第82回CSEC研究会

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

2018年7月25日
中央大学研究開発機構
才所敏明　辻井重男

本発表の構成

1. はじめに
2. 人が情報を送信する場合の匿名性と特定・追跡性
3. 機器（IoT機器）が情報を送信する場合の匿名性と特定・追跡性
4. 連結可能匿名化による匿名性と特定・追跡性の両立方式
5. s-匿名性（層匿名性）についての考察
6. 終りに

1. はじめに

インターネットの歴史は35年余り
- **1984年JUNET　1992年商用サービス**

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外
- **通信内容の真正性の確保や通信相手の厳密な確認などのセキュリティ機能は具備されていない**

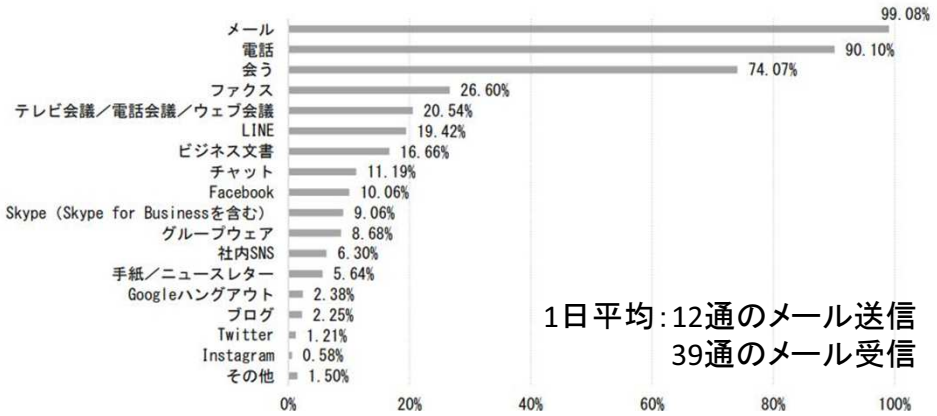
利用者は匿名性に支えられたある種の文化を享受
- **匿名性の制限には抵抗**

社会がますますインターネットへ依存
- **インターネット経由の様々の攻撃もそれに応じ増大**
- **社会の被害も甚大化することが想定**

インターネット経由の攻撃をより確実に排除できる
セキュリティ機能の導入は避けることはできない

2. 人が情報を送信する場合の匿名性と特定・追跡性

仕事で使っている主なコミュニケーション手段（複数回答可、最大５つまで）　（n=2,395）



1日平均：12通のメール送信
39通のメール受信

電子メールがネット経由の通信手段の主役

「ビジネスメール実態調査 2017」（2017年6月2日に一般社団法人日本ビジネスメール協会発表）

電子メールがネット経由の通信手段の主役だからこそ

標的型攻撃の初期潜入には ほとんど電子メールが利用されている

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

5

標的型メール攻撃対策

技術的対策

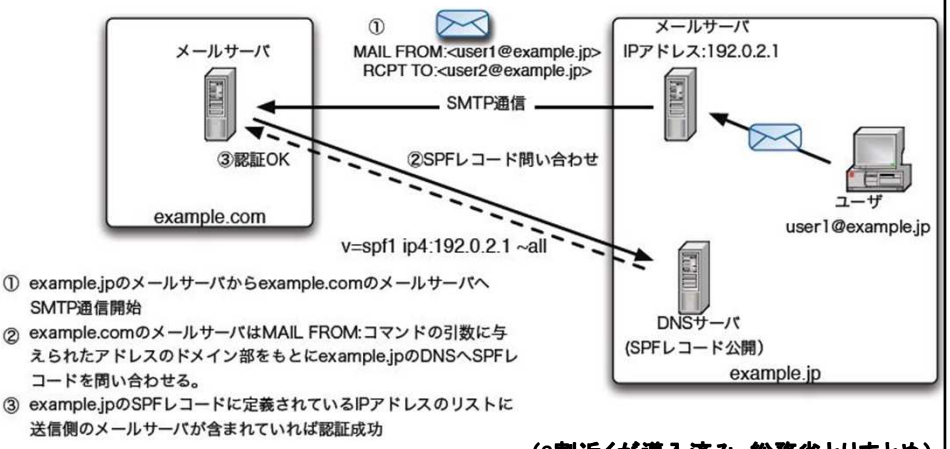
標的型メールかどうかをメールシステムにて確認し、直接排除またはメール受信者への注意喚起等により、標的型攻撃メールの被害回避を目指した対策

人的対策

教育・訓練により、メール受信者（社員・職員）の標的型攻撃メールを見極める能力を高め、標的型メールかどうかを受信者本人に確認させ、標的型攻撃メールの被害回避を目指した対策

6

現在の技術的対策（1）
SPF（Sender Policy Framework）

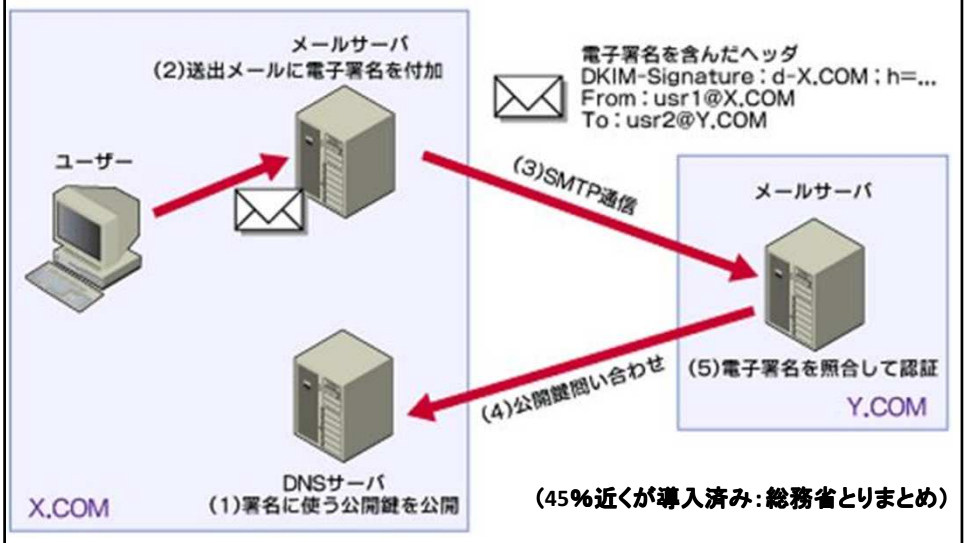


① example.jpのメールサーバからexample.comのメールサーバへSMTP通信開始
② example.comのメールサーバはMAIL FROM:コマンドの引数に与えられたアドレスのドメイン部をもとにexample.jpのDNSへSPFレコードを問い合わせる。
③ example.jpのSPFレコードに定義されているIPアドレスのリストに送信側のメールサーバが含まれていれば認証成功

（9割近くが導入済み：総務省とりまとめ）

http://salt。iajapan。org/wpmu/anti_spam/admin/tech/explanation/spf/#30

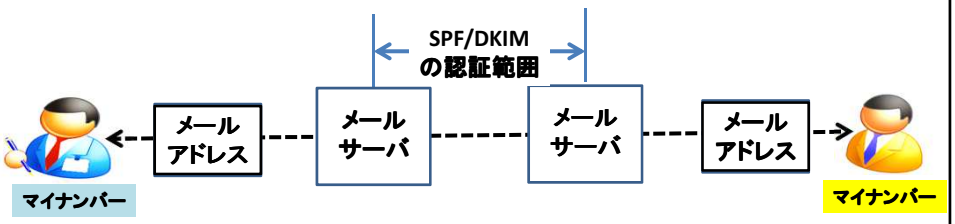
現在の技術的対策（2）
DKIM（Domainkeys Identified Mail ）



（45%近くが導入済み：総務省とりまとめ）

http://www。atmarkit。co。jp/ait/articles/0602/16/news114。html

現在の技術的対策の課題（2）



なりすましメールを防ぐには、
メール送信者の認証が必要！

人的対策の課題
膨大な見えないコスト

[費用試算の前提]①39通のメール受信（1日平均）
②標的型攻撃メールかどうかの判断ため15分程度/1日必要

[公務員のみを対象とした費用試算]
国家公務員　60万人（一般職34万人）　給与41万円
地方公務員　280万人（一般職90万人）　給与38万円
1か月あたりの見えない人的対策費用　約150億/月　（年間1800億！）
≒34万人＊41万円＊（15分/8時間）　・・・　国家公務員
＋90万人＊38万円＊（15分/8時間）　・・・　地方公務員

[日本社会としての負担は莫大]　民間社員（300人以上の事業所）　約1800万人

しかも、効果は限定的
標的型攻撃メール対策の教育・訓練においても、10%程度は開封！

➔人的負担軽減のため、
より効果的な技術的対策の開発・導入に注力すべき！

安全な電子メール利用基盤SSMAX

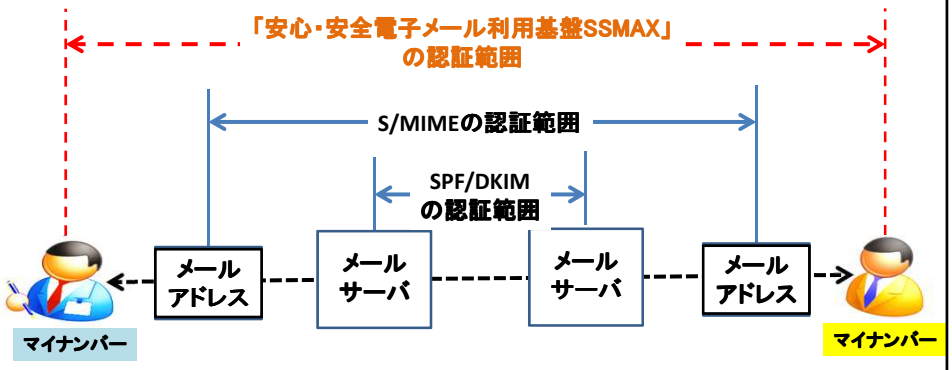
（Secure and Safe eMAil eXchange framework）

（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！

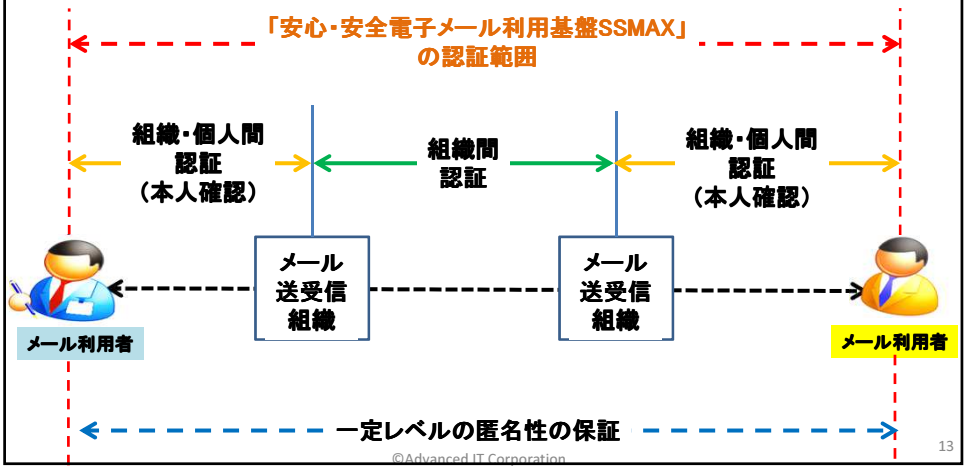
 11

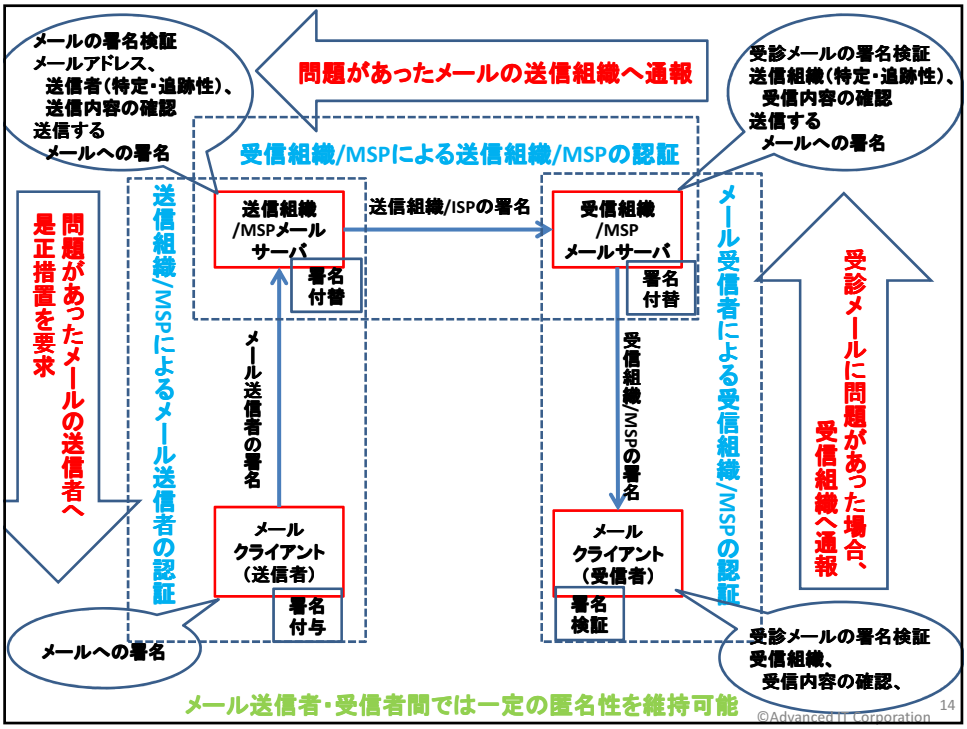
メール送信者の特定・追跡のために



 12

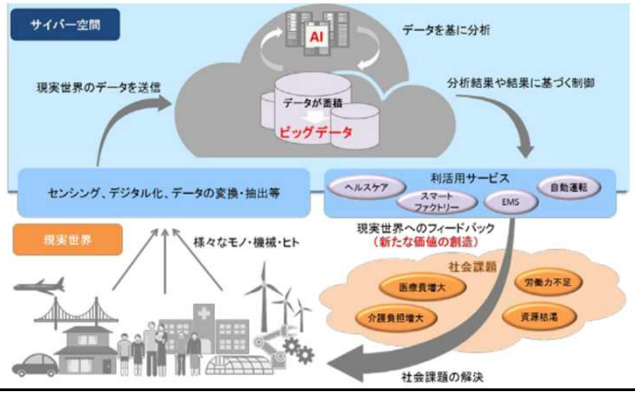
メール送信者の特定・追跡のために





3. IoT機器が情報を送信する場合の匿名性と特定・追跡性

＊2016年・64億台、2017年・84億台、2020年・204億台程度のIoT接続台数（ガートナー報告）
＊2016年9月、史上最大級のIoT利用DDOS事件（KrebsOnSecurity攻撃）
＊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（「Mirai」のソースもインターネット上に公開、亜種も出現）



 15

IoT機器の特定・追跡性と匿名性の必要性

ビッグデータ活用サービスのデータ依存性
　IoT機器・システムへのサイバー攻撃による
　　悪意に満ちたデータのビッグデータへの混入
　＝＞データ収集IoTシステム事業者の責任

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・論理的アドレスの秘匿

 16

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

（1）検討対象機能

＊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

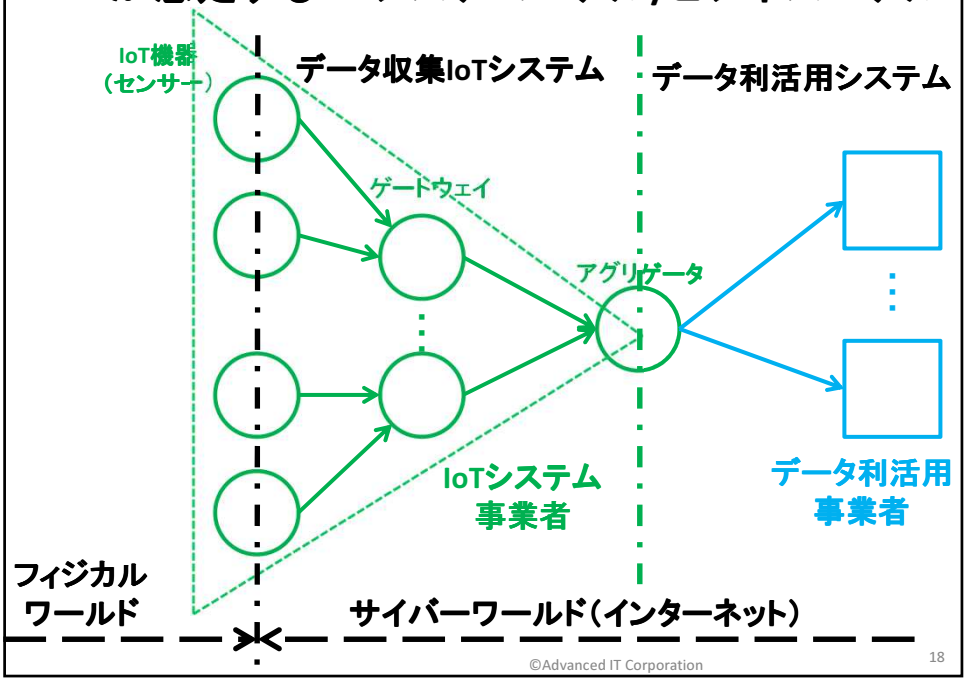
＊被害・加害を早期に収拾させるために

（2）検討対象IoTシステムモデル

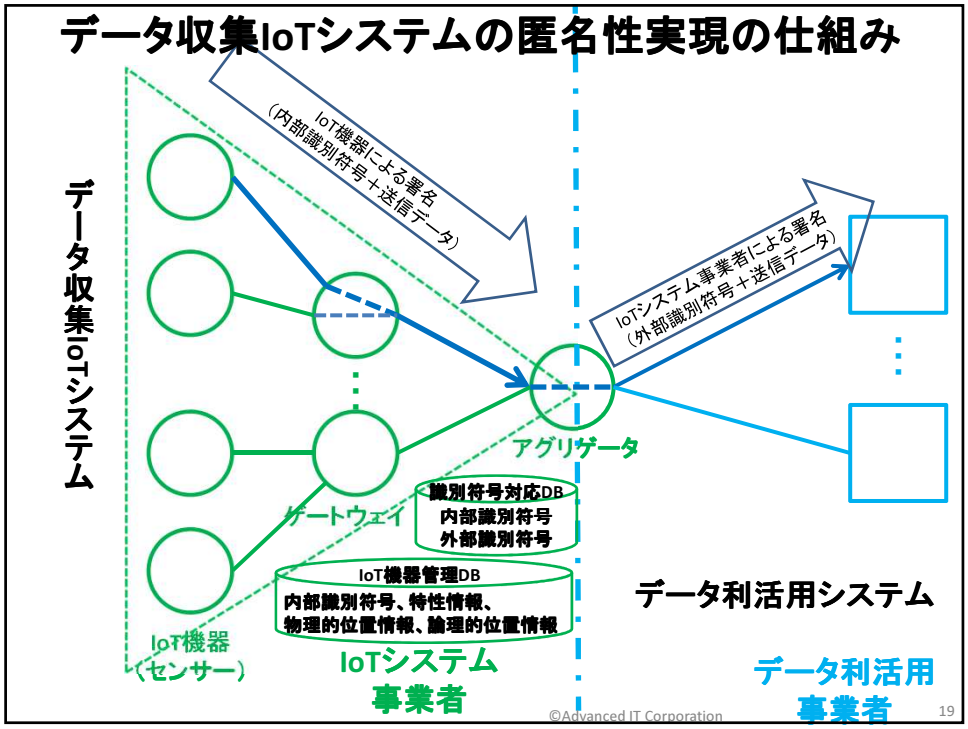
＊データ収集IoTシステム（当面）

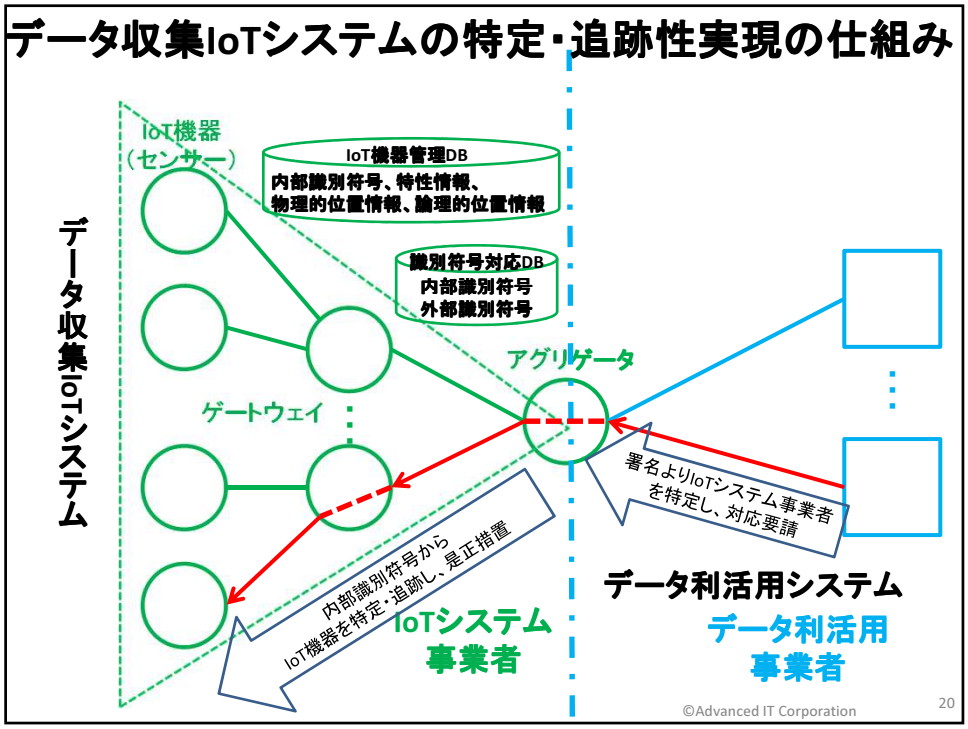
 17

SSIoTが想定するIoTシステムモデル/ビジネスモデル



 18


データ収集IoTシステムの匿名性実現の仕組み
IoT機器による署名
（内部識別符号＋送信データ）
IoTシステム事業者による署名
（外部識別符号＋送信データ）
データ収集IoTシステム
アグリゲータ
識別符号対応DB
内部識別符号
外部識別符号
ゲートウェイ
IoT機器管理DB
内部識別符号、特性情報、
物理的位置情報、論理的位置情報
データ利活用システム
IoT機器
（センサー）
IoTシステム
事業者
データ利活用
事業者
©Advanced IT Corporation
19


データ収集IoTシステムの特定・追跡性実現の仕組み
IoT機器
（センサー）
IoT機器管理DB
内部識別符号、特性情報、
物理的位置情報、論理的位置情報
識別符号対応DB
内部識別符号
外部識別符号
データ収集IoTシステム
アグリゲータ
ゲートウェイ
署名よりIoTシステム事業者
を特定し、対応要請
内部識別符号から
IoT機器を特定・追跡し、是正措置
データ利活用システム
IoTシステム
事業者
データ利活用
事業者
©Advanced IT Corporation
20

4.　連結可能匿名化による匿名性と特定・追跡性の両立方式

現在のインターネットは匿名性が強い状況。
（犯罪者・攻撃者にやさしいインターネット！）

社会（システム）のインターネット依存が高まる中、インターネット経由の悪意のある情報・データの流通の防止・早期発見・早期対応がますます重要に！

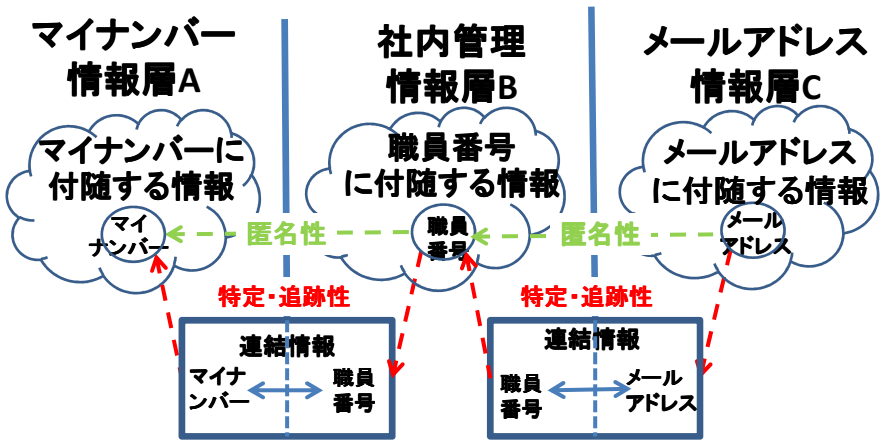
悪意のある情報・データの発信源の容易な特定・追跡が必要。

一方、インターネット利用者・インターネット接続機器の機微情報保護のための一定レベルの匿名性も必要。

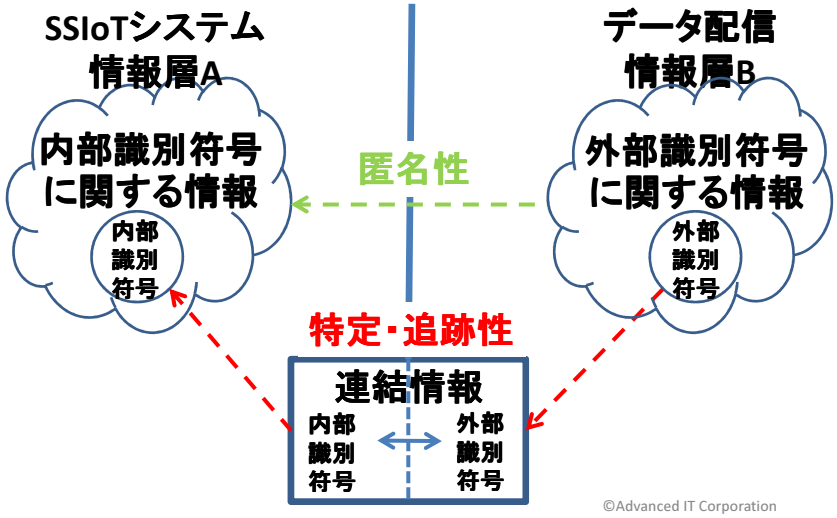
特定・追跡性の確保と一定レベルの匿名性の確保の両立が必要！
➔ 両立実現には連結可能匿名化が重要！

連結可能匿名化の実現には、インターネット利用環境を提供する組織における連結情報の作成・管理が必要。

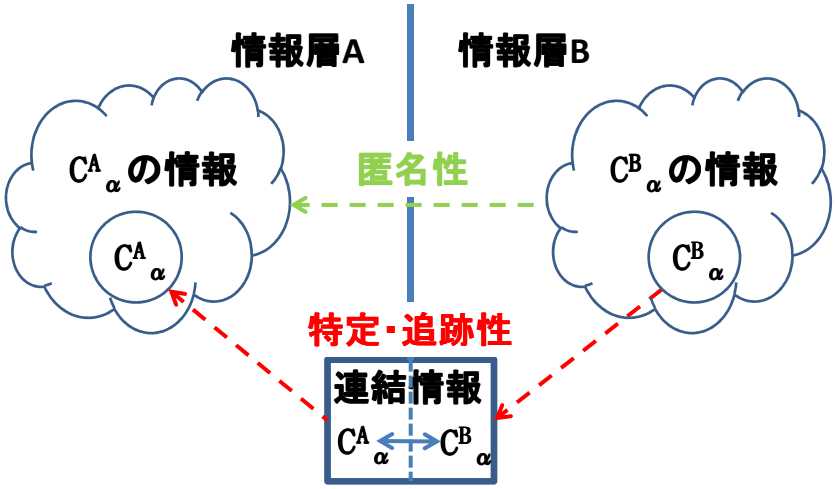
SSMAXにおける連結可能匿名化



SSIoTにおける連結可能匿名化



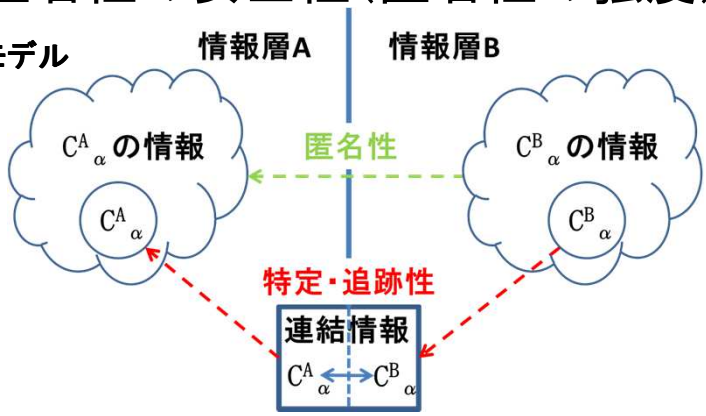
5. s-匿名性(層匿名性)についての考察



s-匿名性(層匿名性):連結可能匿名化で分離された情報層間の匿名性
s-匿名性の強度:攻撃者が匿名性を破るために必要な作業量に比例

情報層Bの情報層Aに対する s-匿名性の安全性（匿名性の強度）

2層基本モデル



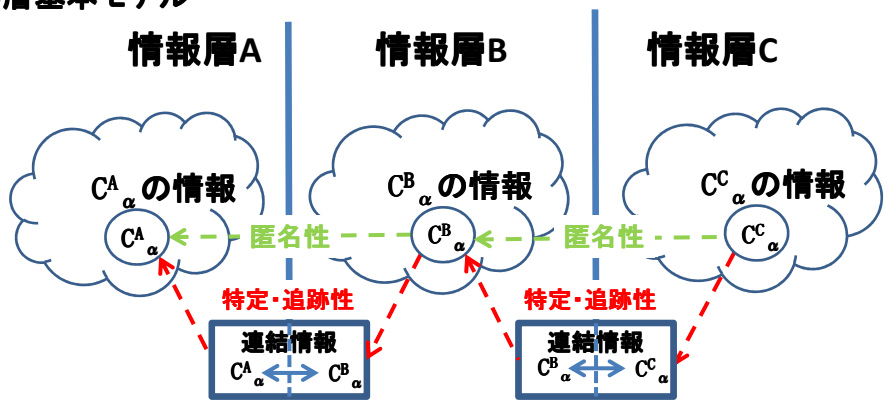
$S^{B,A}_\alpha = \min\left(X^{B,A}_\alpha,\ Y^{B,A}_\alpha\right)$

$X^{B,A}_\alpha$：情報層Bの識別符号C^B_αおよび当該識別符号に関連付けられた情報から、情報層Aの識別符号C^A_αを特定するための作業量

$Y^{B,A}_\alpha$：情報層Bの識別符号C^B_αと情報層Aの識別符号C^A_αとの対応を示す連結情報を、入手するための作業量

情報層Cの情報層Aに対する s-匿名性の安全性（匿名性の強度）

3層基本モデル



$S^{C,A}_\alpha = \min\left(S^{C,B}_\alpha + S^{B,A}_\alpha,\ X^{C,A}_\alpha\right)$

情報層がn層連接するモデルの s-匿名性の安全性（匿名性の強度）

$S^{j,i}_{\alpha}$：情報層1、2、・・・nから構成されるモデルにおける、
エンティティαに関連付けられた
情報層jにおける識別符号C^{j}_{α}および
当該識別符号に関連付けられた情報から
情報層iにおける識別符号C^{i}_{α}に対するs-匿名性の強度
（但し、$1 \leqq i < j \leqq n$）

$S^{j,i}_{\alpha} = \min(R^{j,i,k}_{\alpha})$　　$k=0,\ldots,n-2$

$R^{j,i,k}_{\alpha}$：k個の異なる層を経由した場合の、
情報層jにおける識別符号C^{j}_{α} および
当該識別符号に関連付けられた情報から、
情報層iにおける識別符号C^{i}_{α}に対するs-匿名性の強度の最小値

識別符号および当該識別符号に関連付けられた情報を利用した特定が極めて困難、という条件下では、

$S^{j,i}_{\alpha} = \min(T^{j,i,k}_{\alpha})$　　$k=0,\ldots,n-2$

$T^{j,i,k}_{\alpha}$：情報層jと情報iの間に介在するk個の情報層の、
それぞれの連携情報を入手し、
情報層jの識別符号C^{j}_{α}と情報層iの識別符号C^{i}_{α}との
対応を特定できるための作業量

最もシンプルなケース、情報層が直列に連接されている場合で
連接する2層の連結情報のみが存在する場合は、

$S^{j,i}_{\alpha} = T^{j,i,1}_{\alpha} = \Sigma_{l=j}^{i+1}(Y^{l,1-1}_{\alpha})$
情報層jから下位層へ順次連結情報を入手し
情報層iにおける識別符号C^{i}_{α}を特定する方法が最小値

s-匿名性の強度評価の定式化の試み
評価式は連結可能匿名化を利用したシステムにおける
s-匿名性の強度の根拠把握に利用可能

６．　おわりに

（１）人がインターネットへ情報を送信する場合および機器がインターネットへ（検知した）情報を送信する場合（IoT）のそれぞれについて、匿名性と特定・追跡性の両立の重要性を示した。

（２）電子メールを対象とした安心・安全電子メール利用基盤（SSMAX）におけるメール送信者の特定・追跡性と匿名性の両立方式を具体的に示した。SSMAXは構想策定済みで、今後、システム開発、実証実験等の機会をとらえ、早期の社会実装を目指したい。

（詳細は、情報処理学会論文誌2018年9月を参照）

 29

（３）機器がインターネットへ（検知した）情報を送信する場合（IoT）の例として、現在考案中の安心・安全IoTシステム（SSIoT）における情報送信機器・システムの特定・追跡性と匿名性の両立方式を示した。SSIoTについては構想策定のための調査段階である。

（４）SSMAX、SSIoTの両方で、匿名性と特定・追跡性の両立のために採用した連結可能匿名化について考察、連結可能匿名化による匿名性をs-匿名性と称することにし、S-匿名性の安全性（匿名性の強度）の評価の視点を提案した。

30

本発表は、

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」

の活動の一環として行ったものである。

終