2025年８月22日

各　位

医療機関へのアクセスログ管理システムの販売開始について

～サイバー攻撃に備える取り組み強化～

当社は、医療分野のサイバーセキュリティ対策を強化するため、アクセスログ管理システムを開発し、販売を開始いたします。

記

１．システム開発背景

昨今、医療機関を標的としたサイバー攻撃が急増し、診療の中断や患者データ漏洩など深刻な被害が報告されています。こうした状況や厚生労働省によるサイバーセキュリティ対策への注意喚起*（出典：厚生労働省「医療分野のサイバーセキュリティ対策について」）を踏まえ、当社は医療機関におけるアクセスログ確認の必要性から、本システムを開発いたしました。

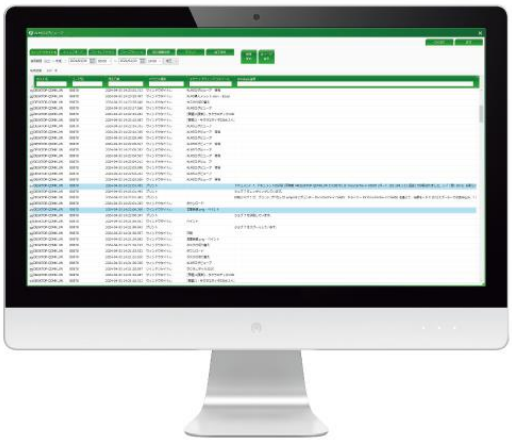
＊医療分野のサイバーセキュリティ対策について
https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/cyber-security.html

２．アクセスログ管理システムとは

本システムは、医療情報を扱うシステムに導入することでサイバーセキュリティ対策の一環となります。主な目的は、「PC ログ監視による注意喚起と不正行為の抑止」そして「インシデント発生時の迅速な原因究明とシステム復旧支援」です。

定期的なアクセスログの監視・分析により、不審な操作を早期に把握し、注意喚起や被害の拡大防止につなげることができます。また、万が一インシデントが発生した場合には、収集されたログをもとに操作履歴を追跡し、原因の特定や復旧対応を効率的に行うことが可能です。

セキュリティ管理者はログをビューアで確認でき、必要に応じて CSV 形式で出力することにより、調査・報告にも活用いただけます。



- PC ログ監視による注意喚起と不正行為の抑止
- インシデント発生時の迅速な原因究明とシステム復旧支援
- セキュリティ管理者はログをビューアで確認ができ、必要に応じて CSV 形式で出力

３．管理対象ログ(使用例)

①リモート接続の検出　～リモート接続の接続情報を確認～
管理外端末から接続されている場合、速やかに悪意のない接続であることを確認します。

②USB メモリ使用の検出　～USB メモリを使用した日時および UID が確認可能～
管理外 USB メモリが接続されていた場合、注意喚起を行いマルウェアの侵入を防ぎます。

③プリンタ使用の検出
プリントを使用したときのファイルや出力先プリンタ名が確認できます。
アクセス権外のファイルをプリントしている場合、印刷物の目的を確認し、情報漏洩を防ぎます。

④誤操作の検出
エクスプローラ操作等で、誤ってファイルを削除してしまった場合、削除してしまったファイル名および日時を確認できます。

⑤Windows ログイン失敗の検出
Windows ログイン失敗時、ログイン日時と接続元 IP が確認できます。
ログ検出後、速やかに状況を確認することで、悪意のある侵入を防ぎます。

４．今後の見通し

本システムは、医療機関におけるセキュリティ強化や効率的な運用改善に資することを目指し、今後積極的に販売を展開してまいります。本システムは、医療分野に限らず、サイバー攻撃への備えを強化したい中小企業においても有効に活用できることから、今後は幅広い業種へのアプローチを進めてまいります。

医療セキュリティ市場は今後も大きな成長が見込まれており*、当社は成長分野におけるシェア拡大を図るとともに、顧客ニーズに応じた製品・サービスの拡充を継続し、医療 DX および中小企業の安全なデジタル活用に貢献してまいります。

なお、本件が当社の単体業績に与える影響は軽微です。

＊Mordor Intelligence のレポートでは、世界の医療機器セキュリティ市場規模は 2024 年に 78.3 億ドルに達し、2029 年には年平均成長率（CAGR）8.20%で 116.1 億ドルに達すると予測されています。

【会社概要】

所在地：東京都品川区大崎 1-6-3
代表者：川倉　歩
事業内容：ヘルスケアソリューション事業、地球環境ソリューション事業
公式サイト：https://www.imageone.co.jp/

【本件に関するお問い合わせ先】

株式会社イメージワン
https://www.imageone.co.jp/inquiry/

以　上