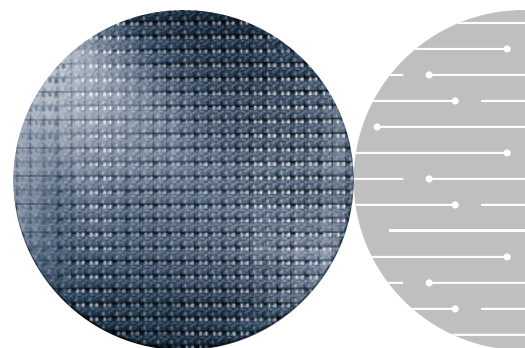




# インテル® ワイヤレス・トラステッド・ プラットフォーム：モバイル機器の セキュリティ

---



# 目次

---

<b>1. はじめに</b>	<b>3</b>
<b>2. インテル® パersonal・インターネット・クライアント・アーキテクチャ(インテル® PCA)のセキュリティ方針</b>	<b>4</b>
<b>3. インテル® ワイヤレス・トラステッド・プラットフォームによって対処可能な脅威</b>	<b>4</b>
<b>4. セキュリティ・ビルディング・ブロック</b>	<b>5</b>
インテル® トラステッド・ブート ROM	5
インテル® ワイヤレス・トラステッド・モジュール	6
セキュリティ・ソフトウェア	7
物理的な保護	7
<b>5. メリット</b>	<b>7</b>
<b>6. 技術仕様</b>	<b>8</b>
暗号化アルゴリズムおよび機能	8
各種機能	8
サポートされているプロトコル	8
<b>まとめ</b>	<b>8</b>

---

## 1. はじめに

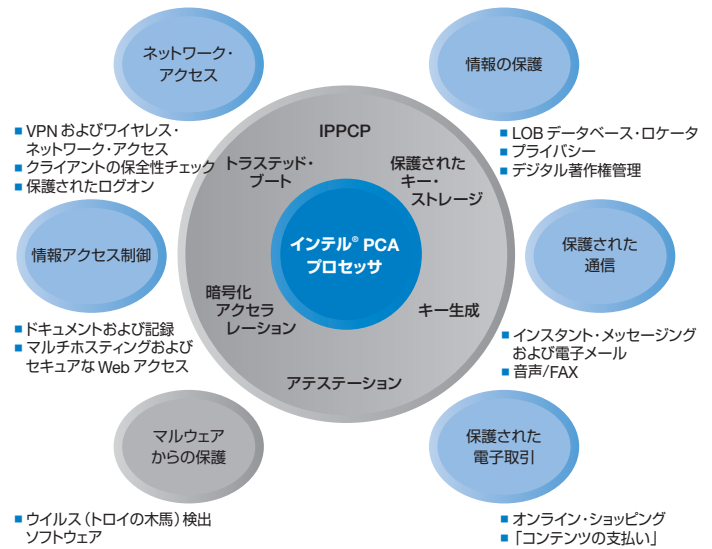
この数年間、携帯電話業界では電話機の盗難とそれに伴う不正使用の件数が急増しています。また、ハッカーによる携帯電話への攻撃件数も同じように増加しています。

- 「テレコム関連の不正使用による損失額は、年間 10 億ドル以上と推定されています。このような不正使用の最大の『市場』の 1 つが、携帯電話のクローニングです。……」  
米国財務省検察局金融犯罪部門 ([http://www.secretservice.gov/financial\\_crimes.shtml#Telecommunications](http://www.secretservice.gov/financial_crimes.shtml#Telecommunications) [英語])
- 「Vodacom は、携帯電話の盗難や不正使用への対策に年間 2,000 万ランド (約 3 億 5,000 万円) 以上を費やし、世界のいかなる GSM 携帯電話網よりも多くの盗難携帯電話をブラックリストに掲載しています。……」  
2004 年 3 月 24 日、Vodaworld Online (<http://www.vodaworld.co.za/showarticle.asp?id=801> [英語])
- 「カメラ付き携帯電話が不正使用や盗難を呼ぶ。……」  
2004 年 3 月 23 日、Denver Post Online (<http://www.denverpost.com/> [英語])  
注：2005 年 10 月現在、この記事は参照できなくなっています。

こうした背景の中、モバイル業界は、豊富なデータサービスの新規導入によって、月間電気通信事業収入 (ARPU) の増加と新たな収入源の確保を図っています。ネットワーク事業者とその顧客は、オンライン・バンキング、デジタル・メディア・サービス、ワイヤレス取引、ネットワーク・ゲーム、サードパーティ製ソフトウェアのダウンロード、ワイヤレス・ネットワーク販売など、魅力的な各種サービスの導入を大いに期待しています。ただし、既存のプラットフォームの脆弱性を伴ったまま各市場分野が融合すると、従来のネットワーク収入源にとってはリスクが高くなります。サービスを新規導入する際は、ネットワークの混乱や停止のほか、携帯電話に格納された顧客の個人情報とコンテンツを危険にさらすプラットフォーム・レベルの攻撃を防がなければなりません。

ネットワーク・プロバイダのワイヤレス・ネットワークや従来の収入源に対するリスクを軽減するには、包括的で一貫性のあるセキュリティ・ソリューションが必要です。ネットワーク・プロバイダの間では、ネットワークで使用されている端末のセキュリティ強化を望む声が高まっています。セキュリティに求められているのは、サービスを拒否することではなく、不正なアプリケーションとウイルスを防ぎつつ、適切なアプリケーションとサービスの利用が可能なインフラストラクチャを提供する手段です。

こうしたニーズを受けて、インテルでは包括的なインテル® ワイヤレス・トラステッド・プラットフォーム・アーキテクチャを開発しました。このアーキテクチャは、拡張性に優れたセキュリティ・フレームワークを構築した上で、幅広いセキュリティ・サービスを提供します。これらのサービスは、信頼性の高いプラットフォーム操作、セキュリティ・プロトコル、アクセス制御機能、個人データの保護などをサポートします。



インテル® ワイヤレス・トラステッド・プラットフォームは、広範なセキュリティ・サービスやプロトコルでの使用を目的とした基本的なセキュリティ・ビルディング・ブロックを提供します (図 1 を参照)。セキュリティ・ビルディング・ブロックは、ハードウェアと、最適化されたソフトウェア (インテル® パフォーマンス・プリミティブおよびインテル® クリプトグラフィック・プリミティブ) で構成されています。このビルディング・ブロックを利用すると、以下のようなプラットフォーム・セキュリティのサービスと機能を実現できます。

- 1) 保護された実行環境：機密情報の安全な処理とトラステッド・ブートをサポート
- 2) 保護されたキー・ストレージ：リスクのあるプラットフォーム上にもキーを格納可能
- 3) アステーション：トラステッド・ブート中にプラットフォームのセキュリティ・ステータスを評価

インテル® ワイヤレス・トラステッド・プラットフォームのビルディング・ブロックは、保護されたログオンと VPN 接続に基づくセキュアなネットワーク・アクセス、保護されたリモート・ドキュメントと記録への情報アクセス、ローカルに格納された貴重な情報 (個人データベース、デジタルトークン、デジタル・コンテンツ、権利オブジェクトなど) の保護、保護された通信、保護された電子取引 (オンライン・ショッピング/バンキングなど) をはじめ、豊富な機能を実現します。インテル® ワイヤレス・トラステッド・プラットフォームは、ウイルス検出/保護機能を直接的には提供していませんが、インテル® トラステッド・ブート ROM によって、プラットフォームが既知の適切な状態にブートすることを支援します。

## 2. インテル® PCAのセキュリティ方針

いくつかの大規模なセキュリティ障害から学んだ教訓として、セキュリティは後から追加することができません。セキュリティは、定義の初期段階からの重要な考慮事項であり、トップダウンのシステム・アプローチで設計する必要があります。この基本的な事実は見過ごされることが多く、開発者は個々の脆弱性を解決するに当たり、セキュリティ・ビルディング・ブロックの追加によってセキュリティにパッチを適用しがちです。個別の局所的なソリューションは、安全に相互運用できるとは限らず、必要なアーキテクチャ・フレームワークなしでは、結果として得られるプラットフォーム・セキュリティのレベルを測定するのはほぼ不可能です。セキュリティに対してプラットフォーム・アプローチを採用しないと、セキュリティ上の潜在的な脆弱性につながるため、攻撃者に悪用されるか、大規模な障害が発生して初めて脆弱性に気付くこととなります。ほとんどの場合は、セキュリティ・パッチを当初からのシステムに適用することになり、脆弱性を解決するのは容易ではありません。さらに、フレームワークがないと、新しいサービスや機能をプラットフォームに追加する際に、結束性を保ちながらセキュリティ・アーキテクチャを拡張するのは困難です。それよりも、個々のビルディング・ブロックの相乗効果を生かした統合的なソリューションを定義して、セキュリティ上の脆弱性を減らす方が効果的です。また、セキュリティ・フレームワークは、プロビジョンから、顧客による使用、使用終了に至るまでの、製品ライフサイクルの全段階で考慮に入れなければならない、使用終了時にはエンドユーザがセキュリティ設定と機密情報を新しいプラットフォームに移行可能である必要があります。

インテル® ワイヤレス・トラステッド・プラットフォームは、拡張性と一貫性に優れたセキュリティ・フレームワークを構築するように設計されており、製品ライフサイクル全体にわたるプラットフォーム保護を実現します。製造およびプロビジョンの間は、プラットフォームにロードされるコンテンツが破壊されておらず、出所が正当なものであるかどうかを、強力なチェックによって確認します。端末に電源を投入する際は、プラットフォームの保全性を評価し、プラットフォームがウイルスや不正なソフトウェアに侵されていないか確認します。使用中には、実行環境が貴重な個人データの安全な処理を提供します。機密情報は保護された環境内で処理されるため、キーやデータの閲覧・盗難・破壊を防ぐことができます。ストレージ保護機能は、個人データの盗難や改ざんを防止します。さらに、物理的な保護を利用し、ハードウェアやソフトウェアによって実装されたセキュリティ機能の無効化と迂回を不可能にします。

セキュリティ・ソリューションを構成するコンポーネントは、信頼性の高いものを使用し、信頼性の高い環境内で実行しなければなりません。基礎となるトラステッド・プラットフォームがない場合、セキュリティ・ビルディング・ブロックの誤用につながるだけでなく、ユーザの知識が欠けていたり、同意を得られないと、迂回されるおそれもあります。トラステッド・プラットフォームには、検証可能な定義済みの設定が用意されており、明確で予測可能な動作を期待することができます。また、個別のセキュリティ/システム・コンポー

ネットの正当性を保証する信頼性の高い環境を提供するほか、強力な暗号チェックを利用してプラットフォーム自体の正当性とセキュリティ・ビルディング・ブロックの正当性を検証できます。その結果、プラットフォームは、拡張性に優れたセキュリティ・フレームワークを構築した上で、幅広いセキュリティ・サービスを提供し、安全なコンピューティング環境の実現に欠かせない信頼性の高い操作、セキュリティ・プロトコル、アクセス制御機能などをサポートすることができます。インテル® ワイヤレス・トラステッド・プラットフォームは、このような基盤の上に築かれています。

## 3. インテル® ワイヤレス・トラステッド・プラットフォームによって対処可能な脅威

ニュースでは毎日、ワイヤレス・ネットワークや、ワイヤレス・ネットワークを使用する端末がセキュリティ上の新たな脅威に遭遇していることを伝えています。ウイルスなどのように、PC ネットワーク上で何年も前から見られている脅威がある一方、小型化、モバイル化、携帯電話の音声網へのアクセスが原因となって新たな脅威も生まれています。潜在的な脅威には極めて多くの種類があり、その一部はハンドヘルド機器向けのもです。例として、携帯電話の内部リソースの破壊、携帯電話によって提供される個人データやサービスへの無断アクセス、クローニング、端末の盗難、端末内の貴重なコンテンツの盗難などが挙げられます。インテル® ワイヤレス・トラステッド・プラットフォームは、この種の脅威に対するリスクを軽減するように設計されています。

ネットワーク事業者やメーカーにとっての大きな課題の1つが、違法ソフトウェアやハードウェアの改ざんからプラットフォームを保護することです。ソフトウェアの改ざんは、ウイルスを介してネットワーク上に広がる可能性があります。攻撃者が端末に物理的にアクセスできるとしたら、メモリのプログラムが修正されたせいかもしれません。こうした攻撃は、携帯電話の盗難やネットワーク・サービスが原因となっています。インテル® トラステッド・ブート ROM 機能は、この種の攻撃からプラットフォームを保護するように設計されており、強力な暗号チェックを利用して、プラットフォーム・ソフトウェアの保全性を検証します。

消費者が豊富なサービスを幅広く採用する前に、強力な保護機能によって、個人データ、クレジット・カード情報、格納された貴重な情報などが攻撃から適切に守られていることを保証する必要があります。たとえクレジット・カード会社の盗難防止保証があっても、個人的な面倒や、消費者の信用格付けおよび財務管理不能のリスクが、貴重な採用への大きな妨げになっています。ネットワーク事業者とサービスベンダは、プロビジョン・データの改ざんや、価値のあるトークン(公共交通機関のトークン)の複製および変更を防止する策を求めています。インテル® ワイヤレス・トラステッド・プラットフォームの保護されたストレージは、強力な暗号化と保全性チェックによって、ユーザとネットワーク事業者のデータ・セキュリティを確保します。このストレージは、知らない間に閲覧・改ざんされるリスクをなくしつつ、大量のデータをシステムメモリ内に格納できるように設計されています。さらに、アクセス制御機能によって、

正当なユーザのみが保護データの復号化に必要なキーを使用できる権限を与えられます。アクセス制御を利用すると、データは所有権に応じたドメインに分類されます。例えばウイルスは、クレジット・カード番号を検出してブロードキャストすることができません。また、トークンの価値を消費者から盗むことや、消費者による改ざんも不可能です。

ネットワーク事業者は、IMEI (International Mobile Equipment Identifier) の改ざん防止策も強く求めています。IMEI は電話の ID であり、IMEI を改ざんすることにより、盗難された電話に別の「有効」な IMEI を与えることができます。IMEI は、格納中も使用時も十分に保護しなければなりません。これは、包括的なセキュリティ・アーキテクチャの必要性を示す代表例です。IMEI を格納中に保護し、使用時に公開するのでは、ネットワーク事業者の求める十分な保護は実現できません。インテル® ワイヤレス・トラステッド・プラットフォームであれば、IMEI の使用時でも、サブシステム間の転送時でも、IMEI を常に保護できます。IMEI の格納中には、暗号化や物理的なパーティショニングによって保護します。

消費者に人気が高いサービスの 1 つとして、MPEG ビデオファイルやオーディオ (MP3) ファイルなどのマルチメディア・コンテンツをダウンロードする機能があります。インテル® ワイヤレス・トラステッド・プラットフォームは、プラットフォーム上のコンテンツを保護し、デジタル著作権管理 (DRM) の違反を防ぐ強力な機能を提供するよう設計されています。プラットフォーム上に一時的に格納されたコンテンツは、強力な暗号化によって保護され、アクセス制御ポリシーが、コンテンツの復号化に必要なキーへの無断アクセスを防止します。個々のファイルの使用に関する具体的な管理情報は、暗号化と健全性チェックによって保護されます。DRM ポリシーを適用するソフトウェアについては、ブート時に健全性を十分にチェックできるほか、DRM アプリケーションを起動するたびに再チェックすることも可能です。

#### 4. セキュリティ・ビルディング・ブロック

インテル® ワイヤレス・トラステッド・プラットフォームは、トラステッド・コンピューティング環境の基礎となる基本的なハードウェア/ソフトウェア・テクノロジーを提供するように設計されています。VPN クライアント、ウイルス・スキャン・ソフトウェア、IPSec プロトコル・スタックなどその他のセキュリティ・コンポーネントは、インテル® ワイヤレス・トラステッド・プラットフォームの基礎セキュリティ・コンポーネント上に構築し、同コンポーネントを活用できます。インテル® ワイヤレス・トラステッド・プラットフォームで提供されるコンポーネントには、以下のものが含まれます。

- インテル® トラステッド・ブート ROM
- インテル® ワイヤレス・トラステッド・モジュール (内蔵セキュリティ・モジュール)
- セキュリティ・ソフトウェア
- 保護されたストレージ
- 物理的な保護

以下では、各コンポーネントについて簡単に説明します。

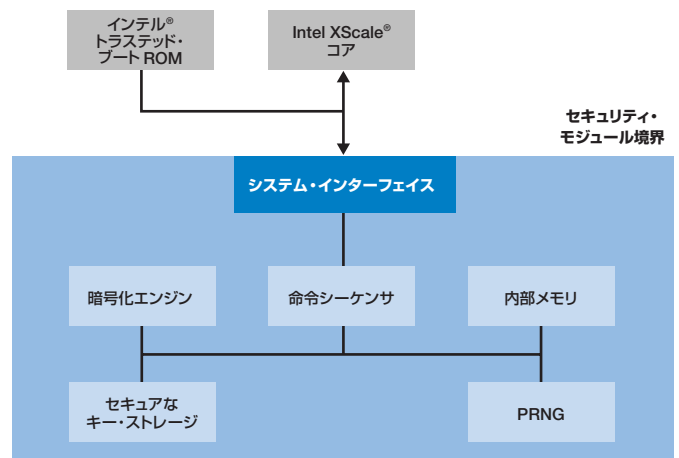


図2. インテル® ワイヤレス・トラステッド・プラットフォーム・モジュールのブロック図

#### インテル® トラステッド・ブート ROM

インテル® ワイヤレス・トラステッド・プラットフォームのコンポーネントであるインテル® トラステッド・ブート ROM は、プラットフォームの健全性を検証し、プラットフォームを「既知の適切」な設定にブートします。トラステッド・ブートは、製造から、販売、消費者による携帯電話の使用に至るまで、製品ライフサイクルの全段階において、セキュリティ・ソリューションの積極的な要素として機能します。電源が投入されたときや、オペレーティング・システム (OS) から命令されたときに呼び出されます。

インテル® トラステッド・ブート ROM は最初に、端末の製造中に呼び出されます。製造ブートの一環として、暗号キーが端末にロードされることがあり、このキーはコード・オブジェクトのデジタル・シグネチャ検証、JTAG インターフェイスのセキュアな実現、非対象キーが必要なその他の機能に使用されます。

キーは公開キーであり、秘密にする必要はありません。製品ライフサイクルのこの段階では、トラステッド・ブートは、コードおよびキーの健全性を検証し、ロード対象オブジェクトがメーカによって署名されていることを認証します。基本的には通常の製造フローへの影響はなく、ロード対象キーのみが公開キーであるため、「セキュア」な製造領域は必要ありません。メーカにとって唯一の要件は、コード・オブジェクトの形式をトラステッド・ブート・ソフトウェアに必要な形式に一致させることです。インテルでは、必要な形式変換を実行するためのソフトウェア・ツールを提供しています。

端末の導入後は、電源の投入によってトラステッド・ブートが開始されます。製品ライフサイクルのこの段階では、トラステッド・ブートは、プラットフォーム上のソフトウェア・コード・オブジェクトの健全性を検証します。これは強力なサービスであり、メーカによって当初からロードされていたプラットフォーム・ソフトウェア設定への改ざんをすべて検出できます。トラステッド・ブート・コードはブート中、プラットフォームのコード・オブジェクトの暗号化を評価し、評価値を既知の適切な値と比較します。評価値は保存されるため、後で何らかのエンティティがブート時のプラットフォームの状態について問い合わせた際に、値を提示できます。トラステッド・ブートは、移行的なトラストモデルに基づいており、トラステッド・ブート・コードによって開始されます。トラステッド・ブートがほかのソフトウェア・オブジェクトの健全性を検証すると、オブジェクトはトラスト境界内に取り込まれます。そのオブジェクトの機能を利用すれば、プラットフォーム全体が「トラステッド」であることを確認するまで、トラスト境界をさらに拡張できます。トラステッド・ブート・コードは、改ざんや迂回が不可能なメモリ内に格納されています。そのため、トラステッド・ブート・プロセスは、電源投入時に必ず実行されます。トラステッド・ブートは、ウイルス、悪意のあるソフトウェア、コーディング・エラーに起因するプラットフォームの改ざんを検出できます。いずれの場合でも、基本的なプラットフォーム設定が改ざんされると、プラットフォームの信頼性が低下し、そのプラットフォームによって提供されるサービスは、信頼性低下の度合いに応じて制限されます。

インテル® トラステッド・ブート ROM は、電源投入後はいつでも、OS やアプリケーションによって呼び出しが可能です。トラステッド・ブート・コードはこのような場合、プラットフォームの現在の動作設定を評価し、評価結果を安全に格納します。評価結果は、アステーションと呼ばれるプロセスの一環として、ユーザ、内部プロセス、外部エージェント（支払サーバなど）に提示できます。このため、リクエストは、プラットフォームの現在の状態をチェックしてから、セキュアなサービスを実行できます。例えば、支払いサーバは、測定可能な特定の設定がプラットフォームに適用されることを要求してから接続を確立することができます。また、ローカル・アプリ

ケーションにおいては、プラットフォーム設定が当初の暗号キー生成時と同じである場合のみ、暗号キーの利用を許可することが可能です。

インテル® トラステッド・ブート ROM は、携帯電話にロードされたソフトウェアに強力な保護機能を提供して、ソフトウェアに対する偶発的または悪質な改ざんを防止します。ブートプロセスが完了し、制御が OS に移譲されると、OS からのサポートによって、ウイルス・スキャン・ソフトウェアなど追加のセキュリティ対策が利用できます。

## インテル® ワイヤレス・トラステッド・モジュール

インテル® ワイヤレス・トラステッド・モジュールは、機密情報を処理する上での安全かつ閲覧不可能な場を提供します。このモジュールには、暗号化エンジンスイートが含まれており、一連の基本的な暗号化サービス（セキュリティ・プリミティブ）をサポートしています。例として、乱数生成、対象/非対象暗号化、キー生成、キー交換、デジタル・シグネチャ処理、ハッシュ、バインド、モニタリング・カウンタなどがあります。インテル® ワイヤレス・トラステッド・モジュールのセキュリティ処理はアトミックです。つまり、いったん開始されると、処理は完了まで継続され、中間結果が公開されないため、モジュール外のエージェントによる改ざんは不可能です。基本的な暗号化サービスは、プラットフォーム・アステーション、保護されたストレージ、セキュリティ・プロトコル/サービス（IPSec および VPN）のサポートなど、より高度なセキュリティ機能の構築に利用されます。

インテル® ワイヤレス・トラステッド・モジュールには、適切なセキュリティ境界が定義されており、隠蔽化した実行が可能です。アプリケーション・プロセッサは、このモジュールによって実行される処理をモニタしたり改ざんすることができません。暗号キー、プリミティブ処理の中間結果、モジュールの処理状態、PRNG の状態、トラステッド・ブートで収集された評価値、その他の機密データはすべて、セキュリティ・モジュールの不透明な境界の内側で処理されます。要求された機能の最終結果のみが、適切に定義された API を介して公開されます。

インテル® ワイヤレス・トラステッド・モジュールは、データ要素を暗号化によって特定のプラットフォームにバインドするよう設計されています。例えば、トラステッド・モジュールによって IMEI を特定のプラットフォームにバインドできます。バインドされたオブジェクトは、バインドに使用した内蔵セキュリティ・モジュールによってのみアンバインドが可能です。また、特定のソフトウェア設定が存在する場合のみアンバインドできるように、制限を強化することも可能です。この機能を利用すると、IMEI を特定のプラットフォームと特定のソフトウェア・モニタにバインドすることができます。

その場合モニタは、隠蔽されたIMEIのクエリを使用中のIMEI値に強制的に適用して、バインドに違反があればすべての処理を停止します。これは、IMEIのクローニングを防止するための極めて強力な機能です。

アテストーションでは、インテル® ワイヤレス・トラステッド・モジュールを利用して、プラットフォーム上の動作環境に関する情報を提供します。アテストーションは、ブート時、またはブート後の任意のときに行われる端末の評価です。いずれの場合でも、アテストーション値は、評価時におけるプラットフォームの健全性の評価結果に相当します。処理の実行前に特定のプラットフォーム設定が必要な場合、必要な設定に適合しているかどうかプラットフォームを評価できます。アテストーションが必要な値に適合しない場合、システムは処理を完了できません。保護されたデータについては、プラットフォームの状態が、データが暗号化された当初と同じでなければ、モジュールはデータの復号化を拒否する場合があります。同様に、支払サーバなどの外部エンティティは、既知の適切な設定が適用された端末とのみやりとりします。上記のいずれの場合でも、アテストーション機能の利用によって、「トラステッド」設定がプラットフォームに適用されていることを確認してから、要求された処理の実行を許可できます。

システム・フラッシュ内の保護されたストレージは、インテル® ワイヤレス・トラステッド・モジュールによって提供される機能です。この機能は、プラットフォーム上にセキュアな不揮発性ストレージを構築して、暗号キー、公開/秘密キーのペア、パスワード、デジタル著作権管理データ、e-ticketなどの機密情報を格納します。セキュアな不揮発性ストレージを必要とするデータ量はモジュールから提供される分を上回る可能性が高いため、システム・フラッシュ・メモリ内の保護されたストレージが必須です。この機密情報は暗号化によってプライバシーと健全性が保たれるため、攻撃者による閲覧や、元のデータから改ざんデータへの置き換えが不可能です。

また、セキュリティ・プリミティブは、高度なプロトコルのサポートに利用できます。IPSec、IKE (Internet Key Exchange)、SSL (Secure Sockets Layer)などのプロトコルや、デジタル著作権管理 (DRM)などのサービスはすべて、暗号化のサポートを必要としており、インテル® ワイヤレス・トラステッド・モジュールによって提供されるプリミティブを利用することでメリットが得られます。このアプローチのもたらす2つのメリットのうち1つは、パフォーマンスの向上です。セキュリティ処理は専用セキュリティ・モジュールに振り分けられ、汎用プロセッサよりも効率的にアルゴリズムが実行されます。汎用プロセッサは、並行してほかの処理の実行にも利用できます。2つめは、機密情報を処理する上で、アプリケーション・サブシステムよりもはるかにセキュアな閉鎖環境を提供することです。そのため、暗号キーや関連する機密データをより強力に保護することができます。

## セキュリティ・ソフトウェア

インテル® ワイヤレス・トラステッド・プラットフォーム・ソリューションには、セキュリティ・ソフトウェア・スタックが含まれており、

OSとアプリケーションが標準的な暗号化APIを介してインテル® ワイヤレス・トラステッド・プラットフォームのリソースにアクセスすることを可能にしています。このため、OSとアプリケーションは、ハードウェアとソフトウェアとの機能分散に関する固有の情報や、ハードウェア・インターフェイスおよびプロトコルに対する認識がなくても、基本的な暗号化サービスにアクセスできます。アプリケーション・インターフェイスは、インテル® インテグレートッド・パフォーマンス・プリミティブの暗号化プリミティブ (インテル® IPP Cryptos)によって提供されます。インテル® IPP Cryptosは、セキュリティ・モジュール内のソフトウェア・サービスとハードウェア・セキュリティ機能を組み合わせ、暗号化サービスの高度な要求を満たします。セキュリティ・モジュールが呼び出されると、インテル® IPP Cryptosは、セキュリティ・サービスの高度な要求を、インテル® ワイヤレス・トラステッド・モジュールによって実行される一連のプリミティブ処理に変換します。また、インテル® IPP Cryptosは、インテル® ワイヤレス・トラステッド・モジュールの機能を高度に管理します。

## 物理的な保護

物理的な保護は、重要なセキュリティ・コンポーネントの削除や置き換えによって携帯電話のセキュリティが侵害されるという脅威を軽減します。物理的な保護には、単一の端末内にセキュリティ・ハードウェアを統合する (システム・オン・チップ: SoC)、あるいは単一の物理パッケージ内に独立したコンポーネントを組み込む (スタック化コンポーネント) という2通りの方法があります。インテル® ワイヤレス・トラステッド・プラットフォーム・ソリューションは、両方の物理的な保護を採用することによって、セキュリティ・コンポーネントの置き換え、削除、迂回を強力に防ぎ、セキュリティの実行を攻撃者から隠蔽するように設計されています。

## 5. メリット

インテル® ワイヤレス・トラステッド・プラットフォームは、ワイヤレス・エコシステム全体にメリットをもたらす強固なセキュリティ・アーキテクチャを提供します。このアーキテクチャから得られる主なメリットは、以下のとおりです。

- 一貫性のある統合的なアーキテクチャであるため、局所的なソリューションで発生しがちな相互運用性に関する問題を削減できます。
- インテル® トラステッド・ブートROMは、プラットフォームの健全性を確保し、携帯電話がネットワークに悪影響を与えるリスクを軽減します。
- セキュリティ・モジュール内の保護機能は、暗号化されていないキーの公開を防止します。セキュリティが強化されることで、デジタル・コンテンツ配信、e-ticket、ビジネス・エンタープライズ・サービスをはじめとする豊富なサービスが実現します。

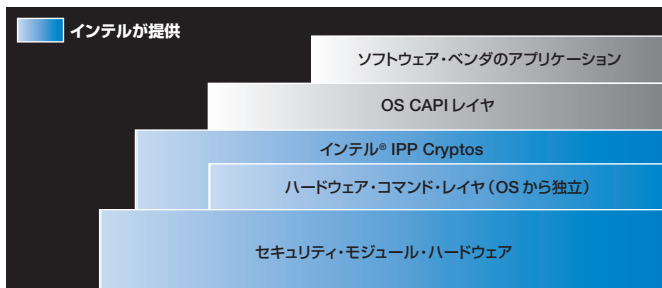


図3. セキュリティ・ソフトウェア・スタック

- インテル® ワイヤレス・トラステッド・モジュールは、専用セキュリティ・モジュールであるため、システム・パフォーマンスの向上につながります。セキュリティ処理をセキュリティ・モジュールに振り分けることによって、プロセッサをほかの処理に利用できます。
- 広く普及している暗号化 API をサポートしているため、アプリケーション開発者は、セキュリティ・ハードウェアに搭載されている強力なセキュリティ機能を容易に活用できます。

## 6. 技術仕様

### 暗号化アルゴリズムおよび機能

Advanced Encryption Standard—Electronic Code Book (ECB)、Cipher Block Chaining (CBC)、カウンタモード  
RSA  
SHA-1 および SHA-1 ベースの HMAC  
デジタル・シグニチャの生成・検証 (EMSA PKCS v15)  
Diffie-Hellman Key Exchange

### 各種機能

トラステッド・ブート ROM  
擬似乱数生成器  
モノニック・カウンタ

### サポートされているプロトコル

IPSec  
Internet Key Exchange (IKE)  
OMA v1 および v2  
Secure Sockets Layer (SSL)  
Trusted Computing Group Main Specification

### まとめ

インテル® ワイヤレス・トラステッド・プラットフォーム・アーキテクチャは、拡張性に優れたセキュリティ・フレームワークを構築した上で、オンライン・バンキング、デジタル・メディア・サービス、ワイヤレス取引、ネットワーク・ゲーム、サードパーティ製ソフトウェアのダウンロード、ワイヤレス・ネットワーク販売など、幅広いセキュリティ・サービスを提供します。これらのサービスは、信頼性の高いプラットフォーム操作、セキュリティ・プロトコル、アクセス制御機能、個人データの保護などをサポートします。

サービスを新規導入する際は、ネットワークの混乱や停止のほか、携帯電話に格納された顧客の個人情報とコンテンツを危険にさらすプラットフォーム・レベルの攻撃を防がなければなりません。インテル® ワイヤレス・トラステッド・プラットフォームは、このような課題に対処することを目的に設計されました。

詳細については、インテルの Web サイト <http://www.intel.co.jp/jp/developer/> を参照してください。

本資料に掲載されている情報は、インテル製品の概要説明を目的としたものです。本資料は、明示されているか否かにかかわらず、また禁反言によるとよらなくにかかわらず、いかなる知的財産権のライセンスを許諾するためのものではありません。製品に付属の売買契約書「Intel's Terms and conditions of Sales」に規定されている場合を除き、インテルはいかなる責を負うものではなく、またインテル製品の販売や使用に関する明示または黙示の保証（特定目的への適合性、商品性に関する保証、第三者の特許権、著作権、その他、知的所有権を侵害していないことへの保証を含む）に関して一切責任を負わないものとします。インテル製品は、医療、救命、延命措置などの目的への使用を前提としたものではありません。

インテル製品は、予告なく仕様変更される場合があります。

インテル® PCA セキュリティ・アーキテクチャのコンポーネントは、エラッタと呼ばれる設計上の不具合が含まれている可能性があり、公表されている仕様とは異なる動作をする場合があります。現在確認済みのエラッタについては、インテルまでお問い合わせください。

インテル® PCA セキュリティ・アーキテクチャの設計ドキュメントおよびこれに記載されているハードウェアとソフトウェアはライセンス契約に基づいて提供されるものであり、そのライセンスの許諾範囲内でのみ使用または複製できます。本書の情報は情報提供の目的でのみ提供されるもので、予告なしに変更される場合があります。本書の情報はインテルが約定として構成したものではありません。本書の内容および本書の内容に関連して掲載されているソフトウェア製品の誤りに関して、インテルは一切の責任や義務を負いません。

ライセンス契約で許可されている場合を除き、インテルからの文書による承諾なく、本書のいかなる部分も複製したり、検索システムに保持したり、他の形式や媒体によって転送したりすることは禁じられています。

最新の仕様をご希望の場合や製品をご注文の場合は、お近くのインテルの営業所または販売代理店にお問い合わせください。

本書で紹介されている資料番号付きのドキュメントや、インテルのその他の資料を入手するには、<http://www.intel.com/> にアクセスするか、1-800-548-4725 (米国) までお問い合わせください。



### インテル株式会社

〒300-2635 茨城県つくば市東光台5-6  
<http://www.intel.co.jp/>

Intel、インテル、Intel ロゴ、Intel XScale は、アメリカ合衆国およびその他の国における Intel Corporation またはその子会社の商標または登録商標です。  
\* その他の社名、製品名などは、一般に各社の商標または登録商標です。

© 2004-2005 Intel Corporation. 無断での引用、転載を禁じます。  
2005年10月

300868-001JA  
JPN/0510/PDF/SE/CHG/HU/IN