IoT 時代のセキュリティとフォレンジックの技術課題と対応策

佐々木良一[1]

自動車や家電品，医療用機器など従来ネットワークにつながっていなかったいろいろな「もの」がインターネットにつながる IoT（Internet of Things）時代が到来しつつある．このような時代においては従来のセキュリティ技術やフォレンジック技術とは異なる技術が必要になる．本稿では，IoT システムを 4 つのレイヤー（サービスレイヤー，プラットフォームレイヤー，ネットワークレイヤー，デバイスレイヤー）にわけ，それぞれ重要性が高まると考えられるセキュリティ技術を示す．特に，IoT 時代を迎え，①セキュリティとセーフティの両方を考える必要がある，②制御システムのように多重のフィードバックを含むシステムを扱う必要がある，③影響の定量化が困難であるなどの理由により従来の方法ではうまくいかなくなってきているリスク評価手法について著者らの最近の研究状況を報告する．併せて IoT 時代に要求されるフォレンジックの特徴とそのために必要となるフォレンジック技術の特徴について上記の 4 つのレイヤーごとに記述する．

Security and forensic technical issues and countermeasures in the IoT era

RYOICHI SASAKI[1]

1. 概要

自動車や家電品，医療用機器など従来ネットワークにつながっていなかったいろいろな「もの」がインターネットにつながる IoT（Internet of Things）時代が到来しつつある．総務省の平成 27 年度の通信白書によると 2020 年には世界で 530 億個の「もの」がインターネットにつながると予想されている．

このような時代においては，リスクが増大するとともに，セキュリティ対策やフォレンジック対策が困難となるため従来のセキュリティ技術やフォレンジック技術とは異なる技術が重要になる．本稿では，IoT システムを 4 つのレイヤー（サービスレイヤー，プラットフォームレイヤー，ネットワークレイヤー，デバイスレイヤー）にわけ，それぞれ重要性が高まると考えられるセキュリティ技術を示す．特に，IoT 時代を迎え，①セキュリティとセーフティの両方を考える必要がある，②制御システムのように多重のフィードバックを含むシステムを扱う必要がある，③影響の定量化が困難であるなどの理由により従来の方法ではうまくいかなくなってきているリスク評価手法について，著者らの最近の研究状況を報告する．

併せて IoT 時代に要求されるフォレンジックの特徴とそのために必要となるフォレンジック技術の特徴について上記の 4 つのレイヤーごとに記述する．

２．IoT 時代のセキュリティの課題

IoT セキュリティガイドライン[1]によると IoT は，図 1 の左側に染めすような性質があるといわれている．これらの性質は，図 1 の右側に示すような理由により，セキュリティ対策がより重要なるような方向で機能する．

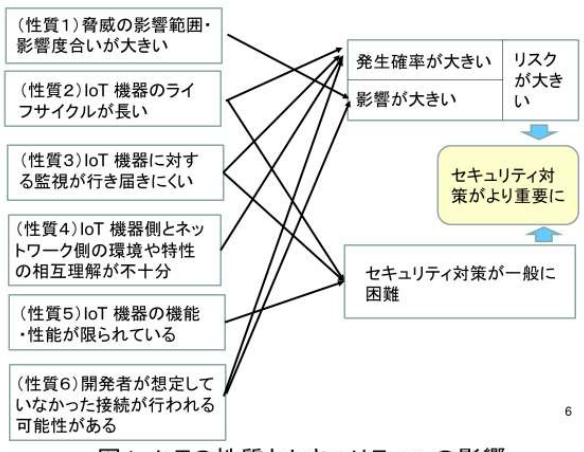


図1 IoTの性質とセキュリティへの影響

また，IoT 端末を含むシステムは制御対象を含むことが多いため，その安全の問題を扱うためには，図 2 に示すように従来のセキュリティだけではなく，セーフティの問題も同時に扱う必要がある．

さらに，IoT システムは空間的に広がった複雑な形態をとることが多いため，対策案などを検討するためには図 3

1 東京電機大学 Tokyo Denki University

に示すように階層化して行うことが望ましい．ここでは総務省の階層化法[2]に従って，サービスレイヤー，プラットフォームレイヤー，ネットワークレイヤー，デバイスレイヤーの 4 つに分類している．

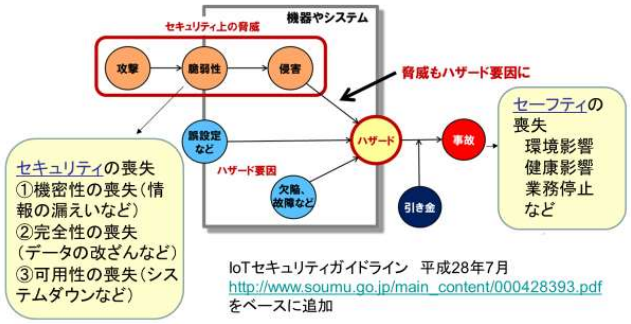


図2　IoTのセキュリティとセーフティ

同じ IoT システムでも対象が異なると，対策すべきレイヤーや適切な対策が異なってくる．例えば小規模な IoT システムを新規に計画する場合の安全対策はデバイスレイヤーにセキュアチップを組み込み，認証と通信路の暗号化をしっかり実施するのが最適である．しかし，既存の小規模な IoT システムのデバイスにあとからセキュアチップを埋め込むことは，手間やそのコストを考えると現実的ではない．この場合は，ネットワークレイヤーでセキュアゲートウエイを設置し，不適切な通信をフィルタリングするというのが適切な対策になるだろう．また，新規の大規模なシステムでは種々の対策を組み合わせるのが適切な対策になる．

それぞれのレイヤーでどのような必要機能があり，どのような研究項目があるかをまとめたのが表 1 である．サービスレイヤーではプライバシー保護などが引き続き重要となり，自己情報コントロール技術などが必要になる．

データ管理レイヤーではデータの秘密管理や，バックアップ，改ざん防止などが必要になる．このためには秘密分散技術やデジタルフォレンジック技術，電子署名技術，ブロックチェーンなどが必要になる．東京電機大学でもデータの安全性とバックアップの両方を実現するための技術の研究を行っている[3].

ネットワークレイヤーでは不適切なデータのフィルタリングや通信情報の秘匿などが必要機能となる．そのためセキュアゲートウエイや，通信路暗号，フォグコンピューティングなどの技術が重要となる．東京電機大学でも Multi-Layer Binding ルータを用いた適応側フィリタリングシステムの研究・開発を実施している[4].

デバイスレイヤーでは，センサーやアクチュエータのなりすましの防止や，IoT 機器側の暗号化機能が必要となる．このため，セキュアチップや省電力モジュール，軽量暗号などの研究・開発が重要となる．

また，全体として必要になるのが，機械学習などの人工知能技術や，リスク評価技術・リスクコミュニケーション技術である．IoT システム向けのリスク評価手法については 3 節で詳しく説明する．

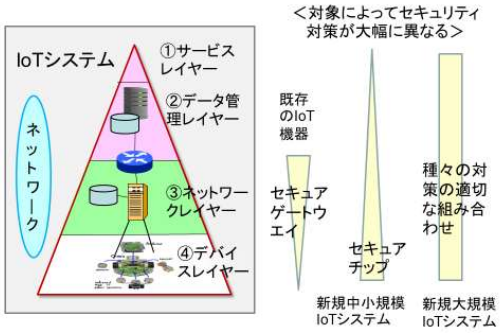


図3　IoTシステムのレイヤーリングと安全対策

表1　IoTのレイヤリングと安全対策

レイヤー	必要機能	研究が必要となる項目
1. サービスレイヤー	プライバシー保護 フィッシング防止	自己情報コントロール技術など
2. データ管理レイヤー	データの秘密管理とバックアップ 改ざん防止	秘密分散技術 デジタルフォレンジック など
3. ネットワークレイヤー	不適切なデータのフィルタリング 通信情報の秘匿	セキュアゲートウエイ 通信路暗号 フォグコンピューティング など
4. デバイスレイヤー	センサーやアクチュエータなどのなりすまし防止 IoT機器側の暗号化機能	セキュアチップ 省電力モジュール 軽量暗号など

全体として、機械学習などの人工知能技術や、リスク評価技術が重要となる

3．IoT システムのリスク評価手法

著者らは，多重リスクコミュニケータ MRC を開発するとともに種々の対象のリスク評価に適用してきた[5]-[18]．ここで扱うのは IoT システムのリスク評価に適用するための改良とその適用結果を示すものである．

3．1　手順の概要

IoT システムのリスク評価を実施する上で必要な要件は以下のとおりであると考えられる[18].

（要件１）セーフティとセキュリティ両方のリスク指標が扱える．

（要件２）多重のフォードバックを含む制御機能のリスク分析が可能である．

（要件３）システムの故障やヒューマンエラー以外にサイバー攻撃などの影響も評価に組み込める．

（要件４）死亡者など生命の価値が評価指標になるが，金

銭などに換算するのが技術的にも道徳的にもむつかしいので準定量的な評価を前提とする．

これらの要件を満足するために開発予定のリスク評価手順は以下のとおりである．

① 事前準備：前提条件の整理
② 準備１：対象アクシデント・インシデントとその評価指標の明確化
③ 準備２：コントロールストラクチャーの構築
④ UCA（非安全動作・非セキュア攻撃）の明確化
⑤ UCA の発生原因 HCF（ハザード誘発要因）の分析
⑥ 追加分析作業：対象アクシデント・インシデント別フォルト・アンド・アタックツリーの完成
⑦ 対策の立案：フォルト・アンド・アタックツリーの最下位項目に対応した対策のリストアップ
⑧ 対策組み合わせの決定：採用すべき対策組み合わせに関する準定量的分析と合意形成

ここで，①－④は，MIT のナンシーレブソンらが提案する STAMP/STPA 手法[19]と同様の方法を用いている．⑤は STAMP/STAPA を安全問題だけでなくサイバー攻撃の影響など従来セキュリティの分野で扱っていた脅威も扱えるようにしている．

３．２　インスリン注入システムへの適用

ここでは，図 4 に示すようなインスリン注入を目的とした医療用 IoT システム（文献[20]を参考にして作成）を想定して手順の説明を行う．

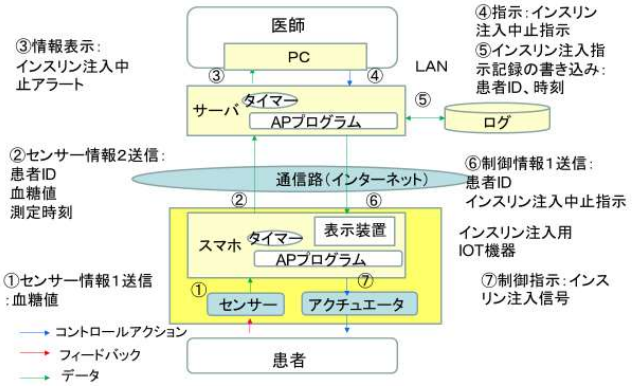
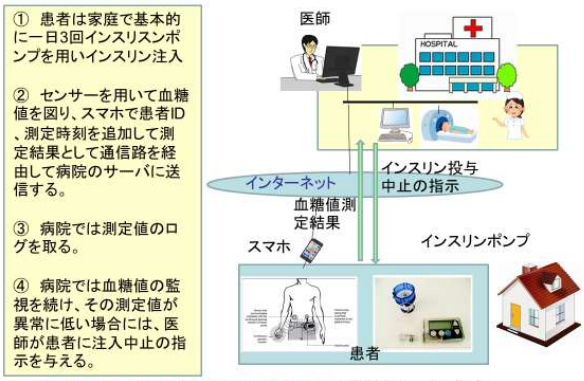


図5　コントロールストラクチャーの構築

① 事前準備：

対象となるシステムの構成や機能などを明確化する．図 4 のようなものを作成するようなことを含む．現実のシステムは病院側からインスリンの注入を指令するのではなく，患者が自分でインスリンの注入を行うようであるが，ここでは適度の分析の複雑さを確保するため図 4 のような機能とした．



https://www.ipa.go.jp/files/000038223.pdfの資料をベースに作成

図4　インスリン注入システムの概要

② 準備１：

対象アクシデント・インシデントとその評価指標の明確化：一般には（１）生命や環境にかかわるアクシデント，（２）対象システムの異常停止，（３）重要情報の流出など影響の大きなアクシデントやインシデントを対象とすることとした．（１）（２）が従来セーフティの分野で扱われ，（３）はセキュリティの分野で扱われていたものである．この例では，（ａ）インスリンを注入すべき時に注入しないことによる血糖値の上昇による健康障害，（ｂ）インスリンが必要以上に投与され健康障害（血糖値の異常低下など），（ｃ）医療データの流出の 3 つとした．これは，セーフティとセキュリティ両方のリスク指標が扱えるという**（要件１）**を満足するものとなっている．

③ 準備２：

図 4 の対象を分析しコントロールストラクチャーを図 5 のように想定した．

④ UCA（非安全動作・非セキュア攻撃）の明確化

図 5 の①－⑦に示したすべてのコントロールアクションに対応して，非安全・非セキュアな結果となる UCA（Unsafe and Unsecure Control Action）を表 2 に示すようにして抽出する． この結果全部で 29 の UCA をリストアップした．

表2　Unsafe and Unsecure Control Actionの抽出

コントロールアクション	Not Providing	Providing Causes hazard	Too early too late	Too soon too long
①センサー情報1送信 血糖値	(UCA①N1)センサーから血糖値が与えられない＝＞血糖値が下がっているのに気つかない＝＞インスリン投入を続け血糖値異常低下(結果1)	(UCA①P1)血糖値を間違えて低くしたり低く改ざんする＝＞インスリン投入の中止＝＞血糖値上昇(結果2) (UCA①P2)血糖値を間違えて高くしたり高く改ざんする＝＞血糖値異常低下(結果1) (UCA①P3)センサーからスマホ間の通信のタッピング＝＞情報漏洩(結果3)	(UCA①L1)センサーから血糖値が与えられるのが遅すぎる＝＞血糖値が下がっているのに気つかない＝＞＝＞血糖値異常低(結果1)	—

UCAの識別表

Too Early や Too Late, Too soon や Too long など種々の制御の状態によって安全でない状態がリストアップできるのが STAMP/STPA の特長である．またここでは，血糖値上昇や血糖値異常低下などどのアクシデントやインシデントにつながるかを記述し，あとで同一の結果となるツリーの要素を結合できるようにした．

⑤　UCA の発生原因（ハザード誘発要因 HCF）の分析：

何が UCA をもたらすかの原因をリストアップするのは容易ではない．特に，システムの故障やヒューマンエラー以外にサイバー攻撃などの影響も考慮してリストアップする方法は従来提案されてこなかった．そこで，図 6 に示すようなガイドテンプレートを考案し，関連するコントロールストラクチャーに，図 6 に示すように記入できるようにした．セキュリティに関する脅威の抽出には STRIDE 法[20]を用いてガイドするようにしている．これはシステムの故障やヒューマンエラー以外にサイバー攻撃などの影響も評価に組み込めるという**（要件３）**を満足するものとなっている．この結果 121 個の HCF を抽出した．

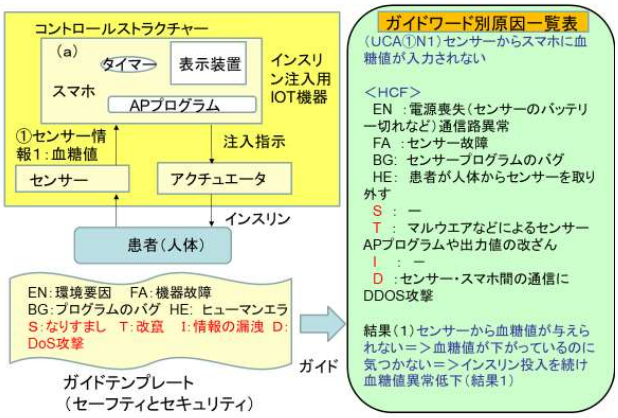


図6　ハザード誘発要因HCFの抽出

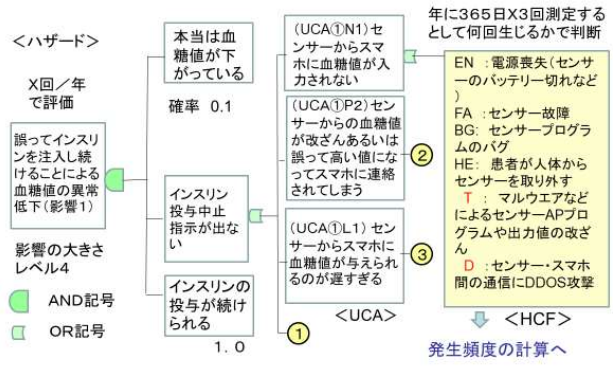


図7　作成したフォルトアンドアタックツリーの一部

⑥　追加分析作業：

同じアクシデント・インシデントをもたらす UCA をリストアップし，それぞれのアクシデント・インシデントに対し，図 7 に示すような，フォルト・アンド・アタックツリーを作成する．

このフォルト・アンド・アタックツリーは一番左側の項目（通常，最上位項目という）を対象アクシデント・インシデントとし，その次が同一の結果をもたらす UCA，その次が図 6 のガイドワードで抽出された原因である HCF をベースにシステムの故障やヒューマンエラー以外にサイバー攻撃などの影響も含むものとなっている．

⑦　対策の立案：

フォルト・アンド・アタックツリーの最下位項目（図 7 では一番右側の項目）に対応した対策のリストアップを行う．その一例を図 8 に示す．このサイバー攻撃などセキュリティ側の対策のリストアップには，米国 NIST の「重要インフラのサイバーセキュリティを向上させるためのフレームワーク」[22]や IPA の[23]などを参考にすればよい．この結果 92 の対策案をリストアップした．

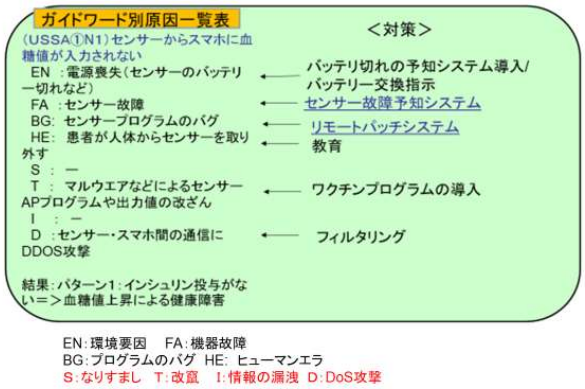


図8　対策案の例

⑧　対策組み合わせの決定：

採用すべき対策組み合わせに関する準定量的分析と合意形成．ここでは**（要件４）**を満足するため次のような準定量的分析を行っている．（図 9 参照）

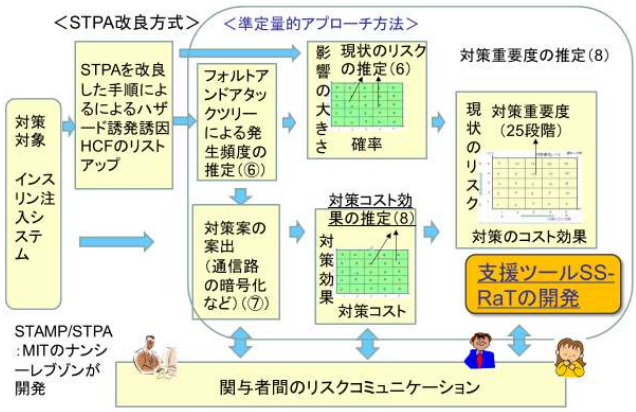


図9　医療用IoT機器対策のためのリスク評価の全体フロー

（a）図 7 のようなフォルトツリーアンドアタックツリーの最上位項目の影響の大きさを 5 段階に分ける．

ここでは図 10 のようなレベル設定を行った．

（b）図 7 のようなフォルトツリーアンドアタックツリーの最下位項目の発生確率の大きさを図 10 に示すようにして 5 段階に分ける．

（c）得られた影響の大きさの段階と発生確率の大きさの段階から，図 10 のようにしてリスクのレベルを設定する．

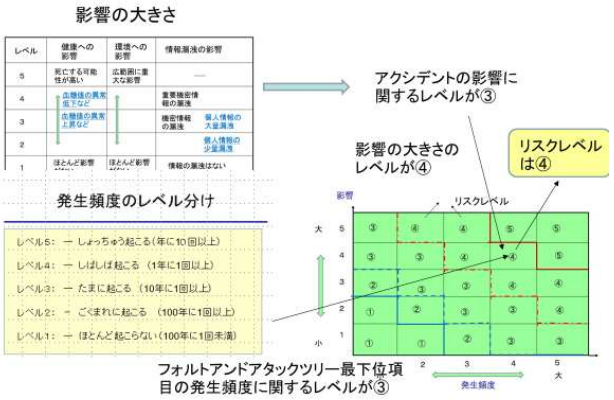


図10 リスクレベルの求め方

（d）一方，各対策案に関し，コスト効果の大きさを図 11 に示すようにしてランク付けする．

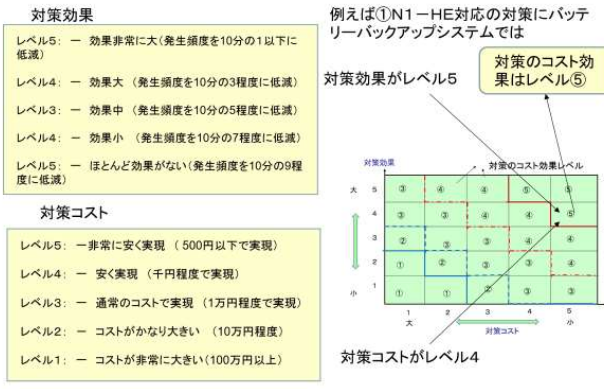


図11 対策コスト効果レベルの求め方

（e）リスクの大きさとコスト効果の大きさから，対策採用推薦でレベルを図 12 に示すように 25 段階に分けて決定する．なお，ここでは，複数の部分に効果のある対策は，加点を加えることとした．対策推薦度レベルを求めた結果の一例を表 3 に示す．

セキュリティ対策，ヒューマンエラー対策，故障対策などを統一的に比較可能になっているのがわかる．

（f）関係者に参加してもらい，対策案のリストアップ，影響の大きさ，発生確率，リスクの分類方法，コスト効果の大きさに関し，意見を言ってもらい，そのようにした場合の対策案の組み合わせ示す．これらを繰り返すことにより対策案の組み合わせに関する合意を形成する．数値を色々変えても対策案の組み合わせはあまり変わらないことから予想以上に早く合意形成できることを従来の MRC の適用から経験しているところである．

図12 リスクと対策のコスト効果の2次元図

表3 重要性の高い対策一覧

重要度21
（1）②N1-BGスマホバグ対策のためのリモートパッチシステムの導入
重要度20
（1）①N1-EN センサー電源喪失対策のためのバッテリバックアップシステムの導入
（2）②N1－EN スマホの電源断防止のためのバッテリーバックアップシステムの導入
重要度18
（1）②N1-T マルウエアなどによるスマホプログラム改ざん防止のためのアンチウイルスの導入
（2）②N1-T マルウエアなどによるスマホプログラム改ざん防止のためのホワイトリストによるプロセス自動制御システムの導入
（3）③N1-T マルウエアなどによるサーバのAPプログラムの改ざん防止のためのアンチウイルスの導入
（4） ③N1-T マルウエアなどによるサーバのAPプログラムの改ざん防止のためのホワイトリストによるプロセス自動制御システムの導入
（5） ③N1-T マルウエアなどによるサーバのAPプログラムの改ざん防止のためのリモートパッチシステムの導入
重要度16
（1）①N1-EN センサー電源喪失対策のためのバッテリ切れ予知システムの導入
（2）⑦N1-EN アクチュエータの電源喪失防止のための電源バックアップシステムの導入
重要度15 END-ENDの暗号、無線LANの暗号化、ファイル暗号、個人や機器の認証機能、DDoS対策、センサー故障検知対策など

セキュリティ対策、ヒューマンエラー対策、故障対策などを統一的に比較可能

本稿で記述した手順は，図 4 で示した対象にはうまく適用しうることを確認できた．これらの作業を効率化するために，分析の前半部（①－⑤）は IPA で開発した STAMP workbench を用いるようにし，後半部分（⑥－⑦）を SS-RAT というツール[24]を開発して適用できるようにした（図 13 参照）．

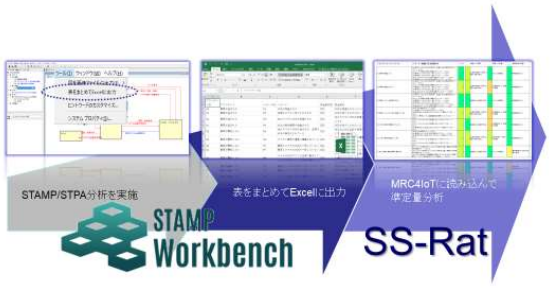


図13 分析の支援ツールの開発

これらは準定量的な分析であるが，定量的な分析方法も

開発して適用した[25][26].

この結果，準定量的分析と定量的分析の長所短所は表４に示すとおりであり，対策案のコスト効果を明確に把握したい場合は定量的方法、その必要がない場合には準定量的方法を使えばよいことが分かった．

表4 定量的方法と準定量的方法の比較と使い分け

	長所	欠点
定量的方法	いろいろな指標を追加して対策案の最適な組み合わせを求めることが可能	用いた値の説明が困難で、第三者の合意が得にくい 人間の生命の価値をお金であらわすことの抵抗
準定量的方法	値のラベル付けには第三者の合意が得やすい 人間の生命の価値をお金であらわさなくても済む	コスト効果の推定が大雑把になり、コストより効果が大きくなるかどうかわかりにくい

64

今後，医療用 IoT システムは現場に専門家がいない場合が大きいということからリモートメンテナンスが導入されてくると考えられる．医療用 IoT システムに必要な安全特性は，

従来のセキュリティ　（Security）

＋　制御対象の IoT 異常のもたらす健康や環境への影響　（Safety）

＋　リモートメンテナンスの容易性　（Maintainability）

となると考えられる．著者らは Maintainability, Security and Safety の同時実現を目指す特性を MSS コンセプト名づけ，このコンセプトに基づく医療用 IoT システム用安全対策の実現を目指している．このためのリスク評価手法については文献[27]を参照いただきたい．

４．IoT 時代のフォレンジックの課題

次に，セキュリティ技術の重要要素の 1 つであるフォレンジック技術に関し，IoT 時代のフォレンジックの課題について解説する．ここでは，フォレンジックの対象としての IoT の特徴を分析するとともに，必要な対策案を記述する [28]- [31].

IoT システムのフォレンジック対策も層別に検討していく必要がある．それぞれの層において考えられるフォレンジック対策の概要は，以下のとおりである（図 14 参照）．

（１）サービス層とフォレンジック：サービス層での直接的なフォレンジック対策はなく，サービスごとに IoT システムの構成や機能が設定され，他の層でのフォレンジック対策が異なってくると考えるべきだろう．例えば，スマートメータを含むシステムでは，IoT 機器側から電力消費量などのセンサー情報を，ネットワークを経由してプラットフォームへ通信するサービスが中心になる．また端末は，スマートメータという比較的小さなものとなる．一方，自動車がインターネットにつながったコネクティドカーのサービスの場合は，経路ガイドや速度制限制御などにおいて双方向の通信が必要となる．また，IoT 端末は自動車という比較的大きくいろいろな機能を持つものとなる．

IoT システムはこのような目的に沿ったものに設計する必要がある．あわせてサービス機能が失われたような場合においては，どの IoT 機器やネットワークやプラットフォームの障害が原因になっているかを IoT システムの構成や機能から推定し，それに基づき IoT 機器のフォレンジック対策やネットワークのフォレンジック対策，プラットフォームのフォレンジック対策を実施する必要がある．

（２）プラットフォーム層とフォレンジック：サーバ群に対するフォレンジック対策と基本的に同じであり，サーバなどに保存されているログを利用してインシデントの状態や原因を調査する．これらのプラットフォームがクラウドで実現されている場合には，クラウドフォレンジックと同様に次のような問題がある[33].

（ａ）多くのユーザーからファイルを含むサーバを扱うことがプライバシー問題を生じさせる可能性がある，

（ｂ）データを直接確認することができないので，証拠の信頼性がクラウドプロバイダーに依存する．最悪の場合は調査そのものをクラウドプロバイダーが実施してくれず証拠が集められない可能性がある．

（ｃ）物理的にデータが分散している可能性があり，データの物理的位置が分からないことが調査を遅らせる可能性がある．

したがって，加入の段階で，どのような構成，機能になっているかよく確認をし，必要な調査をやってもらえるような契約にしておく必要がある．

（３）ネットワーク層とフォレンジック：主にゲートウエイ機能に対するフォレンジックが必要となる．IoT システムにインシデントが生じた場合に，ゲートウエイにおける通信ログなどをフォレンジック分析することにより，原因となる通信がなかったかどうかを調査する．これは従来，ネットワークフォレンジックと呼んでいたものと基本的に同じであり，具体的には，従来，エッジコンピューティングのフォレンジックとかフォグコンピューティングのフォレンジックといわれていたものに相当する[34].

（４）端末とフォレンジック：従来の PC などに対するフォレンジック対策と基本的に同じであるが次に示すような特徴がある．

（ａ）端末となる機器はサービスによって自動車や家電品，医療用機器など多様である．また古い機種も残っているためベースとなる OS も多様である．

（ｂ）IoT 機器は増加の傾向にあり，2020 年には世界で 530 億個に達するといわれている．しかもこれらは固まって存在するのではなく,離れたところに分散して存在する．

したがってフォレンジックを実施するのは簡単ではない.

（ｃ）デジタルフォレンジックは EnCase や FTK のような標準的なツールが存在するのに対し，IoT フォレンジックは IoT 機器のハードやソフトに依存した個別に開発したツールで実施しており，標準的ツールが存在にない.

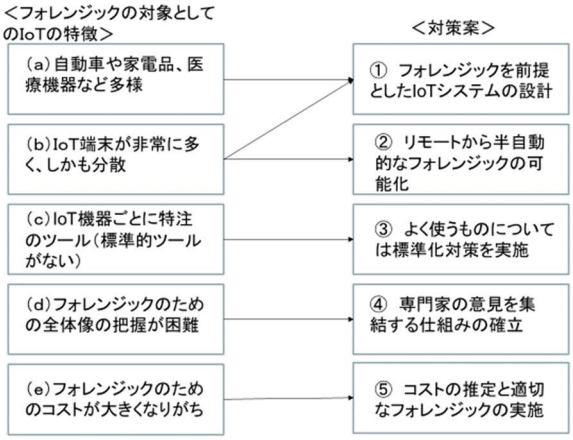


図14 IoTフォレンジックにおける対策案

（ｄ）IoT システムは，一般に複雑で，IoT 機器間の相互干渉や IoT 機器と他のローカルやリモートの機器との関係の把握が困難なのでインシデントのケースを理解し，IoT の証拠として必要となるミニマムセットを検討するのが容易でない.

（ｅ）IoT システムは一般に複雑であり，多くの端末を含むのでそのフォレンジックは，コストが予想以上にかかる可能性がある.

したがって，次のような対策が必要となる.

① IoT フォレンジックの効率的な実施のためにはフォレンジックを前提とした IoT システムに設計の段階からしておく.

② IoT 機器に対し，リモートから半自動的に実施できるようにしておくことが望ましい.

③ よく使うものについてはフォレンジックのための標準フォーマットなどを決める．また，より良いものを標準ツールとして集中的に使うようにする.

④ サービスや IoT 機器開発者，運用者，法律家などの専門家の意見を集結する仕組みを確立する．特に，法に触れないようにするとともに，証拠性を確保するためのリーガルチームとの相談は大切である.

⑤ 事前にコストなどの推定を行い必要最小限の対策を実施する．したがって集められる証拠だけを集め，無理をして集めることによって逆に証拠を壊すのを避ける.

いずれにしても，IoT の普及は，セキュリティ対策や，その一部であるフォレンジック対策の必要性を増大させると考えられる．特に，証拠保全の厳密性よりも効率的な対応を特徴とするファストフォレンジックの重要性が増大していくと考えられる. なぜなら, ファストフォレンジックは, その特徴は次の 3 点であるといわれており[28]，これらは IoT システムにおいても必要な対応だからである.

① 最小限のデータを取得して解析

② ネットワーク経由で直接調査

③ ネットワーク経由でデータを常時収集

また，IoT システムでは膨大なデータを扱うことになり，フォレンジックのためのデータも膨大になる．したがってリモートでのデータの収集機能とともに分析機能も半自動化する必要がある. この分析は手作業だけでは限界があり，機械学習などの AI（Artificial Intelligence）を使った効率的な分析が必要になっていく.

また，IoT のフォレンジック技術を確立するためには，ネットワークフォレンジックの技術とファストフォレンジックの技術を組み合わせて，それに改良を加える形で体系化する必要があると考えている.

５．おわりに

IoT システムを 4 つのレイヤー（サービスレイヤー，プラットフォームレイヤー，ネットワークレイヤー，デバイスレイヤー）にわけ，それぞれ重要性が高まると考えられるセキュリティ技術とフォレンジック技術を示した．特に，IoT 時代を迎え重要性が増しているリスク評価手法について著者らの最近の研究状況を報告した.

IoT のリスク評価方法については，引き続き研究を行い，支援ツールを改良するなどにより多くの人がリスク評価をできるようにしていきたいと考えている.

また，IoT システムのフォレンジック技術については，研究がまだ緒に就いたばかりだといえる．多くの人が研究開発に参加することを期待するとともに，著者らも研究を継続していきたい.

謝辞

本研究は，文部科学省私立大学研究ブランディング事業「グローバル IoT 時代におけるセキュアかつ高度な生体医工学拠点の形成」の一環で行ったものである.

本研究を実施する上で，IoT のリスク分析の方法に関する有益な示唆を与えてくれた情報セキュリティ大学院大学の大久保隆夫教授，東京電機大学の金子朋子氏，高橋雄志氏，林浩史氏，早川拓郎氏に深く感謝申し上げる.

また, 一般社団法人セキュア IoT プラットフォーム協議会のメンバーには IoT システムのレイヤーリングに関する示唆をいただいた．記して感謝申し上げる.

関連文献

[1] 総務省，経済産業省「IoT セキュリティガイドライン」 平成 28 年 7 月
http://www.soumu.go.jp/main_content/000428393.pdf

[2] 総務省 「IoT セキュリティ総合対策」平成 29 年 http://www.soumu.go.jp/main_content/000510701.pdf

[3] Kenji Mori, Yoichiro Ueno, Shuichi Suzuki, Kazuo Ichihara, “Study of a Secure Backup Network Mechanism for Disaster Recovery and Practical Network Applications” International Journal on Advances in Networks and Services,vol3 no1&2,year2010,http://www.iariajournals.org/networks_and_services/

[4] Hiroyuki Kimiyama ; NaokiYonezaki ; Tomoaki Tsutsumi ; Kaori Sano ;Hirofumi Yamaki ; Yoichiro Ueno ; Ryoichi Sasaki, Hiroshi Kobayashi, “ Autonomous and distributed internet security (AIS) infrastructure for safe internet” 2017 8th International Conference on the Network of the Future (NOF)

[5] 佐々木良一, 日高悠, 守谷隆史, 谷山充洋, 矢島敬士, 八重樫清美, 川島泰正, 吉浦裕 「多重リスクコミュニケータの開発と適用」, 情報処理学会論文誌, Vol.49, No.9, pp.3180-3190, 2008

[6] Ryoichi Sasaki, “Consideration on Risk Communication for IT Systems and Development of Support Systems” Journal of Information Processing, Vo.20 (2012) -4, pp814-822 https://www.jstage.jst.go.jp/browse/ipsjjip/

[7] 谷山充洋, 日高悠, 荒井正人, 甲斐 賢, 伊川宏美, 矢島敬士, 佐々木良一「多重リスクコミュニケータの企業向け個人情報漏洩問題への適用」日本セキュリティ・マネジメント学会誌, VOL.23,No.2, pp34-51,2007

[8] 守谷隆史, 千葉寛之, 佐々木良一 「内部統制のための多リスク・多関与者を考慮した費用対効果の評価法の提案と適用」, 日本セキュリティ・マネジメント学会学会誌, 第 22 巻第 3 号,pp.3-14, 2008

[9] 相原遼, 石井亮平, 佐々木良一「イベントツリーとディフェンスツリーを併用した標的型攻撃に対するリスク分析手法の提案と適用」情報処理学会論文誌 Vol.５９, No.3, pp1082-1094, 2017

[10] Ichiro Matsunaga, Ryoichi Sasaki,” Development and Evaluation of a Continuity Operation Plan Support System for an Information Technology System” International Journal of Cyber-Security and Digital Forensics (IJCSDF) 4(2): 327-338, 2015

[11] 梅原悠平, 安藤駿, 佐々木良一「IT リスクの動的特性を考慮した対策案組み合わせ最適化技術の提案と評価」日本セキュリティ・マネジメント学会誌, 30 巻第 3 号 2017 年 3 月 pp11-21

[12] Shota Fukushima and Ryoichi Sasaki, “Proposal and Evaluation of Method for Establishing Consensus on Combination of Measures Based on Cybersecurity Framework”, International Journal of Cyber-Security and Digital Forensics (IJCSDF) 5(3): 155-165, 2016

[13] 佐々木良一, 杉本尚子, 矢島敬士, 増田英孝, 吉浦 裕, 鮫島正樹, 船橋誠壽「ITリスク対策に関する社会的合意形成支援システム Social-MRC の開発構想」情報処理学会論文誌 Vol.52, No.9, pp 2562-2574, 2011

[14] Ryoichi Sasaki, Shoko Sugimoto, Hiroshi Yajima, Hidetaka Masuda ,Hiroshi Yoshiura, Masaki Samejima” Proposal for Social-MRC: Social Consensus Formation Support System Concerning IT Risk Countermeasures” International Journal of Information Processing and Management Vol.2, No.2 pp48-58, 2011

[15] 大河原優, 高草木一成, 矢島敬士, 増田英孝, 小林哲郎, 佐々木良一「IT リスク対策に関する社会的合意形成支援システム Social-MRC の情報フィルタリング問題への試摘用と考察」日本セキュリティ・マネジメント学会誌 25 巻第 3 号 pp15-23, 2012

[16] 安藤駿, 猪瀬裕介, 増田英孝, 佐々木良一「マイクロブログ中のリスクコミュニケーションに関する有益な意見を自動的に抽出する手法の提案と評価」情報処理学会論文誌, Vol.55, No.9, pp2149-2158, 2014

[17] Masaki Samejima, Ryoichi Sasaki,” Chance-Constrained Programming Method of IT Risk Countermeasures for Social Consensus Making” IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS: SYSTEMS, VOL. 45, NO. 5, MAY 2015 pp725-733

[18] 佐々木良一「IoT 時代のリスクコミュニケーション支援ツールの構想」情報処理学会 DICOMO2018

[19] 例えば「はじめての STAMP/STPA ～システム思考に基づく新しい安全性解析手法～」2016 https://www.ipa.go.jp/sec/reports/20160428.html

[20]「医療機器における情報セキュリティに関する調査」2014 IPA https://www.ipa.go.jp/files/000038223.pdf

[21] 「脅威分析モデル STRIDE」 https://hanakutoman.com/threat-modeling-stride/

[22] 米国国立標準技術研究所 (IPA 翻訳)「重要インフラのサイバーセキュリティを向上させるためのフレームワーク」2014 年 2 月 https://www.ipa.go.jp/files/000038957.pdf

[23] IPA「制御システムのセキュリティ分析ガイド」https://www.ipa.go.jp/files/000061925.pdf

[24] 林浩史, 高橋雄志, 金子朋子, 早川拓郎, 佐々木良一「IoT システム向けリスク評価方式と支援ツール SS-Rat の開発」情報処理学会 CSS2018

[25] 早川 拓郎, 佐々木 良一, 金子 朋子, 髙橋 雄志, 大久保隆夫, 猪俣敦夫「IoT を含む医療機器システムのセキュリティ/セーフティ評価手法の提案と適用」情報処理学会 DICOMO2018

[26] Takuo Hayakawa, Ryoichi Sasaki, Hiroshi Hayashi, Yuji Takahashi, Tomoko Kaneko, Takao Okubo “Proposal and Application of Security/Safety Evaluation Method for Medical Device System that Includes IoT”. ICNCC 2018: 157-164

[27] 佐々木良一他「メンテナビリティ・セーフティ・セキュリティを考慮したリスク評価手法の提案と医療用 IoT システムへの適用」日本セキュリティ・マネジメント学会全国大会 2019（予定）

[28] 伊藤耕介「フォレンジックとは？インシデントの原因調査手法を解説！」https://www.secure-sketch.com/blog/fast-forensic 2018 年 11 月 7 日の記事

[29] Jigang Liu, “IoT Forensics – Issues, Strategies, and

Challenges” https://digitalforensic.jp/wp-content/uploads/2016/03/community-12-2015-07.pdf
[30] R.C.Hegarty, D.J.Lamb and A.Attwood “Digital evidence challenges in the internet of things” Proceedings of the Ninth International Workshop on Digital Forensics and Incident Analysis, pp163-172, 2014
[31] Saad Alabdulsalam, Kevin Schaefer, Tahar Kechadi, Nhien-An Le-Khac,”Internet of Things Forensics – Challenges and a Case Study”, Digital Forensics 2018: Advances in Digital Forensics XIV pp 35-48
[33] 佐々木良一編著「デジタル・フォレンジックの基礎と実践」東京電機大学出版局，2017
[34] Yifan Wang , Tetsutaro Uehara , Ryoichi Sasaki, ” Fog Computing: Issues and Challenges in Security and Forensics” 2015 IEEE 39th Annual Computer Software and Applications Conference