GSX
GLOBAL
SECURITY
EXPERTS

事業計画及び成長可能性に関する事項

グローバルセキュリティエキスパート株式会社

2026年６月29日

Agenda

GSX
GLOBAL
SECURITY
EXPERTS

AI台頭時代の成長戦略

AI台頭によりセキュリティニーズが増大する構造的理由とGSXビジネスにもたらす影響

AIの進化はサイバー攻撃者をさらに有利にしている一方で、防御側はAIツールの導入だけで終わらない

企業はこれまでのセキュリティリスクに加え、AI導入に伴う新たなリスクが発生　さらに外部専門家への依存度が高まる

結果的にAIの台頭は当社にとって構造的な成長ドライバーとなる

すでにサイバー攻撃者がAIツールを活用、常に有利な状態に ＋ 企業がAIを導入することでのセキュリティニーズ拡大

- サイバー攻撃者もAIを活用
  攻撃の自動化、激化、巧妙化を助長
- セキュリティ対策はAIツールだけでは
  代替できない

- AI導入に伴い**新たなセキュリティリスクが発生**
  （AIの誤用、情報漏洩、ガバナンス不備 等）
- AIを安全に選定・運用・解釈・統制する難しさ
  外部専門家への依存が増加

AI台頭により
セキュリティニーズ
爆増

AI台頭は脅威ではなく

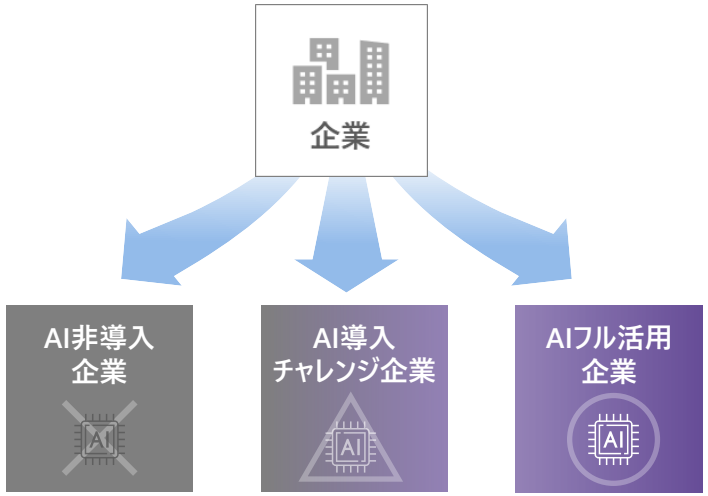
GSXのビジネスにとって強い追い風となる

GSXの考えるAI時代の戦略

GSXの顧客市場においては、AIの急速な進化に対する格差が生まれると予想

GSXは既存ビジネスの強みをAI時代にあわせて進化　すべての企業に寄り添うAI時代のセキュリティサービスを提供

顧客市場の変化とGSXグループの対応



AI導入がスムーズに進む企業とそうでない企業の格差

GSX

全てのコンディションの企業を支援するサービスラインナップ

GSXグループの強み

サイバーセキュリティ事業	準大手・中堅・中小企業を基本にした顧客基盤
セキュリティ教育事業	専門分野の教育講座開発・資格化のノウハウと実績
セキュリティ人材事業（CyberSTAR）	専門人材を育成して増やして提供する独自のビジネスモデル

GSXグループの強みをAI時代にあわせて進化
対応可能な市場を拡大していく

AI時代にあわせたサービス提供

各事業ごとに内側の効率化からAI活用サービスの創出、新規AIビジネスへの参入などの取組みを進める

	AIによる効率化と価格競争力強化	AIによる新サービス創出	セキュリティで実装するAI市場の開拓
	 筋肉質化	 新しい提供価値獲得	 新しい市場開拓
サイバーセキュリティ事業	既存セキュリティサービスの生産性向上	AIガバナンス体制構築 ISO42001（AIMS）認証取得支援 AIDR（AI攻撃検知・対応）サービス	セキュリティ前提のAI実装支援
セキュリティ教育事業	教育コンテンツ開発のスピード向上	AIセキュリティエンジニア セキュアAIエージェント実装講座 AIセキュリティパスポート	EC-Council COASP（AI攻撃・防御技術講座） セキュリティ＆AI講座（AI活用講座）
セキュリティ人材事業（CyberSTAR）	人材育成カリキュラム作成スピード向上	AIエンジニアの育成 セキュリティ×AIのキャリア創出	AIアバターを活用したエンジニアリングサービス 職種別、サービス別のAI最適人材の提供

AI時代にあわせたサービス提供

各事業ごとに内側の効率化からAI活用サービスの創出、新規AIビジネスへの参入などの取組みを進める

	AIによる効率化と価格競争力強化	AIによる新サービス創出	セキュリティで実装するAI市場の開拓
	筋肉質化	 新しい提供価値獲得	 新しい市場開拓
サイバーセキュリティ事業	既存セキュリティサービスの生産性向上	AIガバナンス体制構築 ISO42001（AIMS）認証取得支援 AIDR（AI攻撃検知・対応）サービス	セキュリティ前提のAI実装支援
セキュリティ教育事業	教育コンテンツ開発のスピード向上	AIセキュリティエンジニア セキュアAIエージェント実装講座 AIセキュリティパスポート	EC-Council COASP（AI攻撃・防御技術講座） セキュリティ＆AI講座（AI活用講座）
セキュリティ人材事業（CyberSTAR）	人材育成カリキュラム作成スピード向上	AIエンジニアの育成 セキュリティ×AIのキャリア創出	AIアバターを活用したエンジニアリングサービス 職種別、サービス別のAI最適人材の提供

すでに提供開始 or サービス開発中

主なAIプロジェクト進捗（サイバーセキュリティ事業）

GSX
GLOBAL SECURITY EXPERTS

サイバーセキュリティ事業

AI×コンサルを組み合わせた新サービス「セキュリティ・ドキュメント診断」を開始

概要	セグエセキュリティ株式会社と連携し、同社が提供するAIを活用したセキュリティ規程文書診断サービス「RiskLoom（リスクルーム）」と当社のコンサルティングノウハウを融合
提供価値	・AI×コンサル知見により、セキュリティ規程の文書**ギャップ分析**を効率化 ・サプライチェーン評価制度など11種のガイドラインへの準拠状況を可視化
導入効果	診断期間を従来比**約1/3に短縮**／AIによる**全項目の網羅チェック**で抜け漏れ防止／**11種の基準**（ISMS等）に対応し幅広い評価が可能／コンサルタントは**分析結果の精査・対応優先度に知見を集中**

セキュリティオペレーション統合AIツール「SecOps.AI」を開発 ― 主要機能の開発を終え、チューニング段階へ

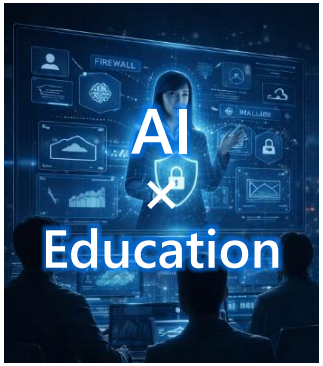
概要	セキュリティオペレーション全般をAIで統合的に支援するツールとして開発。監視製品の検知・分析からレポート作成までを一気通貫で自動化
主要機能	・AI分析レポート自動生成：インシデント検知→報告書作成を数分で完結 ・MCP連携：プロセスツリー解析、脅威インテリジェンス取得、行動相関分析をリアルタイムで収集し思考
導入効果	セキュリティ運用工数を**約50%削減（実績値）**／属人性を排除し、**分析品質を標準化**／分析結果を蓄積・ベクトル化し再活用することで、**継続的に精度向上**するRAGを実現

ログ分析業務の変革

概要	ログ分析～報告書作成までのプロセスを**高度化・自動化**し、従来の人手中心の業務を刷新
主要機能	・熟練アナリストの知見をAIに学習させ、分析ロジックをシステム化 ・AIがログ分析～報告書作成まで実行し、**高速・高精度かつ多角的なデジタルレポート**を生成 ・別AIが成果物をチェックし、**品質整合性の担保＋フィードバックループを構築**
導入効果	分析・報告業務の**大幅な工数削減と高速化**／属人性排除による**品質の標準化**／AIレビューによる**品質の二重担保**

主なAIプロジェクト進捗（セキュリティ教育・セキュリティ人材事業）

セキュリティ教育事業



AI関連の新規講座を複数リリース

講座例	AIセキュリティエンジニア：AIを使えるだけでなく、AIを組み込んだシステムを安全に設計できる技術を学ぶ講座
	セキュアAIエージェント実装講座：AIエージェントをセキュアに開発できる技術を学ぶ講座
	AIセキュリティパスポート：安全にAIを活用するための知識を学ぶ講座
	EC-Council COASP：AIへの攻撃手法と防御技術を実践的に学ぶセキュリティ（Red Team）講座

セキュリティ人材事業

AIで仕組化された教材開発モデルの構築

従来課題	・教材作成に時間がかかる ・固定化された内容 ・案件ごとの最適化が困難
施策	要件定義ー教材生成ー表現強化ーレビューのすべてにAIを活用し、高品質なオンデマンド教材を生成
効果	高速化・高品質化／案件ごとの最適化／提案可能人材の拡大／受注率の向上

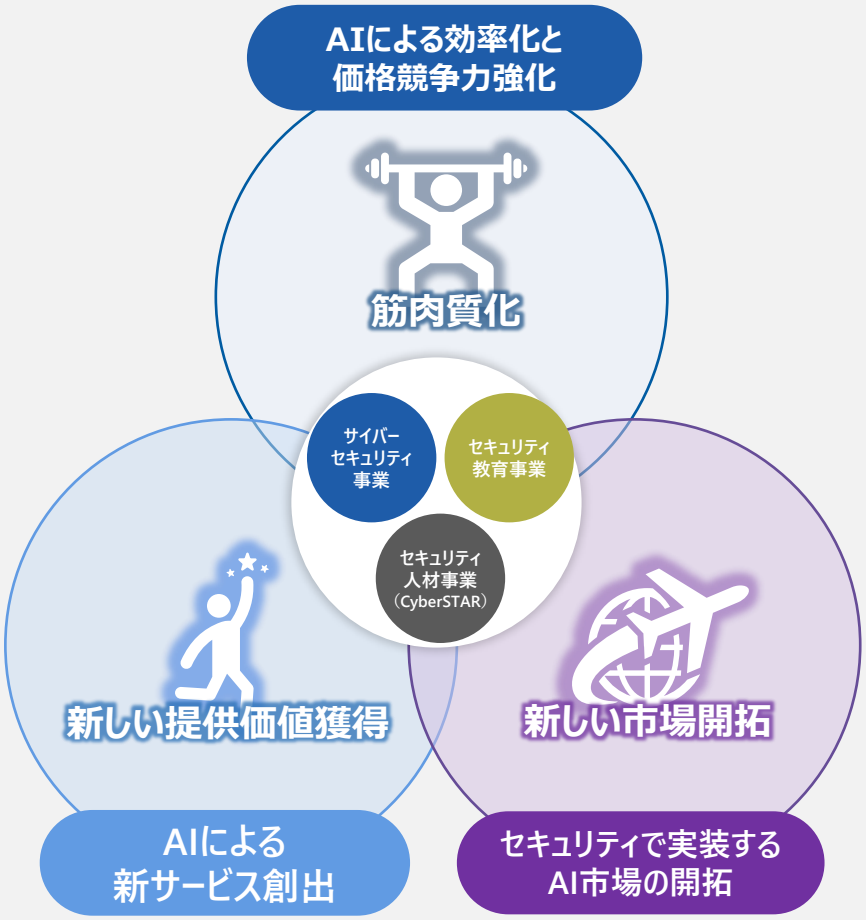
GSX
GLOBAL
SECURITY
EXPERTS

中期経営計画と成長戦略

GSXグループの成長戦略

AI台頭時代の成長戦略と、全国展開による成長戦略を同時に強く推進

AI台頭時代の成長戦略

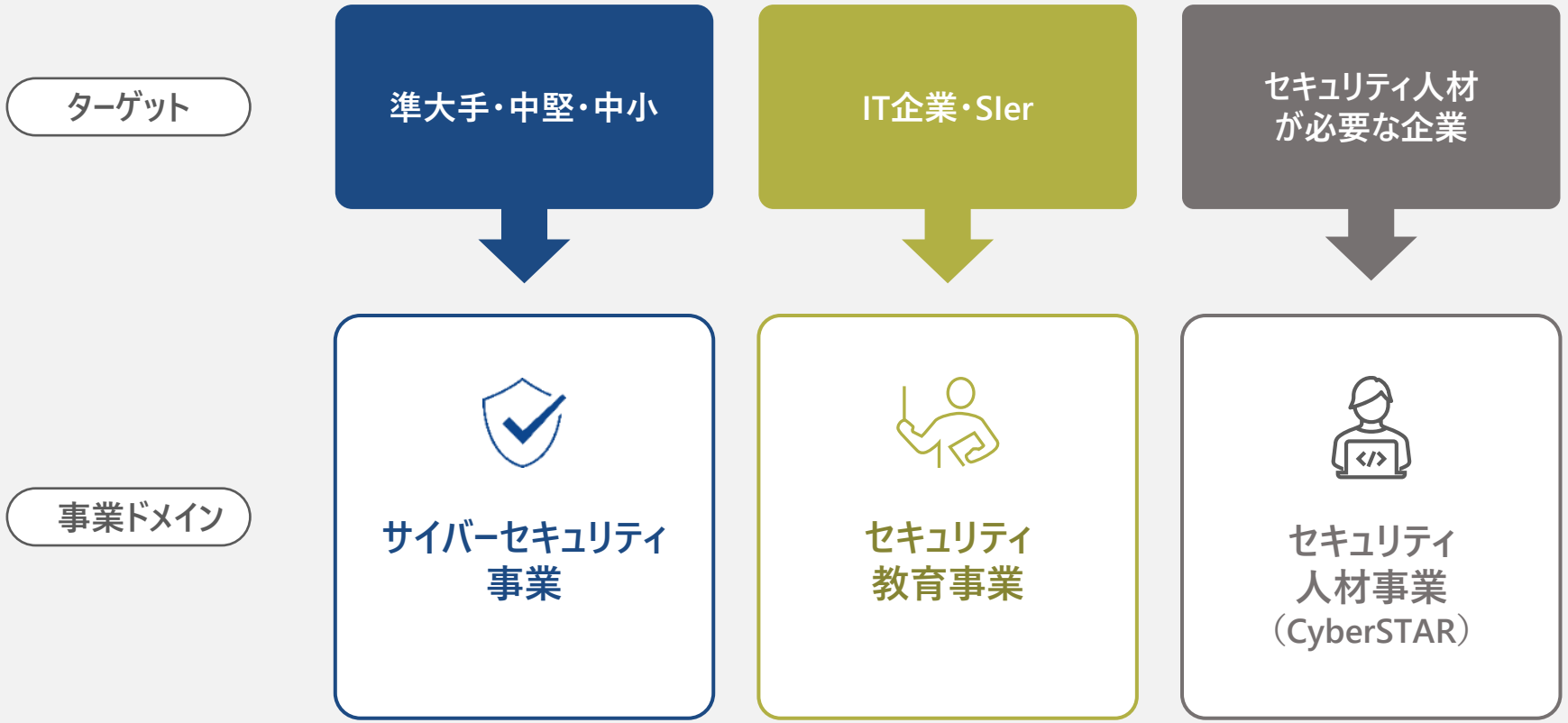


×

全国展開による成長戦略

事業ドメイン

2025年3月期より「準大手・中堅・中小」、「IT企業・SIer」、「セキュリティ人材が必要な企業」の３ターゲットを明確化
それぞれのターゲットに提供するサービスをまとめて事業ドメインとして編成



事業内容：サイバーセキュリティ事業

準大手・中堅・中小企業向けにサイバーセキュリティ対策をワンストップで支援

標的型メール訓練サービス

トラップメール
GSX標的型メール訓練サービス®

OEM供給を含み
トップシェア

累計導入社数
11,000社
以上

コンサルティングサービス（マネジメントコンサルティング）

課題可視化 → 計画策定 → 体制構築

－主なサービス－

- 情報セキュリティ改善計画策定
- 管理体制整備支援
- システム監査・セキュリティ監査
- インシデント対応訓練サービス

従業員のセキュリティ意識向上
組織体制の構築・強化

調査・分析、アセスメント、体制整備など
ワンストップで提供

セキュリティ製品の導入や運用
セキュリティインフラの構築やシステム開発

自社ホワイトハッカーによる
幅広い脆弱性診断を提供

セキュリティソリューションサービス

- 製品導入
- 運用サービス
- 緊急対応
- インフラ構築
- システム開発

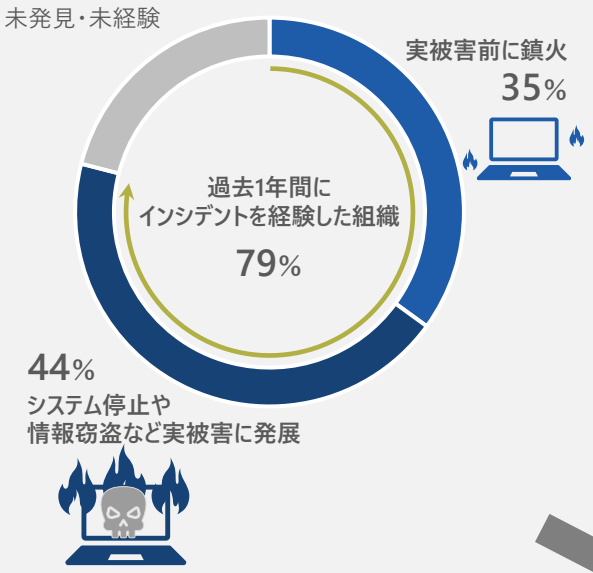
脆弱性診断サービス（タイガーチームサービス）

- 設計書レビュー
- プラットフォーム診断
- IoTセキュリティ診断
- スマホアプリセキュリティ診断
- Webアプリケーション診断

加速する準大手・中堅・中小企業のセキュリティニーズ

セキュリティ事故頻発

過去1年間でインシデントを経験した組織は
約8割



出所：「2020年法人組織のセキュリティ動向調査」（トレンドマイクロ）

社会圧力

各所からのセキュリティ対策プレッシャー

**国や各省庁から降りてくる多数の
セキュリティガイドライン**

**発注側やグループ会社からの
セキュリティ対策圧力が強まる**

AI化の加速

AI推進は、セキュリティ対策とセットで

- ✓ 企業競争力向上にはAI化が急務
- ✓ AI推進はセキュリティ対策とセットで行う必要がある

<u>準大手・中堅・中小企業はセキュリティ対策をせざるを得ない状況</u> に
さらに、AI推進によるセキュリティ対策も意識せざるを得ない状況に

事業内容：セキュリティ教育事業

IT企業・SIer向けにセキュリティ・AI領域の教育を実施、IT人材の付加価値向上を支援する

IT企業・SIer ＋ セキュリティ・AI教育

- エンジニアのセキュリティ水準向上
- 高度なセキュリティ人材の増加
- AIセキュリティ人材の増加

当社オリジナル IT人材/非セキュリティ人材向け教育メニュー

SecuriST®

累計受講者数 23,599名（26/3末時点）

認定Webアプリケーション脆弱性診断士	セキュアWebアプリケーション設計士
受講料金：22万円	受講料金：13.2万円
認定ネットワーク脆弱性診断士	ゼロトラストコーディネーター
受講料金：22万円	受講料金： 8.8万円

セキュリティ人材向け教育メニュー

EC-Council

国際的なセキュリティ資格　累計受講者数 10,442名（26/3末時点）

主なコース例	CND 認定ネットワークディフェンダー	CEH 認定ホワイトハッカー
受講料金	約32万円	約54万円

加速するIT企業・SIerのセキュリティ教育ニーズ

セキュリティがITの品質のひとつに

システム開発　クラウドサービス　ITインフラ構築・運用

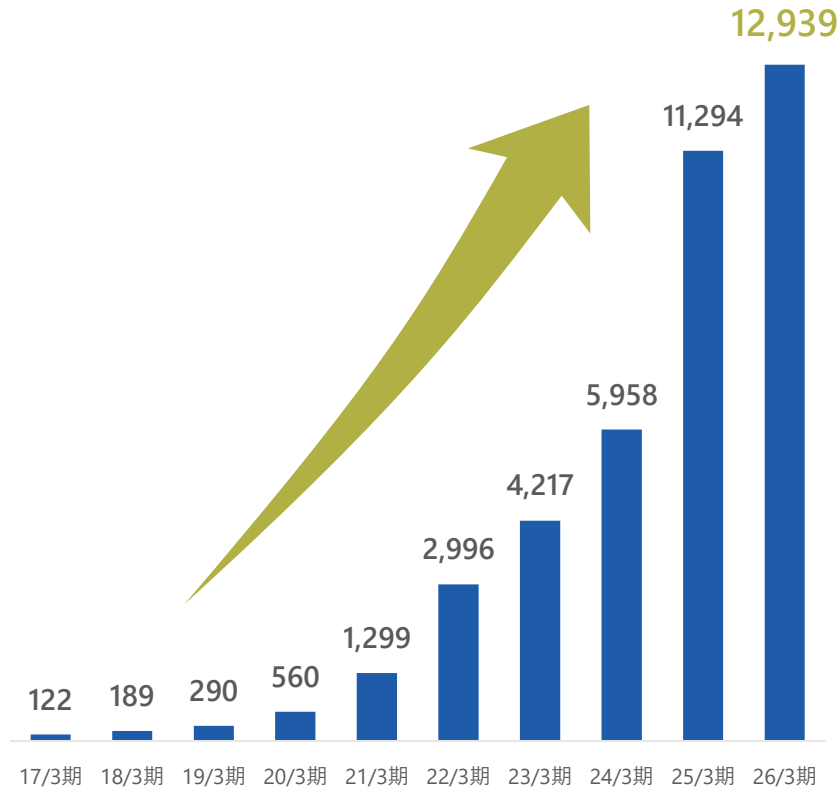
セキュリティでIT商材に付加価値をつける

IT商材　IT商材　・・・

セキュリティはAI推進に不可欠

営業・コンサルタント等　・・・

GSX 教育講座　受講者数の推移（単年度）



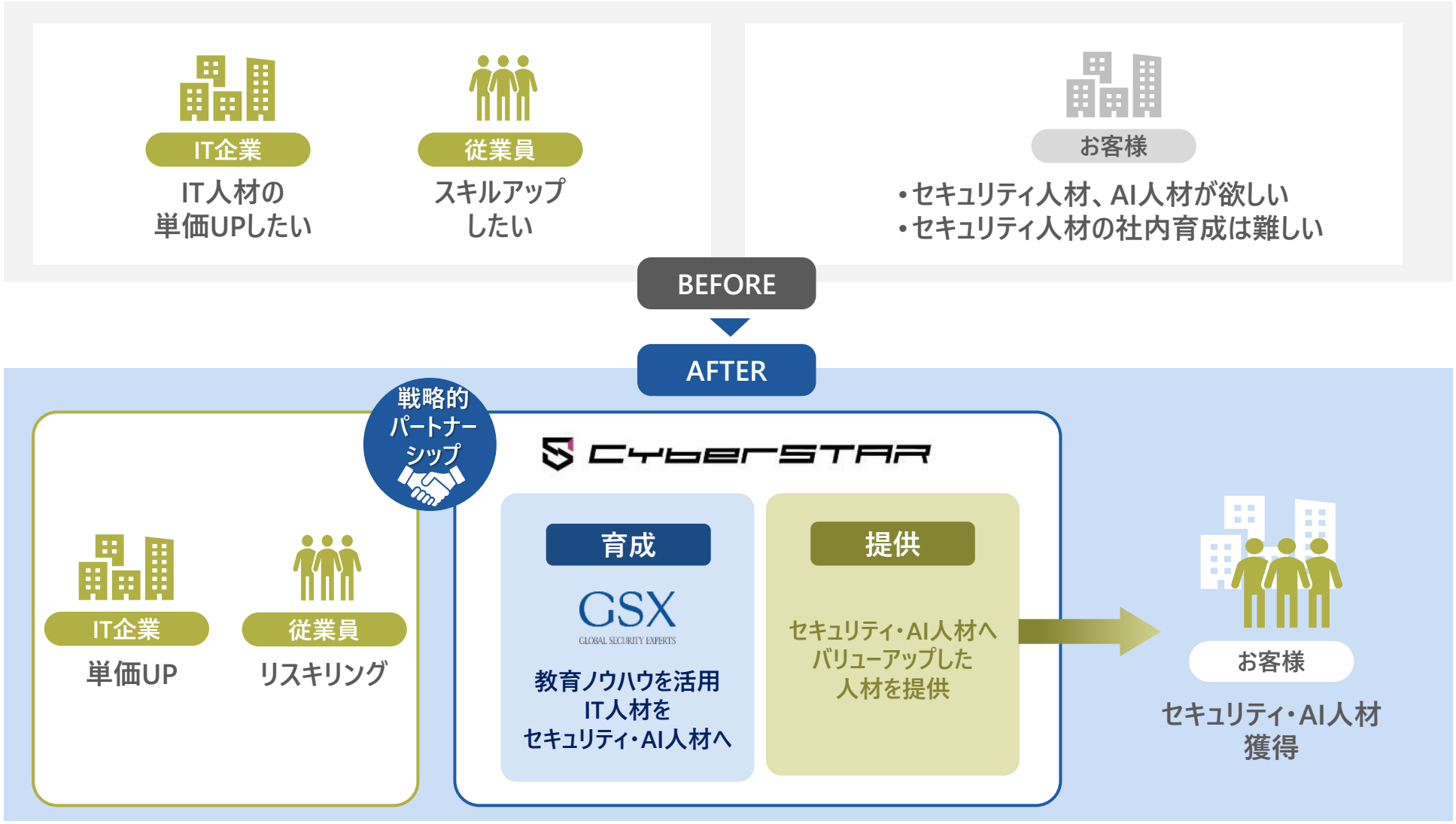
経済産業省「サイバーセキュリティ体制構築・人材確保の手引き」でも「プラス・セキュリティ」※人材の確保を提言

IT企業・SIerのIT人材に向けた セキュリティ・AI教育ニーズが一気に高まっている

※「プラス・セキュリティ」：
自らの業務遂行にあたってセキュリティを意識し、必要かつ十分なセキュリティ対策を実現できる能力を身につけること、あるいは身につけている状態のこと

事業内容： セキュリティ人材事業

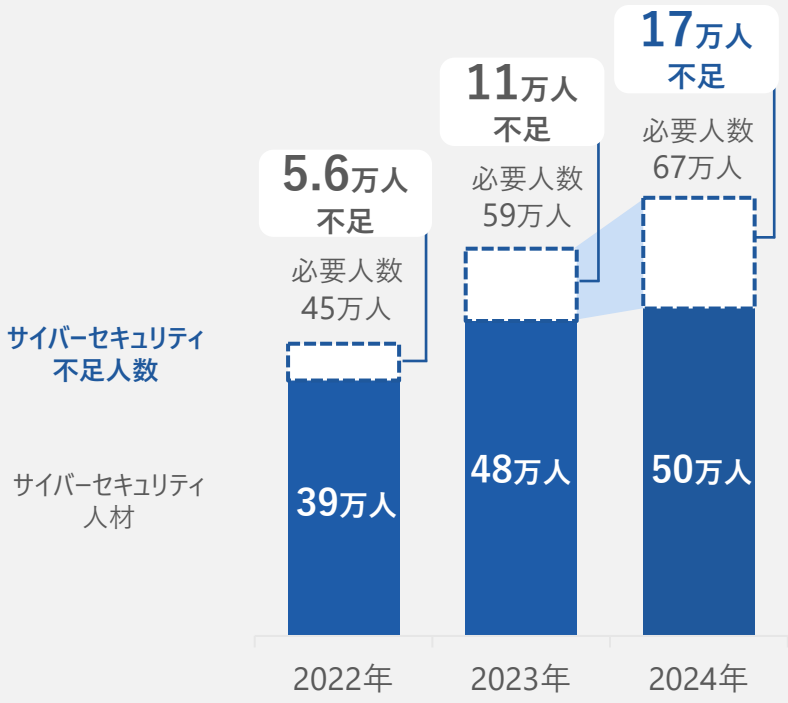
企業規模を限定せずあらゆる企業のセキュリティ・AI人材ニーズに応える
セキュリティ教育カンパニーのGSXならではのビジネスモデルを確立し、IT人材を抱えるIT企業、セキュリティ・AI人材を必要とするお客様双方にメリットを提供



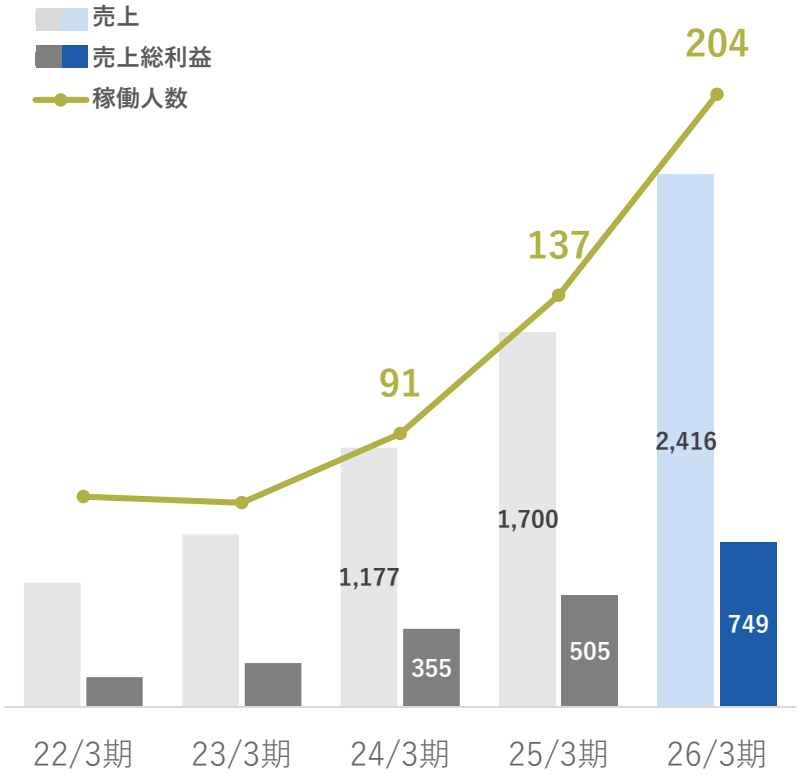
加速するセキュリティ人材SESニーズ

日本のサイバーセキュリティ人材不足

セキュリティ人材の必要数は増加するも、セキュリティ人材数の伸びは鈍化。不足人数は２年前の３倍以上に増加している。



CyberSTAR



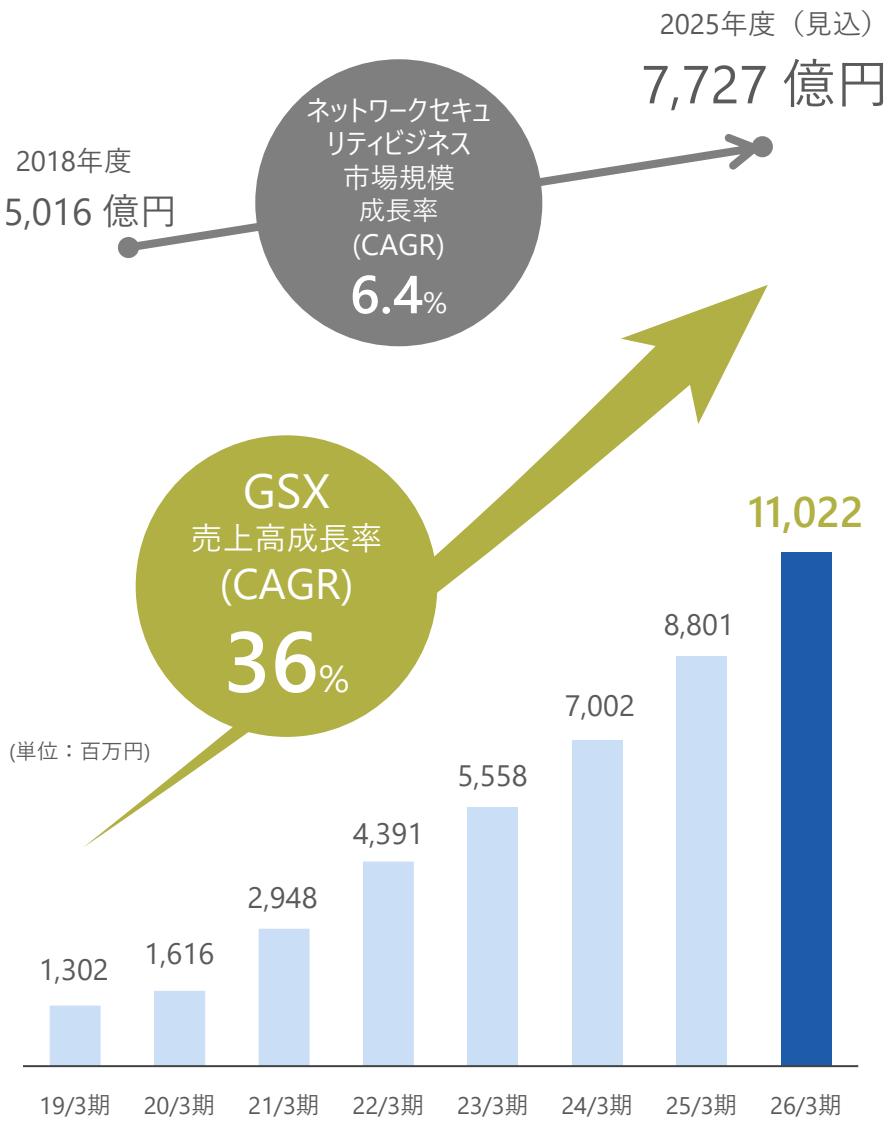
約9割の日本企業がセキュリティ人材不足に悩む一方、キャリアップを望む働き手にとって「情報セキュリティ」は注目の職種

セキュリティ人材ニーズとリスキリングを同時に解決するビジネススキームに注目が集まっている

出所：「ISC2 Cybersecurity Workforce Study」 International Information System Security Certification Consortium（ISC2）

GSXの成長率はセキュリティ市場の成長をはるかに上回る

売上高成長率（CAGR）は36%と市場成長率6.4%を大きく上回る水準で推移



出所：2025 ネットワークセキュリティビジネス調査総覧（市場編）株式会社富士キメラ総研

GSXの高成長の理由と今後の展望

理由 1
準大手・中堅・中小企業における
セキュリティ対策ニーズの飛躍的向上

展望
現時点でホワイトスペース
今後さらにすそ野が広がっていく

理由 2
IT企業・SIerにおける
セキュリティ・AI教育ニーズの飛躍的向上

展望
ITエンジニアのセキュリティ・AIスキル取得が
デファクトスタンダードへ

理由 3
セキュリティ・AI人材を育成して提供する
独自の人材ビジネスモデル

展望
専門人材不足は続く
セキュリティ・AI人材のニーズはさらに拡大

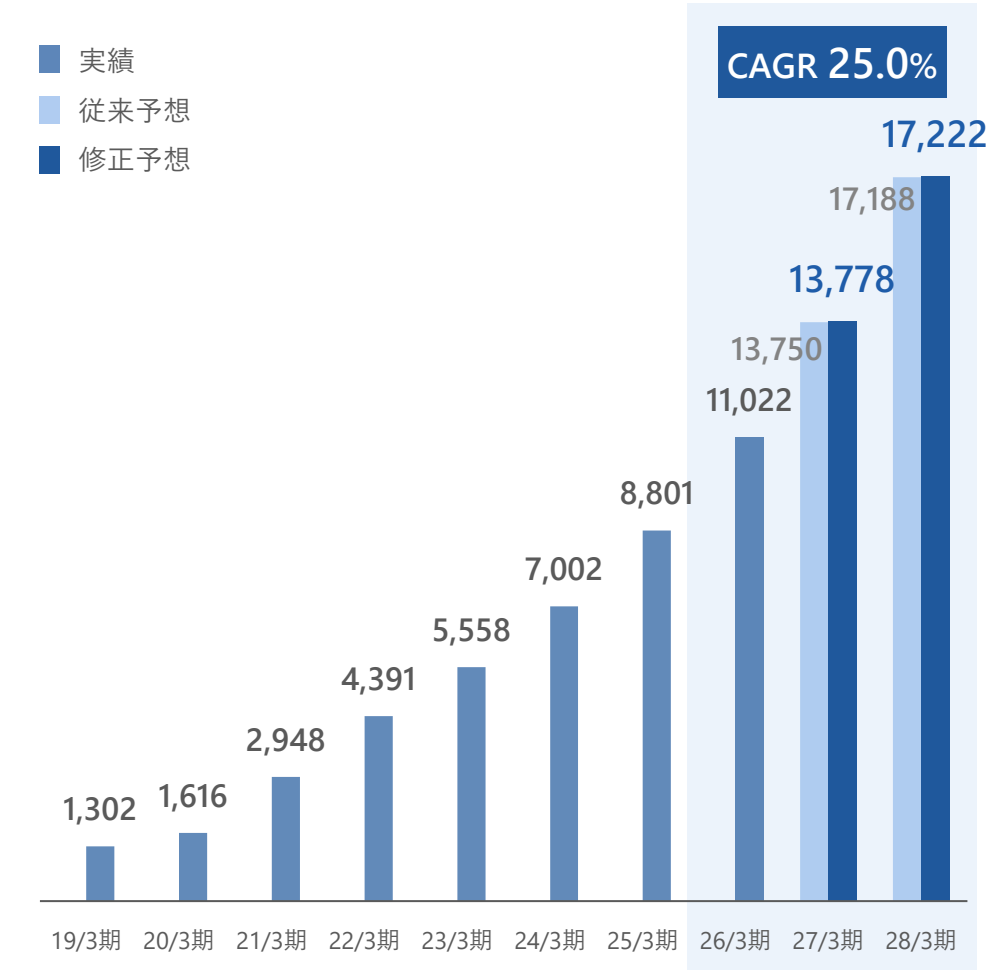
中期数値目標

2026年３月期の実績を踏まえて更新

既存事業で 年率25%の売上高成長　営業利益率は毎年＋1.0ptを目指す

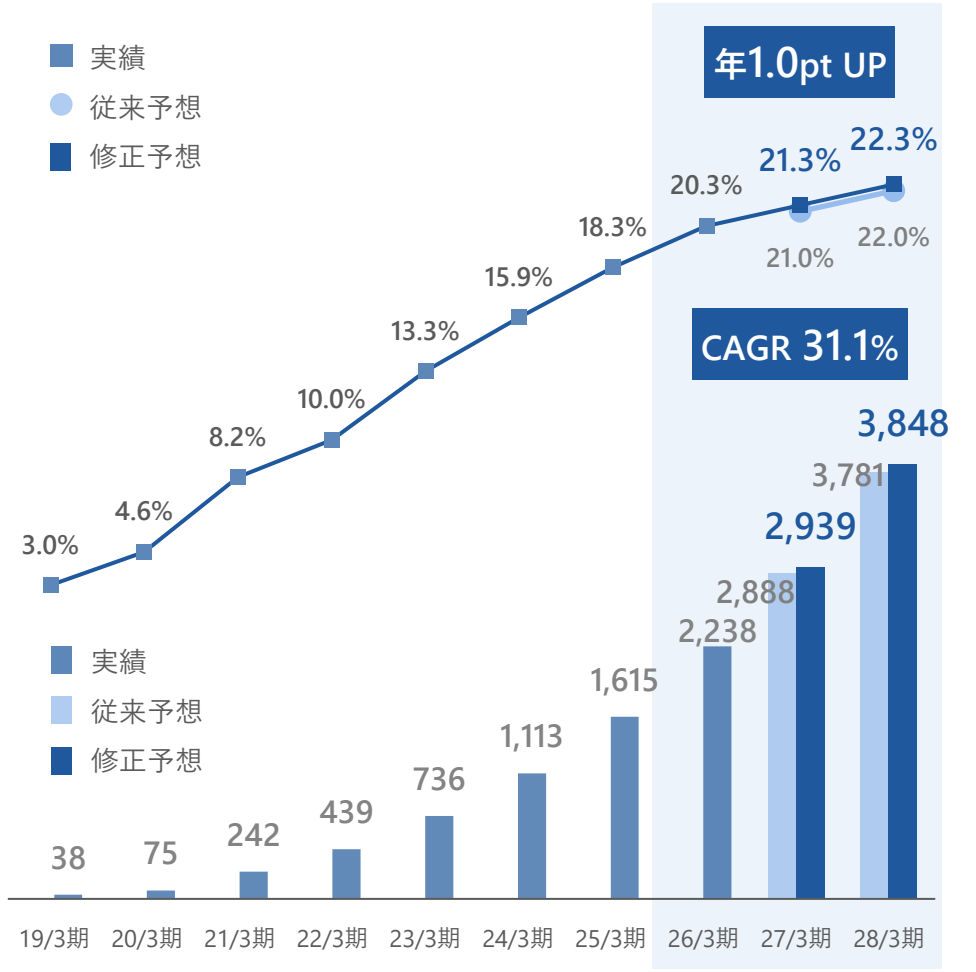
売上高

(単位：百万円)



営業利益及び営業利益率

(単位：百万円)



※2025年3月期より連結業績

中期数値目標の前提

売上高

- ✓ 中堅・中小企業のセキュリティ対策ニーズは引き続き旺盛
- ✓ アップセル・クロスセルを徹底し、全事業がまんべんなく成長
- ✓ IT企業・SIerのセキュリティ人材育成ニーズは引き続き旺盛

営業利益

売上総利益率 Up

セキュリティ教育コンテンツの拡充と**オンライン・オンデマンド配信の活用**

売上総利益率 Up

各事業での**自動化/AI化・フレームワーク採用**

売上総利益率 Up

地方都市を中心にデリバリーパートナー企業を育成
固定人件費を膨らませずにサービス提供のリソースを充足

販管費率 Down

販売パートナー企業の拡大、業界連携による**効率的な販売活動の実現**

※既存事業での中期経営計画であり、新規事業等の影響は織り込んでおりません。

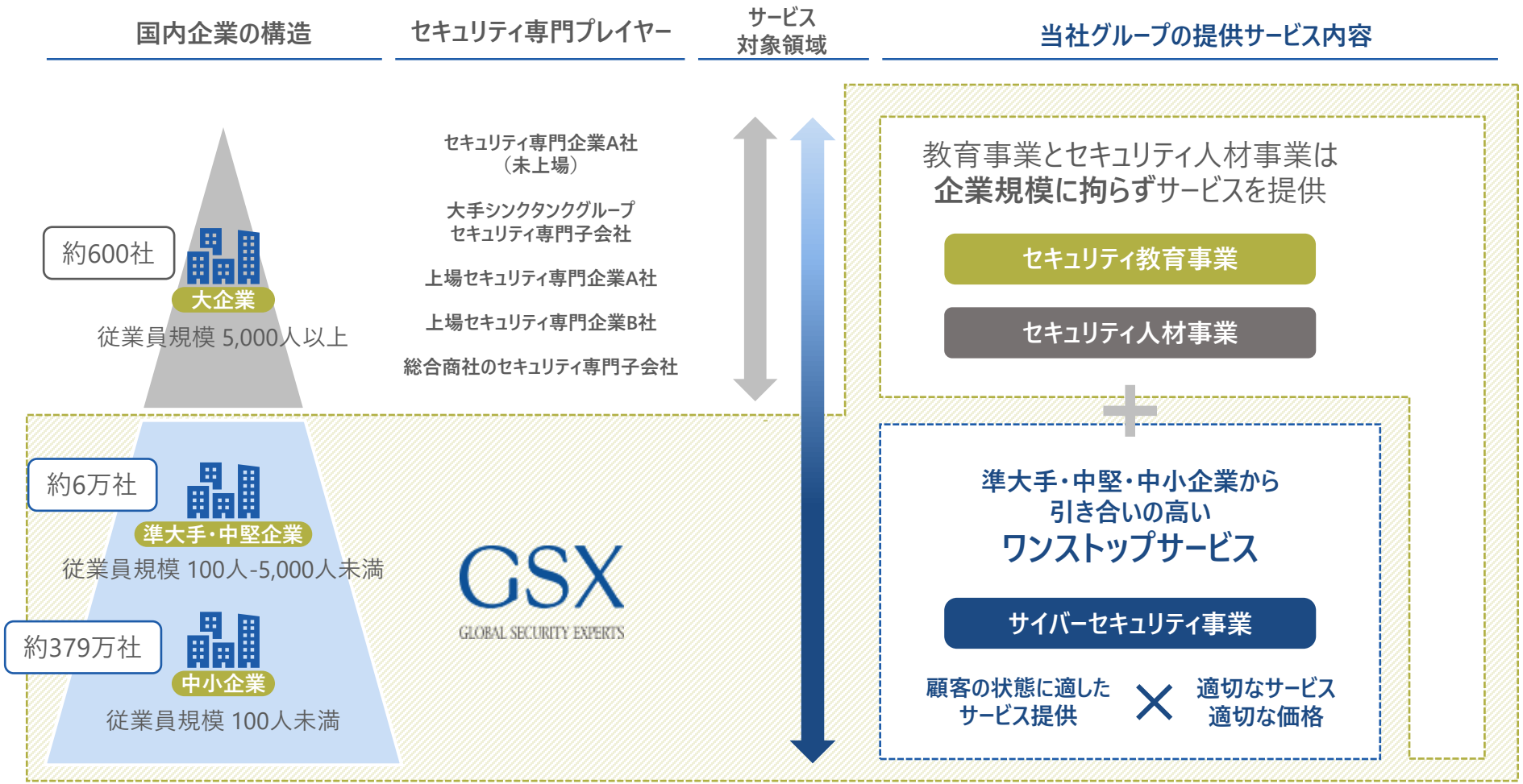
GSX
GLOBAL
SECURITY
EXPERTS

当社の強み

独自のポジショニングである準大手・中堅・中小企業がメインターゲット

セキュリティ対策ニーズは、大企業と、その他の企業の間で大きな格差が存在。このため他のセキュリティ専門企業は大企業向けに絞った戦略を継続してきた

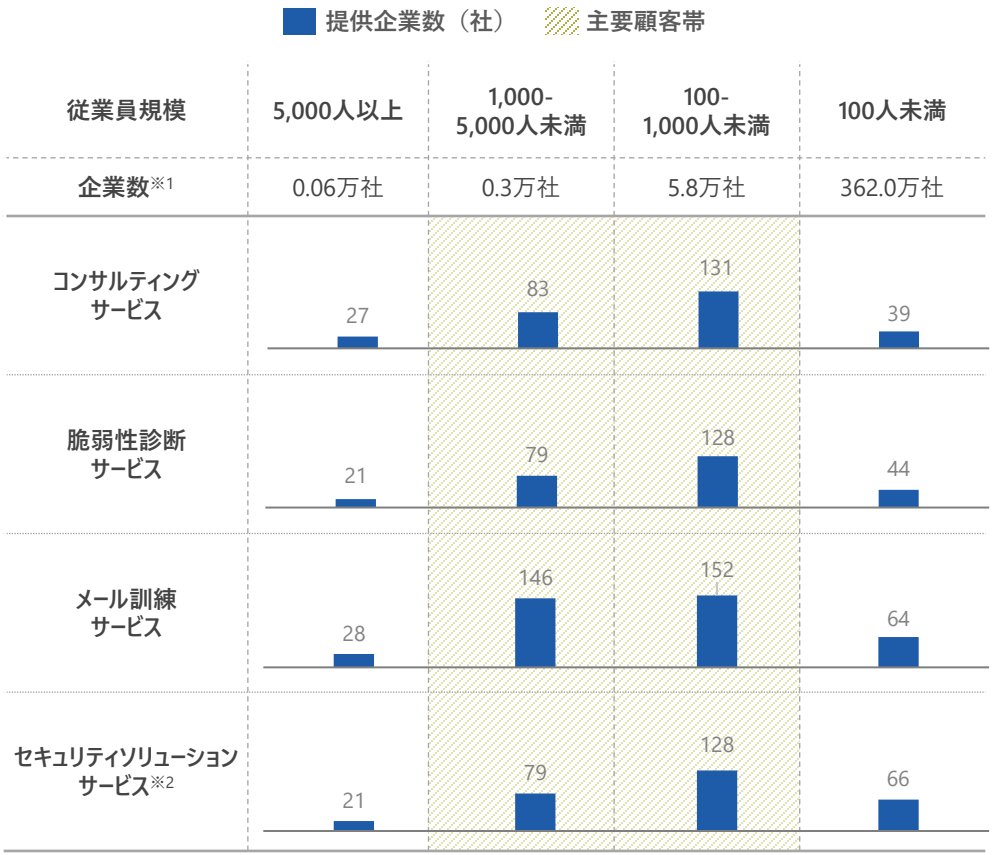
サイバーセキュリティの専門企業というカテゴリーにおいて、GSXは他社が参入しづらい独自のポジションにある



準大手・中堅・中小企業を対象市場とするサイバーセキュリティの巨大な潜在市場規模

当社の対象とする準大手・中堅・中小企業市場は巨大な潜在市場である
セキュリティの実装を支援する関連市場で約1.2兆円、加えて、IT人材を対象としたセキュリティ教育事業で1.2兆円にまで到達し、
現在のセキュリティ関連市場の市場規模を凌ぐグロースポテンシャルが存在

対象顧客層



出所※1：総務省・経済産業省「令和３年経済センサス - 活動調査結果」
https://www.e-stat.go.jp/stat-search/files?page=1&layout=datalist&toukei=00200553&tstat=000001145590&cycle=0&tclass1=000001145666&tclass2=000001145669&tclass3=000001145673&stat_infid=000040067954&cycle_facet=tclass1&tclass4val=0&metadata=1&data=1（2025年６月25日に利用）
注釈 ※2：セキュリティソリューションサービスのフローおよびストック企業数の合計

準大手・中堅・中小企業向け国内サイバーセキュリティ市場の潜在市場規模※3

サイバーセキュリティ事業

コンサルティングサービス **2,151億円**　0.3万社※4×4.5百万円※5+5.8万社※6×3.5百万円※8

脆弱性診断サービス **2,017億円**　0.3万社※4×4.5百万円※5+5.8万社※6×3.2百万円※8

メール訓練サービス **649億円**　0.3万社※4×1.8百万円※5+5.8万社※6×1.0百万円※8

セキュリティソリューションサービス ストック・フロー計 **7,848億円**
ストック：0.3万社※4×22.6百万円※5+5.8万社※6×10.2百万円※8
フロー　：0.3万社※4×3.0百万円※5+5.8万社※6×2.0百万円※8

主要顧客帯のセキュリティ実装支援の潜在市場規模　約**1.2兆円**

＋

セキュリティ教育事業

セキュリティ教育講座 **1.2兆円**（SecuriST 4,219億円+EC-Council 8,247億円）

SecuriST　：95.9万人※7×44万円（脆弱性診断士2講座分の費用）
EC-Council：95.9万人※7×（32万円（CND講座費用）+54万円（CEH講座費用））

注釈 ※3：主要顧客帯における当社が想定する最大の市場規模を意味しており、
当社が2026年6月現在で営む事業に関わる客観的な市場規模を示す目的で算出したものではない
注釈 ※4：主要顧客帯である1,000人-5,000人未満の従業員規模の事業者数（令和３年度経済センサス活動調査より）
注釈 ※5：当社サービスの1,000-5,000人未満の従業員規模の事業者の平均顧客単価（2026/3期）
注釈 ※6：主要顧客帯である100-1,000人未満の従業員規模の事業者数（令和３年度経済センサス活動調査より）
注釈 ※7：IT人材数の推計（IPA：2019年度推定IT企業IT人材数より）
注釈 ※8：当社サービスの100-1,000人未満の従業員規模の事業者の平均顧客単価（2026/3期）

セキュリティニーズの違いとサービスの最適化

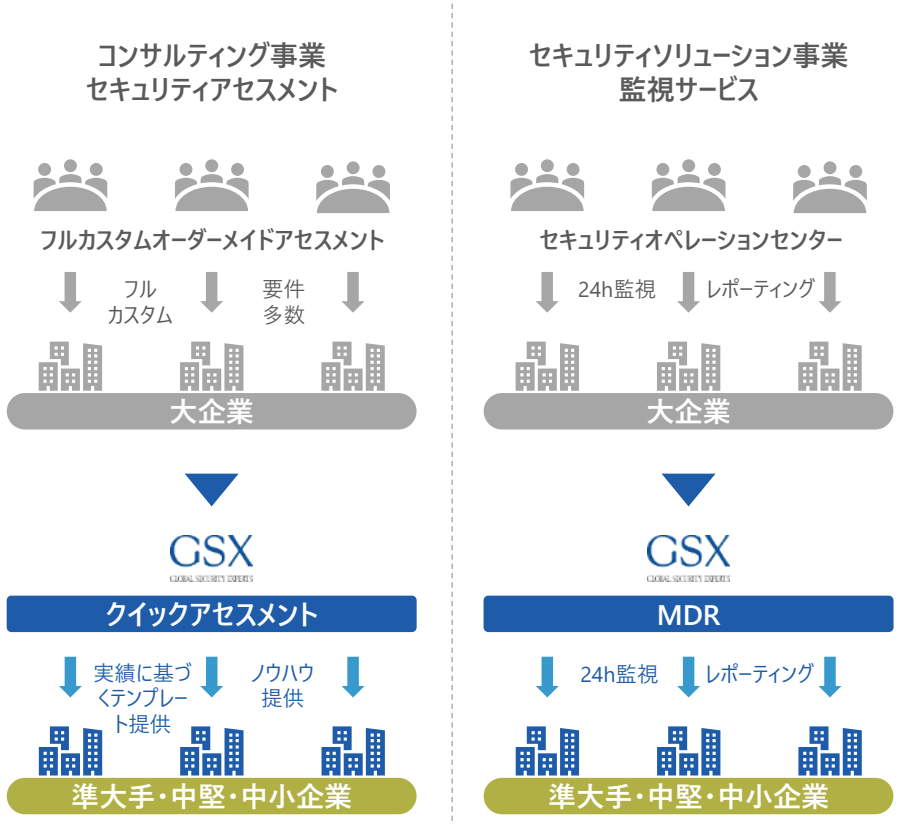
大企業が「脅威を完全に排除」するためのセキュリティ対策を求めるのに対し、準大手・中堅・中小企業は取引先に対してのレピュテーションリスク排除や自社の業態に適合させた必要最低限のセキュリティ対策を求める

当社は豊富なセキュリティノウハウを蓄積していることで、実効性を保ちながら準大手・中堅・中小企業が求める水準へサービスの最適化ができる

企業別のニーズと提供プレイヤー

	大企業	準大手・中堅・中小企業
主な企業ニーズ	セキュリティ脅威の**完全**排除	セキュリティの**監査証明** **自社にとって危険な脅威**の排除
求めるサービス	**フルカスタム** コンサルティングサービス	**ライト**コンサルティングサービス （必要なサービスのパッケージ）
提供プレイヤー	大手シンクタンクグループ セキュリティ専門子会社 セキュリティ専門企業A社(未上場) 総合商社のセキュリティ専門子会社 上場セキュリティ専門企業A社 上場セキュリティ専門企業B社	GSX

準大手・中堅・中小企業向けにセキュリティサービスの最適化



準大手・中堅・中小企業向けセキュリティ市場の参入障壁

準大手・中堅・中小企業向け市場に競合企業が参入するためには、構造的な課題を抱える

短期収益の獲得に不向きな市場環境であり、その中で継続的に顧客から選ばれるためにはセキュリティに関わるあらゆるサービスをワンストップで提供し続けられる知見と基盤が必要

競合企業の構造的な課題

大手向けセキュリティ専門企業

大企業を中心にした顧客基盤

親会社の顧客基盤や
グループ企業戦略に則ったビジネス展開

高価格・高専門性のサービスを提供

大手企業のニーズに合わせたサービスを高価格で提供
高い専門性で高価格、原価構造改革への敷居が高い

顧客基盤と戦略が大きく異なる

参入するには大きな壁がある

GSX
GLOBAL SECURITY EXPERTS

準大手・中堅・中小企業向けに最適化されたサービス、セキュリティ専門人材の確保等に加え、豊富なノウハウの蓄積と実効性のあるセキュリティサービスをワンストップで提供

準大手・中堅企業

中小企業

必要な要素と人員を用意できない

その他のIT企業

セキュリティビジネスは数多く提供するサービスの一つ

セキュリティはSIビジネスを補完する位置づけであり、各部門や子会社などがバラバラにサービス提供しているため、実効性向上に必要な要素をワンストップで提供できない

セキュリティ専門人材の不足

サイバーセキュリティに関わる専門人材※の確保が不足しており、ワンストップで高いレベルのサービスを提供する体制としては不十分（※フルスタック・コンサルタント、ホワイトハッカー、フォレンジッカー、監査員など）

販売戦略　既存顧客：アップセル/クロスセル

多面的なサービス提供によってクロスセル・アップセルを実現。既存顧客のARPU ※は、新規顧客に比べて高く、継続取引が進むことで効率的な事業拡大を実現

事業シナジーを活かした効率的な事業拡大

多角的なサポートを継続的に提供し、
中長期的な取引サイクルを構築

プロセスを網羅しているからできるクロスセル/アップセル

セキュリティ対策に必要な全プロセスを提供しているため
入り口を多彩に構えられ、かつ、次の工程を獲得できる。

教育 → アセスメント → 組織構築・改革 → システム導入・運用

| ランサムウェア対策

初回受注	クロスセル/アップセル
インシデント対応	EDR導入

| 組織力強化

初回受注	クロスセル/アップセル
アセスメント	CSIRT構築・訓練

| 診断内製化

初回受注	クロスセル/アップセル
脆弱性診断	教育講座：SecuriST

注釈 ※：ARPU＝顧客単位の平均売上高（Average Revenue Per USER）

販売戦略：日本全国のIT企業の販売パートナー化

IT企業が持つ顧客基盤とプレゼンスを活用して、ホワイトスペースとなっていた市場を開拓

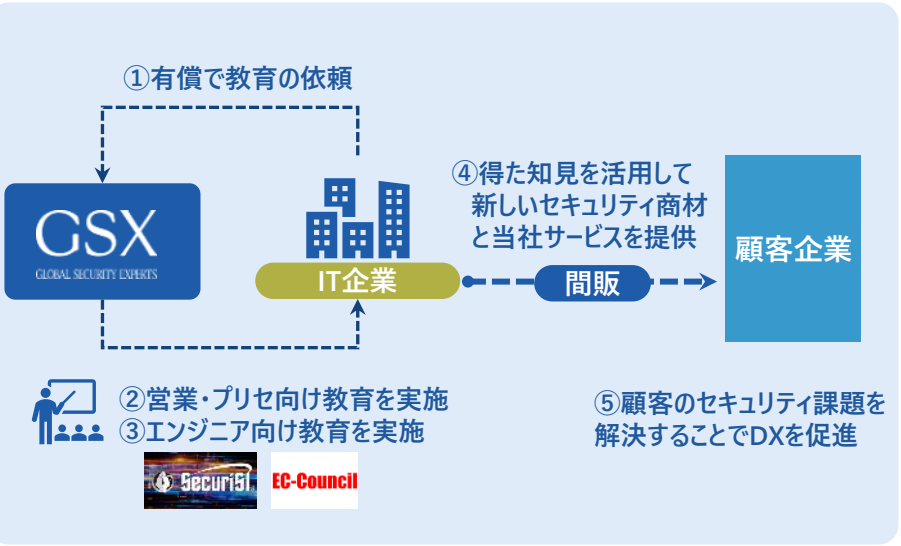
当社とパートナーになることで、IT企業は自社製品・サービスとのシナジーでセキュリティビジネスやDX関連ビジネスの拡大に繋げられる

GSXの販売パートナーになるメリット

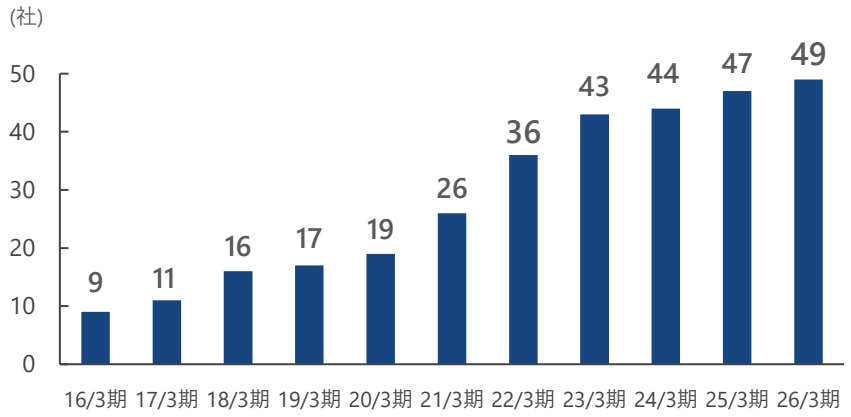
IT企業のニーズ

- DX推進において必要となる新しいセキュリティ商材※は単純販売が難しい
- これらを自社で拡販できるよう社員を教育してセキュリティビジネスを伸ばし、セキュリティをフックとしてさらにDX関連ビジネス（主要事業であるSI）も伸長させたい

※ゼロトラストやマルチクラウドなどの分野



販売パートナー数の推移と全国的拡大



販売戦略　新規顧客：デジタルマーケティング戦略強化

新規顧客獲得については受注に繋がるデジタルマーケティング施策を実行し、質の高いリードを獲得できるよう効率的・効果的なデジタルマーケティング中心に移行

デジタルマーケティング各分野においてセキュリティに強い媒体を選び、動画などを活用したデジタルマーケティング施策を実行

デジタルマーケティング強化

- NewsTV
- YouTube
- Facebook
- Twitter

教育全商材（SecuriST、EC-Council 、CISSP）の動画を制作、NewsTVで配信し、販売促進強化

NEWS TV　わずか１年で受講者３倍！
GSXのサイバーセキュリティ教育の魅力とは

キャパシティ戦略：デリバリーパートナー企業の育成

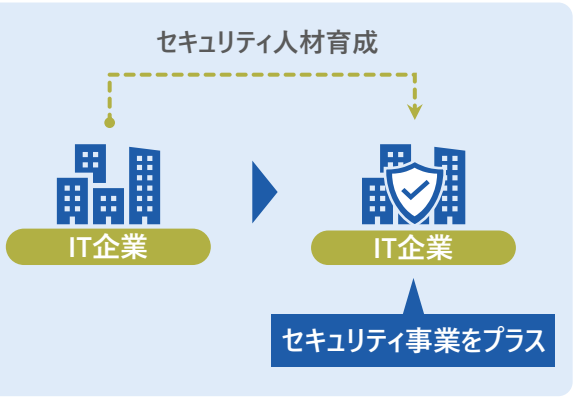
専門性の高い教育コンテンツを活かし、IT企業におけるセキュリティ人材育成や同業他社のパートナー化・育成を進め、セキュリティ市場のプレイヤーを数多く育成することで受注キャパシティを拡大

セキュリティ企業の育成による受注キャパシティの拡大

GSX

新規育成

教育コンテンツ



同業育成

教育コンテンツ

キャパシティ戦略の実績

沖縄のITコールセンターと連携

IT人材をセキュリティ人材へ教育

2020年度は同社で10人のセキュリティ人材化

GSXトレーニングセンター構想

全国展開へ
受注キャパシティ
さらに拡大

全国の同業パートナー育成 を推進

脆弱性診断サービスのリソース確保

資格者の育成で診断内容やレポート品質を担保

販売だけでなく、将来的にリソースを増やし、キャパシティ向上

同業パートナーシップ
さらに拡大

GSX
GLOBAL
SECURITY
EXPERTS

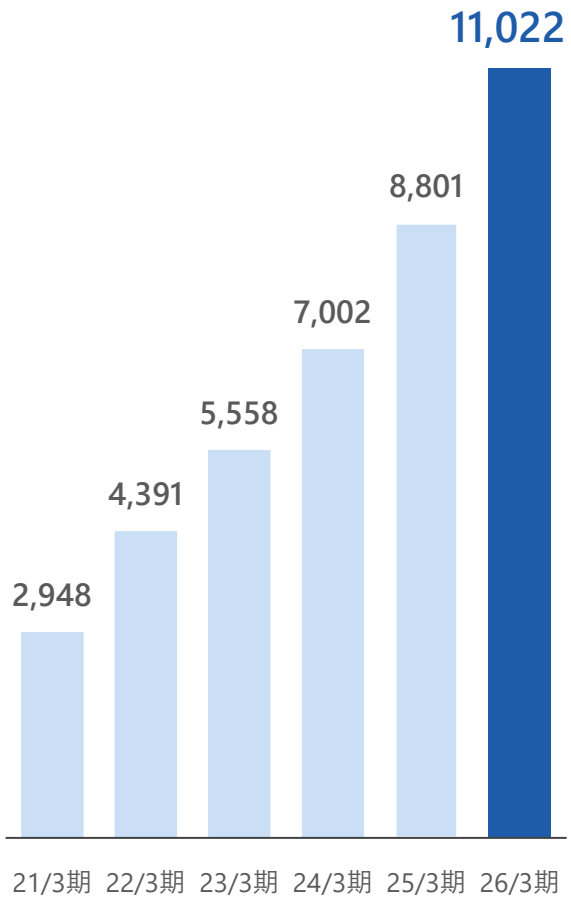
業績ハイライト

通期業績推移

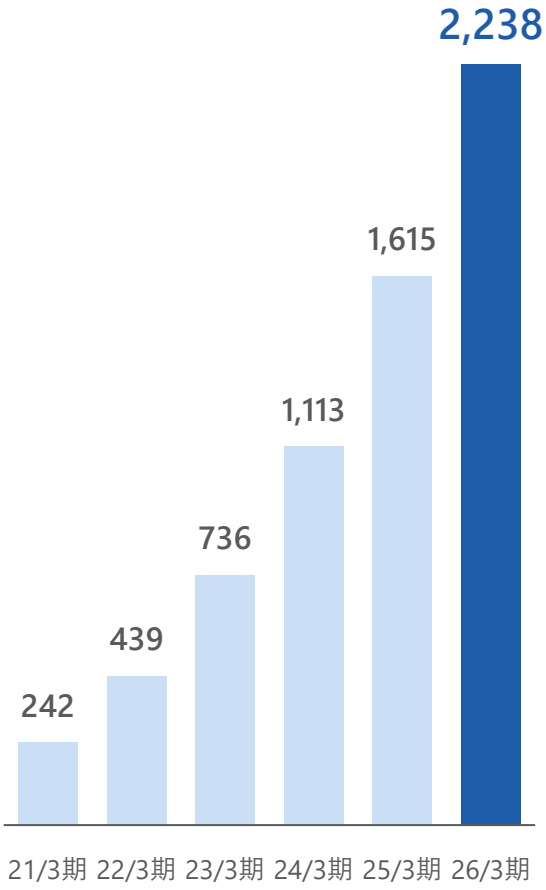
安定的なトップラインの拡大とそれを超える利益の成長スピード

高収益体質の経営を実現

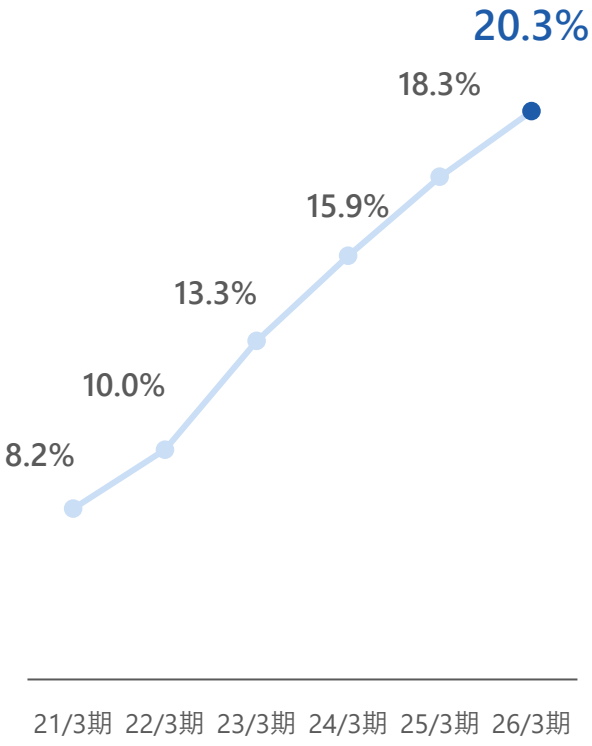
売上高の推移 (単位：百万円)



営業利益の推移 (単位：百万円)



営業利益率の推移

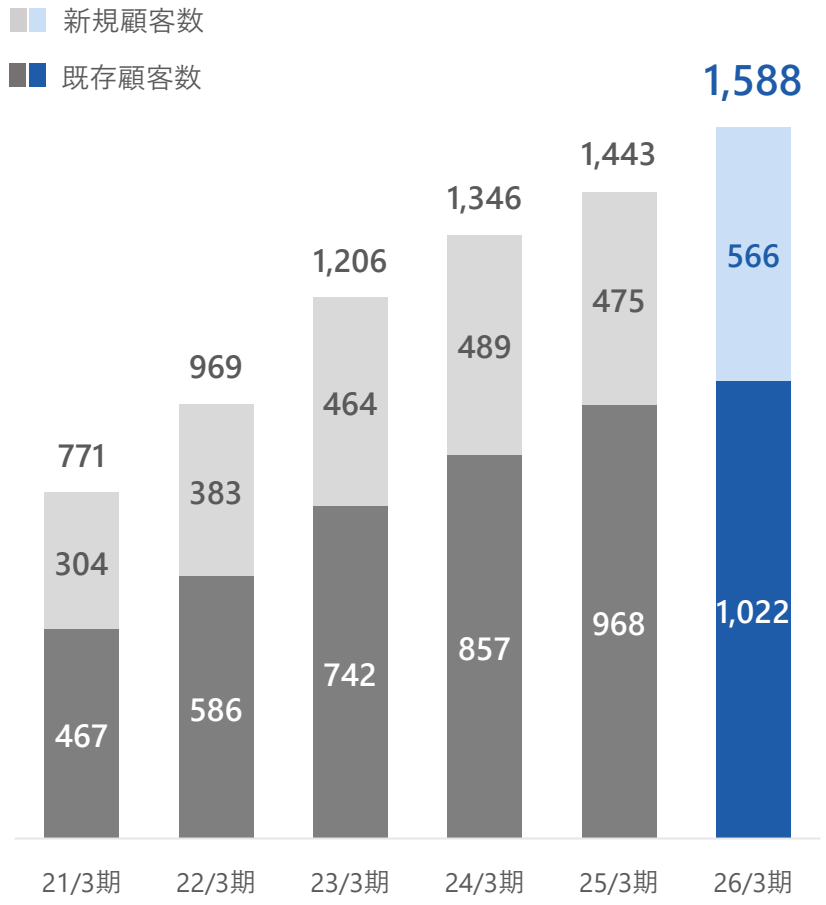


顧客数・ARPU推移

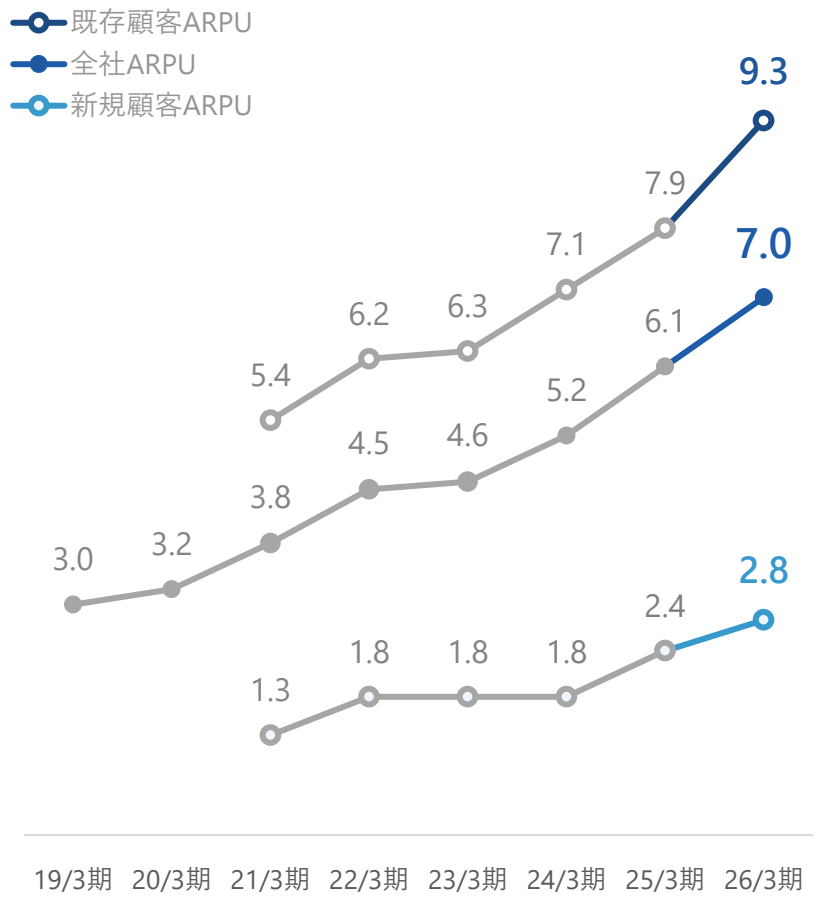
顧客数は新規・既存ともに堅調に増加

2026年3月期はアップセル・クロスセルの効果に加え、準大手・中堅・中小企業のうち準大手よりの案件獲得でARPUが大きく伸長

顧客数推移（単位：社）



ARPU推移（単位：百万円）



※21年3月期以前の数値は参考値です

財務ハイライト

決算期		2022/3期	2023/3期	2024/3期	2025/3期	2026/3期
売上高	（千円）	4,391,317	5,558,022	7,002,941	8,801,647	11,022,080
経常利益	（千円）	414,331	737,512	1,104,319	1,562,981	2,222,786
当期純利益	（千円）	261,099	488,120	783,428	1,010,077	1,486,742
資本金	（千円）	485,000	529,833	544,999	545,921	546,553
発行済株式数	（株）	3,327,000	7,383,000	7,629,600	7,644,600	15,309,600
純資産額	（千円）	1,565,478	1,720,169	2,433,625	3,078,911	4,401,238
総資産額	（千円）	3,482,070	4,124,589	6,536,708	8,141,157	9,959,520
1株当たり純資産額	（円）	117.63	118.13	161.54	205.08	292.4
1株当たり配当額 （うち1株当たり中間配当）	（円）	3.75 （－）	7 （－）	13.11 （－）	20.86 （10.43）	34.60 （16.36）
1株当たり当期純利益	（円）	20.23	36.10	52.42	67.24	98.85
自己資本比率	（%）	44.96	41.71	37.23	37.8	44.2
自己資本利益率	（%）	20.82	29.71	37.72	32.8	39.8
配当性向	（%）	18.5	19.4	25.0	31.0	35.0
営業キャッシュフロー	（千円）	328,219	594,948	713,549	1,018,887	1,134,568
投資キャッシュフロー	（千円）	△294,649	△212,159	△2,005,260	△411,367	△151,230
財務キャッシュフロー	（千円）	460,634	△455,995	1,447,820	△457,415	△725,700
現金及び現金同等物の期末残高	（千円）	1,146,528	1,073,322	1,229,432	1,379,536	1,637,175
従業員数	（人）	118	138	154	195	221

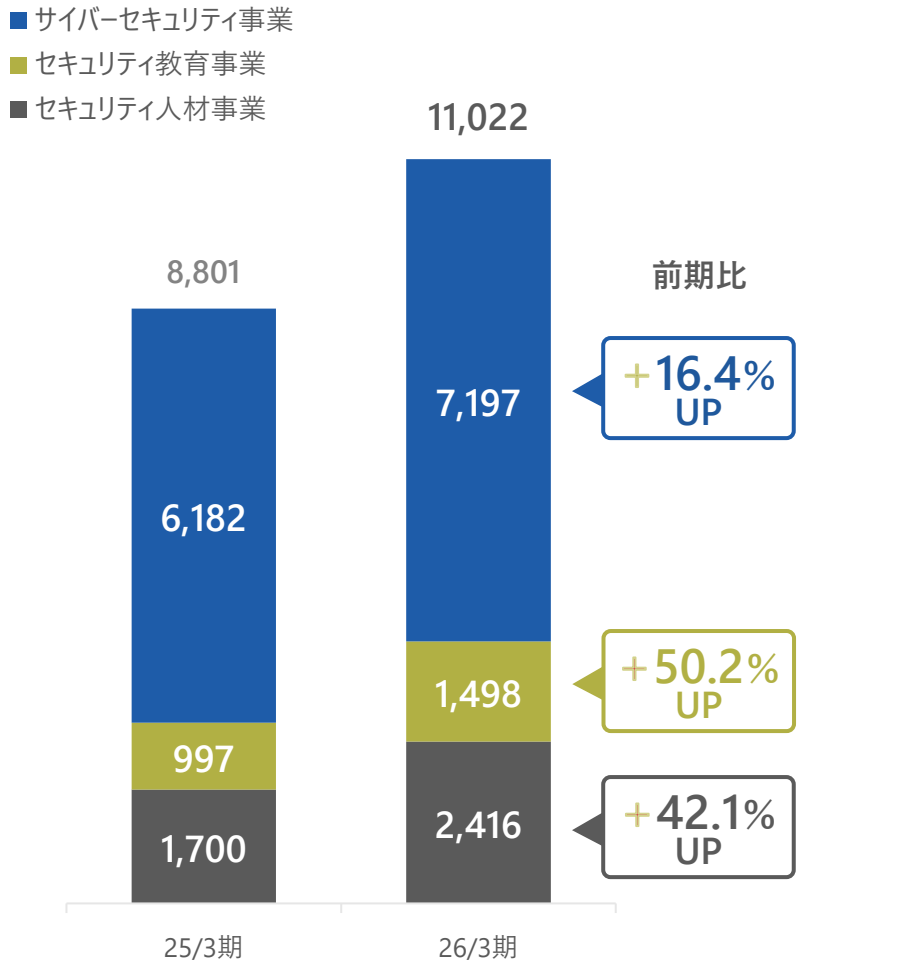
※１：2025年3月期より連結財務諸表を作成しているため、それ以前については、個別財務諸表を記載しております。
※２：2021年10月22日付で普通株式１株につき300株の割合で株式分割、2022年11月１日付で普通株式１株につき２株の割合で株式分割、2025年６月１日付で普通株式１株につき２株の割合で株式分割を行っております。2021年3月期の期首に当該株式分割が行われたと仮定し、１株当たり純資産額及び１株当たり当期純利益を算定しております。また、１株当たり配当額（うち1株当たり中間配当）につきましても、当該株式分割を考慮した額を記載しております。

事業別売上高・売上総利益　前期比（累計期間）

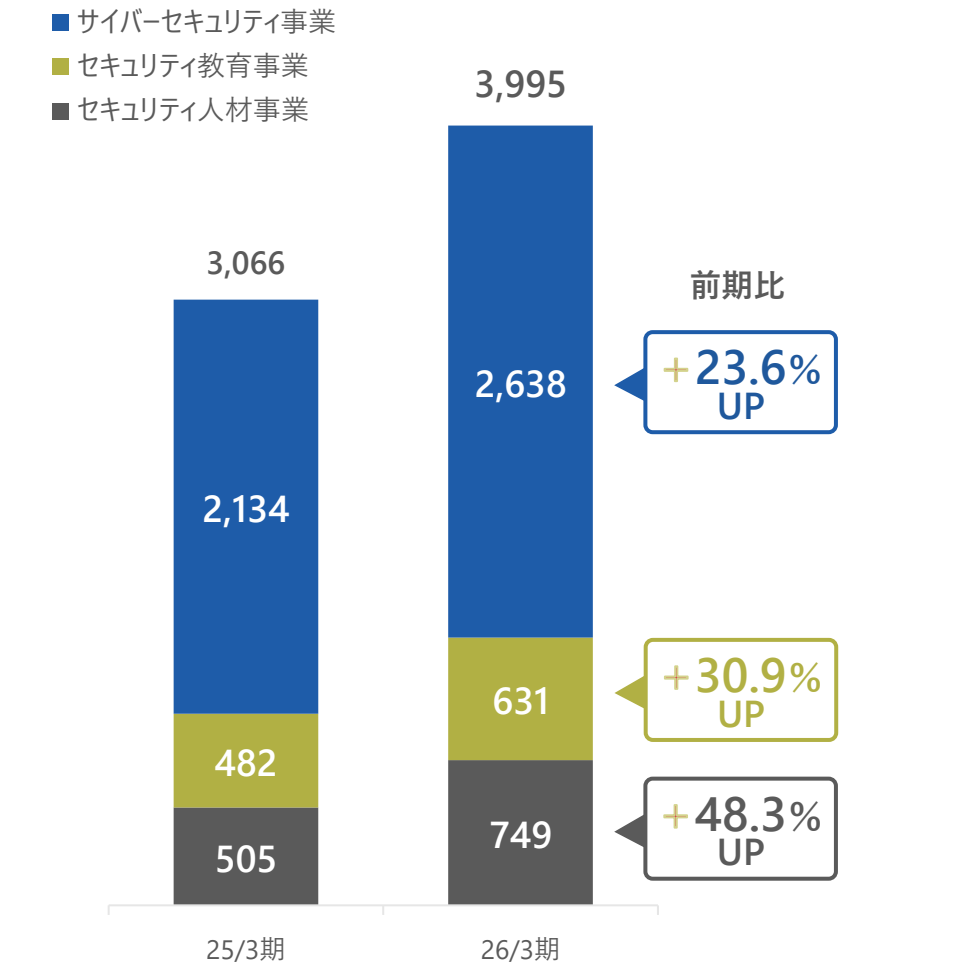
売上高・売上総利益ともに拡大

セキュリティ教育事業、セキュリティ人材事業が大きく躍進

売上高（単位：百万円）



売上総利益（単位：百万円）



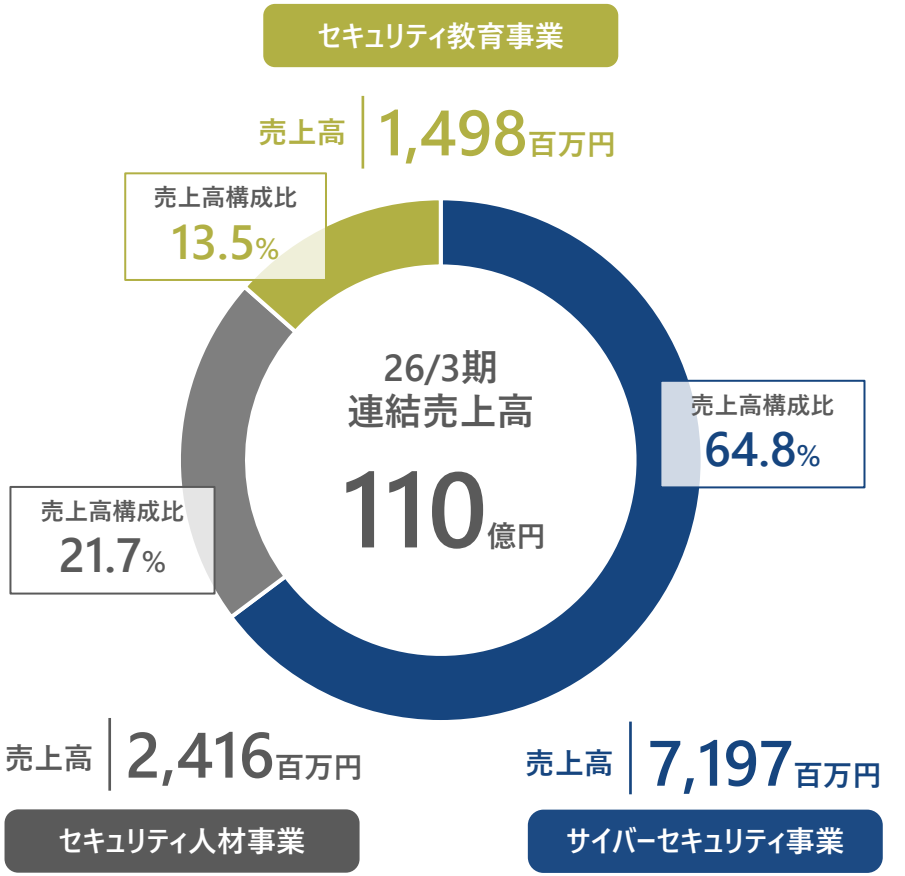
※事業別の売上高は、内部取引消去をする前の金額です

連結売上高・売上総利益構成

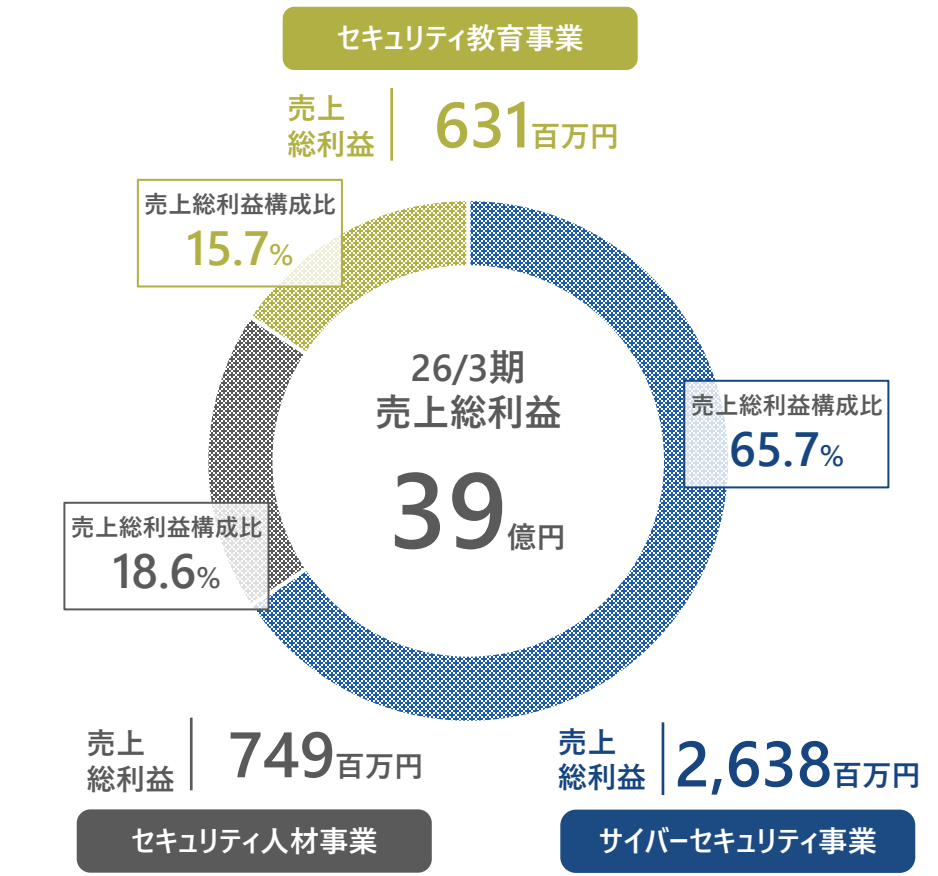
2026年3月期の構成比は計画通り

安定収益のサイバーセキュリティ事業をベースに、高成長のセキュリティ教育事業・セキュリティ人材事業で構成

売上高構成比



売上総利益構成比



※事業別の売上高は、内部取引消去をする前の金額です

GSX
GLOBAL
SECURITY
EXPERTS

2027年3月期連結業績予想

2027年3月期の基本方針と連結業績予想

基本方針

売上高拡大は継続、利益率の向上を重要視し
中長期成長を支える経営基盤を強固にする

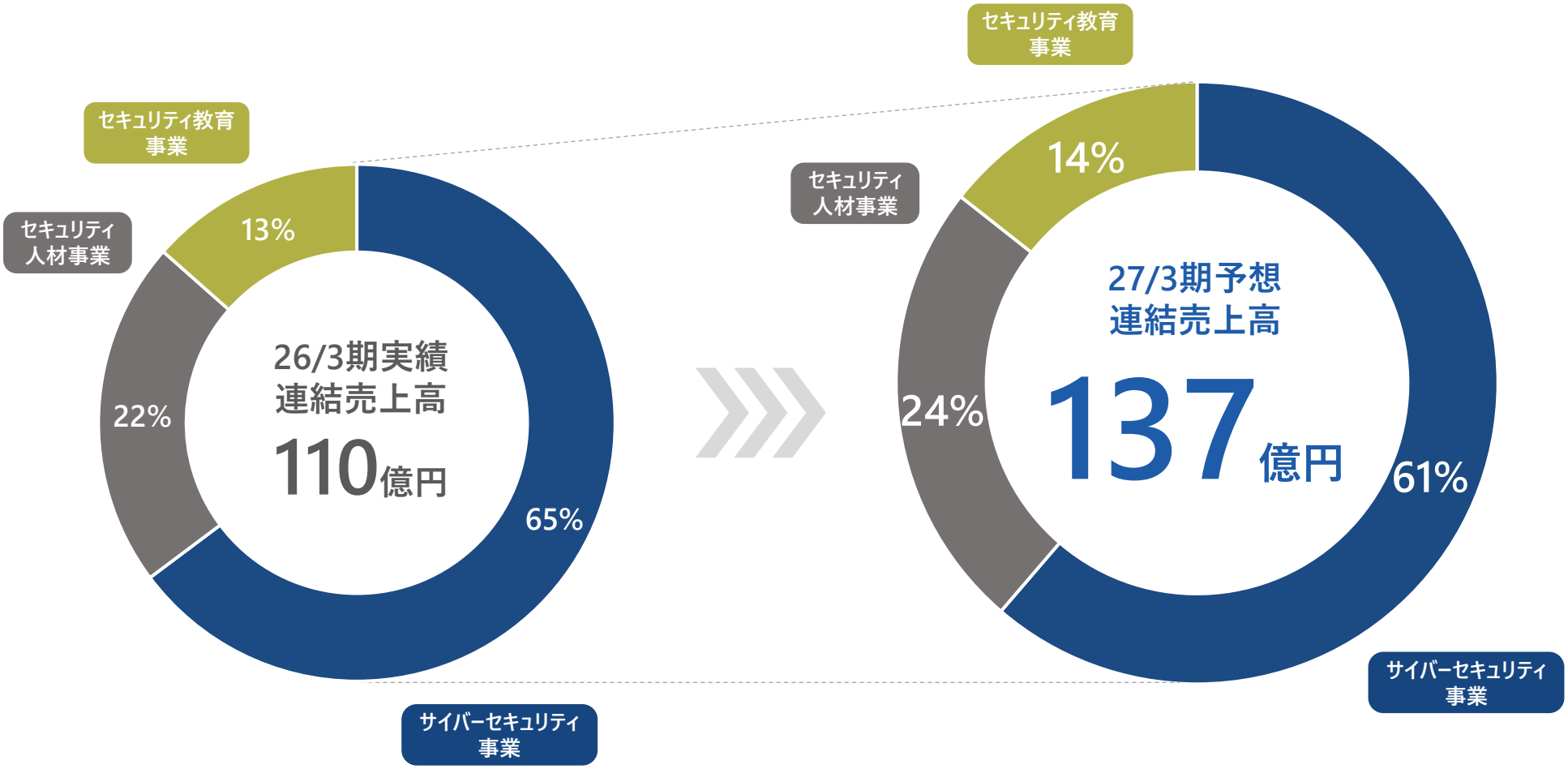
連結売上高は前期比＋25%　営業利益率は21.3%を目指す

（百万円）	2026/3期 実績	2027/3期 予想	増減額	増減率
売上高	11,022	13,778	2,756	+25.0%
営業利益	2,238	2,939	703	+31.3%
営業利益率	20.3%	21.3%	+1.0pt	-
経常利益	2,222	2,973	756	+33.8%
経常利益率	20.2%	21.6%	+1.5pt	-
当期純利益	1,486	1,998	512	+34.4%
EPS（円）※	98.85	132.74	33.89	-

※当社は、2025年6月1日付で普通株式１株につき２株の割合で株式分割を行っております。
前連結会計年度の期首に当該株式分割が行われたと仮定して EPS を算出しております。

2027年3月期 連結売上高の構成予想

サイバーセキュリティ事業の安定成長とセキュリティ教育事業・セキュリティ人材事業の躍進
全ての事業において前期比増収を見込む



GSX
GLOBAL
SECURITY
EXPERTS

長期ビジョン

年率25％売上成長と、さらなる成長を確信する資本提携・業務提携

中期経営計画で掲げる年率 25％の売上成長を実現し、さらなる成長を確かなものにするアライアンス戦略

GSXが成長するための４つの領域で、強力に事業を推進できる戦略的パートナー企業と資本提携・業務提携を締結

販路拡大

販路拡大に伴う業績伸長

提携パートナーの顧客網に対する商材の展開

新エリア進出

事業領域拡大に伴う業績伸長

新たな事業領域に進出することによる新規顧客の獲得

GSX

- サイバーセキュリティ事業
- セキュリティ教育事業
- セキュリティ人材事業（CyberSTAR）

リソース拡大

製造能力拡大に伴う業績伸長

各種サービスを提供し得る人的リソースが増強されることによる売上貢献

サービスラインナップ拡充

提供サービス拡充に伴う業績伸長

提供できるサービスが増えることによる販売機会の拡大

日本サイバーセキュリティファンドのスキーム

残す？

GSX
GLOBAL SECURITY EXPERTS

L.P.（ファンドへ出資する投資家）

KG / KEL / Rococo / DICS Group / BBSec / ALSI / cybertrust
Unite& Grow / SIG GROUP / 電通総研 / AGS / AGS株式会社 / Worldsky / GSX
PSC / SecuAvail / VALTES / SECURE / TOBILA SYSTEMS / SST
AGEST / Aeye Security Lab / Segue Group / TRILOGY Holdings / HAMMOCK / AMIYA

出資

リターン

日本サイバーセキュリティファンド1号投資事業有限責任組合

G.P.（無限責任組合員）
WERU Investment

アドバイザリーボード

投資先検討委員会

事業支援

投資

目利き

投資先企業

セキュリティ企業（シード期・上場検討企業・上場企業）

投資先企業が成功するためのあらゆる支援を実行し、事業成功率をUP

POINT

1. 確度の高さ — アドバイザリーボードの目利き機能とL.P.企業群による事業支援で成功確度が限りなく高い
2. シナジー創出 — 参画企業各社の経営トップが連携することによるビジネスボリュームの拡大とスピードの向上
3. 業界の規模拡大 — セキュリティ企業各社が成長を遂げることで、セキュリティ業界全体が盛り上がる

経営戦略

年率25%の売上成長の礎となる基本戦略と、さらなる成長を確信するアライアンス戦略・ファンド組成

アライアンス戦略

販路拡大
新エリア進出
GSX
リソース拡大
サービス
ラインナップ拡充

成長
加速

ファンド組成

LP
GSX ＋ セキュリティ企業
資金提供
日本サイバーセキュリティファンド1号
事業支援
出資
アドバイザリーボード
事業成功率UP
目利き
出資先セキュリティ企業

基本戦略

相互作用

準大手・中堅・中小企業
セキュリティ体制の強化
をワンストップで

IT企業・SIer
教育でIT人材を
「プラス・セキュリティ」人材
AI人材へ

セキュリティ・AI人材が必要な企業
セキュリティ・AI
特化型の人材ビジネス

新たな収益源

年率25%の売上成長の礎

海外市場への展開による新たな収益基盤の構築

将来的には、国内の強固な顧客基盤を活かし、海外成長市場への参入を目指す

IT活用が進みつつあるASEAN地域を当面のターゲット市場とし、既存顧客の海外子会社へのサービス提供で収益基盤構築と市場でのプレゼンス上昇を図りつつ、海外ローカル企業への展開を見据える

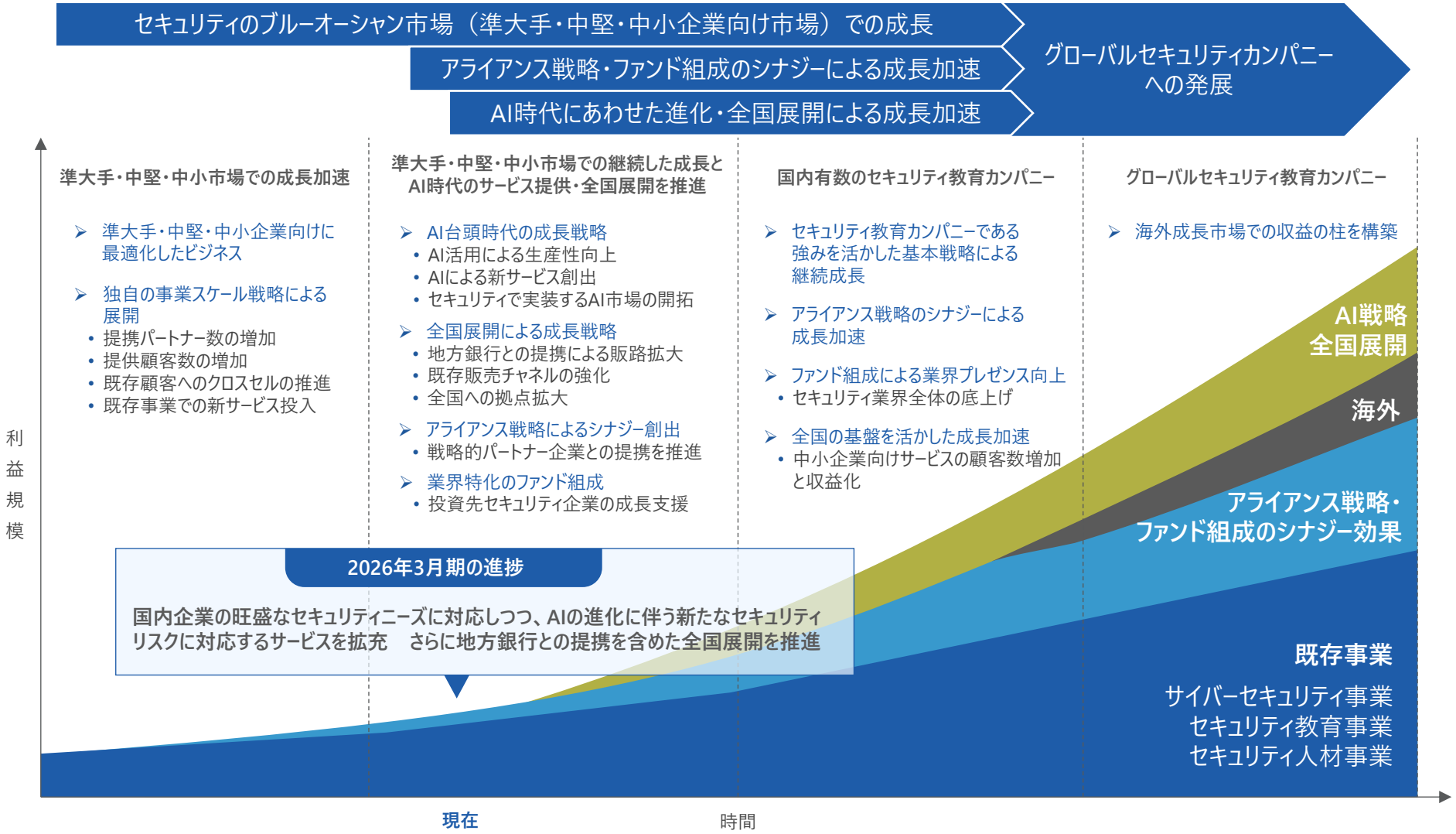
海外展開フロー

【2026年3月期の進捗】
ベトナムのICT（情報通信技術）人材に対し、当社オリジナルのセキュリティ教育講座を提供　現地セキュリティ人材の育成を推進
一方で、日本国内の準大手・中堅・中小企業におけるセキュリティニーズが旺盛なことから、引き続き国内の顧客基盤も拡大中

中長期成長イメージ

セキュリティのブルーオーシャン市場（準大手・中堅・中小企業向け市場）での継続的な成長に加え
AIの進化に伴い増大するセキュリティニーズによって成長加速　地方銀行や戦略的パートナー企業とのアライアンス戦略で全国へと商圏拡大

長期的には国内有数のセキュリティ教育カンパニーとしての専門性を武器に海外市場での収益基盤構築によりさらなる成長を図る



GSX
GLOBAL
SECURITY
EXPERTS

リスク情報

認識するリスク（1/2）

有価証券報告書記載の「事業等のリスク」のうち、当社の成長実現や事業計画の遂行に重要な影響を与える可能性があると認識している主なリスクは以下となります

1.需要の低迷に関するリスク

リスク顕在化の可能性：中

リスク要因	今後、経済環境の変化等、何らかの要因により、中堅企業におけるサイバーセキュリティの需要が著しく低迷した場合にはリスクが顕在化する。
顕在化した場合の影響	当社の今後の事業展開、経営成績や財務状況に影響を及ぼすことが想定される。 ・売上や利益の大幅な低下 ・資金繰りの悪化 ・従業員のモチベーション低下
当社の対応策	① 幅広い業種の顧客にサービスを提供することで、特定の業界環境の変化に左右されない顧客基盤を築く。 ② 中堅・中小企業向けのセキュリティノウハウを蓄積することで、実効性を保ちながら中堅・中小企業が求める水準へサービスの最適化を行う。 ③ 中堅・中小企業向けのサービス水準・価格帯が馴染むと予想される東南アジアへの進出。

2.競合の出現に関するリスク

リスク顕在化の可能性：中

リスク要因	中堅企業を主な顧客とした競合が出現した場合にはリスクが顕在化する。
顕在化した場合の影響	競合が出現した場合には、以下のような事態が想定される。 ・低価格競争 ・売上や利益の大幅な低下 ・資金繰りの悪化
当社の対応策	① 蓄積されたノウハウやニーズを顧客に適したサービス開発や品質向上に反映させることでサービス競争力を向上させていく好循環なビジネスサイクルを確立する。 ② 中堅・中小企業に最適化した複数のサービスを保有していることで、一つのサービス提供をきっかけに顧客の必要性に応じ、様々なサービスのクロスセル・アップセルを実現する。

認識するリスク（2/2）

有価証券報告書記載の「事業等のリスク」のうち、当社の成長実現や事業計画の遂行に重要な影響を与える可能性があると認識している主なリスクは以下となります。

3.人材の確保に関するリスク

リスク顕在化の可能性：小

リスク要因	当社の属するサイバーセキュリティ業界では、専門知識を有する人材の不足が共通課題とされており、今後、当社の業容が拡大する一方で、十分な人材を確保できない場合にはリスクが顕在化する。
顕在化した場合の影響	サイバーセキュリティに関する専門知識を有する人材を確保できないことにより、以下のような事態が想定される。 ・サービス提供の遅れや生産性の低下 ・事業成長力の低下 ・サービス不履行等による社会的信用力の低下
当社の対応策	① 当社のサイバーセキュリティエンジニアを育成する教育講座を通じて、専門人材を育成した企業とのパートナーシップを推進することで、社外より安定的に人材を確保する。 ② 社内人材については、、毎年行う新卒採用及び随時行う中途採用では、サイバーセキュリティ専門人材の採用に拘らず、採用後の教育によって専門人材へと育成する。入社後においても、当社の教育講座を無償で受講する等により専門知識の向上を図るとともに、職場環境の整備やモチベーション向上等に注力することで、人材流出を防ぎ、ノウハウや経験の社内蓄積に努める。 ③ サービスの自動化・プラットフォーム化による生産性の向上に努める。

4.技術革新への対応に関するリスク

リスク顕在化の可能性：小

リスク要因	サイバーセキュリティの分野における、日々発生する新たな脅威や技術革新等による環境変化に伴い、ニーズが変化した場合にはリスクが顕在化する。
顕在化した場合の影響	当社で保有する技術やノウハウが顧客の求めるレベルに達しないことにより、以下のような事態が想定される。 ・競争力の低下 ・事業成長力の低下
当社の対応策	① 新たな脅威や技術革新等に関する情報収集に努める。 ② 新製品やサービス、新しい技術要素を積極的に習得させる。

※当社の成長の実現や事業計画の遂行に影響を与える可能性があると認識しているその他のリスクについては、有価証券報告書の「事業等のリスク」をご参照ください。

GSX
GLOBAL
SECURITY
EXPERTS

Appendix

日本全国の企業の自衛力向上を目指し、セキュリティ業界全域で事業を展開する

サイバーセキュリティ教育カンパニー

－ Purpose －

全ての企業をセキュリティ脅威から護る
そのために必要なことを惜しげもなくお伝えする

－ Mission －

日本全国の企業の自衛力を向上すること

会社概要

サイバーセキュリティの黎明期に設立したサイバーセキュリティ専門企業
サイバーセキュリティ事業、セキュリティ教育事業、セキュリティ人材事業の３つの事業を展開
※2024年4月1日に、サイバーセキュリティ人材事業を分社化し、100％子会社「CyberSTAR株式会社」設立

会社概要

会社名	グローバルセキュリティエキスパート株式会社
設立	2000年4月※1
代表者	代表取締役社長 青柳 史郎
資本金	546百万円　※26/3末
事業内容	準大手・中堅・中小企業向けにサイバーセキュリティ対策をワンストップで支援する「サイバーセキュリティ事業」、IT企業・SIerの人材向けにセキュリティ教育を提供する「セキュリティ教育事業」、セキュリティ人材を提供する「セキュリティ人材事業」を展開
事業セグメント	サイバーセキュリティ事業（単一）
従業員数	連結 221名 単独 187名　※26/3末
主な株主	(株)ビジネスブレイン太田昭和 兼松エレクトロニクス(株) 丸紅I-DIGIOホールディングス(株)

役員一覧

代表取締役社長	青柳 史郎
代表取締役副社長	原　伸一
専務取締役	三木　剛
常務取締役	中村　貴之
取締役	吉見　主税
取締役	鈴木　貴志
取締役	後藤　慶
取締役（社外）	近藤　壮一
取締役（社外）	上野　宣
取締役（社外）	森本　宏一
取締役（社外 監査等委員）	井上　純二
取締役（社外 監査等委員）	古谷　伸太郎
取締役（社外 監査等委員）	水谷　繁幸

注釈 ※1：グローバルセキュリティエキスパートへの商号変更日を設立日として記載

マネジメントメンバー

代表取締役社長 CEO

青柳　史郎

Shiro Aoyagi

1998年 4月　㈱ビーコンインフォメーションテクノロジー（現㈱ユニリタ）入社
2009年 1月　㈱クラウドテクノロジーズ取締役 セキュリティ事業本部長
2012年 3月　当社入社
2012年10月　当社 事業開発部長
2014年 6月　当社 執行役員営業本部長
2017年 4月　当社 取締役経営企画本部長
2018年 4月　当社 代表取締役社長（現任）

代表取締役副社長 COO

原　伸一

Shinichi Hara

1991年 4月　㈱アマダメトレックス(現㈱アマダ)入社
2000年 4月　㈱アドバンスト・リンク代表取締役
2012年 4月　スタートコム株式会社取締役
2018年 4月　当社入社 執行役員副社長兼経営企画本部長
2018年 6月　当社　代表取締役副社長（現任）

専務取締役
エリア統括本部 本部長

三木　剛
Tsuyoshi Miki

常務取締役
教育事業本部 本部長

中村　貴之
Takayuki Nakamura

取締役
西日本支社 支社長

吉見　主税
Chikara Yoshimi

取締役
サイバーセキュリティ事業本部 副本部長
サイバーセキュリティ研究所 所長

鈴木　貴志
Takashi Suzuki

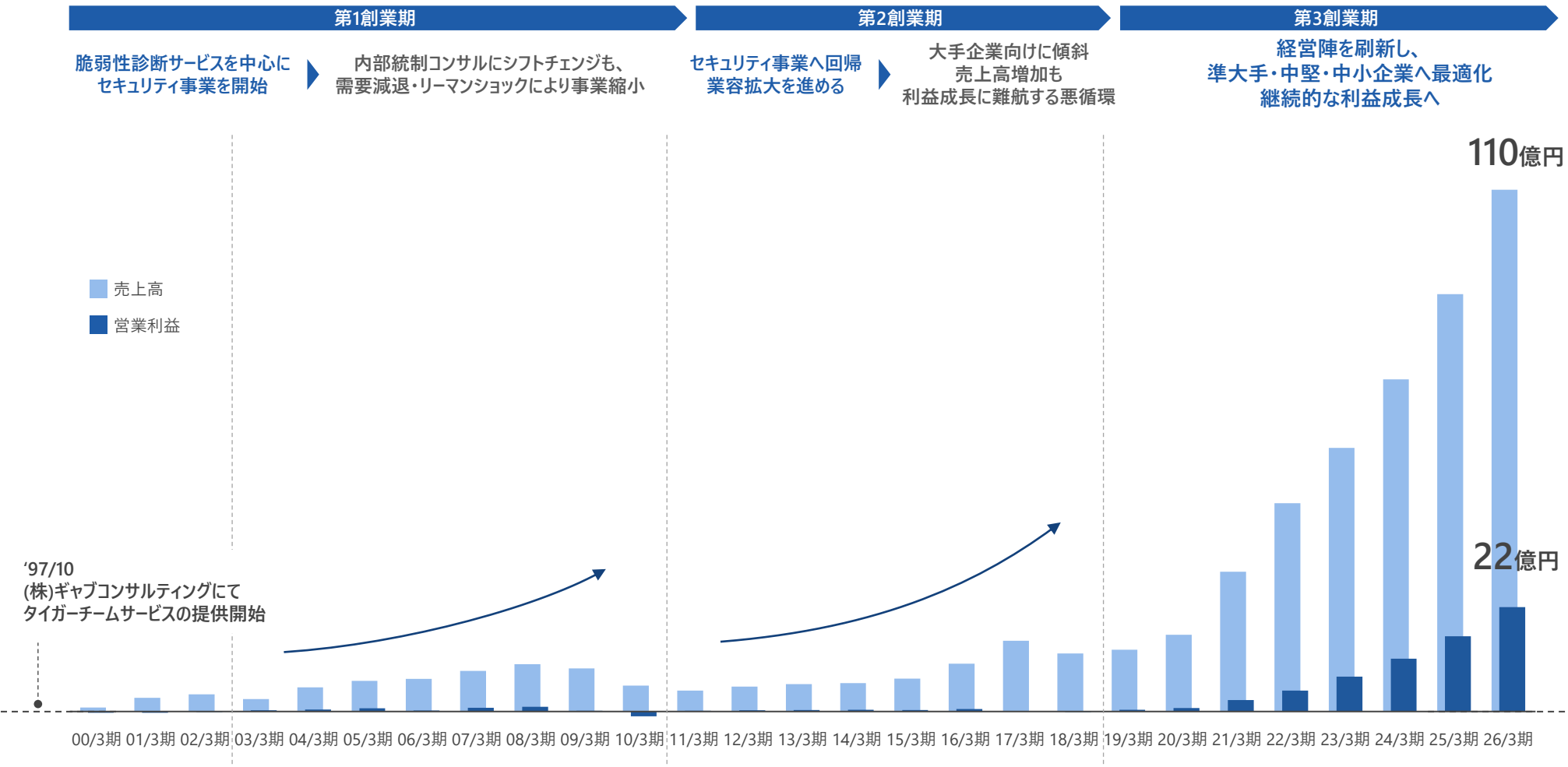
取締役
サイバーセキュリティ事業本部 副本部長

後藤　慶
Kei Goto

沿革：サイバーセキュリティ市場の黎明期から存在するサイバーセキュリティ専門企業

当社の創業事業は、コンサルティング事業の脆弱性診断サービス。脆弱性診断サービスを軸に国内サイバーセキュリティ市場の黎明期からサービスを提供開始し、セキュリティノウハウを蓄積しつつ、周辺領域を取り込みながら事業を拡大

第1創業期・第2創業期の経験を活かし、準大手・中堅・中小企業向けにサービスを最適化することで継続的な利益成長フェーズに突入

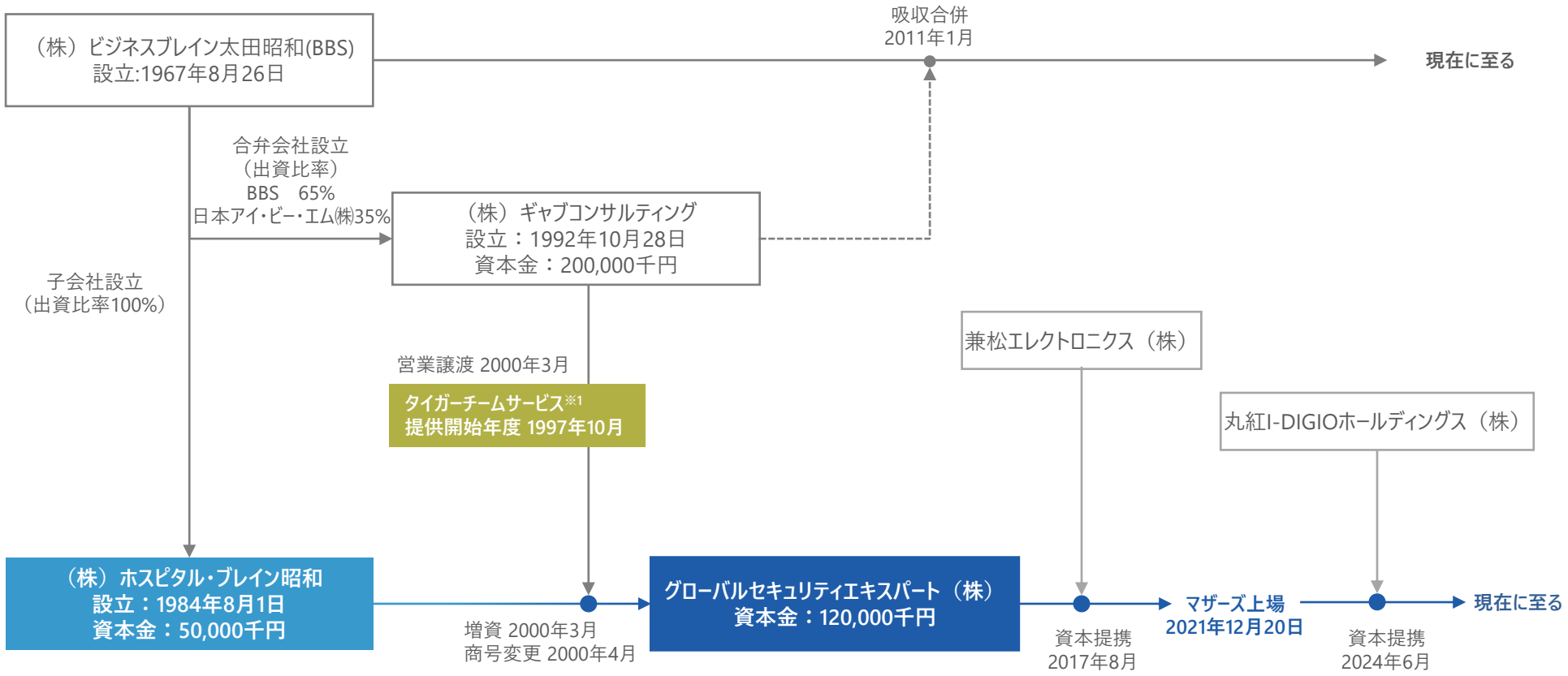


注釈 ※１：創業は1984年設立の(株)ホスピタル・ブレイン昭和。会社の成り立ちについてはAppendix参照
注釈 ※２：21/3期からは、2020年4月1日付で事業譲受したITソリューション事業を含む（21/3期ITソリューション事業の売上高は7.3億円）

当社の成り立ち

前身企業の(株)ホスピタル・ブレイン昭和が(株)ビジネスブレイン太田昭和の連結子会社として設立

2000年に(株)ホスピタル・ブレイン昭和へグループ企業からタイガーチームサービスの営業譲渡が行われ、それを機会としてサイバーセキュリティの専門企業として生まれ変わり、現在の社名に変更

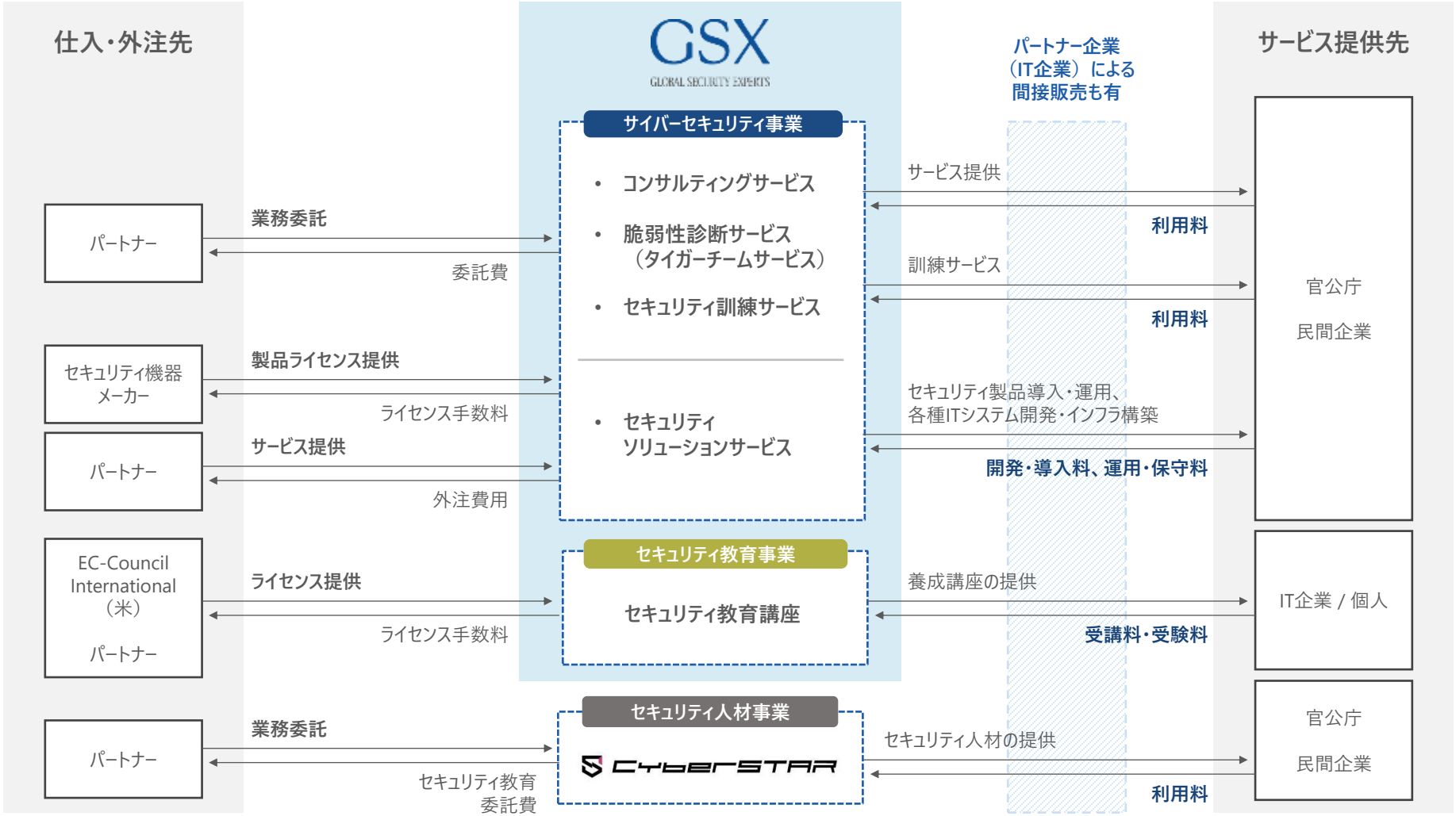


注釈（1）：　タイガーチームサービスとは、侵入検査/模擬攻撃検査サービスのこと

事業系統図

セキュリティソリューションサービス、セキュリティ人材事業は主にストック収入

その他のサイバーセキュリティ事業、セキュリティ教育事業は主にフロー収入



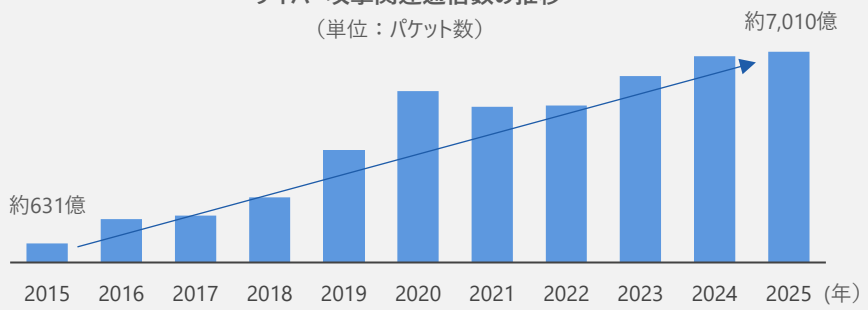
国内サイバーセキュリティ市場を取り巻く市場環境

サイバーセキュリティ市場では、対策需要が増加。また、企業の急速なデジタル化の進展が同市場の成長への追い風
一方で、未曾有のセキュリティ人材不足が課題

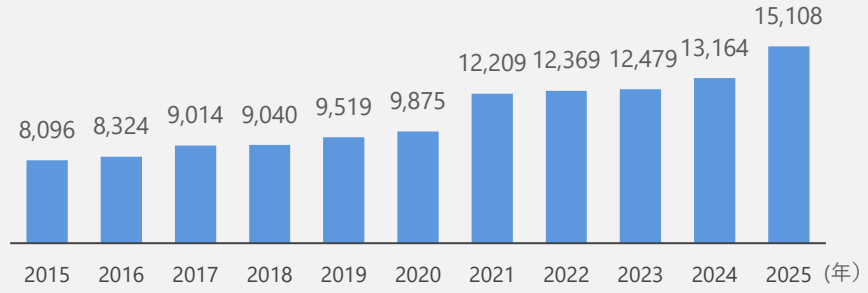
この市場環境の中で、セキュリティ教育やセキュリティ実装の上流から下流までワンストップで展開する当社へのニーズが高まっている

サイバー攻撃（脅威）の増加

－サイバー攻撃関連通信数の推移－※1
（単位：パケット数）



－サイバー犯罪の検挙件数の推移－※2
（単位：件）



急速な企業のデジタル化

－ニューノーマル市場の成長－※3

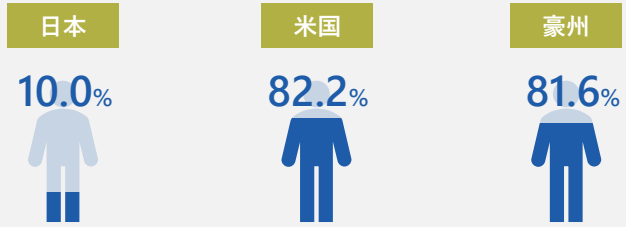
2020年度見込
8,787億円
+66%
2025年度予測
1兆4,593億円

－DX市場の成長－※4

2019年度
7,912億円
+285%
2030年度予測
3兆425億円

セキュリティ人材不足

－セキュリティ対策に従事する人材の充足度(各国比較)－※5



出所 ※１：国立研究開発法人情報通信研究機構「NICTER観測レポート2025」
出所 ※２：「令和７年におけるサイバー空間をめぐる脅威の情勢等について」（警察庁）
https://www.nict.go.jp/press/2026/02/05-1.html
https://www.npa.go.jp/bureau/cyber/pdf/R07_cyber_jousei.pdf

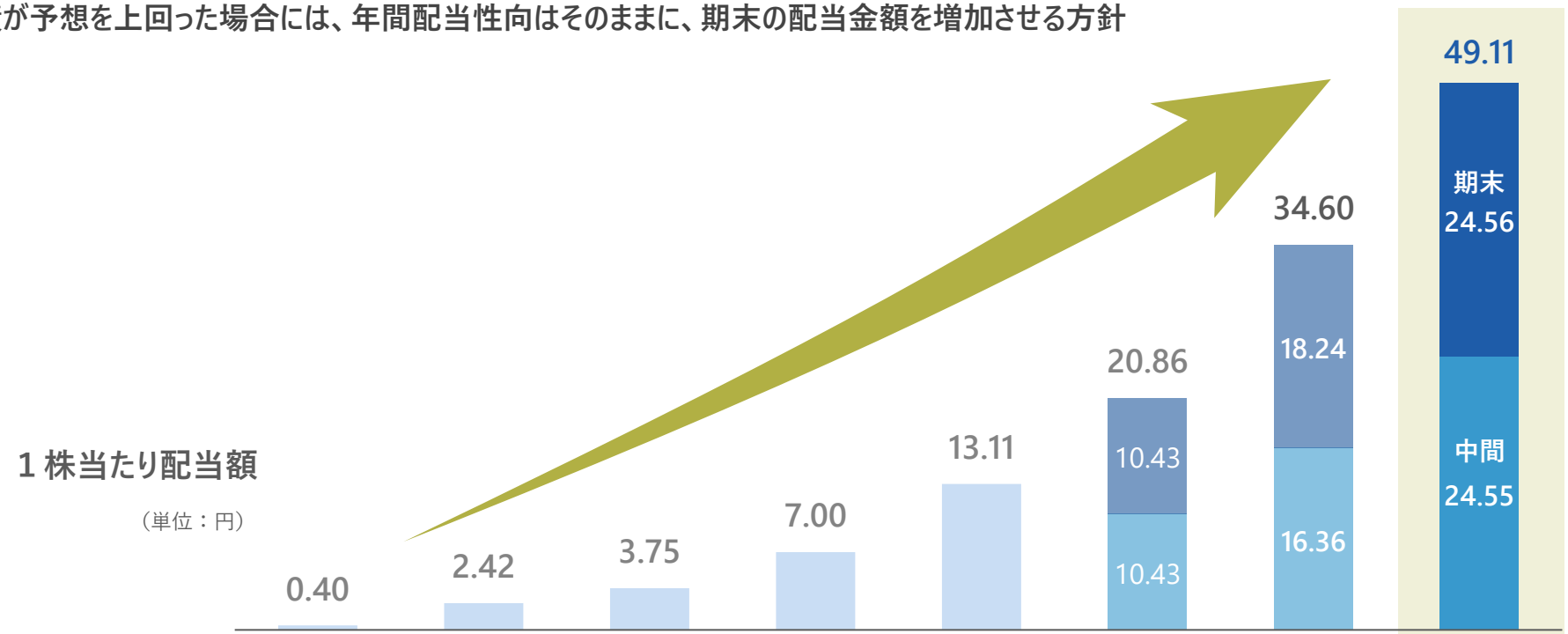
出所 ※３：富士キメラ総研「After／Withコロナで加速するニューノーマル時代のICT変革ソリューション市場」
出所 ※４：富士キメラ総研「2020 デジタルトランスフォーメーション市場の将来展望」
出所 ※５：「企業における情報セキュリティ実態調査2020」NRIセキュアテクノロジーズ

配当について

2026年3月期は期末の配当金額を増加し、従来予想比+1.87円UP

2027年3月期の年間配当性向は前期＋2.0ptの37.0％

業績が予想を上回った場合には、年間配当性向はそのままに、期末の配当金額を増加させる方針



	2020/3期	2021/3期	2022/3期	2023/3期	2024/3期	2025/3期	2026/3期	2027/3期（予想）
配当性向	11.45%	17.67%	18.54%	19.39%	25.0%	31.0%	35.0%	**37.0%**

注釈：2025年3月期以前の配当額は、これまでに実施した株式分割を考慮した金額

株主優待制度

株主の皆様へ日頃のご支援に対する感謝を表すとともに、当社銘柄の保有魅力向上を目的に年２回株主優待を実施

基準日	**年2回** 毎年**3月31日**及び**9月30日**
優待内容	**いずれか1点** ■ QUOカード 2,000円分 ■ （セキュリティ教育サービス）SecuriST CISO 講座 ■ （セキュリティ教育サービス）SecuriST ゼロトラストコーディネーター 入門編／基礎編 ■ （セキュリティ教育サービス）SecuriST 認定 Web アプリケーション脆弱性診断士 ■ （セキュリティ教育サービス）SecuriST セキュリティパスポート
対象となる株主様	各基準日時点の株主名簿に記載または記録された2単元（200株）以上の当社株式を保有され、かつ、**半年以上**継続保有されている株主様

免責事項

- 本資料には、将来の見通しに関する記述が含まれています。これらの記述は、当該記述を作成した時点における情報に基づいて作成されたものにすぎません。さらに、こうした記述は、将来の結果を保証するものではなく、リスクや不確実性を内包するものです。実際の結果は環境の変化などにより、将来の見通しと大きく異なる可能性があることにご留意ください。
- これらの将来展望に関する表明の中には、様々なリスクや不確実性が内在します。既に知られたもしくは未だに知られていないリスク、不確実性その他の要因が、将来の展望に関する表明に含まれる内容と異なる結果を引き起こす可能性がございます。
- また、本資料に含まれる当社以外に関する情報は、公開情報等から引用したものであり、かかる情報の正確性、適切性等について当社は何らの検証も行っておらず、またこれを保証するものではありません。
- 本資料は今後、事業年度末後の6月下旬に、各種KPIの計画数値や実績数値、経営戦略の進捗を更新する予定です。