病院情報システムへの不正アクセスを防止するセキュリティーソリューションの実用性評価

Practical Evaluation of Cybersecurity Solution to Prevent Unauthorized Access to Hospital Information Systems

利光　清 TOSHIMITSU Kiyoshi　加藤　雅一 KATO Masakazu　畠中　一成 HATANAKA Issei　谷　祐児 TANI Yuji

近年，医療機関に対する不正アクセスなどのサイバー攻撃は増加の一途をたどっており，診療への影響が出ている事例も少なくない。これを防止する情報セキュリティー対策が求められるが，病院情報システムでは，構成する医療機器の最新OS（基本ソフトウェア）への更新が難しく，継続的なセキュリティー対策が課題となっている。また，病院情報システムに今後必須となる２要素認証への対応も必要である。

そこで東芝は，当社のIoT（Internet of Things）セキュリティーソリューションであるCYTHEMIS（サイテミス）[(1)]を病院情報システムに適用して，旭川医科大学と共同で実用性評価を行い，システム内の医療機器に手を加えることなく不正アクセスを防止できることを確認した。また，当社の生体認証カードであるBISCADE（ビスケード）カード[(1)]を適用した２要素認証システムを構築して，同大学の大学病院で稼働していたICカード認証と顔認証による認証システムと比較評価し，より低コストで２要素認証システムが実現できることを確認した。

The growing threat of cyberattacks on hospitals, including unauthorized access from outside, has had a major impact on medical treatments in recent years. However, as it is difficult to update individual medical equipment used in hospitals to the latest operating system (OS), there is an increasing need for continuous cybersecurity measures essential for hospital information systems, with two-factor authentication also being essential.

In response, Toshiba Corporation has applied the CYTHEMIS Internet of Things (IoT) security solution to hospital information systems, making it possible to securely network equipment without built-in security measures. We have confirmed that it is effective in preventing unauthorized access to medical equipment used in hospital information systems through real-world testing in cooperation with Asahikawa Medical University Hospital. We have also confirmed that the BISCADE biometric authentication card makes it possible to achieve two-factor authentication system at a lower cost than an authentication system combining integrated circuit (IC) card authentication with face authentication, which is already used at the hospital.

1. まえがき

近年，医療機関に対するサイバー攻撃は増加の一途をたどっており，サイバー攻撃に起因して病院情報システムが長期間停止するなどの事象が発生した場合，診療への影響が出ることになる。サイバー攻撃の手口としては，外部記憶媒体による攻撃や，ウイルスの仕込まれた添付ファイルや不正なリンク付きの電子メールによる攻撃，リモートによる保守業務で使用されているVPN（Virtual Private Network）機器を狙った攻撃など，様々である。

しかし，病院情報システムの構成要素の一部である医療機器は，最新のOSにすることが難しく，また，セキュリティー対策ソフトウェアがインストールできない場合もあり，システムを構成する医療機器自体での対策が困難である。そのため，厚生労働省の手引書「医療機関における医療機器のサイバーセキュリティ確保のための手引書」[(2)]に従って，医療機器のライフサイクル全体を通して継続的にサイバーセキュリティー対策を行うことは，医療機関にとって大変難しい問題である。

そこで，東芝は，CYTHEMISを適用した病院情報システムを構築した。CYTHEMISは，ゼロトラストの考え方に沿って開発されており，相互認証機能とパスリスト方式の通信許可機能を持っている。また，分析装置などのセキュリティー対策として採用実績がある。このCYTHEMISを病院情報システムに適用した場合の，レガシー医療機器・検査機器のセキュリティー対策の効果検証を，旭川医科大学と共同で実施し，実用性があることを確認した。

また，昨今，情報セキュリティー対策強化の観点から，ユーザー認証として知識・所有・生体の組み合わせによる多要素認証が求められている。厚生労働省の「医療情報システムの安全管理に関するガイドライン第6.0版 システム運用編」によると，病院情報システムについても，将来，２要素認証を求められることがあり[(3)]，今後，多要素認証の重要性が増していく。

しかし，多要素認証の実現には認証システムの構築に加え，対応デバイスを各端末に備えなければならないため，

多額の導入コストや維持コストを要するケースがほとんどである。

そこで，当社はBISCADEカードを適用して2要素認証システムを構築した。BISCADEカードは，一般的なICカードに指紋認証機能を搭載したことが特長である。指紋認証が成功するとICカードとして有効になり，その後でID（識別情報）認証を行う。このような構成により，1枚のカードで2要素認証が実現できる。BISCADEカードによる認証システムと，旭川医科大学病院で稼働していた2要素認証システムを比較評価し，BISCADEカードの有用性を確認した。

ここでは，CYTHEMISを用いた病院情報システムのセキュリティー評価，及びBISCADEカードを用いた2要素認証システムの評価の結果を示し，これらの技術の病院情報システムに対する有効性について述べる。

2. CYTHEMISを用いた病院情報システムのセキュリティー評価

2.1 評価環境と脅威シナリオ

一般的に，病院情報システムの医療機器・検査機器は利用目的が明確なため，通信相手や，通信プロトコル，ポート番号などが一意に決まっている。そこで，評価環境では通信相手と相互認証を行うこととし，また，必要な通信プロトコル，ポート番号だけを通信許可するパスリスト方式とした。**図1**と**図2**に，病院情報システムを含む医療ネットワークの評価環境を示す。

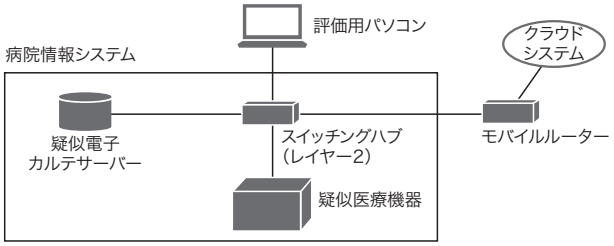


図1. CYTHEMISデバイスがない場合の医療ネットワークの評価環境

最新OSでない医療機器を含む医療ネットワークを疑似的に再現したものであり，セキュリティー対策が困難である。

Experimental environment of medical network without use of CYTHEMIS device

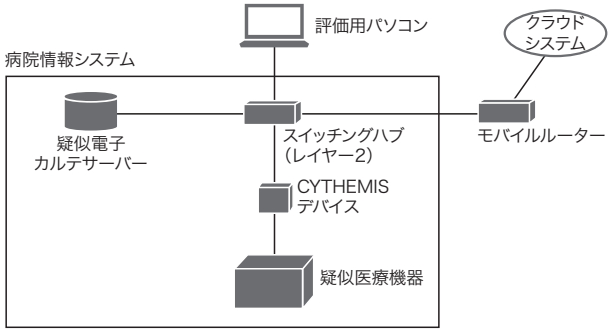


図2. CYTHEMISデバイスがある場合の医療ネットワークの評価環境

スイッチングハブと疑似医療機器の間にCYTHEMISデバイスを入れることでセキュリティーを考慮した構成とした。

Experimental environment of medical network using CYTHEMIS device

今回の評価では最新バージョンではないOSを搭載したパソコンを疑似的な医療機器に見立て，CYTHEMISデバイスを接続しない場合（図1）と接続した場合（図2）の比較評価を行った。

評価に使う脅威シナリオとして，疑似医療機器が医療ネットワークを通して不正なWebサイトにアクセスし，悪意のあるリバースシェル実行ファイルがダウンロード・実行され，疑似医療機器が遠隔操作された場合を想定し，テストを実施した。

2.2 評価結果

表1に，2.1節記載の脅威シナリオを想定したテスト項目と評価結果を示す。CYTHEMISデバイスを接続することにより，脅威シナリオ想定時においても，不正な実行ファイルのダウンロードを阻止し，その後の遠隔操作などを防止できることを確認した。

更に，九つの脅威シナリオを想定したテストを実施し，CYTHEMISによるセキュリティー対策の有効性を確認した[4]。

3. BISCADEカードを用いた2要素認証システムの評価

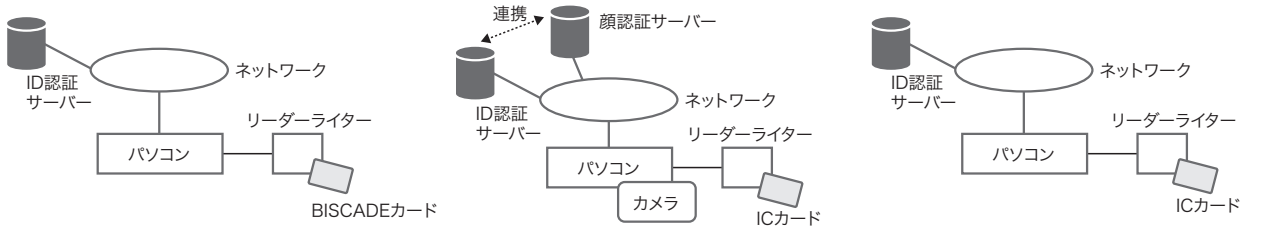
3.1 評価環境

2要素認証システムとして，BISCADEカードによる認証システムと，旭川医科大学病院で稼働中のICカード認証と顔認証による認証システムを評価した。また，1要素認証システムであるICカード認証による認証システムも評価し，比較した。**図3**に，三つの認証システムの評価環境を示す。

表1. CYTHEMISの評価結果

Results of comparative evaluation of medical networks with and without CYTHEMIS device

CYTHEMISデバイスの接続の有無		無	有
テスト項目	パケットキャプチャー	可能	可能
	ネットワークスキャン	可能	可能
	OSスキャン	可能	可能
	サービスのバージョンスキャン	可能	可能
	実行ファイルのダウンロード	実行される	阻止（パスリスト違反）
	実行ファイルの実行	実行される	実行ファイルのダウンロードを阻止したため，それ以上の攻撃が不可能
	セッション確立	確立される	
	情報窃取	窃取される	
	遠隔操作	操作される	



(a) BISCADEカードによる認証システム　(b) ICカード認証と顔認証による認証システム　(c) ICカード認証による認証システム(1要素認証)

図3. 2要素認証システムの評価環境

顔認証の代わりにBISCADEカードを用いて指紋認証することで，顔認証サーバーが不要となる。

Experimental environment of comparative evaluation of two-factor authentication systems

評価は，(1)システム構成，(2)システム導入コスト，(3)認証時間及び認証エラー頻度，(4)ユーザー登録の容易性の4項目について行った。

3.2 評価結果

3.1節に記載した4項目の評価結果を以下に示す。

(1) システム構成　　ICカード認証には，ICカード固有の番号とユーザー IDとのひも付けを行うID認証サーバーが必要である。顔認証には，顔認証サーバーが必要であり，ICカードと2要素認証する場合は，顔認証サーバーとID認証サーバーの連携も必要となる(図3(b))。一方，BISCADEカードによる認証システム(図3(a))は，指紋認証自体はBISCADEカード内で完結し，指紋認証が成功した時点でICカードとして有効になるため，ICカード認証だけの場合(図3(c))と同様のシンプルなシステム構成で実現できる。

(2) システム導入コスト　　三つの認証システムでID認証サーバーの導入コストが必要であり，顔認証には，別途，顔認証サーバーの導入コストが必要である。ただし，BISCADEカードは，一般的なICカードと比較してカード単価は高額である。

(3) 認証時間及び認証エラー頻度　　BISCADEカードによる認証システムとICカード認証による認証システムは，ICカードをかざしてから認証完了するまで，いずれも1秒未満と認証時間が短かった。一方で，顔認証は，10回測定の平均で3.07秒(標準偏差0.27秒)の時間を要した。また，認証エラーについては，ICカード認証及びBISCADEカードは，評価中に認証エラーは発生しなかった。顔認証は，これまでの旭川医科大学病院における使用実績での認証エラー率は16％(過去数年の運用状況における初回認証時の平均認証エラー率)であった。なお，BISCADEカードは，認証エラー自体は発生しないものの，指紋を認識させるための指の当て方に慣れが必要であった。

表2. 2要素認証の総合評価結果

Results of comprehensive evaluation of two-factor authentication systems

項　目	BISCADE カードによる 認証システム	ICカード認証と 顔認証による 認証システム	ICカード認証による 認証システム
システム構築	◎	△	◎
導入コスト	○	△	◎
認証時間	◎	△	◎
ユーザー登録	○	△	◎
セキュリティー	◎	◎	△(1要素認証)

◎：非常に良い　○：良い　△：普通

(4) ユーザー登録の容易性　　三つの認証システムでサーバーへのユーザー登録は必要である。加えて，顔認証は複数枚の顔写真とICカードをひも付けして登録する必要がある。一方，BISCADEカードは，カード自体に指紋を登録するため，ICカードとのひも付け作業が不要であり，顔認証と比較して，ユーザー登録が容易に実現できた。

総合的な評価結果を**表2**に示す。BISCADEカードによる認証システムは，BISCADEカードの調達コストが増加するものの，ICカード認証と顔認証による認証システムと比較して，低コストで2要素認証システムが実現できる。また，認証時間は1秒未満と実用範囲内であり，認証エラー頻度も低いことから，実用上有効である。

4. あとがき

実用性評価の結果，CYTHEMISが病院情報システムのレガシー医療機器・検査機器のセキュリティー対策として有効であること，及びBISCADEカードが病院情報システムの2要素認証対応に有用であることを確認した。

当社は，今後もセキュアな社会の実現に貢献できるセキュリティー製品を開発し，提供していく。

文　献

⑴ 薩川満明，ほか．ユーザー，デバイス，データを認証するセキュリティソリューション．東芝レビュー．2022，**77**，3，p.19–23．<https://www.global.toshiba/content/dam/toshiba/jp/technology/corporate/review/2022/03/a06.pdf>，(参照 2025-04-15).

⑵ 日本医療機器産業連合会 サイバーセキュリティタスクフォース．医政参発0331第１号，薬生機審発0331第16号，薬生安発0331第8号，別添 医療機関における医療機器のサイバーセキュリティ確保のための手引書．厚生労働省，2023，22p．<https://www.mhlw.go.jp/content/11120000/001167218.pdf>，(参照 2025-04-15).

⑶ 厚生労働省．医療情報システムの安全管理に関するガイドライン第6.0版 システム運用編．2023，57p．<https://www.mhlw.go.jp/content/10808000/001112044.pdf>，(参照 2025-04-15).

⑷ 東芝．旭川医科大学病院様 CYTHEMIS™(サイテミス)実証研究レポート．<https://www.global.toshiba/jp/products-solutions/security-automation/card-security/infra-security/column/chapter4.html>，(参照 2025-04-22).

利光　清　TOSHIMITSU Kiyoshi
セキュリティ・自動化システム事業部
紙幣処理機器・セキュリティシステム技術部
Banknote Automation and Security Systems Engineering Dept.

加藤　雅一　KATO Masakazu
セキュリティ・自動化システム事業部
紙幣処理機器・セキュリティシステム技術部
Banknote Automation and Security Systems Engineering Dept.

畠中　一成　HATANAKA Issei
セキュリティ・自動化システム事業部
紙幣処理機器・セキュリティシステム技術部
Banknote Automation and Security Systems Engineering Dept.

谷　祐児　TANI Yuji, Ph. D.
旭川医科大学
博士(商学)　日本医療情報学会・日本放射線技術学会・
日本Mテクノロジー学会会員
Asahikawa Medical University