Zero Trust

NCWG
サムライクラウド部会
2022春

アジェンダ

1. 背景
2. What's “Zero Trust”
3. “Zero Trust” Journey
4. おまけ

背景

世間で「ゼロトラスト」がバズワード化する中、サムライクラウド部会では、ゼロトラストを正しく理解するための講演を2021年3月に実施した。

その後、サムライクラウド部会では、世間で「ゼロトラスト」という言葉が各所で使われる中、ゼロトラストという言葉の理解だけでなく、どのようにゼロトラストを推進すべきか？についてのガイドラインが必要であろうと考えた。

ゼロトラストが非常にハイレベルの概念であるために、正しく道のりを解説するのは困難であり、サムライクラウド部会でも議論が続いてきた。

今般この議論が、一定のまとまりを見せたため、ここに報告をまとめることとなった。

What's “Zero Trust”

“Zero Trust”の概要　振り返り

“Zero Trust” の歴史

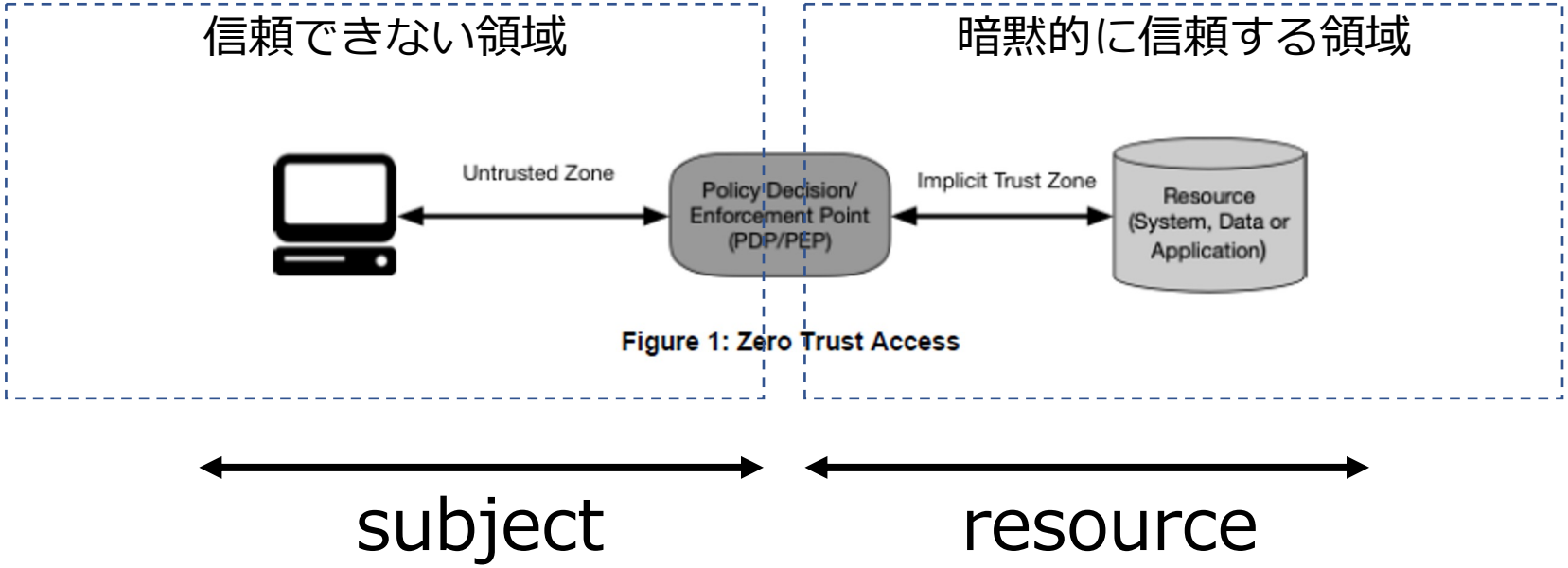
- 2010年　　米国の調査会社フォレスター・リサーチ（Forester Research）のジョン・キンダーバーグ氏が「Zero Trust」という造語を作り概念を提唱した
- セキュリティ関連各社が、”Zero Trust”や、”Zero Trust Network”という言葉で各社のソリューションの利点を説明してた
- 2018年　米国ガートナー（Gartner）はZero Trustの上位概念として、Lean Trustを提唱した
- 2019年　米国政府機関のNIST（アメリカ国立標準技術研究所）が、”Zero Trust Architecture”として文書のドラフトを公開した
- 2020年8月11日　NIST SP800-207: Zero Trust Arvhitecture として文書を公開した

“Zero Trust”のキーポイント

NIST SP800-207 Zero Trust Architecture に基づくZero Trustのキーポイントは以下の通り

- 全てのSubjectからResourceへのアクセスは、**リクエストごと**にアクセス可否を判断し制御する
  - 刻々と変化する状況・環境に応じて判断する
  - リソースへのアクセスは、最小権限で可能な限り細かい粒度で制限する
- 用語
  - リソース（resource）：情報資産として守るべきものの総体（システム、データ、アプリケーションなどを全て含む）
  - サブジェクト(subject)：情報資産にアクセスするアクセス元の総体（人、端末、クライアントアプリなどを全て含む）
  - PDP（Policy decision point)：ポリシーに従ってアクセス可否を判断するポイント
  - PEP（Policy enforcement point）：PDPの決定に従ってアクセスを制御するポイント

ZTAの基本概念



図は、NIST SP800-207 より引用

“Zero Trust” Journey

“Zero Trust”の実現に向けて

“Zero Trust” Journeyとは？

- “Zero Trust” へ至る道のりを、５段階のレベルでまとめたものである
- 各レベルは、全ての要件が満たせて初めて達成できたとみなす
- まず初めに、各レベルの要件概要を示し、少し細かい説明を「詳細」に記載している
- この「“Zero Trust” Journey」は完成品ではない。要件として検討すべき項目がまだまだある。
- 今後検討する要件項目（の一部、わかっている項目）は、「今後の検討」に示す。

Zero Trust Journey

Zero Trust Journey

Level1	Level2	Level3	Level4	Level5
・何もしていないが計画はある	・全てのシステムに対してログインの暗号化（TLS1.2対応） ・全てのリソースに対してユーザ認証が必要 ・ログインせずに利用できるシステムがない ・共有アカウントの禁止（ひとり１ID） ・情報資産台帳がある	・細かく境界が区切られている ・境界毎に守るべきリソースがはっきりしている ・端末の認証が必要 ・防御すべき境界にアクセスするときはユーザ・端末認証が必要 ・IdPは一つしかない（VPNのIdPを使わない）	・個別のグループ専用のVPNはない ・アクセスの証跡を取っている ・VDIやRDP（端末ハックリスク）の制限がかかっている ・アプリ間連携はAPIで認証・認可している	・境界はアプリ毎 ・アプリ内の各機能でアクセス制御する（コンテキスト×リソースアウェアアクセス） ・VPNを撤廃した ・VDIやRDPは使っていない ・システム構築時にゼロトラストガイドラインに準拠 ・ブラウザのみでアプリケーションが動く

Zero Trust Journey 詳細

	Level2	Level3	Level4	Level5
1. IDと端末と認証	・ひとり１ID（業務ユーザ） ・ログインせずに利用できるシステムがない ・社員・協力会社社員の台帳 ・ID管理とプロビジョニング	+すべてSAML化し、IdPは一つ +端末の認証 +社員の受け入れ・棚卸し +社員情報自動プロビジョニング	+端末のクリーン +クライアント証明書	人・端末の認証と、アプリ内の細かいアクセス制御の連動(コンテキスト×リソースアウェアアクセス)
2. 業務とデータ整理と認可	・業務分掌の整理 ・システム台帳	+データは業務と秘密度合いで分類されている。 +境界毎に守るべきリソースがはっきりしている	+システム連携の台帳 +アプリ間連携はAPIで認証・認可し記録している	＋アプリ内の細かいアクセス制御 ＋権限をダイナミックに計算する
境界 (制御単位を小さく)	・社内 or 社外の大きな境界	・社内外をさらに境界でわけている(マイクロセグメンテーション)	・境界はアプリケーション	・境界はデータとロジック
レガシーの撤廃 （時代にあわせた対応）	・全てのシステムに対してログインの暗号化（TLS1.2対応）		・個別のグループ専用のVPNはない ・VDIやRDP（端末ハックリスク）の制限がかかっている	・ブラウザのみでアプリケーションが動く ・VPN/VDIやRDPは使っていない
統制と管理	・アクセスログを取っている	＋アクセス制御を強制している ＋監査ログをとっている	+ログを分析している	+ログから行動を分析している(制御下での不整使用の検知) ＋継続的に改善している

今後の検討

- 特権管理
- inpersonate
- 業務と権限の高度な整理
    - PDPがダイナミックに計算できるための情報

- 本ドキュメントだけではすべてを網羅するには不十分であるため、今後必要な切り口で本ドキュメントを補助するドキュメントを追加公開していくものである。

おまけ

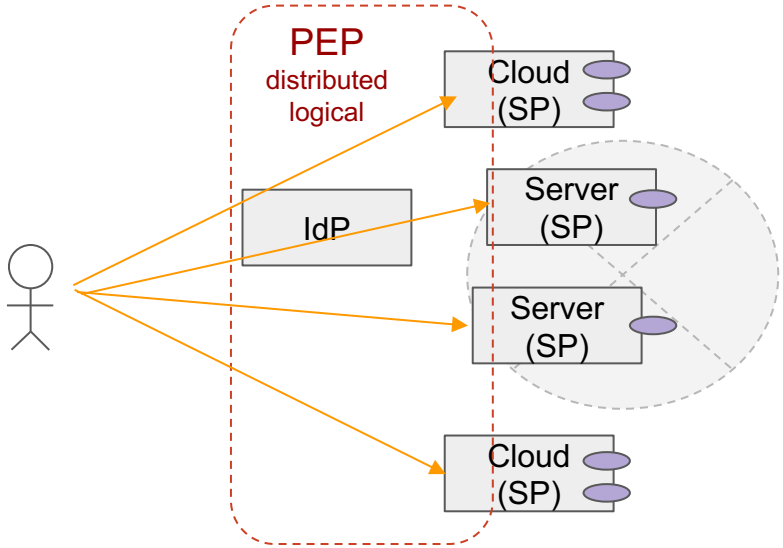
冗談半分に笑ってください

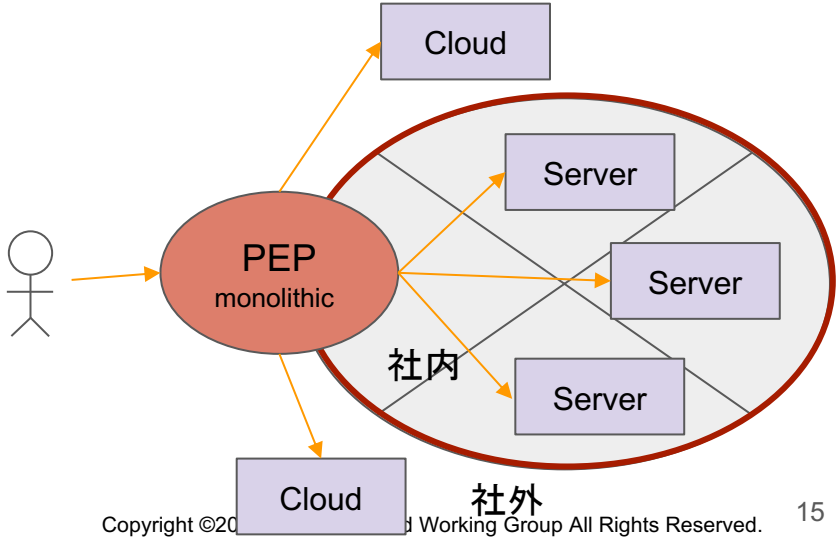
Zero Trust テスト

ID/社員	社員の業務分掌が明確になっている。	10点
	社員のIDは一元管理され、すべてのシステムは唯一の認証システムで認証する。	10点
	認証に多要素認証を使っている。	10点
データ/業務	データの分類ができている。	10点
	業務分掌×データの分類×データ操作権限が、管理できている。	10点
アプリケーション	認証で特定するID(社員)に対し、適切な粒度で、業務権限(データ操作)が実装されている。ログもでる。	10点
	アプリケーション単位(※)で、最小のセグメンテーション化されていて、入出力(FW/権限)が明確に実装されている。	10点
クライアント	業務クライアント(PC)のセキュリティを保っている。	10点
管理	システム/データ/業務の構成を管理している。	10点
	認証/アプリ/クライアントのログを、リアルタイムで収集し関連させて、最小権限での正しいデータ利用がされていることを保証できている。	10点
ネットワーク	ぜんぶVDIからやっている	-100点
	単一のPEP製品を通しているから完璧だ	-200点
	すんごくいいVPNを使っている	-500点
DX	DXよりIDXに取り組んでいる	100点

Zero Trust 構成 ～理想 vs よくある間違い～

理想	よくある間違い
PEPは、柔軟に論理的に構成されている。	PEPは、単一のコンポーネントだと思い込んでいる。
守るべきリソース粒度は、最小で、データ単位。	社内外・サーバ丸ごとで、守ればいいと思っている。
社内外には、こだわらない。	社内外の境界だけにこだわりすぎる。





サムライクラウド部会　執筆者

戒亥　稔	株式会社テッキーズポッド
中川路　充	株式会社プロキューブ
福原　英之	株式会社コンピュート
佐分利　徹	ネットワンシステムズ株式会社
野元　恒志	有限会社ディアイピィ