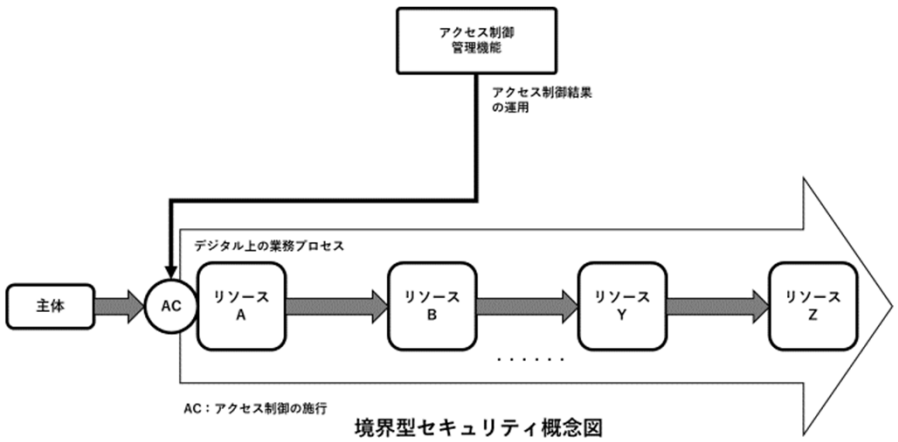
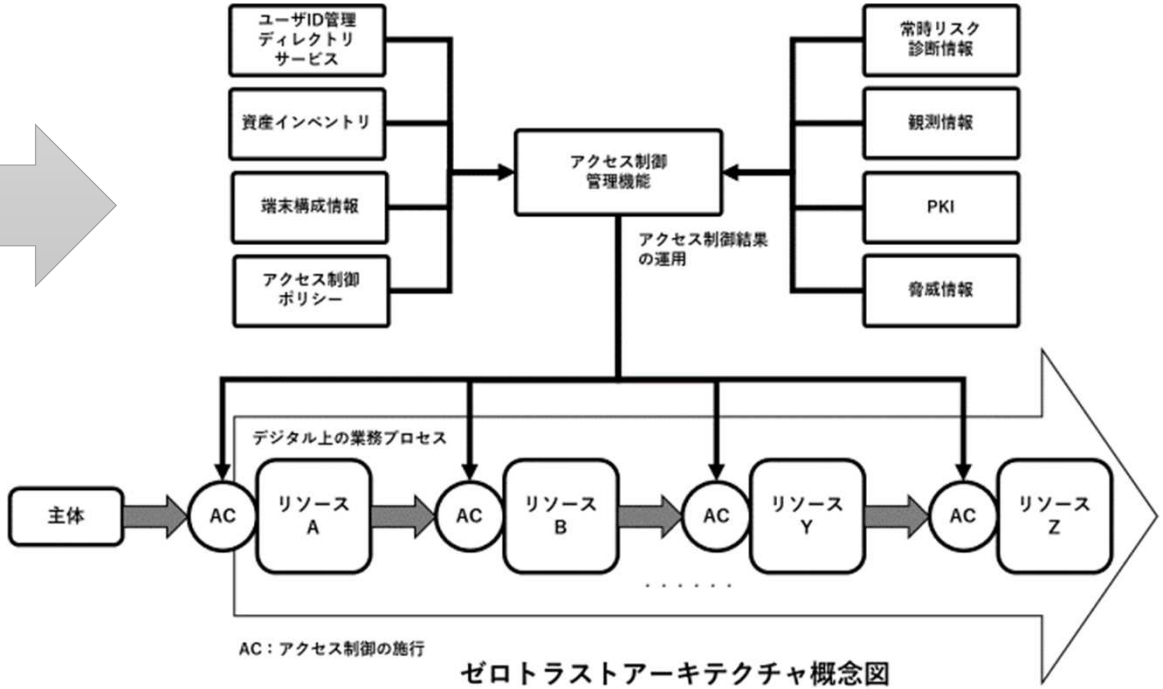
（参考資料1） デジタル社会推進標準ガイドライン 「ゼロトラストアーキテクチャ適用方針」の概要 1/2

ゼロトラストアーキテクチャとは、
ネットワーク上には、**外部/内部を問わず脅威が存在するといった前提**に立ち、ユーザー、デバイスなど個々のID（Digital Identity）に焦点を当て、**「都度必要なアクションに対して必要なレベルの認証を行い、問題なければ適切なアクセス権を認可する」**といった検証を厳密に行うことで、セキュリティを担保し、且つ柔軟なUser Experienceを実現するといった概念

従来の**セキュリティモデル**
からの**考え方の拡張**



境界型セキュリティ概念図



ゼロトラストアーキテクチャ概念図

- ゼロトラストアーキテクチャはセキュリティの**概念モデルであり、ソリューションではない**
- これまでの**ネットワークセグメンテーションを単一の信頼源とせず**、**デジタルアイデンティティを基にした信頼付与**へのシフト

（参考資料1）デジタル社会推進標準ガイドライン「ゼロトラストアーキテクチャ適用方針」の概要 2/2

ゼロトラスト・アーキテクチャを適用する際の基本方針

① リソースを識別し、特定できる状態にする
リソースを正確に特定できる状態でなければ、アクセス制御ポリシーの評価対象とすることはできない。そのため、リソースが識別できる状態で登録されていることが重要である。識別するものとしては、アカウント、デバイス、サービス、データである。

② 主体の身元確認・当人認証を実施する
利用者および端末などの物理的な主体は、システムを利用する際にはデジタルなリソースとして活動しなければならない。そのため、身元確認及び当人認証によって確認しなければならない。

③ ネットワークを保護する
ゼロトラストアーキテクチャは、イントラネットを含めたネットワークを暗黙的に安全であるという前提を信用しない。そのため、ネットワークは通信経路の適切な暗号化によって安全性を確保しなければならない。

④ リソースの状態を確認する
適切に運用・保守されなければ、時間の経過とともに脆弱性が増えるもしくは、設定ミス・構成の不備により脆弱性が生まれることも考えられる。そのため、各種リソースの状態や構成が安全かを常時確認する必要がある。

⑤ アクセス制御ポリシーで評価し、アクセス管理をする
各種リソース同士でアクセスを確立する際に、その可否を事前に定めたアクセス制御ポリシーを基にアクセス制御管理機能が評価し、その結果を施行できるようにしなければならない。

⑥ リソースとアクセスを観測する
運用・保守をし、システムの信頼性を高めるうえで、リソースとアクセスのログの取得、アラートの通知など、政府情報システムを観測することが重要である。

デジタル社会推進標準ガイドライン「ゼロトラストアーキテクチャ適用方針」
https://www.digital.go.jp/resources/standard_guidelines/#ds210