をポーリング監視し，障害を検知したら管制センターに通知する。管制センター担当者はターミナルソフトウェアを用いてリモートアクセスし，故障箇所を特定して部品交換の手配をする。ユーザーが用意するものは公衆インターネット環境のみで，既存の公衆インターネット環境を流用することができる。このように容易に高可用性を維持するための保守メニューを実現した。

*三菱電機インフォメーションネットワーク㈱

1. まえがき

近年の経済活動のグローバル化や24時間化に伴い，“ミッションクリティカルアプリケーション”，つまり停止してしまうとビジネスに莫大(ばくだい)な損害をもたらす重要なアプリケーションが急増している。

そこでMINDでは，止められないシステムに対して無停止型サーバftServerの販売・保守を行っている。

MINDでは，従来の保守サービスに加え，公衆インターネット網を用いた遠隔監視システムを開発し，2015年２月からサービスを開始した。

本稿では，公衆インターネット網を用いた遠隔監視システムの実現方法等について述べる。

2. 無停止型サーバftServer

ftServerは，ミッションクリティカルなシステム，又は24時間365日稼働が必要なシステムのためにハードウェアを二重化した無停止型サーバである[(1)(2)]。特長として次の３点が挙げられる。

(1) ハードウェアの二重化による無停止の実現

1台のftServerには，CPU(Central Processing Unit)・メモリ・チップセットのモジュールとPCI(Peripheral Component Interconnect)とPCIに接続するHDD(Hard Disk Drive)やLANのモジュールからなるエンクロージャが２台内蔵されている。

この２台のエンクロージャをロックステップと呼ばれる完全同期処理によって二重化している。各エンクロージャは同期しながら同じ処理を並行して実行し，OS(Operating System)などの上位層からは１台のハードウェアが動作しているように見える。エンクロージャは互いの障害検知と故障部分の特定機能を搭載しており，万一の障害発生時には故障部分を切り離し，正常な部分で処理を継続する(**図１**)。

(2) シングルシステム同様の操作性

OS・アプリケーションは１台のハードウェアが動作しているように認識するので，OS・アプリケーションのライセンスは１つのライセンス(注2)で運用可能である。エンジニアはシステムの二重化を意識することなく容易にシステムを構築・運用することができる(**図２**)。

(3) 無停止での故障部品の交換

正常運転時は１台のサーバとして動作するが，障害発生時は故障部分をエンクロージャ単位で切り離した上で連続して動作することができる。切り離したエンクロージャはシステムを停止させることなく交換し，復旧できる(**図３**)。

ftServerは先に述べたように，ハードウェア障害が発生しても継続して処理を行うことが可能である。しかし，二重故障が発生した場合のシステムダウンを防ぐためには，障害部位をいち早く検知し，故障部品を交換して二重化状

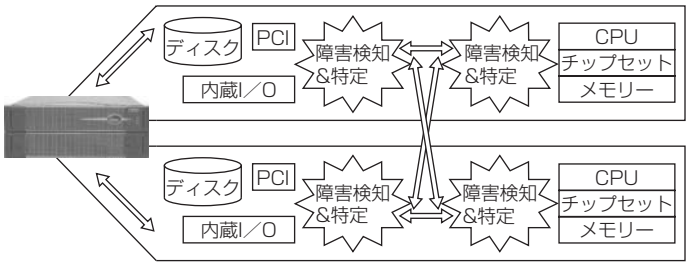


図１．ハードウェアの二重化による無停止の実現

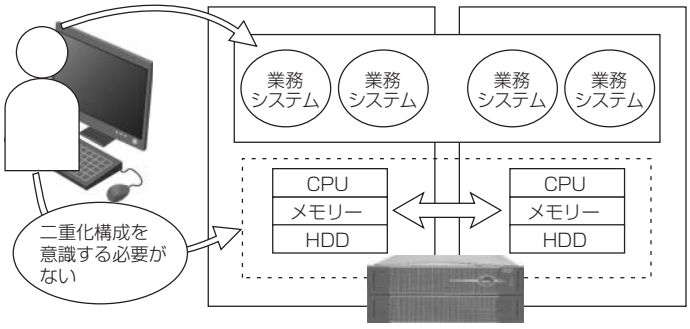


図２．シングルシステム同様の操作性

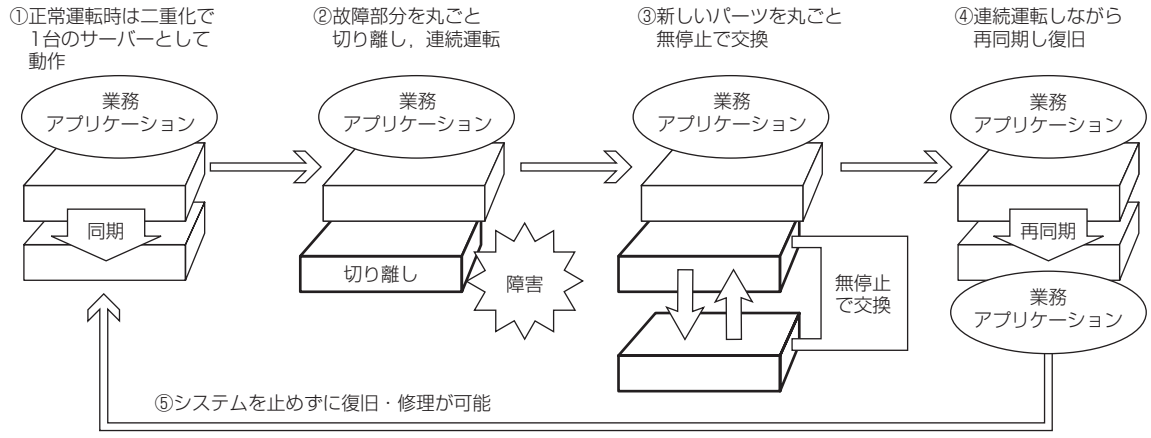


図３．無停止での交換

態へすみやかに復旧することが必要である。

（注２） アプリケーションによっては複数ライセンス必要な場合もある。

3. 公衆インターネット網を用いた遠隔監視のニーズ

MINDが従来提供している次の３つの監視の仕組みとそれぞれが抱える課題について述べる。

⑴ LEDランプの目視による監視

ftServerのフロントパネルのLED（Light Emitting Diode）を目視することによって二重化状態かハードウェア障害状態かを判別することができる。しかし，障害の発生を見落とした場合，もう一方が故障すると二重故障となりシステムダウンが発生するという課題がある。

⑵ ハードウェア障害警告機構による障害発生通知

ハードウェア障害警告機構は，サードベンダー製のネットワーク対応型警告灯とMIND製の障害検知ソフトウェアを連携させることによって，ハードウェア障害が発生すると警告音と警告灯によって障害の発生をユーザーへ伝えることができる。先に述べた⑴の方法に比べると障害の発生に気づきやすいが，警告音の聞こえる範囲や警告灯の見える範囲に制限がある。また，エンジニアがログを採取して障害部位の特定を行ってから部品の手配となるため，復旧までのリードタイムが長くかかり，この間に二重故障が発生するリスクがある。

⑶ ASNによる自動通報

ASN（ActiveService(注3) Network）はftServerのハードウェア障害を電話回線経由によって管制センターへ自動通報する仕組みである。管制センターでは，ASNによって障害が通報されるとユーザーへ障害発生の連絡をするとともに，リモートアクセスで障害解析・故障部位の特定を行って部品とエンジニアの手配を行う。このことによって，二重化状態に復旧するまでのリードタイムを短縮し，先に述べた⑴，⑵に比べ二重故障のリスクを低減することができる。

しかし，設置条件などによって電話回線を敷設できない場合があることや，敷設費用や回線固定費を懸念してASNを使用しないユーザーが増えており，導入が容易で安価な公衆インターネット網を用いたASN相当の監視が求められていた。

（注３） ActiveServiceは，Stratus Technologies Bermuda Ltd. の登録商標である。

4. 公衆インターネット網を用いた遠隔監視システム

MINDでは，ASN相当の監視のニーズを満たすための，公衆インターネット網を用いた遠隔監視システムの開発を行った。

4.1 システム構成

システム構成を**図４**に示す。

⑴ ユーザー拠点

ユーザー拠点にはftServerごとに遠隔監視装置を設置する。遠隔監視装置とftServerをシリアルインタフェースでPPP接続することでIP通信を可能とした。その際にftServerの業務用ネットワークに変更を加える必要がないようにするために，遠隔監視装置とftServerにクラスCの固定のプライベートIPアドレスを割り当てている。

遠隔監視装置に搭載された監視ソフトウェアによって監視を行い，公衆インターネット網を通じて管制センターの中継サーバへ監視結果を送信する。中継サーバとのセキュアな通信は，クライアントゲートウェイ機能を搭載することで実現した。

⑵ 管制センターの中継サーバ

管制センターの中継サーバでは，遠隔監視装置が監視しているftServerの監視結果を受信して管制センターの大型モニタを通じて管制センターの担当者に障害を通知する。

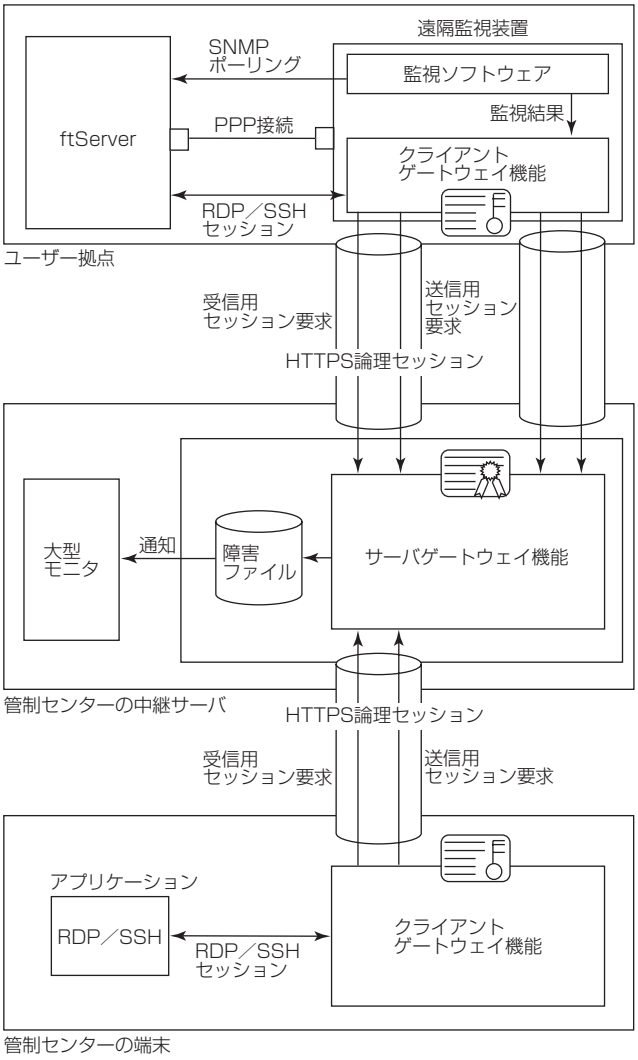


図４．システム構成

また，サーバゲートウェイ機能を搭載することで，管制センターの端末とユーザー拠点に設置した遠隔監視装置の通信をセキュアに中継することができる。

(3) 管制センターの端末

管制センターの端末はWindows(注4)端末である。管制センターの端末は，中継サーバと遠隔監視装置を経由してユーザーのftServerへアクセスすることができる。遠隔監視装置と同様に，中継サーバとのセキュアな通信は，クライアントゲートウェイ機能を搭載することで実現した。

(注4) Windowsは，Microsoft Corp. の登録商標である。

4.2 監視の仕組み

遠隔監視装置にはOSとして組み込みLinux(注5)，アプリケーション基盤として組み込みJava(注6)を採用した。

監視方法は，SNMP(Simple Network Management Protocol)でポーリング監視を行うJavaアプリケーションを搭載し，シリアルインタフェースでPPP接続されたftServerに対して，SNMPでポーリング監視を実施している。監視結果は遠隔監視装置内にファイルとして記載され，CIFS(Common Internet File System)によって中継サーバと共有される。

また，遠隔監視装置は自分自身が正常に動作していることを一定時間ごとに中継サーバに報告する。このことによって，中継サーバは，遠隔監視装置から報告が途絶えた場合，遠隔監視装置自体又はユーザー拠点と管制センター間のネットワークの異常を，管制センターの担当者に通知する。

(注5) Linuxは，Linus Torvalds氏の登録商標である。
(注6) Javaは，Oracle Corp. の登録商標である。

4.3 セキュアな通信接続

公衆インターネット網を活用するに当たり，セキュリティの確保は最重要課題である。

このシステムでは公開鍵認証基盤(Public Key Infrastructure)を最大限活用することによって，遠隔監視装置，管制センターの中継サーバ及び端末間の安全な通信や確実なデバイス認証を実現した。

公開鍵認証基盤では，電子証明書の定期的な更新が必須となる。このシステムではサーバ証明書を商用認証局から1年ごとに更新する運用として，遠隔監視装置にインストールしたクライアント証明書についても1年ごとに更新する運用とした。

4.3.1 通信プロトコル

公衆インターネット網上の通信はすべてHTTPS(Hyper Text Transfer Protocol over SSL(Secure Socket Layer)/TLS(Transport Layer Security))とした。通信をHTTPSのみにすることで，次に挙げる3点のメリットが得られる。

(1) ユーザー側での導入が容易

Webブラウザで使用されている暗号通信方式であるため，公衆インターネット上のWebサイトを閲覧できるネットワーク環境があれば，ユーザー拠点のFirewallやProxyサーバ等のセキュリティのインフラに追加設定などを行うことなく導入可能である。

(2) 中継サーバのシンプルなセキュリティ設計

中継サーバはHTTPSに対応したポート(443/tcp)のみを接続許可し，その他のポートは接続を禁止する設定にすれば良い。また，HTTPSが持つ接続先検証や認証の仕組みを利用できる。

(3) 効率的な開発

このシステムでは，HTTPS関連のライブラリとして，遠隔監視装置では組み込み用Java，管制センターのWindows端末では.NET Framework(注7)を採用し，中継サーバではIIS(Internet Information Server)(注7)のライブラリを採用した。Java，.NET Framework及びIISは世間一般で広く利用されているため，各ベンダーから提供される新たな暗号方式や脆弱(ぜいじゃく)性対策モジュールに対して迅速に対応できる。

(注7) .NET FrameworkとIISは，Microsoft Corp. の登録商標である。

4.3.2 ゲートウェイ機能

先に述べたように通信プロトコルとしてHTTPSを採用したが，HTTPSはリクエスト・レスポンス型のプロトコルであるため，双方向通信を行うRDPやSSHなどのプロトコルには向かない特性がある。

この点については，**図4**に示すように，クライアントゲートウェイで，1つのアプリケーションの通信に対して送信用のHTTPSセッションと受信用のHTTPSセッションを張り，2本のセッションを束ねて論理的な1本の双方向通信のセッションとすることで解決した。この論理的なセッションの上で，このシステムに必要なRDP・SSH・CIFS・SMTP(Simple Mail Transfer Protocol)の各プロトコルのデータをHTTPSデータに載せ，中継サーバと通信している。

サーバゲートウェイは，クライアントゲートウェイから送信されるHTTPSデータから各プロトコルのデータを取り出し，各プロトコルに対応した処理を行う。例えば，RDPやSSHの場合は接続先のクライアントゲートウェイに対して再度HTTPSデータにRDPやSSHのデータを載せてデータを中継する。

接続先のクライアントゲートウェイは，サーバゲートウェイから送信されたHTTPSデータから，各プロトコルのデータを取り出し，対応するアプリケーションへ送信する。

4.3.3 デバイス認証

もう1つの重要なセキュリティ面の課題は，不正なデバイスによる接続防止である。このシステムでは，クライアント証明書及びデバイスID(IDentification)を用いた2要素認証を採用している。

ftServerには，ユニークなサイトIDが割り当てられ，こ

のサイトIDをCN(Common Name)としてクライアント証明書が発行される。クライアント証明書は，工場出荷時に遠隔監視装置にインストールされるとともに中継サーバに記録される。

デバイスIDは，遠隔監視装置の工場出荷時にキーとしてランダム値が発行され，中継サーバに記録される。遠隔監視装置と中継サーバが通信を開始する際には，クライアント証明書とデバイスIDによる認証が行われ，どちらか一方でも異なる場合は通信できない。管制センターの端末も同様である。

さらに管制センターからは，リモートデスクトップやターミナルソフトウェアで，CNを含むホスト名指定での接続操作を可能とした。

4.4 遠隔監視装置へのモジュール自動配布

各ベンダーから提供される脆弱性対策モジュールを迅速に配布する方法や，クライアント証明書を1年ごとに配布する仕組みが必要となり，このシステムではモジュールの自動配布の仕組みを開発した。モジュールを配布する場合は，中継サーバにこのシステムの配布規則に則(のっと)ったモジュールを配置すると，遠隔監視装置はそれを検知し，適用可否を判断した上でモジュールのダウンロードとインストールが実施される。それによって，ユーザー操作は不要となり，迅速にモジュールの適用が可能となり，最新の状態を維持することができる。

5. むすび

無停止型サーバftServerの公衆インターネット網を用いた遠隔監視システムの実現方法について述べた。

この開発によって，ユーザーの既存の業務ネットワーク環境に影響を与えず，かつ既存の公衆インターネット環境を活用することで，安価で容易にセキュアで高可用性を維持するための保守サービスを提供することが可能となった。

この開発ではftServerを対象とした監視システムとなっているが，遠隔監視装置に搭載する監視ソフトウェアの仕組みを変更すれば他製品への応用も可能と考えている。

今後はこのシステムの適用の拡大を検討していく。

参考文献

(1) 平島栄一，ほか：無停止型サーバによるCC-Link IEコントローラネットワークの高信頼化，三菱電機技報，**88**，No. 8，481～484（2014）
(2) 三菱電機インフォメーションネットワーク㈱：フォールトトレラント・サーバ
http://www.mind.co.jp/businessplatform/ftserver/index.html