別紙３

厚生労働科学研究費補助金
（政策科学総合研究事業（臨床研究等 ICT 基盤構築・人工知能実装研究事業））
分担研究報告書

「AI 技術を用いた手術支援システムの基盤を確立するための研究」

研究分担者：慶應義塾大学 環境情報学部　　教授　　村井　純
研究協力者：慶應義塾大学　政策・メディア研究科　特任講師　松谷　健史

研究要旨

SCOT シミュレータは ME 機器やアプリケーションが仕様を満たしているかを調査するものであるが、本年度は関連研究・技術を参考にし、仕様策定のための調査をおこなった。

SCOT では非セキュアなネットワーク状態であるインターネットなどに直接接続されることは想定していない。しかし、SCOT 規格を満たした ME 機器やアプリケーション通信には IP プトロトコルなどの汎用プロトコル、オペレーティングシステムには Linux や Windows などの汎用 OS が用いられているため、閉鎖的ネットワークであったとしても攻撃されるシナリオがあることと対策すべき攻撃をあきらかにした。

また、ユーザビリティを向上するために、ME 機器からのセンサー情報がディスプレイ装置に表示されるまでの遅延時間を計測する手法をあきらかにし、これを SCOT シミュレータで検査する仕様策定に含めた。

A. 研究目的

東京女子医科大学を中心に推進中のＡＭＥＤ事業「安全性と医療効率の向上を両立するスマート治療室　（ＳＣＯＴ：　Ｓｍａｒｔ　Ｃｙｂｅｒ　Ｏｐｅｒａｔｉｎｇ　Ｔｈｅａｔｅｒ）の開発」は、まったく新しいコンセプトに基づく医療システム構築を目論むものであるため、その概念は既存のＩＥＣ、ＩＳＯ等々の医用機器関連国際規格のスコープには含まれていない。つまりＳＣＯＴには製品認証に適用する評価規格が存在しないという問題がある。このことはＳＣＯＴ事業の目的が、“我が国の輸出の切り札としての治療室産業を創出すること”でありながら、輸出に必須である 医用機器もしくは医用システムとして国際認証を得ることが困難となり、我が国の医療機器産業育成への効果が乏しくなる。

この様な隘路を突破するには、新たに医用機器もしくは医用システムとしての基本性能と安全性を担保する要求事項を規定した国際規格と基本性能と安全性を評価する試験方法の規定が必要である。
このために経済産業省の戦略的国際標準化加速事業・政府戦略分野に係る国際標準開発活動、テーマ名：安全性と医療効率を両立する。
スマート治療室に関わる国際標準化、において製品認証に用いる国際規格の策定に着手している。

しかし、該国際標準化事業は規格策定のための調査及び会議運営に特化されており“基本性能と安全性を評価する試験方法”のハードウエア及びソフトウエア開発が含まれていない。
よって慶應義塾大学、国立医薬品食品衛生研究所とのＡＩ技術を用いた手術支援システムの基盤を確立するための研究により、上記のＳＣＯＴ認証規格策定事業と並行してＳＣＯＴシミュレータを開発し、安全性と医療効率の向上を両立するスマート治療室、つまり“ＡＩ技術を用いた手術支援システムの基盤”を構築しＳＣＯＴシステム認証取得の迅速化をはかる。

３年計画の初年度にあたる平成２９年はシミュレータの関連ソフトウエア調査と仕様書策定のための調査と仕様書への反映である。

B. 方法

シミュレータの仕様策定にあたり、関連技術、先行事例より要件となりうる項目を洗い出し、整理する。また、以下の役割を行うソフトウエア開発WGの設置をする。

①接続するＭＥ機器や他の装置に求められるＳＣＯＴとしてのパフォーマンス達成に必要な、画質、リアルタイム性、時間分解能、プロトコルと応答性等々を評価。
②汎用のデータ保存フォーマット、データ長、時間分解能、検索タグ等の評価
③ミドルウエアのフォールトトレラント
④ＯＲ．ｎｅｔで規定された機器及びシステムをＳＣＯＴに接続する場合のパフォーマンスと互換性を評価する。

C. 結果

SCOT のベースで用いられる技術や類似技術に関して、シミュレータの仕様策定上、検討すべき項目について述べる。

①セキュリティ対策の必要性

図 1 は SCOT で用いる OpeLink ネットワークの接続を示したものである。OpeLink の通信プロトコルには IP が用いられる。OpeLink は ME 機器や SCOT 機器など閉ざされたローカルネットワーク環境で利用されることが多くを占めるが、一部、部門システムネットワークと接続し患者情報（入出や麻酔など）と連携する必要があるため、SCOT 以外のネットワークに接続している機器より攻撃を受ける可能性がある。また、SCOT で接続する機器が IP 通信を用いるため、それらのオペレーティングシステムに Linux や Windows などの汎用 OS が使われることが想定される。

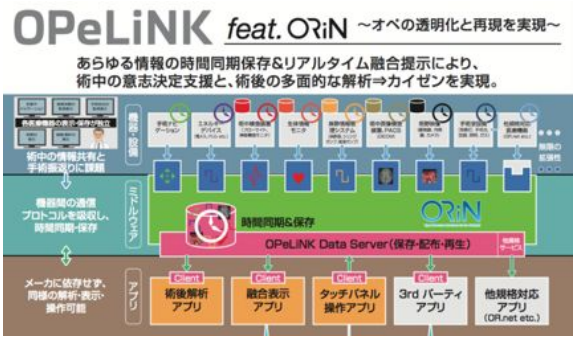

図 1 SCOT と OpeLink ネットワーク

そのため、インターネットに接続される機器と同等のセキュリティ対策が必要になり、これらの対策状況に関して検査する仕組みがシミュレータに必要である。以下に、考慮すべきセキュリティ攻撃手法とシナリオ例をあげる。

A. DoS(Denial of Service)
B. DDos(Distributed Denial of Service
C. ゼロディ攻撃
D. バッファオーバーフロー攻撃
E. SQL インジェクション攻撃
F. パケット改竄攻撃
G. パスワードリスト攻撃
H. 標的型攻撃
I. USB 型攻撃
J. ネットワーク物理設置型攻撃

A は、特定の端末から要求パケットを投げ続けることによりサービスを停止状態にするもので、部門システム内の端末が外付け USB など経由で BOT などに感染した場合に攻撃を受ける可能性がある。

B は、A によって感染した院内ノードがネットワーク内の他のノードにも感染し、複数より攻撃される場合である。この場合、特定のサービスだけでなくネットワーク全体が停止される危険が考えられる。

C は、対策パッチが用意されていないセキュリティホールに対する攻撃である。BOT 化かした端末や院内に不正接続したノードから攻撃を受け、機器の管理者権限やデータなどを取得されるおそれがある。

D は、ME 機器や SCOT アプリケーションに使われている、正常通信パケットの中のデータ部のサイズを極端に増やし、一部不正実行するマシン語を埋め込み、機器に送信することで、アプリケーション上の受信バッファをオーバーフローし管理者権限やデータを取得するものである。

E は、データベースサービスを持つ SCOT アプリケーションに対し、不正な SQL コマンドを送ることで、許可されていないデータベース権限やシステムの管理者権限を取得するものである。

F は、E 機器や SCOT アプリケーションに使われている、正常通信パケットを改竄し、機器に送信することで、管理者権限やデータを取得するものである。

G は、認証やログインなどの機能がある機器にたいして、工場出荷時のログイン、パスワードや登録頻度が多いものを試すことにより、不正アクセスをはかるものである。

H は、ターゲットユーザに一般のメールを装い、添付ファイルや URL を開くことで BOT 化させるものである。

I は、USB が接続できる ME 機器や SCOT アプリケーションに対して、ウイルスを含む USB ストレージや、ハッキングをするためのキーボードやマウス操作が記述された、USB キーボードとして動作可能な小型 USB 装置である。USB ポートを物理的に削除するか、論理的に利用できない対策が好ましい。

J は、SCOT が接続されるネットワーク内に小型の不正アクセス装置を設置する手法である。これらの意図していない機器がネットワーク内に存在した場合に発見する仕組みとシミュレーション可能であるかを検討する必要がる。

H に関してのみ、メールなどを用いて人間をターゲットにしたものであるから、SCOT では対策の必要はないと考えられるが、それ以外の項目は何らかの対策や問題が発生しうることから検討する必要が

あることがわかった。

②計測項目と遅延の計測手法

図 2 は、SCOT シミュレータの全体図を示す。SCOT シミュレータは、試験のため各種 ME 機器が作成するデータを擬似的に生成する機能「SCOT シミュレータフロントエンド」と、SCOT 対応アプリケーションが仕様を満たして、出力されているかを検証する機能「SCOT シミュレータバックエンド」より構成される。

SCOT フロントエンドより出力された ME 機器を模倣したデータが、SCOT 対応アプリケーションを経由し出力される数値に関しては、以下の項目について計測が必要であると考えられる。

A. 表示の精度（丸目や数値の有効桁や範囲）
B. 表示の書き換えの頻度(秒あたり何回)
C. 表示の遅延（入力から出力までの遅延）

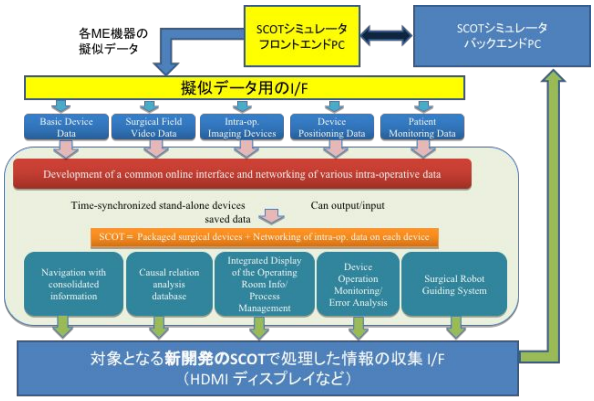

図 2 SCOT シミュレータの全体図

C のデータ表示遅延に関しては、手術中の操作性に大きく関わる。遅延を計測する手法としてはいくつかあるが、図３にディスプレイとカメラを用いた遅延計測手法、図４にディスプレイ信号
用いた遅延計測手法をあげる。

図３では以下の処理を行うことで、ME 機器より出力された数値が反映されるまでの遅延を計測する。

① SCOT フロントエンド側シミュレータが ME 機器を擬似的に生成する
② OpeLink ネットワークを経由する
③ 検査対象の SCOT アプリケーションが処理をする
④ ディスプレイへ表示をする
⑤ ディスプレイへ表示された画面をビデオカメラで撮影する
⑥ 撮影したビデオ情報をビデオキャプチャーボードで取り込む
⑦ SCOT バックエンド側シミュレータがビデオ映像を取り込み、画像から数値を認識する

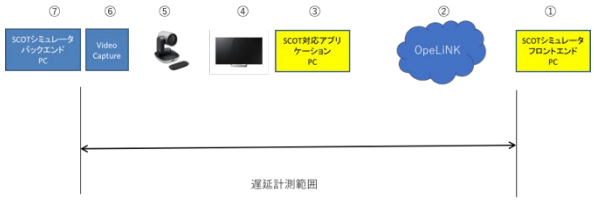

図 3 ディスプレイとカメラによる遅延計測手法

図 3 の手法では、ディプレイの内部の処理遅延やビデオカメラやキャプチャーボード内部の処理遅延が含まれるため、医師が体感する遅延より多くなるなど異なることがある。

次に図 4 は、ディスプレイやビデオカメラを用いないで遅延を検測する手法である。この手法はディスプレイやビデオカメラを用いず、SCOT アプリケーションより出力された画面を HDMI ケーブルで直接 SCOT バックエンド側シミュレータ内のキャプチャーボードで検査する。

図 4 ディスプレイ信号による遅延計測手法

SCOT アプリケーションの遅延計測手法を２つあげたか、図３では実際のディスプレイの遅延も含まれるが、検査で用いるディスプレイと異なるものを医療現場で用いた場合に異なる結果となる。

また図 4 では、ディスプレイの表示遅延を含まないため、実際の遅延より少なくなる。

ディスプレイ内の処理遅延があきらかであれば、図４の手法と組み合わせることで、様々なディスプレイを用いた場合の遅延を算出することができるが、ディスプレイごとの処理遅延はメーカーなどから公開されている例は少なく、難しいことが問題である

③システムレベルの障害対策と検証の必要性

SCOT シミュレータでは、ME 機器やネットワーク、SCOT 機器の障害対策も検証する範囲である。

機器箇所としては以下があげられる。

1. ME 機器の障害
2. ネットワークの障害
3. SCOT アプリケーションの障害

2 のネットワークに関しては冗長化構成をとることにより、一箇所の障害であれば回避することができる。

1 と 3 の障害に関しては、機器単体で障害回避を行うことは個々の機器の機能として実装されていない限り実現できない。しかし SCOT で接続されている機器はネットワークで接続されているため、ME 機器やアプリケーション PC を冗長的に持つことが、個別の障害には対応できない場合でも、おなじ SCOT 上で接続された冗長的に用意された予備機や予備 PC を用いることで、SCOT システム全体としては障害対策をおこなうことが可能と考えられる。しかし、ネットワーク機器と異なり状態を保持している ME 機器や SCOT アプリケーションを稼働中に、切り替えることは技術的に容易なことではない。

このような SCOT ネットワーク全体を用いた、ホットスタンバイによる冗長性構成に関する検証手法の可能性に関して検討する必要があることがわかった。

D. 考察

初年度は SCOT シミュレータのソフト仕様策定にあたって、類似技術や仕様などから考慮すべき点として、ME 機器や SCOT 機器に関するセキュリティ対策、ME 機器からのセンサー情報をディスプレイに表示するまでの遅延の計測の必要性と手法、SCOT をネットワークとして用いることによる単体の機器では対策できない、異なる障害対策の手法が確立できる可能性があることが判明した。
２年目以降は、本年度判明した問題やあらたな可能性に対して、システム実装可能な具体的な解決や実現手法について検討するとともに、引き続き関連する仕様を網羅的に調査し、SCOT シミュレータを作成するのに必要な仕様を策定する。

E. まとめ

SCOT は手術という限られた現場用いられる技術であるが、院内の部門ネットワークの接続の必要性や、SCOT で用いられる通信プロトコルに汎用である IP が用いられ、またその高度な機能性から汎用オペレーティングシステムである Linux や Windows を利用することが想定できる。このため接続が限定されているとはいえ、インターネットで懸念させている様々なセキュリティ問題に対応しなければいけないことがわかり、具体的な攻撃手法について提示した。これらいくつかについては攻撃に対応できることについてシミュレータで検査する必要があることがわかった。

次に、手術中の ME 機器からのセンサー情報をリアルタイムで反映させる場合の遅延について、２つの計測手法を提示した。実際に出力するディスプレイの遅延を含めた場合と、ディスプレイの遅延を含まない場合であるが、現場で使われるディスプレイによって依存する部分であるため、どちらの計測手法が良いかは今後、ディスプレイの遅延計測の手法も含めて検討していく必要がある。

次に、SCOT では ME 機器や SCOT 対応アプリケーションで障害が発生した場合に、SCOT 内に予備機を冗長的に設置することで、障害対策ができる可能性があることを述べ、またそのようなシナリオを含めてシミュレータの仕様として策定することを検討する必要がある。
このことから、SCOT は ME 機器とアプリケーションが機能的に接続するだけではなく、SCOT をネットワークとして、それぞれの障害対策に利用できることがあきらかになった。

H30 年度は以上をふまえ、シミュレータソフトウェアで実装できる具体的な対策と実現手法を検討しながら、シミュレータのソフトウェア仕様の策定を引き続きおこなう。

G. 研究発表

H.29 年度は該当なし

H. 知的財産権の出願・登録状況

H.29 年度は該当なし