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

才所 敏明[†1]　辻井重男[†2]

概要：本論文では，悪意のある人による標的型攻撃やフィッシング・誹謗・中傷・いじめ等を目的とした悪意のある情報の送信による社会の混乱を抑止するためには情報送信者の特定・追跡性の確保が必要であること，一方，自由で活発なコミュニケーションを促進するためには一定の匿名性の確保が重要であることを示し，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示す．次に，インターネットに接続された IoT 機器が想定外のシステムや機器への不正な情報送信による，社会の混乱を抑止するためには，情報送信機器の特定・追跡性の確保が必要であること，一方，送信機器への攻撃リスクを低減するためには IoT 機器の一定の匿名性の確保が重要であることを示し，現在考案中の安心・安全 IoT システムフレームワーク（SSIoT）における情報送信機器の特定・追跡性と匿名性の両立方式を示す．最後に，SSMAX，SSIoT にて匿名性と特定・追跡性の両立のために採用した連結可能匿名化方式を示し，連結可能匿名化により定義される匿名性を層匿名性（s-匿名性）と称することとし，s-匿名性の安全性（匿名性の強度）について考察する．

キーワード：インターネット，匿名性，特定性，追跡性，連結可能匿名性，層匿名性，s-匿名性，標的型攻撃メール，フィッシングメール，安心・安全電子メール利用基盤，SSMAX，Secure and Safe Mail Exchange Framework，IoT, Internet of Thing，安心・安全な IoT システム,SSIoT，Secure and Safe IoT System Framework

Anonymity, Identifiability, Traceability of information sender and information transmission device in the internet dependent society

TOSHIAKI SAISHO[†1]　SHIGEO TSUJII[†2]

Abstract: In order to deter society's confusion caused by the targeted-attack-mails and by the phishing-mails by malicious persons, I argue the necessity of identifiability and traceability of information(mail) senders in the internet. And also, I argue the necessity of Anonymity of information(mail) senders to promote active communication in the internet. And then, I show the mechanism compatible with anonymity and identifiability/traceability of mail senders introduced into the Secure-and-Safe-eMAil-eXchange-framework(SSMAX). Next, I argue the necessity of identifiability and traceability of IoT devices in the internet in order to deter society's confusion that are caused by the malicious data transmission to systems and devices. And also, I argue the necessity of Anonymity of IoT devices for protecting IoT devices from cyber attack. And then, I show the mechanism compatible with anonymity and identifiability/traceability of IoT devices introduced into the Secure-and-Safe-IoT-system-framework(SSIoT). Lastly I show the mechanism of linkable anonymity that I adopted in SSMAX and SSIoT in order to realize the compatibility of anonymity and identifiability/traceability. And then, I define the anonymity defined by linkable anonimity as the layer anonymity (s-anonymity), and I show the consideration results about the safety of s-anonymity (the strength of the anonymity).

Keywords: Internet, Anonymity, Identification, Traceability, Linkable Anonymity, s-Anonymity, SSMAX, Secure and Safe Mail Exchange Framework, IoT, Internet of Thing, SSIoT, Secure and safe IoT system Framework

1. はじめに *【*の文字書式「隠し文字」】

インターネットの歴史は 35 年余りにもかかわらずその普及は目覚ましく，現在はインターネットの利用無しでは企業活動も個人の生活もままならず，社会は機能しないと言っても過言ではない．現代はまさにインターネット依存社会である．インターネットは社会の発展に多大な貢献をしているのは間違いないが，犯罪者やテロリスト等の悪意のある人にとってもインターネットは社会を攻撃する格好のチャネルとなっている．

インターネットはもともと利用者が他の利用者を攻撃することを想定して設計されてはいないため，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．インターネットが広く利用されるにつれ，悪意のある人もインターネットを通じた，社会を支えるシステムやインターネット利用者への攻撃が増大してきた．もちろん，新たな攻撃の出現に応じ，対応策も講じられてきてはいるが，インターネットの仕組みに基本的なセキュリティ機能が織り込まれていないため，抜本的な対策にはほど遠い状況である．

* †1 中央大学研究開発機構
Research and Development Initiative, Chuo University
（Mail：toshiaki.saisho@advanced-it.co.jp）
†2 中央大学研究開発機構
Research and Development Initiative, Chuo University
（Mail：tsujii@tamacc.chuo-u.ac.jp）
【 研究報告用原稿：上記*の文字書式「隠し文字」 】

また，利用者もこれまでのインターネットの強い匿名性に慣れ親しみ，匿名性に支えられたある種の文化を享受しているが故に匿名性の制限には抵抗を感じ，社会を支えるインターネットにはより強固なセキュリティ機能が必要であることには理解を示しながらも，情報送信者の匿名性の解除を可能とする特定・追跡性の確保のためのセキュリティ機能の強化には消極的である．

社会がインターネットへの依存をますます高めていくのは必須であり，インターネット経由の様々の攻撃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．社会がインターネットを活用し発展し続けるためには，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ず，通信内容の真正性の確保や通信相手の厳密な確認および情報送信者の特定・追跡性の確保等の基本的なセキュリティ機能のインターネットへの組込みは不可欠であろう．

本稿では，ますます社会がインターネットに強く依存する時代へ進む中，人がインターネットへ情報を送信する場合の匿名性と特定・追跡性の両立の重要性とその実現方式を提案する（2 章）．また，機器が（検知した）情報をインターネットへ送信する IoT の場合においても，IoT 機器の匿名性と特定・追跡性の両立が重要であることを示し，その実現のための構想について説明する（3 章）．更に，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を説明（4 章）し，連結可能匿名化による匿名性を層匿名性（s-匿名性）と定義，s-匿名性の安全性（匿名性の強度）について考察する（5 章）．

2. 人が情報を送信する場合の匿名性と特定・追跡性

電子メールはインターネットが稼働し始めた当初からのアプリケーションであり，インターネットの急速な普及を支えてきたキラーアプリの一つである．インターネットの歴史と共に発展してきた電子メールは，人と人とのコミュニケーション手段の多様化が進む中でも基礎的・共通的コミュニケーション基盤として，依然として重要な役割を担っている．「ビジネスメール実態調査 2017」[1]によると，ビジネスマンの業務上の通信手段は，メール 99.08%，電話 90.10%, 会う 74.07%などが主要なものであり, LINE19.42%, Facebook10.06%など, 最近のツールも使われ始めているが，メールがネット経由の電子的通信手段の主役であるのは間違いない．しかし，現在の電子メールシステムには送信者の厳密な確認機能や送信内容の真正性の確認機能は無く，送信者のなりすましや送信内容の改ざん等が横行している．

組織間通信分野では，昨年の情報処理推進機構（IPA）の発表資料[2]では標的型攻撃による被害（情報漏洩）が最大の脅威と位置づけられており，これまでのほとんどの標的型攻撃において攻撃対象組織への侵入手段として電子メールが悪用されている．このような標的型攻撃メール対策としては，現在 SPF[3]や DKIM[4]等の技術対策が推進されているが，標的型攻撃メールの横行を抑止することはできていない．そのため，人的対策，電子メール利用者の教育と訓練により標的型攻撃メールの検出を目指す対策も広く実施されてはいるが，組織として膨大な費用負担を強いられながらも，その効果は限定的である[8].

また個人間通信分野でも，フィッシングメールや誹謗中傷・いじめ等の悪意のある電子メールが大量に流通している．このような悪意のあるメール対策としては，送信者を特定・追跡し，注意喚起や警告，法的措置などが必要となるが，一般に送信者を特定・追跡するにはインターネットサービスプロバイダ等の協力を得ての分析・追跡作業を必要とする等ハードルが高く，フィッシングメールや悪意のあるメールの横行を抑止できていないのが現状である．

このように電子メールの課題克服には，セキュリティ機能の不十分な現在の電子メールシステムには手を付けず，周辺の技術対策，人的対策だけでは限界があり，メール送信者の特定・追跡機能等のセキュリティ機能を装備した安心・安全な電子メールシステムの実現が不可欠である．一方，現在の電子メールシステムで許容されている匿名性へのニーズも強く，メール送信者の特定・追跡性を確保しつつ一定レベルの匿名性を確保することが必要である．このような認識の元，筆者らは安心・安全な電子メール利用基盤 SSMAX（Secure and Safe eMAil eXchange framework）の構想を策定・提案し，その実現に向け活動中である．

2.1 安心・安全な電子メールシステム SSMAX

SSMAX とは，メール送信者の一定の匿名性を確保しつつも，標的型攻撃メール，フィッシングメール，誹謗中傷・いじめ等の悪意のある電子メールの氾濫を抑止し，更にメール内容の改ざん検知・漏洩防止が可能な，安心・安全な電子メールの利用基盤である．

SSMAX におけるメール送信者の匿名性は，現在の電子メールと同様, 利用者にメールアドレスを付与する組織（産官学の組織や個人の場合はメールサービスプロバイダ）がメールに表示されるメールアドレスや使用者名として，メール送信者を特定できないメールアドレスやニックネームの利用を許容することにより実現を目指しており，メール利用者の判断により匿名性の利用を可能としている．

SSMAX におけるメール送信者の特定性は，利用者にメールアドレスを付与する組織（産官学の組織や個人の場合はメールサービスプロバイダ）が，メール利用者を特定できる識別符号と付与したメールアドレスやニックネームとの対応を維持･管理することにより, 実現を目指している．

SSMAX におけるメール送信者の追跡性は，利用者にメールアドレスを付与する組織（産官学の組織や個人の場合はメールサービスプロバイダ）が，メール利用者を特定で

きる識別符号（組織の場合は社員番号や職員番号，個人の場合は契約者番号や利用者番号等）とメール利用者を追跡できるマイナンバーあるいはマイナンバーと紐づけられた識別符号との対応を維持・管理することにより，実現を目指している．

メール送信者が送信したメールは，メールアドレスを付与した組織（産官学の組織や個人の場合はメールサービスプロバイダ）が確実に送信者を確認し，その上で送信組織としての署名を付けて，受信者が所属する受信組織へ転送する．受信組織は，受信メールに付与されている署名の検証により送信組織を確認し，受信者へ転送する．

SSMAX のこのような仕組みにより，メール利用者間でのメール送信者の匿名性は，メール送信者の判断で利用可能であると同時に，万一，悪意のあるメールを受信した場合は，受信者が所属する受信組織はメール送信組織を特定し対処を要請でき，またメール送信組織はメール送信者を特定できるので対処要請が可能であり，対処への要請に応じないメール送信者の場合はメール利用の停止措置や，メール送信者の追跡もできるので法的措置なども可能である．SSMAX では，万一，標的型攻撃メール，フィッシングメールや誹謗中傷・いじめ等の悪意のあるメールが発生した場合でも，その送信者を容易に特定・追跡でき，悪意のあるメールの送信を止めることができ，悪意のあるメールの氾濫を抑止可能である．

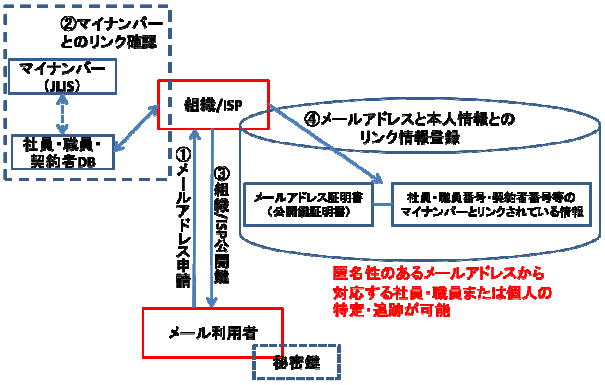

図 1　メール利用を承認する組織でのメール利用者登録

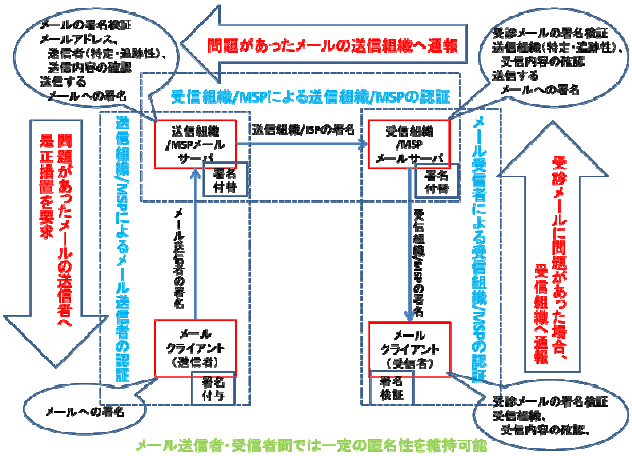

図 2　メールの流れと送信者特定の仕組み

このように，SSMAX では，標的型攻撃メール，フィッシングメールや誹謗中傷・いじめ等の悪意のあるメール送信者の特定・追跡については，そのメール送信者にメールアドレスを付与し，メール利用を可能とした組織が責任を負う仕組みを想定している．

なお，SSMAX の詳細については，論文”「安心・安全電子メール利用基盤（SSMAX）」構想”[8]を参照願いたい．

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

インターネットへ接続される IoT 機器は急増中であり，ガートナーによると 2016 年には 64 億台程度，2017 年には 84 億台程度の接続台数とみられ世界の人口（2017 年には 75 億人程度）を超えるものと予測されている．IoT 機器の急増はその後も続き，2020 年には 204 億台に達すると予測されている[9][10].

IoT 機器の爆発的増加により，これまで得られなかった様々のデータが収集可能となり，大量の時々刻々発生するデータはビッグデータとして蓄積・管理され，AI 等によるビッグデータの分析結果は企業の業務改善や新サービスの創出，様々な社会システムの安全な運用やその改善等での活用が期待されている．IoT，ビッグデータ，AI は相互に連携しながら発展をつづけ，我が国をデータ・ドリブン（駆動・主導）社会，ビッグデータ社会へと発展させることになろう．

データ・ドリブン社会においては，IoT 機器で収集されるデータをデータ利活用事業者へ提供する IoT システム事業者の責任は重大である．データの品質・正誤が AI 等による分析結果を左右することになり，産業活動や国民サービスへ直接的な影響を与え，社会を混乱させることになりかねない．このようなデータ・ドリブン社会のデータ依存性を利用した，IoT システム事業者が担当するデータ収集・送信プロセスへのサイバー攻撃，IoT 機器のなりすましや正規の IoT 機器の乗っ取りによる意図的で悪意のあるデータの送信による攻撃等が想定される．今後爆発的に増加するであろうデータ収集 IoT システムは，IoT 機器のなりすましや正規の IoT 機器の乗っ取りによる意図的で悪意のあるデータ送信が発生しないよう十分なセキュリティ機能の組込みが必要であろうし，万一，そのような事故・事件が発生した場合は，当該 IoT 機器をすみやかに特定・追跡し是正できるような仕組みが，データ・ドリブン社会の安心・安全を維持するためには不可欠である．

一方，IoT 機器の匿名性も重要である．IoT 機器はインターネット経由の攻撃に晒されている．IoT 機器を特定・追跡できる情報，例えば IoT 機器の特性情報（機種・型番・製造番号や動作ソフト等），物理的位置情報（GPS データ等），論理的位置情報（IP アドレス等）が IoT 機器攻撃者に漏れた場合，攻撃を受けるリスクが大幅に増大する．IoT

システム事業者としては，攻撃されるリスクを軽減するため，収集したデータを提供するデータ利用事業者からの要請が無い限り，IoT 機器が特定されるリスクのある情報の提供は避けるのが望ましく，IoT 機器の特定・追跡性の確保は不可欠だが，匿名性確保の仕組みも必要な場合が多い．

このような認識の元，筆者らは安心・安全な IoT システム SSIoT（Secure and Safe Internet of Thing）の構想を策定中である．

3.1 安心・安全な IoT システム SSIoT

SSIoT とは，データ送信 IoT 機器の匿名性を確保しつつも，他の機器やシステムへの悪意のあるデータ送信が検知された場合は当該 IoT 機器を特定・追跡でき，更に IoT 機器からの送信データの改ざん検知・漏洩防止が可能な，安心・安全な IoT システムを目指し考案中のシステムフレームワークである．IoT システムは応用分野に応じ多種多様であるが，SSIoT の検討は，シンプルなデータ収集 IoT システム/ビジネスモデル(図 3)を対象として実施しており，本節で行う SSIoT における IoT 機器の匿名性と特定・追跡性の両立を実現する仕組みの検討もデータ収集 IoT システム/ビジネスモデルを前提とし行っている．

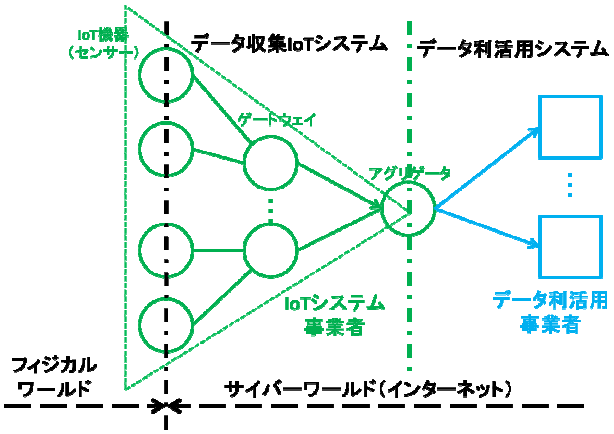

図 3　データ収集 IoT システム/ビジネスモデル

SSIoT における IoT 機器の匿名性とは，IoT システム事業者が管理する IoT 機器を識別ために各 IoT 機器に付与した内部識別符号を，データを利用するデータ利活用事業者に対する隠蔽を意味している．IoT 機器の内部識別符号は，IoT 機器の攻撃に利用されがちな機種・型番・製造番号や動作ソフト等の特性情報，GPS データ等の物理的位置情報，IP アドレス等の論理的位置情報などの IoT 機器の機微情報と連携され管理されることが多く，サイバー攻撃のリスクを低減させるために内部識別符号は公開しない方が望ましい．また，IoT 機器をインターネットに接続し IoT システムを構築・運用する事業者が IoT 機器からのデータをデータ利活用事業者へ提供する際に，提供するデータに IoT 機器の機微情報が含まれている場合は，機微情報を削除するか何らかのコードへの変換による匿名化を想定している．

なお，IoT 機器の機微情報の内，物理的位置情報等はデータ利活用事業者でのデータ分析に必要な場合もあり，匿名性の範囲・方法等は IoT システム事業者の判断で決定することになろう．

SSIoT における IoT 機器の特定性とは，IoT システム事業者が，データ利用事業者へ提供したデータから，管理下の IoT 機器を特定できるという意味で使用している．一般に，IoT システム事業者は管理下の IoT 機器には固有の識別符号（内部識別符号）を付与し管理され，IoT 機器から送信されるデータには送信する IoT 機器の内部識別符号が含まれているが，その内部識別符号によりデータ利活用事業者が IoT 機器の機微情報の一部が推定される可能性があれば，匿名性を確保するためデータ利活用事業者に提供するデータでは IoT 機器を特定できない識別符号（外部識別符号）へ置き換え，内部識別符号と外部識別符号の対応を維持・管理することによる特定性の実現を想定している．

SSIoT における IoT 機器の追跡性は，IoT システム事業者が，IoT 機器を特定できる識別符号（内部識別符号）と IoT 機器の機微情報（特性情報，物理的位置情報，論理的位置情報）との対応を維持・管理することによる実現を想定している．

SSIoT においては，センサー等の IoT 機器が収集したデータは IoT 機器の内部識別符号と共に IoT システム事業者より IoT 機器へ付与された秘密鍵により署名が付与され，ゲートウェイ等を経由し IoT システム事業者のサーバ（アグリゲータ）に送信される．IoT システム事業者は，署名検証により IoT 機器を確認後，客先との契約に応じ，IoT 機器の内部識別符号を外部識別符号へ変換等の匿名化を行い，IoT システム事業者の署名を付与し，それぞれの客先へデータを送信する．客先は受信したデータの署名を検証することにより IoT システム事業者を確認し，受信データを DB 等に格納し分析・加工の上，利用する，という仕組み，ビジネスモデルを想定している．

SSIoT のこのような仕組みにより，IoT 機器の IoT システム外での匿名性は IoT システム事業者の判断で利用可能であると同時に，万一，客先等のシステムが悪意のあるデータや想定外のデータを受信した場合は，送信した IoT システム事業者を特定でき対処を要請でき，IoT システム事業者は外部識別符号から対応する内部識別符号を特定でき，管理する IoT 機器の機微情報から IoT 機器を特定し追跡，対処することが可能である．

SSIoT の具体的な実装方式については今後検討することになるが，特定・追跡性と匿名性の両立については図 4，図 5 のようなイメージでの実現を想定している．

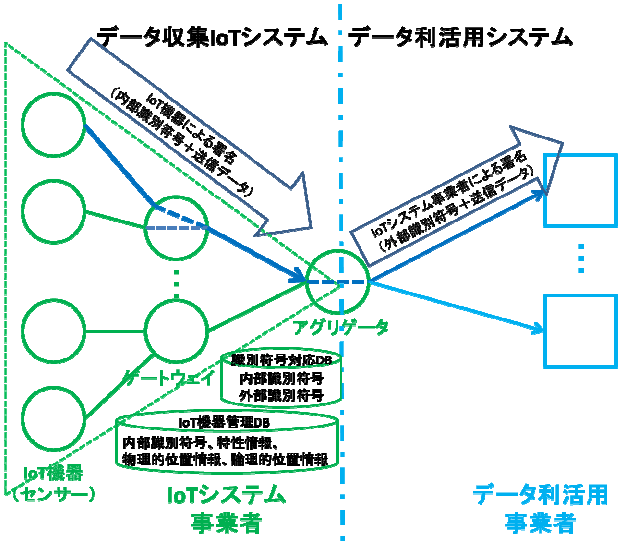

図 4　データ収集 IoT 機器の匿名化の仕組み

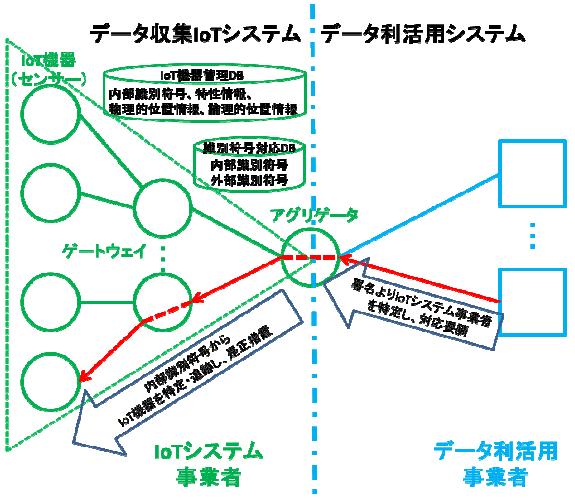

図 5　問題ある情報を送信した IoT 機器の特定・追跡

なお，SSIoT については，”安心・安全な IoT システム (SSIoT)に関する考察“[15]を参照願いたい．

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

人がインターネット上に情報を送信する場合の例としての安心・安全電子メール利用基盤 SSMAX（2 章）においても，機器がインターネット上に情報を送信する場合の例としての安心･安全な IoT システム SSIoT(3 章)においても，特定・追跡性の確保と一定レベルの匿名性の確保の両立のために連結可能匿名化の手法を採用している．

連結可能匿名化とは，例えばデータからデータを送信したエンティティ（人や IoT 機器）を特定するための識別符号を，新たな識別符号へ置き換え，データに含まれている情報と元の識別符号との対応を困難にすることにより匿名化を実現すると同時に，元の識別符号と新たな識別符号との対応（連結情報）を保持しておき，必要な場合には連結情報を利用しデータに含まれている情報と元の識別符号との対応を確認できる匿名化のことである．

安心・安全電子メールシステム SSMAX の場合は，電子メールの利用を許可している組織やメールサービスプロバイダが，マイナンバーなど本人を特定・追跡できる識別符号と登録したメールアドレス（新たな識別符号）との対応（連結情報）を管理することにより，電子メール利用者の特定・追跡性を確保し，一方，電子メール利用者には本人を類推できないメールアドレスの登録をも認めることにより，電子メール利用者の判断で匿名性を実現可能としている．

電子メール利用者が悪意のあるメールを受信した場合，受信者がメールアドレスそのものからメール送信者を特定できない場合でも，送信者が属する組織やメールサービスプロバイダを特定でき，その組織やメールサービスプロバイダは連結情報を逆引きすることにより送信者を特定・追跡でき，送信者に是正を要請することを実施可能としている．

安心・安全な IoT システム SSIoT の場合は，IoT 機器をインターネットに接続し運用している IoT システム事業者が，IoT 機器を特定・追跡できる識別符号（内部識別情報）と IoT システム事業者が送信するデータに含める IoT 機器の識別符号（外部識別情報）との対応（連結情報）を管理することにより，IoT 機器の特定・追跡性を確保し，一方，IoT システム事業者が送信するデータには IoT 機器を特定できない新たな識別符号（外部識別情報）を利用することにより，IoT システム事業者の判断で IoT 機器の匿名性を実現可能としている．

悪意のあるデータをインターネット上のシステムや機器が受信した場合は，受信したデータに含まれている IoT 機器の外部識別符号からは IoT 機器を特定できない場合でも，IoT 機器を管理・運用する IoT システム事業者を特定でき，IoT システム事業者は連結情報を逆引きすることにより IoT 機器を特定・追跡でき，当該 IoT 機器の検査や是正を実施できる仕組みを想定している．

5.　s-匿名性（層匿名性）についての考察

連結可能匿名化により実現される匿名性を，s-匿名性（層匿名性）と称することとし，本章では s-匿名性（層匿名性）について考察する．

連結可能匿名化の 2 層基本モデルを図 6 に示す．

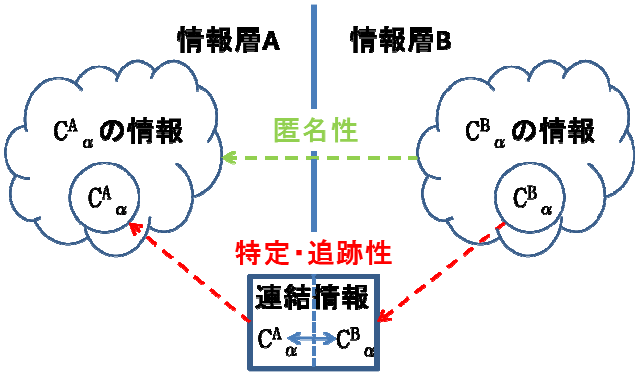

図 6　連結可能匿名化の 2 層基本モデル

基本モデルでは，二つの情報層 A，B から構成され，情報層 B は情報層 A に対し連結可能匿名化により分離されている．連結可能匿名化による匿名性実現には，情報層 A の識別符号 C^A_α および情報層 B の識別符号 C^B_α は共に特定のエンティティ α に関連付けられているが，連結可能匿名化により，識別符号 C^B_α から識別符号 C^A_α の特定を困難にする必要がある．また，識別符号にはそれぞれの情報層内で様々の情報と関連付けられてはいるが，識別符号 C^B_α に関連付けられた情報からも，識別符号 C^A_α の特定を困難にする必要がある．

連結可能匿名化による情報層 B から情報層 A への特定・追跡性は，識別符号 C^A_α と識別符号 C^B_α の対応情報（連結情報）を保有することにより実現される．ゆえに，連結情報が漏れると，特定・追跡可能となり，匿名性は失われることになる．

基本モデルにおける識別符号の連結可能匿名化による情報層 B の情報層 A に対する s-匿名性の安全性（匿名性の強度）は，攻撃者による特定・追跡のための作業量に比例すると考えられる．攻撃方法としては，識別符号（例えば C^B_α）および当該識別符号に関連付けられた情報から対応する識別符号（例えば C^A_α）を特定する方法と，連結情報の入手により識別符号（例えば C^B_α）に対応する識別符号（例えば C^A_α）を特定する方法が考えられる．識別符号の連結可能匿名化による匿名性の強度（s-匿名性の安全性）の尺度となる攻撃者に必要な作業量は，それぞれの攻撃方法で必要な作業量の内, 少ない作業量と考えることができ，エンティティ α に関する情報層 B の情報層 A に対する s-匿名性（層匿名性）の強度 $S^{B,A}_\alpha$ は次の式で推定される．

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

$X^{B,A}_\alpha$：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

このような識別符号の連結可能匿名化による情報層の分離を繰り返し，新たに生成される情報層の識別符号の匿名性を高めることが期待される．図 7 が 3 層基本モデルであり，エンティティ α に関連付けられた情報層 C の識別符号 C^C_α および識別符号 C^C_α に関連付けられた情報の情報層 A の識別符号 C^A_α に対する s-匿名性の強度 $S^{C,A}_\alpha$ は次式で表現される．

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

なお，図 7 のように，情報層 A と情報層 C の連結情報が存在しない場合は，連結情報入手のための作業量 $Y^{C,A}_\alpha$ は存在せず，の情報層 A の識別符号 C^A_α に対する s-匿名性の強度 $S^{C,A}_\alpha$ は次式で表現される．

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

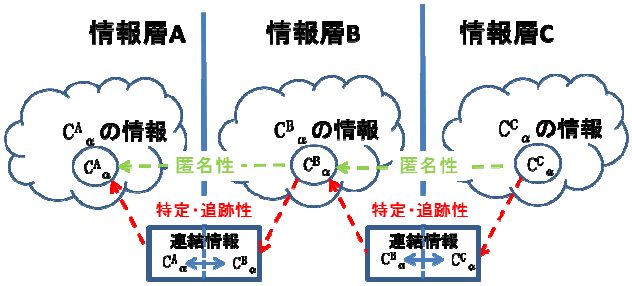

図 7　連結可能匿名化の 3 層基本モデル

更に一般化し，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 $S^{j,i}_\alpha$ は次式で表現される．ただし，1≦i<j≦n，とする．

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

ここで，$R^{j,i,k}_\alpha$ は 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 を特定するための作業量の最小値，とする．

なお，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-匿名性の強度は以下の式へ帰着できる．

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

ここで，$T^{j,i,k}_\alpha$ は情報層 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，とする．

また，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，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 $C^{i}{}_{\alpha}$ を特定する方法が最小値となり，以下の式で表現できる．

$S^{j,i}{}_{\alpha}=T^{j,i,1}{}_{\alpha}=\Sigma_{l=j}{}^{i+1}\ (Y^{l,1-1}{}_{\alpha})$

つまり，このようなケースの場合，s-匿名性の強度は連結情報を管理する組織の情報保護能力の総和に比例すると考えることができる．

本節では，s-匿名性の強度評価の定式化を試みた．評価式を構成する項の定量化については今後の課題であるが，評価式は連結可能匿名化を利用したシステムにおける匿名性の強度の根拠把握に利用可能である．

6. おわりに

本稿では，ますます社会がインターネットに強く依存する時代へ進む中，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．

人がインターネットへ情報を送信する場合の例として，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．なお，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．

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．なお，SSIoT については，まだ構想策定のための準備段階である．今後，SSIoT に必要な機能の実現のための技術検討を深め，早期の構想策定を目指したい．

更に，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）の評価方法を提案した．評価式を構成する各項の定量化については今後の課題であるが，連結可能匿名化による匿名性を考慮したシステムの，提案した評価式の利用により，連結可能匿名化の強度（s-匿名性の強度）の根拠把握が可能である．

社会がインターネット依存性を高める中，悪意のあるインターネット利用が社会の混乱の大きな原因となりつつある．インターネットはもともと利用者が他の利用者を攻撃することを想定して設計されてはいないため，悪意のあるインターネット利用の防止対策とか，悪意のあるインターネット利用が発生した場合の悪意の発生源の特定・追跡・解消対策等のセキュリティ機能が装備されていない．今後ますます高まるであろう社会のインターネット依存を鑑みると，悪意のある利用者にやさしいインターネットから，悪意のある利用が困難な，悪意のある利用が発生してもすみやかに排除できる安心・安全なインターネットへと発展させる必要があろう．匿名性と特定・追跡性の両立の仕組みは，インターネットの安心・安全の強化には不可欠な機能の一つである．

参考文献

[1] “ビジネスメール実態調査 2017 http://www.sc-p.jp/news/pdf/170602PR.pdf. （参照 2018-04-13）
[2] “情報セキュリティ 10 大脅威 2018”, IPA, 2018-03-30. https://www.ipa.go.jp/security/vuln/10threats2018.html. （参照 2018-04-02）
[3] “Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1”, RFC7208. https://tools.ietf.org/html/rfc7208. （参照 2018-04-13）
[4] “DomainKeys Identified Mail (DKIM) Signatures”, RFC6376. https://tools.ietf.org/html/rfc6376. （参照 2018-04-13）
[5]辻井重男，五太子政史，才所敏明：”標的型攻撃・サイバー戦争から日本を守るには”，JSSM 第 30 回全国大会.
[6]才所敏明，五太子政史，辻井重男：”標的型メール攻撃に対抗する「組織通信向け S/MIME」”，CSS2016.
[7]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）」構想”，SCIS2017.
[8]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）」”，CSS2017.
[9] “Gartner Says 8.4 Billion Connected Things Will Be in Use in 2017, Up 31 Percent From 2016”, Press Release, February 2017. https://www.gartner.com/newsroom/id/3598917. （参照 2018-05-07）
[10] “世界の統計 2017”，総務省統計局，平成 29 年. http://www.stat.go.jp/data/sekai/pdf/2017al.pdf. （参照 2018-05-07）
[11] “サイバー攻撃 1281 億件 16 年，IoT 機器狙い急増”，日本経済新聞，2017 年 2 月 8 日. https://www.nikkei.com/article/DGXLASDG08H3L_Y7A200C1000000/. （参照 2018-05-07）
[12]Manos Antonakakis, Georgia Institute of Technology 他，“Understanding the Mirai Botnet”, 26th USENIX Security Symposium, August 2017. https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf. （参照 2018-05-07）
[13]才所 敏明，辻井 重男：” ビッグデータの社会活用推進上の課題に関する考察 “，SCIS2018.
[14]丸山 剛司，才所 敏明，五太子 政史，長岡 篤：“社会インフラ分野におけるビッグデータの利活用に関する調査研究 報告書”，一般財団法人公務人材開発協会，2018 年 3 月.
[15]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“, 第 81 回 CSEC 研究会（2018）.
[16]河野 和宏:“インターネット上で匿名性を有するサービスを実現するために”，社会安全学研究 創刊号，関西大学，2011 年 2 月 14 日.

http://www.kansai-u.ac.jp/Fc_ss/common/pdf/bulletin001_03.pdf.（参照 2018-05-07）
[17]繁富 利恵，大塚 玲，Keith Martin，今井 秀樹，“部分的な linkability を付加した Refreshable Tokens”， 第 26 回 CSEC 研究会(2004). https://ipsj.ixsq.nii.ac.jp/ej/?action=repository_uri&item_id=44923&file_id=1&file_no=1. （参照 2018-05-26）
[18]千田 浩司，小宮 輝之，林 徹，“匿名性確保と不正者追跡の両立が可能な通信方式”，情報処理学会論文誌（2004 年 8 月）. https://ipsj.ixsq.nii.ac.jp/ej/?action=repository_uri&item_id=10834&file_id=1&file_no=1. （参照 2018-05-26）
[19]大谷卓史，“インターネットにおける匿名性はいかに正当化されるか?”，吉備国際大学政策マネジメント学部研究紀要第 3 号（2007 年）. https://kiui.repo.nii.ac.jp/?action=repository_uri&item_id=695&file_id=19&file_no=1. （参照 2018-05-26）
[20]“電子社会における匿名性と可視性・追跡可能性―その対立とバランス―”，日本学術会議・法学委員会「ＩＴ社会と法」分科会，2008 年 7 月 24 日. http://www.scj.go.jp/ja/info/kohyo/pdf/kohyo-20-h60-2.pdf. （参照 2018-06-01）
[21]“NET OF INSECURITY A flaw in the design”， The Washington Post， May 2015. http://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/?utm_term=.d8cacb1e46a0. （参照 2018-05-10）

【 この位置に改ページを入れ, 以降のページを印刷対象外とする 】