

価格性能比が抜群のUTM-1によって、安全なネットワークの構築とアプリケーション・サービスを提供できる環境が整いました。

株式会社ソーキ  
ICT戦略事業室室長  
藤田比呂文氏



## ユーザ



株式会社ソーキ

- 本社所在地：大阪市西区九条南4-2-4
- 設立：1989年4月
- 代表：代表取締役 都志益一氏
- 従業員：112名
- 事業拠点：大阪本社、東京営業所ほか全国6営業所

## 導入ソリューション

- UTM-1™
- Safe@Office 500™
- SmartDefense™
- SSL Network Extender™

## ニーズ

- インターネットを利用した顧客からの安全なリモート・アクセス環境
- 低コストの統合ゲートウェイ・セキュリティ・システム
- 運用負荷を低減できるアプライアンス製品
- 拠点の一律なセキュリティ環境

## チェック・ポイント選択のポイント

- 以前よりアプリケーション・レベルの防御機能およびSmartDefenseの評判を聞き、高く評価していたこと
- 各種の脅威防御に加えてSSL VPN環境が容易に構築できること
- 機種評価・選定の過程でチェック・ポイント（ベンダー）に直接コンタクトでき、情報やアドバイスを求めることができたこと
- チェック・ポイントのコア技術は歴史と実績があり、ベンダーの合併や吸収が頻繁にあるなかで、将来的にも継続的な提供・サポートが期待できること
- 構築～運用開始まで短期間でサービスを立ち上げられること

## 新たなアプリケーション・サービス事業のセキュリティ・インフラにUTM-1を採用 顧客からの安全なWebアクセス環境を実現

測量機・測定機・計測機器のレンタル・販売・修理業務や自動測量システムの開発・実測などを展開する株式会社ソーキ。同社は、3次元計測技術を使ったさまざまな分野における3次元アプリケーションサービスとして提供する新たなサービス事業の展開に乗り出した。顧客が工事現場や事務所、研究拠点などから、そのアプリケーションを安全に利用するためにデータセンターに統合脅威管理（UTM）アプライアンス「UTM-1™」を導入。低コストでファイアウォール、侵入防御、アンチウイルス、アンチスパイウェアおよびSSL VPN環境を実現した。また、同時に同社の各拠点に小規模向けUTMアプライアンス「Safe@Office 500™」を導入し、拠点間ネットワークのセキュリティ向上を実現した。

## 計測の多種多様なニーズに応えるソーキ

1989年創業のソーキは、「はかる」（測る・計る・量る・図る）というキーワードを事業コンセプトとする企業だ。メインの事業は測量機や測定機、各種計測機器のレンタルを中心に、販売および修理業務。取り扱う計測機器の分野は非常に広範囲で、世界最先端、最高の計測技術を有する土木・建築業向け測量機器をはじめ、水質測定器、騒音・振動測定器、気象観測機器、非破壊検査器など、「はかる」ことに関する機器を世界中から調達して、レンタルや販売事業を展開する。また、それらの計測機器をメンテナンスする専任技術者を抱え、常に最良の状態を機器をレンタルできることは他社にない優位性だ。

また同社の信頼性と技術力が評価されている分野に自動測量・自動計測システムがある。例えば、トンネルや地下掘削工事において掘削位置を高精度にマーキングしたり、自動追尾式の測量器によってシールド・マシンの位置を正確に管理して精度の高いシールド掘削管理を支援する、あるいは防波堤などになるケーソンを沈埋する作業でケーソンの3次元位置をリアルタイムに追尾し、計測データを即時表示するボックス誘導システムといったものがある。こうした特殊測量の自動化では、日本で初めて取り組んだ歴史と1000を超える現場実績のノウハウで海外でも高い評価を得ている。

「各メーカーの最先端の測量機器を完備し、それにデータ処理のためのシステム開発やカスタマイズを行い、システム・アップしたソリューションとして提供できることが当社の優位性です」。ICT戦略事業室 室長 藤田比呂文氏は、同社のコア・コンピタンスをこう強調する。



ICT戦略事業室室長 藤田比呂文氏

そうした同社の測量計測ソリューションの中で、3次元計測技術を使ったさまざまな分野における3次元モデル化の新たなソリューションがある。レーザー光を測定対象物に照射し、対象物の正確な3次元の位置座標を計測し、3次元モデルとなる点群データを生成するもの。例えば、3Dレーザー・スキャナーで空間をスキャンして点群データを生成。この点群データから、3Dモデリング・ソフトウェアを使用して3D CADデータへ加工を行い、3DソフトやVR(仮想現実)ソフト上で展開できるフォーマットに変換。それをレンダリング・ソフトウェアなどを使ってリアルな質感のある空間写真に仕上げたり、VRソフトで仮想空間のリアルタイムなウォークスルー画像を生成したりするものである。

## スキャン・データを3Dモデリング化する アプリケーション・サービス事業にチャレンジ

3Dレーザー・スキャン・システムのような測量機とシステムをまるごとレンタルする場合もあるが、ソーキでスキャン・データを預かって3Dモデリング化してCADデータなどで提供するケースもある。

「通常は、圧縮したデータを媒体で持ち込んでいただき、それを当社のシステムで処理し、モデリングした成果を納品することになりますが、その成果を検証しながら現場で作業をすることになり、物理的な時間のロスが生じてしまいます。例えば、トンネル掘削中に測量したデータを基にした3Dモデルを建設現場のゼネコンの事務所で、ほぼリアルタイムに検証しながら作業を進めたいという要望があります。モデリングのためのシステムは当社のデータセンターで用意するので、それを現場からリモートで利用してもらえらるASPのようなサービスを事業として展開することになりました」(藤田氏)と、新たなサービス事業展開の背景を述べる。

土木・建築現場の多くは、工事現場および工事現場近くの作業所、JV(共同企業体)の事務所があるのが一般的。JVの事務所は寄り合い所帯であり、ゼネコン各社の拠点とのネットワークはそれぞれ個別に敷設されている。したがって、計測したデータからモデリングした成果をJVの各社ネットワーク経由でソーキに、それぞれアクセスして利用することは各社の

セキュリティ・ポリシーがそれぞれ異なるために、現実的にはなかなか難しい問題がある。

そこでソーキでは、現場作業所やJV事務所、各ゼネコンの拠点からそれぞれ同社のデータ・センター(東京営業所)にインターネット経由でアクセスしてアプリケーションを利用できるネットワーク環境を構築している。現場事務所の各社のPC環境はばらばらであり、決して十分な設備が用意されているとは限らない。もちろんインターネット経由で安全なアクセスを実現するための手段としてVPNが必要だが、IPsec VPNのようなクライアント・ソフトが必要な環境は利用できない。そうした状況の中でアプリケーション・サービス事業を立ち上げるためには、どこからでも容易にデータ・センターにアクセスして、計測データを転送してアプリケーションを利用したり、成果を閲覧できる安全なネットワーク環境を構築できるゲートウェイ・セキュリティ・システムが必要だった。

## Web経由で安全なアプリケーション 利用を実現したUTM-1

こうしたソーキの新事業における課題を解決するために導入されたのが、チェック・ポイントの統合脅威管理ソリューション「UTM-1」だ。また、同社はこれまで大阪の本社および全国7カ所の営業所でファイアウォール/VPNアプライアンスを導入し、本社の基幹系業務システムやファイル・サーバへアクセスするためのスター型のVPN網を構築していた。しかし、導入していたアプライアンスの運用に不満があったことに加え、東京営業所のデータセンターにUTM-1を導入したのを機に、各拠点のセキュリティ・ツールを1つのベンダーに統一し、運用レベルを一律に保つために、各拠点で使用していた他社のアプライアンス製品を全てチェック・ポイントのSafe@Office 500に移行した。

計画当初は、データ・センターにインターネットからのアクセスに対して、汎用サーバとファイアウォール/VPNソフトでゲートウェイを構築することも検討した。しかし、OSやセキュリティ・ソフトのインストールなど構築作業もさることながら、社内システム、ネットワーク運用を藤田氏一人が担っているのが現状で、極力、運用負担を軽減したいという思惑があった。また、新事業のためのプラットフォームを早急に構築するため、簡単に導入と管理が行えるアプライアンス製品が前提条件とされた。



各社の測量機器をメンテナンスする専任技師が、最良の状態で機器をレンタルできるよう整備する。この保守体制がソーキの強みでもある。

「OSのセキュリティ・パッチ管理、セキュリティ・ソフトの管理、さらにハードウェアの保守など管理対象が増えれば負担が大きくなります。それは極力避けたいため、アプライアンス製品がベターだと判断しました」(藤田氏)。

加えて、顧客のそれぞれのネットワーク環境から容易にアクセスできるようSSL VPN機能が利用できること、ウイルスやワームなどインターネットの脅威を極力シンプルなシステムで防御したいという要件から、脅威を統合的に管理できるUTM-1の導入を計画したものである。

「もともとアプリケーション・レベルの防御機能や新たに登場する脅威にも簡単なアップデートで対応する事ができるSmartDefenseの評価を聞いており、FireWall-1®を使ってみたいという考えがありました。ところが、新事業のユーザ数がどれほどになるのか予測できず、正確なプランがたてられないという危惧がありました。そこへユーザ数の制限がなく価格性能比が抜群のUTM-1が発売され、すぐに飛びついたというのが実状です」(藤田氏)とし、チェック・ポイント製品に対するそれまでの評価とUTM-1を選定した理由を語る。

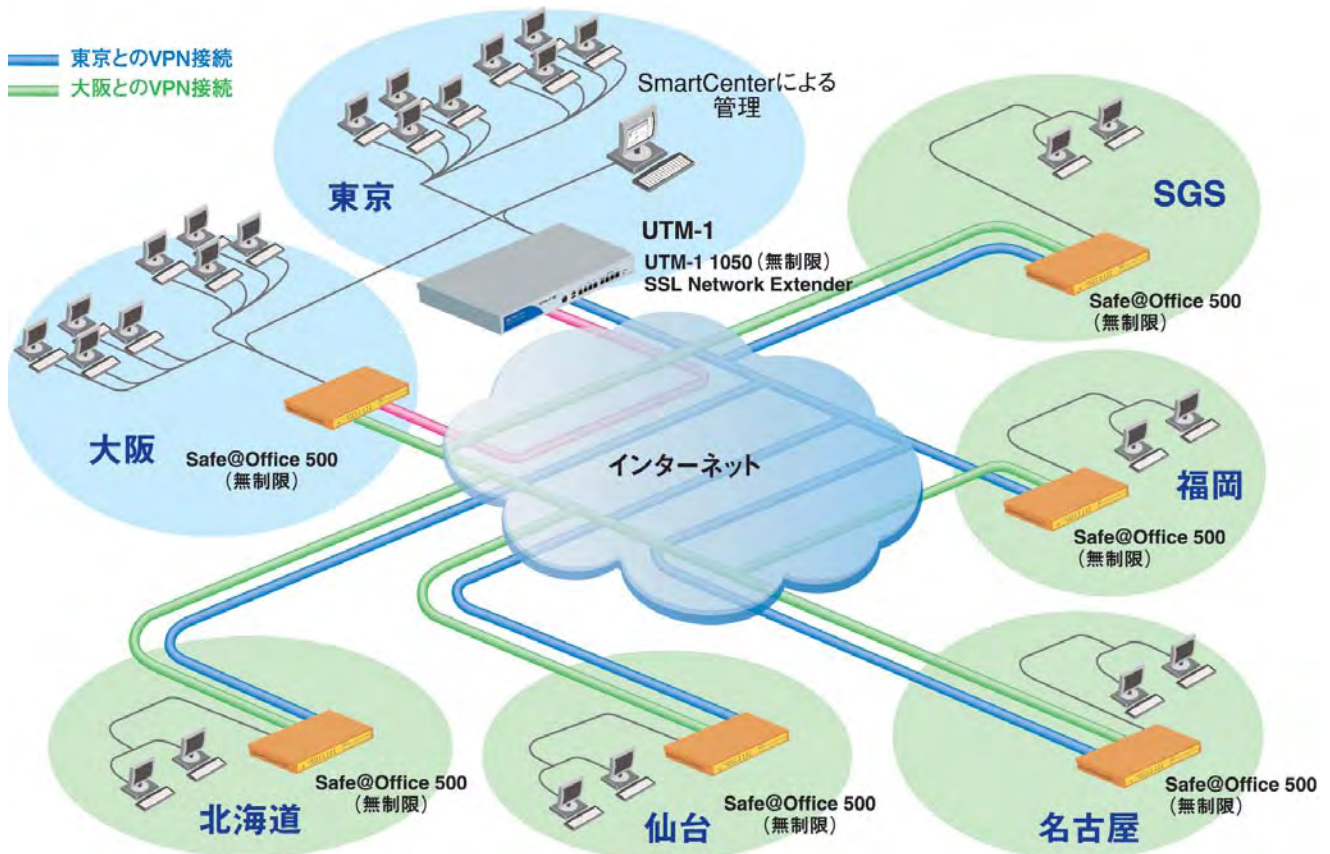
また、機種を評価・選定する過程において、チェック・ポイントに直接コンタクトでき、さまざまな製品情報やアドバイスを提供してくれたことも、他のベンダーとの大きな違いであったと藤田氏は強調している。導入されたモデルは、転送する計測データが高圧縮ソフトを使っても1GBに達するため、ファイアウォール・スループットを考慮し、UTM-1 1050が導入された。また、Web経由でセキュアなFTP転送、アプリケー

ション・アクセスを可能にするため、「SSL Network Extender」を機能追加した。利用している機能は、このSSL VPNに加え、UTM-1に実装されているファイアウォール、侵入防御、アンチウイルス、アンチスパイウェアなどほぼすべてのセキュリティ機能を運用している。

3Dモデリングのアプリケーションは、データセンター内に顧客ごとの仮想サーバ環境を構築し、顧客はインターネット経由でWindows Serverのターミナル・サービスを利用して、それぞれのサイトにアクセスすることができる。

一方、従来の社内の拠点間ネットワークは大阪本社を中心としたスター型のVPNネットワークを構築していたが、基幹系業務システム以外のグループウェア、ファイル・サーバを東京営業所のデータ・センターに移行したこともあり、それぞれの営業拠点にSafe@Office 500を導入、メッシュ型のネットワークに切り替えた。

「データ・センターのゲートウェイ・セキュリティの構築がUTM-1によって、当初の予算額より大きく削減できたため、その予算で各拠点にSafe@Office 500を導入することができました。せっかく主要拠点をUTM-1でセキュリティを強化しても、各拠点のセキュリティ・レベルに差があると、その各拠点のセキュリティが脆弱なポイントとしてセキュリティ・リスクになってしまいます。チェック・ポイントの同じUTM製品であるSafe@Office 500に統一することによって運用が容易になったことに加え、セキュリティ・レベルを一律に高めることが可能になりました」(藤田氏)。



東京と大阪を中心とした、サイト間VPNを構築。各拠点のSafe@Office 500は、ファイアウォール、VPN機能のほか、ウイルスチェックやSmartDefenseによるIPS機能を利用。管理は大阪又は東京より全てのアプライアンスをリモート管理。

# UTM-1の冗長化で可用性を向上、さらなるサービス事業の拡大をめざす

チェック・ポイントのUTM-1およびSafe@Office 500を導入することにより短期間でのセキュリティ・インフラの構築を実現し、ソーキのアプリケーション・サービス事業の早期立ち上げに大きく寄与した。そして、ファイアウォール、侵入防御、アンチウイルス、アンチスパイウェア、SSL Network Extenderによる安全なWebアクセスというさまざまなセキュリティの機能要件に対してシンプルな環境で、かつコストを抑えてそれを実現できた。

「現場の作業所やJVの事務所、ゼネコンの拠点や研究所などさまざまな拠点から容易に、かつ安全にアプリケーションを利用できるようになり、モデリングした3次元画像を検証しながら作業できる環境が整いました。データ計測からモデリングまでの時間を大幅に短縮でき、工期短縮に貢献できるとともに、それぞれの拠点から同時アクセスしてWeb会議などでリアル・タイムな検証作業をしながら工事が進めるといったことも可能になります」(藤田氏)と導入の効果を指摘する。

また、社内の拠点間ネットワークにおいても、以前は大阪本社にIPsec VPNでアクセスしていたためクライアント・ソフトウェアの運用管理が負担になっていたが、Safe@Office 500によるサイト間VPNを実現でき、セキュリティレベルの向上とともに運用管理の向上も成し遂げることができたという。

今後、同社は3次元スキャンニングのモデリング・アプリケーション・サービスに留まらず、計測データを加工処理するさまざまなアプリケー

ション・サービスを提供していく計画だという。そうしたサービス分野の拡大、あるいはサービス利用顧客数の増大に向けて、ネットワーク・インフラの可用性を高めるため、UTM-1やインターネット・アクセス回線の二重化を実施していく予定だ。

「サービス提供を始めてみると、ミッション・クリティカルな業務アプリケーションでなくとも、顧客ユーザは安全性の次にネットワークの信頼性・可用性への要求が高いことがわかりました。まずはClusterXLを使用してUTM-1アプライアンスのクラスタ化を実施して可用性を高めることを実現し、次にインターネット・アクセス回線の二重化もしくはアクセス回線の二重化(マルチ・ホーミング)によってネットワークの信頼性向上を実施していきたいと考えています」(藤田氏)。

また、提供するアプリケーション・サービスによっては、顧客企業サイトにVPN-1 UTM Edgeを導入し、アプリケーション・サービスの提供に加えて、ネットワーク機器の監視サービスも含めた新たなサービスも創出していきたいという。

最後に藤田氏は、新たなサービス事業の展開においてプラットフォームの選定・採用について次のように述べている。

「サービス事業を展開する上では、そこで利用する製品あるいは技術は永続的に提供されるものでなければ、安心して採用することはできません。ベンダーの買収・統合などによって製品ラインナップから消滅したり、継続的なコア技術の進化が止まってしまう製品も多々あります。その点でチェック・ポイントは、歴史と実績のあるコア技術を常に進化させたソリューションを提供しており、安心して使い続けられる製品だと確信しています」(藤田氏)。

## チェック・ポイント製品導入のポイント

お客様のチャレンジ	導入ソリューション	導入効果										
<ul style="list-style-type: none"> <li>インターネット経由でVPNを利用した安全なリモート・アクセス環境の構築</li> <li>低コストで高いセキュリティを実現する統合ゲートウェイ・セキュリティ・システムの構築</li> <li>すべての拠点間で矛盾のない統一されたセキュリティ環境の構築</li> <li>さまざまなセキュリティ機能が統合されたゲートウェイによる集約効果と、すぐれた導入効果</li> <li>常に最新の脅威に対応でき、アプリケーション・レベルの防御を利用することによる安心度のアップ</li> <li>アプリケーションサービスによる新事業の立ち上げ</li> </ul>	<table border="1"> <tr> <td>製品名</td> <td></td> </tr> <tr> <td>UTM-1</td> <td> <ul style="list-style-type: none"> <li>データ・センター・サイトのゲートウェイセキュリティ</li> <li>拠点間VPN</li> <li>IPS機能</li> <li>アンチウイルス機能</li> </ul> </td> </tr> <tr> <td>Safe@Office 500</td> <td> <ul style="list-style-type: none"> <li>リモート拠点セキュリティ</li> <li>拠点間VPN</li> <li>IPS機能</li> <li>アンチウイルス機能</li> </ul> </td> </tr> <tr> <td>SSL Network Extender</td> <td> <ul style="list-style-type: none"> <li>SSL VPNアクセス環境</li> </ul> </td> </tr> <tr> <td>SmartDefense</td> <td> <ul style="list-style-type: none"> <li>IPS機能</li> </ul> </td> </tr> </table>	製品名		UTM-1	<ul style="list-style-type: none"> <li>データ・センター・サイトのゲートウェイセキュリティ</li> <li>拠点間VPN</li> <li>IPS機能</li> <li>アンチウイルス機能</li> </ul>	Safe@Office 500	<ul style="list-style-type: none"> <li>リモート拠点セキュリティ</li> <li>拠点間VPN</li> <li>IPS機能</li> <li>アンチウイルス機能</li> </ul>	SSL Network Extender	<ul style="list-style-type: none"> <li>SSL VPNアクセス環境</li> </ul>	SmartDefense	<ul style="list-style-type: none"> <li>IPS機能</li> </ul>	<ul style="list-style-type: none"> <li>UTMアプライアンスによる短期間でのセキュリティ・インフラの構築</li> <li>シンプルなゲートウェイ・セキュリティ環境を低コストで実現</li> <li>各拠点のセキュリティ・レベルの一律的な向上</li> <li>さまざまなセキュリティ機能が統合されたゲートウェイによる集約効果と、すぐれた導入効果</li> <li>常に最新の脅威に対応でき、アプリケーション・レベルの防御を利用することによる安心度のアップ</li> </ul>
製品名												
UTM-1	<ul style="list-style-type: none"> <li>データ・センター・サイトのゲートウェイセキュリティ</li> <li>拠点間VPN</li> <li>IPS機能</li> <li>アンチウイルス機能</li> </ul>											
Safe@Office 500	<ul style="list-style-type: none"> <li>リモート拠点セキュリティ</li> <li>拠点間VPN</li> <li>IPS機能</li> <li>アンチウイルス機能</li> </ul>											
SSL Network Extender	<ul style="list-style-type: none"> <li>SSL VPNアクセス環境</li> </ul>											
SmartDefense	<ul style="list-style-type: none"> <li>IPS機能</li> </ul>											

### 製品に関するお問い合わせ

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社

〒160-0022 東京都新宿区新宿5-5-3 建成新宿ビル6F <http://www.checkpoint.co.jp/> E-mail: [info\\_jp@checkpoint.com](mailto:info_jp@checkpoint.com) Tel : 03 (5367) 2500

©2003-2007 Check Point Software Technologies Ltd. All rights reserved.

Check Point, AlertAdvisor, Application Intelligence, Check Point Express, Check Point Express CI, Check Pointのロゴ, AlertAdvisor, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoreXL, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, Hybrid Detection Engine, IISecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpect, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protectorm, Policy Lifecycle Management, Provider-1, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecureRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Sentivist, SiteManager-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, UTM-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecureRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, Zone Labsのロゴは、Check Point Software Technologies Ltd. あるいはその関連会社の商標または登録商標です。ZoneAlarm is a Check Point Software Technologies, Inc. Company. その他の企業、製品名は各企業が所有する商標または登録商標です。本書に記載された製品は米国の特許 No.5,606,668, 5,835,726, 5,987,611, 6,496,935, 6,873,988, 6,850,943, および7,165,076により保護されています。その他の米国における特許や他の国における特許で保護されているか、出願中の可能性があります。

PN 950001-J 2007.09 ※記載された製品仕様は予告無く変更される場合があります。