エレクトロニックコマース・セキュリティ特集

UDC 342.738：681.324(100)：061.5.051 OKIDENKI

# 沖電気の情報セキュリティソリューション

## Oki Information Security Solution

矢野達朗 Tatsuro Yano
芦田元之 Asanobu Ashida

**要　旨**

インターネットを活用したビジネスが本格化するにつれ，情報セキュリティがビジネス戦略に欠かせないものになってきている。本稿では，情報セキュリティ対策の課題と効果的な情報セキュリティ対策を実現するための考え方について述べた後，沖電気の情報セキュリティソリューションを紹介する。

## 1．まえがき

近年，インターネットのビジネス利用が本格的になってきた。一方，Webページの書き換えや情報漏洩などの不正行為も数多く報告されており，深刻な問題になってきている。

インターネットビジネスにおいては，受発注データやプライバシー情報などの重要なデータを扱い，さらに多くの場合，企業内に存在する業務システムとインターネットを接続する必要がある。このため，これまで以上に情報セキュリティ対策が不可欠なものになってきている。

本稿では，情報セキュリティ対策の課題を整理し，効果的な情報セキュリティ対策の考え方を述べる。次に，沖電気のソリューションを紹介する。

## 2．情報セキュリティ対策の課題

一般に，不正アクセスに対するセキュリティ対策としては，ファイアウォールの設置だけにたよっている場合が多い。しかし，ファイアウォールだけのセキュリティ対策では不十分である。ファイアウォールは，送受信アドレスとプロトコルにより通信を許可するか否かを決定する。このため，許可されているプロトコルを利用した不正行為は防止できない。たとえば，Webサーバのセキュリティホールを利用すると，外部からWebサーバに対して任意のプログラムを送りこみ，実行させることが可能である。

いったん，Webサーバに侵入されると，Webサーバと連携する企業内システムへの不正侵入も心配される。システムの安全性を高めるために，ファイアウォールを２段構成にし，外部に公開するサーバは２つのファイアウォールの間に配置する構成を採用する場合がある。しかし，外部に公開するサーバを踏み台にして２段目のファイアウォールも突破される可能性は否定できない。さらに多段のファイアウォールを配置することも考えられるが，むやみにファイアウォールを増やしても，費用対効果が疑問である。

セキュリティホールの原因には，設定ミス，プログラムの欠陥などさまざまなものがある。プログラムの欠陥は，プログラム作成者が注意深くプログラム作成を行なえば問題はなくなるはずであるが，実際には，バッファオーバフローをはじめ，新しいセキュリティホールの発見が後を立たない。

## 3．情報セキュリティ対策の考え方

以上述べたように，情報セキュリティ対策にあたっ


矢野達朗
システムソリューションカンパニー　ビジネスソリューション事業部　ソリューション開発第一部　ソリューション開発第四チームリーダ


芦田元之
システムソリューションカンパニー　ビジネスソリューション事業部　情報セキュリティ担当部長

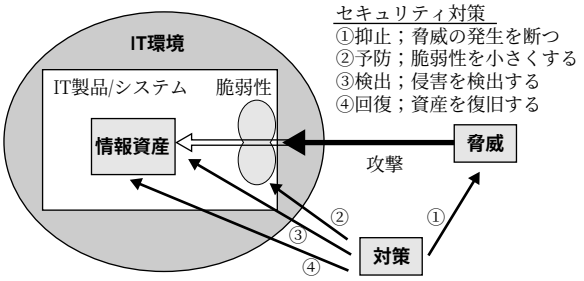


**図1　セキュリティ対策の考え方**
**Fig. 1　Concept of security protection**

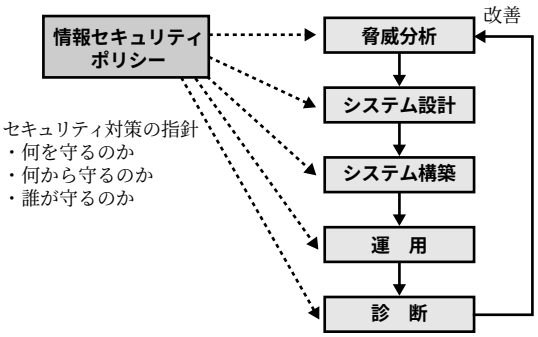


**図2　セキュリティ対策プロセス**
**Fig. 2　Process of security protection**

ては，いくつかの課題がある。これらの課題のうちの主なものは次の３つである。

- ファイアウォールで防止できない脅威への対処。
- 対策コストと実現されるセキュリティのバランス。
- 次々に発見される新しい脅威への対処。

これらの課題を解決するためには，脅威分析，セキュリティポリシー，セキュリティ診断と改善が有効である。これらにより，バランスの取れた，効果的なセキュリティ対策が可能となる。

（1）脅威分析

脅威分析は，国際セキュリティ評価基準ISO15408で採り入れられている設計手法である。脅威分析は，想定されるリスクを洗い出し，それぞれに対して対策を立案する。対策には，抑止，予防，検出，回復の４つの側面がある。図１に概念図を示す。

抑止は，セキュリティ脅威に対して直接的に作用して脅威をなくす対策である。ファイアウォール，アクセス制御，認証などが抑止対策に該当する。

予防は，コンピュータシステムの脆弱性を低減する対策である。最新のソフトウェアを使用してできる限りセキュリティホールのない状態に保つこと，リスクが低減されたセキュアなOSを使用すること，暗号化によるデータ保護などが予防対策に該当する。

検出は，加えられた脅威を検出するための対策である。改ざん検出，不正侵入検知が検出対策に該当する。不正侵入検知システムの詳細については，本誌の別稿を参照されたい[1)]。

回復は，発生した被害から元の状態に復旧するための対策である。バックアップとリストアのほか，被害が発生した場合の復旧計画などが必要になる。

（2）セキュリティポリシー

脅威分析では複数の対策が立案される。どの対策を採用するかは，セキュリティポリシーに基づいて判断することになる。セキュリティポリシーは，セキュリティに関する企業の方針を示すものであり，求められるセキュリティの度合いと対策コストおよび利便性とのバランスを決定する際の指針となる。なお，セキュリティポリシーは，情報システムだけでなく，従業員教育をはじめ企業の中のさまざまなセキュリティ活動に影響を及ぼす。セキュリティポリシーの詳細については，本誌の別稿を参照されたい[2)]。

（3）セキュリティ診断と改善

構築したシステムのセキュリティを維持していくためには，目的のセキュリティを達成しているかどうかを定期的に診断し，改善していくプロセスが重要である。図２にセキュリティ対策プロセスを示す。

## 4．沖電気のソリューション体系

当社では，以上の考察をもとに，情報セキュリティシステムのトータルソリューションを体系化した。図３にソリューション体系を示す。

情報セキュリティに関する知識および技術は，コンサルティングやシステム構築などの情報セキュリティサービスとして提供されている。情報セキュリティサービスを利用して，高信頼性を特徴とするシステム製品群および各種セキュリティコンポーネント製品を統合することにより，ECシステムなど高度なセキュリティが要求されるシステムの提供が可能となる。

情報セキュリティサービスは，情報セキュリティ対策プロセスの分析，設計構築，運用，診断の４つのフェーズに対応して支援サービスを定義している。各


**図３　沖電気の情報セキュリティソリューション体系**
**Fig. 3　Structure of Oki information security solution**

サービスの概要を以下に示す。

### 4.1　セキュリティコンサルティングサービス

セキュリティコンサルティングサービスは，セキュリティポリシーの作成や脅威分析の支援を行なうサービスである。

セキュリティポリシーの作成や脅威分析では，企業独自の基準だけではなく，ネットワーク社会で通用する内容が求められる。このためには，セキュリティ国際評価基準ISO15408，英国標準BS7799をはじめ各種のグローバルスタンダードに沿って，内容を策定することが重要である。

当社では，各種の標準化動向の調査研究を通して，コンサルティングに必要な技術を開発し提供している。

### 4.2　セキュリティシステム構築サービス

セキュリティシステム構築サービスは，セキュリティ製品の具体的な設定パラメータの設計や構築を行なうサービスである。

セキュリティをはじめインターネットに関連する技術の進歩は非常に速く，製品が成熟しないうちに新しい機能追加が行なわれる傾向にある。こういった状況においてシステムを期待通りに動作させるためには，技術動向を見極めた上で製品を選定し，システムに適用する前に，十分な動作検証を行なう必要がある。また，セキュリティホール対応などの最新の情報をシステム構築に反映させる必要がある。

当社では，あらかじめ典型的なシステム形態について脅威分析を行ない，ファイアウォール，セキュアOS，VPN（Virtual Private Network）などの必要となる製品を選定し，システムとしての動作検証と運用評価を実施している。また，各種ベンダーからのソフトウェアの更新情報およびCERTなどの機関から提供されるセキュリティ情報をシステム構築に反映させている。

### 4.3　セキュリティ運用監視サービス

セキュリティ運用監視サービスは，システム構築後の運用を支援するサービスである。当社では，不正侵入検知や改ざん検出などのセキュリティ監視，万が一不正行為が行なわれた場合のバックアップとリストアのシステムなど，各種運用支援システムを提供している。また，これらを使用したアウトソーシングサービスも提供している。本サービスにより，セキュリティを含めてシステムを効率的に運用することができる。

### 4.4　セキュリティレビューサービス

セキュリティレビューサービスは，企業のセキュリティ対策を総合的に診断するサービスである。セキュリティポリシー，規定から実際の運用に至るまで，企業のセキュリティをトータルに診断し，セキュリティの評価を行なうとともに，改善方法を提言する。本サービスにより，問題点を客観的に認識し，セキュリティ対策立案に活用することができる。

## 5．ソリューション適用例

典型的なインターネットシステムにおいて当社のセキュリティソリューションを適用した例を，図４に示す。脅威分析に基づき，暗号化，認証，アクセス制御，ファイアウォール，侵入検知，電子メールのウィルス

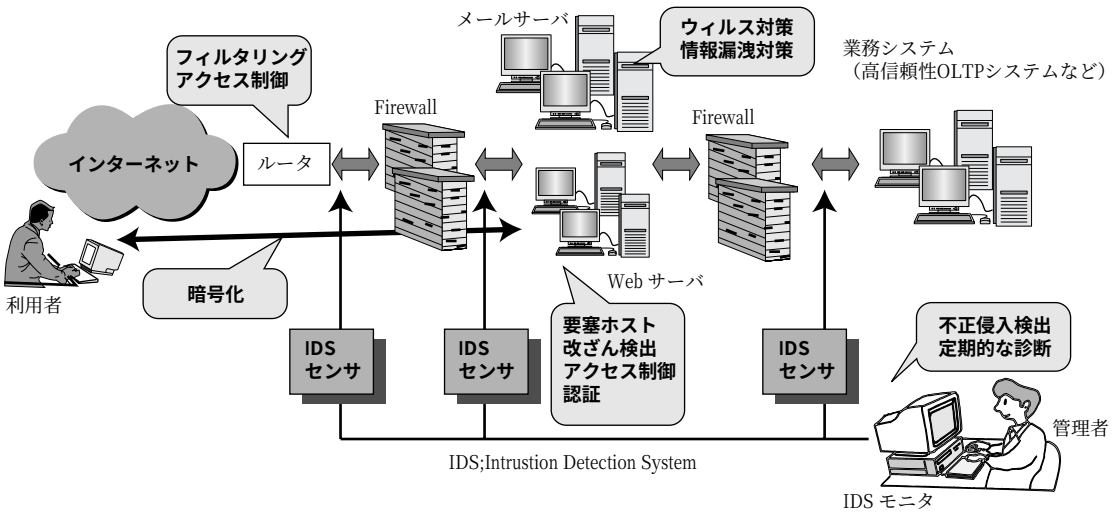


**図４　セキュリティシステム構築例**
**Fig. 4　Example of Oki security system**

チェックなどのセキュリティ対策を実施している。

ファイアウォール，Webサーバなど主要なコンポーネントは，クラスタ化により可用性を高めている。高可用性ファイアウォールについては，本誌の別稿を参照されたい[3)]。

Webサーバは，外部に公開するとともに，内部の業務系システムとも連携する必要があり，特にセキュリティの強化が必要である。通常のWebサーバには，セキュリティホールやWebサーバを踏み台とした内部への侵入の可能性がある。これらの脆弱性を極力小さくするために，HP社のVirtualVaultを採用している。

VirtualVaultは，米国のセキュリティ基準（通称オレンジブック）のBレベル相当の機能を盛り込んだ高信頼性OSを採用し，Web環境に最適化したシステムである。特権の細分化，プログラムの区分実行保護，内部システムとWebサーバを安全に連携させるTrusted Gateway機能，改ざん検出機能などを備えている。これらの機能により，Webサーバの脆弱性を構造的に解消して，高いセキュリティを実現している。VirtualVaultの概念図を図５に示す。

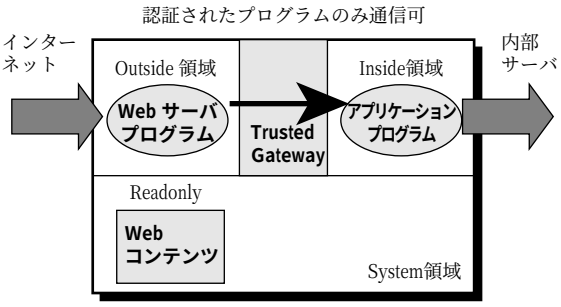


**図５　VirtualVault**
**Fig. 5　VirtualVault**

## 6. あ と が き

情報セキュリティ対策の考え方と，それを採り入れた沖電気の情報セキュリティソリューションの概要を述べた。今後は，具体的な用途別のシステムモデルの開発，検知方法を改善した侵入検知システムの製品化などに取り組む予定である。

## 7. 参 考 文 献

1）武内，他：侵入検知システム，沖電気研究開発第183号，7.2000
2）武内，他：セキュリティポリシー，沖電気研究開発第183号，7.2000
3）橘：高可用性ファイアウォール，沖電気研究開発第183号，7.2000