インターネットを利用するECサイトのセキュリティと信頼性・可用性の実現方法

Example for Enabling Security, Reliability and Availability of B2C System using Internet

中島己範

要　約　インターネットの利用者数は驚異的な勢いで増え続けており，インターネットを利用した新しいビジネスも確実に増加している．店舗の展開など実世界に比べB2Cの分野は新規参入が容易であることなどから市場には多くのシステムが出現している．インターネットを利用したB2Cのシステムでは信頼性・可用性及びセキュリティ対策はどのシステムにおいても共通に検討しなければならない課題である．ここではインターネットを利用したチケット販売代理店システムの事例の中から信頼性・可用性対策及びセキュリティ確保の方法を紹介している．

Abstract　The number of Internet users is increasing with extraordinary speed, and new businesses using Internet services, especially B2C business, are increasing too. Compared with the real worlds, such as deployment of newly opened stores, it is easy for the new entrants to participate in the Internet business. B2C systems using Internet services commonly have the concerns for security, reliability and availability of their systems. This article introduces the Internet ticket selling system by the agent as the example for keeping the security, reliability and availability of the B2C system.

1. はじめに

インターネットの利用者数は2000年に約4千万に達し，現在も毎月数%を超える増加率を記録している．急激な利用者数の伸びの大部分は携帯電話(iモード, EZWeb, J-SKYなど）からの利用数増によるものと考えられるが，ダイヤルアップ，ADSL，CATVなどを利用した家庭からの利用者数も急激に増加の一途をたどっている（平成12年版通信白書によれば2005年には7670万に上ると予測されている)．

インターネットが普及し広く浸透することによって，インターネットを利用したビジネスが急速に発展しつつある．このビジネスの多くはインターネットが持つ視聴覚性と双方向性を活かした形態であり，いわゆる電子商取引（EC : Electronic Commerce）の中でも一般消費者を対象としたB-to-C（Business to Consumer＝B2C）の形態である．

インターネットを利用したビジネスの魅力の一つは短期間に少ない予算で簡単にビジネスを立ち上げることができ，運用する経費も少なくてすむ点にある．すなわち，サーバを立ち上げればインターネット空間上に24時間365日何時でもオープンしている店舗を構築することが可能となる．実際の店舗を構える必要もなく，自らが注文データを入力する端末を準備する必要もなければ，データを入力するオペレータも不要である．これらはすべて顧客が準備してくれるからである．視点を変えてみると，

インターネットビジネスではビジネスに対する経験，基盤，地盤がなくても新規参入が容易であるともいえる．このようにインターネットを利用するビジネスは，既存のビジネスに対する構造改革，構造破壊をもたらすものであり異業種企業との提携による新規ビジネスの展開や，同業他社つまり競合先との共同ビジネスの展開など今まで考えられなかったようなビジネススキームを実現させ始めている．

さて，B2Cサイトの構築においては技術的に考慮しなければならない課題もある．特に，インターネット上でクレジットカードなどの情報や個人情報などを扱うことが多いため暗号化や不正アクセス防止などのセキュリティ対策や24時間365日のサービス提供など運用時間を考慮した可用性対策は多くのサイトに共通な課題といえる．ここでは，インターネットを利用したB2Cビジネスの一形態であるチケットの販売代理店システムのネットワークインフラストラクチャ構築事例から，ネットワークインフラストラクチャの信頼性・可用性及びセキュリティへの対応を中心に紹介する．

2. システムの概要

ここに紹介するシステムは一般消費者を対象にしたインターネットでのチケット予約販売の代理店システムである．このシステムは，実際のチケットを販売する複数のチケット予約販売システムに接続し，利用者のリクエストに該当するチケット情報を各社のチケット予約販売システムから検索し利用者に提供するものであり，利用者が選択したチケットを該当する予約販売システムに対し実際に予約（変更，取り消し）を可能とする．販売するチケットの代金決済はクレジットカードなどを利用し，チケットの引渡しはチケットの利用の際に窓口で行われる．いわゆるチケットレスの予約サービスである．

このシステムを利用したチケット予約の流れ，システムの概要を図1および図2に示す．

2.1 システムの特徴

システムとしての特徴を整理すると次のようになる．

① 24時間365日運用される．このためサーバ，ネットワーク機器及びLAN/回線などの主要なコンポーネントは多重化された冗長構成となっており，負荷分散による同時使用またはアクティブ/スタンバイでの切り替え使用が実施される．

② 実際にチケットを販売する複数社のチケット予約販売システムと専用線を介して接続される．

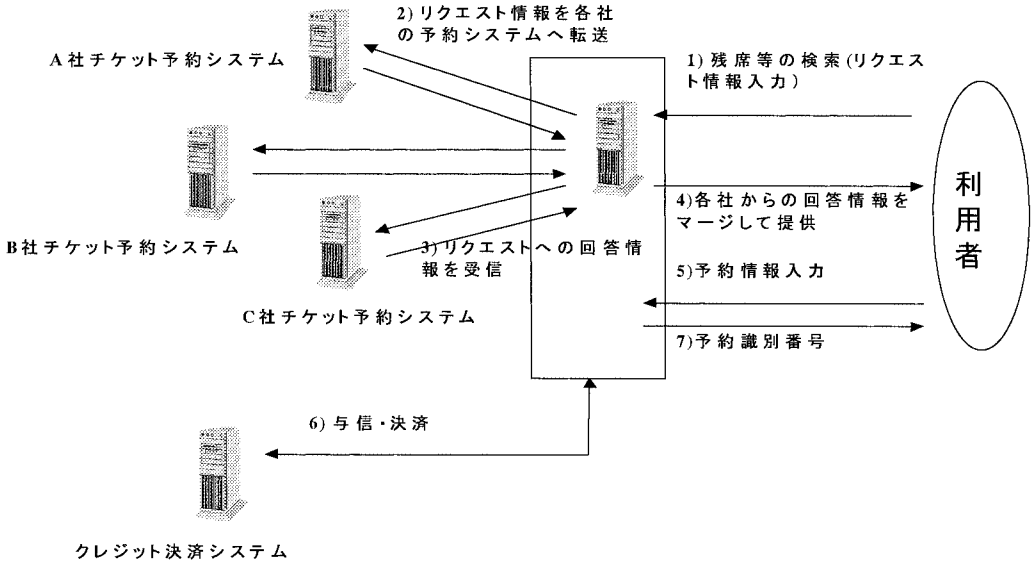
③ チケットの代金決済のためクレジット決済サービスを行う外部システムと接続される．

④ 顧客向けサポートセンターと接続される．

⑤ IDC（Internet Data Center）が提供するインターネット接続サービスを利用してインターネットと接続される．

⑥ IDCにおいてのホスティングという形でアウトソーシングされる．

⑦ 管理機能を持つ本社と接続される．



1) 利用者はWebブラウザによってこのシステムにいつでもアクセスし，日時，チケットの枚数などチケット購入に必要なリクエスト情報を入力する．
2) 入力されたリクエスト情報を，実際にチケットを販売する複数のチケット予約販売システムに送信する．
3) リクエストに適合するチケット情報をチケット予約販売システムから受け取る．
4) それらの情報を利用者にWebで提供する．
5) 利用者はブラウザに示された複数のチケット情報から最も希望に合致するものを選択して購入に必要な個人情報（名前，メールアドレス，クレジットカード番号など）を入力する．
6) チケットを販売する複数のチケット予約販売システムへの予約処理，クレジット決済サービスを行う外部システムでの与信チェック及び決済を行う．
7) 予約処理が終了するとWeb，メールにより利用者に対して予約の識別番号を通知する．
8) 利用者はチケット利用の当日窓口で識別番号を告げることによって予約済みのチケットを入手する．

図 1　チケット予約の流れ

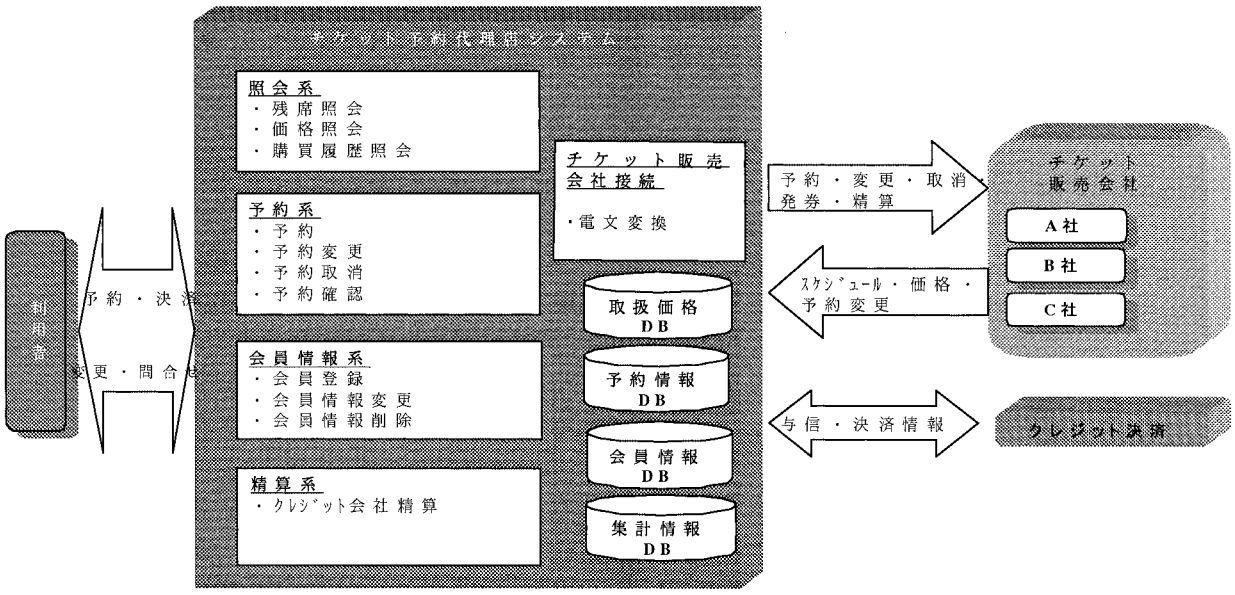


図 2　システムの概要

2.2 主な構成要素

システムを構成する主なコンポーネントは次の通りである．

・Web サーバ：利用者の Web ブラウザがアクセスする Web サーバ
・アプリケーションサーバ：対外部接続での検索/予約，クレジット決済の依頼などの業務処理を行う
・データベースサーバ：顧客情報の管理を行う
・メールサーバ：利用者への通知メールなどのメール送受信を行う
・Proxy サーバ：本社，顧客向けサポートセンターからのインターネットアクセス時の代理サーバ
・ジョブ管理サーバ：24 時間自動運転のためのジョブのスケジューリングを行う
・運用管理・ネットワーク監視サーバ：システムの運用管理及びネットワーク機器/サーバ/プロセスの死活監視，性能監視を行う
・ファイアウォール・セキュリティ監視サーバ：インターネット環境からシステムを保護し，また，インターネットからの不正浸入の監視を行う
・ネットワーク機器：ルータ，スィッチ，負荷分散装置など
・LAN，回線：センター内の LAN 設備，対外部接続用回線

3. ネットワークインフラストラクチャの要件

ここでは EC サイトに比較的共通なネットワークインフラストラクチャの信頼性・可用性及びセキュリティに関連する要件を示す（個々のシステムに依存しがちな性能要件など他の要件については省略する）．

このシステムは，計画的な停止を除いて 24 時間 365 日のサービス提供を基本としている．また，クレジットカードなどの情報や個人情報などを扱うため，暗号化や不正アクセス防止などの十分なセキュリティ対策を行ったものでなければならない．このため，ネットワークインフラストラクチャは以下に示す要件を満足する必要がある．

3.1 信頼性・可用性

信頼性，可用性の観点から各コンポーネントは，局所的な障害がシステムのサービス停止に直結しないような対応を取る必要がある．特に，クリティカルな要素すべてに対して最適な方法で多重化をはかるものとし，システムの停止時間を最少化する必要がある．

3.2 セキュリティ

セキュリティに関しては次に示す三つの要件がある．

1） 自システムのセキュリティ

インターネットなど外部からの不正なアクセス，サービス妨害，ウィルスの浸入などからシステムを防御し，また，自システム自身が踏み台にされないように不要と判断されるサービス，プロトコルを遮断する必要がある．

さらに外部からの攻撃を受けた時は，適切な対応が可能なように攻撃を検出し管理者に通知できる必要がある．

2） 個人情報のセキュリティ

ユーザのクレジット番号などの個人情報がネットワーク上を流れること，システム上に個人情報を保持・更新することを考慮し，データの漏洩・盗聴などがなされないためのセキュリティ対策を施す必要がある．

3) 対外部接続のセキュリティ

各社のチケット予約販売システムセンターなどの外部接続に対してはシステム間で合意された範囲のアクセスだけを認めるものとし，システム間の不用なアクセス（インターネットからこのシステムを経由した外部システムへのアクセス，外部接続システム間の相互アクセスなど）を認めることがない様に閉域性を確保する必要がある．

4. ネットワークインフラストラクチャ構築上の要点

ここでは，インターネットを利用したB2Cシステムに求められる要件の中で，24時間365日稼働の観点から，サービスの継続性・安全性に着目して，システム信頼性・可用性の実現方法とセキュリティ確保方法について記述する．

4.1 高信頼性・高可用性実現のポイント

システムの信頼性・可用性を高めるには，局所的な障害がシステムのサービス停止に直結しないように，サーバ及びネットワークのクリティカルな要素すべてに対して最適な方法で多重化を図ることが重要である．

4.1.1 サーバのリダンダント構成

サーバのリダンダント構成の実現のポイントは次の2点とした．

1) サーバダウン時にもサービスの継続性を維持する為に，筐体の多重化を図る．具体的には，次のいずれかを適用する．

① 負荷分散スィッチを設置しその配下に複数のサーバを配置して同時使用する．一部のサーバに障害が発生した場合，動作可能な他のサーバだけを使用してサービスを継続する．なお，この場合は負荷分散スィッチの多重化も考慮する．

② クラスタ構成によりアクティブとスタンバイの筐体を配置して通常はアクティブ側でサービスを提供する．アクティブ側に障害が発生した場合，自動的にスタンバイ側に切り替えてサービスを継続する．

2) ディスク障害時でも，サービスに影響しないようにディスクをミラー化する．

上記のポイントを踏まえ，Webサーバ，APサーバ，DBサーバに対して各サーバが持つ機能特性を考慮し次のようなリダンダント構成とした．

① WebサーバおよびAPサーバ

・筐体の二重化を図り，その二重化されたすべてのWebサーバおよびAPサーバを負荷分散しながら常時稼働させる（図3）．

・サーバダウン時は，正常に稼働しているサーバに片寄せして，サービスの継続を可能とする．

・障害が発生して切り離されたサーバは，障害復旧後サービスを停止することなく運用を開始することを可能とする．

・ディスクはディスク筐体間で完全ミラー化し，ディスク，ディスクコントロー

ラ障害時には，障害箇所を切り離してサービスの継続を可能とする．

・障害が発生して切り離されたディスクは，障害復旧後サービスを停止することなく運用を開始することを可能とする．

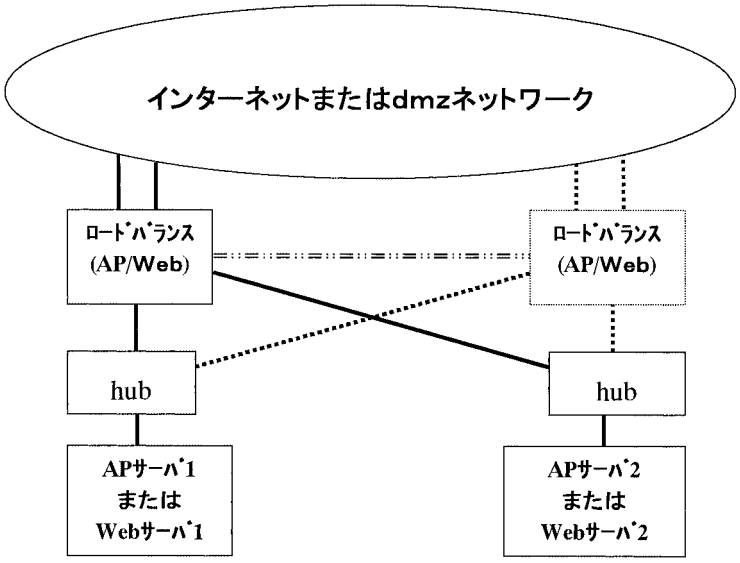


図 3　負荷分散 switch による AP サーバ/Web サーバの二重化

② DB サーバ

・クラスタリング構成を採用し，片系がアクティブの時，他系はスタンバイ状態とする．

・アクティブ状態のサーバがダウンした場合は，自動的にスタンバイ中のサーバがディスクの制御権を獲得した後にサービスを継続する．

・障害が発生して切り離されたサーバは，障害復旧後スタンバイ状態となり，片系のバックアップサーバとなる．

・ディスクはディスク筐体間で完全ミラー化し，ディスク，ディスクコントローラ障害時には，障害箇所を切り離してサービスの継続を可能とする．

・障害が発生して切り離されたディスクは，障害復旧後サービスを停止することなく運用を開始することを可能とする．

4.1.2　ネットワークのリダンダント構成

ネットワークのリダンダント構成の実現のポイントは次の 2 点とした．

① 局部的な通信経路の遮断がシステム全体に影響しないように，通信経路の多重化を図る．

② 通信経路を構成する要素が具備する機能及び位置づけによって，最適なリダンダント構成を設計する．

具体的には，インターネット接続，スィッチングハブ，ハブ，ファイアウォール，LAN および WAN に対して各ネットワーク構成要素が持つ機能特性及び位置づけに適するリダンダント構成とした．

1)　インターネット接続

IDC でのホスティングサービスを利用し，インターネットとはホスティングセンター内での LAN 接続とした．通常の専用線接続と比べ信頼性が高いためインターネット接続は単一とし，接続用ルータは予備機を準備し，障害発生時には手動にて機器の入れ替えを実施する．

2)　スィッチングハブ

・全てのスィッチングハブを二重化し，複数の通信経路を確保する．

・ネットワーク機器を常時監視して，障害発生時には迅速に障害の発生しているスィッチングハブを切り離し，サービスへの影響は最小限に押さえることを可能とする．

3)　ハブ

・全てのハブを二重化し，複数の通信経路を確保する．

・ネットワーク機器を常時監視して，障害発生時には迅速に障害の発生しているハブを切り離し，サービスへの影響は最小限に押さえることを可能とする．

4)　ファイアウォール（図 4）

・ファイアウォールを二重化し，負荷分散，同時使用により複数の通信経路を確保する．

・ネットワーク機器を常時監視して，障害発生時には迅速に障害の発生しているファイアウォールを切り離し，サービスへの影響は最小限に押さえることを可能とする．

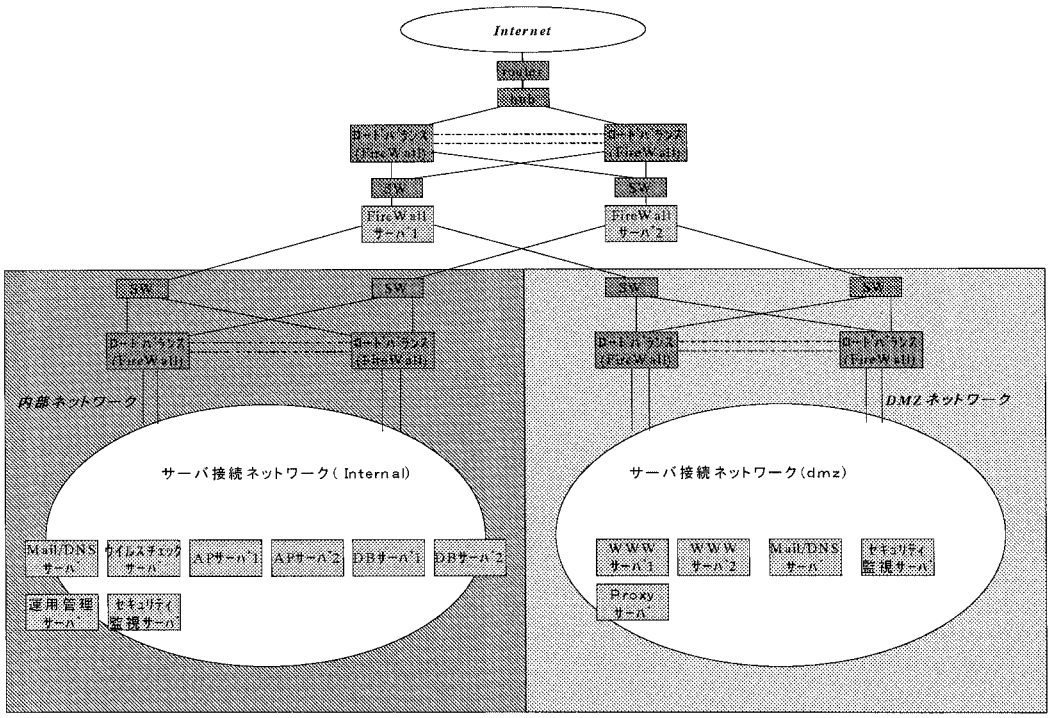


図 4　負荷分散 switch による FireWall の二重化

5） LAN

上記で述べた通り，各ネットワーク機器及びサーバの LAN ポートはリダンダント構成になっており，各々の機器を N : N に接続することによって複数の通信経路を確保することを可能とする．

従って，LAN ケーブルが物理的に断絶してもサービスは継続可能である．

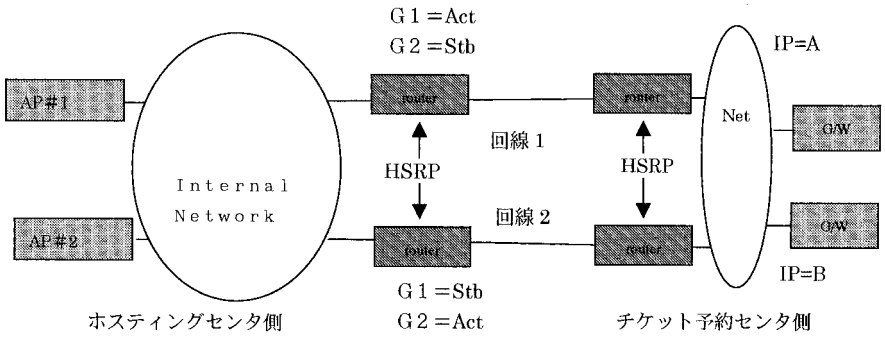
6） WAN

・ホスティングセンターとチケット予約システム，クレジット決済サービス，顧客サポートセンタ，本社間は複数の専用線及び機器(ルータ)により接続する．

・複数の専用線は負荷分散同時使用によって可用性と効率を高める．

・さらに，必要に応じて専用線障害時のバックアップ回線として ISDN 回線を利用する．

具体的には HSRP（Hot Standby Routing Protocol）を使用しながら 2 本の専用回線を負荷分散同時使用する．ホスティングセンターの AP サーバとチケット予約センタ間の接続事例を図 5 および表 1 に示す．この例ではチケット予約センタがリダンダント構成されており，二つの IP アドレス（＝A，B）として見える場合を想定している．



■ルータに二つの HSRP を設定.
HSRP 1：：仮想 IP アドレス＝G 1/Active＝回線 1 用ルータ，Standby＝回線 2 用ルータ
HSRP 2：：仮想 IP アドレス＝G 2/Active＝回線 2 用ルータ，Standby＝回線 1 用ルータ
■AP サーバに静的ルートを設定.
AP サーバ 1：: Dest IP addr＝A/Static＝G 1，Dest IP addr＝B/Static＝G 2
AP サーバ 2 ：: Dest IP addr＝A/Static＝G 2，Dest IP addr＝B/Static＝G 1

図 5　HSRP によるリダンダント回線構成

表 1　障害パターンと迂回経路

From	To	静的ルート	通常回線	#1回線障害	#2回線障害	G/W障害 A	G/W障害 B
AP#1	IP=A	G1	#1回線	#2回線	#1回線	—	#1回線
	IP=B	G2	#2回線	#2回線	#1回線	#2回線	—
AP#2	IP=A	G2	#2回線	#2回線	#1回線	—	#1回線
	IP=B	G1	#1回線	#2回線	#1回線	#2回線	—

4.2　セキュリティ確保のポイント

セキュリティ確保の観点から最も重要な課題の一つである外部からの脅威に対する

システム防衛の実現方法，すなわち，インターネットをはじめとする外部の脅威からシステムを防衛し，安全性と信頼性を維持する為の具体的なセキュリティ対策について記述する．

4.2.1 セキュリティ対策のための構成

システム内のネットワークをセキュリティレベルから低（＝バリアセグメント），中（＝非武装セグメントDMZ），高（Internalネットワーク）の3段階に分類し，重要度に応じてサーバ（情報）を各レベルのネットワークに配置する（図6）．

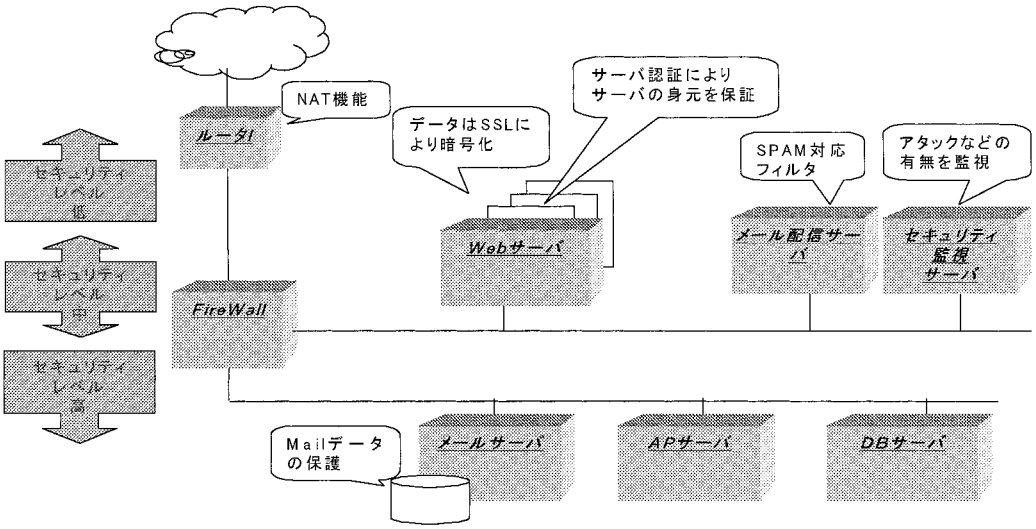


図6　セキュリティ概念図

4.2.2 セキュリティ対策

システムの構成要素に対する具体的なセキュリティ対策を次に示す．

1）　ネットワーク/サーバ

DMZ，Internalのネットワークや各種サーバを外敵から守るため，

・ファイアウォールにより，必要なサービス，プロトコル以外を防御する．

・また，Internet側→DMZ→Internalの順にセキュリティレベルを高くし，不要なアクセスを防御する．

・NAT（アドレス変換Network　Address　Translation）及びプロキシにより，システム内部の実アドレスをインターネット上のグローバルアドレスに変換し，ネットワークの内部構造が外部から見えないようにする．

・これにより，外部からシステム内部への直接的なアクセスや攻撃を行わせにくくする．

・Webサーバ，メールサーバ，APサーバ，プロキシサーバ，ファイアウォールなどの各サーバ及びルータ，スィッチなどのネットワーク機器において不要なプロセス（デーモン）を停止する．

・セキュリティ監視ツールにより，常に流れるネットワークのデータを監視し，ネットワーク，サーバへの攻撃を検知する事で，不正攻撃を検出し，運用管理

者へ注意を促し適切な対応をとる．

2） Web データ

・インターネット上に流れる個人情報，秘密情報に対するデータの盗聴，改竄などを防ぐため SSL（Secure Socket Layer）通信による暗号化を行う．

・電子認証証明書（サーバ証明書）によるサーバ認証を行い，ホームページの運営主体である法人組織の実在性を証明する（Web サーバの身元保証）．

・これらによって，利用者に信頼と安心を提供する．

3） 電子メール

・メールサーバ上に SPAM 対策フィルタを設定し迷惑メールへの対応を行う．

・ウィルスチェックサーバで入出力のメールをチェックし，メールによるウィルス感染を防止する．

・メールの内容に含まれた顧客情報などのプライバシーを守るためにセキュリティレベルの高い Internal ネットワークに設置したメールサーバ上にメールボックスを配置する．

4） 各センター（チケット予約，クレジット決済）

各センターへの接続は接続可能なサーバと利用可能なサービスを限定するために，IDC に設置した AP サーバと各センターとの間の通信に必要な TCP ポートだけを許容する．

それ以外の経路は（インターネット，本社，顧客サポートセンター，チケット予約センター相互，クレジット決済サービスとチケット予約センター間など），ファイアウォールあるいはルータのアクセス制御によって遮断する．

4.2.3 セキュリティ管理

上記のようなシステムのセキュリティ対策を実施した上で，サーバ，ネットワーク機器，ネットワークにおけるセキュリティレベルの維持と向上を目的として，次のようなセキュリティ管理を実施する．

1） ファイアウォールログ解析

定期的にファイアウォールのログを解析し，アクセス状況，異常と想定されるアクセスの指摘・対処方法を検討し，実施する．

2） セキュリティ診断

外部のセキュリティ診断サービスを利用し，定期的にインターネットを介した疑似アタックを実施して，セキュリティホール，脆弱性の検査・診断を実施し，必要な場合は対策を検討し実施する．

3） セキュリティ監視及びログ解析

DMZ 及び Internal ネットワークにおいてセキュリティ監視ツール（ネットワーク型及びホスト型の浸入検知システム）を設置し，常時セキュリティ違反の監視を実施すると共に，セキュリティ監視ツールに蓄積されたログを定期的に解析し，必要な場合は対策を検討し実施する．

5. お わ り に

インターネットを利用した B 2 C の中でも比較的構築事例の多いチケット予約のシ

ステムの構築例から可用性・信頼性の維持及びセキュリティ対策だけに絞ってそれぞれの実現方法を取り上げて紹介した．可用性・信頼性の維持及びセキュリティ対策は多くのシステムで共通な課題ではあるが，費用をどれだけかけるかなどそれぞれのシステムにおける固有の制約の中でそれぞれに適した実現方法を選択する必要がある．ここに紹介した事例が，選択肢の一つとして参考になれば幸いである．

執筆者紹介　中　島　己　範（Minori Nakajima）

1976 年電気通信大学電気通信学部通信工学科卒業．同年日本ユニシス(株)入社．ユーザのネットワーク設計・構築に従事した後，ISO，JIS，INTAP，TTC などの通信プロトコル開発制定やルータ上での ATM インタフェース開発などを担当．現在，ネットワークサービス部ブロードバンド基盤サービス室に所属．

日本情報処理学会会員，電信電話技術委員会第二部門委員会第二専門委員会委員，同第二部門委員会第五専門委員会委員．