仕　様　書

１．件名

組込み機器用半導体チップへのハードウェア攻撃用侵入試験機器

２．研究の概要

国立研究開発法人産業技術総合研究所（以下、「産総研」という。）サイバーフィジカルセキュリティ研究センターでは、国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO）受託研究事業「経済安全保障重要技術育成プログラム／ハイブリッドクラウド利用基盤技術の開発／半導体・電子機器等のハードウェアにおける不正機能排除のための検証基盤の確立」の事業内容〔1〕「半導体設計フェーズにおける検証」において研究項目〔1-4〕「セキュリティ仕様への適合性検証」を実施しており、以下の種別の半導体チップに必要不可欠である最低限のセキュリティ機能について、セキュリティ要求仕様書を取りまとめる研究を進めている。

・組込み機器用ローリソースチップ

・車載イメージセンサー用チップ

そして、取りまとめた要求仕様に応じた評価手法を検討し、パイロット実証を行うため、組込み機器用半導体チップの評価手順およびソフトウェア印加の評価手順を構築する計画を進めている。

なお、組込み機器用半導体チップへのハードウェア攻撃用侵入試験機器は、最低限のセキュリティ要求仕様の策定の目的に鑑み、スマートカード等を対象としないモデルとする。

３．機器の概要

本機器は、以下の(1)「組込み機器用半導体チップへの電力及びクロックによるハードウェア攻撃用侵入試験機器　一式」、(2)「組込み機器用半導体チップへの電磁故障注入によるハードウェア攻撃用侵入試験機器　一式」及び(3)「イメージセンサーの組込み機器用半導体チップの評価ボード関連機器」から構成される。

(1)　組込み機器用半導体チップへの電力及びクロックによるハードウェア攻撃用侵入試験機器　一式

(i)電力及びクロックによる侵入試験機器キット

(ii)電力及びクロック等による侵入試験機器キット用のベースボード

(iii)ターゲットボード

(iv)STM32 シリーズのターゲットボード用のデバッガー

(2) 組込み機器用半導体チップへの電磁故障注入によるハードウェア攻撃用侵入試験機器　一式
(i)侵入試験機器キット
(3) イメージセンサーの組込み機器用半導体チップの評価ボード関連機器
(i)ディスプレイパネル
(ii)USB プログラマー・アダプター

４．機器の基本構成
(1) 組込み機器用半導体チップへの電力及びクロックによるハードウェア攻撃用侵入試験機器　一式
(i) 電力及びクロックによる侵入試験機器キット
(ii) 電力及びクロック等による侵入試験機器キット用のベースボード
(iii) ターゲットボード
(a) STM32F0 マイクロコントローラのターゲットボード
(b) STM32F1 マイクロコントローラのターゲットボード
(c) STM32F2 w/ Hardware Crypto Target マイクロコントローラのターゲットボード
(d) STM32F3 マイクロコントローラのターゲットボード
(e) STM32F4 マイクロコントローラのターゲットボード
(f) STM32F4 w/ Hardware Crypto Target マイクロコントローラのターゲットボード
(g) STM32F4 w/ Hardware Crypto Target for CW308 with CAN Breakout マイクロコントローラのターゲットボード
(h) STM32L4 マイクロコントローラのターゲットボード（CW308T-STM32L4）
(i) STM32L5 w/Hardware Crypto Target マイクロコントローラのターゲットボード
(j) Atmel XMEGA デバイスのターゲットボード
(iv) STM32 シリーズのターゲットボード用のデバッガー

(2) 組込み機器用半導体チップへの電磁故障注入によるハードウェア攻撃用侵入試験機器　一式
(i) 侵入試験機器キット

(3) イメージセンサーの組込み機器用半導体チップの評価ボード関連機器
(i) ディスプレイパネル
(ii) USB プログラマー・アダプター

５．基本構成別仕様

以下に仕様の一覧を示す。

表 1：仕様一覧

項番			名称	仕様
(1)	(i)	—	電力及びクロックによる侵入試験機器キット	サイドチャネル攻撃とグリッチ攻撃の学習のためのオープンソースのツールチェーンとして利用可能な侵入試験機器であり、電力解析によるサイドチャネル攻撃、電力グリッチとクロックグリッチによる故障注入攻撃が実施可能な侵入試験機器キットであり、以下の要求事項を満たした侵入試験機器のキットであること。 ・ターゲットボードと同じクロックを使用して同期した、キャプチャ及びグリッチが可能であること。 ・10 ビット以上、105MS/s 以上の ADC を内蔵していること。 ・ターゲットボードと同じクロック速度と 4 倍のクロック速度の両方でクロックを供給可能であること。 ・+55dB 以上の調整可能な低ノイズゲインにより、小信号を測定できること。 ・FPGA ベースのパルス生成によるクロック及び電源への故障注入が可能であること。 ・XMEGA(PDI)、AVR(ISP)、STM32F(UART シリアル)用のブートローダを内蔵していること。 ・IO (UART および SPI) 及びアナログ波形 (SAD)に対するトリガーを生成できるハードウェア トリガー モジュールの機能を持つこと。 ・98ｋサンプル以上のサンプル バッファー (98k サンプル) を内蔵し、ストリーム モードによるキャプチャが可能であること。 ・液晶画面を搭載したユーザインタフェースを持つこと。

項番			名称	仕様
				・トリガーイン、トリガーアウト用の SMA コネクターを含むこと。 ・防水キャリングケースを含むこと。 ・ターゲットボードを接続して侵入試験を行うベースボードを含むこと。 ・サイドチャネル攻撃試験用 H-Probe を含むこと。 ・サイドチャネル攻撃試験用 Differential-Probe を含むこと。 ・低ノイズアンプと Differential-Probe 用電源サプライを含むこと。 ・低ノイズアンプを含むこと。 ・アナログフィルターを含むこと。
	(ii)	—	電力及びクロック等による侵入試験機器キット用のベースボード	ターゲットボードを接続して、侵入試験機器キットで試験可能であること。
	(iii)	(a)	STM32F0 マイクロコントローラのターゲットボード	STM32F0 マイクロコントローラを実装したターゲットボードであり、ベースボードと接続可能であること。
		(b)	STM32F1 マイクロコントローラのターゲットボード	STM32F1 マイクロコントローラを実装したターゲットボードであり、ベースボードと接続可能であること。
		(c)	STM32F2 w/ Hardware Crypto Target マイクロコントローラのターゲットボード	STM32F2 w/ Hardware Crypto Target マイクロコントローラを実装したターゲットボードであり、ベースボードと接続可能であること。
		(d)	STM32F3 マイクロコントローラのターゲットボード	STM32F3 マイクロコントローラを実装したターゲットボードであり、ベースボードと接続可能であること。
		(e)	STM32F4 マイクロコントローラのターゲットボード	STM32F4 マイクロコントローラを実装したターゲットボードであり、ベースボードと接続可能であること。
		(f)	STM32F4 w/ Hardware Crypto Target マイクロコントローラのターゲットボード	STM32F4 w/ Hardware Crypto Target マイクロコントローラを実装したターゲットボードであり、ベースボードと接続可能であること。

項番			名称	仕様
		(g)	STM32F4 w/ Hardware Crypto Target for CW308 with CAN Breakout マイクロコントローラのターゲットボード	STM32F4 w/ Hardware Crypto Target and with CAN Breakout マイクロコントローラを実装したターゲットボードであり、ベースボードと接続可能であること。
		(h)	STM32L4 マイクロコントローラのターゲットボード	STM32L4 マイクロコントローラを実装したターゲットボードであり、ベースボードと接続可能であること。
		(i)	STM32L5 w/Hardware Crypto Target マイクロコントローラのターゲットボード	STM32L5 w/ Hardware Crypto Target マイクロコントローラを実装したターゲットボードであり、ベースボードと接続可能であること。
		(j)	Atmel XMEGA デバイスのターゲットボード	Atmel XMEGA デバイスを実装したターゲットボードであり、ベースボードと接続可能であること。
	(iv)	—	STM32 シリーズのターゲットボード用のデバッガー	STM32 シリーズのターゲットボードと接続してデバッグが可能であること。
(2)	(i)	—	侵入試験機器キット	以下の要求事項を満たした侵入試験機器のキットであること。 ・Charge Voltage のレンジが 150V ～ 500V を含むこと。 ・Charge Energy が 625 mJ 以上であること。 ・故障注入プローブ（1mm tip の場合）の最小パルス幅が 15 nS (TYP)以下であること。 ・故障注入プローブ（1mm tip の場合）の最大パルス幅が 80 nS (TYP)以上であること。 ・故障注入プローブ（4mm tip の場合）の最小パルス幅が 24 nS (TYP)以下であること。 ・故障注入プローブ（4mm tip の場合）の最大パルス幅が 480 nS (TYP)以上であること。 ・ハードウェア入力トリガーの遅延が 75 nS (TYP)以下であること。

項番			名称	仕様
				・ハードウェア入力トリガーのジッター が 150 pS std-dev (TYP)以下であること ・ハードウェア入力トリガーのパルス幅のジッター(300 to 500V)が 220 pS std-dev (TYP)以下であること。 ・SRAM チップを実装したターゲットボードを含むこと。 ・STM32F303K8T6 マイクロコントローラを実装したターゲットボードを含むこと。 ・径（1mm、4mm）×巻き方向（時計回り、反時計回り)の計４種類のプローブTip を含むこと。 ・メインユニット用の 19V / 3.4A パワーアダプターを含むこと。 ・STM32F303K8T6 マイクロコントローラを実装したターゲットボード用のバッテリーを含むこと。 ・プローブ Tip の電圧と電流を測定するためのオシロスコープ用のアダプターを含むこと。 ・ケーブル（RJ12 シリアル、SMB）及びアダプタ（SMB to SMA、SMB to BNC、SMA(直角）)を含むこと。
(3)	(i)	—	ディスプレイパネル	LED バックライトの 5.5-inch TFT 720 x 1280 ピクセルのディスプレイパネルであり、NXP 社評価キット MIMXRT1170-EVK との接続が可能であること。
	(ii)	—	USB プログラマー・アダプター	25 SPI フラッシュ、24 EEPROM、25 EEPROM、93 EEPROM、95EEPROM のメモリチップへの書き込みが可能な USB プログラマーであり、アダプター、ケーブル、CD-R 一式を含むこと。

６．納入物品

(1) 組込み機器用半導体チップへの電力及びクロックによるハードウェア攻撃用侵入試験機器　一式

(i) 電力及びクロックによる侵入試験機器キット（1 個）

(ii) 電力及びクロック等による侵入試験機器キット用のベースボード（2 個）

(iii) ターゲットボード（一式）

(a) STM32F0 マイクロコントローラのターゲットボード（1 個）

(b) STM32F1 マイクロコントローラのターゲットボード（１個）

(c) STM32F2 w/ Hardware Crypto Target マイクロコントローラのターゲットボード（１個）

(d) STM32F3 マイクロコントローラのターゲットボード（１個）

(e) STM32F4 マイクロコントローラのターゲットボード（１個）

(f) STM32F4 w/ Hardware Crypto Target マイクロコントローラのターゲットボード（１個）

(g) STM32F4 w/ Hardware Crypto Target for CW308 with CAN Breakout マイクロコントローラのターゲットボード（１個）

(h) STM32L4 マイクロコントローラのターゲットボード（CW308T-STM32L4）（１個）

(i) STM32L5 w/Hardware Crypto Target マイクロコントローラのターゲットボード（１個）

(j) Atmel XMEGA デバイスのターゲットボード（１個）

(iv) STM32 シリーズのターゲットボード用のデバッガー（１個）

(2) 組込み機器用半導体チップへの電磁故障注入によるハードウェア攻撃用侵入試験機器　一式

(i) 侵入試験機器キット（１個）

(3) イメージセンサーの組込み機器用半導体チップの評価ボード関連機器

(i) ディスプレイパネル（２個）

(ii) USB プログラマー+アダプター（１個）

７．納入の完了

本機器は、「６．納入物品」に記載された納入物品が過不足なく納入され、仕様書を満たしていることを確認して、納入の完了とする。

８．納入期限及び納入場所

納入期限：２０２５年２月１４日（金）
納入場所：東京都江東区青海 2-3-26
国立研究開発法人産業技術総合研究所
サイバーフィジカルセキュリティ研究センター
臨海副都心センター本館 1F 1106 室

９．付帯事項

（１）納入された製品における能力内の使用中に発生した納入の完了後１年以内の故障については、その修理、調整等責任をもって無償で行うこと。

（２）本仕様書の技術的内容及び知り得た情報に関しては、守秘義務を負うものとする。

（３）本仕様書の技術的内容に関する質問等については、調達請求者と協議すること。また、本仕様書に定めのない事項及び疑義が生じた場合は、調達担当者と協議のうえ決定する。