

愛媛大学医学部附属病院

病院が被災時のBCPをめざす クラウドを利用しセキュアな リモートアクセス環境を整備

導入企業



愛媛大学医学部附属病院

<http://www.hsp.ehime-u.ac.jp/>

〒791-0295 愛媛県東温市志津川

「患者から学び、患者に還元する」という建学以来の精神を貫き、高度先進的な医療、医学教育を通じて社会貢献を目指す愛媛大学医学部附属病院。治療方法の研究だけでなく、診療現場でのIT活用やそのための仕組みのあり方についても先進的な取り組みと研究を続けている。



愛媛大学医学部附属病院
医療情報研究室 准教授
木村 映善 先生

課題

- アクセスに必要なトークンを常時持ち歩いてもらうのは困難
- 有事の際にも必要な情報へのアクセスを確保する認証基盤の構築
- 個人情報を含むデータへのアクセスの制約が情報活用の足かせに

効果

- 物理トークンなしでいつでも使えて、ユーザ増加にも1名単位で即時対応可能
- 災害など万一の事態が発生しても情報へのセキュアなアクセスが可能
- 情報保護から情報活用に進むための高レベルなセキュリティ基盤を構築

導入の経緯

愛媛大学医学部附属病院では、電子カルテの活用など医療情報のIT化に取り組んできた。診療記録を素早く参照できる電子カルテの仕組みは日々の診療に生かされ院内に浸透していたが、一方で紙のカルテに及ばないポイントも指摘されていたという。

「これまでの電子カルテではシステムの容量上の制約や、医師法の保存義務を根拠として、保存期間を5年程度に区切って運用されていることがあります。普段の診療ではそれで十分なこともありますが、“古いカルテを参照する必要”も依然として残っています。近年欧米で広まりつつあるEHR(Electronic Health Record:生涯健康医療電子記録)という考え方を取り入れ、医療サービスの向上とともにビッグデータ分析の基盤としても活用できる電子カルテシステムへと刷新することを目指しました」

そう語るのは、愛媛大学医学部附属病院 医療情報研究室 准教授の木村 映善氏。そして、電子

カルテ刷新に合わせて整備に取り組んでいるのがリモートアクセス環境の再構築だ。これまでも医療機器や医療情報システムのメンテナンス用にリモートアクセス環境を用意していたが、運用上の課題をいくつか抱えていた。ひとつは、IPsec方式のVPNを使っているため、相手先の環境により接続できない場合があるということ。そしてもうひとつが、認証に使われているワンタイムパスワードトークンの運用だった。

「緊急に対応してもらいたいからこそ、来院せずにもメンテナンス可能なリモートアクセス環境を用意しているのですが、実際にはインテグレータの担当者さんがトークンを常時持ち歩いてくれる訳ではありませんでした」

しかし、医療システムへの接続には十分なセキュリティを確保しなければならないと木村氏は言う。電子カルテの刷新に当たり、強固で利便性の高い認証を用いたリモートアクセス環境の再構築が欠かせなかった。

導入決定のポイント

新たなリモートアクセスの仕組みには、IPsecに比べて接続性が高く幅広い端末に対応可能なSSL VPN方式を採用。組み合わせる認証製品にはSECUREMATRIX[®]が選ばれた。最大の要件は、トークンに依存せずに強固なセキュリティを確保できることだ。これから先、災害対策やBCPまで視野にいれて考えた場合、緊急事態発生時にもトークンを所持していることを想定することは現実的とは思えなかったという。同じくBCPという観点から、認証基盤をクラウド上に設置でき

ることも大きな要件となった。

「さらに、必要な情報に医師がスムーズにアクセスできるようになるためには、端末を選ばずに十分なセキュリティを確保できなければなりません。OSに依存しないSECUREMATRIX[®]なら、緊急時に偶然手元にあるPCやスマートデバイスからでも必要な認証を経てシステムにアクセスできます」

木村氏はそう言い、さらにCSEがスマートデバイスにおける二要素認証を開発中であったことも考慮したと付け加えた。

実際の導入までの課題

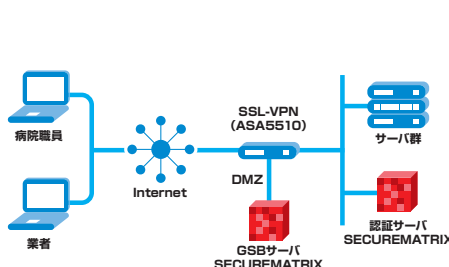
新たな電子カルテの仕組みが出来上がるのは、2014年5月。SSL VPNとSECUREMATRIX®を組み合わせリモートアクセス環境もスタートする。認証サーバはクラウド上で運用されるため、万一の災害が発生して病院内のシステムが大きなダメージを受けたとしても、情報アクセスに必要なセキュリティを維持できるようになる。

新しいリモートアクセス環境はこれまで同様にリモートメンテナンスに使われるほか、病院情報システムに関するセキュリティポリシーを調整の上、医療従事者向けにも開放していきたいと木村氏は語る。

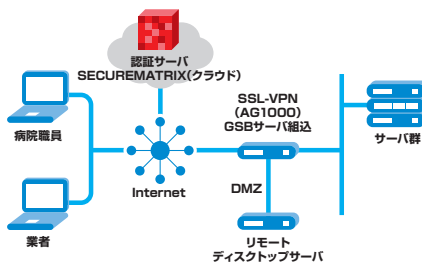
「これまで、電子カルテに接続できる端末は限定されていました。今後は医師の要望に応じて、必要なときに使いやすい端末から電子カルテを参照できるようにすることも視野に入れています。たとえば病院情報システムの端末ではないPCからでも、電子カルテを参照し、診療記録を作成できるようになります」

■ 愛媛大学医学部附属病院

評価環境構成 2013年8月



最終構成 2014年5月(予定)



セキュリティ確保のため、愛媛大学医学部附属病院では診療用ネットワークとは別に病院情報システムの端末ではないPCから接続可能な仮想ネットワーク構築を検討している。電子カルテ端末以外のPCから電子カルテにアクセスするた

めにはSECUREMATRIX®による認証を経て、さらに仮想デスクトップを経由することで端末に情報が残ることを避ける仕組みだ。

現在の運用状況

2014年5月の電子カルテ刷新に先立ち、2013年夏から一部でSECUREMATRIX®の導入が進んでいる。院内にSSL VPN製品とSECUREMATRIX®の認証サーバが設置され、従来のIPsec VPNと並行して利用されている状況だ。

「リモートアクセスのアカウント不足に悩んでいましたが、これからトークンを買い足すのは効率的ではありません。そこで、認証の移行期間を設ける意味合いも兼ねて、リモートアクセス環境のみ一足先に整備しました。こうした短期の運用が簡単にできるのも、デバイスレスな

らではの強みですね」

ユーザ側の使い勝手もよく、平時から緊急時までをカバーし、シームレスに使える認証方法だと再確認しているところだと木村氏は言う。実際に運用しながら2014年の導入に向けて細部を煮詰めることができるので、プロジェクト全体にもいい効果を感じているようだ。

そして、トークン不要で強固な認証を実現するその仕組みとともに、セキュリティを支える企業としての期待をCSEに寄せているとも木村氏は言う。

「認証はシステムを利用するための前提になるも

のですから、セキュリティの高さとともにサービスの継続性、提供する企業の信頼性も高くなければなりません。その点CSEは、SECUREMATRIX®で十分な歴史と実績を築いており、今後も信頼して付き合っていける仕組みだと考えています」

高度化する医療の現場において、ITの機能性と利便性を実現するための裏付けとなる高いセキュリティをSECUREMATRIX®で実装していく愛媛大学医学部附属病院。これからも先進的な取り組みで医療情報の活用範囲を広げていくことになりそうだ。



一般にセキュリティは、攻撃から身を守り情報漏洩を防ぐなど、守りの視点で語られることが多い。しかし木村氏は、セキュリティに攻めの視点を持たなければならないと強調する。「医療サービスの提供範囲と可用性を高めるために、ITをこれまでより積極的に活用していかなければなりません。情報を守るだけでなく、セキュリティを高めることで活用できる範囲を広げていく、そんな視点で新たな基盤づくりに取り組んでいます。成熟したセキュリティ技術を投じてまずは安全な基盤を作り、今後は倫理面や心理面、運用ポリシーの研究など運用面の課題に取り組んでいきます」

※記載内容は取材当時(2013年10月)のものです。

開発元
株式会社シー・エス・イー
CSE <http://www.cseltld.co.jp>
〒150-0002 東京都渋谷区渋谷3-3-1 A-PLACE渋谷金王
TEL.03-5469-6026 FAX.03-5469-6037
E-mail: sales@cseltld.co.jp

●お問い合わせ先