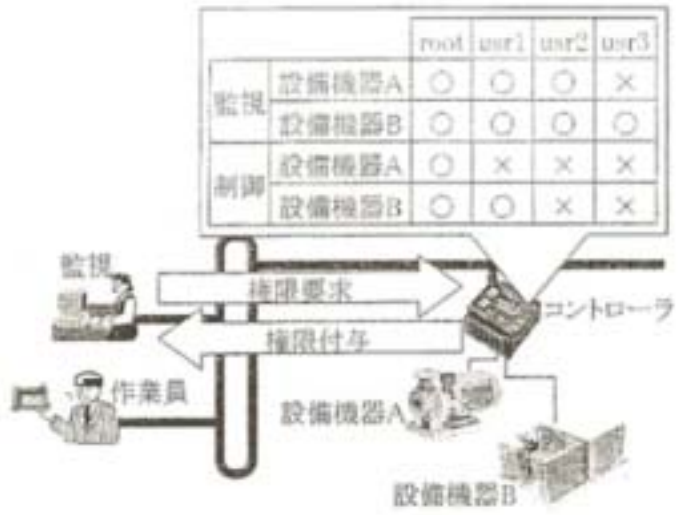
【技術分類】２－７－１　要素・基盤技術／安全・信頼性技術／セキュリティ
【技術名称】２－７－１－１　監視制御操作の権限管理システム

【技術内容】
プラント制御システムにおいては、コントローラなどの設備端末が専用ネットワークを介して設備装置に接続されている。生産管理部門は、イントラネットを介して、コントローラから機器監視データを取得する。逆に、生産管理部門からの制御指令、スケジュール情報は、イントラネットを介してコントローラに通知される。これらの情報は、コントローラにおいて設備機器への制御データに置き換えられる。
こうしたプラントの情報化が進むと共に、セキュリティ対策が大きな課題となっている。プラントの監視･制御システムのセキュリティを考える場合､操作権と監視権の取り扱いが重要な観点となる。
操作権の保護は、権限を有しない作業員が違法に設備機器を操作したり、操作を妨害したりすることを防ぐことである。監視権の保護は、製造現場ノウハウなど企業秘密の漏洩を防ぐことであり、特に無線通信技術の導入にともなう情報漏洩防止技術が重要である。

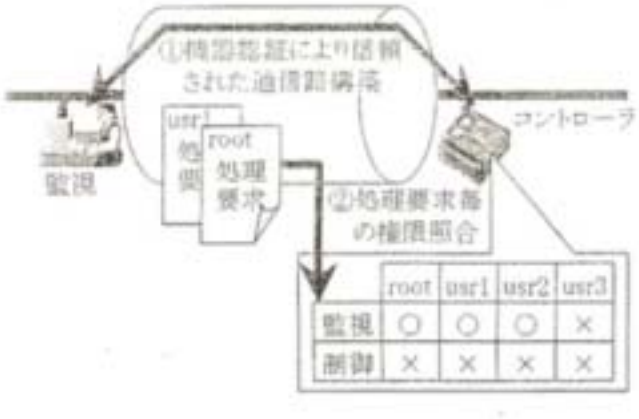
図１に示すシステムは、コントローラが操作権および監視権を管理するセキュリティアーキテクチャに関するものである。コントローラは、正当と認められた作業員と機器に権限付与を行う。
権限付与は、処理単位で行う場合には、受信した個々の処理要求に対してそれぞれ正当性を検証して正当と判断した場合に処理要求を受け付ける。機器単位で行う場合には、機器との通信開始時に、その機器の正当性を検証（認証）する。正当であると判断すれば、以降、その機器からの処理要求は正当なものとみなされる。
処理単位での認証技術として、XML デジタル署名、XML 暗号などの技術を採用したものがある。現状では、処理単位での認証は計算処理の負荷が大きく、リアルタイム性を保証することが難しくなるため、認証と権限付与とを分離する方法が提案されている（図２参照)。

【図１】コントローラによる権限管理システム



出典：「計測制御ネットワークのセキュリティフレームワークの考察」,「計測と制御 Vol.44　No.6」, 2005 年 6 月，日立製作所 斉藤雅彦著,（社）計測自動制御学会発行，407－410 頁　2　コントローラを権限管理主体とする方法

【図２】認証と権限付与の分離



出典：「計測制御ネットワークのセキュリティフレームワークの考察」,「計測と制御 Vol.44　No.6」, 2005 年 6 月，日立製作所 斉藤雅彦著,（社）計測自動制御学会発行，407－410 頁　3　認証と権限付与の分離

【出典／参考資料】
出典：「計測制御ネットワークのセキュリティフレームワークの考察」,「計測と制御 Vol.44　No.6」, 2005 年 6 月，日立製作所 斉藤雅彦著,（社）計測自動制御学会発行，407－410 頁

【技術分類】２－７－1　要素・基盤技術／安全・信頼性技術／セキュリティ
【技術名称】２－７－１－２　インターネットの不正アクセス模擬試験技術

【技術内容】

インターネット上での、擬似のサービス要求を大量に送信して、サービスを提供するサーバに過剰負荷を与え、OS やアプリケーションの脆弱性をついてシステムハングアップをさせる DoS（Denial of Service）[1]攻撃が、ネットワークセキュリティ上の脅威となっている。また、分散環境下において、DoS 攻撃を多数のコンピュータから同時に行う DDoS（Distributed Denial of Service）[2]攻撃も増えてきており、セキュリティの確保がより難しくなってきている。

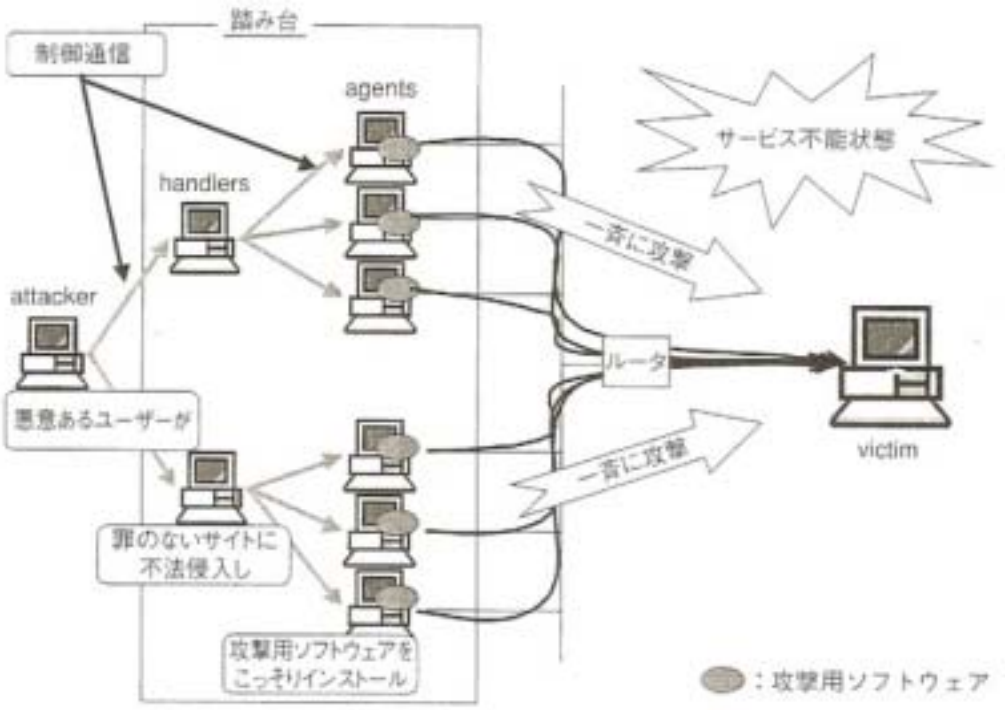
図 1 に示すように、DDoS 攻撃では、Attacker と呼ばれる悪意のあるユーザが、ネット上のセキュリティの脆弱なコンピュータサーバに不正侵入して攻撃ソフトを組み込む。不正侵入されたコンピュータは Attacker の踏み台となって、攻撃対象のコンピュータに、一斉にサービス要求を行い、サービス不能状態に落とし込める。

このような攻撃は、一度に多数の相手からの攻撃を受けるため、不正アクセスが行われているコンピュータを一つ一つ突き止め停止することは難しい。また、Attacker において、コンピュータを識別する IP アドレスが改ざんされている場合は、ほとんどの場合で特定が困難になる。

プラントのネットワークシステムをオープン化するとともに安全を確保するためには、こうしたサイバーセキュリティ上の脅威に対する対策を講じる必要がある。そのためには、ネットワーク上の脅威に対するシステムの脆弱性の把握が、まず必要になってくる。

図２には、このような DDoS 攻撃を模擬し、システムの脆弱性を検証するための実験システムを示した。このシステムは、一台の PC において、管理デーモン[3]が複数の攻撃サーバの役割を担うエージェントを作成し、一斉攻撃を行う仕組みをもつものである。

【図１】DDoS 攻撃の仕組み



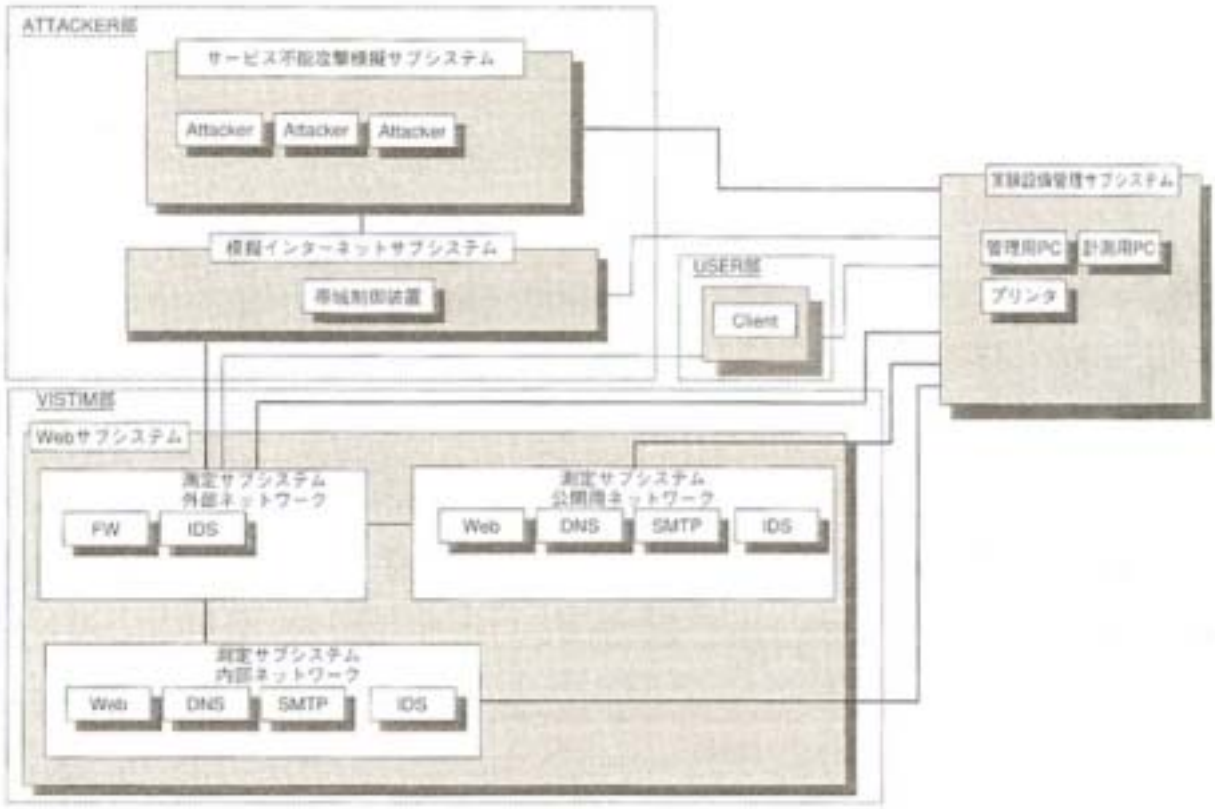
[1] Denial of Services の略。相手のコンピュータやルータなどに不正なデータを送信して使用不能にさせたり、トラフィックを増大させてネットワークを麻痺させる攻撃。

[2] （分散）Distributed Denial of Service の略。DoS を複数のノードからしかけるもの。

[3] サーバ上の常駐プログラムのこと。

出典：「インターネット不正アクセス状況を再現し対処方法を検討する DDoS Attack シミュレータ」，「オートメーション Vol.47 No.3」，2002 年 3 月，横河電機 永島秀己著，日刊工業新聞社発行，63‐69 頁　1　DDoS の仕組み

【図２】DDoS 攻撃のエージェントによるシミュレーション



出典：「インターネット不正アクセス状況を再現し対処方法を検討する DDoS Attack シミュレータ」，「オートメーション Vol.47 No.3」，2002 年 3 月，横河電機 永島秀己著，日刊工業新聞社発行，63‐69 頁　7　不正アクセス模擬実験システム

【出典／参考資料】
「インターネット不正アクセス状況を再現し対処方法を検討する DDoS Attack シミュレータ」，「オートメーション Vol.47 No.3」，2002 年 3 月，横河電機 永島秀己著，日刊工業新聞社発行，63‐69 頁

【技術分類】２－７－１　要素・基盤技術／安全・信頼性技術／セキュリティ
【技術名称】２－７－１－３　ファイアウォールを通過する遠隔制御・監視技術

【技術内容】

監視対象となる設備装置が多数に及ぶ場合や場所が離れた複数のプラントを監視する場合、人手による巡回方式の保守・点検作業では、リアルタイムでのデータ収集が難しいという問題が生じる。

そこで、ネットワークを利用してデータ収集を自動化し、収集データのリアルタイム性と同時性を確保する方法が開発されている。監視データをインターネットで配信することで、オフィスや自宅のパソコンからリアルタイムで設備装置の稼動状態が監視できるようになれば、データ加工等の作業効率が大きく改善される。

これまで、ネットワークを通じて設備装置を監視するシステムの多くは、イントラネット上のシステムとして構築されてきた。イントラネットとインターネットの間には、セキュリティのためにファイアウォールが設置されているが、ファイアウォールは、通信フレームを通過させる方向を固定化し、通信プロトコル（ポート番号[4]）を制限するため、シリアル通信を行う設備装置の場合、アクセスが制限されてきた。

そこで、ファイアウォールを越えて通信することができる HTTP プロトコルを利用して制御・監視機能を実現するために、シリアル通信機能をもつ設備装置の Web 対応化を図るアダプタ装置が開発されてきた。以下に示すのは、このアダプタ装置を使用し、HTTP プロトコルを利用して、ファイアウォールを越えた遠隔監視システムを構築するための基盤技術に関するものである。

図１には、イントラネット内の制御装置に、インターネット上の管理サーバからファイウォールを越えてアクセスする方法を示した。図 2 には、その逆に、インターネット上の制御装置に、イントラネット内の管理サーバからファイアウォールを越えてアクセスする方法を示した。

HTTP プロトコルは、ファイアウォールの内側から外側へのパケット通過が許可されている。ここでは、HTTP プロトコルの POST メソッド[5]を利用してインターネット上の管理サーバ（制御装置）からイントラネット上（ファイアウォールの内側）の制御装置（管理サーバ）にアクセスする方法を示す。それぞれのアクセス方法は以下のとおりである。

・ファイアウォール外のサーバからファイアウォール内の制御装置へのアクセス（図 1 参照）

アダプタ装置から、インターネット上の管理サーバに定期的に HTTP リクエストを送信する。このとき管理サーバから HTTP リクエストに対するレスポンスパケットがアダプタ装置に返されるが、このパケットに管理サーバからのコマンドをのせることで、ファイアウォール内の制御装置に対し制御・監視処理を実行させることができる。アダプタからの HTTP リクエストを送る周期を短くすることで、見かけ上は、管理サーバからのリアルタイムのファイアウォールを越えた制御・監視ができるようになる。

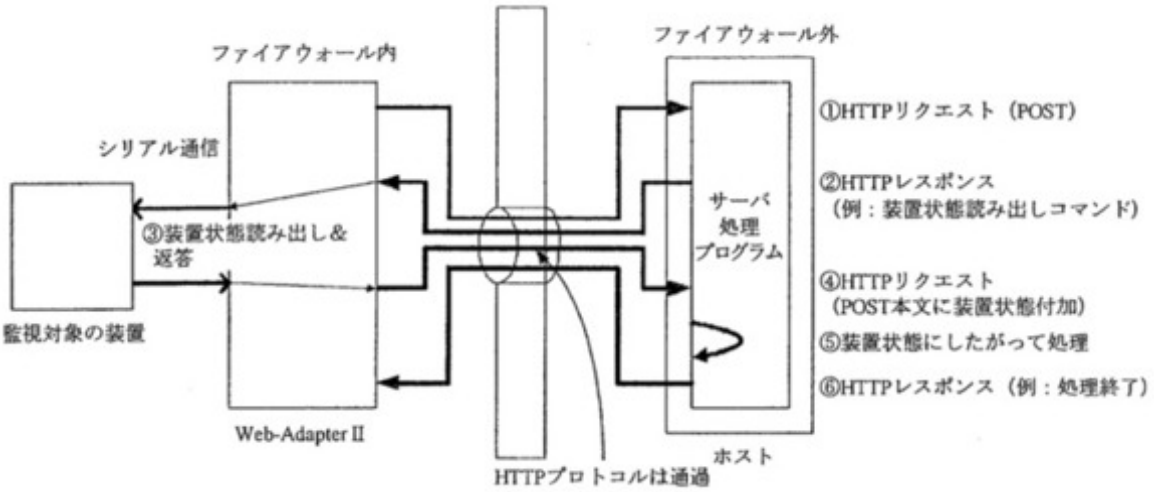
・ファイアウォール外の制御装置にファイアウォール内のサーバからアクセス（図 2 参照）

アダプタ装置は、HTTP の POST メソッドによるリクエストパケットをシリアル通信に流す機能をもつ。また、シリアル通信からアダプタ装置に流されたデータを HTTP のレスポンスパケットとして返す機能をもつ。ファイアウォールは HTTP プロトコルの通過を許可するので、これを利用して、インターネット上の制御装置にファイアウォール越しでイントラネットの管理サーバからアクセスすることができる。

4　インターネットで複数の相手と同時に接続を行なうための IP アドレスの下に設けられた接続先を識別するための番号。IP アドレスとポートを組み合わせたネットワークアドレスを「ソケット」と呼び、実際にはデータの送受信はソケット単位で行われている。

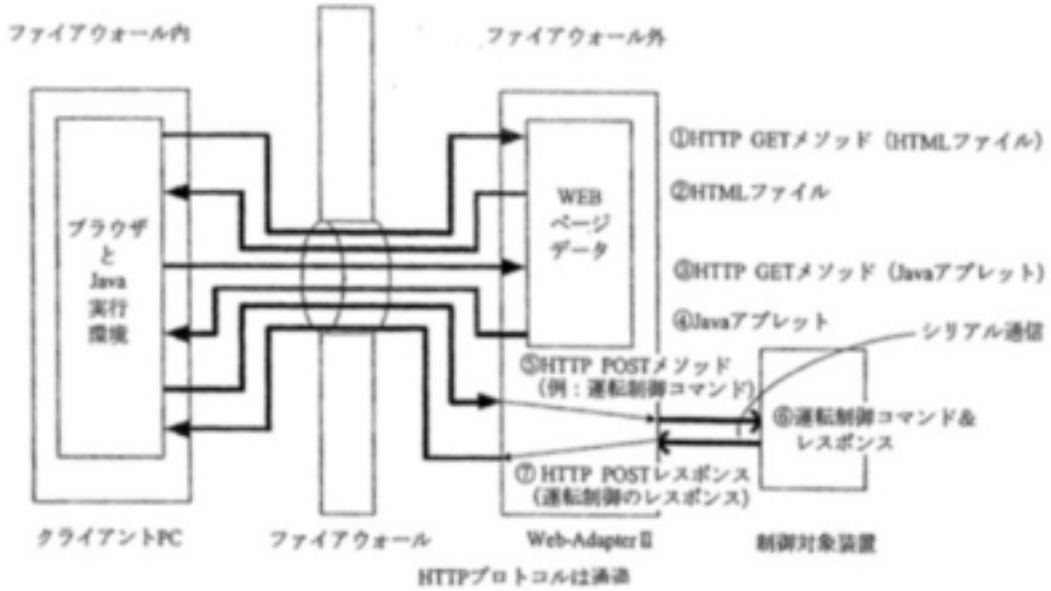
5　HTTP（Hyper Text Transfer Protocol）で利用されるデータの受け渡しの方法の一つ。

【図１】インターネット上の管理サーバからファイアウォール内の制御装置にアクセスする手順



出典：「ファイアウォールを越えるリモート監視技術」,「計装 Vol.45 No.1」, 2002 年 1 月, 山武 高橋誠著, 工業技術社発行, 61-64 頁　2　ファイアウォール外のホストからファイアウォール内の「Web-AdapterII」にアクセスする手順

【図２】ファイアウォール内の管理サーバからインターネット上の制御装置にアクセスする手順



出典：「ファイアウォールを越えるリモート監視技術」,「計装 Vol.45 No.1」, 2002 年 1 月, 山武 高橋誠著, 工業技術社発行, 61-64 頁　3　ファイアウォール内のクライアント PC からファイアウォール外の「Web-AdapterII」にアクセスする手順

「Java」：サン・マイクロシステムズ・インコーポレーテッド の登録商標

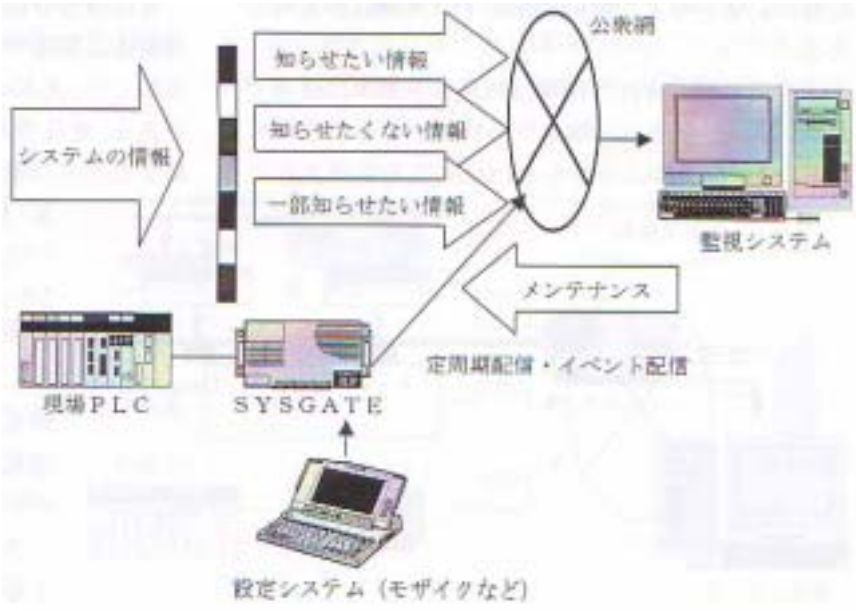
【出典／参考資料】

「ファイアウォールを越えるリモート監視技術」,「計装 Vol.45 No.1」, 2002 年 1 月, 山武 高橋誠著, 工業技術社発行, 61-64 頁　（http://www.ice-keiso.co.jp）

【技術分類】２－７－1　要素・基盤技術／安全・信頼性技術／セキュリティ
【技術名称】２－７－１－４　プラント設備データの漏洩防止技術

【技術内容】
インターネット等の公衆ネットワーク回線網を利用した遠隔監視システムでは、情報の暗号化や専用回線（VPN；Virtual Private Network）化を図り、セキュリティ対策を行っているが、外部接続によるプラントシステムの操作は、重要なデータの漏洩の危険性をともなう。
プラントシステムの情報には、外部への公開が可能な情報、外部には非公開にすべき情報、部分公開が可能な情報が存在する。現状においては、システム情報の公開の可否を差別化していないために、データの中にあまり重要でないものも含まれ、必要な情報が適切に選別できない状況が存在している。
図１には、現場にある設備機器データを収集する仕組みと収集したデータを安全な情報に変換する配信システムを示す。製造情報などの知られたくないデータを保護するために、設備側が送りたい情報のみを配信する仕組みや、送りたい情報に任意の名前を付与して本来の名称を隠蔽する仕組みで、情報の安全化を図っている。
監視側にとって重要なデータを選別し、不要なデータを多く流さないフィルタリング機能としての役割を果たすこのようなシステムを導入することにより、現場設備をリモートから、安全かつ効率的に保守することが可能になる。

【図１】システムの基本構成：モザイク情報の仕組み



出典：「情報セキュリティからみたリモートエンジニアリングの進め方「SYSGATE」」，「計装 Vol.46 No.6」，2003 年 5 月，阪神サイロ 久保田哲、鹿間恵一郎著，工業技術社発行，35－38 頁　1
「SYSGATE」基本構成：モザイク情報の仕組み

「SYSGATE」：オムロン株式会社の登録商標

【出典／参考資料】
「情報セキュリティからみたリモートエンジニアリングの進め方「SYSGATE」」，「計装 Vol.46 No.6」，2003 年 5 月，阪神サイロ 久保田哲、鹿間恵一郎著，工業技術社発行，35－38 頁
（http://www.ice-keiso.co.jp）

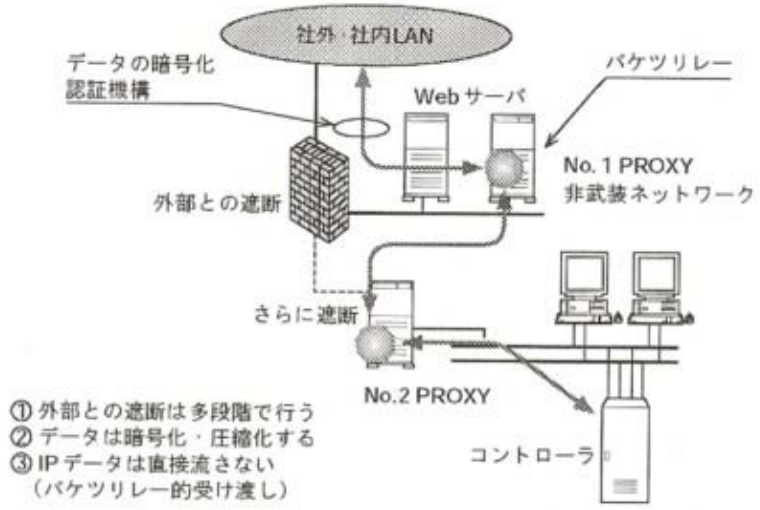
【技術分類】２－７－１　要素・基盤技術／安全・信頼性技術／セキュリティ
【技術名称】２－７－１－５　代理サーバを利用したセキュア通信技術

【技術内容】
ネットワーク技術の進歩によって広域な通信インフラを利用した遠隔監視システムの実用化が進んでいるが、複数に分散するプラント設備を、インターネット網を活用した IP 技術によって遠隔監視する場合、セキュリティ管理と監視サーバの同時性確保の問題が存在する。

遠隔監視に使うコンピュータ通信回線を社外のネットワーク環境から切り離すことができたとしても、社内 LAN やオフィスのネットワークに接続してこれを利用する場合、セキュリティ管理が必要になる。オフィス LAN とプラントの制御ネットワークを接続する場合、ネットワークの間に IP パケットの通過を塞ぐファイアウォールが設けられる。しかしながら、ファイアウォールは全ての IP パケットを遮断するものではなく、通信を行うために入り口となる穴（ポート）を制限するものである。このため、通信を許可したポートから不正アクセスが行われる可能性がある。

このような危険性を回避するために、本システムでは、図１に示すように、制御ネットワークに外部から侵入する IP パケットを中継サーバのソフトウェア（Proxy[6]）で一旦すべて受信し、バケツリレー的にデータの中継を処理するシステムを実現している。バケツリレーを仲介する Proxy は何重にも介在させることができる。Proxy は、認証機能を有し、権限ユーザ以外の操作を制限する。また、プロセス信号を含むすべてのリアルタイム信号については、アプリケーション通信を圧縮・暗号化し、盗聴や改ざんを防止する。

【図１】Proxy サーバの導入によるセキュリティ管理を行ったシステムの例



出典:「発電設備における遠隔監視操作システムの事例」,「三菱重工技報 Vol.40 No.4」, 2003 年 7 月, 三菱重工 森本賢一、高倉朋子、梅田圭次郎著，三菱重工技報社発行，230‐232 頁　3　外部との遮断

【出典／参考資料】
「発電設備における遠隔監視操作システムの事例」,「三菱重工技報 Vol.40 No.4」，2003 年 7 月，三菱重工 森本賢一、高倉朋子、梅田圭次郎著，三菱重工技報社発行，230‐232 頁

6　企業などの内部ネットワークとインターネットの境にあって、直接インターネットに接続できない内部ネットワークのコンピュータに代わって、インターネットとの接続を代理するコンピュータサーバのこと。