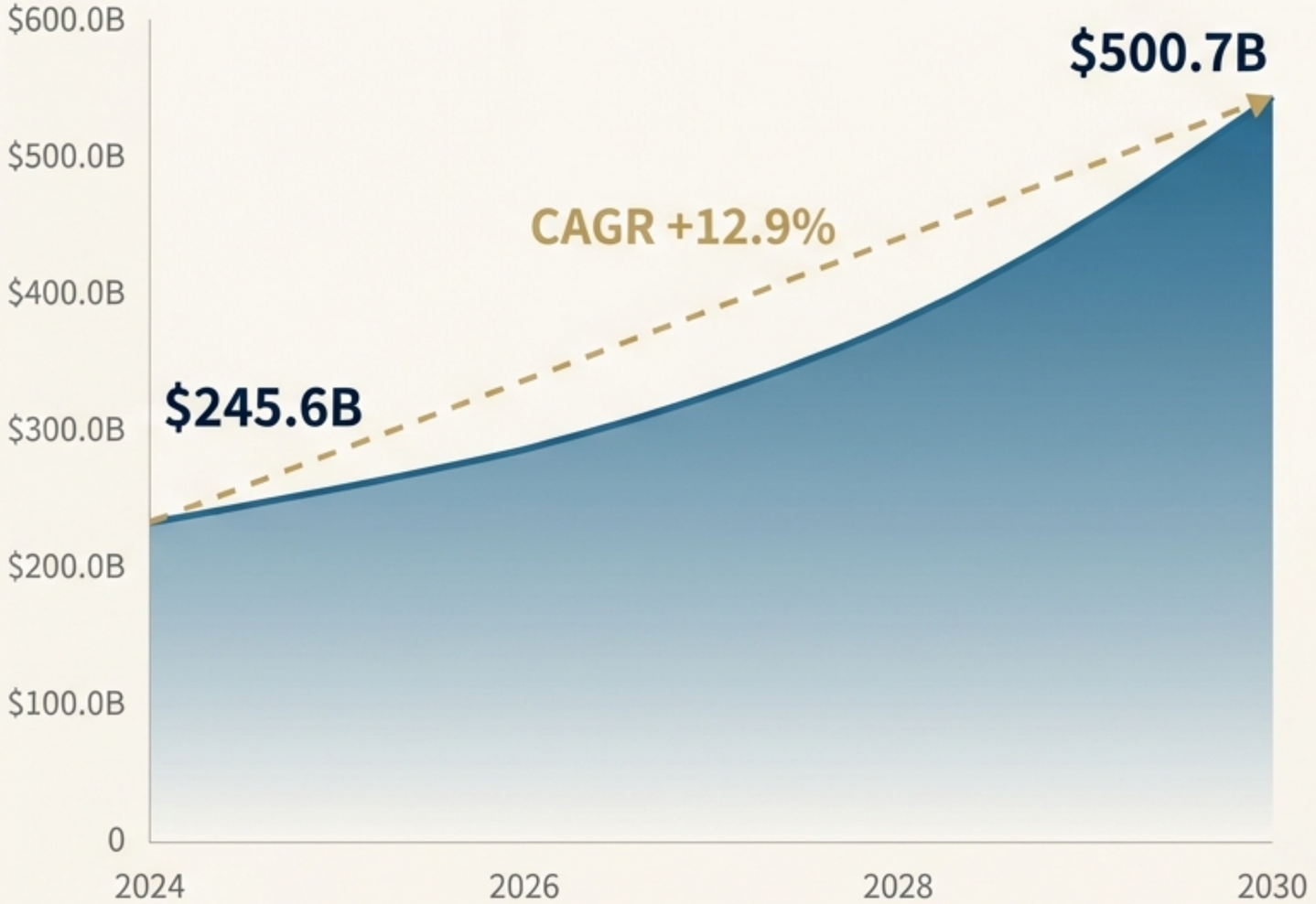
サイバーセキュリティ市場における新たな勝機：3つの戦略領域への資源集中による事業拡大

経営陣向け戦略提言

本レポートは、サイバーセキュリティ市場の構造変化を分析し、自社の強みを最大化する3つの高成長領域を特定、そこへの資源集中を提言するものです。

サイバーセキュリティ市場は2030年に5,000億ドルへ倍増。構造的な追い風が、後退不能な成長を確約する



出典: Grand View Research (2024), Mordor Intelligence (2024)

DXとクラウド移行の加速

全てのビジネスプロセスがデジタル化し、従来の境界型防御が崩壊。市場のCAGRを+2.1%押し上げる最大の要因。

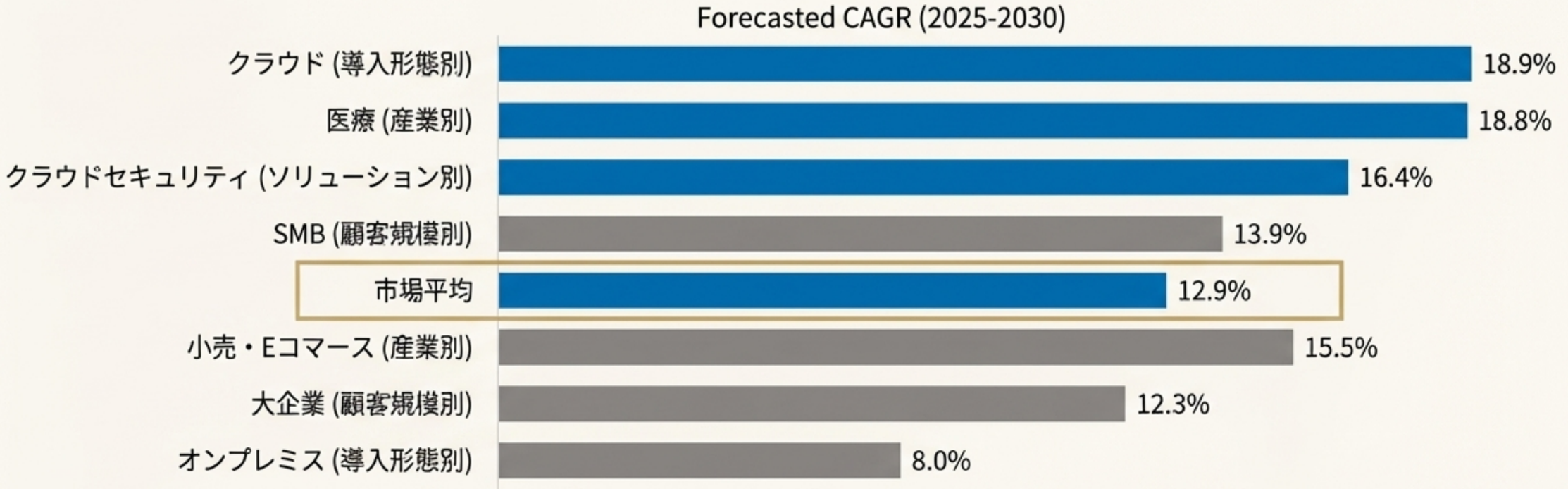
サイバー攻撃の高度化・頻発化

国家関与のAPT攻撃やRaaS（サービスとしてのランサムウェア）が常態化し、防衛投資を半ば強制的に引き上げ。

世界的な規制強化

GDPRやNISTフレームワークがセキュリティ対策を法的に義務化。サイバーセキュリティはITコストから経営リスクへ変貌。

市場成長を牽引するのは「クラウド」と「SMB」。特にクラウド関連セグメントは年率18%超の爆発的成長を示す



見出すべき機会

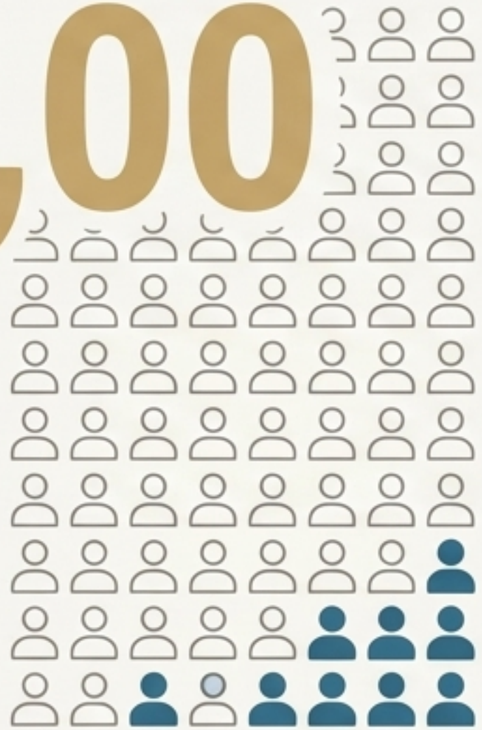
市場の未来はクラウドにあり、これまで未開拓だったSMB市場が次の成長エンジンとなる。この２つの交差点に最大の事業機会が存在する。

出典: Mordor Intelligence, Fortune Business Insights, Grand View Research (2024)

業界最大の課題は480万人に達する深刻な人材不足。この構造的ボトルネックが、新たな需要を創出している

4,800,00

UNFILLED CYBERSECURITY ROLES



出典: DeepStrike (2024), Bureau of Labor Statistics (2024)

1. 深刻な人材不足と人件費高騰

米国の情報セキュリティアナリストの給与中央値: **$124,910**

↓

2. 企業の自社運用が困難に

人材不足の企業はデータ侵害時の平均コストが**$176万**増加

↓

3. 2つの巨大な需要が誕生

→ AIによる自動化

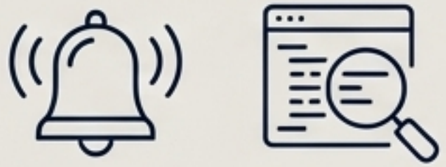
人間の作業を代替する SOARや自律運用AIへの需要

→ 専門サービスのアウトソース

専門家チームを外部から調達するMDR/MSSPへの需要

AIが主戦場を「侵入後の対応」から「脅威発生前の予防」へシフトさせる。競争のルールが変わり、データが勝敗を決する

旧パラダイム：検知・対応
(Detection & Response)



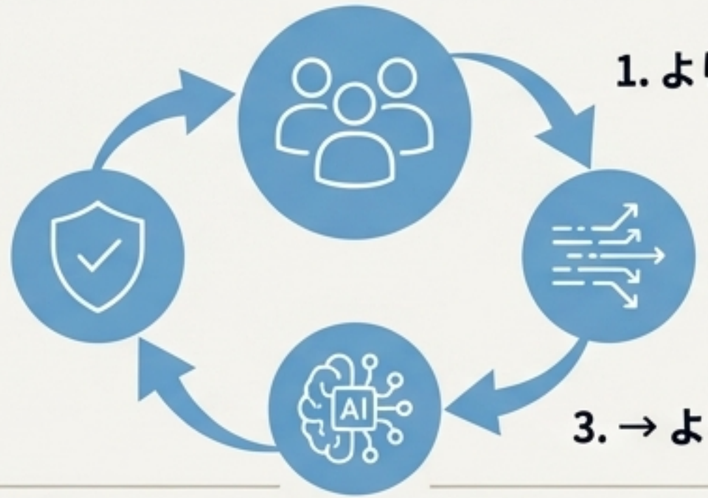
50%

「2030年までに、ITセキュリティ支出の**50%**がAI主導の予防的ソリューションへと移行する」
- Gartner

新パラダイム：予測・予防
(Preemptive Security)

データ・ネットワーク効果

効果的なAIは、学習データの量と質に性能が依存する。



1. より多くの顧客

2. → より多くの脅威データ
(例: CrowdStrikeは1日1兆件のイベントを処理)

3. → より高精度なAIモデル

4. → より強力な防御力

このサイクルは、データを統合管理できる大規模プラットフォームベンダーに圧倒的優位性をもたらし、ポイントソリューションの淘汰を加速させる。

出典: Gartner (2025), CrowdStrike (2021)

攻撃者もAIを悪用。従来の「人間による防御」は限界を迎え、技術的な制御が不可欠に

生成AIによるフィッシング

文法的に完璧で、標的に高度にパーソナライズされたメールを大量生成。

ある調査では、生成AI登場後、フィッシング攻撃が4,151%も急増。

AIフィッシングのクリック率は54%（人間作成のメールは12%）。

ディープフェイク音声詐欺（Vishing）

経営幹部の声をAIで模倣し、偽の指示で従業員に送金させる詐欺が現実の脅威に。人間による見分けは極めて困難。

Strategic Implication

「怪しいメールを見分ける」といった従業員教育の効果は無効化される。「人間は必ず騙される」という前提に立ち、多要素認証（MFA）やゼロトラスト・アーキテクチャといった技術的制御への投資が、より重要になる。

出典: DeepStrike (2025), Abnormal AI

SMBは最も脆弱で、最も対策が遅れている巨大市場。膨大な「セキュリティ負債」が、MDRサービスの機会を生む

脆弱性（High Risk）

全サイバー侵害の**46%**が従業員1,000人未満の企業で発生。攻撃者の主要ターゲット。

＋

リソース不足（Low Resources）

予算の制約。専門人材の不在（IT担当者が兼務）。

＝

結果 (The Outcome)

対策が遅れ、知らず知らずのうちに膨大な「セキュリティ負債」を蓄積。いずれ事業停止につながる時限爆弾となっている。

The Unmet Need

SMBが真に求めているのは、個別のツールではない。「導入が容易」で「運用負荷が低く」「コスト効率が高い」、専門家が脅威の検知から対応までを代行してくれる**「安心」**というサービス。

このニーズは、マネージド・ディテクション＆レスポンス（MDR）にとって持続可能で巨大な市場機会を意味する。

出典: StrongDM (2025), Integrity360 (2025)

DXの波が、これまで隔離されていたOT領域に到達。
社会インフラを標的とする、新たなブルーオーシャン市場が誕生

What is OT Security?

- 工場の生産ライン、電力網、交通システムといった重要インフラを制御する技術（OT）をサイバー攻撃から保護する領域。
- DXの進展により、これらのOTシステムがインターネットに接続され、新たな攻撃対象領域（アタックサーフェス）となっている。

Market Opportunity

High Stakes: 侵害は、物理的な破壊や社会インフラの停止といった深刻な事態を招く。

High Growth: OTセキュリティ市場は2030年に**615億ドル**（CAGR 18.2%）へと急成長。

Blue Ocean: ITとは異なる専門性が求められるため、既存のITセキュリティ大手もまだ確固たる地位を築けておらず、新規参入の余地が大きい。

出典: Grand View Research (2024)

市場の構造変化を捉え、持続的成長を実現するため、我々は3つの戦略領域に経営資源を集中させる

1. AIドリブン・クラウドセキュリティ (AI-Driven Cloud Security)

市場で最も成長率の高いクラウド領域で、AIによる「予測・予防」を武器にリーダーシップを確立する。

2. SMB向けMDRサービス (SMB MDR Services)

人材不足という巨大なペインポイントに応え、安定したリカーリングレベニューを構築する。

3. OTセキュリティ (OT Security)

専門性が高く未開拓なブルーオーシャン市場で、先行者利益を獲得する。

1 / 機会1: AIドリブン・クラウドセキュリティ – 自社技術(Build)を核に、戦略的買収(Buy)で市場投入を加速する

なぜこの領域か？ (The Opportunity)

- **市場の魅力:** 市場で最も高い成長率(**CAGR 16.4%**)を誇るセグメント。
- **トレンドとの合致:** AIを活用し、クラウドの設定ミスを自動で予防・修正するCNAPP/AI-SPMは、「予防的セキュリティ」へのシフトという最大の潮流と完全に合致。
- **強みの活用:** 自社が保有するAI技術とクラウドインフラの知見を直接活かせる。

どのように実行するか？ (The Strategy)

BUILD（中核戦略）:

アクション: 既存のAI技術を応用し、主要クラウド（AWS, Azure, GCP）に対応したCNAPP（Cloud Native Application Protection Platform）を自社開発する。

理由: コア技術の優位性を確立し、自社プラットフォームの基盤とするため。

BUY（加速戦略）:

アクション: データセキュリティ態勢管理（DSPM）など、特定の補完技術に強みを持つAIネイティブ・スタートアップを買収する。

理由: 開発時間を短縮し、いち早く市場での競争力を確保するため。

2 機会2: SMB向けMDRサービス – 自社プラットフォーム(Build)とパートナー網(Partner)の組み合わせで巨大な未充足ニーズを攻略する

なぜこの領域か？ (The Opportunity)

- **市場の魅力:** 人材不足により、セキュリティ運用のアウトソース需要が爆発的に増加。
- **ビジネスモデル:** 成果ベースのサービス提供により、安定的かつ高収益なリカーリングレベニュー（継続収益）を構築可能。
- **アンメットニーズ:** 「低コスト」「簡単」「運用代行」を求めるSMBの巨大な未充足ニーズに直接応える。

どのように実行するか？ (The Strategy)

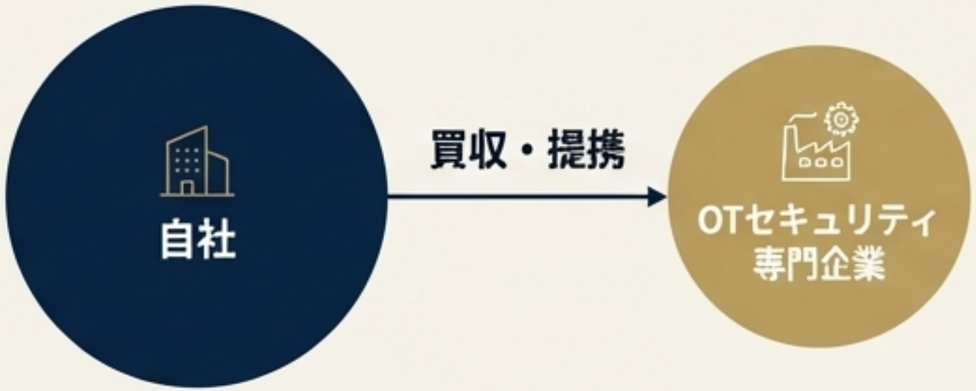
BUILD（技術の核）:
アクション: 脅威の検知・分析・対応のハブとなる、高効率なXDRプラットフォームを自社開発する。
理由: サービス品質の根幹をなし、技術的優位性の源泉となるため。

PARTNER（市場への浸透）:
アクション: 全国のSMB顧客基盤を持つ既存のMSSPやITサービスプロバイダーと提携する。
理由: 広範なSMB顧客へのリーチと、地域に密着したサポート体制を迅速に確立するため。自社単独での開拓は非効率。

機会3: OTセキュリティ – 専門企業の買収(Buy)または提携(Partner)により、成長著しいブルーオーシャン市場へ最速で参入する

なぜこの領域か？ (The Opportunity)

- **市場の魅力**
  - CAGR 18.2%と高い成長率を誇り、社会インフラを守るというミッションクリティカルな領域。
- **競争環境**
  - 専門性が高く、ITセキュリティの巨人もまだ支配的地位を確立していない「ブルーオーシャン」。
- **参入障壁**
  - 独自のプロトコルや制約があり、後発でも専門性を確保できれば高い参入障壁を築ける。



どのように実行するか？ (The Strategy)

- **BUY or PARTNER (最優先戦略):**
  - **アクション**
    DragosやClarotyといった、市場で評価を確立しているOTセキュリティ専門のスタートアップを買収、または資本業務提携を行う。
  - **理由**
    ゼロからの開発は時間がかかりすぎる。買収・提携は、実証済みの技術、専門知識を持つ人材、そして既存顧客を一挙に獲得する最も効率的な手段。

実行計画：3つのフェーズで事業基盤を構築し、サイバーセキュリティ市場のリーダーを目指す

Phase 1: 短期（～1年）- 基盤構築と市場への足掛かり

- サイバーセキュリティ専任事業部門の設立
- M&A/提携候補のリストアップと交渉開始
- クラウドセキュリティ(CNAPP)のプロトタイプ開発着手

Phase 2: 中期（1～3年）- 事業の本格展開とプラットフォーム統合

- 戦略的M＆Aの実行とPMI（統合プロセス）
- パートナー経由でのSMB向けMDRサービス市場投入
- クラウドからOTまでをカバーする統合プラットフォームの発表

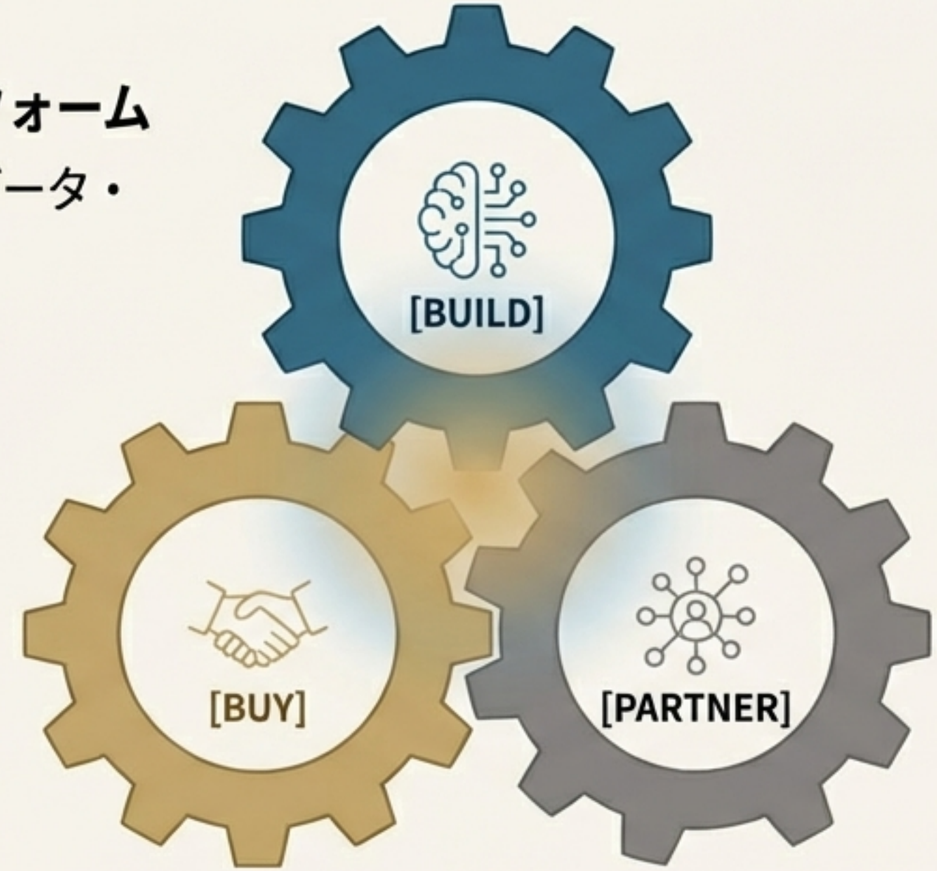
Phase 3: 長期（3年～）- リーダーシップの確立と次世代への投資

- グローバル展開（特にアジア太平洋市場）の加速
- サードパーティ向けエコシステムの拡充
- 耐量子コンピュータ暗号(PQC)など次世代技術へのR&D投資

我々の勝利の方程式：自社開発(Build)、戦略的買収(Buy)、パートナー網(Partner)の融合が、模倣困難な競争優位性を確立する

[BUILD]
独自開発のAIデータプラットフォーム

競争の核となる技術的優位性とデータ・ネットワーク効果を確保。



[BUY]
最先端技術の戦略的買収

市場投入までの時間を短縮し、OTセキュリティなどの専門領域における深い知見を獲得。

[PARTNER]
強力なチャネルパートナー網

自社だけではリーチできないSMB市場へ迅速に浸透し、顧客との信頼関係を構築。

この三位一体のハイブリッドアプローチこそが、急速に変化するサイバーセキュリティ市場において、我々が新たなリーダーとなるための最も確実な道筋です。