Check Point SOFTWARE TECHNOLOGIES LTD.

国立大学法人 北海道大学

概要

北海道大学について

- 設立　1918年
- 学生数　19,939名（2015年5月現在）
- 国内屈指の先端総合大学
- 大規模な無線LAN接続環境を学内で拡張
- 個人所有のデバイスを学内で利用する（BYOD）ことを推奨するオープンなネットワーク環境を提供

分野

- 教育、研究機関

主な課題

- 学内を標的とするサイバー攻撃
- 拡張する無線LAN環境におけるリスクの軽減
- 予算配分を条件とするセキュリティ性能とパフォーマンス

チェック・ポイント・ソリューション

- 12400アプライアンス - NG Firewall　冗長構成
- サンドボックス TE250
- セキュリティ管理サーバ（SIEMを含む）Smart-1 205
- NG Firewall、IPS、Application Control、URL Filteringの各Software Blade

費用対効果

「従来の対策を強化する上で、チェック・ポイント社の提供するSoftware Bladeアーキテクチャは、複数のセキュリティ機能が統合され、脅威対策全般およびセキュリティ管理の面でも費用対効果を期待しています。さらに、優れた価格性能比および今後の拡張性においても、導入の効果が期待できます」

ー北海道大学 情報環境推進本部 情報セキュリティーチーム 永井 謙芝氏

**「教育機関を対象とするサイバー攻撃が増える中、無線LAN環境を整備しBYODなどネットワークを拡張するにあたり、パフォーマンスとセキュリティ強化の両面を満たすソリューションが必要でした。
チェック・ポイントの製品は、総合比較した中でセキュリティおよびコスト条件に適した選択が出来ました。また、管理および今後のボット対策などセキュリティ拡張にも期待しています。**

ー北海道大学 情報環境推進本部 情報セキュリティーチーム 永井 謙芝氏

チェック・ポイントが提供する最良のソリューション

北海道大学は、1876年に設立された札幌農学校を前身とする基幹総合大学です。同校では、2015年3月からの稼動を目指し、学生向けのネットワークインフラ「ELMS（エルムス）」の刷新を計画していました。この「新ELMS」を構築するにあたり求められたのがセキュリティ面の強化です。これまで稼動していた「旧ELMS」のセキュリティといえばファイアウォール程度で、新ELMSのパフォーマンスと現在の情報化社会に対応できるものではありませんでした。インターネット経由でさまざまな脅威が襲い掛かる昨今、緊急の課題としてセキュリティ体制の強化が求められたのです。

また、無線LANシステムの一新もセキュリティ上の重要案件となっていました。

「新ELMSにおける無線LANの拡充により、それだけ接続するデバイス数が増加するため、従来と比べてより強固なセキュリティが必要となります。さらに、“新ELMSの帯域がどのくらいになるのか”、“無線LAN利用率はどこまで上がるのか”といった部分が事前に予測できないため、セキュリティのパフォーマンスを十分に満たすソリューションが必要でした。」

ー北海道大学 情報環境推進本部 情報セキュリティーチーム 永井 謙芝氏

選定プロセス

選定基準

- ✔ 未知のマルウェア対策なども含め、限られた予算内で多層防御が実現可能
- ✔ セキュリティ処理によるアクセス速度の低下などが発生しないパフォーマンス
- ✔ 講義の際の資料閲覧など、将来的に学生向けのセキュアなBYOD環境を構築可能

チェック・ポイントを選んだ理由

「新ELMSの帯域や無線LAN利用率などが事前に予測できなかったため、限られた予算内でいかに効果的かつパフォーマンスの高いセキュリティ対策を施せるかが一番のポイントでした。こうした観点で各社製品から候補を絞り込み、最終的にコストパフォーマンスが極めて高く、性能のバランスにも優れたチェック・ポイントの製品導入を決定したのです。この価格で強固な多層防御を実現でき、なおかつ将来的な拡張性も備えているのは嬉しい限りです」

ー北海道大学 情報環境推進本部 情報セキュリティーチーム 永井 謙芝氏

国立大学法人 北海道大学

導入事例

Check Point SOFTWARE TECHNOLOGIES LTD.

チェック・ポイントのソリューション

1 将来要件にも対応する比類なき多層防御

チェック・ポイントでは包括的なセキュリティ環境を構築するべく、「Software Bladeアーキテクチャ」をご提供しています。各機能は「Software Blade」と呼ばれるセキュリティ・モジュールに分かれており、これらの組み合わせによってあらゆる環境やニーズに対応する多層防御を実現できます。このSoftware Bladeを追加することで、ネットワークの拡充やセキュリティ強度の向上など、将来的な要件にも柔軟に対応することが可能です。

「Software Bladeアーキテクチャにより、当校のセキュリティ要件と予算に応じた最適な多層防御を実現できました。今回はSoftware Bladeとして『Firewall/IPS/Application Control/URL Filtering』を導入しましたが、将来的にはボットによる被害を防ぐ『Anti-Bot』なども順次追加予定です」

2 業界最大規模のアプリケーション制御によるリスクの軽減

近年では「スクール・コンプライアンス」を重視する教育機関も増えていますが、社会的な責任を負う企業の社員と比べて、学生にコンプライアンスを浸透させるのは困難です。実際に、学内のデバイスから不正・危険なアプリケーションを使用して問題になったケースもあります。こうした際に役立つのが、チェック・ポイントがSoftware Bladeとしてご提供している「Application Control」です。本製品では、世界最大規模のアプリケーション・ライブラリ「AppWiki」をベースとして、6800以上のWeb 2.0アプリケーションや約24万におよぶウィジェットを識別。ユーザやグループごとに利用を許可・禁止・制限することが可能です。

3 進化の激しい未知のマルウェア対策が期待できるサンドボックス

従来のセキュリティでは、ネットワーク内に進侵入した“既知の脅威”に関しての検出や対策を重視していました。しかし、攻撃手法やマルウェアが激しい進化を遂げている昨今は、“未知の脅威”に対する防衛策が喫緊の課題となっています。未知の脅威を阻止するSandBlastの仮想サンドボックス「Threat Emulation」は、クラウド上または専用アプライアンス内で疑わしいファイルをエミュレートし、マルウェアに特有の活動をチェックすることにより、こうした未知の脅威をブロックできる製品です。

チェック・ポイント製品の利点

脅威を封じ込める多層防御

- 学外からの不正アクセスやマルウェアの侵入防止、未知の脅威に対する検出・対策などまで、限られた予算内で最適な多層防御を実現しました。
- 学内デバイスにおける危険なアプリケーションの利用について、許可・禁止・制限することが可能になりました。

圧倒的なパフォーマンス

- 新ELMSで求められるセキュリティ要件を満たす、十分なパフォーマンスを実現しました。
- 多くの学生が一斉に教材や動画資料へアクセスするようなBYOD環境下でも、セキュリティ処理による遅延などが発生することなく、スムーズに講義が行えます。

将来的な追加要件に対応する拡張性

- Software Bladeを追加することで、後からでも柔軟にセキュリティ機能の拡張が可能です。
- プロジェクトの初期予算に応じてスモールスタートができるのもメリットです。

まとめ

「多層防御・低コスト・拡張性」

- 予算やニーズに応じて最適な多層防御を実現します。
- 高いパフォーマンスでセキュリティ処理による遅延などが発生しません。
- Software Bladeの追加により、将来的な拡張にも対応できます。

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

Tel : 03 (5367) 2500 E-mail : info_jp@checkpoint.com

http://www.checkpoint.co.jp

P/N EOA3B90 2015.12