ASP におけるコンピュータセキュリティ

Computer Security on ASP

藤 田 一 広

要 約 情報技術の進歩やネットワークの発達により，企業の情報システムへの依存度がますます高くなってきている．これにともない，不正利用や情報システムの不具合といった各種脅威によって発生する損失も増大する傾向にあり，今までよりさらに，コンピュータセキュリティへの関心が高くなってきている．

企業の情報システムへの依存度が高くなる反面，一般企業ではセキュリティやシステム構築などの技術や運用要員の確保が難しく，専門企業へのアウトソーシングや ASP（Application Service Provider）の利用を検討する傾向にある．

このような背景のもと，本稿では，ネットワーク接続を行なうコンピュータシステムのセキュリティについて述べるとともに，ASP におけるセキュリティの特徴，および，日本ユニシス（以下，当社）が提供する ASP のセキュリティ対策などについて述べる．

Abstract Advances in information technology and extended communication networks have led companies to rely heavily on their own information systems. This reliance increases the loss in business activity caused by the abuse and/or mulfunction of the information system, which turns the attention to the computer security.

The greater the dependence to the information system of a company becomes high, in a common company, technology, such as security and system construction, and reservation of an employment staff are difficult, and are in the tendency to consider outsourcing to a special company, and use of ASP (Application Service Provider).

The security of a computer system which makes network connection, the feature of the security in ASP and the measures against attack to ASP provided by Nihon Unisys are described in this paper.

1. は じ め に

昨今では携帯電話やコンピュータの普及に伴い，インターネットの利用が拡大している．その内容も，単なる Web 閲覧や情報収集にとどまらず，BtoC（Business To Consumer）でのオンラインショッピングやオークション，BtoB（Business To Business）での受発注などといった電子商取引も行なわれるようになった．これに伴い，より重要な情報がネットワーク上で取り交わされるようになり，その情報の漏洩や改ざんなどが，大きな脅威として挙げられるようになった．例えば，商取引情報が改ざんされた場合，取引相手とのトラブルや金銭的な損失が発生する可能性があり，他者へ取引額や商品内容が漏洩することによって，プライバシの侵害や企業イメージの低下を招くことがありえる．

インターネットなどの通信ネットワークの発達，情報技術の進歩により，企業の情報システムへの依存度がますます高まる一方，技術者の不足や運用要員不足により，サービス提供者である企業は，アウトソーシングや ASP（Application Service

Provider）の利用を検討する傾向にある．

本稿では，ネットワーク接続を行なうコンピュータシステムのセキュリティについて述べるとともに，ASP におけるセキュリティの特徴，および，当社が提供する ASP のセキュリティ対策などについて述べる．

2. コンピュータセキュリティ

本章では，コンピュータセキュリティの定義と，その脅威と対策について述べる．

2.1 コンピュータセキュリティの定義

日本情報処理振興事業協会（IPA）ではコンピュータセキュリティ（情報セキュリティ）を次のように定義している（出展：[1]「情報セキュリティの現状 2000 年版」IPA）．

「情報セキュリティは，組織における情報およびシステムを，組織の意図通りに制御できる性質である．」

上記の定義は，以下の性質を満足させることを条件とする．

・可用性

「システムが，必要な場合に，所定の方法で利用および制御できること」

システムを構成するハードウェア，ソフトウェア，ネットワークが障害を起こすことなく稼働するという従来の可用性の概念に加え，システムの利用を決められた方法により制御できる性質を示す．スコープとする脅威は，不正アクセス，誤作動，コンピュータウィルス，運用に係わる問題，天災である．

・一貫性

「情報の，正確性および完全性が維持されていること」

主として，データベース中の情報および運用に関わる情報の正確性および完全性が維持される性質を示す．スコープとする脅威は，不正アクセス，誤作動，運用に係わる問題である．

・機密性

「情報が，権限のあるものが権限のある際に，権限のある方式に則って公開されること」

情報が，組織により決められた規定通りに公開される性質を示している．スコープとする脅威は，機密情報漏洩，著作権侵害，プライバシー侵害である．

・道徳性

「情報の公開および流通が，組織の信用失墜を招かないこと」

情報の公開が組織の信用失墜を招かないことを示す性質である．具体的には，個人のプライバシー情報の流出による信用失墜などが該当する．

つまりコンピュータセキュリティとは，情報システムにおいて守るべき資産（ハードウェア，ソフトウェア，ネットワーク）と情報（データ）とに対する数々の脅威を，回避，防止，検出，回復する仕組みであるといえる．

冒頭でも述べたように，昨今のシステムではインターネット接続が前提となるため，ここであげている可用性，一貫性，機密性，道徳性に関しても通信面におけるセキュリティがよく論じられている．しかし，これまでにコンピュータシステムで論じられ

てきたセキュリティ，つまり物理的な盗難などに対する対策もおろそかにしてはならない．例えば内閣情報セキュリティ対策推進室の「情報セキュリティポリシーに関するガイドライン」では次の四つの観点で対策が必要であることが述べられている．

① 物理的セキュリティ
施設，設備を保護する出入り管理等

② 人的セキュリティ
職員に対する教育，訓練，パスワード管理等

③ 技術的セキュリティ
ネットワーク管理，ウィルス対策等

④ 運用
システムの監視，緊急時対応計画の策定

2.2 脅　　威

表１では，ここで想定されるシステム面，物理面での脅威には何があるかを，大きくネットワーク，ホスト，物理面にわけて列挙した．

また，人的脅威に関しても考慮しなければならない．人的脅威にはたとえば利用者の虚偽や内部犯行による不正使用や情報の漏洩といったものが挙げられる．特に内部犯行による脅威においては，システム面での対策では対処できないことが多い．企業であれば社員の行動規範の明確化や，システムに関連する外注，受け入れ社員等に関しても配慮が必要である．また，故意ではなく単なるケアレスミスも人的脅威のひとつである．例えばメールアドレスの流出などは，システム的な不具合によるものもあるが，操作するオペレータのミスにより発生することも多く，人的ミスを防止するための仕組みが必要である．

2.3 対　　策

前節で挙げた脅威に対抗する手段として，セキュリティを実現するためのハードウェアやソフトウェア，システムインテグレーションサービス，セキュリティ運用サービスといった，様々なシステムやサービスが提供されている．これらは通常，単体ではなく複数の組み合わせを検討した上で利用するが，それにより実現される対策は，ほぼ表２で示される．なお，表１にあわせて大きく三つに分類しているが，ひとつの対策が複数の脅威に対して有効なこともあり，内容には一部重複がある．

人的脅威に対しては次のような対策が考えられる．

- 関係する要員を制限し，適切でない人員，教育や啓蒙が徹底されていない要員を配置しない．
- システムの構築や変更が可能なアカウントを制限し，不正行為の可能性を低減する．
- 規則や罰則を定め，行動規範などの教育を徹底する．
- 情報の漏洩を防ぐため，退職時の手続きや解雇などの手順を確立する．
- 複数グループ間での相互けん制や監査を行なう．
- 外部の警備員や警備システムを配する．
- ケアレスミスを防ぐため，二重チェックやシステム的なチェックを行なう．

表1 脅　　威

分類	脅　威	内　　容
ネットワーク	盗聴（漏洩）	ネットワークへの不正アクセスにより，データの盗聴や不正な複製を行う．
	破壊（消去）	盗聴のみならず伝送されるデータそのものを破壊もしくは消去する．
	改ざん	破壊ではなく，一部を変更することにより虚偽のデータを伝送する．場合によっては破壊よりも被害が大きくなる可能性がある．
	なりすまし	第三者がネットワーク上の別の人間になりすまし，データの盗難や虚偽の取引を行う．
	否認	取引相手が取引の成立を否認する．電子商取引などにおいて，システム的には取引が成立したとしても，相手が虚偽の報告を行う可能性がある．
	妨害	大量のメール送信や，サービス妨害を目的としたアクセスを行い，トラフィックを増大させることでサービス提供を困難にする．
ホスト	侵入	データの漏洩や破壊等の実質的な被害がなかったとしても侵入した形跡が明らかになれば，そのシステムやサービスが信用を失うもとになる．
	盗難	ネットワークでの盗難と同じであるが，ネットワーク上で暗号化されているデータもホスト上では暗号化されていない可能性がある．ネットワークでのそれとはことなり，複数のデータがホスト上に集約されているため，つぎつぎとデータが漏洩することが考えられる．
	改ざん	データの改ざんのみならず，アカウントやパスワード等が改ざんされることで次の攻撃に利用される可能性がある．
	破壊（ウィルス等を含む）	ウィルスやワームを仕込まれることでデータの改ざんや破壊，サービスレベルの低下などが発生する．二次災害が発生する可能性が高く，自身が意図しない加害者になり得る．
	なりすまし	他人のアカウントを利用することでデータの漏洩やサービスの不正利用などが行われる．データ破壊等が行われない場合は比較的発覚しにくく，継続的な犯罪が行われる可能性がある．
物理	回線の盗聴	回線に物理的に接続した機器による盗聴．この他，ディスプレイから発する電磁波等を読み取り，内容を盗聴することや，カード番号等，システムに間接的に関係するものに対して盗聴が行なわれ，不正利用される．
	回線の切断	通信回線が切断されることで，データ転送が行われなくなり，サービスが停止する．
	盗難	ホストや周辺機器が盗難に合いサービスが停止することや，ディスク等のメディアに記録された情報が盗難に合う．
	破壊	ホストや周辺機器，メディア等が破壊されサービスが停止することや，設備等が破壊され運用に支障をきたす．
	改ざん	システム構成やネットワーク機器の設定が変更され，意図したセキュリティを維持できなくなる．
	自然災害	停電，地震，漏水，火災，雷といった各種自然災害による破壊や故障が考えられる．

表 2 対　　策

分類	脅　威	対　抗　手　段
ネットワーク	盗聴（漏洩）	データの暗号化を行い，情報が盗聴されても第三者には理解できないものとする．
	破壊（消去）	データの暗号化により改ざんが行えないようにする．
	改ざん	またデータ完全性チェックを行うことで改ざんや破壊にあったことを検知する．
	なりすまし	電子署名や認証局を用いることによりなりすましや否認を防止する．
	否認	
	妨害	不正アクセスを監視し，警告，排除を行う． ネットワーク（およびサービス提供サーバ）を多重化する．
ホスト	侵入	サービスやデーモンの停止，各種フィルタリングを行うことで不正侵入を防止する．
	盗難	防火壁（Proxy Server）等を利用し内部ネットワークを隠蔽する．
	改ざん	アクセス制限を行い，改ざんや破壊を防止する．
	破壊（ウィルス等を含む）	ウィルスチェックを行う． ファイルを暗号化し改ざんを防止する．
	なりすまし	アカウントのアクセス制限とパスワードのチェックを行う． 物理的な鍵（IC カード等）を用いる． 不要なアカウントを停止する． アクセスログを記録する．
物理	回線の盗聴	防犯シャッター，防犯カメラ，警報，警備員を配置する．
	回線の切断	耐震，免震構造とし，地震に備える．
	盗難	消火栓，防火壁を導入する．
	破壊	漏水センサーにより監視し,防水壁を導入する.
	改ざん	無停電電源や自家発電装置の導入，電源の多重化を行い雷，停電対策を施す．
	自然災害	

2.4 セキュリティポリシー

コンピュータシステムを構築する際は，システムを数々の脅威から守るために，前節で挙げたような対策が講じられる．しかし，その対策の基本的な考え方＝ポリシーがシステムごとに都度考えられていたり，構築を担当する部署ごとに独自で行なわれている場合，一連の作業が重複し無駄が生じることや，対策に抜けが生じること，技術的，金銭的な面から偏ったセキュリティ対策を施してしまうこと，などが考えられる．また，その結果としてシステムごとのセキュリティレベル（品質）にばらつきが生じ，組織内で協調して利用されるシステムなど，本来一致していなければならないセキュリティレベルが保てなくなる．

このためには，組織内で統一された「セキュリティポリシー」を定め，トップダウンで徹底させることが重要である．組織内の関連するシステム全体に対し，どこに投資し，どのような対策を施すべきかを検討することで，組織全体のセキュリティレベルを向上させることができる．

なお，セキュリティポリシーを定める際には，コスト，組織の体制，利便性や運用性との兼ね合いを十分に検討しなければならない．例えば，高い機密性や可用性を追求することは重要であるが，かかるコストへの対処や運用性が確保できなければ，そ

のセキュリティの品質を継続的に保証することは難しい．また，セキュリティ面を偏重したシステムは，利用者の手間も多くなりがちで利便性が損なわれてしまう．セキュリティポリシーは，このような二律背反になる問題を十分に検討し，バランスよく定めたものでなければならない．

セキュリティポリシーのガイドラインとしては国際標準 ISO/IEC　TR 13335 (GMITS : Guidelines for the Management of IT Security)，ISO/IEC 17799 が定められている．この他，セキュリティポリシーの作成にあたっては IPA のセキュリティハンドブック IETF RFC 2196 の一読をお奨めする．

2.5 セキュリティのサイクル

セキュリティポリシーの策定とは，いってみればセキュリティに関する要件定義である．この要件定義からセキュリティの構築，実施，改訂は，図 1 のサイクルであらわされる．

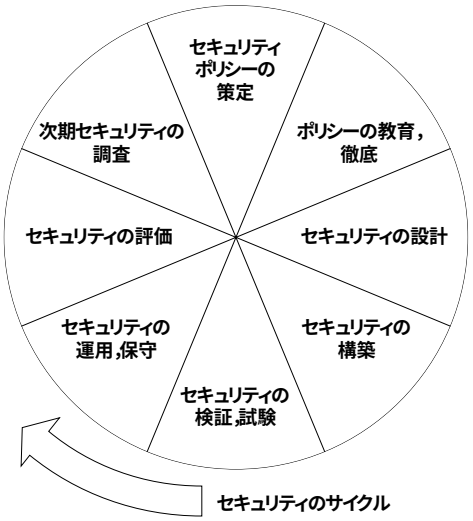

図 1　セキュリティのサイクル

・要求仕様
　企業や組織の理念，戦略に基づいてセキュリティポリシーを策定する．
・教育
　関連する組織がセキュリティポリシーを遵守するよう教育，啓蒙を徹底する．
・設計
　フィルタリング，パスワードの運用，ウイルス対策など具体策のためのセキュリティガイドラインを策定する．
・構築
　設計時に定めたガイドラインに沿って必要なハードウェア，ソフトウェアなどツールの導入を行う．
・試験，検証
　ポリシーおよびガイドラインに則しているか，実際に機能しているかを検証，

確認する．

・運用

ネットワーク管理，システム管理，セキュリティの監視を行う．

・保守

障害対処など日常的な運用，保守業務を遂行する．

・評価

実施されているセキュリティ対策が，ガイドラインや運用マニュアルを遵守しているかどうかなどを監査し，費用対効果が適切であるか，利便性や運用面で問題が発生していないかを評価，診断する．

・調査

セキュリティ情報の収集を行う．

この一連のセキュリティ対策は，システムにとって適切なサイクルで運用され，陳腐化を防ぐため適宜，更新されることが望ましい．

3. ASP におけるセキュリティ

前章までは一般的なコンピュータシステムにおけるセキュリティについて述べた．本章では ASP（Application Service Provider）におけるセキュリティについて述べる．

3.1 ASP とは

ASP とは，ネットワークを介して，特定もしくは不特定多数の利用者に対し，サービス（ひとつまたは複数のアプリケーションで構成される機能）を提供する事業者，およびそのサービス提供形態を指す．

サービス利用者のシステムを，アウトソーシングとして構築し提供する場合と，ASP として提供する場合とで異なる点は，サービスの利用者にシステムを販売する，あるいはその利用者にあわせて専用のアプリケーションを個別に開発するのではなく，汎用的なアプリケーションを組み合わせたサービスを，賃貸契約を前提として提供するところにある．

ASP では，ASP 提供者（日本語訳としてはふさわしくないがここでは便宜上「ASP サービス利用者」に対してサービスを提供する側の「ASP サービス提供者」を略して「ASP 提供者」として表記する）が，サービスを実現するソフトウェアやハードウェア，ネットワークの保守や運用までを，包括的に管理・維持する．この事業形態から，顧客であるサービス利用者は ASP サービスの導入に対し，次のメリットを期待している．

・サービス利用までの期間短縮と，初期投資の削減．

・サービス利用のためのアプリケーションや基盤の保守や運用，および敷地コストの削減（TCO 削減）

・技術者や運用要員の不足を補い，サービス利用を前提とした主たる運営のみに専念できること．

3.2 セキュリティ面におけるアウトソーシングと ASP との違い

サービス利用者が自社でシステムを構築する場合，先に述べたようなセキュリティ

ポリシーの策定から，その具体的な設計や運用にいたるまで，専門知識をもった人的資源や資産を確保・投入して維持・管理しなければならない．しかし，このようなことを一般企業で行うことは難しく，結果としてセキュリティまわりもあわせてアウトソーシング（ASP 利用）に期待することとなる．利用者は ASP 導入により，期間短縮と技術者や運用要員の不足とを解消できるわけだが，セキュリティの面からは次の点に注意しなければならない．

・利用者と関係する企業以外の人間が，利用者情報やその他の情報に触れる．
・利用者の社外に機密情報をおかなければならない．
・セキュリティポリシーは ASP 提供者が定めるものであり，かならずしもその顧客である利用者のポリシーとは一致しない．
・システムがおかれるデータセンタ（iDC）は利用者専用のものではないのが一般的であり，他社と共有される．

これは，利用者専用のシステムを開発する場合や，その資産を預かって管理するハウジング形態のアウトソーシングとは大きく違う点である．

ハウジング形態のアウトソーシングでは，運用面の都合からネットワーク監視やジョブ管理等をアウトソーシング事業者が一元的に管理することはあっても，基本的にそのハードウェアやネットワークは顧客の資産であり，システムごとに個別に用意される．このため，セキュリティレベルは顧客のニーズに応じて設定され，顧客の他のシステムとの接続も含めて，統一のセキュリティポリシーのもと管理がなされるのが普通である．

これに対し，ASP によるホスティング形態の場合，ハードウェア，ソフトウェア，ネットワーク等の資産は ASP 提供者のものであり，その管理も提供者が独自に行う．セキュリティポリシーは ASP 提供者が定めており，セキュリティレベルは顧客のニーズに合わせてある程度選択できるが，その実現方法は SLA（Service Level Agreement：サービス品質保証契約）による制約のもと， ASP 提供者に任せられる． また，顧客の別システムと接続する場合における ASP 提供者の責任範囲は，ASP 提供者が持つデータセンタの内側までであり，データセンタ内のセキュリティレベルと，顧客側のシステムのセキュリティレベルとは，必ずしも一致しない．

ASP 利用者は ASP 提供者を選択する際に，SLA で謳われている内容について，機能面や性能面だけではなく，セキュリティ面に関する品質についても十分に確認し，検討する必要がある．

3.3 ASP におけるセキュリティの課題

ASP 提供者は，ASP におけるセキュリティを考える上で，これまでに述べたコンピュータセキュリティすべてに関して考慮が必要なのはもちろんのこと，前節で述べたように，利用者専用のシステムを構築する場合と異なる点があることにも注意が必要である．また，これに加えて ASP 提供者は，その事業形態から次の項目に関してもセキュリティ面で考慮が必要である．

・複数サービス間でのセキュリティレベルの統一
　通常 ASP では複数のコンテンツ（サービスを実現するためのアプリケーションやコンポーネント）を提供しており，このコンテンツを協調・連携させるこ

とで，より高機能なサービスを実現可能である．これらのコンテンツが複数のコンテンツプロバイダから提供されている場合は，すべてのコンテンツのセキュリティレベルを統一させることが難しい．しかし，ASP 提供者としては，提供者が定めたセキュリティポリシーに準拠したセキュリティレベルで，すべてのコンテンツが用意されることが望ましい．

・複数サービス間での認証

複数のサービスやコンテンツを協調させる場合，他のサービスから別のサービスを利用するときに，再度アカウントの確認（ログイン要求）が行なわれては，利用者の利便性が損なわれてしまう．ASP 提供者はサービスやコンテンツの統合の際に，ことなるサービス間でも認証が一回のみで済まされること（Single Sign On）や，セキュリティレベルを統一するなどの要求に応えなければならない．

・道徳面での対策

システム的なもののみならず，例えば掲示板サービスなど第三者が情報を与えてくる場合など，その内容が著作権や倫理上の問題などに抵触していないかなども確認しなければならない．

なお，悪意ある第三者やウィルスは，日々新たな手段で攻撃してくるため，ASP 運用者は日々，主なものだけでも次のようなセキュリティ対策を実施しなければならない．

・不正アクセスの検知
・ログの監視と管理
・ネットワークソフトウェアのバージョンアップ（パッチの適用）と管理
・ユーザデータのバックアップ
・ウィルスの検出

サービスに対する攻撃への即時対応は当然であるが，ウィルスに対するワクチンの適用やセキュリティパッチ等も即時の判断・適用が必要となる．しかも，本番運用しているサービスであるからには，利用者への負担や損失が最小限でなければならず，適用前と適用後において利用者に対するサービスレベルやサービス内容が異なってはならない．

4. ASP asaban.com でのセキュリティ

前章では一般的な ASP におけるセキュリティについて述べた．本章では当社が提供する ASP 事業において，これまでに述べたセキュリティ対策のうち何を採択し，何に力を入れているかを述べる．

4.1 ASP asaban.com とは

まず当社が行なっている ASP 事業について簡単に述べる．これは大別すると次の二つに分類される．

① ASP 事業者として，ASP asaban.com によるサービスを提供する．
② AIP（Application Infrastracture Provider）事業者として，ASP サービスのための Kiban@asaban を提供する．

前者はコンテンツを ASP サービスとして提供する通常の ASP 事業であるが，後者は ASP を自社で運営したい ASP 提供者へ，その基盤をホスティングサービスとして提供するものである．

セキュリティ面での大きな違いを述べるとすれば，前者の ASP asaban.com におけるセキュリティは，前章の ASP セキュリティとほぼ同じものであるのに対し，後者の AIP　Kiban@asaban は，ASP 基盤であるとともに，顧客専用のアウトソーシング基盤としても適用され，セキュリティポリシーも ASP 提供者独自のもの以外にも，顧客のセキュリティポリシーにあわせて比較的柔軟に対応することが可能である．なお，AIP　Kiban@asaban の場合，直接の顧客は「ASP 利用者」ではなく「ASP 提供者」となり，セキュリティ対策は「ASP 利用者」ではなく「ASP 提供者」と取り交わす SLA の範囲で定めることになる．

4.2 ASP asaban.com および Kiban@asaban におけるセキュリティ対策

ASP　asaban.com および，その AIP 基盤である Kiban@asaban では，次の方針を主軸に，表 3 に挙げるセキュリティ対策を行っている．

- ハードウェア，ソフトウェアの一部に障害が発生した場合，またバージョンアップなどによる入れ替え作業が発生した場合でも，利用者がサービスを利用し続けられること．
- 利用者のデータが消失しないこと．また，破壊されないこと．
- 利用者のデータが盗まれないこと．また，改ざんされないこと．

人的脅威に関しては次のような対策を行なっている．

- 運用部門と運用管理部門（MSP : Management Service Provider）の専任化
- 役割（保守，運用，開発）に応じたアカウントの制限およびアクセス制御の実施
- システム変更および作業内容の記録と監査の実施

4.3 ASP asaban における特長的な対策

ASP　asaban.com および Kiban@asaban では，高可用性や信頼性，保守性，利便性の面から，次の特長的なセキュリティ対策を行なっている．

1)　論理 5 層によるネットワークの遮断

図 2 に示すように，ASP 基盤を「ルータ」,「Gateway サーバ」,「Web/AP サーバ」,「DB サーバ」,「ストレージ」という論理 5 層（tier）アーキテクチャとして実現する．

1 段目のネットワーク層はルータによるフィルタリングを，2 段目の Gateway 層にはアプリケーションゲートウェイを配置し，ネットワークを遮断することで外部ネットワークから内部ネットワークを参照できないようにしている．各層では IP フォワードを禁止しているため， DB 層にあるデータに到達するまでには，Gateway 層および Web/AP 層を順次攻撃する必要がある．この間に攻撃を検知し，被侵入システムを遮断し，ダメージコントロールを行う．また，各層内，各層間で，多重化による完全冗長構成を行い，高可用性を実現する．

2)　Web サーバのリスク対策

Windows アプリケーションでは，Web サーバとして主に IIS（Microsoft Inter-

表 3　Kiban@asaban における対策

分類	脅　威	対　抗　手　段
ネットワーク	盗聴（漏洩）	・ SSL（Secure Socket Layer）によるデータの暗号化
	破壊（消去）	・ IP アドレス，ポート番号によるフィルタリング
	改ざん	・ IP アドレスによる発信元特定
	なりすまし	・ サーバ認証
	否認	・ クライアント認証
		・ 電子署名
		・ Web サーバ Basic 認証済識別によるアクセス制御
	妨害	・ IP アドレス，ポート番号等によるフィルタリング
		・ IP フィルタ不適合データグラムの記録
		・ Application Gateway によるフィルタリング
		・ Web アクセス履歴のチェック
		・ SNMP および ping による内部ネットワーク監視
		・ 複数箇所からの外部 ping 監視
ホスト	侵入	・ 5 層構造による内部ネットワークの分離
	盗難	・ ルータやサーバのシステムログによる不正検知と解析
	改ざん	・ DBMS による利用者認証
	破壊（ウィルス等を含む）	・ DB インスタンスの分離と DBMS によるアクセス制御
		・ 接続装置識別子による論理区画へのアクセス制御
	なりすまし	・ S/W 監視によるリソースの不正変更の検知
		・ ファイルシステムの変更検知ソフトの利用
		・ 定期的なウィルス走査
		・ システム変更時のバックアップ
		・ ファイルシステムレベルでのバックアップ
		・ DBMS 制御ファイル，ログバックアップ
		・ RAID による冗長化
物理	回線の盗聴	データセンタ利用による防犯対策
	回線の切断	・ 24 時間 365 日常駐警備
	盗難	・ 防犯シャッター
	破壊	・ 計算機室入口および室内監視用の防犯カメラ
	改ざん	・ 建物入口/計算機室入口での二要素認証（ID カードおよびバイオメトリクス）
		・ 計算機室への入室制限
		・ 機器格納棚の解錠時の身分確認
		・ 保管テープ取り出し依頼時の身分確認
		・ 入退館/室記録の台帳またはシステムによる管理
		・ テープ取り出し記録
	自然災害	データセンタ利用による各種自然災害対策
		・ UPS，自家発電設備，および 2 系統の電源
		・ 耐震，免震構造等
		・ 蓄熱槽備蓄
		・ 漏水センサーによる監視
		・ ハロンによる消火設備と屋内消火栓
		・ CVCF 経由によるサージ除去
		・ UPS，空調機の予備設備による冗長構成
		・ 耐火金庫によるメディア管理

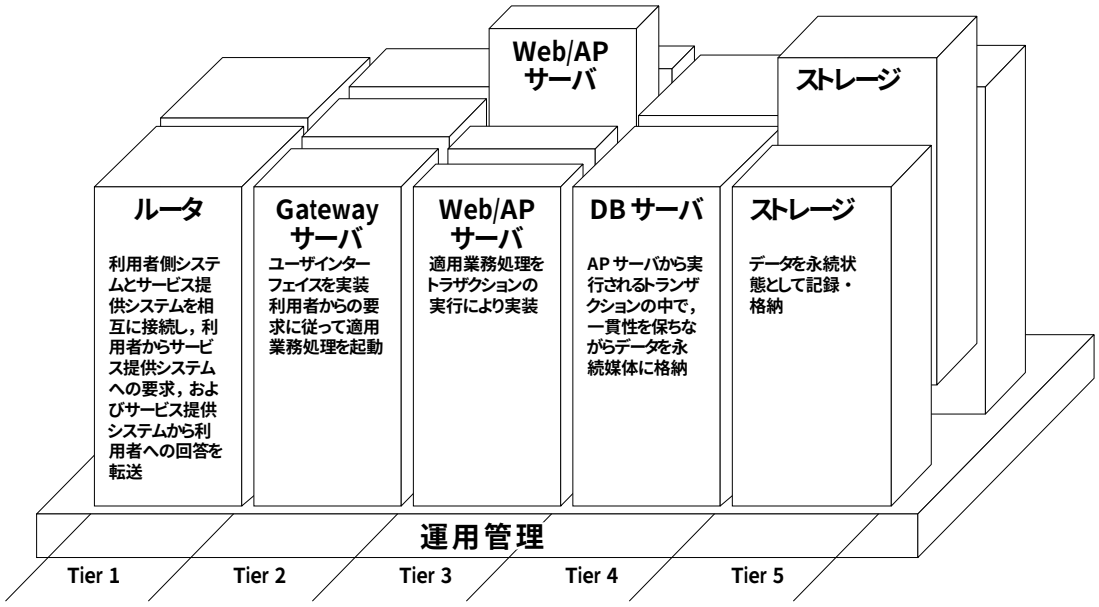

図 2　論理 5 層

net Infomation Services）が利用される．しかし IIS の脆弱性を突いた攻撃が多く発生するため，前述の 5 層構造ではこれを Web/AP 層に配置し，HTTP（S）以外の外部接続境界を超えた通信を遮断している．

Gateway 層における Web サーバは，セキュリティホールに対する攻撃に迅速に対応するため Linux 上でソースコードも含めて公開されている ApacheWeb サーバとセキュリティモジュールとを使用している．

3）システムの多重化による高可用性の確保

図 3 に示すように，構築するシステムのネットワークの二重化のみならず，システムとデータセンタ側のバックボーンネットワークとの接続（通信線およびルータ）をも二重化することで，ネットワークの代替経路を確保し，障害に対するボトルネックが生じないようにしている．

4）保守専用機による保守性の確保とセキュリティの確保

通常は電源を投入しないコールドスタンバイの保守専用機を用意している．保守専用機では，平文でパスワードを伝送するプロトコルは禁止しており，定められたクライアントとアクセス権限をもつアカウントのみが利用可能な SSH（SercureSHell）を使用している．Windows 系の遠隔保守には Citrix 社製 MetaFrame 等を用いるが，この場合も SOCKS を利用するなど，セキュリティを向上させている．

5）複数サービス間でのセキュリティレベルの統一

システムインテグレータであると同時に開発部門を持つ企業として，コンテンツプロバイダから得たコンテンツも運用管理部門で定めたセキュリティポリシーに沿うよう，カスタマイズや改修を行い，セキュリティレベルの統一を図っている．

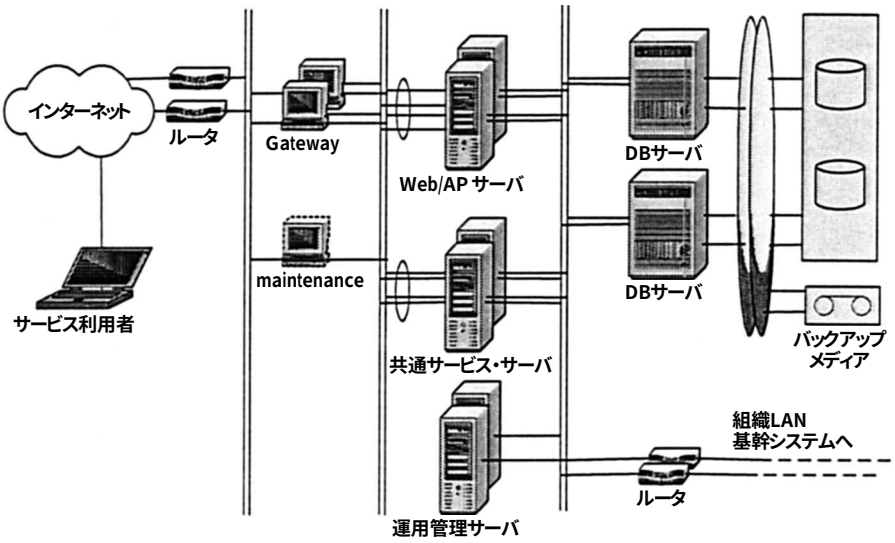

図 3　システムの多重化

6）　複数サービス間による認証（Single Sign On）

Apache による web サーバと, Windows アプリケーションとにおいて, Apache のモジュールと MetaFrame とを利用して Single Sing On を実現している.

7）　運用者判断による即時対応

二次障害が考えられるウィルスおよびセキュリティホールに対するアタックが行われた場合，運用者判断による即時対応を行う.

例えば DDoS（Distributed Denial of Service）等のサービス妨害攻撃のようなものでは, 攻撃の対象となるばかりではなく, その攻撃の中継点にされることや, 犯行の足跡をくらますために利用される恐れがある．このような「踏み台攻撃」や，CodeRed,Nimda 等のウィルスのように，被害者となると同時に自覚なき加害者になる可能性がある場合は，即時の判断と対処が必要である．専門分野における高い技術レベルと，MSP による運用管理の専門体制を確立し，SLA に抵触しない範囲で運用者責任による即時のセキュリティ対策を講じている.

4. 4　asaban.com の今後の対策

ASP　asaban.com および Kiban@asaban では，金融系や医療系など，ASP ではあるが，ミッションクリティカルな分野でも利用されており，セキュリティをより強固なものにすべく，次にあげる項目を検討している.

1）　ウィルスのペイロードチェック

アプリケーションサーバやデータベースサーバでの定期的なウィルスチェックのほかに，ウィルスを Gateway 層でチェックし，内部ネットワークに侵入させないようにする.

2）　ワンタイムパスワードの提供

ホストおよびネットワーク上においてワンタイムパスワードを導入し，セキュリティレベルを向上させる.

3） ローカルデータの暗号化

データベースサーバ等で扱うローカルデータを暗号化し，データが盗難されても実質的な被害が発生しないようにする．

4） データ廃棄の取り扱いの統一

データ廃棄の取り扱いについては顧客の要求に応じて行っているが，Kiban@asaban の統一した取り扱いを定め，セキュリティ品質を高める．

5） 第三者機関による定期的なセキュリティ監査

Kiban@asaban を利用している一部のシステムで実現されているが，他のシステムでも外部のセキュリティ診断サービスを利用し，脆弱性の検査，診断を行なう．

6） 標準制度への適合性評価や法律への準拠

情報セキュリティ管理（ISMS）の国際標準「BS 7799」（ISO/IEC 17799），セキュリティ評価基準「ISO 15408」の認証を受ける．また，個人情報保護法が平成 14 年度の法制化に向けて検討されており，ASP における顧客管理の面からこれへの追従も必要であると考えている．

5. おわりに

残念ながら完璧なセキュリティは存在せず，いくら頑丈なセキュリティを施してもいずれ破られる時がくる．より強固なセキュリティ対策を検討するとともに，なんらかの障害が発生したときに，その事態を迅速に収拾し，被害を最小限にとどめる手立てを検討しておかなければならない．

セキュリティ対策は「保険」であり，脚光を浴びることの少ない，地味な作業の積み重ねである．重要さがようやく認識されるときは，障害が発生したときであり，その際には「失敗」に対する代価も支払わなければならない．運用に携わる者は，定められたセキュリティポリシーに則り，不断の努力をもってセキュリティレベルを維持していかねばならない．

筆者も本稿を執筆するにあたりセキュリティポリシー等を読み返してみたが，常にセキュリティに関して気を配り，行動しなければならないということを，改めて肝に銘じる思いである．

参考文献
［1］“情報セキュリティの現状 2000 年版”, 情報処理振興事業協会, 2001
［2］ 熊谷誠治,“続インターネット・セキュリティのしくみ”, 日経 BP 社, 2001
［3］“サイトセキュリティハンドブック”, 情報処理振興事業協会（http : //www. ipa. go. jp/security/rfc/RFC 2196-00 JA. html), 2001
［4］“平成 11 年度セキュリティセミナー開催報告講演録”, FISC 監査安全部（http : //www. fisc. or. jp/info/l 25_000121. htm), 2000
［5］“平成 12 年度セキュリティセミナー開催報告講演録” FISC 監査安全部（http : //www. fisc. or. jp/info/l 53_010419. htm), 2001
［6］ N+I MAGAZINE 編集部,“ネットワークセキュリティガイドブック”, ソフトバンクパブリッシング株式会社, 2001
［7］“不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号)http : //www. meti. go. jp/kohosys/topics/10000098/esecu 02 j. pdf

［8］“情報システム安全対策基準（平成7年通商産業省告示第518号)http : //www. meti. go. jp/kohosys/topics/10000098/esecu 03 j. pdf
［9］“コンピュータ不正アクセス対策基準（平成8年通商産業省告示第362号）http : //www. meti. go. jp/kohosys/topics/10000098/esecu 06 j. pdf
［10］“コンピュータウイルス対策基準（平成7年通商産業省告示第429号)http : //www. meti. go. jp/kohosys/topics/10000098/esecu 07 j. pdf

URL一覧

情報処理振興事業協会（IPA）セキュリティセンター　http : //www.ipa.go.jp/security/
コンピュータ緊急対応センター（JPCERT/CC）　http : //www.jpcert.or.jp/
財）日本情報処理開発協会（JIPDEC）　http : //www.jipdec.or.jp/
社）日本電子工業振興協会（JEIDA）　http : //www.jeida.or.jp/
高度情報通信社会推進本部　情報セキュリティ対策　http : //www.kantei.go.jp/jp/it/security/index.html

執筆者紹介　藤　田　一　広（Kazuhiro Fujita）
1969年生．1990年私立育英高等専門学校電子工学科卒業．同年日本ユニシス(株)入社．知識システム部にてTippler の開発，アドバンスドソフトウェア開発室にてSystem*ν* の開発に従事．現在asaban.com 事業部技術企画室に所属し，医療系ASPの企画，構築を担当．