

深刻化する医療機関へのサイバー攻撃に対抗するため SOCでファイアウォールの運用を強化

社会医療法人近森会 近森病院様は、病床数512、職員1600人、中四国有数の高度急性期病院です。

近年、医療機関でランサムウェア攻撃による被害が深刻化していることからセキュリティ対策の強化が必要とされる一方で、インターネットと院内ネットワークの境界であるファイアウォールの運用が限られた情報システム担当者では行き届かないことに課題を感じ、統合セキュリティ運用（SOC）サービスである「NetStare」を契約。

ファイアウォールの設定変更やバージョンアップなどがスピーディになったことに加えこれまで活用できていなかったIPSなどのセキュリティ機能が有効活用できるようになってセキュリティがより強固に。アラート対応においてもセキュリティ運用のプロの視点加わり、自院に適したポリシー設計や運用が実現しました。



命を救う。
命をつなぐ。



CHIKAMORI
HEALTHCARE GROUP
近森病院

法人名 社会医療法人近森会 近森病院
所在地 高知県高知市大川筋一丁目1-16

近森病院は昭和21年の開院当初から救急医療を中心とした診療を行い、地域医療連携に力を入れ、また民間病院でありながら全国的にも先駆けてチーム医療を推進するなど、モデルケースとして国内の他の医療機関からの評価も高い中四国有数の医療機関です。

導入前の課題

- ✓ 医療機関においてランサムウェア被害が増加しており対策の必要性を感じていた
- ✓ 特にランサムウェアの侵入経路として多いVPNのセキュリティを強化する必要があった
- ✓ ファイアウォールの運用に十分なリソースを割けずスポットで外部業者に依頼しているため非効率だった

NetStareサービスに対する期待・要件

- ✓ スポットでのメンテナンスではなくSOC（Security Operation Center）で包括的にサポートしてもらえること
- ✓ ファイアウォールの設定変更などを診療時間外に実施してもらえること
- ✓ サポートが手厚く対応が早いこと

選定理由

- ✓ 24時間365日の有人対応でサポートしてもらえる
- ✓ 診療時間外に作業をお願いでき病院の業務に影響が出ない
- ✓ 設定変更やバージョンアップなどの運用業務が標準サービスに含まれている

お客様の声

「NetStareサービス契約前は、必要に応じてファイアウォール機器を購入したベンダーに設定変更などの作業を依頼していました。スポットでお願いするので都度院内稟議が必要だったり、日中の診療を止めるわけにはいかないので作業時間調整の事務手続きに時間をとられていたり、そのような状況なので定期的なOSのバージョンアップもままならずセキュリティ面で不安を抱えていました。

NetStareサービスはSOCによるアラート監視に加えファイアウォールの設定変更やバージョンアップも標準サービスに含まれ、24時間365日いつでも相談できるので、これまでの社内調整の煩雑さやセキュリティ面での不安が一気に解消されました。依頼に対する対応が早いのも評価ポイントです。まさにこのような包括的なSOCサービスを求めていたのでとても重宝しています」（近森病院 長山様）



社会医療法人 近森会 近森病院
診療支援部 電子カルテ管理課 課長
長山 信夫 様

NetStareサービスの効果・活用例

眠っていたIPS機能を活用できるようになった

「契約開始時にさっそくバージョンアップや設定のチューニングを実施してもらい、今までは使いこなせず無効化されていたIPSなどのセキュリティ機能が活用できるようになりました。

セキュリティエンジニアと一緒にファイアウォールのログを見ながら「この経路の通信はある、いない」と吟味しつつポリシーを決めて行ったので、自院に沿った有効な設定ができたと感じています」（近森病院 長山様）

ファイアウォールの有効性が見えるようになった

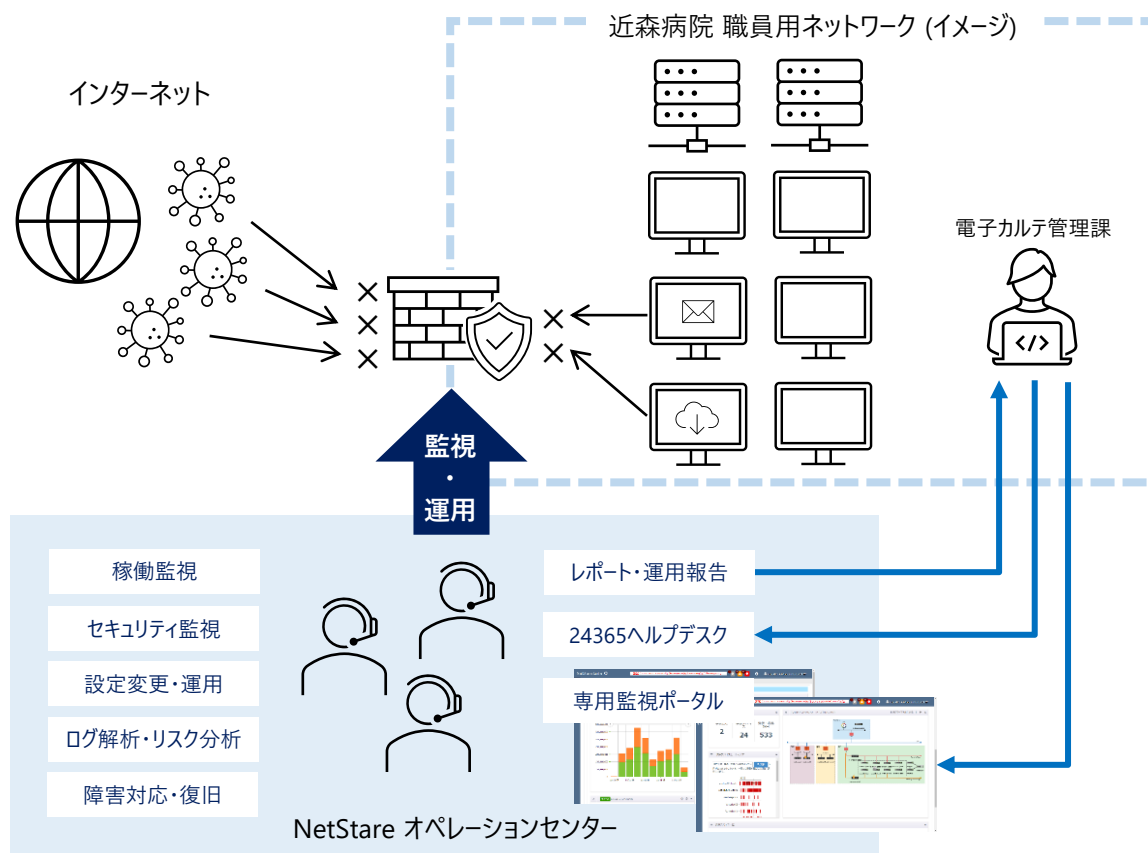
「いつからいつまでのログが見たい、というリクエストにすぐに対応してもらえるので、ファイアウォールがどんな通信をブロックしているのか、ブロックしたことで防げた攻撃はどのようなものか？ が把握できるようになりました。

ファイアウォールのブラックリストをメンテナンスする上でも役立っています」（同）

アラートに対する対応方針を相談できる・提案してもらえる

「ファイアウォールのアラートに対する方針を相談でき、プロの見解からアドバイスがもらえるので病院内で報告する際に役立っています。

ネットワークダウンなどのトラブルが人命に関わることもあるので、SOCに相談して不明点を1つずつぶせるのは有り難いです」（同）



NetStareサービスの提供イメージ。近森病院では職員用ネットワークのゲートウェイに設置されているファイアウォールの監視および運用を24時間365日有人体制で実施している。また、オペレーションセンターが使用する監視ポータルはユーザーもいつでも自由に閲覧できる。