LT：1,000CL
OP：リモート操作

お客さま第一
DAiKO 大興電子通信株式会社 様

政府が推進する情報セキュリティ対策に対応

IT資産管理ツールとセキュリティ製品の2つの特徴を生かして業務改善を実現

コーポレート本部 経理部
シニアマネージャー
中島 満 様

経理部 情報システムグループ
小林 孝充 様

所在地　東京都新宿区

Webサイト　https://www.daikodenshi.jp/

大興電子通信株式会社は、約2万社のお客様にICTに関するコンサルティングからシステム・ネットワークの設計・構築、セキュリティ対策の実装、それらすべての運用・保守までワンストップで提供するシステムインテグレーターです。これまでの豊富な経験を生かした業種・業務パッケージの開発や提供のほか、セキュリティ対策やウェアラブルを中心としたIoW（Internet of Workers）など先進ソリューションにも注力しています。

ポイント

- 「AppGuard®」からのアラート発生時に、前後の操作ログを確認して発生原因を分析
- PCの電源ON / OFFのログとタイムカードの時間を照合し、実働時間を把握

導入の経緯

操作の統一を重視し導入を決定 お客様への提案に自社の経験を活用

当社では、近年の情報セキュリティを取り巻く環境の変化に対応するため、1年半ほど前に情報セキュリティの専任チームを再編。定期的に運用方針や改善計画について検討しています。その第一弾として、ログ収集ツールの導入による情報漏洩対策と、会社が認めていない外部デバイスの接続制御を行うことにしました。そのツールの選定にあたっては、ログ管理とUSBメモリを含めたIT資産管理が行えることと、この2つの機能の操作を1つのツールに統一することで、効率的な運用管理が行えることを要件としました。

3社の製品を比較検討し、機能要件を満たしていることはもちろん、管理コンソールのわかりやすさや、問い合わせに対するレスポンスの早さ、導入後のサポート体制なども考慮。当社が、お客様に製品を提案する際、当社自身の導入や運用の経験を事例としてお客様に紹介することも想定して「SKYSEA Client View」を導入しました。

また、当社の情報システムグループはヘルプデスク業務も担っているので「リモート操作」機能も活用しています。導入後は、問い合わせに掛かる時間の短縮に役立っています。

導入の効果

「AppGuard®」のポリシー設定に必要な情報は「SKYSEA Client View」から収集

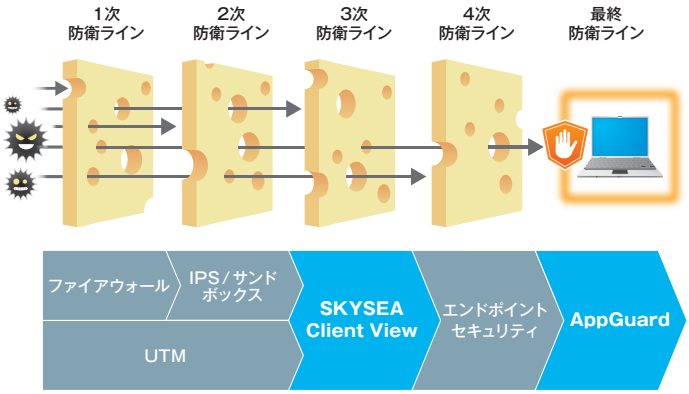
当社では、「AppGuard」というエンドポイントセキュリティ製品を扱っており、既に全社で稼働しています。従来の検知型エンドポイントセキュリティ製品と大きく異なるのは、「マルウェアを探し出して駆除する」のではなく「マルウェアの発症を防ぐ」という点です。Windowsのプロセスを隔離・監視し、アプリケーションが不正な動きをすると瞬時にブロックします。これにより、未知・既知のマルウェアに関係なくシステムに害を与える処理を未然にブロックし、マルウェア感染の脅威から守ります。

「AppGuard」の運用を開始するにあたり、各部署がどのアプリケーションを導入していて、どの共有フォルダにアクセスが必要なのか、といった情報を把握しておくことが重要です。しかし、その現状把握のために現場への聞き取り調査を個別に実施しようとすると、多大な時間と労力が必要となります。「SKYSEA Client View」の「アプリケーション一覧」では、各PCに導入されているアプリケーションがひと目で把握でき、「ログ閲覧」でアクセスしているフォルダの情報も確認することができます。これにより個別の聞き取り実施に比べ「AppGuard」の設定プロセスを短縮でき、スムーズに運用を開始することができました。

また、「AppGuard」が何らかの挙動を検知してアラートが発生したときは、「SKYSEA Client View」でアラート発生時刻前後のログを検索して、PCでどのような操作が行われていたのかを確認しています。アラート発生の原因が、「AppGuard」側の正しい検知によるものなのか、ユーザー側の誤った操作によるものなのかを調査することで、許可されていないアプリケーションの利用を統制することができます。このように、両方のツールの機能をうまく生かすことで、情報セキュリティ対策の強化が図れていると感じています。

操作ログは、情報セキュリティ対策だけでなく勤務実態の把握にも活用しています。人事部門から、「サービス残業を行っていないかPCでの作業時間を調べてほしい」と依頼されることもあり、PC電源のON / OFF時間をリスト化して渡しています。そのリストを基に、人事部門でPCの稼働時間とタイムカードの打刻時間の突き合わせを行い、サービス残業や長時間労働の抑止など労務改善に役立てています。

多層防御でのAppGuard とSKYSEA Client Viewの位置づけ



導入の効果

自社での導入・運用経験は お客様への提案材料として活用

当社におけるセキュリティ対策の次期ステップは、有線・無線を問わず社内ネットワークに接続できるPCのさらなるセキュリティ強化です。まずは不正な接続が行われないよう、「SKYSEA Client View」や「AppGuard」など、当社で指定したアプリケーションがインストールされたPCしか接続できない仕組みにする予定です。そのため、今後はインストール必須アプリケーションを「SKYSEA Client View」に登録し、条件を満たしていないPCの接続を検知した場合には、自動的に遮断を行う仕組みを整えていこうと考えています。

近年、各省庁から情報セキュリティに関する各種ガイドラインが次々に策定され公開されています。内閣サイバーセキュリティセンター（NISC）が公開している「政府機関等の対策基準策定のためのガイドライン」の平成30年度版には、「SKYSEA Client View」や「AppGuard」のようなツールを活用した不正プログラムへの基本的対策に関する具体的な内容が明記されています。政府が推進する情報セキュリティ対策に対応したツールとして、「SKYSEA Client View」や「AppGuard」の必要性は今後ますます高まっていくと考えられます。当社では、すでにこの2つの製品を活用した対策を実装しており、その運用経験をお客様にお伝えすることで、お客様の情報セキュリティ対策強化のお役に立ちたいと考えています。

政府機関等の情報セキュリティ対策のための統一基準群の改定（案）

1. 将来像を見据えたサイバーセキュリティ対策の体系の進化

≪主な内容≫

端末、サーバにおける『未知の不正プログラムの検知／実行の防止の機能の導入』

⇒未知の不正プログラム対策を「侵入後の検知」から「感染の未然防止」へ、「境界監視」に加え「プログラムが動作する内部」へ進化

ソフトウェア等の情報を自動的に収集する『IT資産管理ソフトウェアの導入』

⇒脆弱性の所在の効率的な把握を可能とし、ゼロデイ攻撃等のソフトウェアの脆弱性を狙った攻撃に迅速に対応

情報へのアクセス制御機能として、『デジタル著作権管理による方式』を導入

⇒万が一ファイルが外部に流出しても、オンプレミス※／クラウドを問わず記録された内容の漏洩を防止し、ダメージを無効化

※ オンプレミス:[情報システムのハードウェアを自ら調達し主体的に管理する運用形態]

出典:「サイバーセキュリティ戦略（NISC）」
https://www.nisc.go.jp/conference/cs/dai19/pdf/19shiryou04.pdf

［ 2018年7月取材 ］

Sky株式会社 https://www.skygroup.jp/
東京本社 | 〒108-0075 東京都港区港南二丁目16番1号 品川イーストワンタワー15F TEL.03-5796-2752 FAX.03-5796-2977
大阪本社 | 〒532-0003 大阪市淀川区宮原3丁目4番30号 ニッセイ新大阪ビル20F TEL.06-4807-6374 FAX.06-4807-6376

UR-10000-11 / 18·07·06