

「InterSafe SecureDeviceを導入してから、ウイルス検出件数がゼロになりました。」

潤和リハビリテーション振興財団 潤和会記念病院
財団本部 経営企画部 IT推進室 主任 上級医療情報技師
服部正樹氏



潤和会記念病院のITをシステムと経営の双方の視点から支えるIT推進室服部氏に、InterSafe SecureDevice Professional (以下、InterSafe SecureDevice)の導入の経緯と効果について詳しくお聞きしました。

潤和リハビリテーション振興財団 潤和会記念病院

潤和会記念病院は宮崎市の中核病院としての役割を担っています。長年継続してきたリハビリテーション活動を基盤にして、生活習慣病予防管理、神経疾患の診断治療、消化器疾患の診断治療、リウマチ、関節疾患を中心とした整形外科的疾患の診断治療、痛みしびれに対するペインクリニックを柱とし、専門的かつ高度な医療をすすめています。病床数446床、常勤医40名を有しています。



〒880-2112
宮崎県宮崎市大字小松1119番地
<http://www.junwakai.com/>

IT推進室について

潤和会記念病院に導入するシステムの企画・提案をメインに行っています。病院システムの導入やリプレースを経営的な視点をもって主導的に進めていくのが、IT推進室の仕事です。

当病院は、2003年に宮崎県内でも早期から電子カルテを導入するなど、情報システムに力を入れており、IT推進室では、医療業界とIT業界を幅広く横断する視点から、一歩先を見すえたシステムを企画・構築していく必要があります。



病院のセキュリティ対策の特殊性

一病院のセキュリティ対策では、どのような点に気がつかれますか。

病院でセキュリティを高めるにあたっては、ウイルス・情報漏洩対策とUSBメモリの利用のバランスをとることに気がつかれています。

病院は患者さんの生命・健康を預かっており、究極的にはセキュリティよりも診療が優先されます。職員、特に医師は診療の関係で、いつでも、どこでも患者さんのカルテを見られる状態にしておきたいと考えています。また、学会での発表や論文作成にカルテが必要なこともあり、USBメモリでデータの持ち出しを認めないわけにはいきません。

他方、院内ネットワークがウイルスに感染して、診療が停止してしまうことは絶対に避けなければなりません。またカルテ情報は個人情報の最たるもので、情報漏洩も防止する必要があります。

USBメモリのセキュリティ対策として、潤和会記念病院では、InterSafe SecureDeviceを2010年9月に120ライセンス導入し、翌10月から運用を始めました。現在、医師、看護師含め、全ての部署で使用されています。

職員の利用状況にあわせて利用モードを変更

一InterSafe SecureDeviceをどのようにお使いですか。

職員の個別の利用状況にあわせて、モードを変えて使っています。例えば、研究や学会発表のために院内外で統計資料を活用する医師はパスワードモード、自宅で研究発表資料を作って院内に持ち込む看護師は情報漏洩対策モード、院外の会議用に資料を持ち出す事務員はウイルス対策モードにするなどしています。

一職員によってモードが変わるといっていますが、困惑や反対などはありませんでしたか。

今までの利用に制限がかかるので、反対意見がでることが予想できました。職員は院内外で様々な形態での業務を行っており、その中でUSBメモリを自由に利用し、最大限活用されていました。これに対して、システム管理者側が決めた制限をいきなり設けてもうまくいかないのは明確です。

そこで、段階を踏んで導入することにし、その結果、スムーズに進めることができました。

スムーズに導入するために工夫したこと

一段階を踏んで導入するとは？

3段階を経て導入しました。まず第1段階では、職員のセキュリティ意識を高めるようにしました。

それまでのウイルス検出の統計をとったところ、約9割がUSBメモリが原因で、1か月に2~3回の頻度でUSBメモリからウイルスが検出されるといった状況でした。

ただ、各部署のUSBメモリの利用頻度と、ウイルス検出頻度は比例していませんでした。毎日使っていても全く検出されていない部署と、利用頻度が低いのに何度も検出されている部署に分かれていました。検出されたUSBメモリの所有者にヒアリングしたところ、セキュリティに対する意識が院内でバラバラで、これがウイルス検出頻度に影響していることが分かりました。

そのままでは、USBメモリの使用を禁止しても別の手段でデータを持ち出す職員が現れ、セキュリティ上の弱点がさらに大きくなる可能性があります。そこで、まずは職員のセキュリティ意識を高めることが必要だと考え、全職員を対象にセキュリティ研修を行いました。

一セキュリティ研修はどのような内容でしたか。

研修では、安易にUSBメモリを使うことで増えるリスク、すなわち、①USBメモリ紛失時の個人情報漏洩の問題、②USBメモリを介した、病院ネットワークへのウイルス感染問題などについて、職員全員が参加できるように複数回、説明を行いました。情報漏洩やウイルス感染が発生してしまった場合には、患者さんへ被害が及ぶのはもちろん、病院の社会的信用が失われ、その後の対応と再発防止のための極端な業務制限によって、職員満足度が著しく下がってしまう可能性があることを、実際の他病院で起こった事例を示し、その怖さを強く訴えました。

一次は、どのようなことを行ったのでしょうか。

その次は、トップダウン式でUSBメモリの今後のセキュリティ対策の取り組みについて伝達してもらいました。院内の運営会議で各部署長へ今後の対策予定内容を伝え、各部署長から各職員へ、セキュリティ対策を行うという指示を出してもらい、IT推進室からの依頼ではなく、病院全体の方針と認識してもらいました。

一第3段階ではどのようなことをしましたか。

実際にInterSafe SecureDeviceを導入する段階では、各部署で使用するUSBメモリを決め、それぞれの使用目的と、どのモードにするかを申請書に記入して提出してもらいました。使用目的を書いてもらったのは、そもそもUSBメモリを使わなくても対応できる事案でも、USBメモリを使っているのではないかと考えていたからです。そのような場合には、申請を受け付けず、代替案を個別に提示しました。

それ以外は申請の通りのモードで利用してもらっています。無理のない運用とならないように、IT推進室からは制限しないようにしました。

USBセキュリティ対策製品を導入するための要件

一USBセキュリティ対策の製品導入にあたって、どのような要件をたてましたか。

以下の8つの要件をたてました。

1. 導入・運用が楽であること

職員のITスキルにはばらつきがあるので、業務の負担にならない簡単に使えるものを選びたいと考えていました。また、病院全体で速やかに運用開始できるように、導入が容易であることも条件としました。

2. USBメモリの内容を他人が見ることができないこと

万が一、紛失したときでも、他人がUSBメモリの内容を見ることができないものを選びたいと考えていました。内容を暗号化したり、利用時にパスワードを要求するものがよいと考えていました。

3. ログの集中管理ができること

誰がどのようなファイルを持ち出しているのかなどを集中的に管理するために、ログが自動的にサーバに記録される機能を欲しいと思っていました。

4. セキュリティの段階が複数あること

職員と言っても、学会等で臨床研究結果を精力的に発表する医師や看護師等から、ほとんど院内だけで業務を行う事務職員まで様々な職員がいます。それぞれの利用状況によって、制限の内容を変えられるとよいと考えていました。

5. ピンポイントでセキュリティ対策ができること

セキュリティ対策は実際に当院が必要とすることを、その時の状況に応じて流動的に行う必要があるため、その時点で必要な機能だけを有し、不要な機能は付いていないことを条件としました。不要な機能は、相性問題や機能のバッティング問題を発生させる危険性もあるからです。

6. 各パソコンにインストールしなくてもよいものであること

院内にはパソコンが700台近く存在し、その全てにアプリケーションをインストールするとなるとそれだけで大変な作業となります。また、古いパソコンを長年使っている部署もあり、動作速度低下が起こらないように、各クライアントパソコンにソフトをインストールするのは避けたいと考えていました。

7. 低コストで導入できること

セキュリティ対策は重要ですが、それに膨大なコストをかけ

てしまっては本末転倒です。決して増収となる施策ではないため、できるだけ低コストで導入したいと考えていました。

8. 既存のUSBメモリが利用できること

低コストで導入できることと関係しますが、新たにUSBメモリを購入することなく、現在使っているUSBメモリをそのまま利用できる製品が望ましいと考えました。USBメモリの容量はどんどん大きく、価格はどんどん安くなりますので、USBメモリを買い替えても使用できると良いと思いました。

この条件で複数の製品をカタログで比較検討した結果、InterSafe SecureDeviceが最も要件を満たしていたので、導入することにしました。

一カタログでの比較ということですが、試用はしなくても大丈夫だったのでしょうか。

カタログで比較して、InterSafe SecureDeviceは必要な機能が揃っており、不要な機能が入っていないことが分かりました。まさに「ドンピシャ」という表現がピッタリの製品でした。

念のため試用版をダウンロードして使いましたが、機能的にも十分で、導入・運用も簡単そうでした。

InterSafe SecureDeviceの導入効果

一導入効果について教えてください。

それまで1〜2週間に1回はあったウイルス検知がゼロになりました。誰が、いつ、どのデータを持ち出したかといった、持ち出し状況を具体的に把握できるようになりました。また、事故を防ぐとともに、万が一の場合の病院・職員の負担を軽減することができました。

一InterSafe SecureDeviceへの評価について教えてください。

InterSafe SecureDeviceはポイントを絞ったソフトで、足りないところをピンポイントで補えることができました。お世辞めきで、本当に助かりました。

セキュリティの段階分けがあるので、利用状況にあったセキュリティの設定ができます。特に、様々な職種・部署が混在して、USBメモリの利用目的もそれぞれ異なる病院という組織においては、本製品はピッタリだと思います。

今後の取り組み予定

一今後、セキュリティ対策に関して、どのような取り組みをしていく予定ですか。

不要なデータを持ち出していないか、データ持ち出しの際に個人情報を削除しているかなど、細かなチェックシステムを作っていく予定です。

あとは、全職員のセキュリティ意識を、さらに高めていきたいと考えています。その一環として、セキュリティ対策のための院内Webサイトを立ち上げました。今後はそれを見れば、誰でもウイルス対策や情報漏洩対策ができるようなコンテンツを充実させていくつもりです。



「医療従事者の意見を尊重しながら、セキュリティを高める工夫をしました」

ウイルス検出の危険性を訴える方法

IT推進室ではウイルス検出の状況を把握して危険性を認識していますが、なかなか他部門にはそれが伝わらず、対策の必要性を伝えることが困難でした。

検出時の迅速な対応が目的だったのですが、ウイルス検出と連動して光るパトランプをIT推進室の部屋の真ん中に設置したところ、IT推進室を訪れる多くの職員が興味を持ちました。事務部門ではありますが、同じフロアの職員はこのランプが頻繁に光るのを見て、実際にウイルスが身近なものであり、USBメモリの危険性を感じてもらうことができました。



パトランプをIT推進室の入口に設置し、ウイルスの危険性の理解を深めた。

開発・販売元



アルプスシステム インテグレーション株式会社

〒145-0067 東京都大田区雪谷大塚町1-7

TEL 03-5499-1331 FAX 03-5499-0357

●詳しい情報は <http://www.alsi.co.jp/>

※ALSI, InterSafe, InterSafe SecureDeviceはアルプスシステム インテグレーション株式会社の登録商標です。その他記載の製品名・社名は一般に各社の商標または登録商標です。

※このカタログの内容は2011年7月現在のものです。内容は予告なく変更される場合があります。

■お問い合わせ先