JSS2020：光輝会

私の技術・研究活動紹介

ー安心・安全なインターネット社会を目指してー

2020年9月24日　才所敏明（73歳）
（株）IT企画・代表取締役社長
（株）ZenmuTech・顧問
中央大学研究開発機構・研究員
toshiaki.saisho@advanced-it.co.jp
http://advanced-it.co.jp/

ご紹介項目

［1］東芝における活動

①1970年～1994年（情報システム部門）コンピュータ・ネットワーク関連活動
②1995年～2007年（研究開発部門）　情報セキュリティ技術関連活動

［2］IT企画における活動

①2007年～2015年（新たな活動の模索時期）
産官学の様々の活動に対する支援活動
②2015年～　（研究に軸を置いた活動）
安心・安全なインターネット社会を目指した
研究企画・推進活動

［3］私の研究の視点

ー安心・安全なインターネット社会を目指してー

[1]東芝①1970年～1994年

東芝における活動
コンピュータ・ネットワーク関連活動概要

(1)UNIX(1969年にベル研が開発)のシンプルでオープンなOSに関心　1970年～

ベル研からのレポート・成果物の入手し調査・評価

UNIXの思想に賛同し、その普及・活用を推進する

Software Tools Users Group設立と同時に参加・活動　1976年

➔1979年発足のUSENIXより、Lifetime Achievement Awardを

STUGのメンバの一人として受賞　1996年

(1997年にBrian. W. Kernighan、1998年にTim Berners-Leeが受賞したAward)

(2)社内技術開発・研究標準環境の提唱・推進　1983年～

標準EWSとしてのSUNの選定・導入➔ 東芝として、ASシリーズEWS事業化へ

(3)技術者・研究者の情報活動基盤としてのインターネット/電子メール活用推進　1985年～

InetClub(国際科学技術通信網利用クラブ)　1987年～1994年

東芝も参加、KDDIの国際回線を利用し実験

[1]東芝②1995年～2007年

東芝における活動
情報セキュリティ技術関連活動概要

情報セキュリティ研究開発の企画・推進　1995年～2007年

＜代表的なPJ＞

①“モバイルキャッシュ”を実現するセキュリティ技術

②出所不明のパケットの流通を許さない安心・安全なネットワーク

インターネットアクセスポイントでの認証・認可(IPv6ベース)

③個人ユーザ向け常時接続端末におけるセキュリティ保護技術

④バイオメトリクスリモート認証におけるセキュリティ技術の研究開発

生体認証のための認証コンテキストACBio

(Authentication Context for Biometrics)

2004年SC27WG2ブラジル会合にて初提案、2009年4月に承認

5月に国際標準ISO/IEC 24761として発行

➔プロジェクトエディタとしての活動に対し、国際規格開発賞受賞

[2]IT企画①2007年～2015年

IT企画における活動
教育・企業支援活動から研究活動への移行

(0)2007年10月　IT企画設立

(1)教育・企業支援関連活動推進

①企業・組織向け情報セキュリティ技術・事業支援活動

IT企業(5社)、日本SOHO協会、MCPC、福岡県海外企業誘致センター

②大学での教育活動

招待講演:慶応(年1回)、鳥取環境大、秋田大、九大(年1回)

非常勤講師:法政大(2010年～2017年)、日大(2012年～2017年)

③講演・講義活動

SOHO Dayシンポジューム、JASA九州支部セミナー

④その他の活動

経済産業省「情報処理技術者試験」 試験委員(1984年～2014年)

[2]IT企画①2007年～2015年

(2)中央大学研究開発機構が独立行政法人情報通信研究機構(NICT)より受託した
次の研究開発PJへ参加　(2013年～2015年)

“組織間機密通信のための公開鍵システム の研究開発
—クラウド環境における機密情報・パーソナルデータの保護と利用の両立に向けて—“

本PJの要素技術の成果である
「再暗号化機能を実現する楕円エルガマル暗号ベースの組織暗号」の活用研究を担当。
自治体および医療機関向けに実証実験を企画、
PJメンバと共に全国6か所での実証実験および13か所で説明会を実施。

学会発表:5件　情報処理学会論文誌採録論文:1件

[2]IT企画②2015年～

IT企画における活動
「安心・安全なインターネット社会に向けて」を軸とした研究企画・推進活動へ

(1)活用・普及を推進してきた電子メールの悪用への懸念
（組織暗号の活用の可能性も感じて）
➔安心・安全な電子メール利用基盤（SSMAX）の研究

(2)急増するIoTデバイス/システムのセキュリティへの関心
➔安心・安全なIoTシステムフレームワーク（SSIoT）の研究

(3)ブロックチェーン技術・支えるセキュリティ技術への関心
➔暗号資産の匿名性および特定・追跡性に関する研究

(4)インターネット上の利用者認証（本人確認）の課題への関心
➔日本の本人確認基盤（NAFJP）の研究

[2]IT企画②SSMAX

安心・安全な電子メール利用基盤SSMAX
（Secure and Safe E-mail Exchange Framework）

①様々の対策にもかかわらず、電子メールの悪用に、歯止めがかからず
- 標的型攻撃メールが依然として組織の最大の脅威
- 誹謗中傷・いじめ・デマメールによる被害大、スパムメールも依然として約40%存在
- SPF/DKIM/DMARC等の対策が進められているが、効果は限定的

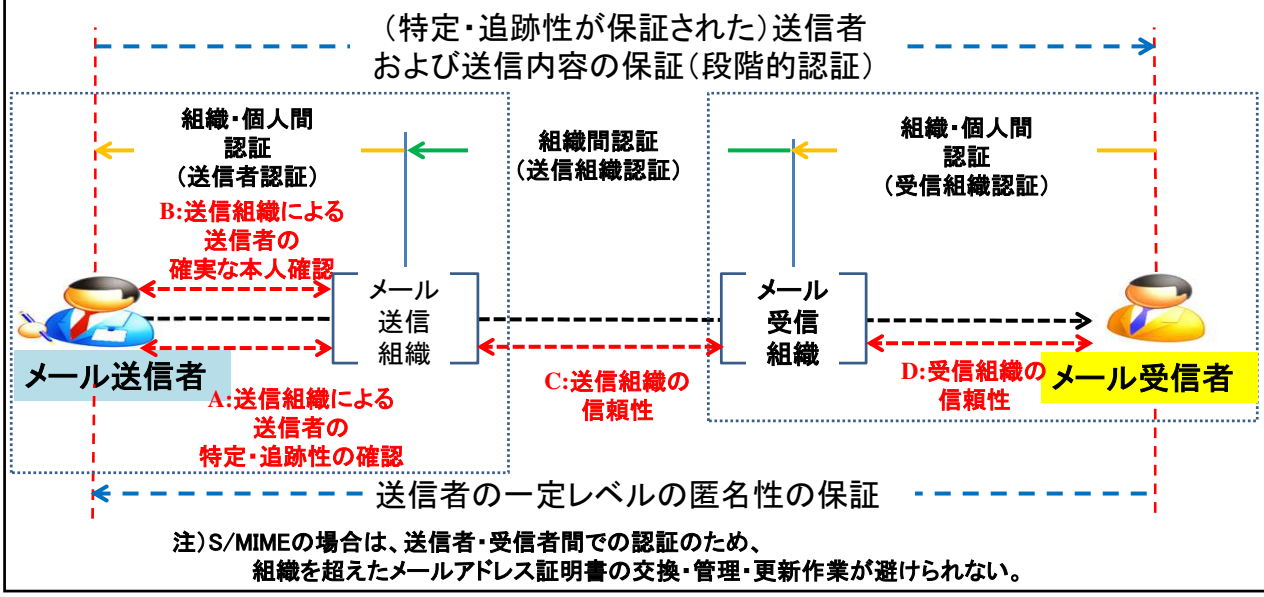
②IETFのセキュアメール規格S/MIMEの普及、遅々として進まず
- 導入費用負担、利用者の管理・更新作業負担、通信秘匿機能の利用困難さ
- 発信者の特定には、発信者（発信組織）の協力が必要

③SSMAXは、社会実装が容易で、悪用を抑止可能な、安心・安全な電子メール利用基盤
- S/MIMEの欠点の克服し、安心・安全な電子メール利用基盤の実現
  - 導入費用の低減、利用者の管理・更新作業負担不要
  - 組織の機密情報漏洩防止・マルウェア流入防止と通信情報の秘匿の両立
  - “発信者の特定には、発信者（発信組織）の協力が必要”、は変わらずだが、SSMAX採用組織間の連携により、非採用組織からのメール受信制限可能

学会発表：4件　情報処理学会論文誌採録論文：1件

[2]IT企画②SSMAX

SSMAXにおける 送信者・送信内容の認証方式



注）S/MIMEの場合は、送信者・受信者間での認証のため、
組織を超えたメールアドレス証明書の交換・管理・更新作業が避けられない。

[2]IT企画②SSIoT

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

①IoT機器の乗っ取りによるサービス/システムへの攻撃急増

セキュリティ機能が脆弱なIoT機器のインターネット接続の急増
DOS/DDOS攻撃に参加させられたIoT機器の特定の困難さ

②SSIoTは、IoT機器の保護、不正・異常IoT機器の排除
を可能とする、安心・安全なIoTシステムフレームワーク

IoT機器のなりすまし、送信データの盗聴・改ざんを防ぐ技術
IoT機器の乗っ取り・改ざんを防ぐアクセス認証・認可技術
攻撃発信源のIoT機器の特定・追跡技術

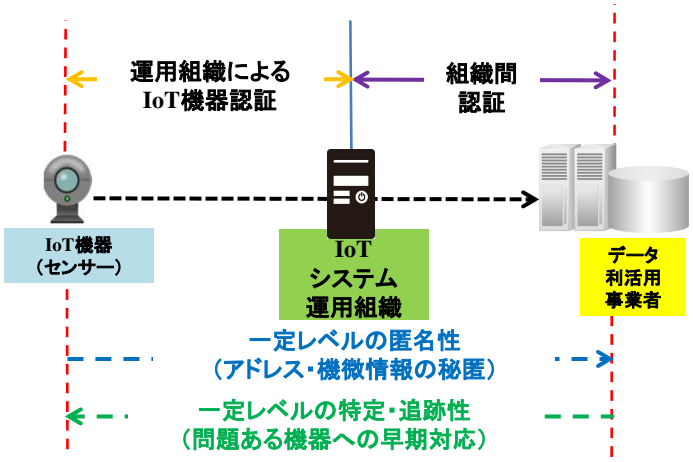
③まずは、SSDTF（Secure and Safe Data Transfer Framework）を検討

IoT機器・送信データの真正性保証をアプリケーション層で実現する仕組み
総務省の戦略的情報通信研究開発推進事業SCOPEで採択された
「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」（2018年~2019年）にて検討実施

学会発表：4件

[2]IT企画②SSIoT

SSIoTの基本構想および活用想定技術



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	

SSDTF（Secure and Safe Data Transfer Framework）

IoT機器・送信データの真正性保証をアプリケーション層で実現する仕組み

総務省・SCOPEのPJにて、IoT向けプロトコルMQTT上でのSSDTFの実現方式を提案

[2]IT企画③暗号資産

暗号資産の匿名性および特定・追跡性に関する研究

①マネーロンダリング、違法薬物取引等、暗号資産の不正・不法目的使用が横行

匿名性が高いがゆえに、不法・不正な資金移譲等に使用され、社会問題に

②暗号資産の特定・追跡性についての研究は、未だこれから

暗号資産のほとんどは、匿名性維持・強化に関心

③本研究では、匿名性と特定・追跡性が両立する

安心・安全な暗号資産システムの可能性を目指す

匿名性要件を整理し、多様な暗号資産を評価、実態を把握

多様な匿名性を高める技術の匿名化効果を評価し、匿名化技術の将来性を把握

主要な暗号資産の特定・追跡性の現状・課題を把握

以上を踏まえて、暗号資産としての要件整理し、

安心・安全な暗号資産システムフレームワークの提言を目指す

学会発表：5件 （+2件）

[2]IT企画③暗号資産

主要な暗号資産の匿名性比較結果

匿名性要件名称	ブロックチェーン				DAGチェーン						
	Bitcoin	匿名性強化			IOTA	Obyte	Nano	Hedera Hashgraph	匿名性強化		
		Monero (TypeSimple)	Zcash (Sapling)	Grin					Aidos Kuneen	Dero	Tangram
Pseudonymity of User Identification Information(UII)（利用者識別情報の仮名性）	○	○	○	○	○	○	○	○	○	○	○
OneTime-ness of UIIs（利用者識別情報のワンタイム性）	○	○	○	○	○	○	×	×	○	○	○
Unlinkability of Assets/UIIs between Transactions（トランザクション間の暗号資産/利用者識別情報の非連結性）	×	△	○	×	×	×	×	×	△	△	○
Unlinkability of Assets/UIIs within Transaction（トランザクション内の暗号資産/利用者識別情報の非連結性）	×	△	○	△	×	△	×	×	△	△	○
Concealment of Asset Amount（移転資産額の秘匿）	×	○	○	○	×	×	×	×	×	○	○

①Nano，Hedera HashgraphはBitcoinより低い匿名性

②匿名暗号資産が採用する匿名性強化技術は多様

MimbleWimble（コインミキシング）、CryptoNote（リング署名）、ゼロ知識証明

③ゼロ知識証明が高い匿名性を実現

[2]IT企画④NAFJP

日本の本人確認基盤NAFJP
（National Authentication Framework in Japan）

①公的サービス分野はマイナンバー制度で一本化、
しかし民間サービス分野は、依然として個別対応が中心

民間のインターネット上のサービス事業者の負担、利用者の利用時の負担大

個別民間事業者の本人確認業務への信頼性を担保する仕組み無し

②海外では、各国政府の指導の元、本人確認基盤の構築・運用

インドは、公的サービス分野、民間サービスも含め、政府が管轄

米国、英国は、民間サービス分野に対し、技術ガイドラインや監査・認定制度を運用

③NAFJPは、インターネット上の様々のサービスで求められる
本人確認を安心・安全・確実に提供する基盤

国や専門機関より技術基準を明確に定め、監査・認定制度により
利用者が信頼できる本人確認事業者を選定可能とする

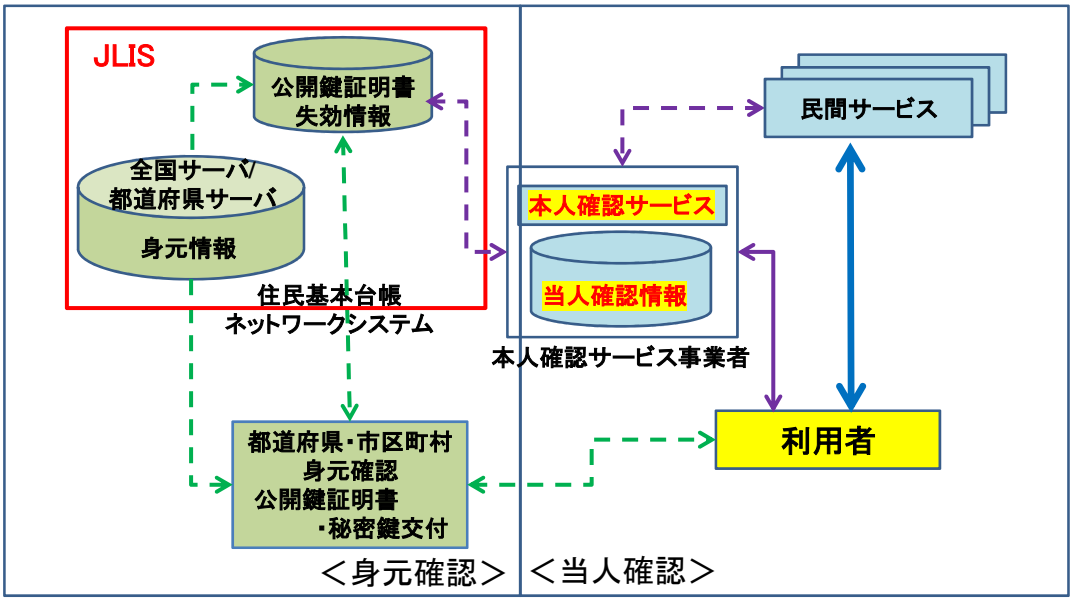
ブロックチェーンを利用した複数事業者による本人確認基盤の構築を目指す

NAFJPによる本人確認結果のグローバルな利用可能性を追求する

学会発表：3件 （+2件）

[2]IT企画④NAFJP

日本の民間サービス向け本人確認基盤NAFJP



[3]研究の視点

インターネットの現状に対する問題意識

インターネットの現状 ➔ 様々の悪意の氾濫

標的型攻撃メール/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/乗っ取られた機器の匿名性

暗号通貨によるマネーロンダリング→送金/受領者の匿名性

諸悪の根源は、インターネットの匿名性（特定・追跡困難性）！

[3]研究の視点

インターネットの利用者認証は古くて新しい問題

On the Internet, nobody knows you're a dog

Cartoon written by Peter Steiner, published by The New Yorker on July 5, 1993

[3]研究の視点

私の研究の視点
安心・安全なインターネット社会を目指して

特定・追跡性の必要性

インターネットの悪用・不正利用を安易に実行できない仕組みはもちろん、
万一の場合、悪用・不正利用者を容易に特定・追跡でき、
すみやかに止めることができる仕組みが必要

匿名性の重要性

利用者の特定・追跡情報の一般公開は以下の点で問題

＊プライバシー情報の無差別な拡散に繋がるリスク
＊自由な発言にブレーキ（インターネット活用にも？）の懸念
＊コミュニティに応じた複数の人物を演じ楽しむ権利の剥奪

➔ インターネット利用者の確実な匿名性と特定・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！

終

ご清聴、ありがとうございました。

学会発表論文等は下記サイトよりダウンロード可能です。

http://advanced-it.co.jp/2016_wp/president/