独立行政法人国立病院機構 http://www.hosp.go.jp/

ヘルスケア現場における情報セキュリティ強化の取り組みを支援

サイバー攻撃の対象はヘルスケア業界にも広がっています。このたび日立は、全国に143病院を運営し、診療、臨床研究ならびに医療人財育成を事業の柱とする独立行政法人国立病院機構（以下、NHO※1）に、セキュリティコンサルティングサービスを提供し、現行セキュリティポリシーの改定ならびにその付随文書としてのガイドライン整備を支援。またセキュリティインシデントが発生した場合の対応体制であるCSIRT（シーサート）※2についても、既存の体制からより実効性のある体制への強化を支援しました。

※1 National Hospital Organization　※2 Computer Security Incident Response Team

迅速・的確な対応で被害を最小化するCSIRT

近年、サイバー攻撃は高度化を極め、それに伴う被害が拡大しています。サイバーセキュリティ対策としては、複数の対策を組み合わせた多重防御や、監視・検知機能の強化をする一方で、実際にセキュリティインシデント（事故）が起こることを前提に、その監視や原因解析、影響範囲の把握や修復などを専門的に行うCSIRTを構築し、迅速・的確な対応によって被害を最小化する動きが進んでいます。

しかし、企業や組織が独自にCSIRTを構築しようとしても、人員やスキルの不足、担当者の育成など数々の問題が立ちはだかります。こうした課題を解決するため、日立はセキュリティの専門知識を持つスタッフが、お客さまの情報セキュリティ対策を包括的に支援する「日立サイバーセキュリティソリューション」を提供し、そのメニューの一つとして「セキュリティコンサルティングサービス」をラインアップしています。

日立は1998年、他社に先駆けて日立グループのCSIRTとなるHitachi Incident Response Team（HIRT）プロジェクトを発足させ、グループ全体でのセキュリティインシデントの発生予防、万一インシデントが発生してしまった場合の迅速な対処法構築などで、多くの実績を積み重ねてきました。その知見とノウハウを活用して提供するセキュリティコンサルティングサービスは、個々のお客さまの状況に合わせた情報セキュリティポリシーの策定支援からCSIRT構築運用支援、情報セキュリティシステム設計など多彩なメニュー（図）をそろえ、これまで金融機関や政府機関、通信系企業など多くの採用実績があります。

高度化するサイバー攻撃に対するNHOの対応

このサービスを利用して、国の医療機関の中でいち早く情報セキュリティの抜本的な強化策に着手したのがNHOです。NHOは全国に143の病院を持ち、NHO本部と各病院をHOSPnetと呼ばれる大規模な専用ネットワークで結んでいます。

NHOでは以前から、機微な医療情報や個人情報を守り、医療機器などのシステム障害を防ぐため、さまざまな情報セキュリティ対策を行ってきました。しかし、ネットワーク経由でのサイバー攻撃の脅威がますます多様化、先鋭化してきたことを踏まえ、さらなる対策強化を検討していました。CSIRTについても、政府の要請を受けて体制を整備したところでした。日立は、このような背景をもつNHOの情報セキュリティのさらなる強化について、2016年1月から支援を行いました。

医療現場に対応したセキュリティポリシーとガイドライン

NHO本部からの依頼により日立が取り組んだ施策は、(1)現状の情報セキュリティ体制における問題点の洗い出しと改善案の提示、(2)情報セキュリティポリシー改定案の作成、(3)セキュリティガイドライン案の作成、(4)CSIRT体制強化支援に分けられます。

日立は、NHOにおける既存の情報セキュリティ規程や各種関連文書を確認するとともに、現在の情報セキュリティ体制の状況などを日立独自のテンプレートを活用しながら関係各部署に効率的にヒアリングを行い、問題点の洗い出しと改善策をふまえた情報セキュリティポリシー改定案の作成作業に取り組みました。

この作業では、「政府機関の情報セキュリティ対策のための統一基準」をベースにしつつ、国内外のセキュリティ標準を広く勘案し、何よりも重要な情報資産の機密性・完全性・可用性の確保を念頭に置いた新たなセキュリティポリシー案と、その具体的な実施方法となる各種ガイドライン案を同時に作成しました。

NHOの143病院は、それぞれ自律的な運営を行っています。このため各病院の経営理念や医療内容、体制も考慮して、診療現場の業務に大きな負担をかけずに最大の効果を生み出すガイドラインの作成が求められました。また、

独立行政法人
国立病院機構
National Hospital Organization

独立行政法人国立病院機構

所在地　東京都目黒区東が丘2-5-21
病院数　143病院
病床数　54,591床（2015年4月1日現在）
職員数　約59,000人（2015年1月1日現在/常勤職員数）
事業内容　全19分野の政策医療の実施、医療業務、医療に関する調査・研究、ならびに医療技術者の育成など

病院は医師や看護師、コメディカルスタッフ、事務職員といった多くの職種の人々が働き、患者さんや見舞い客、医療関連事業者が頻繁に出入りする環境でもあります。日立はNHOとともに、そこで扱われる機微な情報を、医療の緊急性や利便性を損なわずにいかに守っていくかの検討を重ねた結果、さまざまなテーマの15種あまりのガイドライン※3の整備を支援しました。

※3（一部抜粋）
・情報システムセキュリティガイドライン（病院情報システム運用管理編）
・情報システムセキュリティガイドライン（システムセキュリティ要件編）
・情報システムセキュリティガイドライン（システム利用編）
・情報システムセキュリティガイドライン（システム監視編）
・リスク評価手順書

CSIRTの再構築・強化と運用をトータルに支援

そしてCSIRTの体制強化支援では、NHO本部、病院等関連施設、およびHOSPnetの保守事業者などとの連携も含めたCSIRT体制の枠組みを検討しました。日立は、自身のHIRTを運用してきた知見とノウハウを生かしながら、NHOのCSIRTに必要な機能とその実現方法を検討した後、インシデントレスポンス、コーディネーションなどのフローについてシミュレーションを実施し、その実現性・有効性を確認しました。

また、この間の検討事項をわかりやすい運用手順書にまとめる一方、机上シミュレーションを行いました。

日立は、NHOが今回整備した新たなセキュリティポリシーおよびガイドラインを組織内に周知・教育・定着化させていくこと、またCSIRTを実際に運用していくにあたり、それを継続支援するためのさまざまな提案をしていきます。

今後、本プロジェクトで培ったノウハウを生かし、誰もが安全・安心に暮らせる社会の実現に向け、ヘルスケア分野におけるセキュリティソリューションの強化・拡充をめざしていきます。

■日立が提供するソリューションの特長

- セキュリティのプロフェッショナルによる24時間、365日の高度な監視・分析ノウハウを提供
- コンサルティングからセキュリティ対策製品、運用/監視サービスまで幅広いソリューションで、日々進化するサイバー攻撃に対して、迅速かつ継続的なセキュリティ改善プロセスの実現を支援
- 日立グループ30万人のITインフラを支えている実績から、サイバー攻撃対策のノウハウを提供

■ソリューションメニュー

分類	No	ソリューションメニュー	対策	取り扱い製品/サービス例
コンサルティング	1	セキュリティアセスメント	●セキュリティリスク分析支援	●セキュリティリスク分析コンサルティングサービス
	2	脆弱性診断	●脆弱性診断	●Webアプリケーション診断/インフラ診断
	3	CSIRT構築支援	●CSIRT計画策定/構築支援	●CSIRT構築支援コンサルティングサービス
サイバー攻撃対策/保護	4	マルウェア/不正通信検知	●振舞い検知（未知マルウェア対策） ●次世代FW*1（未知マルウェア対策）	●FireEye ●Palo Alto
	5	Webサイトプロテクション	●WebアプリケーションFW、負荷分散（DDoS対策） ●Webサイト改ざん検知	●Akamai Kona Site Defender / A10 Networks Thunder/AX ●Tripwire / WebALARM
	6	Webアクセスセキュリティ	●URLフィルタリング、アンチウイルス	●SaaS型セキュリティサービス（Web）
	7	メールセキュリティ	●アンチスパム/アンチウイルス ●コンテンツフィルタリング	●SaaS型セキュリティサービス（メール） ●標的型メール訓練サービス
	8	サーバセキュリティ エンドポイントセキュリティ	●暗号化/持出し制御/文書管理 ●マルウェア対策（ホワイトリスト型/非シグネチャ型） ●ホストベースIPS（仮想パッチ）	●秘文 / 活文 ●McAfee Application Control / FFR yarai ●Trend Micro Deep Security
	9	認証/アクセス制御	●統合ID管理/特権ID管理 ●シングルサインオン、認証強化	●LDAP Manager / パワーセキュリティ / ESS AdminControl ●SRGate / CA Single Sign-On / HP Icewall
マネージド・セキュリティ・サービス				
セキュリティイベント監視	10	セキュリティイベント監視サービス	●ログ相関分析による攻撃兆候検知	●統合セキュリティログ監視サービス
	11	SOC*2構築	●SOC構築（オンプレミス）	●Splunk / McAfeeSIEM / HP ArcSight　ESM
インシデント対応支援	12	インシデント対応支援サービス	●インシデントの高度解析 ●専門家によるインシデントレスポンス対応支援	●CSIRT運用支援サービス ●SHIELD 110番
	13	マルウェア解析	●仮想環境でのマルウェア解析	●マッシュアップ型マルウェア解析支援システム

*1 Fire Wall　*2 Security Operation Center

図 日立サイバーセキュリティソリューションメニュー

お問い合わせ先

（株）日立製作所 スマート情報システム統括本部
https://www8.hitachi.co.jp/inquiry/it/p-channel/iryo/form.jsp

■ 情報提供サイト
http://www.hitachi.co.jp/Prod/comp/Secureplaza/sec_prod/cyber_security/