



## 常磐大学 チェック・ポイント製品の統合ソリューションで キャンパス・ネットワークのセキュリティを構築

### 常磐大学について

1966年に短期大学として設立された常磐大学は、幼稚園から大学院まですべての教育課程を擁する私立の学校法人です。2005年5月に同大学は、キャンパス全体の教育・研究における利便性を図るとともに関連する授業を効率よく進めることを目的に、情報メディアセンターを開設しました。ネットワークのセキュリティに関しては、チェック・ポイント・ソフトウェア・テクノロジーズ(以下チェック・ポイント)のソリューション、VPN-1/FireWall-1、SmartDefense、およびInterSpectが導入されています。

### 課題

情報メディアセンターの担う役割について、人間科学部教授であり同センター長である阿部昌信氏はこう強調しています。「企業はさらなる最先端のハードウェアやソフトウェア開発に注力し、ブロードバンド・プラットフォームの進展を進めています。しかしながら中小企業においては、その最先端のプラットフォームを活かすコンテンツなどのソフトウェア部分の開発や活用といった点が手薄になっていると考えています。Webプログラミングやコンピュータ・グラフィックス、デジタル映像制作などデジタルメディア系の情報技術を習得した人材を養成することが情報メディアセンターの大きな役割であり、そうした人材を中小企業に送り込もうというのが目的です。」

情報メディアセンターは、コンピュータ施設をはじめ、映像制作のスタジオや機材など、デジタル系の設備を充実。コンピュータ関連の教室や施設などを統合・集中させることによって、離れた場所にあってもネットワークでつながれた学部・学科間で情報を共有することが可能です。その結果、教育・研究の利便性を高める環境が整備されました。

常磐大学では学術情報ネットワーク(SINET)に参加する形で、1995年にインターネットへの接続を開始しました。教職員や学生のニーズがWebやメール以外のさまざまなアプリケーションへと急速に拡大する中で、ネットワーク帯域の増強と可用性確保の課題が持ち上がっていました。情報メディアセンターのシステムエンジニア、根本知計氏は「さまざまなインターネット利用に関するニーズに応えるためにネットワークを増強し、利便性を高めていくことは重要。また、一般学生がインターネットを自由に使える環境にする上で、絶対に必要だったのがセキュリティ対策でした」と、ネットワーク増強と可用性確保の一方で、セキュリティに対する課題を述べています。

### チェック・ポイントのソリューション

同大学はSINETに接続した翌年に、業界で最も高いシェアを誇る境界ファイアウォールVPN-1/FireWall-1を導入しました。環境適合性が高くインテリジェント性を兼ね備えた検査技術であるINSPECT技術が採用されており、ネットワーク層とアプリケーション層の両レベルでの保護を提供します。

### ユーザ

学校法人 常磐大学

### 分野

教育

### チェック・ポイント製品

- VPN-1® Pro™/FireWall-1®
- InterSpect™
- SmartDefense™

### ニーズ

- 不変なアーキテクチャでありながら、新たな脅威に対応して進化するセキュリティ・インフラストラクチャ
- 強力な境界セキュリティ
- 無線LAN向け内部セキュリティ

**「VPN-1/FireWall-1を高く評価する点は、当初から基本的な考え方が確立されており、それがバージョンアップしても、新しい脅威が登場しても、その基本技術で対応し続けていることです」**

常磐大学 情報メディアセンター  
システムエンジニア  
根本知計氏



チェック・ポイントは、境界、内部、WEBなど、ネットワークのあらゆる局面に対するセキュリティ・ソリューションを提供します。これにより、企業はネットワークや、ネットワーク・リソース等を安全に保護しながら、高い接続性を実現するリモート・アクセスを提供し、簡単に管理することができます。

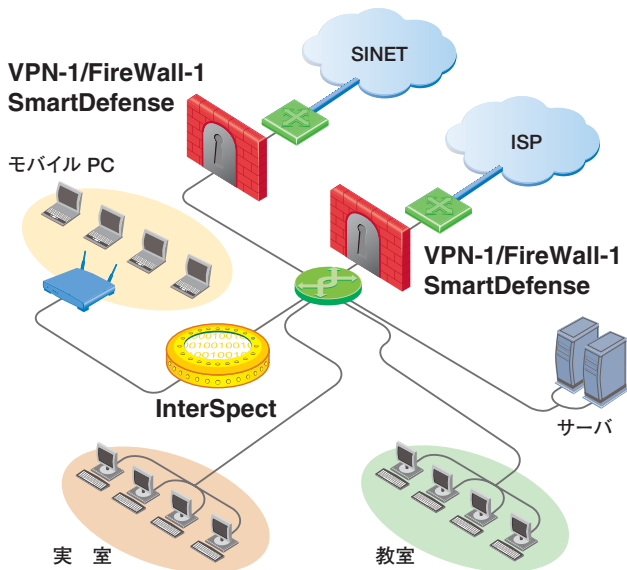
無線LAN環境が整備されて、教職員や学生が自分のモバイルPCをキャンパス・ネットワークに接続し利用できるようになりました。その結果、外部からの脅威だけでなく、セキュリティ対策が不十分なモバイルPCによる、内部からの脅威に対するネットワーク保護も重要な課題になっていました。

こうした課題に対して常磐大学は、チェック・ポイントのInterSpect™内部セキュリティ・ゲートウェイを採用しました。InterSpectはセキュリティに不備があるかもしれない外部から持ち込まれる個人のモバイルPCから、内部ネットワークを保護します。ワームの拡散やその他のネットワーク内部の攻撃を防止する機能を備えており、内部ネットワークを保護されたセキュリティ・ゾーンに学部別にセグメント化し、攻撃やワームを拡散する感染デバイスが検出されると、ネットワークを隔離してネットワークを越えて被害が拡散することを食い止めます。

また同大学は、進化するインターネット・セキュリティ脅威に先手を打つために、SmartDefense™サービスを契約しています。同サービスにより、セキュリティ上の問題や脆弱性が公表された場合には、即座にチェック・ポイントのセキュリティ・インフラストラクチャに取り込み利用できるアップデートがリアルタイムに提供されるほか、セキュリティ・アドバイザリが提供されます。

### チェック・ポイントのセキュリティの利点

1996年のFireWall-1選定にあたっては、同大学では2つの要素が重視されました。使いやすいインタフェースにより、複数のファイアウォールを導入した場合でも、日常の管理作業が大幅に簡素化されること、および、ソフトウェア・ファイアウォールであることから既存のUNIXサーバで稼働できることでした。



常磐大学は、ネットワークの脅威に対する統合ソリューションとして、チェック・ポイントの境界および内部セキュリティ製品を採用しています。

### 安定したネットワーク・セキュリティの基盤

「VPN-1/FireWall-1を高く評価する点は、当初から基本的な考え方が確立されており、それがバージョン・アップした場合や、新しい脅威が登場した場合でも、その基本技術で対応し続けていることです。基本的な考え方とは、データ(パケット)の状態を監視・精査し、その通信に必要なデータだけを自動的に通過させるというルールが確立されていることです。新しい脅威に対して事前防御する目的で導入したSmartDefenseサービスもこの基本的な考えを踏襲したものであり、インタフェースも同じで使いやすいという理由で採用しました」と根本氏は評価しています。

根本氏が評価するチェック・ポイントの基本的なアーキテクチャは、同社のコア技術「INSPECT」で、このINSPECT技術をベースにそれ以降に登場した新しいセキュリティ・技術であるApplication Intelligence™、SmartDefense等へ拡張され、さまざまな製品に実装されてきています。この技術によって、単純なパケットの悪用から大きな影響を及ぼす高度な攻撃まで、あらゆる種類のネットワークやアプリケーション・レベルの攻撃からネットワークを確実に保護することができます。

また、チェック・ポイントの内部セキュリティ・ゲートウェイ製品であるInterSpectと同様の機能を持つ他社製品と比較検討した結果、他社製品はモバイルPCなどの検疫とセキュリティ不備の場合の対策に重点が置かれていることを、根本氏は指摘しています。

「持ち込みPCのセキュリティ対策は自己責任であり、あくまでも内部ネットワークを保護するという目的にInterSpectが合致していました」と、同氏は述べています。現在同大学では、持ち込みPCのLAN接続は、情報メディアセンターの特別にセグメント化されたエリア内に制限していますが、今後学生や教職員が接続できるエリアの数を増やす予定です。

### 今後の計画

情報メディアセンターの完成を機に常磐大学のキャンパスバックボーンは2G~8Gbpsに増強され、教室や研究室には10Mないし100Mbpsで敷設されています。現在、第2期工事を進めており、各研究室までがギガビット・ネットワークへ拡張される予定です。

「DoSやSQLインジェクション攻撃など片っ端からIPアドレスをなめる攻撃は頻繁に検知していますが、今まで一度も被害に遭ったことがないことが、VPN-1/FireWall-1とSmartDefenseの最大の導入効果です。情報メディアセンターの完成をはじめ、バーチャルスタジオの構築なども進めており、今後さまざまなトラフィックがすべてキャンパス・ネットワークを利用ようになる予定で、セキュリティを含めたしっかりと運用がますます重要になってきます」と、根本氏は語ります。

©2003-2005 Check Point Software Technologies Ltd. All rights reserved.  
 Check Point, Application Intelligence, Check Point Express, Check Pointのロゴ, AlertAdvisor, ClusterXL, Cooperative Enforcement, ConnectControl, Connectra, CoSa, Cooperative Security Alliance, Eventia, Eventia Analyzer, Eventia Reporter, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, IMSecure, INSPECT, INSPECT XL, Integrity, InterSpect, IQ Engine, NGX, Open Security Extension, OPSEC, Policy Lifecycle Management, Provider-1, Safe@Home, Safe@Office, SecureClient, SecureKnowledge, SecurePlatform, SecuRemote, SecureXL Turbocard, SecureServer, SecureUpdate, SecureXL, SiteManager-1, SmartCenter, SmartCenter Pro, Smarter Security, SmartDashboard, SmartDefense, SmartLSM, SmartMap, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartView Tracker, SofaWare, SSL Network Extender, Stateless Clustering, TrueVector, Turbocard, UAM, User-to-Address Mapping, UserAuthority, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 VSX, VPN-1 XL, Web Intelligence, ZoneAlarm, ZoneAlarm Pro, 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、サービス・マーク又は登録商標です。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。本書で記載された製品は米国の特許No.5,606,668、5,835,726、6,496,935、6,873,988、および6,850,943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が、出願中の可能性があります。