ゼロトラストを支える
エンドポイントセキュリティ

ゼロトラストの概念

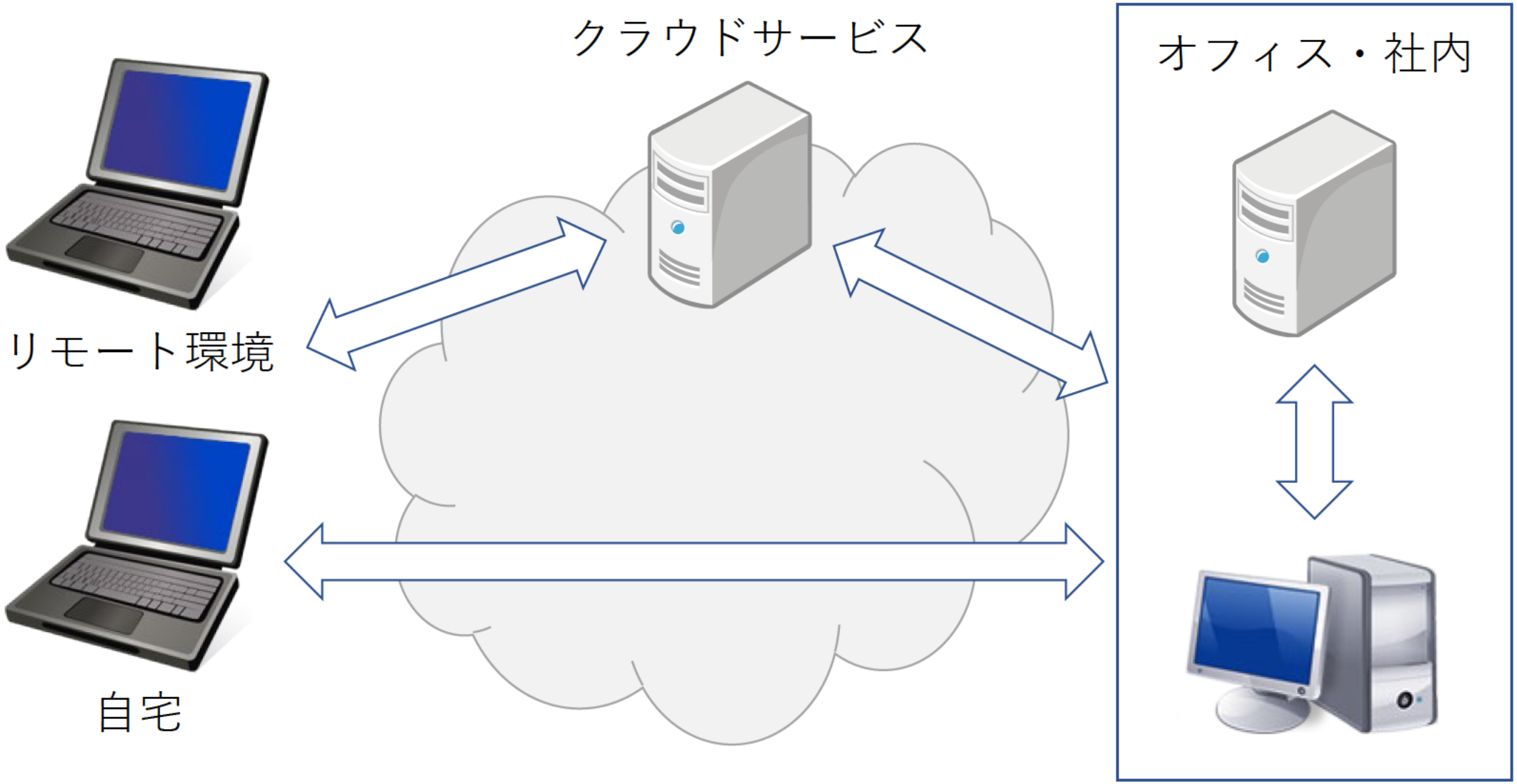
- 「社内」「社外」「境界線防御」にとらわれないセキュリティのあり方
- 情報資産・アクセス権者の分散

他にも・・・

- ID管理
- 属性をもとにしたアクセス権管理
- クラウドを含めたシステム全体のセキュリティデザイン
- リスクマネジメント

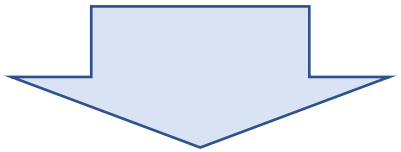
従来型のセキュリティ対策が一新されるわけではない

守るべきポイントはどこか



働き方の変化

- 新しい働き方におけるIT要素
  - VPN + VDI/シンクライアント
  - FAT PC貸与、あるいはBYOD
  - リモート環境にあるPCやスマートフォン
  - クラウドサービスの利用促進
    - オンラインミーティングツール



- それぞれの要素におけるセキュリティの担保が必要
- リモートワーク、出勤型が混在して残り続ける
- 多額の費用を掛けずに最大限のセキュリティ担保が理想

エンドポイントと業務リソース

- 働き方、働く環境が変化しても、エンドポイントは残り続ける
  - 境界線内のPC端末 → 境界線内の業務リソースへのアクセス
  - 境界線内のPC端末 → クラウド環境のリソースへのアクセス
  - リモート環境のPCの端末→ 境界線内の業務リソースへのアクセス
  - リモート環境のPCの端末→クラウド環境のリソースへのアクセス

すべてのパターンにおいて、同じ考え方のセキュリティを実現するためには、ゼロトラストの考え方が不可欠

ゼロトラストの神髄

- アクセス権者の認証
- リソース、サービスへのアクセス認可

⇒ 可能な限り動的に割付

⇒ (例えば)
ルールに合致しないアクセスをアノマリとして検出する

- エンドポイントセキュリティ
  - EPP+NGAVで可能な限りマルウェアから防御
  - どうしても漏れてしまうものはEDRで検知、対応

⇒ 境界線内、リモート環境で同様に対策できることが肝要

エンドポイントセキュリティの分類

- EPP (EndPoint Protection)
  - いわゆるアンチウイルスソフト
- NGAV (Next Generation AntiVirus)
  - FFRI yaraiをはじめとする振る舞い検知型・シグニチャレスのマルウェア対策ソフト
- EDR (Endpoint Detection and Response)

ただし・・・

- 多機能なEDRは、高度なセキュリティスキルを持った人材が運用する必要があることに留意

リモート環境におけるセキュリティ

- リモート環境の端末
  - BYOD
  - 会社貸与のPC端末
- これらをリモートでセキュリティ管理する必要性
  （インシデントは必ず発生するため）
  - MDM (mobile device management)
  - リモートからのThreat hunting
  - 検知後の駆除または隔離
  - リモートフォレンジック、詳細調査
- インシデントが発生した場合の対応範囲と深度を予め想定
- 逆算して、EDRに求める機能を決定する

ゼロトラストおけるエンドポイントセキュリティ

- EPP＋NGAVで、侵入する脅威を最小化する
- EDR：上記をすり抜けてきたものを事後検知

- EPP, NGAV, EDRそれぞれの機能を組み合わせた製品は存在するが、搭載する機能名が同じでも、その性能が同じとは限らない。

FFRI yarai が持つゼロトラスト実現機能

- EPP
  Windows Defenderとの連携機能強化(v3.4)
- NGAV
  FFRI yaraiが最も強みとする「先読み型」検出技術の数々
- EDR
  脅威の検索・駆除・端末隔離

実績あるNGAV機能＋Windows Defender連携管理
により、脅威の侵入を最小限にとどめ、シンプルな
EDR機能により運用負荷が少ないインシデント対応を実現。