インターネットにおける
匿名性と特定・追跡性の両立の重要性
ー安心・安全電子メールシステムSSMAXを中心にー

2019年3月5日　才所敏明（（株）IT企画）
toshiaki.saisho@advanced-it.co.jp　http://www.advanced-it.co.jp
中央大学研究開発機構
セキュアIoTプラットフォーム協議会

略歴

1970年　東京大学・工学部・計数工学科卒業
1970年～1994年　本社情報システム部門
東芝社内技術部門・研究部門向け
計算機利用環境の整備・高度化を担当
EWS（SUN）の全社導入・活用推進、
社内インターネット網・UNIXメール網の構築・活用推進
1995年～2007年　セキュリティ技術研究開発部門
セキュリティ技術の研究開発および事業支援活動を指揮しつつ、
我が国としてのセキュリティ研究開発課題を
中央省庁へ多数提案し受託・研究開発指揮
2007年～　（株）IT企画
大学向けの講義・講演、IT企業向けコンサル活動
2014年～　中央大学研究開発機構（研究員）
研究対象分野：サイバーセキュリティ、IoT、ビッグデータ、FinTech
2018年～　セキュアIoTプラットフォーム協議会（研究員）
研究対象分野：IoT

説明項目

（1）インターネットの匿名性と特定・追跡性に関する問題提起（5分）
（2）安心・安全電子メールシステムSSMAX（提案内容紹介）（20分）
　①SSMAXが目指す電子メール利用環境
　②送信者の匿名性と特定・追跡性の両立
　③送信情報の秘匿と情報漏洩防止・マルウェア流入防止の両立
　④SSMAXとS/MIMEの比較（S/MIME普及の課題）
　⑤悪意のあるメール対策の社会実装に向けて
（3）送信デバイス・データの真正性保証（研究内容紹介）（10分）
　①SCOPE-PJにおける課題設定
　②送信デバイス・データの真正性確保方式案
　③送信デバイスの匿名性と特定・追跡性の両立案
　④送信情報の保護案
　⑤SCOPE-PJの今後の計画
（4）仮想通貨における匿名性と特定・追跡性に関する問題提起（10分）

（1）インターネットの匿名性と特定・追跡性に関する問題提起

匿名性の功罪

現在のインターネットは、利用者の判断で匿名利用が可能

匿名性のメリット
　➔表現の自由を保護するうえで非常に重要な役割

匿名性のデメリット
　➔悪意のある無責任な発言の横行

現在のインターネットは、
　匿名利用者の特定・追跡性が保証されていない
➔犯罪者に優しいインターネットになってしまっている！

（1）インターネットの匿名性と特定・追跡性に関する問題提起

インターネットの脆弱性

A flaw in the design
The Internet's founders saw its promise
but didn't foresee users attacking one another.
NET OF INSECURITYに関する記事
（The Washington Post: Published on May 30, 2015）
Vinton G. Cerf
（インターネットの父：TCP/IPプロトコルの提案等）

インターネットは、そもそも悪用されることを、想定していない
➔匿名性を悪用した犯罪等への対応機能が未装備というのが
インターネットの重大な脆弱性！

（1）インターネットの匿名性と特定・追跡性に関する問題提起

匿名性と特定・追跡性の両立の重要性

社会はインターネット依存へ邁進中！
➔特定・追跡性保証の裏付けのない匿名性は
ますます社会の大きな脅威に！

安心・安全なインターネット社会の実現を！
➔インターネットにおける匿名性と特定・追跡性の両立が不可欠！

（2）安心・安全電子メールシステムSSMAX

①SSMAXが目指す電子メール利用環境

Secure and Safe eMAil eXchange framework(SSMAX)

（1）送信者の匿名性と特定・追跡性の両立

送信者の匿名性を保証しつつ、

悪意のある電子メールの流通・氾濫を抑止可能！

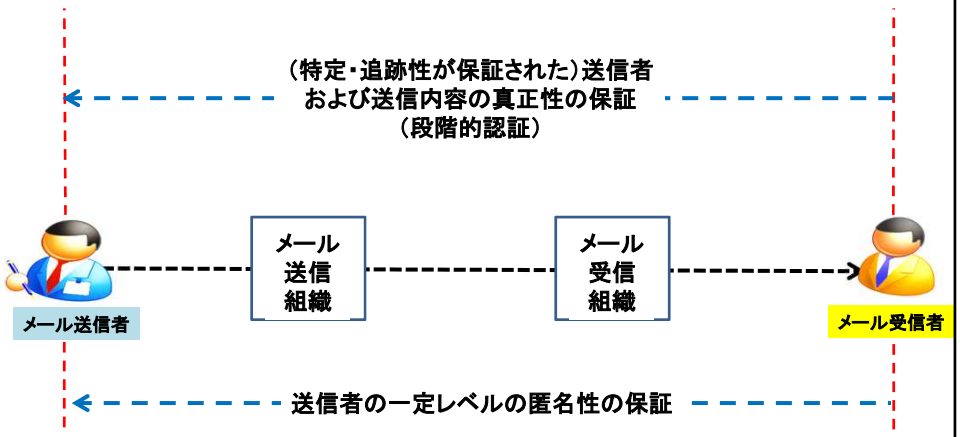
（2）送信情報の秘匿性と検査可能性の両立

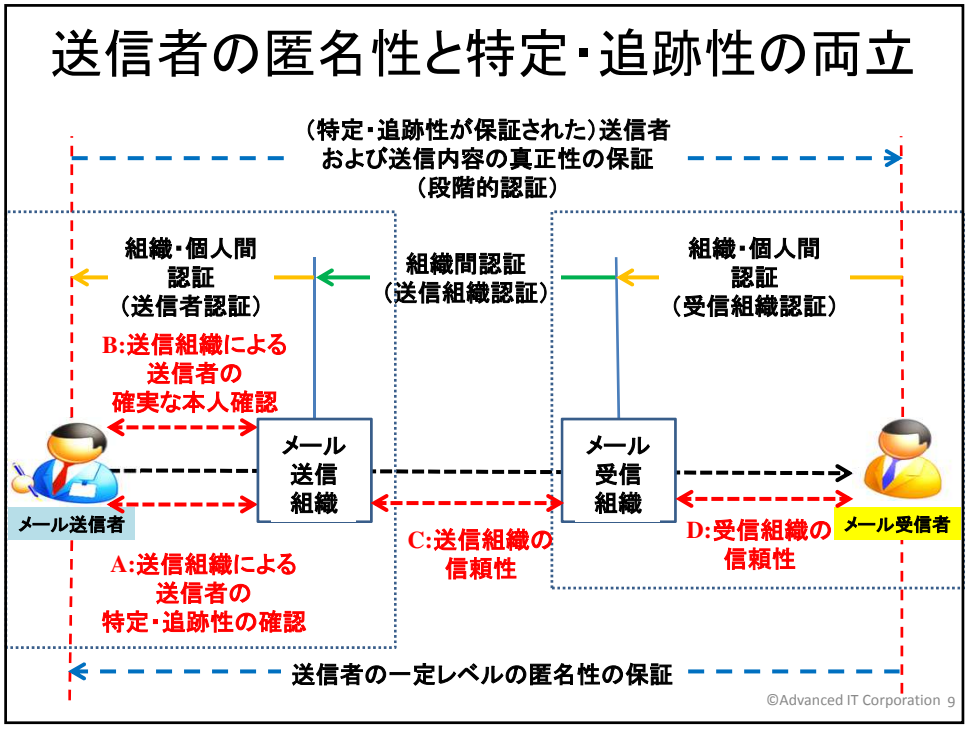
個人・機密情報の保護を保証しつつ、

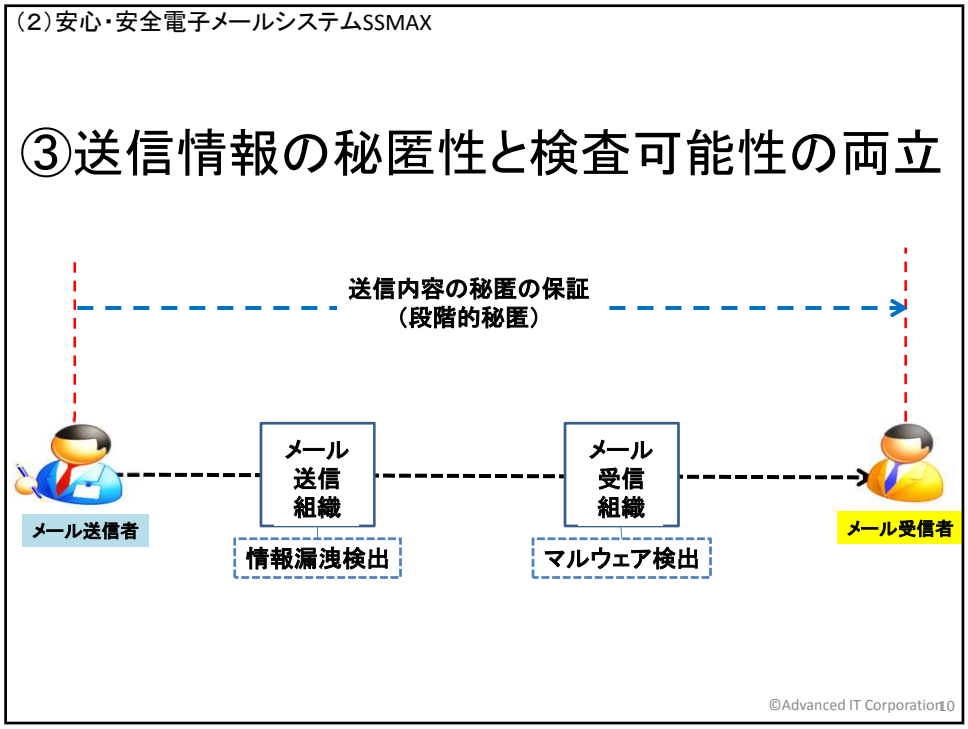
情報漏洩を防止しマルウェアの流入を防止可能！

（2）安心・安全電子メールシステムSSMAX

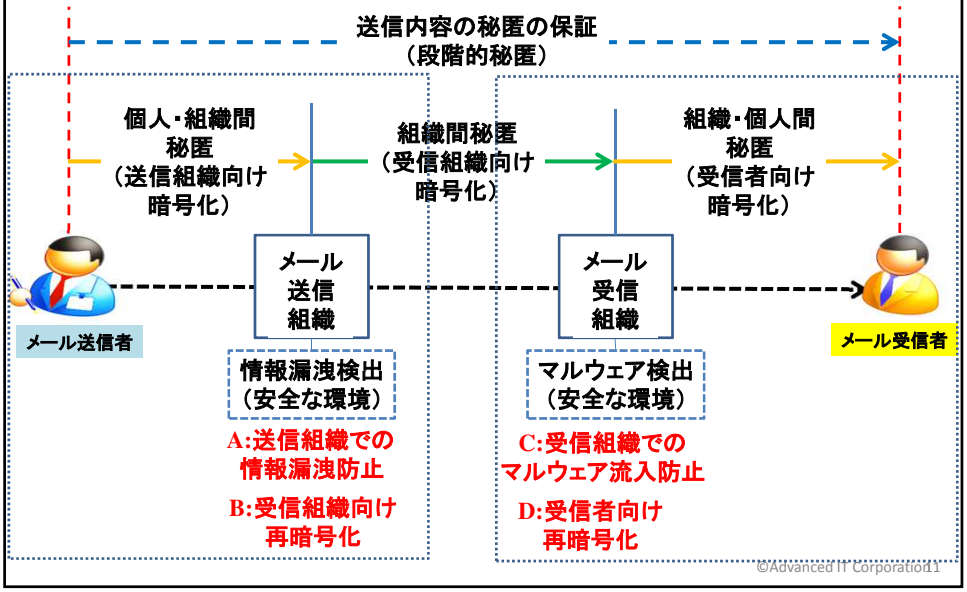
②送信者の匿名性と特定・追跡性の両立




送信者の匿名性と特定・追跡性の両立
（特定・追跡性が保証された）送信者
および送信内容の真正性の保証
（段階的認証）
組織・個人間
認証
（送信者認証）
組織間認証
（送信組織認証）
組織・個人間
認証
（受信組織認証）
B:送信組織による
送信者の
確実な本人確認
メール
送信
組織
メール
受信
組織
メール送信者
メール受信者
C:送信組織の
信頼性
D:受信組織の
信頼性
A:送信組織による
送信者の
特定・追跡性の確認
送信者の一定レベルの匿名性の保証
©Advanced IT Corporation 9


（2）安心・安全電子メールシステムSSMAX
③送信情報の秘匿性と検査可能性の両立
送信内容の秘匿の保証
（段階的秘匿）
メール
送信
組織
メール
受信
組織
メール送信者
メール受信者
情報漏洩検出
マルウェア検出
©Advanced IT Corporation 10

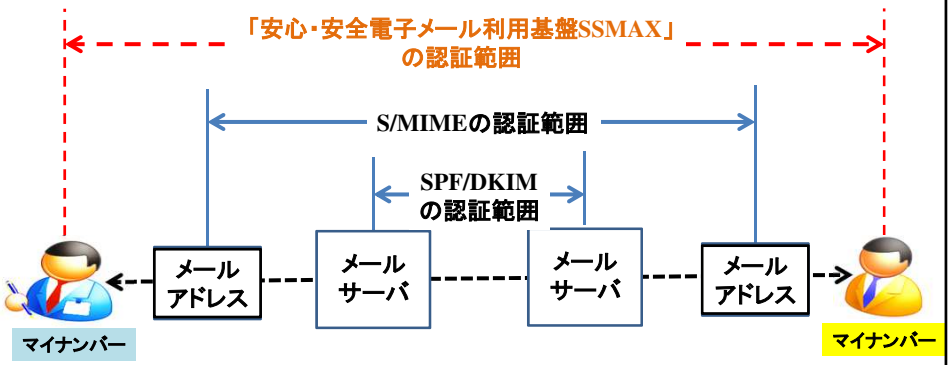
送信情報の秘匿性と検査可能性の両立



（2）安心・安全電子メールシステムSSMAX

④S/MIMEとの比較

SSMAXとS/MIMEの認証方式・範囲の違い



SSMAXでは、メール送信者の特定・追跡まで可能！

SSMAXが目指す電子メール利用環境とは

Secure and Safe eMAil eXchange framework(SSMAX)

（1）送信者の匿名性と特定・追跡性の両立

送信者の匿名性を保証しつつ、

悪意のある電子メールの流通・氾濫を抑止可能！

（2）送信情報の秘匿性と検査可能性の両立

個人・機密情報の保護を保証しつつ、

情報漏洩を防止しマルウェアの流入を防止可能！

13

SSMAXとS/MIMEの比較
S/MIME普及の課題

(1)利用者はパブリックなメールアドレス証明書（電子証明書）が必要
費用負担が発生（一人当たり年間数千円）➔SSMAXは不要

(2)通信相手のメールアドレス証明書の更新・管理が必要
➔SSMAXは不要

(3)自らのS/MIME導入努力・投資だけでは効果無し
社会基盤として普及させることが必要　➔SSMAXも同じ

(4)機密情報の不正流出を防げない
暗号化ファイルのコンテンツ検査が困難　➔SSMAXは可能

(5)ウイルス等のマルウェアの流入を防げない
暗号化ファイルのセキュリティ検査が困難➔SSMAXは可能

14

（2）安心・安全電子メールシステムSSMAX

⑤悪意のあるメール対策の社会実装に向けて

(1)電子メール利用リテラシーの普及、そのためのプロモーション
- ＊メールを含め、インターネットの自由な利用には責任を伴うこと！
- ＊なりすましメールの責任は、なりすまされる組織・個人にも！

(2)S/MIMEの普及促進を！
- ＊なりすましメール対策として現時点で利用可能なもっとも効果的なツール
- ＊S/MIMEの課題は送信情報の秘匿のための暗号化機能に！
  組織間、組織から個人へのメールの、真正性保証面の利用から！

(3)将来的には、SSMAXの開発・普及を！
- ＊試作・評価・実証実験
- ＊国民的合意形成
- ＊強力な政策による社会実装推進
  （組織独自の経営判断に任せていては社会実装は進まない！）

なりすましメール対策としてのS/MIMEの可能性
S/MIMEの課題は回避可能

(1)パブリックなメールアドレス証明書（電子証明書）が必要
　費用負担が発生（一人当たり年間数千円）
　➔なりすましメール被害が想定される送信組織のみの負担で良い

(2)通信相手のメールアドレス証明書の更新・管理が必要
　通信相手それぞれのパブリックなメールアドレス証明書
　➔不要

(3)自らのS/MIME導入努力・投資だけでは効果無し
　社会基盤として普及させることが必要
　➔送信組織の努力・投資のみで良い

(4)機密情報の不正流出を防げない
　暗号化ファイルのコンテンツ検査が困難
　➔暗号化を行わないので、問題にならない

(5)ウイルス等のマルウェアの流入を防げない
　暗号化ファイルのセキュリティ検査が困難
　➔暗号化を行わないので、問題にならない

なりすましメールの責任は、なりすましされる組織に！

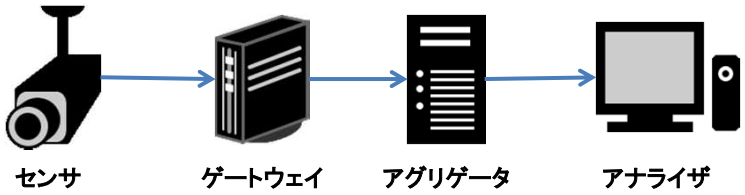
（3）送信デバイス･データの真正性保証

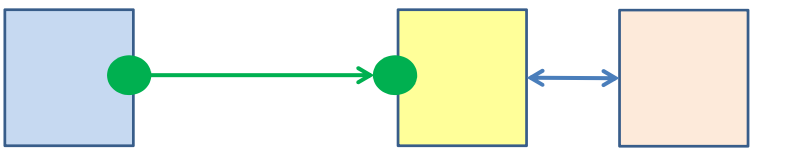
①SCOPE-PJにおける課題設定

「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」（2018～）

基軸理念	階層・重点テーマ	各層の目的
真正性保証	**情報サービス層** 基盤理論構築	リーマン幾何学を用いた新AIによる、敵対学習による誤認識の防止・真正性の高い表情を認識する手法の確立。デバイス層と連携し、要介護施設等で実証実験。
	データ管理層 耐改竄性強化	情報漏洩・改竄防止の為の、論理式に対する暗号化状態処理手法・組織暗号の安全性・秘匿検索
	ネットワーク層 **データ送信プロトコルの提案** **Secure and Safe Data Transfer Framework （SSDTF） for IoT System**	**送信デバイスや送信データの真正性の確保、送信データの保護、送信デバイスの匿名性と特定・追跡性の両立が可能な認証方式の提案、および組織・個人・IoT を対象とする認証方式全体の枠組の提案**
	デバイス層 IoT基盤実装	重要デバイスへの電子認証の埋め込みと監視・見守りカメラへの実装

SCOPE研究開発課題の全体像と「ネットワーク層」の位置付け

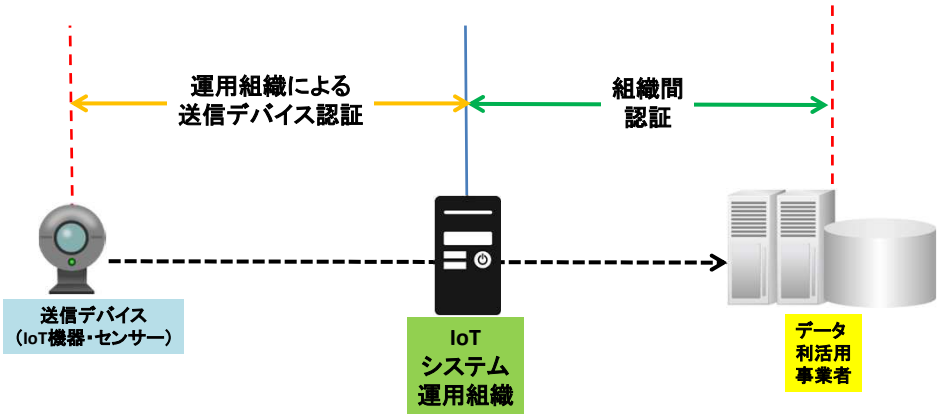




デバイス層	ネットワーク層	データ管理層	アプリケーション層
デバイスの真正性を示す鍵ペアの保有	**送信デバイス･データの真正性の確認が可能な送信方式**	格納データの真正性の確認が可能な管理方式	使用データの真正性を確認の上の表情認識

（3）送信デバイス・データの真正性保証

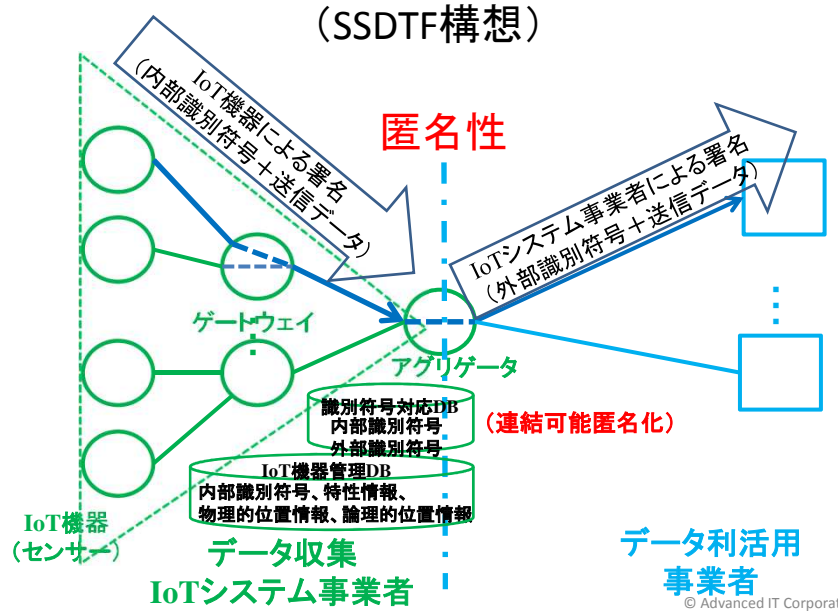
②送信デバイス・データの真正性確保方式案



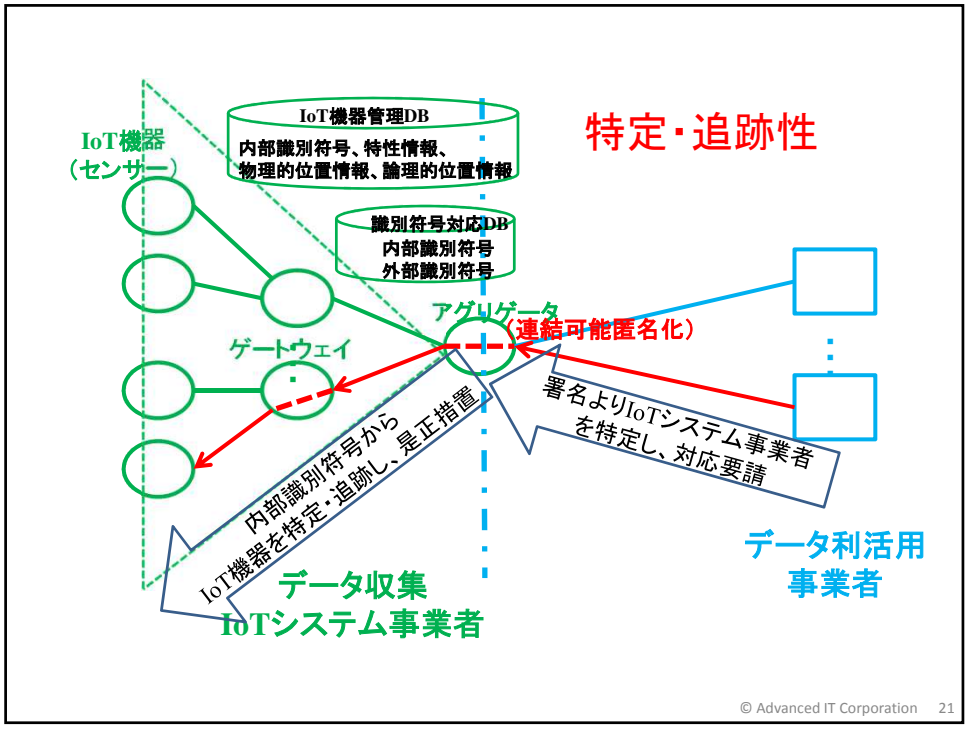
 19

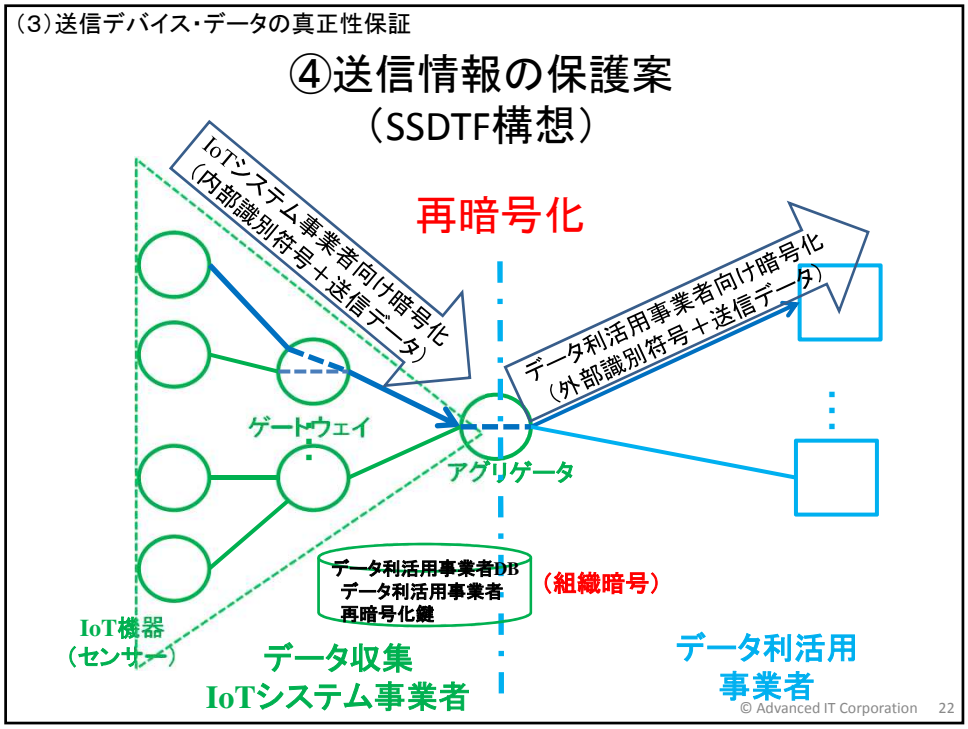
（3）送信デバイス・データの真正性保証

③送信デバイスの匿名性と特定・追跡性の両立案（SSDTF構想）



 20


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
特定・追跡性
IoT機器
（センサー）
識別符号対応DB
内部識別符号
外部識別符号
アグリゲータ
（連結可能匿名化）
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
事業者
データ収集
IoTシステム事業者
© Advanced IT Corporation 21


（3）送信デバイス・データの真正性保証
④送信情報の保護案
（SSDTF構想）
IoTシステム事業者向け暗号化
（内部識別符号＋送信データ）
再暗号化
データ利活用事業者向け暗号化
（外部識別符号＋送信データ）
ゲートウェイ
アグリゲータ
データ利活用事業者DB
データ利活用事業者
再暗号化鍵
（組織暗号）
IoT機器
（センサー）
データ収集
IoTシステム事業者
データ利活用
事業者
© Advanced IT Corporation 22

IoTシステム向けデータ送信プロトコル

Protocol	Transport	Security	Architecture
AMQP	TCP	TLS/SSL	Publish/Subscribe
CoAP	UDP	DTLS	Request/Response
DDS	UDP(TCP)	DTLS(TLS)	Publish/Subscribe
MQTT	TCP	TLS/SSL	Publish/Subscribe
REST	HTTP	HTPPS	Request/Response

主要なIoT向けデータ送信プロトコル

AMQP（Advanced Message Queueing Protocol)　OASISが標準化（もともと、AMQPコンソーシアムが金融・企業向けのメッセージ標準として定義）

CoAP（Constrained Application Protocol）　IETFでRFC（8ビットコントローラ/ネットワーク（6LoWPAN）を対象、HTTPとのインタフェース）

DDS（Data Distribution Service)
Object Management Groupで標準化

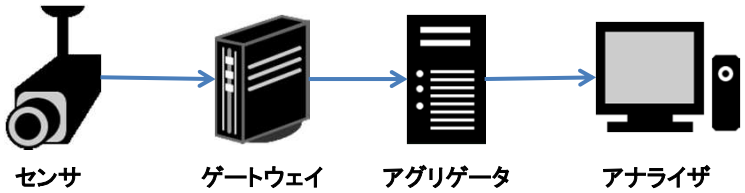
MQTT（Message Queueing Telemetry Transport）　OASISが標準化（IBMが90年代にテレメトリ用の軽いプロトコルとして開発、IoTのデータ送信の標準プロトコルとして注目されている）

REST（Representational State Transfer）
IETFでRFC（HTTP プロトコルの作成者の1人Roy Fieldingが提案、主にWorld Wide Web とHTTP に適用）

 23

（3）送信デバイス・データの真正性保証

⑤SCOPE-PJの今後の計画



デバイス層

デバイスの
真正性を示す
鍵ペアの保有

アプリケーション層

使用データの
真正性を確認
の上の表情認識

実証実験の構成

24

（3）送信デバイス・データの真正性保証

SCOPE-PJにおけるネットワーク層の目標

①SSDTP（Secure and Safe Data Transfer Protocol for IoT System）の提案
＊送信デバイスや送信データの真正性の確保
＊送信データの保護
＊送信デバイスの匿名性と特定・追跡性の両立
が可能な認証方式を
既存のIoTシステム向けデータ送信プロトコルの拡張により提案

②組織・個人・IoT を対象とする認証方式全体の枠組の提案
＊組織・個人を対象とするSSMAXのコンセプトと、
IoTを対象とするSSDTPのコンセプトとの
共通部分、異なる部分を明確にし、全体の枠組を提案

 25

（4）仮想通貨における匿名性と特定・追跡性に関する問題提起

仮想通貨の匿名性の現状

（1）一定レベルの匿名性が存在
利用者は公開鍵、アドレスにより表現され、一般に特定は困難

➔匿名性の犯罪での利用が社会問題
各国での規制が強化される方向、EUでは統一規制の動きも
仮想通貨システムへの特定・追跡性への要求
EU第5次マネーロンダリング対策指令（2018年7月9日施行）
“仮想通貨のアドレスとその仮想通貨の所有者のIDを
紐づけられる情報を各国の金融情報機関は得るべき”
仮想通貨の流れを追跡する技術開発が活発
追跡をサービスとして提供するビジネスの発展
ELLIPTIC（英国）、CHAINANALYSIS（米国）
顧客：法執行機関、徴税機関、金融情報機関等
警察庁、取引履歴を追跡するシステム導入へ（昨年8月）

 26

（2）仮想通貨の匿名性

仮想通貨の匿名性の現状

（2）一般の仮想通貨の匿名性は脆弱

プライバシー・機密情報の確実な保護は困難

➔通貨としての本格活用は困難

匿名性強化のための技術開発が活発、匿名仮想通貨の発展

匿名仮想通貨名称	主要な技術・仕組み	利用者の秘匿	支払額の秘匿
Monero[5]	リング署名、リングCT、ワンタイムアドレス、Kovri （CryptoNoteプロトコル）	○	○
Zcash[6]	zk-SNARKプロトコル （Zerocashプロトコル）	○	○
Bytecoin[7]	ワンタイムアドレス、ワンタイムリング署名（CryptoNoteプロトコル）	○	×
Verge[8]	ステルスアドレス（Wraithプロトコル）、TorやI2P	○	×
Electroneum[9]	ワンタイムアドレス、ワンタイムリング署名（CryptoNoteプロトコル）	○	×

仮想通貨における匿名性と特定・追跡性

匿名性の必要性

プライバシー保護、企業秘密保護のために

特定・追跡性の必要性

犯罪者早期逮捕、犯罪利用抑止のために

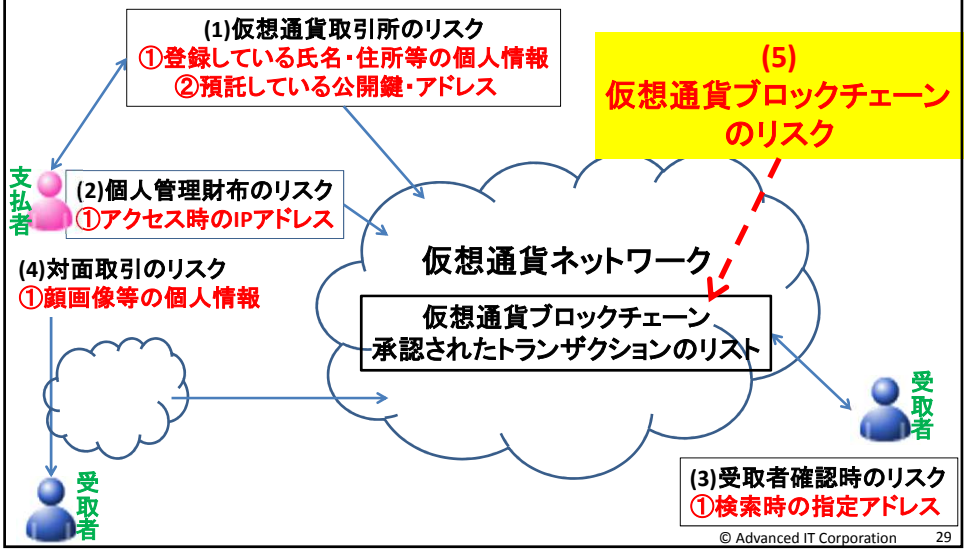
公平な徴税のために

監査可能性を保証するため

➔安心・安全な仮想通貨システムのためには、

匿名性と特定・追跡性の両立は不可欠！

仮想通貨システムにおける匿名性に関するリスクの現状



 29

トランザクション内に格納されている匿名性に関連する情報

入力欄		出力欄	
入力項目1	使用する資金の位置（支払者のアドレス、金額が指定されている）	出力項目1	支払先（受取者）の指定（受取者のアドレス）
	指定資金の使用権の証明（公開鍵、署名）		支払額の指定（金額）
入力項目2	使用する資金の位置	出力項目2	支払先（受取者）の指定
	指定資金の使用権の証明		支払額の指定
・・・・・		・・・・・	
入力項目n	使用する資金の位置	出力項目m	支払先（受取者）の指定
	指定資金の使用権の証明		支払額の指定

＜入力欄：今回の支払いで使用する原資を指定＞
＜出力欄：今回の原資による支払先・支払額を指定＞ 30

匿名性強化策として提案されている主要な技術・仕組み

匿名性に関する要件	主要な提案技術・仕組み
（1）公開鍵/アドレスからの利用者の特定不能性	ー
（2）多数のトランザクションの公開鍵/アドレスからの利用者の特定不能性	①CryptoNoteのワンタイムアドレス
（3）トランザクション間の受取者・支払者の特定不能性	②CryptoNoteのワンタイムリング署名
（4）トランザクション内の支払者・受取者の対応の特定不能性	③チャウミアンコインジョイン ④タンブルビット
（5）支払額の特定不能性（秘匿）	⑤コンフィデンシャルトランザクション（CT）

 31

仮想通貨における匿名性と特定・追跡性

匿名性の必要性←プライバシー保護、企業秘密保護のために

特定・追跡性の必要性←犯罪者早期逮捕、犯罪利用抑止のために
←公平な徴税のために
←監査可能性を保証するため

➔安心・安全な仮想通貨システムのためには、
匿名性と特定・追跡性の両立は不可欠！

今後、仮想通貨における匿名化技術の調査・分析を進め、仮想通貨における匿名性強化技術の整理・体系化を試み、その上で、特定・追跡性との両立方式の研究へ発展させることができれば・・・。

 32

インターネットにおける
匿名性と特定・追跡性の両立の重要性

インターネットは、十分なセキュリティ機能が具備されず発展
　匿名性の強いことが、その発展の起爆剤の一つであったことも事実

しかし、現在、社会の多くのシステムがインターネットベースで運用され、
また、多くの人がインターネット経由入手する情報を意思決定に利用
➔匿名性を利用した悪意のある情報の発信等の
　　インターネットの悪用が社会に与える被害は甚大に！

特定・追跡性の裏付けのある匿名性へ！
➔インターネットの悪用を困難にする仕組みの実装と、
　インターネット利用モラルの徹底が、
　　安心・安全なインターネット社会の発展には不可欠！

終