DFFTに向けた研究開発

An R&D Strategy for DFFT

データの自由で国際的な流通が，人類に巨大な価値をもたらすことは疑う余地がない。一方，それが個人の人権や，自国の経済利益，国や地域の安全保障などを棄損し得るとの懸念も存在する。DFFTはその解決に向けた日本から世界へのメッセージであり，トラスト概念導入を主眼とする。本稿ではこれへの技術的アプローチのために，まずトラストと従来のセキュリティの差異を考察する。次にDFFTのモデル化を試み，その中で特にデータ流通場面におけるトラストとは何かを定義する。以上を踏まえてDFFTを実現するための基本と考える技術課題を挙げ，その解決に向けた日立の研究開発の取り組みを紹介する。

武田 晴夫 | Takeda Haruo
石川 晃 | Ishikawa Akira
鍛 忠司 | Kaji Tadashi
高橋 健太 | Takahashi Kenta
鈴木 敏明 | Suzuki Toshiaki
手嶋 達也 | Teshima Tatsuya
山本 京子 | Yamamoto Kyoko
加藤 博光 | Kato Hiromitsu
花岡 誠之 | Hanaoka Seishi
影広 達彦 | Kagehiro Tatsuhiko
西村 信治 | Nishimura Shinji
鈴木 教洋 | Suzuki Norihiro

1. はじめに

データの自由で国際的な流通が，人類に巨大な価値をもたらすことは疑う余地がない。ウイルス性感染症の抜本的解決は直近の顕著なニーズである。一方，それが個人の人権や，自国の経済利益，国や地域の安全保障などを棄損し得るとの懸念も存在する。この問題解決のために，国際的ルール形成と革新技術開発の文理両輪の努力が世界で加速している。本稿では，特に後者を中心とする，日立の研究開発の取り組みを紹介する。

DFFT（Data Free Flow with Trust）は，2019年に日本で開催されたG20首脳会合や，2020年のWEF（The World Economic Forum：世界経済フォーラム）のダボス会議などで，日本の安倍首相（当時）から提起されたメッセージである。WEFは，これを受けて2020年5月に白書「Data Free Flow with Trust（DFFT）：Paths towards Free and Trusted Data Flows」[1)]を発行した。この白書をまとめるにあたり，日立の中西宏明会長がステアリングコミッティメンバーに加わり，その専門家グループメンバーに日立の技術戦略室の石川晃技術顧問（本稿共著者）と吉澤聡部長が加わった。WEFではこれに続いて，C4IRJ（The Centre for the Fourth Industrial Revolution Japan：第四次産業革命日本センター）から，DFFTを含むデータガバナンスのあるべき姿について，2021年3月に白書を発行予定である[2)]。同白書執筆には，経済産業省と共に日立が共同執筆者として加わっている。日立ではシステムイノベーションセンタの加藤博光センタ長と鍛忠司主管研究長（いずれも本稿共著者）が中心に活動した。日本政府としては首相メッセージに続き，2020年10月に日本の内閣官房にTrusted Web推進協議会が設立された。2021年3月にTrusted Webに関する白書を発行する予定である[3)]。同協議会には，日立の武田晴夫技師

長（本稿共著者）がメンバーとして加わっている。

本稿では，DFFT技術開発に産業界として具体的にアプローチするために，まずトラストとセキュリティの区別について2章で考察する。これに基づき，3章ではDFFTのモデル化を試みる。4章ではそのモデルの中で，特にデータ流通場面におけるトラストとは何かを定義する。5章では，以上を踏まえてDFFTを実現するために基幹と考える技術課題を挙げ，併せてそれらの解決に向けた日立の研究開発の取り組みを述べる。

2. セキュリティとトラスト

データ通信分野では従来，トラストに類似する概念としてセキュリティ／セキュアが，多く使われてきた。**図1**に示すように，一般に，ある事物がセキュアであればそれはトラストされるが，トラストされていてもセキュアとは限らない。セキュリティが完全であれば少なくとも通信路自体へのトラスト概念の導入は不要であろう。

ただし一般に完全無欠な人工物の実現は困難である。また仮に完全無欠な技術解が存在しても，それは過大仕様になり，経済性など他の要因によって実社会にとっての最適解にはならないかもしれない。実際，データ通信において，最高レベルのセキュリティ解とされるのが量子暗号であるが，特にそのようなレベルを必要としない応用にとっては，コストや処理性能などの点から過大仕様となるため，一般の社会実装には至っていない。広く実用されている技術暗号の堅牢性も，秘密鍵の安全管理を前提としているが，現実には鍵漏洩の人間系を中心とするリスクの考察が重要である。完全無欠な人工物，特に人工システムの技術的困難性と，人間系を含めた社会実装でのより大きな最適性の観点から，今，トラスト概念の導入に向かうのは必然と筆者らは考える。

図1｜セキュリティとトラスト

1. セキュア（ならば）→トラスト，トラスト（逆は偽）→セキュア
2. セキュリティが完全であればトラストは不要だが，人工物で極めて困難，少なくともオーバースペックとなり，実社会で最適解にならない，トラスト概念導入が必然である
3. セキュリティは客観（ex. The web is secure）
   トラストは主観（ex. The web is trusted by ～）
   トラストには主語が必要である
4. データ流通におけるトラストの主語は，
   送信者（S）or 受信者（R）である

3. DFFTのモデル化

セキュアとトラストのもう一つの重要な差異は，通常，セキュアが客観的な形容を表す用語であるのに対して，トラストは主観的な動作を表す用語であり，その，他動詞としての主語が必要なことである。筆者らは，データ流通の文脈でのトラストの主語は，まずデータの送信者と受信者であるべきと考える。

データの直接の送信者と受信者は，金融，企業間取引やIoT（Internet of Things）をはじめとする多くの分野で，近年，機械（コンピュータなど）であるのが普通である。ただし，たとえいかに高度な人工知能であっても，その機械のデータ送受信のルールや，データを作るロジックや，そのロジックを作るロジックなどを司っているのは人間であるべきとの立場を筆者らはとり[4]，本稿におけるデータの送信者と受信者は機械ではない人間であるとする。

なおデータの権利保持者や，権利保持者からデータを収集した者，さらに収集したデータを統計処理などしてデータ著作権を保持する者などを，送信者とは独立させるべき議論がある。しかし，筆者らは，データ権利保持者やデータ著作権者の意向に反して別人がデータを通信路に送信するケースは，そのような別人からデータ送信者にデータが渡るときの問題と，データ送信者がそのデータを通信路に送るときの問題を，分割して捉えることとする。このとき，その流通が通信路を介する場合には本稿記載のモデルが適用されるとする。通信路によらないケースについては，2者間の契約問題などの他の人間系の問題と捉えるものとする。

一方，送信者と受信者にとってのトラストの目的語は，（A）通信路と，（B）通信相手と，（C）通信するデータ

図2｜狭義通信路と（広義）通信路

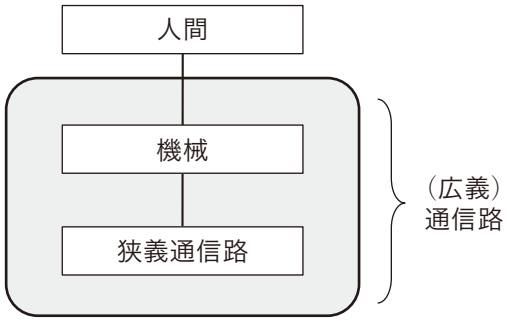
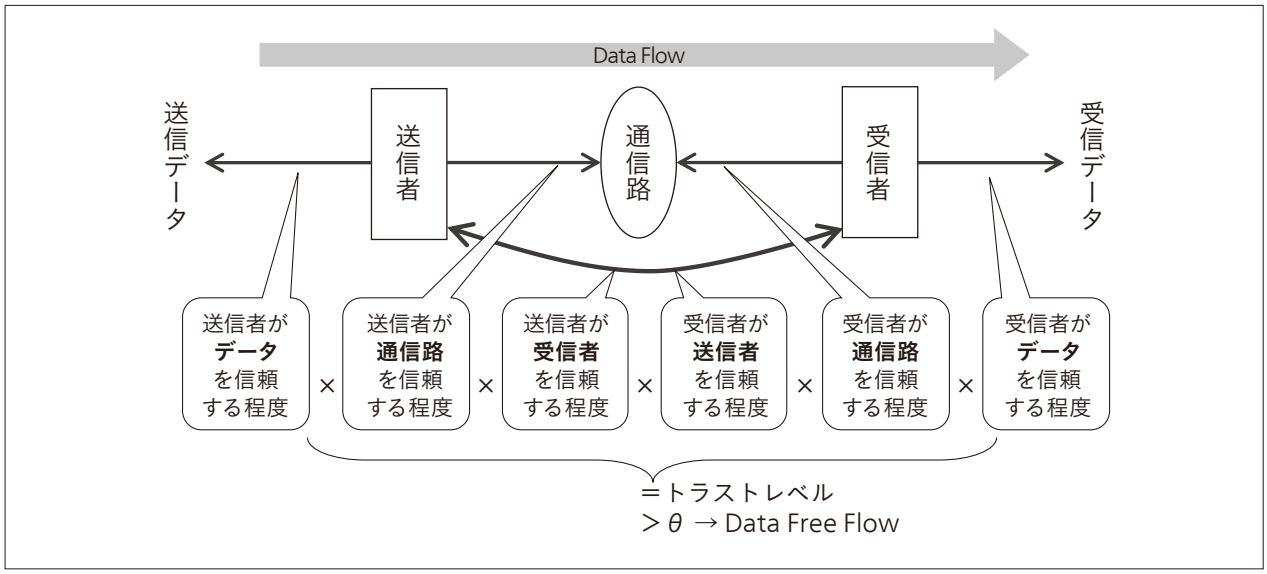


図3｜DFFTのモデル



であると筆者らは考える。通信路は，狭義には，電線や光ファイバーなどの通信線，あるいはこれにアナログ信号変調装置やデジタルプロトコル変換などのための情報処理装置，さらにこれらを運用する事業体などを加えたものである。本稿では，そのような狭義の通信路に，送受信者が司るルールやロジックなどに則ってデータを発生させて送受信する機械を加えたものを，**図2**に示すように（広義の）通信路と呼ぶことにする。

図3に筆者らが考えるDFFTのモデルを示す。データ通信の最も基本的な構成は，送信データを送信者が通信路に送り，通信路から受信者がそれを受信データとして受領するものである。データ通信のトラストとは，受信者および送信者にとっての通信路と，通信相手と，通信するデータに関するもの，と本章冒頭で定義した。それを，送信者（S：Sender）が

S(A) 通信路を信頼する程度
S(B) 受信者を信頼する程度
S(C) 送信するデータを信頼する程度

および，受信者（R：Receiver）が

R(A) 通信路を信頼する程度
R(B) 送信者を信頼する程度
R(C) 受信したデータを信頼する程度

の6指標であると書き下す。このとき，これら6指標の積をトラストレベルと定義し，このトラストレベルがある閾値／閾ベクトルを超えたときに，あるいはそのようなトラストのレベルを個々の通信場面で人間が明確に意識できるとき，データの自由な流通が起こるとし，これを筆者らはDFFTのモデルと呼ぶことにする。

このうち，（B）通信相手へのトラストおよび（C）通信するデータへのトラストなど．人間系でのトラストの定量化に関して，OECD（Organisation for Economic Co-operation and Development）より白書「OECD Guidelines on Measuring Trust」[5] が発行されている。また特に前者につき，トラストアンカーの公的ルール形成を含めた議論が活発化している。

4. 通信路のトラストの定義

技術開発の観点からは（A）通信路へのトラストの定義が当面まず重要となる。ここで通信路とは，3章で**図2**を使い述べた広義の通信路を意味している。

送信者にとっての通信路へのトラストを，「送信データが，送信者が意図した通りに受信者に伝わることを，送信者がシステムに期待できる程度」と，筆者らは定義する。また受信者にとっての通信路へのトラストを，「受信データが，送信者が意図した通りに受信者に伝わったことを，受信者がシステムに期待できる程度」と定義する。

これらは，**図4**に示すように，さらに以下のような問題分割が可能と考える。

送信データが，送信者が意図した通りに受信者に伝わることを，送信者がシステムに期待できる程度について，S→Rで忠実に伝わる程度$S(A)_1$，その間に漏洩する程度$S(A)_2$，その間に改ざんされる程度$S(A)_3$は従来，セキュリティ分野で長く論じられてきた。加えて，特に実時間性が重要な応用においては，S発信からR受信までに要する時間遅れの程度$S(A)_4$も，トラストの必要条件と考えられる。受信した相手がR本人である程度$S(A)_5$は，ネッ

図4｜通信路へのトラストの定義

送信者が意図した通りに，受信者に伝わることを， 送信者がWEBシステムに期待できる程度：	送信者が意図した通りに，受信者に伝わったことを， 受信者がWEBシステムに期待できる程度：
$S(A)_1$ S→Rで忠実に伝わる程度	$R(A)_1$ S→Rで忠実に伝わった程度
$S(A)_2$ その間に漏洩する程度	$R(A)_2$ その間に漏洩した程度
$S(A)_3$ その間に改ざんされる程度	$R(A)_3$ その間に改ざんされた程度
$S(A)_4$ S発信からR受信までに要する時間遅れの程度	$R(A)_4$ S発信からR受信までに要した時間遅れの程度
$S(A)_5$ 受信した相手がR本人である程度	$R(A)_5$ 送信した相手がS本人であった程度
$S(A)_6$ 発信を事後キャンセルできる程度	$R(A)_6$ 受信を事後キャンセルできる程度
$S(A)_7$ 当該データが流れることが合法であることが確認できる程度	$R(A)_7$ 当該データを受け取ることが合法であることが確認できる程度
$S(A)_8$ Sが当該データを意図せずに漏洩している程度	$R(A)_8$ Rが当該データを意図せずに漏洩する程度
$S(A)_9$ R受信後にSが意図しない負の波及効果を生む程度（例：炎上，自殺）	$R(A)_9$ R受信後にRが意図しない負の波及効果を生む程度（例：ウィルス拡散）
$S(A)_{10}$ 以上を事後検証可能な程度	$R(A)_{10}$ 以上を事後検証可能な程度
（a）送信者から通信路へのトラスト	（b）受信者から通信路へのトラスト

トワーク上の通信者のアイデンティティ管理の要否について，近年，活発に議論が行われている。発信を事後キャンセルできる程度$S(A)_6$は，メール誤送信による情報漏洩リスクなどから，企業情報システムを中心にニーズがある。当該データが流れることが合法であることが確認できる程度$S(A)_7$は，次章でも記載する知識処理の高度な技術課題であるが，通信路へのトラストレベルを高め，人間への負荷を減ずるためにニーズは高い。Sが当該データを意図せずに漏洩している程度$S(A)_8$は，狭義の通信行為以前の問題ではあるが，（広義）通信路の問題であり，$S(A)_2$とは区別して挙げた。R受信後にSが意図しない負の波及効果を生む程度$S(A)_9$は，不特定多数を受信者とする送信が，しばしば「炎上」し，その結果として自殺者が出るなどに至る社会問題の大きさに鑑み，通信路のトラストの要件に加味を検討することとした。以上を事後検証可能な程度$S(A)_{10}$は，今後のデータ流通のトラストにおいて，特に重要な条件となろう。

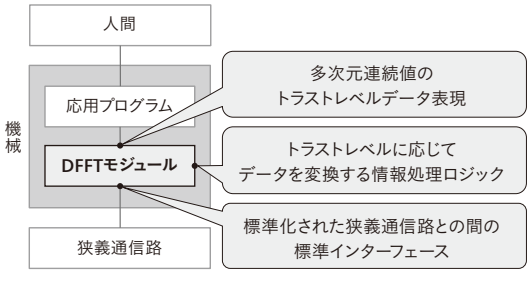
受信データが，送信者が意図した通りに受信者に伝わったことを，受信者がシステムに期待できる程度については，S→Rで忠実に伝わった程度$R(A)_1$，その間に漏洩した程度$R(A)_2$，その間に改ざんされた程度$R(A)_3$，およびS発信からR受信までに要した時間遅れの程度$R(A)_4$は，$S(A)_1$〜$S(A)_4$と同じ要素を受信者側から記述したものである。送信した相手がS本人であった程度$R(A)_5$，受信を事後キャンセルできる程度$R(A)_6$，当該データを受け取ることが合法であることが確認できる程度$R(A)_7$，およびRが当該データを意図せずに漏洩する程度$R(A)_8$は，$S(A)_5$〜$S(A)_8$を反対の立場から挙げた双対問題である。R受信後にRが意図しない負の波及効果を生む程度$R(A)_9$は，コンピュータウイルス拡散が通信路トラストを失うことが明らかなように，広義通信路へのトラスト上考慮することが必須であろう。以上を事後検証可能な程度$R(A)_{10}$は，今後のデータ流通のトラストにおいて，$S(A)_{10}$と同様に重要条件となろう。

5. DFFTの技術課題と日立の戦略

図2で人間と狭義通信路の媒介であるとした機械を，(イ)応用に依存した情報処理機能である応用プログラムと，（ロ）応用に依存せずDFFTを汎用で担うDFFTモジュールに二分する。DFFTモジュール（ロ）に関する主要な技術開発課題は，**図5**にも示すように，応用プログラムとのインタフェース，モジュール自体の情報処理機能，および狭義通信路とのインタフェースにつき，下記と考える。

第一はトラストレベルのデータ表現である。トラスト表現については，従来の一次元離散値(classifiedか否か，

図5｜DFFTへの技術課題



など）を基本とするセキュリティの表現レベルから，多次元連続値に進化させるべきと考える。その次元とは，3章で述べた通信路や通信相手を含めたトラストであり，通信路については4章で列挙したレベルの条件を記述できるものであり，さらにはそのデータが，誰がいつどこでなぜどのように使うのか，など，多様な利用条件などを表現できる形式であるものとすべきである。そのような多様な記述力をもつトラストレベルに応じて，応用プログラムは標準インタフェースを介してDFFTモジュールにアクセスする。

第二はトラストレベルに応じてデータを変換する情報処理ロジックである。高いトラストレベルから低いレベルへの変換は非可逆情報圧縮の一般化と捉えることもできる。低いトラストレベルから高いレベルへの変換は，近年研究が活発化している暗号空間における情報処理の一般化と捉えることもできるが，特に逆問題としての知識処理が中心的役割を果たすと考える。さらに後者は，現行システムからの移行において，応用プログラムや人間送受信者への負荷の増大を極力抑制する観点から，DFFT実現の加速にとっても重要となろう。

第三は標準化された狭義通信路とDFFTモジュールの間の標準インタフェースである。ここではそのインタフェースとして通信データを通信路で保護するための暗号に関する検討も重要な要素となる。暗号は，セキュリティのレベルに加えて，符号化・復号化に要する時間や経済コストなど，社会実装上の最適化の観点で，その時々の最有力技術が採用されるべきである。現時点では，秘密鍵とバイオメトリクスとを対応させるPBI（The Public Biometrics Infrastructure）技術を，筆者らは今後の有力技術と，本号別稿[6]で紹介している通り考えている。

日立製作所の研究開発グループの技術開発部門は，カバーすべき技術領域ごとに，現在10余りの研究センタの組織に分割運営されている。

以上，本稿で述べたDFFT研究は，このうち人工知能技術領域を担う人工知能イノベーションセンタと，通信技術領域を担うデジタルテクノロジーイノベーションセンタと，暗号技術領域を担うシステムイノベーションセンタとの3研究センタが中心となり，組織を横断する立場にある技師長，技術戦略室などのメンバーから成るステアリングチームが統括の任にあたり，組織を横断するプロジェクトの日立の仕組みである「特別研究」の名の下に現在進められている。

6. おわりに

DFFTに向けた産業界の取り組み例として，日立の活動を紹介した。これらをオープンにすることにより，世界の産官学の多くのステークホルダー各位との協創[7]がさらに加速・拡大し，DFFTの早期の実現に貢献できることを願っている。

参考文献など

1）“Data Free Flow with Trust(DFFT):Paths towards Free and Trusted Data Flows”, The World Economic Forum（2020.5）, http://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20_Flows_2020.pdf

2）“Updating Governance Mechanism for Rebuilding Trust”, World Economic Forum Centre for the Fourth Industrial Revolution Japan（2021）

3）Trusted Webホワイトペーパー ver.1.0，Trusted Web推進協議会，内閣官房デジタル市場競争本部事務局（2021.3）

4）武田晴夫：人間を指向した研究開発，日立評論，91，4，349～353（2009.4）

5）”OECD Guidelines on Measuring Trust”, Organisation for Economic Co-operation and Development（2017.11）https://doi.org/10.1787/9789264278219-en

6）鍛忠司，外，Society 5.0を支えるトラスト＆セキュアなサービス・システム，日立評論，103，2，247～251（2021.3）

7）武田晴夫：日立グループのR&D戦略，日立評論，95，6-7，416～423（2013.6）

執筆者紹介

武田 晴夫
日立製作所 研究開発グループ 技師長

石川 晃
日立製作所 研究開発グループ 技術戦略室 技術顧問

鍛 忠司
日立製作所 研究開発グループ システムイノベーションセンタ 主管研究長

高橋 健太
日立製作所 研究開発グループ システムイノベーションセンタ セキュリティ研究部 主管研究員

鈴木 敏明
日立製作所 研究開発グループ デジタルテクノロジーイノベーションセンタ コネクティビティ研究部 主任研究員

手嶋 達也
日立製作所 研究開発グループ 中央研究所企画室 主任研究員

山本 京子
日立製作所 研究開発グループ 人事総務本部

加藤 博光
日立製作所 研究開発グループ システムイノベーションセンタ センタ長

花岡 誠之
日立製作所 研究開発グループ デジタルテクノロジーイノベーションセンタ センタ長

影広 達彦
日立製作所 研究開発グループ 人工知能イノベーションセンタ センタ長

西村 信治
日立製作所 研究開発グループ 基礎研究センタ センタ長

鈴木 教洋
日立製作所 執行役常務 CTO 兼 研究開発グループ グループ長