■ Application Control 導入事例 ― 立教大学

デジタルサイネージ端末向けセキュリティ対策として、McAfee Application Control を導入

教務情報を必要な場所、必要な時に配信するために、キャンパス各所にディスプレイを設置

― はじめにデジタルサイネージを導入した背景・目的について、お聞かせください。

デジタルサイネージは、フレキシブルに必要な情報を必要な場所へ展開することが可能です。そのため、本学では学生向けに授業の休講や教室変更のお知らせを表示する媒体として、デジタルサイネージを利用しています。また、授業の休講や教室変更以外にも、学内イベントや施設利用案内、さらには留学生向けのインフォメーション等、様々な切り口での情報をそれぞれの特性に合わせた場所に展開しています。

デジタルサイネージとして従来より大型のディスプレイを池袋キャンパスで10台（設置は2ヵ所）、新座キャンパスで6台（設置は1ヶ所）設置してきました。ところが、キャンパス内には教室が点在しているため、例えば授業のため教室へ行った学生が教室内の状況を見て大型ディスプレイが設置されている場所に休講や教室変更のお知らせを確認しに行ったりと、キャンパス内を行き来する状況が発生しておりました。

そこで、各教室の入口に配置させたのが、教室入口ディスプレイ（小型ディスプレイを活用したデジタルサイネージ）です。本学では「立教未来計画」と題して「教学環境設備支援プロジェクト」が立ち上がっておりましたので、その中での新教室棟の建設や既設教室の改修に合わせて、この教室入口ディスプレイの設置もキャンパス内に広めていくことになりました。

そして、2011年4月より今後のサイネージ端末の増設も踏まえて、デジタルサイネージ用コンテンツ制作・配信ソフトとして、大日本印刷株式会社（DNP）の『SmartSignage』を導入し、2011年12月現在、池袋キャンパスではエントランスと教室入口に合計21台、新座キャンパスではエントランスと教室入口に合計44台のサイネージ端末を配置しています。また、これらのサイネージ端末のセキュリティ対策として、McAfee Application Controlを導入しています。

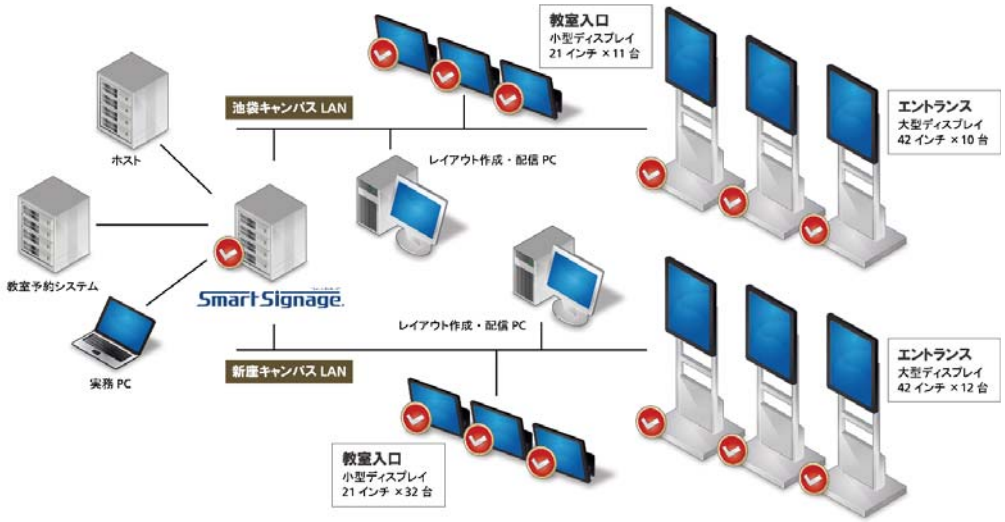
立教大学

プロファイル

学生の個性と自主性を尊重しながら、建学の精神と教育理念を実践することを理念として、10の学部と14の研究学科から構成される総合私立大学である。学生数20,681名（2011.5.1現在）
大学・大学院在籍者数にて、池袋キャンパス、新座キャンパスでの授業を行っている。

立教大学　教務事務センター
間中賢治 氏

エントランスに設置された大型ディスプレイ



LAN接続するサイネージ端末へのマルウェア対策及び、物理的にオープンな環境での不正アクセスを考慮

― デジタルサイネージ環境のセキュリティ対策で配慮されたのはどのような点ですか。

ある程度のサイネージ端末台数があり、頻繁なコンテンツ配信を前提とする場合、システム構成として、コンテンツ管理・配信サーバーから、ネットワークを介して、制御装置付きディスプレイへとコンテンツを配信することになります。そして、この制御装置付きディスプレイには、Windows 7が搭載されているため、マルウェア対策の配慮が必要と考えました。サイネージシステムそのものが、本学のLANネットワークに接続・利用される以上、サイネージシステムでのウイルス感染に留まらず、他のネットワークへの感染拡大というリスク対策も考慮したわけです。

さらに、デジタルサイネージ端末は、池袋キャンパス、新座キャンパスの拠点に、分散されて配置されています。外部からの物理的なアクセスも可能である以上、万が一ではありますが、ディスプレイ・制御PCに対する直接的な操作、プログラムの改ざんといったセキュリティリスクからも守りたいとも考えました。

決まったアプリケーションのみを実行する、限定的なHWリソースであるサイネージ端末では、ホワイトリスト方式マルウェア対策が向いている

― 実際の製品比較はどのような結果でしたか。

最終的には、マルウェア対策、プログラム改ざん防止の機能要件や運用性に則して、一般的なブラックリスト方式ウイルス対策ソフトとホワイトリスト方式ウイルス対策であるMcAfee Application Controlを比較したことになります。特に、マルウェア対策の点では、サイネージ端末の特殊性である限定的なハードウェア・リソースでのパフォーマンス性も考慮しました。

実は、本システム導入に関わって頂いた大日本印刷株式会社（DNP）からMcAfee Application Controlの製品紹介を受けるまで、この製品があることを知らなかったのです。ホワイトリスト方式のマルウェア対策製品の説明を受けて、こちらの潜在的な課題にマッチした製品であると判断しました。

― McAfee Application Controlを導入されて、すでに数か月が経過しますが、運用面など当初の期待通りでしたか。

運用ですが、正直言うとほったらかしというのが実状です。逆に、保護機能が効いているのか、心配になるぐらいです。そこで、試しに新たなプログラムを追加してみるのですが、導入ができませんので、やはり、保護が効いていることが確認できます。その意味では当初の想定通りと評価しています。

取材日時 2011年12月

製品機能の比較軸	ブラックリスト方式マルウェア対策	McAfee Application Control ホワイトリスト方式マルウェア対策
ウイルス対策機能	× サイネージ端末の限定的なHWリソースでは、定義ファイルの肥大化によるリソース圧迫、システム性能への劣化が懸念された。 ブラックリスト方式では、定義ファイルの更新、駆除の動作状況の確認といった運用面での負担がかかる。	○ 登録済み以外のプログラムの実行を防止することで、定義ファイル・スキャン不要のマルウェア対策が取れるため、システムリソース、性能の劣化を引き起こさない。 また、定義ファイルの更新、配布が不要となるため、ブラックリスト方式と比較し、運用・管理面の負荷が少ない。
プログラム改ざん防止	× 市販のウイルス対策製品に、プログラム改ざんを検知・防止する機能は含まれていなかった。	○ ホワイトリストに登録されたプログラムに対する変更作業のロギング、または、変更防止機能を有している。

McAfee
An Intel Company
マカフィー株式会社
www.mcafee.com/jp

●製品、サービスに関するお問い合わせは下記へ

東京本社　〒150-0043　東京都渋谷区道玄坂1-12-1 渋谷マークシティウエスト20F
TEL：03-5428-1100(代)　FAX：03-5428-1480

西日本支店　〒530-0003　大阪府大阪市北区堂島2-2-2 近鉄堂島ビル18F
TEL：06-6344-1511(代)　FAX：06-6344-1517

名古屋営業所　〒460-0002　愛知県名古屋市中区丸の内3-20-17 中外東京海上ビルディング3F
TEL：052-954-9551(代)　FAX：052-954-9552

福岡営業所　〒810-0801　福岡県福岡市博多区中洲5-3-8 アクア博多5F
TEL：092-287-9674(代)　FAX：092-287-9675

MCACS-APBK-1111-MC