事業計画及び成長可能性に関する事項

株式会社ＦＦＲＩセキュリティ

東証グロース：3692

2025年6月

目次

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	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	田中　重樹		社外取締役（監査等委員）	山口　功作
	取締役　事業開発本部長	川原　一郎		社外取締役（監査等委員）	中山　泰秀
	取締役　技術本部長	梅橋　一充			

設立：　2007年7月3日

資本金：　286,136,500円（2025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）

設立の経緯

ＦＦＲＩセキュリティ設立以前

- セキュリティ対策技術を**海外輸入に依存**
- 日本を狙った**サイバー脅威の拡大**
- 自国で問題解決できない
- 国内に**研究開発企業が不在**

未知の脅威拡大

国産の対策技術が必要

ＦＦＲＩセキュリティ設立

コア技術の研究開発能力や、広範なリサーチ能力を発揮し、サイバー安全保障を支える

日本発

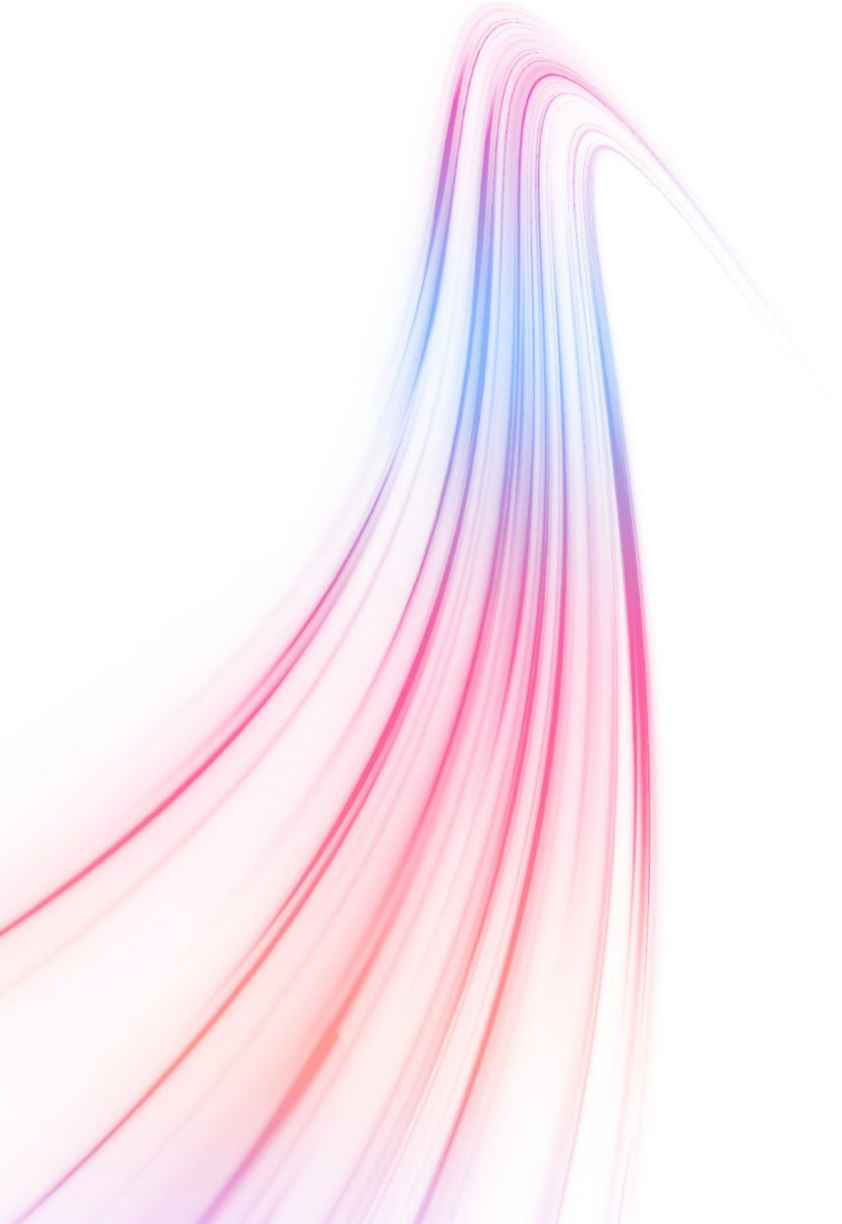
純国産

高い技術力

関係会社

株式会社シャインテック
株式会社エヌ・エフ・ラボラトリーズ

社名とコーポレートマークに込めた思い



「ＦＦＲＩ」は、「Fourteenforty Research Institute」の略称です。

「１４４０」は、スノーボード・ハーフパイプ競技における
ジャンプの回転数に由来しています。

設立当時、４回転ジャンプできる競技者が存在せず、
前人未到の領域への挑戦を志し、
「１４４０（360° ×４回転）」を社名に採用しました。

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。

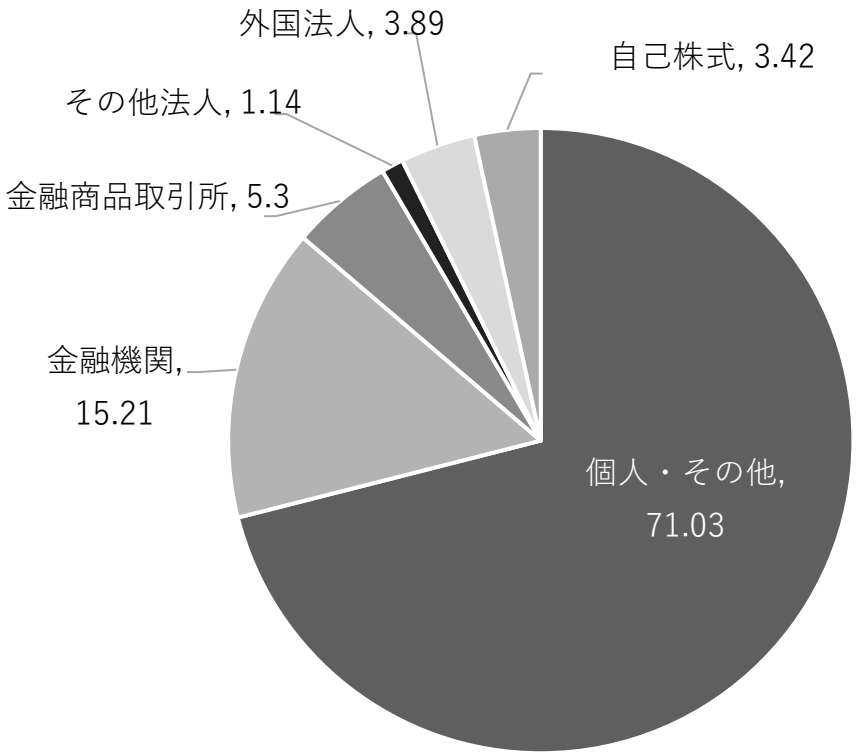
その他の社会における活動（抜粋）

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 (2025.3.31)

発行済株式数	8,190,000 株
株主数	10,985 株

株主構成



大株主（上位10名）	持株数(株)	持株比率(%)
鵜飼　裕司	1,942,000	24.55
金居　良治	1,441,600	18.23
田中　重樹	170,000	2.15
株式会社ＳＢＩ証券	127,800	1.62
楽天証券株式会社	125,000	1.58
ＪＰモルガン証券株式会社	65,094	0.82
BOFAS INC SEGREGATION ACCOUNT	58,900	0.74
永田　哲也	53,000	0.67
石山　智祥	47,000	0.59
BNYM SA/NV FOR BNYM FOR BNYM GCM CLIENT ACCTS M ILM FE	37,990	0.48
合計	4,068,384	49.68

※1．当社は自己株式を280,378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。

ＦＦＲＩセキュリティが果たすべき役割

日本発

純国産

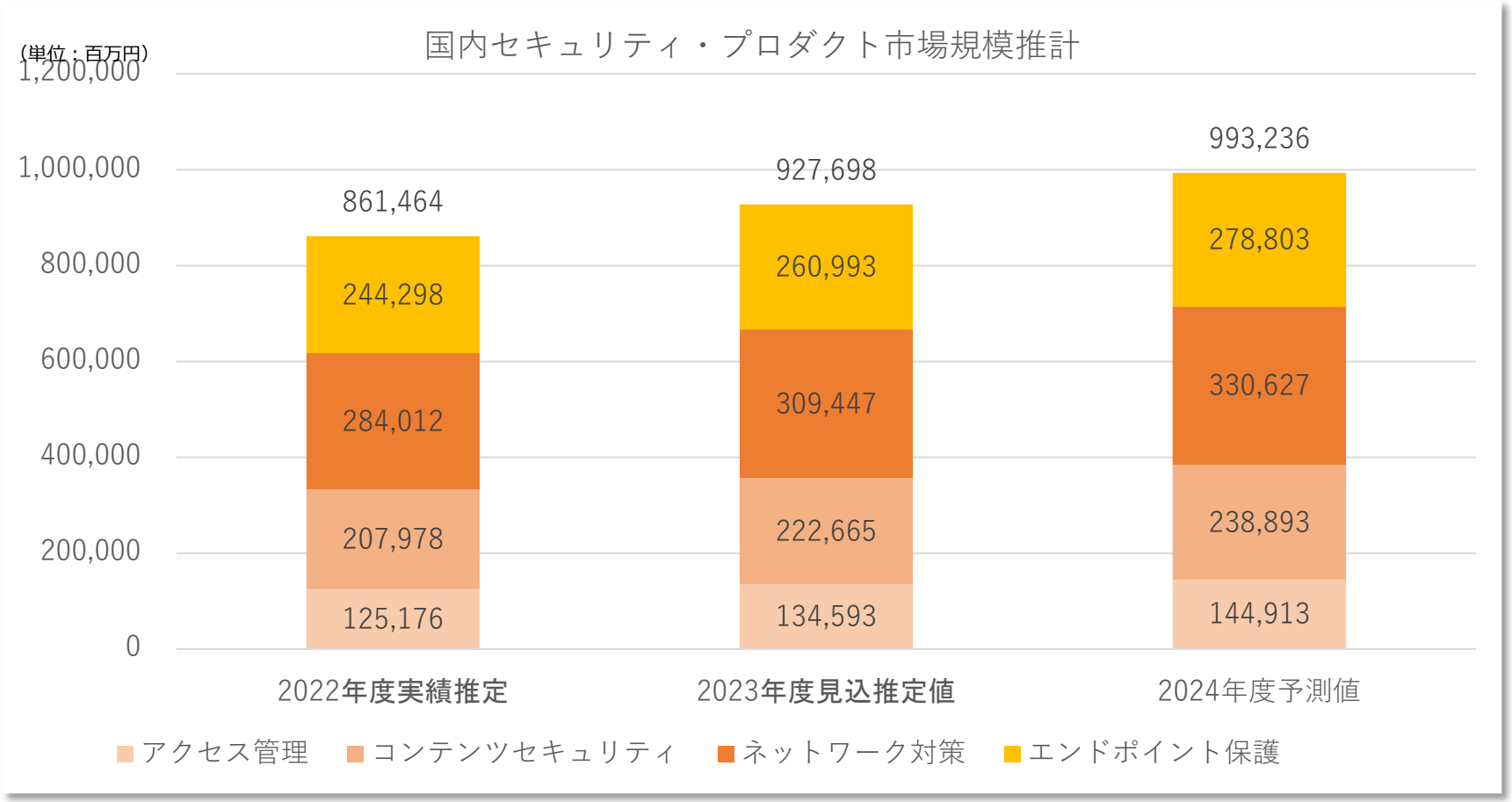
高い技術力

創立以来培い磨き上げてきた高い技術力で、
日本のサイバー領域における安全保障を実現する

目次

セキュリティ・プロダクト市場

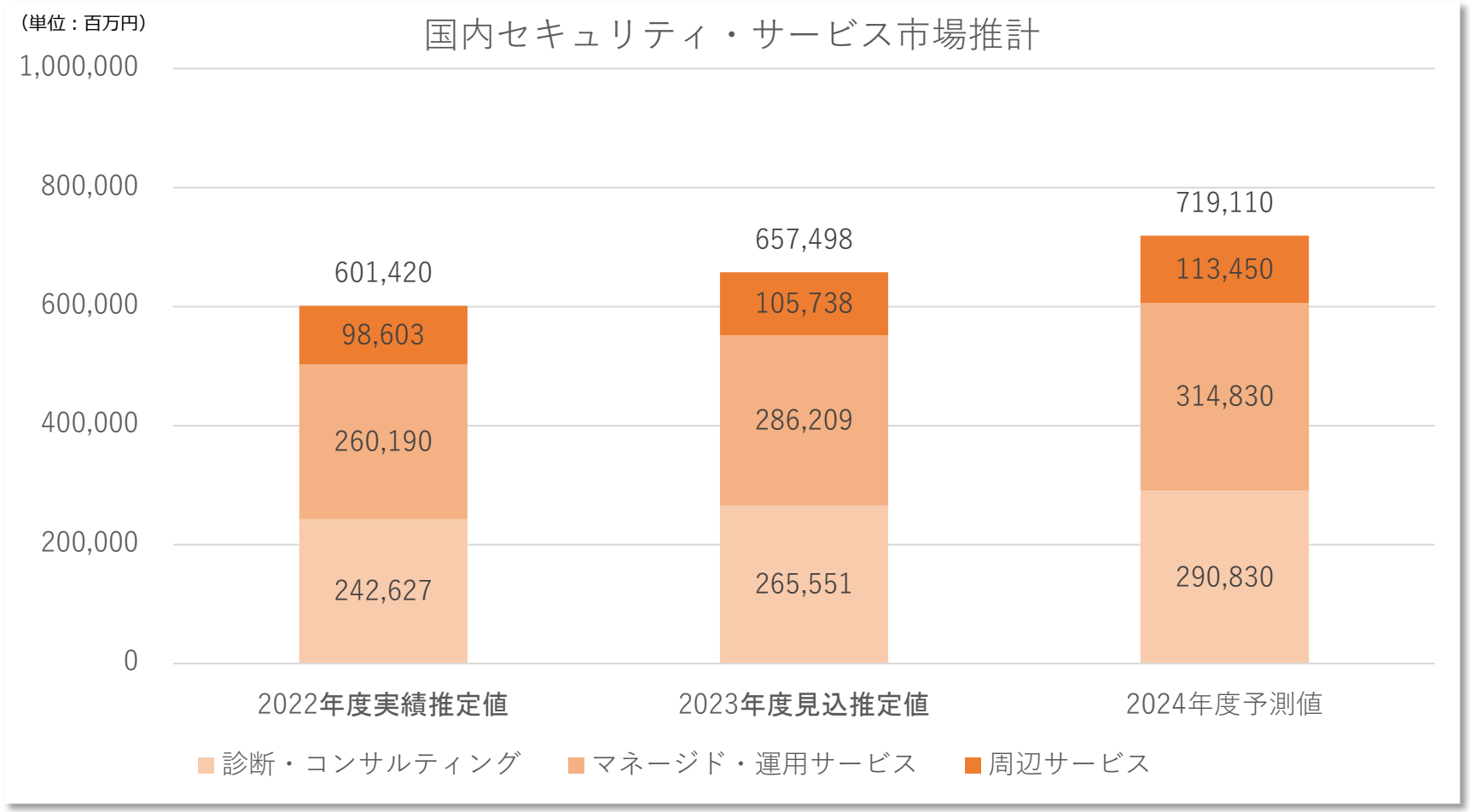
- 当社製品 FFRI yarai はエンドポイント保護製品に分類
- 国内市場はサイバー攻撃による被害の増加や、テレワークやDXの推進を受けて年々拡大している



参考：JNSA調査研究部会　「国内情報セキュリティ市場　2023年度調査報告」より

セキュリティ・サービス市場

- 当社セキュリティ・サービスは、診断・分析、教育、インテリジェンス提供など多岐に渡る
- 高度化するサイバー攻撃への対策や、専門人材の慢性的な不足から、市場全体で拡大傾向が続く



参考：JNSA調査研究部会　「国内情報セキュリティ市場　2023年度調査報告」より

サイバー安全保障領域の現状

- 国家の関与が疑われる組織化・洗練化されたサイバー攻撃の脅威が拡大している
- エネルギー関連企業や医療機関、金融機関といった重要インフラを狙ったサイバー攻撃が増加しており、サイバー攻撃が国家安全保障に与える影響が顕在化している

国家間の競争の場となったサイバー空間

国家が関与するサイバー攻撃集団

豊富な資金と人材で
継続的かつ執拗な攻撃をしかける

国家関与が疑われる
サイバー活動の目的

中　国：	軍事・先端技術の情報窃取
ロシア：	軍事・政治的目的
北朝鮮：	政治的目的・外貨獲得

※サイバーセキュリティ戦略／NISC より

サイバー攻撃が安全保障に与える影響の顕在化

組織的で洗練された
サイバー攻撃

機密情報・先端技術情報
金銭などの窃取
サービス妨害 等

狙われる重要組織

政府・関連組織	情報窃取・政治的干渉 (偽情報・選挙妨害) 等
防衛関連組織/施設	機密情報の窃取・破壊 サービス妨害 等
インフラ企業/施設	情報窃取 . 破壊 . 金銭要求 サービス妨害 等

国内市場の課題

- 欧米主要国では、サイバー安全保障に関する問題解決を自国で行うために、国内産業の育成や国産技術の研究開発が行われている
- **我が国では、国内でサイバーセキュリティの研究開発を行う有力なベンダーはほぼ当社のみ**

サイバーセキュリティ自給率の低迷

海外技術に過度に依存

国内企業のほとんどは技術を輸入に頼っており、研究開発能力を持っていない

自国の問題を自国で解決できない

重要インフラを標的としたサイバー攻撃など、緊急性の高い事案でも、海外ベンダーの対策技術開発を待たねばならない

データ負けのスパイラル

国内に情報がない

海外製品で検知されたサイバー攻撃の情報は開発元である海外企業の元に集約されており、国内に情報が存在しない

研究開発ができない

国内に利用可能なデータがないので研究開発ができず、国内で技術が生まれない。
そのため技術を輸入に頼らざる負えない
負のループが続く

セキュリティ人材の不足

高度セキュリティ人材

サイバーセキュリティの研究開発を行う企業がほとんど無い事から、高度専門人材は一握り

人材不足

企業のセキュリティ担当など、一般的なセキュリティ人材も含め、セキュリティ人材は11万人以上不足しているとみられる

※2023 ISC2 Cybersecurity Workforce Study より

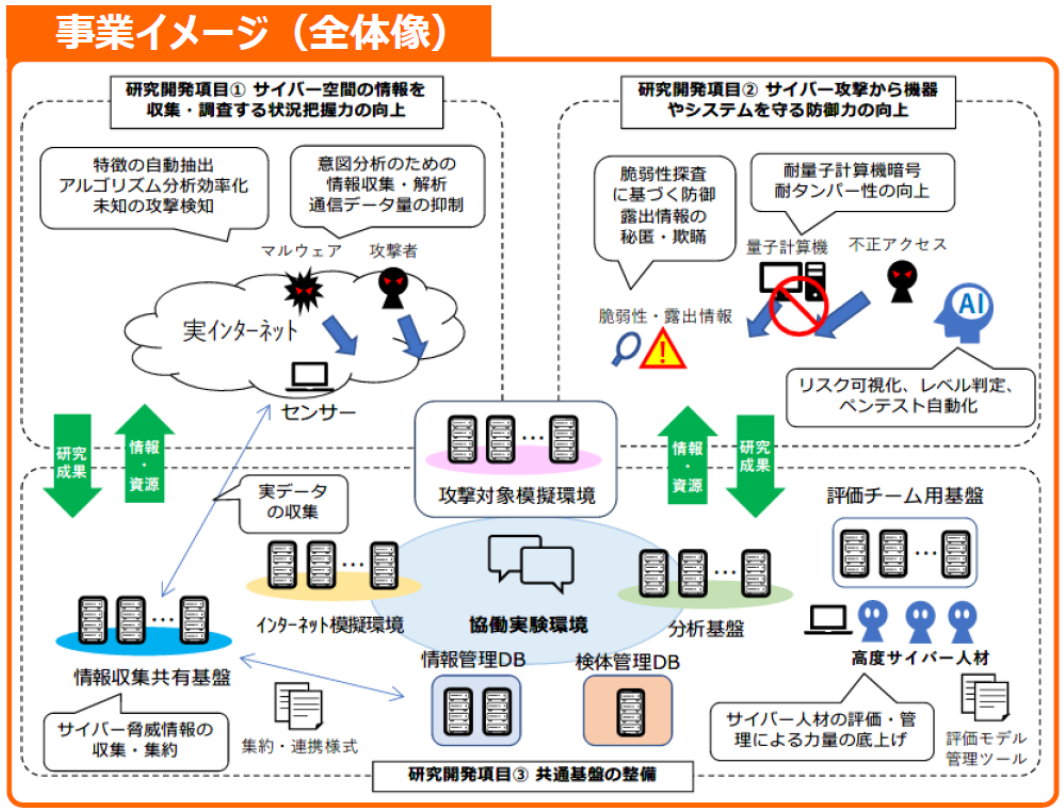
我が国における政府の取り組み

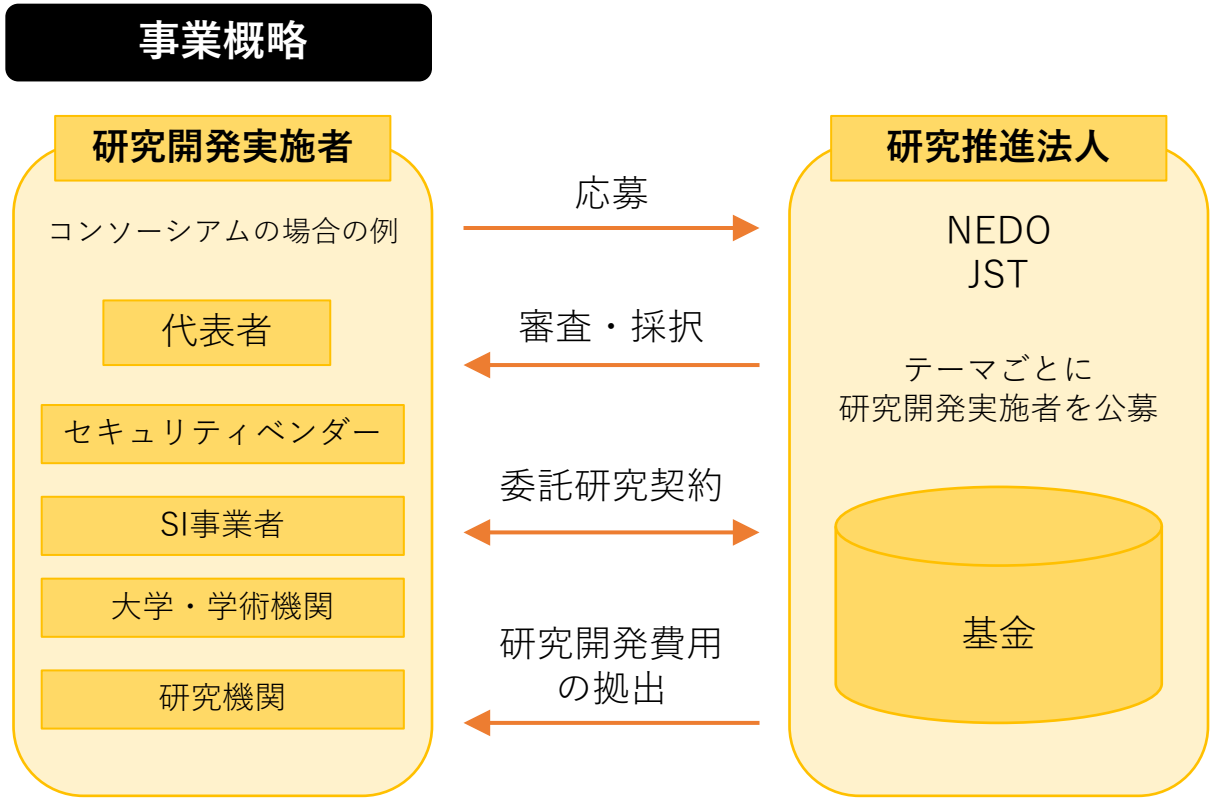
- 国内産業の育成や、国産技術の開発、能動的サイバー防御の実現などに向けた施策が進められている

2022年５月	経済安全保障推進法 制定
▼	
2022年12月	防衛３文書の制定
▼	「国家安全保障戦略」「国家防衛戦略」「防衛力整備計画」の制定
2023年３月	**①経済安全保障重要技術育成プログラム 開始**
▼	サイバーセキュリティを含む先端技術領域における国産技術の研究開発促進
2024年５月	セキュリティ・クリアランス法 施行
▼	
2025年３月	**②サイバーセキュリティ産業振興戦略 公開**
▼	国内サイバーセキュリティ産業の育成及び人材育成を支援する政策パッケージ
2025年５月	**③能動的サイバー防御法 成立**
	重大なサイバー攻撃のおそれがある場合、これを未然に排除、被害の拡大防止を目的とする

①経済安全保障重要技術育成プログラム

- 経済安全保障推進法に基づき、我が国の安全保障にとって重要な技術に係る研究開発に対し、政府がその資金を拠出する。研究を推進するのは、新エネルギー・産業技術総合開発機構（NEDO）及び科学技術振興機構（JST）
- 支援対象の研究テーマごとに研究開発実施者の公募が行われ、審査を経て採択。実施者はNEDOまたはJSTと契約を締結し、研究開発費用について基金から拠出を受ける仕組み





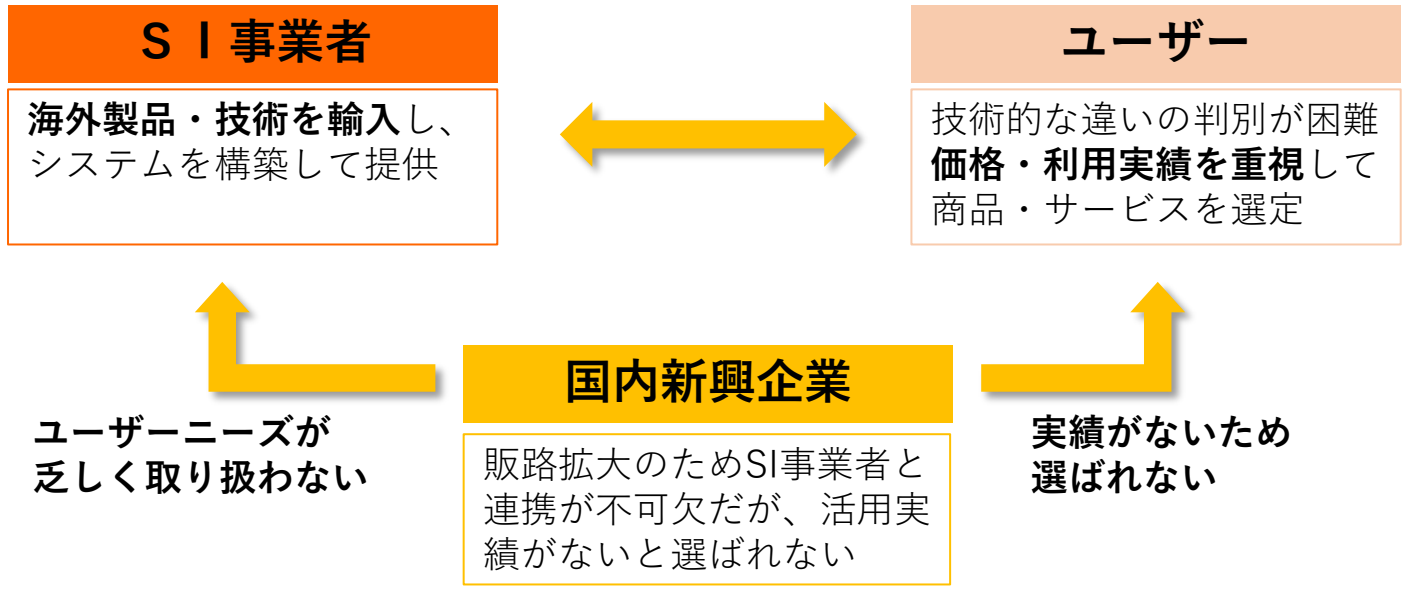
※経済安全保障重要技術育成プログラムの概要/国土交通省 参考

②サイバーセキュリティ産業振興戦略　国内産業の現状と問題点

- サイバーセキュリティ産業・技術基盤を強化するための包括的な政策パッケージ「サイバーセキュリティ産業振興戦略」が経済産業省より公表された
- 国内サイバーセキュリティ産業は、利用実績を重要視する商習慣から**新規参入のハードルが高く、海外製品に強く依存している**。そのため、リスクのある研究開発に投資する企業数は少ない。

経済産業省：サイバーセキュリティ産業振興戦略　より抜粋

国内産業の現状



問題点

・買い手がつかないリスクから、研究開発への投資がされない

・製品を開発するトップ人材が育たない（国内産業が成長する下地がない）

・成長率の大きい分野のシェアを外資系企業に奪われている

・海外製品への依存から抜け出せない（**デジタル赤字の拡大**）

参考：サイバーセキュリティ産業振興戦略

②サイバーセキュリティ産業振興戦略　今後の方針

- 製品開発の出口を確保しつつ、製品ベンダーの競争力を強化し、優れた国産製品・サービスが市場に受け入れられる絵姿を作っていく
- ＫＰＩとして10年以内に**国内企業の売上高を足元から３倍増（約0.9兆円⇒約３兆円超）を目指し**、政策を進める

経済産業省：サイバーセキュリティ産業振興戦略　より抜粋

目指すべき方向性

国産製品・サービスが活用されるための環境整備

・政府機関が調達を通じて有望な製品・サービスの実績作り
・有力スタートアップの公表や、有望製品・サービス・企業の審査・表彰を行う
・製品・サービスの信頼性を確認する制度の構築・運用を進める

優れた国産製品・サービス創出

・NICT CYNEX 等を通じたデータの提供や、専門人材の派遣など環境整備を行う
・Kプログラムを通じて、技術開発・社会実装を推進する

産業全体を支える基盤の強化

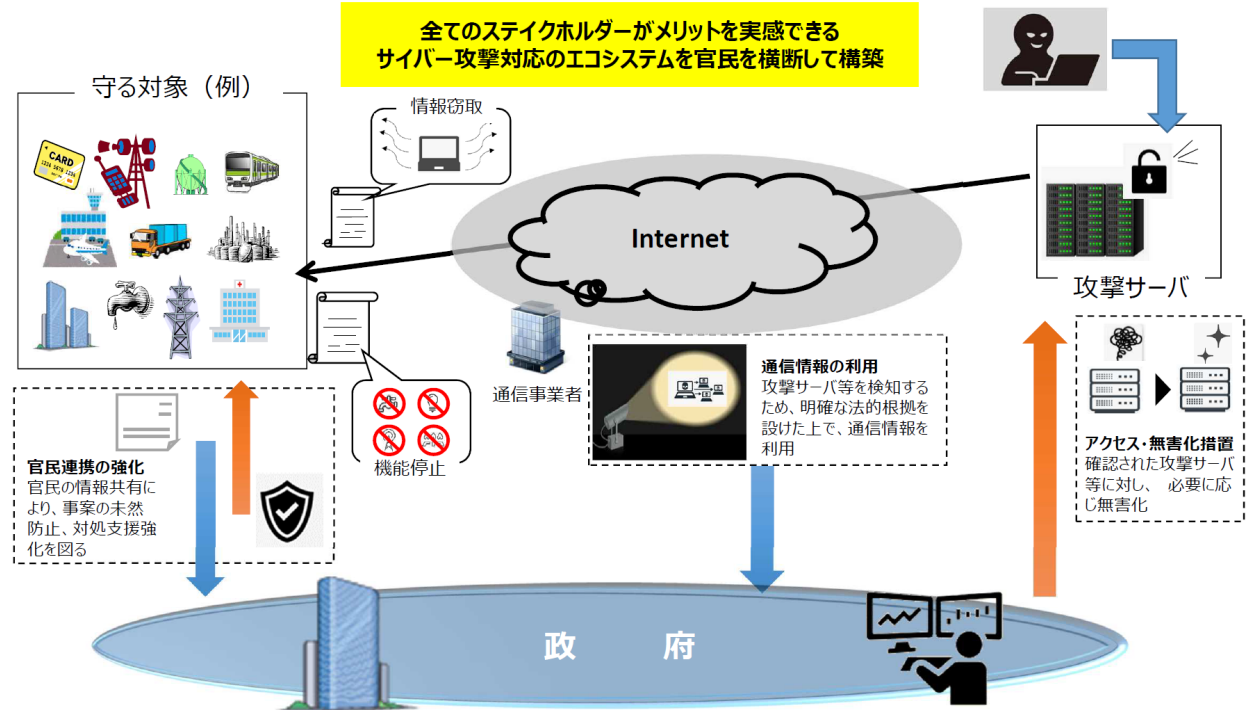
・人材育成プログラムの拡大
・産官学が連携して人材育成する枠組みを検討
・国際的な競争力を強化するよう各国とも連携

ロードマップ

初年度	予算編成など取組の具体化、 継続的なフォローアップ
３年以内	スタートアップ数、 高度セキュリティ人材の増加、
５年以内	先端技術の社会実装、 国産製品のシェア拡大
10年以内	安全保障の確保、デジタル赤字解消 KPI：国内企業の売上高３倍増 （約0.9兆円→約3兆円）

③能動的サイバー防御法案

- セキュリティ・クリアランス制度や、NISCの後継となる司令塔組織の編成など、サイバー安全保障関連の法及び制度整備が進んだほか、足元では能動的サイバー防御の法案も国会を通過し、運用開始に向けた議論が重ねられている
- 「国家安全保障戦略」で示された「**サイバー防衛能力を欧米主要国と同等以上に強化する**」という方針に基づき、サイバー対処能力の向上に向けた取り組みが進む



内閣官房：サイバー安全保障分野での対応能力の向上に向けた提言 より
能動的なサイバー防御の全体イメージ

具体的な方向性

- **官民連携の強化**
  官のみ・民のみでのサイバーセキュリティ確保は困難
  官民双方向の情報共有を促進
- **通信情報の利用**
  重大なサイバー攻撃対策のため、一定の条件下での通信情報の利用を検討
- **アクセス・無害化**
  サイバー攻撃の特徴（①危険の認知の困難性、②意図次第でいつでも攻撃可能、③被害の瞬時拡散性）を踏まえ、被害防止を目的としたアクセス・無害化を行う

目次

事業モデル：サイバーセキュリティ事業／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は、研究開発活動を事業の源泉**とし、自社開発の技術を使った製品・サービスを提供している
- ソフトウェア開発・テスト事業は、子会社のシャインテックにて品質保証業務などを提供

事業セグメント	販売区分	事業内容	主な顧客
サイバー・セキュリティ事業（研究開発による新技術の創出）	セキュリティ製品	**FFRI yarai シリーズなどセキュリティ製品の提供** 法人向けには販売パートナー経由で自社製品やOEM販売を行っており、個人向けには上記の他に直販も行っている	官公庁・法人 個人など
	ナショナルセキュリティ・サービス	**安全保障関連のセキュリティ・サービスの提供** サイバー安全保障に関連した政府のプロジェクトに参加するなど、セキュリティ調査・研究・分析・開発・教育などを請け負い提供している	防衛省・官公庁 防衛産業企業など
	その他セキュリティ・サービス	**安全保障以外のセキュリティ・サービスの提供** 官公庁や一般企業に対して、セキュリティ調査・研究・分析・開発・教育の他、運用などのサービスを提供している	官公庁・法人など
ソフトウェア開発・テスト事業		**ソフトウェアの設計・開発・評価・解析などの提供**	法人

セキュリティ・サービスについて

- サイバーセキュリティの研究開発能力を持つ当社の競争優位性を活かしたサービスを提供
- 日本発のサイバーセキュリティ企業として安全保障関連の案件に注力

サイバーセキュリティの課題を革新的な技術で乗り越える

国内ではほぼ当社のみ

他ベンダーでは技術を輸入しているか、研究開発の拠点が海外にある場合がほとんど。**当社は国内でサイバーセキュリティの研究開発を行っている日本発の企業**で、純国産の技術の研究開発・提供を行っている。

高度な技術力と研究開発能力

事業の源泉はサイバーセキュリティ技術の研究開発。
創業以来磨き上げられたリサーチ能力や高度な技術力を活かし、既存の技術では乗り越えられない課題も技術で乗り越えていく

サイバー安全保障に注力

需要が急増している安全保障の領域では、海外企業の参入は困難であり、広範な研究開発能力を持ち、かつ**日本発の企業である当社にしかできないサイバー安全保障の案件に注力**している。

多様な提供形態

顧客それぞれの課題に寄り添い、自社開発技術やリサーチ能力を基にセキュリティ調査・分析・研究・開発・教育などのサービスをオーダーメイドで提供。

セキュリティ・サービスの主なメニュー

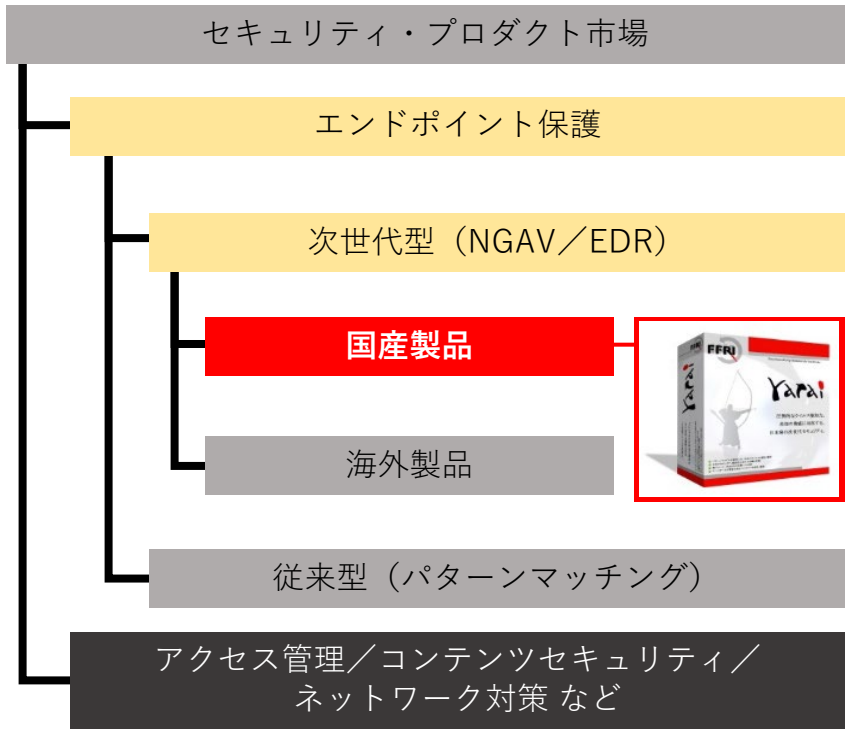
- 特定のプロジェクト等のための調査・分析・研究・開発など顧客の要望に合わせた請負契約型の他に、技術力や研究開発力をベースとした各種サービスを提供

主なメニュー	内容
高度セキュリティ技術者トレーニング（Expert Seminar)	コンピュータ・システムのセキュリティ堅牢性調査と、実際にサイバー攻撃を受けた場合の影響調査などユーザーのニーズに応じたサービスを行います。
Prime Analysis	組織が抱える0-day脆弱性、標的型攻撃といった課題の解決を支援する包括的リサーチサービスです。
サイバーセキュリティ国際動向調査	海外公的機関や大企業に対するサイバー攻撃の調査や、日本の行政や企業・団体へのサイバー攻撃の特徴や予兆などの調査し、サイバーインテリジェンス情報の収集と分析を行います。
先端技術領域セキュリティ分析	IoT機器や組込みシステムをはじめ、AIシステムや5Gネットワークに対して脅威分析を実施し、潜在する脅威を洗い出すことで、対策方法や改善案などを提案します。

セキュリティ・プロダクトについて

- 主なプロダクトは 次世代エンドポイントセキュリティ FFRI yarai
- 現在主流となっているNGAV/EDR製品の中で、**ほぼ唯一の純国産製品**
- 自社開発の５つの検出エンジンを搭載したふるまい検知型マルウェア対策製品で、主要な検知実績を公開している

FFRI yarai の市場



５つの検出エンジン

自社開発の５つの検出エンジンが多角的にプログラムを監視し、未知・既知問わず高精度でマルウェアを検出します。

ZDPエンジン	OS・アプリケーションのセキュリティ脆弱性を狙った攻撃を検出 0-day脆弱性にも対応
Static分析エンジン	ファイルの内部構造をスキャンし、実行前にマルウェアか否かを判定
Sandboxエンジン	保護された領域内でプログラムを動作させ、悪意ある動作を検出
HIPSエンジン	不審なプロセスの一挙一動を監視。動き出したマルウェアも瞬時に検出
機械学習エンジン	大量のマルウェアや正常なファイルからなるビッグデータを、 機械学習を用いて自動的に解析し、得られた特徴からマルウェアを検出

主要なセキュリティ・プロダクト

- FFRI yarai の他、個人・小規模事業者向け製品や、マルウェア解析などの専門的な機能を搭載した FFRI yarai analyzer Professional などを提供している

名称	内容
FFRI yarai	自社開発の完全ヒューリスティック検知技術による、 純国産の標的型攻撃マルウェア対策製品 パターンファイルに依存せず、未知・既知のマルウェア及び セキュリティ脆弱性を狙った攻撃を防御します。
FFRI yarai Home and Business Edition	FFRI yaraiをベースに個人向けにチューニングしたセキュリティソフトで、 パターンマッチング技術を使用する一般的なウイルス対策ソフトでは 対応することが難しい未知の脅威に対しても効果を発揮します。
FFRI yarai analyzer Professional	プログラムや文書ファイル、各種データファイルを自動的に解析し、 マルウェア混入のリスク判定が可能なレポートを出力することで、 セキュリティ担当者のマルウェア解析をサポートします。

FFRI yarai の防御実績（一部抜粋）

FFRI yaraiが検出したマルウェアのうち、著名なもので公開可能なものを随時公開。
被害発生以前にリリースされたバージョンでマルウェアを検出できることを確認している。

発生・ 報道時期	防御エンジン リリース時期	当時の未知脅威及び標的型攻撃
2022年11月	2021年10月	マルウェア「Emotet」(2022年11月版)
2021年3月	2019年1月	ファイルレスマルウェア「AlumniLocker」
2020年11月	2018年2月	マルウェア「IcedID」
2018年7月	2018年3月	マルウェア「Emotet」
2018年4月	2017年6月	ランサムウェア「GandCrab」
2017年12月	2017年5月	仮想通貨採掘マルウェア「CoinMiner」
2017年5月	2016年10月	ランサムウェア「WannaCry/WannaCrypt」
2015年6月	2014年8月	日本年金機構を狙うマルウェア「Emdivi」

目次

サイバー安全保障へ注力

- 政府の施策によって**サイバー安全保障に関する需要は中長期に渡って増加する見込み**
- 国産技術の必要性が高まっているが、**国内でセキュリティコア技術の研究開発を行う有力なベンダーはほぼ当社のみ**
- 創立以来磨き上げてきた高い技術力で、**日本のサイバー領域における安全保障を実現する**

サイバー安全保障の領域へと注力し、成長のドライバーとする

日本発 純国産	研究開発能力	安全保障領域 の豊富な実績
強みが最も発揮される 安全保障領域に注力	高度な技術と 広範なリサーチ能力	創業以来培ってきた 実績と信頼

採用力の強化

- サイバー安全保障の需要増加は著しく、**キャパシティボトルネックとなっている**
- 今後も安定的にサイバー安全保障の需要を取り込み、我が国におけるサイバー安全保障をリードするため、人材採用を強化

新卒採用市場

セキュリティに関する知見の有無に関わらず、
コンピューターサイエンス能力や研究開発への適正などを評価

国内人材市場

セキュリティ人材

〔11万人不足〕

※2023 ISC2 Cybersecurity Workforce Study より

人材の取り合い

セキュリティ企業

監視・開発人材など

大手・外資系企業

社内運用人材など

コンサルタント企業

提案人材など

ＦＦＲＩセキュリティ

新卒採用と育成

セキュリティエンジニアは新卒採用を中心に採用強化
優秀な学生との接点を増やす取り組みを継続

- 大学研究室との連携
- インターンシップ
- 人材育成イベントへの参加・協力

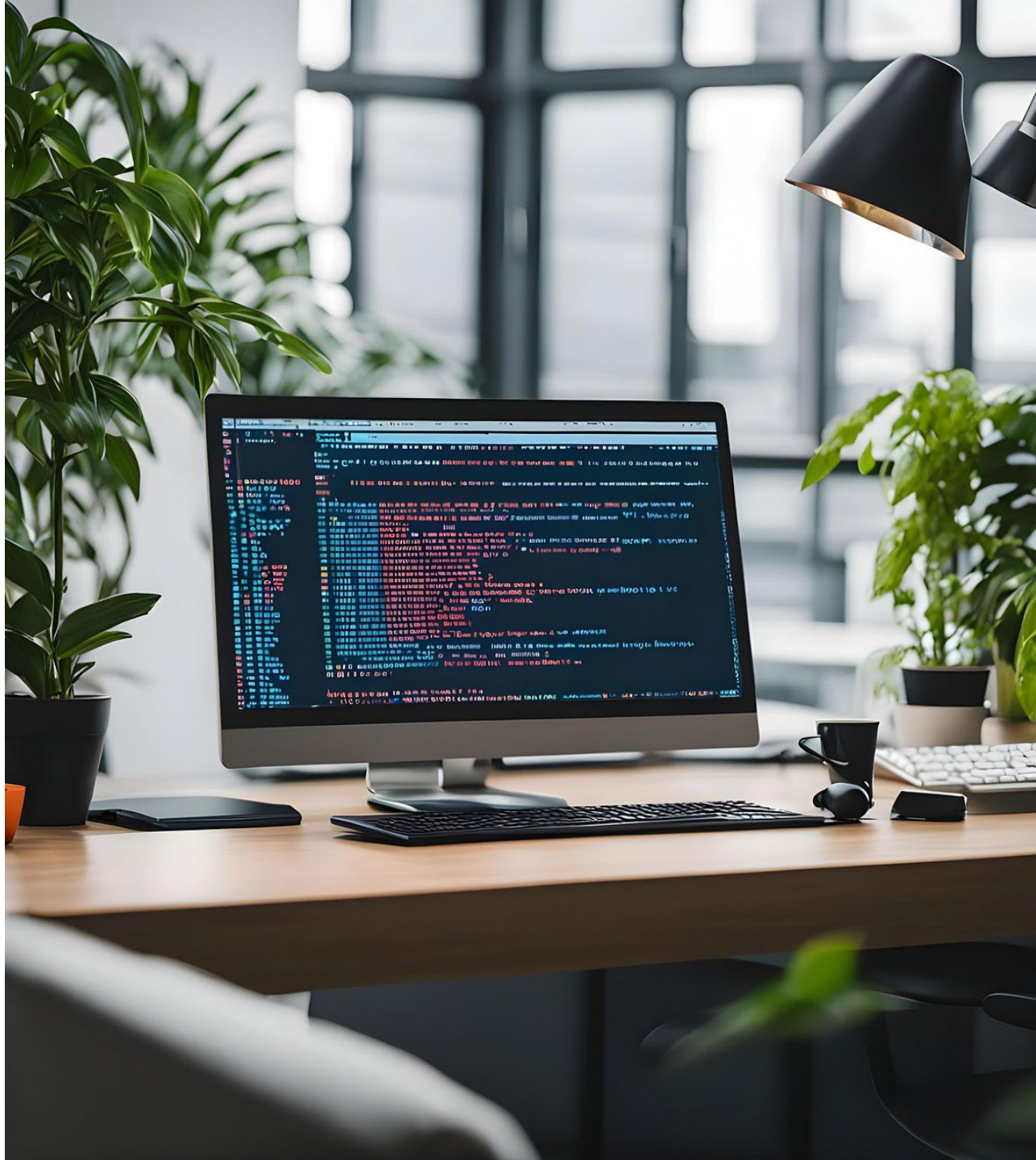
プロジェクトリーダー・マネジメント層

マネジメント層は国内の人材不足が特に顕著
採用と並行して社内での育成を進める

マネジメント人材

マネジメント能力
問題解決力・リーダーシップ
コミュニケーション能力など

目次



業務遂行上の重要なリスクと対応方針

- 以下は、成長の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する主要なリスクです。
- 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。

重要なリスク	リスク対応の方針
製品及びサービスに瑕疵が発生する可能性について **発生可能性：小　　発生する可能性のある時期：特定時期なし** 製品及びサービスを提供する際には、開発過程においてプログラムにバグや欠陥の有無の検査、ユーザーの使用環境を想定した動作確認などの品質チェックを行い、販売後のトラブルを未然に防ぐ体制をとっております。しかしながら、プログラムの特性上、これらを完全に保証することは難しいものとなっております。 万が一、製品又はサービスにバグや欠陥が発見された場合の対策として、当社ではプログラムの修正対応や、販売時の契約において免責条項の設定などにより損失を限定する体制をとっておりますが、これらの対策はリスクを完全に回避するものではなく、バグや欠陥の種類、発生の状況によっては補償費用が膨らみ、当社の業績に影響を及ぼす可能性があります。	製品及びサービスの提供にあたっては、事前に適切なテスト等の品質チェックを行うほか、万一販売後のトラブルが発生した際は早急な情報共有と対処を行う体制を敷き、被害を最小限に抑制する体制整備を行っております。
サイバー攻撃等を受けることにより信頼性を喪失する可能性について **発生可能性：小　　発生する可能性のある時期：特定時期なし** サイバー・セキュリティ事業を営む当社は、当社及び当社製品又はサービスを導入されたユーザーにおいて、当社製品又はサービスの効果の及ぶ範囲内でサイバー攻撃等による機密情報等の改鼠・搾取等をされた場合、当社の技術力を否定されることにより、結果として当社製品又はサービスに対する信頼性を喪失する恐れがあります。このようなことが発生した場合、信頼を回復するまでの間、製品及びサービスの販売が停滞することが考えられ、当社の業績に影響を与える可能性があります。	製品・サービスにおいては適宜最新の研究開発の成果を反映し、サイバー攻撃による被害を防ぐ他、情報管理規程の整備、インフラのセキュリティ強化、 社内情報システムへの外部からの侵入防止対策を講じるなど、管理の強化・徹底に努めております。

業務遂行上の重要なリスクと対応方針

- 以下は、成長の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する主要なリスクです。
- 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。

重要なリスク	リスク対応の方針
技術革新又は陳腐化に対応できない可能性について **発生可能性：小　　発生する可能性のある時期：特定時期なし** 当社グループが属するサイバー・セキュリティの分野は、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、ニーズが変化しやすい特徴があります。このような中、当社グループは継続的な研究開発活動による新技術の開発を行っている他、高度なリサーチ能力を持つ日本発のサイバー・セキュリティ企業である当社の強みを発揮できるナショナルセキュリティに注力することで差別化を図り、競争力の維持向上に努めております。 しかし、当社グループが環境変化に対応することができず、当社製品及びサービスの陳腐化又は競合他社の企業努力などの要因により、当社グループが競争力を維持することができない場合、当社グループの業績に影響を与える可能性があります。	当社グループでは、基礎技術研究部にて注目すべき技術革新や技術トレンドを見極めながら、新技術の研究開発を進めており、そこで得た知見を製品・サービスに反映し、競争力の向上を図っております。また、複数の販売パートナーへ当社製品をOEM提供することにより、付加価値の異なる製品を市場に提供することにより、他社製品との差別化を図っております。
事業環境の変化について **発生可能性：小　　発生する可能性のある時期：特定時期なし** 当社が製品・サービスを提供している標的型攻撃対策を始めとする高度なセキュリティ・サービスの市場は、サイバー・セキュリティに対する脅威の複雑化・多様化を背景に今後拡大していくものと見込んでおりますが、市場の黎明期であるため不確定要素も多く、市場の成長スピードが当社の想定よりも遅れる可能性があります。また、市場が順調に拡大した場合でも、競合他社の参入や他社から無償又は安価なセキュリティ機能が供給されることにより、当社が市場シェアを伸ばして行くことができない可能性があります。このような当社を取り巻く事業環境の変化に有効な対抗策を講じることができなかった場合、当社の業績に影響を与える可能性があります。	競合他社の動向だけでなく、社会基盤や法制度の変化によりもたらされる機会やリスクを精査し、提供する製品やサービスを進化させることで、市場や顧客ニーズの変化に柔軟に対応してまいります。

目次

業績サマリー

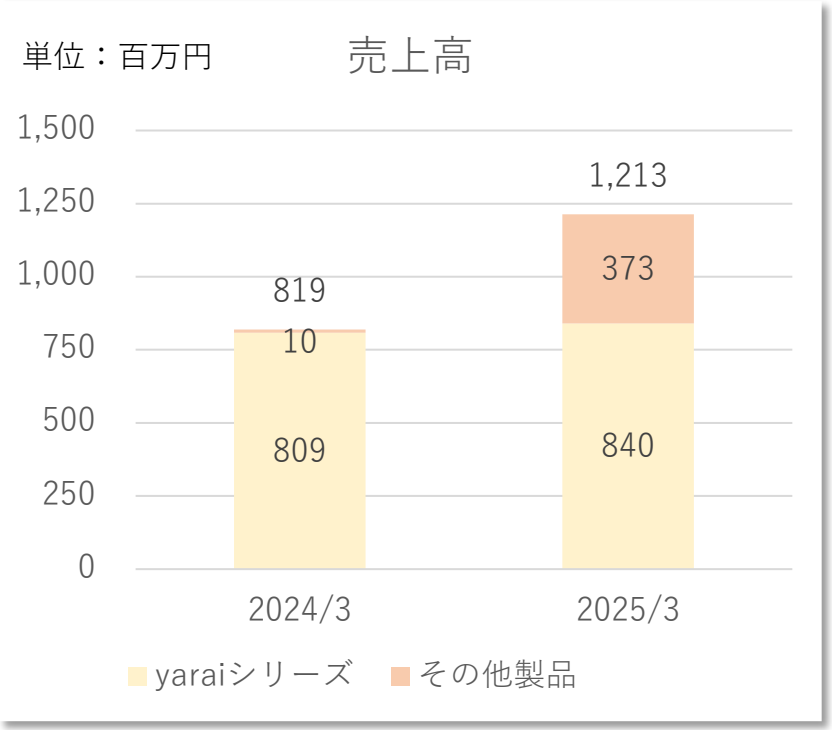
・ FFRI yarai シリーズのOEM販売が好調に推移した他、安全保障関連のセキュリティ・サービス案件の増加によって売上高は前年を上回って推移した

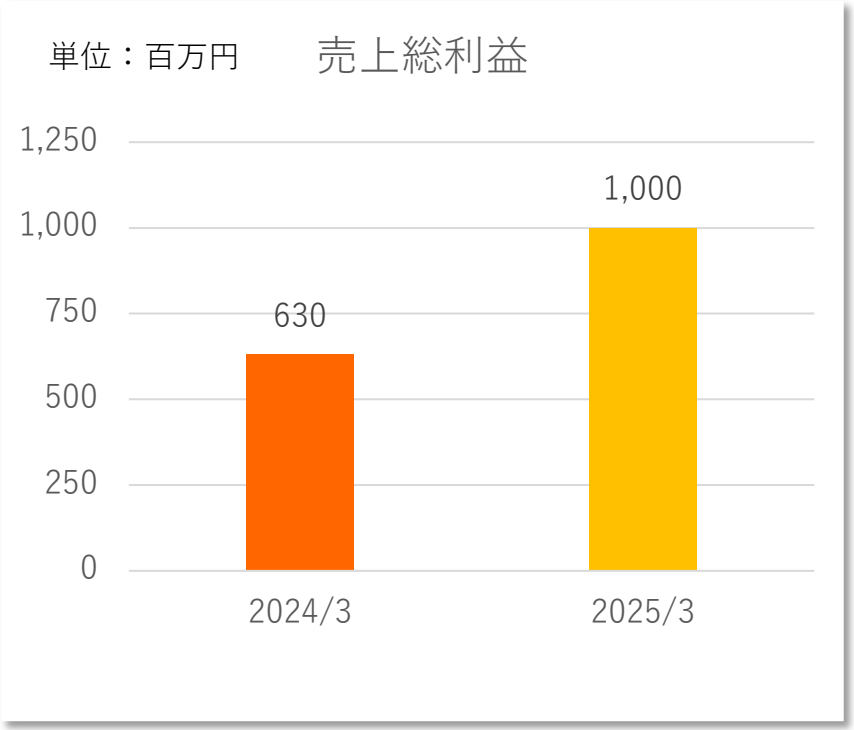
・エンジニアの待遇向上や採用活動の強化を行った結果、人件費及び採用コストが増加したものの、売上高の増加がこれを上回り増益での着地となった

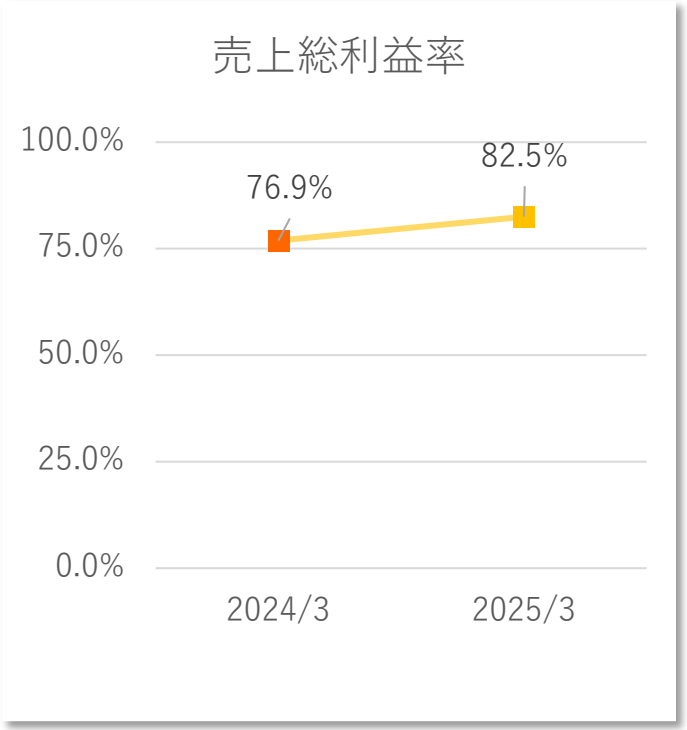
単位：百万円	2024/3	2025/3	YoY(%)
売上高	2,446	3,039	24.2
営業利益 (利益率:%)	497 (20.3)	817 (26.9)	64.1
経常利益 (利益率:%)	540 (22.1)	880 (29.0)	62.8
親会社株主に帰属する四半期純利益 (利益率:%)	432 (17.7)	687 (22.6)	59.0

販売区分別の概況　セキュリティ製品

・Ｓｋｙ株式会社及び、株式会社アレクソンによるOEM販売が増加し、 FFRI yaraiシリーズの売上高は前年を上回った
・FFRI yarai Analyzer の販売数増加もあり、セキュリティ製品の売上高は前年を上回って推移

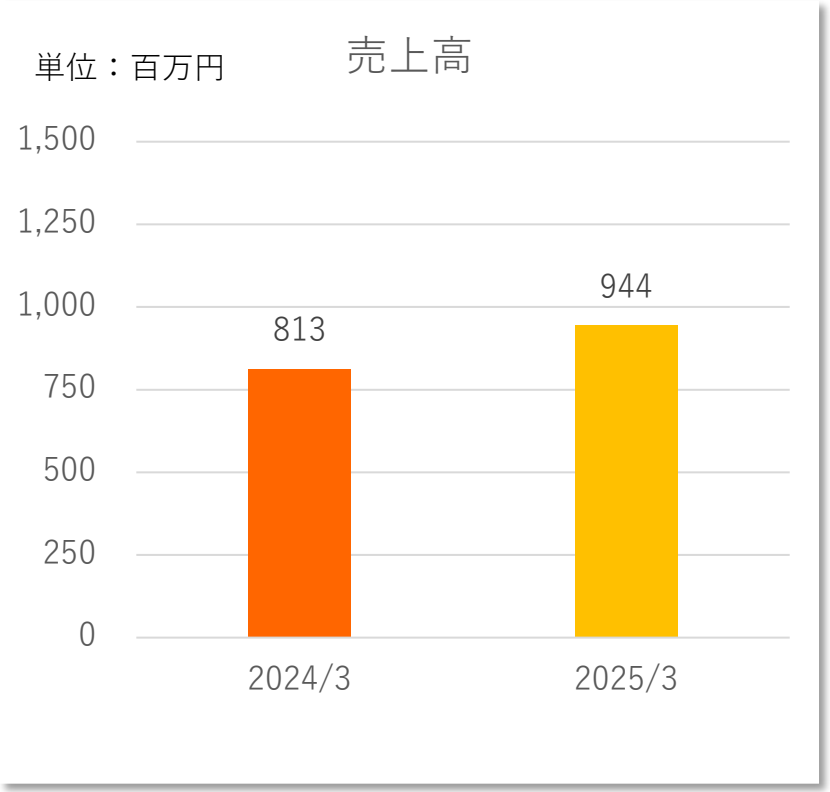


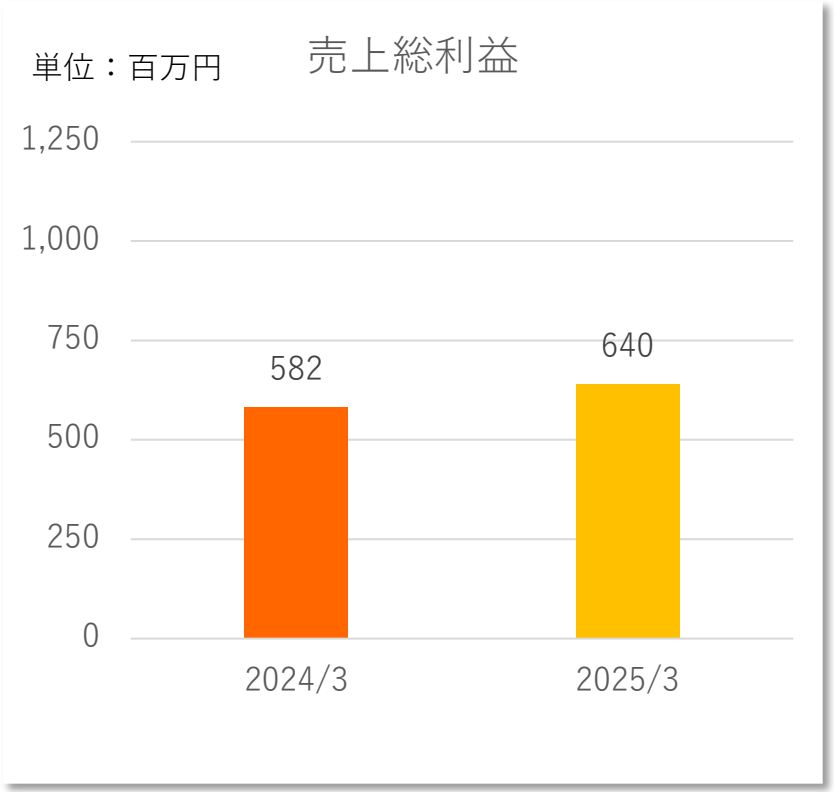


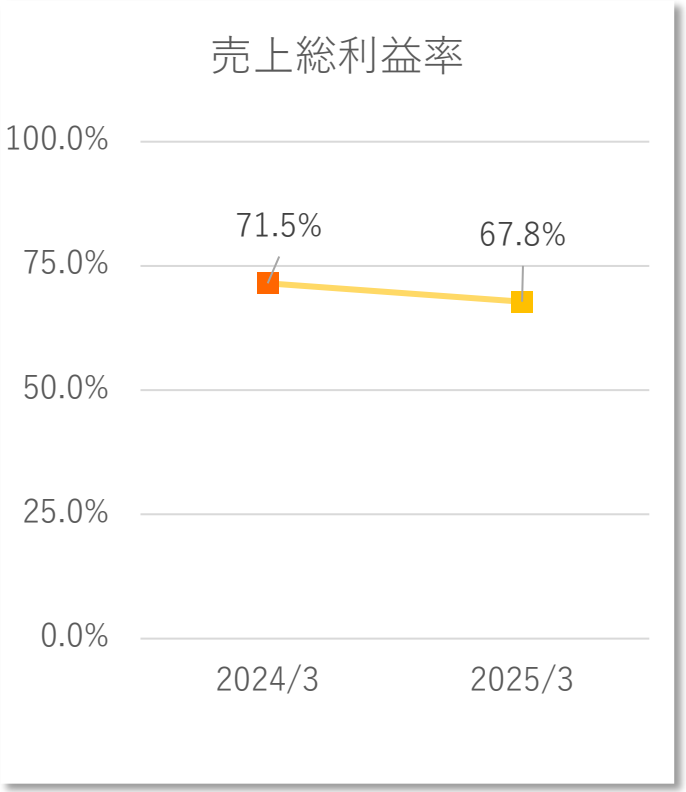


販売区分別の概況　ナショナルセキュリティ・サービス

・安全保障関連の需要増加によるナショナルセキュリティ・サービスの売上高が増加
・経済安全保障重要技術育成プログラム（Kプログラム）関連案件は第３四半期より開始となり、増収に貢献
・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影響で利益率は微減



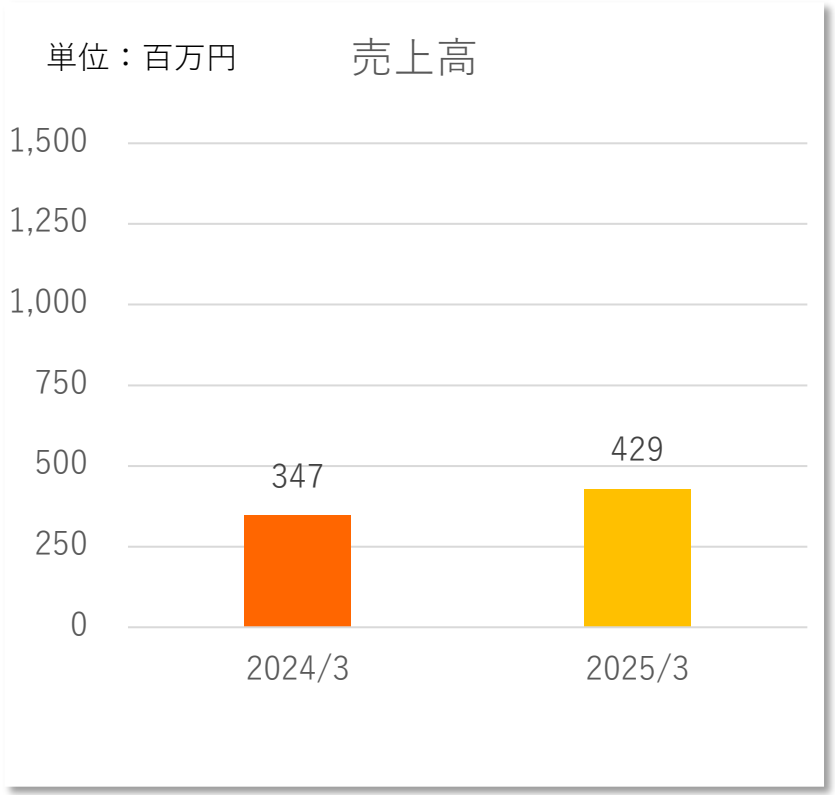


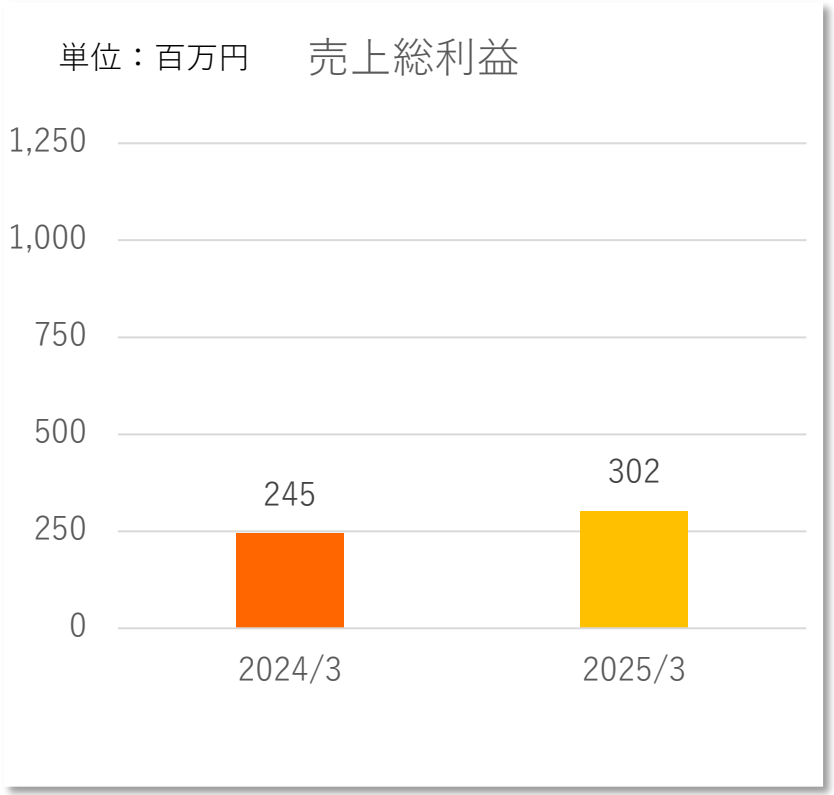


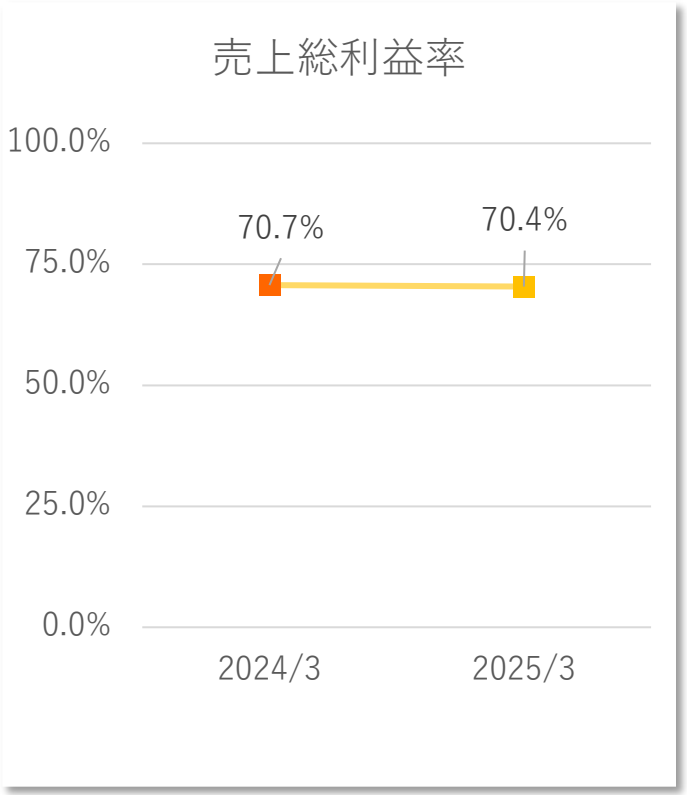
販売区分別の概況　その他セキュリティ・サービス

・セキュリティ情報提供や、受託開発、調査・研究案件などを実施

・エンジニアのリソースをナショナルセキュリティ・サービスへ集中しているため、新規案件の受注は制限しているものの、前年同期では増加となった

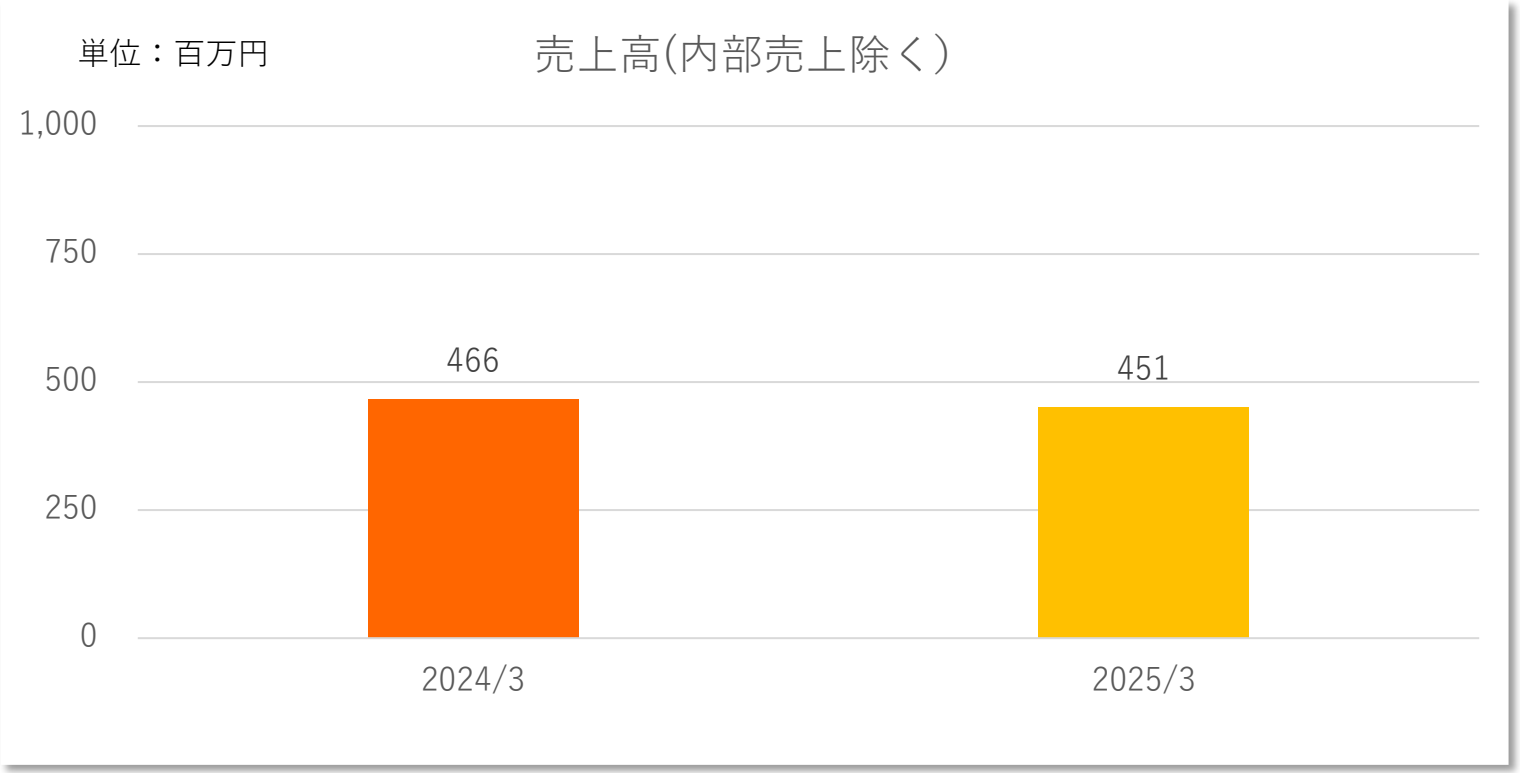






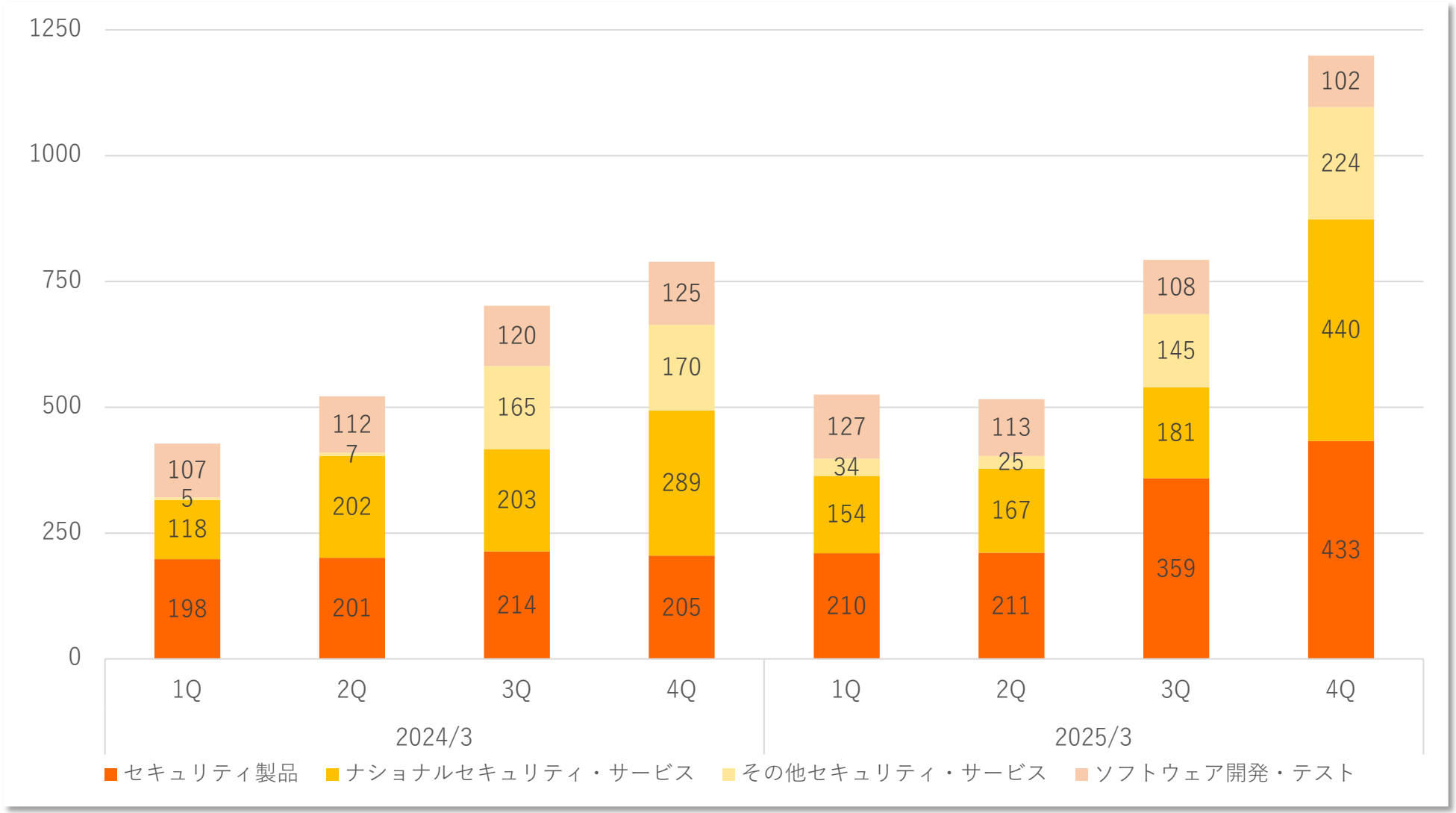
販売区分別の概況　ソフトウェア開発・テスト事業

・一部案件の解約により売上高は微減となったものの、利益面への影響は少ない
・新規顧客の開拓及び、既存案件における単価の向上に取り組む



四半期毎の売上推移

単位：百万円



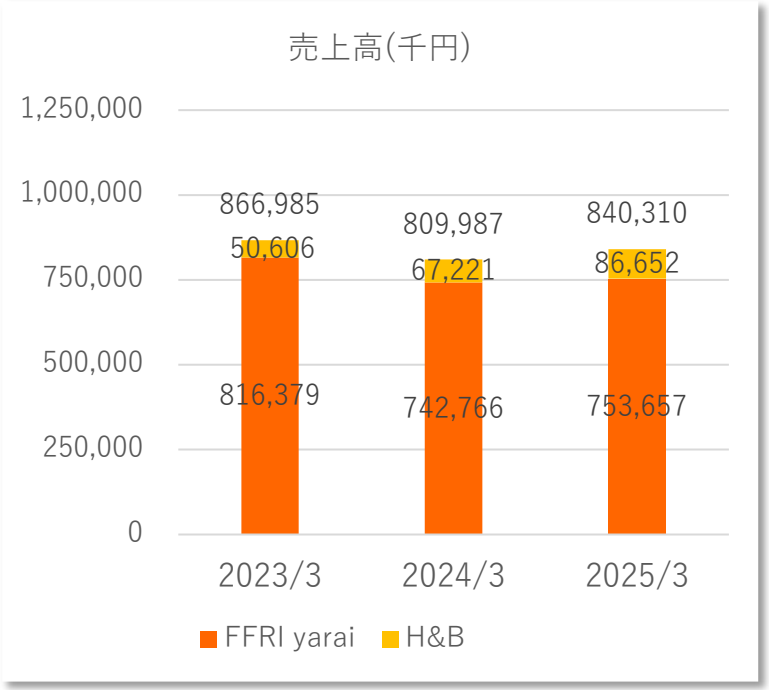
FFRI yarai シリーズの販売状況

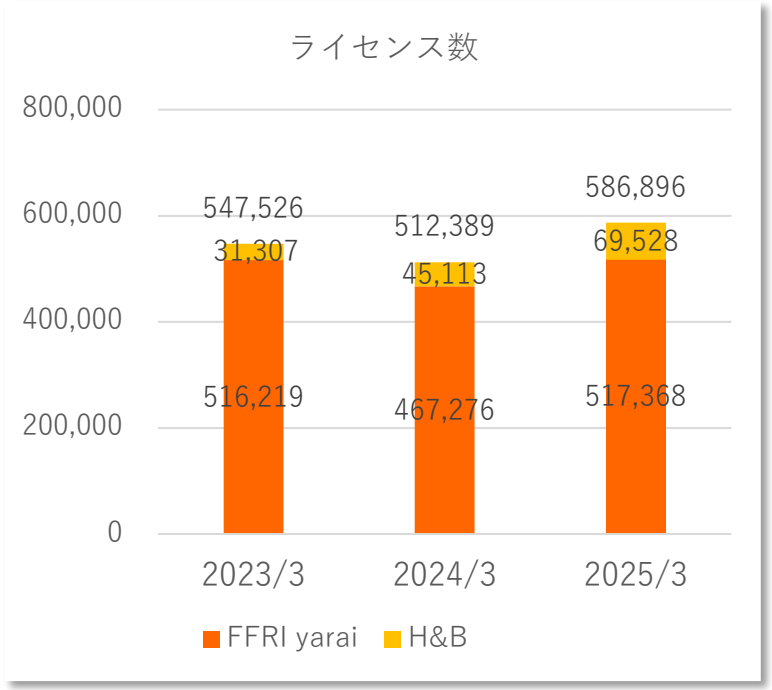
・戦略的販売パートナーによる中小企業等へのOEM販売が好調に推移し、前期末に比べ74,097ライセンス増加となった。

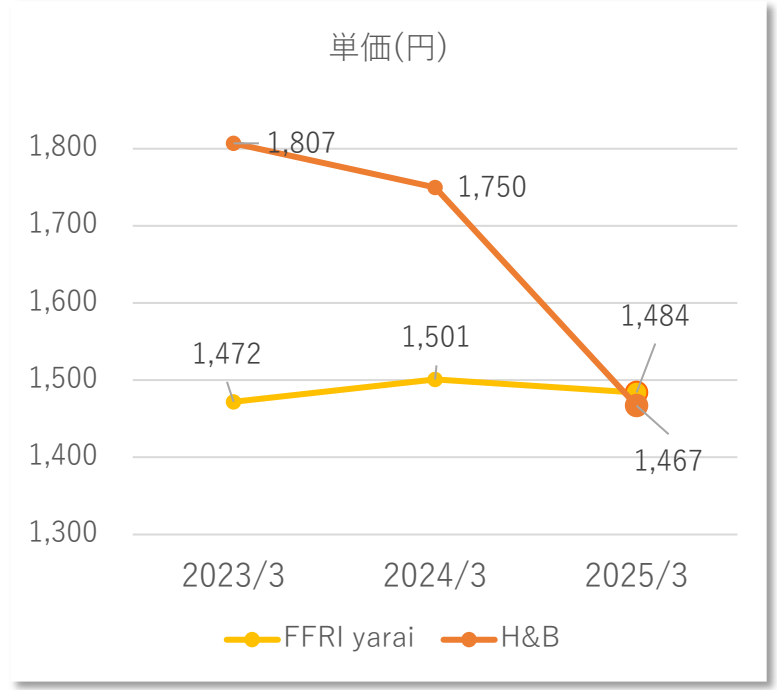
・FFRI yarai Home and Business Edition では、OEM販売が増加した結果、単価の高い自社オンライン・ショップでの販売比率が減少し、単価は減少となったものの、売上高・ライセンス数ともに前期末を上回って推移した

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：官庁及び自治体、公法人などにおける契約の増加
- 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

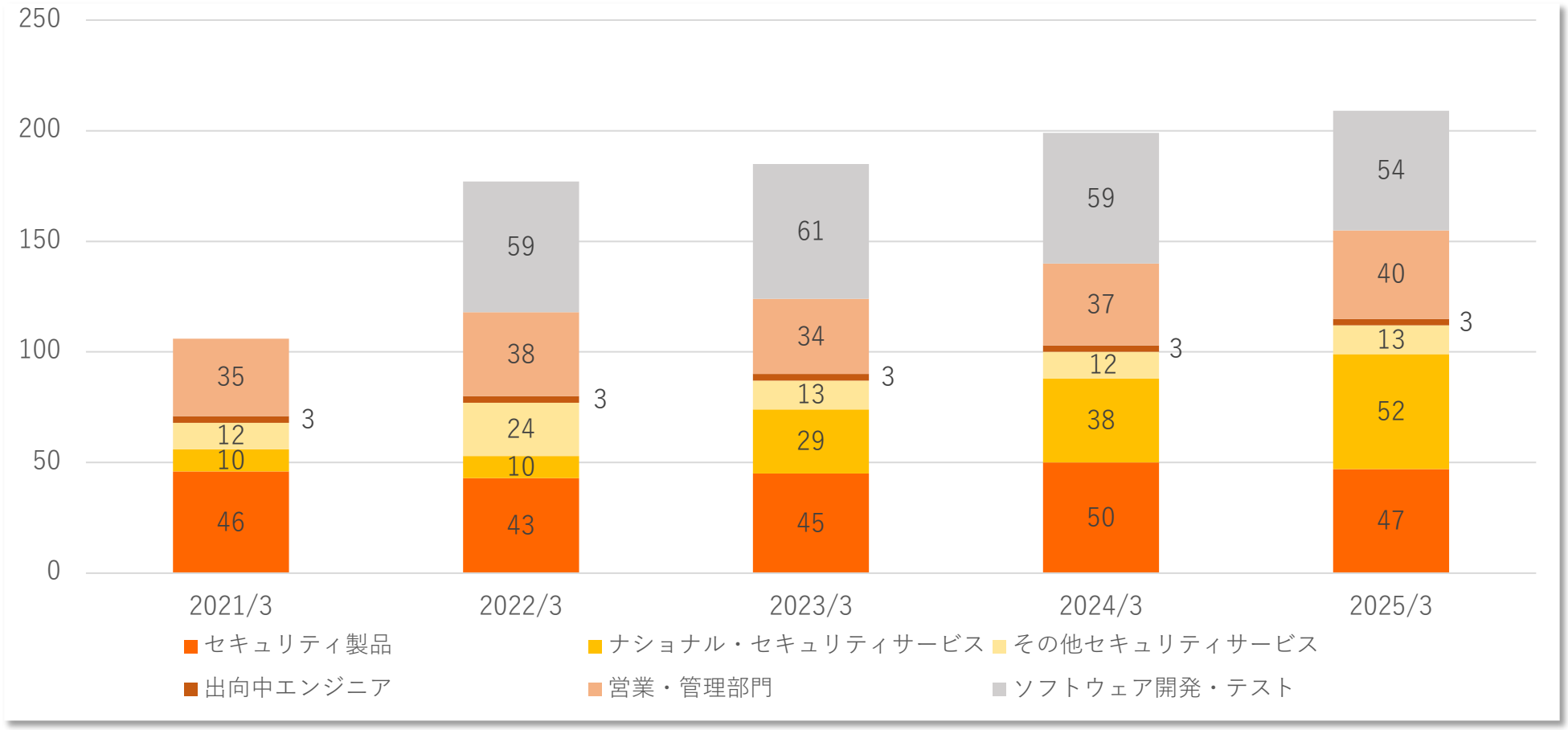
※FFRI yarai 及び FFRI yarai Home and Business Edition のライセンス数の合算となります

業種	2024/3		2025/3	
	ライセンス	割合(%)	ライセンス	割合(%)
官公庁	174,911	34.1	225,255	38.4
金融サービス	49,013	9.6	44,270	7.5
情報通信	47,181	9.2	38,798	6.6
産業インフラ・サービス	24,231	4.7	24,932	4.2
その他業種・個人	217,053	42.4	253,641	43.2
合計	512,389	100.0	586,896	100.0

人員数の推移（連結）

・前年同期比でセキュリティ・エンジニアは９名増加（98名⇒107名）となった

単位：人



原価及び販売管理費の内訳

- 労務費：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
- 採用費：採用強化・採用人数の増加による増加
- 販売促進費：提案活動など販売促進活動にかかるセキュリティ・エンジニアの人件費増加による

売上原価

単位：百万円	2024/3	2025/3	YoY
売上原価	904	1,009	11.7
労務費	925	1,113	20.2
経費	255	270	6.1
期首・期末棚卸及び他勘定振替	△275	△374	-
（研究開発費への振替）	△144	△120	-
（ソフトウェアへの振替）	△0	△21	-
（その他の振替）	△131	△232	-
売上総利益	1,542	2,029	31.6
売上総利益率	63.0	66.8	3.8

販売管理費

単位：百万円	2024/3	2025/3	YoY
販売管理費	1,044	1,212	16.1
人件費	462	490	6.0
研究開発費	189	165	△12.7
採用費	27	50	82.1
販売促進費	140	254	80.5
その他	223	251	12.4
営業利益	497	817	64.1
営業利益率	20.3	26.9	6.6

業績サマリー（B／S）

- 売掛金及び契約資産：セキュリティ・サービス案件の受注に伴う増加
- 契約負債：主にFFRI yaraiの契約増加に伴う増加
- 出資金：一般社団法人サイバーリサーチコンソーシアム設立に伴うもの

資産

単位：百万円	2024/3	2025/3	YoY
資産合計	3,381	4,310	27.5
流動資産	2,799	3,234	15.5
現金及び預金	2,078	2,162	4.1
売掛金及び契約資産	675	978	44.8
固定資産	581	1,076	85.1
のれん	101	87	△13.8
出資金	50	480	860.0

負債・純資産

単位：百万円	2024/3	2025/3	YoY
負債合計	1,199	1,521	26.8
流動負債	1,186	1,497	26.2
契約負債	914	1,151	25.9
固定負債	12	24	88.9
純資産合計	2,181	2,788	27.9
株主資本	2,181	2,788	27.9
利益剰余金	2,056	2,664	29.6

業績サマリー（C／F）

- 営業活動によるキャッシュ・フロー：増益によるもの
- 投資活動によるキャッシュ・フロー：一般社団法人サイバーリサーチコンソーシアム設立に伴う基金を拠出したことによるもの
- 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	2024/3	2025/3
営業活動によるキャッシュ・フロー	390	641
税引前当期純利益	540	880
減価償却費	28	30
売上債権及び契約資産の増減額(△は増加)	△356	△302
契約負債の増減額(△は減少)	208	236
法人税等の支払額	△74	△140
その他	44	△64
投資活動によるキャッシュ・フロー	△70	△477
財務活動によるキャッシュ・フロー	△0	△79
現金及び現金同等物の期末残高	2,078	2,162

経済安全保障重要技術育成プログラム

- 「経済安全保障重要技術育成プログラム」（通称“K Program”）は、経済安全保障推進会議及び統合イノベーション戦略推進会議の下、内閣府、文部科学省及び経済産業省が中心となって、府省横断的に、経済安全保障上重要な先端技術の研究開発を推進するもの(内閣府HPより)
- 本プログラムに基づき、国立研究開発法人 新エネルギー・産業技術総合開発機構（NEDO）と国立研究開発法人科学技術振興機構（JST）がそれぞれ実施する研究開発プロジェクトに参加

NEDO

※当社が正会員として参加する一般社団法人サイバーリサーチコンソーシアム（CRC）が実施先として採択
当社はCRCと業務委託契約を締結し、研究開発活動を行う

課題名	先進的サイバー防御機能・分析能力強化
事業期間	2024年 7 月～2029年 6 月
事業規模	290億円以下/委託事業
概要	・サイバー空間の情報を収集・調査する状況把握力向上 ・サイバー攻撃から機器やシステムを守る防衛力向上 ・共通基盤の整備

JST

※「サプライチェーンセキュリティに関する不正機能検証技術の確立（ファームウェア・ソフトウェア）」に関する個別研究型の研究開発構想における研究開発課題に当社が採択

課題名	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
事業期間	2025年 4 月から 5 か年
事業規模	最大 6 億円（間接経費含む）
概要	不正機能事例の調査および不正機能の類型化・体系化を行った上で、意図性評価の方法論整理および意図性評価ツールの開発

人材の確保および採用活動の強化

- 安全保障の需要増加を取り込むため、優秀なエンジニアの確保が必要
- 人材確保のためセキュリティエンジニアの待遇向上を実施
- 採用力強化のため、新卒採用の待遇（給与）を向上したほか、採用体制を強化

採用市場

日本国内のサイバーセキュリティ人材は
2023年時点で約11万人不足しているとされ、
様々な企業で人材の取り合いとなっている

参考：ISC2, Inc.「ISC2 Cybersecurity Workforce Study 2023」

コンピューターサイエンスや、
サイバーセキュリティ能力の高い学生は
大手企業や外資系企業との取り合いになっている

施策・成果

※グループ会社を除く

	2024/3 実績	2025/3 実績
採用チームの強化	2 名	4 名
新卒採用の待遇向上 （給与）	約30万円	東京勤務 約40万円 横須賀勤務 約50万円以上
エンジニアの中途採用数	8 名	8 名
エンジニアの新卒採用数	8名(24年4月入社)	21名(25年4月入社)
離職率（ＦＦＲＩ平均）	11.4%	5.7%

その他の主な取り組み

- 販売パートナー各社との連携を強化し、FFRI yaraiの販売拡大施策を推進
- 国立研究開発法人情報通信研究機構（NICT）の推進するサイバーセキュリティ情報収集・分析に係る実証事業に参加
- シャインテック社の人材育成および、当社サイバーセキュリティ事業におけるテスト業務への参加
- NTTコミュニケーションズとの合弁会社であるNFラボラトリーズにおける人材の育成と輩出を継続

FFRI yarai の販売拡大	NICTの実証事業	シャインテック	N.F.ラボラトリーズ
・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強化 ・FFRI yaraiの機能強化を継続 ・純国産製品の強みを活かして、官公庁・重要インフラ企業への販売施策を強化	・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～）に参加 ・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	・将来的なセキュリティ・サービスの提供を目指し、セキュリティ技術のトレーニングを継続	・教育研修事業などを中心に需要増加に対応するため人材の採用・育成を進めている ・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

採用及び教育の強化

- 採用を強化し着実にエンジニア数も増加しているが、旺盛な需要の全てを取り込めてはいない
- 新卒採用を中心にエンジニア採用の強化を継続し、中長期に渡る需要の増加を取り込める体制を構築
- プロジェクトマネジメント（PM）人材の採用及び、社内での育成を進める

必要な人材

セキュリティ・エンジニア

エンジニアは、高度な能力や研究開発に関心のある学生を中心に新卒採用で増員している

プロジェクトマネジメント層

長期案件や大型案件を安定してこなしていくためのマネジメント層（プロジェクトマネジメントまたはプロジェクトリーダー）の採用

・PL人材は国内の人材不足が顕著
・需給の問題で採用が難しいため、この先さらに人材難となる可能性が高い
・PM人材の持つノウハウを落とし込み、PL人材を社内で育成する

大手SIer出身
PM人材

マネジメント能力
問題解決力
リーダーシップ
コミュニケーション能力
など

エンジニアの
PL能力の育成

優秀な学生との接点を増やす取り組み

・インターンシップの実施（前年度は年２回実施）
・政府主導の人材発掘・育成イベントへの参加、講師の派遣（セキュリティ・キャンプや、SecHack365など）
・各大学の研究室での説明会開催や、共同研究の実施

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を進める

販売強化の取り組み

FFRI yaraiシリーズの売上・ライセンス数

売上高

2024年3月期末		2025年3月期末
809,987千円	⇒	840,252千円

ライセンス数

2024年3月期末		2025年3月期末
512,389Lic	⇒	586,896Lic

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

その他の主な取り組み

- 経済安全保障重要技術育成プログラム（K Program）関連案件もスタートしており、NICTの行う実証事業のサポート等、より一層安全保障領域への注力を強めていく
- シャインテックにおいてはサイバー・セキュリティ事業における一部テスト業務の請け負いなどグループシナジーの強化の他、ソフトウェア開発・テスト事業における新規顧客の獲得を進める
- 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（仮称）	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

※4　2026年4月1日以降については、CRCにおけるNEDOのステージゲート審査通過後に委託契約が締結された場合、再契約を行う予定です

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～）に参加

・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

シャインテック

・安定的な品質保証業務を継続しつつ、新規顧客の獲得も進める

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

連結業績予想

- セキュリティ製品の契約ライセンス数増加による増収や、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
- エンジニアの人員増による人件費の増加及び、採用活動の強化による採用コストの増加を織り込む
- 大型案件の増加によって期初よりセキュリティ・サービスの稼働があり、例年ほどの下期偏重傾向にはならない見込み

単位：百万円	2025/3(実績)	2026/3(予想)	YoY(%)
売上高	3,039	4,260	40.2
営業利益 (利益率:%)	817 (26.9)	914 (21.5)	11.9
経常利益 (利益率:%)	880 (29.0)	964 (22.6)	9.5
親会社株主に帰属する当期純利益 (利益率:%)	687 (22.6)	715 (16.8)	4.2

連結業績予想（売上高の内訳）

- 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と、前年度におけるFFRI yarai及びその他製品の契約ライセンス数増加による増収を見込む
- 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おけるテスト業務にアサインする予定もあり減収の見込み

単位：百万円	2025/3（実績）	2026/3（予想）	YoY（%）
サイバー・セキュリティ事業	2,587	3,856	49.0
セキュリティ製品	1,213	1,745	43.8
ナショナルセキュリティ・サービス	944	1,522	61.2
その他セキュリティ・サービス	429	588	37.0
ソフトウェア開発・テスト事業	451	403	△10.6
合計	3,039	4,260	40.2

中期経営計画（2026年３月期～2028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（2025.5.14公開）

単位：百万円	2026/3（予想）	2027/3（計画）	2028/3（計画）
売上高	4,260	5,073	5,966
営業利益 (利益率:%)	914 (21.5)	1,112 (21.9)	1,386 (23.2)
経常利益 (利益率:%)	964 (22.6)	1,163 (22.9)	1,436 (24.1)
親会社株主に帰属する当期純利益 (利益率:%)	715 (16.8)	843 (16.6)	1,033 (17.3)

当初計画（2024.5.14公開）

2026/3（当初計画）	2027/3（当初計画）
3,765	4,479
663 (17.6)	844 (18.8)
689 (18.3)	870 (19.4)
480 (12.8)	606 (13.5)

株主還元（配当）

- 当期の連結業績や、足元の市場状況等を踏まえ、当初計画から増配（10円→14円）とした
- 今後も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

	2025年3月期	2026年3月期（予想）
親会社株主に帰属する当期純利益	687百万円	715百万円
１株当たりの当期純利益	86.86円	90.49円
１株当たりの配当金	14.0円	14.0円
配当性向(連結)	16.1%	15.5%

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。

なお、本資料の更新は、今後、本決算発表後の６月に開示を行う予定です。事業計画の進捗につきましては、四半期毎の開示を予定しております。また、記載内容に重要な変更が生じた場合には、速やかに開示を行います。