セキュリティ：マルウェア・ランサムウェア対策

BlackBerry Protect × CITYASCOM

USERS REPORT

導入ソリューション

BlackBerry Protect

検知率99%以上の人工知能と流入経路追跡で実現する、次世代型マルウェア対策ソフト。従来のパターンファイルを使わない独自のAI技術でマルウェアを検知。

成 果

管理部門の負荷軽減！
インシデント対応の効率化！
（LANSCOPE連携）

九州最大手の独立系ICT企業 BlackBerry Protectで日々進化するサイバー攻撃に備える

金融系や流通系などの業務システム開発を核に、ネットワークの設計やシステム保守・運用といった多様なソリューションを提供しているシティアスコム。日々発生する未知のマルウェアの侵入を防ぎ、企業と社員の安心・安全を守るため、信頼性の高いウイルス感染対策ソフト「BlackBerry Protect」を2021年に導入した。その導入の背景と過程を聞く。

Summary

■ 背 景 ■

1. マルウェアの変化

身代金要求型のコンピューターウイルス等が増加。これらは変異を遂げ、従来のソフトでは検知できない事例も発生。ウイルス感染の脅威が増している。

2. 社外からのアクセス増加

働き方改革やコロナ禍での在宅ワークの広まりによって社外から社内ネットワークへのアクセスが増加。インターネットに常時接続し感染リスクが高い。

3. 個人情報保護法改正の社会的背景

2022年4月の個人情報保護法改正により、情報漏えい等に対する企業責任が重くなる。社会的・道義的責任から従来のソフトの見直しを図った。

■ 選定ポイント ■

1. ウイルスの発見率・誤検知数

最新のAI技術が未知のウイルスを予測する「次世代型ウイルス感染対策ソフト」である。迅速にウイルスを検知し、誤検知も少ない。

2. ウイルス定義ファイル不要

導入時1回のスキャンでPC内のアプリ、ファイルを調べ、ウイルスを検出する。定義ファイルを必要とせず、運用管理がしやすい。

3. 「LANSCOPE」との連携

資産管理のために「LANSCOPE」を導入しており、このソフトウェアとの連携によって感染原因の特定と再発防止ができる。

■ 効 果 ■

1. 脆弱性アプリの即時検出

従来型ソフトで検知されなかった“グレーゾーン”のアプリ等を4,500件検知・隔離した。即時検出によって確実なウイルス感染対策を実現した。

2. 管理・運用負荷軽減

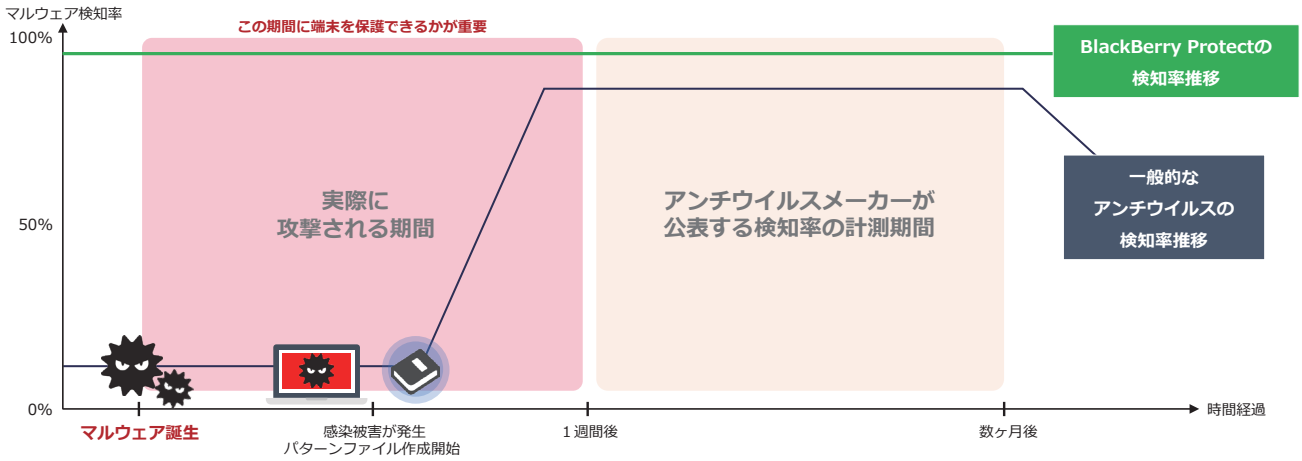
導入時1回のスキャンで済み、その後は自動隔離設定のためPCの定時スキャンが不要。定義ファイル最新化のための運用・管理業務が軽減された。

3. 原因究明と再発防止

「LANSCOPE」との併用によってウイルスの侵入経路や問題となるプロセスを発見でき、再発防止策を検討できる。

BlackBerry Protect × CITYASCOM **USERS REPORT**

セキュリティ：マルウェア・ランサムウェア対策



――ウイルスソフトを入れ替えた理由・きっかけを教えてください。

マルウェア、ランサムウェアと呼ばれるコンピューターウイルスは日々変異し、新しいウイルスが1日100万件以上も生まれています。機密情報の窃取やビジネスメール詐欺による金銭被害に加え、身代金要求型のウイルスも増えており、ネットワークに脆弱な部分が少しでもあれば、そこを狙って攻撃されます。
特にランサムウェアに感染するとデータが暗号化されてPCが使えなくなり、復旧には身代金を払うか、PCを買い替えてデータを入れ直すしかありません。どちらも莫大な費用と日数を要し、企業の信用・信頼も逸します。
当社と付き合いのあった企業もサイバー攻撃を受けており、その脅威は他人ごとではありません。また、2022年4月には個人情報保護法が改正され、情報漏えい等に対してより一層注意を払う必要があります。ソフトウェアの開発等を担う当社は企業と社員の安心・安全を守り、企業としての社会的責任を果たすためにもウイルス感染対策ソフトの見直しを急ぎました。

――「BlackBerry Protect」を選んだ理由は？

これまでのウイルス感染対策ソフトは「ウイルス定義ファイル型」が多く、定義ファイルに合うものをウイルスとして検出します。その定義を最新化するために定期的にフルスキャンを行う必要がありました。しかし、ウイルスは日々変異しており、従来のソフトが新しいウイルスを定義し検出している間にまた別のウイルスが生まれてしまいます。従来のソフトではウイルスの検出が間に合わず、感染の危機から逃れられません（図参照）。
「BlackBerry Protect」は次世代AI型マルウェア・ランサムウェア対策ソフトであり、最新のAI技術により、定義ファイルがなくても未知のマルウェア・ランサムウェアを99%予測検知・隔離します。それに誤検知が少ない。一度導入すれば、定期的なスキャンは不要です。最先端のソフトで、日本の企業はもとより世界各国の企業が導入しており、信頼性も高い。当社では従来のソフトより若干のコスト増となりましたが、“もしものための備え”は必要だと判断し、未知の脅威を防ぐことに重きを置きました。他のソフトとの併用により、ウイルスの侵入経路発見や再発防止ができることも魅力でした。

――導入から運用までの手順を教えてください。

経営管理本部コーポレートIT部
課長　藤田 徹郎氏
主任　古賀 大輔氏

2021年9月、社員1,000台のPCに導入し、全社一斉に切り替えました。まず、ソフトをインストールするとスキャンが始まり、“ウイルスに狙われる可能性のある”アプリやファイルを検出します。当社ではそれが4,500件に上りました。従来のソフトでは検知されなかったものです。
次に、検知されたものの精査を行い、使用可否を決定。それに伴う設定をして運用を開始します。当社では4,500件を精査して、3,000件は使用可、1,000件は使用不可としました。残りの500件は使っている社員に話を聞き、安全性を確認して使用の可否を決定しました。プロジェクトごとに必要なアプリのインストールやサイトの閲覧を行っているのですが、それらの脆弱性が露呈し驚きました。

――導入による効果は？

ウイルス検出のためのスキャンは導入時の1回で済み、その後は自動隔離設定で定時スキャンは不要のため、管理部門の負担は軽減しました。
「BlackBerry Protect」はウイルス感染を予防するためのものですから、“何も起こらない”ことが当たり前です。安心や満足は表面に現れにくく、数値化することができませんが、そのような企業や社員の安心・安全を担保するのが管理部門の役目ではないかと思います。
働き方が多様化する一方でサイバー攻撃は複雑化・高度化しており、従来の対策では対処できなくなっています。「BlackBerry Protect」は業務内容や予算に合わせて段階的に導入することもできますので、ウイルス感染対策ソフトの見直しをおすすめします。

マルウェア、ランサムウェアとは？

マルウェアとは、ユーザーのデバイスに不利益をもたらす悪意のあるプログラムやソフトウェアの総称です。身代金要求型コンピューターウイルスはRansom（身代金）とSoftware（ソフトウェア）を組み合わせてランサムウェアと呼ばれます。

CITYASCOM
株式会社　シティアスコム
〒814-8554　福岡県福岡市早良区百道浜2-2-22　AITビル
TEL：092-852-5120
https://www.city.co.jp/