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

2025年６月27日

Agenda

1	会社概要	P 3
2	事業内容	P 7
3	当社の強み・成長戦略	P 13
4	業績ハイライト	P 24
5	2026年3月期連結業績予想	P 29
6	中期経営計画	P 32
7	長期ビジョン	P 41
8	リスク情報	P 47
9	Appendix	P 50

GSX

GLOBAL
SECURITY
EXPERTS

会社概要

Corporate Profile

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SES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	545百万円　※25/3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SESの「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 195名 単独 165名　※25/3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

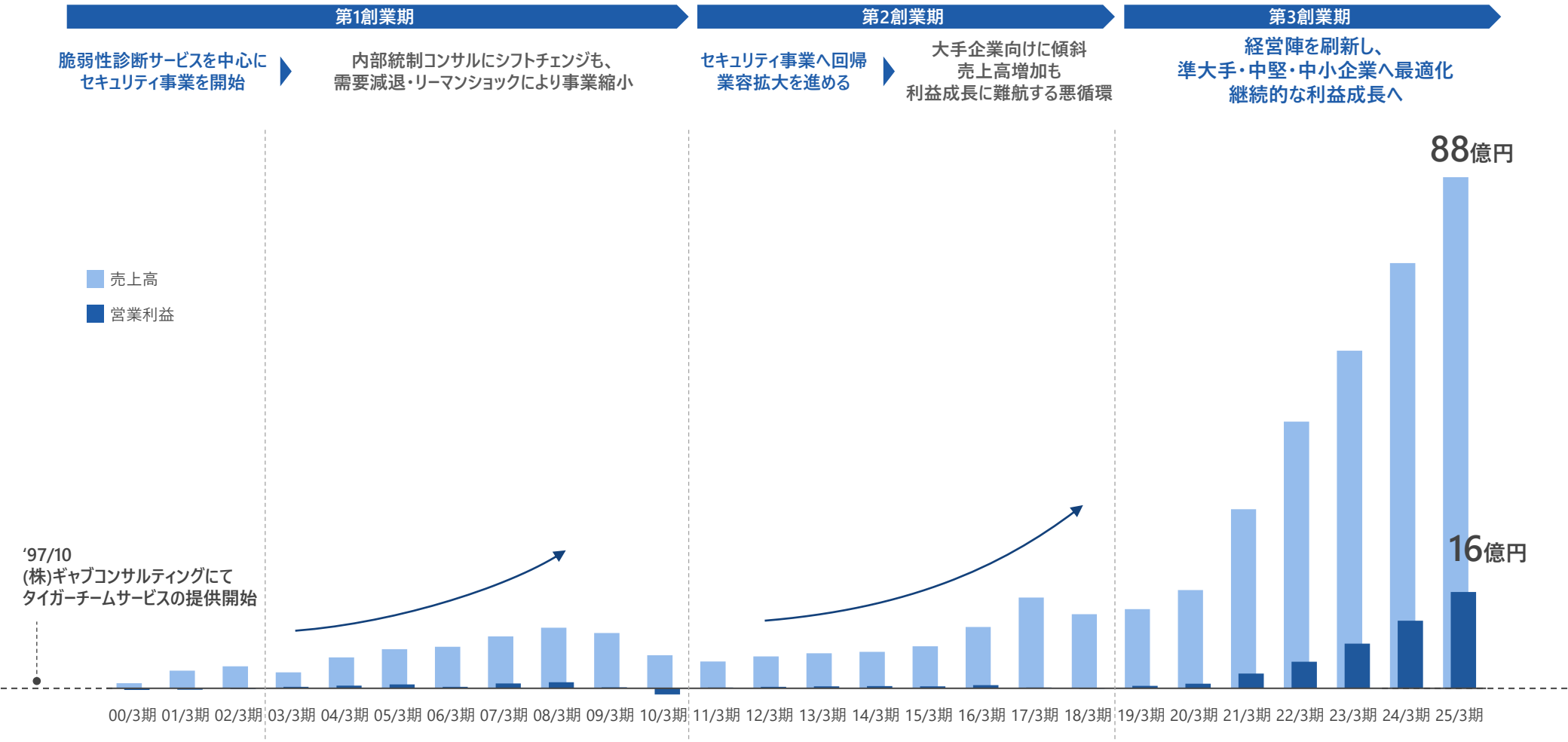
代表取締役社長	青柳 史郎
代表取締役副社長	原　伸一
常務取締役	三木　剛
常務取締役	中村　貴之
取締役	吉見　主税
取締役	鈴木　貴志
取締役	後藤　慶
取締役（社外）	近藤　壮一
取締役（社外）	岡田　幸憲
取締役（社外）	上野　宣
取締役（社外 監査等委員）	井上　純二
取締役（社外 監査等委員）	古谷　伸太郎
取締役（社外 監査等委員）	水谷　繁幸

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

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）

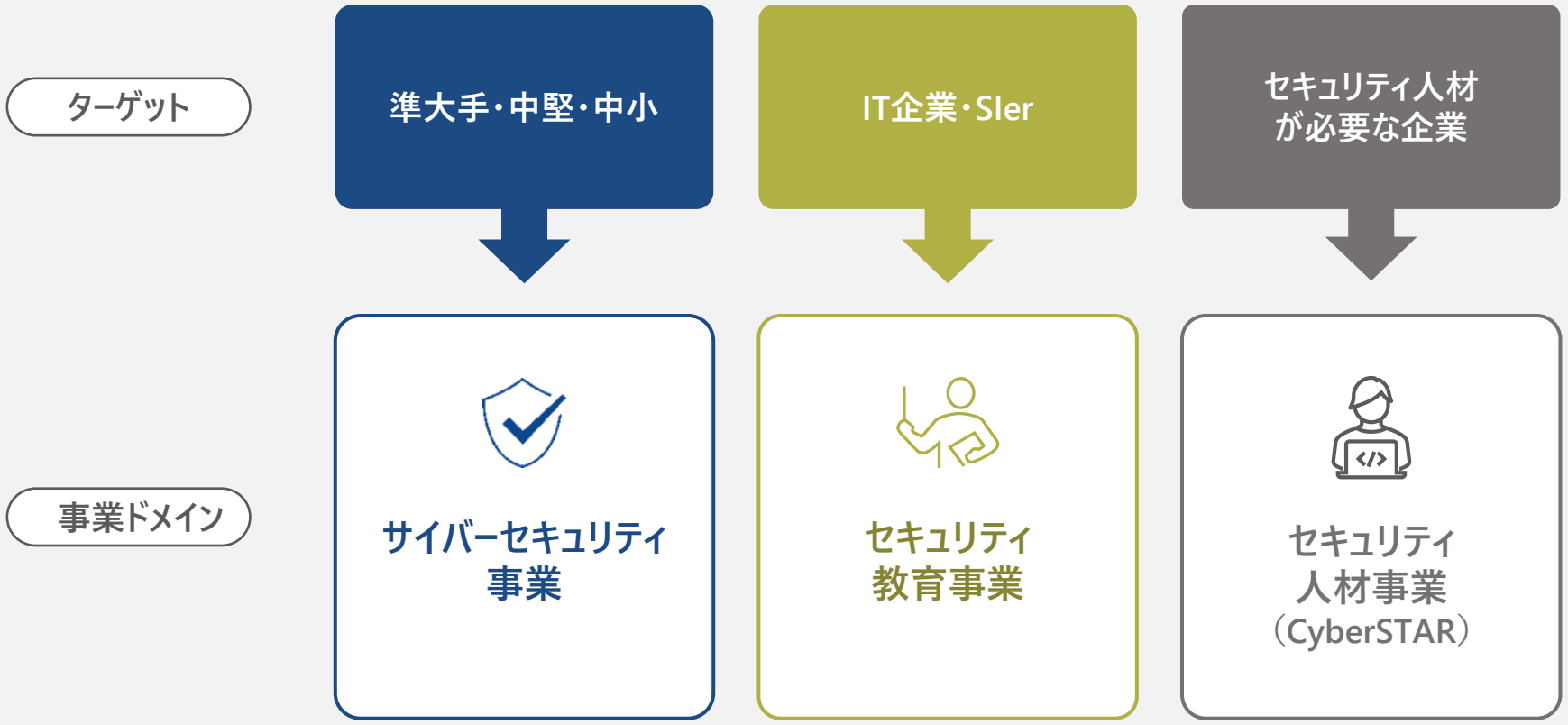
GSX

GLOBAL
SECURITY
EXPERTS

事業内容

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

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

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 17,113名（25/3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 8,332名（25/3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

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、セキュリティ人材を必要とするお客様双方にメリットを提供

BEFORE

IT企業
IT人材の
単価UPしたい

従業員
スキルアップ
したい

お客様
- セキュリティ人材が欲しい
- セキュリティ人材の社内育成は難しい

AFTER

戦略的
パートナー
シップ

IT企業
単価UP

従業員
リスキリング

CyberSTAR

育成
GSX
GLOBAL SECURITY EXPERTS
教育ノウハウを活用
IT人材を
セキュリティ人材へ

提供
セキュリティ人材へ
バリューアップした
人材を提供

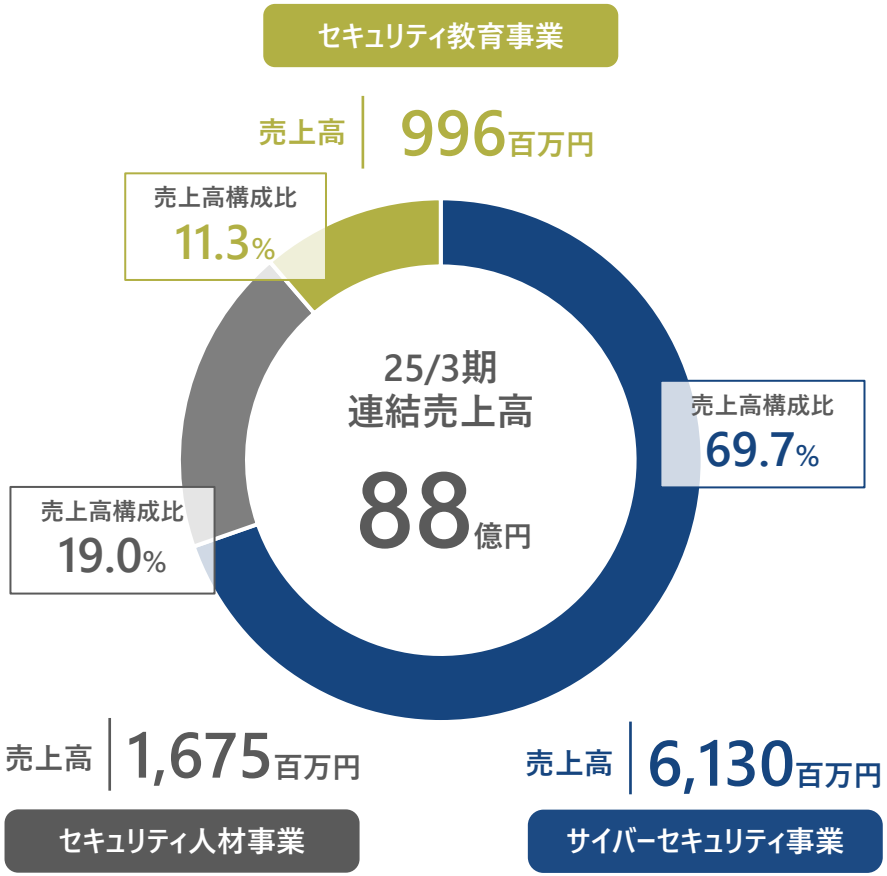
お客様
セキュリティ人材
獲得

連結売上高・売上総利益構成

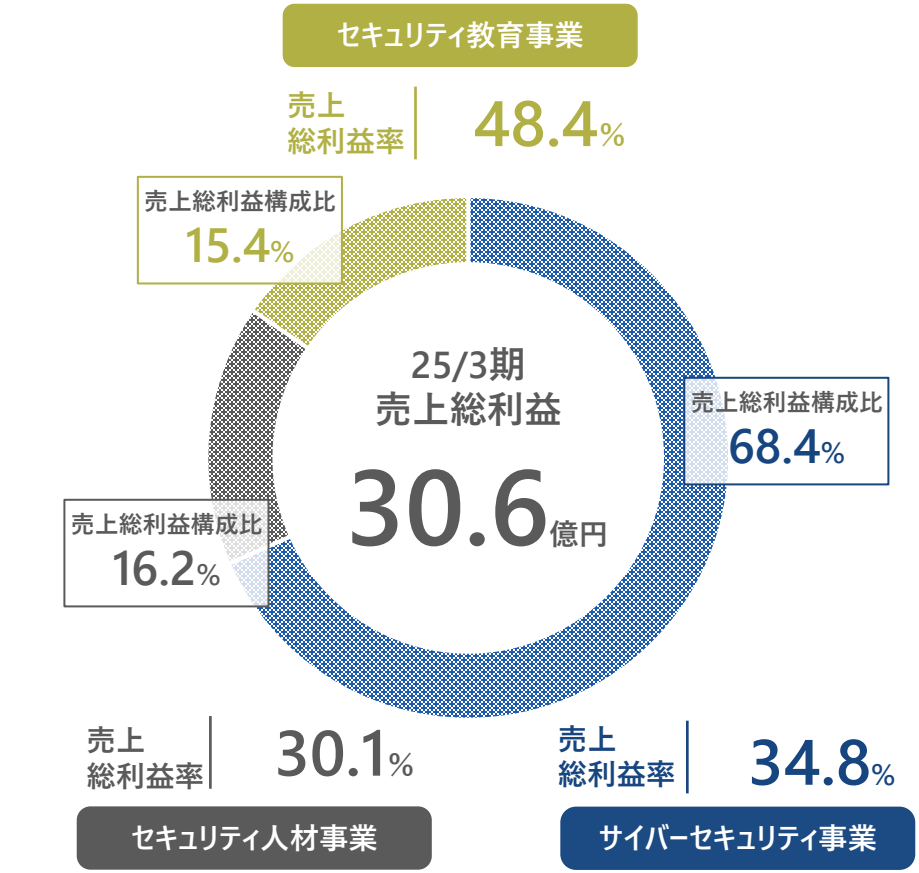
2025年3月期の構成比は計画通り

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



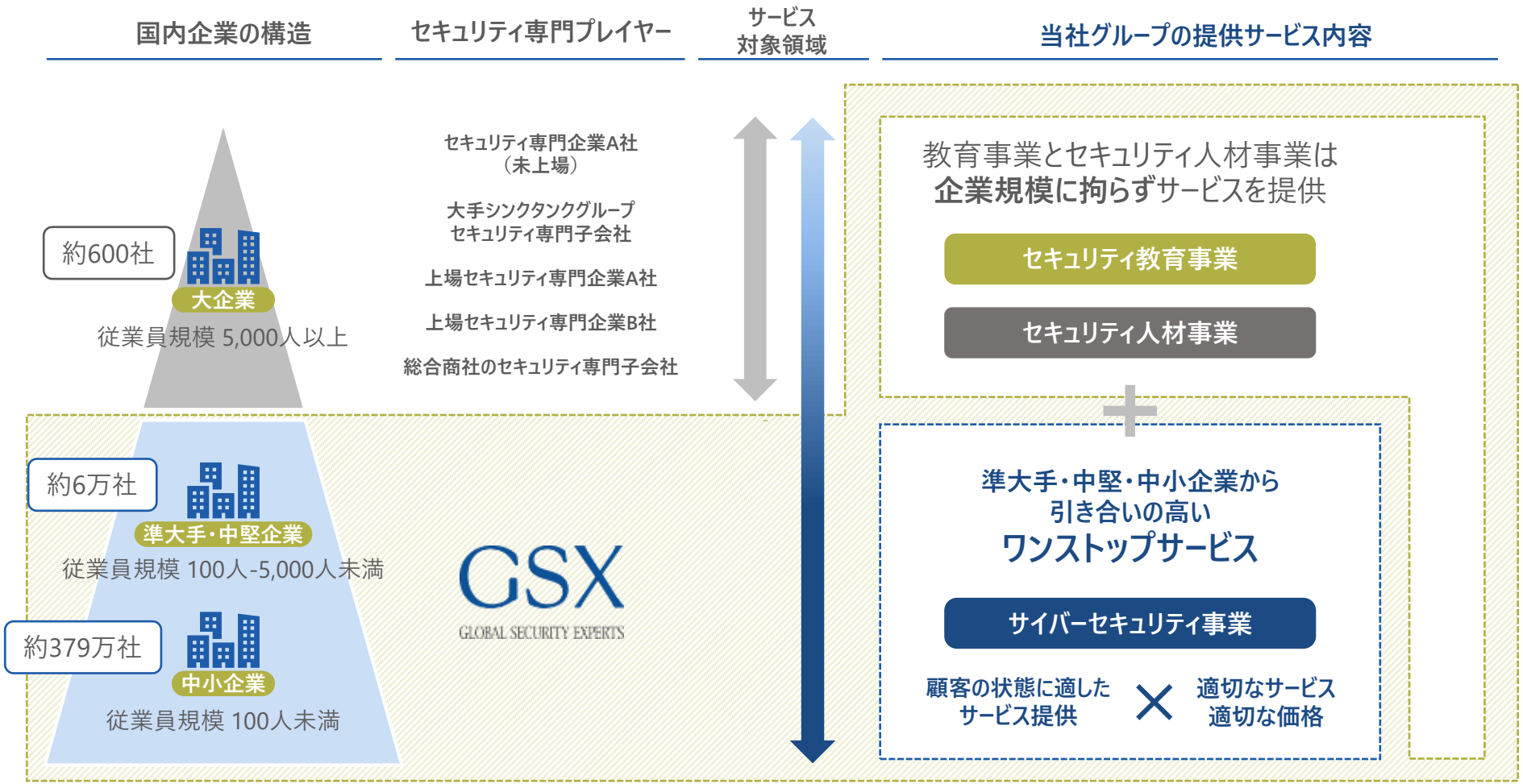
GSX
GLOBAL
SECURITY
EXPERTS

当社の強み・成長戦略

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

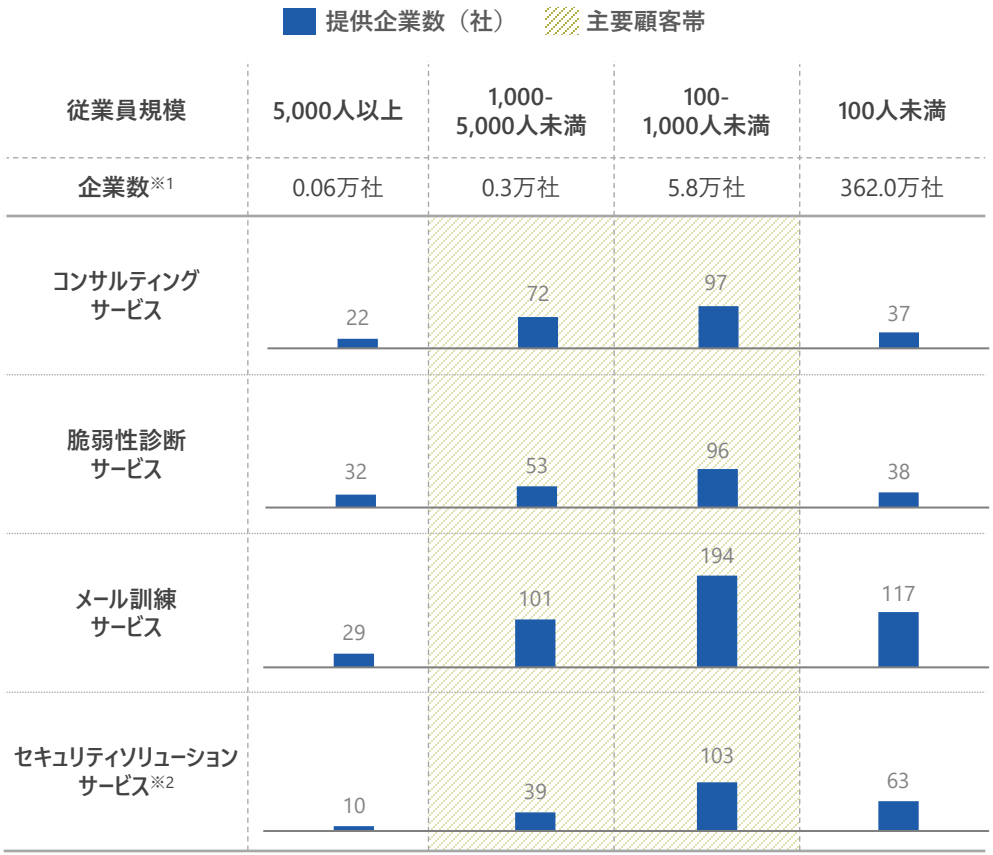
サイバーセキュリティの専門企業というカテゴリーにおいて、GSXは他社が参入しづらい独自のポジションにある



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1.4兆円、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 **1,919億円**　0.3万社※4×4.2百万円※5+5.8万社※6×3.1百万円※8

脆弱性診断サービス **2,058億円**　0.3万社※4×3.3百万円※5+5.8万社※6×3.4百万円※8

メール訓練サービス **507億円**　0.3万社※4×1.6百万円※5+5.8万社※6×0.8百万円※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 **9,633億円**
ストック：0.3万社※4×19.5百万円※5+5.8万社※6×10.5百万円※8
フロー　：0.3万社※4×2.6百万円※5+5.8万社※6×5.0百万円※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1.4兆円

＋

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2025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（2025/3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（2025/3期）

セキュリティニーズの違いとサービスの最適化

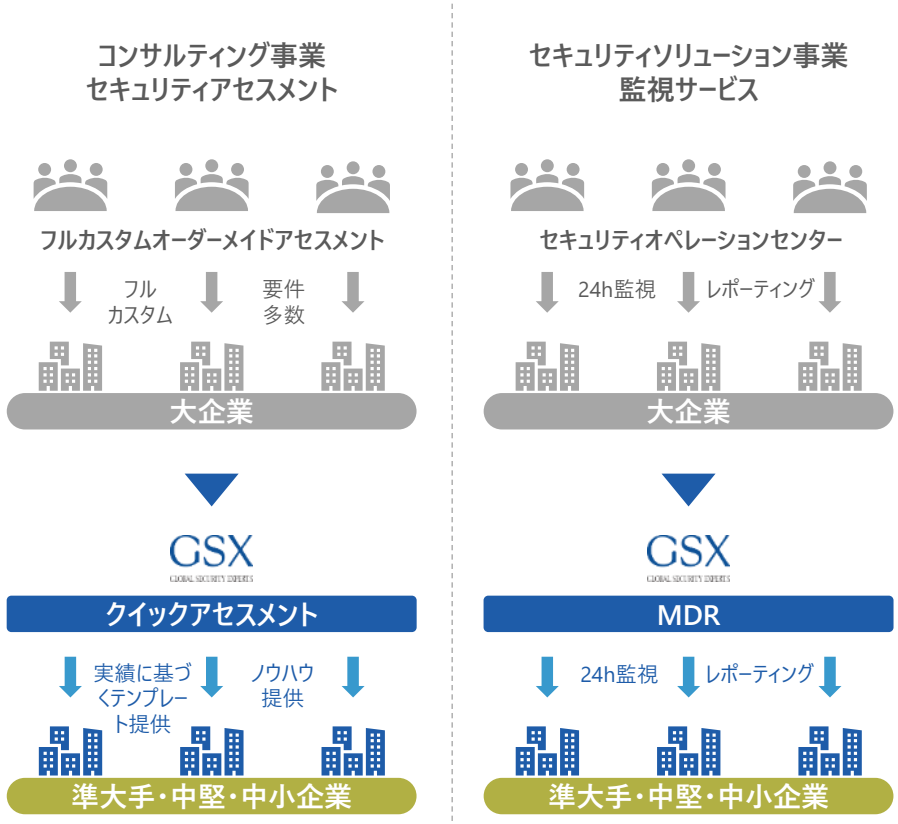
大企業が「脅威を完全に排除」するためのセキュリティ対策を求めるのに対し、準大手・中堅・中小企業は取引先に対してのレピュテーションリスク排除や自社の業態に適合させた必要最低限のセキュリティ対策を求める

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

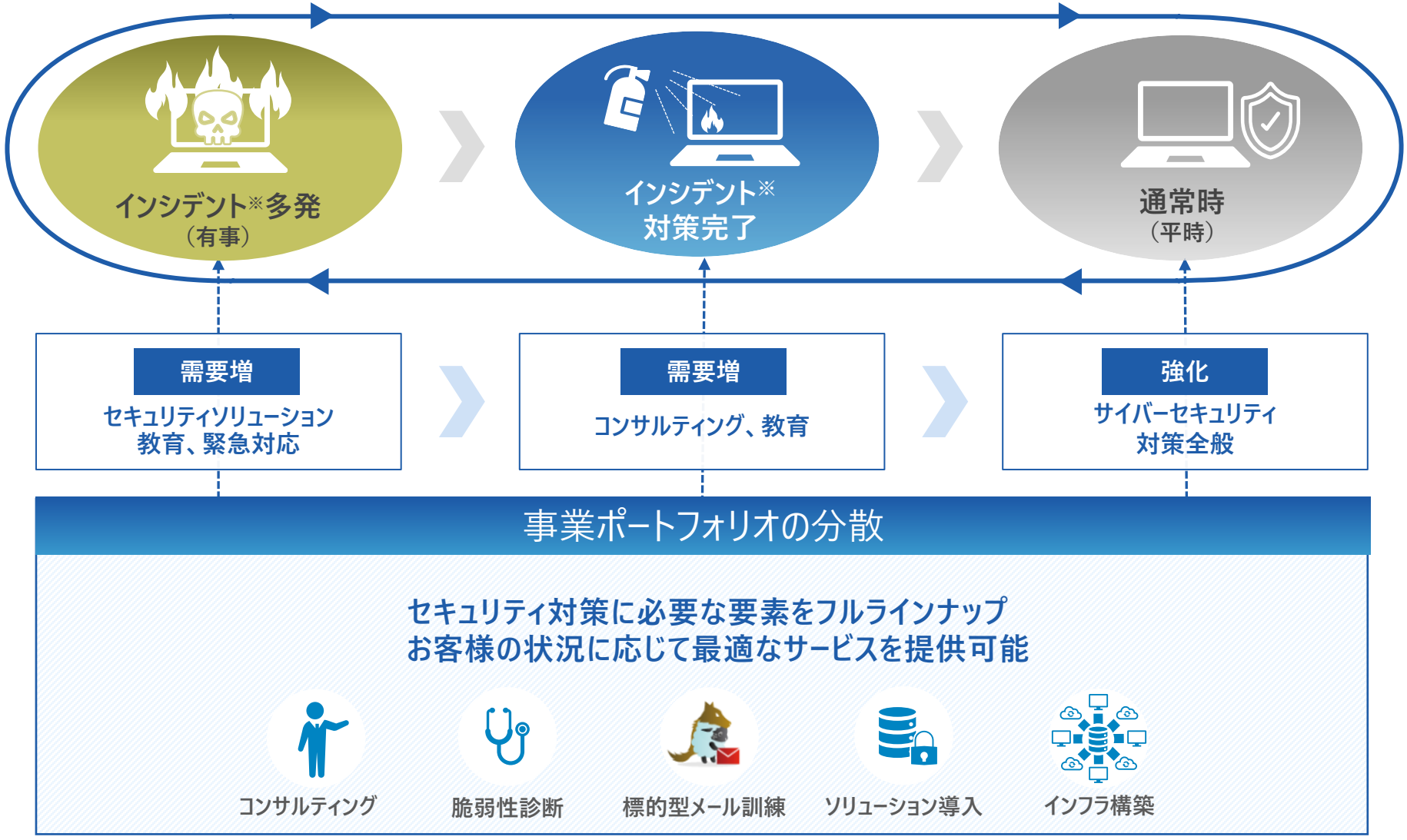
セキュリティ専門人材の不足

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）

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：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

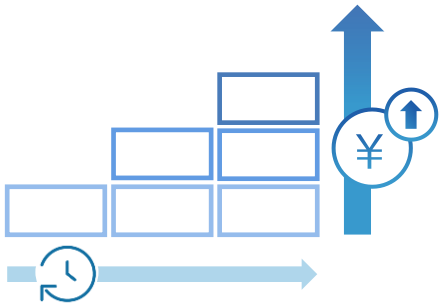
受注増加に対応すべく、IT企業におけるセキュリティ人材育成や同業他社のパートナー化・育成を進めキャパシティ戦略を実行

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

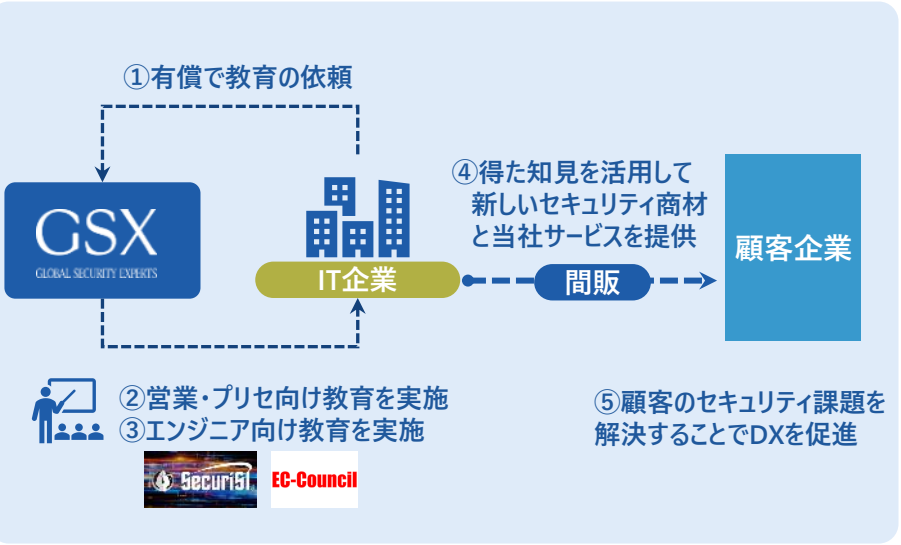
当社とパートナーになることで、IT企業は自社製品・サービスとのシナジーでセキュリティビジネスやDX関連ビジネスの拡大に繋げられる

GSXの販売パートナーになるメリット

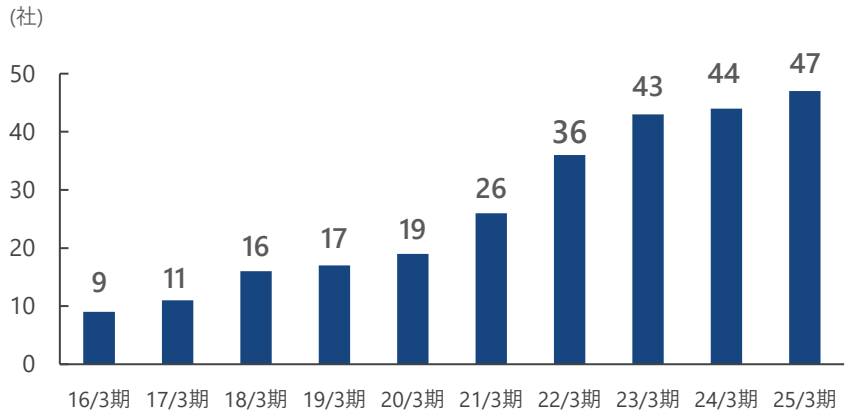
IT企業のニーズ

- 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



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

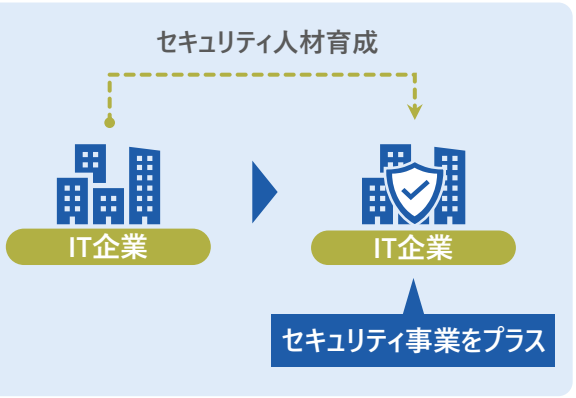
専門性の高い教育コンテンツを活かし、IT企業におけるセキュリティ人材育成や同業他社のパートナー化・育成を進め、セキュリティ市場のプレイヤーを数多く育成することで受注キャパシティを拡大

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

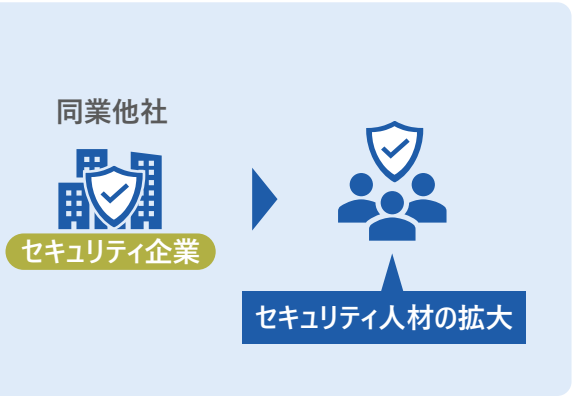
新規育成

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

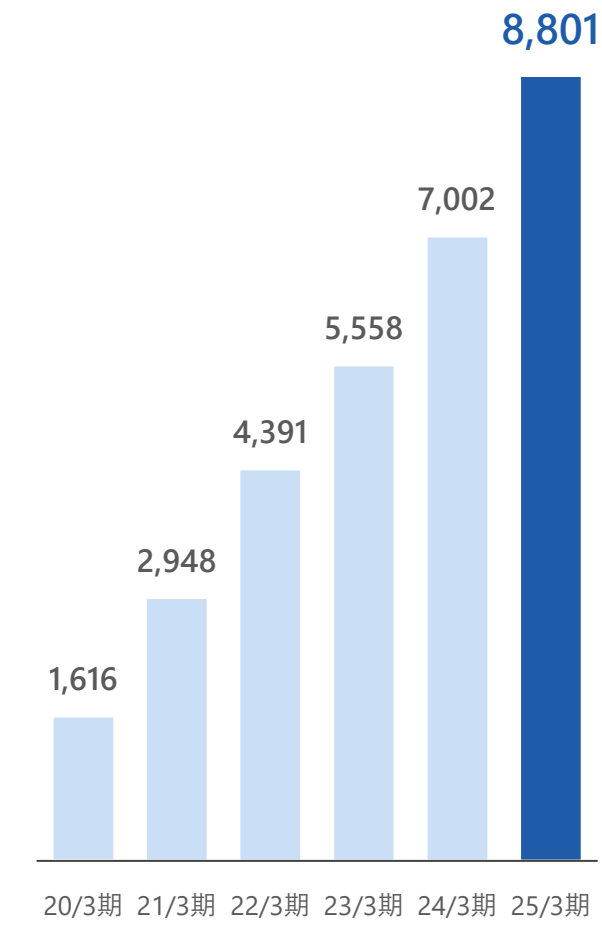
業績ハイライト

通期業績推移

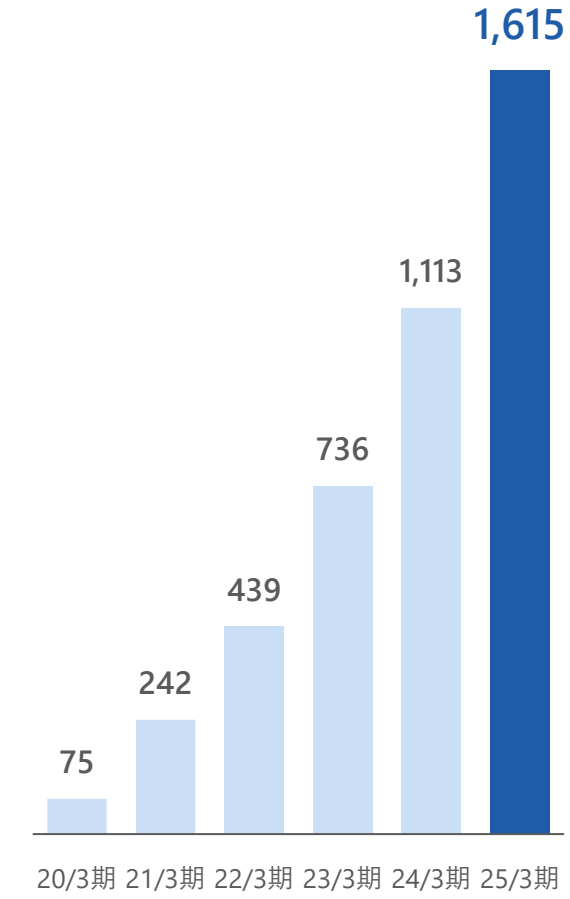
安定的なトップラインの拡大とそれを超える利益の成長スピード

高収益体質の経営を実現

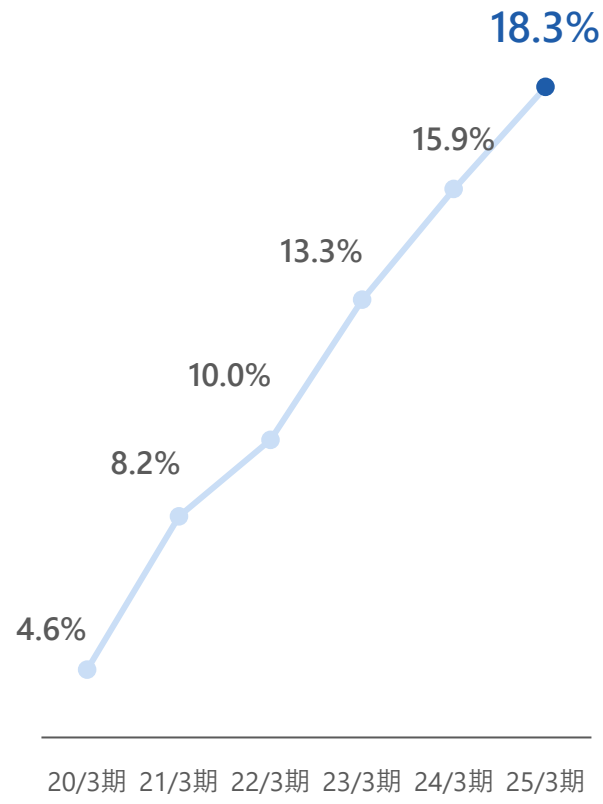
売上高の推移 (単位：百万円)



営業利益の推移 (単位：百万円)



営業利益率の推移

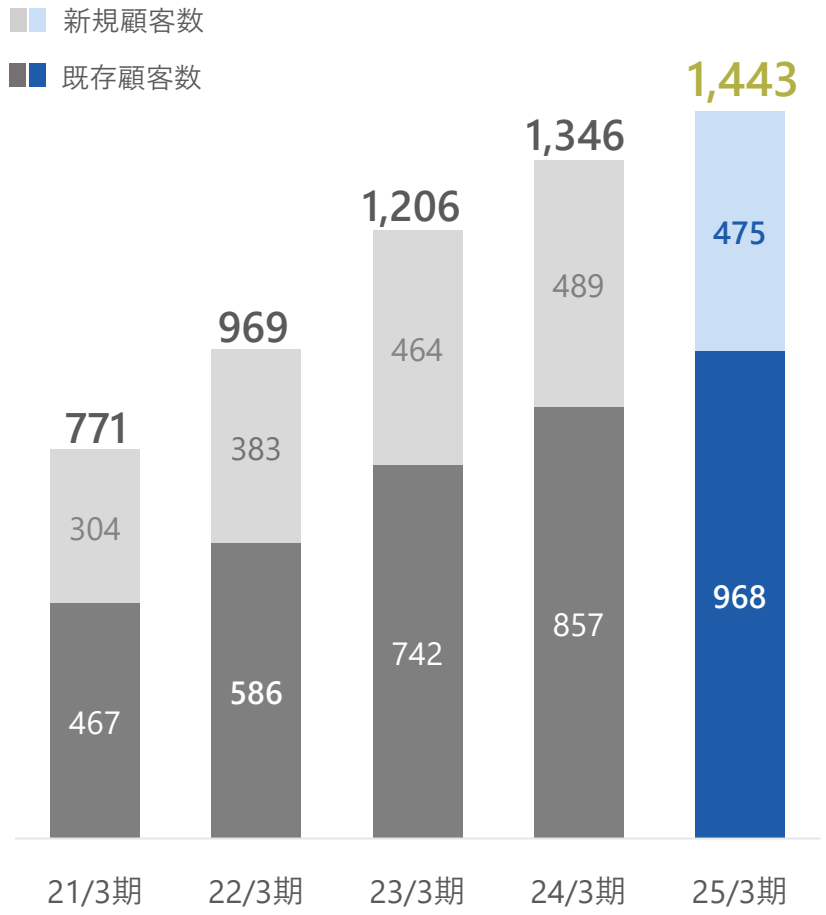


顧客数推移・ARPU推移

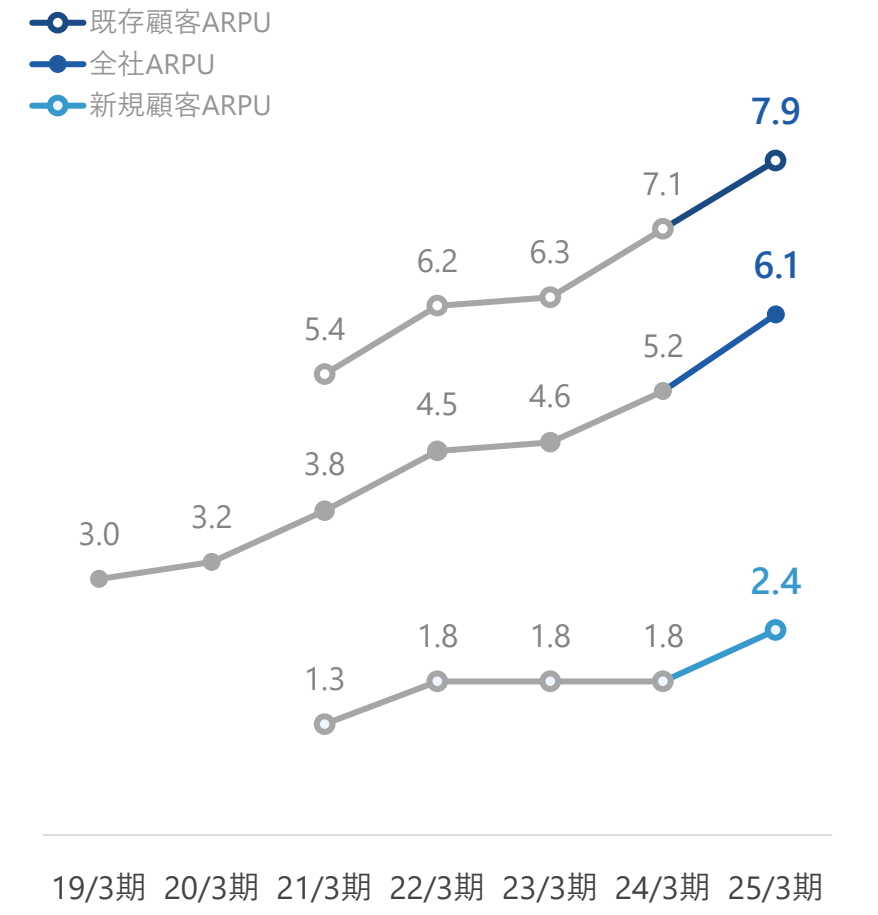
緊急対応を起因とした関連サービスの提供により新規顧客はARPUが伸長

セキュリティ教育、セキュリティ人材提供の旺盛な需要により、既存顧客は顧客数・ARPUともに伸長

顧客数推移（単位：社）



ARPU推移（単位：百万円）



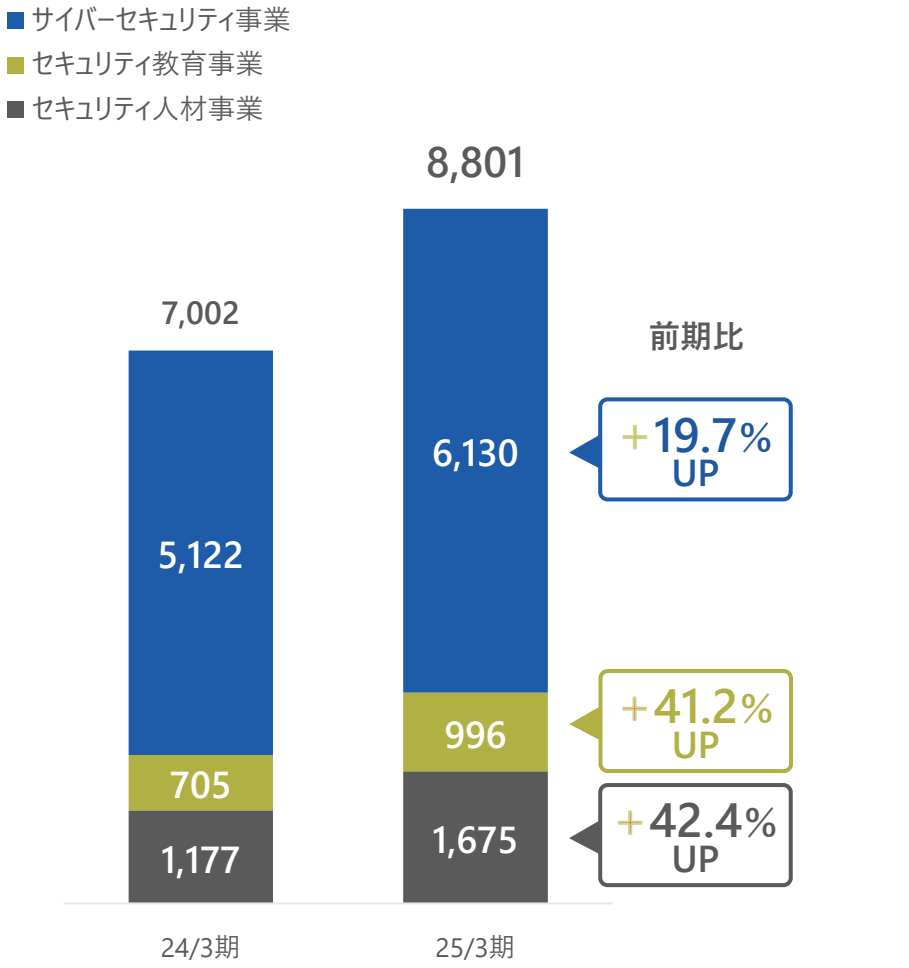
※21年3月期以前の数値は参考値です

事業別売上高・売上総利益　前期比（累計期間）

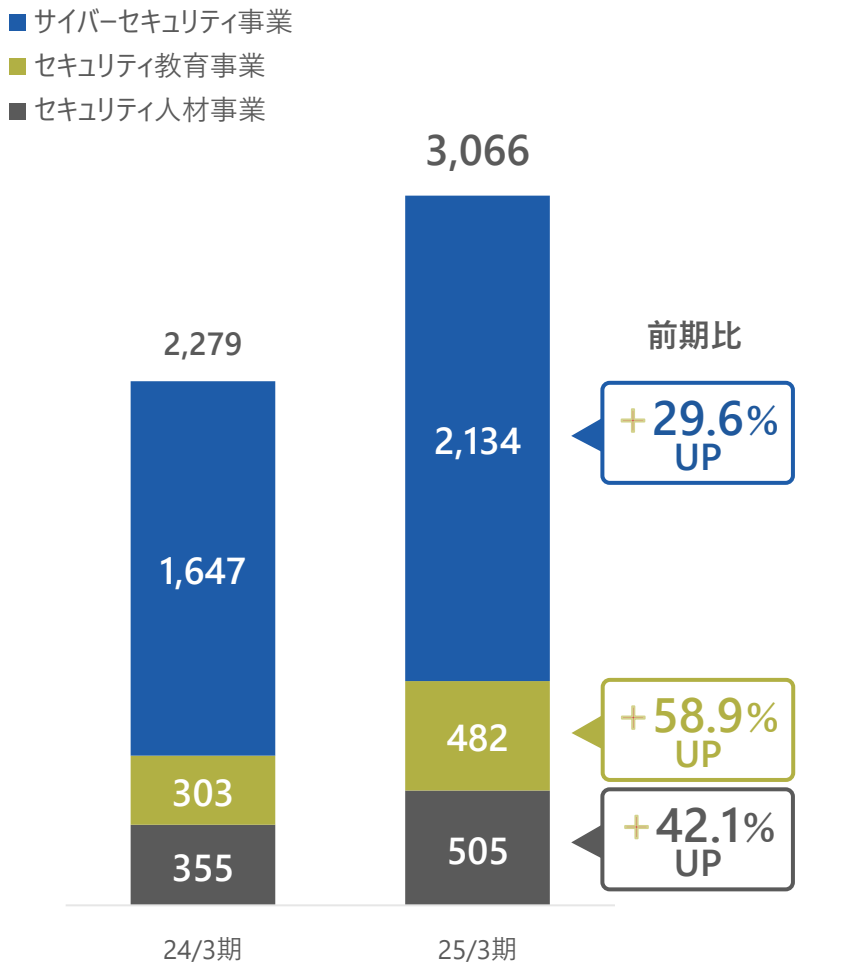
売上高・売上総利益ともに拡大

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）



財務ハイライト

決算期		2020/3期	2021/3期	2022/3期	2023/3期	2024/3期	2025/3期
売上高	（千円）	1,616,613	2,948,871	4,391,317	5,558,022	7,002,941	8,801,647
経常利益	（千円）	73,103	239,370	414,331	737,512	1,104,319	1,562,981
当期純利益	（千円）	38,658	167,657	261,099	488,120	783,428	1,010,077
資本金	（千円）	270,000	291,800	485,000	529,833	544,999	545,921
発行済株式数	（株）	10,000	10,590	3,327,000	7,383,000	7,629,600	7,644,600
純資産額	（千円）	736,113	942,201	1,565,478	1,720,169	2,433,625	3,078,911
総資産額	（千円）	1,712,769	2,384,273	3,482,070	4,124,589	6,536,708	8,141,157
1株当たり純資産額	（円）	122.69	148.28	235.27	236.26	323.09	410.16
1株当たり配当額	（円）	500	2,900	15	14	26.21	41.71
1株当たり当期純利益	（円）	7.28	27.35	40.46	72.20	104.84	134.48
自己資本比率	（%）	42.98	39.52	44.96	41.71	37.23	37.8
自己資本利益率	（%）	6.93	19.98	20.82	29.71	37.72	32.8
配当性向	（%）	11.5	17.7	18.5	19.4	25.0	31.0
営業キャッシュフロー	（千円）	△284,882	767,002	328,219	594,948	713,549	1,018,887
投資キャッシュフロー	（千円）	△76,692	△240,397	△294,649	△212,159	△2,005,260	△411,367
財務キャッシュフロー	（千円）	387,400	△91,241	460,634	△455,995	1,447,820	△457,415
現金及び現金同等物の期末残高	（千円）	216,959	652,324	1,146,528	1,073,322	1,229,432	1,379,536
従業員数	（人）	75	110	118	138	154	195

※2025年3月期より連結決算

GSX
GLOBAL
SECURITY
EXPERTS

2026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

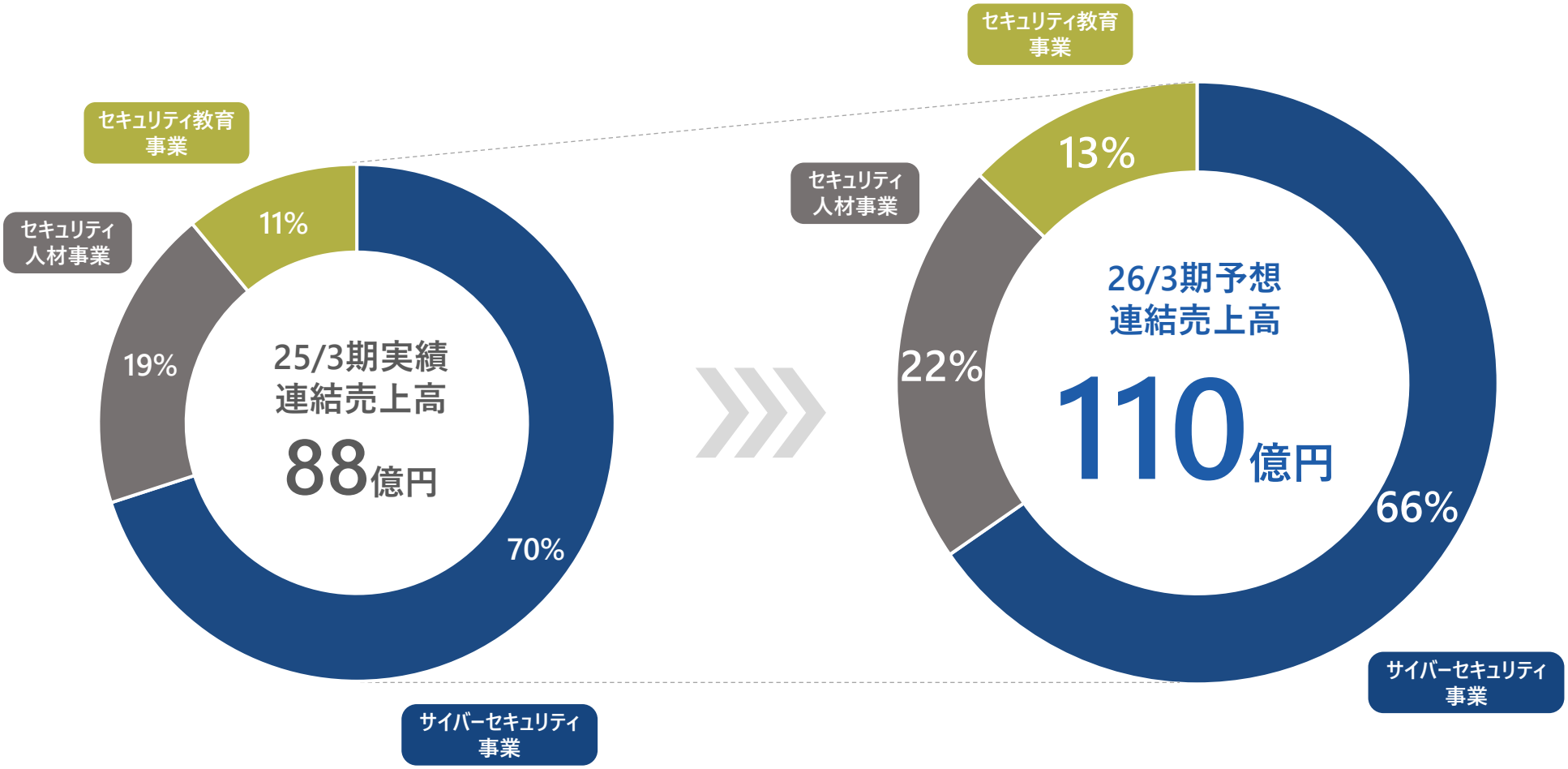
連結売上高は前期比＋25%　営業利益率は20%を目指す

（百万円）	2025/3期 実績	2026/3期 予想	増減額	増減率
売上高	8,801	11,000	2,198	+25.0%
営業利益	1,615	2,200	585	+36.2%
営業利益率	18.3%	20.0%	+1.7pt	-
経常利益	1,562	2,181	619	+39.5%
経常利益率	17.8%	19.8%	+2.0pt	-
当期純利益	1,010	1,417	407	+40.3%
EPS（円）※	134.48	188.77	54.29	-

※2025年6月1日を効力発生日として普通株式１株に対して２株の株式分割をしました。
2025年3月期実績のEPSは当該株式分割前の額であり、2026年3月期予想のEPSは当該株式分割を考慮しておりません。

2026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

中期経営計画

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洩
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洩

・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、情報漏洩)

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、情報漏洩)

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洩

GSXグループのビジネスモデル

GSX
GLOBAL SECURITY EXPERTS

ターゲット

GSXグループの提供価値

準大手・中堅・中小企業（エンドユーザ）

中堅・中小企業に必要な
セキュリティサービスを**フルラインナップ**

従業員教育
セキュリティ人材育成

診断 | 緊急対応 | コンサル

サイバーソリューション
導入・運用

IT企業・SIer

セキュリティ教育・資格制度で
IT人材を**プラス・セキュリティ人材へ**

当社オリジナル
SecuriST

EC-Council

CISSP

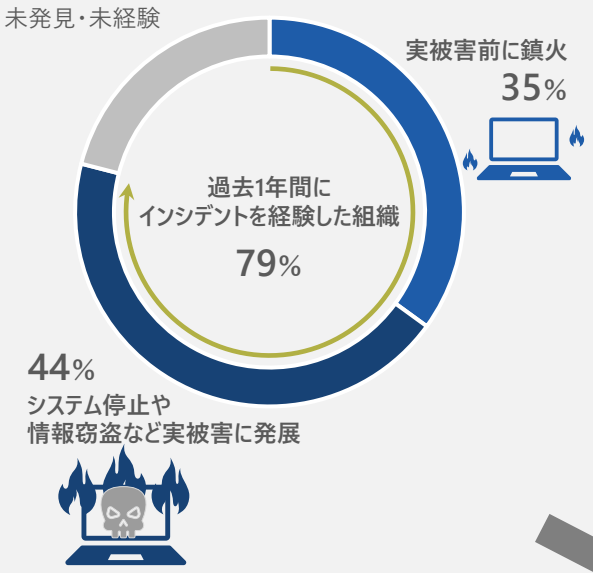
エンドユーザー・IT企業 問わず セキュリティ人材が必要な企業

セキュリティ人材不足を背景に
セキュリティ人材育成スキームにより
IT人材をバリューアップ
セキュリティ人材SESの提供

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

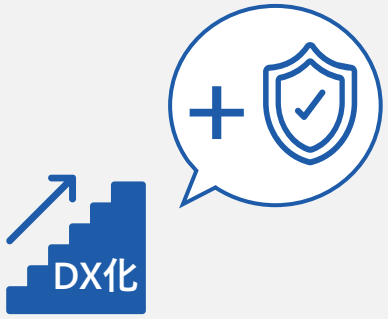
**国や各省庁から降りてくる多数の
セキュリティガイドライン**

**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**

DX化の加速

DX推進は、セキュリティ対策とセットで

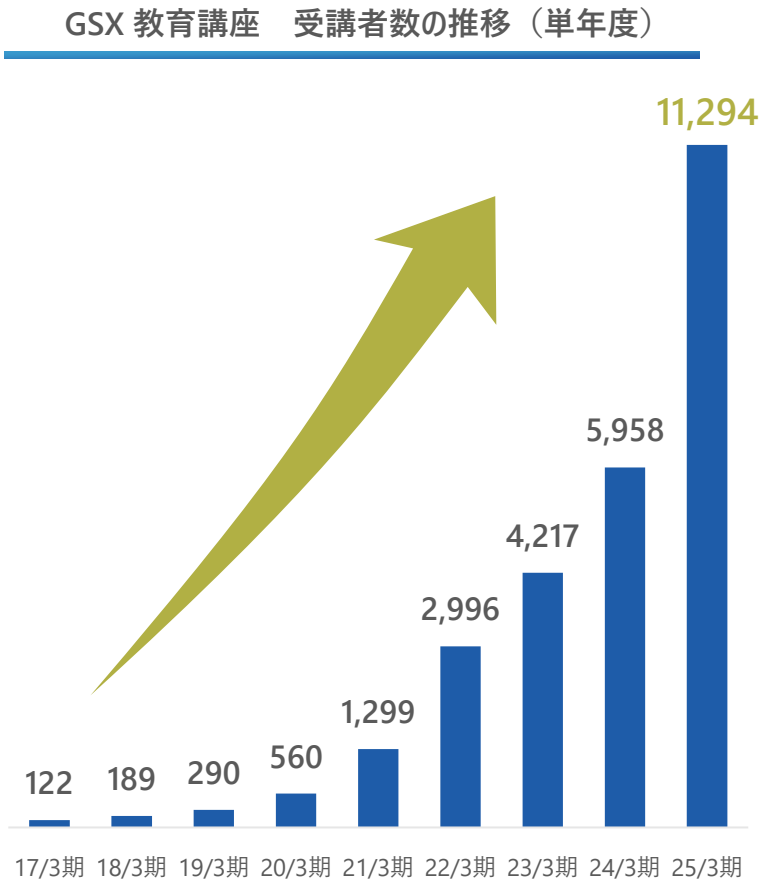
- ✓ 企業競争力向上にはDX化が急務
- ✓ DX推進はセキュリティ対策とセットで行う必要がある



準大手・中堅・中小企業

大企業においては、セキュリティ対策は常識となったが、
準大手・中堅・中小企業においてもセキュリティ対策をせざるを得ない状況 に

加速するIT企業・SIerのセキュリティ教育ニーズ



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

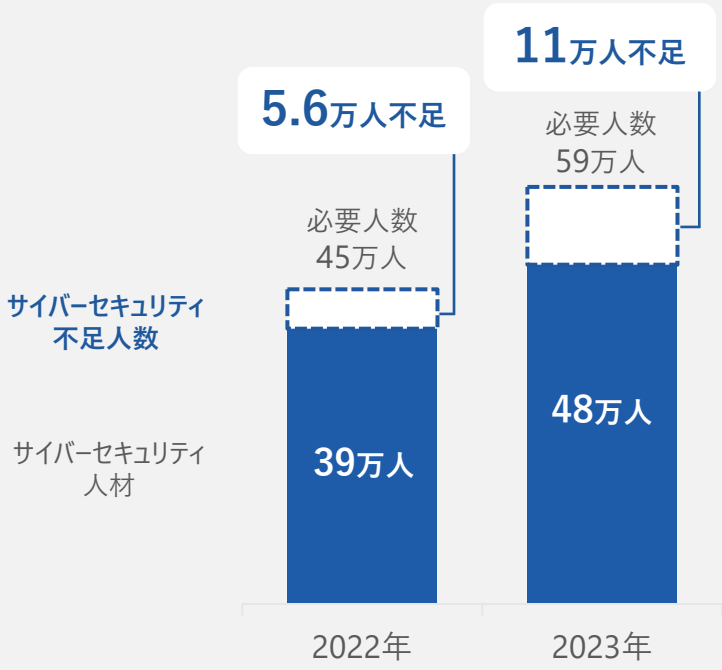
IT企業・SIerのIT人材に向けた セキュリティ教育ニーズが一気に高まっている

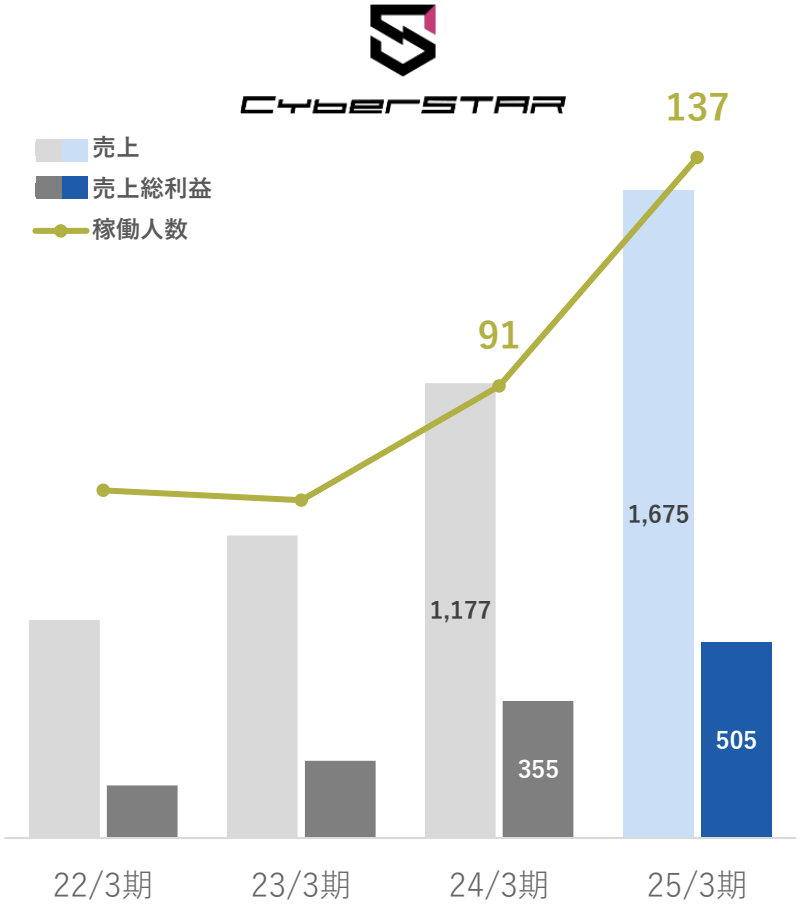
※「プラス・セキュリティ」：
自らの業務遂行にあたってセキュリティを意識し、必要かつ十分なセキュリティ対策を実現できる能力を身につけること、あるいは身につけている状態のこと

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

セキュリティ人材数は増加するも、不足人数は約２倍に増え、
人材の増加でカバーできていない





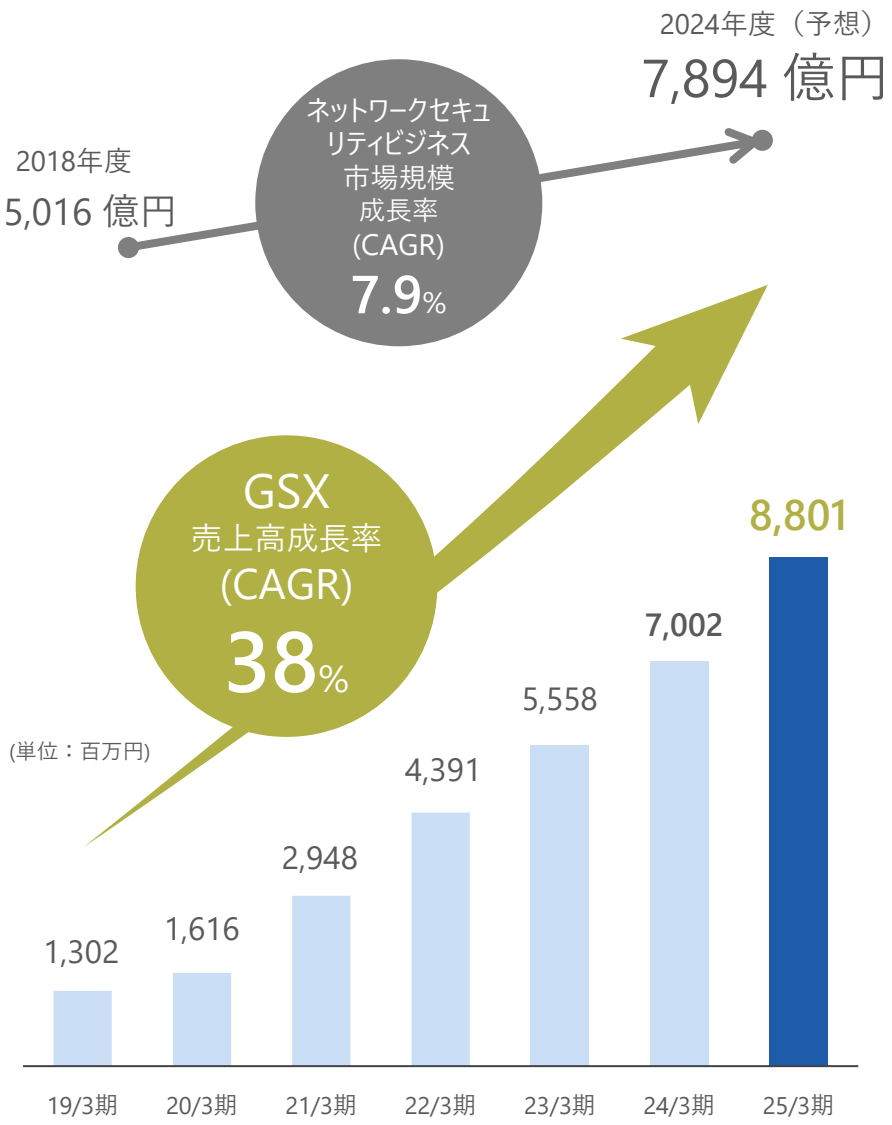
約9割の日本企業がセキュリティ人材不足に悩む一方、キャリアップを望む働き手にとって「情報セキュリティ」は注目の職種

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38%と市場成長率7.9%を大きく上回る水準で推移



出所：2023 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

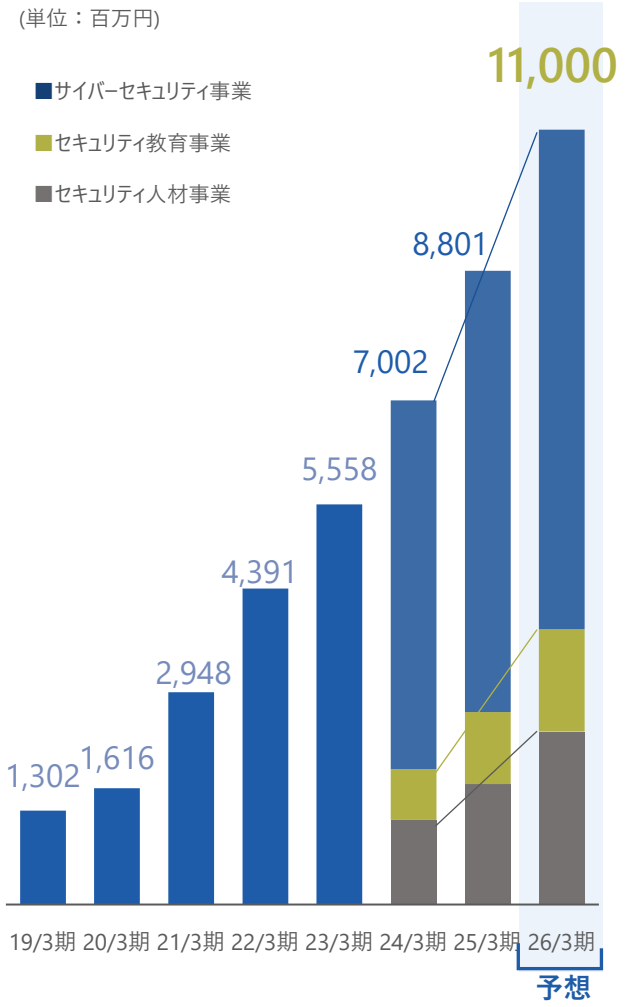
理由 3
セキュリティ人材を育成して提供する
独自のセキュリティ人材ビジネスモデル

展望
分社化により
セキュリティ人材SESが加速度的に拡大

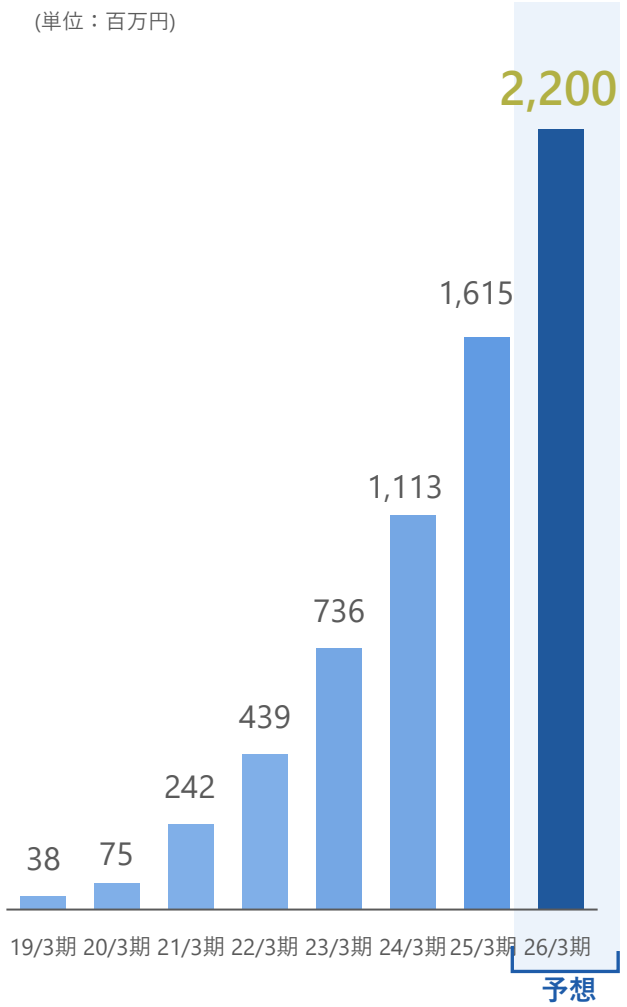
既存事業で 年率25%の売上成長

営業利益率の向上を重視し、持続的な成長を支える強固な経営基盤に

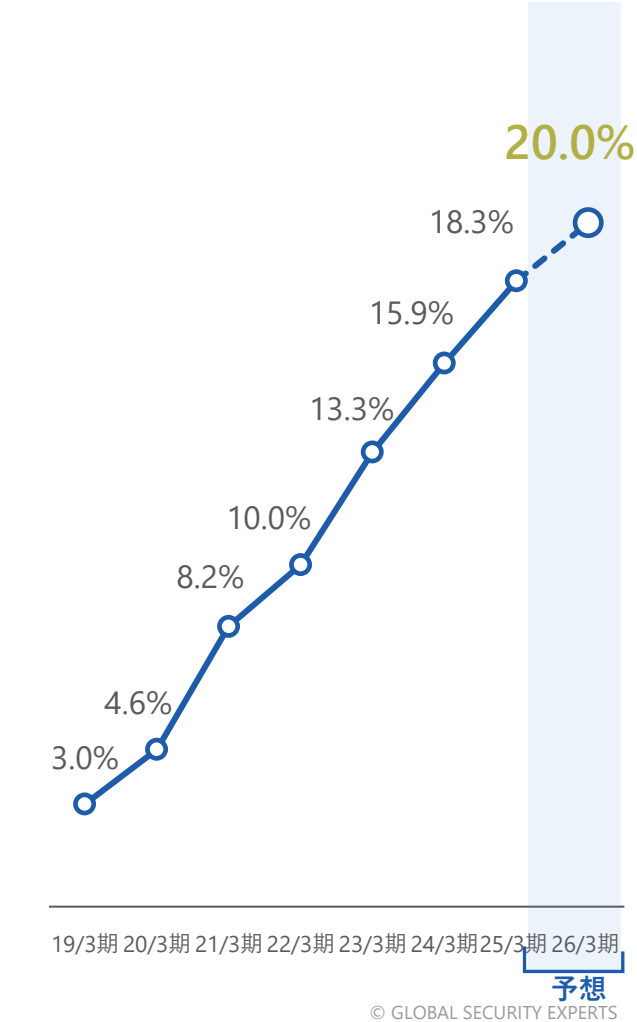
売上高および売上構成比



営業利益



営業利益率



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

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

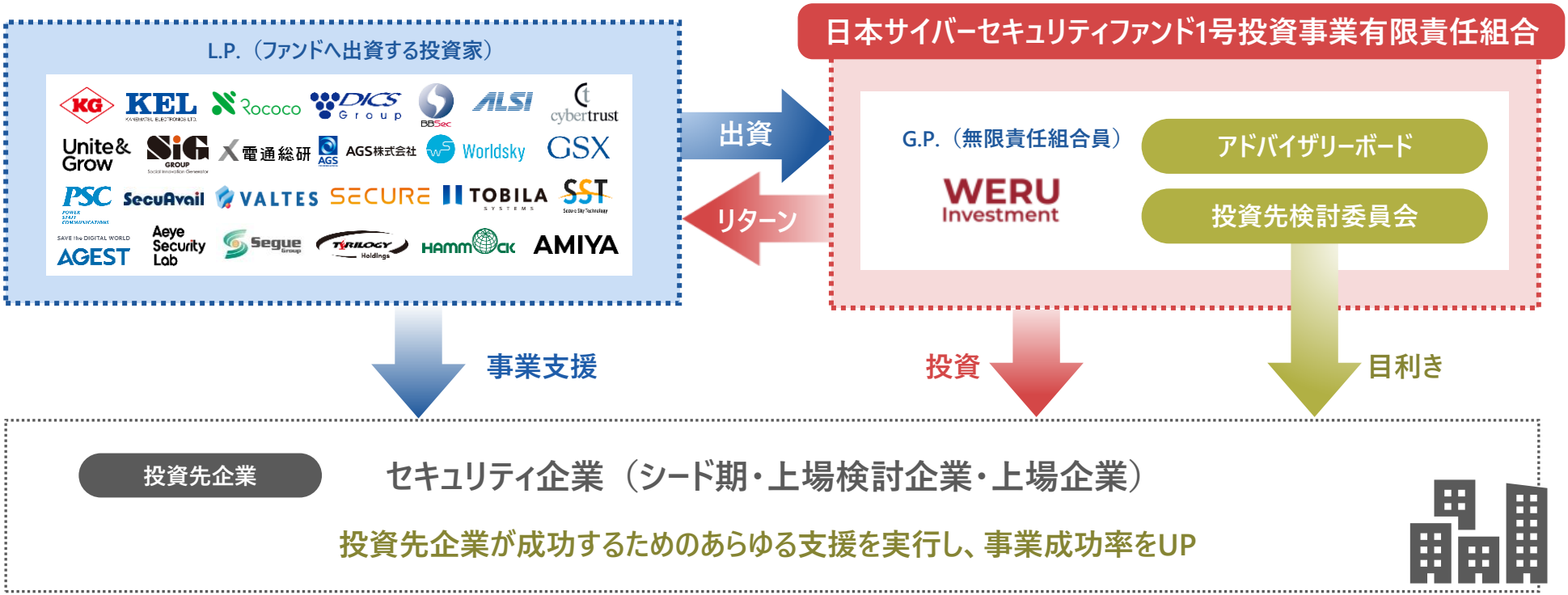
各種サービスを提供し得る人的リソースが増強されることによる売上貢献

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



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

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

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
セキュリティ教育でIT人材を
「プラス・セキュリティ」人材へ

セキュリティ人材が必要な企業
セキュリティ特化型の
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

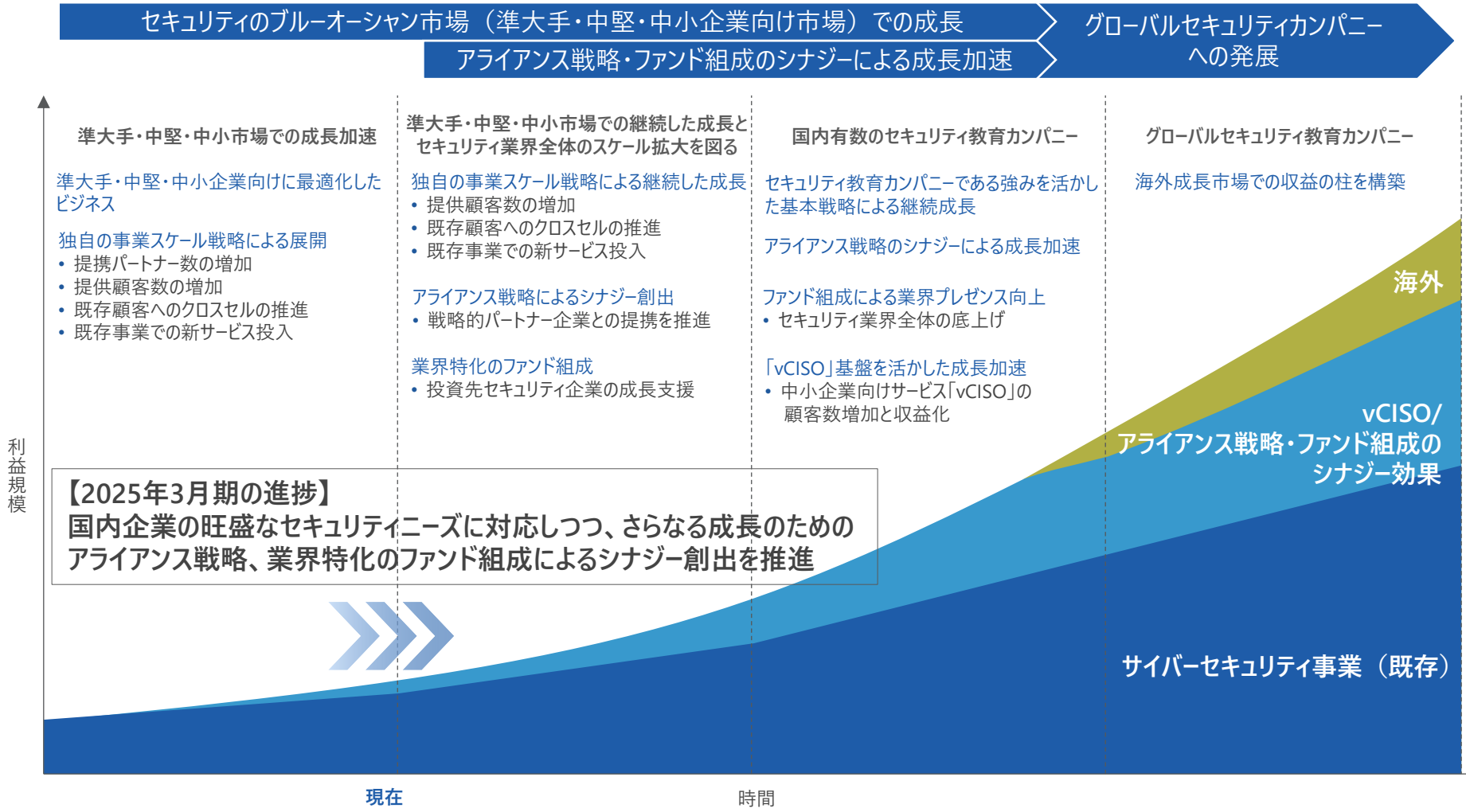
海外展開フロー

【2025年3月期の進捗】
コロナ禍により、いったん休止した海外展開は、ASEAN地域の現地エンジニア向けにセキュリティ教育講座を展開することで検討再開
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）にて早期の市場シェア拡大・市場創造を図りつつ、戦略的パートナー企業とのアライアンス戦略で成長を加速　業界特化のファンド組成によりサイバーセキュリティ業界全体の底上げを推進

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

国内サイバーセキュリティ市場を取り巻く市場環境

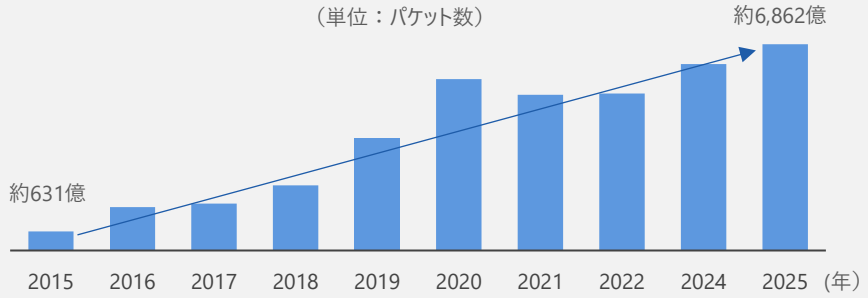
サイバーセキュリティ市場では、対策需要が増加。また、企業の急速なデジタル化の進展が同市場の成長への追い風
一方で、未曾有のセキュリティ人材不足が課題

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

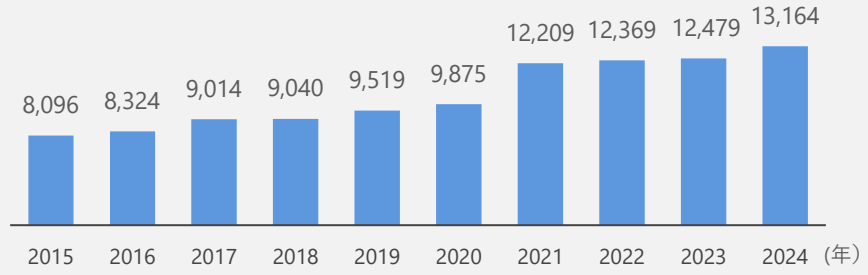
－サイバー攻撃関連通信数の推移－※1

（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－

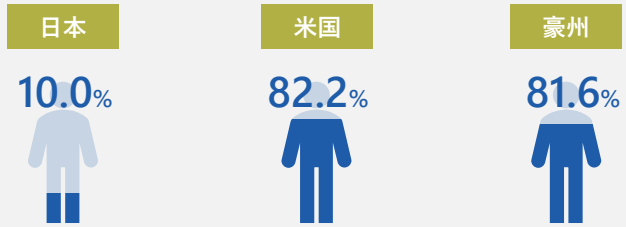
2020年度見込
8,787億円
+66%
2025年度予測
1兆4,593億円

－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



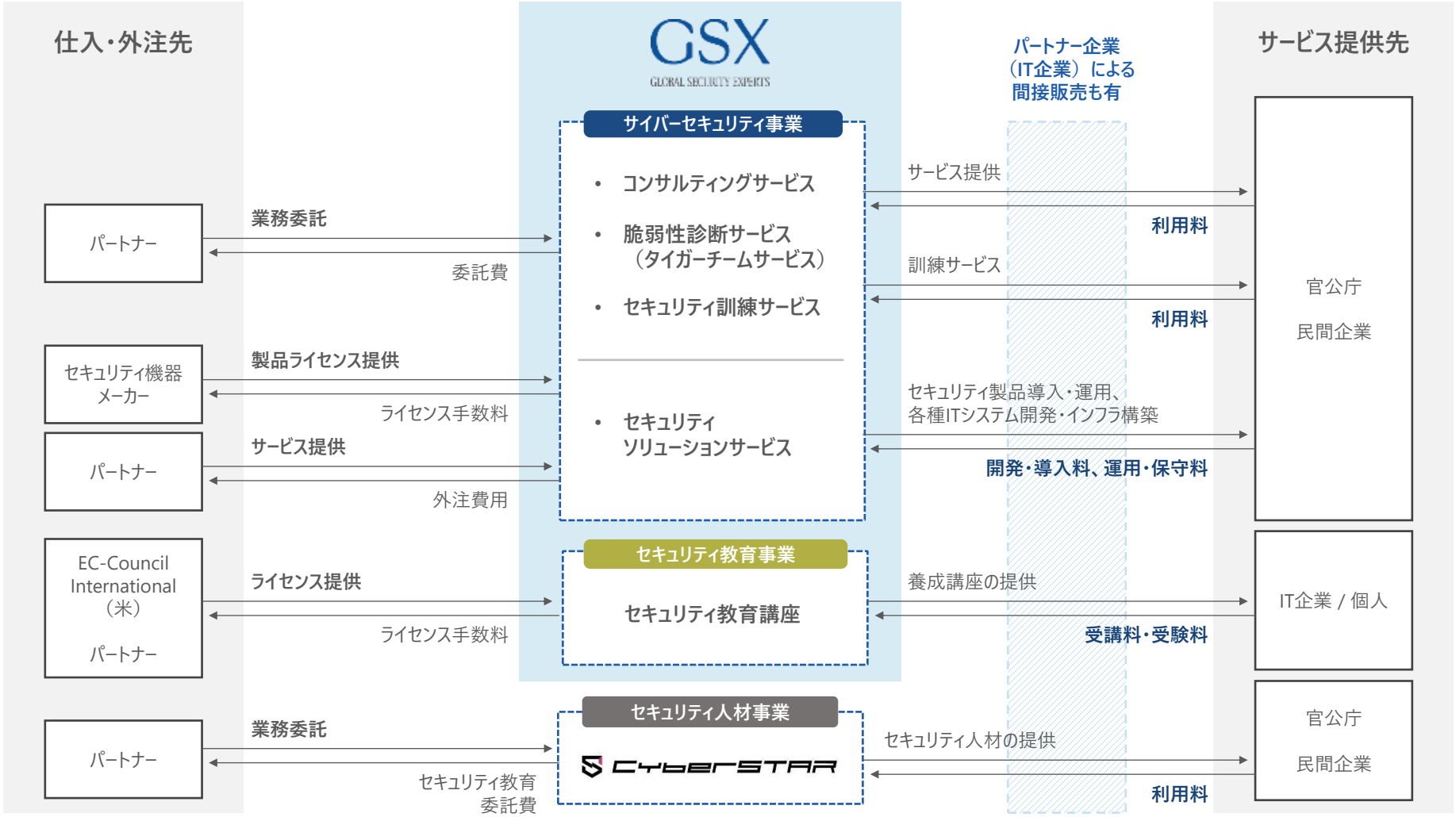
出所 ※１：国立研究開発法人情報通信研究機構「NICTER観測レポート2024」
出所 ※２：「令和６年におけるサイバー空間をめぐる脅威の情勢等について」（警察庁）
https://japansecuritysummit.org/2025/03/11204/
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6/R06_cyber_jousei.pdf

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

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

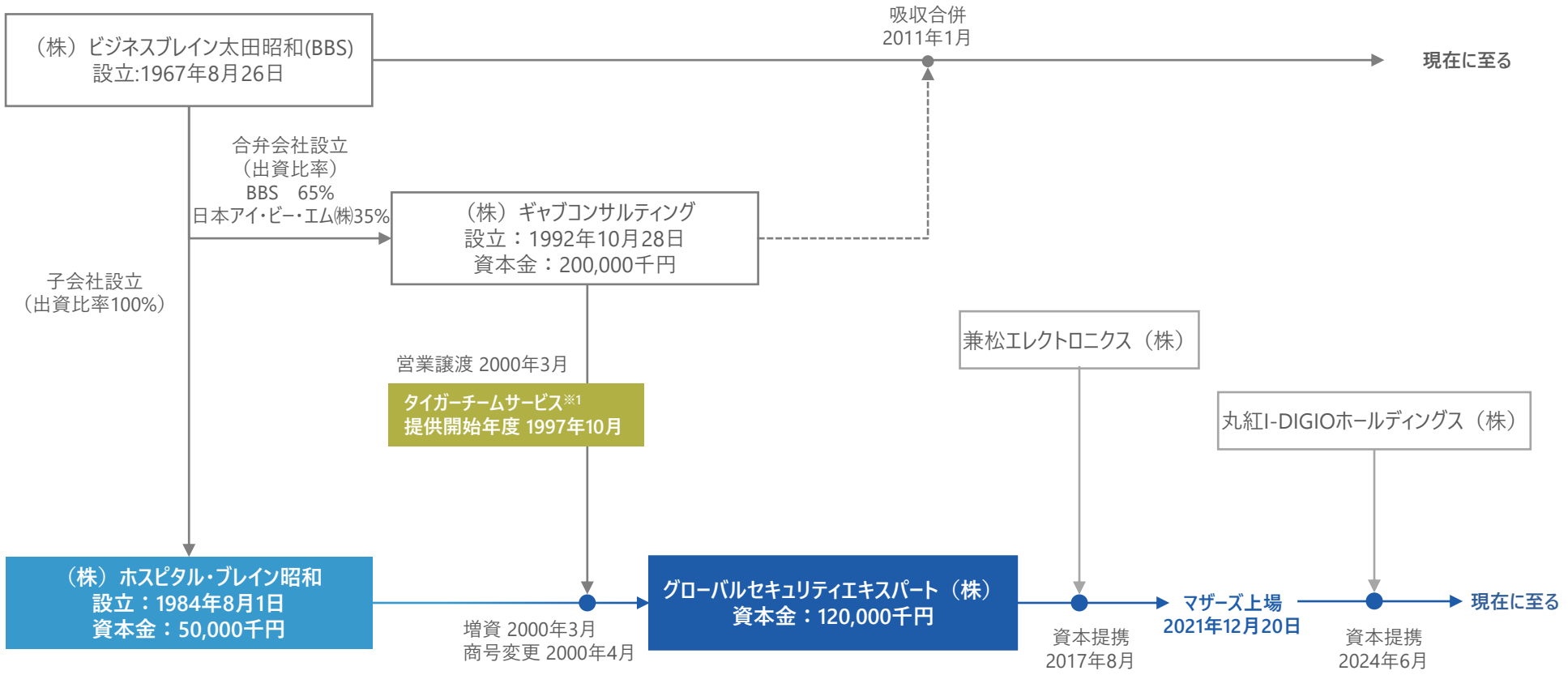
その他のサイバーセキュリティ事業、セキュリティ教育事業は主にフロー収入



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

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）

常務取締役
エリア統括

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

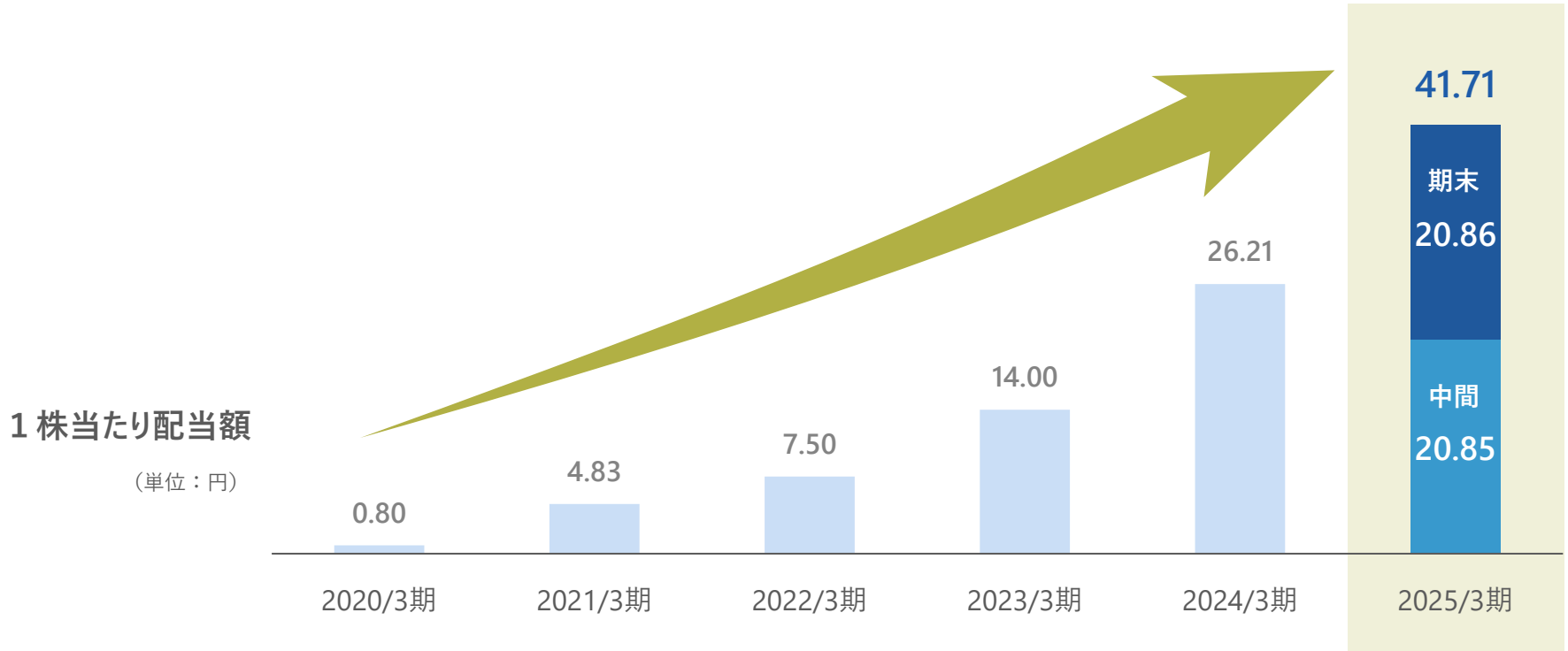
取締役
サイバーセキュリティ事業本部 副本部長

後藤　慶
Kei Goto

配当について

毎期の配当性向を向上させながら継続して配当を実施

2025年３月期は中間配当を新たに開始。年間の配当性向は31%に向上



配当性向	11.45%	17.67%	18.54%	19.39%	25.0%	**31.0%**

注釈：2020/3期から2022/3期の１株当たり配当額は、2021年10月22日付の株式分割（1：300）および2022年11月1日付の株式分割（1：2）を考慮した金額

株主優待

株主の皆様の日頃のご支援に感謝するとともに、当社株式の投資魅力を高めることを目的に、2025年3月期より株主優待制度を開始

優待内容

保有株式数	優待内容
200株以上	QUOカード 2,000円

➢ **対象となる株主様**

以下の①、②を両方満たす株主様
①毎年3月31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ている株主様
②1年以上継続保有されている株主様

➢ **進呈予定時期**

毎年６月下旬予定

こちらを進呈

※2025年5月31日を基準日とする株式分割に伴い保有株式数の基準を変更しました。
　本変更は、株式分割に伴う変更であり、実質的な変更はありません。

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。