■ McAfee Embedded Control 導入事例 ―

シスメックス株式会社

シスメックス株式会社

プロファイル

シスメックス株式会社（以下、シスメックス）は、病気の診断や治療に欠かせない検体検査に使われる検査機器を製造、世界中に向けて販売している。1963 年に国内初の自動血球計数装置を実用化、今ではヘマトロジー（血球計数検査）からライフサイエンス領域にまで事業領域を拡大している。ヘルスケアをデザインするという使命のもと、医療従事者の負担を軽減し、人々のクオリティオブライフの向上に取り組んでいる。

「検査機器へのWindowsの普及は、利便性とともにセキュリティ脅威をもたらしました。患者の個人情報を守り、医師に正確なデータを提供するために必要だったのは、McAfee Embedded Controlです。」

シスメックスでは、医療機関や検査機関で使われる精密な検体検査機器を製造しています。これらの機器で取り扱うデータは、患者のプライバシーに深く関わる情報であり、医師が診断の材料とする重要な情報でもあります。外部に漏えいしないこと、データ改ざんの恐れがないことを保証することが、安心して診療を受けられる環境と、医師の間違いのない診断を支えます。

検査機器が扱う情報を守るために、検査機器にもセキュリティが求められる現代。そこにはどのような危険が潜み、セキュリティ機能の実装にはどのようなハードルがあるのでしょうか。McAfee Embedded Controlの導入でセキュリティ強化を実現した、シスメックスの例をご紹介します。

医療現場において、ヘマトロジー検査が担っている役割

シスメックスの主力となっているのは、ヘマトロジー検査と呼ばれる分野で使われる検査機器です。ヘマトロジー検査とは、採取した血液中の赤血球や白血球などの数や種類、大きさを測定し、分析する検査。これらの検査は医師ではなく、国家資格を持つ検査技師によって行われます。

実際の利用シーンを、総合病院を例にご紹介しましょう。血液検査が必要な患者は、診察室や処置室で血液を採取されます。採取された血液は検査室へと運ばれ、検査技師の手によって検査機器にかけられます。検査結果はネットワークを通じてサーバーへ送られ、医師はそのデータに基づいて診断を行います。通常なら1マイクロリットルに4千～9千個程度の白血球が1万個ほどになっていたら風邪かもしれない、数万にもなっているようなら白血病を疑ってみる、といった具合です。

実際には血液の検査は1種類だけではなく、数種類の検査機器にかけられ、検査結果はネットワークを通じてサーバーへと集約されます。医師は集まった情報を総合的に判断して、診断を下します。ネットワークを通じて複数のデータを自動的に集約できるメリットと、ネットワーク接続によるセキュリティ脅威のデメリットとが考えられますが、クローズドネットワークとして構築される場合が多く、セキュリティが意識されることはあまりありませんでした。

組み込み機器へのWindowsの普及が検査機器開発のセキュリティに大きく影響

検査機器のセキュリティが注目され始めたのは、2000年頃からのことです。組み込み機器にもWindowsが使われはじめたことがきっかけでした。汎用性が高く開発環境を整えやすいことから、開発スピードの向上やアプリケーションの高機能化に大きく貢献しましたが、セキュリティ面ではその汎用性がマイナスに作用しました。

また、医療機器の高度化や病院内のネットワーク化が急速に進んだことも影響しています。ほとんどの病院では、個人情報を漏えいさせないために医療機器のネットワークをクローズドな設計にしています。しかしそこには、診察室のPCやWindowsが組み込まれた機器が含まれています。USBメモリー等の外部媒体によってウィルスが持ち込まれたり、感染した端末から情報が持ち出される危険性はゼロではないのです。

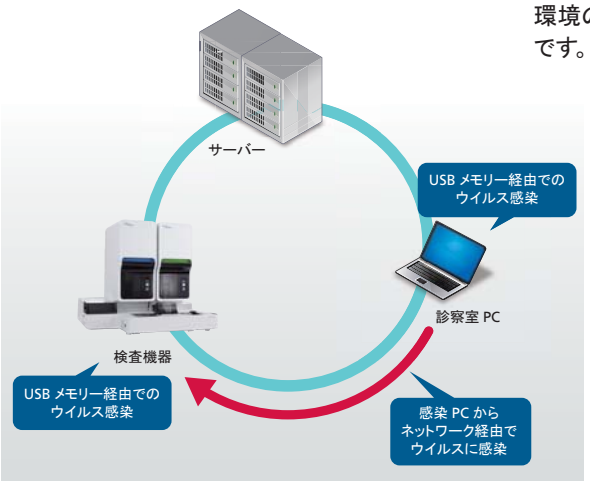

図 1. 想定されるウイルス感染経路

医療の現場は「セキュリティの脅威＝情報漏えい」だけでは済まないシビアな世界

一般に語られるセキュリティの脅威といえば、個人情報や企業の機密情報の漏えいがほとんどです。これらももちろん大切な情報であり、漏えいすれば事業を継続できないほどの重大なインパクトをもたらす恐れがあります。

しかし、医療現場におけるセキュリティの脅威は、それを上回る問題を引き起こしかねない重大な危険をはらんでいます。

冒頭に紹介したように、医師は検査機器からもたらされたデータに基づいて、病気を特定し、治療方法を決定します。もし、検査機器がウイルスに侵されて正常に機能せず、判断の材料となるデータが信頼できなくなったら。もし、誤ったデータに基づいて誤った診断、誤った治療を行ってしまったら。最悪の場合、財産や事業ではなく、生命さえ危険に晒しかねません。

ウイルス感染が引き起こしかねない被害

- 検査機器の誤動作により検査結果データの精度が低下、誤った診断や治療が行われる
- 検査機器や医療情報機器が正常に動作せず、必要な情報にアクセスできないために診断や施術に遅れを生じる
- 診療情報の漏えいにより、弱みに付け込むような悪質なビジネスの標的にされる

組み込み機器の限界、性能保証、クローズドネットワークでの運用など、いくつものハードルが立ちはだかる

しばらくの間はユーザー側での対応に任せる運用が続きました。Windowsをベースとしているので、一般的なWindows PC用のウイルス対策ソフトをインストールし、使うことは可能だったからです。しかし、セキュリティに敏感な医療機関ばかりではありません。そもそも医師の本分は目の前の患者を治療することであって、そのための道具であるIT環境の整備に時間をかけられない場合がほとんどです。

しかしその間も、シスメックスは手をこまねいていた訳ではありません。ウイルス対策の有効な手段を講じてほしいという利用現場からの声に応える方法について、検査機器にWindowsを使い始めた当初から検討を始めていたのです。しかし、その対策は一般のPCのように容易ではありませんでした。

一つめの課題は、検査に必要なだけの処理能力しか持っていない組み込み機器に、ウイルス対策ソフトを動作させるだけの余裕がなかったことでした。これは時代が進むにつれて解消されていきましたが、検査実施中のウイルススキャンを禁止するなど運用面での対策は続きました。高い精度を求める検査のため、アプリケーションは万全の状態で動かすのが理想だからです。

もう一つの課題は、出荷後の改変について責任を持てないということでした。検査機器の精度に責任を持つためには、できる限り出荷時に検査した状態のままで使ってもらう必要があります。しかし、一般的なウイルス対策ソフトは定義ファイルや処理エンジンの定期的な更新が欠かせず、出荷後の改変が前提となってしまいます。また、多くはクローズドネットワークで運用されており、定義ファイルの更新自体も困難です。

いくつものウイルス対策ソフトを検討したものの、先述の課題を解決できる製品は見つかりませんでした。そこには、根本的な構造の問題があったからです。

一般的なウイルス対策ソフトは、ウイルスの特徴をリスト化した定義ファイルに照らしてファイルや通信をスキャンし、当てはまるものをウイルスと認めて排除する方式を取っています。これはブラックリスト方式と呼ばれる方式です。常に最新のウイルス情報を定義ファイルに追加し続けなければ運用できませんし、定期的に全ファイルのスキャンを実行しなければなりません。

ホワイトリスト方式を採用し、様々な課題を解決してウイルス対策を実現したMcAfee Embedded Controlを採用

根本的な解決策を求めて情報収集を続けるシスメックスが、McAfee Embedded Controlと出会ったのは、2007年のことでした。システムインテグレータから、新たに取り扱いを始めた製品として紹介されたものでした。

紹介されたその製品は、まさに求めている機能を備えていました。定義ファイルの更新も、ファイルスキャンも不要で、ウイルスに対しては完全な防御を実現していたのです。

課題解決の秘密は、McAfee Embedded Controlが採用するホワイトリスト方式にありました。阻止すべきものを定義するブラックリスト方式とは違い、ホワイトリスト方式では許可すべきものを定義します。それ以外のアプリケーションは、一切起動させません。万一、ウイルスが混入したとしても、そのウイルスはプログラムとして起動することができず、感染活動も破壊活動もできないのです。

ブラックリスト方式では新たな脅威が生み出されるたびにリストに追加しなくてはなりませんでしたが、許可すべきものを定義するホワイトリスト方式なら、システムに変化がない限り定義ファイルを変更する必要もありません。アプリケーションの追加やバージョンアップが頻繁に行われる一般のPCとは違い、検査機器の場合は出荷時の状態のままで使われます。ホワイトリスト方式ならセキュリティのための余分な運用の手間をかけることなく、ウイルス対策ができるのです。

	ブラックリスト方式	ホワイトリスト方式
アプリケーション性能への影響	× ウイルス定義ファイルの更新、ウイルス検知・駆除のためのスキャン作業時にシステム負荷が発生する為、アプリケーション性能の劣化が懸念される。	○ 予めホワイトリストに登録されたアプリケーションのみを実行する仕組みの為、定義ファイルによるスキャンは不要となり、性能劣化が抑えられる。
システム管理者による運用負荷	× 定期的なウイルス定義ファイルの更新とスキャン作業の実施により、システム管理者の運用負担が伴う。	○ ホワイトリストによる保護機能が実装されると、定義ファイルの更新、スキャン作業は不要となり、運用負荷が軽減される。
未知のウイルス脅威に対する保護機能の優位性	× 定義ファイルで対応していない、未知のウイルス感染リスクからの回避が難しい場合がある。	○ 実行するアプリケーションを限定することで、未知のウイルスの実行を防止、感染リスクを回避できる。

図2. ブラックリスト方式とホワイトリスト方式の違い

オプション販売からスタートし、セキュリティ意識の高まりを受けて標準装備へ

McAfee Embedded Controlは、まずヘマトロジー検査機器のオプションとして導入されました。セキュリティ対策を求められた場合に、付加機能として購入してもらう形態です。しかしセキュリティ機能は備わっていて当然と考えるユーザーが増え、最新モデルの検査機器からは標準的な装備として扱われています。内部のセキュリティポリシーでセキュリティベンダーを指定されているなど一部のケースを除き、McAfee Embedded Controlがインストールされた状態で検査機器は出荷されます。

医療現場でのセキュリティに対する不安の声から始まったウイルス対策の取り組みは、その声の高まりに応じて、付加機能から、なくてはならない機能へと重みを増していったのです。

セキュリティ機能は、検査機器に求められる主機能ではありません。そのため、セキュリティ機能を備えていることがその製品の優劣に直接関係する訳でもありません。しかしシスメックスが考える信頼できる検査機器には、セキュリティ機能はいまや不可欠です。そして市場にもそれは受け入れられています。

日本製の高品質な機器を送り出し続けることで、ブランドを守るためにも、セキュリティへの取り組み、品質へのこだわりを忘れない

シスメックスの検査機器は、日本国内だけではなく世界中で利用されています。海外の競合に対して絶対の自信を持ち、優位に立っていられるのは品質の高さという裏付けがあるからにほかなりません。シスメックスというブランド、日本製品への品質の期待に応えるため、シスメックスのエンジニアは努力を重ねてきました。

品質へのこだわりは、自社で開発した機器やソフトウェアだけではなく、セキュリティ機能として組み込んだMcAfee Embedded Controlにも向けられました。

実は製品を知ってから実際に採用されるまでに、開発エンジニアを交えたミーティングが繰り返されました。それまでになかったホワイトリスト方式という新しい概念、それを実現する実装方法について理解するためでした。自社製品の機能として世に出すからにはそこまでして当然と考えるエンジニアの姿勢が、シスメックスのブランドを支えています。

検査や予防医療の重要性を訴え、医療コストの削減と人々の健康増進に尽力

ヘマトロジー、ノンヘマトロジーを含めた検査機器の開発や、ライフサイエンス分野での新たな商品の開発を支えているのは、人々の健康を支えたいという思いです。だからこそ、ひとつひとつの製品の品質にこだわっています。

機器の高度化が進んだ現在、そうした品質のこだわりの中でセキュリティは欠かせません。McAfee Embedded Controlを得たことでシスメックスは、本来の領域での品質向上により邁進できるようになりました。

検査精度についても、セキュリティについても、安心して使ってもらえる機器を提供するというシスメックスのこだわりの一部を、マカフィーが担っています。

取材日時 2013年3月

McAfee An Intel Company
マカフィー株式会社
www.mcafee.com/jp

●製品、サービスに関するお問い合わせは下記へ

東京本社　〒150-0043　東京都渋谷区道玄坂1-12-1 渋谷マークシティウエスト20F
TEL:03-5428-1100(代)　FAX:03-5428-1480

西日本支店　〒530-0003　大阪府大阪市北区堂島2-2-2 近鉄堂島ビル18F
TEL:06-6344-1511(代)　FAX:06-6344-1517

名古屋営業所　〒460-0002　愛知県名古屋市中区丸の内3-20-17 中外東京海上ビルディング3F
TEL:052-954-9551(代)　FAX:052-954-9552

福岡営業所　〒810-0801　福岡県福岡市博多区中洲5-3-8 アクア博多5F
TEL:092-287-9674(代)　FAX:092-287-9675