



# 国際標準化動向からみた、近接型非接触通信の最新技術

やまもと ひであき やまこし きみひろ もりた てつし  
山本 英朗 / 山越 公洋 / 森田 哲之  
NTTセキュアプラットフォーム研究所

近年、NFC (Near Field Communication) 対応スマートフォンや非接触ICカードなどに代表される近接型非接触通信を用いたサービスが急速に普及しています。ここでは、国際標準化動向からみた、近接型非接触通信の最新技術を紹介します。

## 近接型非接触通信とは

近接型非接触通信とは、最大通信距離がおおむね10 cm程度、搬送周波数13.56 MHz帯の磁界を通信媒体に用いた双方向無線通信技術です。この技術は、ICカードとしての使い方においては、入退室管理・鉄道改札・電子決済の分野を中心に定着しています。

近年、携帯電話への適用を中心に、近距離無線通信 (NFC: Near Field Communication) が普及しています。NFCとは、近接型非接触ICカード同様、13.56 MHz帯の磁界を通信媒体に用いた双方向通信方式です。

NFCでは、その利用シーンに応じて3種類のモードが定義されています。

- ・NFC端末をICカードのように機能する「カードエミュレーションモード」
- ・デバイスとの情報を読み書きする機能を果たす「リーダーライタモード」
- ・NFC搭載端末間どうして通信を行う「P2Pモード」

## 近接型非接触通信の特徴

近接型非接触通信は、ほかのシステムにはない特徴的なヒューマンインタフェースを持っています。それは、サービスを受けたいという利用者の意思を、非接触ICカードをリーダーライタに「かざす」という行為によって表すことです<sup>(1)</sup>。

従来の近接型非接触通信は、非接触ICカードとリーダーライタを組み合わせた使い方が中心でした。近年では、近接型非接触通信機能を備えた端末がNFC対応スマートフォンやタブレットなどに拡大してきました。これらの高度な機能・性能 (バックエンドのネットワーク、画面保有、高速なCPU、セキュアチップ) により、「端末をかざす」という意思表示後に多彩なサービスを楽しむことができるようになりました。

より具体的には、従来の非接触ICカードを用いて提供されてきた認証や決済に加え、端末をかざすことによってURLやクーポンを取得し、それらに関連するインターネットサイトへの誘導、またプリンタ等の民生機器にかざすことによって、従来は煩雑だった、無線LAN・Bluetoothの通信設定手順の簡素化が期待されています。

## 関連標準化団体の概要

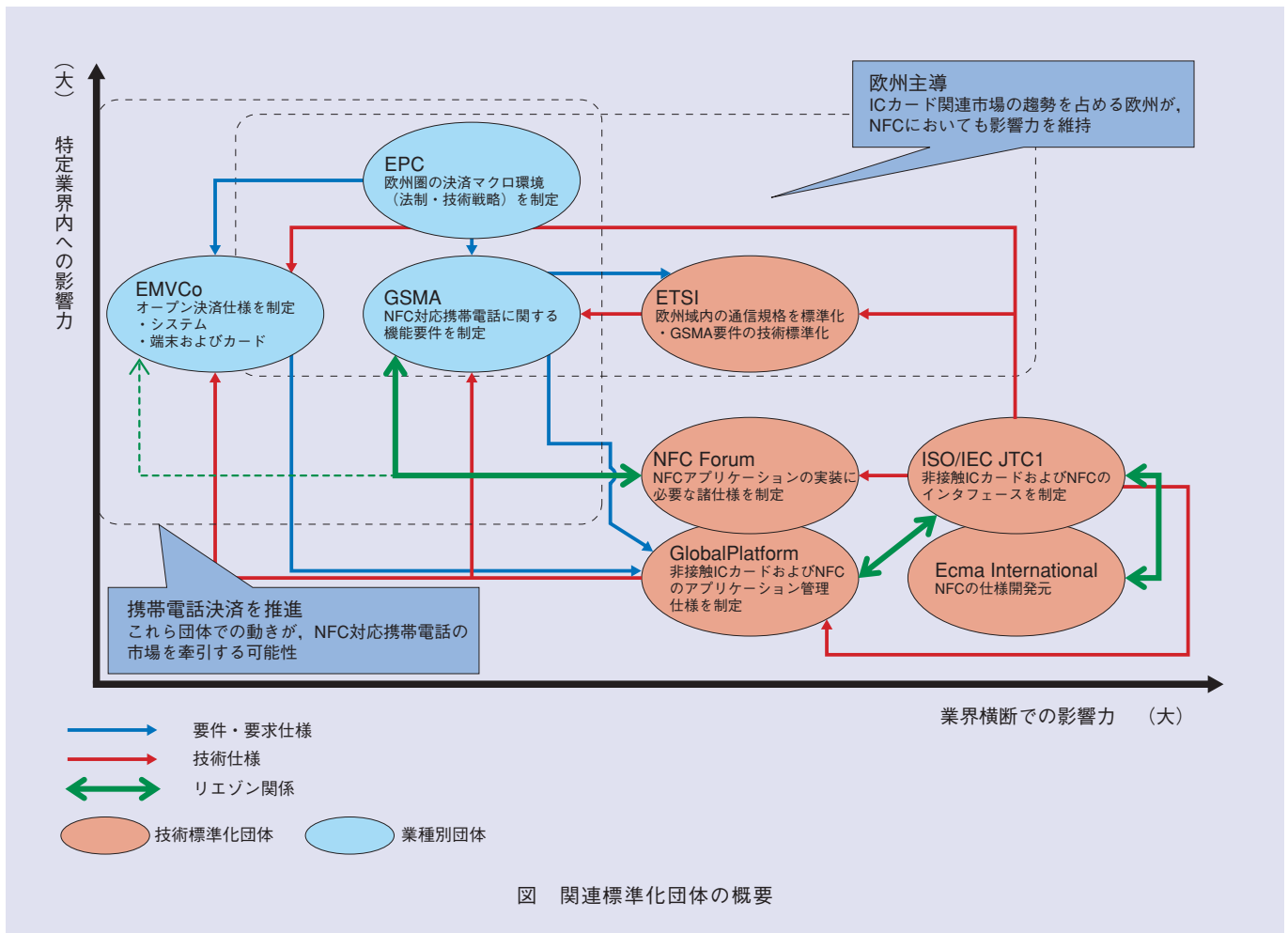
近接型非接触通信にかかわる標準化団体の概要を図に示します。一口に

「非接触通信」といっても、その技術仕様はさまざまな団体に制定されています。また、当該仕様は他団体の規格を引用したり、自団体に制定した規格を他団体に提案したりすることにより、相互に連携しています。近接型非接触通信の分野において業界横断的な影響力の強い標準化団体は、ISO/IEC JTC1 (Joint Technical Committee 1)、NFC Forum、GlobalPlatformです。また、業種ごとに影響力の強い標準を制定している標準化団体は、GSMA、EMVCo、EPC (European Payments Council) です。また図に示すように、他団体とのリエゾンを構築し、仕様提案・情報交換がなされています。

近接型非接触通信の規格において、無線インタフェースなど下位レイヤの規格は、主にISO/IEC JTC1が制定しています。プラットフォーム・アプリケーションなど上位レイヤの規格は、主にGlobalPlatform・NFC Forumが制定しています。決済・携帯電話などを扱う業種別団体では、既存規格の引用と当該団体に独自に定めた規格を組み合わせ、当該団体としての規格を制定しています。

以上により、近接型非接触通信を用いたシステムを実現するためには、異なる標準化団体がそれぞれ制定した規格を俯瞰したうえで、上位レイヤから下位レイヤまでの全体システムを整合性をもって構築する必要があるといえます。

次に、各団体の概要を示します。



- ・ ISO/IEC JTC1：ISOおよびIECにまたがった標準化団体。情報技術の分野に関する規格を制定<sup>(2), (3)</sup>
- ・ Ecma International：情報通信分野における国際的な標準化団体であり、NFCに関する実質的な仕様開発元<sup>(4)</sup>
- ・ GlobalPlatform：VISAを中心に開発されたOpen Platform技術をベースに設立された、マルチアプリケーションカードの管理システムに関する標準化団体<sup>(5), (6)</sup>
- ・ NFC Forum：NFC技術を普及させ、定めた仕様に適合した製品を広めることを目的とした団体<sup>(7)</sup>

- ・ ETSI (The European Telecommunications Standards Institute)：情報通信分野における欧州連合域内の標準化団体<sup>(8)</sup>
- ・ GSMA：GSM (Global System for Mobile Communications)方式 (現在は3G方式含む)を採用している通信事業者の団体。NFC対応携帯電話技術の標準化および普及を推進<sup>(9)</sup>
- ・ EPC：EU域内での決済インフラに関する標準化団体<sup>(10)</sup>
- ・ EMVCo：接触・非接触ICカードおよびNFC対応携帯電話を利用した決済の国際的な互換性を保証するためにクレジットブランド

4社が出資して設立した企業体<sup>(11)</sup>  
以下では、近接型非接触通信の分野において業界横断での影響力の強い3団体について説明します。

## 各標準化団体の活動概要

### ■ISO/IEC JTC1

非接触ICカードおよびNFCに関する技術は、「情報技術の分野」と位置付けられており、JTC1が標準化を行っています<sup>(12)</sup>。

ISO/IEC JTC1配下には、18のSC (Sub Committee) が構成されています。近接型非接触ICカードは、SC17で審議されており、NFCはSC6



で審議されています。これらの規格を表1に示します。

近接型非接触ICカードに関する国際標準規格（ISO/IEC14443シリーズ）は、2001年に初版が制定されました。一方、NFCに関する国際標準は、日本国内・欧州でそれぞれ普及している通信方式を基に進められ、2004年にISO/IEC18092（NFC IP-1）が制定されました。その後、ISO/IEC18092およびISO/IEC14443などの

通信方式を共存させて、どれを利用するかを選択する仕組みが、ISO/IEC21481（NFC IP-2）として規定されました。

ISO/IEC JTC1では、規格制定後に定期的に規格の見直しがかかるルールになっており、現在は、近接型非接触ICカード・NFCとも、その見直しを中心です。その状況において、注目すべき技術を以下に紹介します。

- ① 超高速伝送：大容量データを

格納したICカードを使うシステムにおいては、データ通信を高速に行えることが重要です。現状、ISO/IEC14443シリーズで規定されているリーダライタ・ICカード間の通信速度は106～848 kbit/sと比較的低速です。現在、1.70～6.78 Mbit/sに対応する通信方式がISO/IEC14443シリーズへの追加仕様として審議中で、2013年に制定の見通しです。

表1 ISO/IEC JTC1における、近接型非接触通信に関する規格一覧

(2012年10月現在)

	規格書名	概要	版数（出版年月）
近接型非接触ICカード	ISO/IEC 14443-1 Physical characteristics	物理的特性	2（2008年6月）
	ISO/IEC 14443-2 Radio frequency power and signal interface	電力伝送および信号インタフェース	2（2010年9月）
	ISO/IEC 14443-3 Initialization and anticollision	初期化および衝突防止	2（2011年4月）
	ISO/IEC 14443-4 Transmission protocol	伝送プロトコル	2（2008年7月）
	ISO/IEC 10373-6 Test Methods-Proximity cards	ISO/IEC 14443の試験方法	2（2011年3月）
NFC	ISO/IEC 18092 Interface and Protocol (NFCIP-1)	近距離通信用インタフェースおよびプロトコル（NFC IP-1）	1（2004年4月）
	ISO/IEC 21481 Interface and Protocol -2 (NFCIP-2)	近距離通信用インタフェースおよびプロトコル（NFC IP-2）	2（2012年7月）
	ISO/IEC 22536 NFC IP-1 RF interface test method	NFCIP-1における、RFインタフェースの試験方法	1（2005年7月）
	ISO/IEC 23917 NFC IP-1 Protocol Test Methods	NFCIP-1における、プロトコルの試験方法	1（2005年11月）
	ISO/IEC 28361 Near Field Communication Wired Interface	近距離通信ワイヤードインタフェース	1（2007年10月）
	ISO/IEC 13157-1 NFC-SEC: NFCIP-1 Security Services and Protocol	NFCIP-1における、セキュリティサービスプロトコル	1（2010年4月）
	ISO/IEC 13157-2 NFC-SEC cryptography standard using ECDH and AES	ECDHおよびAESを用いるNFC-SEC暗号基準	1（2010年4月）

NFC IP-1：ISO/IEC 14443 Type-AとFeliCa（ソニーが開発した非接触通信方式）に対応したインタフェースおよび通信プロトコルを定義した規格

NFC IP-2：NFC IP-1に、ISO/IEC 14443 Type-BインタフェースおよびISO/IEC 15693インタフェース（近傍型非接触通信）を追加した規格

ワイヤードインタフェース：NFCトランシーバとNFCフロントエンドとの間の有線によるデジタルインタフェース

ECDH（Elliptic Curve Diffie-Hellman）：楕円曲線暗号方式を用いた鍵配送方式

AES（Advanced Encryption Standard）：米国商務省標準技術局によって制定された、新世代標準暗号化方式



② PXD (Proximity Extended Device) :ISO/IEC 14443シリーズの初版制定当時、リーダライタとICカードは別々のデバイスであることが前提でした。その後の技術進歩により、1台の携帯端末でリーダライタ機能およびICカード機能を兼用できるようになりました。1台のモバイル端末にこれら2つの機能を実装し、両機能を切り替えて使うニーズが顕在化し、そのための仕組みがISO/IEC14443シリーズへの追

加仕様として審議中です。

#### ■NFC Forum

NFC Forumは、ISO/IEC JTC1で規定されていない、上位レイヤ・実装規約の規格制定が主な標準化の対象領域です。

NFC Forumが公開している技術仕様を表2に示します。NFC Forumは、前述の3モードと、3種類の通信インタフェース (ISO/IEC14443 Type-A, 同Type-B, FeliCa) とを適切に組み合わせるようするための機能を「モード・スイッチ」とし

て定義しています。また、2010年には、NFCを実装した機器がNFC Forum規格に準拠していることを認証するプログラム (N-Mark) が始まりました。

NFC Forumにおいて注目すべき技術として、NDEF (NFC Data Exchange Format) およびRTD (NFC Record Type Definition) を紹介します。NDEFとは、NFCのアプリケーションにおけるデータフォーマットであり、RTDとは、アプリケーション種別ごとに規定されたNDEFレコードのフォーマットです。これらの規格を用

表2 NFC Forumの規格一覧

(2012年10月現在)

	規格書名	概要	版数 (出版年月)
上位層に関する規定	NFC Data Exchange Format (NDEF)	NFCアプリケーション用のデータフォーマット	1.0 (2006年7月)
	NFC Record Type Definition (RTD)	NDEFで使用されるレコード	1.0 (2006年7月)
	Text Record Type Definition	文字表示用のレコード	1.0 (2006年7月)
	URI Record Type Definition	WEB TO系のサービス用のレコード	1.0 (2006年7月)
	Signature Record Type Definition	電子署名用のレコード	1.0 (2009年10月)
	Smart Poster Record Type Definition	スマートポスタ用のレコード	1.0 (2006年7月)
	Generic Control Record Type Definition	複数機能実装用のレコード	1.0 (2008年3月)
	Type 1 Tag Operation Specification	TOPAZでのNDEFデータの読み書き	1.1 (2011年4月)
	Type 2 Tag Operation Specification	MIFARE UltralightでのNDEFデータの読み書き	1.1 (2011年5月)
	Type 3 Tag Operation Specification	FeliCaでのNDEFデータの読み書き	1.1 (2011年6月)
	Type 4 Tag Operation Specification	伝送プロトコルがISO/IEC14443-4準拠, APDUがISO/IEC 7816-4に準拠の製品でのNDEFデータの読み書き	2.0 (2010年11月)
ハンドオーバに関する規定	Connection Handover	民生機器での無線インタフェース選択	1.2 (2010年7月)
	Bluetooth Secure Simple Pairing Using NFC	Bluetoothへのハンドオーバ	1.0 (2011年10月)
P2Pに関する規定	Logical Link Control Protocol	独自伝送プロトコル	1.1 (2011年6月)
	Simple NDEF Exchange Protocol	LLCP上でのデータ伝送プロトコル	1.0 (2011年8月)
国際標準規格のサブセットに関する規定	NFC Digital Protocol	ISO/IEC 14443およびNFC関連標準のサブセット	1.0 (2009年4月)
その他	NFC Activity Specification	NFCファームウェアのAPI	1.0 (2010年11月)
	NFC Analog Specification	NFCのアナログインタフェース	1.0 (2012年7月)

TOPAZ: Innovision R&T社の製品。非接触インタフェースは、ISO/IEC 14443 Type-Aに準拠

MIFARE Ultralight: NXPセミコンダクタ社の製品。非接触インタフェースは、ISO/IEC 14443 Type-Aに準拠

FeliCa: ソニーが開発した近接型非接触通信方式。非接触インタフェースは、ISO/IEC 18092に準拠

APDU: Application Data Unit



表3 GlobalPlatformにおける、近接型非接触通信に関する規格一覧

(2012年10月現在)

	規格書名	概要	版数 (出版年月)
カード関連	Card Specification	GP準拠のマルチアプリケーションICカードにおける、コマンド仕様やセキュリティ	2.2.1 (2011年1月)
	Amendment C-Contactless Services	GP準拠のマルチアプリケーションICカードにおける、非接触インタフェースによるサービス	1.0.1 (2012年2月)
デバイス関連	Secure Element Access Control	上位装置がセキュアエレメントにアクセスする方法	1.0 (2012年5月)
システム関連	System Messaging Specification for Management of Mobile-NFC Services	モバイルNFCサービスにおけるシステム間のメッセージやプロファイル	1.0 (2011年2月)

セキュアエレメント (Secure Element) : 外部からの悪意を持った解析攻撃に耐えられるように設計され、データを安全に格納するメモリや暗号機能を実装した半導体の総称。SEの実装形態は、カード形状のほか、SIM、機器組み込みデバイスなどがある

いることで、URLへの誘導やNFCスマートフォン画面への表示・電子署名などが可能となり、NFC対応スマートフォンを用いた多彩なサービスの展開が可能となります。

## ■GlobalPlatform

GlobalPlatform (GP) は、業界中立的な立場で多様な分野に対してICカードアプリケーションの管理を中心とした標準の策定・展開を推進しています。GPで規定された規格は、SIM (Subscriber Identity Module) にも採用されており、モバイル系ICカードアプリケーションの管理における事実上の標準となっています。また、GPには、適合性試験による認定プロセスが存在し、当該試験の仕様が規定されています。近年、GPは非接触通信デバイスを管理する仕様の標準化にも取り組んでいます。

GPが公開している規格のうち、近接型非接触通信に関連するものを表3に示します。NFC対応スマートフォンのさらなる普及により、GPが近接型非接触通信デバイスを用いたサービスに及ぼす影響は、ますます大きくなるものと想定されます。

この状況において、NTTはGPの理

事や会議ホストを務めるなど、規格制定や会議体運営に貢献しています。

GPにおいて審議されている注目すべき技術として、マルチセキュアエレメント (マルチSE) を紹介します。マルチSEとは、携帯端末内に存在する複数のSEをサーバから遠隔で安全管理するための仕組みです。これにより、携帯電話内の複数のアプリケーションを連携させたサービス (例えば、SIM内の本人情報と携帯電話本体の電子マネーアプリケーションを組み合わせ、電子マネーチャージ) が実現できます。



NFC対応スマートフォンに代表される携帯端末の普及により、従来の非接触ICカードでの使い方を超えた、新たな利用シーンが広がっていくことが期待されます。また、携帯電話の利用に不可欠なSIMも、従来の加入者識別専用から、SIM空きメモリ領域へのアプリケーション搭載による高セキュリティなサービスの用途に広がるものと見込まれます。

この流れにおいて、近接型非接触通信技術、およびセキュアデバイスを活

用しつつ、上位レイヤの標準規格が整備されていくものと想定されます。

NTTは、これらにかかわる標準化活動を通じて、誰もが世界中どこにいても、安心・安全かつ簡単にICTサービスを利用できるような、オープンかつ相互運用可能な情報インフラストラクチャの実現を目指します。

## ■参考文献

- (1) 技術基礎講座：“非接触ICカード技術第2回 サービスに応じた非接触ICカードとリーダライタ,” NTT技術ジャーナル, Vol.20, No.2, pp.75-78, 2008.
- (2) <http://www.iso.org/iso/home.html>
- (3) <http://www.iec.ch/>
- (4) <http://www.ecma-international.org/>
- (5) 庭野・五郎丸：“GlobalPlatformにおける標準化動向,” NTT技術ジャーナル, Vol.18, No.9, pp.76-79, 2006.
- (6) <http://www.globalplatform.org/>
- (7) <http://www.nfc-forum.org/>
- (8) <http://www.etsi.org/>
- (9) <http://www.gsm.com/>
- (10) <http://www.europeanpaymentscouncil.eu/>
- (11) <http://www.emvco.com/>
- (12) 山本・五郎丸・池田・庭野：“ISO/IECにおける、ICカード関連技術の標準化動向,” NTT技術ジャーナル, Vol.19, No.4, pp.64-67, 2007.