事業計画及び成長可能性に関する説明資料

2024.6.27

株式会社ＦＦＲＩセキュリティ ｜ 東証グロース：3692

目次

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　事業開発及びyarai事業担当	川原　一郎	社外取締役（監査等委員）	中山　泰秀
	取締役　製品開発本部長	梅橋　一充		

設立：　2007年7月3日

資本金：　286,136,500円（2024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

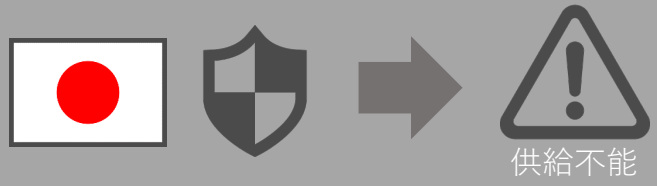
2014年9月30日　東証マザーズ市場に上場（現在はグロース市場）

設立の経緯

これまで日本は対策技術を海外からの
輸入に頼っていた…

セキュリティ分野

セキュリティ製品の有力な研究開発ベンダーが不在



海外のセキュリティベンダーの技術を輸入して供給する。

国内に研究開発企業が不在

標的型攻撃を含む
未知の脅威の拡大

自国で問題解決できないリスク

国産の対策技術の必要性

FFRI

日本発の
サイバー
セキュリティ

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

「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

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

Fourteenforty Research Institute

↓

ＦＦＲＩセキュリティ

コーポレートマーク

コーポレートマークにも「1440」の文字とスノーボードの回転をイメージした矢印で、
設立当初から変わらない「未踏の分野への挑戦」を表現

世界トップレベルのセキュリティ・リサーチ・チームを作り、
コンピュータ社会の健全な運営に寄与する

ＦＦＲＩセキュリティが果たすべき役割

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

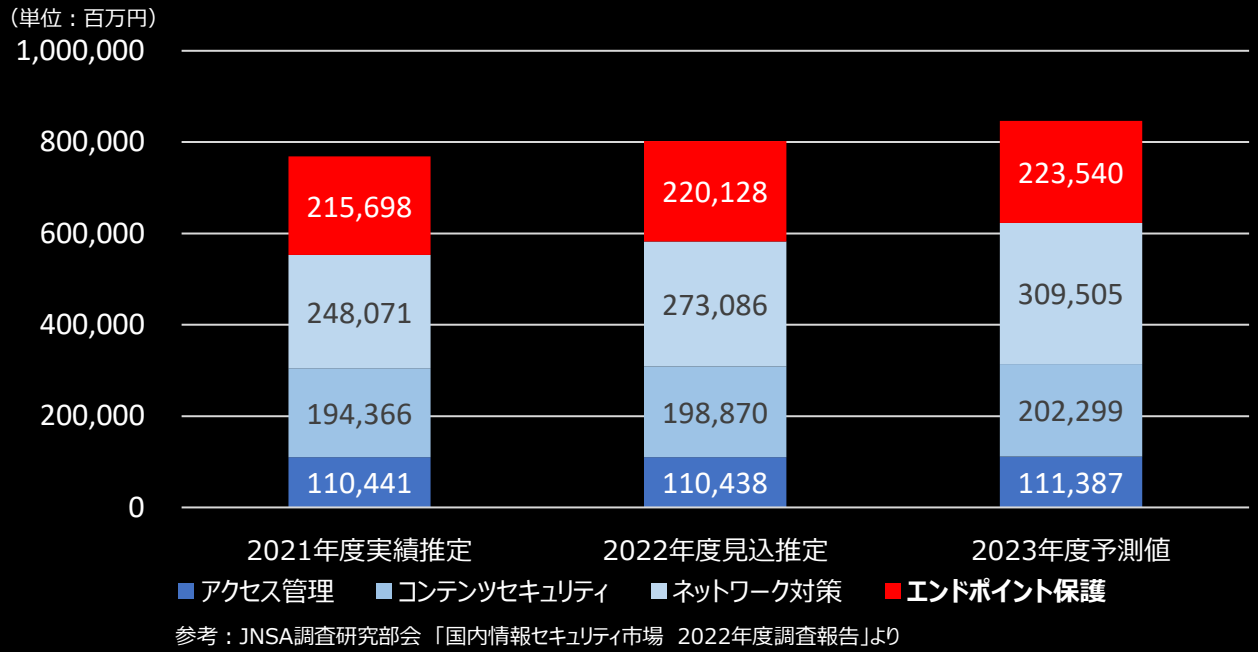
高い技術力

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

目次

事業環境　セキュリティ・プロダクト市場

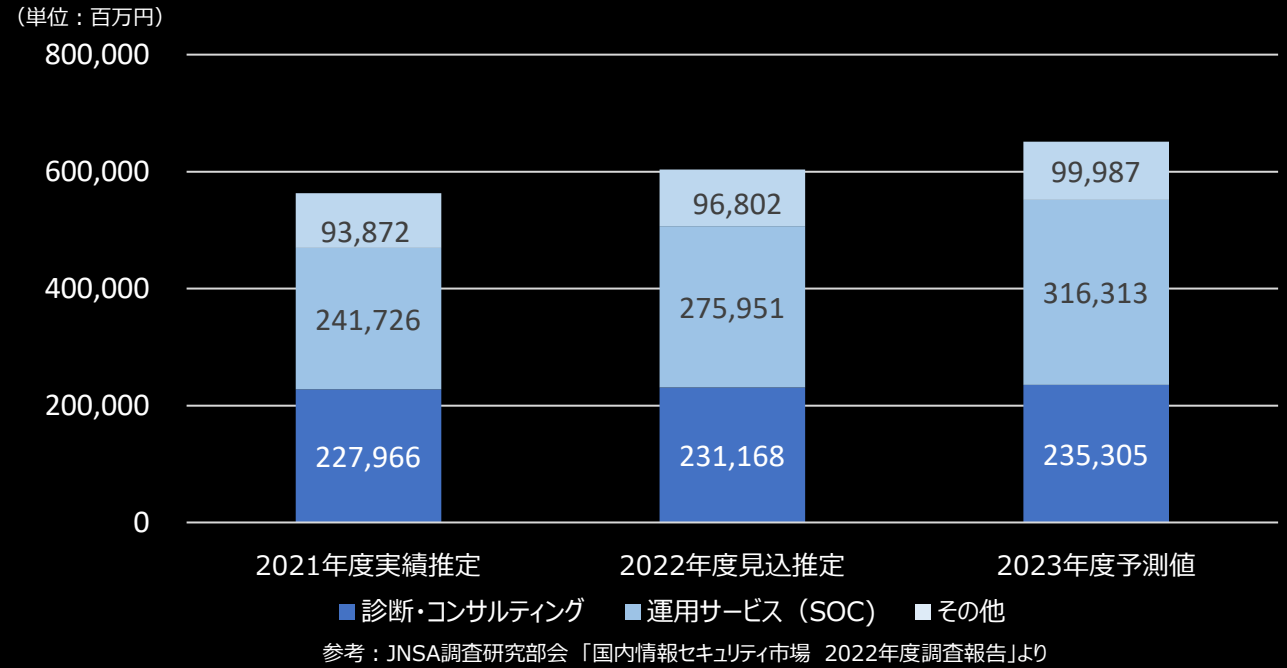
当社製品 FFRI yarai はエンドポイント保護製品に分類
国内市場はサイバー攻撃による被害の増加や、テレワークやDXの推進を受けて年々拡大している



参考：JNSA調査研究部会「国内情報セキュリティ市場　2022年度調査報告」より

事業環境　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や、法律改正に伴うセキュリティ体制強化により、市場全体で拡大傾向が続くと見込まれる



参考：JNSA調査研究部会「国内情報セキュリティ市場　2022年度調査報告」より

サイバー安全保障領域におけるトピックス

当社が注力しているサイバー安全保障領域は、「経済安全保障推進法」及び「防衛３文書」の制定以降、
大幅に需要が増大しており、今後も中長期に渡る市場の拡大が見込まれる

サイバー安全保障領域の事業環境

近年、国家安全保障におけるサイバー領域の重要性が高まっている
「サイバー空間は平素から、地政学的緊張を反映した国家間の競争の場の一部ともなっている」

参考：次期サイバーセキュリティ戦略(NISC他各省庁)より抜粋

米中の対立による国際社会の緊張の高まり

政治 **経済** **軍事**

「第二の冷戦」とも形容される

米中間で様々な面で覇権争いの活発化

参考：新たな国家安全保障戦略等の策定に向けた提言(自由民主党)

国家間の競争の場となったサイバー空間

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の増大

重要インフラの機能停止 **情報・知的財産の窃取** **民主プロセスへの干渉**

※公正な選挙の妨害等

国家安全保障に影響を与えうる
サイバー攻撃が猛威を奮っている

参考：次期サイバーセキュリティ戦略(NISC他各省庁)より抜粋

サイバー安全保障領域の事業環境

ロシアはウクライナ侵攻の１ヶ月以上前からウクライナにサイバー攻撃を仕掛けるなど、
国家の関与が疑われるサイバー攻撃による情報窃取や、通信・重要インフラへの妨害といった
サイバー領域をめぐる争いが安全保障上の重要なリスクとなっている

**ロシアのウクライナ侵攻で顕在化した、
戦争手段としてのサイバー攻撃**

侵攻の１ヶ月以上前

ウクライナ政府や、大手銀行への
大規模なサイバー攻撃を確認

侵攻開始以降

軍事活動とサイバー攻撃を複合的に組合せた「ハイブリッド戦」が展開される

サイバー空間が新たな戦場となっている

参考：新たな国家安全保障戦略等の策定に向けた提言(自由民主党)

国民生活に影響を与えるサイバー攻撃の脅威

国家主導のサイバー攻撃を平時より行っているとみられる

中国	軍事・先端技術保有企業の情報窃取
ロシア	軍事及び政治的目的にむけた影響力行使
北朝鮮	政治目標の達成や外貨獲得のため

**重要インフラへのサイバー攻撃が日常的に発生
サイバー空間の情勢は最早純然たる平時とは言えない**

参考：次期サイバーセキュリティ戦略(NISC他各省庁)

日本の課題：サイバーセキュリティ自給率の低迷

国内サイバーセキュリティ産業は、海外技術・製品に過度に依存しており、
技術・ノウハウが蓄積されておらず、自国の問題を自国だけで解決できない問題が生じている

国内サイバーセキュリティ産業は
海外技術へ過度に依存している

海外ベンダー

研究開発コストを投じ、
コア技術の研究開発を行う

技術や製品を輸入

国内ベンダー

事業上のリスクを避け
技術を輸入に頼っているため
技術やノウハウが蓄積できていない

サイバーセキュリティ自給率の低迷

参考：サイバーセキュリティ研究・技術開発取組方針
（サイバーセキュリティ戦略本部/NISC）

情報通信インフラを構成するハードウェアや
ソフトウェア、クラウドを始めとする情報通信の
主要機能や関連する人材の海外依存は、
戦略的自律性※の観点から大きな課題である。

※いかなる状況の下でも他国に過度に依存することなく、
国民生活の持続と正常な経済運営を実現すること

参考：新国際秩序創造戦略本部　中間取りまとめ（自由民主党）より抜粋

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、
安全保障に絡む緊急性の高い事案等においても、
海外ベンダーの対策技術開発を待たねばならない

日本の課題：データ負けのスパイラル

海外セキュリティ製品の利用によってデータが集まらず、研究開発が進まない
データ負けのスパイラルに陥っている

国内サイバーセキュリティ産業の問題点

国内サイバーセキュリティ事業者のほとんどが
海外のセキュリティ製品を導入・運用する形態

国内にサイバー攻撃の情報が存在しない

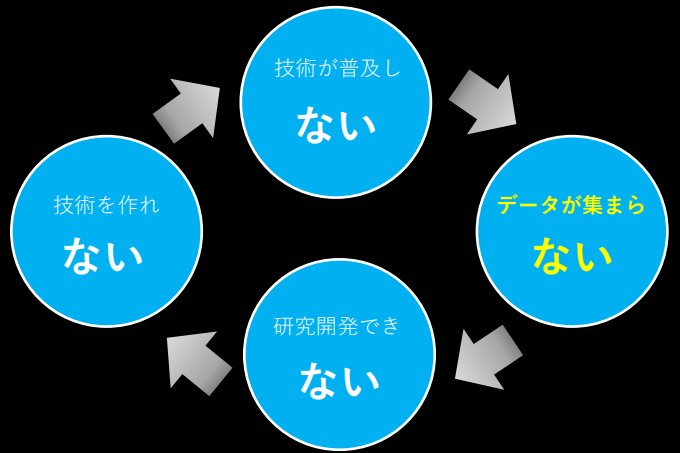
脅威情報を海外事業者から購入している

国内サイバーセキュリティ産業が育たない

セキュリティ人材が不足している

国内産業はデータ負けのスパイラル

**海外技術・製品に依存しているため、
研究開発に必要なデータが集まらない**



参考：セキュリティ情報の自給に向けたサイバーセキュリティ知的基盤構想
（国立研究開発法人　情報通信研究機構）

日本政府の取り組み：防衛３文書の制定

パワーバランスの歴史的変化と地政学的競争の激化に伴う、戦後最も厳しく複雑な安全保障環境を背景に
「国家安全保障戦略」・「国家防衛戦略」・「防衛力整備計画」の防衛３文書を制定

※国家安全保障局「国家安全保障戦略」（令和４年12月）より一部抜粋

国家安全保障戦略	国家防衛戦略 （防衛計画の大綱に代わる文書）	防衛力整備計画 （中期防衛力整備計画に代わる文書）
国家安全保障に関する最上位政策文書	**防衛の目標を設定、それを達成するためのアプローチと手段を示すもの**	**保有すべき防衛力の水準を示し、その水準を達成するための中長期的な整備計画**
安全保障に関する基本的な原則や目標を定める	**サイバーを含む７つの重視分野における自衛隊の役割を定める**	**５ヵ年の防衛力整備の具体的事業を定める**
外交、防衛に加え、経済安保、技術、サイバー、情報等の国家安全保障戦略に関連する分野の政策に戦略的指針を与える。	防衛力の抜本的な強化にあたって重視する能力を示す 国全体の防衛体制の強化 同盟国・同志国等との協力方針	５ヵ年の経費と主要装備品の数量（特に重要な装備品等の研究・開発事業とその配備開始等の目標年度など）

日本政府の取り組み：経済安全保障推進法の制定

「経済安全保障推進法」では、法制上の手当てが必要な４つの課題に対応する制度を創設
基幹インフラ事業者及び委託先に対して、セキュリティ体制の審査が行われるほか、
先端技術の研究開発を政府が積極的に支援する

経済安全保障上の４つの課題

- **重要物資の安定的な供給の確保**
- **基幹インフラ役務の安定的な提供の確保**
- **先端的な重要技術の開発支援**
- **特許出願の非公開**

サイバーセキュリティ関連の取組（一部）

電気・ガス・電気通信など14の分野の事業者に対して外部からの妨害行為を防ぐための枠組みを整備

基幹インフラ事業者及びその委託先に対し、
セキュリティ体制を含めた審査が実施される

先端技術の研究開発を政府が積極的に支援

特に優先して育成すべきものについて指定基金を活用
政府がリスクを取って投資を行い、知見を有する民間企業・
大学等との官民連携の下、研究開発を協力に推進

CYNEXの設立

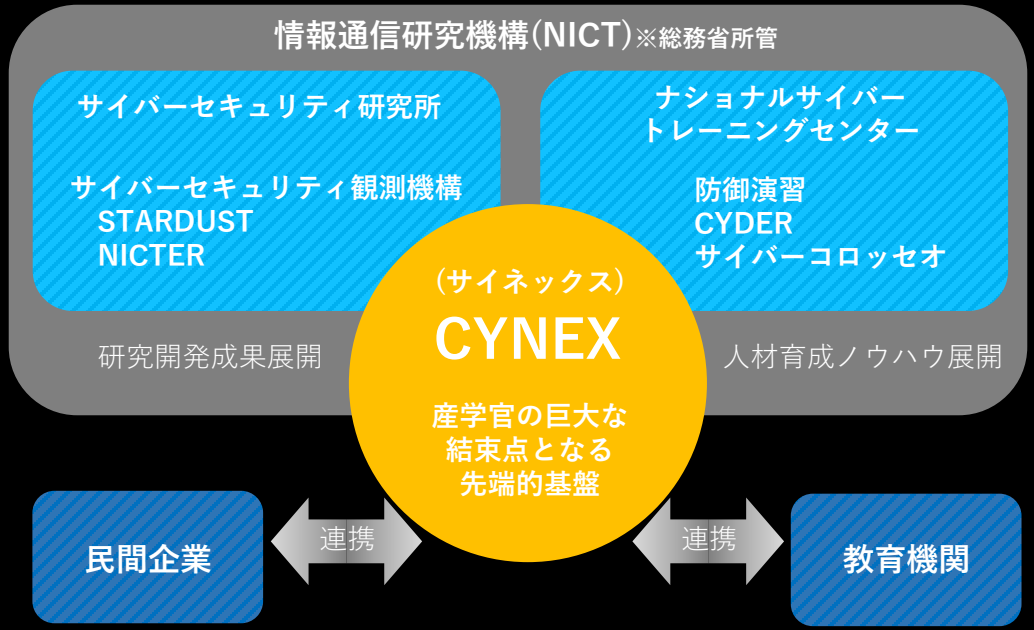
国内のサイバーセキュリティ産業育成を後押しする CYNEX を設立し、データ負けのスパイラル脱却を図る

CYNEXの役割・目的

「サイバーセキュリティに関する産学官の結束点」

■サイバーセキュリティ自給率の低迷
■データ負けのスパイラル
という課題解決に向けて、
・実データを **大規模に収集・蓄積**する仕組み
・実データを **定常的・組織的に分析**する仕組み
・実データで **国産製品を運用・検証**する仕組み
・実データから **脅威情報を生成・共有**する仕組み
の実現を目指す

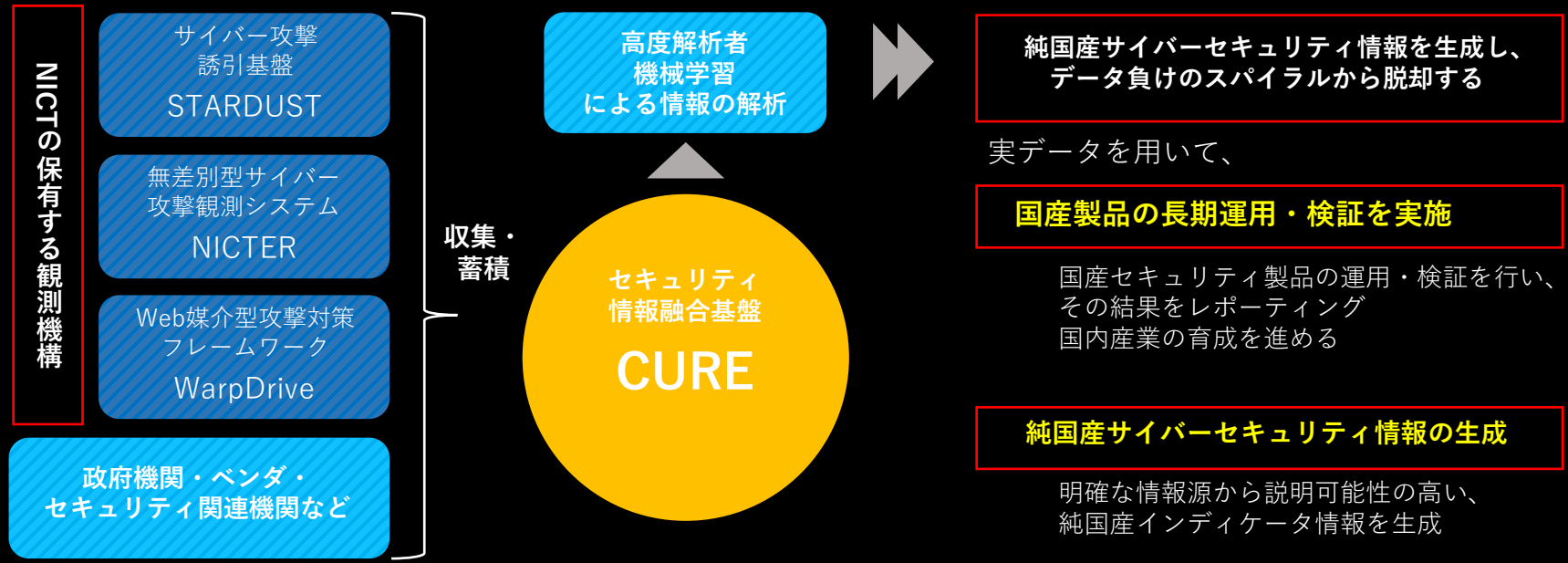
母体組織であるNICTの研究成果や
サービスの一部を産学に半開放



参考：CYNEXの構築について(国立研究開発法人 情報通信研究機構/NICT)

CYNEXの設立

NICTの保有する観測機構を活用して収集した実データを元に、国産製品の長期運用・検証や、
純国産サイバーセキュリティ情報の生成を行う。



参考：CYNEXの構築について(国立研究開発法人 情報通信研究機構/NICT)

NICTの推進する実証事業

国立研究開発法人 情報通信研究機構（NICT）が、純国産サイバーセキュリティ情報の生成に向けた実証事業を開始。

安全性・透明性の検証が可能な政府端末向けセキュリティソフトをNICTが開発

NECと共に開発の技術的な支援

政府端末に導入し、マルウェア情報等を収集・分析

- 純国産のサイバーセキュリティ情報の生成に向けた具体的な事業も進み始めている
- NICTによる政府端末向けセキュリティソフト開発を当社も技術的に支援
- 一部の政府端末に導入し、得られたマルウェア情報等の収集、分析を行う

セキュリティ・クリアランス制度の導入

日本の情報保全措置は「特定秘密保護法」のみで、
保護される情報の種類や領域が限定されていた

セキュリティ・クリアランス制度では、保護される情報
（重要経済安保情報）は政府が指定し、アクセスには
事前の認証が必要となった

※経済安全保障版セキュリティ・クリアランス制度の創設（内閣委員会調査室）
資料を基に図解

主要国では既に定着しており、米国のクリアランス保有者
は400万人以上、そのうち３割程度が民間となっている

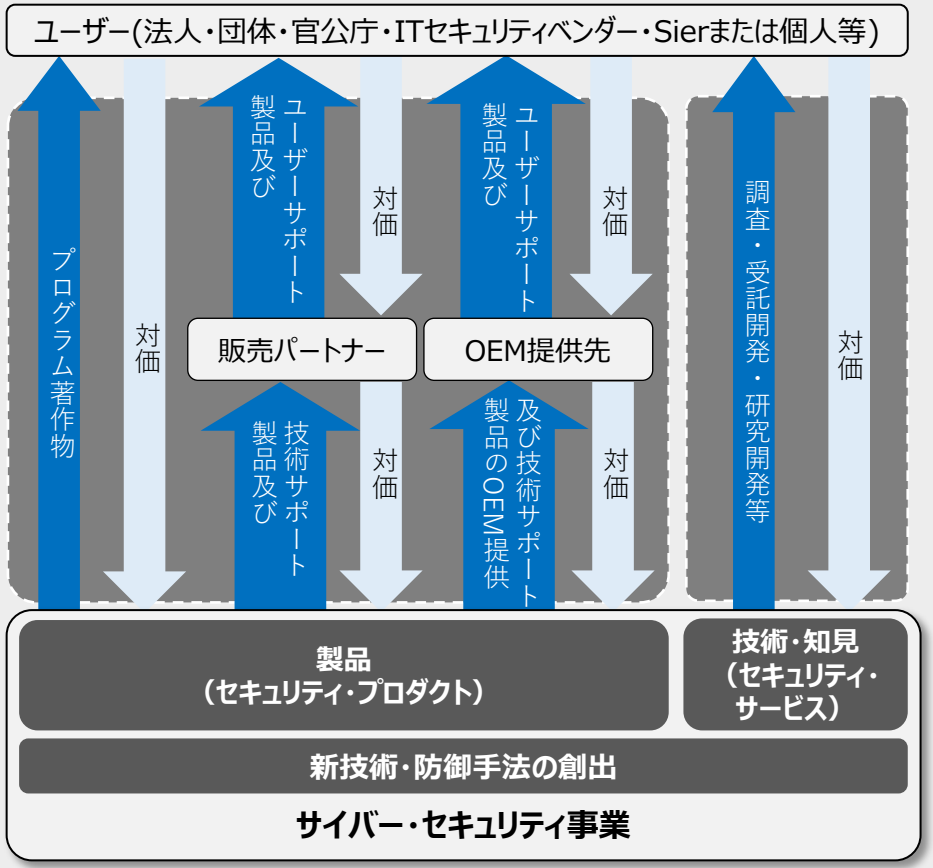
・セキュリティ・クリランス制度とは、政府が保有する
安全保障上重要な情報として指定された情報に対して、
アクセスする必要がある者のうち、情報を漏らすおそれが
ないという信頼性を確認した者の中で取り扱うとする制度
※重要経済安保情報の保護及び活用に関する法律案（内閣官房）より抜粋

・情報保全の強化は、同盟国・同志国との間での
情報共有や、国際共同開発などにおいては必要不可欠

・クリアランス保有が前提の国際会議や入札への参加、
情報共有が可能となる

目次

事業モデル：サイバーセキュリティ事業



・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、
セキュリティ・プロダクトと、セキュリティ・サービスを提供している

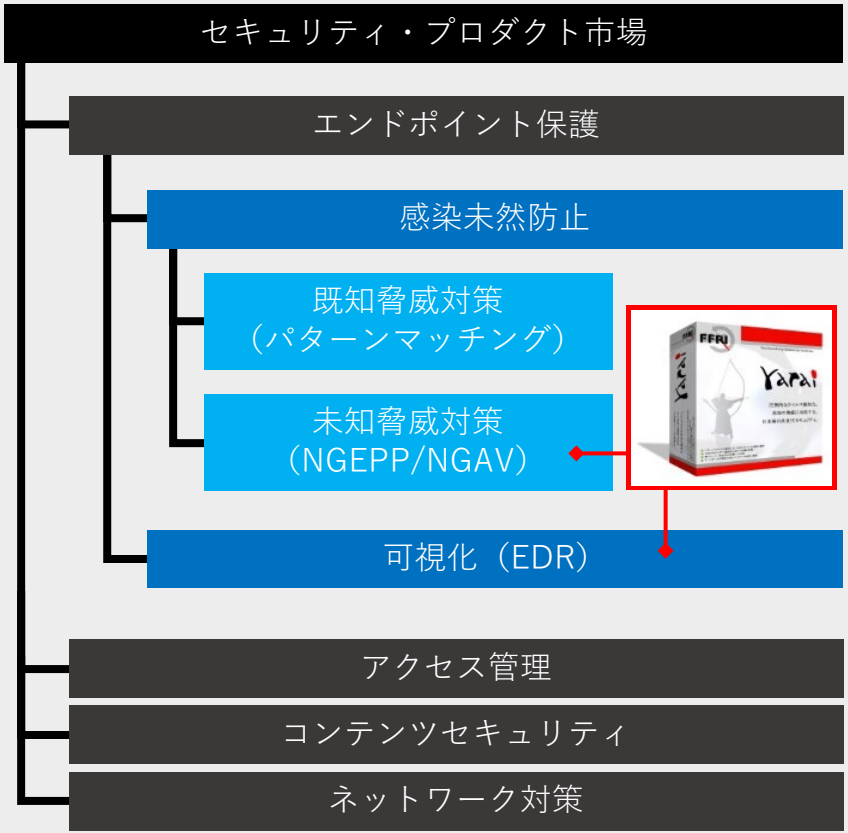
・セキュリティ・プロダクトは、販売パートナーによる代理店販売や
製品のOEM提供による販売、当社からユーザーに対する直接販売を
行っている

・セキュリティ・サービスは、
調査・研究・開発・教育等のサービスを
提供している

主要なセキュリティ・プロダクト

名称	内容
FFRI yarai	パターンファイルに依存しない、完全ヒューリスティック検知技術による 標的型攻撃マルウェア対策製品で、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	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、 自社内でマルウェア初動解析が可能です。

FFRI yarai の市場



・「FFRI yarai」及び「 FFRI yarai Home and Business Edition」は、セキュリティ・プロダクト市場において、未知脅威対策及びEDRに分類

・標的型攻撃や、ゼロデイ脆弱性攻撃などの未知の脅威対策としての優位性を持つ

・国内に同様の機能を持つ製品を提供するベンダーはほぼおらず、競合企業のほとんどは海外ベンダー

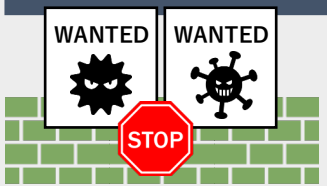
FFRI yarai の強み

FFRI yarai
振る舞い検知型マルウェア対策
（先読み技術）

マルウェア特有の怪しい振る舞いなどの特徴を判断
未知のマルウェアも検知

・FFRI yaraiは、振る舞い検知技術により、マルウェア特有の怪しい振る舞いを検知するため、標的型攻撃やゼロデイ脆弱性攻撃などの未知のマルウェアを使用した攻撃も防御することができる。

従来型ウイルス対策ソフト
パターンマッチング型マルウェア対策
（後追い技術）



定義ファイルを用いたパターンマッチングにより既知のマルウェアを検知する
定義ファイルに無い未知の脅威は防ぐことができない

・従来のパターンマッチング型製品は、ベンダーが収集したマルウェアをパターンファイルとして登録し、パターンファイルとの照合によってマルウェアを検出するため、パターンガイルに登録されていない未知のマルウェアは防ぐ事ができない

FFRI yarai 独自の技術

独自のプログレッシブ・ヒューリスティックエンジン

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

・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

・パターンファイルに依存しないため、オフライン環境においても１００％の防御力を発揮します

・全ての技術は国内で自社開発しています

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。

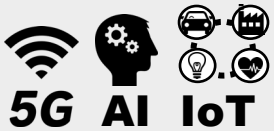
発生・ 報道時期	防御エンジン リリース時期	当時の未知脅威 及び標的型攻撃
2022年11月	2021年10月	マルウェア「Emotet」(2022年11月版)
2021年3月	2019年1月	ファイルレスマルウェア「AlumniLocker」
2020年11月	2018年2月	マルウェア「IcedID」
2018年7月	2018年3月	マルウェア「Emotet」
2018年4月	2017年6月	ランサムウェア「GandCrab」
2017年12月	2017年5月	仮想通貨採掘マルウェア「CoinMiner」
2017年5月	2016年10月	ランサムウェア「WannaCry/WannaCrypt」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

セキュリティ・サービスの強み

請負契約型

サイバー安全保障関連のサービス案件はほぼ請負契約
高い技術力や調査力、研究開発体制が必要な案件が多く、
マーケットの拡大ペースに対してキャパシティは不足し、
新規参入の障壁も高い

サービス・メニュー型



先端技術領域
セキュリティ分析・診断

高度セキュリティ
技術者トレーニング

サイバーインテリジェンス
の提供

・高度な技術力や研究開発力が必要なサービスを提供

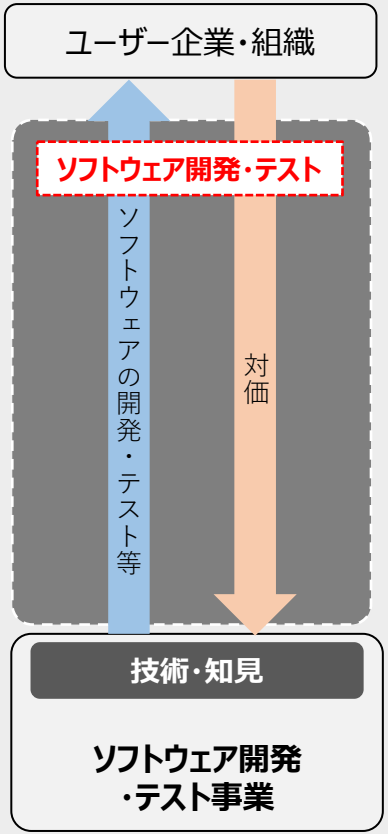
・サイバー安全保障関連需要はほとんどが請負契約型
特定のプロジェクト等のための調査・研究・開発などを提供

・国内の他ベンダーにはない、IoT機器やAIなどの先端技術領域のセキュリティ調査の他、リバースエンジニアリングや、セキュリティ脆弱性の発見をテーマとした実践的なトレーニングの提供など、高い技術力や研究開発力をベースとしたサービスを提供

セキュリティ・サービスの主なメニュー

名称	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。

事業モデル：ソフトウェア開発・テスト事業



・子会社の株式会社シャインテックの主な事業

・ソフトウェア開発・テスト事業は、ソフトウェアの設計・開発・評価・解析などに業務に関わる技術者の派遣を行う

ソフトウェア開発・テスト事業の展望

ShineTec

テスト事業　×　セキュリティ事業

セキュリティ領域を含めた、より幅広いサービスを提供することで、
シナジーを発揮していく

・子会社の株式会社シャインテックよりソフトウェアの
企画・開発、テストのサービスを提供

・当社の持つセキュリティ技術の教育を実施しており、
将来的に当社のセキュリティ・サービスの案件における、
テスト業務の委託を目指している

目次

成長実現における２つの柱

1 サイバー安全保障関連の需要を取り込み成長のドライバーとする

2 FFRI yarai の販売拡大

サイバー安全保障関連の需要の増加

政府の進めるサイバー安全保障の取組は急速な進展を見せており、需要増加は今後も中長期に渡って続く見込み


サイバーセキュリティ自給率の向上


データ負けのスパイラル脱却


サイバー防衛能力強化


防衛産業のサイバーセキュリティ対策


防衛費の増額

・各省庁で様々な取り組みが進んでおり、
需要が急速に拡大している

・経済安全保障推進法や、防衛３文書、セキュリティ・
クリアランス法案など法整備も進む

・防衛費を2027年度までにGDP比２％とするなど
急速に市場規模も拡大している

ＦＦＲＩセキュリティの役割

急速に増加する需要に対して、国内でセキュリティコア技術の研究開発を行う、有力な研究開発ベンダーはほぼ当社のみ

当社事業の特徴

国内に研究開発拠点を持ち、
純国産技術を活用した
製品・サービスを提供している

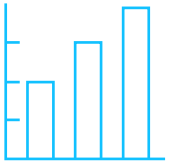
サイバー攻撃技術を研究し、
その対策を開発することで
防御技術を生み出す

需要の増加に対応するため、組織体制の整備や採用体制を強化し、キャパシティの増加やリソースの集中を進めてきた

- 海外企業の参入が困難な安全保障領域において、研究開発能力を持つサイバーセキュリティ企業はほぼ当社のみ
- エンジニアのリソースをサイバー安全保障に集中。採用体制も強化するなど、キャパシティの向上を進めているが、需要の増加はそれ以上に旺盛
- サイバー安全保障の需要を将来に渡って取り込み、成長のドライバーとするため、キャパシティの拡大が必要

採用力の強化

需要の増加を取り込めるだけの人材を確保するため、採用力の更なる強化



国内の人材市場においては、
セキュリティ人材の不足が顕著

様々な企業で人材の取り合い
となっている

新卒採用の待遇向上

企業としてのプレゼンスの向上
による採用力の強化を実施

・採用力の強化のため新卒採用の待遇（給与）を向上

・ＦＦＲＩセキュリティのプレゼンス向上のため
大学の研究室向けの会社説明会を実施するほか、
当社主催の勉強会などを実施
認知向上およびプレゼンスの向上を進める

FFRI yarai の販売強化

OEM販売や販売パートナーによる販売の強化
また、純国産製品としての価値を切り口とした
販売を進める

FFRI yarai の独自性/優位性

- 完全な純国産製品
- データが海外に出ない

販売ルート

- OEM販売
- 戦略的販売パートナー
- 販売パートナー

- 官公庁・地方自治体
- 重要インフラ企業
- 一般企業
- 個人・小規模事業者

・純国産製品でデータが完全に国内でのみ処理されるという独自性は、安全保障上の優位性

・これまでの戦略的販売パートナーによる販売やOEM製品の販売は継続して強化を行う

・FFRI yarai を安全保障のツールとして、官公庁や重要インフラ・防衛産業企業などへの販売を進める

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、当社は研究開発部門による新技術の開発や研究成果のカンファレンス等での発表、各種メディアへの情報発信などの取り組みにより、当社製品及びサービスの競争力の維持向上に努めております。 しかし、当社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、当社が競争力を維持することができない場合、当社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

単位：百万円	2023/3	2024/3	YoY
売上高	1,952	2,446	25.3
営業利益 (利益率:%)	202 (10.4)	497 (20.3)	145.3
経常利益 (利益率:%)	247 (12.7)	540 (22.1)	118.6
親会社株主に帰属する当期純利益 (利益率:%)	187 (9.6)	432 (17.7)	130.8
ROE	10.8	22.0	

・安全保障関連の需要増加を取り込んだことにより、ナショナル・セキュリティセクター及びパブリックセクターにおけるセキュリティ・サービスの売上高が前年比で大幅に増加した

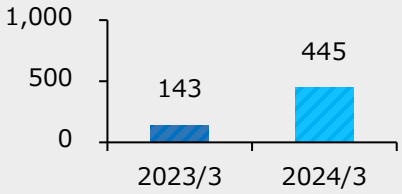
・ソフトウェア開発・テスト事業においても新規顧客の獲得及び単価上昇により前年を上回って推移した

・セキュリティエンジニアを中心に採用を強化
採用費及び人件費が増加したが、売上高の増加でカバー

セグメント・販売区分別の概況(１)

ナショナルセキュリティセクター

単位：百万円



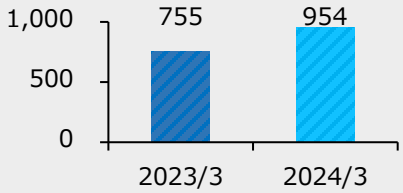
YoY

+301M

+209%

・国家安全保障関連のセキュリティ・サービス案件を受託。
・セキュリティ調査・研究及び教育案件を中心に実施。
・需要の増加に伴い、エンジニアの採用・教育体制の強化を進めている。

パブリックセクター



YoY

+198M

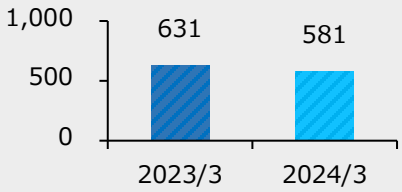
+ 26%

・経済安全保障関連の政府の積極的な取組みにより、
セキュリティ・サービスの需要が増加
・官公庁向けのセキュリティ調査・研究案件を中心に実施。
・NICTの実証事業に参加し、NICTの政府端末向けセキュリティソフトの開発をサポート

セグメント・販売区分別の概況(２)

プライベートセクター

単位：百万円



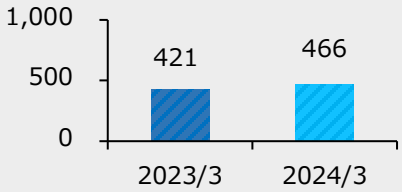
YoY

-50M

- 8%

・プロダクト販売においては、法人向け・個人向けとも、
販売パートナーによるOEM製品の販売が増加
・FFRI yaraiのライセンス数減少によって売上高は前年を下回った。

ソフトウェア開発・テスト事業



YoY

+44M

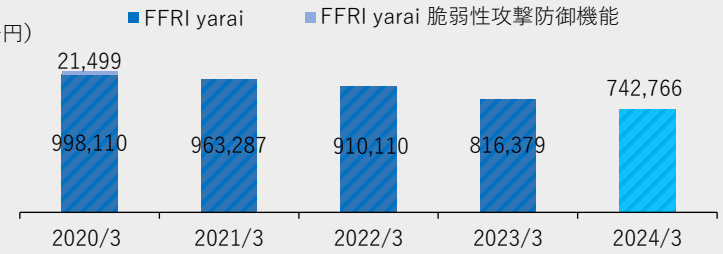
+ 10%

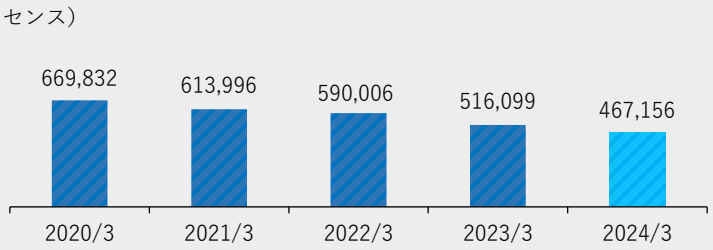
・将来的なセキュリティ・サービスの提供に向けて、セキュリティ教育
を進めている
・業務範囲拡大による単価の上昇や、新規顧客の獲得によって増収となった
※内部取引消去後の売上高となります

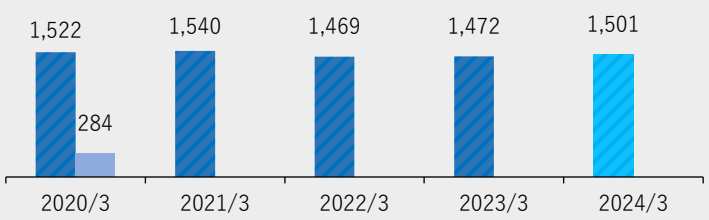
セグメント・販売区分別四半期会計期間毎の売上推移

				2023/3				2024/3			
単位：百万円				1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q
サイバー・セキュリティ事業	ナショナルセキュリティセクター	セキュリティ・プロダクト		0.5	0.5	0.5	0.5	0.4	0.4	0.4	0.4
		セキュリティ・サービス		32.4	31.2	11.3	66.5	92.7	93.3	137.0	120.3
	パブリックセクター	セキュリティ・プロダクト		68.6	68.0	67.0	68.9	61,7	61.0	75.4	68.8
		セキュリティ・サービス		7.0	52.2	128.9	294.7	24.3	104.2	222.4	335.8
	プライベートセクター	セキュリティ・プロダクト	法人	143.4	143.8	135.2	130.6	120.5	123.3	120.9	117.9
			個人	10.8	12.5	13.4	13.7	15.6	16.2	17.4	17.8
		セキュリティ・サービス		13.2	3.3	4.3	6.8	6.4	11.9	9.3	3.4
ソフトウェア開発・テスト事業				104.0	104.0	106.3	107.0	107.6	112.4	120.8	125.4
				380.3	415.9	467.3	689.1	429.6	523.0	703.9	790.1

FFRI yarai シリーズの販売状況







・FFRI yarai 売上高

海外に拠点を持つエンタープライズなどで、グローバルで調達できる製品への乗り換え等があった影響によりFFRI yaraiの売上高は前年同期比で減少となった。

・契約ライセンス数（22/3→23/3継続率87.6％）

第４四半期に一部官公庁・地方自治体における解約があった影響で、前期末に比べ48,943Lic減少となった。

・FFRI yarai 売上単価

特別価格で提供しているアカデミックライセンスの減少などにより、単価は増加傾向

FFRI yarai シリーズの業種別契約ライセンス数

業種	2023/3		2024/3	
	ライセンス	割合(%)	ライセンス	割合(%)
官公庁	231,655	44.9	174,911	37.4
金融サービス	61,978	12.0	49,013	10.5
情報通信	34,345	6.7	47,181	10.1
産業インフラ・サービス	29,534	5.7	24,231	5.2
その他	158,587	30.0	171,820	36.8
合計	516,099	100.0	467,156	100.0

・官公庁：一部官公庁・地方自治体における解約の影響で減少

・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、
様々な業種の企業で広く増加

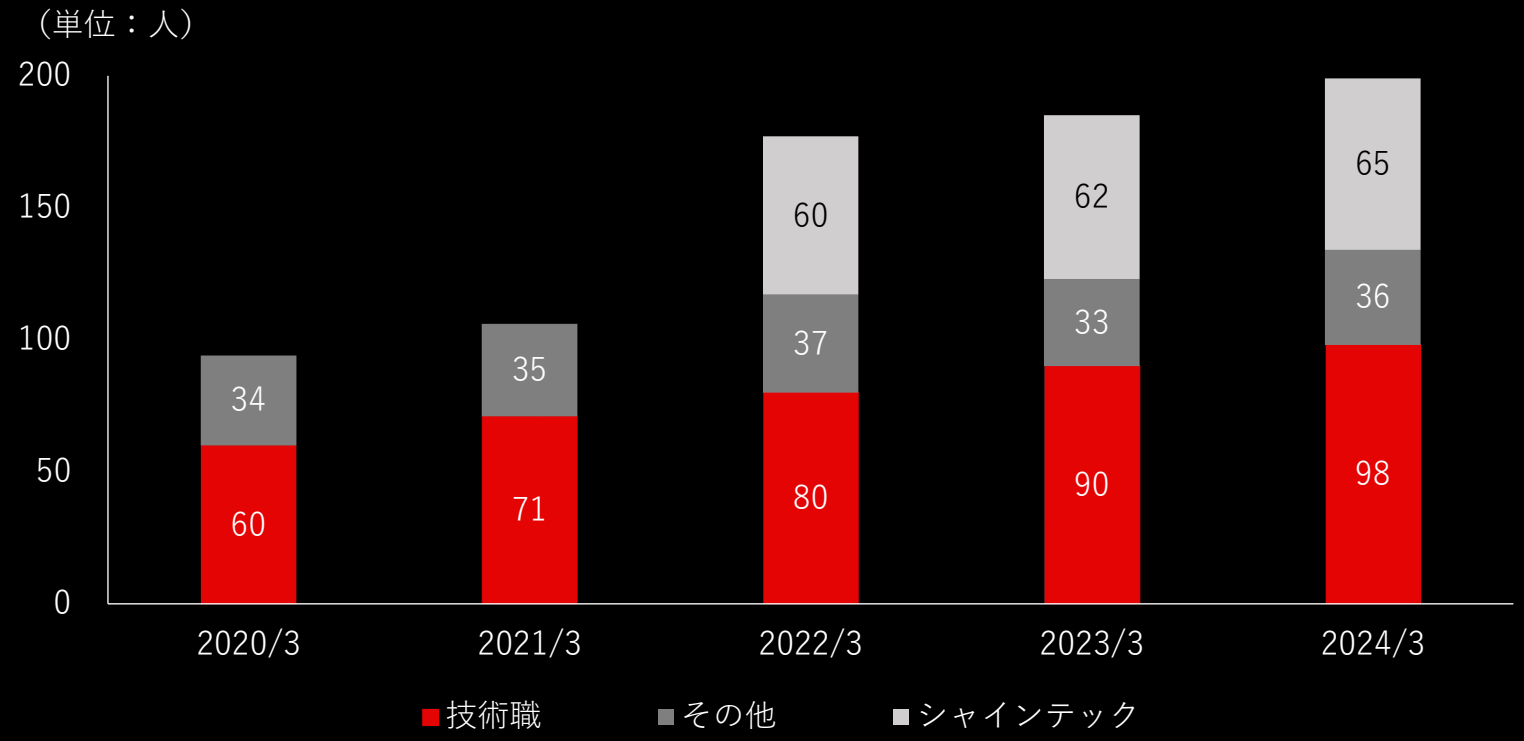
原価及び販売管理費の内訳

単位：百万円	2023/3	2024/3	YoY
労務費	817	925	13.3
経費	222	255	15.0
期首・期末棚卸及び他勘定振替	△255	△275	-
（研究開発費への振替）	△84	△144	-
（ソフトウェアへの振替）	△15	△0	-
（その他の振替）	△54	△131	-
売上原価合計	785	904	15.2
人件費	472	462	△2.1
研究開発費	111	189	70.2
販売手数料	0	0	△31.6
その他	380	392	3.1
販売管理費合計	964	1,044	8.3

・労務費：エンジニアの増加に伴う増加

・研究開発費：FFRI yaraiの機能向上に関する研究の他、安全保障関連のセキュリティ研究開発などを実施

人員数の推移


（単位：人）
200
150
100
50
0
34
60
35
71
60
37
80
62
33
90
65
36
98
2020/3
2021/3
2022/3
2023/3
2024/3
技術職
その他
シャインテック

業績サマリー(B/S)

単位：百万円	2023/3	2024/3	YoY
流動資産	2,115	2,799	32.3
現金及び預金	1,758	2,078	18.2
売掛金	318	671	110.8
固定資産	511	581	13.7
のれん	115	101	-12.1
資産合計	2,627	3,381	28.7
流動負債	868	1,186	36.7
契約負債	706	914	29.5
固定負債	9	12	29.8
負債合計	878	1,199	36.6
株主資本	1,749	2,181	24.7
利益剰余金	1,624	2,056	26.6
純資産合計	1,749	2,181	24.7
負債純資産合計	2,627	3,381	28.7

・売掛金・契約負債

セキュリティ・サービスにおける複数年契約や長期案件の増加による増加

業績サマリー(C/F)

単位：百万円	2023/3	2024/3
営業活動によるキャッシュフロー	302	390
税引前当期純利益	247	540
減価償却費	40	28
売上債権及び契約資産の増減額(△は増加)	△64	△356
契約負債の増減額(△は減少)	80	208
法人税等の支払額	△26	△74
その他	25	44
投資活動によるキャッシュ・フロー	△26	△20
財務活動によるキャッシュ・フロー	△161	△50
現金及び現金同等物の期末残高	1,758	2,078

・営業活動によるキャッシュ・フロー

売上債権及び契約資産の増加

セキュリティ・サービスの案件増加によるもの

・財務活動によるキャッシュ・フロー

2023年３月期は自己株式の取得によるもの

2024年３月期の主な取組み

2024年３月期の主な取り組み

ナショナルセキュリティ事業本部
の規模拡大

2024年3月末時点／38名
（前期末比　＋9名）

教育プログラムによって早期の戦力化

採用

研修（３～６ヶ月）

戦力化

・増大する需要を取り込むため、優秀なエンジニアの
採用・育成体制を強化

・サイバー攻撃技術の研究から防御技術を開発する
ＦＦＲＩにしかできない価値を市場に提供する

・採用の強化、組織体制の整備を進め、
ナショナルセキュリティ事業本部の規模を拡大

NICTの実証事業への参加

安全性・透明性の検証が可能な
政府端末向けセキュリティソフト
をNICTが開発

NECと共に
開発の技術的な支援

政府端末に導入し、
マルウェア情報等を収集・分析

・国立研究開発法人 情報通信研究機構(NICT)の
推進する実証事業に参加

・NICTの行う 政府端末向けセキュリティソフトの
開発をNECと共にサポート

・政府端末向けセキュリティソフトは段階的に
政府端末に導入予定

2024年３月期のその他の取り組み

販売パートナー各社との連携強化
FFRI yaraiの販売拡大施策を推進

・国産製品の強みを活かして、官公庁への販売施策を進める
・FFRI yaraiの機能強化を継続
・戦略的販売パートナーとの連携強化を継続

株式会社シャインテックの人材育成

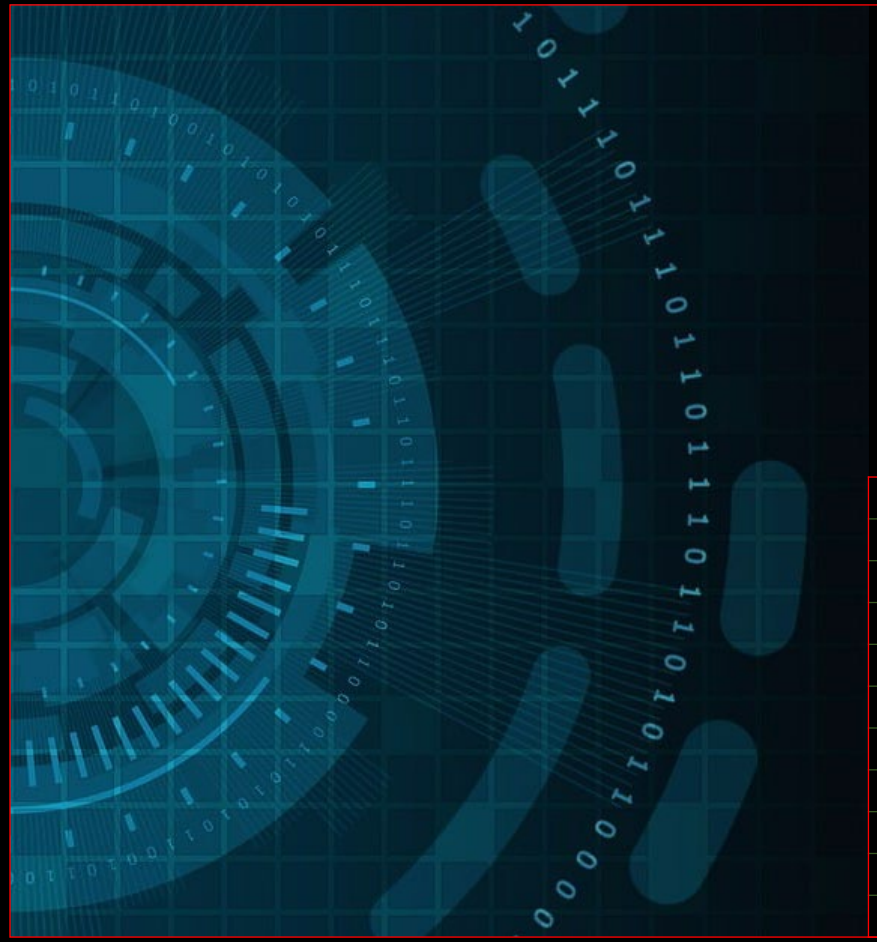
・堅調な品質保証・テスト業務等は継続
・将来的なセキュリティ・サービスの提供を目指し、ＦＦＲＩセキュリティの教育メソッドを活用したセキュリティ技術のトレーニングを実施

多様なセキュリティ・サービスのノウハウを蓄積

・ＦＦＲＩセキュリティ マネージド・サービスやサービスの案件、研究開発を通じて様々なノウハウを獲得・蓄積を進めている
・多様化するニーズに応えられる体制を構築する

エヌ・エフ・ラボラトリーズ
（エヌ・ティ・ティ・コミュニケーションズとの合弁会社）

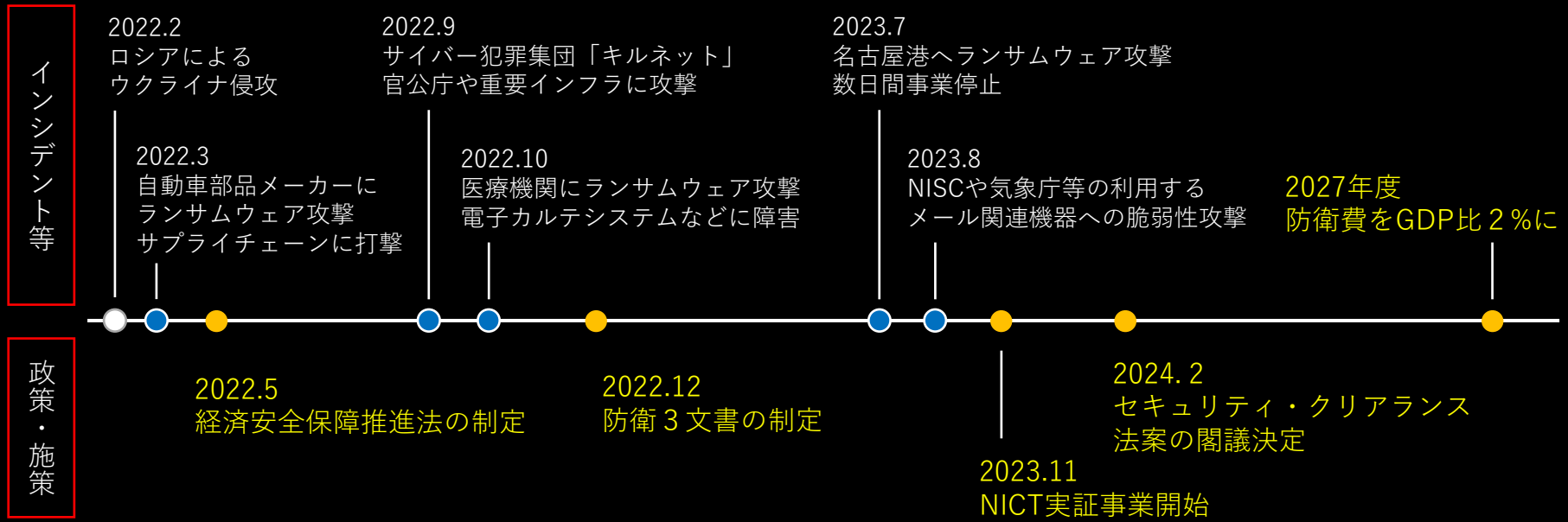
・国内で人材不足となっている「高度セキュリティ人材」の育成および輩出を推進
・教育研修事業などを中心に需要増加に対応するため人材の採用・育成を進めている



2025年３月期の主な取り組み

市場の状況

- 世界各国で重要インフラや政府組織を狙ったサイバー攻撃が増加している
- サイバー領域における安全保障関連の施策もかつてない速度で進む



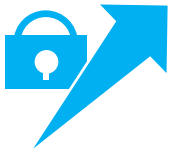
※内閣サイバーセキュリティセンター「重要インフラを取り巻く情勢について」より抜粋

市場の状況

政府の取り組みも一層加速し、
安全保障関連の需要増加が続く

防衛省 2024年度予算は
約7.7兆円（歳出ベース）

2027年に防衛費をGDP比２％に
増額、サイバー専門部隊4000人、
サイバー要員２万人規模まで拡大



防衛力そのものである
防衛生産・技術基盤の体制整備

防衛産業におけるサイバーセ
キュリティ対策事業を実施

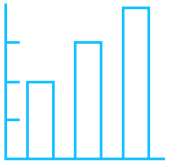
・2024年度の防衛省予算は７兆円を超えるなど、
防衛力強化を図る政府方針を反映し大幅に増加

・「防衛生産・技術基盤は、いわば防衛力そのもの」
（国家防衛戦略/防衛省 2022年12月）
と位置付け、力強く持続可能な防衛産業の構築を進める

・防衛省と契約関係にある企業の防衛部門のみならず、
下請け企業に対しても総合的・一体的なサイバー
セキュリティ対策を実施
（令和６年度予算の概要/防衛省 2024年3月）

2025年３月期の主な取り組み

需要の増加を取り込めるだけの人材を確保するため、採用力の更なる強化



国内の人材市場においては、
セキュリティ人材の不足が顕著

様々な企業で人材の取り合い
となっている

新卒採用の待遇向上

企業としてのプレゼンスの向上
による採用力の強化を実施

・採用力の強化のため新卒採用の待遇（給与）を向上

・ＦＦＲＩセキュリティのプレゼンス向上のため
大学の研究室向けの会社説明会を実施するほか、
当社主催の勉強会などを実施

2025年３月期の主な取り組み

販売パートナー各社との連携強化
FFRI yaraiの販売拡大施策を推進

- 戦略的販売パートナーとの連携強化を継続
- FFRI yaraiの機能強化を継続
- 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進める

株式会社シャインテックの人材育成

- 堅調な品質保証・テスト業務等は継続
- 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

エヌ・ティ・ティ・コミュニケーションズ株式会社との合弁会社である
エヌ・エフ・ラボラトリーズにおける
人材の育成と排出

- 国内で人材不足となっている「高度セキュリティ人材」の育成および輩出を推進
- 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

株主還元（配当）

配当予想	2024年3月期	2025年3月期（予想）
親会社株主に帰属する当期純利益(百万円)	432百万円	433百万円
1株当たりの当期純利益	54.64円	54.76円
１株当たりの配当金（期末）	10.00円	10.00円
配当性向	18.3%	18.3%

・活発な事業環境を踏まえ、株主の皆様に対する継続的な利益還元の実施が可能であるとの判断のもと、剰余金の配当開始を決定

・今後も株主の皆様への安定的かつ継続的な利益還元を目標とする

連結業績予想

単位：百万円	2024/3 （実績）	2025/3 （予想）	YoY
売上高	2,446	3,158	29.1
営業利益 （利益率:%）	497 （20.3）	515 （16.3）	3.6
経常利益 （利益率:%）	540 （22.1）	541 （17.2）	0.1
親会社株主に帰属する四半期純利益 （利益率:%）	432 （17.7）	433 （13.7）	0.2
ROE (%)	22.0	20.6	

・安全保障関連の案件増加を着実に取り込み、
ナショナル・セキュリティセクター及び、
パブリックセクターにおける売上高の増加を見込む

・中長期に渡る需要の増加を取り込むため、引き続き
積極的な採用活動およびプレゼンスの向上を推進するため、
採用コストおよび人件費の増加を見込む

連結業績予想(売上高の内訳)

単位：百万円	2024/3 (実績)	2025/3 (予想)	YoY
サイバー・セキュリティ事業	1,980	2,662	34.4
ナショナル セキュリティ セクター	445	1,102	147.5
パブリック セクター	954	1,010	5.9
プライベート セクター	581	549	△5.5
ソフトウェア開発・ テスト事業	466	496	6.4
合計	2,446	3,158	29.1

・サイバー安全保障関連の需要を取り込み、
ナショナル・セキュリティセクター及びパブリックセクターが
成長する見込み

中期経営計画(2025年３月期～2027年３月期)

単位：百万円	修正後計画（2024.5.14公開） 2025/3（予想）	2026/3（計画）	2027/3（計画）	当初計画(2023.5.15公開) 2025/3（計画）	2026/3（計画）
売上高	3,158	3,765	4,479	2,789	3,080
営業利益 (利益率:%)	515 (16.3)	663 (17.6)	844 (18.8)	406 (14.6)	491 (16.0)
経常利益 (利益率:%)	541 (17.2)	689 (18.3)	870 (19.4)	434 (15.6)	519 (16.9)
親会社株主に帰属する当期純利益 (利益率:%)	433 (13.7)	480 (12.8)	606 (13.5)	304 (10.9)	363 (11.8)

・好調な事業環境を元に、
中期経営計画をローリング

・足元のサイバー安全保障関連の需要を
確実に取り込み、成長のドライバーとする

・将来に渡る需要の増加に備え、エンジニア
を中心とした採用活動の強化を進めるため
利益率は横ばいとなる計画

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。