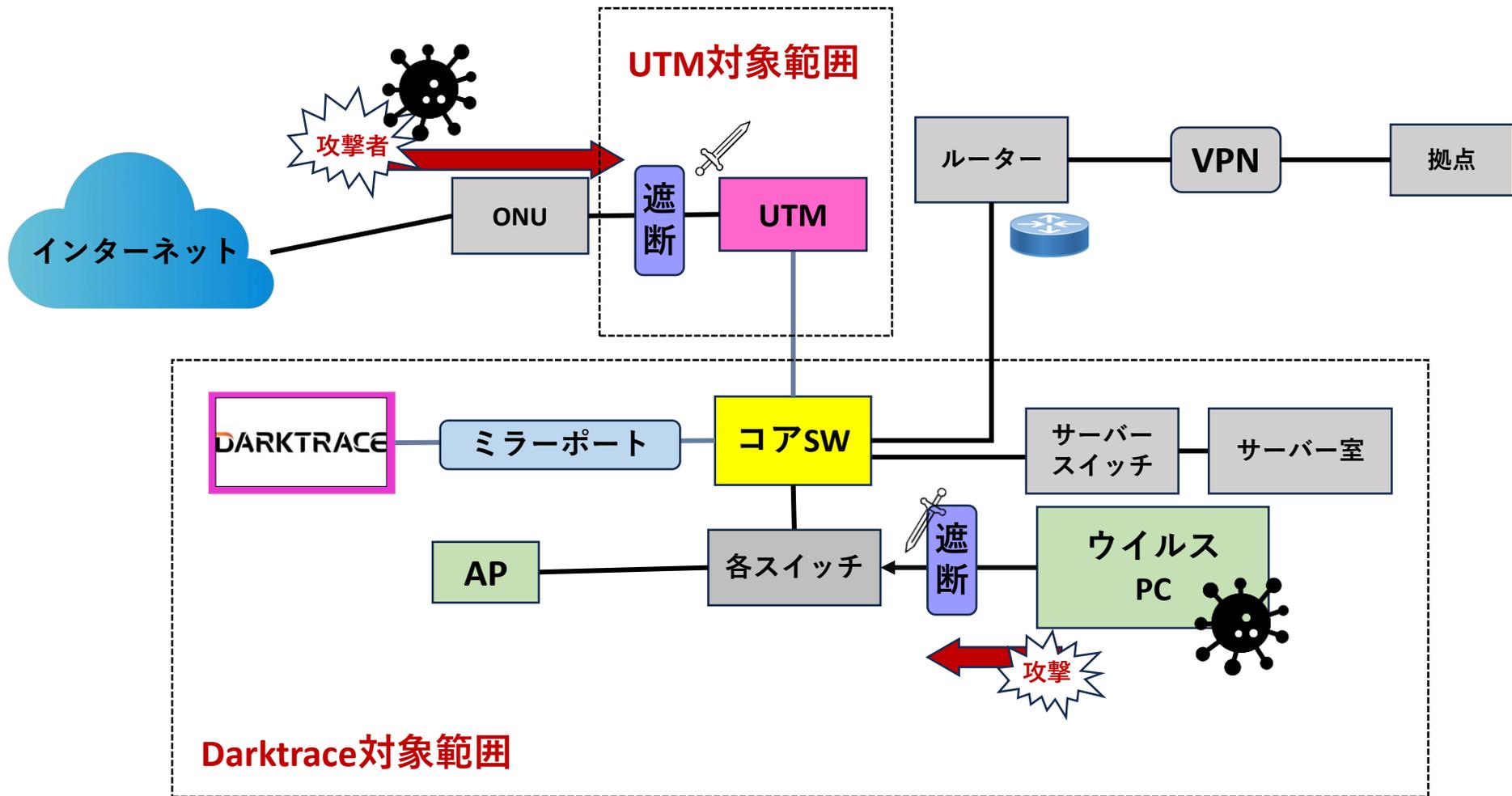




セキュリティ UTM・Darktrace

2025年8月



NDR(Network Detection and Response)

ネットワークの脅威をリアルタイムで検知し迅速に対応するセキュリティソリューション

製品名：  **DARKTRACE**

EDR(Endpoint Detection and Response)

PCやサーバーなどのエンドポイントにおける不審な動きを検知し迅速な対応を支援するソリューション

製品名：  **CROWDSTRIKE**



UTM(Unified Threat Management)

複数のセキュリティ機能を一つの機器で運用管理し、包括的に社内ネットワークを保護する製品

製品名：  FortiGate  **YAMAHA**

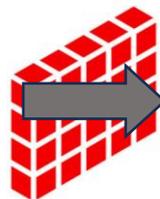
機能比較表

| | UTM（総合脅威管理） | Darktrace |
|------|-------------------|-----------------|
| 基本機能 | ファイヤーウォール、IPS/IDS | ネットワーク異常検知、自動防御 |
| 対応範囲 | ネットワークの入口・出口 | 内部ネットワーク |
| 防御方法 | 通信遮断、パケット破棄 | IPベースの通信遮断、自動隔離 |

使い分けイメージとしては...



すり抜けて
しまった場合



対応範囲が別なので併用導入することでセキュリティ度が上がる

EDR導入メリット

 FortiGate

 YAMAHA

一括管理による
運用不可軽減

院内の複数拠点やネットワーク機器を
まとめてセキュリティ管理できる

医療機器や
電子カルテの
入口防御

外部からの攻撃を入口で遮断し、
医療機器や院内システムを保護

コスト
パフォーマンス

多機能を1台で提供するため、
中規模病院でも導入しやすい

NDR導入メリット

DARKTRACE

未知の脅威、
内部異常に強い

医療機器や電子カルテに潜む
マルウェアを**早期発動**

内部ネットワーク
監視可能

UTMをすり抜けた攻撃や、
職員の誤操作による**感染拡大も発見可能**

可視化・分析が
容易

どの機器・ユーザーが異常か
一目で把握できる。