推薦論文

制御系ファイアウォールのためのセキュア遠隔操作プロトコル STP

加藤博光[†] 玉野真紀[†]
古谷雅年[†] 宮尾健[††]

本研究は，プラント制御系システムに対して IP ネットワークから安全に遠隔操作を行うためのプロトコルに関し，特に「操作権」の概念による制御系システムへのアクセス制御機構を提案するものである．情報系システムと制御系システムが融合されていく中，制御系システムは IP ネットワークを通じて利便性高くアクセス可能となった反面，セキュリティ上の脅威にもさらされるようになった．特に制御系システムに向かって情報が流入する操作コマンドは，情報としてのフィルタリングだけでなく，操作というアプリケーションでのフィルタリングによってチェックされたものだけが制御系システムに渡される仕組みが，安全性を確保するうえで必要不可欠となる．本研究では，操作権を管理する制御系向けファイアウォールを考案し，このファイアウォールへアクセスするためのプロトコルとしてセキュア遠隔操作プロトコル STP を設計した．制御系ファイアウォールは STP サーバとして機能し，内部で動作するエージェントが操作員認証，アクセス制御，操作権管理を行う．操作権を取得してはじめて操作が可能となる排他制御を実現しつつ，操作権は交渉によって譲渡可能として柔軟性を持たせた．プロトタイプを用いた実証実験の結果，提案するプロトコルの実現可能性を確認した．さらに，脆弱性分析により，プロトコル自身に対して想定される脅威に対する耐性も示し，実用上の安全性を確認した．

Secure Tele-operation Protocol for the Firewall in the Control System

Hiromitsu Kato,[†] Maki Tamano,[†] Masatoshi Furuya[†]
and Takeshi Miyao[††]

This research is related to secure tele-operation protocol for the plant control systems via IP networks. We propose the access control mechanism for the control system by using the concept of “operation privilege.” In the fusion of information systems and control systems, it has been possible to have access to the control systems from IP networks with high usability. At the same time, however, the control systems have been exposed to various threats of the IT security. Especially in case of operations, whose information is inbound flow for the control system, the command must be inspected in the application layer to ensure the security. In this research, the firewall for the control systems with capabilities of operation privilege management is considered, and Secure Tele-operation Protocol (STP) is designed to communicate with the firewall, which behaves as the STP server. The agents inside the firewall manage the operator authentication, access control, and operation privileges. The proposed protocol realizes the exclusive operation with operation privilege management, even though the privileges can be transferred to another operator after negotiation. Experimental results showed the feasibility of the proposed protocol. Additionally, the vulnerability analysis showed the practical security against the supposed threats for STP.

1. はじめに

水道，ガス，電力などの公共施設は元来，遠隔監視，遠隔制御を行う必要があり，ネットワーク化されたシステムとして構築されている．この大規模プラントネットワークシステムにはリアルタイム処理や高信頼性が要求されるため，これまで専用システムとして構築され，それ自身で閉じた系として存在していた．し

† 株式会社日立製作所システム開発研究所
Systems Development Laboratory, Hitachi, Ltd.
†† 株式会社日立製作所情報制御システム事業部
Information and Control Systems Division, Hitachi, Ltd.

本論文の内容は 2001 年 5 月のコンピュータセキュリティ研究会にて報告され，CSEC 研究会主査により情報処理学会論文誌への掲載が推薦された論文である．

かし，専用システムは高コストであり，また部分的変更が全体に影響するため柔軟なシステム構築や拡張が課題であった．そのため，近年は標準技術を用いてシステムを構築する方向にシフトしており，ネットワークにはイントラネット技術が取り入れられ，プロセスコンピュータやコントローラが IP（Internet Protocol）で相互接続されるようになってきた．

IP で接続されることにより，監視制御業務にもインターネットで培われた技術を利用することが可能になり[1),2)]，また拡張性や相互接続性も飛躍的に向上してきた．これは今後の広域分散制御システムに不可欠な要件である．たとえば水道の分野では，運転管理や水質管理などの技術業務を複数の事業体が連携して実施できるように法改正がなされた[3)]．しかし，事業統合や委託を行うためにシステムを大幅に改変することはコスト高であり，これを効率的・効果的に実現するためにはオープンな技術による相互接続はなくてはならないものになる．

しかし，一方でネットワークのオープン化によって，制御系システムは情報セキュリティ上の脅威にさらされることになる[3),4)]．特に操作の際には IP ネットワークから送信された制御コマンドを制御系システムが受け付ける必要があり，制御コマンドの正当性のチェックを十分に行う必要がある．

さらに，広域に分散かつ連携する制御系システムでは，複数の操作員が同じ操作対象を異なる意図の下で操作する可能性がある．たとえば，通常運用と保守操作のための制御コマンドを混在して受け付けてはシステムが不安定になる可能性がある．しかし，この資源競合問題に対して単純な排他制御を適用しては，代行運転など操作を遠隔で交代したり連携したりする柔軟な運転への対応が困難になる．よって，セキュリティに配慮しながらも，操作主体を正当な第三者に移行可能な柔軟性もあわせ持ったシステム構築が必要になる．

そこで本研究では，操作権というコンセプトを導入し，広域分散制御システムにおいて安全かつ柔軟な遠隔操作を実現するセキュア遠隔操作プロトコル STP（Secure Tele-operation Protocol）を提案する．以下，2 章では制御系システムの概要を述べ，制御系と情報系の融合，システム要件，情報制御セキュリティ上の脅威について概観する．3 章では従来の関連技術をレビューし，解決すべき問題点を明確化する．4 章では，権限と権利を区別した提案技術の基本コンセプト，プロトコルスタック上での位置づけ，システムアーキテクチャを述べ，プロトコル概要を説明する．5 章では，STP の実現可能性を検証するために開発したプロトタイプシステムの仕様について説明する．6 章では，STP に対して想定される攻撃への耐性/脆弱性について分析した結果を議論する．

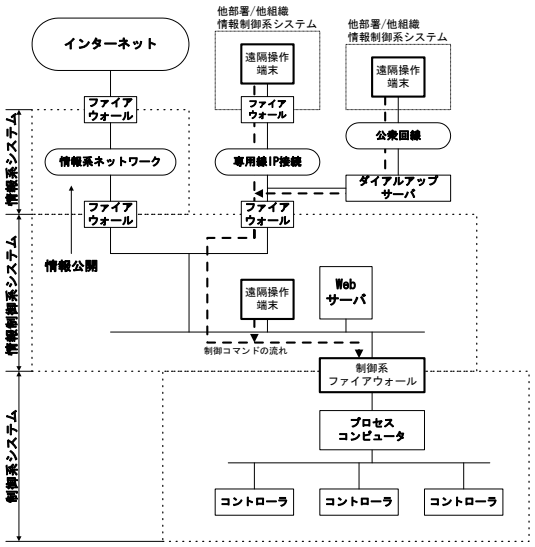

図 1 情報系システムと連携した制御系システムの概要
Fig. 1 Overview of the control system with cooperation of the information system.

2. 制御系システムにおける課題

2.1 制御系と情報系の融合

従来，デバイスを直接制御する制御系システムは，業務情報を扱う情報系システムと物理的にも切り離された存在であった．しかし，近年では制御系システムはローカルなデバイスを制御するだけでなく，生産管理などの業務情報と密接に関連して制御を行ったり，外部機関から気象情報などを取り込んで運用管理を行ったりする必要性が増してきた．このような情報系システムと制御系システムの統合には，オープンな情報系システムの技術を利用した制御系システムの構築が必須になる．このように，制御系システムであるが情報系システムの技術を使うシステム層を情報制御系システムと定義することにする（**図 1**）．

2.2 広域分散制御システムの要件

異なる制御系システムがネットワークにより相互接続されると，代行運転や遠隔保守のために遠隔の他組織から制御を行うことが可能になる．しかしながら，制御系システムはインターネットにおける情報系システムとは異なり「いつでも・だれでも」アクセスできてしまうことは許可されない．操作は権限が与えられた操作員のみに限られなければならず，操作可能な場合のみに限られなければならない．

広域分散制御システムは，情報制御系システム間で専用線またはダイアルアップ接続によってイントラネットを形成する連携形態が一般的である（図1）．インターネットと情報系システムの間にはファイアウォールを設置するなどセキュリティ対策を施すが，現状では情報系システムと情報制御系を含めた制御系システムの間には十分なセキュリティ対策が施されていない場合が多い．本研究では，制御系システムの視点から考えて，情報制御系システムは信頼できない情報空間ととらえる．よって，情報制御系システムと制御系システムの間には，制御系システムを保護する最後の砦として，制御系ファイアウォールを設置する必要があると考える．以降，この制御系ファイアウォールを中心としたシステムのあり方を考察する．

2.3 情報制御セキュリティ上の脅威

情報制御系システムでは，悪意の攻撃だけでなく，広域分散環境に起因する誤操作も主たるセキュリティ上の脅威と考える．

たとえば，保守員が遠隔から保守している最中に，通常の操作員が誤って保守中の系統にコマンドを送ってしまった場合には，通常時は正当なコマンドだとしても，保守用に系統の設定を変更していると，制御系が不安定な挙動に陥りかねない．よって，保守員が作業中は作業対象の制御系へのアクセスを制限する排他制御をいかに実現するかが課題となる．

逆に系統が通常モードであるにもかかわらず保守時のテストコマンドが正常な系統に流れ込んでしまってもやはり非常に危険な状態に制御系が陥る可能性がある．よって，制御系の状態に応じたアクセス制御・フィルタリング機構の実現についてもあわせて課題としてとらえた．

3. 従来技術と問題点

上記課題を解決するためにはアクセス制御技術が必要となる．ネットワーク上でのアクセス制御技術としては，一般的にはファイアウォールを用いて情報流のアクセス制御を行う方法が普及している[5]．ところが，オープン化した制御系システムは情報系システムから見るとアプリケーションの1つにすぎず，汎用的なファイアウォールはアプリケーションレベルで情報系と制御系を区別することができない．アプリケーションレベルのアクセス制御に関しては，Webサービス[6),7)]の標準化を見据えた議論としてXACML（eXtentible Access Control Markup Language），SAML（Security Assertion Markup Language）などのXMLを基盤とした新技術が提案されてきている[8),9)]．しかし，これらの標準技術はユーザに対する認証と権限付与に焦点が絞られており，競合操作の解消や操作対象の状態と連動したアクセス制御を実施する枠組みまでは提供しない．

よって，現在操作を実施している操作員にのみ操作許可を限定し，アクセス権限はあっても操作権利のない操作員による操作をフィルタリングする制御系向けアプリケーションゲートウェイが必要と考える．また制御系の状態によって操作権利の取得やコマンド通過可否の判断が可能であることが望まれる．

一方，資源競合に対して典型的にとられる手法は排他制御と待ち行列である[10)]．資源が不可分な場合には，排他的にアクセス権限を与え，他の誰かが利用中にアクセス要求を行うと待ち状態になるものである．しかしながら，広域分散制御システムでは操作行為を厳密に排他制御するよりは，代行運転などに対応可能なように譲渡可能として，柔軟な運用に対応する方が有効である．操作を行う権利を譲渡することで，アクセス権を変更することなく，権利を手放した操作員による誤操作を防止することが可能となる．本論文では，このようにアクセス権を規定する権限に加えて次章に述べる「操作権」というコンセプトを導入し，操作権を譲渡することで誤操作防止に対処するフレームワークを提案する．しかし，この譲渡交渉は信頼できない情報空間を経由しながら安全に行われる必要があり，そのためのプロトコルが望まれる．

4. 提案技術

4.1 操作権コンセプトの導入

従来技術の問題点を解決するために，まずはじめに操作権という概念を導入した[11)~13)]．操作権は「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」と定義される．つまり，操作権を取得することによって操作対象に対して排他的に操作を実行することが可能になり，他の操作員が操作権を取得している最中はアクセス不能となる．

本論文では権限と権利を区別して使う．権限（authority）は「操作対象またはその特定の機能を利用可能な範囲」ととらえ，管理者があらかじめ設定しておく静的なものと考える．一方，権利（privilege）は「権限の範囲内で取得可能な資格」ととらえ，権利にはつねに権利所有者があると考える．この意味で，操作権は権利の一種である．たとえば利用者AとBが機器Xを利用することが許可されており，現時点ではAがXを利用しているとする．この場合，A，B

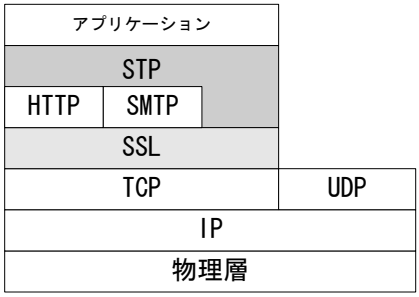

図 2 プロトコルスタックから見た STP の位置づけ
Fig. 2 Position of STP in the protocol stack.

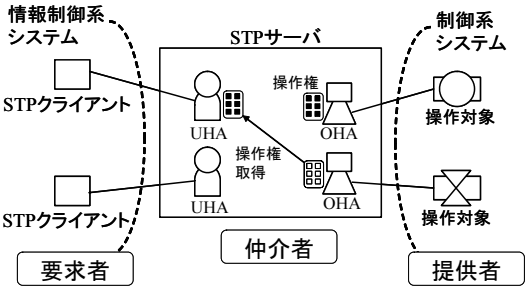

図 3 三層仲介モデル
Fig. 3 Three-tier mediation model.

ともに X へのアクセス権限はあるが，実際の操作権は A にあると考える．この操作権は B に譲渡可能である．

以上の操作権コンセプトを利用して全体システムアーキテクチャとともにセキュア遠隔操作プロトコル STP（Secure Tele-operation Protocol）を設計した．

4.2 プロトコルの位置づけ

本研究で対象としているセキュリティシステムは制御系アプリケーションでのセキュリティをターゲットとしている．しかし，すべてを独自に構築することは情報制御系システムのオープン化の流れに反し，相互接続性が損なわれてしまう．そこで，既存の汎用なセキュリティ技術で有用なものは利用し，かつアプリケーションプロトコルとして汎用的かつ拡張性高く実装可能なように XML メッセージングによるプロトコル[14]として設計した．

一方，STP をアプリケーションプロトコルと位置づけたとき，下位レイヤのプロトコル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．よって，通信路の暗号化，メッセージ改ざん検知，サーバ認証には SSL[15]（Secure Socket Layer）を用いることにした．SSL でもクライアント認証が可能であるが，操作員認証と操作権管理は密接に関連するため，操作員（クライアント）認証は STP で行うものとした．

そこで STP は SSL を前提とし，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た[16]（**図 2**）．

4.3 システムアーキテクチャ

4.3.1 三層仲介モデル

STP を実施する全体システムは**図 3** に示す三層仲介モデル[17]をベースに設計した．システムは，要求者（requester）である操作員，サービス提供者（provider）である操作対象，仲介者（mediator）である STP サーバによって構成される．STP サーバは操作対象を保護する制御系ファイアウォールの役目を果たす．操作員は STP クライアントを操作端末として STP サーバにアクセスする．三層仲介モデルとすることで，要求者は個々のサービス提供者ごとに認証を受けなくても，仲介者に対して認証を受ければよく，操作権管理も仲介者に代行してもらうことが可能になり，要求者である操作員の利便性が高まる．また，要求者はサービス提供者へ直接アクセスできないため安全性も増す．

STP サーバ内には情報制御系と制御系を論理的に分離するために 2 種類のエージェントを配した．これらのエージェントが実際のセキュリティチェックを行う．1 つはユーザホスティングエージェント（User-Hosting Agent: UHA）であり，アクセスを試みる各々の操作員に 1 対 1 で対応し，認証と権限確認を行う．もう 1 つはオブジェクトホスティングエージェント（Object-Hosting Agent: OHA）で，個々の操作対象に対して 1 対 1 で対応する．OHA は操作対象の状態を監視するとともに操作権を管理する．ここで操作権はリモコンのメタファで考えることができる[11]（図 3）．つまり，OHA が管理しているリモコンを UHA が取得すると，UHA はリモコンを使って操作対象を制御できるようになる．ある UHA がリモコンを取得すると，別の UHA が操作権取得要求を同じ OHA に対して行っても，リモコンがないため操作権を取得することはできないことになる．

4.4 基本プロトコルの概要

通常時に利用する基本プロトコルとして，ログイン—操作権取得—操作—操作権解放—ログアウトのそれぞれのプロトコル概要を以下に示す．

(1) **ログイン（図 4）**

まず最初に STP サーバにログインする必要がある．ログインするためには STP クライアントは UHA と SSL セッションを張り，UHA に対して認証情報を提示する必要がある．認証に成功すると UHA はチケット

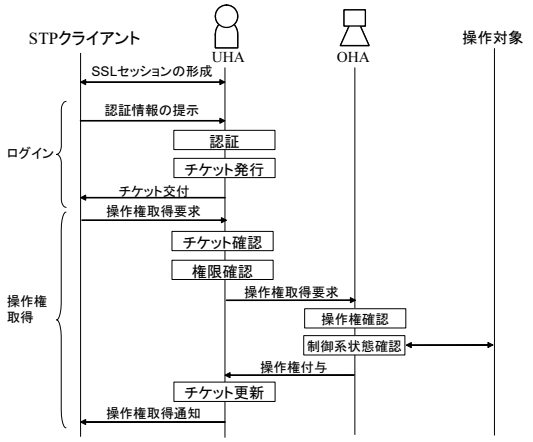

図 4 ログインおよび操作権取得プロトコルの概要
Fig. 4 Protocol overview for login and operation privilege acquisition.

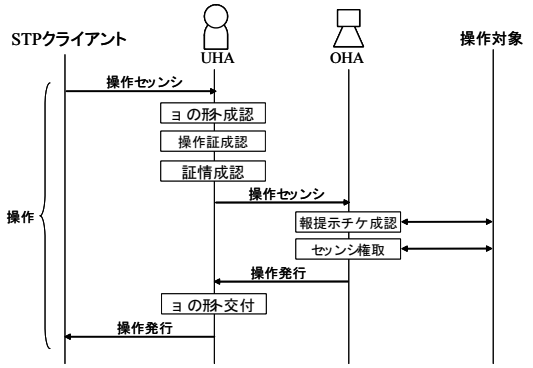

図 5 操作プロトコルの概要
Fig. 5 Protocol overview for operation.

を発行する．ここで，チケットとは乱数によって生成されるデータである．以降，ログアウトするまで STP クライアントから出されるすべてのメッセージにはチケットを添付し，STP サーバはメッセージを応答するたびにチケットを更新する．チケットの発行により，認証情報の繰返し提示を省くとともに，乱数であるためメッセージが解読された場合の被害を最小限にとどめることができる．

(2) **操作権取得**（図 4）

ログイン後，目的の操作対象に対して操作を行うために UHA に対して操作権取得要求を行う．UHA は受信したメッセージに基づき，チケットが自分が発行したものと合致するか確認し，操作員認証を行う．次に，要求している操作対象に対するアクセス権限があるかチェックを行う．アクセス権限があれば，操作対象にホストする OHA に対して操作権の取得要求を行う．OHA は操作権があって，操作対象が制御可能な状態であれば，操作権を UHA に渡す．UHA は操作権を取得できたか否かを操作員に通知する．

(3) **操作（図 5）**

操作権を取得した後にはじめて操作コマンドを送信することができる．UHA は操作コマンドに添付されているチケットを確認し，同時にコマンド送信先の操作対象への操作権を有しているかチェックする．次に，コマンドの内容が権限の範囲内であるかどうかチェックし，許可されていないコマンドの場合には拒否する．

UHA によるチェックに合格したコマンドは OHA に転送される．OHA は指示されたコマンドを現在実行してよいかどうか操作対象の状態を確認し，許可されれば操作対象へコマンドを送信する．操作対象からの応答は OHA-UHA 経由で操作員に応答メッセージとして返される．

(4) **操作権解放**

操作権解放プロトコルは操作権取得プロトコルとほぼ同様である．取得の場合と同様に，権限の範囲外で不正に操作権が解放されないようにチケットのチェックとアクセス権限のチェックも行う．適正な解放要求であれば，UHA は操作権を元の OHA に返却し，操作員に解放処理結果を通知する．

(5) **ログアウト**

UHA へのログアウト要求によって操作員は制御系システムからログアウトする．第三者によって不正にログアウトさせられないように，ここでもチケットをチェックする．チケットが正当であれば所有している操作権をすべて解放し，ホストしている UHA を消滅させる．

4.5 操作権譲渡交渉プロト コルの概要

4.5.1 優先順位の考え方

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，まず「上位優先」と「所有者優先」という 2 つのポリシーがあると考えた．以下，それぞれの内容について述べる．

- 上位優先
  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ポリシー．この場合，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．譲渡に合意するまでのタイムリミットを設定し，タイムリミットが過ぎると無条件に操作権が譲渡される．タイムリミットはポリシーによって設定する．タイムリミット 0 の場合には，優先順位の高い操作員が絶対的に優先され，操作権所有者の同意の必要なく操作権を取得できるポリシーになる．

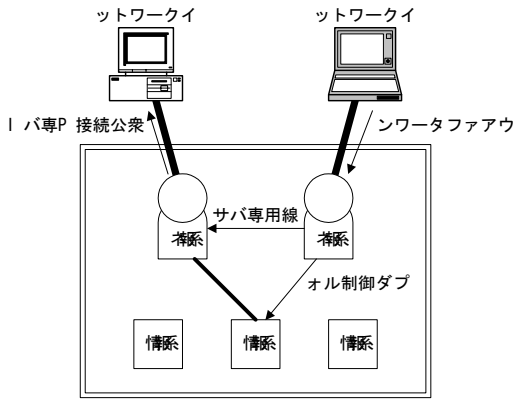

図 6 操作権譲渡要求
Fig. 6 Request of operation privilege transfer.

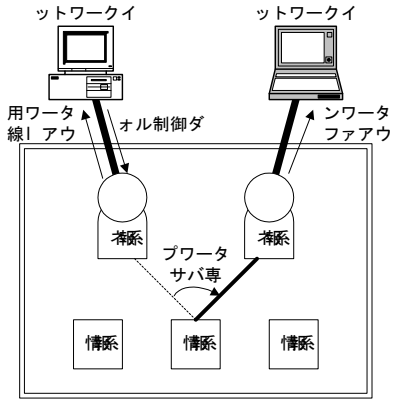

図 7 操作権所有者切替え
Fig. 7 Switch of the owner of the operation privilege.

- 所有者優先
  操作権の所有優先権が現所有者にあり，所有者の判断によって譲渡が決められるポリシー．所有者は譲渡に合意することも拒否することもできる．判断はタイムリミット内に行う必要がある．タイムリミットはポリシーによって設定する．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，操作権放置によるデッドロックを避けるために，優先者である現所有者よりも要求者を例外的に優先し，要求者に操作権を譲渡する．

ここで，優先順位ポリシーは制御系システム管理者が組織の長の判断に基づいて STP サーバに設定する．組織の中に階層関係があり，上位の操作員に高度な運転ノウハウがある場合には，上位優先ポリシーを適用することが望ましい．逆に，権限を与えられた操作員に差がない場合や，上下関係に依存せず操作権の現所有者が継続して操作することが望ましい業務では所有者優先ポリシーを適用することが望ましい．

4.5.2 操作権譲渡

上記ポリシーの下で次のような譲渡交渉プロトコルを考案した．

操作権譲渡交渉では，まず操作権の取得要求を行う（**図 6** ①）．このとき，所望の操作対象と関連する OHA の利用がすでに占有されている場合には占有者を確認し（図 6 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 6 ③）．UHA はこれを受けて，操作員に譲渡するかどうかを問い合わせる（図 6 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行い，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 7** ⑤）．この判断を受けて UHA 間で操作権が譲渡

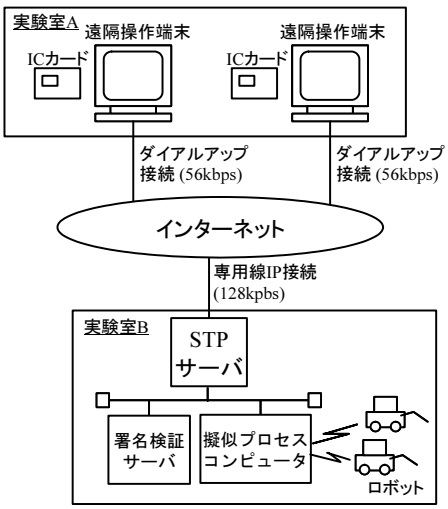

図 8 インターネットを経由した実験環境
Fig. 8 Experimental environment via the Internet.

され，操作権取得要求者にホストする UHA が新たな操作権所有者になる（図 7 ⑥）．UHA 間で操作権譲渡が完了すると，元の操作権所有者には操作権解放通知が（図 7 ⑦），新たな操作権所有者には操作権取得通知が（図 7 ⑧）それぞれ送られる．

5. プロトタイプシステムの仕様

STP を用いて遠隔操作を行うプロトタイプを試作し，実証実験を行うことによって STP の実現可能性を確認した．実証実験は LAN 環境とインターネット環境の両者で行った．インターネット環境における実験システム構成を**図 8** に示す．操作員認証はディジタル署名による方式を採用し，操作員が保有する IC カードの中に秘密鍵を格納した．ディジタル署名の検証は，公開鍵データベースを持つ署名検証サーバによって行

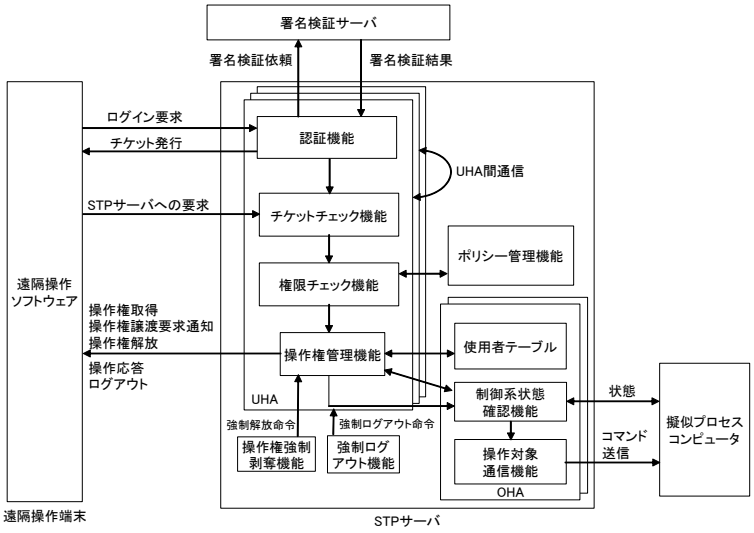

図 9 プロトタイプシステムの機能ブロック図
Fig. 9 Function block diagram of the prototype system.

うものとし，制御系ネットワークを模擬した LAN 上に設置した．ログイン要求が STP サーバに送られた際には，STP サーバは署名検証サーバにディジタル署名の正当性を問い合わせる．操作対象としてはロボットを用い，これらを遠隔で操作するシステムとした．

プロトタイプシステムの概要仕様として機能ブロック図を**図 9** に示す．遠隔操作端末は Web ブラウザ上で遠隔操作ソフトウェアを STP サーバからダウンロードして実行する．遠隔操作ソフトウェアから STP サーバへアクセスを試みると，UHA をスレッドとして起動し 1 対 1 でホストするものとした．遠隔操作ソフトウェアと UHA スレッド間には SSL セッションが張られる．

UHA は内部に，認証機能，チケットチェック機能，権限チェック機能，操作権管理機能を有する．認証機能は，操作員の認証子として提示されるディジタル署名を検証することで操作員を認証する．実際の検証処理は，操作員の公開鍵データベースを持つ署名検証サーバ上で行う．認証に成功した場合には UHA は自ら乱数を生成し，Base64 エンコードした値をチケットとして遠隔操作ソフトウェアに送信する．チケットチェック機能は，以降のセッションで提示されるチケットが自らが発行したものであるかどうかを確認するものである．権限チェック機能は，アクセス制御ルールを管理しているポリシー管理機能に問い合わせることで，操作員からの要求が権限内であるかどうかを確認する．

操作権管理については，UHA が OHA の使用者テーブルと連携しながら行うものとした．OHA の使用者テーブルは，操作権を与えた操作員，すなわち OHA がホストしている操作対象の現在の使用者を登録しておくものである．UHA の操作権管理機能は OHA の使用者テーブルによって操作権取得の可否を判断し，また OHA の制御系状態確認機能によって操作対象が現在アクセス可能かどうかチェックする．操作権取得可能であれば UHA は OHA の使用者テーブルに自身がホストする操作員を登録し，操作権を取得したことを遠隔操作ソフトウェアに通知する．操作権解放は，逆に，使用者テーブルへの登録を解除することによって行う．

```
<STP:Message xmlns:STP="Some-URI">
  <STP:Body usage="usage 値"
            opcode=" チケット">
    .........
  </STP:Body>
</STP:Message>
```

図 10 STP メッセージ基本形
Fig. 10 Basic form of the STP message.

操作コマンドの実行は，操作員認証，権限，操作権所有のチェックを通過した後，OHA の制御系状態確認機能によって操作対象へのアクセスの最終チェックを行い，操作対象通信機能によって操作コマンドが擬似プロセスコンピュータに送信される．

実装した XML メッセージの基本形を**図 10** に示す．Body タグの属性値として，usage には**表 1** に列挙する usage 値が，opcode には STP サーバによって発行

表 1 STP メッセージ内の要素情報
Table 1 Element information in the STP messages.

usage 値	利用目的	内部タグ名	内容
LOGIN	操作員認証	username	ユーザ名
		authent-icator	操作員認証子
		seed	ディジタル署名対象の乱数
ACQUIRE	操作権取得	acquire	属性値として target（操作対象），allow（操作権取得フラグ．デフォルト 0 で操作権取得成功時に 1），query（譲渡要求フラグ．デフォルト 0 で譲渡要求の場合に 1），queue（待ち行列投入フラグ．デフォルト 0 で待ち行列投入を要求する場合に 1）を設定
CALL	操作	call	操作コマンド．target 属性によって操作対象指定．
RELEASE	操作権解放	release	target 属性によって操作対象指定
DELEGATE	操作権譲渡	delegate	属性値として target（操作対象），allow（譲渡同意フラグ．デフォルトは 0 で同意のとき 1），time-limit（同意/拒否判断の制限時間）を設定
LOGOUT	ログアウト	—	—

されるチケットが格納される．usage 値は利用目的を指し，usage 値の指定の仕方によって Body の子エレメントで利用するタグおよび記載内容が表 1 に示すものを利用するようにした．

6. 脆弱性分析

前章まで STP の仕組みと実現可能性について議論した．STP を用いて操作対象を保護する機能については述べたが，安全性を検証するためには STP 自体への能動的な攻撃に対して STP が脆弱か否かを分析する必要がある．

制御系システムではつねにフェールセーフに基づいてシステム設計がされることから，脆弱性分析についても前提条件がくずれた状態でも安全な状態でいることができるかという観点で分析を行うことにする．ユーザ認証についてはパスワードや暗号など既知の脆弱性分析結果に従うため，ここでは STP に特有な部分のみについて考察する．STP を危殆化するためには，(a) チケットを入手し，(b) SSL セッションを含めた STP セッションを利用する必要がある．そこで，これらの条件のうち，どちらか一方が成立した場合にも安全性を保っていられるかどうか分析した．加えて，両方の条件が成立してしまった場合の緊急時対応方法についても考察した．

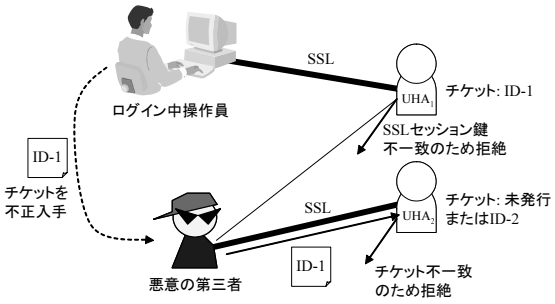

図 11 チケット漏洩によるなりすまし攻撃
Fig. 11 Masquerade attack derived from ticket disclosure.

(1) **チケット不正利用によるなりすまし**

正当な操作員が STP サーバにアクセスしているときに，当該セッションで用いているチケットを悪意の第三者が不正に入手することができたと仮定する．このチケットを用いて不正に操作権を取得したり，コマンドを送信したりする脅威を考える．

別のユーザが新たな接続を試みる場合には，新たな UHA が立ち上がりホストすることになり，新たな認証を求め，チケットも新しいものが発行されるために，別の操作員のチケット（ID-1）を新規の UHA（チケット未発行または ID-2）に提示しても無効とされる（**図 11**）．プロトタイプシステムにおいても，この攻撃を仮想的に実現するために，ログインした後に STP メッセージの内容を変更可能とするユーザインタフェース（**図 12**）を実験用に設けた．ログイン中の別のユーザのチケットを用いてメッセージを送信した場合には，チケット不一致によってアクセス拒否することを確認した．

チケットの不正利用を行うには，チケットの現所有者にホストしている UHA に対してメッセージを投げる必要がある（図 11）．他の操作員にホストする UHA に接続するには SSL セッションをハイジャックする必要があり，事実上困難である．

(2) **操作端末を踏み台としたなりすまし**

遠隔操作端末を何らかの理由によって乗っ取ることに成功した場合，これを踏み台として STP サーバに不正アクセスを試みる脅威が可能となる．しかし，単

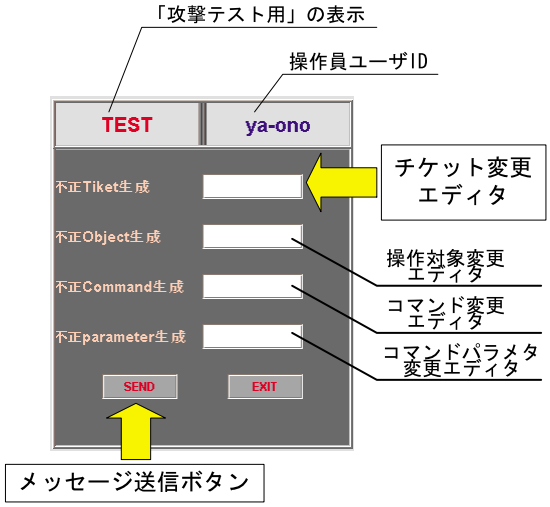

図 12 仮想攻撃用ユーザインタフェース
Fig. 12 User interface for the virtual attack.

に乗っ取るだけでは認証に成功しないため UHA から正規のチケットを受け取ることができない．

正当な操作員が認証に成功した STP セッションを第三者が乗っ取っり，接続中の通信路を利用して不正なコマンドを送信可能な状態になったと仮定する．しかし，この場合にもチケットを推測する必要がある．チケット長が 16 バイトの場合には，チケットの値としておよそ 3.4×10^{38} 通り（1.08×10^{23} [MIPS×Year]）の場合の数があり，推測することは事実上困難である．このバイト長が短い場合には，短さに応じた脆弱性が顕在化する．チケット未更新期間がチケット解読期間よりも長い場合にも脆弱性が顕在化する．これに対しては，長期間利用しないときにはログアウトする運用を実施するなどして対処する．

(3) **緊急時対応**

いったん操作権を保持した後，解放を忘れてそのまま操作権を放置してしまい，他の操作員が操作不能となる脅威が考えられる．操作権を保持した状態で回線障害などが起こり通信不能な場合にも同様な状況が発生しうる．この脅威に対しては STP サーバ管理者が操作権を強制解放することで対処する．

さらに，万が一操作員が第三者によってなりすまされた場合に対する救済措置として，STP サーバ管理者は操作員を強制ログアウトさせることも可能としている．強制ログアウトさせた後は，再ログインを防ぐために，なりすまされたユーザアカウントを一時的に抹消する運用も必要である．

7. ま と め

本論文では IP ネットワークを経由して遠隔から制御系システムを操作する際のセキュリティを確保する制御系ファイアウォールへのアクセスプロトコルとしてセキュア遠隔操作プロトコル STP を提案した．リモコンのメタファとして考えられる「操作権」という概念を導入し，譲渡可能な操作権によって柔軟な排他制御を実現した．また，STP サーバ内のエージェントによってアクセス制御を行うシステムとした．また，プロトタイプによる実証実験により実現可能性を確認し，脆弱性分析によって STP 自身への脅威に対する対策状況を確認した．ただし，アプリケーションプロトコルであるため，基盤として利用している情報システムのセキュリティ確保が前提となる．

STP は基本的には操作権を管理するフレームワークを提供しているものなので，今後は，認証と静的アクセス制御の部分には SAML や XACML[8),9)]，ベースとする転送プロトコルとして SOAP（Simple Object Access Protocol）[7)]の採用を検討する等して，標準化動向に合わせた仕様検討も進めていく．また，安全性に加え信頼性の確保も含めたトータルシステムとしての検討を進めていく．さらに，権利だけでなく業務の引継ぎも含めた譲渡の検討も必要と考える．

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はじめ，関係会社・関係各位のご支援に感謝する．

参 考 文 献

1) 長谷川義朗，江幡良雄，林 秀樹：イントラネット応用電力系統監視制御システム，東芝レビュー，Vol.54, No.6, pp.30–33 (1999).
2) 佐藤正行，中道功二，井上勝行：公共プラント Web 応用監視制御システム，三菱電機技報，Vol.74, No.12, pp.7–10 (2000).
3) 梅田富雄：プラントネットワークセキュリティの充実，水道協会雑誌，Vol.70, No.10, pp.55–62 (2001).
4) 情報処理振興事業協会：「重要インフラセキュリティ対策事業」関連論文集—サイバー・クライシス対策セミナー資料 (2001).
5) Cheswick, W.R. and Bellovin, S.M.: *Firewalls and Internet Security*, Addison-Wesley Professional Computing Series (1994).
6) 青山幹雄：ソフトウェアサービス技術へのいざな

い，情報処理，Vol.42, No.9, pp.857–862 (2001).
7) 高瀬俊郎：SOAP，情報処理，Vol.42, No.9, pp.863–869 (2001).
8) DeJesus, E.X.: SAML Brings Security to XML, *XML Magazine*, Vol.3, No.1, pp.35–37 (2002).
9) Fontana, J.: Top Web Services Worry: Security, *Network World*, Vol.19, No.3, pp.1–10 (2002).
10) 吉田貴英，浅野孝夫：分散システムにおけるプライオリティ付き相互排他制御，情報処理学会研究報告 1998-AL-61, Vol.1998, No.28, pp.55–62 (1998).
11) 古谷雅年，瀬古沢照治，加藤博光：リモコンアプレットとプラントファイアウォール，平成 11 年電気学会産業応用部門大会講演論文集（3），pp.551–554 (1999).
12) 加藤博光，玉野真紀，古谷雅年，宮尾 健，金子茂則，中野利彦：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，情報処理学会研究報告 2001-CSEC-13, Vol.2001, No.53, pp.25–30 (2001).
13) Kato, H., Furuya, M., Tamano-Mori, M., Kaneko, S. and Nakano: Risk Analysis and Secure Protocol Design for WWW-based Remote Control with Operation-Privilege Management, *Proc. SMC2001 Conference*, Tucson, Arizona, pp.1107–1112, IEEE (2001).
14) Munson, M., et al.: Flexible Internetworking of Devices and Controls, *Proc. IECON '99*, San Jose, California, pp.1139–1145, IEEE Industrial Electronics Society (1999).
15) Dierks, T. and Allen, C.: The TLS Protocol Version 1.0, RFC2246, The Internet Engineering Task Force (1999).
16) Kato, H., Furuya, M., Tamano-Mori, M., Kaneko, S. and Nakano: Secure Communication Protocol for the Internet-based Teleoperation, *INTERMAC2001 Joint Technical Conference*, Tokyo, Japan, ISA, JEMIMA, and SICE (2001). CD-ROM distribution.
17) Funabashi, M., et al.: Development of Open Service Collaborative Platform for Coming ECs by International Joint Efforts, *Proc. SSGRR 2000 International Conference on Advances in Infrastructure for Electronic Business, Science, and Education on the Internet* (2000). CD-ROM distribution.

(平成 13 年 11 月 30 日受付)
(平成 14 年 6 月 4 日採録)

推 薦 文

本論文はプラント制御系システムへの遠隔操作に関するアクセス制御機構を提案するものであり，「操作権」という概念を導入し，これを譲渡する場合も考慮することを特徴とする．『プラント制御系システム』という，これまであまり議論されていないシステムを対象としており，非常に興味深い．また，アクセス権限とは独立に「操作権」という権利を導入することによって，柔軟な排他制御を実現していることも評価できる．

（CSEC 研究会主査 佐々木 良一）

加藤 博光（正会員）

昭和 45 年生．平成 7 年東京大学大学院工学系研究科航空宇宙工学専攻修士課程修了．同年（株）日立製作所入社．現在，同システム開発研究所にて情報制御システムの運用監視制御，リスク管理の研究開発に従事．平成 11 年山下記念研究賞，平成 12 年計測自動制御学会技術賞受賞．計測自動制御学会，電気学会各会員．

玉野 真紀（正会員）

昭和 42 年生．平成 3 年大阪府立大学工学部化学工学科卒業．同年（株）日立製作所入社．現在，同システム開発研究所にてヒューマンインタフェース，情報制御システムセキュリティの研究開発に従事．

古谷 雅年（正会員）

昭和 41 年生．平成 2 年慶應義塾大学大学院理工学研究科修士課程修了．同年（株）日立製作所入社．現在，同システム開発研究所にて情報制御システム・公共情報システムの研究開発に従事．計測自動制御学会会員．

宮尾 健

昭和 38 年生．昭和 62 年東京大学工学部電子工学科卒業．同年（株）日立製作所入社．現在，同情報制御システム事業部にて制御用計算機およびセキュリティ関連の開発に従事．