TOSHIBA
Leading Innovation

※ 本資料の内容は2018年5月15日当時のものです。

LSIとシステムのワークショップ2018

もうひとつのサイバーセキュリティ戦場

～メモリセキュリティ

2018年5月15日
東芝デバイス＆ストレージ株式会社
半導体研究開発センター
エンベデッドコア技術開発部

東芝グループのセキュリティ・機能安全関連製品

- （株）東芝

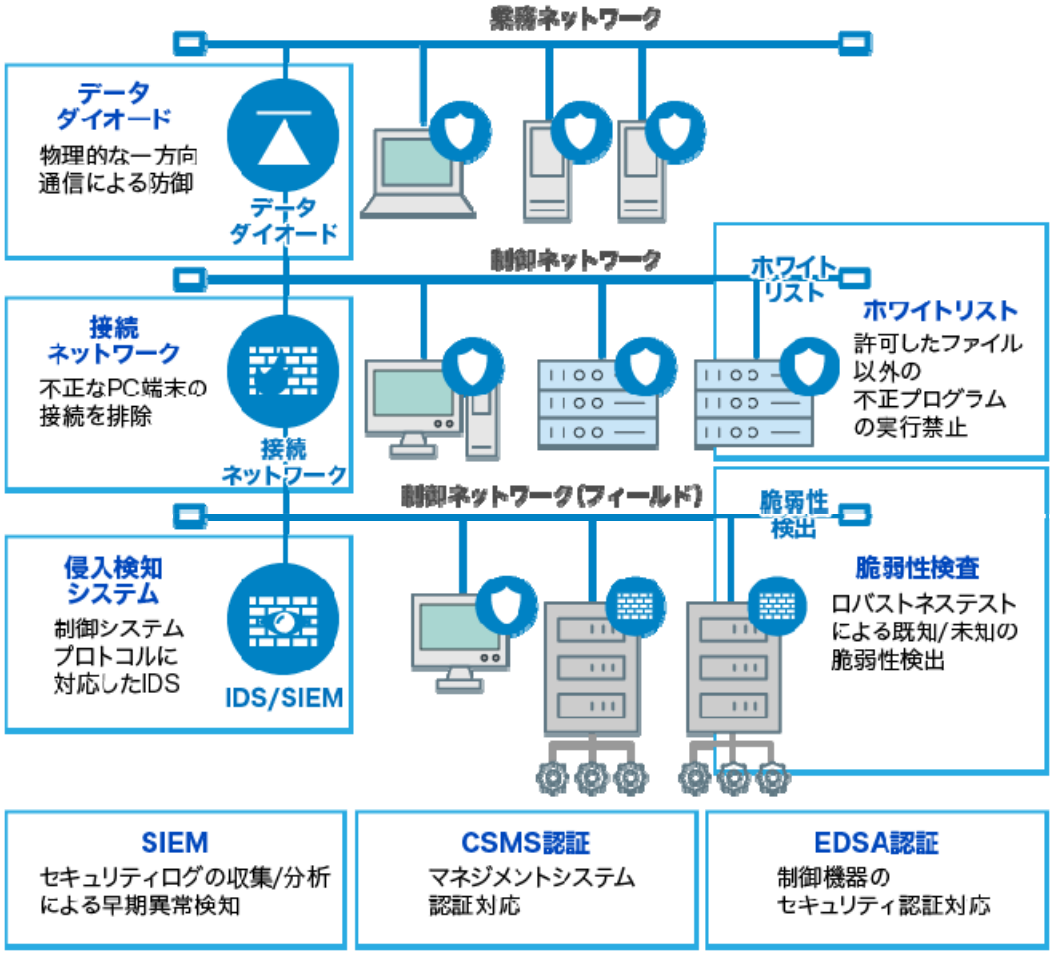
		セキュリティ・機能安全関連プロダクト例
●東芝エネルギーシステムズ㈱	エネルギー事業領域	スマートメータシステム
●東芝インフラシステムズ㈱ ●東芝テック㈱	社会インフラ事業領域	制御装置 鉄道システム
●東芝デバイス＆ストレージ㈱ ●東芝メモリ㈱	電子デバイス事業領域	マイコン（汎用、車載） メモリカード
●東芝デジタルソリューションズ㈱	デジタルソリューション事業領域	制御システム ゲートウェイ
●東芝クライアントソリューション㈱		

東芝デジタルソリューションズの取り組み

ITとOT(Operational Technology)のセキュリティをワンストップで提供

- **社会インフラの制御システムセキュリティ**

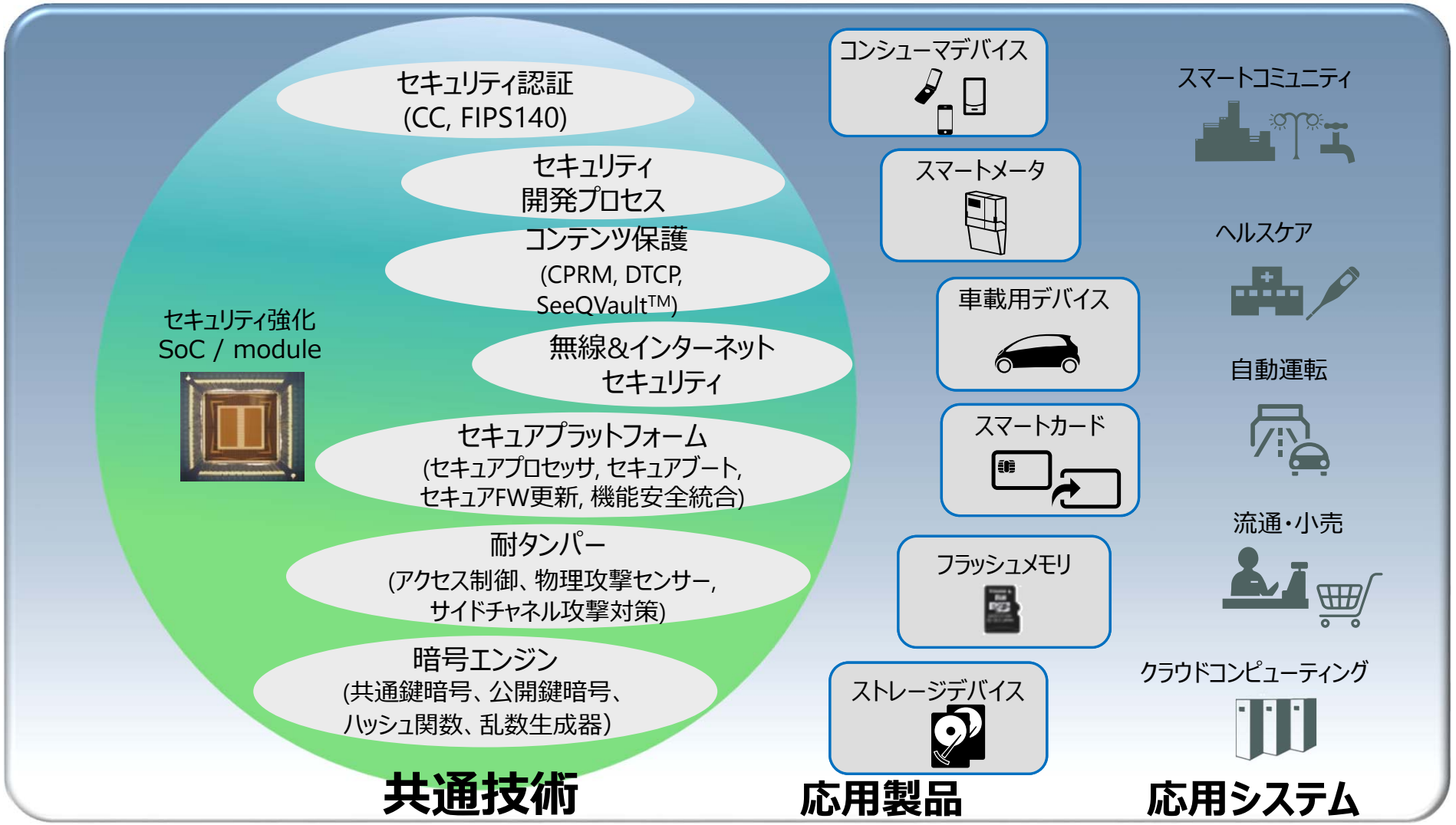
社会インフラシステムの
ドメイン知識を生かした
セキュリティソリューション



出典　http://www.toshiba-sol.co.jp/sol/security/solution/control.htm

東芝デバイス＆ストレージ社セキュリティ技術/製品

コンシューマ向けを中心に半導体・ストレージ製品におけるセキュリティ対応で数多くの実績

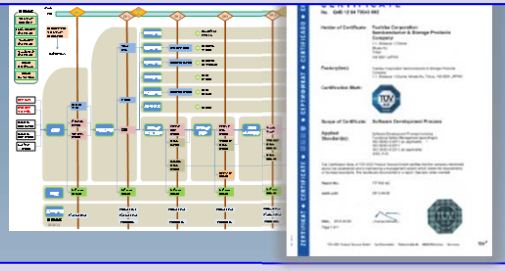


東芝デバイス＆ストレージ社の半導体向け機能安全

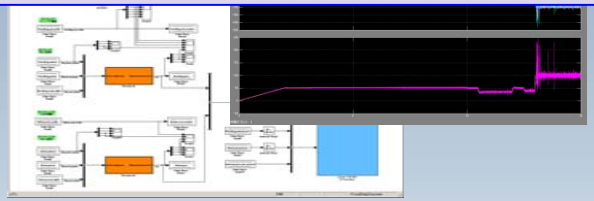
アナログ・MCU・S/Wが一体となりシステムレベルの機能安全実現をサポート

ソフトウェア

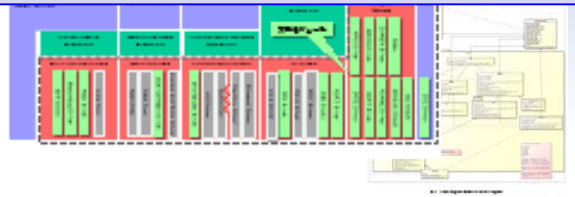
ISO 26262 に基づいた 開発プロセス



モデルベース開発



車載SWプラットフォーム/故障検出ライブラリ



ハードウェア

TM-SIL™

システム監視技術と
認証機関によるSIL3認証取得

東芝機能安全サポートパッケージ"TM-SIL™"
Total Managed SIL package

サポート体制

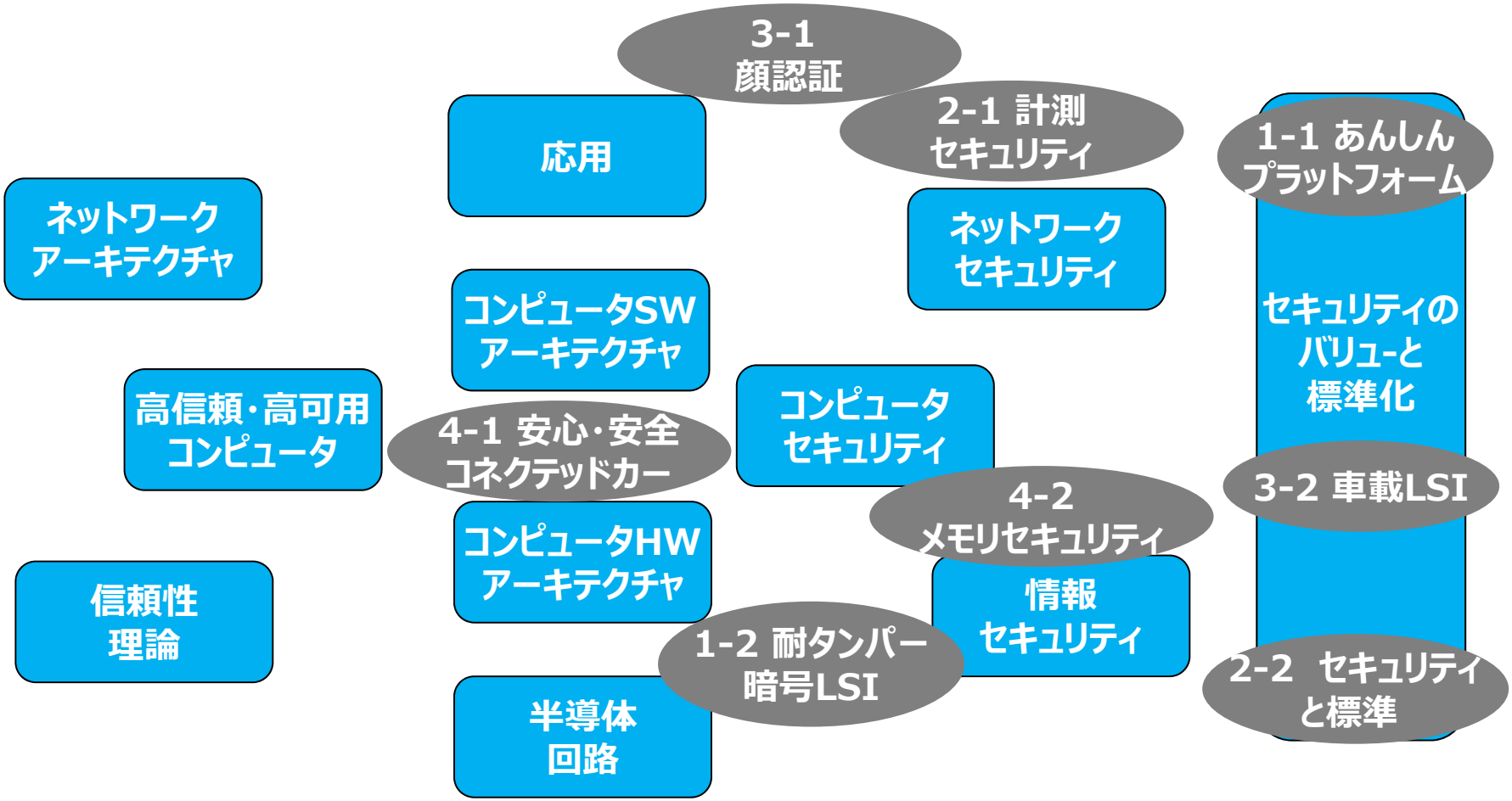
ECUメーカー様

一体で整合
全体最適化

東芝グループ

MCU　S/W　アナログ LSI

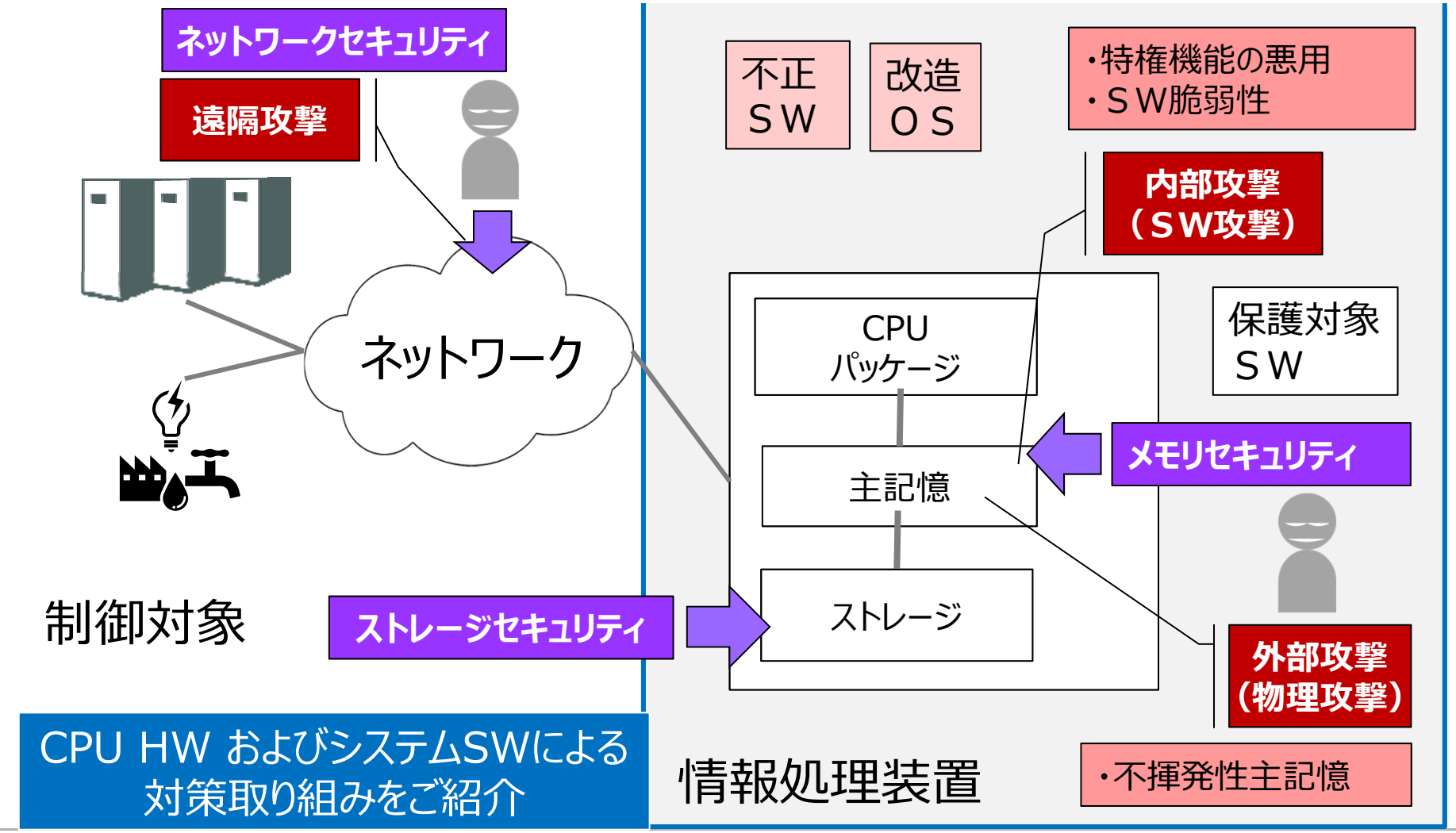
ワークショップにおける技術分野の位置づけ



メモリセキュリティ

メモリセキュリティ～もうひとつのセキュリティ戦場

メモリに対する盗聴・改ざん攻撃はネットワーク遠隔攻撃に次ぐ脅威

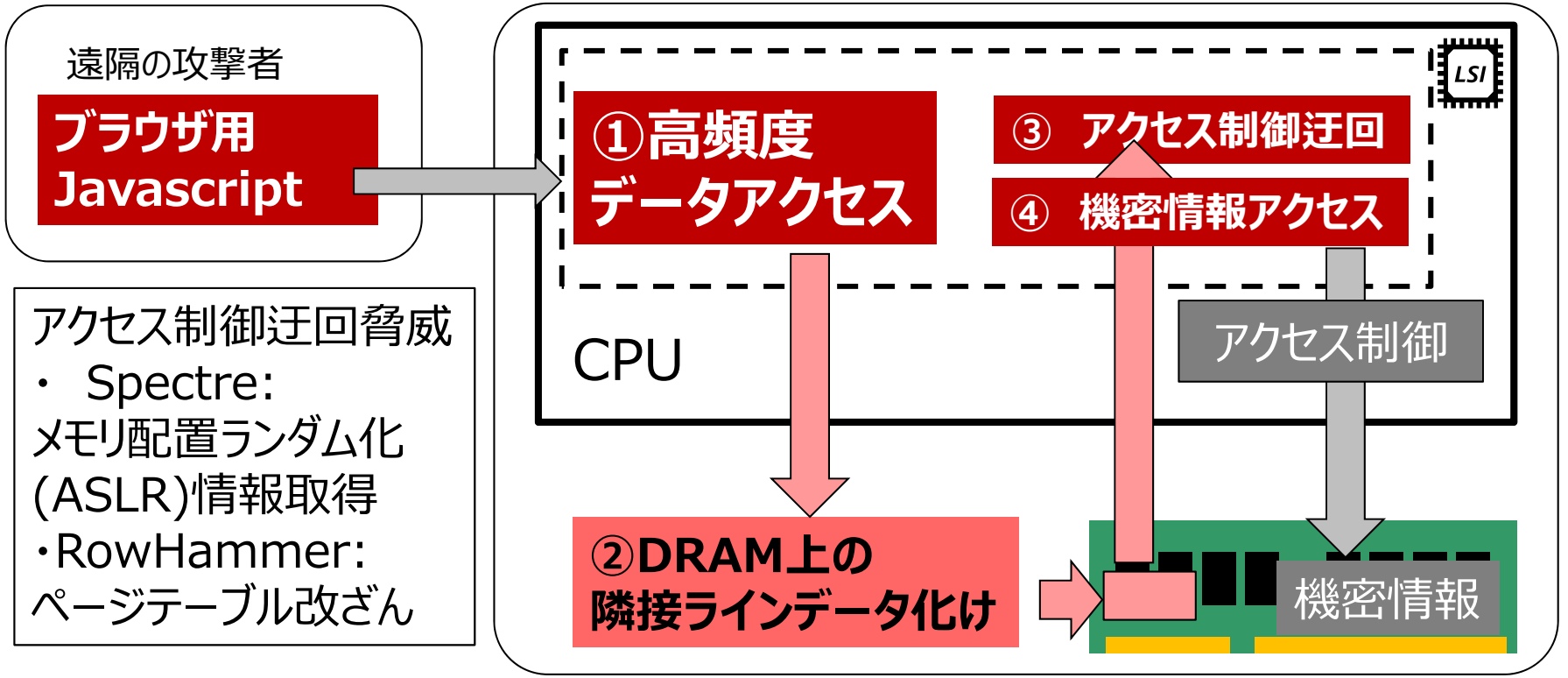


CPU HW およびシステムSWによる
対策取り組みをご紹介

アーキテクチュラルサイドチャネル攻撃との関連

暗号処理に加えて**アクセス制御の迂回**も脅威

- **事例：RowHammer attack**
  - 高頻度アクセスにより**DRAM上隣接ラインのデータが書き換えられる**
  - アプリ権限のみで**カーネルおよび別の仮想マシンがデータ操作**される脅威



LSI セキュリティのターゲット変化

ニーズとシーズの両方に変化

	応用	目的
1980～	IC カード	ICカードの遠隔認証と複製防止
1990～	デジタルコンテンツ保護	コンテンツの暗号化保護と複製規則の迂回防止
2010～	制御システム(IoT)	システム動作の不正変更防止

機密性中心

機密性＋
オープンシステム

＋完全性

右記は重要なアイテムだが
本講演のスコープ外

SW脆弱性対策

メモリセキュリティの応用変化と技術提案

- **応用１：デジタルコンテンツ保護**
  - CE機器における汎用ＯＳ利用
  - 課題
    - ＯＳ特権を利用した不正行為（不正コピー）対策
  - 提案技術

メインメモリデータ暗号化対応のセキュリティプロセッサ(LMSP™)

- **応用２：IoT･社会インフラ**
  - 不揮発性主記憶の導入
  - 課題
    - 重要プログラム･データの改ざんによる異常動作防止
    - システム状態の証拠保全（フォレンジック）手段
  - 提案技術

不揮発メモリ向けメモリ完全性検証技術(TREBIVE)

応用と事業環境の変化

機密性＋
オープンシステム

セキュリティ技術の進化

＋完全性

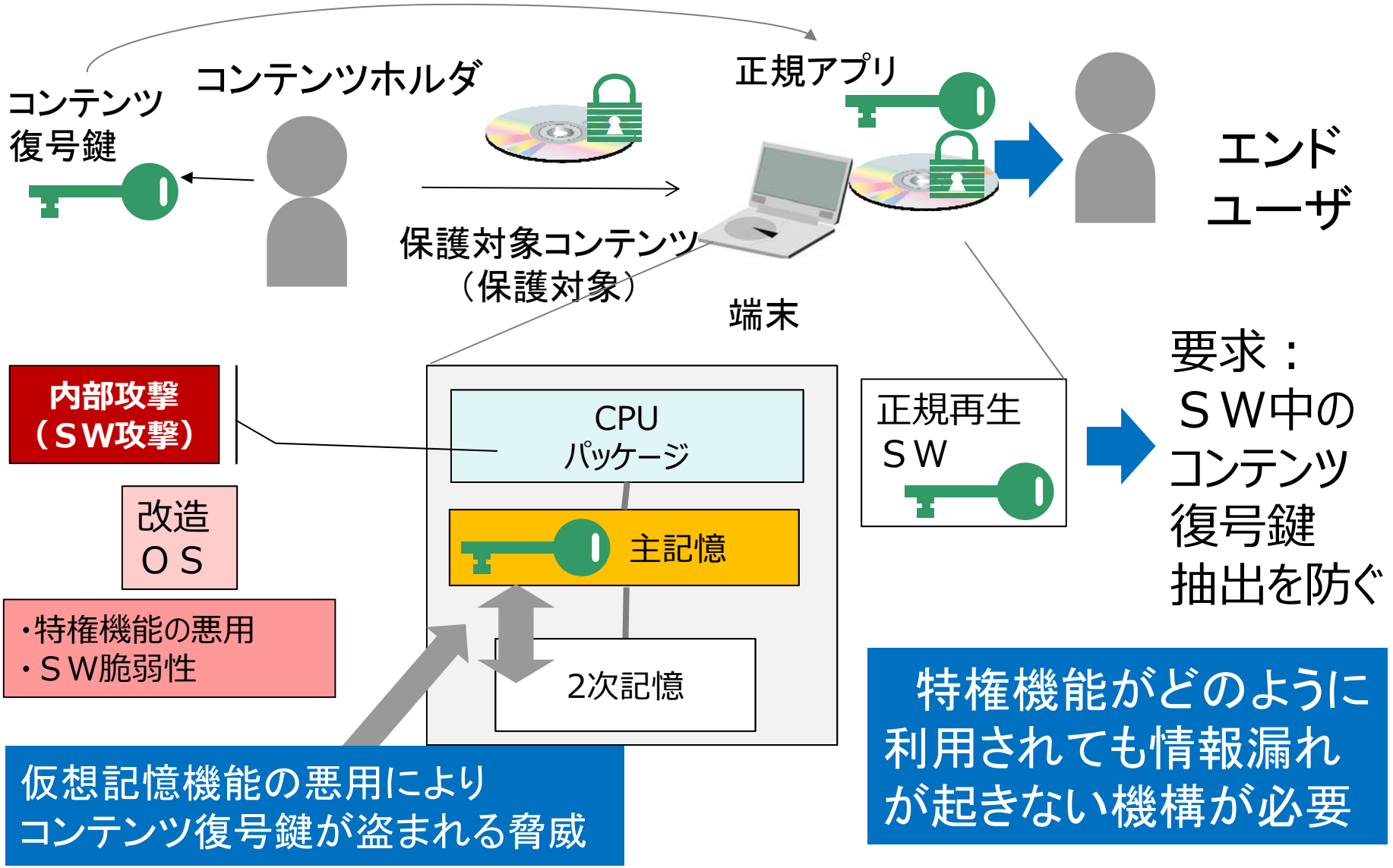
セキュアプロセッサ LMSP

背景課題：コンテンツ保護

デジタルコンテンツの不正コピー防止要求が顕在化

- **DVD 保護方式(CSS)への攻撃(1999)**
  - 再生ソフトのリバースエンジニアリングからコンテンツ復号鍵が暴かれる
- **目指す価値**
  - コンテンツと不正ソフトウェアの不正リバースエンジニアリングを防止
  - オープンソースOS: 攻撃者によるOS特権の利用
  - 同時期のセキュリティプロセッサ提案
    - XOM(2000), Aegis (2003), LMSP (2004),…
    - OSが信頼できないことを前提としたプロセス保護

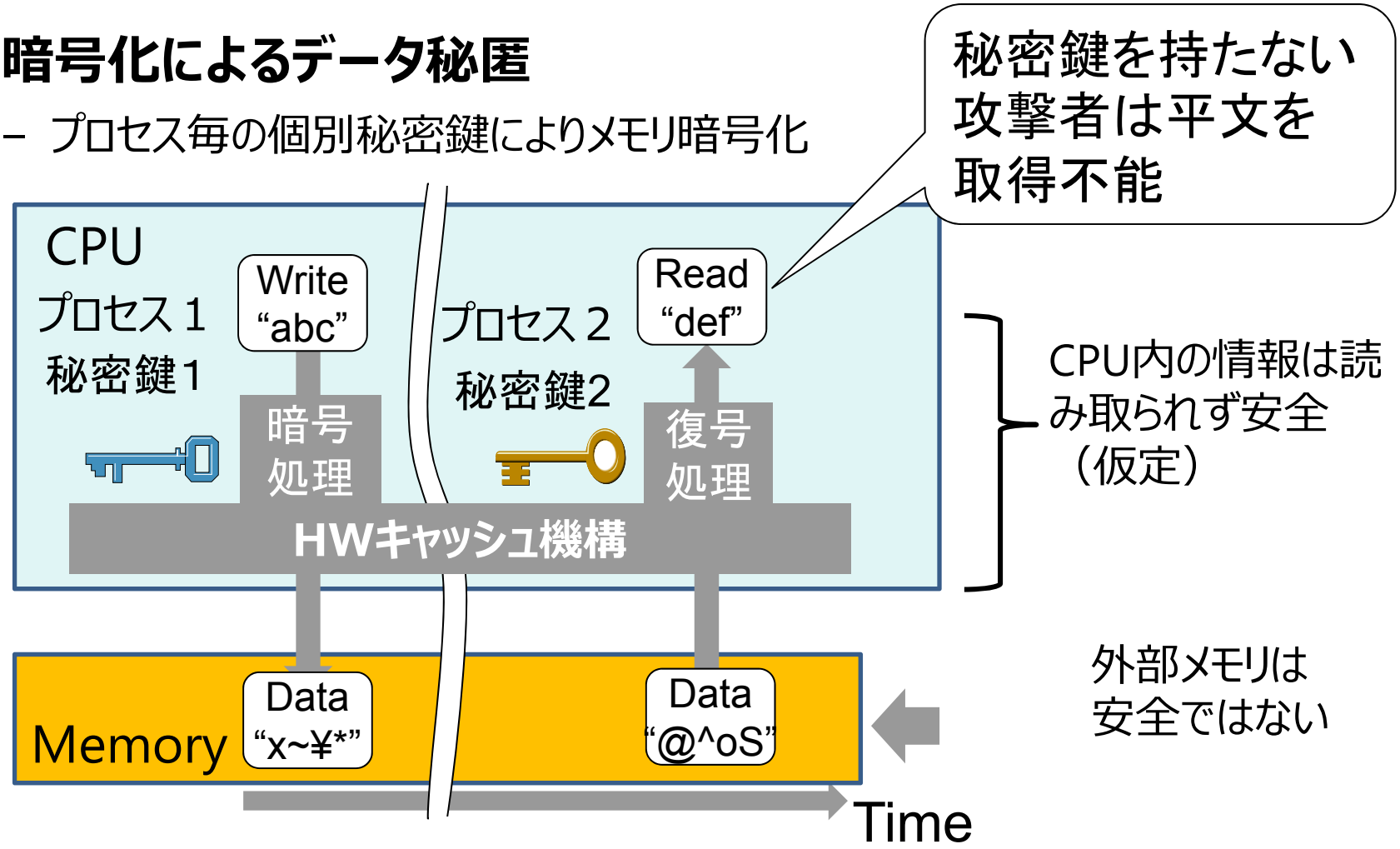
技術課題：コンテンツ保護とソフトウェア保護



メモリ暗号化によるプログラム＆データ秘匿

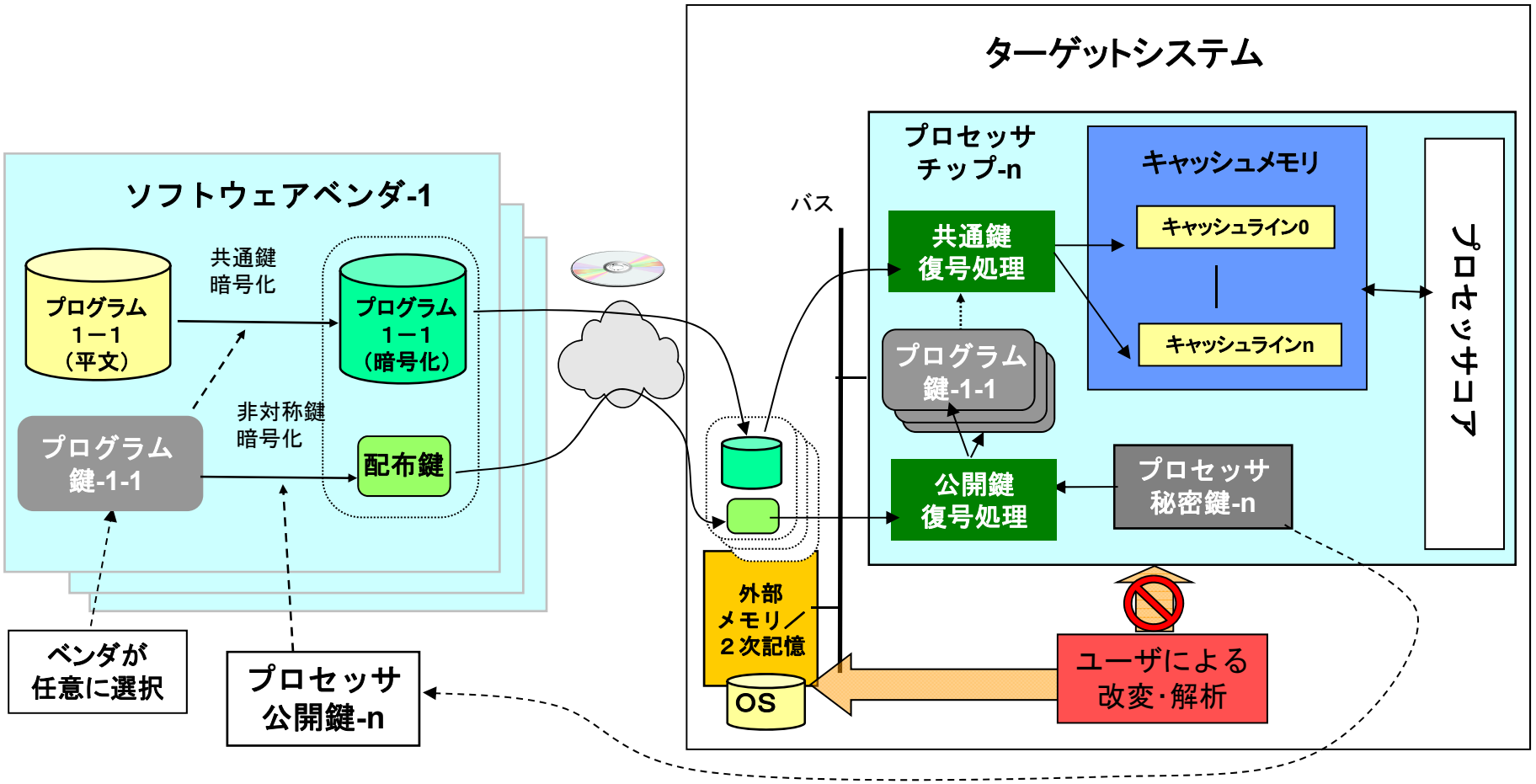
問題：暗号化してもソフトウェア配布と実行は可能か？

- **暗号化によるデータ秘匿**
  - プロセス毎の個別秘密鍵によりメモリ暗号化



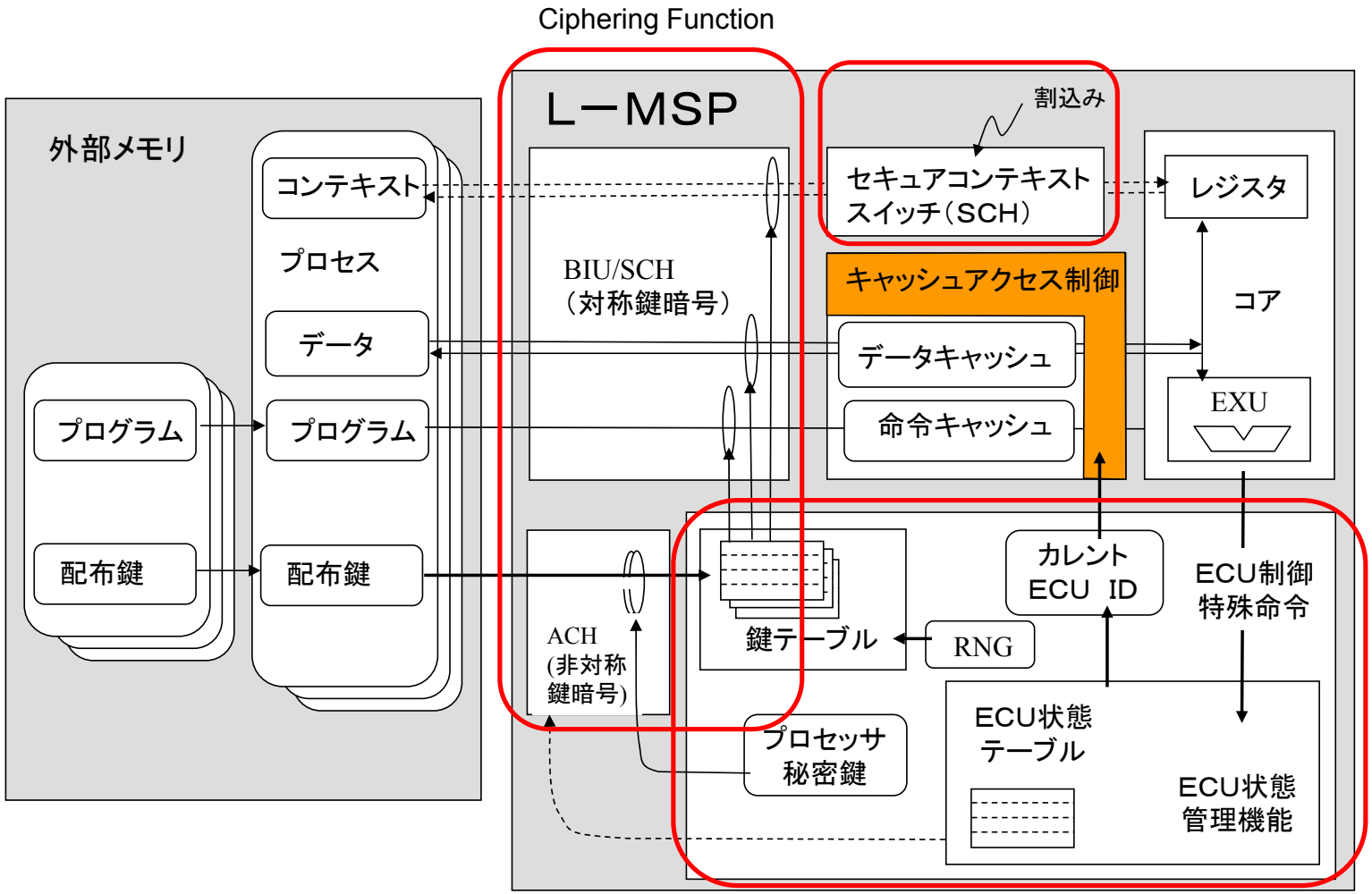
LMSPにおけるソフトウェア配布

ハイブリッド暗号により秘匿化状態でソフトウェアを配布



LMSPのハードウェア構成

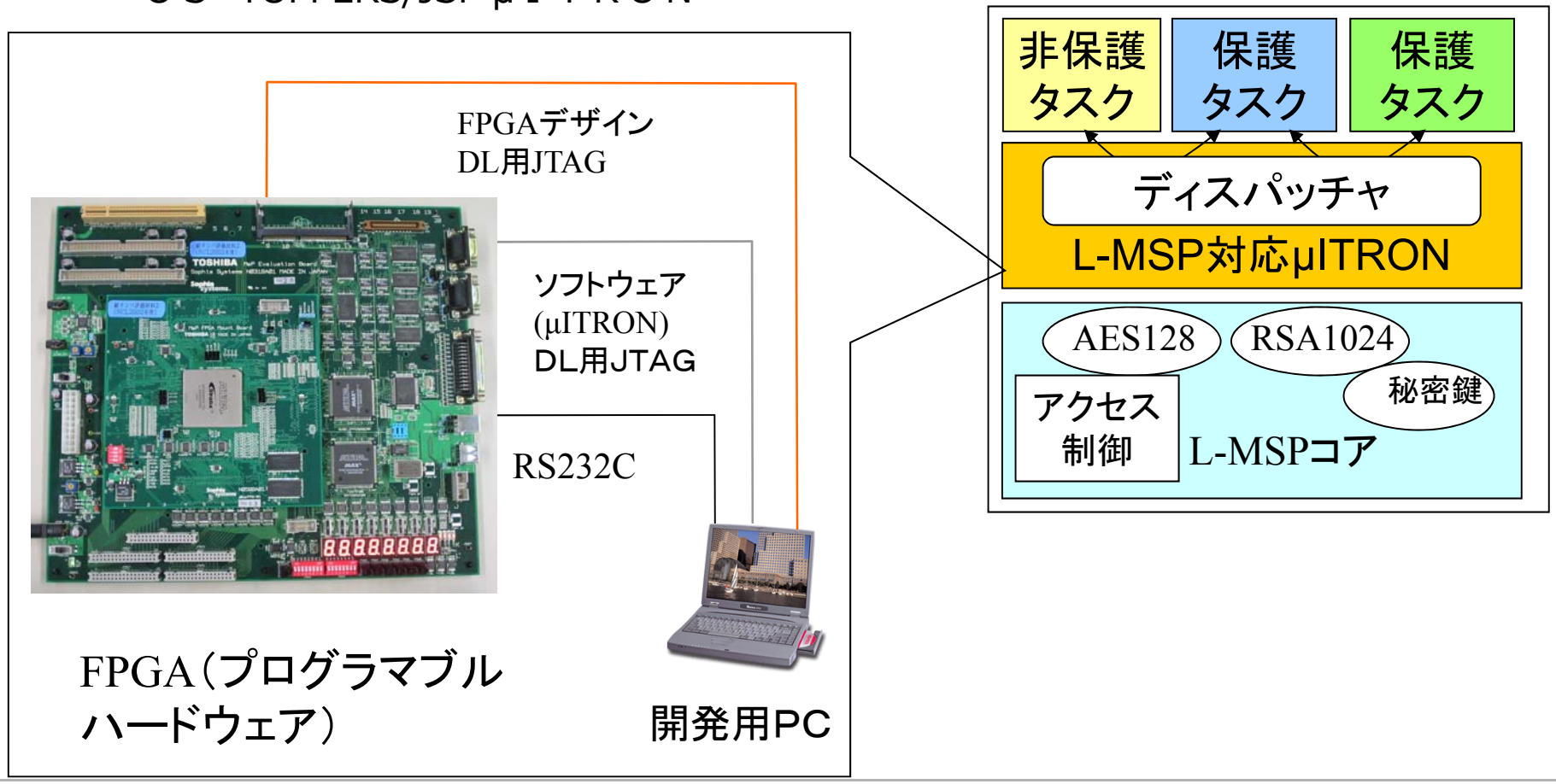
レジスタ情報を含む全てのプロセス情報を暗号化



LMSP機能試作

暗号化状態でのプロセス実行を機能テストベッドにより実証

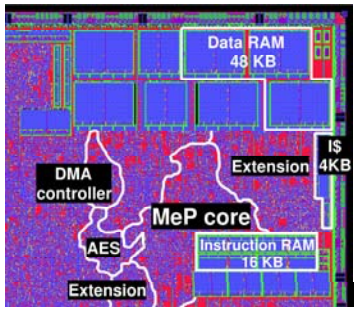
- 東芝独自　RISC MeP ベースLMSP（ＦＰＧＡ実装）
- ＯＳ　TOPPERS/JSP μＩＴＲＯＮ

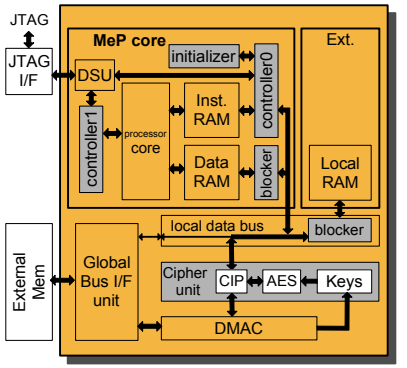


機能テストベッドとその後

LMSPはコンテンツ保護にはオーバスペック

- **シンプルな保護機構をもつ　MeP-c4A 実用化**
  - 独自アーキテクチャCPU MeP の新規開発中止
- **コンテンツ保護は下記技術が適用**
  - ソフトウェア難読化
  - ARM® Trustzone®
- **2018現在：メインメモリ暗号化ＣＰＵ実用化**
  - PC･サーバ　CPUでは標準機能に
    - Intel® SGX (2014)
    - AMD SEV (2017)





未解決課題と環境変化

未解決課題と環境変化

- **未解決課題**
  - データ完全性
    - LMSPでは未解決
    - Aegis(2003)：小規模メモリ向け提案
- **環境変化**
  - 社会インフラ・制御システムセキュリティ
  - システム動作の不正変更防止が最優先
    - 厳密な完全性の要求
  - 物理攻撃の脅威
    - 不揮発メモリに対する改ざん

ニーズの変化

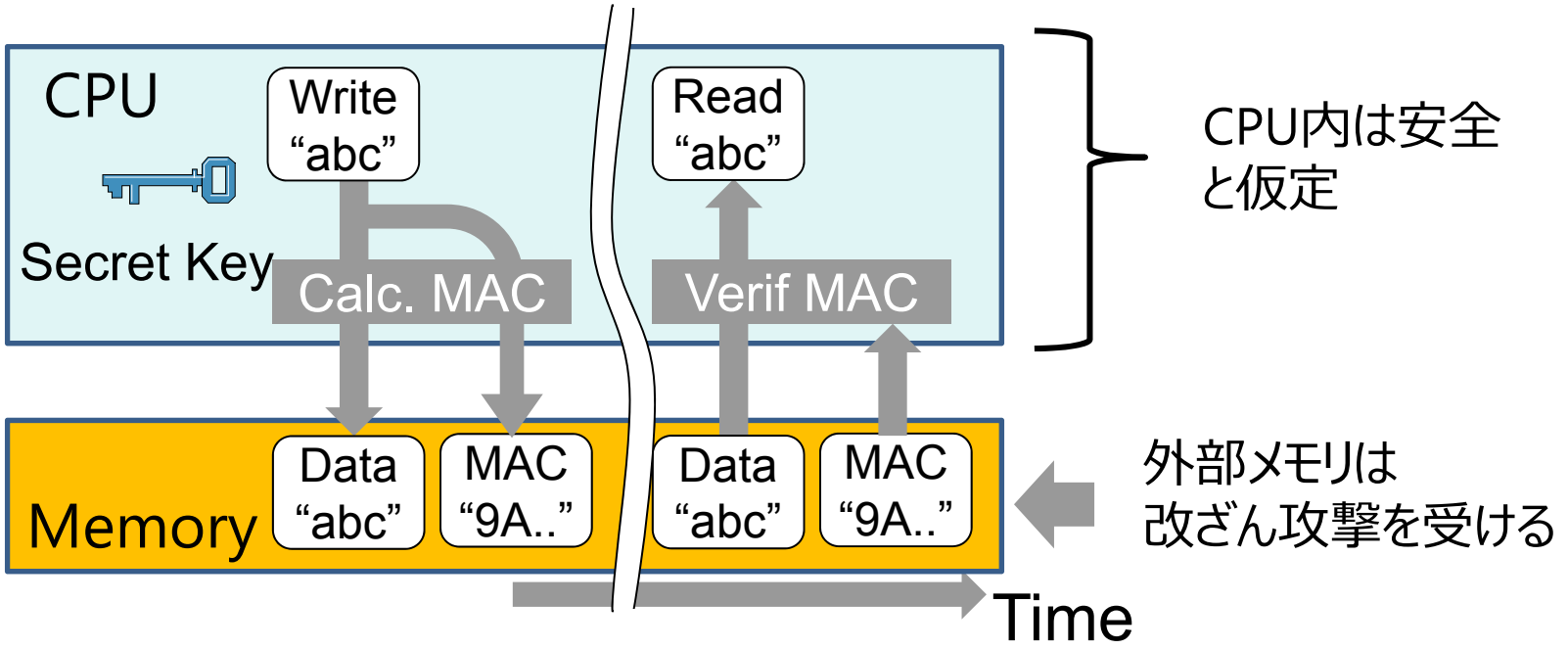
セキュリティ技術のシーズ進化

＋完全性

完全性検証

秘密鍵を持たない攻撃者は正しいMACを作れない

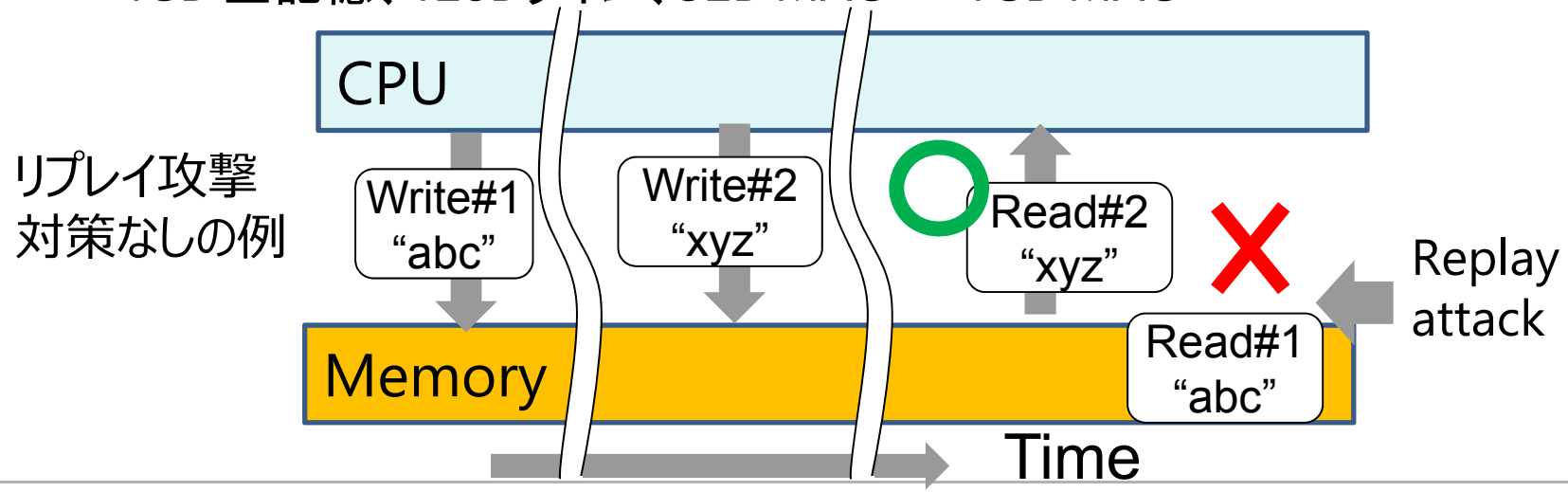
- **定義**
  - 読込データが直前の書込みデータと一致
- **MAC (Message Authentication Code)**
  - データと秘密鍵に基づいて生成、検証



脅威: リプレイアタック

- リプレイによるMAC 検証の迂回
  - 過去のデータ-MACペアを最新データに上書き
- リプレイ攻撃対策
  - **MAC を改ざん不能なセキュアメモリに保持**
  - **MACに関連付けたカウンタをセキュアメモリに保持**
- ランダムアクセスメモリは工夫が必要
  - ブロック毎のMAC or カウンタを個別に保持
    - 4GB 主記憶、128Bライン、32B MAC ⇒ 1GB MAC

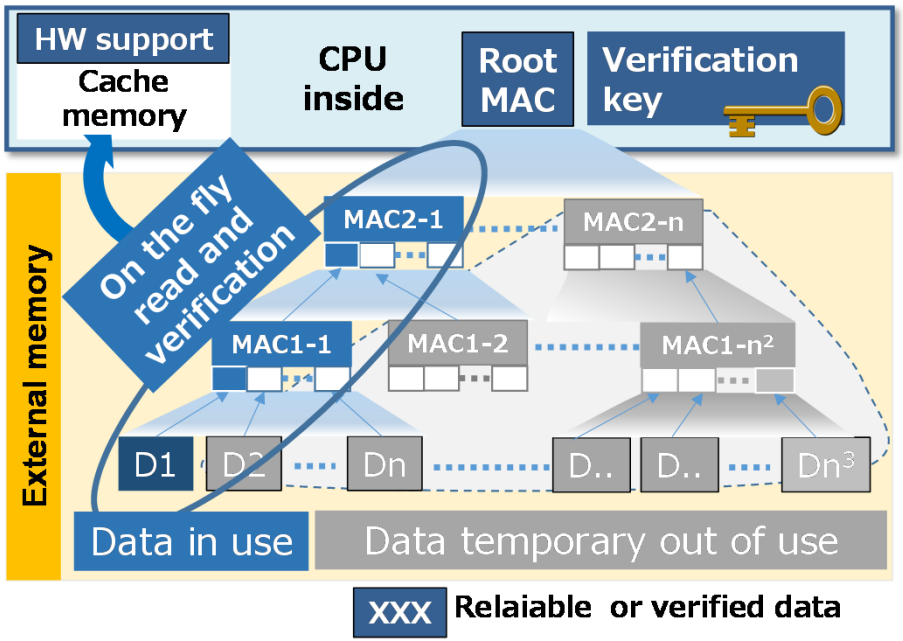
CPU内蔵セキュアメモリ容量は、OS全体のブロック毎MAC格納には不足



MACツリー検証

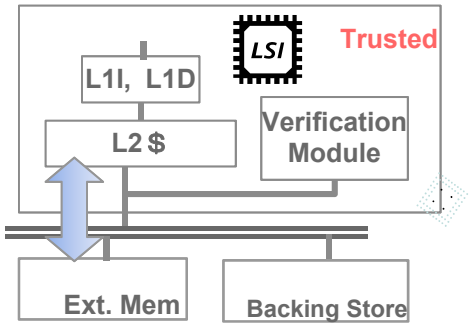
MACツリーにより多数のMACを集約してCPU内に格納

- **リプレイ攻撃対策**
  - MAC ツリー技術 (Merkle Tree, Bonsai Merkle Tree,...)
  - 多数のブロックから成るメモリの状態を1個のRoot MACに集約
- **データリード**
  - CPU内MACキャッシュ内に検証サブツリーを読み込んで検証
  - 検証サブツリー
    - 読込対象データから Root MAC までの部分木
- **データ処理前に必ず検証**

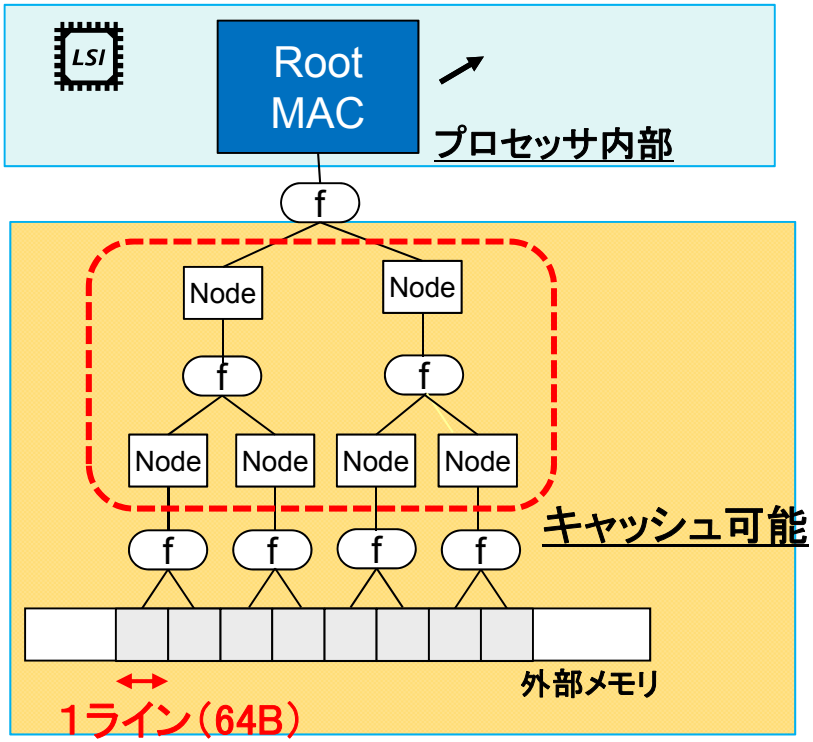


Aegis(2003) のHW MACツリー検証機構

- ツリー検証と暗号処理をHW実装
  - キャッシュ機構に統合



- 課題
  - 専用HWが必要
    - ツリー検証は状態管理が複雑
  - 階層の深いツリーと検証領域の制限
    - 4:1の場合、64GB空間は14階層
    - 実証ではOSクリティカル領域に限定
  - ツリー読込時のキャッシュ競合
    - 新規ノードの読込でキャッシュ済みの上位ノードが破棄されてしまう
      - 補償には複雑な機構が必要



アプローチの見直し

汎用仮想化機構によるMACツリー検証を考える

- **ターゲット**
  - 社会インフラ・制御システムセキュリティ
    - 改ざんによる異常動作防止とフォレンジック強化
  - 不揮発主記憶導入（メモリモジュール）の予想
- **技術課題**
  - リプレイ攻撃を含む改ざんの厳密な対策
    - 大容量メモリへの対応
- **実現手段**
  - 汎用HWの利用
    - 仮想化機構とシンプルな暗号HW （DMAC）を想定

メモリ完全性検証

背景とゴール

ゴール：制御機器のOSイメージ全体をカバー可能な改ざん対策

- **物理攻撃対策の必要性**
  - 既存DRAMにおけるセキュリティ脅威（コールドブートアタック）
    - 不揮発性メインメモリNVDIMM (MRAM, FeRAM,…)導入より拡大
  - 現在の課題は遠隔攻撃だが…
    - 遠隔攻撃対策の改良により物理攻撃が相対的に顕在化
  - 不揮発化により事故発生直後の主記憶状態が保存可能に
    - **事故発生後の主記憶改ざんによるフォレンジック妨害の脅威**
  - 稼働中の一時停止時の改ざん
    - 破壊による利用不能攻撃：　影響は単一機器に限定
    - 機器の意図的な異常動作：　**影響が他の機器に波及**
- **本提案のゴール**
  - OSイメージ全体に対するメインメモリ完全性＆機密性保護手段の提供

物理攻撃関連の組込/制御システムへの攻撃事例

- **トルコの石油パイプライン破壊**
  - 2008発生。初の組織的インフラ攻撃と言われる
  - 監視カメラの脆弱性を利用して制御ネットワークに侵入、制御室に対して送られるセンサデータの値をごまかすことでオペレータの目くらましとした
  - さらにパイプラインの圧力を高めて爆発を起こした
  - 米セキュリティ教育機関 SANS security reportのコメント(*)
    - Control equipment in the field is **vulnerable to physical attacks but when combined with cyber-attacks** pose a significant threat. This is not a theoretical discussion

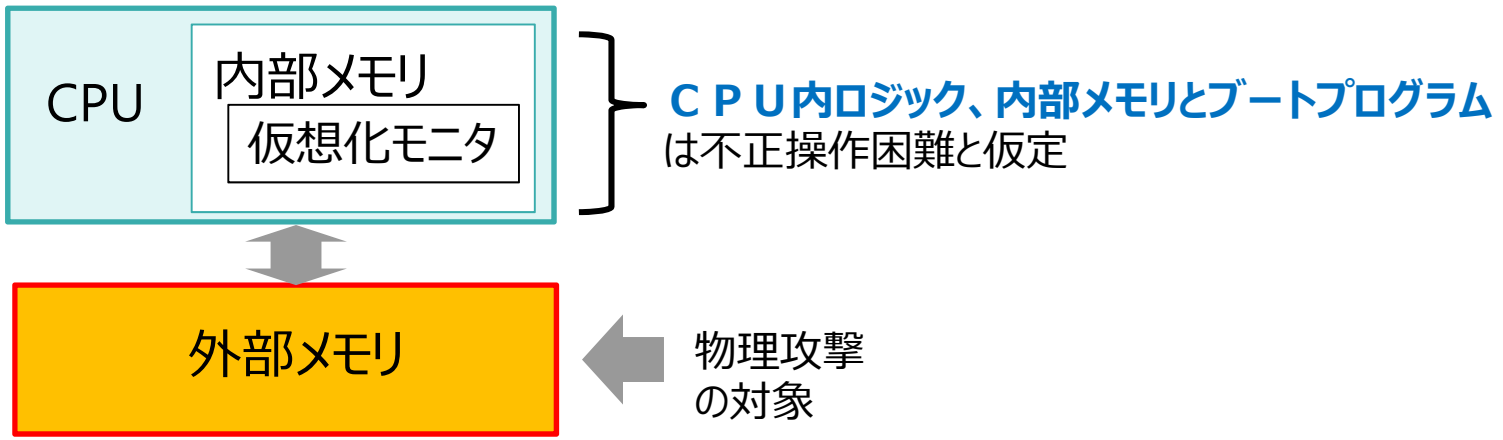
物理攻撃と遠隔攻撃の組み合わせ攻撃の脅威を指摘

(*) https://ics.sans.org/media/Media-report-of-the-BTC-pipeline-Cyber-Attack.pdf Page 6

前提と脅威

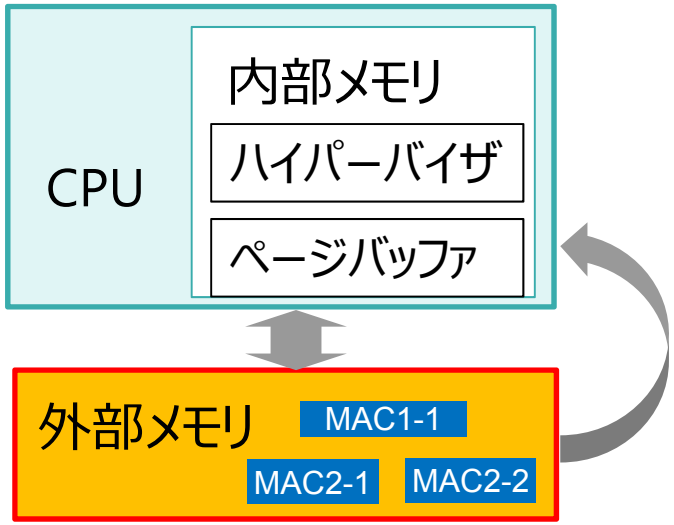
CPU内部メモリに格納可能なシンプルな仮想化モニタ

- **信頼境界 (Trust Boundary)**
  - CPU内部とCPU内蔵のブート用ソフトウェア、仮想化モニタを信頼
- **脅威**
  - メモリ内容の直接観測と操作
  - 複合攻撃(ネットワークサービスを経由した攻撃との組み合わせ)
    - 準備:アクセス制御の制御フラグを物理操作
    - リモートから不正な操作要求を発行→アクセス制御迂回



提案方式: TREBIVE

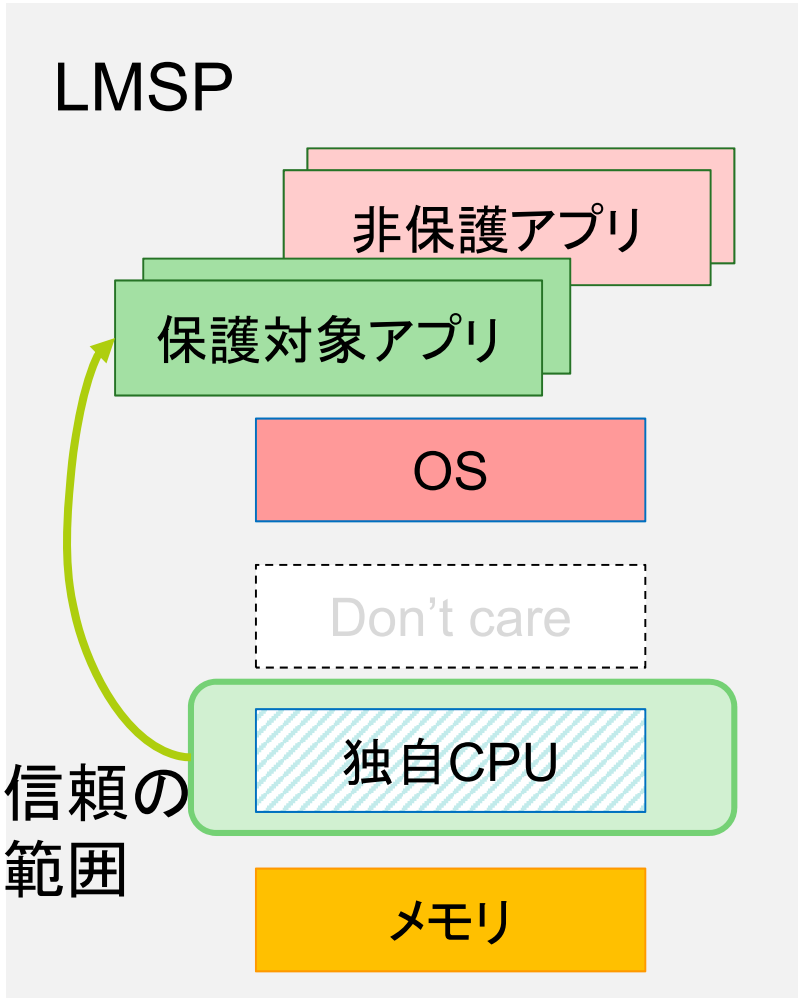
- **TREe Base Integrity Verification Environment**
- **ハイパーバイザによるMACツリーメモリ改ざん検証**
  - CPUの内部ワークメモリ上にハイパーバイザとバッファを格納
    - 1MB以上の内部ワークメモリを想定（東芝 TZ2000等製品あり）
  - 汎用CPUの仮想化HW
- **検証ツリーをページ単位で構成**
  - 検証ツリーのレベル数を縮小

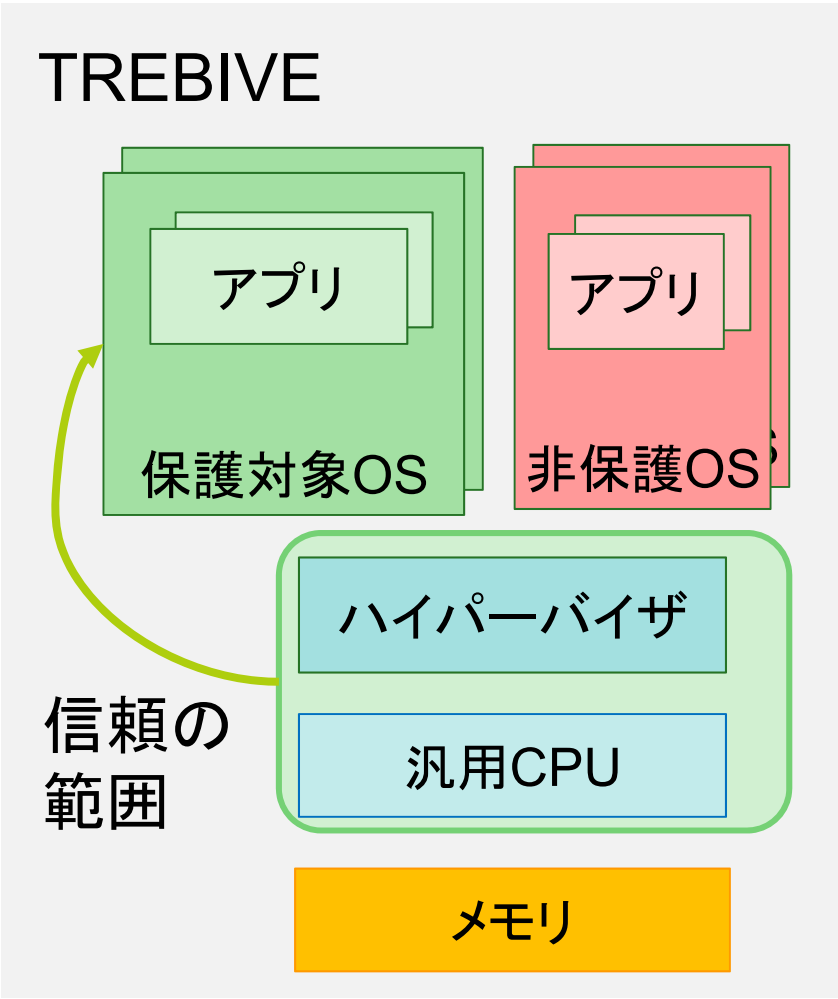


- 内部メモリへのページ読込時
  - ツリー検証を実行
- 1ページ毎に256bit(32B)MAC
  - 128:1 の圧縮
- 64GBをカバーするツリー階層
  - 4階層で実現
  - キャッシュ処理では14階層

信頼の範囲の違い

社会インフラ応用を考慮して基盤ソフトに信頼をおく

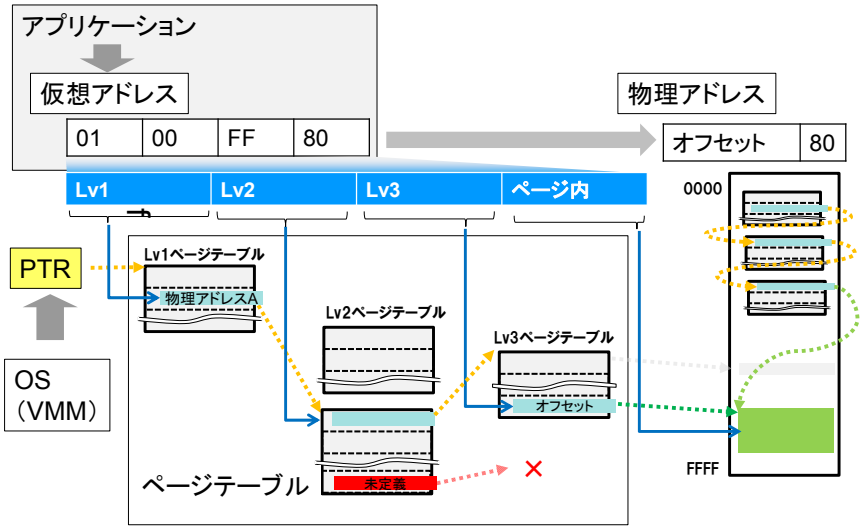




仮想アドレス機構の意義

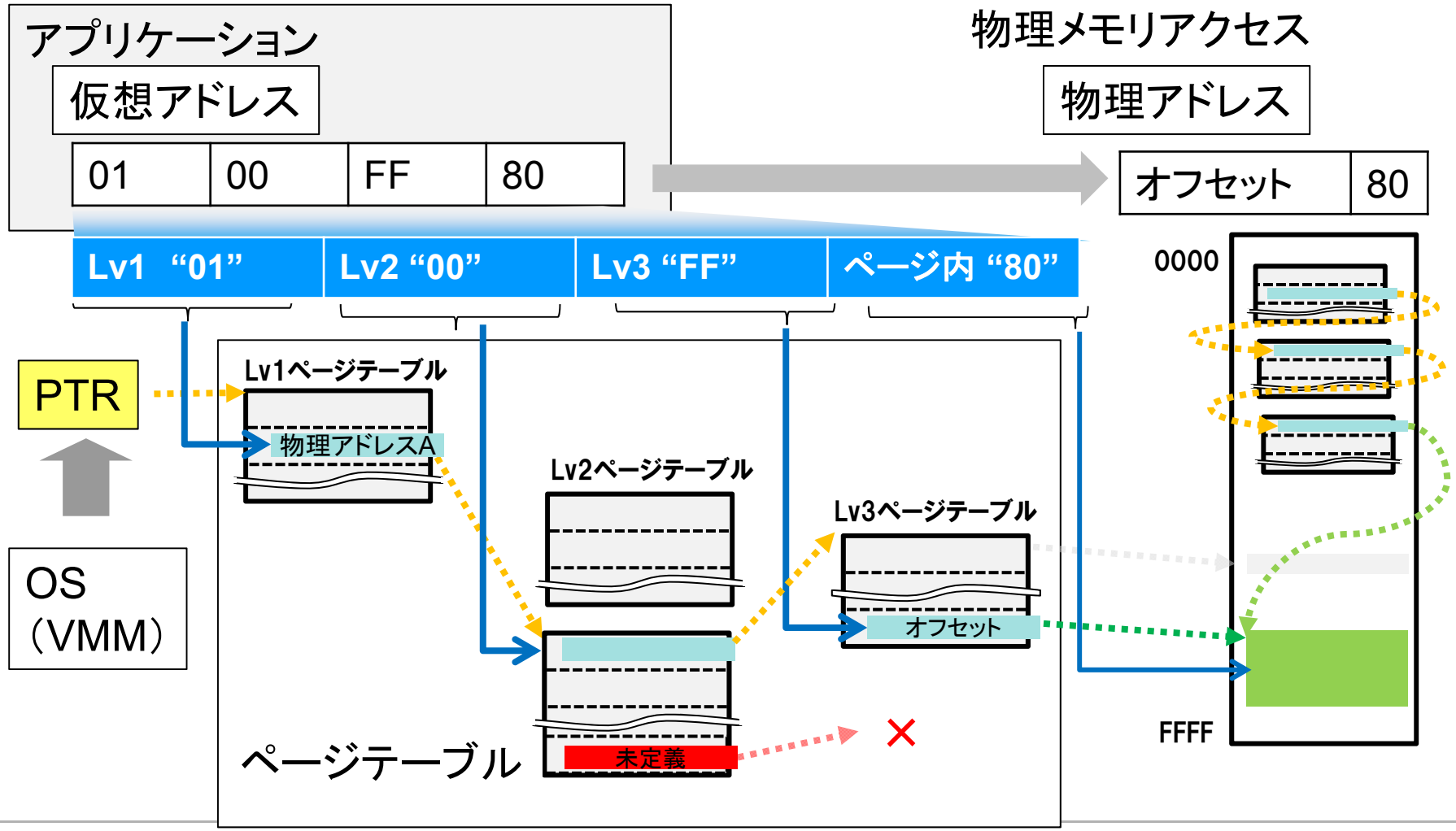
- 2つの意義
- 小容量の物理メモリを大容量の記憶として活用
  - 仮想アドレスをページ（4KB）毎に物理アドレスにマッピング
    - 物理メモリ未割当の場合OSが介入

- アクセス制御の管理
  - プロセス毎ページテーブル
    - ページテーブルの切替により アクセス範囲を切替
  - 未定義ページの参照
    - ⇒ OSが介入
      - 例："Segmentation Fault"



仮想アドレスの実現機構

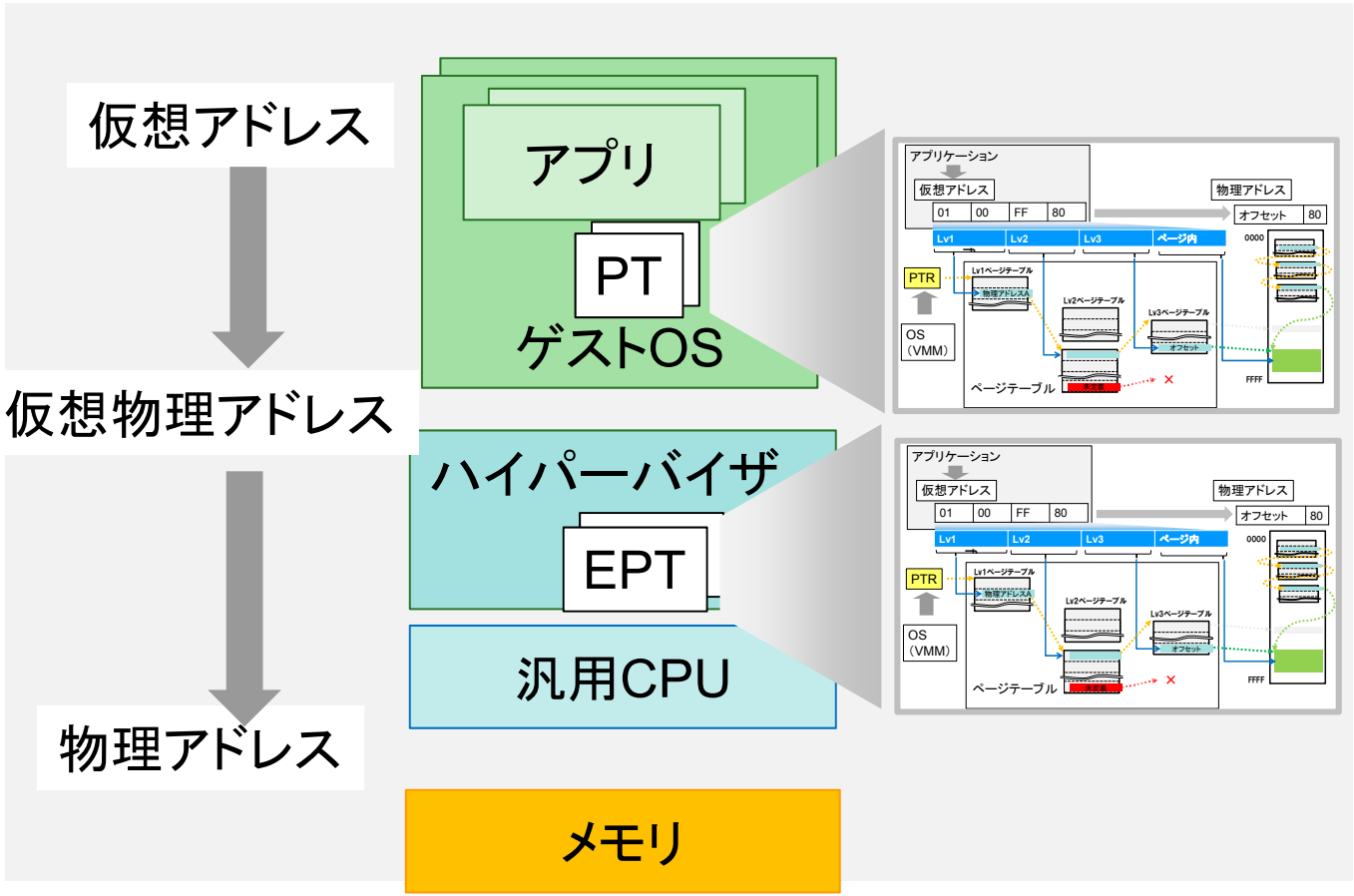
- 自由度の高い変換定義　－　ページテーブル
  - 階層化によりテーブルサイズを削減



ハイパーバイザにおけるアドレス変換

ハイエンドCPUでは2段階アドレス変換をHWサポート

- **2段階のアドレス変換 （Nested Page Table)**

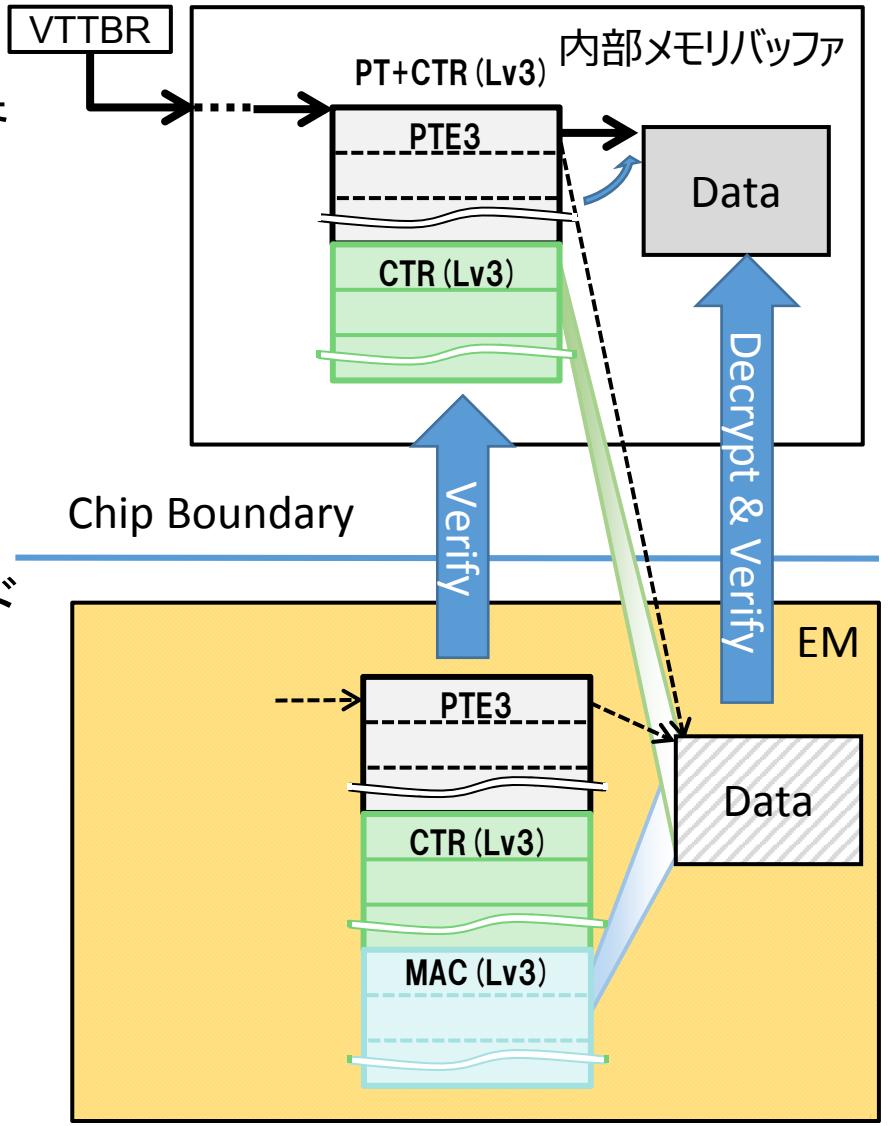


ページテーブル
(PT)
→ プロセス隔離

拡張
ページテーブル
(EPT)
→ ゲストOS隔離

仮想化機構による未検証ページアクセスの検出

- **未検証メモリアクセス検出**
  - 右図のページテーブルは検証済
  - 未検証データのページテーブルエントリ(PTE)は無効状態
- **ハイパーバイザ操作**
  - ページ読込と検証
    - MAC検証
    - データの内部メモリへのロード
  - 検証成功
    - PTEの参照先アドレス書換
    - PTEエントリの有効化
  - 検証失敗
    - PTEは無効のまま変更せず
    - 不正データ検出の報告



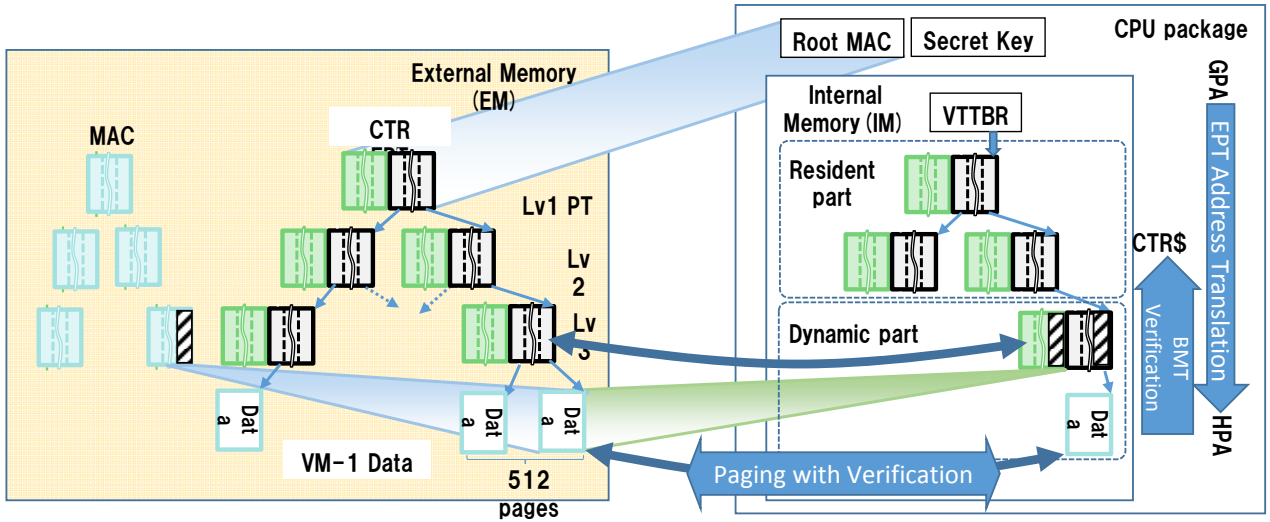
TREBIVEの特徴(1)

- **ゲストOS透過性**
  - 検証済みメモリを外部メモリから内蔵セキュアメモリに移動(ページング)
  - 2ステージアドレス変換機構の利用による移動の隠ぺい
  - ハイパーバイザによるExtended page table (EPT) 操作
    - ページアドレスリダイレクト
- **検証処理はCPU内部で完結**
  - 外部メモリ改ざんに対してHW処理と同等の安全性
- **暗号演算処理はHWオフロード可能**
  - 暗号エンジン連携DMACの利用
- **データ秘匿も可能**
  - BMT (2007) の手法によるワンタイムパッド暗号化
  - ページ毎に信頼できる書換カウンタを保持

TREBIVEの特徴(2)

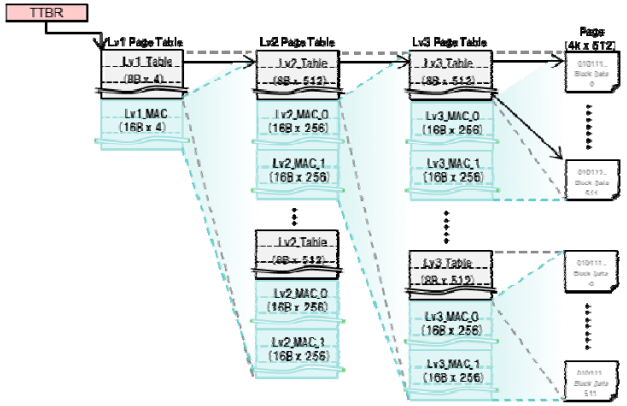
仮想化と検証ツリー連携による効率化とフォレンジック支援

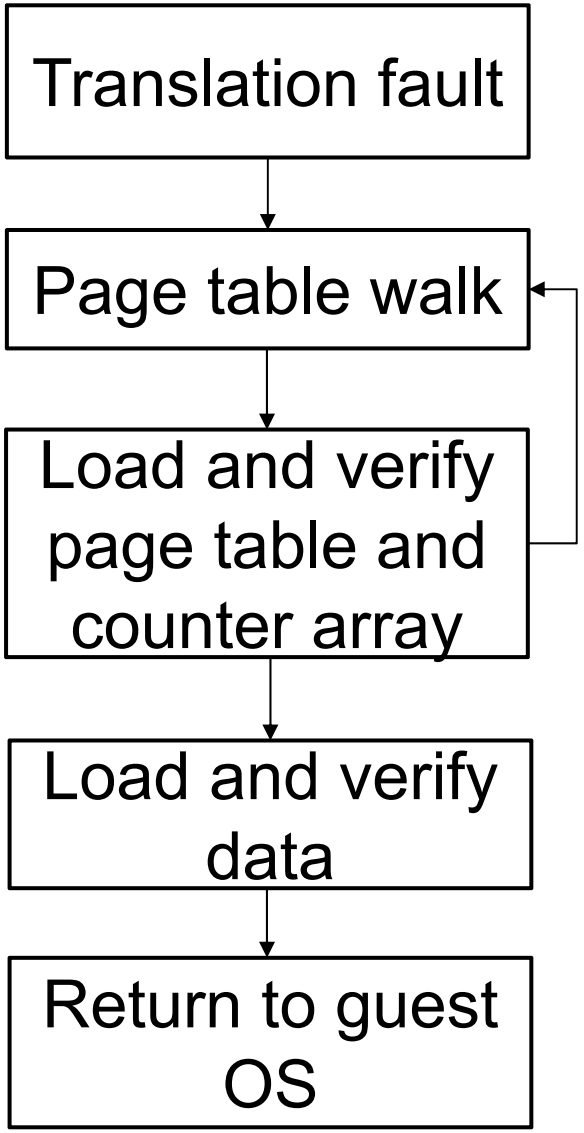
- **アドレス変換解決とツリー検証の連携**
  - EPTとMACツリーは同一トポロジとして一体化
  - 未検証データおよび検証ツリーの参照をHWで検出
    - ページフォールトおよびアドレス変換フォールト
- **ゲストOSのメモリ状態が最上位のMACに集約**
  - メモリ状態の事後改ざん検出能力によりフォレンジック性を強化



ページテーブルの保護

- テーブル構造
  - ページテーブルと検証ツリー
    - 512-ary tree
  - ページテーブルと検証カウンタを連続配置
- ツリー検証とページテーブル読込連携の利点
  - 内部バッファ管理の簡略化
  - ハイパーバイザ起動回数の削減





提案方式 TREBIVE のまとめ

- ゴール
  - OS全体をカバー可能な方式
- 課題
  - リプレイ攻撃対策とHWツリー検証の困難性
- 提案方式
  - ハードウェア仮想化を利用したページングベースの検証
  - ページテーブル操作とツリー検証の連携
    - 未検証データ検出とページテーブル保護の効率化
- 利点
  - 既存CPU，既存OSとの互換性、フォレンジック応用
- 要検証
  - ハイパーバイザのフットプリントサイズ
  - 性能インパクト – ページングオーバヘッド

機能テストベッドと評価

Item	description
Hardware	Arm Versatile™ Express with CoreTile Express A15x2 A7x3
Memory	DRAM 2GB (DDR2 400MHz 32bit bus)
CPU	Arm Cortex® A15 x 1 with 1MB L2 U$
Guest OS Image size	Linaro Linux® stable 3.14 for vexpress 2015.03 1512KB
VMM	Footprint 43.2K with XTS-AES, 4.2K SLOC
Replacement	pLRU with simple priority control

ハイパーバイザのフットプリントは40KB程度

- **Measurement item (Linux boot example)**

	imem-in		imem-out		Imem WB		pLRU	TLB	Measured	estimat
test_name	table	page	table	page	table	page	flash	flash	time	Pseudo cipher
DT 4MB	7	3182.0	0.0	2172.0	0.0	1984.3	5.0			
EMU 4MB	7	3203.3	0.0	2193.3	0.0	2002.7	5.			14
DT 2MB	9	19607.3	2.0	19109.3	2.0	7347.7	92.			
EMU 2MB	9	18928.3	2.0	18430.3	2.0	7100.7	88.			74

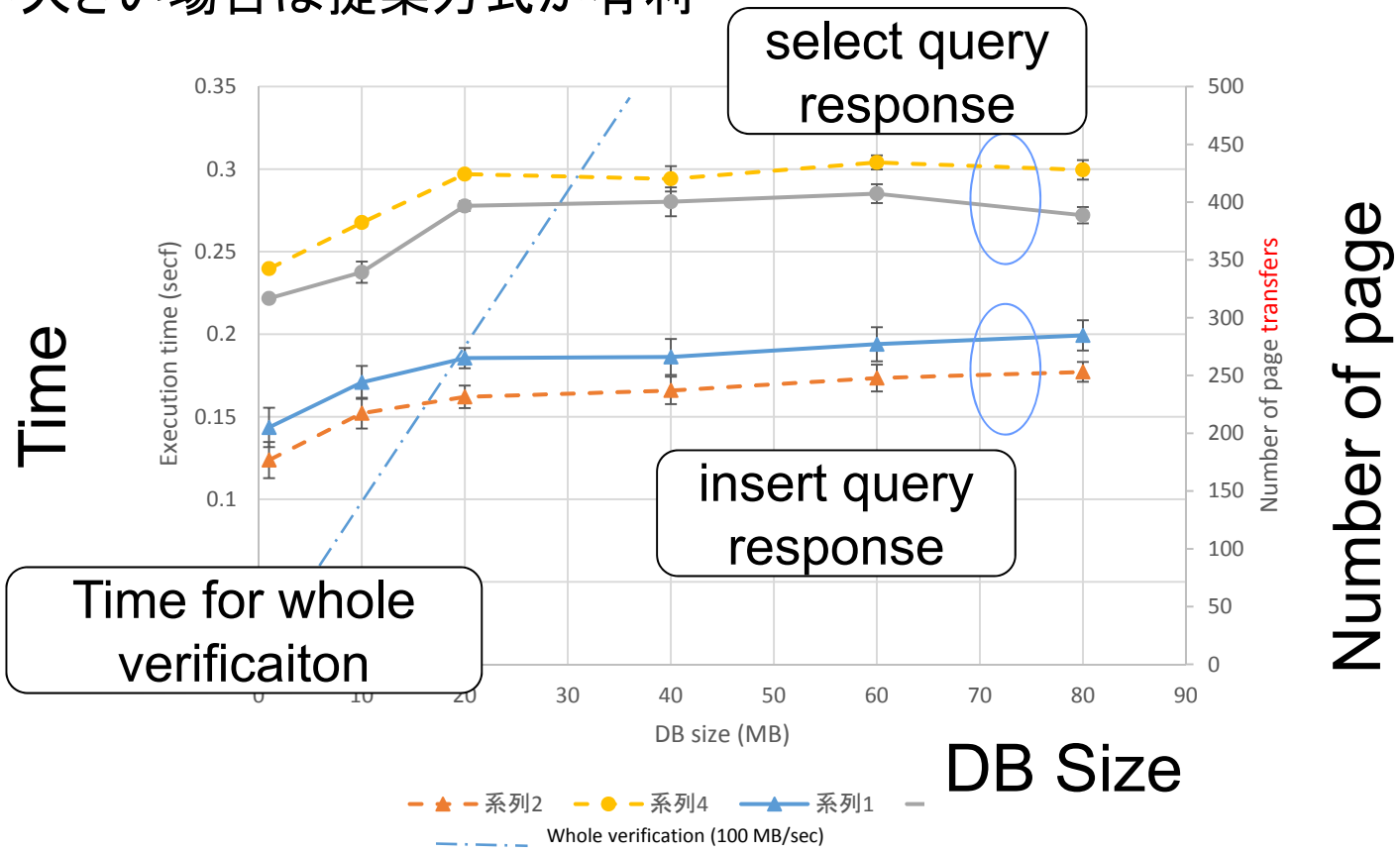
ページング統計

仮想化関連CPU処理時間

暗号HWありの値を推定⇒次ページ

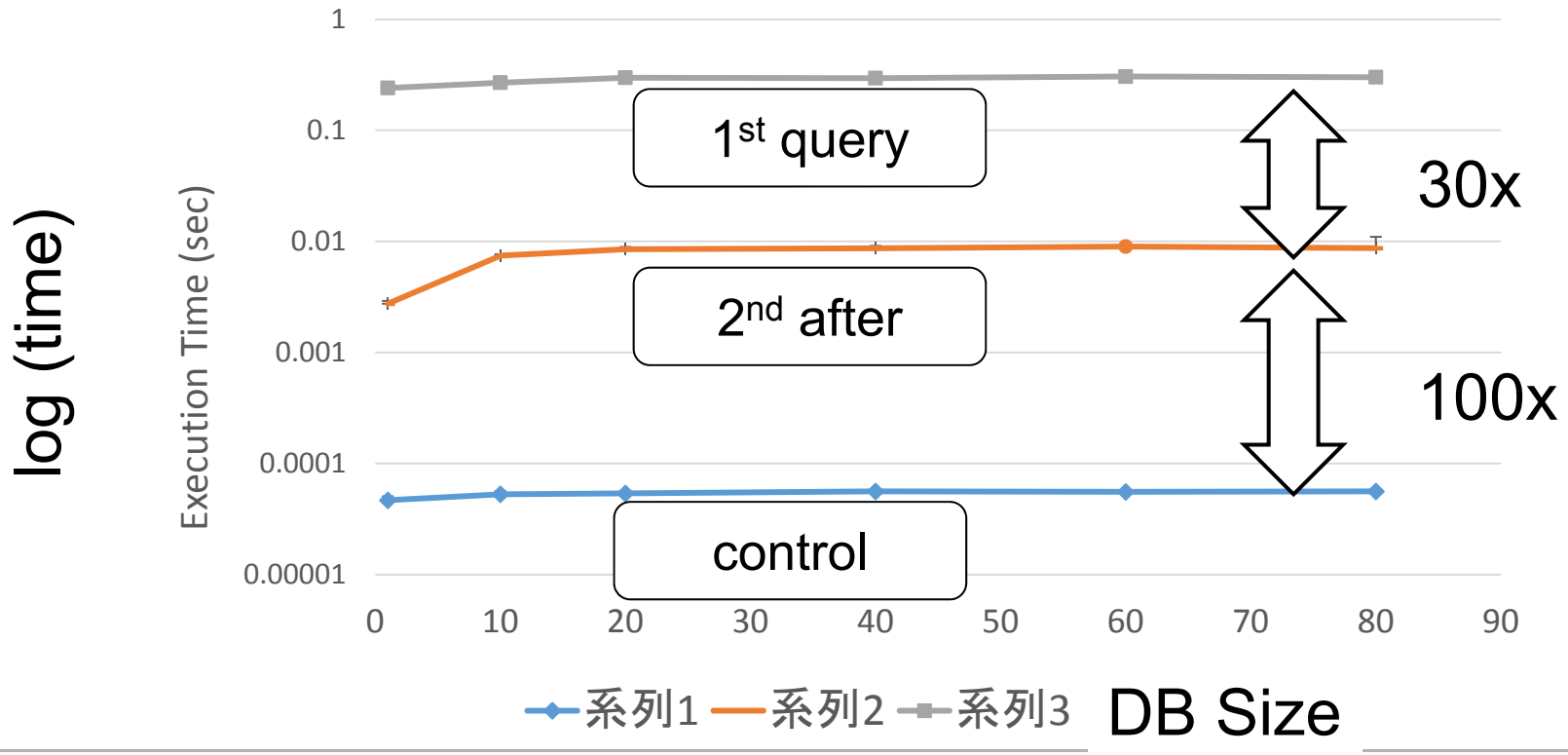
組込みデータベースにおける評価（1）

- インメモリデータベースのクエリ応答時間（4MB内部バッファ）
  - DBイメージ未読込状態からの応答時間
  - アプリによるDBファイルの事前検証時間とのベンチマークでは、DBサイズが大きい場合は提案方式が有利



組込みデータベースにおける評価（1）

- **1回目と2回目の応答時間の比較**
  - 1st to 2nd after: 2回目は30倍速い
  - 2nd to control: 検証なしと比較した場合、2回目は100倍遅い
- **ページキャッシュは有効だがオーバヘッドは大きい**



議論

- **課題：性能オーバヘッドの低減**
  - 内蔵メモリと外部メモリの速度差
  - ARMv8における改善
  - 非保護OSの仮想マシン上共存
- **機密性との館れ：　完全性は厳密な秘匿の基盤**
  - メモリ機密性の担保には改ざん不能なセキュアカウンタが必要
    - 提案方式は不正なカウンタ操作を排除可能
    - 外部メモリ、バスには平文は一切出力されない
- **安全機構への適用**
  - 緊急安全操作むけの決定木処理について完全性の保護
    - プログラムとデータベース
    - わずかな決定木処理の不正でも大きな災害につながる可能性
      - 厳密な完全性が求められる

IoTにおける役割

エッジサーバのフォレンジック強化と安全設計の容易化

- **主記憶のフォレンジック強化による事故原因解析の高信頼化**
- **クラウドに依存しないエッジサーバの安全設計**
  - クラウドに対するディスコネクテッドオペレーション
    - 例：クラウド非接続時の一部センサ/アクチュエータ機器の故障
      - エッジサーバによる判断がない場合、機器単体でのフェールセーフ動作　→　IoTによるリソース最適配置の効果が得られず
  - エッジサーバ故障時
    - エッジサーバ故障（単純故障）
      - 制御機器単体のフェールセーフでカバー可能
    - メモリ改ざん攻撃の存在を仮定したエッジサーバ異常動作
      - 機器単体のフェールセーフを越えた安全率が必要となり効率低下
- **メモリ物理攻撃の排除⇒IoTシステムの安全設計を容易化**

まとめ

- **メモリセキュリティ技術の取り組み**
  - 機密性のみから、完全性と機密性の両方を担保
  - 独自プロセッサから汎用仮想化機構の利用へ
  - コンテンツ保護から社会インフラ・IoT
- **TREBIVE 機能試作による性能評価**
- **応用における意義**

参考文献

- **XOM**

D. Lie, C. Thekkath, M. Mitchell, P. Lincoln, D. Boneh, J. C. Mitchell, M.Horowitz: Architectural Support for Copy and Tamper Resistant Software. ASPLOS 2000: 168-177

- **LMSP**

M. Hashimoto, H. Haruki, T. Kawabata: Secure Processor Consistent with Both Foreign Software Protection and User Privacy Protection. Security Protocols Workshop 2004, LNCS-3957: 276-286

- **Aegis**

G. Edward Suh, Dwaine E. Clarke, Blaise Gassend, M. van Dijk, S. Devadas: AEGIS: architecture for tamper-evident and tamper-resistant processing. ICS 2003: 160-171

- **MeP-c4A**

T. Kawabata, T.Tamai, M. Hashimoto, T. Miyamori: Security Enhanced Embedded Processor using Local Memory Protection Mechanism, Cool Chips IX, 2006, pp. 143-157.

- **BMT (2011)**

S.Chhabra, B. Rogers, Y. Solihin and M. Prvulovic: SecureME: a hardware-software approach to full system security. ICS 2011: 108-119

- **Intel SGX**

Intel Corporation: Intel Software Gurad Extension, ISCA 2015, https://software.intel.com/sites/default/files/332680-002.pdf

- **AMD SEV**

D. Kaplan, J. Powell and T. Woller: AMD Memory Encryption, 2016, https://developer.amd.com/wordpress/media/2013/12/AMD_Memory_Encryption_Whitepaper_v7-Public.pdf

- **TREBIVE**

M. Hashimoto, N. Yamada, J. Kanai: TREBIVE: A TREe Based Integrity Verification Environment for Non-volatile Memory System. IEEE PRDC 2015: 279-289

商標について

※ SeeQVaultは、NSM initiatives LLCの商標です。
※ Arm、Cortex、TrustZone、Versatileは、米国および／あるいはその他の国における Arm Limited (またはその子会社)の登録商標あるいは商標です。
※ Intelは、アメリカ合衆国および/またはその他の国におけるIntel Corporationまたは その子会社の商標です。
※ AMDはAdvanced Micro Devices, Inc.の商標です。
※ Linux® は、Linus Torvalds 氏の米国およびその他の国における登録商標です。
※ TM-SIL™は、東芝デバイス＆ストレージ株式会社の商標です。
※ その他の本資料に記載されている社名・商品名・サービス名などは、それぞれ各社 が商標として使用している場合があります。

TOSHIBA

Leading Innovation

ご清聴ありがとうございました