令和９年３月期　第２四半期（中間期）決算短信補足説明資料

株式会社ＦＦＲＩセキュリティ

東証グロース：3692

目次

・2027年3月期第２四半期　業績説明

・市場環境

・2027年3月期の取り組み

・2027年3月期　業績予想



業績サマリー

・ナショナルセキュリティ・サービスにおける経済安全保障重要技術育成プログラム（Kプログラム）案件が増加し、前年比で増収となった

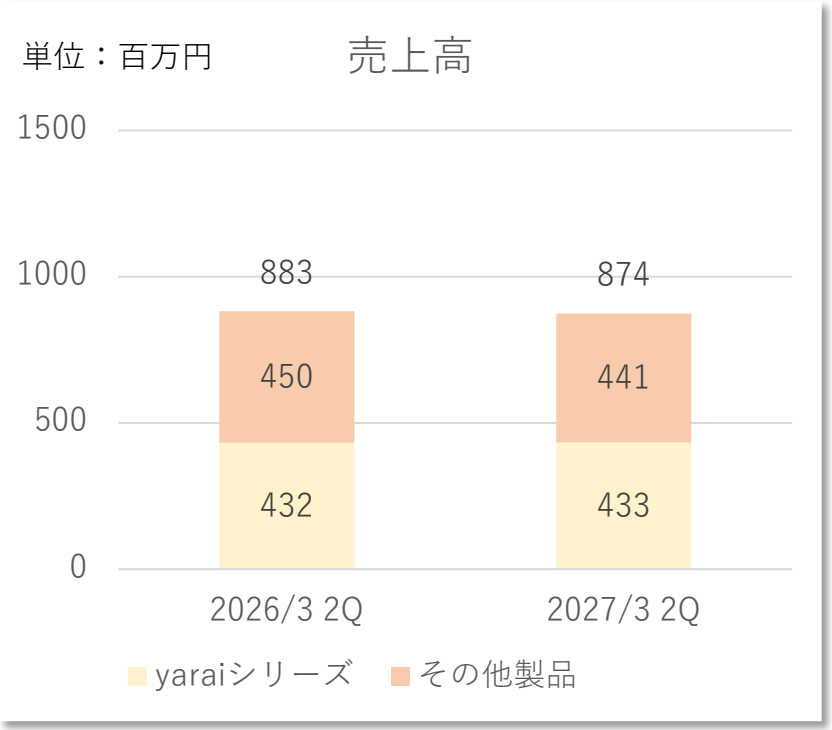
・Kプログラムにおける利益排除案件増加の影響及び、人員の増加、当社及び子会社における採用強化に伴うコスト増加の影響などにより利益率が減少しているものの、売上・利益ともに計画通りに進捗している

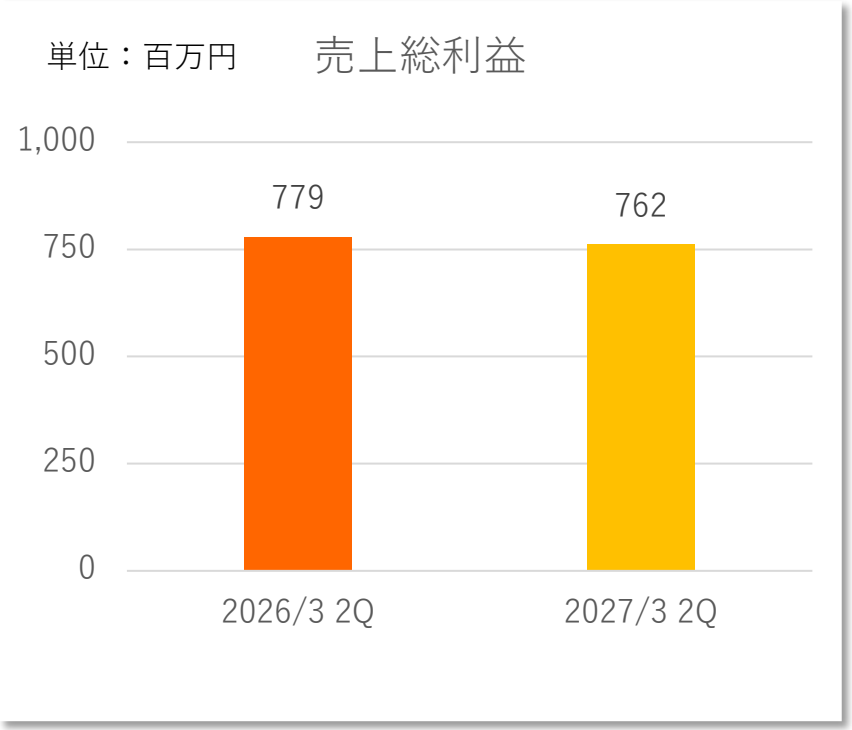
単位：百万円	2026/3 2Q	2027/3 2Q	YoY(%)
売上高	1,826	1,865	2.2
営業利益 (利益率:%)	548 (30.1)	416 (22.3)	△24.1
経常利益 (利益率:%)	574 (31.5)	426 (22.8)	△25.9
親会社株主に帰属する中間純利益 (利益率:%)	441 (24.2)	308 (16.6)	△30.1

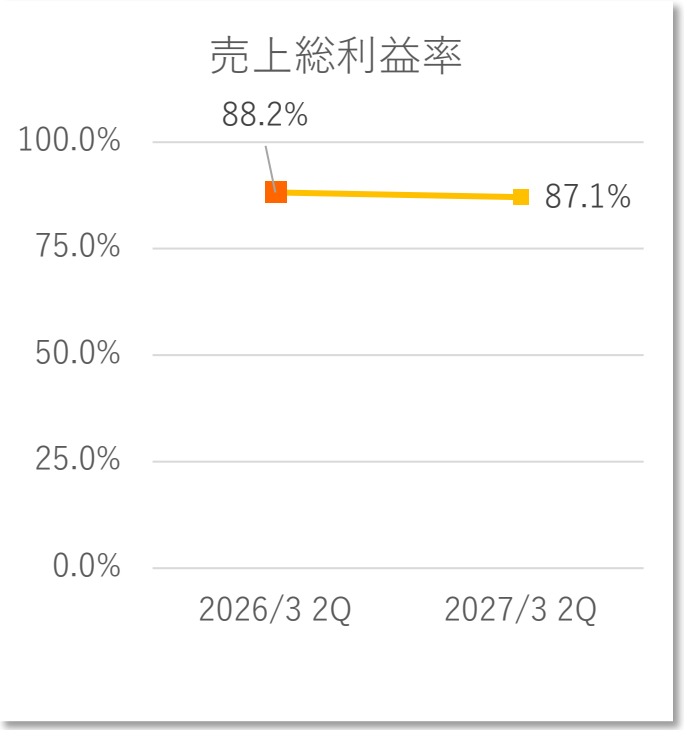
販売区分別の概況　セキュリティ製品

・yaraiシリーズにおいては期初の解約の影響もあるものの、OEM販売が好調に推移しており、売上高は前年を上回った

・その他製品におけるFFRI yarai analyzer は、前期にスポットの契約があったため減収となったものの、ライセンス数は横ばいで推移



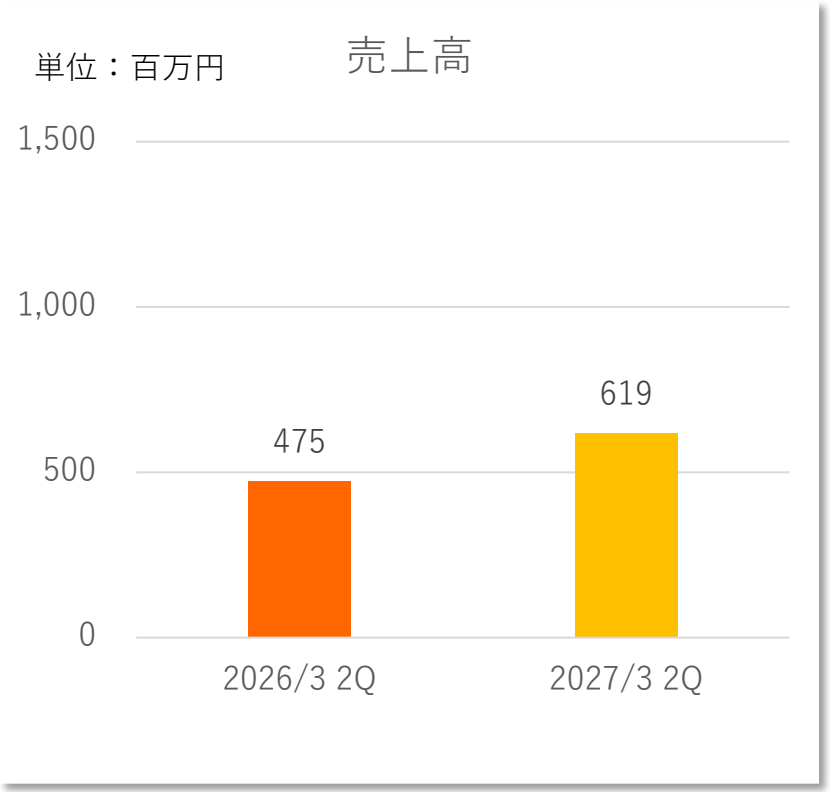


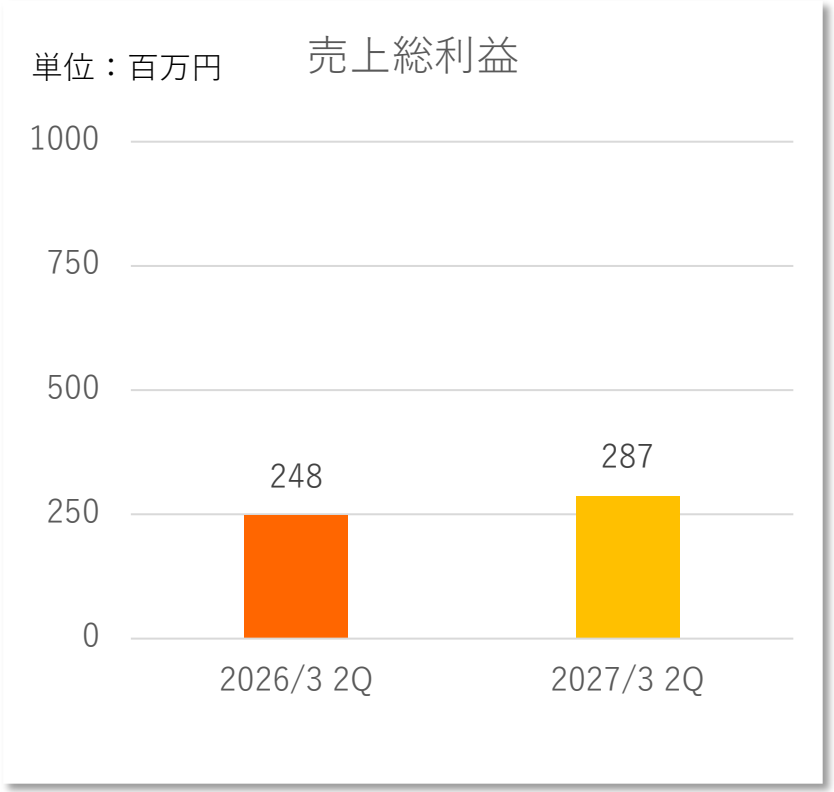


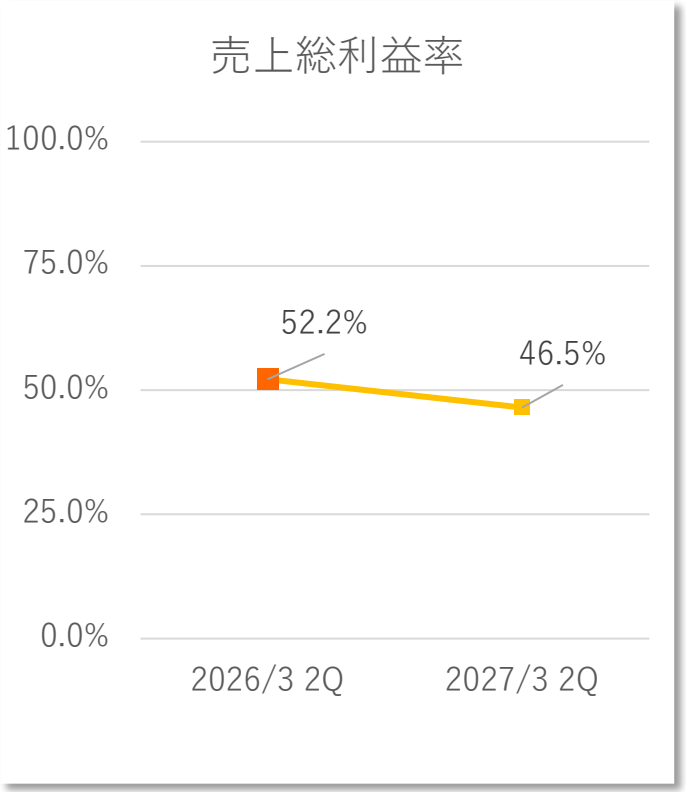
販売区分別の概況　ナショナルセキュリティ・サービス

・経済安全保障重要技術育成プログラム（Kプログラム）や、サイバー安全保障関連の案件を実施

・利益排除を条件に、研究成果（プログラム著作物など）が当社に帰属する研究開発案件の割合が増加し、一時的に利益率が減少。将来的に研究成果を製品・サービスとして提供することで利益貢献する見込み







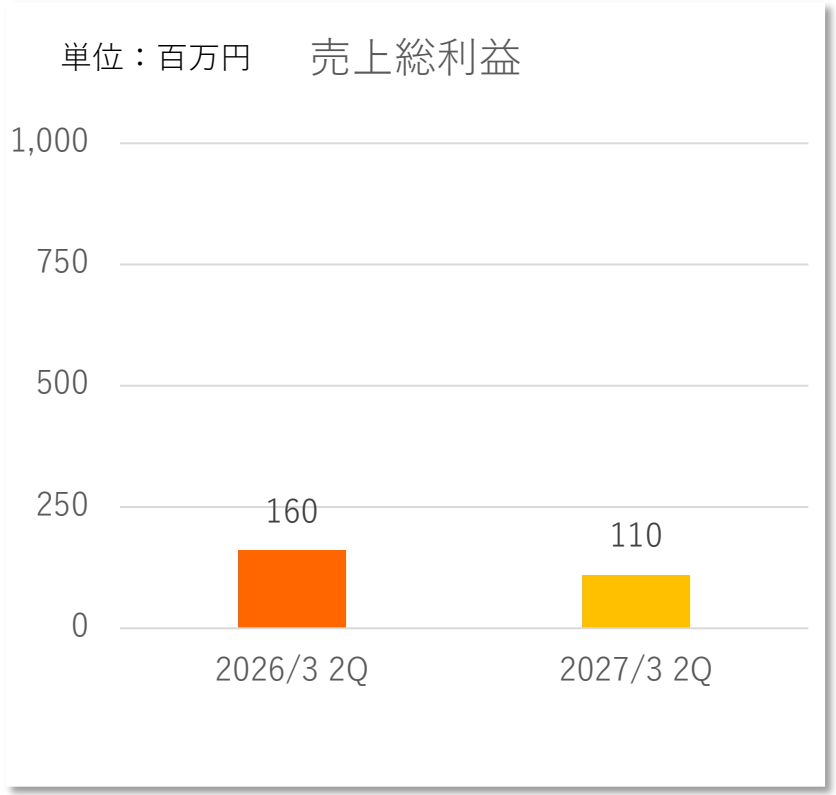
販売区分別の概況　その他セキュリティ・サービス

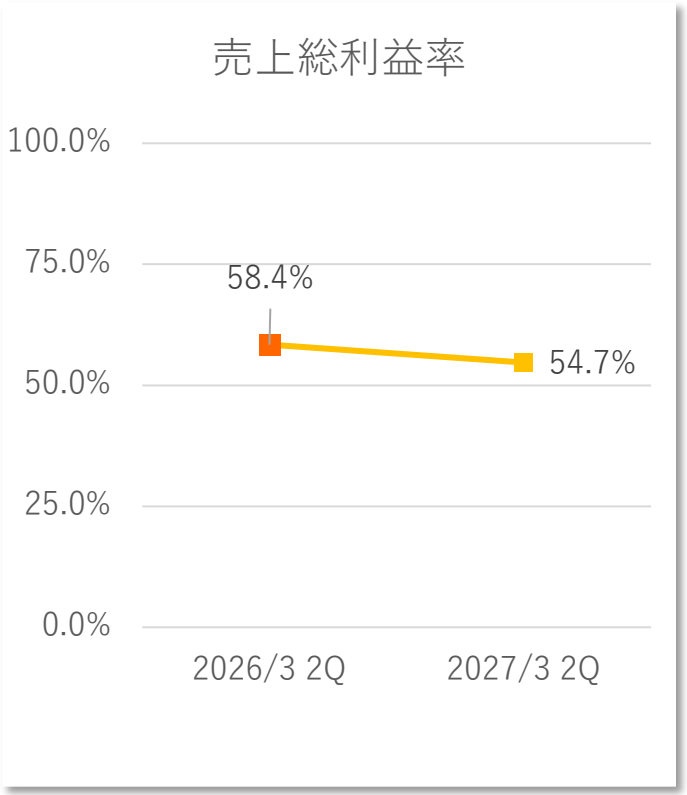
・主に官公庁にセキュリティ情報提供や、受託開発、調査・研究案件など長期案件を中心に実施

・前年同期にスポットの案件を実施した影響により、売上高・売上総利益ともに前年同期比では減少となったものの、計画どおりの進捗

・売上総利益率の変動は受注案件のミックスの変化による影響

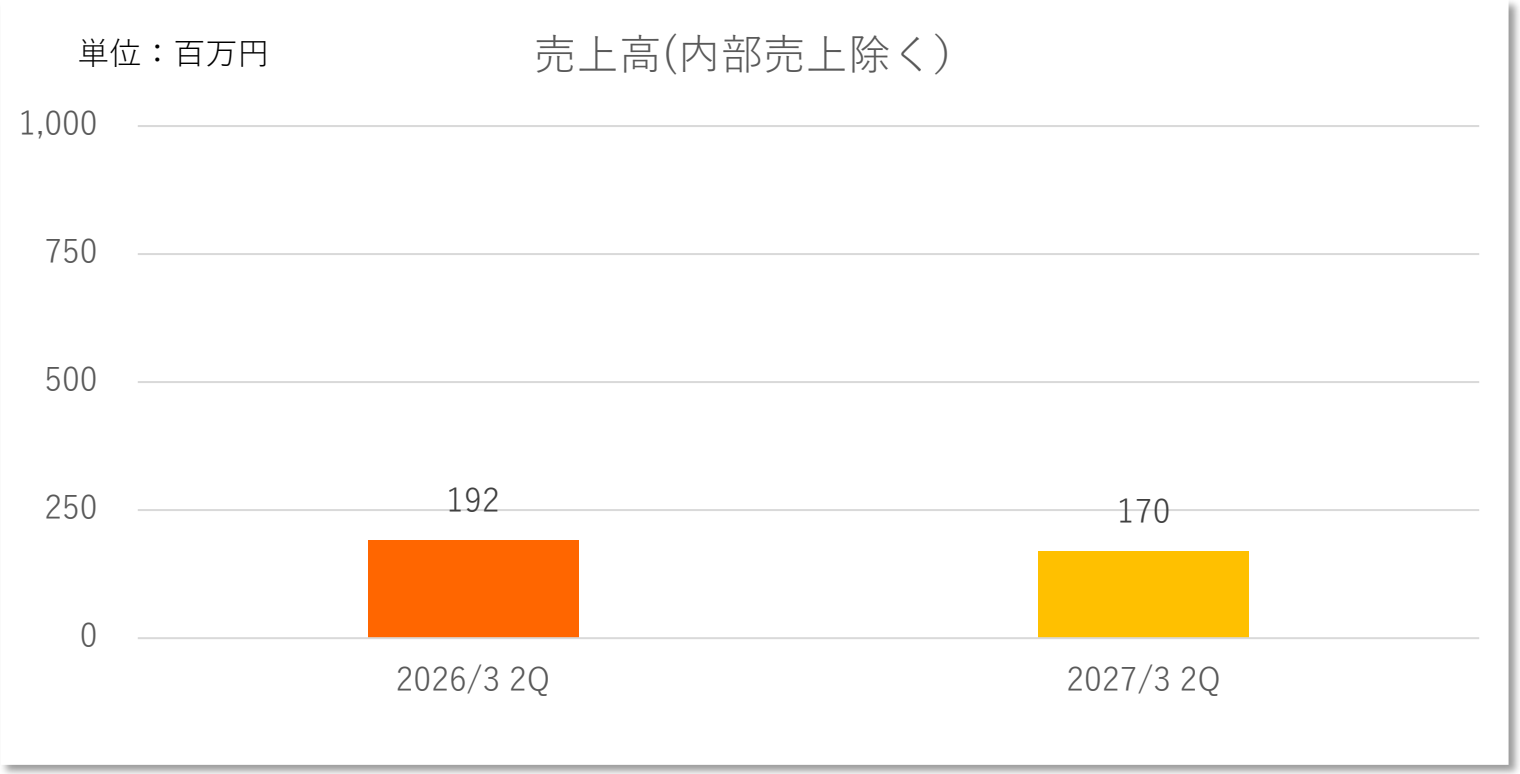






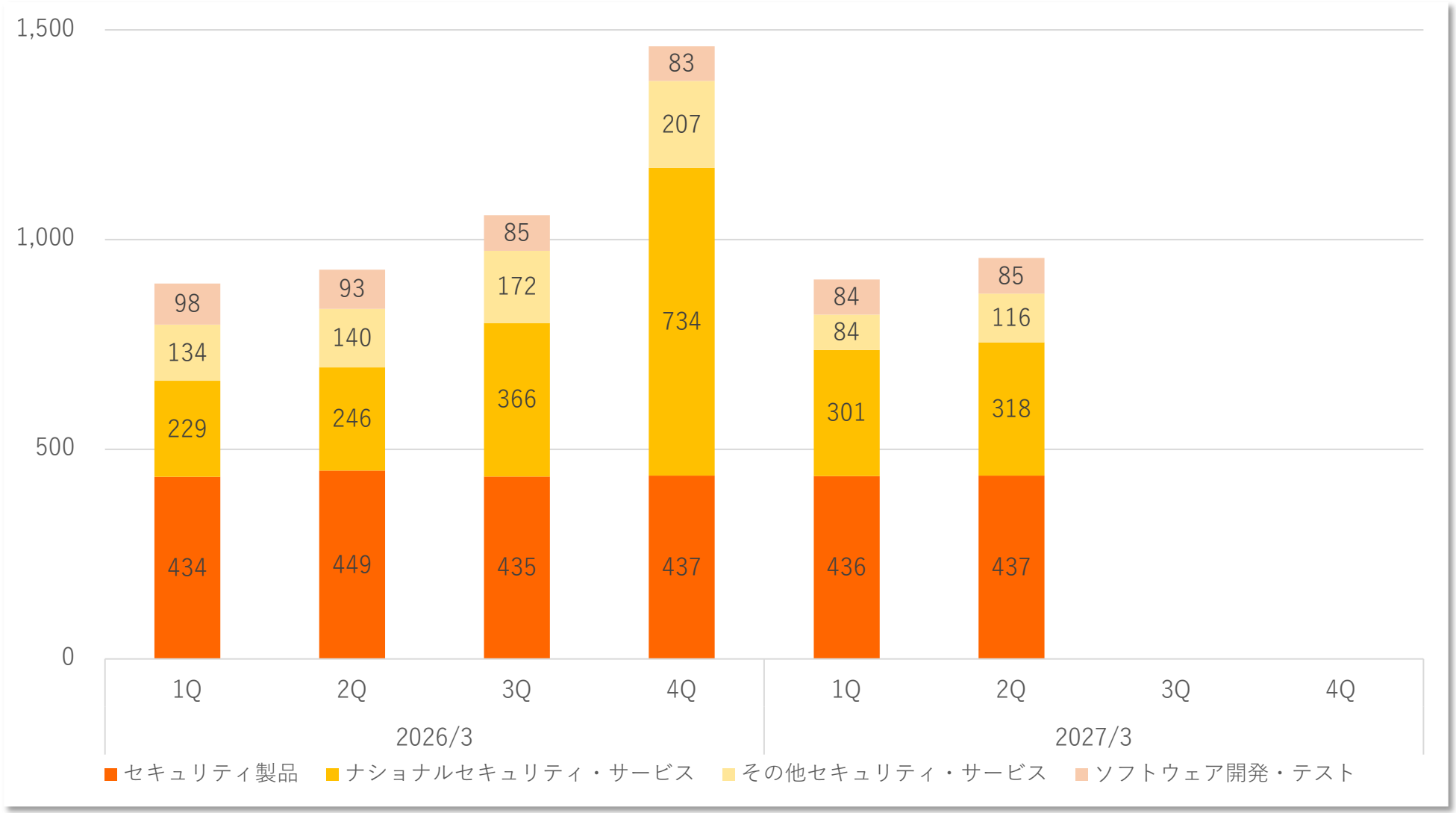
販売区分別の概況　ソフトウェア開発・テスト事業

・サイバーセキュリティ事業へと人材をシフトしており、当期も人員の一部をサイバーセキュリティ事業の業務にアサインしているため売上高は前年比で減少となった。



四半期毎の売上推移

単位：百万円



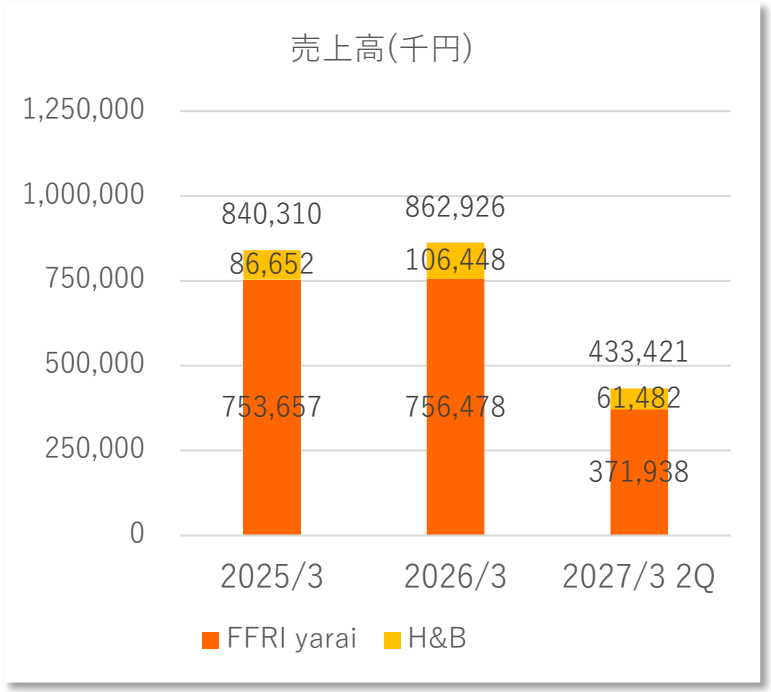
FFRI yarai シリーズの販売状況

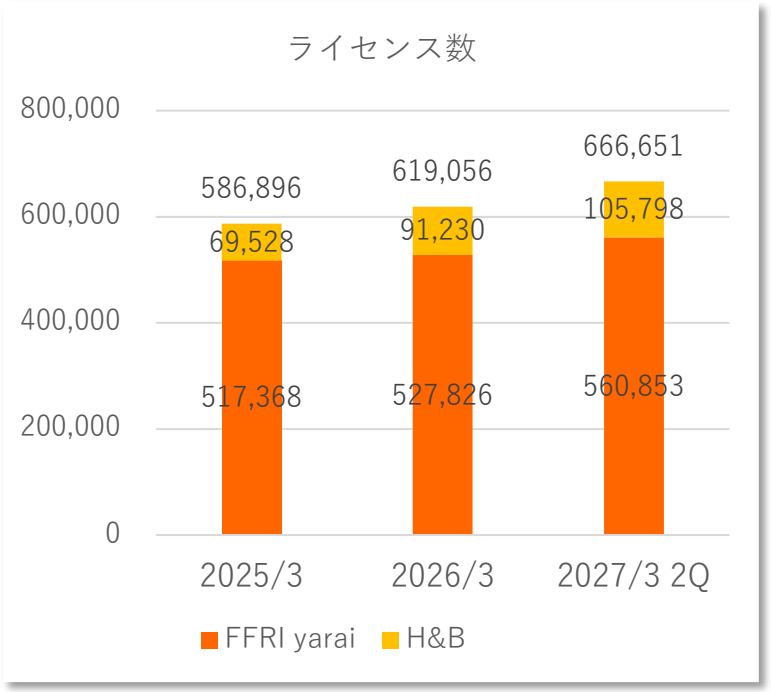
・戦略的販売パートナーによる中小企業等へのOEM販売が好調に推移し、前期末に比べ47,595ライセンス増加となった。

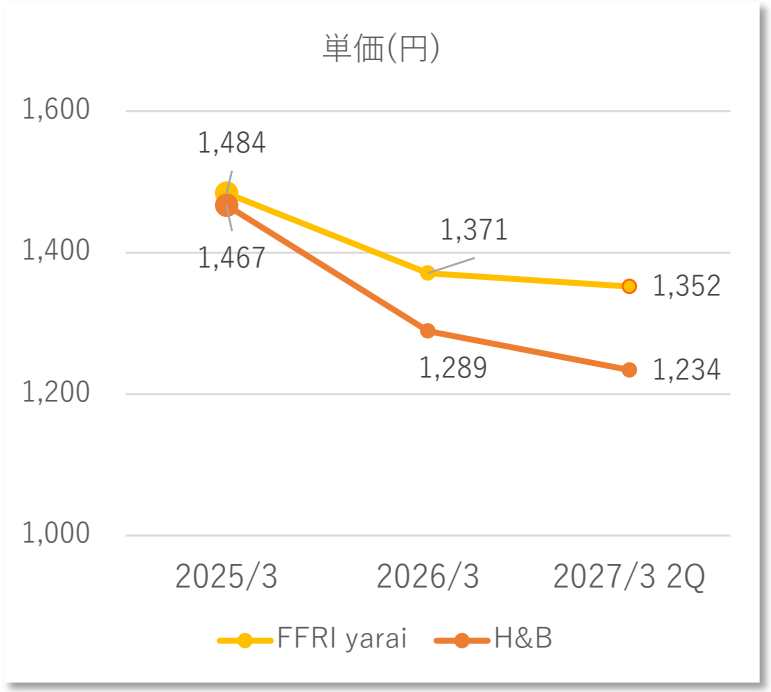
・FFRI yarai Home and Business Edition では、OEM販売が増加した結果、単価の高い自社オンライン・ショップでの販売比率が減少し、単価は減少しているものの、売上高・ライセンス数ともに前年同期を上回って推移している

FFRI yarai

※H&B ・・・FFRI yarai Home and Business Edition







FFRI yarai シリーズの業種別 契約ライセンス数

- 官公庁：期初の大口顧客の解約に伴い減少
- その他の業種：販売パートナーによる販売拡大施策を進めた結果、幅広い業種で契約が増加

※FFRI yarai 及び FFRI yarai Home and Business Edition のライセンス数の合算となります

業種	2026/3		2027/3 2Q	
	ライセンス	割合(%)	ライセンス	割合(%)
官公庁	245,708	39.7	230,264	34.5
金融サービス	20,215	3.3	22,894	3.4
情報通信	31,534	5.1	32,356	4.9
産業インフラ・サービス	27,482	4.4	25,845	3.9
その他業種・個人	294,117	47.5	355,292	53.3
合計	619,056	100.0	666,651	100.0

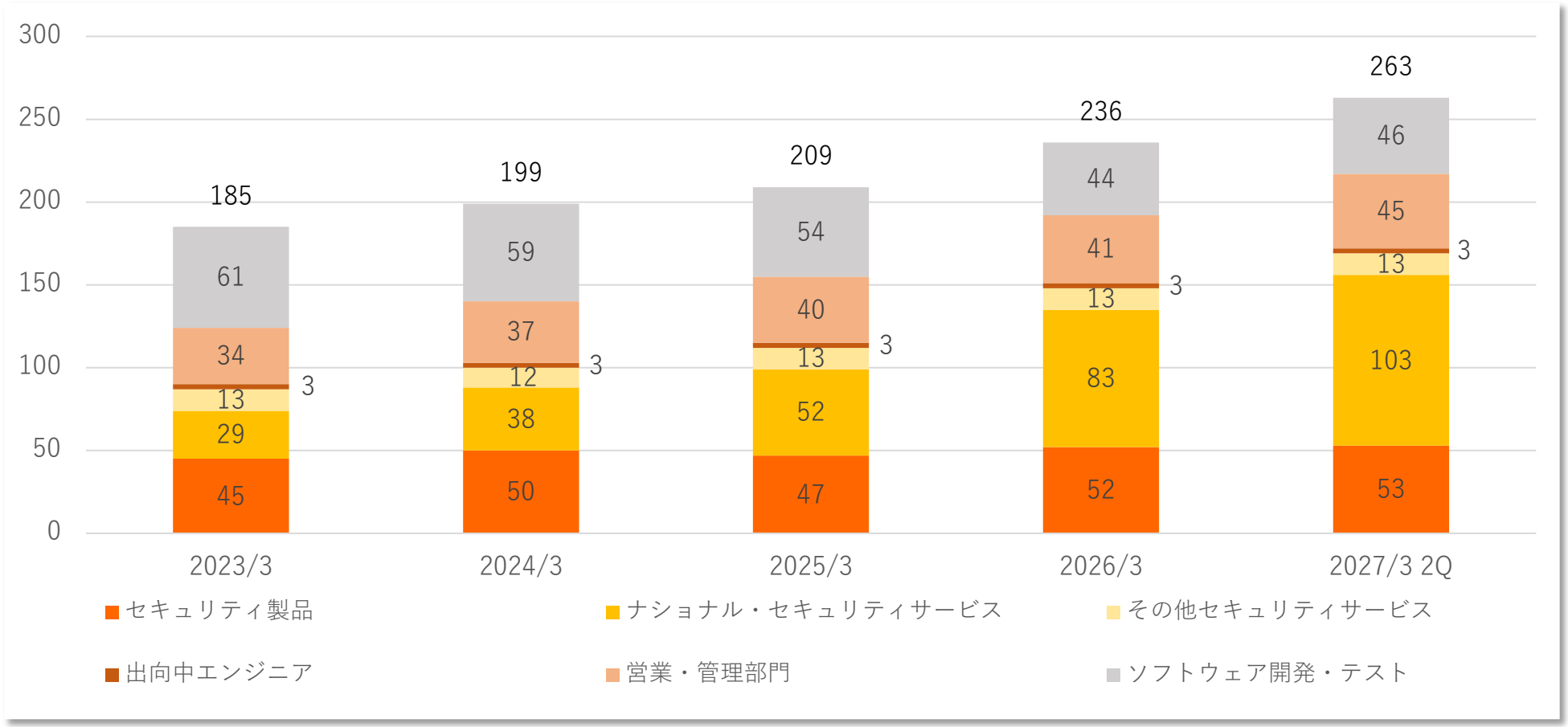
人員数の推移（連結）

・26年春入社のセキュリティエンジニア18名は8月より各部門に配属（セキュリティ製品：１名、ナショナルセキュリティ・サービス17名）

・エンジニアの中途採用では、プロジェクトマネージャークラスを中心に４名が入社

・ＦＦＲＩセキュリティ・ワークスでも４名が入社し、セキュリティ・サービス事業を開始

単位：人



原価及び販売管理費の内訳

- 労務費/人件費：セキュリティ・エンジニアの増員及び待遇向上に伴う増加
- 研究開発費：FFRI yaraiの機能強化に関する研究実施などに伴う増加
- 採用費：当社及び子会社において採用強化に伴う増加
- その他：人員増に対応するためのコスト増や、採用活動強化に伴う諸費用の増加による

売上原価

単位：百万円	2026/3 2Q	2027/3 2Q	YoY
売上原価	599	659	10.1
労務費	619	731	18.0
経費	140	133	△5.0
期首・期末棚卸及び他勘定振替	△159	△205	-
(研究開発費への振替)	△29	△78	-
(ソフトウェアへの振替)	△19	△7	-
(その他の振替)	△111	△120	-
売上総利益	1,226	1,205	△1.7
売上総利益率	67.2	64.6	

販売管理費

単位：百万円	2026/3 2Q	2027/3 2Q	YoY
販売管理費	678	789	16.4
人件費	315	330	4.8
研究開発費	52	102	97.1
採用費	33	50	48.8
販売促進費	114	124	9.1
その他	162	180	11.3
営業利益	548	416	△24.1
営業利益率	30.1	22.3	

業績サマリー（B／S）

- 売掛金及び契約資産：セキュリティ・サービス案件の入金に伴う減少
- 流動負債：外注利用に伴う買掛金の支払による減少

資産

単位：百万円	2026/3	2027/3 2Q	YoY
資産合計	5,879	5,526	△6.0
流動資産	4,706	4,549	△3.3
現金及び預金	3,334	3,472	4.2
売掛金及び契約資産	1,288	951	△26.2
固定資産	1,173	976	△16.7
出資金	480	280	△41.7

負債・純資産

単位：百万円	2026/3	2027/3 2Q	YoY
負債合計	2,101	1,582	△24.7
流動負債	2,072	1,553	△25.1
買掛金	355	9	△97.2
契約負債	1,179	1,269	7.6
固定負債	28	29	3.7
純資産合計	3,777	3,943	4.4
株主資本	3,777	3,943	4.4
利益剰余金	3,653	3,820	4.6

業績サマリー（C／F）

- 営業活動によるキャッシュ・フロー：（その他）外注利用に伴う買掛金の支払いによる減少
- 財務活動によるキャッシュ・フロー：配当金の支払いによるもの

単位：百万円	2026/3 2Q	2027/3 2Q
営業活動によるキャッシュ・フロー	1,416	105
税引前中間純利益	574	427
減価償却費	23	21
売上債権及び契約資産の増減額(△は増加)	457	337
契約負債の増減額(△は減少)	548	89
法人税等の支払額	△133	△256
その他	△54	△513
投資活動によるキャッシュ・フロー	△57	175
財務活動によるキャッシュ・フロー	△110	△142
現金及び現金同等物の期末残高	3,411	3,472

目次

・2027年3月期　第２四半期　業績説明

・**市場環境**

・2027年3月期の取り組み

・2027年3月期　業績予想



サイバー安全保障に関する政策

・国家及び社会基盤全体のサイバーセキュリティ能力の底上げを進めている

令和８年５月 **Project YATA-Shield が策定**

令和８年４月 **サイバー通信情報監理委員会が設置**

※能動的サイバー防御における審査・承認・事後監視を担う政府から独立した第三者機関。

令和８年７月 **重要インフラのサイバーセキュリティ対策のための統一基準が策定**

※同10月１日より施行

令和８年８月 **サプライチェーン・セキュリティ対策評価制度（SCS評価制度）が施行**

令和８年10月 **サイバー対処能力強化法（能動的サイバー防御法）が段階的に施行**

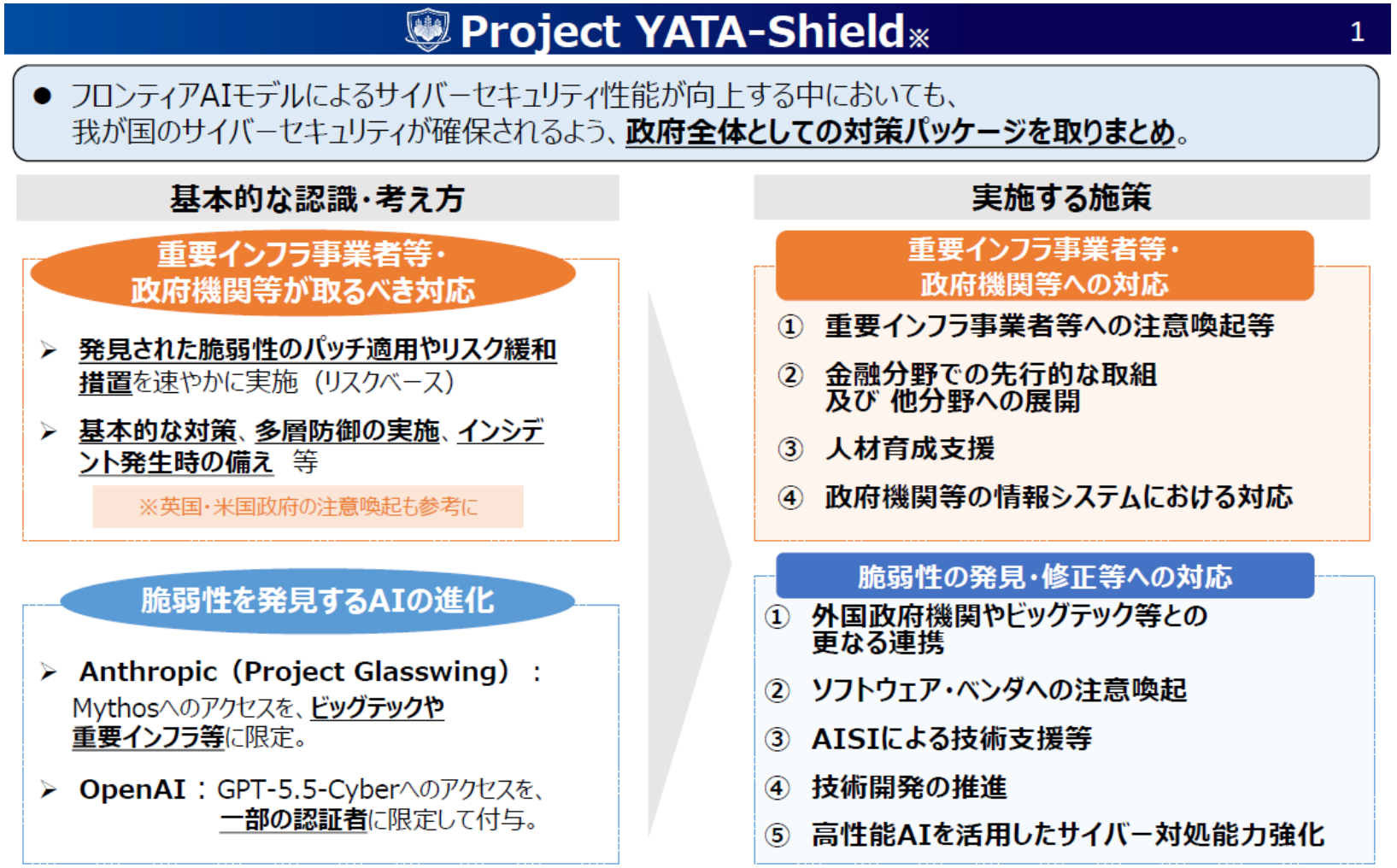
令和８年10月 **「サイバーセキュリティ対策の抜本的強化に関する提言」が申し入れ**

AIを悪用したサイバー攻撃の高度化を受け、サイバー防衛能力強化を求める政策提言

令和８年11月 **「サイバーセキュリティ緊急対策パッケージ」を決定**

Project YATA-Shield

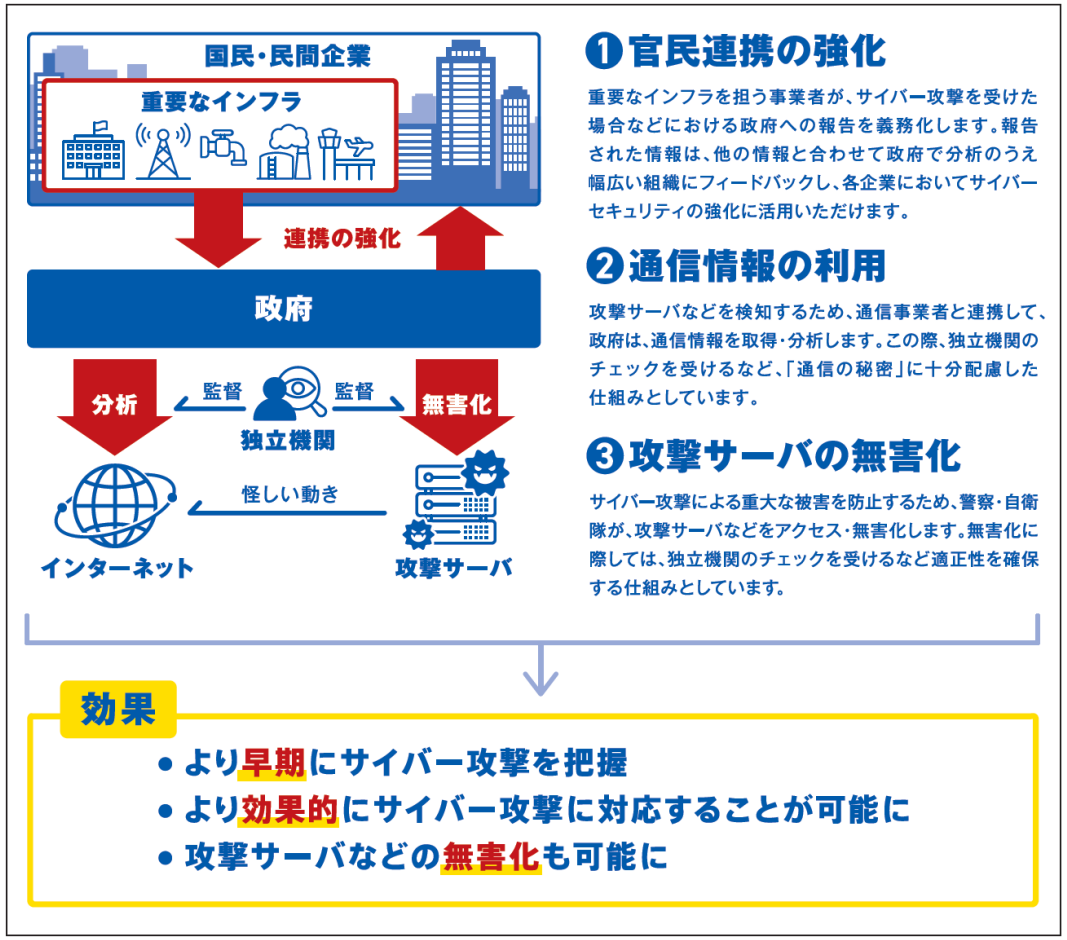
- AI技術の高度化に伴うサイバー攻撃の高速化・大規模化に対処するため、日本政府が取りまとめた官民一体のサイバーセキュリティ緊急対策パッケージ



※国家サイバー統括室 公開資料より

能動的サイバー防御の施行

- 重要インフラ事業者の重要システムに関する届け出や、サイバー攻撃の被害・兆候を速やかに報告することが義務化
- 重大な攻撃のおそれがある場合、サイバー通信情報監理委員会の事前承認のもと、無害化措置が可能に



※内閣官房「みんなで備えよう。新・サイバー防御、はじまる」より

重要インフラ事業者の義務

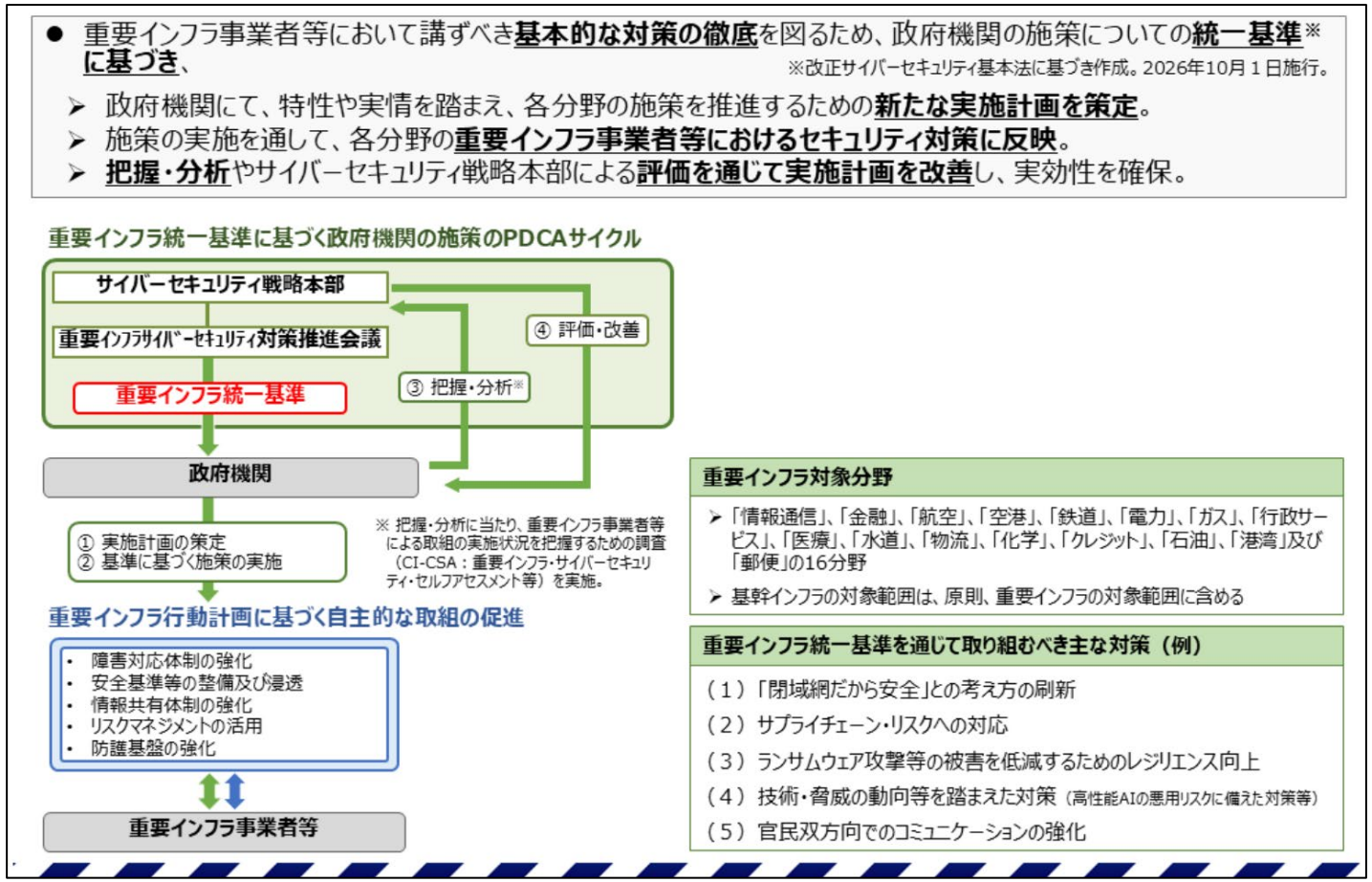
・重要インフラを支えるシステムの中でも特に重要なシステムにおいて使用する機器製品名等を所管大臣に届け出
・不正アクセスや攻撃の兆候、被害につながる可能性のある異常を認知した場合直ちに所管大臣及び内閣総理大臣に報告

サイバー通信情報監理委員会の役割

・能動的サイバー防御の運用に必要な通信情報の取得・分析が必要最小限の範囲に留まっているか審査・監視する
・深刻な攻撃が懸念される場合のアクセス無害化措置について、適切で不可欠なものか審査・監視する

重要インフラのサイバーセキュリティ対策のための統一基準

- 重要インフラ事業者等において講ずべき基本的な対策の徹底を図るための具体的かつ統一的な基準
- 技術的な対策のみならず、経営層の責任とリーダーシップを最上位課題とし、セキュリティ対策の構築とインシデント時の早期復旧体制の構築を求めている



※国家サイバー統括室「重要インフラ対策関連」資料より

基本的な考え方

・重要インフラを取り巻く情勢は、システム利用の高度化、複雑化、サイバー空間の脅威の急速な高まりを受け、重要インフラ事業者等においては、経営層、CISO、戦略マネジメント層、システム担当者を含めた組織全体での対応を一層促進する。特に、経営の重要事項としてサイバーセキュリティを取り込む方向で推進する。

・自組織の特性を明確化し、経営層からシステム担当者までの各階層の視点を有機的に組み合わせたリスクマネジメントを活用し、自組織に最も適した防護対策を実施する。

・重要インフラを取り巻く脅威の変化に適確に対応するため、サプライチェーン等を含め、将来の環境変化を先取りした包括的な対応を実施する。

※国家サイバー統括室「重要インフラ対策関連」資料より

SCS評価制度

- サプライチェーンを構成する企業のセキュリティ対策状況を共通の基準で評価・可視化する制度で、サプライチェーン全体のセキュリティ水準の底上げを図る
- 現在は★1～2の評価（自己評価）のみであり、★3～5の要求事項は令和9年3月以降段階的に公開予定

構築する評価制度

	★3		★4		★5 [検討中※5]
想定される脅威	• 広く認知された脆弱性等を悪用する一般的なサイバー攻撃		• 供給停止等によりサプライチェーンに大きな影響をもたらす企業への攻撃 • 機密情報等、情報漏えいにより大きな影響をもたらす資産への攻撃		• 未知の攻撃も含めた、高度なサイバー攻撃
対策の基本的な考え方	全てのサプライチェーン企業が**最低限実装すべき**セキュリティ対策: • 基礎的な組織的対策とシステム防御策を中心に実施		サプライチェーン企業等が**標準的に目指すべき**セキュリティ対策: • 組織ガバナンス・取引先管理、システム防御・検知、インシデント対応等包括的な対策を実施		サプライチェーン企業等がさらに目指すべき高度な対策: • 国際規格等におけるリスクベースの考え方に基づき、自組織に必要な改善工程を整備、システムに対しては現時点でのベストプラクティスの対策を実施
要求事項	26件	有効期間 1年	43件	有効期間 3年（毎年自己評価を実施し結果を評価機関へ提出）	（今後検討）
評価スキーム	専門家確認付き自己評価 ※4		第三者評価		第三者評価

[※4] 専門家：登録セキスペ、CISSP等の資格を有し、かつ制度が定める研修を受講したセキュリティ専門家　[※5] ISMS適合性評価制度、★3・4との整合性も踏まえ、対策事項を今後検討

※経済産業省「サプライチェーン強化に向けたセキュリティ対策評価制度（SCS評価制度）」より

サイバーセキュリティ対策の抜本的強化に関する提言 ～サイバー有事前夜/AIのサイバー飽和攻撃に備えよ！～

- 生成AI等の急速な発展と普及に伴い、サイバー攻撃はより自律化・高度化しつつある
- 今後これまでよりも影響の大きな事態が発生することも否定できない「サイバー有事前夜」ともいうべき重大な危機
- 官邸主導で「サイバー対処本部（仮称/事務局NCO）」を立ち上げ、司令塔の役目を担う

※国家サイバーセキュリティ戦略本部「サイバーセキュリティ対策の抜本的強化に関する提言」より

政府全体に対する基本提言

官邸主導で「サイバー対処本部（仮称）」を立ち上げ、司令塔として迅速に本部会議を開催。不安の払拭へ。

（1）サイバー対処能力強化法の取組強化
自衛隊・警察の能力構築、官民協議会の活用、通信情報の利用、同盟国連携の加速

（2）経営層の意識改革と開示の充実
経営の最重要課題とし、平時からの体制構築を促す

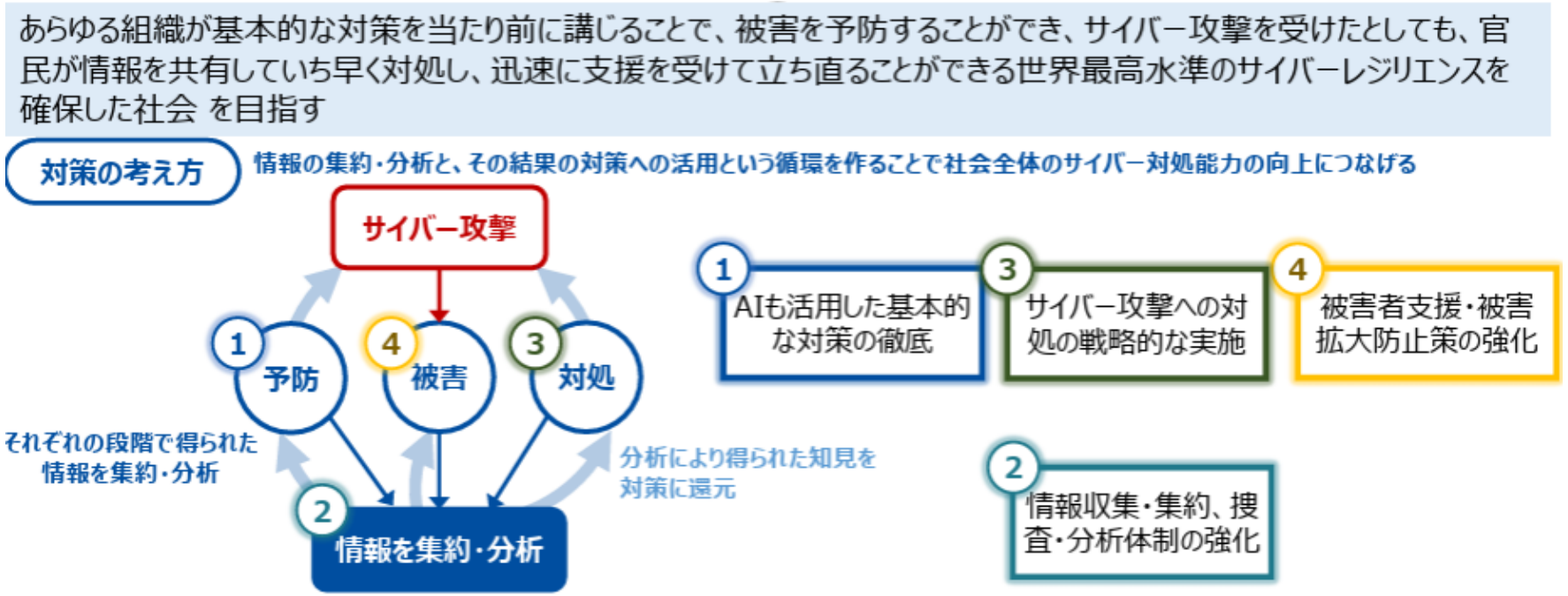
（3）人材の育成・確保
「トップガン」人材の待遇のため、公務員の新たな人事・給与制度、実践演習を通じた人材の裾野拡大

■サイバー空間の優劣は、国力を左右
来るべき「AIのサイバー飽和攻撃」を前に、政府は直ちに必要な予算措置及び法制化の検討に着手し、国民の安全と我が国の産業競争力を死守する責務がある。

■国内通信情報の利用検討を含む強い対応
サイバー対処能力強化法における外国関連通信情報の利用にとどまらず、国内通信情報の利用の検討も求める。

サイバーセキュリティ緊急対策パッケージ

- 相次ぐサイバー攻撃による情報漏洩を受け、早期に実施又は着手できる施策を中心に取りまとめた政策パッケージ
- 警察に新設する「ファスト・フォレンジック・フォース（仮称）」や、NCOに新設する「アウトリーチ・チーム」など、政府によるサポートのもと、特定の組織・業界に限らず我が国社会全体で基本的な対策を当たり前に講じる社会へ
- AIを活用し、攻撃者より先に脆弱性を見つけて塞ぐ「トップガン人材チーム」をIPAに立ち上げる



- 早期に実施又は着手できる施策を中心に、４つの柱の下に取りまとめ、スピード感をもって実施
- 情報収集の在り方を含む制度面の整備、政府の基準の見直し、ベンダとその契約事業者のシステム関連契約の在り方の周知、政府システム等のサプライチェーンにおけるリスク点検とこれを踏まえた対応、高性能AIのサイバー攻撃への悪用や量子技術の進展など将来の脅威への備えといった中長期的な課題についても検討

※国家サイバー統括室「サイバーセキュリティ緊急対策パッケージ」より

目次

・2027年3月期　第２四半期　業績説明

・市場環境

・2027年3月期の取り組み

・2027年3月期　業績予想



採用方針

- 採用を強化し着実にエンジニア数も増加しているが、現状ではまだエンジニアの人数がボトルネックとなっている
- 中長期に渡る需要の増加を取り込むため、引き続き新卒・中途ともに採用活動を強化
- 当社及びＦＦＲＩセキュリティワークスの人材採用を併行して実施

採用方針

	新卒採用		中途採用	
	主な施策	求める人物像	主な施策	求める人物像
ＦＦＲＩ セキュリティ	・インターンシップ ・政府主導の人材発掘・育成イベント（セキュリティ・キャンプ、SecHack365など）への講師の派遣 ・有力大学の研究室向けの説明会の開催や共同研究実施 ・優秀な学生との接点を増やす取り組みを継続して実施	・低レイヤー技術に興味関心のある方 ・物事の原理や仕組みを追求することが好きな方	・エージェント紹介 ・リファラル採用 ・大手Sierなどでプロジェクトマネジメントに長年携わってきたシニア人材の採用	・セキュリティ業界での実務経験者のほか、IT関連のプロジェクトマネジメント経験者など
ＦＦＲＩ セキュリティ ワークス		・脆弱性診断に興味関心がある方 ・ベストプラクティスや確立された方法論を理解・活用しながら、顧客の課題解決に主体的に取り組める方		・脆弱性診断、インフラ運用、ソフトウェアテスト、開発などの実務経験者など即戦力人材

FFRI yarai シリーズの販売強化

- 戦略的販売パートナーとの連携強化の他、好調なOEM販売を推進
- 純国産製品の強みを活かして、官公庁・重要インフラ企業、医療法人等への販売施策を進める
- 新たな戦略的販売パートナー獲得による販路拡大を目指す

販売強化の取り組み

「NEC Cyber Secure Package powered by CyIOC」の提供開始

NEC、NECネッツアイ、デジタルアーツと共同開発の国産技術を基盤としたサプライチェーン全体のセキュリティ強化を支援するサービスを提供

新たな販売パートナーの獲得

シー・シー・ダブルよりSOCサービス
「相防サイバー SOC for FFRI yarai」の提供を開始

戦略的販売パートナーとの連携強化

・当社グループ製品の販売を積極的に行う戦略的販売パートナーとの連携を強化、OEM販売含め販売力を強化

純国産製品の強み

・純国産製品の利用に積極的な官公庁、重要インフラ企業、医療法人等への販売施策を進める

機能強化の継続

・FFRI yarai の機能強化を継続
検出エンジンのロジック更新による
検出精度の向上やユーザビリティ向上

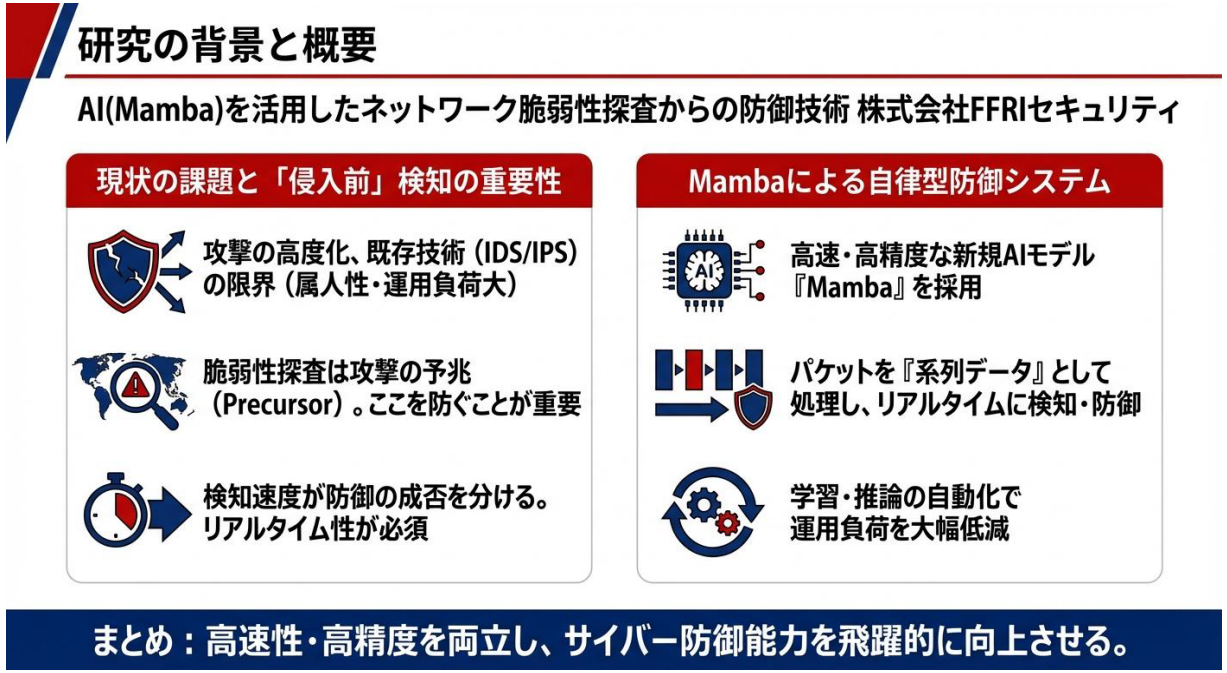
新たな戦略的販売パートナーの獲得

・更なる販売拡大に向けて、新たな販売パートナーの獲得を目指す

AI × サイバー に関する研究開発（一例）

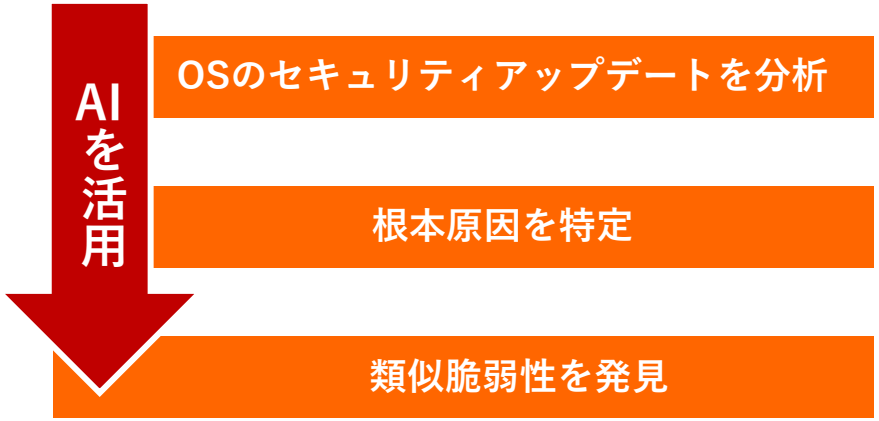
- 「AI × サイバー」の研究開発をKプログラム及び当社独自でも実施
- Kプログラムでは次世代AI「Mamba」を独自に実装し、高速かつ高精度の脆弱性探査の検知・防御技術を開発
- AIを用いて既知の脆弱性を分析、類似の脆弱性を発見する研究などを独自に実施し、既に複数の脆弱性を発見・報告済

Kプログラム



「経済安全保障重要技術育成プログラム／先進的サイバー防御機能・分析能力強化」（JPNP24003）の成果の一部

当社独自の研究開発



OSのセキュリティアップデートを分析し、
脆弱性の根本原因を特定、類似の脆弱性を発見する技術の研究開発を実施
既に複数の脆弱性を発見し、ベンダーにも報告済み

その他の主な取り組み

- 急速に需要が増加しているサイバー安全保障関連案件や、Ｋプログラム、NICTの行う実証事業のサポート等、より一層サイバー安全保障領域への注力を強めていく
- ＦＦＲＩセキュリティ・ワークスはサイバーセキュリティ事業を開始
- N.F.ラボラトリーズにおいては、人材採用と育成を推進し、高度セキュリティ人材の市場への輩出を継続する

経済安全保障重要技術育成プログラム への貢献

・NEDO※1、JST※2の進めるK Programへと参加
当社の持つ研究開発能力を発揮していく

受注先	事業名	研究開発期間	予算規模
CRC ※３	先進的サイバー防御機能・分析能力強化	2024年7月から5か年 ※4	290億円以下
JST	不正機能の意図性評価に関する方法論整理及び 評価ツールの開発	2025年4月から5か年	最大6億円(間接経費含む)

※1　国立研究開発法人新エネルギー・産業技術総合開発機構
※2　国立研究開発法人科学技術振興機構
※3　一般社団法人サイバーリサーチコンソーシアム

NICTの実証事業

・NICT が開発する安全性や透明性の検証が可能なセキュリティソフトを政府端末に導入し、得られたマルウェア情報等を収集・分析する実証事業（2023年11月～）をサポート

・NICTによる政府端末向けセキュリティソフト開発のサポートの実施

ＦＦＲＩセキュリティ・ワークス

・中途人材が加入し、サイバーセキュリティ事業を開始

・引き続き新卒・中途とも採用活動を続ける

N.F.ラボラトリーズ

・需要増加に対応するため人材の採用・育成を継続

・不足が顕著な高度セキュリティ人材の育成と輩出を推進

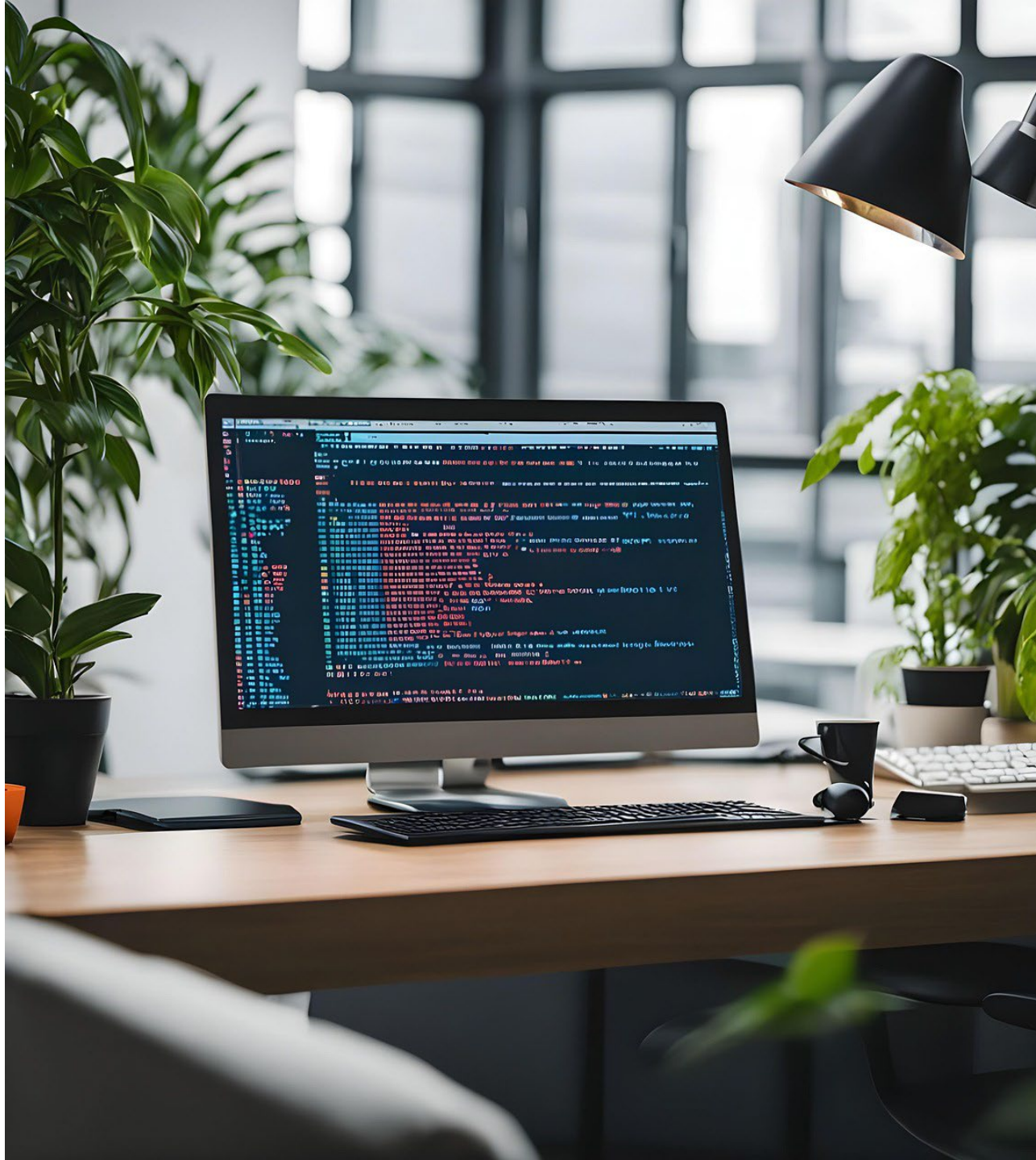
目次

・2027年3月期　第２四半期　業績説明

・市場環境

・2027年3月期の取り組み

・2027年3月期　業績予想



連結業績予想

- ナショナルセキュリティ・サービスの案件増加による増収を見込む
- 2027年3月期もKプログラムにおける利益排除が必要な案件の実施を予定
- ＦＦＲＩセキュリティ及びＦＦＲＩセキュリティワークスにおけるセキュリティ・エンジニアの人員増による人件費の増加や、採用活動の強化による採用コストの増加を見込む

単位：百万円	2026/3(実績)	2027/3(予想)	YoY(%)
売上高	4,348	5,135	18.1
営業利益 (利益率:%)	1,364 (31.4)	1,452 (28.3)	6.5
経常利益 (利益率:%)	1,458 (33.5)	1,509 (29.4)	3.5
親会社株主に帰属する当期純利益 (利益率:%)	1,099 (25.3)	1,133 (22.1)	3.0

連結業績予想（売上高の内訳）

- サイバー安全保障関連の案件増加によるナショナルセキュリティ・サービスの売上高増加を見込む
- ソフトウェア開発・テスト事業は、人員の一部をサイバーセキュリティ事業にアサインした影響により減収の見込み

単位：百万円	2026/3（実績）	2027/3（予想）	YoY（%）
サイバー・セキュリティ事業	3,987	4,796	20.3
セキュリティ製品	1,756	1,767	0.6
ナショナルセキュリティ・サービス	1,576	2,159	37.0
その他セキュリティ・サービス	654	870	32.9
ソフトウェア開発・テスト事業	361	338	△6.2
合計	4,348	5,135	18.1

中期経営計画（2027年３月期～2029年３月期）

- ナショナルセキュリティ・サービスを成長のドライバーとし、増収増益とする計画
- 引き続きセキュリティ・エンジニアを中心に増員を進め、需要を取り込んでいく

修正後計画（2026.5.15公開）

単位：百万円	2027/3（予想）	2028/3（計画）	2029/3（計画）
売上高	5,135	6,069	7,029
営業利益 (利益率:%)	1,452 (28.3)	1,730 (28.5)	1,951 (27.8)
経常利益 (利益率:%)	1,509 (29.4)	1,788 (29.5)	2,009 (28.6)
親会社株主に帰属する当期純利益 (利益率:%)	1,133 (22.1)	1,339 (22.1)	1,492 (21.2)

当初計画（2025.5.14公開）

2027/3（当初計画）	2028/3（当初計画）
5,073	5,966
1,112 (21.9)	1,386 (23.2)
1,163 (22.9)	1,436 (24.1)
843 (16.6)	1,033 (17.3)

株主還元（配当）

- 2027年３月期の配当は、１株当たり18円を予定しております
- 株主の皆様への安定的かつ継続的な利益還元を基本としながら、機動的な株主還元も適宜実施してまいります

	2024年3月期	2025年3月期	2026年3月期	2027年3月期（予想）
親会社株主に帰属する当期純利益	432百万円	687百万円	1,099百万円	1,133百万円
１株当たりの当期純利益	54.64円	86.86	139.06円	143.25円
１株当たりの配当金	10.0円	14.0円	18.0円	18.0円
配当性向（連結）	18.3%	16.1%	12.9%	12.6 %

本資料の取り扱いについて

本資料に含まれる将来の見通しに関する記述等は、現時点における情報に基づき判断したものであり、マクロ経済動向及び市場環境や弊社の関連する業界動向、その他内部・外部要因等により変動する可能性があります。従いまして、実際の業績が本資料に記載されている将来の見通しに関する記述等と異なるリスクや不確実性がありますことを、予めご了承ください。

会社概要

会社名：	株式会社ＦＦＲＩセキュリティ（FFRI Security, Inc.）			
所在地：	東京都千代田区丸の内３丁目３番１号　新東京ビル２階			
役員：	代表取締役社長	鵜飼　裕司	社外取締役（監査等委員）	平山　孝雄
	専務取締役最高技術責任者（兼）yarai事業本部長	金居　良治	社外取締役（監査等委員）	松本　勉
	常務取締役最高財務責任者（兼）経営管理本部長	田中　重樹	社外取締役（監査等委員）	山口　功作
	取締役　ナショナル・セキュリティ事業本部長	松木　隆宏		

設立：　2007年7月3日

資本金：　286,136,500円（2026年3月31日現在）

事業内容：
1. コンピュータセキュリティの研究、コンサルティング、情報提供、教育
2. ネットワークシステムの研究、コンサルティング、情報提供、教育
3. コンピュータソフトウェア及びコンピュータプログラムの企画、開発、検証、販売、リース、保守、管理、運営及びこれらに関する著作権、出版権、特許権、実用新案権、商標権、意匠権等の財産権取得、譲渡、貸与及び管理
4. コンピュータハードウェアの企画、開発、製造、検査、販売、リース、保守、管理及び運営
5. 労働者派遣事業
6. 上記事業に関連する一切の業務

2014年9月30日　東証マザーズ市場に上場（現在はグロース市場）

代表紹介



株式会社ＦＦＲＩセキュリティ
代表取締役社長
**　鵜飼　裕司　（Ukai Yuji）**

1973年徳島県生まれ。博士（工学）。
北米のセキュリティベンチャー eEye Digital Security社にてセキュリティエンジニアとして活躍。
Windowsなど著名なソフトウエアのセキュリティホールを100件以上発見するなど、世界的に知られるセキュリティ技術者として活躍。その後、日本に戻り2007年に株式会社フォティーンフォティ技術研究所（現株式会社ＦＦＲＩセキュリティ）を創業。
日本国内の情報セキュリティカンファレンス「CODE BLUE」の審査員や世界最大の情報セキュリティカンファレンス「Black Hat」で審査員を務める、世界的に知られるセキュリティの有識者でもある。

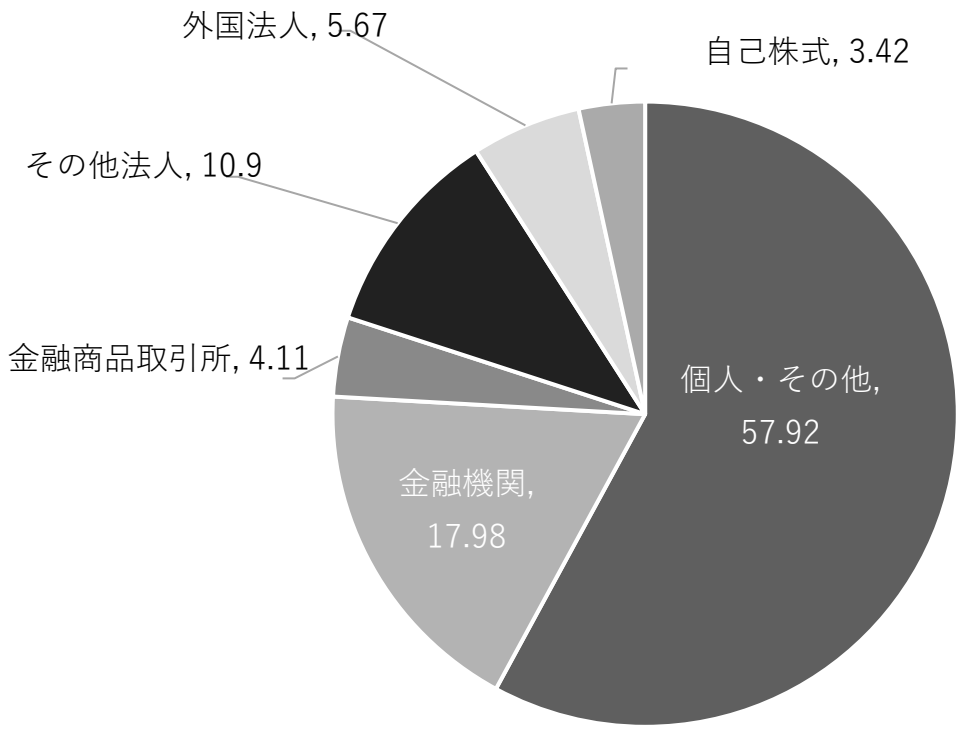
その他の社会における活動（抜粋）

2007年　独立行政法人情報処理推進機構（IPA）　研究員（非常勤）就任
2010年　国立大学法人　徳島大学　講師（非常勤）　就任
2012年　BlackHat Conference（米国）のContent Review Board Member 就任
2013年　CODE BLUE（東京）の委員 兼 レビューボード就任
2013年　内閣官房「高度情報通信ネットワーク社会推進戦略本部
　　情報セキュリティ政策会議普及啓発・人材育成専門委員会」委員就任
2015年　経済産業省「セキュリティ人材確保に関する研究会」委員就任
2016年　一般財団法人日本情報経済社会推進協会（JIPDEC）「IoTセキュリティWG」構成員就任
2017年　総務省「サイバーセキュリティタスクフォース」構成員就任
2017年　総務省「サイバーセキュリティタスクフォース 情報開示分科会」構成員就任
2018年　内閣官房「内閣サイバーセキュリティセンター本部研究開発戦略専門調査会」委員就任
2018年　経済産業省「産業サイバーセキュリティ研究会WG3」委員就任
2018年　JNSA「サイバーセキュリティ事業における適正な事業遂行の在り方に関する検討委員会」委員
2021年　経済産業省「情報サービス産業の管理体制強化に向けたセキュリティ技術検討委員会」委員
2024年　経済産業省「産業界のセキュリティ対策強化とセキュリティ産業の振興の好循環（仮題）」
　　に向けての検討会　委員

株式の状況 (2026.9.30)

発行済株式数	8,190,000 株
株主数	16,066 名

株主構成



大株主（上位10名）	持株数(株)	持株比率(%)
鵜飼　裕司	1,622,000	20.51
金居　良治	1,441,600	18.23
ＧＭＯインターネットグループ株式会社	750,800	9.49
日本マスタートラスト信託銀行株式会社（信託口）	237,900	3.01
THE BANK OF NEW YORK, TREATY JASDEC ACCOUNT	208,181	2.63
楽天証券株式会社共有口	179,700	2.27
田中　重樹	140,000	1.77
BNY GCM CLIENT ACCOUNT JPRD AC ISG (FE-AC)	83,190	1.05
モルガン・スタンレーＭＵＦＧ証券株式会社	55,682	0.70
源利株式会社	52,500	0.66
合計	4,771,553	60.33

※１．当社は自己株式を280,495株保有しておりますが、上記大株主からは除外しております。
２．持株比率は自己株式を控除して計算しております。
３．上記鵜飼裕司氏の所有株式数には、令和３年３月16日付で締結した管理信託契約に伴い株式会社SMBC信託銀行が保有している株式数（600,000株）を含めて表記しております。
４．上記金居良治氏の所有株式数には、令和４年６月30日付で締結した管理信託契約に伴い株式会社SMBC信託銀行が保有している株式数（600,000株）を含めて表記しております。