医療分野における「データダイオード」の適用に関する提言

2017 年 1 月 23 日

社団法人 メディカル IT セキュリティフォーラム
データダイオード分科会

医療分野における「データダイオード」の適用に関する提言

昨近の個人情報漏洩事故発生の状況を受け、外部侵入を防止することが各所で議論されている。医療情報システムにおいてもセキュリティ強化が必要であり、個人情報を扱うシステムとその他のシステムを分離するしくみが検討されている。このしくみとして、社団法人 メディカル IT セキュリティフォーラム(以降、MITSF と記す)では、データダイオードに注目し医療分野での活用の可能性を考えているが、我が国においては社会的認知度が低いものであるため、データダイオードの社会的認知を図り、医療だけでなく、有効活用することを目指す活動の提案が必要と考え、データダイオード分科会を設置し、データダイオードの定義、機能要件の明確化を行った。

また、医療分野での適用を促進するため、厚生労働省が作成・発行している「医療情報システムの安全管理に関するガイドライン」に、定義と適用方の記述を追加することを検討した。この結果、以下の記述を追加することを提言する。

1.「医療情報システムの安全管理に関するガイドライン」への要求事項の反映について

下記1. 1、1. 2のように、追記箇所案に追記文案を追記することを提言する。

1. 1 追記箇所案

「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」において、P77 の B-4 記事の次に B-5 として以下の文章を追記する。

1. 2 追記文章案

B-5.医療情報データを外部へ公開・保存する場合の手法とセキュリティ確保について

外部からの侵入拒否をソフトウェアの構造で実現している装置としてはファイアウォールが有るが、物理原理に基づきハードウエアで情報伝達を一方向に制限することで侵入拒否を実現している一方向情報伝達のネットワーク装置があり、近年、北米などの世界の重要インフラなどで普及が進んでいる。この一方向情報伝達を実現しているネットワーク装置を欧米ではデータダイオードと呼んでいる。

データダイオードは、物理原理に基づきハードウエアで情報伝達を一方向に制限した装置であり、 古くから存在する電気的なもの、また、欧米を中心に普及が進んでいる光の一方向性を用いたものがある。近年、重要なインフラなどで普及が進んでいる。

データダイオードに代表される一方向情報伝達を実現する装置は、外部ネットワークからの攻撃が物理的に不可能であり、システムの脆弱性、リモートアクセスアカウントなどを悪用した攻撃ができず、パッチが適用されていないシステムへのリスクをネットワークから切り離したシステムと同等まで大きく削減できる。

重要インフラに限らず、個人情報など重要データを守るために、海外で活用が進んでおり、国内においても活用が期待される装置である。

(1) 患者へデータを公開する場合

公開するためのデータを置くサーバを準備し、このサーバへ外部からのアクセスを許すが、このサーバへデータを送る手法として通信を使用し送信データをシステム化することで、汎用の可搬型媒体によるデータを送る手法に対して、漏洩リスクを減らすことができる。

この通信においては、データダイオードに代表される一方向情報伝達を実現する装置を中継することにより、外部からの公開サーバ経由での個人情報を含む医療情報システムへの侵入を拒否し、標的型攻撃を含む外部からの攻撃から個人データを守ることができる。

このため、データダイオードに代表される一方向情報伝達を実現する装置を中継する情報伝達のしくみに限定することが望ましい。

⑵ 地域連携でデータを公開する場合

地域連携においてデータを公開する場合も公開するためのデータを置くサーバを準備し、外部からはこの公開サーバへのアクセスだけを許すことが望ましい。

地域連携において公開すべきデータを公開サーバへ送る手法として、上記⑴の患者へのデータを公開する場合と同様に、個人情報を含む地域連携において公開するデータを保持している医療情報システムと公開サーバを通信により接続する場合は、データダイオードに代表される一方向情報伝達を実現する装置を中継することが望ましい。

⑶ 外部システムでデータを保存する場合

システムとして個人情報など重要なデータを扱うサーバを外部ネットワークへ繋ぎ通信により外部システムへデータを送り保存する方法が、いつ、誰が、何をしたのか記録する観点で、システムとして自動化できる点において優れている。しかし、繋ぐことにより外部からの侵入リスクが発生する。

この侵入リスクを軽減するため、接続点には、ファイアウォールなどの侵入を防止する装置の設置が必須となるが、侵入を拒否する視点では、データダイオードに代表される一方向情報伝達を実現する装置で中継させることが望ましい。

2. 参考資料

データダイオードに関する理解を助けるため以下参考資料として示す。

(1)　一方向ネットワークとデータダイオード

一方向ネットワーク(unidirectional networks)とは、セキュアでないネットワークからデータを収集し、セキュアなネットワークへのデータ伝送を可能としつつ、セキュアなネットワークからのデータ転送を不可能にするなど、データ伝送を一方向だけに制限する技術の総称である。

一方向ネットワークによってセキュリティを向上させるアイデアは 1960 年代から存在していたが実現したのは 1990 年代にオーストラリアの軍事科学技術院(DSTO)が開発した Data Diode が最初とされている。米国では一時期ネットワーク・ポンプ(Network Pump)と呼ばれていた。

例えば FTP を完全に片方向にしか電気信号として許可しない

図1. システム構成イメージ

応用事例としては、電子投票システムやダムの制御システムがある。国内応用事例としては交通管制システム、航空管制システム、大規模プラント制御システム、発電システムなどがあるが、いずれも秘匿事例として扱われている。オープン系ネットワークと高度なセキュリティが要求されるネットワーク間の時刻同期を行なう場合に使用される等用途は広い。銀行の勘定系システムとオンライン・バンキングシステムとの間に設置されている装置は、プロトコル変換機であり，データダイオードとは異なる。

国内でも事実上の適用義務化とされることも予想される。適用対象は、政府、自治体、金融、医療、重要インフラ(電力、ガス、石油，化学プラント、交通、航空、水道、治水ダム、・・・)など広範囲に及ぶ。データ漏えいの心配がなく基幹業務(もしくは制御系)システムと情報系システム間の情報共有を可能とすることができ，ネットワークの切断より安全性が高い。

図2. 装置例

(2)データダイオードと物理切断やファイアウォール切断

ファイアウォールと比較して運用負荷・コスト削減が期待できる

－外部から内部への通信ログが発生しないためモニタリングの運用負荷・コストが 軽減

－複雑なファイアウォールの設定がないため定期的な脆弱性診断コストが軽減

－セキュリティドキュメント量を大幅に削減

－監査対象の少量化に伴う、外部監査の対応コスト削減

－システム担当者のトレーニング時間の削減

確実なセキュリティ

－完全な外部ネットワークとの隔離

・データも、コマンドも、プロトコルも、パケットも、外部から内部ネットワークに 流入不可

・マルウェアの C&C 通信も攻撃司令パケット(外部からの Ack パケット)が流入不可、 活動抑制

物理的な切断にともなうリスクがない

・情報共有のために USB などの可搬記録媒体の使用が想定されるが、媒体の盗難、紛失、ウイルス感染など、切断によるリスクが増加

－設定ミスによる脆弱性誘発がない

・ 片方向ゲートウェイの設定にミスが発生した場合にも外部から侵入できる脆弱性は発生しない

(3) 米国国土安全保障省が推奨するデータ・ダイオード

3. REDUCE YOUR ATTACK SURFACE AREA

Isolate ICS networks from any untrusted networks, especially the Internet. Lock down all unused ports. Turn off all unused services. Only allow real-time connectivity to external networks if there is a defined business requirement or control function. If one-way communication can accomplish a task, use optical separation ("data diode"). If bidirectional communication is necessary, then use a single open port over a restricted network path.

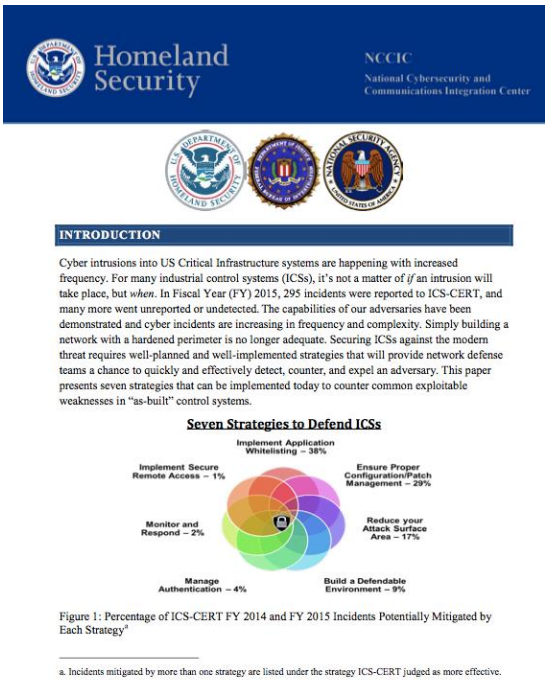

図3. ホームページ画面

出展：

https://www.dhs.gov/blog/2016/03/07/dhs-works-critical-infrastructure-owners-and-operators-raise-awareness-cyber-threats

記事中の"Seven Steps to Effectively Defend Industrial Control Systems."


MEDICAL
IT SECURITY
FORUM