Zero Trust Architecture

クラウド利用にあたっての「ゼロトラスト」の現状と現実的な対応は？

2021年3月3日　第６３回NCWG会合

- 公立大学法人会津大学　客員上級准教授
- 株式会社コンピュート　取締役
- 三井物産セキュアディレクション株式会社
プリンシパル・コンサルタント

福原　英之

アジェンダ

1. ゼロトラストとは？
2. ゼロトラストの背景
3. ZTA実装？
4. 今後の展望

1．ゼロトラストとは？

Zero Trust

2010年　米国の調査会社フォレスター・リサーチ（Forrester Research）のジョン・キンダーバーグ氏（John Kindervag）が提唱した概念/造語

~~TRUST BUT VERIFIED~~

“never trust, always verify”

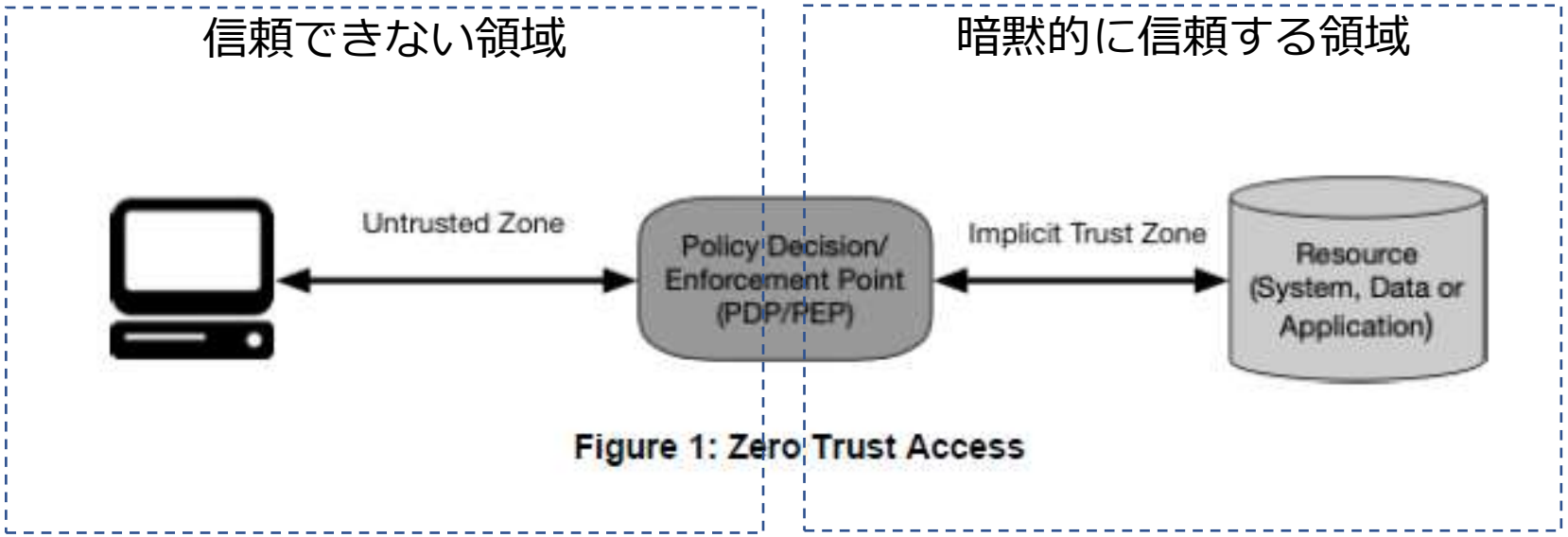
全てのデバイス、サーバ、ネットワークからのアクセスを信頼できない前提でセキュリティ対策を講じる

NIST (National Institute of Standards and Technology, , アメリカ国立標準技術研究所)

SP 800-207: Zero Trust Architecture (ZTA)
2019/9/23: Draft1, 2020/2/13: Draft2, 2020/8/11: Final

https://www.nist.gov/news-events/news/2020/08/zero-trust-architecture-nist-publishes-sp-800-207

1-2. ZTAの基本概念



subject

resource

図は、NIST SP800-207 より引用

2. ゼロトラストの背景

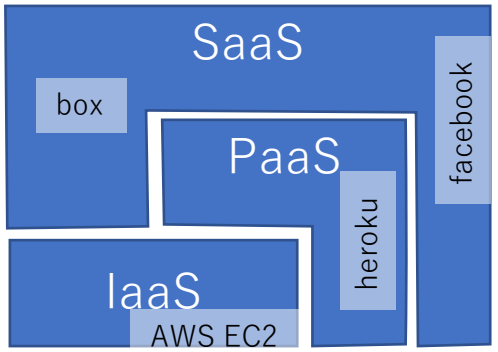
1. 境界防御の崩壊
   - マルウェアによる内部攻撃
   - 内部犯による攻撃
   - 標的型攻撃の高度化
2. SOAの成熟
   - Web-API、マイクロサービス化
3. 認証（AAA）技術の普及
   - 個人IDの普及
   - 多要素認証の普及
4. クラウドサービスの普及

＜参考＞クラウドサービスのおさらい

Definition of Cloud Computing:　（NIST　SP800-145, Sep. 2011）

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.

- 特徴
  On-demand self-service, Broad network access,
  Resource pooling, Rapid elasticity, Measured Service
- サービスモデル
  SaaS, PaaS, IaaS
- デプロイメントモデル
  Private cloud, Community cloud,
  Public cloud, Hybrid cloud



その後いろいろな　“X as a Service” が登場してきた。
（今では、“Ransomware as a Service” まで・・・）

３．ZTAの実装？

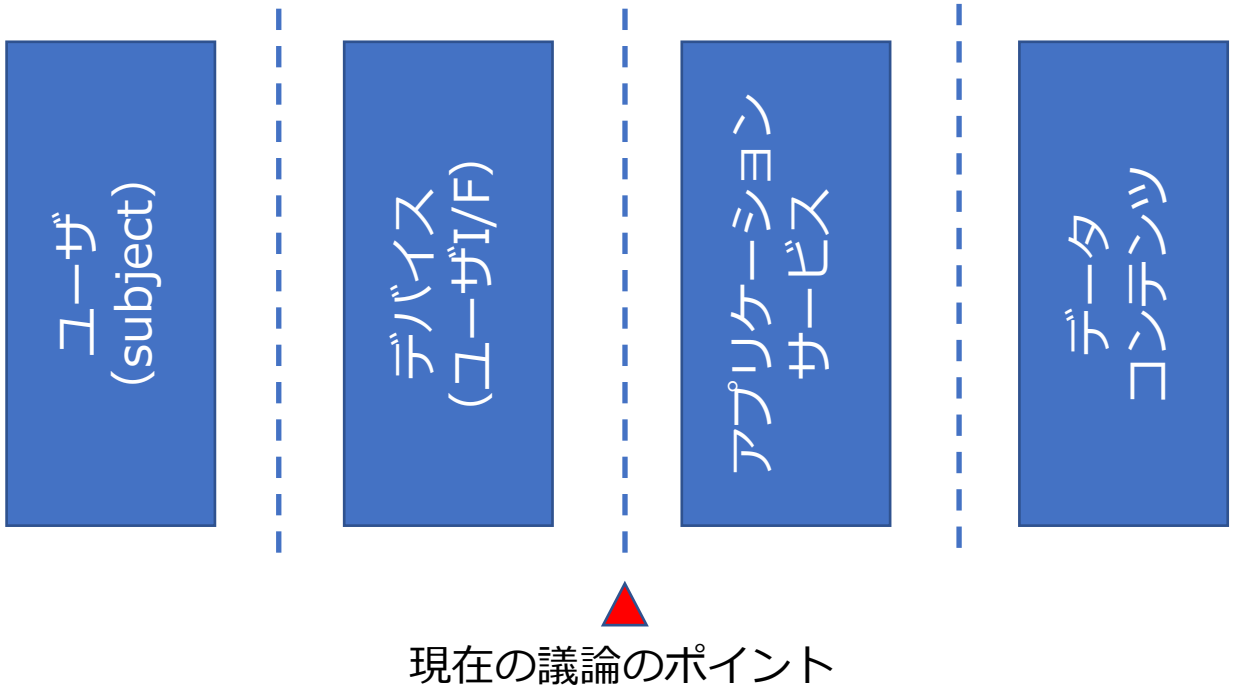
“never trust, always verify”

3-1. 改めて現状を整理

- ZTAは言葉が先行（バズワード）
- ZTAをバズワードにベンダーが自己主張
  - micro segmentationには次世代FW
  - 個人認証にはIDMサービス
  - クラウドにも対応するにはCASB(Cloud Access Security Broker)
- ZTAは新しいテクノロジーではない
- ZTAはすべてが新しい概念ではない
- ZTAは1つの製品で実現できない
- とはいえ、ZTA実装によってセキュリティレベルの向上が期待できる

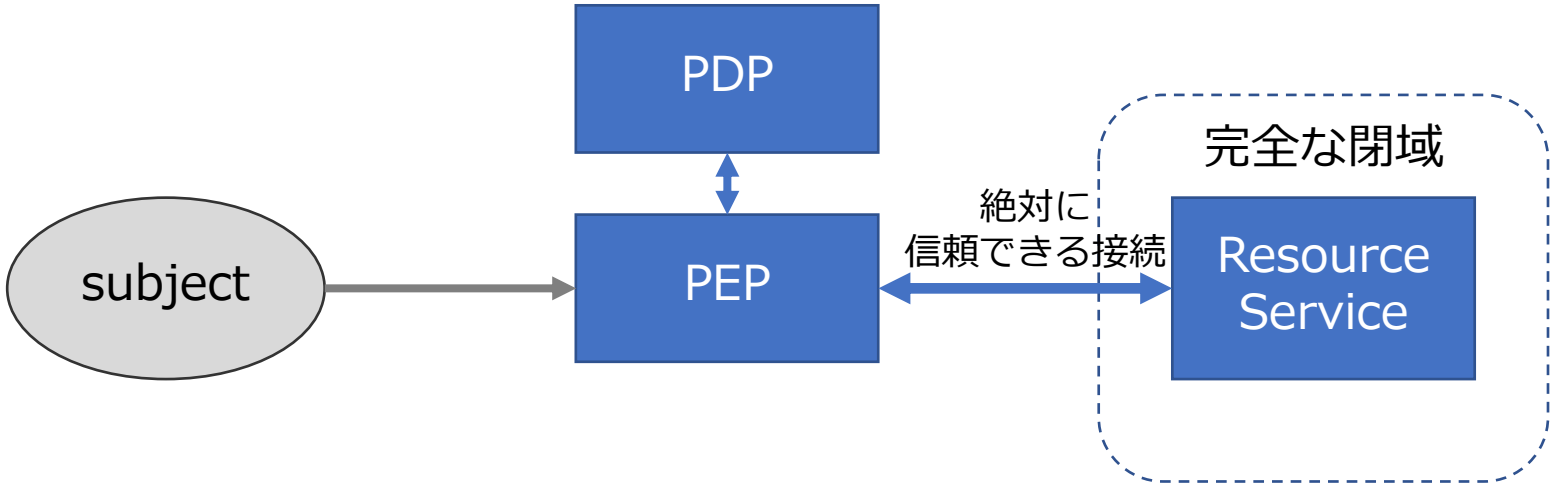
3-2. どこまでやるか？どうやるか？

- すべての境界でVerifyが必要
- Verifyするための情報が必要

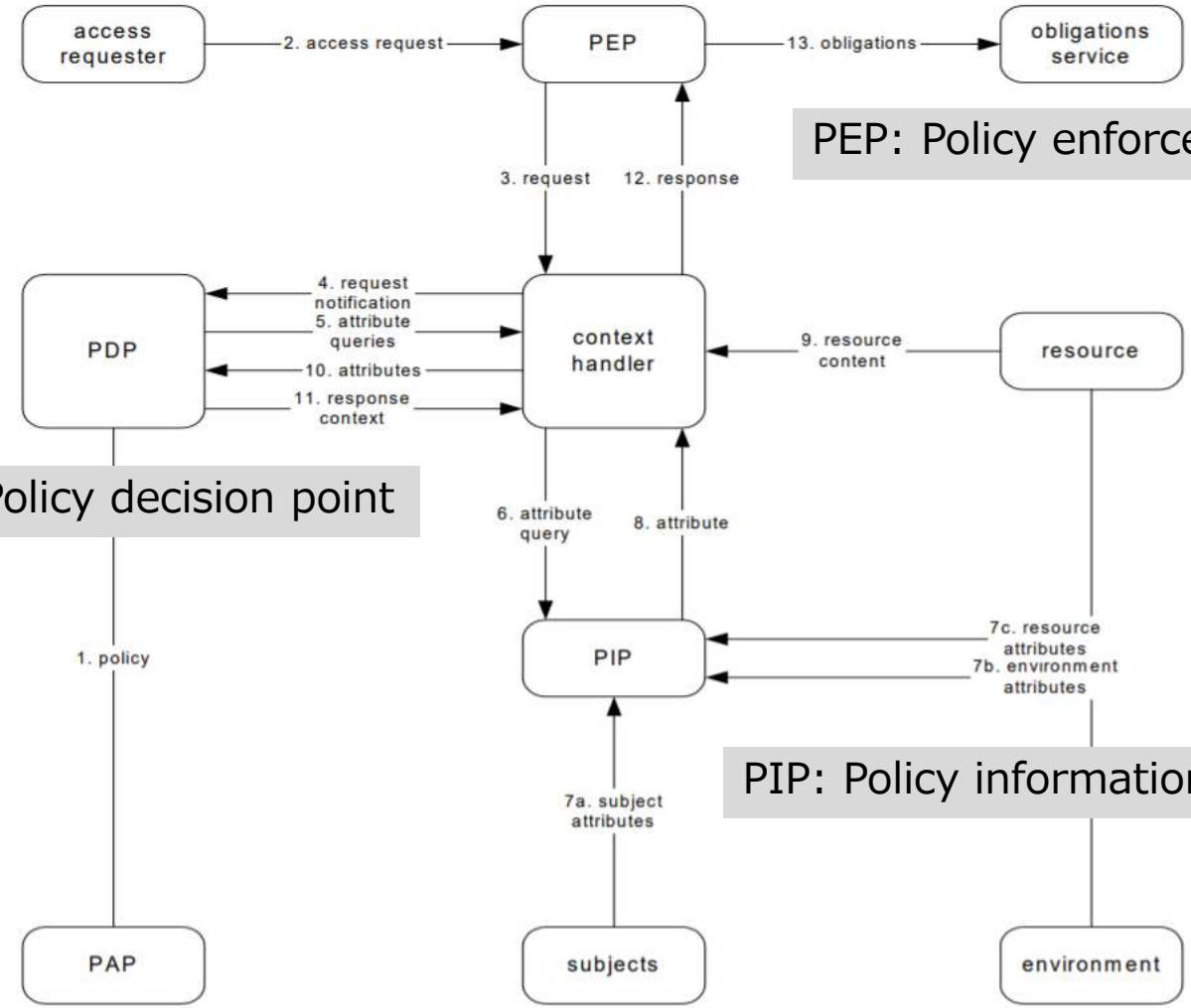


3-2. ZTAに絶対必要な要素

- リソースの閉域化
- PEPの配置
- PDPの配置
- アクセスポリシー
- アクセス可否を判断する情報



<参考> OASIS　xACML v2 (Feb. 2005)



PEP: Policy enforcement point

PDP: Policy decision point

PIP: Policy information point

PAP:
Policy administration point

Figure 1 - Data-flow diagram

- https://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf

3-3. ZTAは「アクセスポリシー」次第

- もしも、アクセスポリシーが・・・

Subjectの要件	Resourceの条件
IPアドレスが社内	すべてにアクセス

➡境界防御と同じ

- アクセスポリシーの要件が増えるほど、判断のための情報が増える

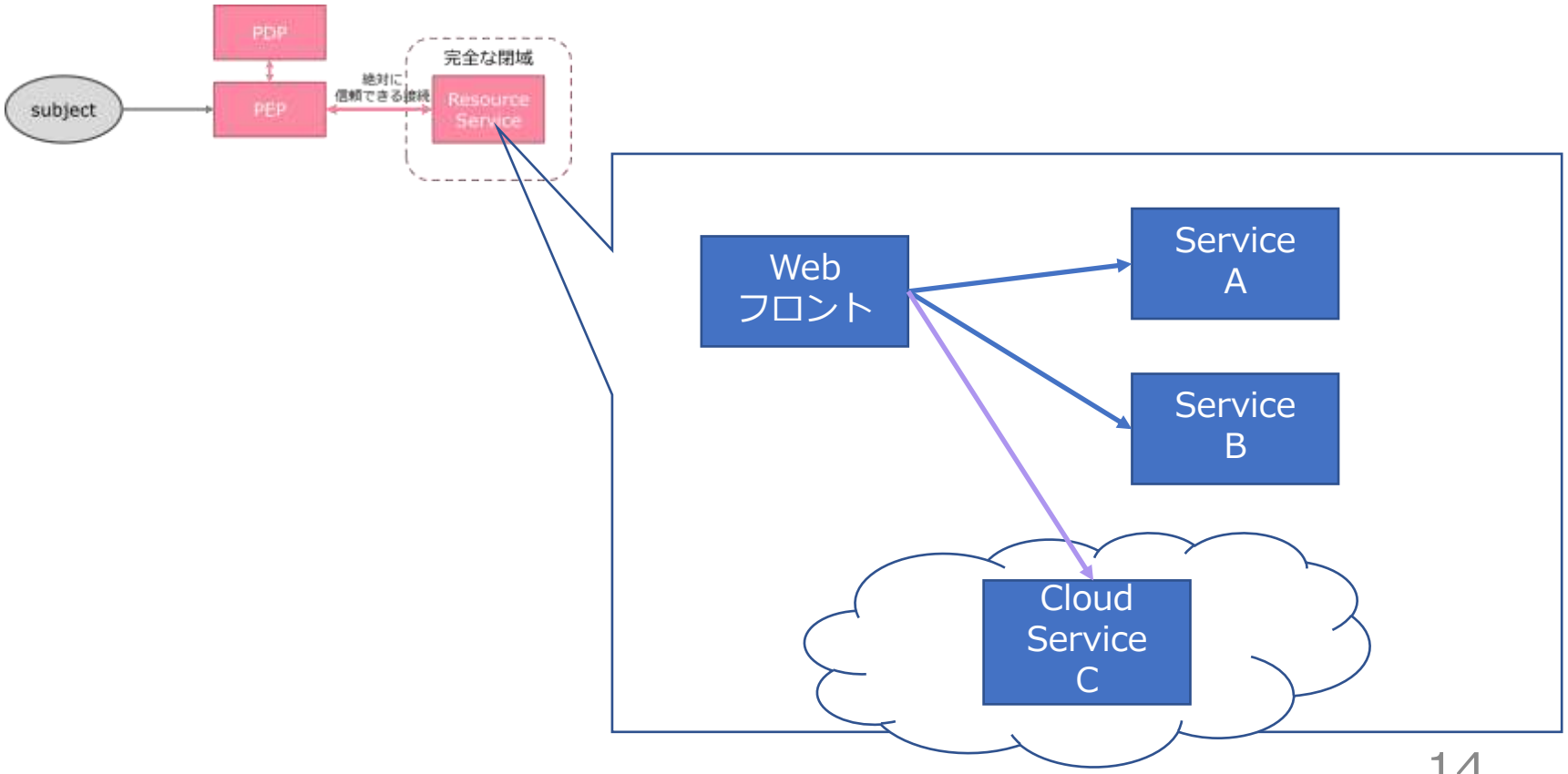
Subject要件	Resource条件	必要な情報
登録ユーザである		ユーザ一覧
安全な端末である		端末のパッチ情報、AV情報
攻撃者のIPでない		Threat Inteligence
	機密情報である	機密情報の一覧・ラベル
	時間制限	開示時間情報
	頻度制限	許容アクセス頻度情報

3-4．ZTAは厳密な「境界防御」が必要

- 言葉だけだと矛盾するが・・・
  - PEPの後ろ側は無防備
  - セキュリティコンポーネント間通信は絶対の信頼
  - Resourceへのバックドアがあると論外
- クラウド間通信の信頼性確保は？
  - 物理セキュリティ？
  - Software Define Perimeter?
  - Data encryption?

3-5. バックエンドコンポーネントにZTA?

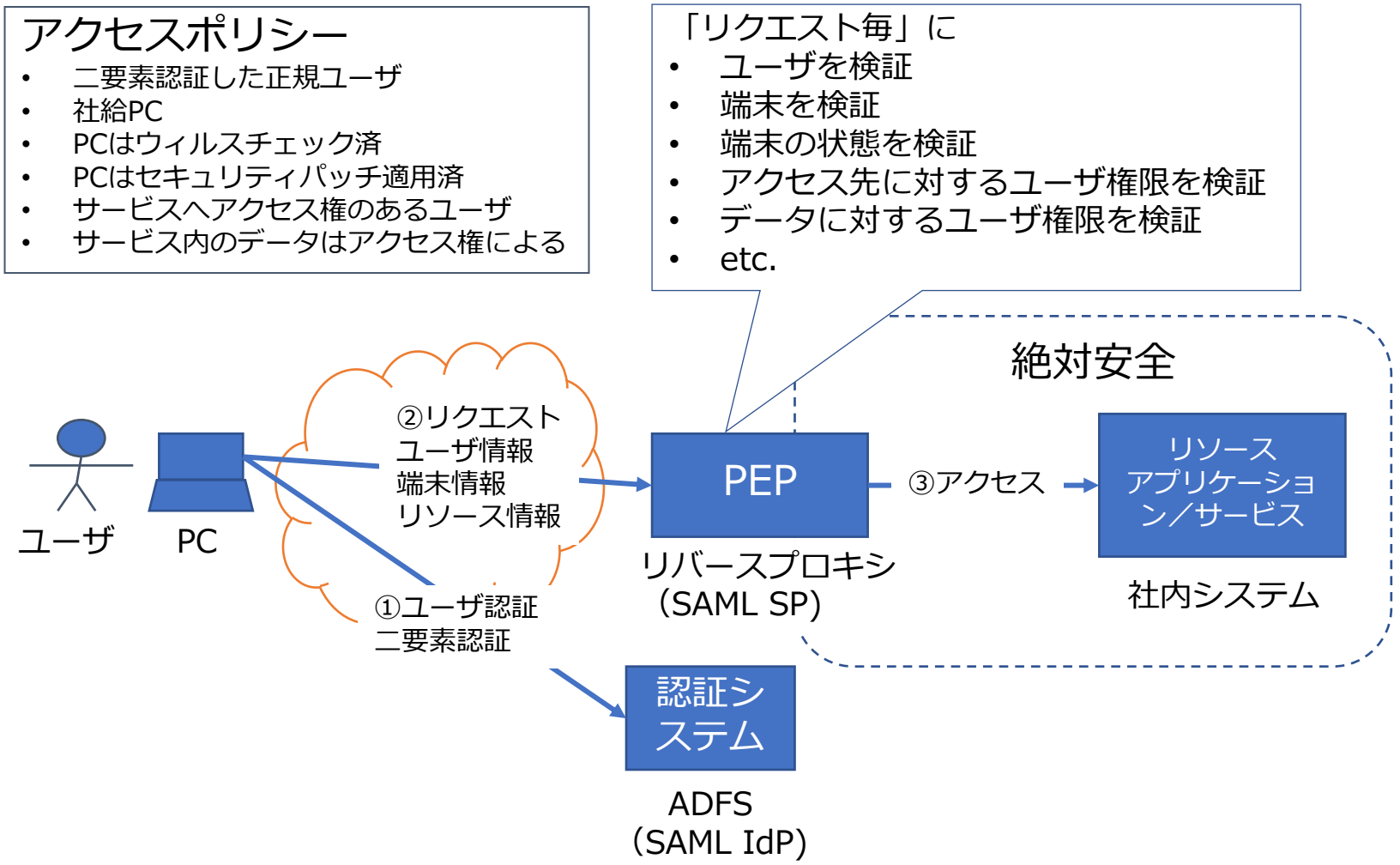
- クライアントPCとシステム間の防御に目がいっているが、
- システムの内部こそ侵害の危険があるのでは？



3-６. 厳格な個人認証は絶対必要

- 厳格な個人認証のために必要なこと
  - 管理されないユーザを認めないポリシー
  - 自然人とIDは1対1で紐ずける
  - 本人確認が厳格にできるシステム
  - 多要素による本人確認
  - ID管理システムによって、自動でプロビジョニングできる
  - IDの持つ幅広い属性が参照できる
- 権限管理も必要
  - IDの持つ属性にしたがって、論理的に権限を設定できるのが理想
  - 例外を排除するためのビジネスプロセス

3-7. ZTA実装例


アクセスポリシー
• 二要素認証した正規ユーザ
• 社給PC
• PCはウィルスチェック済
• PCはセキュリティパッチ適用済
• サービスへアクセス権のあるユーザ
• サービス内のデータはアクセス権による
「リクエスト毎」に
• ユーザを検証
• 端末を検証
• 端末の状態を検証
• アクセス先に対するユーザ権限を検証
• データに対するユーザ権限を検証
• etc.
絶対安全
ユーザ
PC
②リクエスト
ユーザ情報
端末情報
リソース情報
①ユーザ認証
二要素認証
PEP
リバースプロキシ
(SAML SP)
③アクセス
リソース
アプリケーション／サービス
社内システム
認証システム
ADFS
(SAML IdP)

4. 今後の展望

“never trust, always verify”

4-1. ZTAは必要か？

Question：ZTAは必要か？

Answer：必要！

- ZTAは実はすでに始まっている。
- ZTAはこれまで実施してきたセキュリティ対策の延長
- ZTAをツールとして、セキュリティ対策・システムアーキテクチャを見直すことが肝要

4-2. ZTAの実現に向けたステップ

- 既存システム
- ID管理システム
  自動プロビジョニング、権限付与
- 認証システム

- アクセスポリシー
- 必要情報の集約
  ポリシーの判定に必要なリアルタイム情報

- PEP周辺の整備
  フロントエンド
  バックエンド

- フィロソフィーを固めないと始まらない
  - “never trust, always verify”か？
  - ファシリティセキュリティ、境界防御に頼るか？
- 理想論からのドリルダウンでは困難
  - 全システムの一斉再構築はかなり困難
  - 現状からの順次移行をいかに早くできるか？

4-3. まとめ

- ZTAはテクノロジーではない
- ZTAは全く新しいものではない
- ZTAアクセスポリシーの策定が最重要

- アクセスポリシー実現のために情報集約強化やシステムアーキテクチャの見直しが必要

- ZTAの核心をとらえて、表面的な対応にならないことが肝要

Some Questions?