A10

Always Secure. Always Available.

ゼロから分かる『ゼロトラスト』実現に向けたステップ

A10ネットワークス株式会社

目次

- ゼロトラストアーキテクチャについて
  - ゼロトラストアーキテクチャとは
  - 構成要素
  - ネットワークに対する要件
  - 導入後に想定される脅威
  - 移行ステップ
- ゼロトラストアーキテクチャにおけるA10製品の活用領域
  - Policy Enforcement Point（PEP）としての活用・振る舞いの可視化
  - 通信の安全性の確保
  - 脅威インテリジェンスの活用
  - 新たな脅威への対応
- ゼロトラストアーキテクチャ実現に向けたステップ
- まとめ

ゼロトラストアーキテクチャについて

ゼロトラストアーキテクチャとは

- 境界内のネットワークに存在するユーザーや端末・サービスを全面的に信頼して全てのリソースへのアクセスを許可するあり方を廃し、場所によって完全に信頼される（トラストな）状態を作らない（ゼロにする）構成
  - 内部・外部の全てのユーザーや端末・サービスに対して等しくその振る舞いや脅威の情報などに基づき、リソースへのアクセスに対する要求ごとに動的に認証・認可を行うことによりセキュリティを担保
  - トラストな領域を作らず、また、同じユーザーや端末から同じリソースに対するアクセスであっても信頼し続けることが無いようにすることで、攻撃を受けた場合の影響を小さくする
- 境界型のセキュリティを適用することが難しい状況に対しては、ゼロトラストアーキテクチャによるセキュリティの担保がより適すると考えられている
- それ自体が一つのセキュリティ技術を指すものではなく、企業や組織が取るべきセキュリティ戦略を表したもの

NIST SP 800-207における基本原則

1. 全てのデータソースとコンピューティングサービスをリソースとみなす
2. ネットワークにおける場所に関わらず、全てのコミュニケーションが保護される
3. 個々の組織のリソースへのアクセスは、セッションごとに許可（認証・認可）される
4. リソースへのアクセスは―クライアントID、アプリケーションやサービス、要求している資産の観測可能な状態、およびその他の振る舞いや環境の属性を含む―動的なポリシーによって決定される
5. 組織が所有する、または関連する資産の完全性とセキュリティ体制を監視し測定する
6. 全てのリソースに対する認証と認可は動的に行われ、アクセスが許可される前に厳密に適用される
7. 資産、ネットワークインフラとコミュニケーションの現在の状態に関する情報を可能な限り収集し、セキュリティ体制の強化に利用する

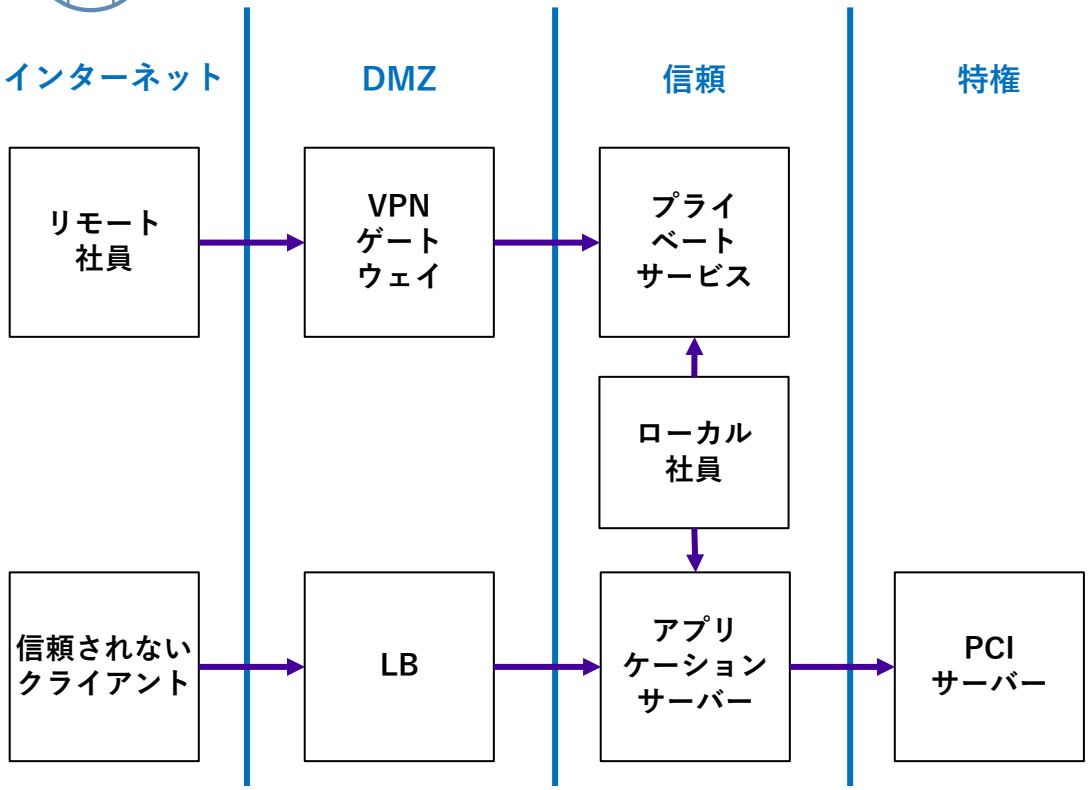
*NIST SP 800-207 “Zero Trust Architecture”, 2020. （https://csrc.nist.gov/publications/detail/sp/800-207/final）

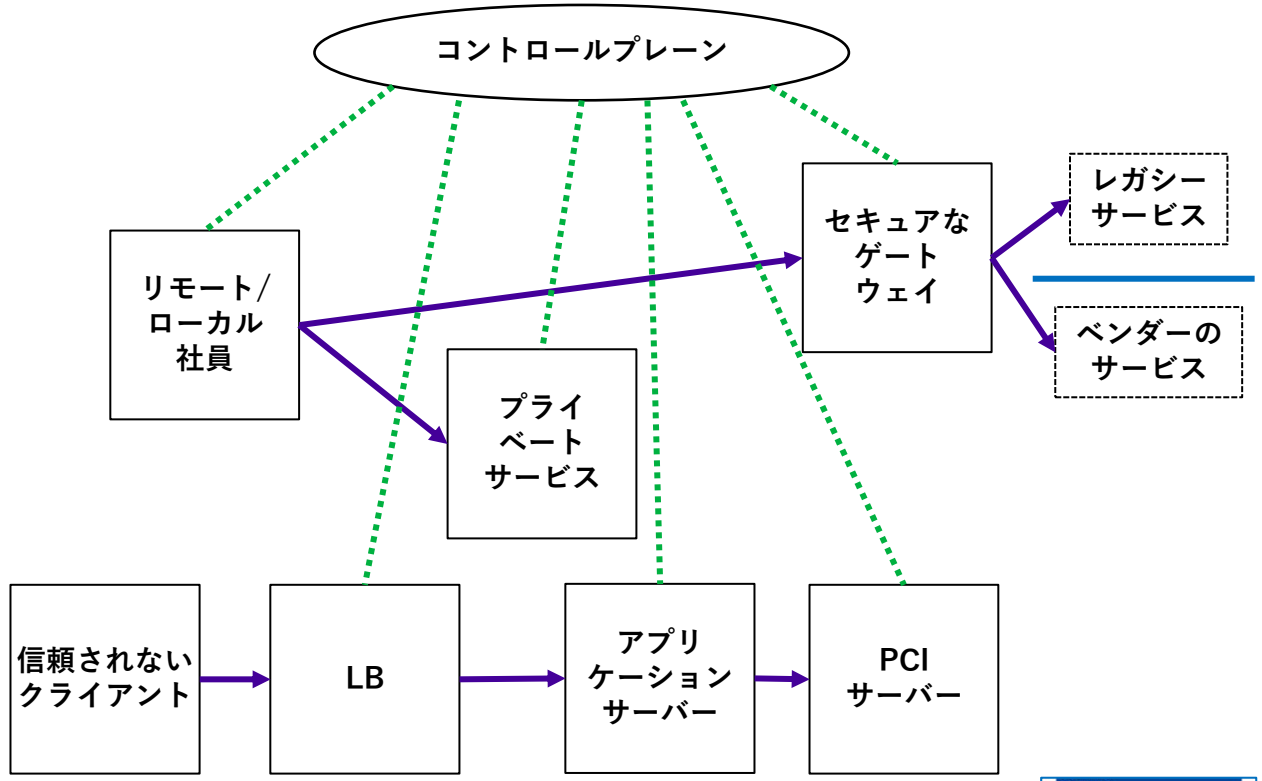
ゼロトラストネットワークの考え方

- ネットワークが完全に危険にさらされていることを前提とする
- 信頼ゾーンを設けずに全てのホストを認証する
- トラフィックの傍受を防ぐために通信を暗号化する
- 3つの構成要素に基づくクライアントのリソースへのアクセス制御
  - ユーザー/アプリケーション認証
  - デバイス認証（ハードウェア・ソフトウェアの構成管理）
  - 信用（スコア）
- 継続的な認証・認可を繰り返し信用を更新する
- 暗号化されているトラフィックも含めたユーザー行動の監視
- IPsec+mTLS（相互TLS）による通信による安全性の担保
- パブリックPKIよりプライベートPKI

*“ゼロトラストネットワーク―境界防御の限界を超えるためのセキュアなシステム設計”, Evan Gilman, Doug Barth著, 鈴木 研吾 監訳, オライリージャパン, 2019.

ゼロトラストネットワークとは？





従来のネットワークセキュリティアーキテクチャ

ゼロトラストアーキテクチャ

*“ゼロトラストネットワーク―境界防御の限界を超えるためのセキュアなシステム設計”, Evan Gilman, Doug Barth著, 鈴木 研吾 監訳, オライリージャパン, 2019.