IoT システムにおける送信デバイス・データの真正性確保に関する考察

Consideration about the authenticity of transmitting devices and data in IoT systems

才所 敏明[†‡]　　辻井 重男[†]

Toshiaki Saisho　Shigeo Tsujii

1. IoT の課題

IoT 機器・技術の発展、IoT システムの普及に伴い、従来は収集し得なかった様々のデータの収集が可能となり、またビッグデータおよび AI によるデータ利活用技術の発展と連動し、我が国は IoT で収集されるデータが社会活動や国民生活を支える社会、データドリブン社会へと移行しつつある。

一方、IoT 機器・システムの活用促進、データドリブン社会への移行は新たなリスクも発生し、既に多くの事故・事件が発生している。このような事故・事件を未然に防ぐ、あるいは早期に収拾させるための、IoT 機器・システムに求められるセキュリティ対策は以下の通り大きく 5 つに分類される[1]。

①被害者にならないための IoT 機器・システムの保護対策
②IoT 機器・システムが送信・収集するデータの保護対策
③加害者とならないための IoT 機器・システムの保護対策
④IoT 機器・システムの適切な状態を維持するための対策
⑤被害・加害を早期に収拾させるための対策

IoT、ビッグデータ、AI のそれぞれの発展、相互連携の推進に伴う安心・安全なデータドリブン社会を目指すには、IoT 機器・システムのセキュリティ面の対策を強化する必要があろう。

2. IoT システムにおける真正性保証

セキュア IoT プラットフォーム協議会および中央大学研究開発機構は、このような IoT 機器・システムに求められるセキュリティ対策の中で特に②に着目し、総務省の重点領域型研究開発推進事業（SCOPE）へ「IoT デバイス認証基盤の構築と新 AI 手法による表情認識の医療介護への応用についての研究開発」（以下、IoTAI-PJ と略記）を提案、昨年度採択され、2018 年度より 2020 年度までの予定で現在実施中である IoTAI-PJ では、「IoT、Big Data, AI が普及する中で、デバイス層、ネットワーク層、データ管理層、情報サービス層の 4 階層に亘って、真贋判定・真正性保証の基盤的重要性を理念として、上記 4 層の総合的連結性を考慮しつつ、各層における重要性の高い課題を選別し、真正性保証技術を提案」することを目指している。

具体的には、図 1 のような構成を想定し、センサにおける真正性保証をデバイス層の課題として、アグリゲータにおける真正性保証をデータ管理層の課題として、アナライザにおける真正性保証を情報サービス層の課題として、更には層間のデータ転送における真正性保証をネットワーク層の課題として、研究活動を展開中である。

本稿では以下、筆者らが担当するネットワーク層の課題として、層間のデータ転送における送信デバイス・データの真正性確保に関する課題・目標および考察結果等を報告する。

† セキュア IoT プラットフォーム協議会
Secure IoT Platform Consortium
‡ Mail:toshiaki.saisho@advanced-it.co.jp

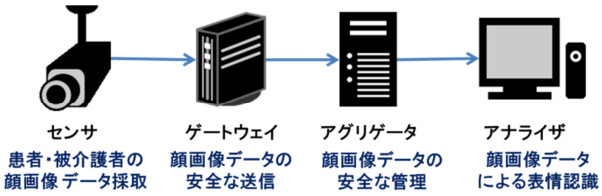

図 1　IoTAI-PJ の想定構成

3. ネットワーク層の課題・目標

IoTAI-PJ では、ネットワーク層の課題である送信デバイス・データの真正性確保を実現する方策として、筆者らの研究成果である SSMAX（拡張 S/MIME） コンセプトに基づき、OSI 参照モデルのアプリケーション層における、送信デバイス・データの真正性確保のための仕組み（SSDTF：Secure and Safe Data Transfer Framework）の提案を、目標としている。

4. 安心・安全な電子メール基盤 SSMAX

SSMAX（Secure and Safe eMAil eXchange framework）は、電子メールの犯罪（標的型攻撃メールやフィッシングメール）が多発する中、より安心・安全な電子メールの利用環境を目指し、2016 年、組織暗号の実業務への適用可能性検討の一環として着手、2018 年の情報処理学会論文誌に SSMAX のコンセプトから具体的実現構想まとめている[2]。なお、組織暗号は、2013 年～2015 年、中央大学研究開発機構が受託した平成 25 年度 SCOPE 研究課題：「組織間機密通信のための公開鍵システムの研究開発」の成果物の一つである[3]。

SSMAX の主要な機能の一つは、メール送信者の特定・追跡が可能であることである。その結果、悪意のあるメールの送信者は容易に特定・追跡でき、悪意のある電子メールの流通・氾濫が抑止可能となる。

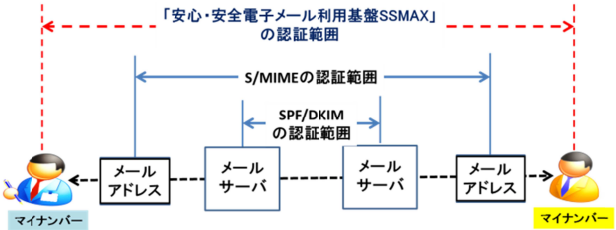

図 2　SSMAX におけるメール送信者の特定・追跡

一方、電子メール送信者の匿名性もまた個人間の活発なコミュニケーションを促すには重要な機能である。一般に、特定・追跡性と匿名性の両立は難しいが、SSMAX ではそれぞれが必要な状況（レイヤ）に応じ機能する仕組みを考案している。

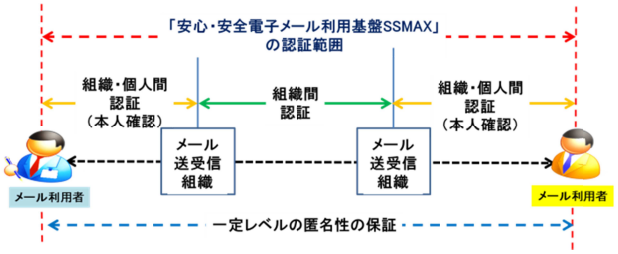

図 3　SSMAX における匿名性と特定・追跡性の両立

5. SSDTF の実現方式に関する考察

SSDTF は送信デバイス・データの真正性確保を実現する仕組みを目指している。送信デバイスの真正性の確認は、データを送信してきたデバイスが想定したデバイスであることを確認することであり、送信データの真正性の確認は、受信したデータが送信デバイスにより送信されたデータであることを確認することである。同様の機能は、SSMAX では電子メール送信者・送信メール内容の特定・追跡性として組み込まれており、SSDTF においても、同様の方式にての実現を目指している。

なお、IoT システムにおいても、IoT 機器の匿名性は重要である。本稿では、IoT 機器の匿名性を IoT 機器の攻撃に利用される情報を隠ぺいできる性質とし、具体的には IoT 機器の物理的位置を特定可能な GPS 情報等、IoT 機器の論理的位置を特定可能な IP アドレス等、その他、IoT 機器の脆弱性を特定可能な機器製造メーカ・型番・OS・ミドルウェア等のシステム情報等を対象としている。

上記の、匿名性と特定・追跡性の両立には、SSMAX にて採用した連結可能匿名化により実現を想定している。

5.1 SSDTF における匿名性に関する考察

送信デバイスの匿名性は、セキュリティ維持に必要な送信デバイスの情報の、IoT システム運用組織による隠ぺいにより実現する。契約の関係でリスクを承知で顧客（データ利活用事業者）へ提供せざるを得ない場合もあろうが、原則、IoT 機器の攻撃に利用されるリスクのある情報は内部管理に留めることが重要である。IoT システム内で使用される IoT 機器の内部管理コードは IoT 機器の機微情報の管理にも利用されることが多く、IoT システム外へデータを提供する場合は、内部管理コードが外部に漏れないよう外部管理コードへ変換することが望ましい（図 4）。

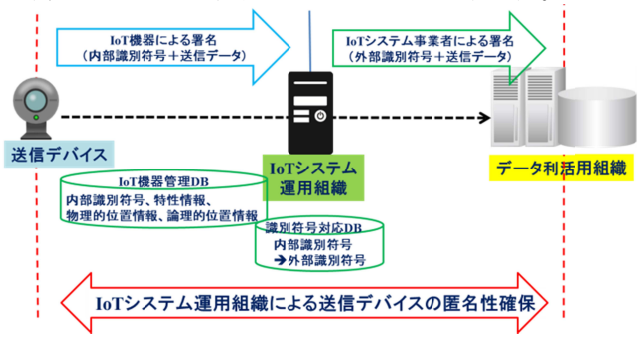

図 4　送信デバイスの匿名性を確保する仕組み

5.2 SSDTF の特定・追跡性に関する考察

送信されたデータに異常があった場合は、IoT システム運用組織は直ちに送信デバイスを特定し、原因を究明し是正措置を取る必要がある。万一、データ異常が IoT システム外のデータ利活用事業者側で発見された場合、通知を受けた IoT システム運用事業者は異常データに含まれる送信デバイスの外部管理コードを内部管理コードへ変換し、送信デバイスの機微情報を把握しつつ原因追究にあたる必要がある（図 5）。

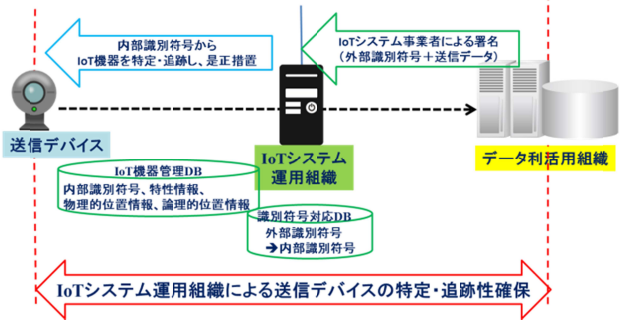

図 5　送信デバイスの特定・追跡性を実現する仕組み

6. SSDTF の実装方式に関する考察

IoTAI-PJ においては、SSDTF の具体的実装は対象外のため、性能面等の実装の実用性の詳細な検討は行わないが、SSDTF の実装可能性を示すための実装方式の検討は行う必要がある。そこで、既存の主要な IoT 向けデータ転送プロトコルのセキュリティ機能を調査・分析し、SSDTF に必要な機能の組込み方式を検討する予定である。

現在、主要なプロトコルの一つ MQTT のセキュリティ機能の調査・分析し、SSDTF の機能組込み方式を検討中である。MQTT のセキュリティは、OSI 参照モデルのネットワーク層については TLS の利用が想定され、アプリケーション層については機器 ID/パスワードによる認証機能のみが用意されている。MQTT の仕様には一定の拡張機能が用意されており、この拡張機能を利用し SSDTF の機能が実現できるかどうか、今後調査する予定である。

謝辞

本研究は，総務省「戦略的情報通信研究開発推進事業 SCOPE（受付番号：181603006）」にて、セキュア IoT プラットフォーム協議会及び中央大学のチームが採択を受けた「IoT デバイス認証基盤の構築と新 AI 手法による表情認識の医療介護への応用についての研究開発」の活動の一環として行ったものである。

参考文献

[1]才所 敏明，辻井 重男，”安心・安全な IoT システム(SSIoT)に関する考察”, CSEC81 (2018).
[2] 才所 敏明，五太 子政史，辻井 重男，”「安心・安全電子メール利用基盤（SSMAX）」, 情報処理学会論文誌 59 巻 9 月号(2018).
[3] 才所敏明，近藤健，庄司陽彦，五太子政史，辻井重男，”組織暗号の構成と社会的実装－個人情報の安全な利活用を目指して－”, 情報処理学会誌論文誌 56 巻 9 月号(2016)