株式会社ラック

# 中期経営計画

## （2024-2026年度）

2024年5月13日

# 前中期経営計画の振り返り

# 前中期経営計画目標値との差異

## 計画時点からは伸長したものの、事業機会やM&Aなど成長投資の創出の遅れ、生産性改善の遅れなどから目標値に対して下回る

| 科目 | 2020年度 | 2023年度<br>中期経営計画目標 | 2023年度 | 増減 | |
|---|---|---|---|---|---|
| | | | | 2020年度対比 | 目標対比 |
| 売上高 | 436億円<br>ｾｷｭﾘﾃｨ事業 186億円<br>SI事業 250億円 | 550億円<br>ｾｷｭﾘﾃｨ事業 255億円<br>SI事業 295億円 | 494億円<br>ｾｷｭﾘﾃｨ事業 221億円<br>SI事業 273億円 | +57億円<br>(+13.2%) | △55億円<br>(達成率90.0%) |
| 営業利益 | 21億円 | 30億円 | 21億円 | +0億円<br>(+2.7%) | △8億円<br>(達成率72.5%) |
| ROE | 2.6% | 10%以上 | 9.1% | +6.5P | △0.9P |

# 前中期経営計画の進捗状況

## 主な成果

**1 耐久力**

- セキュリティ対策の認知度をもとに、個別監視サービスを軸とした高付加価値サービスやリカーリング案件の拡大

**2 適応力**

- 自動化×ノウハウによる診断サービスの拡大
- AIを活用した金融犯罪対策ソリューション展開

**3 デジ力（りょく）**

- テレワーク勤務体制を踏まえた社内IT環境×ゼロトラストの推進
- 生成AIの自社開発と社内活用、外部への導入支援や診断などのサービス展開

## 課題認識

事業ノウハウをデジタル化したセキュリティ事業のサービス展開は道半ば

社内基幹システム開発の中止もあり経営のDX推進は大きく遅延

# 新中期経営計画

# ラックを取り巻く事業環境認識

## IT環境

### デジタル活用はより多様で広範囲に深く

システム間連携が浸透し、相互依存性がより複雑かつ深化
至る所でサイバーセキュリティが必須に

- ▶サイバーセキュリティはデジタル社会の基幹産業といえる
- ▶桁が違う水準でのセキュリティ人材の不足

### サイバー脅威がより深刻に

業務停止が現実的脅威に、金融犯罪も急拡大
AIなど先端テクノロジーの悪用（フェイク等含む）が顕著に

- ▶攻撃者以上のテクノロジー活用が必至

### 安全保障上の要求も高まる

社会基盤となったIT環境でビジネスや生活を行うために、
サイバー空間において自由主義・民主主義を守るための
安全保障の観点が必須に

- ▶サイバーセキュリティが安全保障の要となる

## 社会（お客様）の課題

### デジタル活用に見合った費用対効果の追求

- ▶AIや自動化による対策の効率化
- ▶わかりやすく求めやすい対策

### 複雑化・高度化する脅威への対抗

- ▶点（個別対策）から線や面（総合対策）へ
- ▶高度な金融犯罪対策の要請

### サプライチェーン全体のレジリエンス確保

- ▶中堅・中小企業へのセキュリティ対策
- ▶海外拠点のセキュリティ対策
- ▶業務停止への考慮と対策

### セキュリティ対策の継続性担保

- ▶デジタル・セキュリティ投資戦略の策定と継続運用

### 経済安全保障の担保

- ▶重要インフラ事業者へのサプライチェーン対策
- ▶海外でも通用するセキュリティベンダー

# 社会の課題に対するラックへの要請

約30年にわたり磨き続けてきた現場経験からの知見をもつ（インテリジェンス）

## サイバーセキュリティ対策の専門集団として

**自動化・AIを活かした対応**

AI活用により人のノウハウをデジタル化し
高度で費用対効果の高いサービスを提供

**総合サービス力による対応**

従前以上に複雑化・高度化するサイバー脅威に
ワンストップで最適なサービスを提供

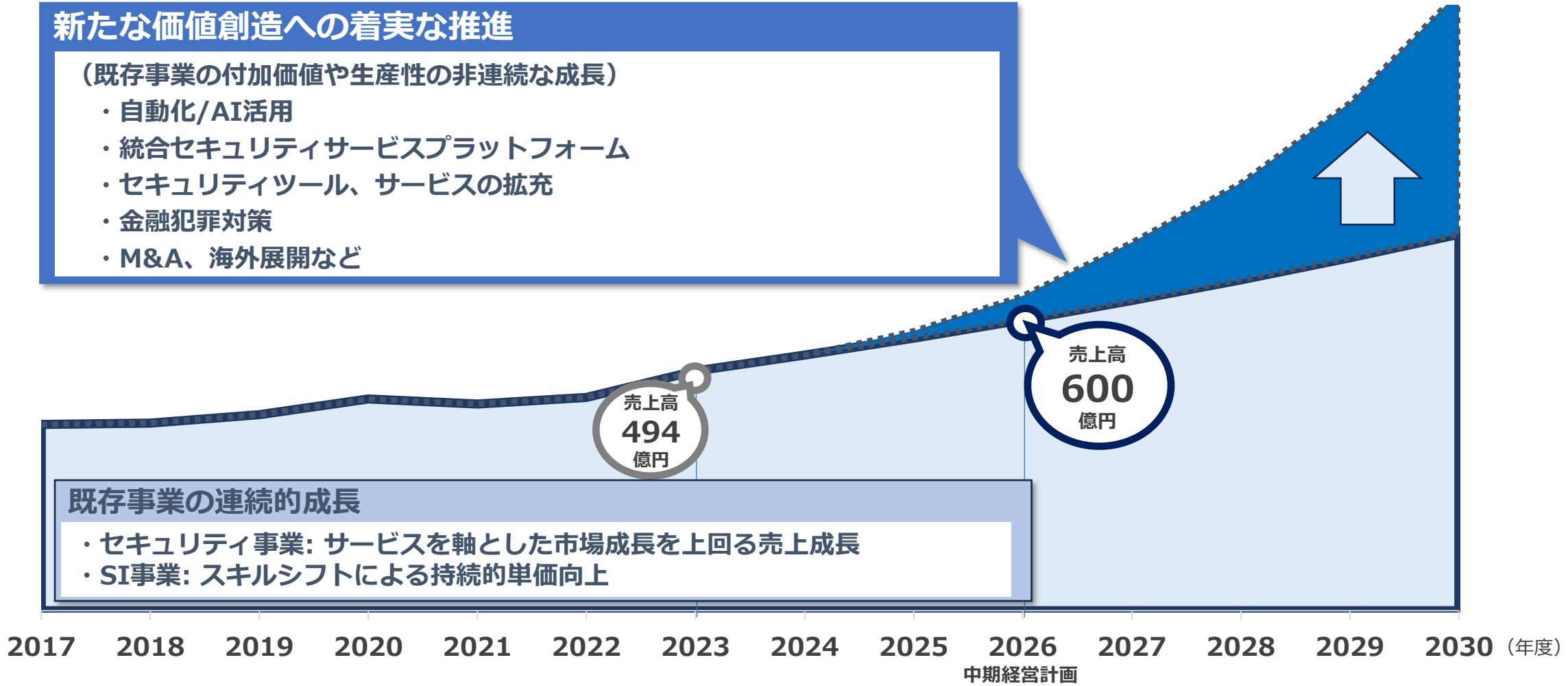
中堅・中小企業の対策につながるサービス提供

**セキュリティ・SI事業の付加価値をさらに向上させ**

**中長期的な観点で新たな価値創造を推進**

# 中長期的な価値創造に向けて

## 中期経営計画目標値は既存事業の連続的成長を軸に設定し
## 中長期施策によりさらなる成長を目指す



# 新中期経営計画目標値

## 売上高600億円、営業利益・経常利益40億円、 ROE 15%を目標
## 中長期施策により上積みを目指す

## 株主還元は引き続きDOE 5%を基本指標として配当する方針

| 科目 | 2023年度 | 2026年度<br>中期経営計画目標 | 増減 | |
|---|---|---|---|---|
| | | | 額 | 率 |
| 売上高 | 494億円 | 600億円 | +105億円 | +21.3%<br>(年平均+6.6%) |
| 営業利益 | 21億円 | 40億円 | +18億円 | +83.9%<br>(年平均+22.5%) |
| 営業利益率 | 4.4% | 6.7% | +2.3p | - |
| 経常利益 | 21億円 | 40億円 | +18億円 | +87.6%<br>(年平均+23.3%) |
| ROE | 9.1% | 15.0% | +5.9P | - |

### 株主還元

中長期的な視点に立った投資やキャッシュ・フローの状況を勘案のうえ利益配分を実施

**DOE（株主資本配当率）**

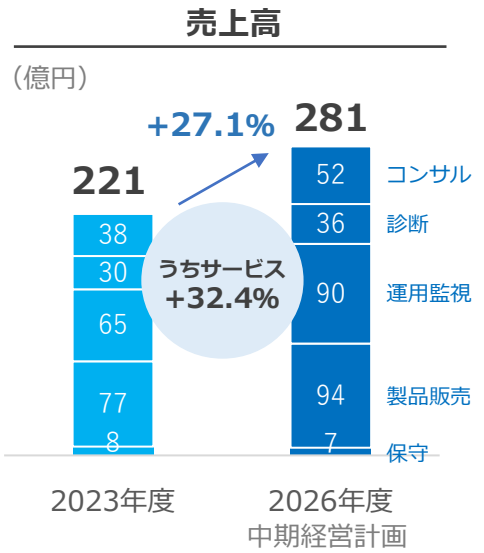
**基本指標 5%**

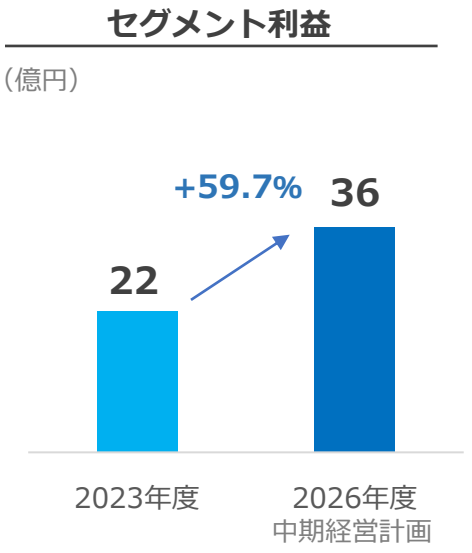
# 新中期経営計画 既存事業-セグメント別

## セキュリティ事業

### 運用監視を軸としたサービス事業拡大

- リカーリング増大によるコンサルティング案件の拡大
- 対応力強化による大規模の緊急対応サービス案件の拡大
- エンジニアと自動化のバランスを最適化した診断サービス案件の拡大
- 個別監視を切り口にした総合的・包括的な運用監視サービス案件の拡大
- 製品ベンダーとの継続的な連携とコンサルカによる製品販売の大規模案件拡大

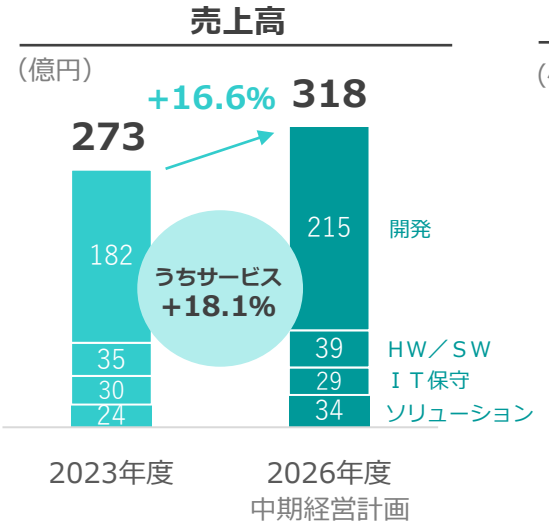


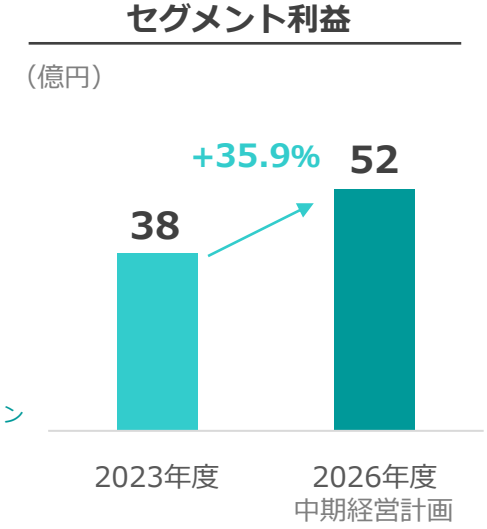




## SI事業

### 高単価案件へのスキルシフト推進

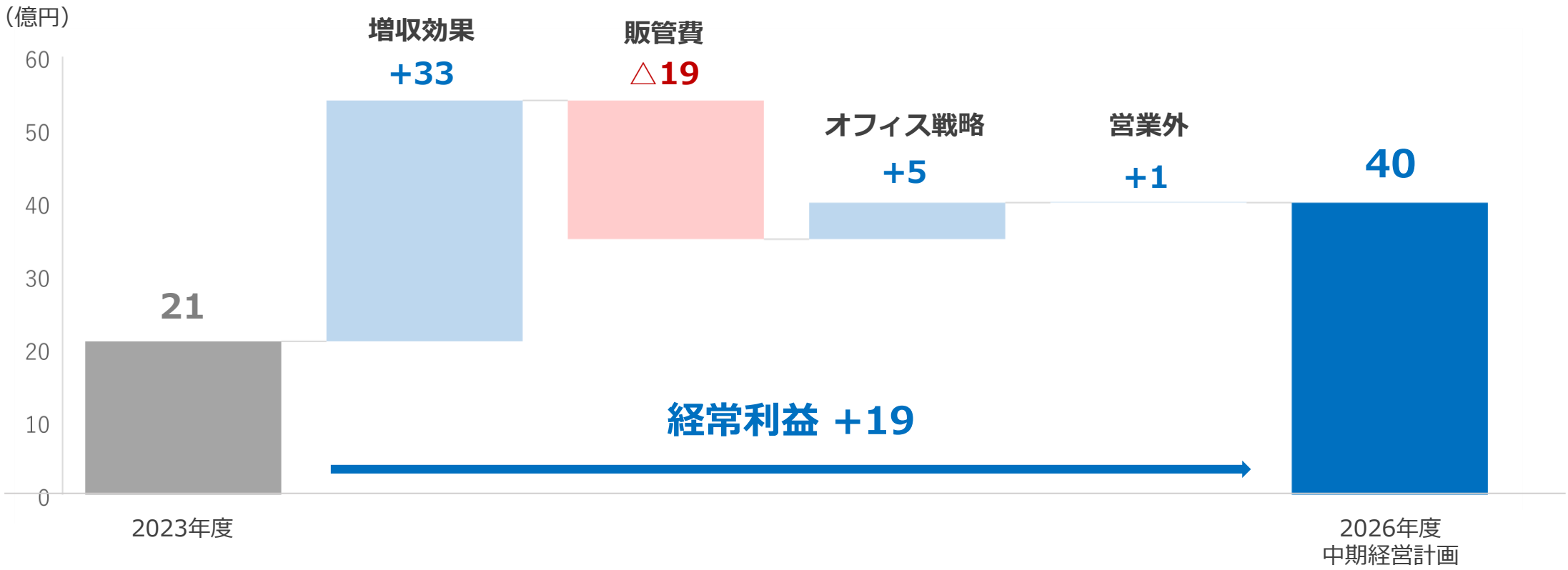
- ソリューションをもとにした特定技術領域へのスキルシフトによる高単価システム開発案件の拡大
- オンプレミス回帰などの顧客需要に対するHW/SW・保守の一定案件の確保
- 特定技術領域のもととなるサブスクリプション型ソリューションの継続拡大



# 新中期経営計画 経常利益 増減要因分析

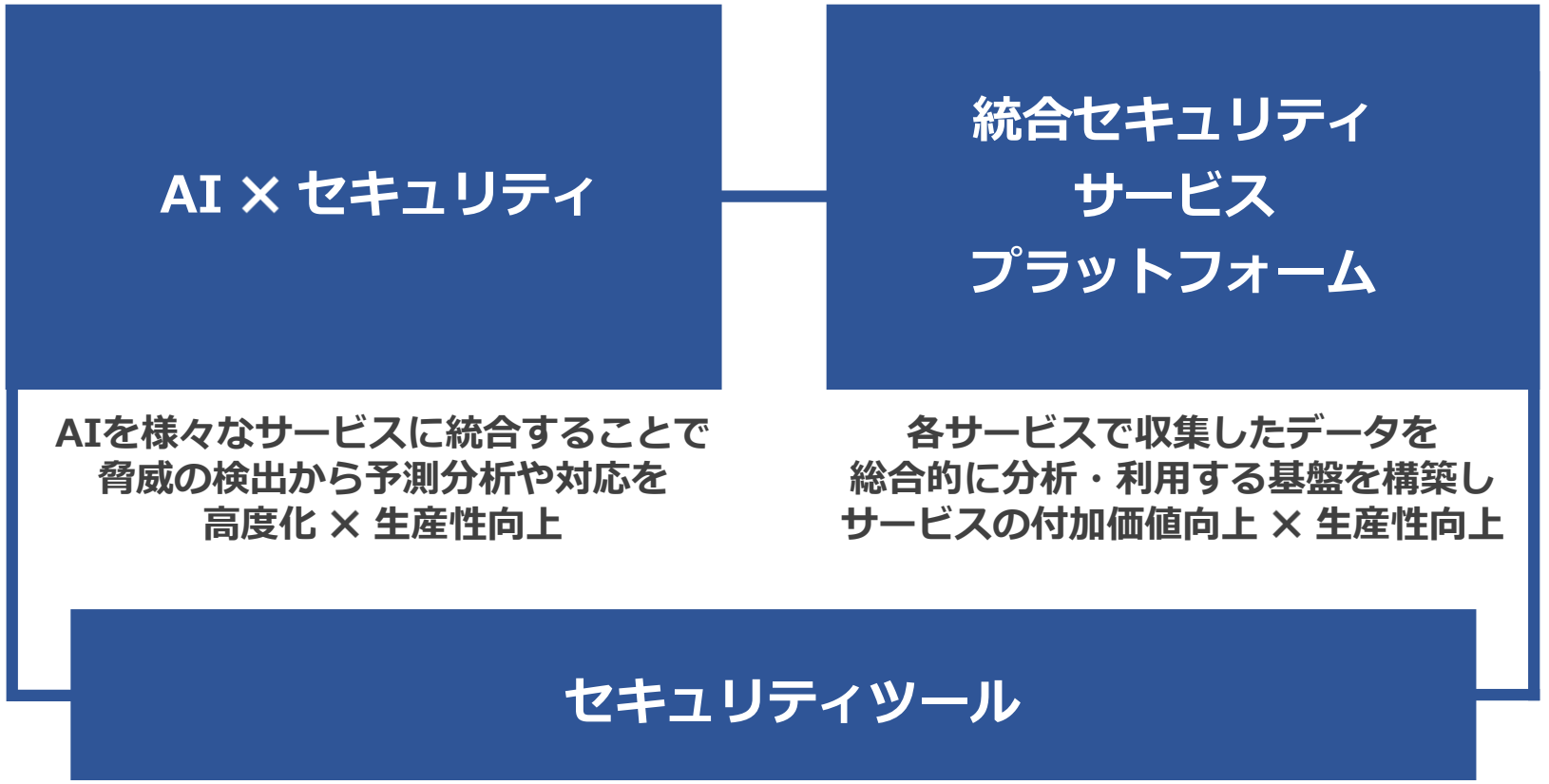
## 販売体制強化を軸とした販管費の増加等による費用増を見込むものの
## 増収効果やオフィス戦略による費用削減効果などにより経常増益を予想




（注）オフィス戦略の費用は販管費に含まれますが、グラフでは抜き出して表記しています。

# 新たな価値創造への着実な推進

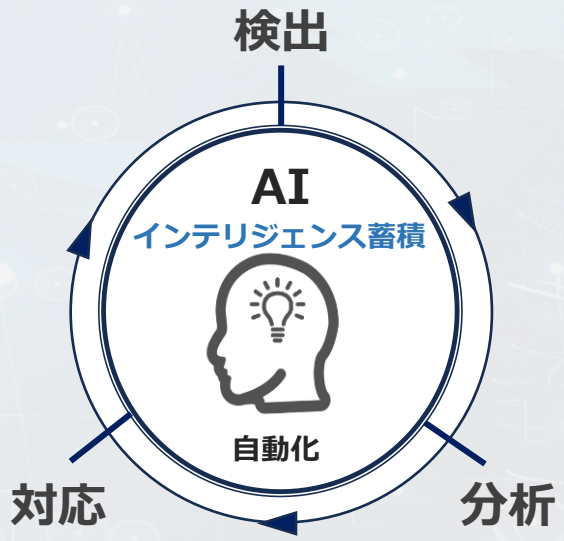
## AIとエンジニアリングを組み合わせ、セキュリティサービスの付加価値や生産性を向上
## 世界に通用するセキュリティツールへの挑戦




セキュリティツールベンダーとの戦略的連携も視野に世界に通用するツールの獲得

# ＡＩ×セキュリティ

## 人による対応をＡＩ・自動化によりサービスの高度化と急拡大するニーズに対応
## 市場競争力強化とともに費用対効果の高い新サービスにより中小企業向けにも対応




**優位性を確保する**
**大手企業を軸とした高い実績**

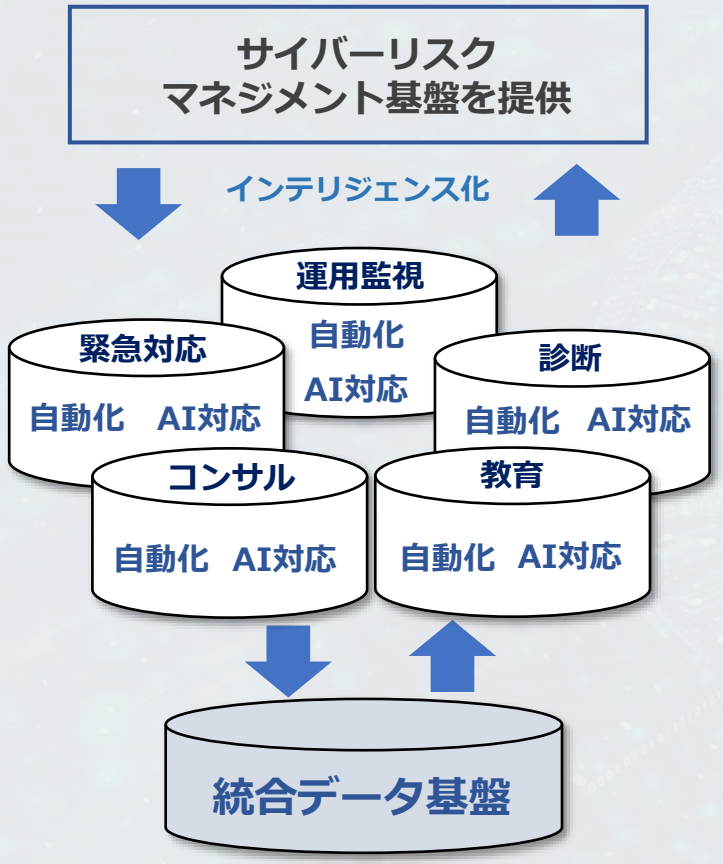
・JSOC顧客数　約1,000社
・診断実施数　累計約27,500件
・緊急対応件数　累計約4,800件

### サービスポイント（提供価値）

- 大量に蓄積されている脅威データを高度分析
- 人手で行っている対応をAI／自動化により生産性向上
- 巧妙化・深化する攻撃への新たな分析手段を開発
- 自動化によって費用対効果の高い新サービス開発につなげ
  中小企業向けにも対応したサービスを提供

# 統合セキュリティサービスプラットフォーム

## 運用監視からサイバーリスクマネジメントへと昇華
## 各種セキュリティサービスのデータ分析・活用基盤を統合




### サービスポイント（提供価値）

- ネットワーク、アプリケーション、端末などに分断されているサイバーリスクを統合し可視化
- 様々なツールを導入しているお客様へ統合したプラットフォームを提供し利便性を向上
  （ツール例：SASE、UEBA、CASB等）
- 統合データ基盤による知見を活用しお客様に最適な対策を提供
- 大規模グループ企業にも提供予定

SASE：Secure Access Service Edge、UEBA：User and Entity Behavior Analytics、
CASB：Cloud Access Security Broker

# セキュリティツール

## 約30年に及ぶ現場経験からのインテリジェンスの知見を活かし
## 他社とのアライアンスを含めた新たなセキュリティツールの獲得を推進

### アライアンス推進例

**運用監視**

AI・自動 × 脅威情報
（NRI社との合弁会社）

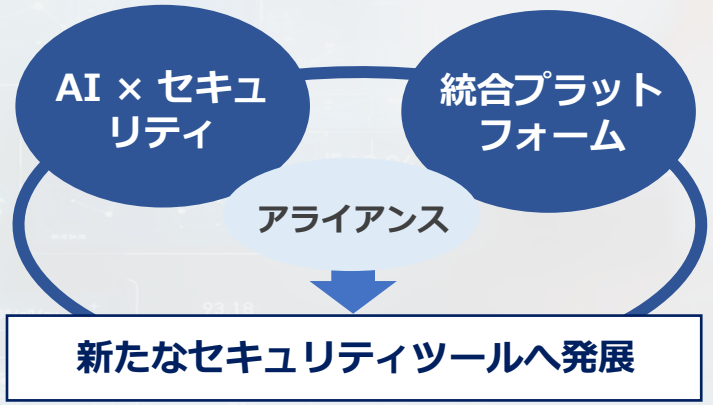
**診断**

AI・自動 × ノウハウ
（エーアイセキュリティラボ社と協業）

### 自社開発ツール例

マルウェア調査ツール
「FalconNest」

PC自己診断ツール
「自診くん」




### サービスポイント（提供価値）

- AI × セキュリティ、統合セキュリティサービスプラットフォームなどの脅威情報と連携したセキュリティツールの獲得

  自社開発だけでなく、戦略的提携や買収も選択肢

- 中堅・中小企業向けのセキュリティ市場にも展開

  領域を広げてインテリジェンスを蓄積しサービスをさらに高度化

# ラックが掲げるパーパス・ビジョン

## Purpose

## たしかなテクノロジーで「信じられる社会」を築く。

デジタル社会はより高度化・複雑化するなか、
私たちは練度の高い多様なテクノロジーを駆使して安心安全な社会基盤を築き、
人々が互いを支え合い、笑顔でいられる社会を実現します。


## Vision

## デジタル社会を生き抜く指針となる。

サイバーセキュリティをリードしてきたパイオニア精神を絶やさず、
深化・高度化するデジタル化社会における人々のいとなみを守り、業界文化を牽引し、
新しい時代を生き抜く指針でありつづけます。

※本資料は2024年5月13日時点の情報に基づいて作成しており、記載内容は予告なく変更される場合があります。
※本資料において、セキュリティソリューションサービス（SSS）事業を「セキュリティ事業」、システムインテグレーションサービス（SIS）事業を「SI事業」と簡略化して表記しております。
※この配付資料に記載されている業績目標、将来の見通しなどの記述はいずれも、当社グループが作成時点で入手可能な情報を基にした予想または想定に基づく記述であり、これらは経済情勢や社会動向等の様々な経営環境の変化によって、直接・間接に影響を受けるものであり、実際の業績、戦略などは、この配付資料に記載されている予想または想定とは大きく異なる可能性があります。