譲渡可能な操作権を保護するセキュア遠隔操作プロトコルの開発

○加藤 博光[*]　古谷 雅年[*]　玉野 真紀[*]　宮尾 健[**]　金子 茂則[**]　中野 利彦[**]
[*] (株)日立製作所 システム開発研究所　[**] (株)日立製作所 情報制御システム事業部

あらまし：社会が高度情報化するにつれてプラント制御系のような社会インフラシステムもオープンなネットワークに接続されるようになってきた。これにより、操作員一人一人に対する制御系へのアクセス管理を強化する必要性が増してきたが、連携運転や代理運転を依頼する場合に必要となる操作権の譲渡可能性も維持していく必要もある。本稿では、譲渡することが可能な操作権を管理するプロトコルを提案し、これを実装したプロトタイプを用いておこなった実験結果について報告する。

Secure Tele-operation Protocol Protecting the Negotiable Operation Privilege

Hiromitsu Kato[*]　Masatoshi Furuya[*]　Maki Tamano[*]
Takeshi Miyao[**]　Shigenori Kaneko[**]　Toshihiko Nakano[**]
[*] Systems Development Laboratory, Hitachi, Ltd.
[**] Information and Control Systems Division, Hitachi, Ltd.

Abstract: In the highly information-oriented society, even social infrastructure such as plant control systems has been connected to open communication networks. Hereby, the necessity to strengthen access control management of controlling systems for each operator is increasing. On the other hand, it is also necessary to maintain negotiability of operation privilege that is used to request cooperative or delegated operations. In this paper, we propose the protocol to manage the negotiable operation privilege, and report the experimental results proved by using our prototype that implements the proposed protocol.

1. はじめに

昨今の情報通信技術の急速な発展と普及によって、いたるものが情報ネットワークによって接続されるようになってきた。石油化学プラントをはじめ電力、ガス、水道といった重要社会インフラシステムについても同様に、ネットワークによって物理的・地理的には遠隔に存在する複数のシステムを連携させることが可能になってきた。特に、プラントの監視だけでなく操作も可能になると、夜間代行運転などの部署間連携運転や、保守作業のアウトソーシングもネットワーク経由でおこなうことが可能になる。さらに従来の専用線接続に比べて通信コストを大幅に削減することが可能となり、情報系システムとの連携も容易になる。

しかし、プラントの監視制御はこれまで、閉じた専用システムとして構築され、かつ、専用の操作室において専用の操作卓(Process Operation Console)を用いて、限られた操作員のみが監視制御をおこなっていた。これがインターネットのようなオープンなネットワークに接続された途端、操作をおこなうためのインターフェースが一般に開放され、悪意の第三者による不正操作の脅威が発生する。さらに、悪意の第三者だけでなく、組織内の正当な利用者であっても、専用操作卓から離れることによる緊張感の減少や判断材料の縮小により、悪意のない誤操作が妨害操作や越権操作

等に発展する可能性が増す。重要インフラの場合、これらセキュリティ上の脅威が社会的に重大な影響を与えかねないため、単なるデータの機密性・完全性・可用性を保護するだけでなく、操作行為を保護対象としたアプリケーションレベルのセキュリティが必要となる。

操作行為を保護するためにこれまで「操作権」という概念を取り入れて研究をすすめてきた[1)2)]。ここで、操作権とは「操作対象の状態に応じて動的に取得することができ、これを取得することで操作対象に対して優先的に操作することが許可される資格」と定義できる。

また、監視制御システムの特徴として、複数人の操作員で連携したり、役務を交代したりする必要がある。このため一度取得した操作権を別の操作員に譲渡する必要がある。ところが、このような譲渡可能な操作権は、利便性や運用の柔軟性と引き換えに、不正や誤操作によって組織のセキュリティポリシーにそぐわない譲渡につながる危険性も併せ持つことになる。

本研究では、操作権を安全に管理しつつ、譲渡可能という柔軟性を実現するために、操作員の操作対象に対する操作を中継し、操作権管理をおこなうセキュア遠隔操作プロトコル STP(Secure Tele-operation Protocol)を提案する。

2. 従来技術と課題

カメラを用いた遠隔監視制御において操作権を管理し排他制御をおこなう技術は既に存在する[3)]。しかし、操作権を取得している人以外は完全に排他されてしまったり、操作権取得要求に従って待ち行列に入り、一定時間経過後に操作権が割り当てられたりするものがほとんどである。実際のプラント制御系では、複数の操作員間での連携や、長い待ち時間なしで即座に操作権が取得できることが望まれている。

また、ある装置を操作中は別の装置を他の操作員に操作されたくない場合もある。例えば、河川管理システムでは、ポンプとゲートを操作して一方の河川の水を別の河川に放流する制御をおこなうが、ポンプを稼動中にゲートを閉鎖されると水が滞留して放水路が溢れてしまう危険性がある。よって、操作権は時間によって管理されず、各操作員の判断や組織のポリシーによって管理されることが望ましい。

これらの課題を解決することを目的として、以降セキュア遠隔操作プロトコル STP を提案する。

3. 提案技術

3.1 プロトコルの位置付け

STP はアプリケーション層のプロトコルである。よって下位のプロトコルに対しては極力既存の情報系セキュリティ技術を適用することが汎用性・拡張性の面からも望ましい。また、既存の組織のセキュリティポリシーに対する影響がでないような透過性を確保するために HTTP, SMTP, FTP のようなファイアウォール・フレンドリなアプリケーションプロトコルの上でも実現できることが実用上望まれる。

一方、アプリケーション側からの要請では、プログラミング言語やアーキテクチャに依存しないプロトコルであることが必要とされる。このような目的から近年 XML メッセージングによるプロトコルが数多く提案されるようになっている[4)5)]。

そこで STP は TCP/IP のアプリケーションプロトコル上で実現可能な XML メッセージベースのプロトコルとして設計した(図 1)。上位アプリケーションのメッセージは STP の XML メッセージに内包される子エレメントとして表現できる。

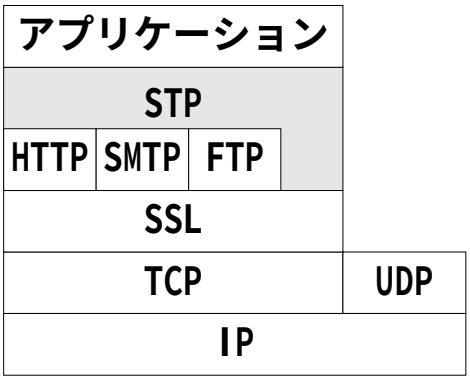

図 1 プロトコルスタックと STP の位置付け

3.2 システム構成

本研究で提案するプロトコルで前提としているシステム構成を図2に示す。操作員は遠隔操作端末からインターネット/イントラネットを介して操作をおこなう。情報系と制御系を中継する本プロトコルの要となるゲートウェイをSTPサーバと呼ぶ。操作員の認証やアクセス権限管理をおこなうだけでなく、動的に割り当てられる操作権の管理をおこなう。

操作員認証については、ディジタル署名[6]を利用するものとし、署名に用いる秘密鍵に対応する公開鍵はSTPサーバ上にあってもよい。しかし、公開鍵が公開されないことによって得られるセキュリティ強度を確保するために、STP サーバよりも内部(制御系側)のネットワークに署名検証サーバをおいて、この中に信頼できる公開鍵を格納しておくことを推奨する。署名検証サーバは公開鍵を用いてディジタル署名を検証し、検証結果をSTPサーバに返す。

組織のセキュリティポリシーはポリシーサーバにて一元管理され、分散しているSTPサーバに配信される。ポリシー配信プロトコルも「STP サーバに対する操作」としてSTPに準拠するものを用いる。

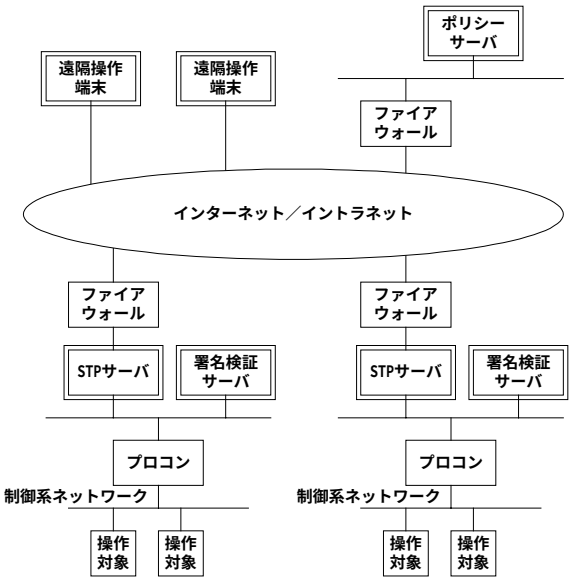

図2　システム構成

3.3 チケットと操作権

本研究では、操作対象にアクセスする前に制御系システムに論理的にログインするモデルとした。ログイン時にチケットを配布することによって、以後はチケットによって操作員を認証するものとする。ここで、チケットはランダムに生成されるバイト列とし、同じ操作員であってもログインする度に毎回変わるものとする。ただし、ログインしてからログアウトするまでは同じチケットを使い続ける。

一方、操作権はログイン後に操作対象の状態に応じて動的に取得するものである。操作対象が操作中であったり、運転ルール(Aを操作中はBを操作できない等)を逸脱したりする場合には操作権を取得することはできない。

正当なチケットを提示することで初めてSTPサーバは操作員からのメッセージを受け付け、必要に応じて操作権の割り当て・解放管理や操作コマンドの転送をおこなう。

3.4 プロトコル概要

まずSTPを支えるエージェント群について説明する。STP サーバ内では、操作員に対してホストするユーザ・ホスティング・エージェント(User Hosting Agent)と、操作対象に対してホストするオブジェクト・ホスティング・エージェント(Object Hosting Agent)が動作し、それぞれの役割の範囲においてアクセス制御をおこなう。

ユーザ・ホスティング・エージェント(UHA)は、各々の操作員に対して一対一で動的に割り当てられ、ユーザおよびメッセージの認証と、操作員毎に異なるアクセス管理を司る。UHA と操作員の間の通信セッションはSSLによって暗号通信路を確立するものとし、操作員が誤りや不正によって別の操作員にホストしているUHAにメッセージを送ることはできないようにした。

オブジェクト・ホスティング・エージェント(OHA)は、操作対象毎に一対一に割り当てられ、操作対象毎の操作権を管理し、操作対象毎の異なるアクセス管理やコマンドフィルタリングを司る。

このとき、操作権はUHAからOHAに対するリンクの割り当てとして表現することができる。

STP の主目的は遠隔操作端末から制御系内の操作対象までの間の安全な通信路を動的に確立することにある。すなわち、(1)UHA との間にセキュアなセッションを張り、(2)UHA と OHA の間に操作権としてリンクを張ることで、遠隔操作端末から操作対象までのパスが通り、このパスを通して制御対象にコマンドを送信する(図 3)。このパスの構築、解体、再構成をおこなう手順として STP を設計した。

まず(1)のセキュアなセッションは SSL/TLS によって張られ、加えてディジタル署名による操作員認証をおこなう。認証に成功した場合にはチケットが発行され、以後の XML メッセージにはこのときに発行されたチケットが要求される。次に(2)の操作権を取得するために、チケット付きの操作権取得要求を送り、操作対象が操作可能な状態にあれば、操作権として該当する操作対象を管理する OHA との間にリンクを張り、操作コマンドを通すためのパスを確立する。パス解体時には、操作権の解放およびログアウトをおこなう。

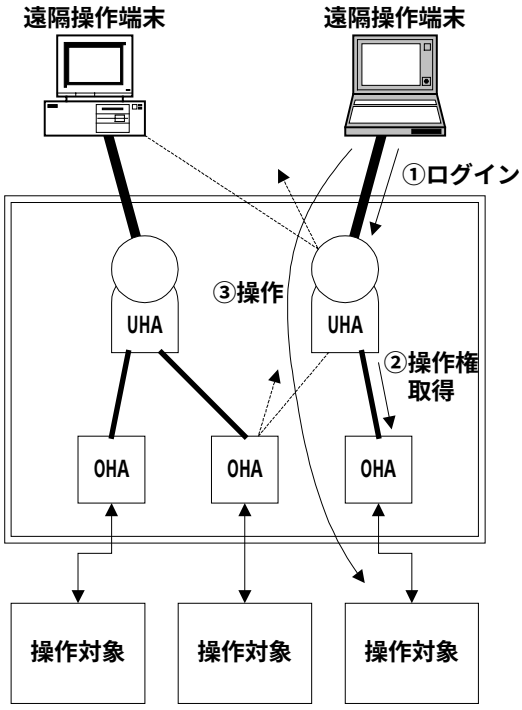

図 3　STP サーバの機能概要

3.5 三層フィルタリング

STP サーバでは UHA および OHA によって三段階のフィルタリングがおこなわれる。

(1) チケット/権限チェック

まず、UHA に送付されたメッセージに内包されているチケットが、UHA が管理しているチケットの値と等しいかどうか確認する。チケットが合致しなければ UHA はメッセージを受け付けない。

チケットが正当であることを確認した上で、合わせて操作員からの要求が権限の範囲内であるかどうかをチェックする。アクセス権限のない操作対象へのアクセス要求は拒否され、また、同じ操作対象であっても許可されていないコマンドの送信は拒否される。つまり、第一段階のフィルタリングでは、UHA が操作員毎に異なる静的に決定可能なアクセス制御ルールを適用したアクセス管理をおこなう。

(2) 操作権チェック

UHA は静的なフィルタリングだけでなく、動的に決定される操作権のチェックもおこなう。操作権は操作要求をおこなう操作員にホストする UHA と所望の操作対象にホストする OHA の間のリンクとして表現される。操作対象への操作コマンドを送付した場合には操作権の有無によってコマンドを通すかどうかフィルタリングをおこなう。

(3) コマンドフィルタリング

UHA と対称的に、OHA は操作対象毎に異なる静的アクセス制御ルールを適用したフィルタリングをおこなう。例えば利用可能時間帯に基づくコマンドフィルタリングは OHA によっておこなわれる。

4. 操作権譲渡交渉

4.1 譲渡の形態

操作権の譲渡に際しては、

- 譲渡相手は既にログインしている
- 操作員は自分から自発的に譲渡しない

という前提条件の下で譲渡の形態を考察した。

操作権譲渡要求に対して、システムがどのよう

に対応すべきかについては「上位優先」と「所有者優先」という２つの考え方があると考えた。以下にそれぞれの考え方について述べる。

4.1.1 上位優先

操作員の役割には優先順位があり、優先順位の高い操作員が優先的に操作権を取得できるとするポリシーをここでは上位優先と言う。上位優先ポリシーはさらに次の２種類のポリシーに分けられると考えた。

(1) 無条件： 優先順位の高い操作員が、操作権の現所有者の同意なく無条件に操作権の譲渡を強要するもの。

(2) 同意：優先順位の高い操作員が、操作権所有者の同意のもとに操作権の譲渡を受けるもの。操作中に強制的に操作権を譲渡させられるよりも、操作を完了してから譲渡するほうが制御系システムの安全を確保できる場合に用いる。この場合、上位の者の操作権要求が優先するため、下位の現所有者は譲渡に合意することはできるが、拒否することはできない。また、現所有者による同意にはタイムリミットが設定され、タイムリミットを越えて譲渡要求が放置された場合には、要求者に操作権を移す仕組みとしている。

4.1.2 所有者優先

操作権の所有優先権が現所有者にあり、現所有者の判断によって譲渡が決められるポリシーであり、所有者は譲渡に合意することも拒否することもできる。ただし、判断は設定したタイムリミット内におこなう必要があり、タイムリミットを過ぎて現所有者からの応答がない場合には、システムが自動的に要求者に操作権を譲渡する。

上位優先ポリシーであっても、優先順位が同格の場合には、所有者優先ポリシーに従う。

4.2 譲渡交渉プロトコル

操作権譲渡交渉では、まず操作権の取得要求をおこなう(図４ステップ①)。このとき、所望の操作対象と関連する OHA の利用が既に占有されている場合には占有者を確認し(図４ステップ②)、占有者にホストしている UHA に操作権の譲渡依頼を出す(図 4 ステップ③)。UHA はこれを受けて、操作員に譲渡するかどうかの問い合わせる(図 4 ステップ④)。

ここで、上位優先で同意を求めるポリシーの場合には操作員は同意を、所有者優先ポリシーの場合は同意または拒否をおこない、譲渡の判断を下す。譲渡に同意した場合には、譲渡同意メッセージを UHA に送る(図 5 ステップ⑤)。この判断によって、UHA-OHA 間のリンクが操作権取得要求者にホストする UHA と OHA 間のリンクに再割り当てされる(図 5 ステップ⑥)。これが操作権の譲渡になる。再割り当てが完了すると、元の操作権所有者には操作権解放通知が(図 5 ステップ⑦)、新たな操作権所有者には操作権取得通知が(図 5 ステップ⑧)それぞれ送られる。

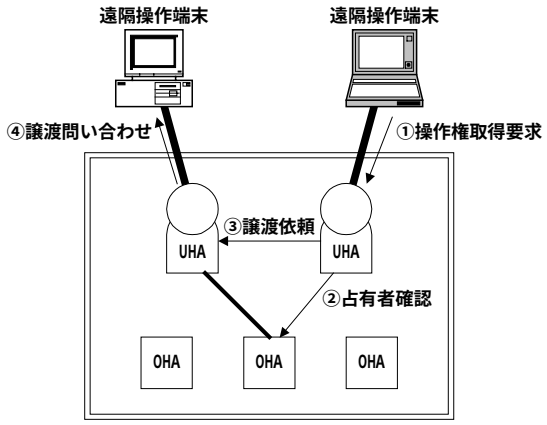

図４　操作権取得要求

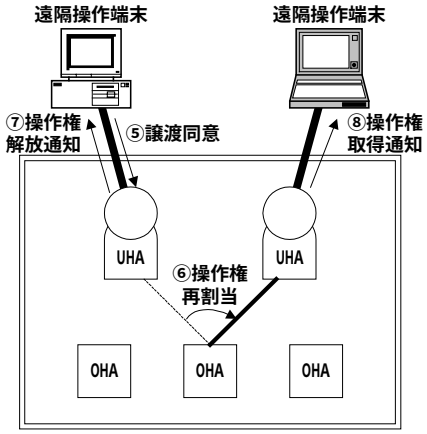

図５　譲渡による操作権再割り当て

5. 実験結果および考察

実証実験では、実験室 A 内に 2 台の遠隔操作端末、実験室 B 内に STP サーバ、署名検証サーバ、制御系エミュレータを設置した(図 6)。STP サーバは Linux[1]サーバにネットワークカードを二枚差し、一方を専用線 IP 接続によりインターネットに、もう一方を 10Mbps の LAN(制御系 LAN を模擬)に接続した。実験室 A 内の 2 台の遠隔操作端末はそれぞれダイアルアップによってインターネットに接続した。操作員によるディジタル署名に用いる秘密鍵は IC カード内に格納した。ソフトウェアはさまざまな機器に組み込める拡張性、ユービキタス性に配慮してすべて Java[2]で実装した。

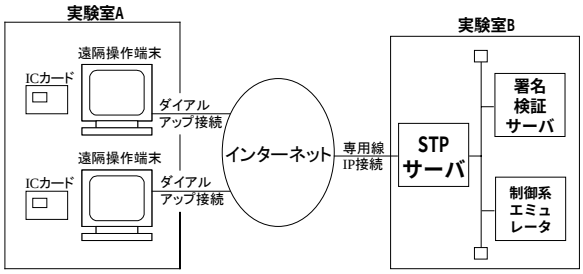

図 6 構築した実証実験環境の概要

実験により提案するプロトコルの実現可能性を確かめた。また、インターネットを利用することによるプロトコル処理の遅延の影響が 1〜2 秒あることを観察した。

6. まとめ

プラント監視制御系における操作行為を保護する必要性に着目し、特に操作権の譲渡も安全に実現することを目的としてセキュア遠隔操作プロトコル STP を提案した。

実機による実証実験により、提案するプロトコルの実現可能性を確認したが、インターネットを介して操作コマンドを送る場合に伝送遅延があることも確認した。ネットワークの高速化によってこの遅延は縮小される方向にあるが、リアルタイム性が要求される制御系に対する影響についても今後調査する必要がある。

また、今回の譲渡交渉は問い合わせ形式を主体としたが、実際には所有者から能動的に操作権を譲渡する形式も必要と考え、今後プロトコルの拡張を検討する。さらに、代理操作を柔軟に実現するために操作権の譲渡だけでなく、権限の委譲方法についても今後検討していく必要がある。

[1] Linux は, Linus Torvalds 氏の米国およびその他の国における登録商標あるいは商標です。

[2] Java 及びすべての Java 関連の商標及びロゴは, 米国およびその他の国における米国 Sun Microsystems,Inc.の商標または登録商標です。

謝辞

本研究は、情報処理振興事業協会の石油精製業ネットワークセキュリティ対策事業「大規模プラントネットワークにおける遠隔操作、遠隔保守のためのセキュア通信プロトコル技術の研究開発」の一部として行った。情報処理振興事業協会を始め、関係会社・関係各位のご支援に感謝します。

参考文献

[1] 古谷, 玉野, 加藤 : 遠隔操作・保守のためのセキュア通信プロトコル技術の研究開発, 重要インフラセキュリティ対策セミナー, pp.51-58, 2001

[2] 古谷, 加藤, 瀬古沢, 小泉:操作権認証と操作コマンドフィルタリング機能を有する情報系ー制御系連携のためのファイアウォール, 情報処理学会コンピュータセキュリティシンポジウム, pp.147-152, 1999

[3] http://www.canon-sales.co.jp/Product/appli/webview/webview3.html

[4] W3C Note “Simple Object Access Protocol (SOAP) 1.1”, May 8, 2000, http://www.w3.org/TR/SOAP/

[5] uddi.org:UDDI Technical White Paper, September 6, 2000

[6] W.Ford, M.Baum 著. 山田訳:ディジタル署名と暗号技術, プレンティスホール出版, 1997