GSX

GLOBAL
SECURITY
EXPERTS

2027年3月期 第1四半期
決算説明資料

グローバルセキュリティエキスパート株式会社　4417

2026年7月

Agenda

GSX
GLOBAL
SECURITY
EXPERTS

2027年3月期 第1四半期 業績ハイライト

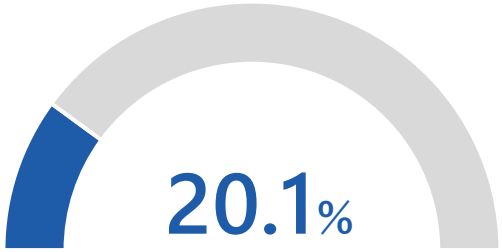
2027年3月期　第1四半期業績ハイライト

売上高

26/3期 1Q
2,237百万円

2,772百万円

前年同期比 ＋23.9%



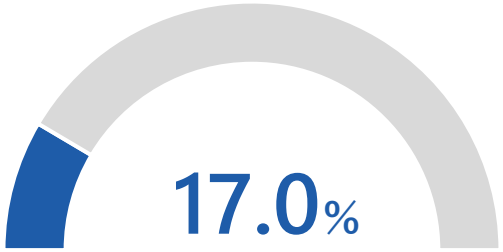
20.1%
進捗率

営業利益

26/3期 1Q
352百万円

499百万円

前年同期比 ＋41.7%



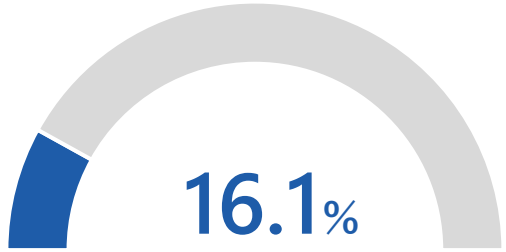
17.0%
進捗率

四半期純利益

26/3期 1Q
200百万円

321百万円

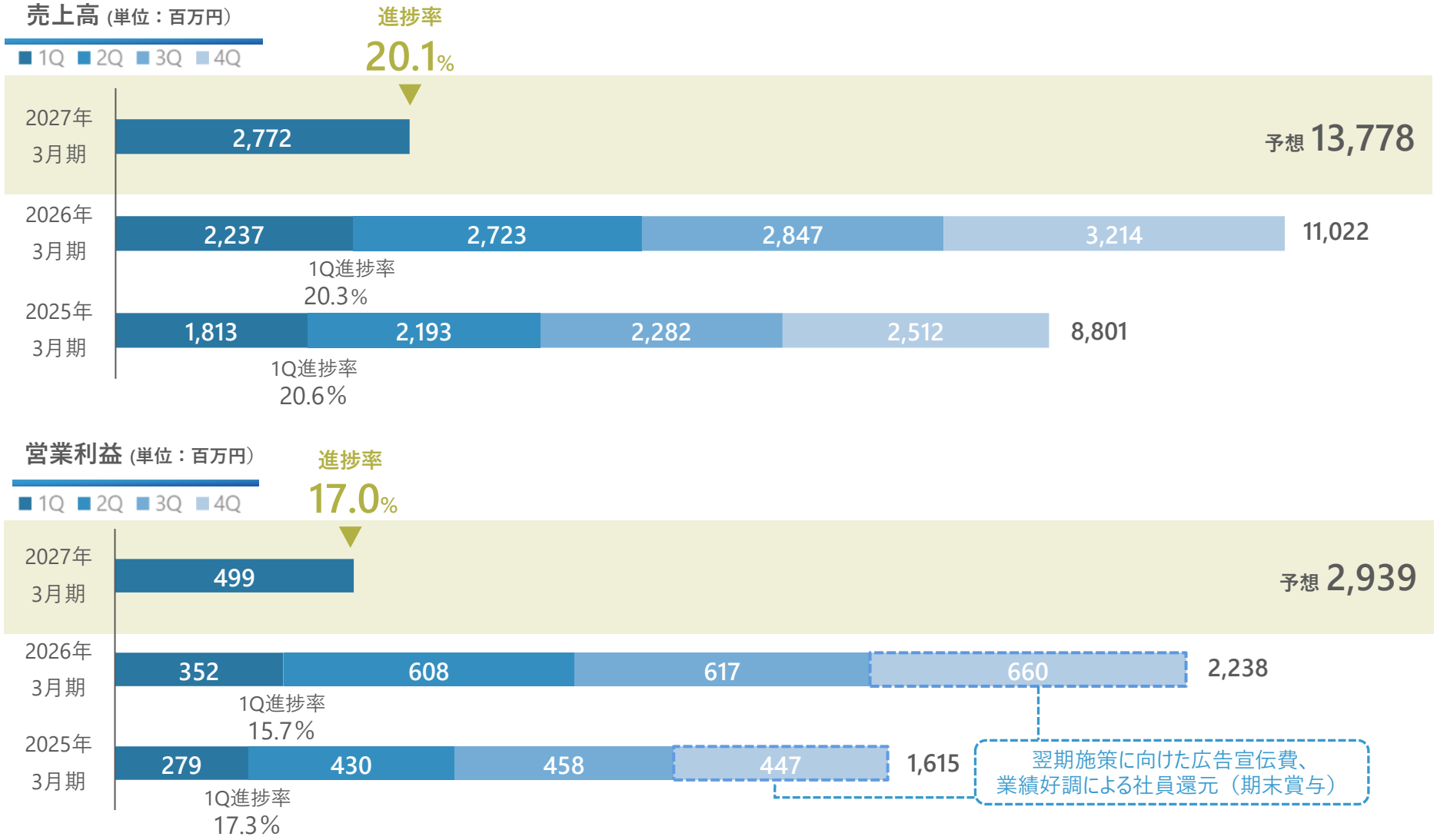
前年同期比 ＋60.9%



16.1%
進捗率

通期業績予想に対する進捗

売上高・営業利益ともに計画通りの進捗

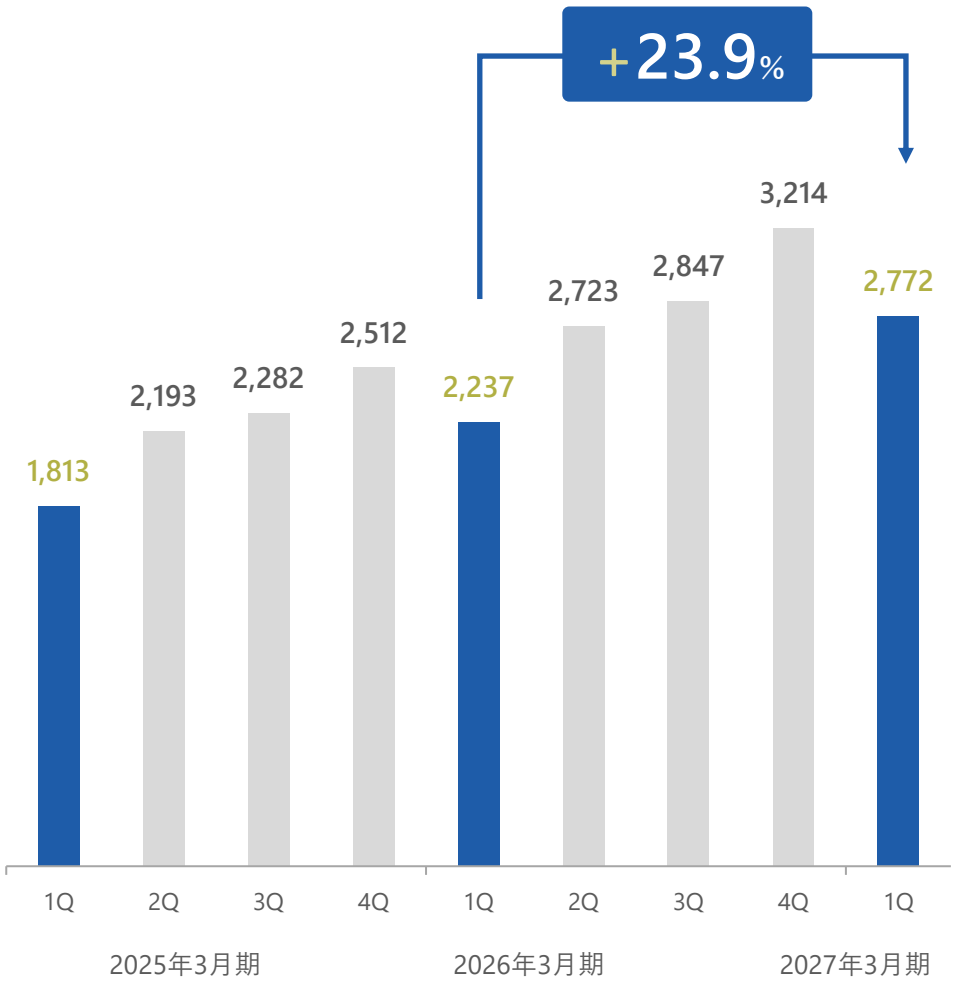


- 前年同期比増収増益　第１四半期業績として過去最高額を更新
- 通期業績予想に対して計画どおりの進捗
- 「準大手・中堅・中小企業向けセキュリティサービス」
  「IT企業・SIer向けセキュリティ人材育成」「あらゆる企業向けセキュリティ人材提供」
  顧客ターゲットごとのビジネス戦略によりすべての事業ドメインで業績伸長
- 「AI台頭時代の成長戦略」「全国展開による成長戦略」を着実に遂行

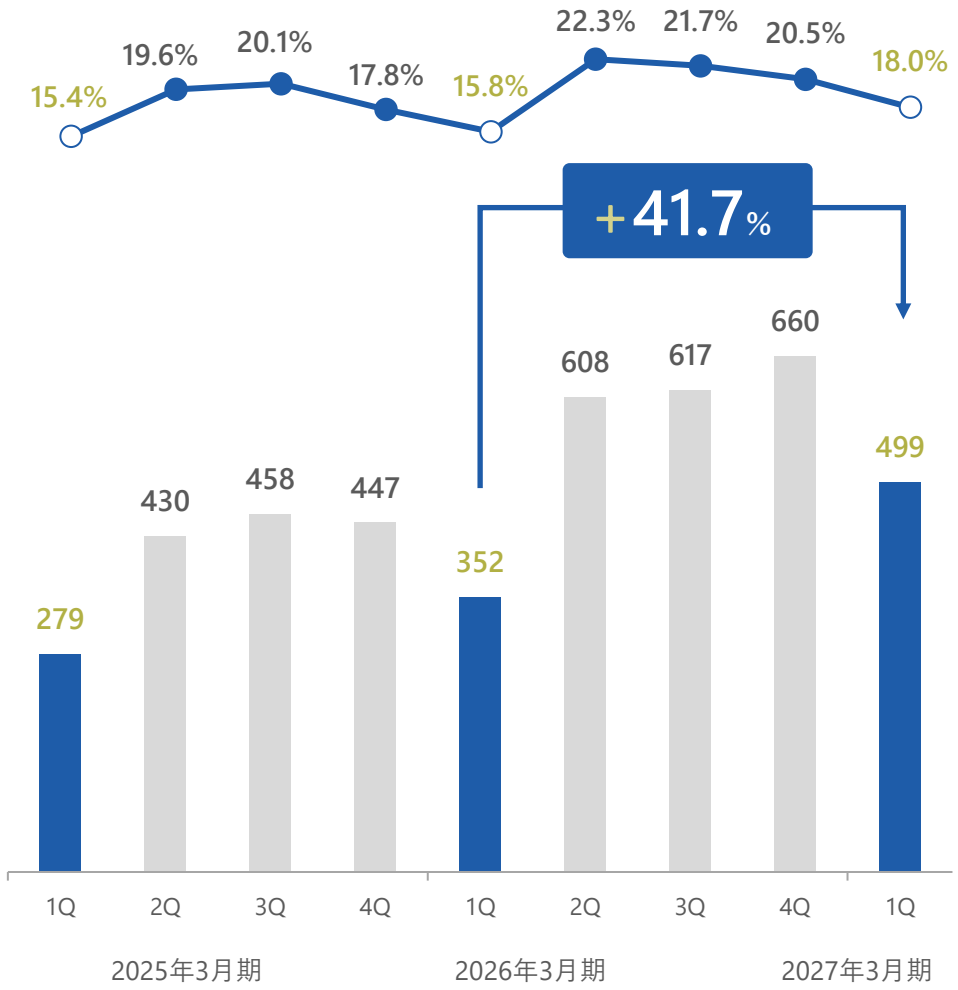
売上高・営業利益　四半期推移（会計期間）

前年同期比で売上高は+23.9%、営業利益は+41.7%と計画通りに成長

売上高（単位：百万円）



営業利益・営業利益率（単位：百万円・%）



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

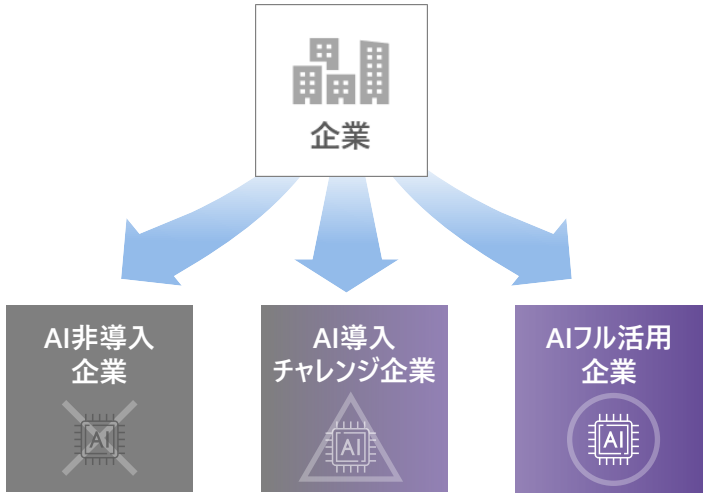
GSXのビジネスにとって強い追い風となる

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

フロンティアAIがGSXビジネスにもたらす影響

2026年5月　政府は、AI性能の高度化を踏まえたサイバーセキュリティ対策強化について注意喚起を発出

政府　**電力・ガス・金融・情報通信・交通などの重要インフラ事業者に対する要請**

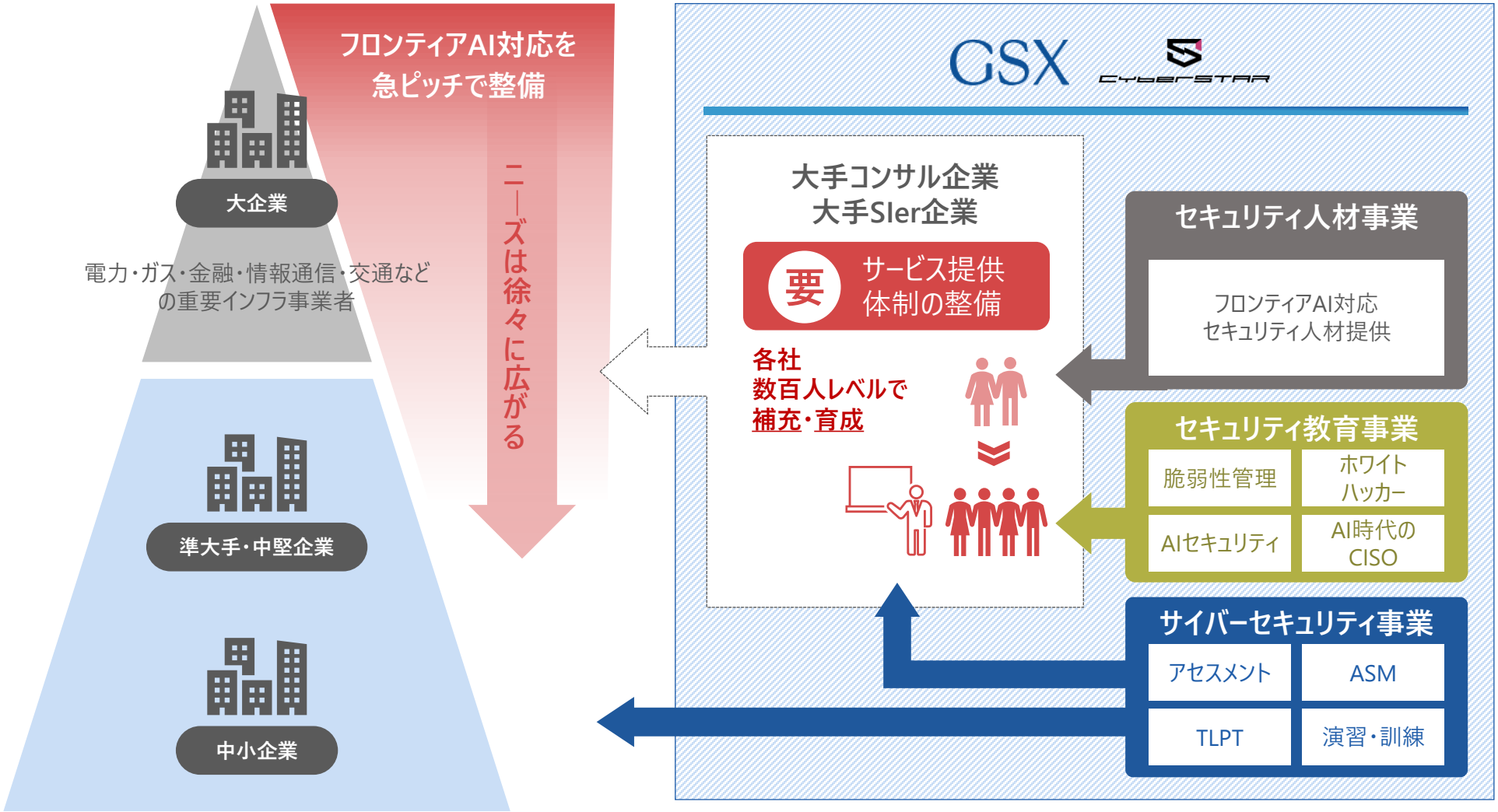
- フロンティアAIの活用により、高速かつ大量に脆弱性が発見・修正されることへの対応
- フロンティアAIの悪用リスクに備えたサイバーセキュリティ対策の強化

金融庁・日本銀行が金融機関に求める９つの短期的対応要請

	要請事項	主旨
①	経営課題として扱う	全社横断連携・経営トップのコミットメント
②	優先対応すべきサービス／ITシステムの特定	リスクベースで選別。外部公開系（ネットバンキング等）を最優先
③	特定資産の技術負債を解消	構成把握、不要ポート閉塞、特権ID削除、EOL製品更新
④	パッチ適用の人的リソース追加	自組織＋ベンダー双方のリソース確保
⑤	ベンダー維持保守契約の内容確認	役割分担、夜間・休日対応、SLA／SLO遵守の確認
⑥	パッチ適用プロセスのリスクベース化	CVSS依存の限界。攻撃成立の蓋然性評価、テストの合理化
⑦	パッチ適用以外の対策も強化	仮想パッチ／WAF、NW分離、MFA、EDR、多層防御
⑧	優先サービス／ITシステム停止への備え	BCPの有効性、能動的停止の判断基準・手順の明確化
⑨	外部との連携を維持・強化	金融ISAC・当局・コミュニティからの情報収集と共有

フロンティアAI対応ニーズとGSXグループの提供サービス

フロンティアAI対応ニーズはGSXグループのすべての事業に追い風



第43回定時株主総会
質疑応答集より

（ご参考）脆弱性診断サービスはAIに代替されず、需要はむしろ拡大

AIで自動化が進むのは診断工程の一部　発見した脆弱性への対応判断は人間にしかできない領域

AI活用の広がりで診断対象は増加、脆弱性診断サービスの需要は一層拡大していく

AIの進化により、脆弱性の発見は高速化・大量化

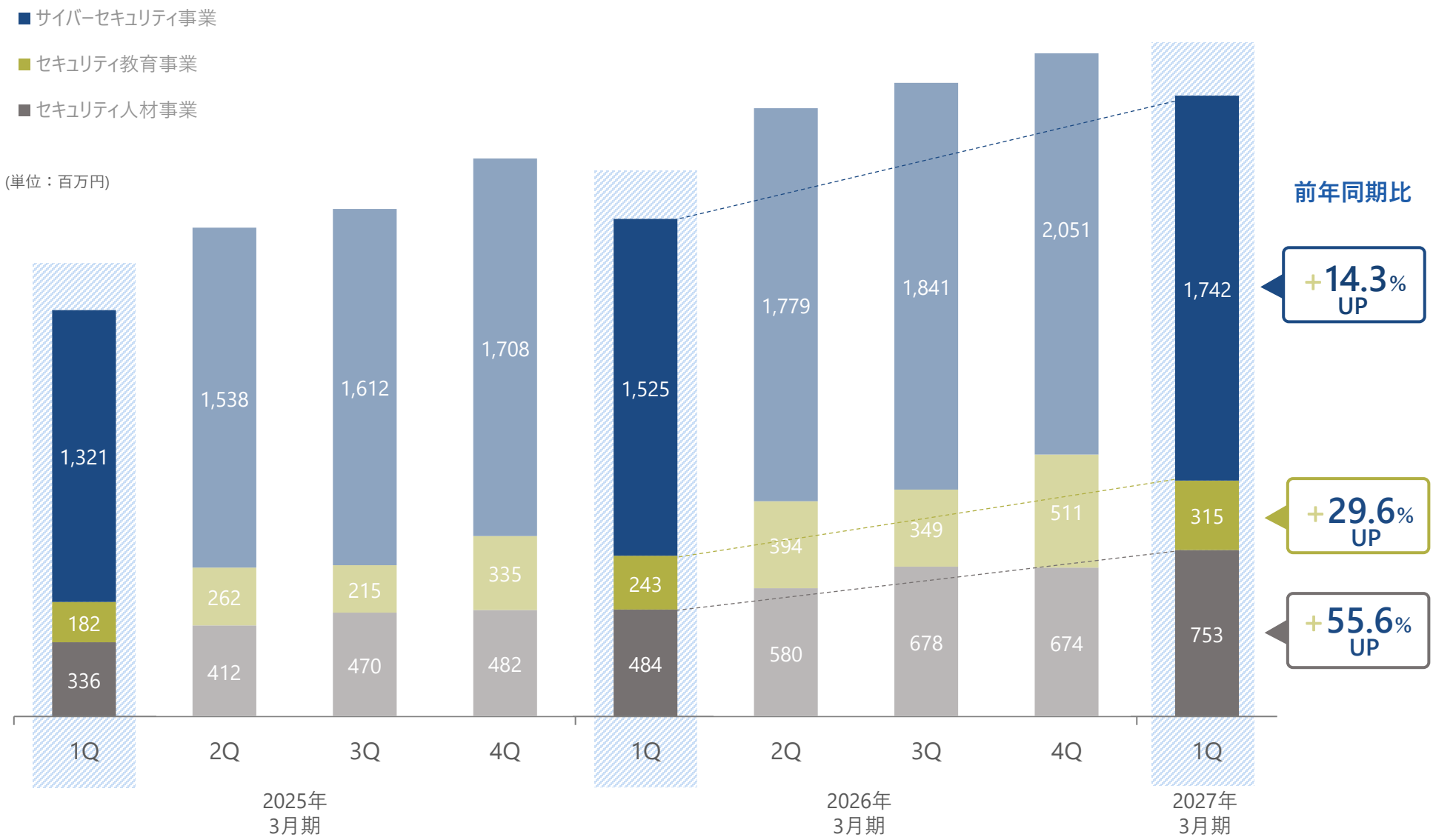
対策の優先順位付けや企業ごとに最適な対応は人の専門性が不可欠

AIと人を組み合わせた脆弱性診断サービスの需要は今後さらに拡大

GSX
GLOBAL
SECURITY
EXPERTS

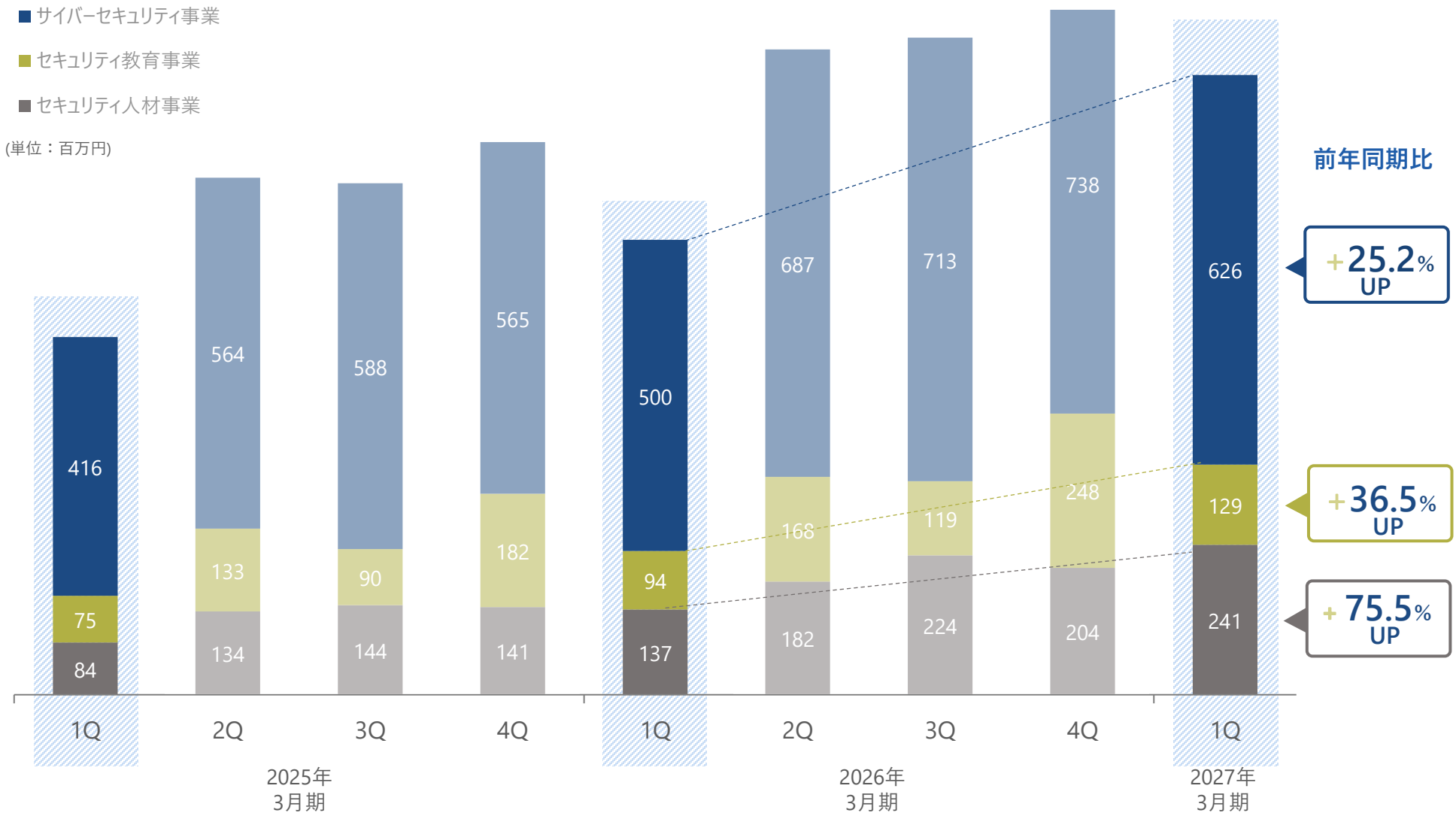
2027年3月期 第1四半期 事業別の業績概況

事業別売上高　四半期推移（会計期間）



※事業別売上高は内部取引消去前の数値

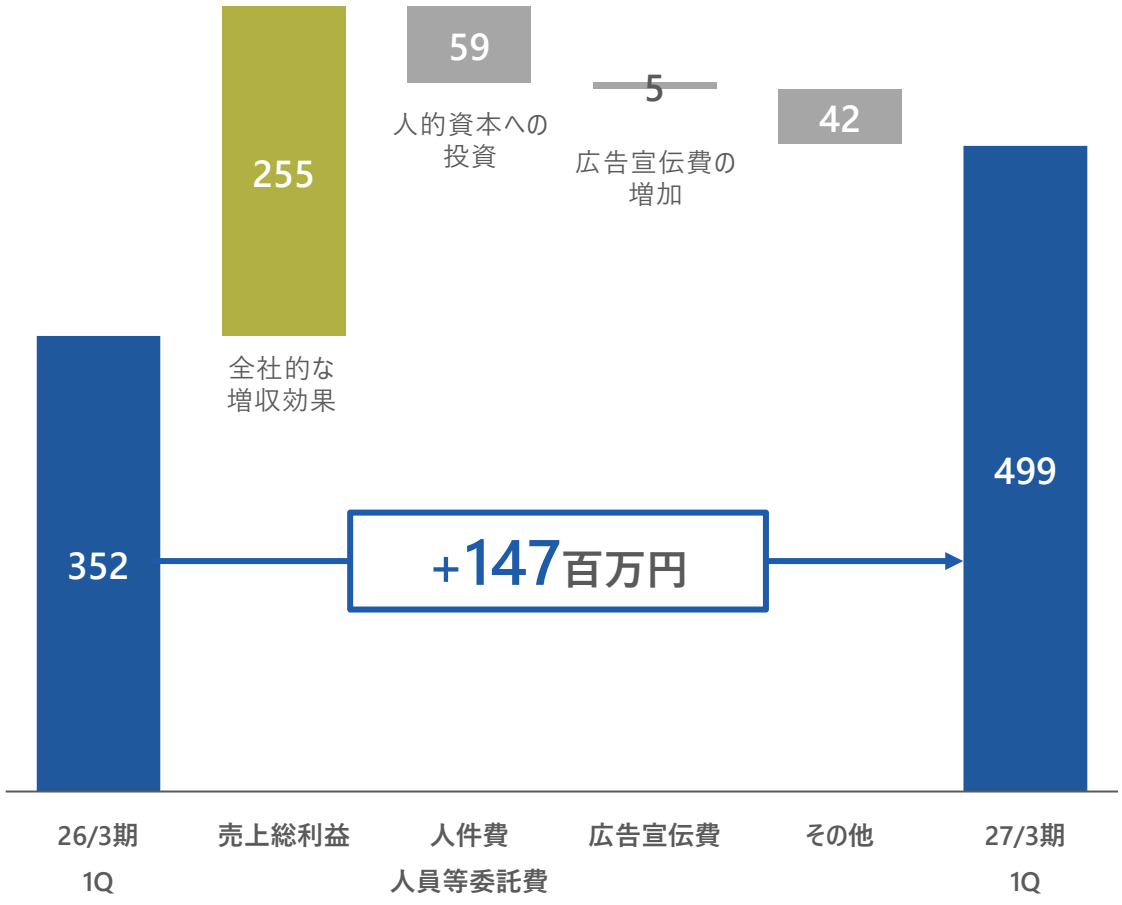
事業別売上総利益　四半期推移（会計期間）



営業利益増減分析 前年同期比

人的資本への投資を積極的に実施するも、それを超える成長により営業利益は前年同期比+147百万円

（単位：百万円）



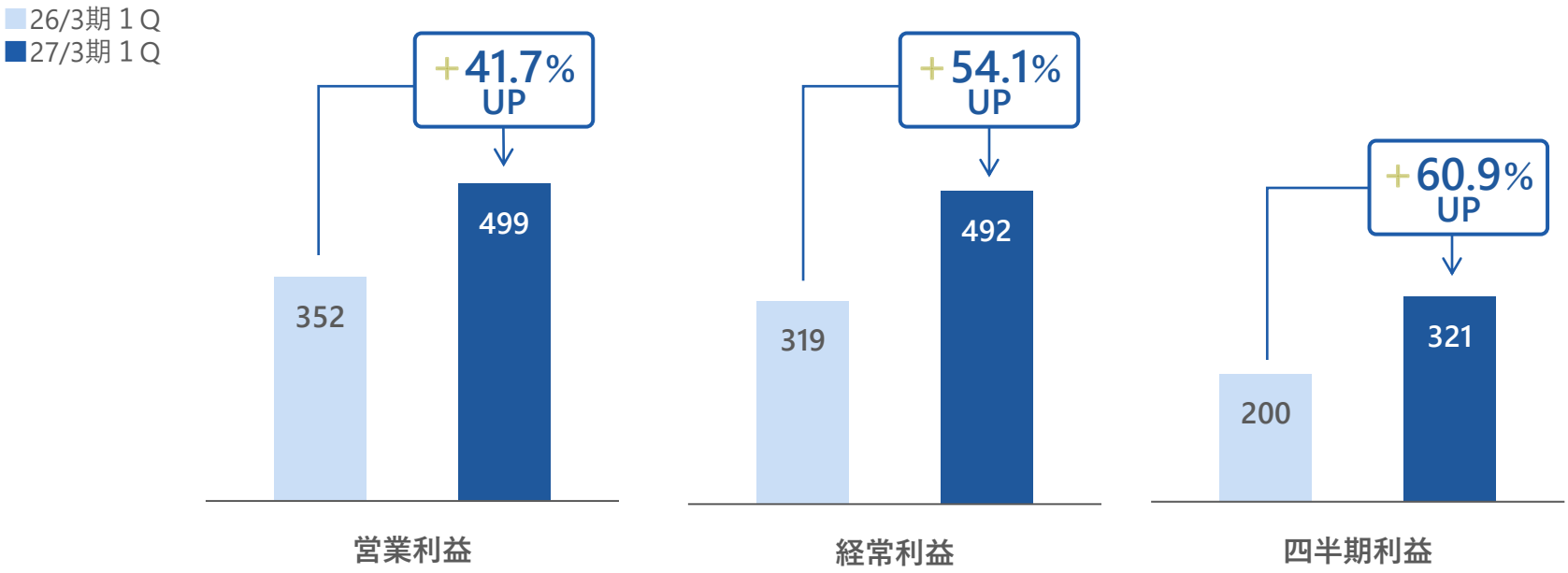
人的資本への投資 59百万円

- 新卒を含む社員数増加に伴う人件費増
- 社員の教育研修費

持分法適用会社による当社業績への影響

2025年3月期より連結決算に移行　株式会社ブロードバンドセキュリティ、株式会社セキュアイノベーションの損益を反映

利益の前年同期伸長率（単位：百万円）



経常利益の伸長率の理由

・持分法による投資損失の減少（前年31.1百万円→当期2.6百万円／ブロードバンドセキュリティ社等の業績改善による）

四半期純利益の伸長率の理由

・持分法による投資損失の減少に加え、前年計上の投資有価証券評価損等が当期は発生なし（3.0百万円）

連結P/L（累計期間）

（百万円）	2026年/3期 1Q実績	2027年/3期 1Q実績	前年同期比 増減額	前年同期比 増減率
売上高	2,237	2,772	+534	+23.9%
売上総利益	748	1,003	+256	+34.2%
売上高総利益率	33.4%	36.2%	+2.8pt	-
販売費・一般管理費	395	503	+109	+27.4%
販売費・一般管理費率	17.7%	18.2%	+0.5pt	-
営業利益	352	499	+147	+41.7%
営業利益率	15.8%	18.0%	+2.2pt	-
経常利益	319	492	+172	+54.1%
経常利益率	14.3%	17.7%	+3.4pt	-
当期純利益	200	321	+121	+60.9%
EPS（円）	13.32	21.42	+8.10	-

※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。

連結B/S

（百万円）	2026/3期	2027/3期 1Q	前期比 増減	前期比 増減率
流動資産	6,344	5,570	-774	-12.2%
現金及び預金	1,644	1,570	-73	-4.5%
売掛金及び契約資産	2,749	1,795	-953	-34.7%
その他	1,950	2,203	+253	+13.0%
固定資産	3,614	3,890	+275	+7.6%
有形固定資産	250	253	+3	+1.2%
無形固定資産	114	112	-1	-1.7%
投資その他の資産	3,249	3,524	+274	+8.4%
資産合計	9,959	9,460	-498	-5.0%
流動負債	4,280	3,679	-600	-14.0%
買掛金	512	383	-128	-25.1%
短期借入金	300	0	-300	-100.0%
1年内返済予定の長期借入金	217	203	-14	-6.4%
その他流動負債	3,250	3,092	-158	-4.9%
固定負債	1,277	1,334	+56	+4.4%
長期借入金	1,091	1,050	-40	-3.7%
その他固定負債	186	284	+97	+52.2%
純資産	4,401	4,446	+45	+1.0%
自己資本比率	44.2%	47.0%	+2.8pt	–

GSX

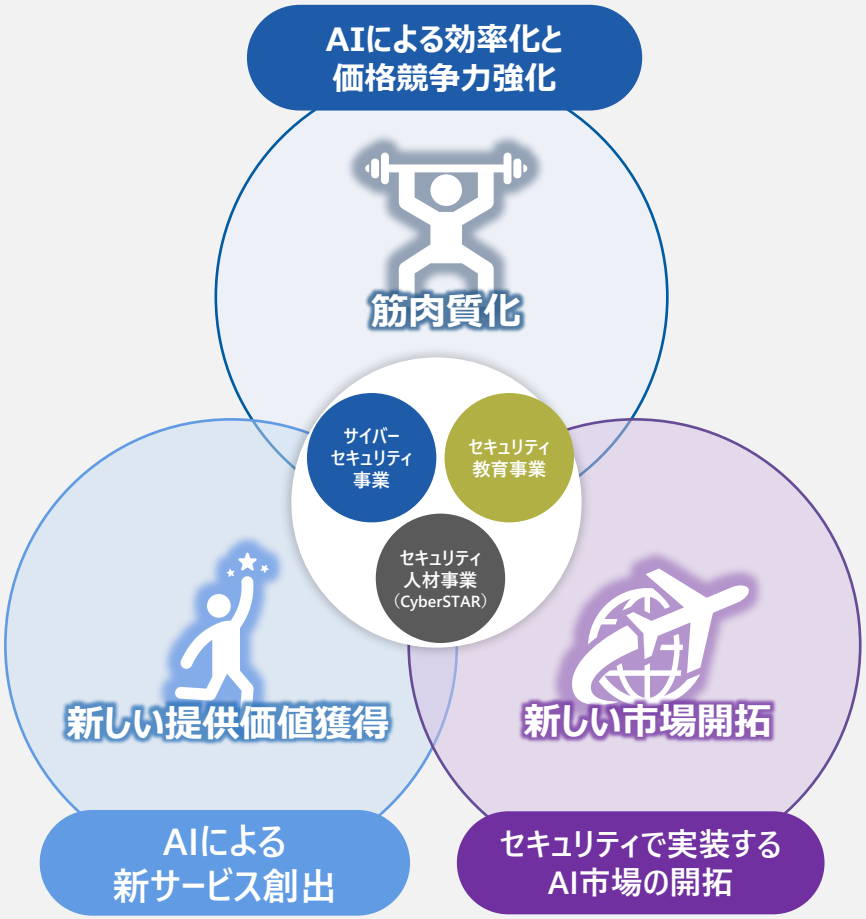
GLOBAL
SECURITY
EXPERTS

経営トピックス

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

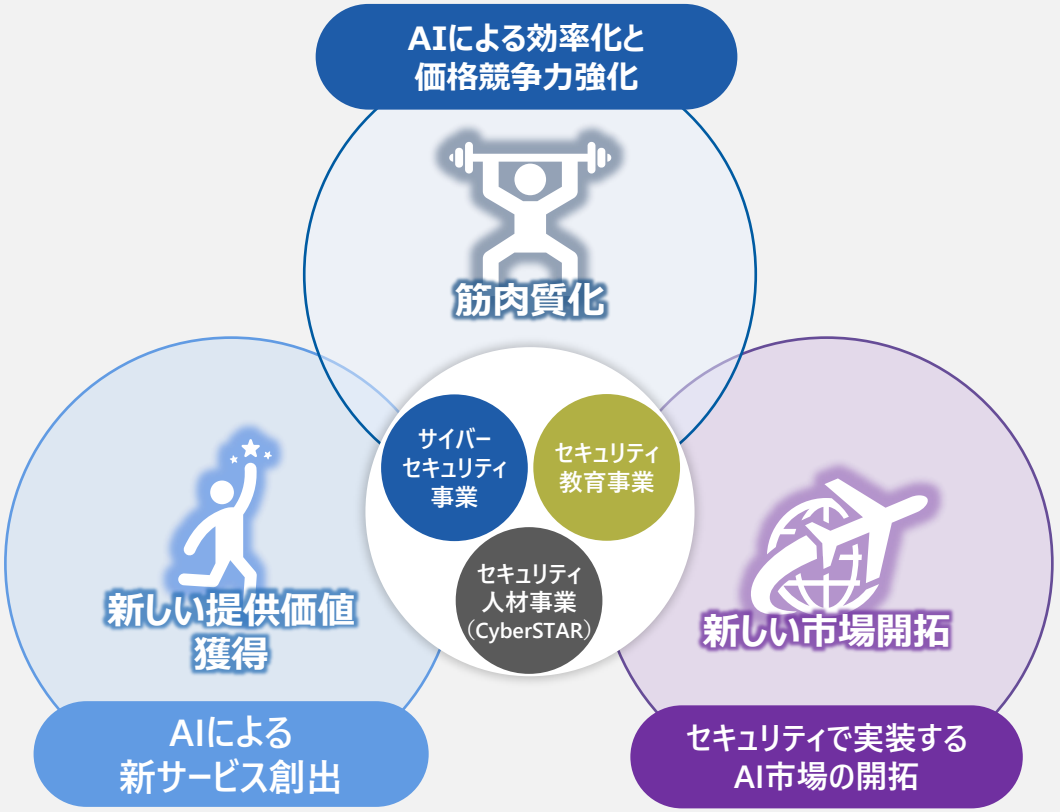
AI台頭時代の成長戦略



×

全国展開による成長戦略

AI台頭時代の成長戦略



AI台頭時代の成長戦略を実行する開発パートナーの獲得

AI・セキュリティ分野に強みを持つCoWorker株式会社と戦略的業務提携を締結

新サービスの開発やAI市場の開拓をより迅速かつ確実に推進する

戦略的業務提携

CoWorker
The Digital Improvement Studio

AIとセキュリティに特化したITコンサルティングおよび
サービス（製品）開発を得意とする技術者集団
顧客課題認識からAIを活用した戦略策定、新規サービスの立ち上げ
運用最適化までを伴走するスタイル
“0→1→運用最適化”を実践しビジネスを伸長

技術力　スピード　0→1　AIセキュリティ

戦略実行の「スピード」「確からしさ」アップ

本提携を通じ
- **成長戦略を具体施策へ落とし込む**
- **開発・提供のリードタイムを短縮**
- **サービス品質を担保する体制構築**

AI台頭時代の成長戦略

→GSXグループの既存ビジネスの強みをベースに
AI技術を取り込み実現し得る

AIによる効率化と価格競争力強化 → 筋肉質化

AIによる新サービス創出 → 新しい提供価値獲得

セキュリティで実装するAI市場の開拓 → 新しい市場開拓

生成AI時代に対応する「AIプロンプト診断」を提供開始

生成AIの利用拡大により、新たなセキュリティリスクへの対応が企業の重要課題に

GSXはAI時代に対応した診断サービスを提供し、新たなセキュリティ需要を取り込むサービスとして展開

市場環境

生成AI活用の拡大

- 企業で生成AI導入が急速に拡大
- AI特有のセキュリティリスクが顕在化
- 従来の脆弱性診断だけでは対応困難

機密情報の漏えい

著作権侵害

ハルシネーションによる
誤情報拡散

企業の信用を揺るがす
重要なインシデントに繋がる可能性

GSXの新サービス

AIプロンプト診断

- AI特有の脆弱性を網羅的に診断
- 生成AIの利便性を享受しながら
  経営層が安心できるセキュリティレベルを確保

※OWASP（Open Web Application Security Project）：ソフトウェアのセキュリティ向上を目的とした非営利団体
LLM Top 10：大規模言語モデル（LLM）を活用したアプリケーションにおけるセキュリティリスクに対処するためのガイドライン

AI関連の教育講座を続々リリース

GSXオリジナル講座「SecuriST 認定AIセキュリティエンジニア」はリリースから4か月で受講者数900名を突破

AIセキュリティ人材を育成する教育講座を続々リリース

リリース4か月
受講者数
900名超

受講者アンケートの結果

「AIセキュリティの全体像が体系的に理解できた」との声が多数

受講者全員が「業務に活用できる」と回答

100%
講座全体・講師への満足度 ※

100%
業務への活用期待度 ※

アプリケーション開発やインフラ系エンジニア向け
AIを組み込む際のリスク判断や安全設計のポイントを習得

近日リリース予定のAI関連講座

◆ **経営層向けAIセキュリティ講座**
ビジネスとしてのAI活用・対応を、経営層としてどの様に判断し、推進すべきかの指針を学ぶ

◆ **セキュアAIエージェント実装**
AIエージェントを安全に設計・実装するための実践知を習得

◆ **脆弱性管理士（フロンティアAI対応）**
AI時代に求められる脆弱性管理の考え方と「何から優先して対応すべきか」を学ぶ

◆ **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

他にも複数準備中

※2026年3月24~25日に実施した初回講義のアンケート結果をもとに作成

AIを活用した新サービスのローンチ

AIが80%自動化・専門家が20%伴走

相談の一次回答やリスク検知をAI が常時自動で実行　複雑案件やインシデント対応はGSX の専門家が対応

近日リリース予定

GSX One

AIを活用した中小企業向けのサブスクリプション型総合セキュリティサービス。リーズナブルな価格で導入でき、AIによる脅威の検知とセキュリティ専門家による分析・対応を組み合わせることで、企業のセキュリティ運用を包括的に支援。

- AI セキュリティ相談
- チェックリスト AI
- ASM※ / Security Scorecard

など

※アタックサーフェスマネジメント／攻撃者視点によるIT資産の脆弱性管理

GSXグループ　AI活用の進捗

「2026年度 上期中にGSXグループの全社員がAIを使いこなす」を全体方針として掲げ

「AI台頭時代の成長戦略」を強く推進する基盤を構築中

これまでの動き

2026.04
AI推進チーム 組成
各本部・拠点・CyberSTAR横断のメンバーで発足

2026.06
AI利用規程 制定
全員が安心してAIを最大限活用できる土台を制定。AIコンサルティングサービスのベースが完成

2026.06
AIスキルレベル 定義
全員が目指すべきAI活用スキルのレベルを明確化

2026.06
AIスキルレベルテスト 実施
全員がAIスキル レベル 0 テスト合格。AI活用のベースが完成

2026.06
AIライセンス配布
全社員がClaudeライセンスを完全保有。その他のAIライセンスも申請・入手できる環境を整備

2026.05 継続
AIに関する情報共有
AI活用に関する知見・業界動向を毎週社内共有。全社員が常時アップデート

これからの動き

1. 人材育成
外部専門家によるAI研修
全社員のAI活用スキルを底上げ。

2. 業務変革
利用推進による業務効率化
具体的なAI利用を推進し、日々の業務における効率化を実現していく。

3. 事業成長
サービス拡充
サービス特別サイトのローンチを含め、AI関連サービスを拡充していく。

全国展開による成長戦略

- ✓ 地方銀行との提携による販路拡大
- ✓ 既存販売チャネルの強化
- ✓ 全国へのGSX拠点拡大

全国へのGSX拠点拡大

全国規模でより安定的なサービス提供体制に　GSXのミッション・パーパスをさらに加速させる

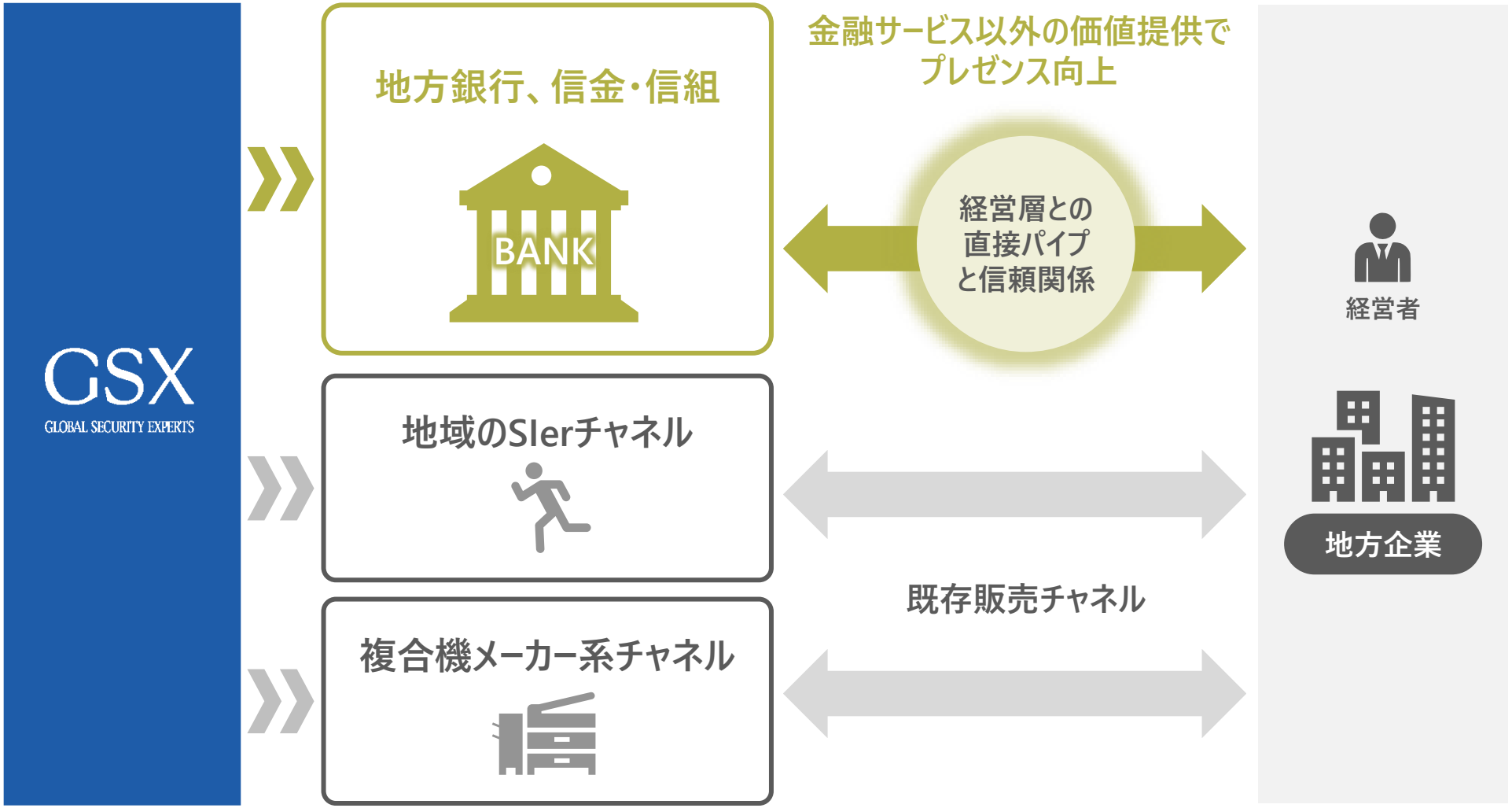
-Mission-
日本全国の企業の自衛力を向上すること

-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

既存販売チャネル・地方銀行との提携による販路拡大

従来の主要販売経路に、地方銀行を入口としたチャネルが追加され、サービス提供機会が大きく拡大

地方銀行のプレゼンス向上にも寄与する提携モデルで全国展開を加速



GSX
GLOBAL
SECURITY
EXPERTS

2027年3月期 連結業績予想

基本方針

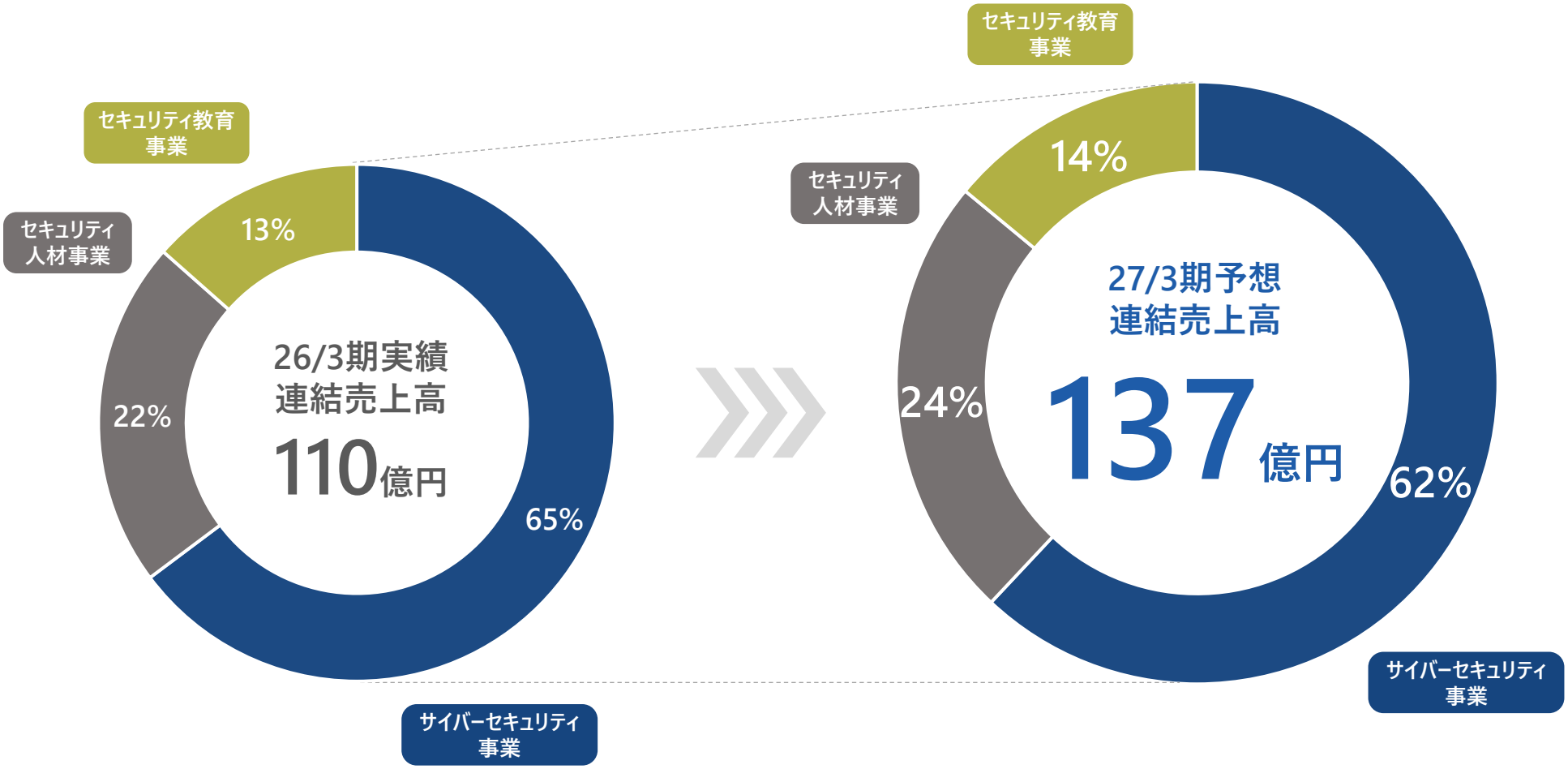
売上高拡大は継続、利益率の向上を重要視し
中長期成長を支える経営基盤を強固にする

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	701	+31.3%
営業利益率	20.3%	21.3%	+1.0pt	-
経常利益	2,222	2,973	750	+33.8%
経常利益率	20.2%	21.6%	+1.4pt	-
当期純利益	1,486	1,998	511	+34.4%
EPS（円）※	98.85	133.19	34.34	-

※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。

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

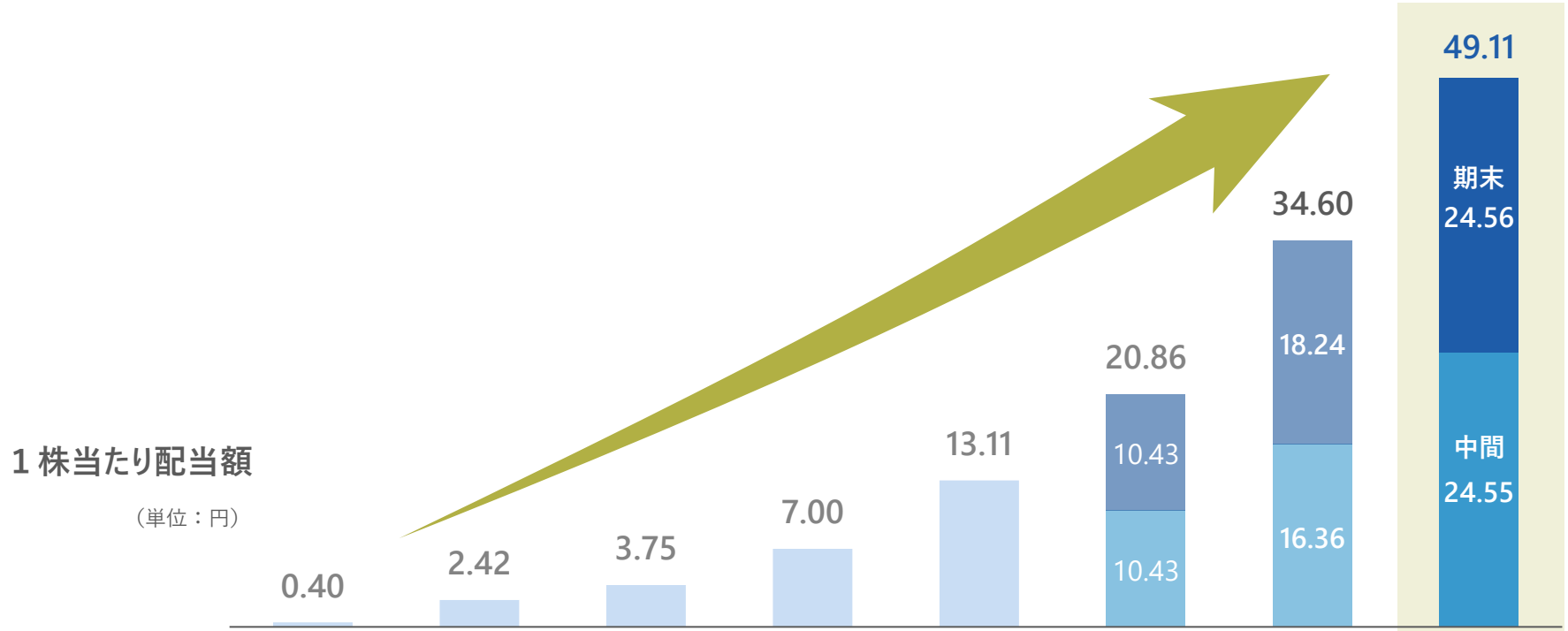
GLOBAL
SECURITY
EXPERTS

株主還元

配当について

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

株主優待の拡充

株主の皆様の利便性向上を目的に、QUOカードをデジタルギフトに変更

選択できるセキュリティ教育サービスに大好評の「SecuriST 認定AIセキュリティエンジニア」をラインナップ

	従来の優待内容	変更後の優待内容
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 • SecuriST ゼロトラストコーディネーター 入門編／基礎編 • SecuriST 認定 Webアプリケーション 脆弱性診断士 • SecuriST セキュリティパスポート	デジタルギフト®2,000円相当 NEW セキュリティ教育サービス  SecuriST CISO講座／SecuriST ゼロトラストコーディネーター 入門編／基礎編／SecuriST 認定Webアプリケーション脆弱性診断士／SecuriST セキュリティパスポート／SecuriST 認定AIセキュリティエンジニア NEW

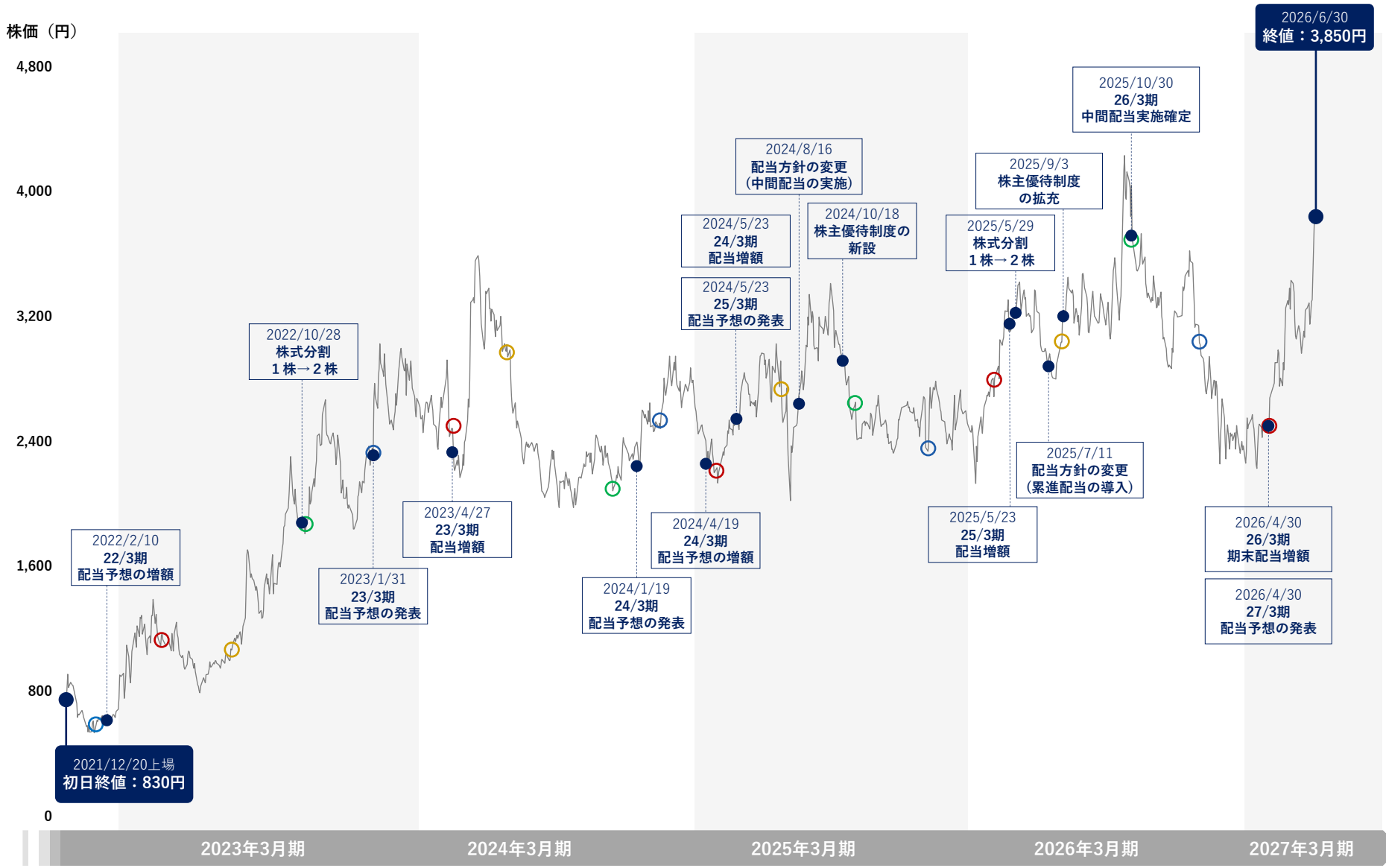
▼変更なし

基準日	年2回 毎年**3月31日**及び**9月30日**
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

株価推移（上場～2026/6/30）

決算発表：1Q 2Q 3Q 4Q

株価は上場時から安定的に上昇



※初日終値は、上場以降に実施した株式分割を考慮した金額を表示しております。

GSX
GLOBAL
SECURITY
EXPERTS

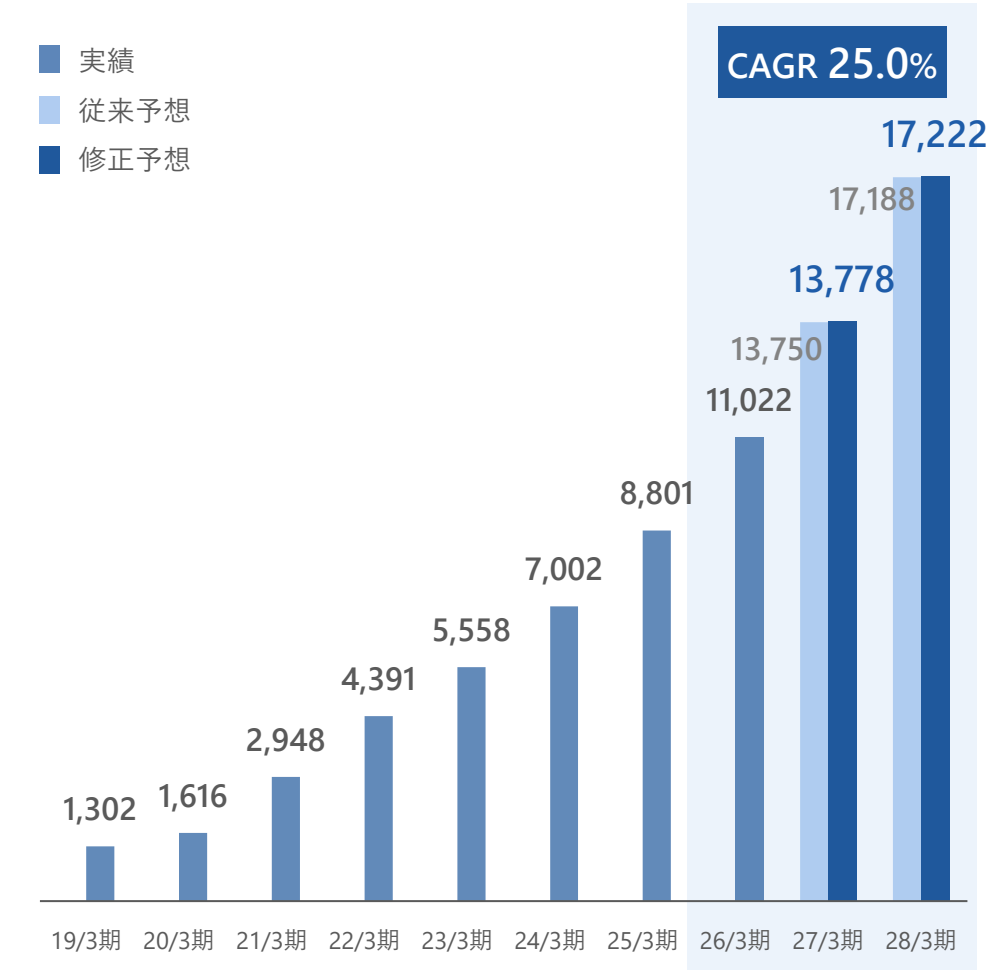
中期経営計画と成長戦略

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

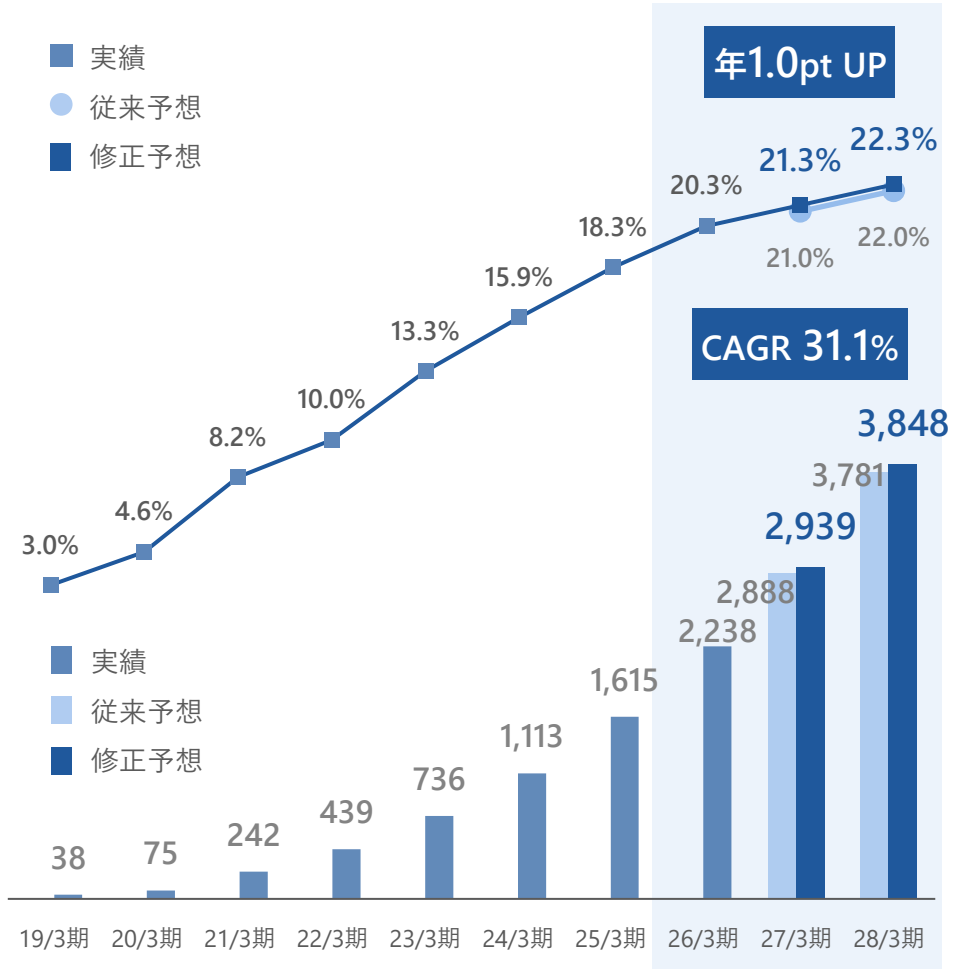
売上高

(単位：百万円)



営業利益及び営業利益率

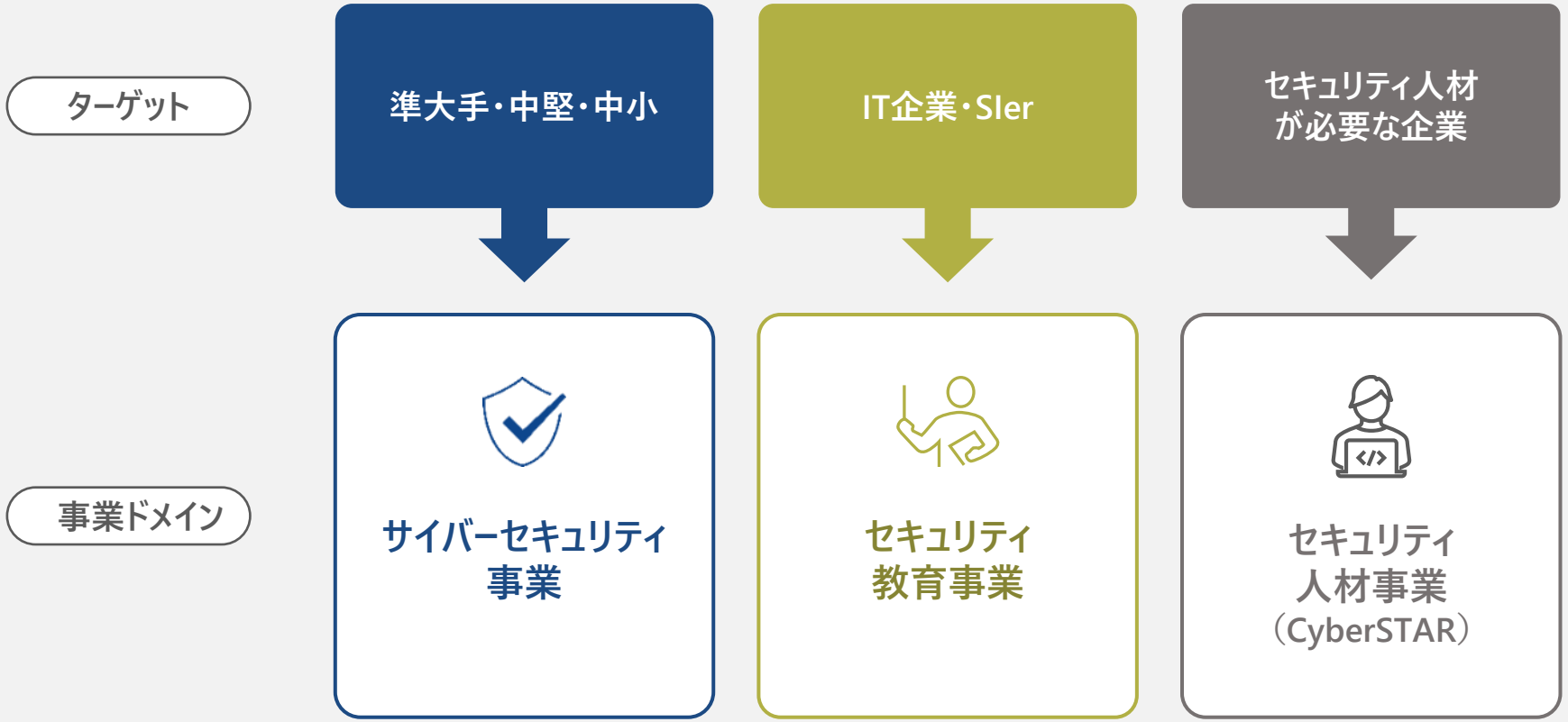
(単位：百万円)



※2025年3月期より連結業績

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

GSX
GLOBAL SECURITY EXPERTS

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

セキュリティ訓練サービス

コンサルティング

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

緊急対応

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

セキュリティソリューション
導入・運用

脆弱性診断

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

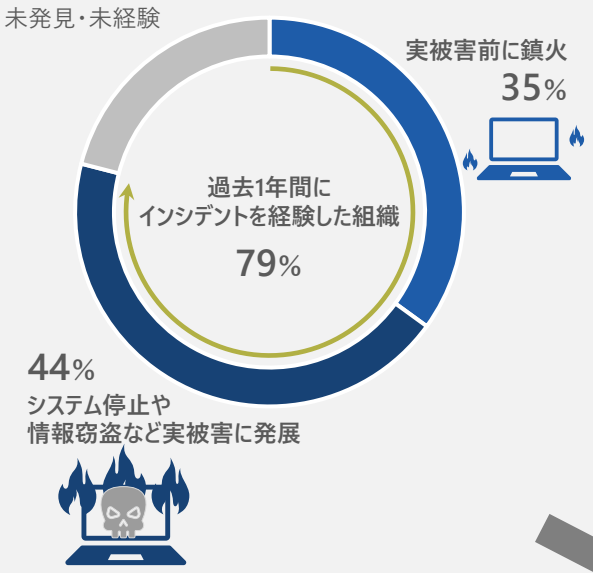
脆弱性診断サービス（タイガーチームサービス）

- 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

GSX
GLOBAL SECURITY EXPERTS

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

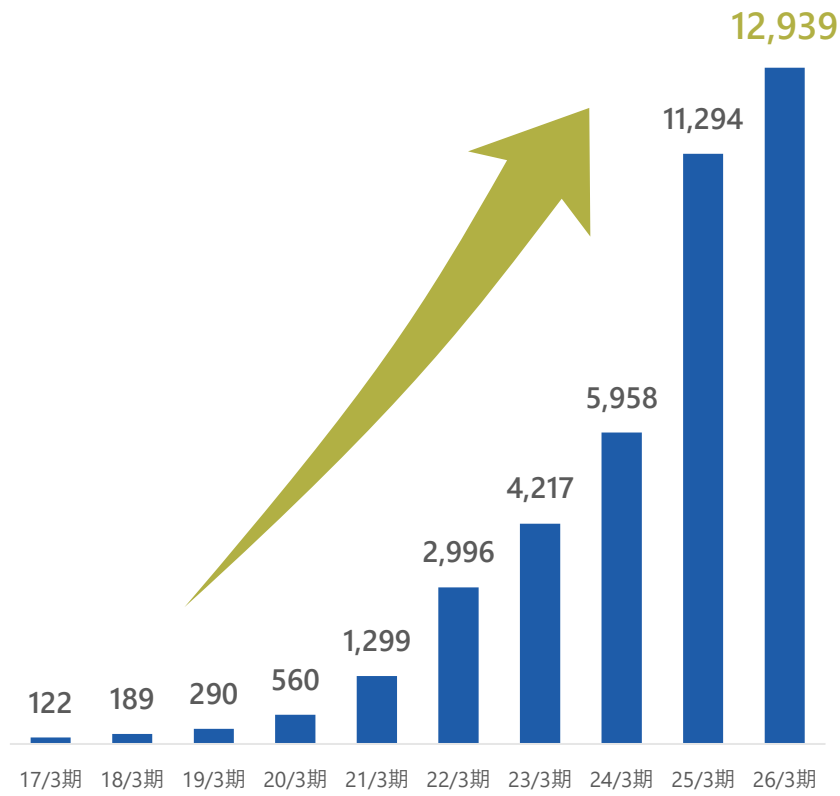
セキュリティでIT商材に付加価値をつける

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）



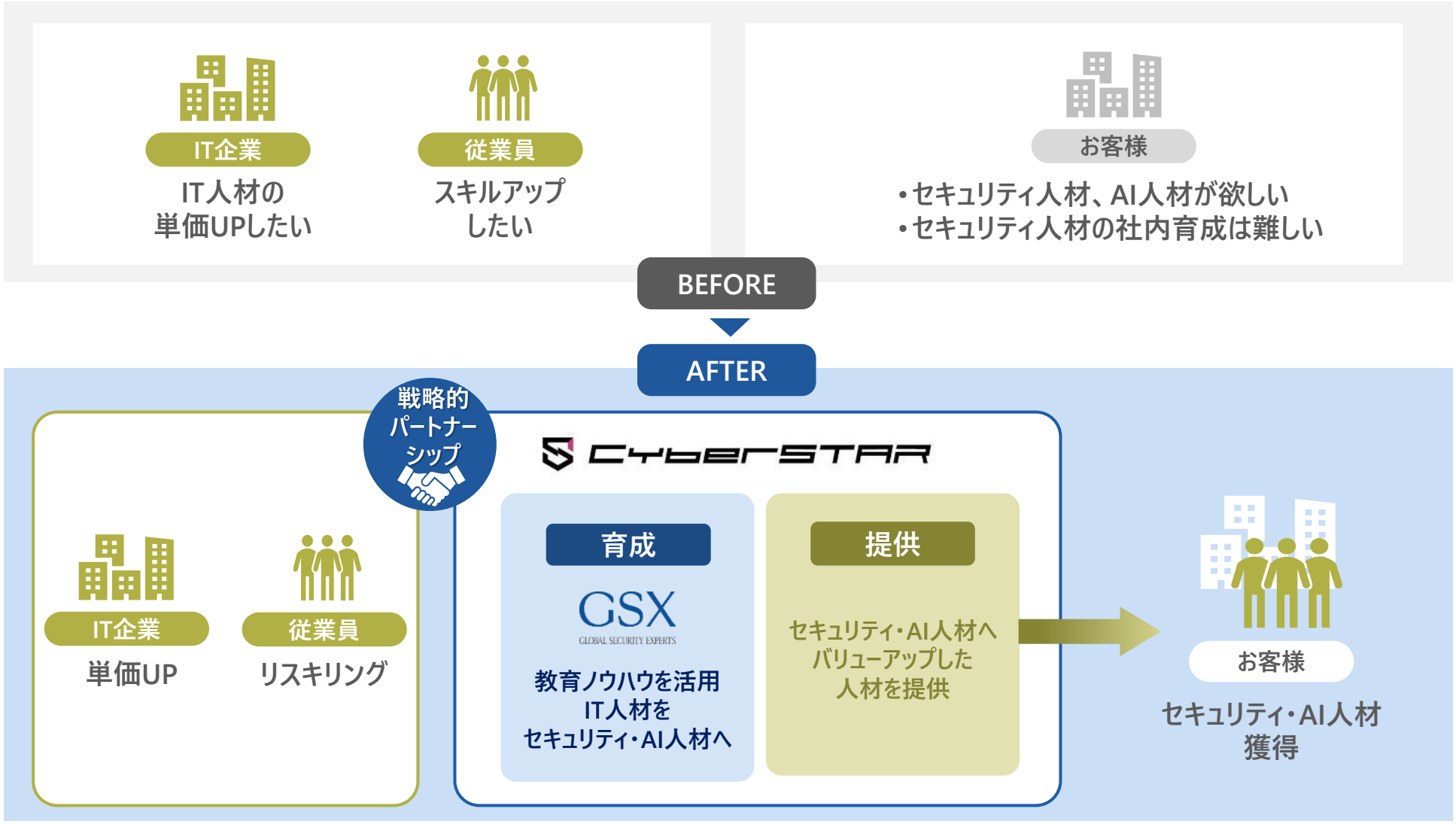
経済産業省「サイバーセキュリティ体制構築・人材確保の手引き」でも「**プラス・セキュリティ**」※人材の確保を提言

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

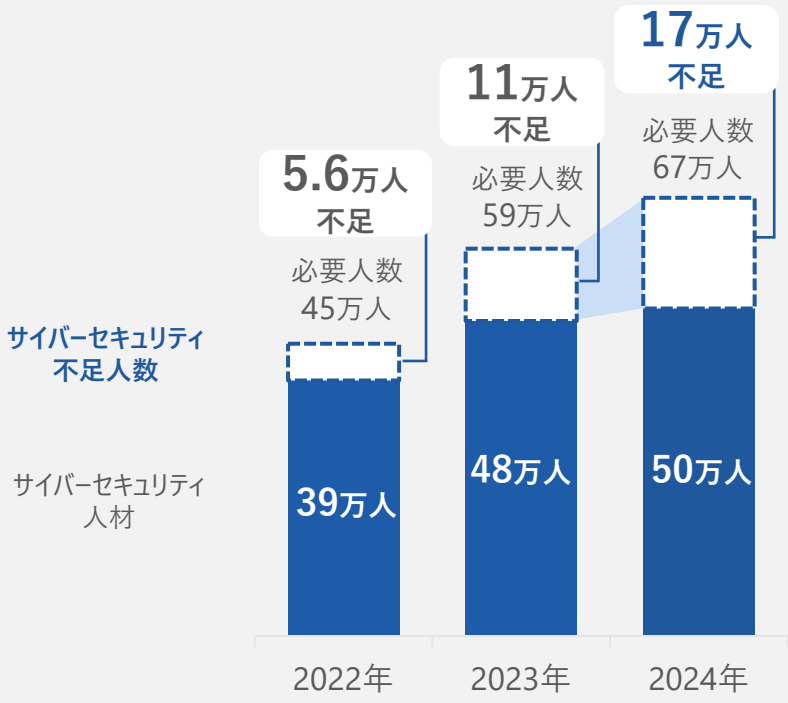
企業規模を限定せずあらゆる企業のセキュリティ・AI人材ニーズに応える
セキュリティ教育カンパニーのGSXならではのビジネスモデルを確立し、IT人材を抱えるIT企業、セキュリティ・AI人材を必要とするお客様双方にメリットを提供



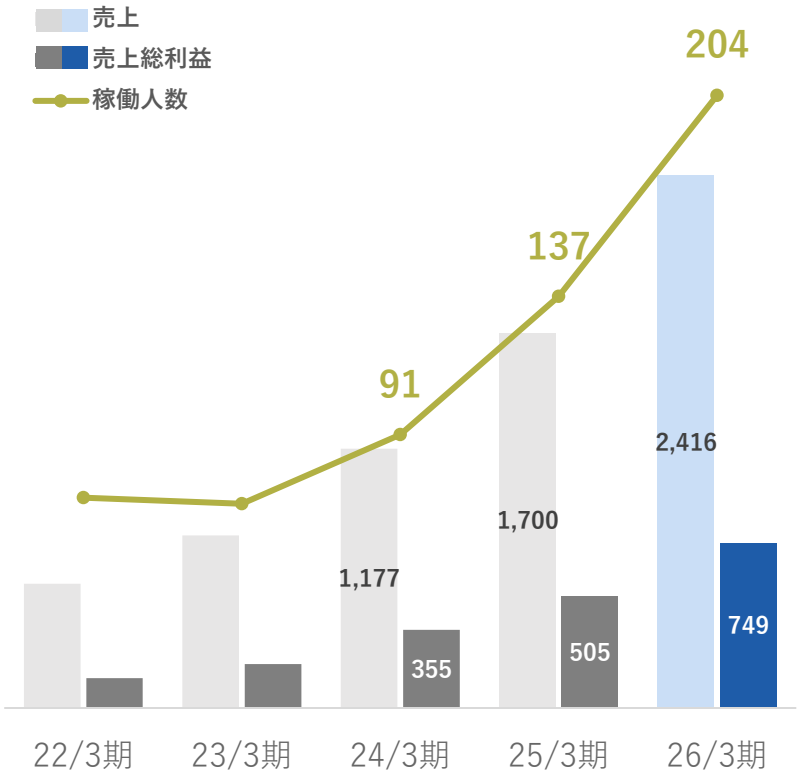
加速するセキュリティ人材SESニーズ

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



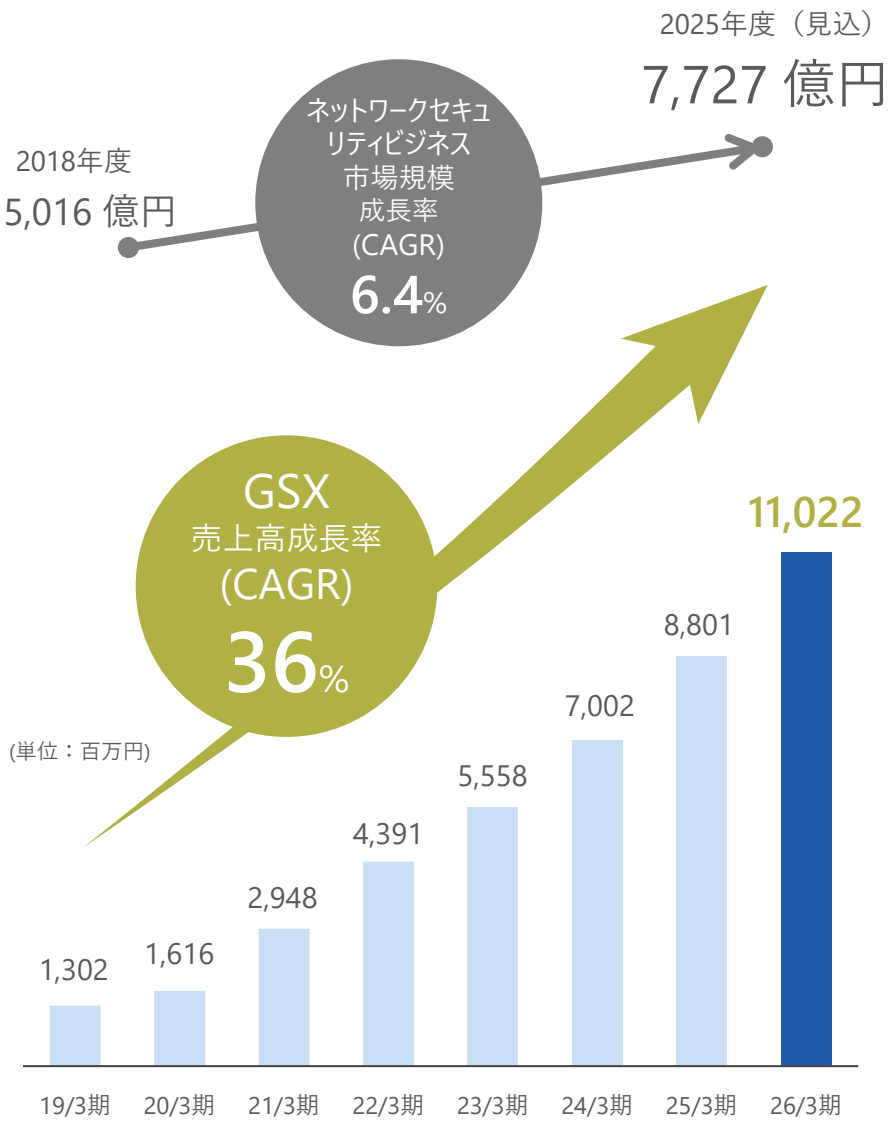
約9割の日本企業がセキュリティ人材不足に悩む一方、キャリアップを望む働き手にとって「情報セキュリティ」は注目の職種

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

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

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

GSX
GLOBAL
SECURITY
EXPERTS

ESGの取組み

GSX
GLOBAL SECURITY EXPERTS

持続可能な社会の実現と企業価値向上の両立を目指し、ESG/SDGsに積極的に取り組みます。

インターネット社会において、サイバーセキュリティの脅威は、人々の命や生活をもおびやかす重要な社会課題のひとつです。またそれらを解決できるサイバーセキュリティ人材が圧倒的に不足しています。当社は「サイバーセキュリティ教育カンパニー」として事業を通してだれもが安心して暮らせる豊かな社会の実現を目指します。

E Environment

- 「気候変動イニシアティブ（JCI：Japan Climate Initiative）」に参加
- BBSグループ温室効果ガス削減目標は、2030年度温室効果ガス排出量 Scope1+2：42%、Scope3：25％削減（2023年度比）、2050年度はグループの温室効果ガス排出量ネットゼロを目指す
- ペーパーレスの推進

S Social

- 人権を尊重する取組みを推進
- 人材育成、働きやすい環境づくり
- ダイバーシティ＆インクルージョンの推進
- 健康・安全への取組み
- 地方創生・雇用創出

G Governance

- コーポレート・ガバナンス強化
- コンプライアンスの遵守
- リスク管理への取組み
- 各種通報窓口の設置
- ステークホルダー・エンゲージメント強化

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　※26/6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 237名 単独 194名　※26/6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

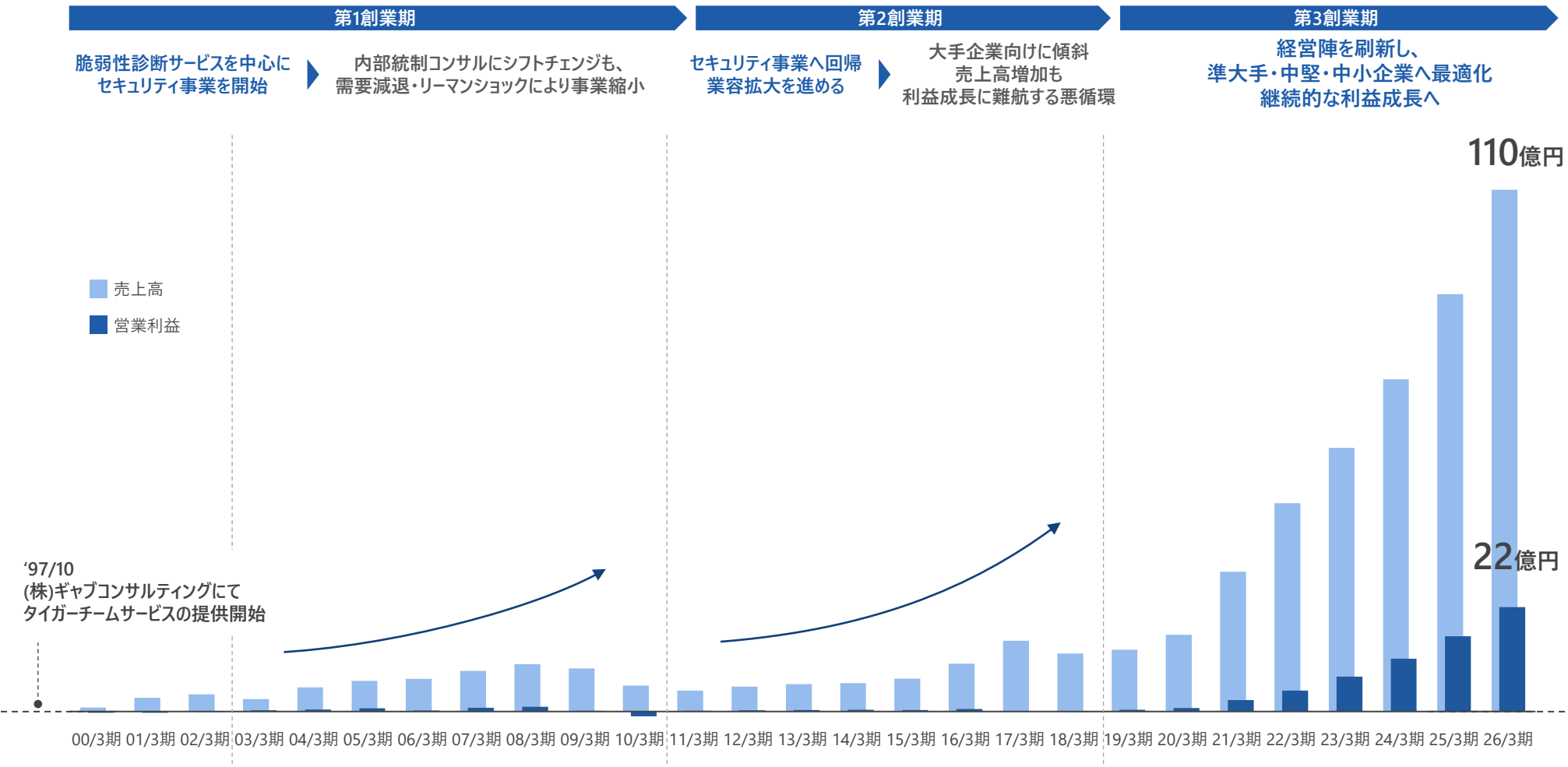
取締役
サイバーセキュリティ事業本部 副本部長

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

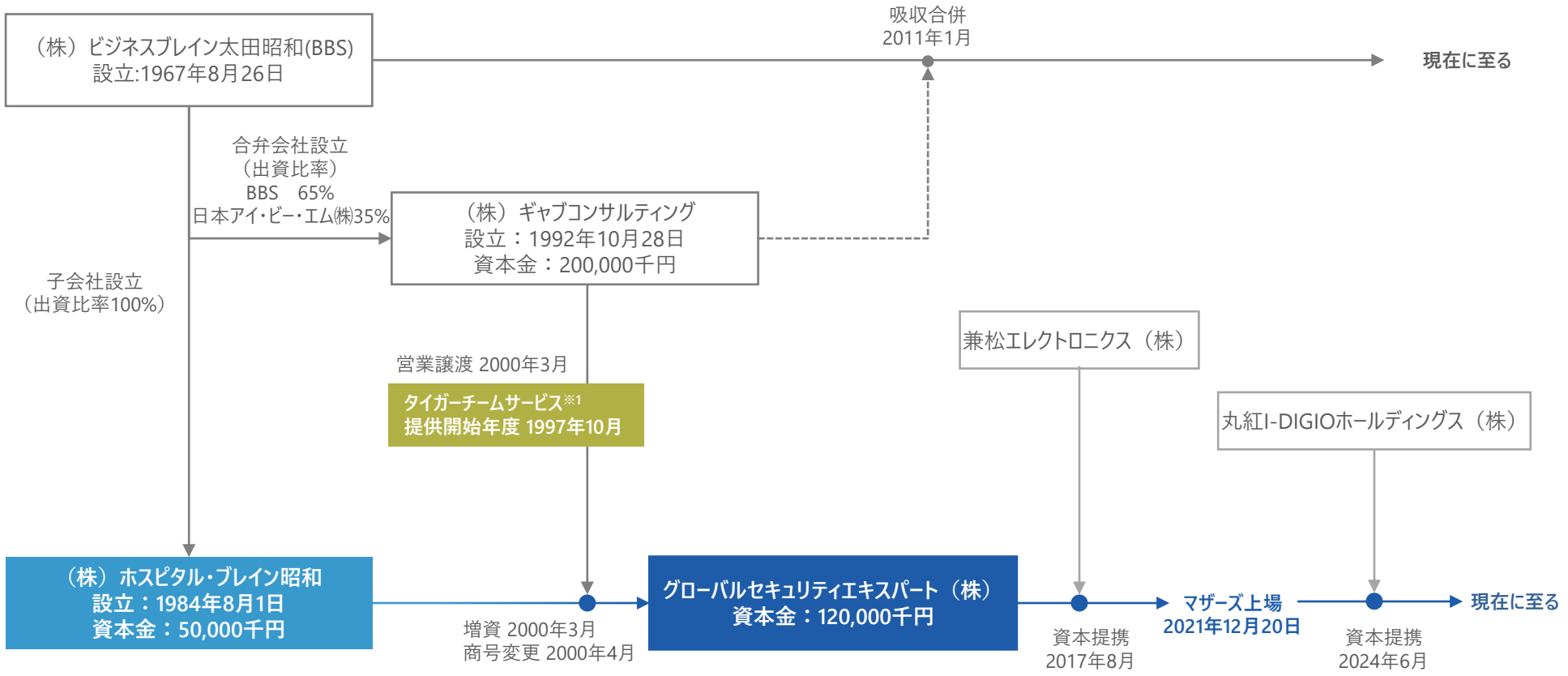


注釈 ※１：創業は1984年設立の(株)ホスピタル・ブレイン昭和。会社の成り立ちについてはAppendix参照
注釈 ※２：21/3期からは、2020年4月1日付で事業譲受したITソリューション事業を含む（21/3期ITソリューション事業の売上高は7.3億円）

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

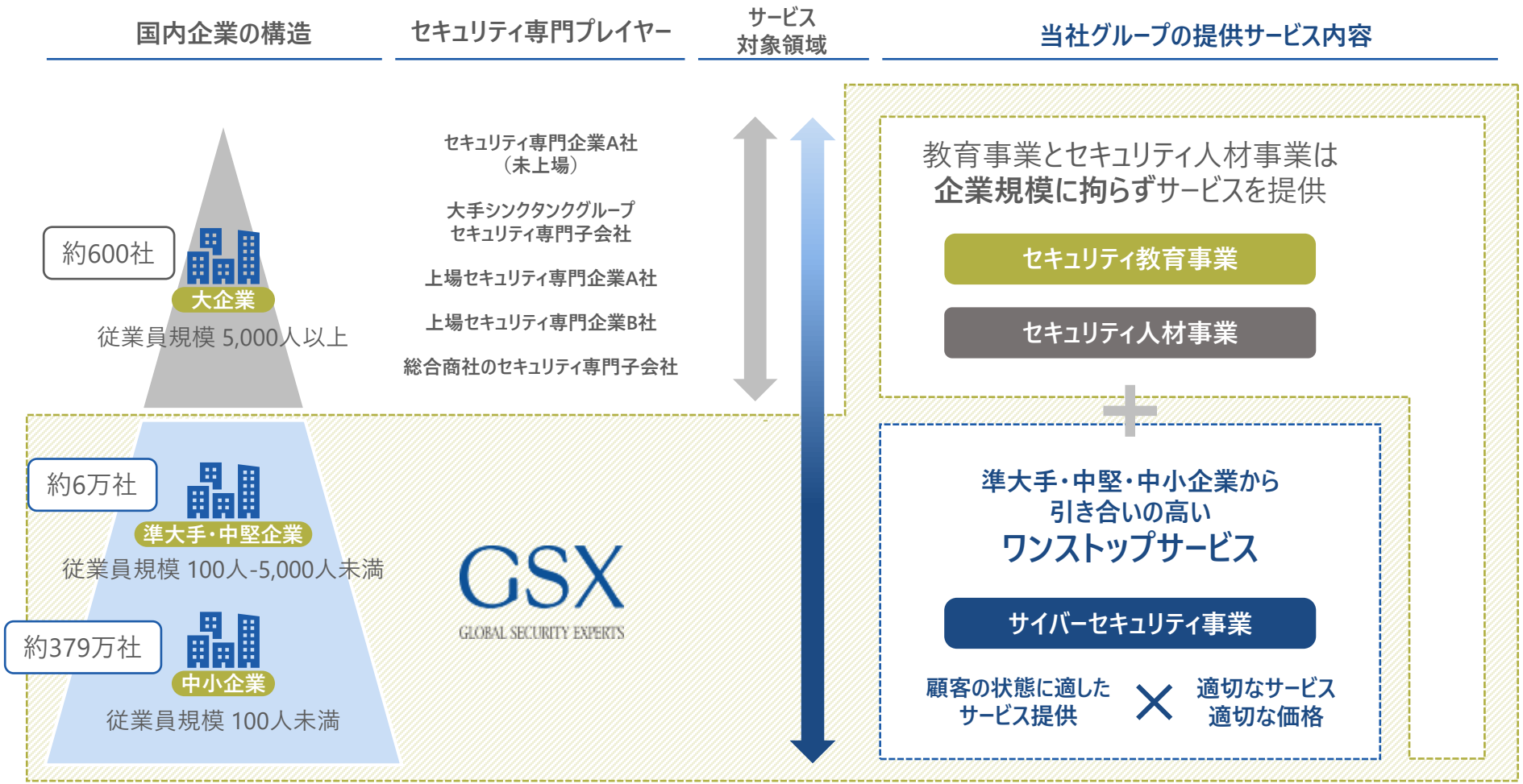


注釈（1）：　タイガーチームサービスとは、侵入検査/模擬攻撃検査サービスのこと

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



セキュリティニーズの違いとサービスの最適化

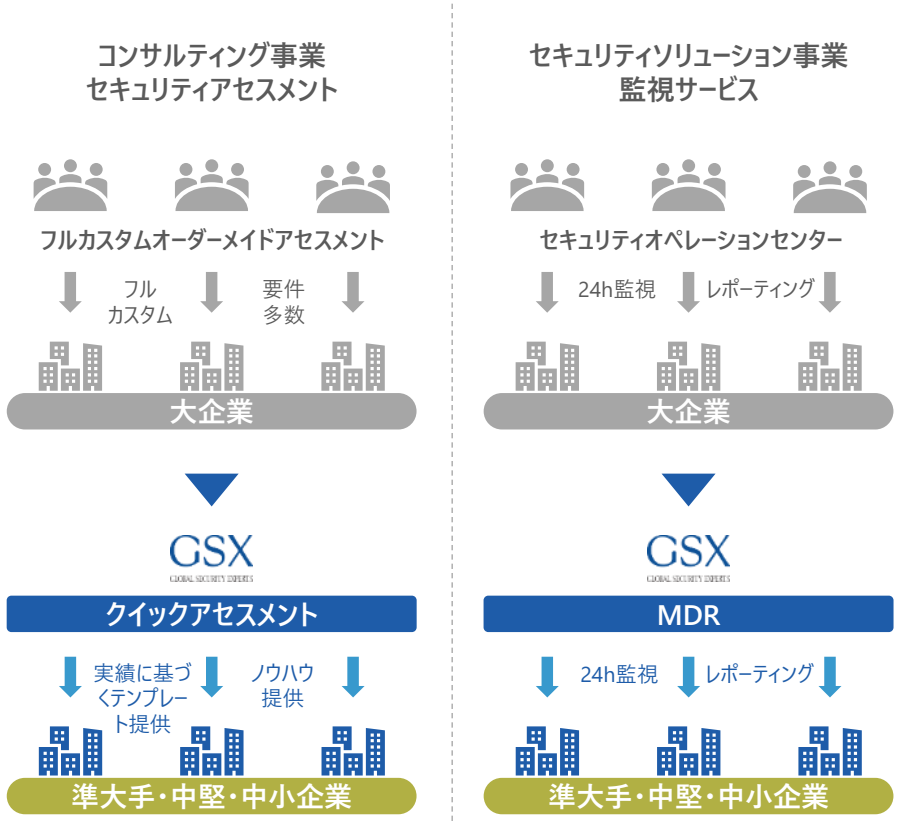
大企業が「脅威を完全に排除」するためのセキュリティ対策を求めるのに対し、準大手・中堅・中小企業は取引先に対してのレピュテーションリスク排除や自社の業態に適合させた必要最低限のセキュリティ対策を求める

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

必要な要素と人員を用意できない

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）

顧客状況に合わせた適切なサービス提供が可能なラインナップ

GSX
GLOBAL SECURITY EXPERTS

状況に合わせた最適なサービスを提供することで、長期取引となりやすい構造

インシデント※多発（有事）	インシデント※対策完了	通常時（平時）
需要増	需要増	強化
セキュリティソリューション 教育、緊急対応	コンサルティング、教育	サイバーセキュリティ 対策全般

事業ポートフォリオの分散

セキュリティ対策に必要な要素をフルラインナップ
お客様の状況に応じて最適なサービスを提供可能

※インシデント：マルウェアやウィルス感染による情報漏えい、システムロックやWEBサイト改ざんによる情報漏えいなどの恐れ

GSXの販売戦略とキャパシティ戦略（事業拡大モデル）

新規、既存顧客に対し、別アプローチを実行することで顧客数増、ARPU増を実現

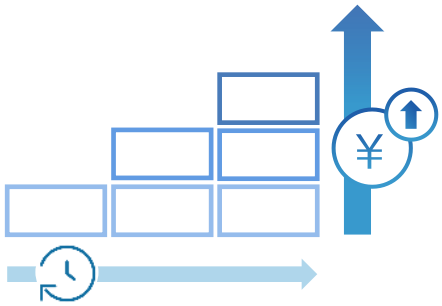
受注増加に対応すべく、IT企業におけるセキュリティ人材育成や同業他社のパートナー化・育成を進めキャパシティ戦略を実行

販売戦略

キャパシティ戦略

既存顧客

アップセル



新規顧客

パートナー戦略

マーケティング戦略

売上高拡大

顧客数

ARPU

キャパシティ戦略

デリバリー

パートナー戦略

IT企業

同業他社

セキュリティ企業

既存と新規のバランスが良いのも GSXの強み

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

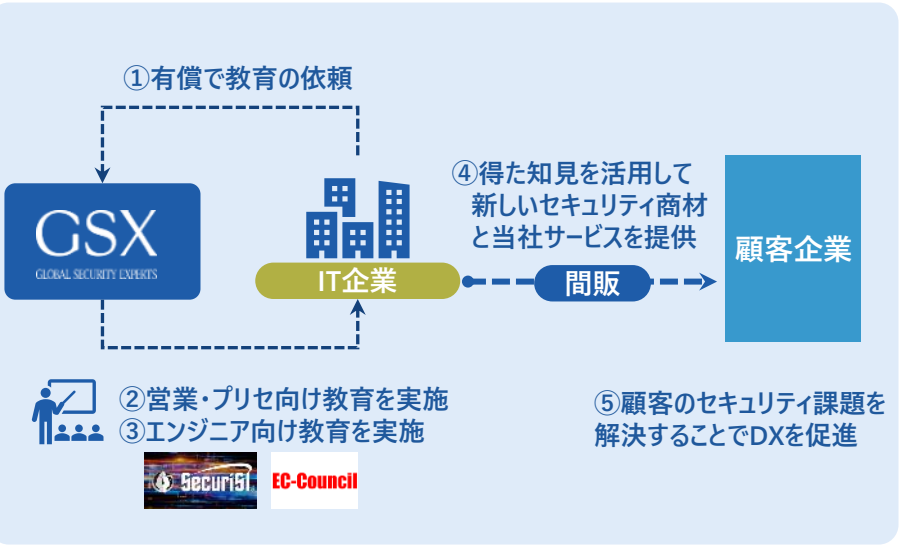
当社とパートナーになることで、IT企業は自社製品・サービスとのシナジーでセキュリティビジネスやDX関連ビジネスの拡大に繋げられる

GSXの販売パートナーになるメリット

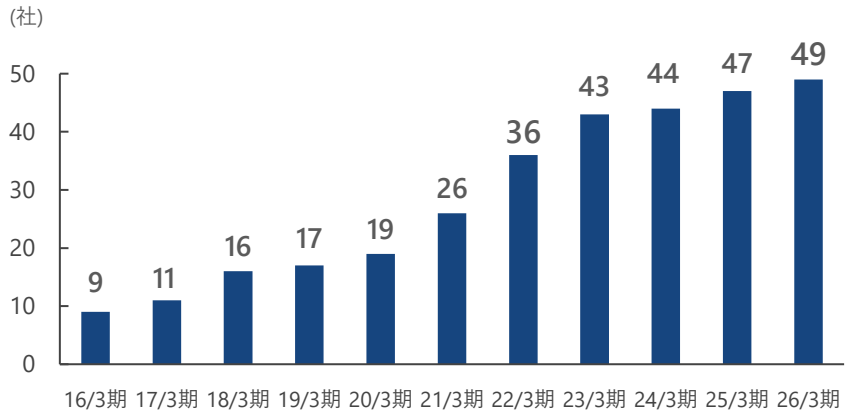
IT企業のニーズ

- 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



キャパシティ戦略：デリバリーパートナー企業の育成

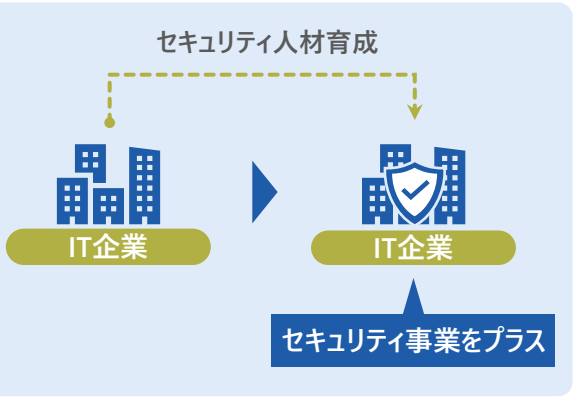
専門性の高い教育コンテンツを活かし、IT企業におけるセキュリティ人材育成や同業他社のパートナー化・育成を進め、セキュリティ市場のプレイヤーを数多く育成することで受注キャパシティを拡大

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

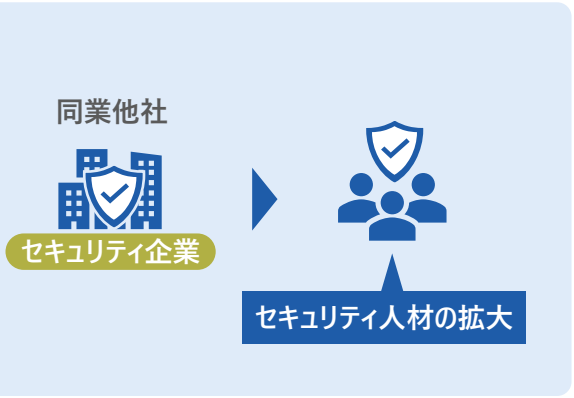
新規育成

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

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
- X（旧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

GSXが準大手・中堅・中小企業に選ばれる理由

GSX
GLOBAL SECURITY EXPERTS

ポジショニング

準大手・中堅・中小企業

- ✓ 顧客数が多い
- ✓ 高まる外部からの対策要請
- ✓ 課題が多岐に渡る
- ✓ 予算に制約

GSX
GLOBAL SECURITY EXPERTS

多岐に渡る課題 ⋙ **多くの顧客のニーズを捉える** ＋ 自社独自商材による **高い利益** →

ちょうどいいサービス ⋙ **競争優位性の発揮** ＋ **セキュリティベンダーとのアライアンス** →

→ 経験に基づく**ちょうどいいサービスレベル設計** →

ちょうどいい価格 ⋙ → サービスの標準化 ジュニア採用・教育による **コスト抑止** →

クロスセル・アップセルによる売上高の拡大

セキュリティを取り巻く環境

IoT、クラウドの利用も含めたDXの推進やテレワークの増加等により、「つながる」相手が増え、組織における内外の脅威は変化し、様々なインシデントが発生

内部からの脅威

【故意】社員や関係者による脅威

・不正な持ち出し
(個人情報/機密情報の漏えい)

S工業：外国企業からの接触による機密情報漏えい
I社：委託先従業員による顧客情報持ち出し
S社：従業員による同業他社への転職時の機密情報持ち出し

【過失】社員や関係者による脅威

・システムの誤設定/メールの誤送信
(情報漏えい、情報の消失・改変)

M社：就活生へのメール誤送信
A社：メルマガの宛先をBCCではなくCCで送信
R社・P社・AB社他： Salesforceの設定ミス

外部からの脅威

サイバー攻撃による脅威

・不正アクセス
(アカウント窃取、WEBサイトの脆弱性)

MD社：Office365のアカウント窃取→情報流出
ECサイト（複数）：個人情報、クレジットカード情報漏えい

・標的型攻撃(ランサムウェア)
(機密情報漏えい、生産・サービスの停止)

米P社：操業停止
K社：サービス停止
N社：決算報告の遅延
H社：国内外オフィス閉鎖、工場操業停止

海外グループの脅威

・海外グループ会社への攻撃
(生産停止、情報漏えい)

D社：メキシコ、ドイツの子会社
B社：アメリカの子会社
P社：カナダの子会社
D証券：イギリスの子会社

サプライチェーンの脅威

・サプライチェーンへの攻撃、脆弱性、管理ミス
(生産停止、情報漏えい)

T社：サプライヤのサイバー攻撃により、一時全工場生産停止
K社：同社のサービス利用によりランサムウェアの被害
T社：販売店の個人情報漏えい

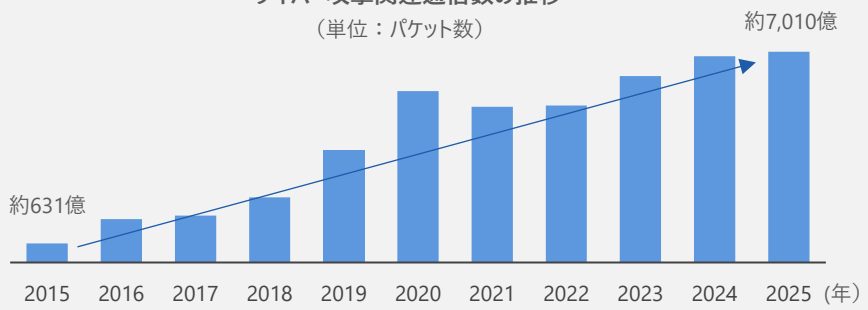
国内サイバーセキュリティ市場を取り巻く市場環境

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

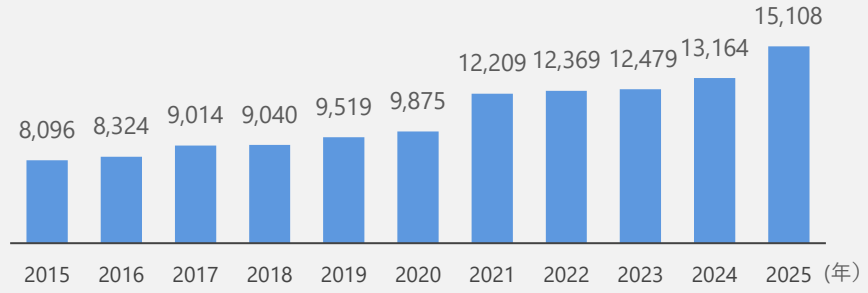
この市場環境の中で、セキュリティ教育やセキュリティ実装の上流から下流までワンストップで展開する当社へのニーズが高まっている

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

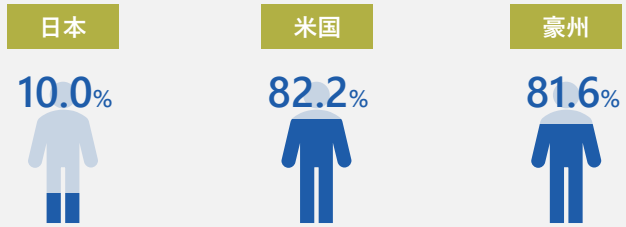
2020年度見込
8,787億円
+66%
2025年度予測
1兆4,593億円

－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

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。

ご留意事項

本資料は、グローバルセキュリティエキスパート株式会社の決算、事業内容および業界動向について、グローバルセキュリティエキスパート株式会社による現時点における予定、推定、見込み又は予想に基づいた将来展望についても言及しております。

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。

グローバルセキュリティエキスパート株式会社の実際の将来における事業内容や業績等は、本資料に記載されている将来展望と異なる場合がございます。

本資料における将来展望に関する表明は、 作成時点において利用可能な情報に基づいてグローバルセキュリティエキスパート株式会社によりなされたものであり、将来の出来事や状況を反映して、将来展望に関するいかなる表明の記載も更新し、変更するものではございません。

また、監査法人による監査を受けていない数値が一部含まれていますが、参考数値として記載しています。

GSX

GLOBAL
SECURITY
EXPERTS