セキュア・ゲートウェイ

山本　正　　齋藤　彰宏

近年，不正侵入，情報漏洩，コンピュータウィルスなど，セキュリティの被害がメディアを賑わせており，セキュリティ対策がますます重要になっている。とりわけ金融機関では，セキュリティの被害が発生し信用不安を引き起こしてしまえば莫大な損失につながりかねない。そのため，金融機関は外部との接続に関して，極めて慎重に対応しており，内部の基幹ネットワークと外部ネットワークを分離して，セキュリティを確保している例が非常に多い。

一方，保険の銀行窓口販売や証券仲介業の解禁などの規制緩和により，金融機関が外部の金融商品を販売する機運が高まっている。そのためには金融機関と外部の企業が何らかの手段で連携する必要がある。連携の手段としては，電話，FAX，郵便などの方法があるが，効率化の面でネットワーク接続になると考えられる。

沖電気では，セキュリティ確保と外部ネットワーク接続という相反するニーズに応えるため，金融機関内のネットワークについて，セキュリティをレベル分けし，レベルごとにセキュリティポリシーを定めるセキュアゾーンモデルを考案した[1) 2)]。**図1**にセキュアゾーンモデルを示す。この方式を実現するためには，ネットワーク境界に高度なセキュリティ機能を持つゲートウェイが必要である。これをセキュア・ゲートウェイと呼ぶ。

本稿では，セキュア・ゲートウェイの要件と実現方式について述べる。

セキュア・ゲートウェイの要件

セキュア・ゲートウェイに求められる要件を**図2**に示す。以下の3つの機能が必要である。

(a) アクセス制御機能
(b) データ内容の検査機能
(c) 脆弱性対策機能

以下に詳細を述べる。

(a) アクセス制御機能

許可されたアクセスのみを通過させる機能である。この機能は，一般的なファイアウォールで実現されている。

アクセス制御は，パケットのIPヘッダやTCP（UDP）ヘッダに含まれる宛先アドレス，送信元アドレス，宛先ポート，送信元ポートなどの情報を元に行う。

アクセス制御は，アドレスなどの情報を元にパケットの通過を制御するのみであり，データの中身にウィルスなどが含まれていないかどうかはチェックしない。

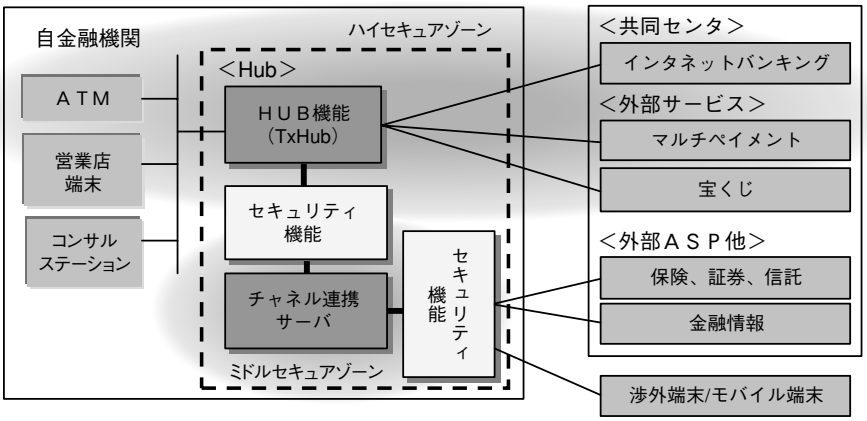


図1　セキュアゾーンモデル

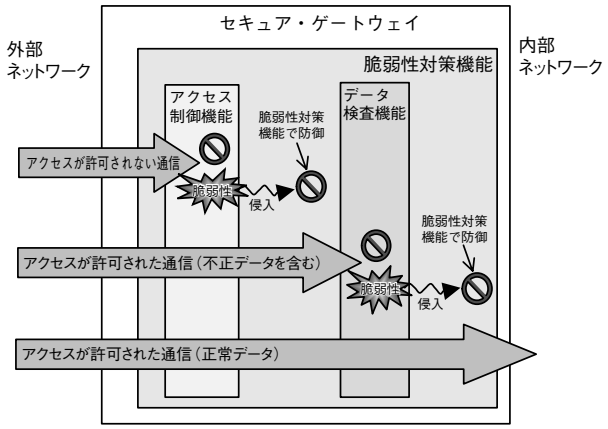


図2　セキュア・ゲートウェイの要件

(b) データ内容の検査機能

データの中身にウィルスや攻撃コードが含まれていないかどうかを検査する機能である。この機能は，IDS（Intrusion Detection System：侵入検知システム）技術を使ったIPS（Intrusion Prevention System：侵入防御システム）や，Webアプリケーション・ファイアウォール，アンチウィルス・ゲートウェイなどによって実現されている。

データ内容の検査手法は，攻撃の特徴情報に基づく不正検出（misuse detection）と，正常アクセスの情報に基づいて正常時と異なる異常データを検出する異常検出（anomaly detection）がある。

多くの製品では不正検出が採用されている。不正検出は，攻撃の特徴情報を保持するデータベースに無い攻撃は検出できないという課題がある。一方，異常検出では，事前に必要なものは正常な状態の情報であり，攻撃の特徴情報は必要としないので，データベースに無い未知の攻撃も検出できる。

既に，当社は異常検出により，未知の攻撃も防御できることを示した[3)]。

しかし，異常検出が全てのシステムで有効なわけではない。なぜならば，異常検出を用いるには，正常なデータ形式を定義する必要があるからである。たとえばブラウザで各種Webサイトを閲覧する場合は，多種多様なデータ形式が存在するため，正常データを定義することは現実的には困難である。一方，企業内に閉じたシステムや企業間連携システムの場合は，XMLなどでデータ形式が定義される傾向にあるので，異常検出が有効である。
セキュア・ゲートウェイでは，未知の攻撃も対応可能な異常検出技術を採用する。

(c) 脆弱性対策機能

機器の脆弱性が攻撃されて制御を奪われ，内部ネットワークへの侵入を許すことが無いようにする機能である。

この機能は，一般の製品では実現されておらず，脆弱性に対するパッチなどの運用でカバーする場合が多い。しかし，運用によるカバーでは，脆弱性が発見されてからパッチを当てるまでの間の攻撃に対応できないという課題がある。

一部の製品では，セキュリティ機能を強化したOSであるセキュアOSを採用することによって安全性を確保している。しかし，セキュアOS自体の脆弱性も報告されることがあるので万全ではない。

当社は，改善の余地が残されている機器の脆弱性対策機能について，ネットワーク的な対策を検討し，セキュアなゲートウェイを実現した。

機器の脆弱性が攻撃されて内部ネットワークが脅威にさらされる問題の要因は2つある。

① 攻撃を受けて制御が奪われたときに容易に反対側のネットワークにたどり着ける。
② ネットワークが良く知られたTCP/IPで構成されている。ネットワーク感染型ワームに見られるように，システムを踏み台にして内部のネットワークに侵入するような攻撃コードを容易に書くことができる。

そこで，我々は，独立したコンピュータ2台をTCP/IPではない特殊通信路で接続し，1つのゲートウェイとして動作させる方式を考えた。

この方式により，上で述べた2つの課題は，以下のように解決できる。

① 2台の構成なので，1台のコンピュータに侵入されても反対側のネットワークに到達できない。
② 2台のコンピュータをつなぐ通信路は非公開の独自プロトコルなので，特殊通信路を介した攻撃コードを書くことはできない。

セキュア・ゲートウェイの実現方式

図3に特殊通信路方式によるセキュア・ゲートウェイの構造を示す。各々のコンピュータには，外部と接続するTCP/IPインタフェースと，2台のコンピュータを接続する特殊通信路インタフェースを備える。特殊通信路は，たとえばIEEE1394などの物理メディア上で独自のプロトコルを実装することで実現できる。

TCP/IPネットワークの入出力部分には，パケットの通過を許可／拒否するアクセス制御モジュールがあり，ア

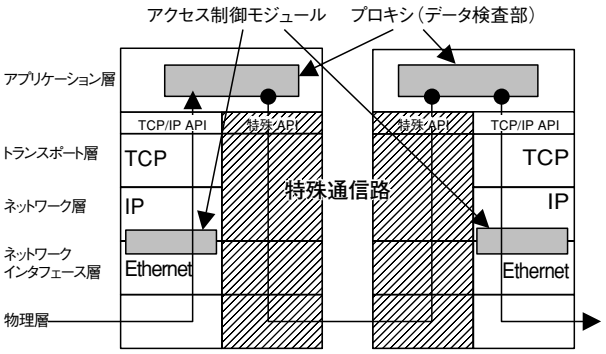


図3　セキュア・ゲートウェイの構成

プリケーション層には，データの検査とプロトコルの変換を行うプロキシ（データ検査部）を備えている。

このプロキシはアプリケーションプロトコルごとに用意する。HTTPをはじめ，FTPやtelnetなどさまざまなプロトコルのプロキシを用意することにより，各プロトコルのセキュア・ゲートウェイとして動作が可能となる。

セキュア・ゲートウェイの動作の仕組みは以下の通りである。

片方のコンピュータによって受信されたパケットは，アクセス制御モジュールによってアクセス制御され，その後プロキシで処理される。

プロキシはデータの検査を行ったあと，パケットを加工し特殊通信路を通してもう片方のコンピュータのプロキシへ向けて送信する。このとき，通信するデータ内容が定型データのみを扱う場合には，フォーマットを変換して送信を行う。受信側コンピュータのプロキシは，特殊通信路経由で受信したパケットを復元し，通常のTCP/IPの通信で目的のコンピュータへ送信する。

このようなメカニズムにより，セキュア・ゲートウェイを介した通信はあたかも通常のTCP/IPの通信であるかのように行われる。しかし，実際にはTCP/IPの通信はプロキシで終端されており，プロキシが対応していないプロトコルを使った通信は不可能である。

本方式では以下のような仕組みでセキュリティが確保される。

前述の要件で述べた3つの機能は，それぞれ，アクセス制御モジュール，プロキシのデータ検査，特殊通信路で実現されている。アクセス制御モジュールとプロキシのデータ検査によって，アクセスの許可された，正常なデータのみがセキュア・ゲートウェイを介して受け渡される。

万が一，アクセス制御モジュール，またはプロキシに脆弱性があったとしても，特殊通信路によってセキュリティが確保される。**図4**に，特殊通信路の効果を示す。セキュア・ゲートウェイでは，脆弱性をついた攻撃が成功したとしても，2台構成の特殊なプロトコルのため内部に侵入することはできない。

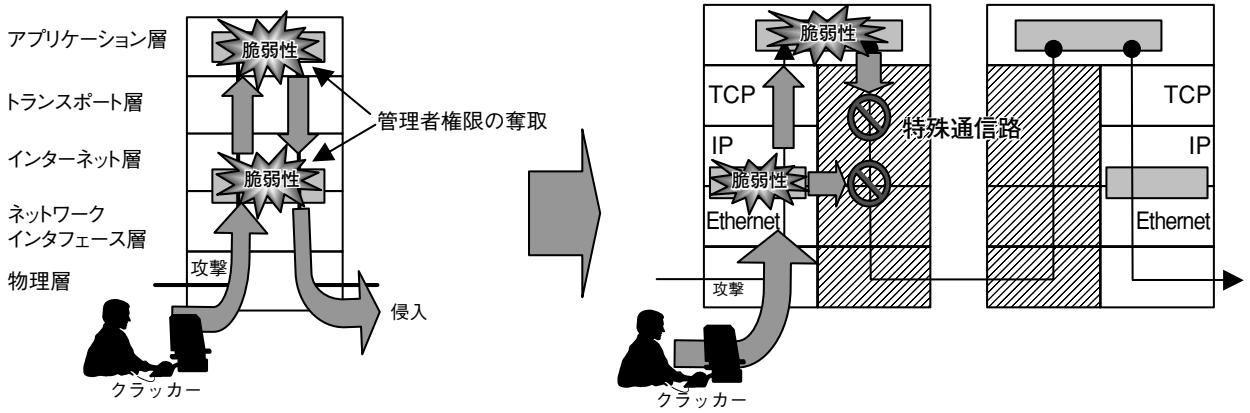
セキュア・ゲートウェイの適用例

この仕組みは，さまざまな用途に応用できる。以下に一例を示す。

（1）外部接続の例

冒頭で述べたように，金融機関の基幹ネットワークのセキュリティを保ちつつ外部のネットワークが接続できるようになり，ネットワークを介して外部の金融商品を販売するシステムを構築することが可能となる。

図5に保険や証券の窓口販売システムの例を示す。従来はセキュリティ対策のために，基幹ネットワークから切り離された窓口販売専用のPCを設置していた。セキュア・ゲートウェイを使用することにより，セキュリティの不



a)既存の製品　　b) セキュア・ゲートウェイ

図4　特殊通信路の効果

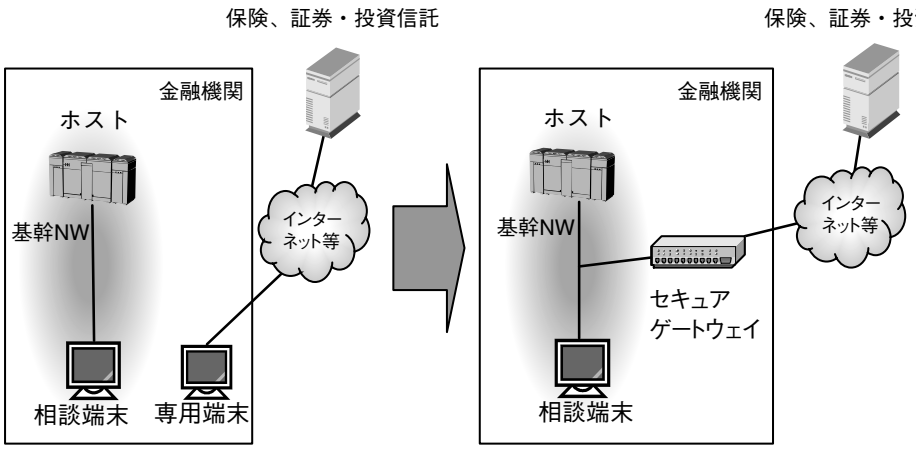


図5　外部接続の例

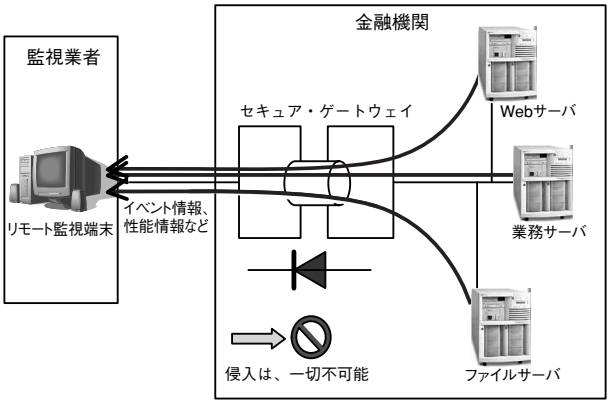


図6　リモート監視の例

安が解消され，基幹ネットワークと接続された既存の端末から，外部のサービスを利用することができる。これにより，事務の効率化や端末スペースの節約が期待できる。

(2) リモート監視

金融機関の基幹システムの機器やネットワークの運用監視は，従来であれば，専門の監視員がセンタに常駐し監視を行っていた。しかし，コスト削減のためSIベンダやMSP（Management Service Provider）が提供するリモート監視サービスのニーズが高まっている。しかし，金融機関においては，セキュリティの不安から，監視サービスの利用を躊躇する場合が多い。

セキュア・ゲートウェイにより，セキュリティの不安を解消し，安全なシステムを構築することが可能となる。

図6にリモート監視の例を示す。セキュア・ゲートウェイの特殊通信路を完全に片方向しかデータが流れない（一般にデータダイオード方式と呼ばれている）ようにし，特定の監視データのみを定期的に監視マネージャへ送信する。監視業者から金融機関へのアクセスはまったくできないため，不正侵入の不安は解消される。

ま と め

セキュア・ゲートウェイは，2台のコンピュータを特殊通信路で接続する仕組みにより，従来のファイアウォール製品などでは実現できないような非常に高いセキュリティを確保することができる。

金融機関では，セキュリティ上の不安から外部接続に対して非常に慎重であるが，外部接続のニーズは次第に高まっている。セキュア・ゲートウェイは金融機関のセキュリティの不安を解消し，外部接続を実現するために非常に有効な技術である。 ◆◆

■参考文献

1）新田哲二：“次世代金融サービスを実現するネットワークアーキテクチャ”，沖テクニカルレビュー191号，Vol69 No.3，pp.10–17，2002年7月
2）鈴木一義，広重克典：“次世代金融ネットワークソリューション”，沖テクニカルレビュー198号，Vol71 No.2，pp.10–13，2004年4月
3）露口和弘，橘喜胤，矢野達朗：“アプリケーション・ファイアウォールによるWebサーバの保護”，沖テクニカルレビュー191号，Vol.69 No.3，pp.76–79，2002年7月

●筆者紹介

山本正：Tadashi Yamamoto. 金融ソリューションカンパニー金融ソリューション開発本部ネットトランザクション開発部
齋藤彰宏：Akihiro Saito. 金融ソリューションカンパニー金融ソリューション開発本部ネットトランザクション開発部