2021 年 5 月 11 日
株式会社電通国際情報サービス

ISID、ANA グループにサイバーセキュリティ製品 AppGuard を導入

～国内最大規模、端末約 3 万台への導入設計から運用までワンストップで支援～

株式会社電通国際情報サービス(本社:東京都港区、代表取締役社長:名和 亮一、以下 ISID)は、ANA ホールディングス株式会社(本社:東京都港区、代表取締役社長:片野坂 真哉)を親会社とする ANA グループが保有する約 3 万台の情報機器に対してサイバーセキュリティ製品「AppGuard」の導入を支援しました。導入対象には、空港で一般客が利用する自動チェックイン機や手荷物預け機等も含まれ、AppGuard 導入事例としては国内最大規模となります。

■背景■

ANA グループは、航空運送事業を中心としたエアライングループとして、国内外の航空ネットワークや顧客基盤を生かした多様な事業を展開しています。空港サービスや飛行計画・運航管理等の業務を支えるシステムは 24 時間・365 日の安定稼働が求められると共に、その中で取り扱う顧客個人情報や航空保安情報をはじめとする情報の高度な管理が求められます。

一方、サイバー攻撃のリスクはますます増大しており、マルウエア(悪意のあるプログラムやコード)の難読化※1 や環境依存型攻撃※2、ゼロデイ攻撃※3 など、その手法も高度化しています。ANA グループでは従来の施策に加えて、より強力な対応を行うために今般、情報機器などエンドポイントにおけるセキュリティ対策の抜本的な見直しを実施。未知のマルウエアによるサイバー攻撃からエンドポイント製品を防御するサイバーセキュリティ製品 AppGuard の導入に至りました。

■AppGuard の概要と導入におけるポイント■

AppGuard は、Windows で稼働する情報機器を最新のサイバー攻撃から保護するエンドポイントセキュリティ製品です。ウイルス対策ソフトは一般的に、マルウエアを検知・駆除して「感染させない」ことを目的としており、検知するための定義の最新化が常に必要となりますが、AppGuard は、マルウエアの動作そのものを封じ込め「発症させない」という新しい概念で開発された製品であり、未知のマルウエアに対しても非常に強い防御を実現します。

今回、ANA グループに導入された AppGuard Enterprise※4 は、監視対象機器の集中管理機能を持つ大企業向け製品です。部門やオフィスごとに独自のポリシーを設定し、各情報機器に一斉配布することや、各情報機器からログを収集し、一括で閲覧することが可能です。

大規模導入にあたり、ISID は事前検証から導入支援、導入後のサポートまでをワンストップで提供しています。ISID の持つ ANA グループの業務領域に対する深い知見を生かし、大規模ユーザーに耐えうるインフラ構成を独自に導出、約 3 万台の端末への AppGuard 適用を実現しました。展開に際しては、同グループで従来から使用されている資産管理ツール※5 を活用し、AppGuard 標準機能との組み合わせにより効率的で確実性の高い手法を提案・実現しています。

全日本空輸株式会社デジタル変革室　企画推進部　担当部長の和田氏は次のように述べています。「当社は航空運送事業を中核に事業を進めています。昨今クラウド化が進むにつれて、データセンターの多層防御に課題を感じたこと、セキュリティ運用を担う人材の不足感の課題への対応として、AppGuard を導入しました。ISID には AppGuard の詳細技術

情報の提供とスムーズなシステム導入を支援いただきました。今後は効率的な運用へのアドバイスを期待しています。」

AppGuard の開発・提供元である株式会社 Blue Planet-works 代表取締役 CEO 小林ヤンネ孝貢氏は次のように述べています。「ANA グループから高くご評価いただけたのは、ISID のセキュリティに対する深い知見と、長年培われた AppGuard ノウハウによる優れた運用支援によるものと存じます。ISID は AppGuard を大規模に展開されるお客様にご導入いただくうえで当社にとっても欠かせないパートナー様です。今後も当社はより多くのお客様のお声を取り入れ、製品の改善に努め、ISID のご提案活動を支援していく所存です。」

ISID はかねてより、専門特化した業務ノウハウとシステム構築力を強みとして、金融業や製造業など、幅広い顧客企業の業務改革を支援する多彩なソリューションを提供してきました。これらの知見に革新的なセキュリティ技術を組み合わせることで、サイバーセキュリティ対策の領域においても、顧客企業や社会の課題解決に貢献する、新たな価値を創出してまいります。

■電通国際情報サービス(ISID)について

ISID は、「HUMANOLOGY for the future～人とテクノロジーで、その先をつくる。～」をビジョンに、社会や企業のデジタルトランスフォーメーションを、確かな技術力と創造力で支援しています。金融、製造、ビジネスソリューション、コミュニケーション IT の 4 領域で培ったソリューションの提供に加え、テクノロジーや業界、企業、地域の枠を超えた「X Innovation(クロスイノベーション)」を推進し、顧客、生活者、社会の進化と共存に寄与するソリューションを生み出し続けます。詳細は、公式 WEB サイトをご覧ください。

※1 マルウエアの難読化:マルウエアのコードが悪性なファイルであると検知されないようにコードを読みづらくすることで、検知型 AV ソフトでは検出が困難になっている。

※2 環境依存型攻撃:ファイルレス攻撃ともいわれ、コマンドプロンプトや PowerShell などの Windows 標準のアプリケーションや、Excel や Word などの Microsoft 製品のマクロに攻撃コードを埋め込む手法。検知型 AV ソフトでは正規のアプリケーションと認識されるため、検出が困難になっている。

※3 ゼロデイ攻撃:新たな脆弱性が発見された場合に、修正プログラムが提供される日より前に行われるサイバー攻撃を指す。脆弱性を解消する手段がない状態で脅威にさらされるため、従来型のサイバー攻撃と比べて対策が取りづらく、重大な被害をもたらしやすいとされる。修正プログラムが提供される日を 1 日目＝ワンデイと考え、それより前に行われるため 0 日目＝ゼロデイと呼ばれる。

※4 AppGuard Enterprise:エンドポイント端末向けの AppGuard のエディションの一つであり、集中管理サーバによる集中管理が可能な大企業向けのソリューション。その他にも中小企業向けの AppGuard Small Business Edition、AppGuard Solo がある。さらにサーバ端末向けに AppGuard Server が存在する。

※5 資産管理ツール:エンドポイント端末上で稼働するソフトウェアの情報を収集し、稼働しているソフトウェアの種類やバージョン、ライセンスを管理することで、ガバナンスとセキュリティ対策の強化を目的に使用するツール。

＊ 本リリースに記載された会社名・商品名は、それぞれ各社の商標または登録商標です。

【製品・サービスに関するお問い合わせ先】
株式会社電通国際情報サービス コミュニケーション IT 事業部 SI 営業部 SW ビジネス推進グループ 武田、山本、伊藤
E-Mail:g-appguard-sales@group.isid.co.jp

【本リリースに関するお問い合わせ先】
株式会社電通国際情報サービス コーポレートコミュニケーション部 赤瀬、金野 TEL:03-6713-6100 E-Mail:g-pr@isid.co.jp