ゼロトラストと標準化部会の活動の関係について

2023年8月23日

JNSA　標準化部会　副部会長　松本 泰

ゼロトラストと標準化部会の活動の関係について

- JNSA標準化部会では、現在４つのワーキンググループが活動しています。
- ４つのワーキンググループは、それぞれ比較的独立性の高い活動を行なってきまいたが、近年、ゼロトラストアーキテクチャに関連する活動も目立つようになってきました。
- これは、４つのワーキンググループの活動が、そもそもゼロトラストアーキテクチャにとって必要だということが、再認識されつつあるというのが正解かもしれません。
- ここでは、ゼロトラストとの関連性という観点からJNSAの標準化部会の４つのワーキンググループの活動の概観を説明します。

JNSA標準化部会の４つのWGの成り立ち

- 各WGの活動とゼロトラストのつたつの側面
  - ゼロトラスト以前からゼロトラストを核心となる部分の活動を長年に渡り行ってきた！！
  - 2023年現在のWG活動にも影響を与えつつあるゼロトラスト
  - → しかしゼロトラスト全体像を見ている訳ではない。
  - → 各WGにおいて、ゼロトラストの捉え方が違う？
  - → ４つのWGを合わせるとそれなりに全体像や、今後の課題も浮かび上がるかも？？
- 各WGの成り立ち → 各WGの成り立ちは、さまざま
  - 日本ISMSユーザグループ
    - 2004年より任意団体として活動開始、2018年からJNSA標準化部会にて活動
  - デジタルアイデンティティワーキンググループ
    - 2005年よりJNSAにて活動開始
  - 電子署名ワーキンググループ
    - ECOM、JIPDECにて2000年頃より活動開始、2013年からJNSA標準化部会にて活動
  - PKI相互運用技術ワーキンググループ
    - 2001年よりJNSAにて活動開始

本日の【講演3】【講演４】【講演５】【講演６】JNSA標準化部会の各WGの異なる視点から見たゼロトラスト

- 日本ISMSユーザグループ　リーダー：魚脇 雅晴（エヌ・ティ・ティ・コミュニケーションズ株式会社）
  - ゼロトラストとISMS.
    - ゼロトラストを有効活用するためには？
    - ゼロトラスト（技術）とISMS（マネジメントシステム）との関係
- デジタルアイデンティティワーキンググループ　リーダー：宮川 晃一（日本電気株式会社）
  - ゼロトラスト環境実現に必要なIGA（アイデンティティガバナンス管理）とPBAC（ポリシーベースアクセス制御）について
    - ゼロトラストの核心の一つID管理に基づくアクセス制御
- 電子署名ワーキンググループ　リーダー：宮崎 一哉（三菱電機株式会社）
  - ゼロトラストにとってのデジタル署名 vs. 電子署名にとってのデジタル署名
    - そもそもの（デジタル）トラストの考え方
    - （PKI的には）ゼロトラストアーキテクチャ≒トラストアーキテクチャ
- PKI相互運用技術ワーキンググループ
  - Always Verifyの実装となるリモートアテステーション
    - ゼトトラスト環境下にあるサブジェクトのalways Verify

昔から（伝統的に）存在する境界線防御をベースとしたトラスト

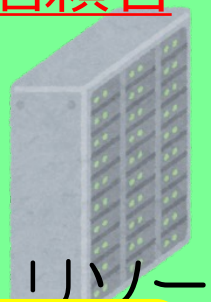
ZeroTrust　Environment??

物理的ゾーニングで守られたトラストな場所に構築されるトラステッドネットワーク

Trusted Party(TP)
被信頼者

Relying Party(RP)
信頼者

静的なトラスト？？
暗黙のトラスト（Implicit Trust）？？



サブジェクト

リソース

被信頼者（TP）と信頼者（RP)が境界線内であれば（暗黙的に）トラスト

昔から存在する
境界線防御

出典：**客家**（はっか、ハッガー、ハッカ）福建土楼
https://ja.wikipedia.org/wiki/福建土楼

境界線防御（のコンセプトや課題）は、
　静的なアクセス制御、暗黙のトラストとすると
ゼロトラストは、動的なアクセス制御
ゼロトラストのNever trust→　Never　implicit trust
　暗黙のトラストを置かない（最小限にする）

NIST SP800-207 ゼロトラストアーキテクチャ 論理コンポーネントを各WGの活動とのマッピング

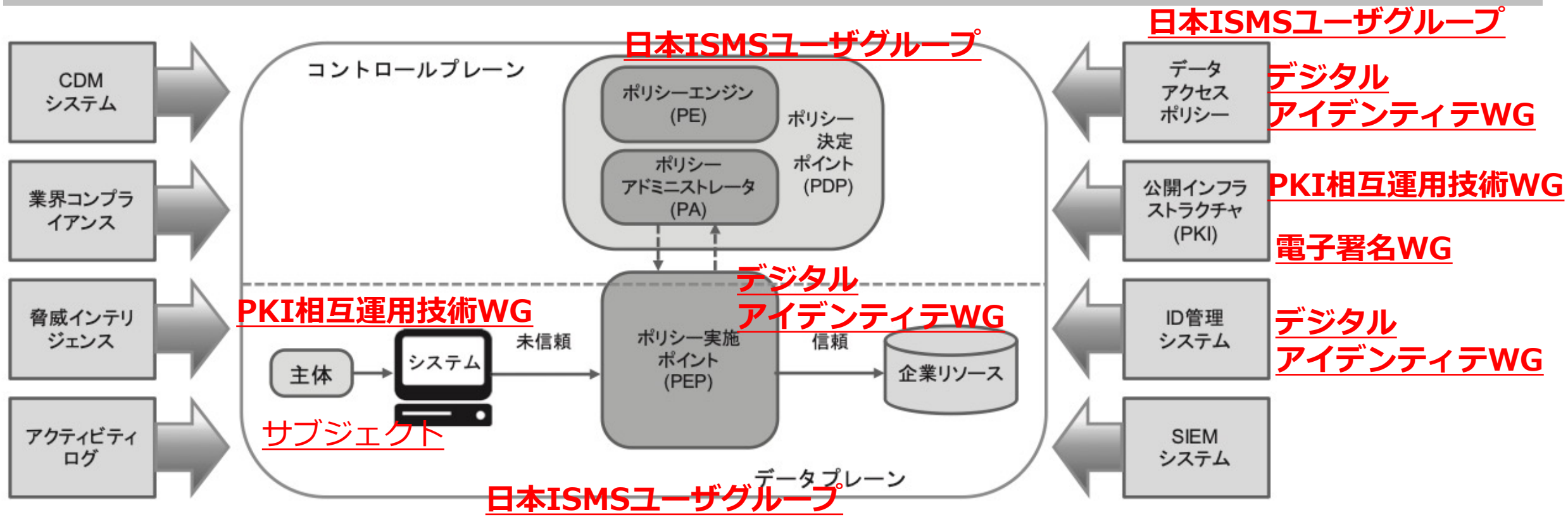
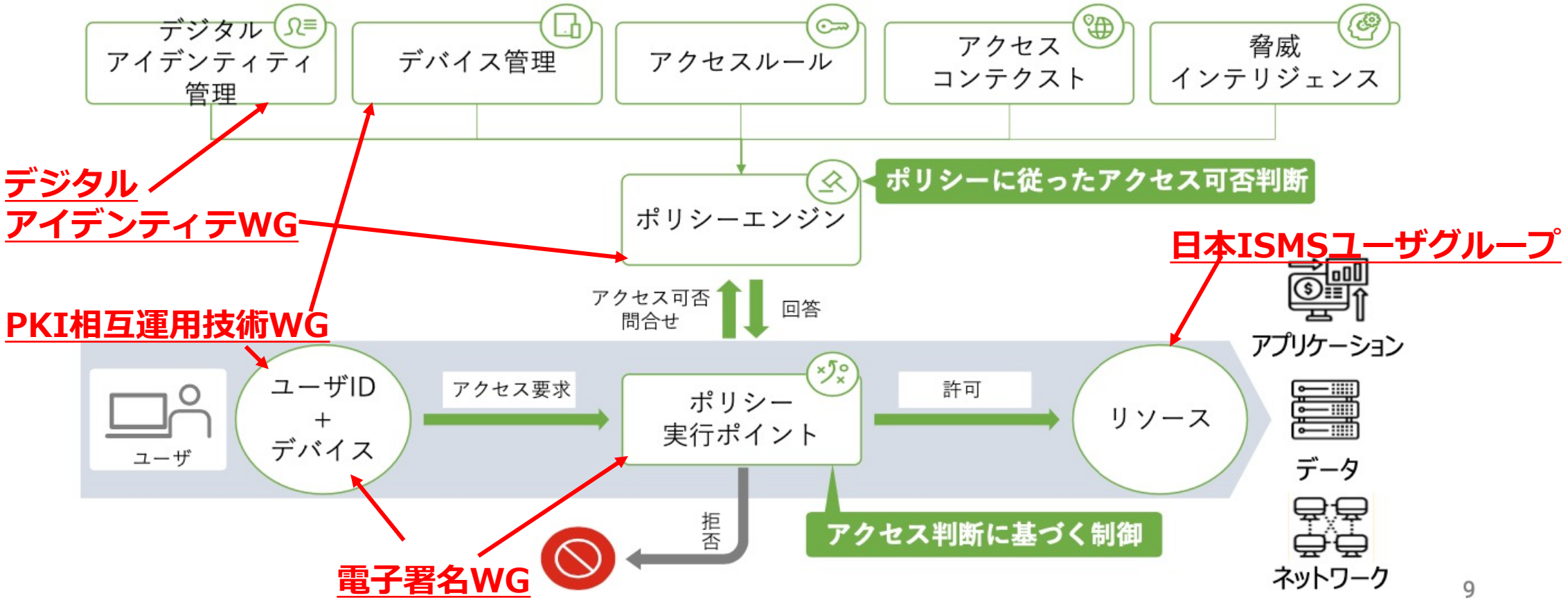


図 2：ゼロトラストの中核となる論理コンポーネント

出典：https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/assets/pdf/zero-trust-architecture-jp.pdf

2．ゼロトラストアーキテクチャについて

各リソースへのアクセスはデジタルアイデンティティを元にそのアクセス可否を決定する



9

デジタル庁　技術検討会議　2022年2月24日(木)
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/5589466b-5eb7-447d-9164-2cfa048a0d0f/67c7208c/20220224_meeting_security_architecture_guideline_02.pdf

ゼロトラストの概念と用語の理解
Never Trust, Always Verify.

- Never trust　→　Never implicit trust
  - 暗黙のトラストをしない（最小限にする）
  - たぶん、理想的なゼロトラストアーキテクチャにおいては、（責任が明らかにならない）電子署名が付されていないすべてのインプット情報（トランザクション）は、トラストしない。
- Always Verify　→　explicit trust
  - 検証することにより得られる明示的なトラスト、かつ、検証は自動化の方向へ
  - 検証の自動化のために必要となる「信頼点(トラストアンカー)の重要性」
    - →「ゼロトラストにとってのデジタル署名 vs. 電子署名にとってのデジタル署名」
  - Always Verifyの手段のひとつ
    - →「Always Verifyの実装となるリモートアテステーション」
  - Always Verifyなどの結果に基づく動的なアクセス制御
    - →「ゼロトラスト環境実現に必要なIGA（アイデンティティガバナンス管理）とPBAC（ポリシーベースアクセス制御）について」
- 動的なアクセス制御の対象となるリソース管理を中心に捉えた「ゼロトラストとISMS」