2017 年 5 月 19 日
独立行政法人情報処理推進機構（IPA）

欧州ネットワーク情報セキュリティ機関（ENISA）「スマートホスピタルのサイバーセキュリティとレジリエンス」概要

本概要は、欧州ネットワーク情報セキュリティ機関（ENISA）発行の以下文書の概訳となります。
内容の詳細につきましては、原文をご確認ください。

Smart Hospitals – Security and Resilience for Smart Health Service and Infrastructures
https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals

本概要では、スマートホスピタルのサイバーセキュリティとレジリエンス改善のための上記ガイドについて、以下の項目の概略を日本語でまとめている。

- 対象読者（target audience）
- 規制政策（regulatory policy）
- 資産（assets）
- 脅威／リスク（threats and risk analysis）
- 攻撃シナリオ（attack scenarios）
- 対策（good practices）
- 提言（recommendations）

「スマートホスピタルのサイバーセキュリティとレジリエンス」は、患者の安全を守るため、電子カルテシステム、医用画像管理システム（PACS）、スマート輸液ポンプなど、病院システムにつながる“スマートデバイス”におけるサイバー攻撃による障害の発生を防ぎ、病院システムのサイバーセキュリティおよびレジリエンスを向上させることを目的としている。

本ガイドでは、欧州におけるスマートホスピタルの現状およびセキュリティ上の課題の調査結果として、スマートホスピタルを構成するシステムやスマートデバイス等の資産、想定される脅威、対策のグッドプラクティス、およびセキュリティ強化のための提言をまとめている。

「スマートホスピタルのサイバーセキュリティとレジリエンス」概要（1/4）

掲載項目	概要
対象読者	• 経営陣、特にセキュリティ担当役員（最高医療情報責任者（CMIO）や最高情報セキュリティ責任者（CISO）等） • 業界関係者（スマート医療機器メーカー、技術ベンダ、コンサルティング会社等） • EU 加盟国の政策立案者
規制政策	• 現行、スマートホスピタルに特化した政策や規制はない • 以下のような参考文献は存在する – 技術ベンダやコンサルティング会社によるホワイトペーパー – 「IEC80001-1：医療機器を組込む IT ネットワークのためのリスクマネジメントの適用」等の医療機器に関する国際標準 – 「医療機器に関する EU 指令（MDD）」、「対外診断機器（IVD）に関するEU 指令」、「能動型埋め込み式機器（AIMD）に関する EU 指令」等の EU 指令
想定資産	• ネットワークにつながる医療機器 ・・・ 67% • 相互接続された医療情報システム ・・・ 67% 例）病院情報システム（HIS）、臨床検査情報システム（LIS）、医用画像管理システム（PACS）等 • ネットワーク機器 ・・・ 43% • 遠隔医療システム ・・・ 40% • ID システム ・・・ 30% 例）ID タグ／ブレスレット、スマートバッジ等 • モバイル端末 ・・・ 30% 例）ノート PC、タブレット、スマートフォン、モバイルアプリケーション等 • データ ・・・ 30% 例）患者の医療情報、病院の財務データ、研究データ等 • 建物・設備 ・・・ 10% 例）電源、空調、医療ガス、入退管理等 ※数字（%）は、インタビュー／アンケートで当該資産が重要と回答された割合

「スマートホスピタルのサイバーセキュリティとレジリエンス」概要（2/4）

掲載項目	概要
脅威／リスク	• 自然災害：火事、洪水、地震等 • サプライチェーン障害：クラウドサービス、ネットワークサービス、電力供給等 • ヒューマンエラー：設定ミス、誤った利用、対策の迂回等 • システム障害：ソフトウェアや機器の不具合、過負荷等 • 悪意による攻撃行為（過失による攻撃行為とは区別すること） – マルウェア感染：ウイルス、ランサムウェア等 – ハイジャック（乗っ取り） – ソーシャルエンジニアリング – 機器やデータの窃取 – 医療機器の改ざん – サービス妨害（DoS）
攻撃シナリオ	• 病院スタッフへのソーシャルエンジニアリング攻撃 【危険度：高、 発生／被害に遭う可能性：高】 病院スタッフがメールの添付ファイルを開いて PC がマルウェアに感染し、マルウェアによって認証情報やデータが窃取される • 医療機器への侵入や、病院ネットワークへの侵入 【危険度：高、 発生／被害に遭う：高】 攻撃者が脆弱な医療機器を見つけて侵入し、医療機器に障害を発生させたり、医療機器を介して他の機器やシステムに侵入を拡大し、データが窃取される • 病院の器具／備品の盗難 【危険度：中、 発生／被害に遭う：中】 医療機器や、ノート PC、ハードドライブなどの盗難により、機微な医療情報が窃取される • 病院の医療情報システム（HIS）へのランサムウェア攻撃 【危険度：高、 発生／被害に遭う：中】 攻撃者の仕掛けた水飲み場型攻撃によって病院スタッフの PC がランサムウェアに感染し、データ等が暗号化され、PC 上に身代金要求の画面が表示される • 病院サーバへの分散型サービス妨害（DDoS）攻撃 【危険度：高、 発生／被害に遭う：低】 攻撃者が病院サーバの IP アドレスを調査し、ボットネットに当該 IP アドレスへの DDoS 攻撃を指示し、病院ネットワーク（サービス）がダウンする ※原文では、上記にまとめた「概要」「危険性」「発生／被害に遭う可能性」のほか、各攻撃シナリオについて「影響を受ける資産」「二次被害」「復旧時間・作業」「対策」「課題」を記載している

「スマートホスピタルのサイバーセキュリティとレジリエンス」概要（3/4）

掲載項目		概要
対策	組織的対策	GP1：セキュリティ上の役割と責任の明確化 GP2：セキュリティポリシーと手順の策定 GP3：セキュリティト教育／意識向上プログラムの実施 GP4：リスク、資産、脅威の特定 GP5：緊急時対応計画の策定 GP6：セキュリティ基準・標準の適用 GP7：監査の実施 GP8：セキュリティ評価の実施 GP9：製造ベンダとの契約条項（内容）の確認と合意
	技術的対策	GP10：監視および侵入検知の仕組みの導入 GP11：動的なネットワークセグメンテーションの実施とファイアウォールの利用 GP12：マルウェア対策ソフトの導入 GP13：定期的なバックアップの取得 GP14：システム構成管理の見直し（自動化の検討） GP15：パッチ適用 GP16：アクセス制御の徹底 GP17：データ暗号化 GP18：データの格付け GP19：遠隔医療システム・モバイル医療システムの防護

「スマートホスピタルのサイバーセキュリティとレジリエンス」概要（4/4）

掲載項目		概要
提言	検討課題	GAP1： 病院ネットワークに接続される機器の管理（制限）の欠如 GAP2： IT 資産管理ツール導入の必要性 GAP3： アプリケーションホワイトリスティングの欠如 GAP4： システム・機器のセキュリティ確保（調達時のセキュリティ要件の明確化） GAP5： 機器（システム）認証導入の必要性 GAP6： セキュリティ教育・訓練の不足 GAP7： サーバ、ワークステーション、ネットワーク機器等のリモート管理方法 GAP8： IT 技術の進化の速さ vs.標準化・認可の遅さ） GAP9： 費用対効果の明確化
	推奨策	＜病院＞ • サイバーセキュリティポリシーの策定と施行 • 最新のセキュリティ対策の導入 例） スマートファイアウォール、侵入検知等 • 調達仕様に記載するセキュリティ要件の策定 • 医療業界向けセキュリティソリューションのニーズの提示 市場規模が拡大すれば、スケールメリットが生まれ、コストも下がることが見込まれる • 病院間におけるサイバーセキュリティ関連情報の共有の仕組みの確立 • リスク評価・脆弱性評価の実施 • ペネトレーションテスト・監査の実施 • 医療業界全体におけるサイバーセキュリティ関連情報の共有の仕組みの確立 ＜業界＞ • 現行の品質保証の仕組みへのセキュリティの統合 • セキュリティテストへの第三者の参画 • 「医療機器に関する EU 指令（MDD）」の情報通信インフラへの適用 本来範囲外ではあるが、スマート化によって重要度が増していることから、情報通信インフラの中でも重要なコンポーネントについて、MDD の適用を検討する • セキュリティ基準・標準の適用

以上