最新の研究活動紹介

インターネットにおける匿名性と特定・追跡性

2018年10月1日
才所敏明（（株）IT企画）
toshiaki.saisho@advanced-it.co.jp
セキュアIoTプラットフォーム協議会
中央大学研究開発機構

 1

ご説明項目一覧

1. 問題提起（研究に着手した背景）
   - ＊インターネットの現状・課題
   - ＊諸悪の根源はインターネットの匿名性？
   - ＊安心・安全なインターネット社会に向けて
   - ＊Differential Traceability
2. 研究活動紹介：IoPを対象
   - ＊安心・安全な電子メール利用基盤（SSMAX）
3. 研究活動紹介：IoTを対象
   - ＊安心・安全なIoTシステムフレームワーク（SSIoT）
   - ＊IoTデバイス間通信の認証方式の研究
     （平成30年度SCOPE研究課題：「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」研究活動の一環）

 2

1．問題提起

インターネットの課題

＊日本のインターネットの歴史は1984年に始まり、
未だ35年余りだが、産業界の様々の活動、
国民の日々の生活に欠かせないものに。

＊TCP/IPが発表されインターネットという言葉がはじめて使われた
1974年当時は、インターネット利用者が他の利用者を
攻撃することは想定されていなかった。

＊ICT技術の発展は留まるところを知らず、
社会はますますインターネットへ依存を強めるのは必至。
インターネット経由の様々の攻撃（悪意）もそれに応じ増大し、
社会の被害も甚大化することが想定される。
標的型攻撃、フィッシング攻撃、誹謗・中傷/いじめ、
フェイクニュース、DOS/DDOS攻撃等々

 3

1．問題提起

諸悪の根源
インターネットの匿名性？

匿名性の課題
標的型攻撃/フィッシングメール→送信者の匿名性
誹謗・中傷・いじめ→発信者/発言者の匿名性
DOS/DDOS攻撃→攻撃サイト/機器の匿名性
暗号通貨によるマネーロンダリング→送金者/受領者の匿名性

➔ インターネットは犯罪者（悪意のある人）に優しいシステム！

匿名性の重要性
プライバシー情報の拡散
→自由な発言にブレーキ（インターネット活用にも？）
発言者の容易な同定
→コミュニティに応じた人物を演じ楽しむ権利の剥奪

 4

1．問題提起

安心・安全なインターネット社会へ

インターネット経由の犯罪（悪意）をより確実に排除できるためには
セキュリティ機能の強化は避けて通れない！

一定レベルの匿名性は必要だが、
社会的に許されないインターネットの利用に対しては、
利用者の容易な特定・追跡を可能とすべき！

インターネット利用における
一定レベルの匿名性と特定・追跡性の両立が、
安心・安全なインターネット社会の実現に不可欠！

1．問題提起

Differential Traceability

ACMの8月号にインターネットの父の一人
Vinton Gray Cerf氏の、”Traceability”の記事で提案された概念。

ここ数年、インターネットの利用に関し報告者が主張してきた、
「特定・追跡性が保証されない匿名性は有害」
「匿名性と特定・追跡性の両立が不可欠」
に相通じる概念と理解。

Vinton G. Cerf氏は、「Differential Traceability」の現実世界での例として、「自動車のナンバープレートに記載されている記号・番号は匿名性があるが、警察等の正式の要請により所有者情報が開示される」を提示し、インターネットの世界でも、同様の匿名性と特定・追跡性の両立が必要なのでは、という問題を提起したもの。
今後、国際の場でも議論が活発化することを期待。

2．研究活動紹介・IoP：SSMAX

電子メールにおける匿名性と特定・追跡性の両立

安心・安全な電子メール利用基盤（SSMAX）

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

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。

インターネットメールの活用を推進してきた一員として、
電子メールのセキュリティ課題を選定

1984年、日本でインターネットが稼働（JUNET）、その後すぐに産業界での活用を検討するグループ（Inet Club）が結成され東芝も参加、インターネットメールの有用性の検証とそれを踏まえての普及活動を展開。

電子メールは、産業界のみならず国民生活の基礎的・共通的コミュニケーションの基盤に成長したが、最近の電子メールを利用した様々の犯罪・悪意の氾濫への対応の必要性を痛感。

標的型攻撃メール、フィッシングメール、誹謗・中傷・いじめメール、フェイクメール、スパムメール等々

2．研究活動紹介・IoP：SSMAX

電子メールを利用した犯罪（悪意）への対策が不十分・非効率な現状

技術対策（下記の推奨技術導入による対策）

SPF（ Sender Policy Framework）普及率94.74%

DKIM（DomainKeys Identified Mail）普及率54.82%

➔かなりの普及率ではあるが、
犯罪目的や悪意のあるメールの氾濫は止まらず、
特に標的型攻撃メール対策として、人的対策が広く展開されている。

人的対策（電子メール受信者の確認・検査能力向上教育・訓練による対策）

教育・訓練された組織でも開封率は10％程度発生 ➔効果は限定的

検査・確認作業時間15分/日（平均受信メール数40通/日）の場合
公務員の人件費1800億/年（一般職約120万人を対象に試算）

➔産業界を含めると、我が国の人件費負担（見えないコスト）は
1兆円/年に迫るか。 ➔より効果的な技術対策の必要性！

情報セキュリティ10大脅威2018（IPA発表）

昨年順位	個人	順位	組織	昨年順位
1位	インターネットバンキングやクレジットカード情報等の不正利用	1位	標的型攻撃による被害	1位
2位	ランサムウェアによる被害	2位	ランサムウェアによる被害	2位
7位	ネット上の誹謗・中傷	3位	ビジネスメール詐欺による被害	ランク外
3位	スマートフォンやスマートフォンアプリを狙った攻撃	4位	脆弱性対策情報の公開に伴う悪用増加	ランク外
4位	ウェブサービスへの不正ログイン	5位	脅威に対応するためのセキュリティ人材の不足	ランク外
6位	ウェブサービスからの個人情報の窃取	6位	ウェブサービスからの個人情報の窃取	3位
8位	情報モラル欠如に伴う犯罪の低年齢化	7位	IoT機器の脆弱性の顕在化	8位
5位	ワンクリック請求等の不当請求	8位	内部不正による情報漏えい	5位
10位	IoT機器の不適切な管理	9位	サービス妨害攻撃によるサービスの停止	4位
ランク外	偽警告によるインターネット詐欺	10位	犯罪のビジネス化（アンダーグラウンドサービス）	9位

2．研究活動紹介・IoP：SSMAX

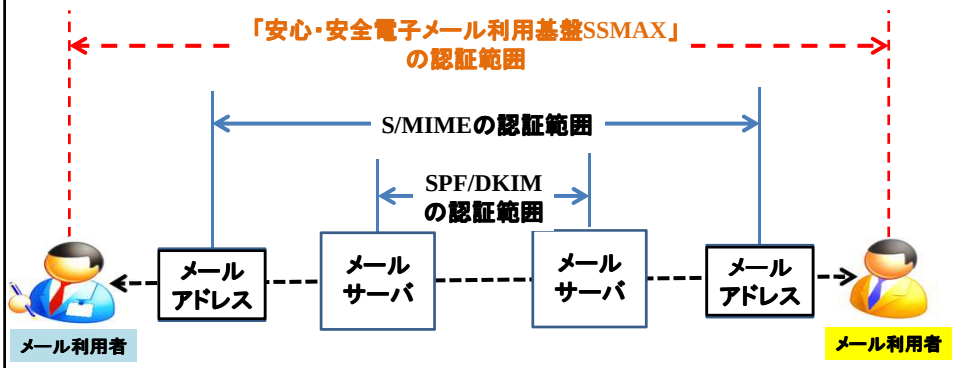
安全な電子メール利用基盤SSMAX

（Secure and Safe eMAil eXchange framework）

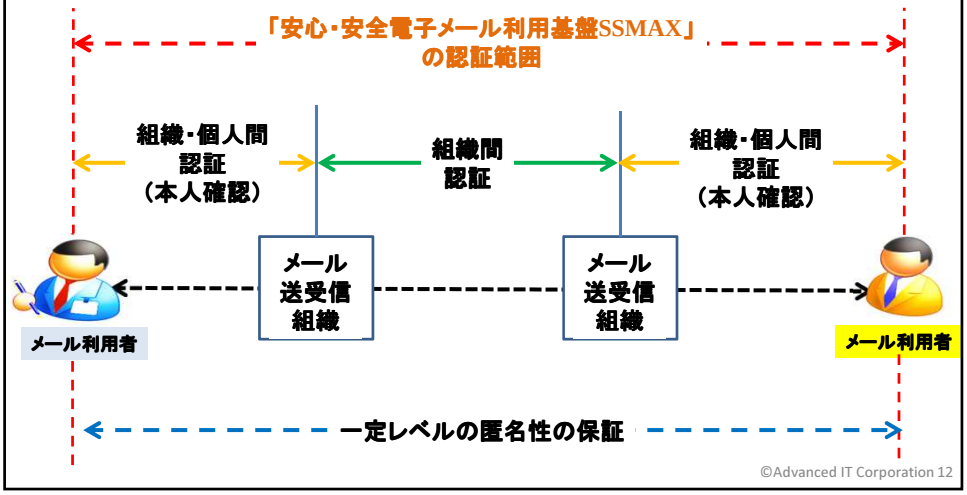
（1）送信者の特定・追跡が可能な電子メール利用基盤
悪意のある電子メールの流通・氾濫を抑止可能！

（2）送信情報の保護が可能な電子メール利用基盤
個人情報・秘密情報の送信にも利用可能！

SSMAX
メール送信者の特定・追跡



SSMAX
匿名性と特定・追跡性の両立



２．研究活動紹介・IoP：SSMAX

安心・安全な電子メール利用基盤（SSMAX）

＊2016年より4件の学会発表実施、段階的にSSMAXの構想を具体化。

＊SSMAXの技術仕様、他の対策に対するSSMAXの優位性、
SSMAXの社会実装上の課題と克服方策等を下記論文に掲載。

情報処理学会論文誌 2018年9月号（ Vol.59，No,9），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）」悪意のあるメールの根絶とメール内容の確実な保護を目指して“（2018年9月15日発行）

＊今後は、SSMAXの試作・検証、実証実験等の機会をとらえ、
我が国が世界に先駆け、安心・安全な電子メール利用基盤を構築・整備し、
我が国の産業や国民の生活を支える安定した
基礎的・共通的コミュニケーション基盤の確立を目指したい。

＊「世界一安全な日本」を目指す我が国は，
世界に先駆け「安心・安全電子メール利用基盤（SSMAX）」を実現し、
世界一安全なサイバー空間の実現においても世界を先導する役割を
担うべきであろう。

３．研究活動紹介・IoT：SSIoT

IoTシステムにおける匿名性と特定・追跡性の両立

安心・安全なIoTシステムフレームワークSSIoT

IoTの急増（ガートナー報告より）

2016年・64億台，2017年・84億台、2020年・204億台程度のIoT接続

2017年末には、世界の人口（75億人程度）を超えるIoT接続

IoTサイバー事故・事件の多発

2016年9月、史上最大級のIoT利用DDOS事件（KrebsOnSecurity）

IoT向けマルウェア「Mirai」：脆弱なIoT機器を奴隷化し，奴隷化したIoT機器には
脆弱なIoT機器の探索作業を行わせ，急速にボットネットを巨大化
2016年10月に「Mirai」のソースがインターネット上に公開

2017年10月、新たなマルウェア（IoTroop、IoT_reaper）による
大規模なボットネットが構築されつつあるとの警告

2018年1月、金融セクター向けのDDOS攻撃が発生、
13000のハイジャックされたIoTが利用された
既に100万以上の組織のIoTが感染、との推測も

安心・安全なIoTシステムフレームワークSSIoT（Secure and Safe IoT System Framework）

2017年に研究着手

2018年5月、情報処理学会第81回CSEC研究会にて発表

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“

本発表では、SSIoTとして期待される機能の定義および活用可能な既存技術を調査の上、各機能実現における基本的な考え方を提示

SSIoTで実現すべき機能

- **＊IoT機器の保護（被害者にならないために）**
- **＊IoT機器が送信するデータの保護**
- **＊IoT機器の保護（加害者にならないために）**
- **＊IoT機器の適切な状態を維持するために**
- **＊被害・加害を早期に収拾させるために**

機能実現に活用が可能な既存技術

- **＊PLA（パケットのIPアドレスへのIoTデバイスの署名付与によるパケットの認証）**
- **＊HIP（IoTデバイスのIDとIoTデバイスの署名付与によるホストの認証）**
- **＊組織暗号（IoTデバイスが収集した情報の安全な送信）**

IoT機器の匿名性と特定・追跡性

特定・追跡性の必要性：

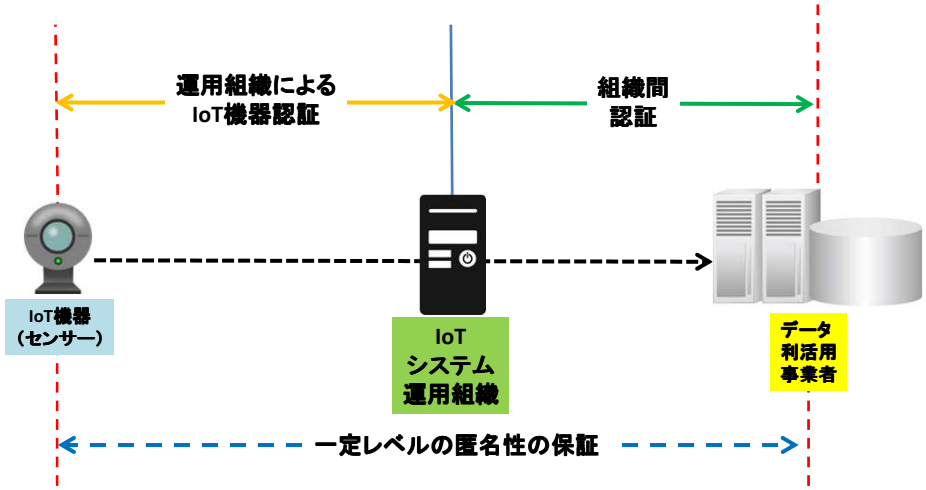
被害拡大防止、早期正常化のための
問題のあるデータ送信IoT機器への早期対応

匿名性の必要性：

サイバー攻撃等のリスク低減のための
物理的・論理的アドレス、その他の機微情報の秘匿

3．研究活動紹介・IoT：SSIoT

SSIoT
匿名性と特定・追跡性の両立



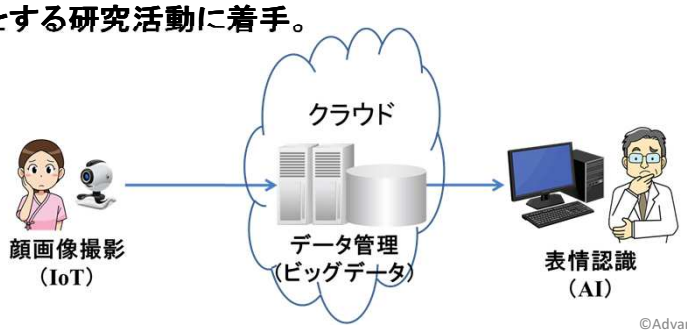
OSI参照モデルにおける
活用想定技術の適用想定階層

階層	名称	活用想定技術
7	アプリケーション層	SSMAX（組織暗号、他）
6	プレゼンテーション層	
5	セッション層	HIP（Host Identity Protocol） PLA（Packet Level Authentication）
4	トランスポート層	
3	ネットワーク層	
2	データリンク層	
1	物理層	

IoTデバイス間通信の認証方式の研究

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にて平成30年度SCOPE研究「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」を受託。

本研究の一環として、「IoTシステムにおける送信者・送信機器・送信内容の真正性確保のために、拡張S/MIME（SSMAX）のコンセプトに基づくIoTシステム向けの認証方式の提案およびその普及方策の策定」を目標とする研究活動に着手。



IoTデバイス間通信の認証方式

2018年7月、夏のセキュリティシンポジューム in 札幌（CSEC82：第82回コンピュータセキュリティ研究会）にて、発表

才所敏明，辻井重男：“インターネット依存社会における情報送信者・情報送信機器の匿名性と特定・追跡性”

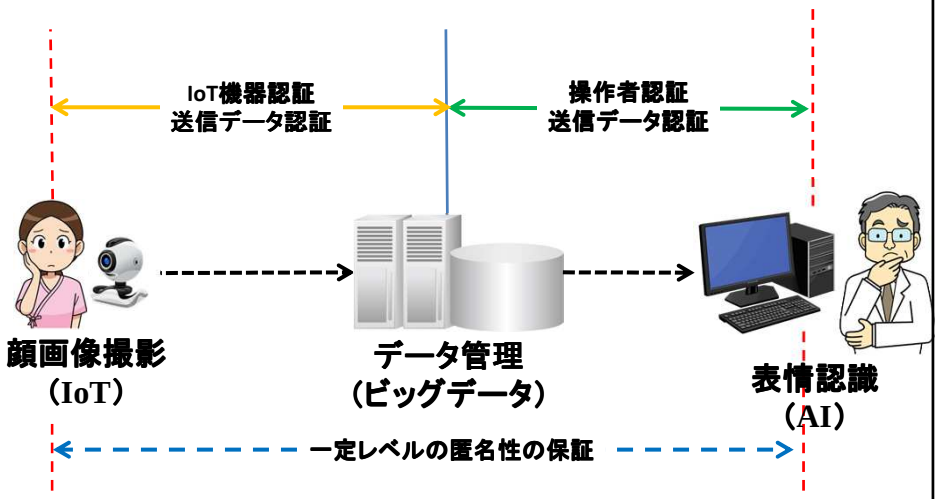
発表概要

＊人が情報を送信する場合の匿名性と特定・追跡性の両立の必要性、およびSSMAXで採用した「連結可能匿名化」による実現方策を説明

＊IoT機器が情報を送信する場合の匿名性と特定・追跡性の両立の必要性、およびSSMAXと同等の「連結可能匿名化」による実現の可能性を提示

3．研究活動紹介・IoT：デバイス間通信の認証方式

IoTデバイス間通信の認証方式



4．おわりに

おわりに

（1）社会実装を目指したシステムセキュリティ技術の研究開発を推進

（2）社会のインターネット依存が強まる中、
インターネットのセキュリティ課題に着目

（3）インターネットを利用した犯罪（悪意）の氾濫は、
その強すぎる「匿名性」にある、との認識の元、
インターネットにおける「特定・追跡性」の実現方式、
「一定レベルの匿名性」との両立方式に関する課題を研究対象

今回の、IoP、IoTに関するテーマの他、仮想通貨・ブロックチェーンにおける「匿名性」および「特定・追跡性」の実現方式、その両立方式も研究対象

本発表で紹介した研究活動
　「IoTデバイス間通信の認証方式の研究」は、

総務省「戦略的情報通信研究開発推進事業（SCOPE）」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」

の一環として実施中のものである。

終

