JICSAP
一般社団法人 ID認証技術推進協会

HCE 導入ガイドライン

Version 1.0

一般社団法人 ID 認証技術推進協会

2019 年 3 月 4 日

目次

1. はじめに

本ガイドラインは、非接触 IC カードを使ったシステムを導入済みの企業・組織が HCE（Host-based Card Emulation）技術を使ったスマートフォンに対応する、または新規に非接触 IC カードを使ったシステムを導入する企業・組織が HCE 技術を使ったスマートフォンにも対応しようとする際に、参考となるべく情報を取りまとめたものである。

また本ガイドラインでは、HCE 技術を使ったスマートフォンに対応するにあたって、どのようなメリットがあり、どのような観点で検討し、どのように導入すればよいかについても説明している。

2. HCE の概要

本章では、HCE の概要と特徴について述べる。

HCE は、スマートフォンなどのデバイス（以下、総称してスマートフォン）において、ホスト CPU（アプリケーションを実行するプロセッサ）で非接触 IC カード（以下、IC カード）をエミュレートする仕組みである。従来のスマートフォンでは、セキュアエレメント（以下、SE）と呼ばれる IC チップによって IC カードをエミュレートしていた。HCE を使うと、SE を持たないスマートフォンでも IC カード機能を実現できる。

HCE は、Android OS のバージョン 4.4 以降でサポートされている。とくに断りのない限り、本書の説明は Android OS の HCE 機能を前提としている。また、とくに断りのない限り、スマートフォンは Android スマートフォンを指す。なお、HCE 機能を使うためには、スマートフォンが NFC（Near Field Communication。近接無線通信技術）に対応している必要がある。

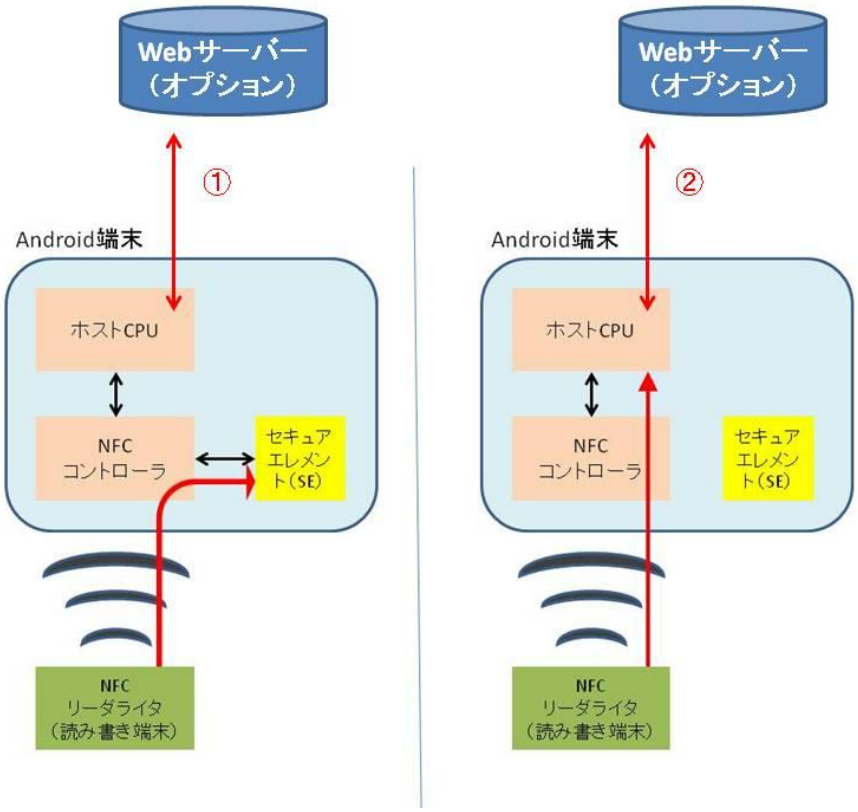

図 2-1 SE によるカードエミュレーション（左）と、HCE によるカードエミュレーション（右）

2.1 HCE の特徴

HCE の特徴を、IC カードそのものを使用する場合や、SE によるカードエミュレーションを使用する場合と対比させながら述べる。

2.1.1 機能の実現方法

HCE は、スマートフォン上のアプリケーションプログラム（以下、アプリケーション）によって IC カードの機能をエミュレートする。アプリケーション次第では、IC カードとほぼ同じ機能を実現することも可能である。また、高速なホスト CPU の性能やスマートフォンの通信機能を活かして、IC カードや SE では困難な処理、たとえば大量のデータを取り扱ったり、サーバと連携（表 2-1 図中の②の部分）したりすることも可能である。

一方で、IC カードや SE ではその機能が OS ベンダーやデバイスベンダーなどによって提供されるのに対して、HCE では OS ベンダーによって提供される部分はごく基本的な通信層のみで、機能のほとんどをアプリケーションで作り込まなければならないという違いもある。

2.1.2 対応する通信技術方式

NFC の通信技術方式には、ISO/IEC 14443-3 Type A および ISO/IEC 18092 106kbps に基づく NFC-A（MIFARE カードの通信技術方式）、ISO/IEC 14443-3 Type B に基づく NFC-B、ISO/IEC 18092 212/424kbps に基づく NFC-F（FeliCa カードの通信技術方式）、ISO/IEC 15693 に基づく Type-V という方式がある。

IC カードや SE は、対応する通信技術方式はデバイスによって決まり、ひとつの通信技術方式にのみ対応していることが多い。

一方、HCE の場合は通信技術方式をアプリケーションが選択することができる。

2.1.3 利用時の操作

IC カードが電池不要でリーダライタにかざすだけで動作するのに対して、HCE が動作するにはスマートフォンの電池が動力として必要であり、かつスマートフォンの画面がオンになっている（スリープモードから抜けている）必要がある。スマートフォンの画面をオンにするには、ユーザの操作が必要である。また、HCE のうち NFC-F の場合は、リーダライタにかざす前にアプリケーションを立ち上げる必要がある。

なお、SE の場合は通常は操作なしで動作するが、複数の仮想的な IC カードを切り替えられるようになっているものは、リーダライタにかざす前にユーザによる選択が必要な場合もある。

2.1.4 目視確認用情報の提示

学生証や社員証では、IC カードの表面に氏名や所属、顔写真などを印刷し、目視での確認に利用している場合が多い。

一方、HCE はスマートフォンのアプリケーションで実現されるため、IC カードとは異なり固定の印刷面を持たず、スマートフォンの画面上にこれらの情報を表示するか、情報をリーダライタで読み出してリーダライタ端末の画面上に表示することになる。スマートフォンの画面上への表示にはユーザの操作が必要であり、時間もかかる。また、スマートフォンの画面は容易にコピーが可能なため、セキュリティ面の懸念もある。目視確認用の情報をスマートフォンの画面に表示する場合は、表示を動画にするなど、容易にコピーできないようにする対策が求められる。

この特徴は、SE でも同様である。

2.1.5 対応デバイス

SE はスマートフォン内部にあらかじめ組み込まれるか、スマートフォンに挿入する SIM カードなどに組み込まれた形で使用される。そのため、対応するスマートフォンの機種が限られている。ただし、国内では多くのスマートフォンに SE が組み込まれており、SE を利用したサービスも広く普及している。

HCE はスマートフォンのアプリケーションで実現されるため、本来は、スマートフォンの機種ごとの対応の差は少ない。ただし、OS としての対応は Android OS のバージョン 4.4 以降に限定される。NFC-A や NFC-B への対応はバージョン 4.4 以降であるが、NFC-F への対応はバージョン 7.0 以降である。

Android OS バージョン 4.4 以降を搭載したスマートフォンであっても、NFC や HCE への対応は必須ではないため、HCE に対応していないものもある。スマートフォンが HCE に対応する場合、NFC-A の対応は必須であるが、NFC-B や NFC-F への対応は必須ではないため、NFC-B や NFC-F の HCE に対応していない場合がある。これらの対応有無は個別の機種によって異なるので、対応端末を調べるときは、個別の機種の仕様を確認する必要がある。

2.1.6 利用許諾

SE はプラットフォーム提供者によって管理されており、その利用にはプラットフォーム提供者の許諾が必要である。

一方 HCE はアプリケーションで実現するため、利用許諾は不要である。

なお、利用許諾は不要であるが、HCE では正規に割り当てられたアプリケーション識別子やシステムコードを使用する必要がある。（「5.1 アプリケーション識別子やシステムコードの割り当て」参照）

2.1.7 特徴のまとめ

HCE の特徴を表 2-1 にまとめる。

表 2-1 IC カードと SE、HCE の違い

項目	IC カード	SE	HCE
機能の実現方法	デバイスで実現	デバイスで実現	アプリケーションで実現
通信技術方式	デバイスで決まる	デバイスで決まる	アプリケーションで選択
利用時の操作	なし	なし（場合による）	画面をオンにする
目視確認用情報	カードに印刷	画面に提示	画面に提示
利用許諾	（場合による）	必要	不要

2.2 HCE を導入するメリット

既存の IC カードシステムに HCE を導入する、または新規の IC カードシステムを構築する際に HCE にも対応させることにより、システムの利用者およびシステムを提供する事業者にさまざまなメリットがある。

2.2.1 利用者のメリット

利用者の主なメリットは以下のとおりである。以下のメリットはいずれも、SE の場合でも該当する。

- 利用者が普段使っているスマートフォンを、IC カードの代わりとして使用できる。
- IC カードは発行に時間がかかることが多いが、HCE はアプリケーションをインストールすれば利用できるため、時間がかからない。IC カードが発行されるまでの間、臨時で HCE のみを利用する、といった使い方も可能である。
- 利用履歴をスマートフォン上でリアルタイムに確認することができる。

2.2.2 事業者のメリット

事業者の主なメリットは以下のとおりである。

- 利用許諾が不要である。
- HCE の場合は、スマートフォンの通信機能を使って任意のタイミングで情報（利用者の属性情報など）を書き換えることができる。SE の場合も通信機能を使って情報を書き換えることができるが、SE 内の情報を書き換えるために特別なサーバが必要となる。HCE の場合は、特別なサーバは不要である。IC カードの場合、書き込まれた情報を書き換えるには、書き換え対応のリーダライタに IC カードをかざす必要があり、運用上の難しさがある。
- HCE のユースケースの一例として入退出のアクセスコントロールがあるが、HCE では権限情報を任意のタイミングでスマートフォンに配信することができるため、従来はリーダライタで保持していた権限情報をスマートフォンに持たせることができる。SE の場合も SE 内に権限情報を持たせることができるが、SE は記憶容量が限られているため、多くの情報を格納できない。HCE の場合は、スマートフォンの大容量のデータ領域に多くの権限情報を格納することができる。
- 入退出のアクセスコントロールを IC カードで行う場合、来客や一時的な作業者に対して臨時の IC カードを貸与する必要があり、IC カードの管理や入退室システムへの権限登録などに手間がかかる。HCE を使うと、利用者のスマートフォンにアプリケーションと権限情報を臨時でインストールすることによって、スマートフォンでのアクセスコントロールが可能になる。この特徴は SE の場合も該当するが、上記の通り、HCE の場合は特別なサーバなしで多くの権限情報をインストールすることができる。
- 利用履歴を、リーダライタからだけではなく、スマートフォンからもリアルタイムに収集することができ、セキュリティの向上などに活用できる。SE の場合も利用履歴をスマートフォンから収集できるが、利用と同時にリアルタイムに収集することが難しい場合がある。
- スマートフォンの機能（生体認証、カメラ、位置情報など）をリアルタイムに使って、セキュリティや利用者の使い勝手を向上させることができる。

- スマートフォンの通信機能を使うことで、任意のタイミングで利用者に情報を通知することができる。この特徴は、SE の場合も該当する。
- リーダライタのハードウェアは、IC カード用、SE 用、HCE 用とで共用できる。ただし、HCE 対応するためにはリーダライタのソフトウェアの変更が必要になる場合がある。

2.3 HCE の留意点

「2.1 HCE の特徴」で述べたように、HCE と IC カードや SE には差異があるため、導入に際して留意が必要な点がある。

2.3.1 セキュリティ

HCE には、IC カードや SE が持つような認証機能やデータ保護機能がない。したがって、認証機能やデータ保護機能が必要な場合は、スマートフォンのアプリケーションで実現しなければならない。この場合、認証用の鍵情報やその他の機密データを、アプリケーションのデータエリアに格納することになる。

一般に、スマートフォンのアプリケーションは、一定の知識と技術と時間があれば解読が可能である。アプリケーションのデータエリアからデータを読み出したり、アプリケーションのコピーを作ったりすることも可能である。

このような攻撃に対抗するには、アプリケーション自体の難読化やデータの暗号化を行うなどの方法がある。また、Trusted Execution Environment（TEE）のように OS とは隔離された環境に機密データを格納するという方法や、アプリケーションには短期間の期限付き認証トークンだけを保持させ、トークンが漏洩しても実質的な影響がないようにするという方法もある。

難読化などのアプリケーション単体でのセキュリティ対策には限界があるため、HCE におけるセキュリティはシステム全体で検討する必要がある。

2.3.2 同じ権限を持つデバイスが複数になる

IC カードに加えて HCE も使用可能にした場合、利用者が使用可能な同じ権限を持つデバイスが複数（IC カードとスマートフォン）になる。

これにより、たとえば片方のデバイスが第三者に貸し出されて使用される場合がある。また、紛失時に紛失したことに気付くのが遅れる可能性があるため、システムや運用で考慮する必要がある。

ID による認証やアクセスコントロールを行う場合で、複数のデバイスに同じ ID を付与する場合は、片方を紛失したときに ID を無効化するため、紛失していないデバイスの ID も変更する必要がある。

この留意点は、SE の場合にも該当する。

2.3.3 デバイスの所有者が利用者になる

IC カードの場合、IC カード媒体そのものは事業者が所有権を持ち、利用者に貸与する形をとる場合が多い。そのため、利用者が在籍しなくなったり、万が一不正利用が発見されたりした場合は、媒体を回収することが可能である。

利用者のスマートフォンで HCE を実現する場合、スマートフォンの所有者は利用者

自身であるため、スマートフォンを回収することはできず、アプリケーションを確実にアンインストールさせることも難しい。デバイスの無効化は、システムで対応する必要がある。

また、利用者の意向や故障、紛失によってスマートフォンが機種変更される場合があり、機種変更に対応できる仕組みをシステムで用意する必要がある。

従業員に貸与する業務用スマートフォンで HCE を実現する場合、上記の課題はない。

この留意点は、SE の場合にも該当する。

2.3.4 多様なスマートフォンへの対応

HCE は多様なスマートフォンで利用できるが、反面、アプリケーションは多様なスマートフォンに対応しなければならない。スマートフォンの OS のバージョンアップや、OS ベンダーによるアプリケーション規制の変更に伴い、アプリケーションを随時バージョンアップさせていく必要もある。これらに対応したアプリケーションの開発、検証、配信体制が求められる。

とくに検証については、リーダライタとの通信の安定性や、機種ごとの OS 動作の差異を確認するために、対応するすべてのスマートフォンについての検証が求められる場合がある。

この留意点は、SE の場合にも該当する。

2.3.5 アプリケーションの配布方法と配布範囲

スマートフォンのアプリケーションの配布は、Google Play などの一般のアプリケーションストアで配布する方法と、限られたメンバーだけに配布する方法がある。後者は配布範囲を限定できるが、利用者によるダウンロードやインストール、バージョンアップ作業が煩雑になる。前者は配布範囲を限定できないため、無関係の第三者がインストールすることを想定して、認証などの必要なセキュリティ対策を検討する必要がある。

この留意点は、SE の場合にも該当する。

2.3.6 通信料金

利用者のスマートフォンで HCE を実現する場合、アプリケーションのダウンロードや HCE の利用に伴うデータの送受信にかかる通信料金の負担について、利用者と事業者間で取り決める必要がある。

この留意点は、SE の場合にも該当する。

2.3.7 他の HCE アプリケーションとの競合

スマートフォンには複数の HCE アプリケーションをインストールすることができる。リーダライタがアプリケーションを選択する際に指定する ID（アプリケーション識別子やシステムコード）が正規に割り当てられたものか認証する仕組みはなく、アプリケーションは任意の ID を使用できる。したがって、第三者のアプリケーションと ID が重複する可能性がある。

アプリケーションが正規に割り当てられたアプリケーション識別子やシステムコードを使用するとともに、リーダ／ライタが第三者のアプリケーションと通信してしま

わないように、ID 以外の識別方法を持つことが望ましい。
　なお、アプリケーション識別子やシステムコードの割り当てについては、「5.1 アプリケーション識別子やシステムコードの割り当て」に記載している。

3. IC カードシステムへの HCE 導入時の検討事項

本章では、既存の IC カードシステムに HCE を導入する、または新規の IC カードシステムを HCE に対応させる際に検討すべき事項について述べる。

IC カードシステムが提供するサービスの内容や提供範囲によって、IC カードシステムに求められるセキュリティや使い勝手は異なる。本章では、IC カードシステムに応じた HCE の導入のしやすさや、HCE の導入時に検討すべき対策について述べる。

3.1 サービスの提供範囲

IC カードシステムは、そのサービスの提供範囲が 1 つの企業や組織のみである場合と、複数の企業や組織に跨る場合がある。ここでは、前者を単独システム、後者を共通利用システムと呼ぶ。

3.1.1 単独システム

利用できる地域や施設が限定されていて、利用者も会員や社員などに限定される。利用できるサービスや IC カードの種類も限られる。

利用範囲が限定されるので、システムの管理・運用は独自に決められる。

例：社員証、独自発行の学生証。

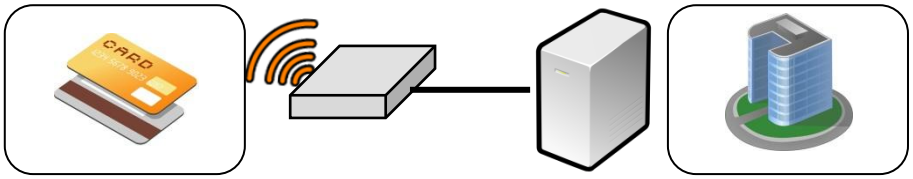

図 3-1 単独システム

単独システムでは、HCE 導入のためのセキュリティ向上施策を単独で実施できる。利用可能なスマートフォンを制限することで、動作検証対象を限定することもできる。また、企業などでは、従業員全員に HCE 対応のスマートフォンを貸与することで IC カードをすべて HCE に置き換えることも可能である。

モバイルデバイス管理ツール（MDM ツール）などを使用してスマートフォンの管理を行うことで、セキュリティを向上させることも可能である。

3.1.2 共通利用システム

利用できる地域や施設は広範囲に及び、多様な人が利用する。利用できるサービスや IC カードの種類も多様である。

複数の企業や組織に跨った運用を行うため、カードフォーマットの共通化や、運用ルールの整備、システム間のデータの連携などが必要である。

例：共通利用可能な学生証、交通系カード、汎用電子マネー。

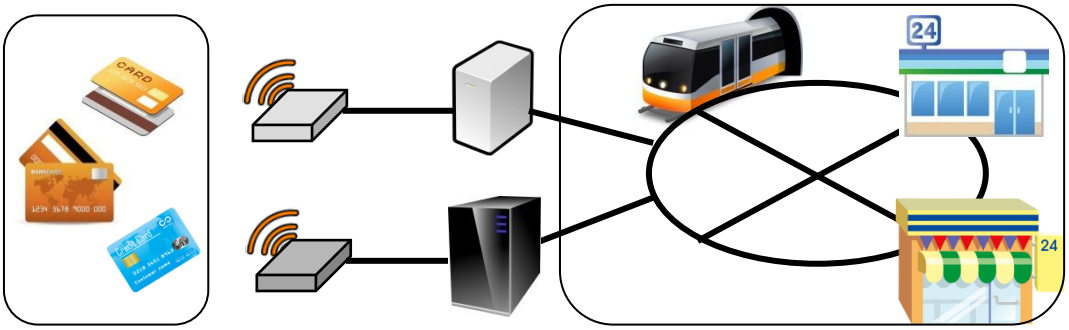

図 3-2 共通利用システム

共通利用システムでは、HCE 導入のためのセキュリティ向上施策を複数の企業や組織に跨って実施する必要がある。不特定のスマートフォンが利用されることが想定されるため、動作検証対象も幅広くなる。また、HCE 対応スマートフォンを所持していない利用者のために、IC カードや、QR コードなどのスマートフォンで利用できる代替手段と併用する必要がある。

一方、共通利用システムでは、セキュリティ向上施策の検討や導入、スマートフォンアプリケーションの開発や動作検証を、複数の企業や組織で共同で実施することにより、一組織あたりのコストを削減することも可能である。

3.1.3 HCE の導入のしやすさ

サービスの提供範囲の違いによる HCE の導入のしやすさの比較を、表 3-1 にまとめる。

表 3-1 HCE の導入のしやすさ（単独・共通利用分類での比較）

	単独システム	共通利用システム
セキュリティ	・単独でセキュリティ向上施策を実施可能。 ・MDM ツールによるスマートフォンの管理が可能。	・セキュリティ向上施策を複数の企業や組織に跨って実施する。
コスト	・利用可能なスマートフォンを制限することで、動作検証対象を限定することが可能。	・幅広いスマートフォンでの動作検証が必要。 ・IC カードや QR コードなどの他の手段との併用が必要。 ・セキュリティ向上施策の検討や導入、スマートフォンアプリケーションの開発や動作検証を共同実施することにより、一組織あたりのコスト削減が可能。

利便性	・利用可能なスマートフォンを制限することで、操作性を統一させることが可能。	・幅広いスマートフォンやその他の手段が利用可能。
HCE 適応性	・スマートフォンを利用者に配布することで､IC カードをすべて HCE に置き換えることも可能。	・HCE を導入する際は、セキュリティ検討やアプリケーション開発を共同で実施するとよい。

3.2 IC カードによるセキュリティ対策

一般に IC カードには認証やデータ保護などのセキュリティ機能が搭載されている。IC カードシステムはそれらの機能を前提として構築されるが、システムによっては IC カードが持つセキュリティ機能のうち一部しか利用しない場合もある。

HCE で認証機能やデータ保護機能を実現するには、アプリケーションの作り込みが必要である。また、スマートフォンのアプリケーション単体で高度なデータ保護機能を実現することは難しい。そのため、システムが前提とする IC カードで利用しているセキュリティ機能によって、HCE の導入しやすさは変化する。

3.2.1 書き換え自由

(1) IC カードの場合

セキュリティ被害が起こりにくい、または起きても影響がほとんどないサービスでは、IC カードを自由に書き換えられるように設定して、IC カードのセキュリティ機能をまったく利用しない場合がある。

例：幼児用の玩具、遊園地内のスタンプラリーなど。

(2) HCE を導入する場合

デバイスにセキュリティが求められないので、HCE の導入はしやすい。

3.2.2 改ざん防止

(1) IC カードの場合

IC カードを書き込み禁止にすることで、IC カード内の情報の改ざんを防ぐ。

IC カードの発行時に、発行事業者がたとえばフォーマット管理団体とのライセンス契約に基づいて書き込み権限を取得し、情報の書き込みを行う。利用時は、リーダライタには読み出し権限しかなく、情報の読み出しのみで運用される。読み出される情報は、ID などそれ自体には意味のない情報であることが多い。

盗聴やなりすましは防止できない。

例：学生証、社員証。

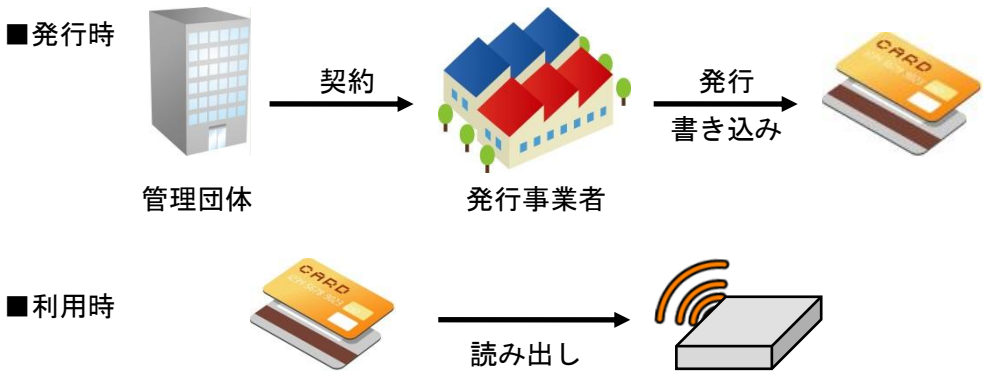

図 3-3 改ざん防止

(2) HCE を導入する場合

HCE を導入する際は、情報の改ざん防止手段を独自に実装する必要がある。たとえば、情報に対してデジタル署名やメッセージ認証符号（MAC）を付加し、それを読み出すリーダライタで検証することで改ざんを防ぐ方法が考えられる。

3.2.3 改ざん防止＋偽造・なりすまし防止

(1) IC カードの場合

IC カードの認証機能を使用して、IC カードが正しいこと、もしくはリーダライタと IC カードが相互に正しいことを認証する。

IC カードの発行時に、発行事業者が認証用の秘密情報(鍵)を IC カードに書き込む。利用時は、リーダライタが認証用のアルゴリズムを使って、IC カードが正しい秘密情報を持っていることを認証する（内部認証とよぶ）。

盗聴を防ぐことはできない。

例：ハウス電子マネー。

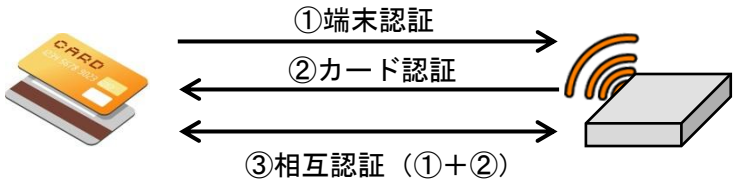

図 3-4 認証機能

(2) HCE を導入する場合

HCE を導入する際は、HCE アプリケーションにリーダライタとの認証手段を独自に実装する必要がある。

HCE アプリケーションの初期登録時に、サーバから認証用の秘密情報（鍵）を受信して、データエリアに保存する。利用時は、リーダライタが認証用のアルゴリズムを使って、HCE アプリケーションが正しい秘密情報を持っていることを認証する（内部認証

とよぶ）。
　認証用の鍵はスマートフォンに格納されるため、ウイルス感染やマルウェア、解析による漏洩を防ぐ必要がある。たとえば、鍵やアプリケーションプログラムの暗号化、難読化などの対策が考えられる。

　HCE を IC カードと同じ認証方式にする必要はない。たとえば以下のような方法がある。

公開鍵方式や PKI を利用した個別認証鍵

　IC カードでは共通鍵を使った認証を行い、HCE では公開鍵を使った認証を行ってもよい。HCE ではスマートフォンの高性能な CPU が利用できるため、公開鍵を使った認証を高速に行うことができる。また、公開鍵基盤（PKI）を採用することで、認証用の鍵をスマートフォンごとに個別に設定することが容易になり、鍵が漏洩した場合の影響を限定できる。

期限付きのトークンによる認証

　期限付きのトークンによる認証を行うこともできる。期限付きのトークンは、スマートフォンの通信機能を使って、サーバからスマートフォンに認証の都度配信するか、または定期的に配信して更新する。トークンには期限があるので、漏洩時の影響は限定される。

認証の都度サーバから認証情報を取得する

　リーダライタにスマートフォンをかざしたときに、リアルタイムでサーバと通信し、認証に必要な情報を取得してリーダライタと認証を行う。アプリケーションはリーダライタとの認証情報がないため、漏洩のリスクもない。一方で、スマートフォンがサーバと通信できない場合は利用できない。

　HCE で IC カードと異なる認証方式を使用する場合は、リーダライタにもその認証方式を実装する必要がある。
　なお、スマートフォンの通信機能を使う場合は公衆網を経由することになるため、サーバとスマートフォンの間で認証や通信路の暗号化を行う必要がある。

3.2.4 改ざん防止＋偽造・なりすまし防止＋盗聴防止

(1) ICカードの場合

　認証に加えて、リーダライタと IC カード間の通信路を暗号化する。送受信されるコマンドや情報を秘密にすることができる。
　例：交通系カード、電子マネー

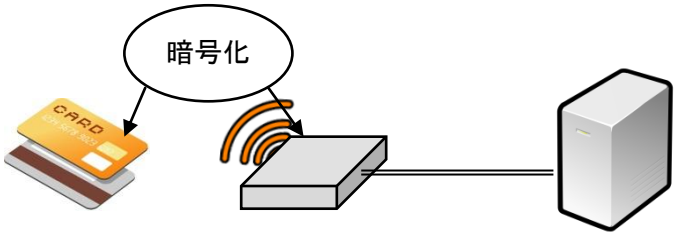

図 3-5 盗聴防止

(2) HCE を導入する場合

HCE を導入する際は、認証手段に加えて、リーダライタとの通信路の暗号化手段も独自に実装する必要がある。

通信路の暗号化方式は、IC カードと異なっていてもよい。この場合、リーダライタにもその暗号化方式を実装する必要がある。

3.2.5 データ保護

(1) IC カードの場合

認証を行わなければ IC カードに格納されるデータを読み書きできないように IC カードを設定して、権限を持たない第三者の読み書きからデータを保護する（データの改ざんからの保護も含む）。または、データを暗号化することで、権限を持たない第三者の読み出しからデータを保護する。

認証によってデータを保護する場合は、IC カードとリーダライタに認証用の情報（鍵）を格納する。利用時は、IC カードが認証用のアルゴリズムを使って、リーダライタが正しい認証情報を持っていることを確認する（外部認証とよぶ）。

たとえば IC カードにマネー残高が記録されている場合は、IC カードおよびデータの偽造・なりすまし防止のための内部認証と、データ保護のための外部認証の両方を行う必要がある。すなわち、IC カードとリーダライタが相互に認証し合う（相互認証とよぶ）。

例：ハウス電子マネー。

(2) HCE を導入する場合

HCE を導入する際は、HCE アプリケーションにリーダライタとの認証手段を独自に実装する必要がある。

このとき、HCE を IC カードと同じ認証方式にする必要はない。HCE で IC カードと異なる認証方式を使用する場合は、リーダライタにもその認証方式を実装する必要がある。

3.2.6 HCE の導入のしやすさ

システムが前提とする IC カードのセキュリティ機能の違いによる HCE の導入のしやすさの比較を、表 3-2 および表 3-3 にまとめる。

表 3-2 HCE の導入のしやすさ（IC カードによるセキュリティ対策での比較）(1/2)

	書き換え自由	改ざん防止
セキュリティ	・改ざん防止などのセキュリティ対策は不要。	・情報に対してデジタル署名やメッセージ認証符号（MAC）を付加して改ざんを防ぐ。
コスト	・利用時のシステム（リーダライタを含む）は、IC カードのみに対応する場合と同じものが使用可能。	・改ざん防止手段を、HCE アプリケーションとリーダライタの双方に実装する。

利便性	・IC カードとほぼ同じ利便性。 ・加えて、スマートフォンのアプリケーションと連動したサービスの提供が可能。	・左記と同じ。
HCE 適応性	・HCE への適応性は高い。	・改ざん防止手段が必要となるが、HCE の適応性は高い。

表 3-3 HCE の導入のしやすさ（IC カードによるセキュリティ対策での比較）(2/2)

	改ざん防止+偽造・なりすまし防止	改ざん防止＋偽造・なりすまし防止＋盗聴防止
セキュリティ	・リーダライタと認証を行う。 ・認証鍵をスマートフォンに格納する場合、漏洩を防ぐために鍵やアプリケーションプログラムの難読化を行う。 ・PKI を採用し、個別の認証鍵を使った認証を行ったり、サーバを使って認証鍵を定期的に変更したりするなど、鍵が漏洩した場合の影響を限定する。	・リーダライタとの認証に加えて、通信路の暗号化も行う。
コスト	・認証手段を、HCE アプリケーションとリーダライタに実装する。 ・認証鍵の漏洩防止手段や漏洩対策を、HCE アプリケーションやサーバに実装する。	・左記に加え、通信路の暗号化手段を HCE アプリケーションとリーダライタに実装する。
利便性	・IC カードとほぼ同じ利便性。 ・加えて、スマートフォンのアプリケーションと連動したサービスの提供が可能。	・左記と同じ。
HCE 適応性	・HCE の利用は可能だが、セキュリティを高めるためのコストが課題。	・左記と同じ。

3.3 システムによるセキュリティ対策

IC カードシステムのセキュリティは IC カードのセキュリティ機能だけで実現される

ものではなく、サーバを含めたシステムによる対策との組み合わせで必要なセキュリティを実現している。

システムによるセキュリティ対策は、HCE を使う場合でも有効である。システムによるセキュリティ対策を強化することで、HCE に不足しているセキュリティ機能を補うこともできる。また、スマートフォンの機能を使ってセキュリティ対策を行うことも可能である。

3.3.1 システムによるセキュリティ対策なし

(1) IC カード用システムの場合

セキュリティ被害が起こりにくい、または起きても影響がほとんどないサービスの場合や、IC カードによるセキュリティ機能だけで十分なサービスの場合は、システムでのセキュリティ対策が不要なことがある。

(2) HCE 対応システムの場合

必要なセキュリティ機能を HCE アプリケーションに実装する。HCE アプリケーションによるセキュリティ対策では不十分な場合は、システムでセキュリティ対策を行う必要がある。

3.3.2 ID の照合

(1) IC カード用システムの場合

リーダライタが IC カードから読み出した ID を、利用を許可された ID のリスト（許可 ID リスト）と照合することで、IC カードの正当性を確認する。偽造・なりすましなどの不正利用が検出された ID を許可 ID リストから取り除くことで、それ以上の不正利用を防ぐこともできる。

ID の照合をオフラインで実施する場合と、オンラインで実施する場合がある。

オフラインでの照合

許可 ID リストを利用端末に保持しておく。ID の照合は利用端末内で完結する。利用端末が複数ある場合、すべての利用端末の許可 ID リストを更新する必要がある。

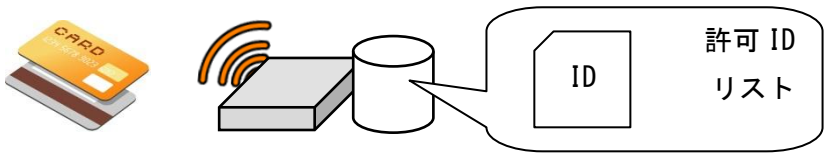

図 3-6 オフラインの ID 照合システム

オンラインでの照合

許可 ID リストをネットワーク上のサーバに保持しておく。ID の照合はサーバで行う。利用端末が複数あっても、ネットワーク上で常に最新の許可リストを参照することができる。

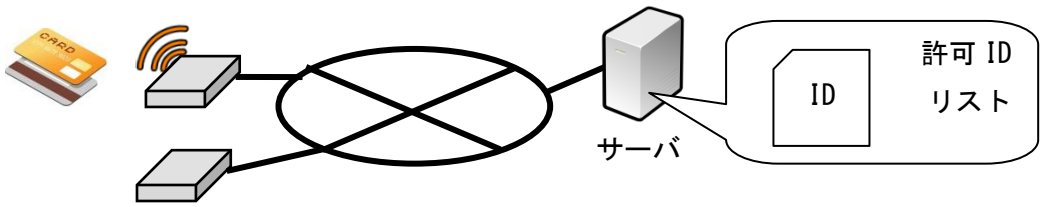

図 3-7 オンラインの ID 照合システム

(2) HCE 対応システムの場合

リーダライタが HCE アプリケーションから読み出した ID を、許可 ID リストと照合する。

オフラインでの照合

利用端末への許可 ID リストの配信には時間がかかるため、偽造・なりすましへの対応が迅速にできない可能性がある。そのため、オフラインで ID を照合するシステムに HCE を導入する際は、HCE に偽造・なりすまし防止機能を実装することが望ましい。HCE に偽造・なりすまし防止機能を実装しない場合や、IC カードの偽造・なりすまし防止機能を利用しない場合は、利用ログによる不正検出（後述）を合わせて行うことが望ましい。

オンラインでの照合

オンラインで ID を照合するシステムに HCE を導入すると、偽造・なりすましを検出した場合に、迅速な対応が可能である。

3.3.3 本人認証

(1) IC カード用システムの場合

IC カードを利用する際に、利用端末で本人認証を行い、利用者を特定する。権限を有する利用者でない者には利用させない。

本人認証の方法として、たとえば以下が考えられる。

- 暗証番号（PIN）入力による認証
- 生体情報による認証（指紋など）

認証情報は、IC カードに保持する場合と、利用端末に保持する場合とがある。

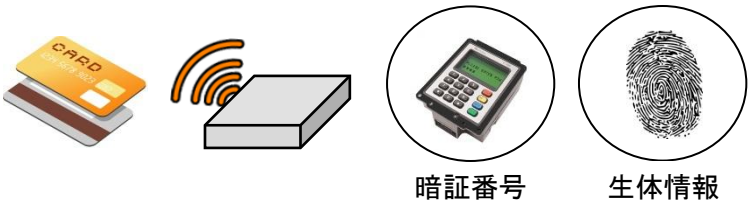

図 3-8 本人認証システム

例：社員証と本人認証による入退室

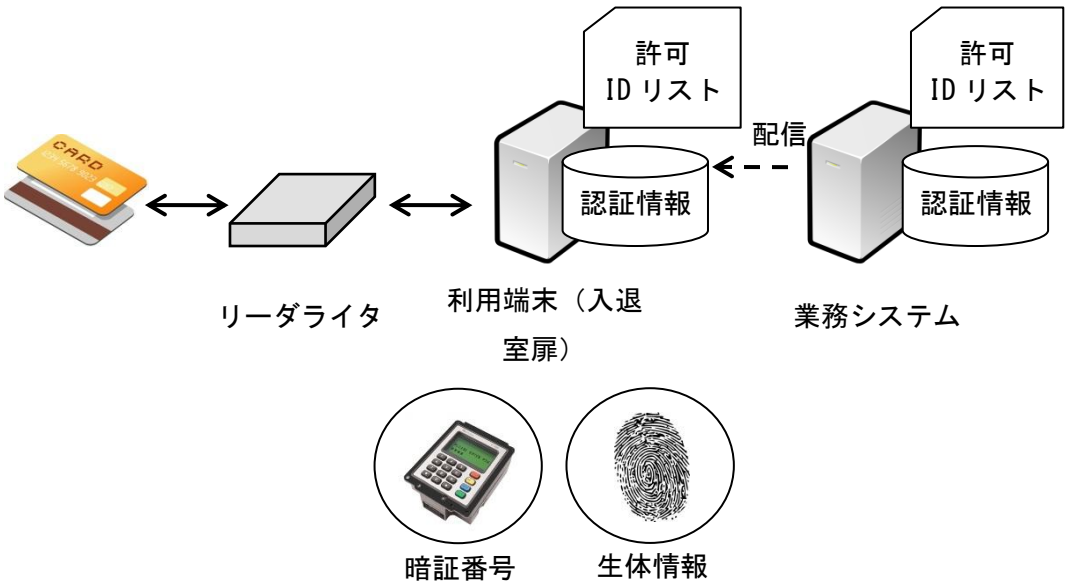

図 3-9 社員証と本人認証による入退室システムの例

(2) HCE 対応システムの場合

HCE によって IC カードの偽造・なりすましを行っても、本人認証が成功しない限り利用することができない。したがって、本人認証を行うシステムには HCE を導入しやすい。

本人認証情報を IC カードに保持するシステムに HCE を導入する場合は、HCE アプリケーション内に認証情報を保持させ、利用端末から認証情報を読み出せるようにする必要がある。この場合、HCE アプリケーション内に保持する認証情報には、偽造防止対策を行うことが望ましい。

暗証番号の入力や生体認証は、スマートフォンでも実施できる。スマートフォンには、生体認証や個人認証を実現する API が揃っている。また、認証情報をサーバに格納し、サーバに問い合わせることで認証を行う方法もある。

たとえば、偽造・なりすまし機能を備えた IC カードでは本人認証を求めず、偽造・なりすまし機能がない HCE スマートフォンではスマートフォンでの本人認証を求める、といった形にすることで、利便性とセキュリティを両立させることも可能である。

3.3.4 利用ログによる不正検出

(1) IC カード用システムの場合

IC カードの利用ログをシステムに集約、分析し、複数地点での同時利用や、未登録カードの利用などの不正を検出する。

利用時の不正は防止できないが、後から不正を検出することで不正利用に対する抑止力が期待できる。不正利用の効果を後から取り消すことも可能である。

例：学生証を利用した出席管理システム

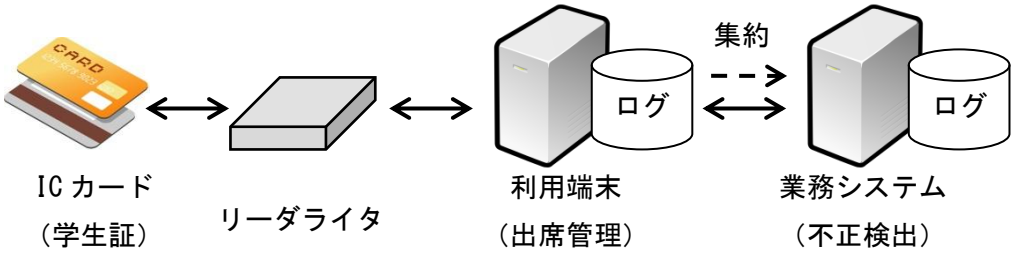

図 3-10 学生証による出席管理システムと利用ログによる不正検出

(2) HCE 対応システムの場合

HCE によって IC カードの偽造・なりすましが行われても、利用ログによって不正利用を検出することができる。したがって、利用ログによる不正検出を行うシステムには HCE を導入しやすい。

HCE の場合、さらにアプリケーションの利用ログをスマートフォンの通信機能を使ってサーバに収集することもできる。スマートフォンから収集したログと利用端末から収集したログとの差分の有無を突き合わせることによって、不正な HCE アプリケーションを検出することができる。

3.3.5 データのサーバ管理

(1) IC カード用システムの場合

サービスの提供に必要なデータを IC カードに格納するのではなく、サーバに格納することで、情報の改ざんや偽造、漏洩（ろうえい）を防ぐ。

たとえば社員証の場合、IC カードには ID のみを格納し、社員番号や氏名、入場できるエリアの情報などはサーバに格納する。利用端末において、必要に応じてサーバから情報を取得することによって、サービスを提供する。

(2) HCE 対応システムの場合

IC カードの場合と同様に、必要なデータは HCE アプリケーションには格納せず、サーバに格納する。デバイスによるセキュリティ対策の範囲を限定することができるため、HCE の導入はしやすい。

3.3.6 HCE 導入のしやすさ

システムによるセキュリティ対策の違いによる HCE の導入のしやすさの比較を、表 3-4 および表 3-5 にまとめる。

表 3-4 HCE の導入のしやすさ（システムによるセキュリティ対策での比較）(1/2)

	システムによるセキュリティ対策なし	ID の照合
セキュリティ	・必要なセキュリティ対策を HCE アプリケーションに実装する。 ・HCE アプリケーションによるセキュリティ対策では不十分な場合は、システムによる追加のセキュリティ対策を行う。	・偽造・なりすましによる不正利用を防止することが可能。 ・HCE アプリケーションから読み出した ID を、リーダライタがオフラインまたはオンラインで照合する。 ・偽造・なりすまし対策を HCE アプリケーションに実装する。または、オンラインによる照合を行うか、システムによる追加のセキュリティ対策を行う。
コスト	・HCE アプリケーションやシステムでのセキュリティ対策が必要。 ・HCE アプリケーションによるセキュリティ対策で十分な場合、利用時のシステム（リーダライタを含む）は、IC カードのみに対応する場合と同じものが使用可能。	・左記と同じ。
利便性	・IC カードとほぼ同じ利便性。 ・加えて、スマートフォンのアプリケーションと連動したサービスの提供が可能。	・左記と同じ。
HCE 適応性	・HCE への適応性は高い。	・オンラインで ID を照合する場合は、HCE 適応性は高い。 ・オフラインで ID を照合する場合は、追加のセキュリティ対策が必要。

表 3-5 システムによるセキュリティでの比較（2/2）

	本人認証	ログ確認によるセキュリティ
セキュリティ	・偽造・なりすましによる不正利用を防止することが可能。 ・HCE アプリケーションから読み出した認証情報、または利用端末内の認証情報に基づいて本人認証を行う。 ・または、スマートフォンの機能を利用して本人認証を行う。	・偽造・なりすましによる不正利用を検出することが可能。 ・スマートフォンの通信機能を使ってアプリケーションの利用ログを逐次収集することが可能。
コスト	・HCE アプリケーションから認証情報を読み出して認証を行う場合や、スマートフォンの機能を利用して本人認証を行う場合は、その機能を HCE アプリケーションに実装する必要がある。 ・利用端末内の認証情報に基づいて本人認証を行う場合は、利用時のシステム（リーダライタを含む）は、IC カードのみに対応する場合と同じものが使用可能。	・利用時のシステム（リーダライタを含む）は、IC カードのみに対応する場合と同じものが使用可能。 ・スマートフォンの通信機能を使って利用ログを収集する場合は、その機能を HCE アプリケーションとサーバに実装する。
利便性	・IC カードとほぼ同じ利便性。 ・加えて、スマートフォンのアプリケーションと連動したサービスの提供が可能。 ・IC カードの場合は本人認証を求めず、HCE の場合に本人認証を求めるなどの使い分けも可能。	・IC カードとほぼ同じ利便性。 ・加えて、スマートフォンのアプリケーションと連動したサービスの提供が可能。
HCE 適応性	・HCE への適応性は高い。	・HCE への適応性は高い。

4. HCE 対応 IC カードシステムの例

本章では、HCE 対応の IC カードシステムの例について述べる。

4.1 IC カードシステムの例

本節では、HCE の導入が想定される IC カードシステムの具体例をいくつか挙げる。

4.1.1 学生証利用システム

学生証を使用して、入退室、出席管理、授業予約、レポート提出、学生食堂の利用などを行うシステム。学生証（IC カード）には、学生の ID が格納されている。

(1) サービスの提供範囲

ひとつの学校内だけでサービスが利用できる単独システム、または複数の学校に跨って IC カードが利用できる共通利用システムである。

(2) IC カードによるセキュリティ対策

改ざん防止までを行っている場合が多い。偽造・なりすまし防止まで行うことは少ないが、重要なエリアへの入退室においては、偽造・なりすまし防止や盗聴防止まで行う場合がある。

(3) システムによるセキュリティ対策

入退室、出席管理、学生食堂の利用などでは処理速度を要求されるため、ID の照合をオフラインで行うことが多い。そのため、利用ログによる不正検出を行うことが望ましい。

出席管理、授業予約、レポート提出では、IC カードを利用する際にパスワードによる本人認証を行う場合もある。

4.1.2 社員証利用システム

社員証を利用して、入退室、出退勤管理、ログイン認証、電子署名、社員食堂の利用などを行うシステム。社員証（IC カード）には、社員の ID が格納されている。社員証に、認証用の PIN や鍵情報、生体情報が格納されている場合もある。

(1) サービスの提供範囲

社内のみにサービスを提供する単独システムである。

(2) IC カードによるセキュリティ対策

改ざん防止までを行っている場合が多い。重要なエリアへの入退室においては、偽造・なりすまし防止や盗聴防止まで行うこともある。

(3) システムによるセキュリティ対策

入退室、出退勤管理、社員食堂の利用などでは処理速度を要求されるため、ID の照合をオフラインで行うことが多い。そのため、利用ログによる不正検出を行うことが望ましい。

重要なエリアへの入退室では、IC カードに加えて、PIN や生体認証による本人認証を行う場合もある。また、ログイン認証や電子署名などでは、IC カードを利用する際にパスワードや PIN による本人認証を行う場合もある。

4.1.3 地域カード利用サービス

一定の地域内で配布される地域カードを利用して、施設予約、地域マネーやポイントの利用などを行うシステム。地域カード（IC カード）には、カードの ID が格納されている。地域マネーやポイントの残高は、サーバに保持されている場合と、地域カードに格納されている場合がある。地域カードに、電子署名の証明書情報などが格納されている場合もある。

(1) サービスの提供範囲

地域内のさまざまな施設にサービスを提供する共通利用システムである。

(2) カードによるセキュリティ対策

少なくとも改ざん防止までは行うことが多い。地域マネーやポイントの残高が地域カードに格納されている場合は、改ざん防止に加えて、偽造・なりすまし防止や盗聴防止まで行うこともある。

(3) システムによるセキュリティ対策

施設予約や、地域マネー・ポイントの利用は、オンラインで行われることが多い。ID の照合もオンラインで行われる。残高照会などがオフラインで行われる場合もある。

4.2 システム構成例

本節では、HCE に対応した IC カードシステムのシステム構成例を示す。ここでは 3 種類のサーバを想定しているが、ひとつのサーバに複数の役割を持たせてもよい。

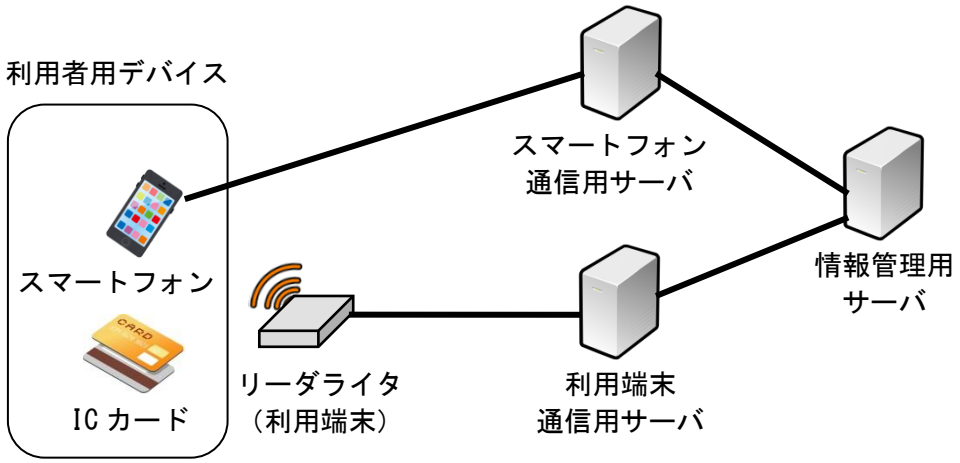

図 4-1 システム構成例

4.2.1 利用者用デバイス（IC カード + スマートフォン）

利用者が所持し、利用時にリーダライタにかざすデバイス。IC カードに加えて、スマートフォンも利用できるようにする。

HCE 導入のためには、スマートフォン上で HCE を実現するアプリケーションを利用者に提供する必要がある。

IC カードによるセキュリティ対策を行うシステムでは、HCE アプリケーションでも同様のセキュリティ対策を行う必要がある。また、スマートフォンの機能を利用してシステムによるセキュリティ対策を行う場合は、その機能の実装が HCE アプリケーションに必要になる。

- 情報の改ざん防止：情報へのデジタル署名やメッセージ認証符号の付加（「3.2.2 改ざん防止」参照）
- 偽造・なりすまし防止：リーダライタとの認証機能（内部認証）、認証鍵の暗号化や難読化（「3.2.3 改ざん防止＋偽造・なりすまし防止」参照）
- 盗聴防止：リーダライタとの通信路の暗号化機能（「3.2.4 改ざん防止＋偽造・なりすまし防止＋盗聴防止」参照）
- データ保護：リーダライタとの認証機能（外部認証、相互認証）（「3.2.5 データ保護」参照）
- 本人認証をスマートフォンの機能を使って行う（「3.3.3 本人認証」参照）
- スマートフォンの通信機能を使って利用ログを収集する（「3.3.4 利用ログによる不正検出」参照）

4.2.2 利用端末（リーダライタ）

利用者が IC カードやスマートフォンをかざす端末。

リーダライタのハードウェアは、IC カード用と HCE 用とで共用できる。ただし、リーダライタが対応している通信技術方式(NFC-A、NFC-F など)を確認する必要がある。

セキュリティや利便性向上のために、リーダライタのソフトウェアで HCE 用の追加の処理を行う。HCE による独自のセキュリティ対策を行うシステムでは、リーダライタにもその対向となる機能の実装が必要になる。また、HCE 用にシステムによる追加のセキュリティ対策を行う場合は、その機能の実装がリーダライタに必要になる。

- 情報の改ざん防止：情報へのデジタル署名やメッセージ認証符号の付加を HCE 独自の方法で行う（「3.2.2 改ざん防止」参照）
- 偽造・なりすまし防止：リーダライタとの認証（内部認証）を HCE 独自の方法で行う（「3.2.3 改ざん防止＋偽造・なりすまし防止」参照）
- 盗聴防止：リーダライタとの通信路の暗号化を HCE 独自の方法で行う(「3.2.4 改ざん防止＋偽造・なりすまし防止＋盗聴防止」参照）
- データ保護：リーダライタとの認証（外部認証、相互認証）を HCE 独自の方法で行う（「3.2.5 データ保護」参照）

- ID の照合を行う（「3.3.2 ID の照合」参照）
- 本人認証を行う（「3.3.3 本人認証」参照）
- 利用ログによる不正検出を行う（「3.3.4 利用ログによる不正検出」参照）

4.2.3 利用端末通信用サーバ

利用端末と通信し、利用端末への許可 ID リストを配信や、利用端末からの利用ログの収集などを行うサーバ。

HCE 用にシステムによる追加のセキュリティ対策を行う場合は、その機能の実装が利用端末通信用サーバに必要になる。

- ID の照合を行う（「3.3.2 ID の照合」参照）
- 利用ログによる不正検出を行う（「3.3.4 利用ログによる不正検出」参照）

4.2.4 スマートフォン通信用サーバ

スマートフォン上の HCE アプリケーションと通信し、アプリケーションの初期登録（ID の付与や認証鍵の配信など）や、アプリケーションからの利用ログの収集などを行うサーバ。セキュリティ向上のために、利用端末が求めるアプリケーションの認証や本人認証、通信路の暗号化などを、アプリケーションに代わって（またはアプリケーションと協調して）行うこともできる。また、利便性向上のためにスマートフォンに通知を送るようにすることもできる。

本サーバは HCE 対応のために新たに必要となる。

- アプリケーションの初期登録を行う
- アプリケーションに通知を行う
- スマートフォンの通信機能を使って期限付きの認証トークンを HCE アプリケーションに配信する（「3.2.3 改ざん防止＋偽造・なりすまし防止」参照）
- 認証の都度サーバから認証情報を取得する（「3.2.3 改ざん防止＋偽造・なりすまし防止」参照）
- スマートフォンの通信機能を使って利用ログを収集する（「3.3.4 利用ログによる不正検出」参照）

4.2.5 情報管理用サーバ

利用端末通信用サーバやスマートフォン通信用サーバと通信し、許可 ID リストの管理、認証情報の管理、利用ログによる不正検出などを行うサーバ。

HCE 導入時は、許可 ID リストの管理などの主な機能は IC カードと HCE とで共用できるが、セキュリティや利便性向上のためにスマートフォンを活用する場合は、そのための機能の追加が必要となる。

- スマートフォン通信用サーバを通じてアプリケーションに通知を行う

- スマートフォンの通信機能を使って収集された利用ログと、利用端末から収集された利用ログを解析し、不正利用を検出する（「3.3.4 利用ログによる不正検出」参照）

4.2.6 利用に必要な情報の保持方法

サービスの利用に必要な情報（ID など）は、スマートフォンに持たせる方法と、サーバ（スマートフォン通信用サーバ）に持たせる方法がある。

(1) HCE アプリケーション完結型

HCE アプリケーションは、初期登録時のみサーバと通信を行う。その後の利用時は、アプリケーションが保持する情報のみで、リーダライタとの通信を行う。

スマートフォン通信用サーバの機能は、初期登録機能のみなので、シンプルである。一方で、初期登録後は情報の更新ができない。また、利用に必要な情報をアプリケーション内に保持することになるが、スマートフォンのウイルス感染やマルウェアなどによる情報の漏洩や改ざんのリスクがあるため、システムによる追加のセキュリティ対策を行うことが望ましい。

(2) サーバ通信型

HCE アプリケーションにはサーバとの認証を行うための最小限の情報のみを保持する。リーダライタにスマートフォンをかざしたときに、リアルタイムでサーバと通信し、利用に必要な情報を取得してリーダライタと通信を行う。

アプリケーションには情報を持たないため、漏洩のリスクが小さくなる。一方で、スマートフォンがネットワーク通信できない場合は利用できない。

(3) ハイブリット型

初期登録時や決められた時間間隔、使用回数ごとにサーバと通信を行って、サーバから利用に必要な情報を取得する。リーダライタにスマートフォンをかざしたときに、取得した情報を使ってリーダライタと通信を行う。

スマートフォンがネットワーク通信できない場合でも利用できる。また、初期登録後も情報の更新ができる。一方で、アプリケーション内に情報を保持するため、情報の漏洩のリスクがある。利用に必要な情報を定期的に変更したり、他の値（トークン）に変換するなどして、情報漏洩のリスクを減らす対策が可能である。

4.3 システム例（学生証利用システム）

本節では、学生証利用システムに HCE を導入する例について述べる。

4.3.1 利用者用デバイス

学生が所有するスマートフォンに HCE アプリケーションをインストールし、学生証として利用する。学生割引を利用するなど学生証の提示が必要な場面もあるため、IC カードの学生証も必要である。

4.3.2 セキュリティ対策

IC カードのみを使用する学生証利用システムでは、偽造・なりすまし防止まで行うことは少ないが、HCE を使用する場合は偽造・なりすましのリスクが高まるため、以下のような対策を行うことが望ましい。

- 認証用の鍵やアプリケーションプログラムの暗号化、難読化を行う（「3.2.3 改ざん防止＋偽造・なりすまし防止」参照）
- 偽造・なりすまし防止：リーダライタとの認証（内部認証）を HCE 独自の方法で行う（「3.2.3 改ざん防止＋偽造・なりすまし防止」参照）
- ID の照合を行う（「3.3.2 ID の照合」参照）
- 本人認証を行う（「3.3.3 本人認証」参照）
- 利用ログによる不正検出を行う（「3.3.4 利用ログによる不正検出」参照）

4.3.3 HCE による利便性向上

HCE 導入により「2.2 HCE を導入するメリット」に挙げた利点が得られる。

とくに学生証の場合は、毎年有効性の確認と更新が行われる場合があるが、HCE の場合は、アプリケーション内の有効性情報の自動更新が可能である。また、出席状況や授業予約状況などに応じてアプリケーションに通知を行うことにより、学生とのコミュニケーションを向上させることができる。

4.4 システム例（社員証利用システム）

本節では、社員証利用システムに HCE を導入する例について述べる。

4.4.1 利用者用デバイス

会社から従業員に支給されるスマートフォンに HCE アプリケーションをインストールし、社員証として利用する。ビルの入館などで警備員に社員証の提示が必要な場面もあるため、IC カードの社員証も必要である。小規模なオフィスで入退室のみの場合は、スマートフォンのみで利用することも可能である。

4.4.2 セキュリティ対策

入退室やログイン認証などで高いセキュリティが求められることがあるため、HCE を使用する場合は以下のような偽造・なりすまし対策を行うことが望ましい。

- 認証用の鍵やアプリケーションプログラムの暗号化、難読化を行う（「3.2.3 改ざん防止＋偽造・なりすまし防止」参照）
- スマートフォンの通信機能を使って期限付きの認証トークンを HCE アプリケーションに配信する（「3.2.3 改ざん防止＋偽造・なりすまし防止」参照）

- 認証の都度サーバから認証情報を取得する（「3.2.3 改ざん防止＋偽造・なりすまし防止」参照）
- ID の照合を行う（「3.3.2 ID の照合」参照）
- 本人認証を行う（「3.3.3 本人認証」参照）
- 利用ログによる不正検出を行う（「3.3.4 利用ログによる不正検出」参照）

また、必要に応じて盗聴対策を行うことが望ましい。

- 盗聴防止：リーダライタとの通信路の暗号化を HCE 独自の方法で行う(「3.2.4 改ざん防止＋偽造・なりすまし防止＋盗聴防止」参照)

5. HCE 対応 IC カードシステムの開発

本章では、HCE 対応 IC カードシステムの開発時に参考となる情報について述べる。

5.1 アプリケーション識別子やシステムコードの割り当て

NFC-A や NFC-B を使用する場合は、正規に割り当てられたアプリケーション識別子を使用する必要がある。アプリケーション識別子の先頭 5 バイトであるアプリケーション提供者登録識別子（RID）は、ISO/IEC 7816-5 に基づく登録制度によって割り当てられる。日本国内だけで運用されるサービスに対する RID の登録については、以下のページに記載がある。

https://www.jsa.or.jp/iso/iso_rid

NFC-F を使用する場合は、正規に割り当てられたシステムコードを使用する必要がある。システムコードの割り当てについては、以下のページの『Host-based Card Emulation for NFC-F アプリケーション開発ガイドライン』に記載がある。

https://www.sony.co.jp/Products/felica/business/tech-support/index.html

5.2 HCE アプリケーションの開発

HCE は、Android OS のバージョン 4.4 以降（NFC-F についてはバージョン 7.0 以降）でサポートされている。HCE アプリケーションは Android アプリケーションとして開発する。一般的な Android アプリケーションの開発方法は、インターネットの解説記事や書籍などが参考になる。

Android OS の API は、以下のページから参照できる。

- https://developer.android.com/reference/

HCE 機能を利用する場合に必要となる主なパッケージは、android.nfc.cardemulation である。このパッケージには、以下のクラスが含まれている。

- CardEmulation, HostApduService : NFC-A、NFC-B のカードエミュレーションを行う場合に実装が必要
- NfcFCardEmulation, HostNfcFService : NFC-F のカードエミュレーションを行う場合に実装が必要

HCE アプリケーションは通信を行うため、通信の動作確認にはスマートフォンの実機が必要である。Android Studio のような開発環境でビルドしたアプリケーションを、実機にインストールし、動作確認を行うことになる。

HCE アプリケーション開発時の留意事項を以下に挙げる。

- アプリケーション識別子やシステムコード
  リーダライタがアプリケーションを選択する際に指定するアプリケーション識別子（NFC-A、NFC-B）やシステムコード（NFC-F）は、正規に割り当てられたものを使用する（「2.3.7 他の HCE アプリケーションとの競合」参照）。
  なお、アプリケーション識別子には任意の値が設定できるが、システムコー

ドとして設定できる値は 4000 から 4FFF（ただし 4*FF を除く）に限定されている。また、NFCID2（IDm）として設定できる値は 02FE000000000000 から 02FEFFFFFFFFFFFF に限定されている。

- アプリケーション識別子の部分指定
  NFC-A や NFC-B をエミュレートする場合、SELECT コマンドでパーシャル AID による選択はできない。

- アプリケーション識別子のカテゴリの設定
  NFC-A や NFC-B は、アプリケーションのカテゴリとして、CATEGORY_PAYMENT か CATEGORY_OTHER を設定する。CATEGORY_PAYMENT を設定した場合は、Android のメニュー「タップ&ペイ」にてデフォルトアプリを指定することができる。

5.3 リーダライタの開発

HCE に対応する場合でも、リーダライタの処理は大きくは変わらない。カードの捕捉やアプリケーションの選択を行ったあと、カードにアクセスする。

NFC-A および NFC-B の場合、HCE が動作するにはスマートフォンの画面がオンになっている必要がある。NFC-F の場合、さらに HCE アプリケーションがアクティブになっている（画面に表示されている）必要がある。これらの注意事項については、利用者の混乱を避けるため、リーダライタ(利用端末）の画面や案内文において周知することが望ましい。

6. 付録

6.1 HCE 対応機種

各キャリア別の HCE 対応機種は以下のとおりである。(NFC 搭載かつ Android OS 4.4.（コードネーム：KitKat）以降の機種）

表 6-2 各キャリア別の HCE 対応機種一覧（2018 年 8 月現在）

※各キャリアの公式ホームページ参照

ブランド	機種名	型番	メーカー
au	HTC J One	HTL22	HTC
au	HTC J butterfly	HTL23	HTC
au		HTV31	HTC
au	HTC 10	HTV32	HTC
au	HTC U11	HTV33	HTC
au	URBANO V01	KYV33	KYOCERA
au	URBANO V02	KYV31	KYOCERA
au	TORQUE G01	KYV34	KYOCERA
au	TORQUE G02	KYV24	KYOCERA
au	TORQUE G03	KYV35	KYOCERA
au	DIGNO rafre	KYV41	KYOCERA
au	Qua phone	KYV36	KYOCERA
au	INFOBAR A03	KYV37	iida
au	BASIO3	KYV43	KYOCERA
au	TORQUE G03	KYV41	KYOCERA
au	isai	LGL22	LG
au	isai VL	LGV31	LG
au	isai FL	LGL24	LG
au	isai vivid	LGV32	LG
au	isai V30+	LGV35	LG
au	Qua phone PX	LGV33	LG
au	isai Beat	LGV34	LG
au	GALAXY S5	SCL23	Samsung
au	GALAXY Note 3	SCL22	Samsung
au	GALAXY Note 8	SCV37	Samsung
au	GALAXY Note Edge	SCL24	Samsung

au	Galaxy S6 edge	SCV31	Samsung
au	Galaxy A8	SCV32	Samsung
au	Galaxy S8	SCV36	Samsung
au	Galaxy S8+	SCV35	Samsung
au	Galaxy S7 edge	SCV33	Samsung
au	AQUOS SERIE	SHV32	SHARP
au		SHV34	SHARP
au		SHL25	SHARP
au	AQUOS SERIE mini	SHV31	SHARP
au		SHV33	SHARP
au		SHV38	SHARP
au	AQUOS U	SHV35	SHARP
au		SHV37	SHARP
au	AQUOS R	SHV39	SHARP
au	AQUOS R compact	SHV41	SHARP
au	AQUOS sense	SHV40	SHARP
au	Xperia Z Ultra	SOL24	SONY
au	Xperia Z1	SOL23	SONY
au	Xperia Z3	SOL26	SONY
au	Xperia Z4	SOV31	SONY
au	Xperia ZL2	SOL25	SONY
au	Xperia Z5	SOV32	SONY
au	Xperia X Performance	SOV33	SONY
au	Xperia XZs	SOV35	SONY
au	Xperia XZ1	SOV36	SONY
au	Xperia XZ	SOV34	SONY
docomo	ARROWS NX	F-01F	FUJITSU
docomo		F-05F	FUJITSU
docomo		F-02G	FUJITSU
docomo		F-04G	FUJITSU
docomo	arrows NX	F-02H	FUJITSU
docomo	arrows NX	F-01J	FUJITSU
docomo		F-01K	FUJITSU
docomo	arrows Fit	F-01H	FUJITSU
docomo	arrows SV	F-03H	FUJITSU

docomo	arrows Be	F-05J	FUJITSU
docomo	Disney Mobile on docomo	DM-01G	LG
docomo		DM-02H	LG
docomo		DM-01K	LG
docomo	V20 PRO	L-01J	LG
docomo	Nexus 5X	—	LG
docomo	V30+	L-01K	LG
docomo	GALAXY S5	SC-04F	Samsung
docomo	GALAXY J	SC-02F	Samsung
docomo	GALAXY Note 3	SC-01F	Samsung
docomo	GALAXY S5 ACTIVE	SC-02G	Samsung
docomo	GALAXY S4	SC-04E	Samsung
docomo	GALAXY Note Edge	SC-01G	Samsung
docomo	GALAXY Note8	SC-01K	Samsung
docomo	Galaxy S6	SC-05G	Samsung
docomo	Galaxy S6 edge	SC-04G	Samsung
docomo	Galaxy S8	SC-02J	Samsung
docomo	Galaxy S8+	SC-03J	Samsung
docomo	Galaxy Feel	SC-04J	Samsung
docomo	Galaxy Active neo	SC-01H	Samsung
docomo	Galaxy S7 edge	SC-02H	Samsung
docomo	AQUOS PHONE ZETA	SH-01F	SHARP
docomo	AQUOS ZETA	SH-01G	SHARP
docomo		SH-03G	SHARP
docomo		SH-04F	SHARP
docomo		SH-01H	SHARP
docomo		SH-04H	SHARP
docomo	AQUOS EVER	SH-04G	SHARP
docomo		SH-02J	SHARP
docomo	AQUOS R	SH-03J	SHARP
docomo	AQUOS sense	SH-01K	SHARP
docomo	Disney Mobile on docomo	SH-02G	SHARP
docomo		DM-01H	SHARP
docomo		DM-01J	SHARP
docomo	AQUOS Compact	SH-02H	SHARP

docomo	Xperia Z3 Compact	SO-02G	SONY
docomo	Xperia Z3	SO-01G	SONY
docomo	Xperia A2	SO-04F	SONY
docomo	Xperia A4	SO-04G	SONY
docomo	Xperia Z4	SO-03G	SONY
docomo	Xperia Z	SO-02E	SONY
docomo	Xperia Z1	SO-01F	SONY
docomo	Xperia Z1 f	SO-02F	SONY
docomo	Xperia Z2	SO-03F	SONY
docomo	Xperia Z5	SO-01H	SONY
docomo	Xperia Z5 Compact	SO-02H	SONY
docomo	Xperia Z5 Premium	SO-03H	SONY
docomo	Xperia XZ	SO-01J	SONY
docomo	Xperia XZ1	SO-01K	SONY
docomo	Xperia XZ1 Compact	SO-02K	SONY
docomo	Xperia XZ Premium	SO-04J	SONY
docomo	Xperia XZs	SO-03J	SONY
docomo	Xperia X Performance	SO-04H	SONY
docomo	Xperia X Compact	SO-02J	SONY
SoftBank	HTC U11	601HT	HTC
SoftBank	Nexus 6P	—	HUAWEI
SoftBank	Galaxy S6 edge	404SC	Samsung
SoftBank	AQUOS CRYSTAL 2	403SH	SHARP
SoftBank	AQUOS Xx	404SH	SHARP
SoftBank		304SH	SHARP
SoftBank	AQUOS ea	606SH	SHARP
SoftBank	AQUOS Xx2 mini	503SH	SHARP
SoftBank	AQUOS Xx2	502SH	SHARP
SoftBank	AQUOS Xx3	506SH	SHARP
SoftBank	AQUOS R	605SH	SHARP
SoftBank	AQUOS R Compact	701SH	SHARP
SoftBank	AQUOS CRYSTAL	305SH	SHARP
SoftBank	AQUOS CRYSTAL Y	402SH	SHARP
SoftBank	AQUOS sense basic	702SH	SHARP
SoftBank	STA リーダライタ ARS mobile	SW001SH	SHARP

SoftBank	AQUOS Xx3 mini	603SH	SHARP
SoftBank	Android One	S3	SHARP
SoftBank	Xperia Z3	401SO	SONY
SoftBank	Xperia Z4	402SO	SONY
SoftBank	Xperia Z5	501SO	SONY
SoftBank	Xperia X Performance	502SO	SONY
SoftBank	Xperia XZ	601SO	SONY
SoftBank	Xperia XZ1	701SO	SONY
SoftBank	Xperia XZs	602SO	SONY
SoftBank	HTC U11	601HT	HTC
SoftBank	Nexus 6P	—	HUAWEI
SoftBank	Galaxy S6 edge	404SC	Samsung
SoftBank	AQUOS CRYSTAL 2	403SH	SHARP
SoftBank	AQUOS Xx	404SH	SHARP
SoftBank		304SH	SHARP
SoftBank	AQUOS ea	606SH	SHARP
SoftBank	AQUOS Xx2 mini	503SH	SHARP
SoftBank	AQUOS Xx2	502SH	SHARP
SoftBank	AQUOS Xx3	506SH	SHARP
SoftBank	AQUOS R	605SH	SHARP
SoftBank	AQUOS R Compact	701SH	SHARP
SoftBank	AQUOS CRYSTAL	305SH	SHARP
SoftBank	AQUOS CRYSTAL Y	402SH	SHARP
SoftBank	AQUOS sense basic	702SH	SHARP
SoftBank	STA リーダライタ ARS mobile	SW001SH	SHARP
SoftBank	AQUOS Xx3 mini	603SH	SHARP
SoftBank	Android One	S3	SHARP
SoftBank	Xperia Z3	401SO	SONY
SoftBank	Xperia Z4	402SO	SONY
SoftBank	Xperia Z5	501SO	SONY
SoftBank	Xperia X Performance	502SO	SONY
SoftBank	Xperia XZ	601SO	SONY
SoftBank	Xperia XZ1	701SO	SONY
SoftBank	Xperia XZs	602SO	SONY
EMOBILE	Nexus 5	EM01L	LG

Y!mobile	Android One	X2	HTC
Y!mobile	Nxus 6P	—	HUAWEI
Y!mobile	Android One	X3	KYOCERA
Y!mobile	Nexus 5X	—	LG
Y!mobile	Spray	402LG	LG
Y!mobile	Nexus 6	—	MOTORO
Y!mobile	Android One	507SH	SHARP
Y!mobile	AQUOS CRYSTAL Y	402SH	SHARP
Y!mobile	AQUOS CRYSTAL 2	403SH	SHARP
Y!mobile	AQUOS Xx	404SH	SHARP
その他	ZenFone2	ZE551ML	ASUS
その他	ZenFone 4	ZE554KL	ASUS
その他	SAMURAI REI	FTJ161B	FREETEL
その他	arrows	M04	FUJITSU
その他	arrows	M03	FUJITSU
その他	arrows	M02	FUJITSU
その他	arrows	M01	FUJITSU
その他	Ascend P7	P7-L10	HUAWEI
その他	honor 6	PE-TL10	HUAWEI
その他	honor 8	FRD-L02	HUAWEI
その他	honor 9	STF-L09	HUAWEI
その他	P9	EVA-L09	HUAWEI
その他	P10	VTR-L29	HUAWEI
その他	P10 Plus	VKY-L29	HUAWEI
その他	Ascend Mate7	MT7-J1	HUAWEI
その他	Mate 9	MHA-L29	HUAWEI
その他	Nexus 4	—	LG
その他	AQUOS	SH-M02	SHARP
その他	AQUOS sense lite	SH-M05	SHARP
その他	Xperia J1 Compact	D5788	SONY
その他	m15	—	TONE
その他	VAIO	VA-10J	VAIO
その他	AXON7	A2017G	ZTE

6.2 HCE-F 対応機種

各キャリア別の HCE-F 対応機種は以下のとおりである。（2018 年 8 月末現在）

表 6-2 各キャリア別の HCE-F 対応機種一覧（2018 年 8 月現在）

ブランド	機種名	型番	メーカー
au	Galaxy S8+	SCV35	Samsung
au	Galaxy S8	SCV36	Samsung
au	GALAXY Note 8	SCV37	Samsung
docomo	Galaxy S8	SC-02J	Samsung
docomo	Galaxy S8+	SC-03J	Samsung
docomo	Galaxy Feel	SC-04J	Samsung
docomo	GALAXY Note8	SC-01K	Samsung
docomo	arrows NX	F-01K	FUJITSU

6.3 HCE 対応サービスの事例

HCE 対応サービスの商用事例としては、海外（アジア、ヨーロッパ、米国）において、Visa および Mastercard ブランドによる決済用途での利用が 2015 年から開始されている。（参考 URL：https://www.bbva.es/eng/general/apps/bbva-wallet.jsp）

具体例の 1 つとして、スペイン BBVA 銀行の「BBVA Wallet」が挙げられる。「BBVA Wallet」では、クレジットカード番号に代わる Token 番号をスマートフォンの Wallet アプリ（スマホアプリ）内に保持した上で、HCE 機能を用いて加盟店での決済に利用されている。

従来、このようなケースにおいてはスマートフォンのセキュアチップ内にクレジットカード番号を保持した上で利用されていたが、HCE 機能を用いることでセキュアチップを保持しないスマートフォンにおいても同様のサービスを提供できるメリットがある。

Version 1.0

一般社団法人 ID 認証技術推進協会