CUSTOMER SUCCESS STORY

NetApp

「防御」から「早期復旧」へ――大分県立病院が築く医療データ保護への戦略

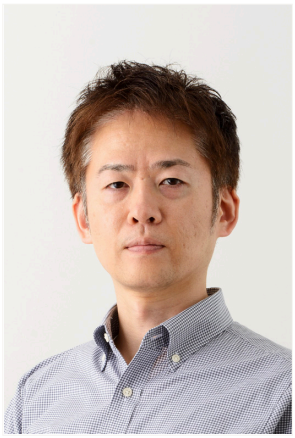
NetApp社の標準機能を活用し、省コストの「データ可用性」保護対策を実現

医療機関を狙ったランサムウェア攻撃が相次ぐ中、大分県立病院は「防御中心」から「復旧重視」へと発想を転換。NetAppのストレージに標準搭載されたバックアップ機能（スナップショットとイミュータブル機能など）を活用し、短時間でのデータ復旧を可能にする仕組みを構築しました。この仕組みにより、予算や人員に制約がある中でも、ランサムウェア感染時において、データ「可用性」を確保する運用が実現できました。

限られた予算と人員の中で効果的なランサムウェア対策を実施したい

大分県立病院は、大分県唯一の県立病院であり、約560床のベッド数と約1,300人の職員を有し、救急・周産期・精神といった政策医療から高度先進医療まで幅広く提供している医療機関です。しかし、同院含む日本の医療機関は、デジタル化が高度化する現代において、医療機関を狙ったランサムウェア攻撃の増加により、病院運営そのものが脅かされるリスクが顕在化しました。

「2018年から2020年にかけて、国内の公的な医療機関にて相次いでランサムウェア被害が発生しました。各病院の報告書を分析すると、『バックアップはあったが復旧に数カ月を要した』という共通点が浮かび上がりました。データをいつでも利用できるようにするという『可用性』に問題があったということがあらわになった事件であり、事業継続そのものが脅かされた象徴的な事例でした」（情報システム管理室 副主幹：田代雄一氏）



2023年当時
会計管理課施設管理班
（兼）情報システム管理室
副主幹　診療放射線技師
BEng,Meng　医療情報技師
田代 雄一 氏

一方で、医療業界特有の課題も対策を困難にしています。全国の多くの大病院では7～8年毎に数十億規模のシステム更新が行われます。しかし、電子カルテを中心に50～100以上のシステムが連携することも珍しくなく、さらに多数のベンダーが関与するため複雑さを増している状況です。中には専任のセキュリティ担当者がいないケースも少なくありません。

さらに、医療機関は構造的にIT投資が行いにくいという現状があると田代氏は指摘します。「診療報酬制度は病院が提供する医療サービスに対して、国が定める診療報酬を請求できるものですが、デメリットとして各病院はIT化によってどんな良いサービスを提供してももらえるお金は一定であり、結果として、法的に請求できるサービス以外に投資することが非常に難しい状況です。限られた予算と人員の中で、いかに効果的な対策を講じるかが課題でした」

「防御中心」から可用性を維持する「早期復旧」へ―発想の転換

従来のセキュリティ対策は、情報セキュリティの3要素であるCIA（機密性、完全性、可用性）のうち、機密性と完全性を重視したものが主流でした。田代氏も、医療系のコンサルタントに相談すると、この考えに準じたマルウェアの防御、感染の検知、データの流出防止といった対策を提示されることが大半だったと振り返ります。

「一方で、脅威は日々進化しており、セキュリティソリューションで対応できるのは全体の脅威のうち2割と提言する専門家もいます。そのため、限られた予算をこうしたセキュリティ製品に集中投資することは最適解ではないと判断しました。実際のランサムウェア被害事例でも、リモートアクセスが原因で正規ルートからのアクセスを悪用されていることが多く、管理者権限で操作されてしまえば、データの改ざん、削除、アクセス制御を防ぐのは非常に困難だと考えられます。」

「多くの事例では、データの可用性が失われたことで事業継続ができない状況に陥っています。そこで発想をかえて、今後はマルウェアに感染することは避けられないという前提のもと、データの『完全性』と『可用性』を維持する対策にフォーカスすることが効果的ではないかと考えました」（田代氏）

多重化されたデータ保護対策を、Netappストレージの標準機能で実現

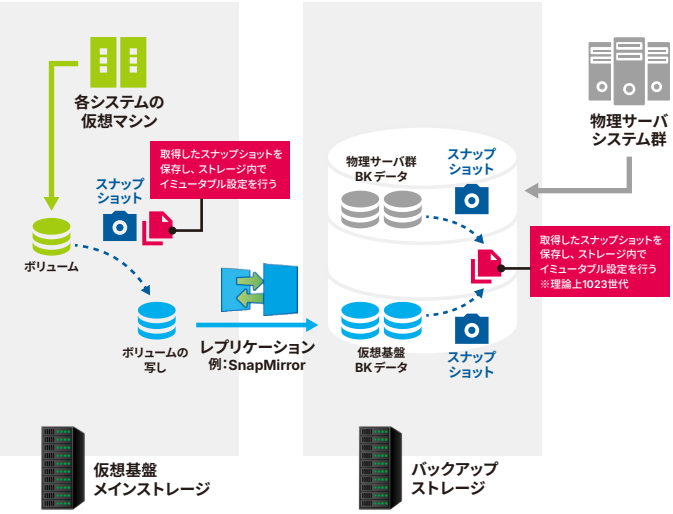
こうして大分県立病院が2022年から2023年にかけて構築した対策は、次の三本柱で構成されています。

1. 防御・拡大抑止：許容範囲のセキュリティソリューションによる一次的な防御
2. 感染を前提としたバックアップ：スナップショットとイミュータブル機能で改ざん不可能なデータ保護
3. 迅速なリストア・リカバリ：SnapMirror技術による高速同期で、短時間復旧を可能に

そして、このストレージ基盤に選ばれたのが、NetAppのAFF A250とFAS2720となります。特別な追加ソフトウェアやライセンスは不要でストレージの標準機能のみを使用して、エンタープライズグレードの保護を実現しました。技術プロセスは次のとおりです。

- イミュータブルなスナップショット：管理者権限でも改変不可能なバックアップが、ランサムウェアによるデータの暗号化を阻止
- 高速レプリケーション：SnapMirror技術により、プライマリストレージとバックアップストレージ間でデータを素早く同期し、迅速なリストアが可能
- 統合的な保護：、仮想化された業務システム群と仮想化が難しい物理サーバーのデータの双方を、バックアップストレージで保護

「イミュータブル設定を適用したスナップショットは、たとえ管理者であっても変更することができず、データの侵害を強固に防止します。ストレージの標準機能で構築しているため、業務システムを担当するベンダー側の作業に影響が少なく、簡単な作業だけで済むのもメリットの1つです」（田代氏）



大分県立病院が構築したデータ保護のシステム構成

最短2時間～2日で医療行為に必要なデータを復旧可能に

NetAppのストレージ導入したことで、大分県立病院は万が一データが侵害されたとしても部門システム群に関しては迅速に復旧できる体制を構築。地域の中核病院として、いかなるときも医療を継続する機能を強化しました。

「メインストレージが被害に遭いスナップショットから復旧する場合では約2時間程度、もしメインストレージのデータが完全に被害に遭いバックアップサーバーから復旧する場合でも、約2日という短時間での復旧が可能になるでしょう」と田代氏は見込んでいます。

この復旧時間の短縮は、単なる技術的成果ではありません。例えば業務停止が生じることは、患者の受け入れ停止を余儀なくされることであり、一刻を争う状況にある救急患者を受け入れることもできません。復旧時間の短縮は、患者の救命率を左右する重要な要因となります。

またコスト面での効果も見込まれます。「ストレージの標準機能を活用し、バックアップとイミュータブルという多重的な対策を実施することで、本来データ保護のために追加で導入するべきソリューションのコストが不要になりました」と田代氏は、NetApp製品の投資対効果の良さを評価します。

本構成の有用性に関して、田代氏が確信を持てたのは、構築後に発生した名古屋港ターミナルのランサムウェア被害の事案でした。「前提条件は色々ありますが、この事例では、3日間で復旧したとされています。これは業務システム群が仮想化されており、利用できるバックアップデータがあった、という条件が早期復旧要因の一つと考えられています。これこそが、当院の対策が実際に機能した事例に近しいものだと考えています」（田代氏）

もちろん、まだ課題も残されており、一部のハードウェアと一体化した基幹系システムのデータ対策を別途考える必要があると田代氏は語ります。

最後に田代氏は「基本的なセキュリティ対策を徹底した上で、NetAppの標準的なバックアップ技術を活用することで、地域医療を守る効果的な対策が可能であることを実証できました」と語ります。自治体医療機関ならではの多くの制約がある中、標準技術を組み合わせることでコストを抑えた効果的な高度な対策を実現した大分県立病院の取り組みは、他の医療機関や一般企業にも有用な、ランサムウェア時代における新しいベストプラクティスといえるでしょう。

NetApp製品について、詳しくはこちら

NetApp

ネットアップ合同会社
https://www.netapp.com/ja/forms/sales-contact/