次世代のセキュリティ対策について

2022年1月13日

Thelemaassist

次世代のセキュリティ対策～ゼロトラスト～

働き方改革や新型コロナウイルス感染によりリモートワークが加速度的に推進され、サイバー攻撃が高度になり、従来の境界防御型セキュリティでは対策が難しくなっています。

そのため **「ゼロトラスト」** を考慮したシステムの構築が必要になってきています。

- ●徹底したID&アクセス管理：IAM（Identity and Access Management）
- ●緻密なデバイス管理： EDR（Endpoint Detection and Response）
- ●継続したふるまい分析と信頼度設定：UEBA（User and Entity Behavior Analytics）

大項目	小項目	境界防御	ゼロトラスト
資産	守るべき情報資産	境界内部に	どこでも
	利用者アクセス	境界内部から	どこでも
脅威	脅威・攻撃者	境界の外に留める	どこでも
	攻撃者初期目的	境界内に入る	なりすまし
対策	安全性の拠り所	境界防御	緻密なアクセス管理
	安全性の確認	基本、出入り	常に
	防御のコア技術	FW・VPN	IAM・**EDR**・UEBA
利便性	働く環境	境界内のみ	世界中どこでも
	勤務時間	営業時間	いつでも
	企業間コラボ	考慮なし	考慮あり

EDR(Endpoint Detection and Response)とは

エンドポイントの監視を行い、攻撃を発見次第対処するセキュリティソフトウェアの総称

エンドポイントにおけるシステムのアクティビティとイベントを記録し、

セキュリティチームがインシデントを発見するのに必要な**可視性**　と

悪質な振る舞いに対して　**高度な対応**　を提供するということです。

◆EDRセキュリティの重要な側面（Gartner社）

- インシデントデータの検索および調査
- アラートのトリアージまたは不審なアクティビティの検証
- 不審なアクティビティの検知
- 脅威ハンティングまたはデータ探索
- 悪質なアクティビティの阻止

なぜEDRが注目されているか