XAPP1309 (v1.0) 2017 年 3 月 7 日

Zynq-7000 All Programmable SoC のメジャー ブート

著者: Lester Sanders

概要

Zynq®-7000 All Programmable (AP) SoC のセキュア ブート機能では、ブート時にロードされるすべてのパーティションを RSA-2048 認証を使用して認証できます。この機能は、機密性を必要とするパーティションの AES (Advanced Encryption Standard) 暗号化もサポートします。Zynq-7000 AP SoC の変更不可能な bootROM には、早期のロード攻撃から保護するためのハードウェアによる信頼のルート (HROT) を提供するセキュリティ機能が含まれています。

このアプリケーション ノートでは、接続環境で使用される Zynq-7000 AP SoC にメジャー ブート機能を追加する方法について説明します。信頼できるソフトウェアを使用してエンベデッド システムがブートすることを、セキュアなネットワーク経由でサーバーがリモートで認証します。この方法では TPM (Trusted Platform Module) を使用して HROT 機能を強化します。TPM は、Zynq-7000 SoC セキュリティ機能を効果的に補完する、コスト効果の高い不正操作防止デバイスに暗号化機能を提供します。

このアプリケーション ノートのリファレンス デザイン ファイルは、ザイリンクスのウェブサイトからダウンロードできます。

はじめに

現在のほとんどのアプリケーションでは、ザイリンクス FPGA/SoC はファクトリで一度プログラムされ、通常はデバイスのライフサイクル期間中にリコンフィギュレーションされません。機能を追加したり、エンベデッド システムの総保有コスト (TCO) を削減したりする方法として、フィールド アップデートのサポートがあります。Zynq-7000 AP SoC では、SoC およびプログラマブル ロジックをアップデートできるため、フィールド アップデートは非常に効果的な手段といえます。フィールド アップデートは通常はインターネットを介するため、ネットワークにアクセス可能なすべての人がエンベデッド システムへの攻撃の機会を得ることになります。ファームウェア アップデートには、メジャー ブートおよびネットワーク セキュリティが重要になります。

図 1 に、メジャー ブートを使用するシステム環境の例を示します。サーバーは Zynq-7000 AP SoC に基づくフィールド展開されたエンベデッド システムのソフトウェアのロード、アップデート、および検証を管理します。エンベデッド システムはイーサネットを使用してサーバーに接続します。エンベデッド システム上のソフトウェアをアップデートするほか、サーバーは信頼できる適切なソフトウェアがロードされているか検証します。サーバーによってブート時およびランタイム中に実行されるこの検証はリモート認証です。

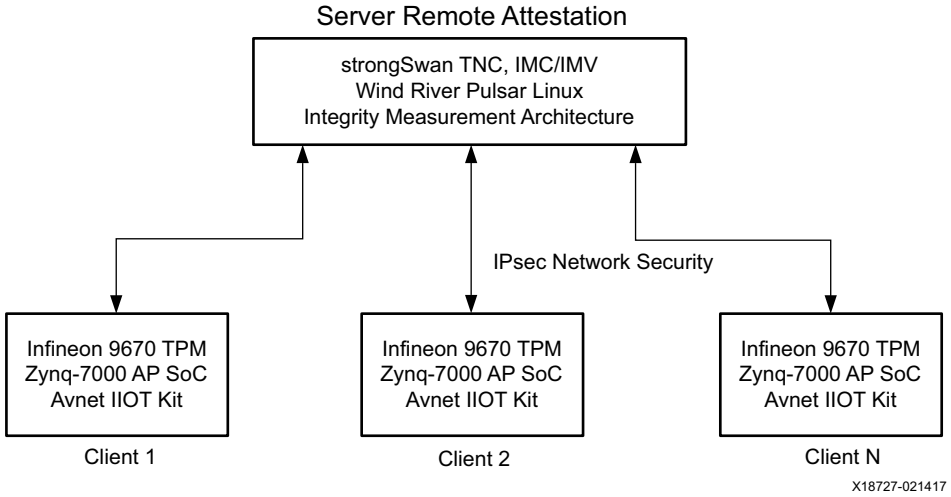


図 1: Zynq-7000 AP SoC エンベデッド システムのメジャー ブート

リモート認証機能は 2.6.3 以降の Linux に導入され、一般的には IMA (Integrity Measurement Architecture) と呼ばれています。IMA と共に Linux EVM (Extended Verification Module) が使用されます。「メジャー ブート」という用語が使用されるのは、ロードされる各パーティションの値がクライアントから返されるためで、この値は通常は SHA-1 (Secure Hash Algorithm-1) ダイジェストです。リモート認証では、サーバーは測定されたログを既知の正常な測定値と比較します。

認証サーバーは、エンベデッド システムにロードされるパーティションの特性 (測定値)、つまりパーティションのサイズやダイジェストなどを認識しています。ロード時にエンベデッド システムはパーティションの測定値が格納されたログ ファイルをサーバーに送信します。サーバーは測定値を検証し、想定されたものと異なるソフトウェアをクライアントがロードした場合、サーバーはサーバー管理者によって設定されたポリシーを実行します。ポリシーとは、測定結果に基づいてサーバーによって実行される一連の動作です。リファレンス デザイン内のポリシーには、Allowed、Quarantined、Blocked、Isolated などがあります。

ポリシーの例として、エンベデッド システムをネットワークから切り離し、ソフトウェアをアップデートし、リモート認証を再実行し、ソフトウェアが信頼できる場合はクライアントがネットワークへの接続を許可するといったものがあります。不正なエンベデッド システムをネットワークから分離することで、ほかのエンベデッド システムに悪影響を及ぼす可能性が制限されます。このポリシーは一般的にアプリケーションによって定義されるため、リモート認証のサーバーの標準的なポリシーであって唯一のポリシーではありません。

メジャー ブートはセキュア ブートの代わりではなく、追加として実行されます。メジャー ブートでは悪意のあるソフトウェアがロードされることは防止できません。TPM は HROT の機能を強化し、ソフトウェアのロード/アップデート プロセスのセキュリティを高めます。このモジュールは Zynq-7000 AP SoC と同じボードに配置されます。デバイス ID は Zynq-7000 SoC-TPM プラットフォームに関連付けられます。TPM はメジャー ブートに使用される暗号化機能を提供します。ROT の機能は TPM によって強化されているため、敵対者が攻撃を成功させるには Zynq-7000 AP SoC と不正操作防止機能を持つ TPM の両方を攻略する必要があります。

図 2 は、クライアント プラットフォーム上の Zynq-7000 AP SoC および Infineon OPTIGA SLB 9670 TPM の機能コンポーネントを示したものです。

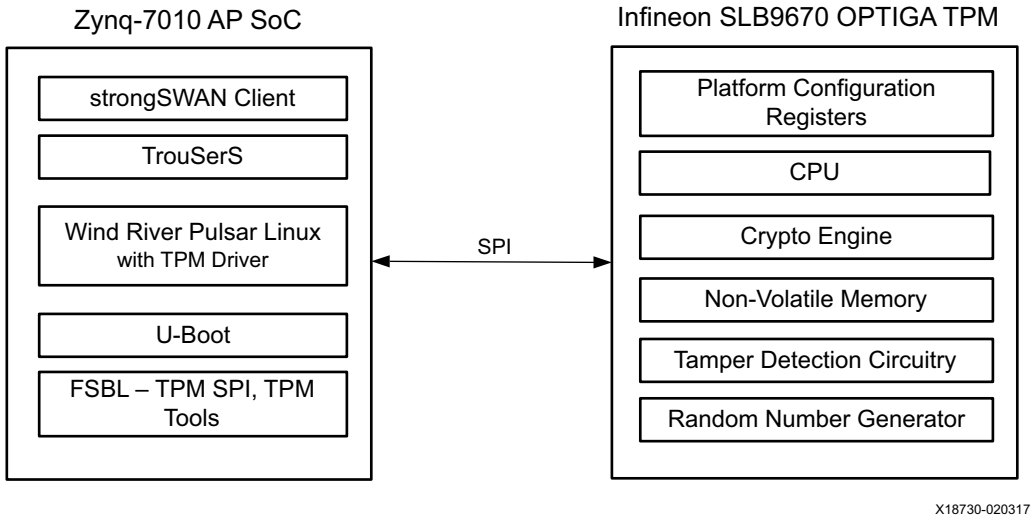


図 2: Zynq-7000 AP SoC に基づくクライアント プラットフォームの機能図

電源投入時に、Zynq-7000 AP SoC のオンチップ bootROM コードは第 1 段階ブート ローダー (FSBL) をロードします。FSBL は U-Boot をロードし、U-Boot は Linux カーネル、ルート ファイル システム、デバイス ツリー、および Linux アプリケーションソフトウェアをロードします。信頼の連鎖を使用してブートする 1 つの方法として、bootROM が FSBL を認証/測定し、FSBL が U-Boot を認証/測定し、U-Boot が Linux パーティションを認証/測定します。

SHA-1 測定ログは、TPM のプラットフォーム構成レジスタ (PCR) 内に格納されます。bootROM および FSBL の測定は FSBL によって実行され、シリアル ペリフェラル インターフェイス (SPI) 接続を使用して PCR に配置されます。測定値はリモート認証用にサーバーへ送信されます。TPM は PCR 内の SHA-1 値を暗号で署名するため、パーティション測定値はエンベデッド システムからプレーン テキストでは送信されません。

ファームウェア アップデートのリモート認証のために、認証サーバーとクライアント間のネットワーク接続はセキュアである必要があります。X.509 証明書を生成するプライバシー認証局 (CA) を含む IPsec 機能によって、サーバーとクライアント間のトランスポート レイヤー セキュリティ (TLS) ハンドシェイクが実装されます。メジャー ブートのリファレンス デザインで使用されるネットワーク セキュリティについては、12 ページの「メジャー ブートのネットワーク セキュリティ」で説明します。

必要なハードウェアおよびソフトウェア

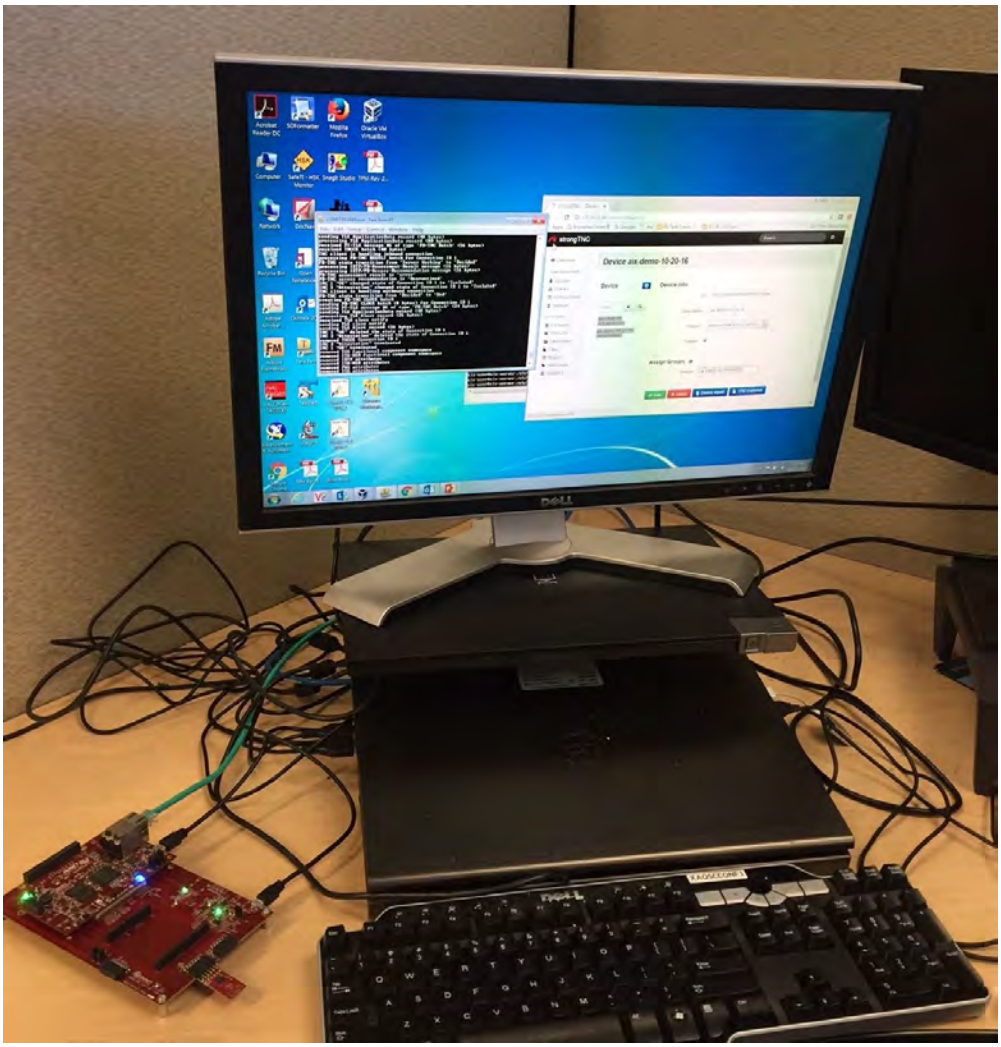
リファレンス システムのハードウェア要件およびソフトウェア要件には次のものが含まれます。

- Avnet 社 MicroZed ボード付き Industrial Internet of Things (IIoT) スターター キット
- Infineon 社 OPTIGA TPM 1.2 SLB 9670 ペリフェラル モジュール (Pmod) 互換ボード
- USB Type-A/mini-B ケーブル 2 本 (UART および JTAG 通信用)
- Micro Secure Digital (microSD) メモリ カード (16GB)
- イーサネット ケーブル
- ザイリンクス ソフトウェア開発キット 2017.1
- ザイリンクス Vivado® Design Suite 2017.1 (オプション)
- Wind River Pulsar Linux 8.0
- VirtualBox 5.0.26 以降 (または同等の VMware)
- Open Virtual Appliance 形式の Ubuntu または Ubuntu コマンド ライン仮想マシン イメージ
- strongSwan TNC ソフトウェア
- Tera Term または同等の通信端末ソフトウェア

システムのセットアップによっては、上記のすべてのソフトウェアが必要ではない場合もあります。

リファレンス システムの説明

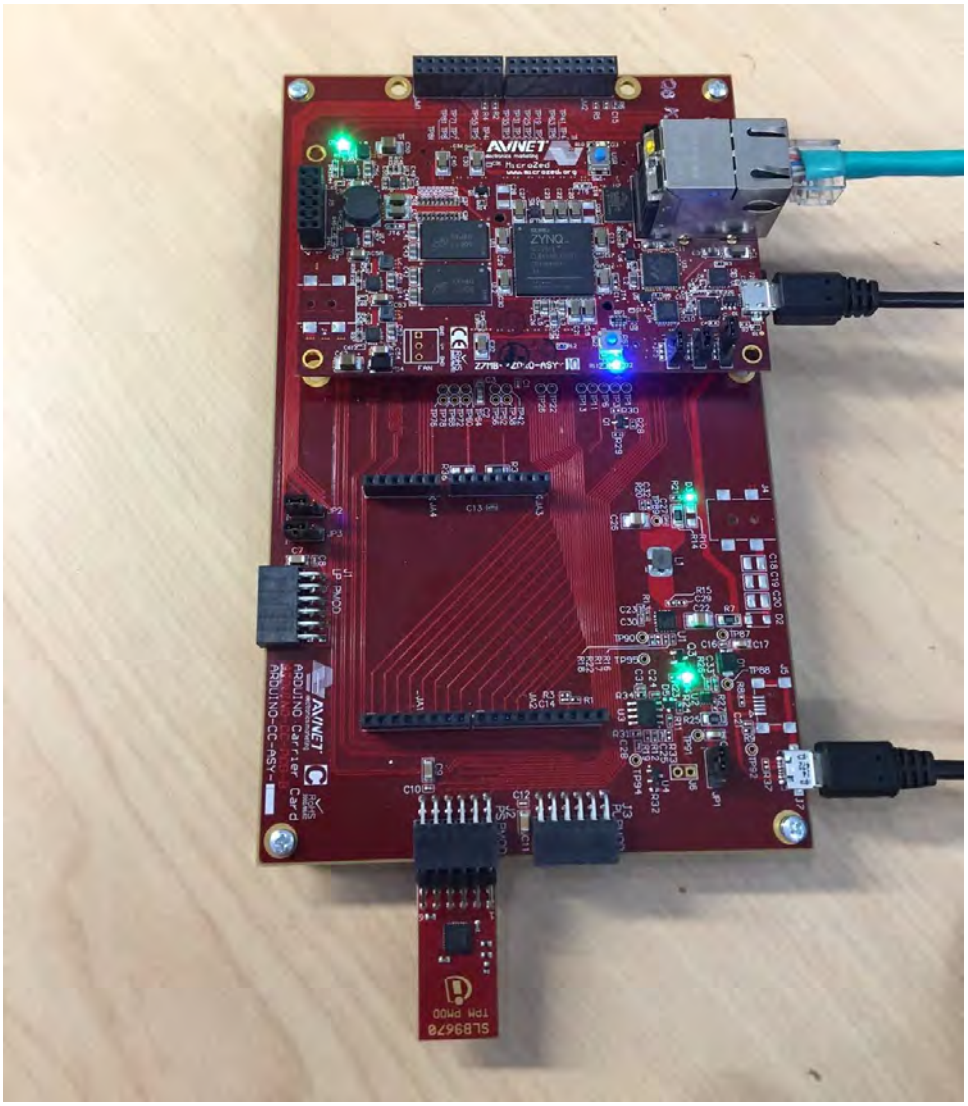
図 3 に、リファレンス デザインで使用される単一クライアント システム用のデスクトップ セットアップを示します。Avnet 社の IIoT 内のクライアントが通信端末を駆動します。strongSwan 検証サーバーは VirtualBox から実行します。ブラウザーを使用して、測定値およびポリシーのインプリメンテーションを表示します。



X18725-020317

図 3: メジャー ブートのリファレンス デザイン

図 4 は、Avnet 社の Arduino キャリア カードに MicroZed ボードがマウントされた Avnet 社の IIoT スターター キットを示しています。また、J2 PS PMOD コネクタに差し込まれた Infineon 社の OPTIGA TPM 1.2 SLB 9670 Pmod も示しています。



X18724-020317

図 4: Infineon 社の OPTIGA SLB 9670 TPM を接続した Avnet 社の IIOT スターター ボード

PMOD コネクタ J2 に接続した Infineon 社の OPTIGA SLB 9760 は、プロセッシング システム (PS) シリアル ペリフェラル インターフェイス (SPI) ドライバーを使用して Zynq-7000 AP SoC と通信します。Wind River Pulsar Linux (WRPL) 8.0 は MicroZed 上で実行され、strongSwan クライアント ソフトウェアが含まれています。WRPL をブートする前に、Zynq-7000 AP SoC は FSBL を実行します。FSBL は bootROM および FSBL のプリブート認証を実行します。

FSBL は次に PCR 拡張コマンドを実行して、bootROM および FSBL SHA-1 ダイジェストを PCR[0] および PCR[4] に記録します。PCR 拡張コマンドは書き込みコマンドに似ています。書き込み値と異なる点は、PCR にロードされる値が PCR にロードされる SHA 値を累積した SHA だということです。書き込みではなく PCR 拡張が実行されるため、敵対者は PCR を読み取って適切な値を得ることができません。

図 5 に、考えられる 3 つのシステム セットアップを示します。Ubuntu サーバー上で実行する strongSwan ソフトウェアによりリモート認証とネットワーク セキュリティの確保の両方が実行されます。イーサネット接続は、PC と Avnet 社製ボードを直接接続するか、イーサネットの壁コンセントを使用して DHCP (Dynamic Host Configuration Protocol) で接続できます。(a) では、サーバーは PC 上の VirtualBox または VMware のいずれかの Ubuntu インストール環境で実行されます。(b) では、Ubuntu ベースの PC で strongSwan サーバーが実行されます。(c) では、サーバーはアマゾン ウェブ サービス (AWS) 上で実行されます。ザイリンクスは AWS アカウントを提供していません。

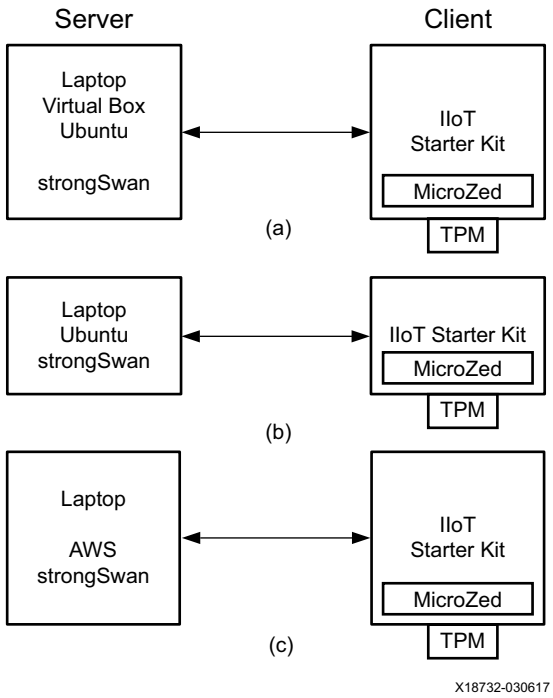


図 5: リファレンス システムのハードウェア セットアップ オプション

リファレンス システムでは単一クライアントのメジャー ブート方法が提供され、エンベデッド システム向けの新機能である早期ロード ソフトウェア (bootROM、FSBL) のリモート認証が提供されます。実際に接続されるシステムには複数のエンベデッド デバイスがあり、strongSwan サーバーは早期ロード ソフトウェアだけでなく、ロードされるすべての Linux パーティションを測定します。

ハードウェアによる信頼のルート (HROT)

Zynq-7000 AP SoC では、HROT は電源投入時に ARM® CPU0 によって実行される最初のコードに基づきます。このコードはオンチップのメタルマスクされた ROM に格納され、bootROM コードと呼ばれます。bootROM コードは変更不可能であり、その基本機能はデバイスの初期化と読み出し/書き込み可能なオンチップ メモリ (OCM) への FSBL のロードです。bootROM も OCM もデバイス ピンからアクセスできません。『Zynq-7000 All Programmable SoC テクニカル リファレンス マニュアル』(UG585) [参照 1] の bootROM コンフィギュレーションのフローチャート図には bootROM コード機能のフローが記載されています。セキュア ブートが指定された場合、bootROM は FSBL を実行する前に RSA-2048 標準を使用して FSBL を認証します。Zynq-7000 AP SoC の HROT は、エンベデッド プラットフォームに TPM を追加して強化されます。TPM は、パーティション測定、暗号化機能、および Zynq-7000 AP SoC が使用するキーを格納するためのセキュアなキー ストレージを提供します。

Zynq-7000 AP SoC では、「セキュア ブート」という用語は、電源投入時のビットストリームおよびソフトウェアのセキュアなロードを定義するために使用されます。ビットストリームはオンチップ コンフィギュレーション メモリにロードされます。不揮発性メモリ (NVM) 内で暗号化されたソフトウェア パーティションは一般的に、認証および復号化されて DDR メモリにコピーされます。図 6 に示すように、RSA-2048 認証ではロードされる各パーティションに対して信頼の連鎖が順に適用されます。各パーティションは独自の秘密キー /公開キーのペアを使用できます。パーティションは必要に応じて、キー付き HMAC (Hash Message Authentication Code) を使用して認証できます。最も単純な形態として、FSBL によってロードされたすべてのパーティションが XILRSA ライブラリの RSA-2048 を使用して認証されます。代替のブート フローでは、U-Boot が XILRSA ライブラリにアクセスします。セキュア ブートでは、RSA 認証または HMAC 認証が失敗すると、Zynq-7000 AP SoC はロックダウン状態に遷移します。

悪意ある攻撃者はデバイスに格納されていない RSA 秘密キーと HMAC キーを盗む必要があります。内部攻撃から守るために、SDK Bootgen キー管理を分割して、RSA キー、AES キー、および HMAC キーを独立して扱うようにすることが可能です。

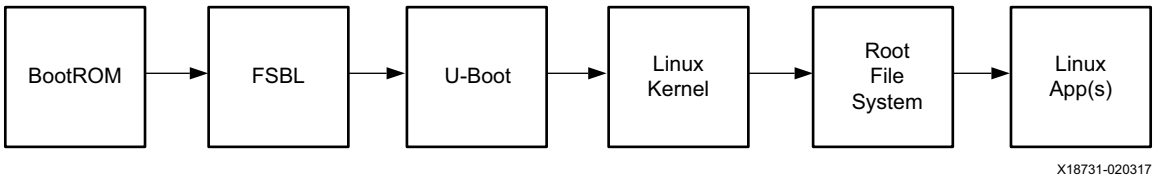


図 6: Zynq-7000 AP SoC のブートの信頼の連鎖

メジャー ブート

エンベデッド システムがネットワークに接続されているときはメジャー ブートが推奨されます。メジャー ブートを使用するシステムでは、セキュア ブートも引き続き使用する必要があります。セキュア ブートとメジャー ブートは補完的な機能です。エンベデッド システムをネットワークに接続すると、ファームウェア アップデートの手段が得られます。ネットワークに接続されたエンベデッド システムは、クローズド システムに比べて多方面からの攻撃にさらされます。ネットワークにアクセスするハッカーは一般にセキュリティ上の脅威です。リモート認証は、ブート時およびランタイム中にこの脆弱性に対処します。セキュア ブートおよびメジャー ブートでは、すべてのファイル/パーティションが認証および測定されます。

基本的なメジャー ブートについては、「IMA (Integrity Measurement Architecture)」を参照してください。リファレンス デザイン内のメジャー ブートでは、セキュリティを高めるために TPM が使用されています。「Trusted Platform Module」、「Zynq 7000 SoC-TPM インターフェイス」、および「メジャー ブートのネットワーク セキュリティ」で、TPM を使用したメジャー ブートについて説明しています。セキュア ブートおよびメジャー ブートではプログラマブル ロジック リソースが使用されないため、メジャー ブート使用時の Zynq-7000 AP SoC ユニットのコストに影響はありません。

認証サーバーは測定内容を使用してクライアントに対してランタイム インテグリティ チェックを定期的に実行し、結果に基づいてポリシーを実行できます。ランタイム中は攻撃の可能性が高いため、接続システムではこれは重要です。ポリシーを実行する機能はランタイム インテグリティ チェッカー (RTIC) からの機能向上で、『Zynq-7000 AP SoC システム メモリのラン タイム インテグリティと認証チェック』(XAPP1225) [参照 2] に記載されています。

IMA (Integrity Measurement Architecture)

IMA はメジャー ブートの基盤となります。IMA の概要は strongSwan の資料 [参照 3] に記載されています。

IMA によるリモート認証では、サーバーはクライアントから受け取った測定内容をリファレンス インテグリティ測定値 (RIM) と比較し、事前に定義されたポリシーに従って動作します。リファレンス デザインでは、これはポリシー決定ポイント (PDP) と呼ばれます。メジャー ブートを実行した後、サーバー ウェブサイトは測定のサマリとリファレンス デザインのポリシーを表示します。

IMA インプリメンテーションでは、クライアントはインテグリティ測定収集 (IMC) を実行します。サーバーはインテグリティ測定検証 (IMV) を実行します。図 7 に、Linux のパーティションがすべて測定されたときのログの例を示します。

```
ls /sys/kernel/security/ima
ascii_runtime_measurements  binary_runtime_measurements  runtime_measurements_count  violations

sudo cat /sys/kernel/security/ima/runtime_measurements_count
1271

sudo less /sys/kernel/security/ima/ascii_runtime_measurements
10 ef2be9c304d9bbbd8ecb40f0d296176d2b5d3078 ima-ng sha1:4663ed64e5dbbb9755a0914b1a15fa76a1797806 boot_aggregate
10 ef411bae164fd624ea94fc9ef82f892c82d78dcd ima-ng sha1:bbe98e20b850f3907611fb96354b5e007a9179f4 /init
10 bd32e452e14f84eb22d6ac9e9e1c61eeac3cd7a4 ima-ng sha1:dc3e621c72cde19593c42a7703e143fd3dad5320 /bin/sh
10 eefd4a6bebd6b001ff587c2335a3dd03535d5a17 ima-ng sha1:d11ce2e31ab441be705df3061a3d6fb7e41a504e /lib64/ld-linux-x86-64.so.2
10 8e8844cba6dc9df17c6980122890487f818e4b28 ima-ng sha1:34efdbd6d562ac04f7e02195022c3f65f7553bd2 /etc/ld.so.cache
10 1f60da15c941fe25a18ee4e8378f0bf3b447a0ab ima-ng sha1:65228a2bbff8ca52d2040ac55499b348f648cc81 /lib/x86_64-linux-gnu/libc.so.6
10 223eb68bfb9f72922506747d3bc4dd76d813b5da ima-ng sha1:65030975e1f3887efd00fbb568f00409b7c256d0 /conf/arch.conf
10 f548183aeb29921c995b625a93c4acd3ef7faaec ima-ng sha1:feb140057713c4f1e383d79b71f6efdafbed7476 /conf/initramfs.conf
10 de528d81c1c203a597c313f54bbe45d54fd0cc18 ima-ng sha1:2231aa397f5b6327973d8fcaf540735fd1e39496 /conf/conf.d/resume
10 cf9a07066457e26219a6f345957a727b07096d8b ima-ng sha1:2199e965dcc97c6814b78528e5a5e690a29c0fd5 /scripts/functions
10 246635237cb7beaec50809203292f8623db6a83f ima-ng sha1:c7c7f8b3ae433ebe08189f143840f737d7711936 /scripts/init-top/ORDER
10 d0dc06f1a392d4505448572cd520b1ba6e53ff14 ima-ng sha1:4975101256fea3bf1e9a6a9ea5a4d97947f4097d /scripts/init-top/all_generic_ide
10 e2aab17444614530ec77595ef3f361bb00490100 ima-ng sha1:76dfee4b97d5327820a87ad4ec99a132a5f32cca /scripts/init-top/blacklist
10 a3dd75cea37a4330c6abefdeaa291feace1ee3a4 ima-ng sha1:869c43fa9e2c561d612c657ff45eb743beadc873 /scripts/init-top/ima_policy
10 465108cd35c590785a52eaecd9e997a0f570ada5 ima-ng sha1:a3f4886df912c0550f4e32cec1814e7f92e0218b /sbin/init
10 c78f4cecff4b004c9956c84628e6514a4d39881d ima-ng sha1:d11ce2e31ab441be705df3061a3d6fb7e41a504e /lib/x86_64-linux-gnu/ld-2.19.so
10 847203248af633d214e91dd1b3397e9d462771c7 ima-ng sha1:26837b475d0fb26d4256ce1744f52b264d67b58f /lib/x86_64-linux-gnu/libnih.so.1.0.0
10 367f76edbab585e2441bed7ee66fab6c7a1c0dad ima-ng sha1:d52c92a8019c259f40ae1240372dd598c2a1c54c /lib/x86_64-linux-gnu/libnih-dbus.so.1.0.0
10 b35e07f368b2d129dc9f3fd8ae325a9e3cf01a36 ima-ng sha1:d3892d8e70b27c4638ca8fbeceeed0386b7d672e /lib/x86_64-linux-gnu/libdbus-1.so.3.7.6
10 465a4a6342823c30427ca8374de54acb26bbb9fb ima-ng sha1:580764ad1cb67e7c37f49581ebf6369456795440 /lib/x86_64-linux-gnu/libselinux.so.1
10 5e8baf31a7f08a8e103f0f8174a3432e39161262 ima-ng sha1:91de58ef6be75cf952caecab0f2830c5b3527bbc /lib/x86_64-linux-gnu/libjson-c.so.2.0.0
10 d482b0fa3c1755c99380c279d73b77088c2a5d62 ima-ng sha1:011ea7ea14e6874e9da0245e4e6ed472d02814ed /lib/x86_64-linux-gnu/librt-2.19.so
10 a2733a6feac3a4d293af84f2ce47c1305cabc870 ima-ng sha1:65228a2bbff8ca52d2040ac55499b348f648cc81 /lib/x86_64-linux-gnu/libc-2.19.so
10 5da2378816b820601c8c708614784a7b5de5e8b8 ima-ng sha1:9ecd4089b74f1036c9825c2d082356e9ffb964f3 /lib/x86_64-linux-gnu/libpthread-2.19.so
10 cb8fc9859356d3802b365108d4a8baadf9251135 ima-ng sha1:9afccef2b8c4944cd78d25b87bc9198a3cb82406 /lib/x86_64-linux-gnu/libpcre.so.3.13.1
10 a3d30aa5bc7a24c3dd341d2eaa2ae4824915245a ima-ng sha1:cf26e327ee6f69694b080ae66c2572a6cb9c9c66 /lib/x86_64-linux-gnu/libdl-2.19.so
10 8b39d375a031075939a1621b2b470d0284c1f534 ima-ng sha1:c799f2ccebf69f87afc91520793631b3f0b9692b /lib/x86_64-linux-gnu/libnss_compat-2.19.so
10 ffab1636ff997c9b5040b637fe1cbfeae36988a5 ima-ng sha1:b74430744e6927384b34fd93385f8229b53e2dd7 /lib/x86_64-linux-gnu/libnsl-2.19.so
10 980f0b3422677f12d5af8850067e0b777358a013 ima-ng sha1:7fe4a578af95b0ebf1426573d088f110e5cdd8fe /lib/x86_64-linux-gnu/libnss_nis-2.19.so
10 60bd11e71fcd550996d557efaf1206832fe60cc5 ima-ng sha1:e12cc6838353f93bf43663081293d5891479f96f /lib/x86_64-linux-gnu/libnss_files-2.19.so
10 214c1d89e94ef8e89248a9b010cb7c050b6eef37 ima-ng sha1:8599d27418cf321a855d0c79091f1dfd5bec202d /bin/hostname
10 cb69d6e743aa7b96f011e7b74a37493bca7c5c26 ima-ng sha1:647437c3d7543c7c8d381903834c9ef42eb4cf69 /bin/sh
```

X18726-020317

図 7: IMA の証拠ログ

Trusted Platform Module

TPM 機能の資料は Trusted Computing Group (TCG) によって提供されており、『TPM Main Specification』[参照 4] が最初の資料です。2016 年に最もよく使用された TPM は TPM 1.2 でした。Infineon 社の OPTIGA SLB9670 TPM は TPM 1.2 および 2.0 をサポートします。TPM は Root of Trust for Reporting (RTR) および Root of Rrust for Storage (RTS) によるセキュリティを提供する非常に小型のコスト効果の高いデバイスです。このアプリケーション ノートでは、TPM の PCR に保持される測定ログ ファイルがサーバーに報告される RTR に注目します。

RTR のサポート以外に、TPM には Zynq-7000 SoC アプリケーションに役立つ機能が提供されていることがあります。TPM は再プログラム可能な不揮発性メモリを備えています。TPM の強固な暗号化機能によって、キーを Zynq-7000 デバイスに対してオンデマンドで安全に送信できます。TPM には乱数ジェネレーター (RNG) があります。RNG はキーを生成するために使用できます。

TPM RTR サポートは IMA フレームワーク内で動作し、セキュリティが大幅に強化されます。TPM が追加されると、クライアントに対するサーバーのリモート認証は引用に基づいて実行されます。引用とは、ブートされるパーティションの測定または証拠です。TPM 1.2 では、ロードされるパーティションの測定として SHA-1 ダイジェストが使用されます。TPM 2.0 では、ロードされるパーティションの測定ログとして SHA-2 ダイジェストが使用されます。SHA ダイジェストは PCR に格納されます。図 8 に、リモート認証の場合のサーバーとクライアントの通信を示します。

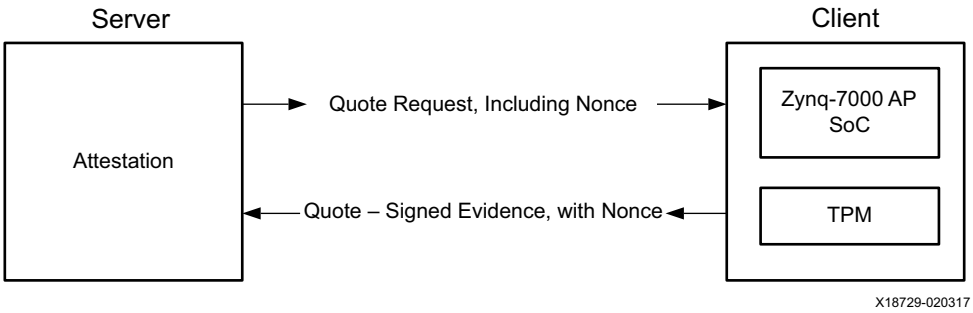


図 8: TPM を使用したリモート認証

図 8 のフローの概要は次のとおりです。

1. strongSwan 検証サーバーはクライアントからの引用を要求します。引用を要求する際、サーバーはプレイバック攻撃から保護するために使用される乱数であるノンスを送信します。
2. クライアントまたは Zynq-7000 SoC/TPM はロードされたパーティションの証拠を生成します。SHA-1 ハッシュは TPM PCR に格納されます。bootROM コードの SHA-1 は PCR[0] に格納され、FSBL の SHA-1 ダイジェストは PCR[4] に格納されます。
3. Zynq-7000 SoC/TPM クライアントはサーバーに引用を送信します。これには署名済みの証拠と元のノンスが含まれます。
4. strongSwan サーバーは引用を評価し、その結果に基づいて、システム管理者によって設定されたポリシーに従います。

Zynq 7000 SoC-TPM インターフェイス

Zynq-7000 SoC-TPM インターフェイスは、Zynq-7000 デバイスと Infineon 社の OPTIGA SLB9670 TPM 間の通信機能を提供します。このインターフェイスでは tpm_toolbox からのコマンドが使用されます。tpm_toolbox では次のカテゴリのコマンドがサポートされます。

- PCR リセット
- 物理的存在
- 取得機能
- TPM スタートアップ/アクティブ化/物理的有効化
- PCR 読み出し/PCR 拡張

各カテゴリには複数のコマンドがあります。リファレンス デザインではコマンドのサブセットが使用されます。Zynq-7000 AP SoC は SPI バスを使用して SLB9670 TPM に接続します。Zynq-7000 AP SoC にはハード化された SPI IP が PS 内に含まれ、ソフト AXI SPI IP がプログラマブル ロジック (PL) 内に含まれています。PS SPI がリファレンス デザイン内で使用されているのは、PL リソースが節約されるためです。

図 9 は、リファレンス デザインの FSBL でインプリメントされる SPI-TPM 機能を示します。

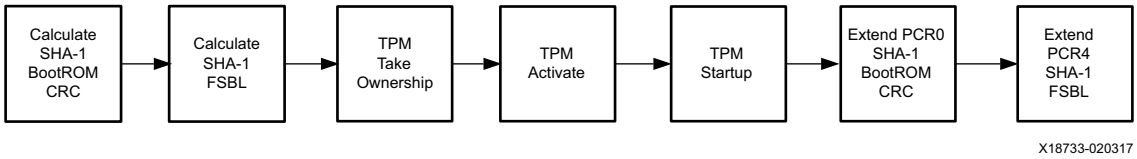


図 9: FSBL TPM SPI ドライバー機能図

メジャー ブート リファレンス デザインの FSBL は bootROM および FSBL の SHA-1 を計算し、SHA-1 ダイジェストを TPM の PCR に拡張するように変更されています。SHA-1 値は `sha1.c` で計算されます。所有権を獲得して TPM をアクティブ化するコードは `slb9670_tpm_spi.c` にあります。PCR は `slb9670_spi_tpm.c` で拡張されます。`fsbl/src` に追加されるその他のファイルには、`tpm_tools.h`、`tpm_tools.c`、`tpm_spi.c`、`tpm_spi_tis.c`、`tpm.h` などがあります。bootROM コードは FSBL でアクセスできないため、bootROM について計算される SHA-1 は、bootROM コードによって書き込まれる巡回冗長検査 (CRC) で計算されます。

FSBL TPM ドライバーは NVM への格納時に暗号化でき、後に復号化して OCM から実行できます。FSBL で早期ロード測定値を使用して TPM PCR を拡張する理由は、悪意ある攻撃者がコードを変更する時間を制限するためです。

Avnet 社のスターター IIoT ボードでは、SLB9670 Pmod に対する PS SPI のインターフェイスの MIO 接続が使用されます。TPM のピン リセットを駆動するために、Zynq-7000 AP SoC ハードウェア デザインにそのための PS GPIO が追加されます。ResetTPM 関数は `main.c` にあります。

メジャー ブートのネットワーク セキュリティ

ソフトウェア アップデートおよびリモート認証では、サーバーとエンベデッド システム クライアント間のセキュアな接続が必要です。インターネットにアクセスできるあらゆる敵対者がネットワークを攻撃できるため、ネットワークは多方面からの攻撃にさらされます。ファームウェア アップデートには、サーバーからクライアントへの接続が使用されます。一部のファクトリ オートメーション環境では、操作手順を調整するためにクライアント間の通信も必要です。

図 10 に、strongSwan による TCG の Trusted Network Connect (TNC) のインプリメンテーションの概略図を示します。TNC アーキテクチャでは、サーバーはインテグリティ評価レイヤーでクライアントに接続します。クライアントでインテグリティ測定収集 (IMC) が実行され、サーバーではインテグリティ測定検証 (IMV) が実行されます。クライアント側のソフトウェアは Platform Trusted Service (PTS)、トラスト ソフトウェア スタック (TrouSerS)、および TPM ツールです。

PTS は TrouSerS ライブラリを使用して TPM 測定値および IMA 測定値にアクセスします。レポートではアプリケーションとベンダー間の相互運用性のために標準の PTS 形式が使用されます。

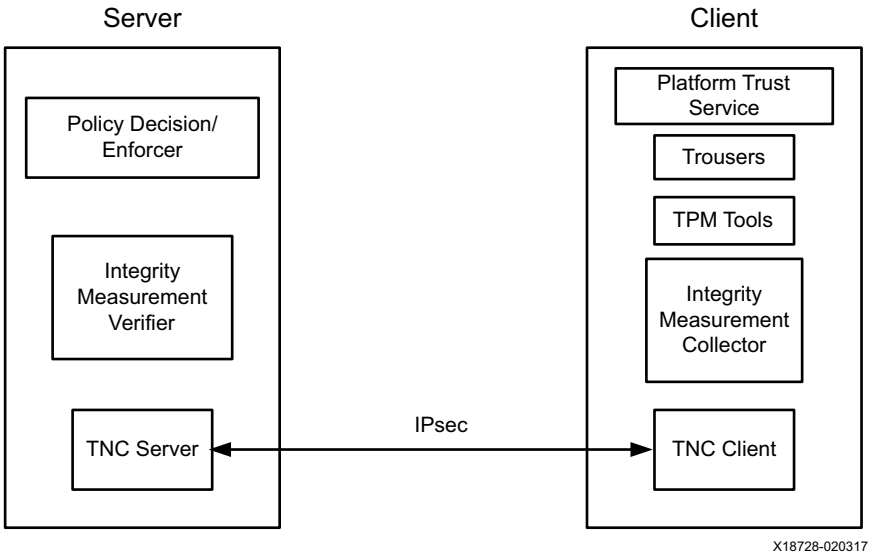


図 10: リモート認証のための Trusted Network Connect

ポリシー決定ポイント (PDP) は、測定検証後にサーバーによって実行される動作を定義します。標準的なポリシー /アクションでは、対策が実行されるまでネットワーク アクセスを制限します。可用性が重要な要素である場合は別のポリシーが使用され、一部の範囲外の測定検証は重要な問題として扱われません。『TPM Main Specification』[参照 4] に、TNC アーキテクチャの概要が記載されています。

リファレンス デザインでは TNC の下位のセキュリティとして IPsec が使用されます。これにはインターネット キー交換 (IKEv2)、公開キー基盤 (PKI)、トランスポート レイヤー セキュリティ (TLS) ハンドシェイクなどの従来の技術が使用され、これらの技術では暗号化アルゴリズムおよび認証アルゴリズムがネゴシエートされて事前共有キーが交換されます。strongSwan アーキテクチャに仮想プライベート ネットワークが設定されます。プライバシー CA が x509 証明書を生成します。strongSwan の `Readme.txt` に IPsec フローに関する情報があります。

リファレンス デザインの機能概要

IMA、TPM、およびネットワーク セキュリティを設定するために、リファレンス デザインでは次のステップが実行されます。

- Linux カーネル内の IMA のアクティブ化
- IMA ポリシーの設定
- TPM のアクティブ化
- プライバシー認証局 (CA) の設定
- 検証クライアントの設定 (Zynq-7000 AP SoC)
- 検証 ID キー (AIK) の生成
- インテグリティ測定コレクターの設定
- TNC クライアントの設定
- VPN 接続の設定
- 認証サーバーのセットアップ/設定 (strongSwan VPN/TNC サーバー)
- 測定値の収集
- ポリシー マネージャーへのデバイスの登録

プロセスは strongSwan のウェブサイトに定義されています。

まとめ

同じデバイス上のハードウェアおよびソフトウェアの両方をプログラムできる Zynq-7000 AP SoC の機能は、非常に大きなアドバンテージとなります。エンベデッド システムの性能を高めて TCO を削減するメンテナンス性を実現する上で重要なのは、コスト効果の高いファームウェア アップデートです。リモートからのファームウェア アップデートはインターネットの使用に依存し、エンベデッド システムを暗号化攻撃にさらすことになります。このアプリケーション ノートでは、接続デバイスにおいて実証済みのセキュリティを実現するメカニズムを提供します。

参考資料

注記: 日本語版のバージョンは、英語版より古い場合があります。

1. 『Zynq-7000 All Programmable SoC テクニカル リファレンス マニュアル』(UG585: 英語版、日本語版)
2. 『Zynq-7000 AP SoC システム メモリのラン タイム インテグリティと認証チェック』(XAPP1225: 英語版、日本語版)
3. 『Linux Integrity Measurement Architecture』wiki.strongswan.org/projects/strongswan/wiki/IMA
4. 『TPM Main Specification』www.trustedcomputinggroup.org/tpm-main-specification
5. 『Zynq-7000 All Programmable SoC のセキュア ブート』(XAPP1175: 英語版、日本語版)

改訂履歴

次の表に、この文書の改訂履歴を示します。

日付	バージョン	内容
2017 年 3 月 7 日	1.0	初版

重要な法的通知

本通知に基づいて貴殿または貴社 (本通知の被通知者が個人の場合には「貴殿」、法人その他の団体の場合には「貴社」。以下同じ) に開示される情報 (以下「本情報」といいます) は、ザイリンクスの製品を選択および使用することのためにのみ提供されます。適用される法律が許容する最大限の範囲で、(1) 本情報は「現状有姿」、およびすべて受領者の責任で (with all faults) という状態で提供され、ザイリンクスは、本通知をもって、明示、黙示、法定を問わず (商品性、非侵害、特定目的適合性の保証を含みますがこれらに限られません)、すべての保証および条件を負わない (否認する) ものとします。また、(2) ザイリンクスは、本情報 (貴殿または貴社による本情報の使用を含む) に関係し、起因し、関連する、いかなる種類・性質の損失または損害についても、責任を負わない (契約上、不法行為上 (過失の場合を含む)、その他のいかなる責任の法理によるかを問わない) ものとし、当該損失または損害には、直接、間接、特別、付随的、結果的な損失または損害 (第三者が起こした行為の結果被った、データ、利益、業務上の信用の損失、その他あらゆる種類の損失や損害を含みます) が含まれるものとし、それは、たとえ当該損害や損失が合理的に予見可能であったり、ザイリンクスがそれらの可能性について助言を受けていた場合であったとしても同様です。ザイリンクスは、本情報に含まれるいかなる誤りも訂正する義務を負わず、本情報または製品仕様のアップデートを貴殿または貴社に知らせる義務も負いません。事前の書面による同意のない限り、貴殿または貴社は本情報を再生産、変更、頒布、または公に展示してはなりません。一定の製品は、ザイリンクスの限定的保証の諸条件に従うこととなるので https://japan.xilinx.com/legal.htm#tos で見られるザイリンクスの販売条件を参照してください。IP コアは、ザイリンクスが貴殿または貴社に付与したライセンスに含まれる保証と補助的条件に従うことになります。ザイリンクスの製品は、フェイルセーフとして、または、フェイルセーフの動作を要求するアプリケーションに使用するために、設計されたり意図されたりしていません。そのような重大なアプリケーションにザイリンクスの製品を使用する場合のリスクと責任は、貴殿または貴社が単独で負うものです。https://japan.xilinx.com/legal.htm#tos で見られるザイリンクスの販売条件を参照してください。

自動車用のアプリケーションの免責条項

ザイリンクスの製品は、フェイルセーフとして設計されたり意図されてはおらず、また、フェイルセーフの動作を要求するアプリケーション (具体的には、(I) エアバッグの展開、(II) 車のコントロール (フェイルセーフまたは余剰性の機能 (余剰性を実行するためのザイリンクスの装置にソフトウェアを使用することは含まれません) および操作者がミスをした際の警告信号がある場合を除きます)、(III) 死亡や身体傷害を導く使用、に関するアプリケーション) を使用するために設計されたり意図されたりもしていません。顧客は、そのようなアプリケーションにザイリンクスの製品を使用する場合のリスクと責任を単独で負います。

この資料に関するフィードバックおよびリンクなどの問題につきましては、jpn_trans_feedback@xilinx.com まで、または各ページの右下にある [フィードバック送信] ボタンをクリックすると表示されるフォームからお知らせください。いただきましたご意見を参考に早急に対応させていただきます。なお、このメール アドレスへのお問い合わせは受け付けておりません。あらかじめご了承ください。