

セキユアな次世代医療体制を目指す 慶應義塾大学病院の挑戦

医療機関などにおけるサイバーセキュリティのあり方が問われるなか、慶應義塾大学病院ではこの4月にアメリカ発のエンドポイントセキュリティシステム「HP Sure Click Enterprise (HP S C E)」を導入したという。そこで、今号ではその背景やHP S C E にかける期待感について、慶應義塾大学病院の情報システム関連の皆さんに聞いてみた。

「インターネット分離」と 誓約書による意識醸成を推進

—— 昨年末、徳島県つるぎ町の半田病院が「ランサムウェア（身代金ウイルス）」に感染し、電子カルテなどにアクセスできなくなつたほか、診療費の請求作業などでもできなくなり、新規患者の受け入れをストップするという事態に陥りました。通常診療を再開するまでに約2カ月も要するなど、まさに地域医療におけるサイバーセキュリティの重要性を再認識させられる事件だったように思います。そこで、今回は大学病院としてセキュリティ対策にどのような取り組みを組まれているかといったことを中心に伺いたいと思うのですが、そもそも慶應義塾大学病院ではいつ頃から電子カルテを導入しはじめたのでしょうか。

電子カルテに関するシステムは2012年に導入していま

す。また、サイバーセキュリティ対策に関しては、厚生労働省の「医療情報システムの安全管理に関するガイドライン」などにもとづき、できるだけスピーディに対応しています。

—— 電子カルテのシステムはどのように守られているのでしょうか。昨今、一般的なセキュリティ対策では検知しにくい「EMOTET（エモテット）」をはじめとしたマルウェア（悪意のあるプログラムの総称）の被害が増えています。それらのリスクにさらされる恐れはないのでしょうか。

電子カルテをはじめとした病院の中核にあるシステムは通常のインターネットと接続されていないため、インターネット経由の攻撃や悪質な不審メールにさらされるリスクは最小限に留めることができていると思えます。

—— いわゆる「インターネット

分離」（特定のデバイスやシステムをインターネットから切りはなすこと）がセキュリティの要になっているわけですね。ただインターネット分離も100%

安全というわけではなく、ときには保守用の入口からマルウェアに侵入されることもあると聞いています。

そういった点を考慮し、「特権アカウント」（操作権限を持つアカウント）をいかに死守するかといった対策を講じたり、ほかのセキュリティツールを導入するなどして、複合的なリスクマネジメントに努めたりしています。テレワークを実施する医師と誓約書を交わしているのも、そういった取り組みの一環です。その内容は「ウイルス対策ソフトをかならず入れて最新のバージョンにしておくこと」「画面のスクリーンショット（撮影）をしないこと」「怪しいメールを開かない」など基礎的な

ことなのですが、こうやって注喚起することがセキュリティ意識の醸成につながっていくと思っています。

—— そのほか、最近は公共の場でのセキュリティ対策をどうするかといったことも課題になっていますね。ホテルやカフェ、コワーキングスペースといった場所で作業を行う際に、公共ネットワークの脆弱性をつかれたり、端末の盗難・紛失のリスクが高くなったり、パソコンの画面そのものが人目にさらされることで、知らず知らずのうち情報漏洩したりしてしまう恐れがあるということですが、そのあたりについてはどうでしょうか。

に最善の注意を払っています。
テレワークの推進を背景に「HP S C E」を導入

—— この4月にエンドポイントセキュリティツール「HP Sure Click Enterprise (HP S C E)」を導入したのも、そういった対策のひとつということですね。その背景にはどういった事情があったのでしょうか。大きなキッカケになったのはコロナ禍でした。医師や職員の健康を維持しながら感染拡大をどう抑えるのかということ懸念に考えつづけた結果、病院内の事務作業をテレワーク化していくことになり、最先端のエンドポイントセキュリティツールであるHP S C Eを導入することにしました。今回はテレワーク用に統一した環境のPCを事務職員向けに用意していたため、HP S C Eについては管理上の観点からも当該PC（テ



左から、山本幸二病院情報システム部課長、病院情報システム部の永尾元裕氏、大貫亮病院情報システム部課長補佐、三保谷照和事務局次長(情報システム担当)

レワーク用)のみに導入しました。

——それにしても、最近のマルウェアは通常、やりとりしている業者を装ったメールに添付されていたりするので厄介ですね。実際、ランサムウェアに関しては、2021年に警察庁に報告された被害件数だけでも146件に達しているそうです。

——そういった時代背景もHP SCEを導入した理由のひとつです。HP SCEはマイクロVM(仮想パソコン)でメールやインターネットなど外部から受領するファイルの一切を開いて閲覧・操作し、あらかじめリスクがあるファイルをユーザーが意識することなくすべて安全に隔離できるという特徴を有しているのです。「怪しいメールを開いてしまった」といったミスでエンドポイントが侵害されることはなくなると確信しています。

——使用感のほうはどうでしょうか。

HP SCEの起動時にPCの動きがやや鈍くなってしまうといった声があるので、HP SCEの総代理店として販売・サポートを担っている(株)ブロード(東京都千代田区)に調整してもらっているところです。そのほかの点については順調に機

能しているのですが、今後はさらに多くの端末への導入も視野に入りたいと考えています。そのためにも、Macに対応されることを期待しています。

——昨今はテレワークだけでなく、オンライン診療も大きなテーマになっているかと思いますが、オンライン診療とセキュリティについてはどのような考えですか。

東京総合医療ネットワークが発足されるなど、政府も東京都も地域医療連携ネットワークの構築やオンライン診療を積極的に後押ししていますが、実際には各医療機関のセキュリティレベルをどう合わせるか、さらにはそれぞれの電子カルテシステムの互換性をどうするかなど、まだまだ多くの課題があります。医療機関単独ではなかなかこういった課題を解消することはできないので、ブロードをはじめとしたセキュリティ分野の皆さんの知見を借りながら改善に向けて歩んでいければと思います。

——ぜひ慶應義塾大学病院にはその先陣を切っていただきたいと思います。医療機関のセキュリティレベルがさらに向上し、オンライン診療が安全かつ当たり前に行われる日が来ることを願っています。

もう無駄な時間と費用は「0」にしましょう



HP Sure Click Enterprise

おかげさまで Bromium は HP Sure Click Enterprise に進化しました



エンドポイントのサイバー対策に関する費用や専門家は、もう必要ありません。100%* 防衛し、レポートします。是非ブロードにお問い合わせください。

※2013年以降、Bromiumは推計20億以上のMicroVMが実行されましたが、侵害報告件数はゼロです。(Bromium社調べ)

詳細は「BROAD Security Square」で… <https://bs-square.jp/columbus>

株式会社ブロード

〒100-0014 東京都千代田区永田町1-11-30 サウスビル永田町7F
TEL: 03-6205-7463 (代表)

