LANSCOPE

IT資産管理ツール

虎の巻

TORANO-MAKI

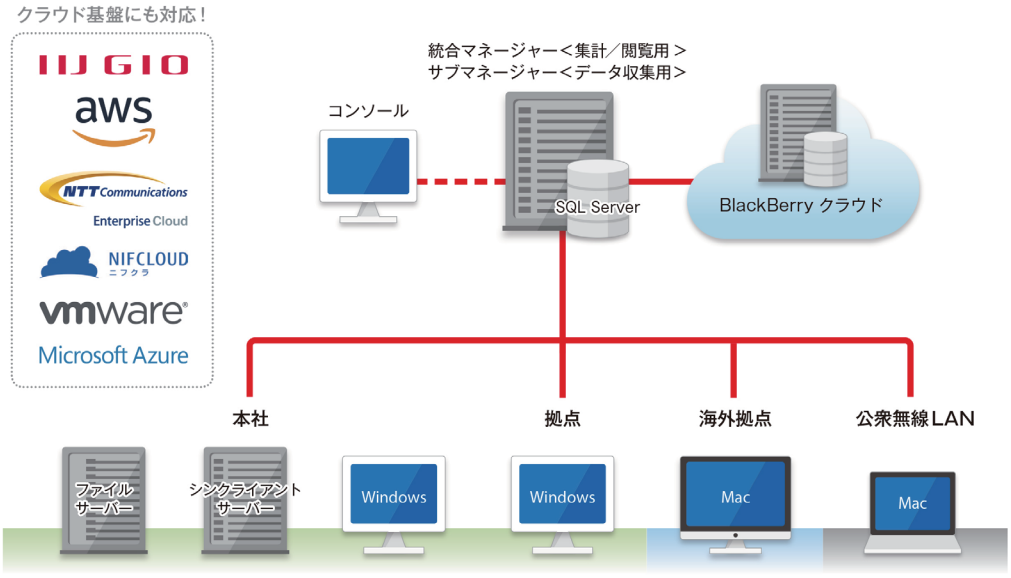
～そもそもIT資産管理ツールとは？～

そもそも「IT資産管理ツール」とは？

MOTEXではLANSCOPE オンプレミス版（旧名称：LanScope Cat）というIT資産管理ツールを開発・販売しています。開発メーカーとしては実は「LANSCOPE オンプレミス版＝IT資産管理ツール」と明確に定義しているわけではなく、「IT資産管理」は勿論、「ログ管理」「外部媒体制御」等々、様々な用途でご活用していただいています。まず整理する意味を含めてIT資産管理ツールって何だろう？と言う部分から振り返ってみました。

セキュリティ市場調査資料を出版している富士キメラ総研によると、「端末構成管理・セキュリティツール」という大きなカテゴリーがあります。更に4つのカテゴリーに分けられており、その中に「IT資産/PC構成管理ツール」という項目があります。その他3つは「端末操作ログ収集・管理ツール」「持ち出し制御ツール」「暗号化ツール」になっていました。市場では正直明確な切り分けが無く、メーカー毎に「全てを網羅」「一部に特化」という形で各カテゴリーの機能が混在して実装されており、そういった製品が市場ではざっくりと「IT資産管理ツール」という名称で呼ばれているように感じます。ちなみに富士キメラ総研のカテゴライズで「端末構成管理・セキュリティツール」に分類されている製品は数えてみると71製品もありました。筆者はこの業界に携わり10年以上となりますが、各製品の特徴・強み・弱みが語れないくらい製品が増えたと感じます。

製品毎に実装機能が異なりますが、管理サーバを構築する、エンドポイントに管理用ソフトウェアをインストールする、というシステム構成（図1）はほぼ共通していると思います。



※保有するライセンスによって、以下のエージェントをインストールする必要があります。
クライアントエージェント（Windows用／Mac用）、検知エージェント、サーバーエージェント（Windows用／NetApp用）
BlackBerry Protect エージェント、Web フィルタリングのクライアント、ISLOnline のクライアント

図1

「IT資産管理ツール」の機能は様々ですが、「エンドポイントを統合管理する」という部分は基本的に共通していると言えるのではないでしょうか？ちなみにLANSCOPE オンプレミス版一製品でも実装する機能は多岐に渡り、50個以上もの機能が実装されています。なぜ1つのパッケージソフトでここまで多機能なツールになったのか？IT資産管理ツールの歴史を振り返って説明していきます。

IT資産管理ツールの歴史

筆者は2004年にMOTEXに入社したのですが、今までのLANSCOPE オンプレミス版の機能実装の流れを、「市場背景」「求められるニーズ」「実装機能」という形で簡単にまとめてみました（図2）。

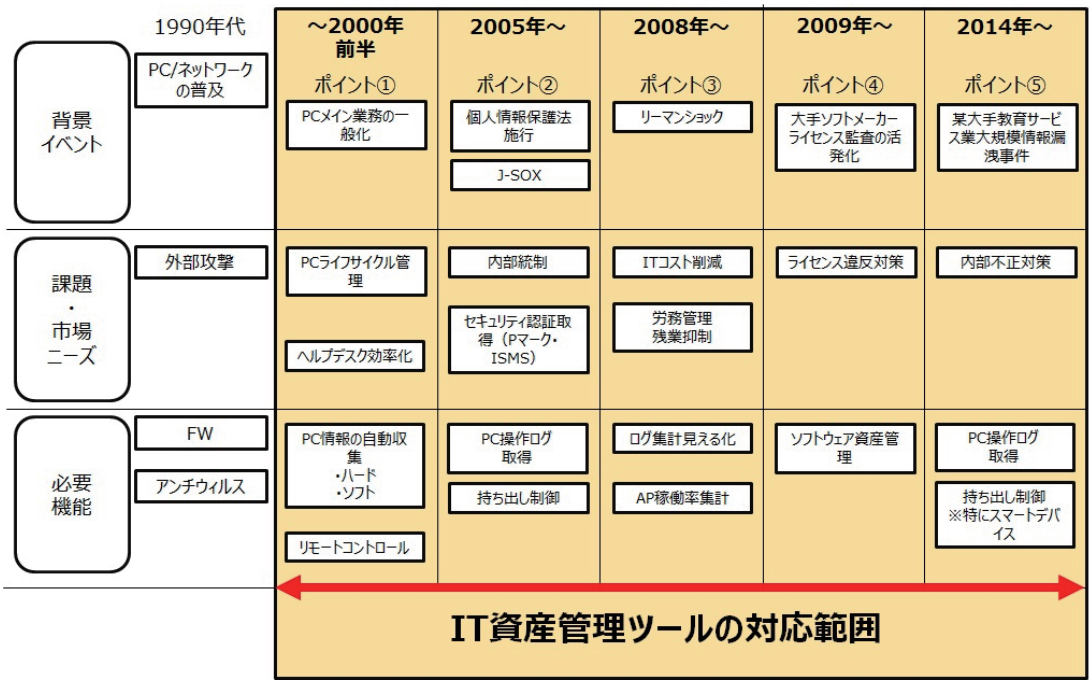


図2　IT資産管理ツールの歴史（LANSCOPE オンプレミス版の場合）

整理していく中で再確認できましたが、時代背景に合わせて様々なニーズを取り込んで進化してきたと思います。「IT資産管理ツール」登場前の時代背景としては「ネットワークの普及」に伴う「外部攻撃」からの対応が大きな課題・ニーズで、「ファイアウォール」「アンチウイルスソフト」といった製品が普及していました。

～IT資産管理ツール5つのポイント～

IT資産管理とは何かを明らかにするための5つのポイントを、時代の変遷と共に追っていきます。
記憶に残っている事件や事例もあるかと思います。

ポイント①：PC大量導入



2000年代初期、業務スタイルの変化の中でPCを使用した業務が当たり前になり、共有PCでの業務から「PC1人1台環境」に変遷していきました。その中で高価なPC自体の正確な資産管理の為にハードウェア情報収集、ソフトウェア情報収集といったIT資産管理のベースとなる機能が普及していきました。

LANSCOPE オンプレミス版はこの時期に「PC操作ログ収集機能」を実装しています。今でこそ「内部統制・内部不正対策」という意味合いでメジャーな機能として認知されていますが、当時は珍しい機能でした。MOTEXとしても実はセキュリティを意識して実装したわけでなく、「PC操作を記録しておくことで、IT管理者のトラブルシューティング時の原因究明を効率化する為」を目的として開発した機能でした。

PCトラブル発生時に社員に「何をしたんですか？」と問いかけても「何もしてません」というありがちなやり取りに終始し、原因が分からない。原因さえ分かれば対処は早かったというありがちなシーンに対して直前の操作が把握できれば対応が効率化できるという意図で実装した機能でした。

「2000年代初期」と書きましたが、ネットワークに繋がる新しいデバイスは日々増加しており、IT資産管理に対するニーズは継続して発生するものとなっています。

ポイント②：個人情報保護法



2005年に施行された「個人情報保護法」の影響でIT資産管理ツールに求められる機能が大きく変わりました。ハードウェア・ソフトウェアといった「モノの資産」からその中で動く「データが資産」という考え方に変化していきます。

ハード、ソフトの情報だけでなくそれを使った「人のデータ操作」の把握が必要となり、機能としては「PC操作ログ」が求められるようになりました。セキュリティ認証の取得も個人情報保護法の施行と共に流行を見せPマークやISMS取得の為にもPC操作ログ機能が必要というニーズもこの時期から増加したように感じます。

もう一つ、内部不正での情報漏洩対策としてマスト機能となる「外部媒体制御」機能もこのタイミングで実装されました。IT資産管理ツール市場がセキュリティ市場と混ざりあい商業的にも大きなブレイクポイントとなります。LANSCOPE オンプレミス版は前述したようにIT管理者の運用支援の意図でいち早くPC操作ログの機能を実装していました。

この頃から市場が一気に拡がり、IT資産管理ツール市場に続々と新規メーカー・製品が参入します。

ポイント③：リーマンショック

2005年の個人情報保護法の施行以降、順調に成長してきたIT資産管理ツール市場でしたが、2009年のリーマンショックによる不景気の影響を受けてしまいました。IT業界全般で大変な逆風が吹き荒れ、IT資産管理ツール市場も同様の状況でした。どこの企業でもIT部門に対してコスト削減の大号令が掛けられている時期です。

その影響で保守契約の見直しを行うユーザー様もいましたが、IT資産管理ツールを無くてはならないものと捉えて多くのユーザー様に保守契約を継続いただきました。

ただ、一部ではツールが「セキュリティ認証等の取得の為に、導入することが目的となり活用は特にしていなかった」という現実も浮き彫りになりました。こういったケースでは自社が生きるか死ぬかの瀬戸際になると、「IT資産管理ツール・セキュリティツールは贅沢品」扱いとなってしまいコスト削減の対象となってしまったのも事実です。

そんな状況の中で、LANSCOPE オンプレミス版を使ってこの危機を乗り切ろうと新しい活用方法が生まれてきました。主に「労務管理での活用」と「アプリケーション稼働率集計によるライセンスコストの最適化」の二つになります。

当事PC操作ログの機能は、「データセキュリティ、内部不正対策の為」が導入目的の主流でしたが、一部のお客様が「PCを操作して社員が何をしているか分かる」という本質的な価値に着目されたのです。「PC操作ログによる労務状況の確認⇒無駄な残業削減」や「高価な有償アプリケーションの稼働率集計⇒未稼働ライセンスを必要なところに割り振る運用」を行い、コスト削減としても大きな効果を上げられました。

ポイント④：ライセンス監査の活発化、ソフトウェア資産管理（SAM）

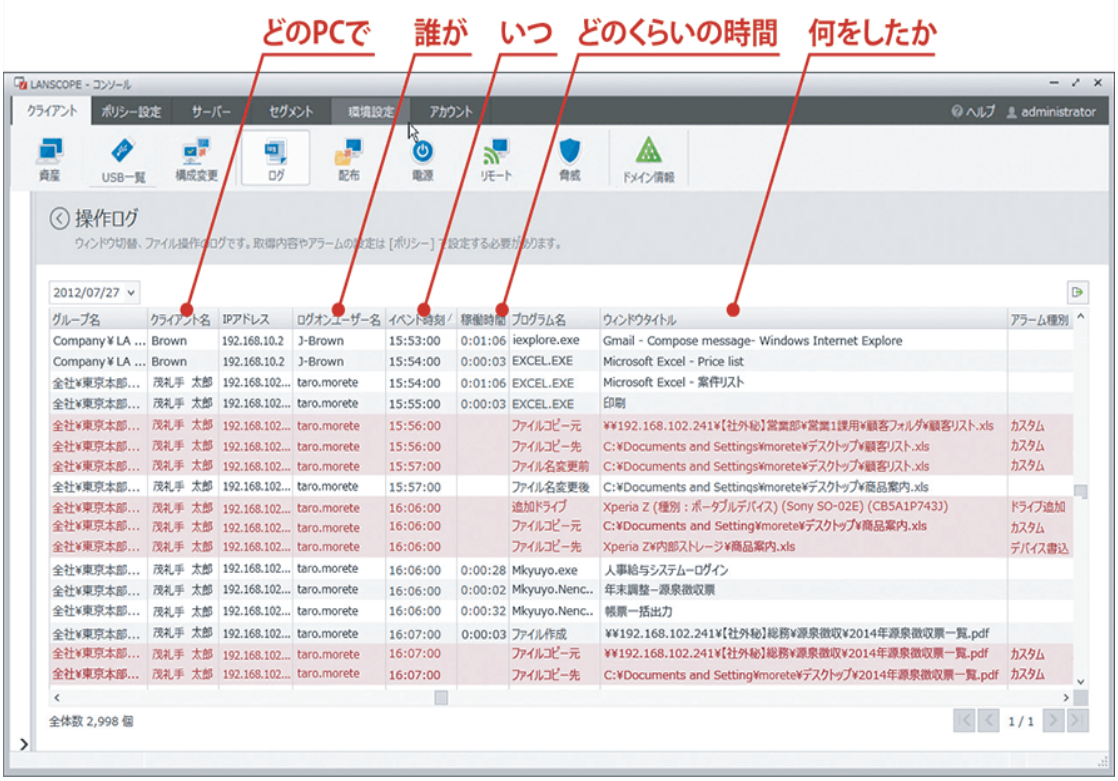


2009年になると大手ソフトウェアメーカーによる本格的なライセンス監査が始まりました。ライセンス違反による多額な賠償事例が頻発したことからユーザー企業の危機意識は高まり、各社対応に追われることになります。IT資産管理ツールに求められる機能もこの流れで高度化しました。

ここまではExcelの台帳管理でなんとか対応してきた組織も、SAM対応では「インストールされたソフトは有償ライセンスなのか？無償ライセンスなのか？」「監査に対応できる4つの台帳が作成できるのか？」など、高度な要件への対応が必要となりました。LANSCOPE オンプレミス版も「SAMACのソフトウェア辞書連携によるライセンス有償・無償棚卸し機能」「各種台帳作成機能」「高度な運用実現のためにSARMS連携」など、ソフトウェア資産管理に対する機能強化を行いました。

IT資産管理ツールの機能実装はリーマンショック後の様に「新しい活用法が増える」ケースもあれば、この時期の様に「元々あった機能の更なる深掘り」が行われるケースもあります。

ポイント⑤：某大手教育サービス業の大規模情報漏洩事件



LANSCOPE　オンプレミス版「操作ログ管理」

「どのPCで」「誰が」「いつ」「どんな操作をしたか」を記録。許可していないFree Wi-Fiへの接続や
顧客リストのUSBメモリへの書込みなど、違反操作があった場合、ユーザーに警告表示し不正操作を抑止します

2014年の内部不正要因による大規模情報漏洩事件をきっかけに、ポイント②で記載した内部セキュリティリスクに対してのニーズが再燃しました。この事件はIT資産管理ツール市場に対して大きなインパクトがありIT資産管理ツールはより機能の深掘りを求められました。

1つ目は「スマートデバイスの制御」になります。外部媒体制御機能は各社製品で実装していましたが、LANSCOPE オンプレミス版も含めてスマートデバイス含むWPD（Windows Portable Devices）機器の制御には穴があることが判明した為です。

MOTEXはWPD制御可能なカスタムモジュールを開発中の時期にこの事件が発生したこともあり
市場の中ではかなり早いタイミングで対応機能をリリースできています。

2つ目として「PC操作ログ」に求められるものが変化しました。これまでPC操作ログ取得の目的は「何かあったときの証跡としてログを残すため」というお客様がほとんどでした。しかしこの事件の教訓として、「何かあった後にログを追って犯人が分かったところで大損害になってしまう」ことが明確になったのです。

当事、ニュースであるセキュリティ有識者の方が「今回の事件で痛恨だったのは、捕まった犯人が『ばれると思わなかった』と言っている事。トレースできる環境を構築していたがそれが伝わっていなかった為に牽制効果が発揮できていないかった」と話されていたのがとても印象に残っています。昨今「ビッグデータの活用」について盛んに取り上げられていますが、内部不正対策分野でも「ログの収集」から「ログの活用」の必要性を実感させられる事件だったと感じています。

～IT資産管理ツールのトレンドと課題～

IT資産管理ツールに求められるニーズと今後の課題について切り込んでいきます。

ポイント6－1：最近のトレンド①働き方改革/テレワークの普及

ここまで過去の振り返りを書いてきましたが、ここ2年くらいの中でIT資産管理ツールに求められる新しいニーズが生まれてきました。一つ目は「働き方改革」というキーワードです。

二つの要素があると考えていて、一つは大手企業の長時間労働問題をきっかけに取り組まれている残業対策といった側面。個人的には「残業対策＝働き方改革」になってしまっている企業様も多く少々違和感もあるのですが、お問い合わせいただく機会は増えています。
もう一つは労務時間削減にも絡みますがITを使った業務効率化に関連するご検討。テレワーク時の就業状況の確認や労務実態の現状把握の為の操作ログ収集・分析によるIT資産管理ツールの活用です。特に在宅勤務を含むテレワークへの移行は、コロナ下で急速に拡大し、労務実態の現状把握必要性が2020年から大きく高まっています。

前者はポイント③のリーマンショック時期にも同様の使い方がありましたが、更に強制力が強くなり、「定時でのPC電源オフ」といった機能もマストになってきたようです。

難しいのが後者のニーズです。「操作ログが取得できる＝労務実態が把握できる。効率化できる」というプロモーションを最近良く目にしますが（LANSCOPE オンプレミス版も同様ですが・・・）実際にやってみると結構難しいというのが現実です。まずはツールの機能云々以前にプライバシー周りの調整が大きなハードルになります。

「セキュリティのためにログチェック」は大分抵抗感が小さくなってきましたが、「労務実態の把握のためにログチェック」となるとかなり圧迫感があるようです。経営層や人事部門との調整、一般職員の合意と言った根回しが重要になりますし、ここがクリアできなければどの製品を導入したとしても運用まで踏み込めません。



LANSCOPE オンプレミス版「勤怠レポート」画面

機能面では今までは「如何に早く分かりやすくログを確認できるか？可視化できるか？」という観点での機能強化が多かったのですが、ここにきて「必要な時に必要な内容を丁度いい範囲で確認できる」という可視化のレベル感にも気を使う必要が出てきました。

また、「PC操作ログの内容＝自組織の労務内容」に出来る限り近づける為の「ログ加工ノウハウ」も各組織の業務内容に応じてチューニングが必要になるかと思います。ツールの導入が目的の実現ではないのが現実です。このあたりはソフト開発メーカーの立場ではありますがツールだけではなくノウハウも含め提供できるように取り組む必要があると感じています。

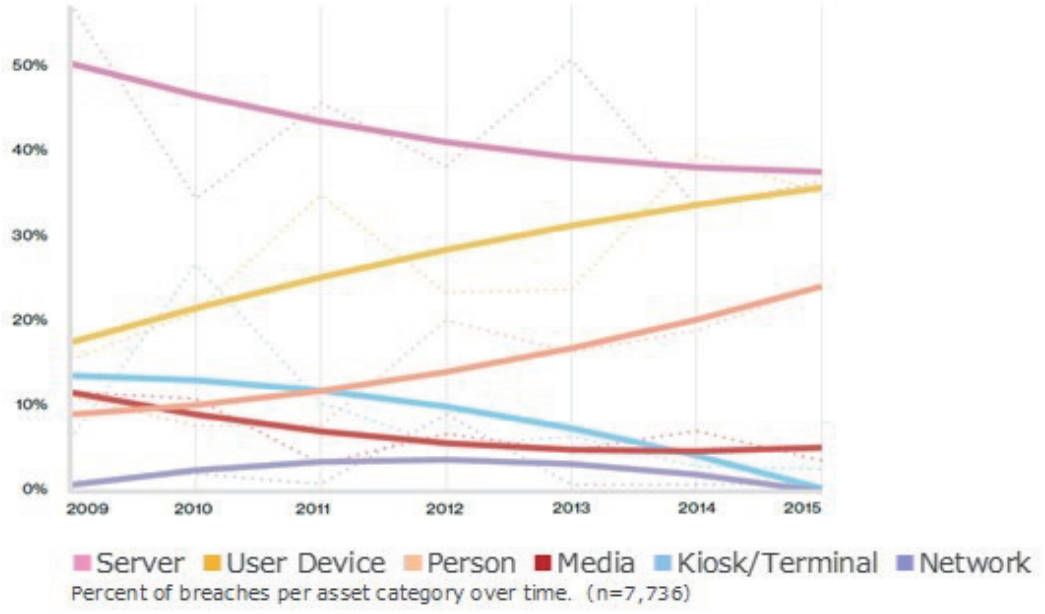
ポイント6－2：最近のトレンド②サイバーセキュリティ

働き方改革に関連する需要は過去にもあったニーズの延長線ともいえますが、サイバーセキュリティ関連で生まれたニーズはIT資産管理ツールにとって新しい領域へのチャレンジと感じています。

2014年の大規模情報漏えい事件から内部不正対策の需要が再燃し市場も一時的に盛り上がりましたが、2015年の年金機構での標的型攻撃による大規模情報漏えい事件からお客様のサイバーセキュリティへの意識がシフトしたように感じます。

「・・・昔からだよ！」というご指摘もあるかと思いますが、IT資産管理ツール開発ベンダーから感じる肌感ということでご容赦ください。特に仮想通貨の流行から匿名性をもって身代金を要求できる環境が整い、ランサムウェアが再度流行することになったのもサイバーセキュリティへの意識が高まる大きな要因になったと感じます。

潜伏型の標的型攻撃は気づけない事もあり、リスクに対する具体的なイメージを持ちづらいものでした。2017年のWannacryの流行が分かりやすいですが、ランサムウェアによる攻撃は自分の端末もしくはファイルが「使えなくなる⇒業務が止まる」という分かりやすい被害をもたらし、スペシャリストだけでなく広く一般的なリスクとして捉えられるようになったと感じます。



（図3）攻撃対象の変化（VERIZON DBIR 2016 レポート）

VERIZONのレポート（図3）にもありますが、現状狙われているのはサーバから我々が普段利用するエンドポイントのユーザーデバイスにシフトしてきています。背景として、攻撃者が簡単に新しいマルウェアを作成・拡散できる環境が整ったことで、広く普及しているシグネチャ式のウイルス対策ソフトが効果を発揮しなくなったことが技術的な大きな要因の一つだと考えられます。

結果、「メールを開いて感染」「Webのリンクから感染」といった事例が相次いで発生しています。ウイルス対策ソフトでの防御が不完全となり、サンドボックスでの解析や次世代ファイアウォールによる出口通信から攻撃を止める・気づくといった「入口・出口対策」に対して活発に投資がなされましたが、境界防御も昨今の攻撃ではすり抜ける手法が既に生み出されています。

マルウェア感染後、正規のサービスにアクセスをさせて時限式で一斉に新規のC2サーバにアクセスする手法や、正規のアプリケーションを改ざんしてマルウェア化したものを普及させるサプライチェーン攻撃などの新しい攻撃が次々と生み出されています。

また前述した、働き方改革によるモバイルワークによって社外での業務形態にシフトする動きもあり、境界防御の外での業務が当たり前になる、つまり「中は安全」という対策が業務スタイルとして合わなくなっている現状もあります。その結果、再度エンドポイントでの対策強化が必要となり、エンドポイントで稼動するIT資産管理ツールもサイバーセキュリティに関連する運用がなされるようになりました。

資産管理機能では「脆弱性対応のパッチ配信」、操作ログ機能では「マルウェア感染時の流入経路の特定」「拡散状況の確認」「フォレンジック調査」といった使われ方が増えているように感じます。今までの使われ方と違い緊急時の対応といった意味でリアルタイム性を求められるケースが増えている事も大きな変化です。

我々MOTEXも過去5年ほど経産省のセキュリティ人材育成期間にてIT資産管理ツールのサイバーセキュリティでの活用方法について講義を実施しており、サイバーセキュリティの文脈でもIT資産管理ツールが有効に活用いただく手ごたえを得ることができました。

また、各IT資産管理ツールでシグネチャに依存しない次世代型のウイルス対策製品との連携機能の提供も始めています。例えばLANSCOPE オンプレミス版ではBlack Berry社のAIを活用したシグネチャレスのウイルス対策ソフトBlack BerryProtectと連携したOEM製品であるCyber Protection Managed Service powered by BlackBerryを提供しています。IT資産管理ツールベンダー毎に協業製品はバラバラでこちらもそれぞれの製品ごとの特徴があります。IT資産管理ツールのみだけでなく将来性も考え連携できるソリューショントータルの評価で検討する必要もあるでしょう。

この領域についてIT資産管理ツール出身ベンダーは「これからの領域」であり、正直まだまだ模索中の部分がありますが、今後エンドポイント管理製品ならではの新しい価値を提供するベンダーが増えていく事を期待しています。

サイバーセキュリティの領域はとりあえず「多層防御」という言葉がエスカレートしていった結果、「あれもこれも必要です重ねましょう」という提案が飛び交い「システム揃える予算が無い」「システム揃えても使いこなせるスタッフがいない」という状況が置き去りになり、現実的ではない無茶な教科書が出来上りつつあるような気がします。MOTEXとしてはエンドポイントを軸としてシンプルでありながら効果的な価値を生めるように取り組んでまいります。

～IT資産管理ツールの選び方～

IT資産管理ツール市場の背景／課題／ニーズ

６つのポイントに分けて、IT資産管理ツール市場の今までを振り返り整理してみました。振り返ってみると世の中の課題に対してIT資産管理ツールは柔軟に広範囲をカバーして対応してきたことに気づきます。何故、その時その時の時代背景、課題に対応してこられたのかというと、一つの要素としてエンドポイント管理の特性が大きいと感じています。

時代の流れに応じて様々な課題が生まれますが、掘り下げていくと本質的には「人」に起因する課題が多数存在します。個人用PCでの業務が一般化して以降、IT資産管理ツールで対応する「PC(エンドポイント)の管理」が「人の管理」に限りなく近いものになっていた事で自然と時代の流れの中で様々なニーズに対応してきたのだと考えています。

背景	年代	課題	求められるもの
①PC大量導入	～2000年	正確な台帳管理	・ハード/ソフト情報の自動収集
②個人情報保護法	2005年～	内部不正対策	・操作ログ取得による監視、不正抑制 ・外部記憶媒体制御
③リーマンショック	2008年～	コスト抑制	・AP稼動集計で不必要アプリの削減 ・操作ログ集計による不稼動業務削減 ・無駄な残業削減
④ライセンス監査活発化	2009年～	正確なソフトウェア台帳作成	・詳細なソフトウェア情報の収集、台帳
⑤内部不正情報漏洩対策	2014年～	情報持ち出し対策	・外部記憶媒体制御強化 （スマホ等、新規デバイス関連）
⑥サイバーセキュリティ	2015年～	境界防御の限界 （予防・流入後）	・ログによる流入経路の特定 ・感染拡大状況の把握 ・パッチマネジメント　　等々・・・

【一般的な「端末構成管理・セキュリティツール」導入目的】

１：IT資産管理・効率化
２：セキュリティ（内部不正対策寄り）
３：労務管理
４：ソフトウェアライセンス管理
５：紛失対策（暗号化）　※LANSCOPE オンプレミス版では機能実装していない
６：サイバーセキュリティ

それぞれまったく違う検討領域にみえますが、IT資産管理ツールはカバー範囲が広いこともあり、どのカテゴリーでも提案されています。よく提案の場で「機能実装の〇×比較表」を使って「〇が多くて安い製品がいい」という商談を見かけますが、導入後に失敗してしまうケースが多いのがこの進め方です。気をつけていただきたいのが、「機能実装している（〇がついている）からといっても同じものではない」という事実です。

IT資産管理ツール選定で気をつけたいこと

先ほど歴史と機能実装の流れで紹介させていただいた通り、メーカーごとに市場参入の時期や注力している領域は違います。SAM監査の全盛期に参入してきたベンダーはソフトウェア資産管理の機能に特化していますし、個人情報保護法に絡んだ内部不正対策に注力したベンダーはログの詳細さと可視化に力を注いだ製品が多いです。

一部領域に特化して自社で全て開発しているメーカーもあれば、広範囲を他ベンダーとの協業やOEM提供でカバーしているメーカーもあります。

結果、あるカテゴリーでは優秀な製品が他のカテゴリーでは凡庸というパターンもあれば、どのカテゴリーでも平均点以上ながら尖ったところは無いという製品や製品ではなく運用サポートで差別化を出しているベンダーもあります。このあたりを考慮せずに機能〇×だけで判断してしまった結果、良くある例としてリプレイスで製品を入れ替えた際に、「機能は確かにあるけども前の製品で出来ていた運用が実現できなくなった」といった残念な状況に陥ったりします。これはLANSCOPE オンプレミス版から他社製品に入れ替えた場合も、他社製品からLANSCOPE オンプレミス版に入れ替えていただいた場合も同様です。

重要なのは自社に必要な要件を明確にし、そこに対してベストな製品はどれか？という検討をする事です。「一部の課題に高いレベル対応すべきなのか？」「複数の課題をまとめてある程度のレベルでつぶしたいのか？」「今はここまでだが将来を考えると何処まで領域を広げて検討しておくべきか？」等々・・様々な視点で検討して自組織にあったIT資産管理ツールを選んでいただければ幸いです。

ここまでIT資産管理ツールについて紹介させていただきました。多機能な製品なので製品毎に強み弱みのバランスの見極めが必要となりますが、上手く活用すれば大きな効果を生む様々な機能が実装されています。また、ひらめき次第でメーカーも考え付かない新しい使い方も生まれます。

皆様も一度自社に導入されているIT資産管理ツールを確認いただき、様々な課題対応にお役立ていただければ幸いです。



MOTEX

●開発／販売

エムオーテックス株式会社

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：06-6308-8980
東京本部	〒108-0075 東京都港区港南 1-2-70 品川シーズンテラス 5F　TEL：03-5460-1371
名古屋支店	〒460-0003 名古屋市中区錦 1-11-11 名古屋インターシティ 3F　TEL：052-253-7346
九州営業所	〒812-0011 福岡市博多区博多駅前 1-15-20 NMF 博多駅前ビル 2F　TEL：092-419-2390

TEL：03-5460-1372 受付時間 9:00-18:00（月～金曜日）

E-mail: sales@motex.co.jp　URL: www.motex.co.jp