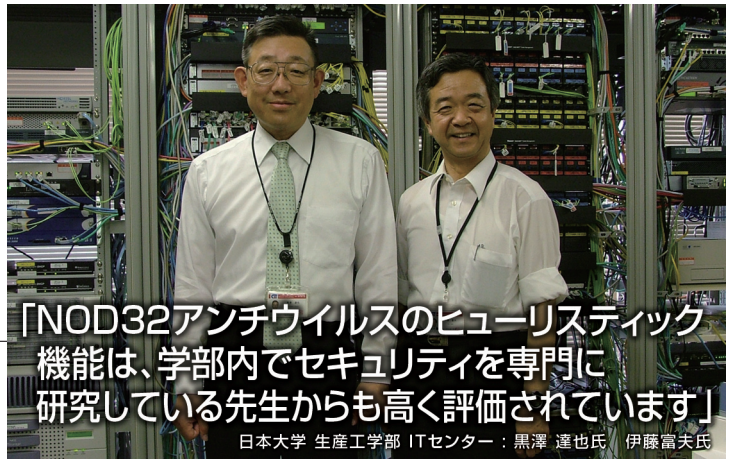
ESETライセンス 導入事例

日本大学 生産工学部

[導入製品]
NOD32アンチウイルス エンタープライズアカデミック ライセンス

日本大学 生産工学部 IT センター 黒澤達也氏（写真左）、伊藤富夫氏（写真右）に、NOD32アンチウイルスへの評価をくわしく聞いた。



日本大学 生産工学部の概要

Q. 日本大学 生産工学部（以下、日大 生産工学部）の概要を教えてください。

日大 生産工学部では、実社会でのものづくりに即した工学を研究しています。学生は全員、一般企業に一定期間実習生として勤務し、その後レポートを提出し、発表することが義務づけられています。2008年現在の学生数は約7,000人です。
日本大学は学生数の合計が約8万人を超える大規模大学です。各学部だけで、通常の大学一つに匹敵するほどの学生数を抱えています。
各学部は、独立性が強く「学部」というよりは「一つの大学」としてみなした方が適切です。
情報システムについても学部ごとに、それぞれ独自に構築、運営しています。

NOD32アンチウイルスをどのように活用しているか

Q. 日大 生産工学部では、NOD32アンチウイルスをどのように活用していますか。

2008年現在、NOD32アンチウイルスを3,270ライセンス購入しています。3,270ライセンスの概算内訳は以下の通りです。

ライセンス数	インストール場所
400ライセンス	パソコン教室
1,100ライセンス	教職員の学内パソコンおよび自宅パソコン
1,600ライセンス	2008年度入学生（1年生）が持つノートパソコン※1

今後、2009年、2010年、2011年に新入生が入学する度に1,600ライセンスを買い足します。
2011年度には、ライセンス数は約8,000に達している予定です※1。

なお、日大 生産工学部では、NOD32アンチウイルスの導入に先立ち「学部内セキュリティ現況把握」プロジェクトを実施しました。
NOD32アンチウイルスの導入は、そのプロジェクトの一環です。

※1：日大 生産工学部では、2008年度より学生がノートパソコンを持つことを半ば義務化しています。
NOD32アンチウイルスは、そのノートパソコンのウイルス対策ソフトに採用されています。今年2008年度はノートパソコン所持の半義務化1年目です。
まずは今年入学する1年生1,600人分のライセンスを購入しました。2011年までに1年生から4年生まで全学部学生分のライセンスを調達する予定です。

まず「学部内セキュリティ現況把握プロジェクト」を実施

Q.「学部内セキュリティ現況把握プロジェクト」とは具体的には。

日大　生産工学部では、キヤノンITソリューションズと共に、2002年に約1年間かけて、学部内のセキュリティ脆弱性の調査とその脆弱性への対策を行いました。

生産工学部のような工学系の学部は、原理的にセキュリティが脆弱化しやすいと考えます。「セキュリティ現況把握プロジェクト」の目的は、その脆弱化を防いで、必要十分なセキュリティレベルを確保することでした。

工学系の学部でセキュリティが「原理的に」脆弱化しやすい?

Q.「生産工学部のような工学系の学部は、原理的にセキュリティが脆弱化しやすい」とは具体的にどういうことですか。

あくまで単純化した話ですが、セキュリティは「管理が重要視される場所」で強固になり、「自由が重要視される場所」で脆弱化しやすいといえます。
そして、大学は、本来的に「研究の自由を重視する場所」です。
したがって、セキュリティが脆弱化しやすいといえます。

次に、コンピューターセキュリティという観点でいえば、「文系の学部と理系の学部では、理系の学部の方がコンピューターの自由活用が盛んなので、コンピューターセキュリティが脆弱化しやすい」といえます。

工学系学部では、日常の研究においてコンピューターを積極活用します。コンピューターに明るい教授や学生も多く、ネットワークも自分たちで簡単に構築してしまいます。工学系学部という場所では、ネットワークは上から与えるものではなく、現場で自由に作り上げるものです。

このような「(工学系学部ならではの)自由闊達にネットワークが自由発生する状態」は、「研究の促進」という観点から見れば良い状態です。
しかし「セキュリティの強化」という観点で見た場合は望ましくありません。
また、自由活発なネットワーク使用の負の側面として「ネットワーク放置」が発生するおそれがあります。「ネットワーク放置」とは、ある研究のために構築したネットワークが、それを構築した当人が卒業したため、管理者不在になる状態のことを指します。
最悪の場合、そうしたネットワークが外部からアタックを受けたり、踏み台にされることもありえます。

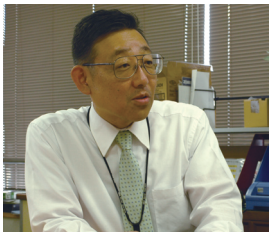
いくら、大学が自由な研究の場だとはいえ、学部内のパソコンが踏み台にされて、そこから大学外部に迷惑をかけることはあってはなりません。

ITセンターとして「研究の自由を制限しない範囲で、学部内のセキュリティを強化する」措置が必要だという結論に達しました。
以前から付き合いのあったキヤノンITソリューションズに相談し、「セキュリティ現況把握プロジェクト」に着手することにしました。
2002年はじめのことです。

「セキュリティ現況把握プロジェクト」で行ったこと

Q.「セキュリティ現況把握プロジェクト」では何を行いましたか。

「セキュリティ現況把握プロジェクト」は以下の順番で作業を進めました。
そうした「机上の構想」を終えた後、後半では実際のセキュリティ対策の実行、実装を行いました。


まず学部内の
セキュリティ現況把握から始めました

Q. 具体的に、どのようなセキュリティ対策を実行したのですか。

「セキュリティ現況把握プロジェクト」で実行したセキュリティ対策は以下の通りです。

1. 「ガイドラインづくり」
   まず日大 生産工学部としての「セキュリティのあるべき姿」を概念的に定めました。
   キヤノンITソリューションズとも話し合いながら、「事実を把握する」、「被害者にならない」、「加害者にならない」という三原則に基づく、ガイドラインを策定しました。
2. 「脆弱IPの洗い出し」
   学部内で使われているIPすべてについて、外部からの攻撃の対象となりかねない「脆弱IP」をすべて洗い出しました。
   ツールとしてはNetworkViewを使いました。
3. 「脆弱かどうかの判定」
   手順2で判明した脆弱IPが振られている機器について、セキュリティ面で脆弱性があるかどうかをチェックしました。
   ツールとしては、WALLScannerWebを使いました。
4. 「脆弱部分の修正」
   手順3において、「脆弱である」と判定された機器に対し、その脆弱性を修正する措置を行いました。
   ツールとしては、SecureIIS Webを使いました。

以上の作業を通じて、「学部内のセキュリティ状況の現況把握」と「弱い部分への対策」を相当に進展させることができました。

統一的なウイルス対策が必要だと考えた理由

Q. 続いて、NOD32アンチウイルスによるウイルス対策の強化についてお聞きします。
最初の質問です。NOD32アンチウイルスを導入する以前には、ウイルス対策をどのように行っていましたか。

NOD32アンチウイルスが製品化される以前からフィールドテストに協力していましたが、2005年にNOD32アンチウイルスを導入するまでは、ITセンターとして統一的に行っていたウイルス対策は、メールサーバーでのウイルス対策だけでした。学部内の個々のクライアントマシンでのウイルス対策は、そのマシンを管理している個々の先生方の自主性に任せていました※2。

Q. ウイルス対策製品を、ITセンターで統一導入するようになったのはなぜですか。

先ほど述べた「セキュリティ現況把握プロジェクト」などを通じ、「統一的なウイルス対策を施すべきだ」という意識が学部内で高まったためです。

2004年頃の、各科の代表者や事務方の主要職員を集めた、情報システム委員会で話し合いがもたれ、その席上で、「学部内に統一的なウイルス対策を施すべきである」、「ウイルス対策製品は各教授がバラバラに購入するよりも、学部で一括購入した方がコストも安くなる」という結論に達しました。

※2：一部の先生方は、その頃からNOD32アンチウイルスを自主的に使っていました。

製品選定の要件

Q. 学部内に統一導入するウイルス対策製品を選定するにあたり、何を要件としましたか。


ヒューリスティック機能は必須です。

ウイルス対策製品の比較検討の要件としたのは、「動作の軽さ」、「設定の簡単さ」、「ヒューリスティック機能の優秀さ」の3点でした。

この3点を基準にしてNOD32アンチウイルスおよび他のウイルス対策ソフトウェア数種類を相互比較しました。
その結果、NOD32アンチウイルスが最も要件を良く満たしていたので、これを採用することに決めました。

NOD32アンチウイルスは、ヒューリスティック機能が特に優れており、これが採用の決め手となりました。

なぜヒューリスティック機能を重視したか

Q. 日大 生産工学部では、なぜ「ヒューリスティック機能の優秀さ」を重視したのですか。

ウイルスによっては、本種が出た後に、亜種が立て続けに発生することがあります。そのような「進化の早いウイルス」においては、定義ファイルの更新を待っているだけでは間に合いません。その場合は、「疑わしきは罰する」のヒューリスティック機能が有効です。

かつてNimdaウイルスが大発生し、亜種が大量に出てきたときに、学部内のマシンにおいてNOD32アンチウイルスを導入し、ヒューリスティック機能を使用していたため無事でした。一方、他のウイルス対策ソフトウェアを導入していた他学部では、定義ファイルの更新が間に合わず、Nimda亜種に感染しました。

この経験を通じて、NOD32アンチウイルスのヒューリスティック機能への信頼が深まりました。

なお、キヤノンITソリューションズからは、NOD32アンチウイルスのヒューリスティックによる新種ウイルスの検出成功率は88%であるという説明を受けています。

**Q. ここでキヤノンITソリューションズに質問です。
NOD32アンチウイルスのヒューリスティックによる未知ウイルス検出成功率は88%とのことですが、
この数字の根拠は何ですか。**

88という数字は、NOD32アンチウイルスの開発元であるESET社での自主テストの結果に基づいています※3。

ESETでは「古いウイルス定義ファイルを使って、今現在のウイルスをどれだけ見つけられるか」というテストを行いました。

仮にここ3ヶ月の間に新種ウイルスが100個出現したと仮定します。それらのウイルスを3ヶ月前の過去の定義ファイルを使って検査した場合、定義ファイル参照だけでは、それらウイルスは一切、検出できません。しかしヒューリスティック機能を使えば、それら新種ウイルスを検出できると期待できます。100個の新種ウイルスのうち、いくつを検出できるかで、ヒューリスティック機能の優秀性が計れます。

2005年の導入当時、NOD32アンチウイルスはこのテストにおいて新種ウイルスのうち88%を検出しました※3。
これが88%という数字の根拠です。

※3：国際的な第三者機関であるVirus Bulletinによるウイルス検出率テストにおいても、NOD32アンチウイルスは「ウイルス検出率100% AWARD」を受賞しています。
2008年10月現在の受賞回数は52回で、これは業界最多です。(くわしい情報は弊社ホームページをご覧ください。

管理機能への評価

Q. NOD32アンチウイルスを3年間、使い続けてみて初めて分かった良さなどあればお聞かせください。

NOD32アンチウイルスは、管理機能がとても優れた製品であると思います。
特にウイルス検出情報や定義ファイル更新情報などを「現況把握」する機能が優秀です。

管理コンソールを使えば、「今現在、保有している3,270ライセンスのうち、いくつのライセンスが実際にインストールされているのか(いくつが未使用なのか)」、「各マシンのNOD32アンチウイルスが、最後にウイルス定義ファイルを更新したのはいつか」、「どのパソコンでどんなウイルスが発見され、NOD32アンチウイルスがそれにどう対処したか」などの情報が一括把握できます。

これらの情報は、各クライアントのNOD32アンチウイルスから、インターネットを経由して、中央の管理マシンに「報告」されてきます。
秀逸のなのは、そうした「報告」が、学部内のネットワークに参加しているマシンからだけでなく、大学外の普通のインターネットに接続しているマシンからも集められる点です。システム管理者にとって、良い仕様です。

今後の期待

Q. NOD32アンチウイルスへの今後の期待をお聞かせください。

日大 生産工学部には、コンピューターセキュリティを専門で研究している先生がいます。
NOD32アンチウイルスは、その先生からも高く評価されています。

かつてはNOD32アンチウイルスは、知る人ぞ知る、隠れた高性能ソフトウェアでした。
しかし、最近は一般的な認知度も上がってきました。

私たちがNOD32アンチウイルスを選んだことは、方向性として正しいことだったと、今、確信を持っています。
なお、本ソフトはWindowsに特化していることは始めから承知していますが、近年Macintoshも多数利用されていることから、Mac対応版も検討していただきたいと思っています。

キヤノンITソリューションズには、今後も開発元のESET社と緊密に連携し、NOD32アンチウイルスをさらに高性能のソフトウェアに進化させていくことを期待します。
今後とも宜しくお願いいたします。

■日本大学 生産工学部

日本大学さまは、私立大学の中でも学生数が非常に多く、情報システムに関しては、学部ごとに構築・運営されています。
生産工学部の IT センターの方々は、セキュリティに対する意識がとても高く、万全なセキュリティ体制を整えています。

販売元/
Canon
キヤノン ITソリューションズ株式会社
セキュリティソリューション事業部
〒108-0073　東京都港区三田3-11-28
TEL：03-5730-7198
http://canon-its.jp/

■お買い求めは‥‥

開発元/ eset
ESET, LLC and ESET, spol. s.r.o.

ES0409065000CITS-442