

LanScope Cat 導入事例集



日本事務器株式会社様

Stimulative



Move everyone to tears

Customer Satisfaction

1924年の創業以来、80年以上の歴史を通じて高い技術力を培い、時代の変化の中で常に最先端技術を世の中に発信されてきた日本事務器株式会社 (NJC) 様。ISMS、Pマークをはじめとした認証を数多く取得され、社会的信頼度の高さには定評がある。特に積極的に取り組まれているセキュリティ対策において、LanScope Catを活用されている様子取材させていただいた。

Innovative

Dream-inspiring

事例 LanScope NEWS

12

2008年3月

●お問い合わせは当社へ

エムオーテックス株式会社

大阪本社 / 〒532-0011 大阪市淀川区西中島5-12-12 エムオーテックス新大阪ビル TEL:06-6308-8989 (代)
東京本部 / 〒107-6022 東京都港区赤坂1-12-32 アーク森ビル22階(私書箱514) TEL:03-5575-3101 (代)
<http://www.motex.co.jp/>



NJC 日本事務器

日本事務器株式会社(以下NJC)は、40年以上にわたるお客様のICT化をお手伝いするソリューションプロバイダ。

各種コンサルティングから、システム企画・構築、導入後の運用、保守に至るまであらゆるフェーズでのサポートを提供している。

医療・福祉、公共・文教、製造・流通・サービスなど多種多様な分野のお客様の課題に対応。豊富な技術ノウハウをベースにネットワーク、セキュリティ等ICTインフラ構築から業種・業務アプリケーションの開発までお客様のご要望に合わせた最適なソリューションを実現している。



創業:1924年(大正13年)
設立:1948年(昭和23年)
事業内容:トータルソリューションサービス
資本金:3億6,000万円
従業員数:1,137名(2007年3月期)
認証:経済産業省SI登録企業
ISO9001 認証取得
[JQA-QM3916, JQA-QM6257]
ISO14001 認証取得 [JQA-EM3761]
プライバシーマーク 認証取得
[10822333 (03) JISQ15001:2006準拠]
CMMIレベル2達成
ISMS 認証取得 (BS7799-2:2002/ISMS 認証基準 (Ver.2.0)) [IC05J0118]

URL: <http://www.njc.co.jp/>

LanScope Cat 導入活用事例集

Pマーク認証、ISMS認証取得にLanScope Catを活用! Catによる社員教育の浸透で、更なるセキュリティ向上を目指す

日本事務器株式会社様

常にお客様の目線で ICTトータルソリューション&サービス

活用POINT!!

- 1 LanScope Catを、Pマーク認証、ISMS認証の取得・更新に活用!
- 2 LanScope Catによる最適なポリシーで、社員モラルアップ!
- 3 正確な資産管理を、最小限の労力で実現!



写真左端より 内部統制対策部兼クオリティ推進部標準化グループリーダー 高橋茂氏 (ISMS審査員補)、クオリティ推進部標準化グループリーダー 佐藤裕一氏、執行役員 クオリティ推進部長兼内部統制対策部長 梅山勉氏、情報システム部リーダー 梅田敬氏

90年代からイーサネット管理ツールLanScope NERI(イーサネットパケットモニタ)をご活用いただくなど、MOTEXとのつながりが強いNJC様。

2004年11月LanScope Cat3を導入、その後2005年11月にCat5にバージョンアップされた。

現在標準パッケージ・Webアクセス監視・デバイス制御を3,000ライセンス、サーバ監視を1ライセンス保持されていて、全国41拠点にあるすべてのPCにLanScope Catが導入済みである。セキュリティ推進に関係の深いNJCのCIO梅山執行役員ならびに、高橋氏、佐藤氏、そしてLanScope Catの運用に携わる梅田氏に話をうかがった。

導入のきっかけ

セキュリティ製品に必要な機能が網羅されているのは、Catだけ!

MOTEX(以下M):セキュリティツール導入のきっかけを教えてください。

梅山氏:PCが一人一台普及されるようになり、情報漏えい対策の実装が急務となったのがきっかけですね。セキュリティに関しては社会的責任ですから、トップダウンで指示があり、その後経営企画部と情報システム部で製品を検討しました。

M:LanScope Catを選んでいた理由は?
梅山氏:数社からツールの提案をもらいましたが、そのほとんどで、提案する自社製品の機能の補完ツールとしてLanScope Catを併せて提案していただきました。数あるセキュリティ製品の中でも、機能が網羅されているのはCatだけでした。追加でツールを購入する必要がないという魅力がありましたので、先々を見越した結果、Catに決めました。もともとLanScope NERIの導入実績もありますから、製品選定はスムーズに進みましたよ。

導入時

Catのインストール、トラブルはほぼゼロ!

M:今は御社に存在するすべてのPCにLanScope Catを入れていただいていると伺いました。

梅田氏:当初社内からは、セキュリティツールをインストールすること自体に抵抗があったという声もありました。理由をつけてなかなかインストールしてもらえなかったり…しかし、個人情報保護法施行やTCOも含めて情報資産の棚卸が必要であることから、一気に導入を進めることができました。

M:インストール時に問題はありませんでしたか?
梅田氏:特殊なプリンタサーバや、業務上必要な古いバージョンのPCも存在するため、若干のトラブルがあり、MOTEXさんに対応を依頼しました。

それでも2,500台存在する中で5件程度ですから、大変優秀な結果ですね。
M:インストール後の負荷はいかがですか?
梅田氏:Catが入ったPCを現場で3年以上使用していますが、PC端末に負荷がかかっているとは感じませんし、トラブルもありません。

一人のユーザとして、安心できるセキュリティツールだと自信をもってお勧めできます。

導入効果①

Catで資産管理の労力節減、費用対効果の高さを実感!

M:現在最も活用いただいている機能は、資産管理だそうですね。

高橋氏:はい、昔は各社員にエクセルシートを配布して情報を手入力、各拠点の上長がそれを合体させて報告していたんです。

労力が膨大にかかる割に、正確性に乏しい管理しかできませんでした。

梅田氏:今はCatから日々正しい情報を得られるので、大変楽に管理できています。

高橋氏:企業として管理しておくべき基本的な資産が把握できるようになったのは、Catのおかげです。

導入効果②

Catが社内ポリシーの浸透に貢献!

M:ユーザ企業様が一番悩まれているのは、社員に対するセキュリティ教育だとよく耳にします。御社ではいかがですか?
高橋氏:そうですね。当社の社員は一人ひとりのリテラシー(技術)がとても高いのですが、その分ポリシーを理解しない社員がいると、いろいろ好き勝手にできてしまうというのが問題でした。

梅田氏:上層部が一方的に指導する社員教育は大変数がかかるものです。しかし、Catのアラームポリシーだと明確な基準があるので、どういう行動が“正しい”のかが“悪い”のか受け入れられやすいことがわかりました。

またCatによる現状把握で、会社としてベストのポリシーが設定できるようになりました。例えばアラーム一つにせよ、そのポリシーが業務に支障をきたしてしまえば本末転倒です。ネットワークで業務を効率化するためのポリシー設定は、Catがあつてこそ可能になります。

導入効果③

Catがファイル交換ソフトを未然に防止、被害なし!

M:セキュリティ対策にはどのように活用されていますか?
梅田氏:WinnyやWinMXは、強制的にプログラム実行を禁止するアラーム設定にしています。

ウイルス感染の危険性が高いので、アラームがあがれば本人にすぐに確認するという緊急措置を取ります。当人の自覚のないファイル交換ソフトのインストールを未然に防ぐことができ、世間でファイル交換ソフトの問題が騒がれた時に、短期間で対策を講じることができました。

Pマーク認証

Pマーク認証の取得・更新に、Catが力を発揮!

M:御社はたくさん認証をお持ちで、素晴らしいですね。特にセキュリティに関して大変熱心に取り組まれているのわかります。

梅田氏:ありがとうございます。当社のPマーク認証とCatは、切っても切れないつながりがあります。

佐藤氏:昨年1月に更新の審査があったのですが、クライアントPCに保管している個人情報の操作履歴を採取していることを評価され、無事更新できました。

梅田氏:これからの審査は今まで以上に、個人情報保護への取り組みの如何を求められるようになると思いますから、当社におけるCatの役割はますます大きくなるでしょう。

佐藤氏:Pマークは取得がゴールではありません。社内ルールや規定を現場で正しく理解されるよう、継続的に取り組んでいくのが今後の課題です。

ISMS認証

全12のセキュリティツールの中でもダントツの貢献率!

セキュリティ確保に係る活動の半分はCatでカバー

M:ISMSの昨年度の定期審査にて、LanScope Catはどのようにお役に立てましたか?
高橋氏:ライセンス管理・資産管理を強化していること、また検疫ネットワークの導入を検討していることを評価していただきました。

具体的には、こちらの表をご覧ください。※1 ISMS (ISO/IEC27001)で規定されている管理策は全部で133個(※1の①)あります。

そのうち、当社内でLanScope Catによる規制・監視を行っているもの(LanScope Catのメリット)は35個(②)あり、全体の26.3%(③)です。それに対し、LanScope Cat自身が規制を受ける管理策(LanScope Catのコスト)は5個(④)あり、全体の3.8%(⑤)に当たります。

このコストをメリットから単純に引くと22.5%になり、当

社のISMSにおいてLanScope Catの貢献率は2割以上という結果になりました。当社では、合計12のセキュリティツールを導入しているのですが、その中の一つであるCatで全体の1/4近くをカバーできているのは素晴らしいですね。

M:なるほど。特にどの分野で一番役立っているのでしょうか?
高橋氏:LanScope Catのメリットを最も享受している分野は「A.7 資産の管理」で、60.0%(⑥)を担っています。

また間接的な関与として「A.14 事業継続管理」ですが、事業継続計画の中で資産の保全が重要視されていることからLanScope Catの関与も高く、80.0%(⑦)の貢献率となり、大変満足のいく結果です。

高橋氏:この表に表すことは難しいですが、Catはサーバやクライアントの操作履歴のログ採集など、ISMSにおいて最も重要なエビデンス(証拠)作成に欠かせないものです。

そのことも踏まえると、LanScope Catの導入により、確実にこの表の数値以上の効果が得られています。個人的な感覚ですが、当社のセキュリティ確保に係る活動の半分近くに、LanScope Catが役立っていると思いますよ。

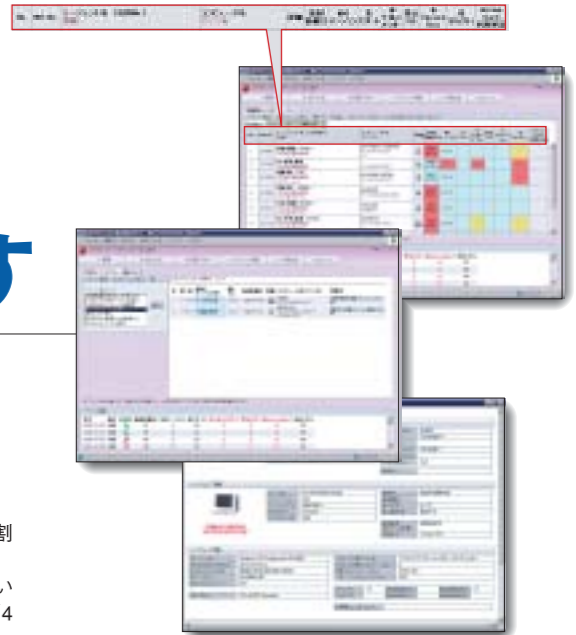
運用の工夫

社員のリテラシーの高さを活かし、Catの情報からオリジナルのセキュリティ管理を実現!

M:LanScope Cat5からデータを取り、独自のシステムで資産管理をされていると伺いました。

梅田氏:こちらの画面です※2。当社の特徴として“開発用PC”と“業務用PC”が混在するのですが、正確な情報をより早く聞き出すためCatのメッセージポリシー配信機能を活用しています。おかげで、その情報を数として捉えることができるようになりました。

M:この情報は全社で閲覧可能ですか?
梅田氏:はい、全社員がこれらの画面を見ることができ、



※2 日本事務器様独自開発の管理画面

各部署の上長は、内部署の情報を確認し対策を打つことができます。

“セキュリティソフト未導入”や“禁止ソフト導入”などの項目の現状把握ができるため、大きな抑止効果が出ています。

データベースの仕様がわかるので、直接データベースを触り必要な情報だけを取得するのが便利です。

M:他社のセキュリティツールを見ると、独自のデータベースを使用しているものも多いようです。実績のあるデータベース※3を使用し、仕様を公開しているLanScope Catだからこそ、実現した運用ということですね。

梅田氏:そうですね。その点でもCatは利便性が高く、重宝しています。

※3 LanScope Cat5はSQL Serverを採用。LanScope Cat6からOracle Databaseも使用可能。

今後の展望

コンプライアンス向上にも期待が高まるCatの力

M:では最後に、今後のLanScope Cat活用の展望をお聞かせください。

梅田氏:今後は個人情報保護の更なる徹底のため、取得したログを活用していきたいですね。

また、Catの不正PC検知機能、Webアクセス監視機能、アプリケーションID監視機能をセキュリティ管理やコンプライアンスの向上に役立てていきたいと思っています。

これからCatがますます強化されることを期待しています。M:ありがとうございます。

※1 ISO管理策とLanScopeの相関表

No.	ISO/IEC27001規格項番	LanScopeが関与する管理策の数						ISO/IEC27001の管理策	
		LanScopeによる監視・規制			LanScopeを規制	計			
		運用中	間接的に関与	小計					
1	A.5 セキュリティ基本方針	0	0	0	0.0%	0	0.0%	0	2
2	A.6 情報セキュリティのための組織	4	0	4	36.4%	0	0.0%	4	11
3	A.7 資産の管理	3	0	3	60.0%	0	0.0%	3	5
4	A.8 人的資源のセキュリティ	2	0	2	22.2%	0	0.0%	2	9
5	A.13 情報セキュリティインシデントの管理	2	0	2	40.0%	0	0.0%	2	5
6	A.15 順守	0	0	0	0.0%	5	50.0%	5	10
	管理的対策 小計	11	0	11	26.2%	5	11.9%	16	42
7	A.9 物理的及び環境的セキュリティ	4	0	4	30.8%	0	0.0%	4	13
	物理的対策 小計	4	0	4	30.8%	0	0.0%	4	13
8	A.10 通信及び運用管理	6	0	6	18.8%	0	0.0%	6	32
9	A.11 アクセス制御	6	0	6	24.0%	0	0.0%	6	25
10	A.12 情報システムの取得、開発及び保守	4	0	4	25.0%	0	0.0%	4	16
	技術的対策 小計	16	0	16	21.9%	0	0.0%	16	73
11	A.14 事業継続管理	0	4	4	80.0%	0	0.0%	4	5
	緊急対策 小計	0	4	4	80.0%	0	0.0%	4	5
	総計	31	4	35	26.3%	5	3.8%	40	133

[ISMS認証 (ISO/IEC27001)とは]

・ISO/IEC 27001:2005 (Information technology —Security techniques— Information security management systems—Requirements:情報技術—セキュリティ技術—情報セキュリティマネジメントシステム—要求事項)は、組織がISMSを構築するための要求事項をまとめた国際規格である。ISMSの国際規格ISO/IEC 27001:2005の発行に伴い、現在、組織のISMS認証審査に適用されているISMS認証基準 (Ver.2.0)は、ISO/IEC 27001へ移行される。