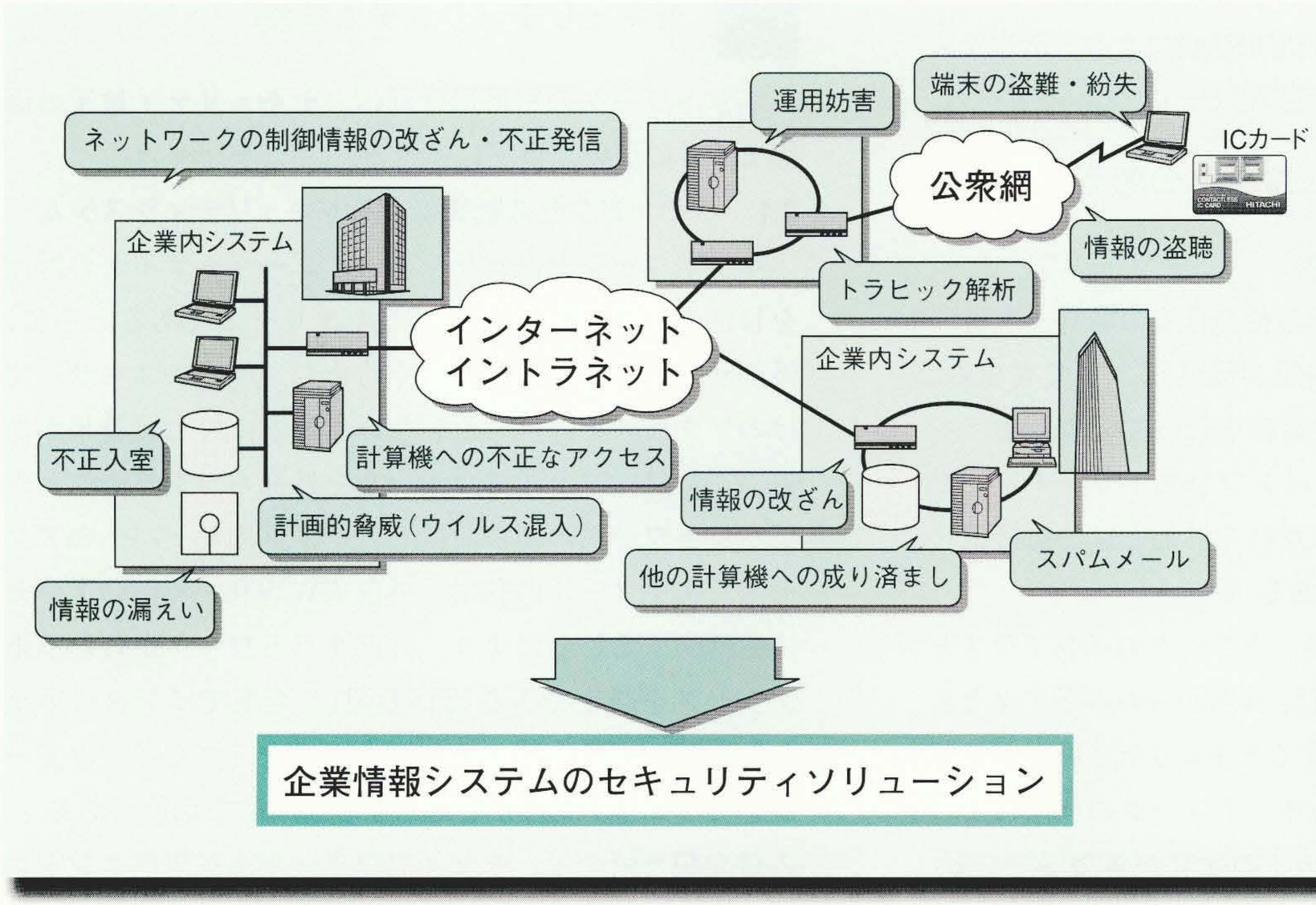
セキュア企業情報システムの構築提案モデル

Formulation Examples of Secure Enterprise Information Systems

角田光弘　*Mitsuhiro Tsunoda*　　一村政司　*Masashi Ichimura*
山田知明　*Tomoaki Yamada*



ネットワーク上の脅威とセキュリティ強化の必要性

近年，ネットワークへの侵入による犯罪が増加している。日立製作所は，企業内のデータ保護を目的とした，セキュリティについての総合的なサービスを提案している。

現在，インターネットやイントラネットでの企業のネットワークインフラストラクチャー構築が増加しつつあり，それに伴ってネットワーク上の犯罪も増加の一途をたどっている。ネットワーク上の犯罪は，その利用形態によって異なる。成り済ましによる内部ネットワークへの侵入やネットワーク上のデータの盗聴，ホームページの改ざんなどである。被害にあった企業では，信用の失墜，さらには法的問題に発展する可能性があり，コンピュータ業界を取り巻く社会問題となっている。

日立製作所は，企業の情報システムを守るため“Secureplaza”でトータルソリューションを提案しており，ユーザーのネットワーク運用に合わせて，適切なセキュア企業情報システムを提案，構築，運用している。

イントラネット環境では部門間でのセキュリティ，インターネット接続環境ではファイアウォールとVPN(Virtual Private Network)の導入，さらにエクストラネット環境での適切なセキュリティを提案する。このように，ネットワーク構成の規模や特性に応じてそれぞれのセキュア情報システムの対策モデルを提案している。また，サービスとしては，日立企業ネットワーク アウトソーシング サービス“Compassport”により，セキュリティシステムの計画，設計から監視，運用代行までを提案している。

1　はじめに

近年，インターネット上での犯罪が増加しつつあり，WWWサーバ上のページのハイジャックやスパムメール※）が頻繁に行われている。インターネット・イントラネットを利用した企業ネットワークのインフラストラクチャーが進み，さらにエクストラネットでの企業間ネットワークシステムの構築，運用が主流になりつつある中で，ネットワーク犯罪はもはや他人事ではなくなってきた。企業のデータを盗難したり，サーバをダウンさせるなどのネットワーク犯罪は，サイト運営している企業やネットワーク上で取引業務を行っている金融機関にとって，大きな問題となっている。WWWサーバ上のページの改ざんや顧客情報の盗難の被害にあうと，信用の失墜，法的責任など，ばく大な企業損失につながるからである。これらの危険性から企業の情報システムを保護するためには，守るべき対象を明確にし，コストに見合った最適なセキュリティ対策を講じる必要がある。

※）スパム：同じ内容や類似のものを，何度も出したり，無差別に送りつけること

日立製作所は，ネットワーク上のセキュリティに着目し，企業内のデータ保護を目的としたセキュリティについての総合的なサービスを“Secureplaza”で提案している。

ここでは，ネットワークの利用形態別による，情報システムセキュリティのシステム構築提案モデルについて述べる。

2 ネットワークセキュリティの考え方

2.1 ネットワークの利用形態

ネットワーク形態は，企業の業種や建屋の場所・規模，通信の頻度と運用費用など各種の要素によって異なる。インターネットを中心に取引業務を行っている企業，イントラネットでネットワークインフラストラクチャーを整備している企業，社内LANだけで外部とは一切接続していない企業などさまざまである。

例えば，インターネットをネットワークのインフラストラクチャーとしている企業では，外部からの不正アクセスやデータの盗聴などから身を守るセキュリティ対策が必要となってくる。また，利用するネットワークの種類によっても，ネットワークセキュリティの強度が異なってくる。一般に，ポイントーポイントで接続する専用線や公衆回線〔電話，ISDN(Integrated Services Digital Network)〕の強度は高いが，インターネットのようにルータを経由するオープンなネットワークの強度は低いと考えなければならない。ネットワークシステムを構築する場合やネットワークセキュリティを強化する場合には，これらの要素のすべてを考慮したうえで対策を講じる必要がある。

2.2 セキュリティポリシーの必要性

情報システムのセキュリティを強化するには，既成のセキュリティ製品を導入するだけでなく，どのプロトコル，どのユーザーについては通過させるか，DNS(Domain Name System)の設定はどうするか，WWWサーバ・メールサーバの設置場所は外部ネットワークか内部ネットワークかなどの諸条件を，ネットワーク運用に合わせて正しく設定する必要がある。この設定に必要な条件として，何を守るのか，どの脅威から守りたいのか，だれからどのように守りたいのかが入力条件となる。これらが「セキュリティポリシー」であり，(1) 脅威分析，(2) 保護対象の明確化，(3) 利用許可者・許可内容の整理，(4) セキュリティ実装方式の考え方・方針，および(5) 運用形態を明確化したものである。

日立製作所は，こうした経験とノウハウが必要となるセキュリティポリシーの作成を含め，セキュリティ分野の専門家による「ネットワークセキュリティコンサルテーション」を提案している。

3 インターネットシステムでのセキュリティシステム構築

ネットワークの利用形態別に，セキュリティ対策の構築モデルについて以下に述べる。

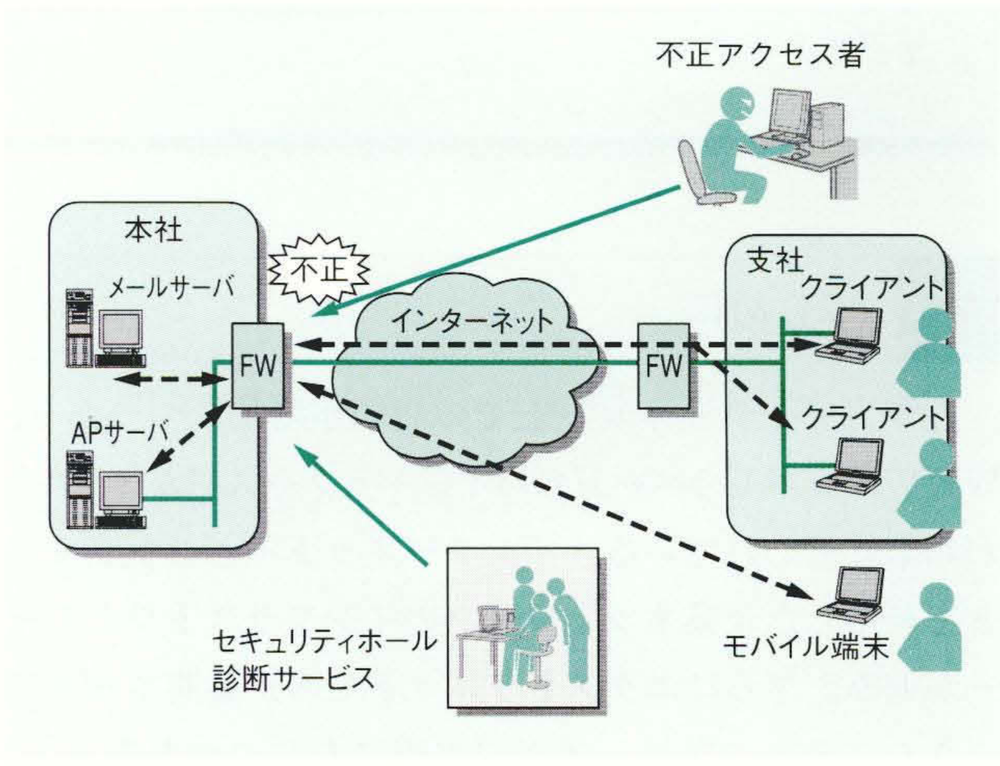
3.1 サイトアクセス制御によるセキュリティシステム

ネットワークセキュリティは，ユーザーサイトの保護を目的とした情報システムセキュリティである。主に，外部からの不正なアクセスを防止し，所定のユーザーだけのアクセスを許可したいという要求に対して効果がある。これは，ファイアウォールを外部ネットワークと内部ネットワークの間に設置し，サイト内サーバへのアクセス，電子メールの利用，外部WWWサーバへのアクセスを制御することにより，外部ネットワークからの不正アクセスを防止できる(**図1**参照)。企業でインターネットと接続してサービスを利用する場合，ファイアウォールをセキュリティのかなめとする基本的な形態である。

日立製作所では，ファイアウォール構築専門エンジニアが，強固なネットワークセキュリティシステムを実現するための設計を支援している。また，セキュリティポリシーを維持するために，ユーザーサイトにセキュリティホールがないかを診断するサービスを提案している。

3.2 VPNによるセキュリティシステム

このセキュリティは，ファイアウォールとVPN(Virtual Private Network)を利用したネットワークセキュリティである(**図2**参照)。例えば，出張先の営業員や



注：略語説明　FW(Firewall)，AP(Application Program)

図1　ファイアウォールによるアクセス制御
ファイアウォールの適切なポリシー設定により，不正アクセスからユーザーサイトを保護することができる。

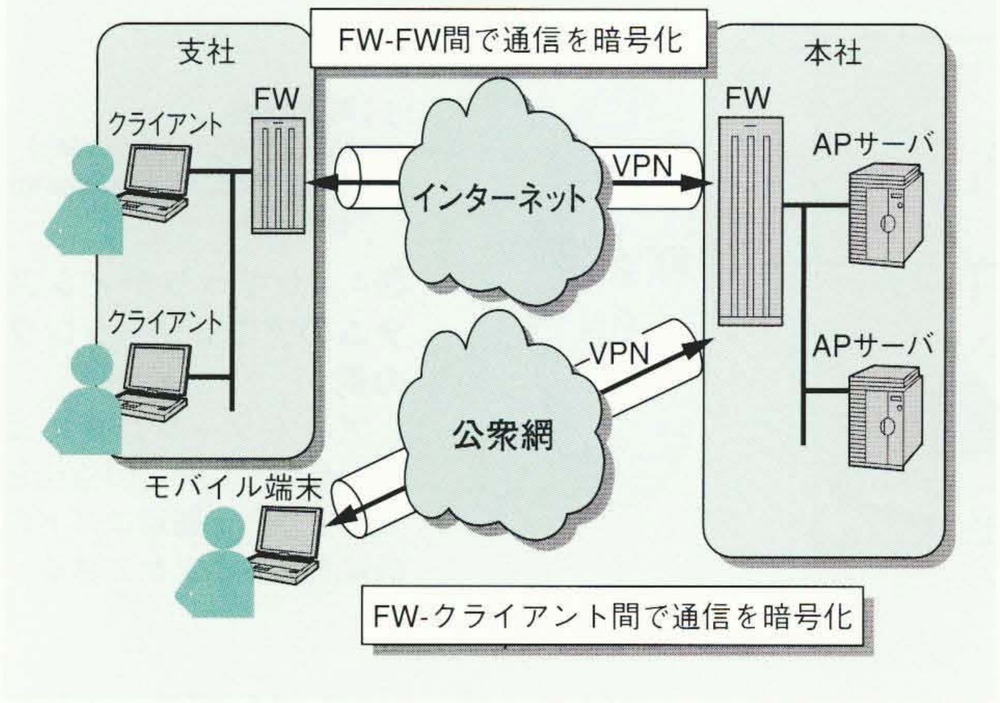


図2　リモートオフィスによるVPN通信
暗号を使用することにより，ネットワーク上での盗聴・盗難を防止することができる。

在宅勤務者が，モバイル接続でインターネットを経由してメールの送受信を行う場合に有効となるセキュリティである。VPN機能によって認証と暗号通信を実現し，パスワードや電子メールなどの暗号通信を，安全かつ低コストで行うことができる。これには，インターネットの利用が可能な場所ならどこからでも，安全に社内サーバにアクセスできるという利点がある。

日立製作所は，256ビットのかぎ長を持つ“MULTI2”で，世界最高水準の暗号技術を使用したVPN機能を提案しており，これにより，強力な暗号通信が実現できる。

VPNは，SOHO・モバイル接続でインターネットを利用する場合の必須機能となっている。さらに，インターネットで取引先と接続したり，会員向け情報サービスを行う際にも，セキュリティ対策として推奨する形態である。

4　イントラネットシステムでのセキュリティシステム構築

企業によっては，社内ネットワークでセキュリティポリシーの異なる部門が存在する場合がある。利用許可者や利用許可内容が異なる（例えば，人事情報サーバとウェブサーバ）システムでは，相互にアクセスを制御したいと考えるユーザーもいる。また，内部に悪意を持つ人員がいる場合，内部ネットワークでの犯罪の可能性も考えられる。これらの内部ネットワークセキュリティの強化にはサイト内複数（多段）ファイアウォールシステムが有効であり，かつシステムを安全に統合することができる。さらに，インターネットなど外部ネットワークに接続している場合には，ファイアウォールを多段に設置することにより，セキュリティの強度を向上させることができる。

日立製作所は，インターネットだけでなく，イントラネット環境内でイントラネットのセキュリティ強度に合わせた，適切なセキュリティを設計，提案している。社内でセキュリティポリシーの異なるLAN，部署，拠点を分ける場合に推奨する形態である。

5　エクストラネットシステムでのセキュリティシステム構築

エクストラネットとは，インターネットをバックボーンとしてイントラネットどうしを相互接続する情報システムネットワークであり，関連企業や関連グループで情報を共有し，統一的な情報システムを構築できる。セキュリティとしては，イントラネット・インターネットと同様のセキュリティ強化対策が有効となるが，企業間のデータのやり取りとなると機密情報が含まれる場合も多いため，特にVPNによる相手認証と暗号化が必要となる。関連企業や関連グループのすべてが同一のファイアウォールを使用している場合には，VPN機能を追加するだけで，比較的単純な構成で通信データの暗号化を実現することができる。異種ファイアウォールの場合には，システム間でVPN機能が必要となる（**図3**参照）。

日立製作所は，「Secure Socket Serverシステム」により，VPN機能を実現するプログラムプロダクトを提案している。この製品も，前述のMULTI2暗号技術により，かぎ長256ビットの強固な暗号通信を実現する。

また，証明書および認証のための運用基盤を，認証サ

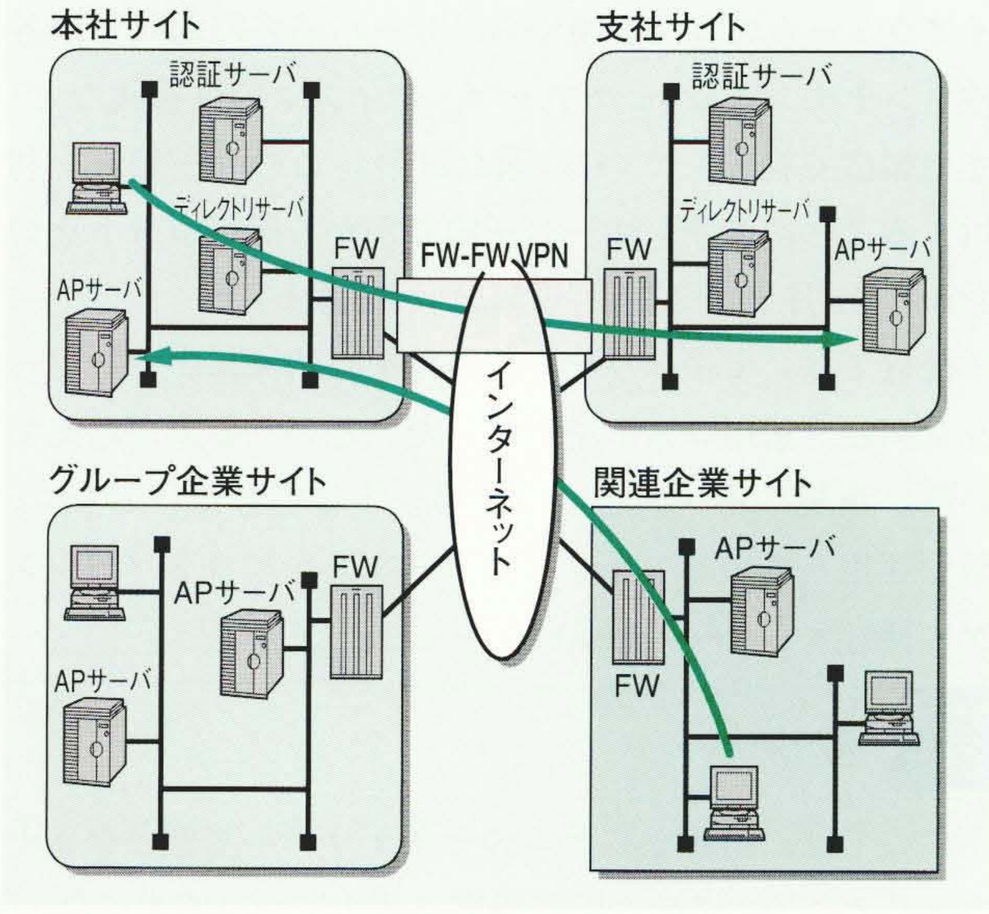
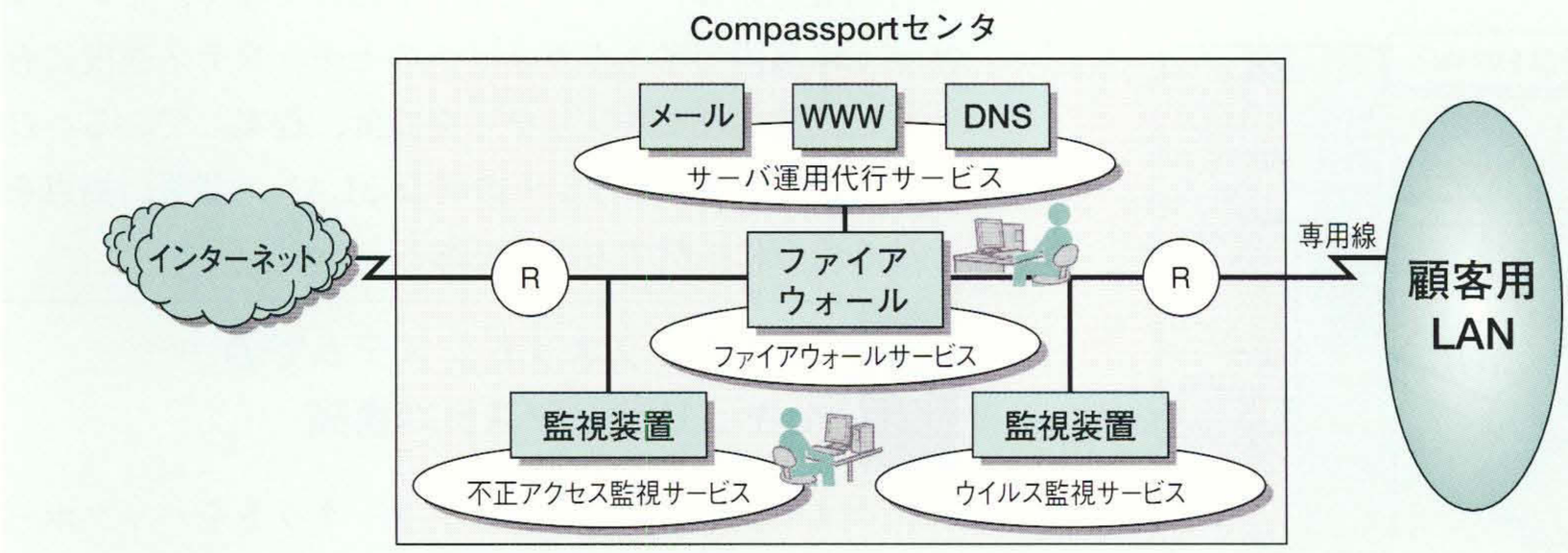


図3　エクストラネットによるシステム構成例
エクストラネットでのセキュリティでは，サイトアクセス制御，VPN，さらに認証機能についても考慮しなければならない。



注：略語説明
WWW(World Wide Web)
DNS(Domain Name System)
R(ルータ)

図4 セキュリティシステムのアウトソーシングの例
アウトソーシングにより，セキュリティの強化とセキュリティ運用コストの低減を図ることができる。

ーバとディレクトリサーバを組み合わせたシステムで実現できる。エクストラネットのような大規模ネットワークには必要となる機能である。

6 セキュリティシステムのアウトソーシング

ネットワークセキュリティシステムを構築するには，専門知識が必要となる。また，構築後のネットワーク運用時にも，セキュリティの監視だけでなく，各種サーバの監視，運用，メンテナンスのために専門員を配属し，常に監視できる体制が必要である。ユーザー側で365日，24時間運用を実現するには，最低でも月当たり4人の費用と専門技術者の育成を余儀なくされる。

このような負担を軽減するため，日立製作所は，セキュリティサービス実現のための「Compassportセンタ」を設置して，快適かつ安全なネットワーク運用を提案している。サービス内容は，セキュリティ専門家によるファイアウォールのログ監視から，サーバ障害時の対応，各種メンテナンス(バックアップ，ディスク容量監視など)まで幅広く提供している(**図4**参照)。このサービスを利用することにより，ユーザー側でかかる運用コストを約$\frac{1}{3}$から$\frac{1}{4}$(月当たり1人程度)に削減できる。

最近では，セキュリティの運用を専門家にアウトソーシングし，運用コストを削減したいという要望が増えている。新規にインターネット接続する場合だけでなく，現行運用しているファイアウォールでもアウトソーシングに移行するケースも多い。

7 おわりに

ここでは，情報システムのセキュリティ基盤となるセキュリティのシステム構築提案モデルについて述べた。

100%安全というセキュリティは存在しないと言ってよく，いかに効果的に対策を行い，いかに維持していくかがポイントと言える。そのため，日立製作所は，セキュリティポリシーを明確にし，それに応じたセキュリティ機能を選択,組み合わせた対策システムを構築し,さらに,セキュリティポリシーを維持するために,“Compassport”によるセキュリティサービスを展開している。

今後は，セキュリティ基準の国際標準化に伴って，ネットワークでの対策だけでなく，情報システム全体のセキュリティポリシーの作成と対策システムの構築がますます重要になるものと予想する。情報システムのセキュリティ対策についても，ネットワークセキュリティでのノウハウにメインフレーム・サーバシステムで培ったノウハウを組み合わせ，コンサルテーションを中心とするサービス商品を提案していく考えである。

参考文献

1) 金野，外：セキュア システム ソリューションとセキュリティ技術，日立評論，**80**，5，397～402(平10-5)

執筆者紹介

角田光弘
1987年日立製作所入社，情報・通信グループ 情報システム事業本部 情報システム事業部 ネットワーク＆サービス本部 ネットワークビジネス企画部 所属
現在，セキュリティ ソリューション サービスの企画・開発に従事
E-mail：tsunoda @ system. hitachi. co. jp

山田知明
1993年日立製作所入社，情報・通信グループ 情報システム事業本部 情報システム事業部 ネットワーク＆サービス本部 ネットワークビジネス企画部 所属
現在，セキュリティ コンサルテーション ファイアウォールのシステムインテグレーション業務に従事
E-mail：t-yamada @ system. hitachi. co. jp

一村政司
1986年日立中部ソフトウェア株式会社入社，日立製作所情報・通信グループ 情報システム事業本部 情報システム事業部 ネットワーク＆サービス本部 ネットワークビジネス企画部 所属
現在，ネットワークセキュリティ製品の拡販，構築に従事
E-mail：ichimura @ ts. hitachi. co. jp