事業計画及び成長可能性に関する説明資料

2023.6.30

株式会社ＦＦＲＩセキュリティ

（東証グロース：3692） https://www.ffri.jp

1．会社概要
2．事業環境
3．事業内容・強み
4．成長戦略
5．事業等のリスク
6．業績サマリ

1. 会社概要
2. 事業環境
3. 事業内容・強み
4. 成長戦略
5. 事業等のリスク
6. 業績サマリ

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）	松本　勉
	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）	山口　功作
	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）	平山　孝雄
	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		
	取締役（常勤監査等委員）	原澤　一彦		
設立：	2007年7月3日			
資本金：	286,136,500円（2023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

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

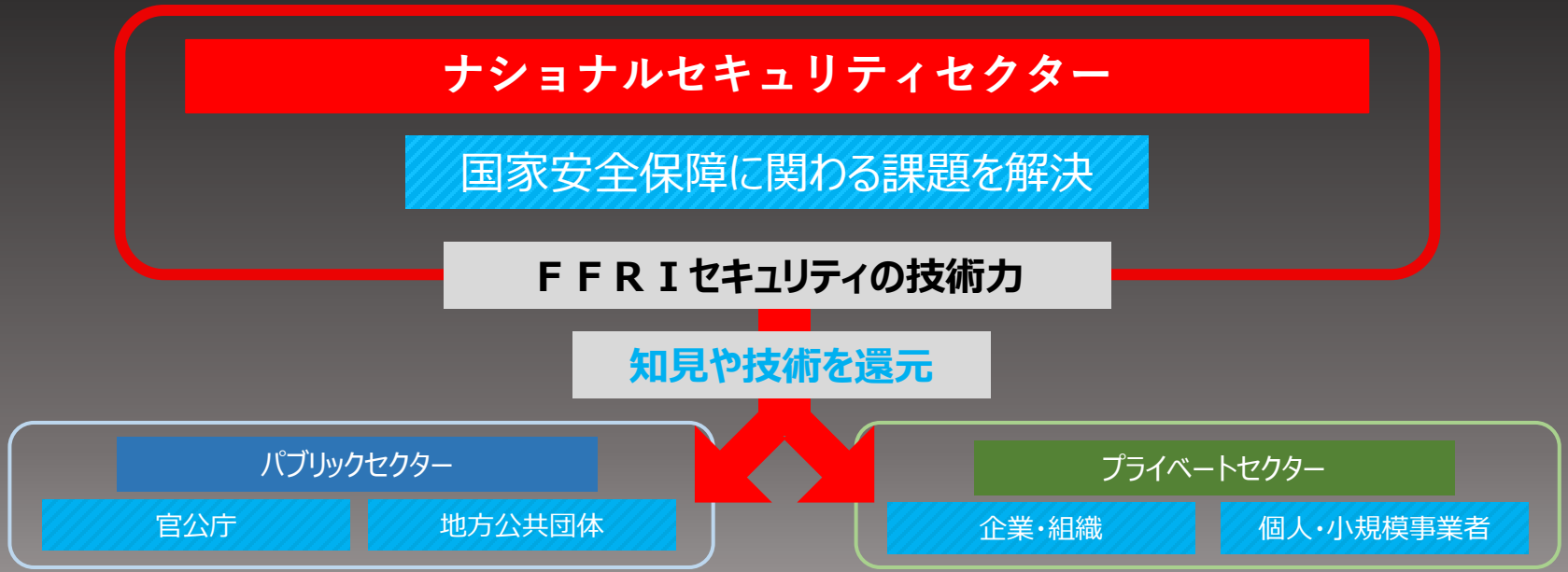
コーポレートマークにも「1440」の文字とスノーボードの回転をイメージした矢印で、設立当初から変わらない「未踏の分野への挑戦」を表現

コーポレートマーク

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セキュリティが目指す姿

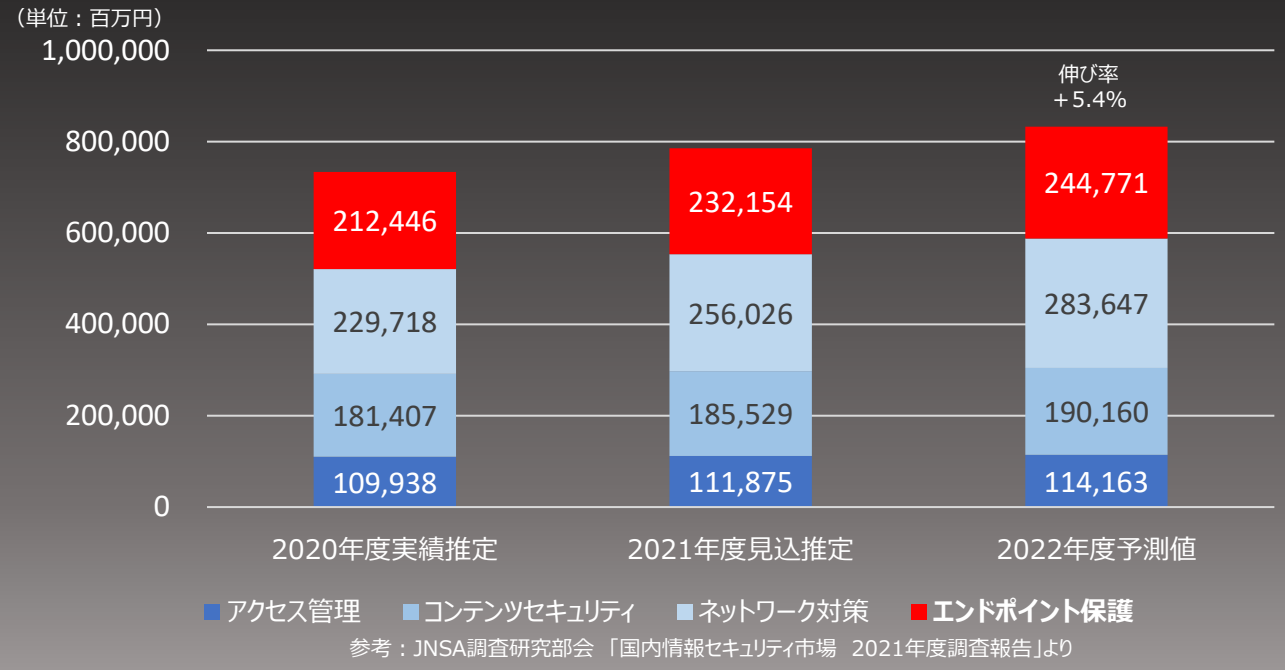
- 実現困難な課題を突破する技術力をコアに、日本発の研究開発型サイバーセキュリティ企業として
  国家や企業・組織、個人が抱える課題を解決するソリューションを提供する



1. 会社概要
2. 事業環境
3. 事業内容・強み
4. 成長戦略
5. 事業等のリスク
6. 業績サマリ

事業環境　セキュリティ・プロダクト市場

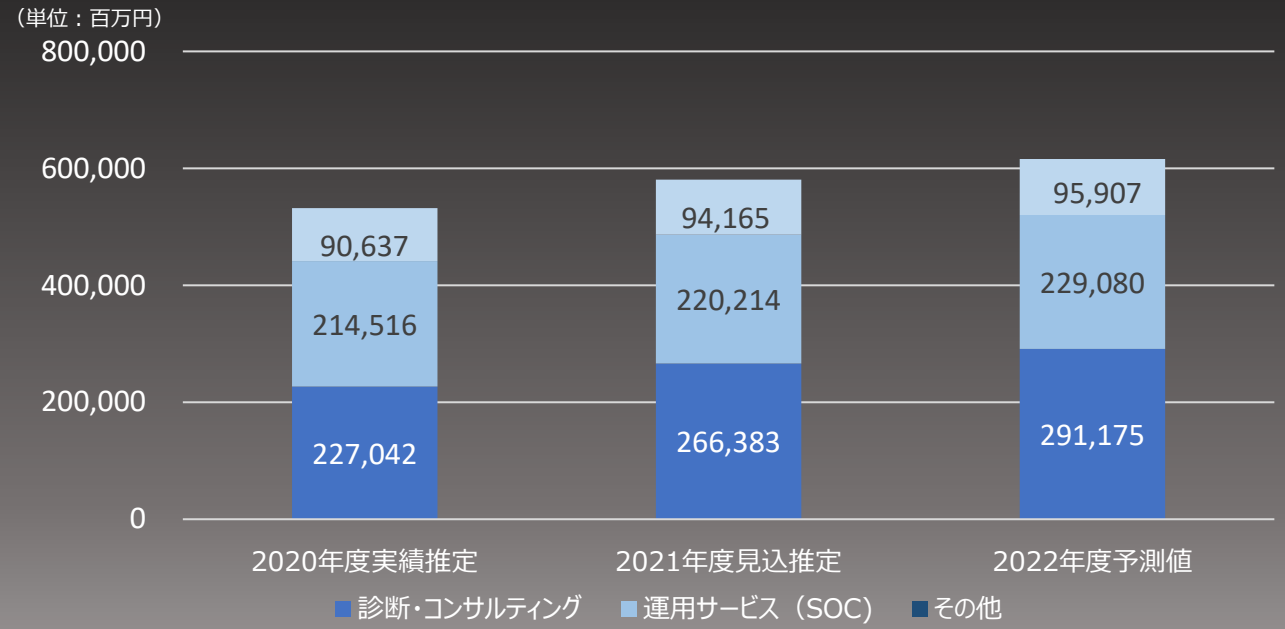
当社製品 FFRI yarai はエンドポイント保護製品に分類
国内市場はサイバー攻撃による被害の増加や、テレワークやDXの推進を受けて年々拡大している



参考：JNSA調査研究部会「国内情報セキュリティ市場　2021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　2021年度調査報告」より

事業環境　ナショナルセキュリティセクター

当社はサイバー領域における国家安全保障分野（ナショナルセキュリティセクター）へ注力している
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いる

事業環境　ナショナルセキュリティセクター

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

事業環境　ナショナルセキュリティセクター

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)

日本が抱える課題と政府の取り組み

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

※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

日本が抱える課題と政府の取り組み

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

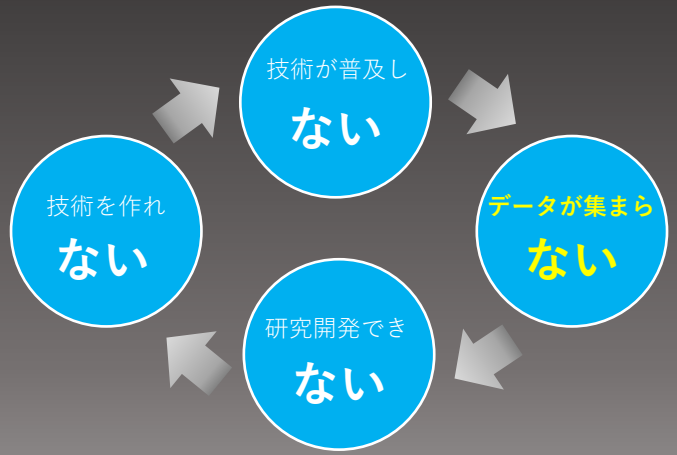
脅威情報を海外事業者から購入している

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）

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）

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

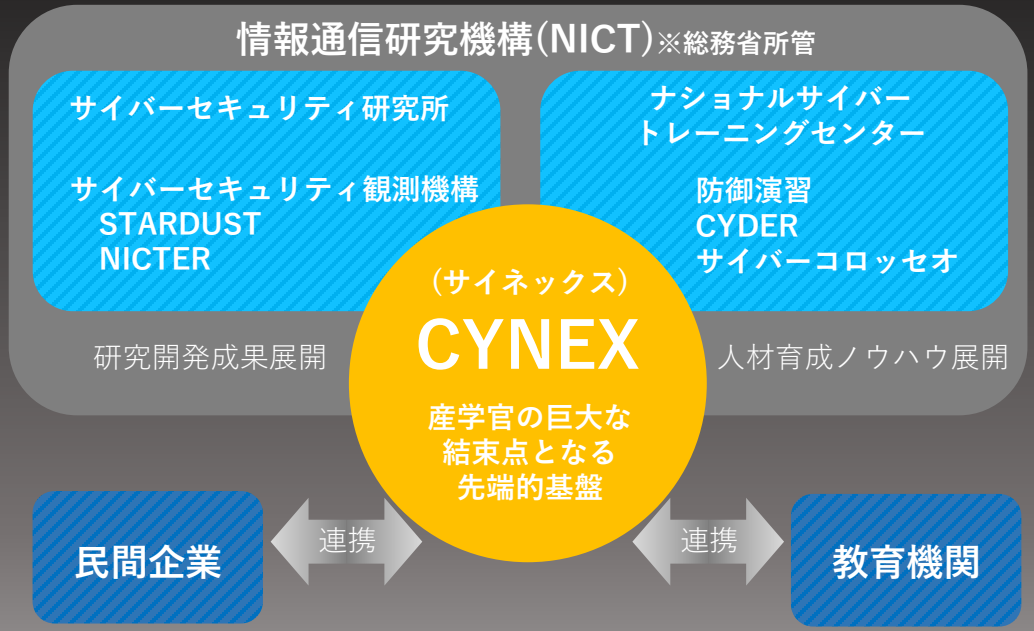
国内のサイバーセキュリティ産業育成を後押しする CYNEX を設立し、データ負けのスパイラル脱却を図る

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

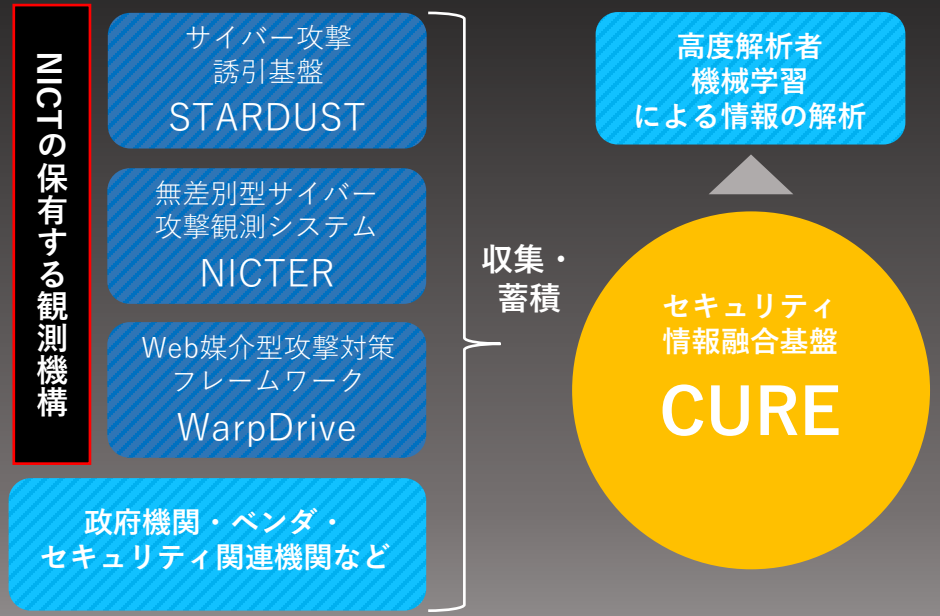
母体組織であるNICTの研究成果やサービスの一部を産学に半開放



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。



純国産サイバーセキュリティ情報を生成し、データ負けのスパイラルから脱却する

実データを用いて、

国産製品の長期運用・検証を実施

国産セキュリティ製品の運用・検証を行い、
その結果をレポーティング
国内産業の育成を進める

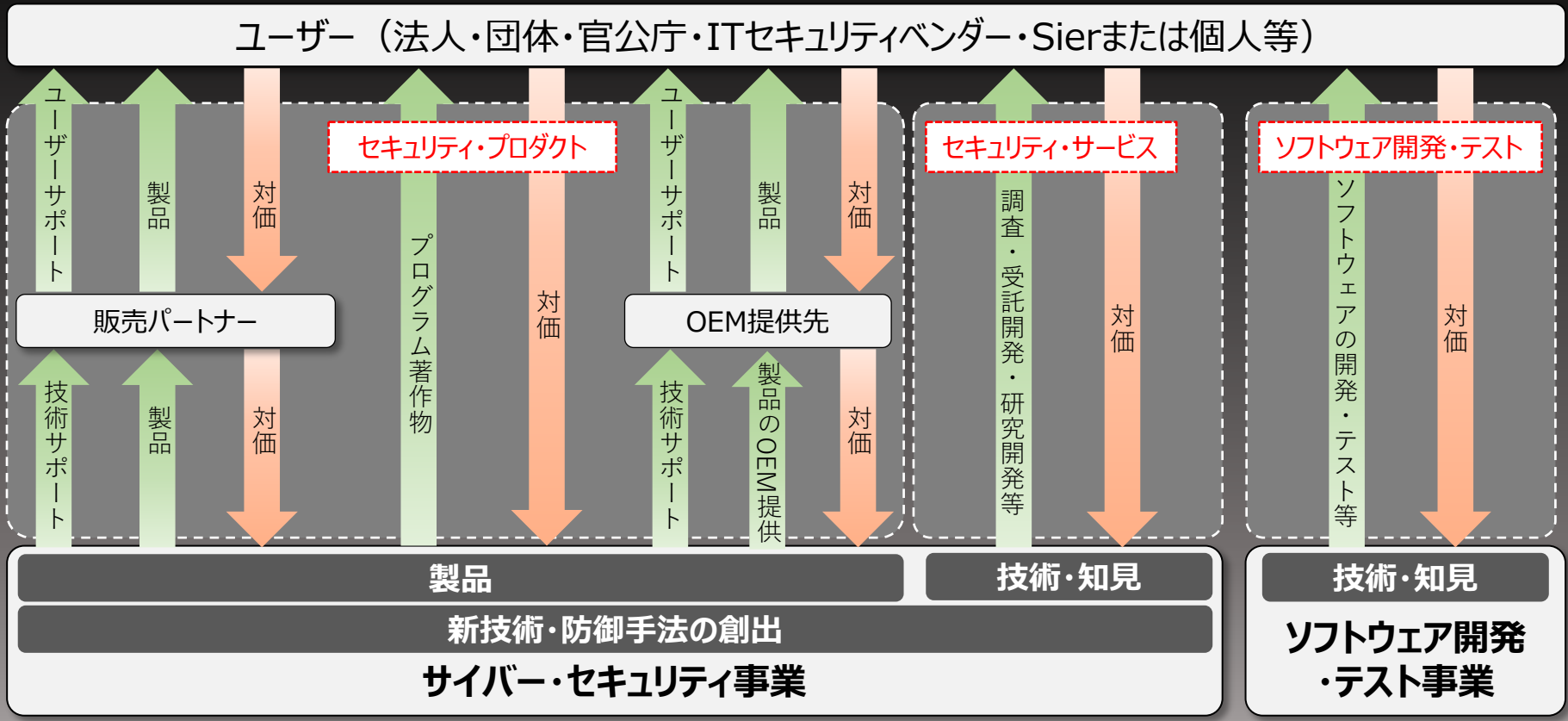
純国産サイバーセキュリティ情報の生成

明確な情報源から説明可能性の高い、
純国産インディケータ情報を生成

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)

1. 会社概要
2. 事業環境
3. 事業内容・強み
4. 成長戦略
5. 事業等のリスク
6. 業績サマリ

事業モデル


ユーザー（法人・団体・官公庁・ITセキュリティベンダー・Sierまたは個人等）
セキュリティ・プロダクト
セキュリティ・サービス
ソフトウェア開発・テスト
ユーザーサポート
製品
対価
販売パートナー
技術サポート
製品
対価
プログラム著作物
対価
ユーザーサポート
製品
対価
OEM提供先
技術サポート
製品のOEM提供
対価
調査・受託開発・研究開発等
対価
ソフトウェアの開発・テスト等
対価
製品
技術・知見
新技術・防御手法の創出
サイバー・セキュリティ事業
技術・知見
ソフトウェア開発・テスト事業

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。

当社プロダクトの分類

サイバー・セキュリティ対策の中で、FFRI yaraiはエンドポイント対策製品に分類される

サイバーセキュリティ対策市場

人的対策

セキュリティ
教育・研修
セミナー
　など

物理的対策

防犯カメラ
デスク・
オフィスの施錠
入退室管理
　など

技術的対策

ネットワーク

ファイアウォール
IDS・IPS
WAF
SSL通信　など

エンドポイント

競合環境

当社製品「FFRI yarai」及び「FFRI yarai Home and Business Edition」は
未知脅威対策（NGEPP）およびEDRに分類。標的型攻撃や、ゼロデイ攻撃などの未知の脅威対策
としての優位性を持つ。

エンドポイント対策

感染未然防止

既知脅威対策

パターンマッチング技術

国内ベンダー
海外ベンダー
など

未知脅威対策（NGEPP/NGAV）

ＦＦＲＩセキュリティ
ふるまい検知・
プログレッシブ・ヒューリスティック技術

海外ベンダー など

可視化

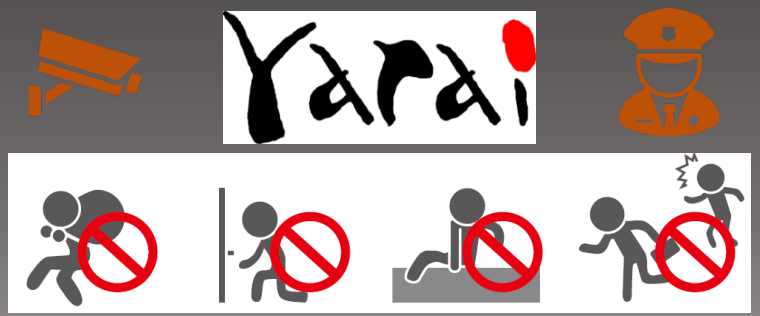
・EDR製品

海外ベンダー
など

FFRI yarai の強み

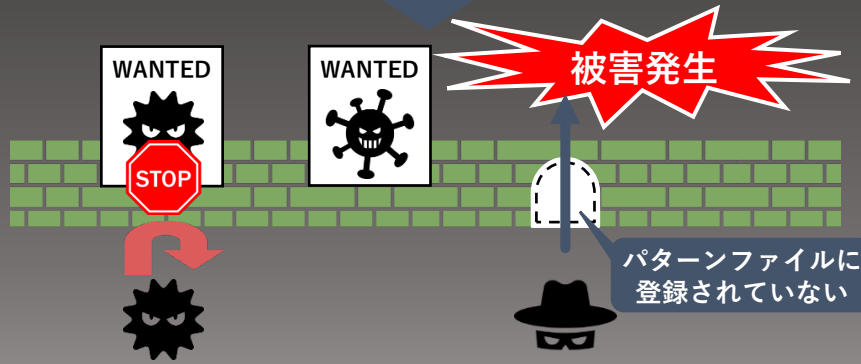
パターンマッチング型製品は、パターンファイルに登録されていない未知のマルウェアを防ぐ事ができない
FFRI yaraiは振る舞い検知技術により、マルウェア特有の怪しい振る舞いを検知するため、標的型攻撃などの未知のマルウェアを使用した攻撃も防御することができる。

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

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

FFRI yarai 独自のプログレッシブ・ヒューリスティックエンジン

振る舞い検知技術を使用した独自開発の５つの検出エンジンで、
多角的にプログラムを監視し、未知の脅威をブロックする

アプリケーションを脆弱性攻撃から守る

ZDPエンジン

マルウェアを検出する

Static分析エンジン

Sandboxエンジン

HIPSエンジン

機械学習エンジン

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」

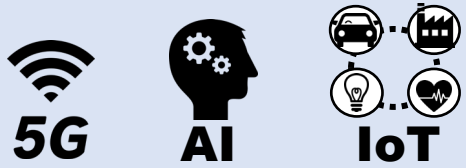
主要なセキュリティ・サービス

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。

セキュリティ・サービスの強み

国内の他ベンダーが提供できていない分野を中心に、高度セキュリティ領域のサービスを提供
技術力を活かし、IoT機器やAIなどの先端技術領域のセキュリティ調査なども提供

先端技術領域 セキュリティ分析・診断

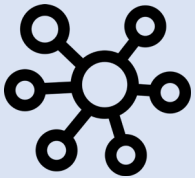


IoT機器や５Gネットワーク、AIシステムの脅威分析や、バックドア検出などのセキュリティ検査を提供します。

高度セキュリティ 技術者トレーニング

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を提供します。

サイバーインテリジェンスの提供



日本を標的としたマルウェアのIoC情報提供や、セキュリティ・コンサルティング、インシデントの対応相談などを提供します。

ソフトウェア開発・テスト事業

子会社のシャインテック社よりソフトウェアの企画・開発、テストのサービスを提供
将来的に当社の持つセキュリティ技術を組み合わせた幅広いサービスの提供を目指しており、
セキュリティ教育を進めている

Shine Tec

（株式会社シャインテック）

事業内容

ソフトウェアのテスト
ソフトウェアの企画・開発
など

＋

FFRI

当社のもつセキュリティ技術を
組み合わせ、より付加価値の
高いサービスを提供する

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

1. 会社概要
2. 事業環境
3. 事業内容・強み
4. 成長戦略
5. 事業等のリスク
6. 業績サマリ

成長実現における２つの柱

1 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を成長のドライバーとする

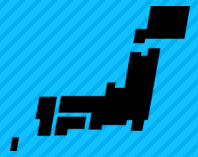
2 販売パートナーとの協業によるプロダクト販売の拡大

安全保障関連の需要の増加

国際社会の緊張を背景に、政府の進める安全保障の取組も急速な進展を見せており、
国産技術の発展や、国内産業育成に向けた様々な取組がスタートしている

安全保障実現に向けた政府の取組

サイバーセキュリティ自給率の向上



産学官の連携を振興し、研究開発の充実を図ることで国内産業の育成と発展を推進する

参考：経済財政運営と改革の基本方針2021
次期サイバーセキュリティ戦略

国内産業を育成し、データ負けのスパイラル脱却

産業育成を後押しするCYNEXを設立。
国産製品の運用・検証を行い、国内産業の育成を支援する

参考：「サイバーセキュリティ統合知的・人材育成基盤（CYNEX）」の構築（総務省）

サイバー領域における国家安全保障及び経済安全保障能力の強化

人員拡大や組織体制の整備が進むほか、国内サイバーセキュリティ産業の成長を後押し

参考：経済安全保障推進法
国家安全保障戦略

ＦＦＲＩセキュリティが果たすべき役割

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となっており、
純国産技術の発展や、サイバー領域における安全保障の実現に向けて当社の果たすべき役割は大きい

当社事業の特徴

国内でほぼ唯一、セキュリティコア技術の研究開発を行う

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

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

将来発生しうるサイバー攻撃を予測し、その技術を研究することで防御技術を開発する手法をとっている

ＦＦＲＩセキュリティが果たすべき役割

安全保障関連の取組の加速によって需要が増大するナショナルセキュリティへの注力を一層強め、
安全保障の実現へと貢献するとともに、当社事業成長のドライバーとする

ナショナルセキュリティへの注力

安全保障関連の需要増加

緊張感の増す国際情勢や政府が進める積極的なサイバーセキュリティへの取り組みを背景に、需要のさらなる増大が見込まれる

政府と一体となった取り組み

政府分科会（※）などの活動を通じて、安全保障の実現に向けて政府と一体になって取り組んでいる。

※参加組織の一例
サイバーセキュリティタスクフォース(総務省)
研究開発戦略専門調査会（NISC）
産業サイバーセキュリティ研究会WG3(経済産業省)
など

当社体制も強化中

エンジニアのリソースをナショナル・セキュリティに集中。採用体制も強化し、さらなる需要増加を取り込む体制を構築している

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、ナショナルセキュリティを支える

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

セキュリティエンジニアの採用及び育成を進める

- 国家安全保障・経済安全保障関連の政府の取り組みが加速し、さらなる需要の増加が見込まれる
- 増大する需要を取り込むため、優秀なエンジニアの採用・育成を継続する
- 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

ナショナルセキュリティセクターの規模拡大

2022年3月期末時点

少数精鋭

10名未満

2023年3月期末時点

研究開発第一部

研究開発第二部

基礎技術研究部

合計　約３０名に増員

2024年3月期末目標

エンジニア40名規模まで拡大

・安全保障関連のサービス案件が増加
・エンジニアの増員が増収に直結する状況であり、採用活動の強化、人材の早期戦力化を進める

販売パートナーとの協業によるプロダクト販売の拡大

官公庁や地方自治体、個人・小規模事業者など、各顧客層に対して販売力のある販売パートナーと協力し、OEM製品やマネージド・サービスの提供による販売の拡大を進める

官公庁・地方自治体	個人・小規模事業者
Soliton® NEC NTT AT TKC Sky	SOURCENEXT® ALEXON 株式会社 No.1

OEM提供や、共同研究、販促活動など緊密な連携を構築

1. 会社概要
2. 事業環境
3. 事業内容・強み
4. 成長戦略
5. 事業等のリスク
6. 業績サマリ

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。

1. 会社概要
2. 事業環境
3. 事業内容・強み
4. 成長戦略
5. 事業等のリスク
6. 業績サマリ

業績サマリー

- 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いては、安全保障関連のセキュリティ・サービス案件が増加
- セキュリティエンジニアを中心とした採用強化を継続したことにより、採用費及び人件費のコストが前年比で増加
- 安心アプリチェッカーの販売終了により、プライベートセクターの売上高が減少したが、利益面への影響は軽微

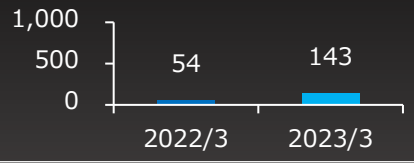
単位：百万円	2022/3 (連結)	2023/3 (連結)	YoY
売上高	1,779	1,952	9.7%
営業利益(利益率:%)	103 (5.8)	202 (10.4)	96.2%
経常利益(利益率:%)	156 (8.8)	247 (12.7)	58.4%
親会社株主に帰属する 当期純利益(利益率:%)	120 (6.8)	187 (9.6)	54.8%

セグメント・販売区分別の概況

売上高（単位：百万円）

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

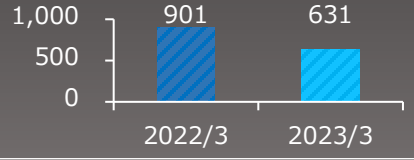


・国家安全保障関連のセキュリティ・サービス案件を受託。
・セキュリティ調査・研究及び教育案件を中心に実施。
・需要の増加に伴い、エンジニアを大幅に増員。

パブリックセクター

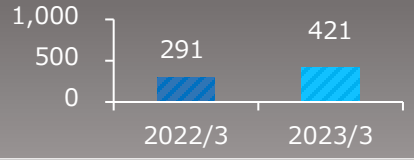
・官公庁向けのセキュリティ調査・研究案件を中心にサービス案件が増加。
・デジタル化が進む地方自治体への販売に強みを持つ販売パートナーと連携し、OEM製品やマネージドサービスなどを提供。協力して販売拡大施策を進めている。

プライベートセクター



・Android向けアプリ「安心アプリチェッカー」の販売が2022年3月末をもって終了したため売上高が減少しているものの、OEM製品の個人・小規模事業者向け販売は増加

ソフトウェア開発・テスト事業



・シャインテック社において、テスト業務等を中心に提供
・将来的なセキュリティ・サービスの提供に向けた教育体制整備など準備を進めた

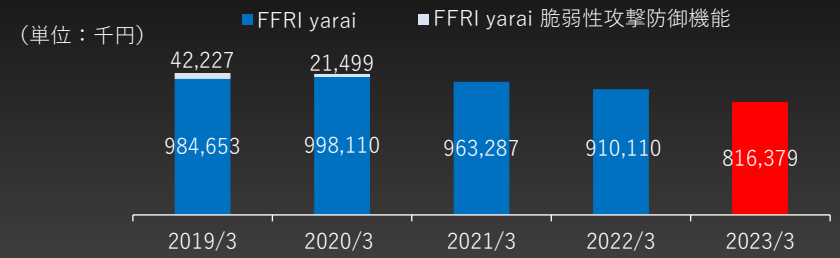
※内部取引消去後の売上高となります
※シャインテック社の業績は2022年3月期第２四半期より連結しております

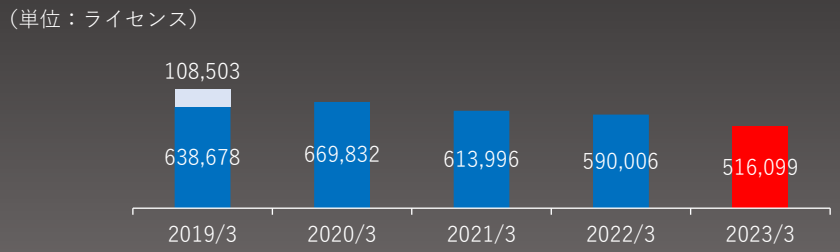
セグメント・販売区分別 四半期会計期間毎の売上推移

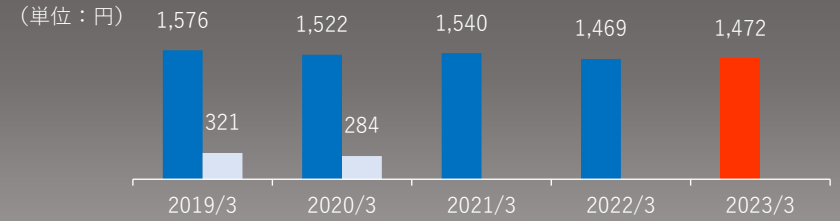
※内部取引の消去後の売上高となります

			2022/3				2023/3			
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	1.3	1.3	0.4	0.4	0.5	0.5	0.5	0.5
		セキュリティ・サービス	13.4	9.6	5.0	22.6	32.4	31.2	11.3	66.5
	パブリックセクター	セキュリティ・プロダクト	78.5	78.7	79.4	73.1	68.6	68.0	67.0	68.9
		セキュリティ・サービス	6.4	21.4	78.6	115.1	7.0	52.2	128.9	294.7
	プライベートセクター	セキュリティ・プロダクト 法人	156.9	157.6	150.6	146.4	143.4	143.8	135.2	130.6
		セキュリティ・プロダクト 個人	64.2	60.9	60.5	59.7	10.8	12.5	13.4	13.7
		セキュリティ・サービス	4.7	14.4	6.9	18.4	13.2	3.3	4.3	6.8
ソフトウェア開発・テスト事業			-	97.8	98.5	95.1	104.0	104.0	106.3	107.0
		合計	325.7	442.1	480.0	531.1	380.3	415.9	467.3	689.1

FFRI yarai シリーズの販売状況







- FFRI yarai 売上高

  グローバルで使用できる製品への乗り換えや、ユーザー企業のシステム入れ替えに伴う契約満了などにより、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%）

  前期末に比べ73,907Lic減少となった。現在、販売パートナーによるOEM製品やマネージドサービスの販売活動の他、純国産製品である強みを活かし、官公庁を中心に積極的な提案活動を進めている

- 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、単価は微増となった

FFRI yarai シリーズの業種別契約ライセンス数

業種	2022/3		2023/3	
	ライセンス	割合(%)	ライセンス	割合(%)
官公庁	245,477	41.6	231,655	44.9
金融サービス	97,995	16.6	61,978	12.0
運輸	36,738	6.2	3,503	0.7
情報通信	40,056	6.8	34,345	6.7
産業インフラ・サービス	32,012	5.4	29,534	5.7
その他	137,728	23.3	155,084	30.0
合計	590,006	100.0	516,099	100.0

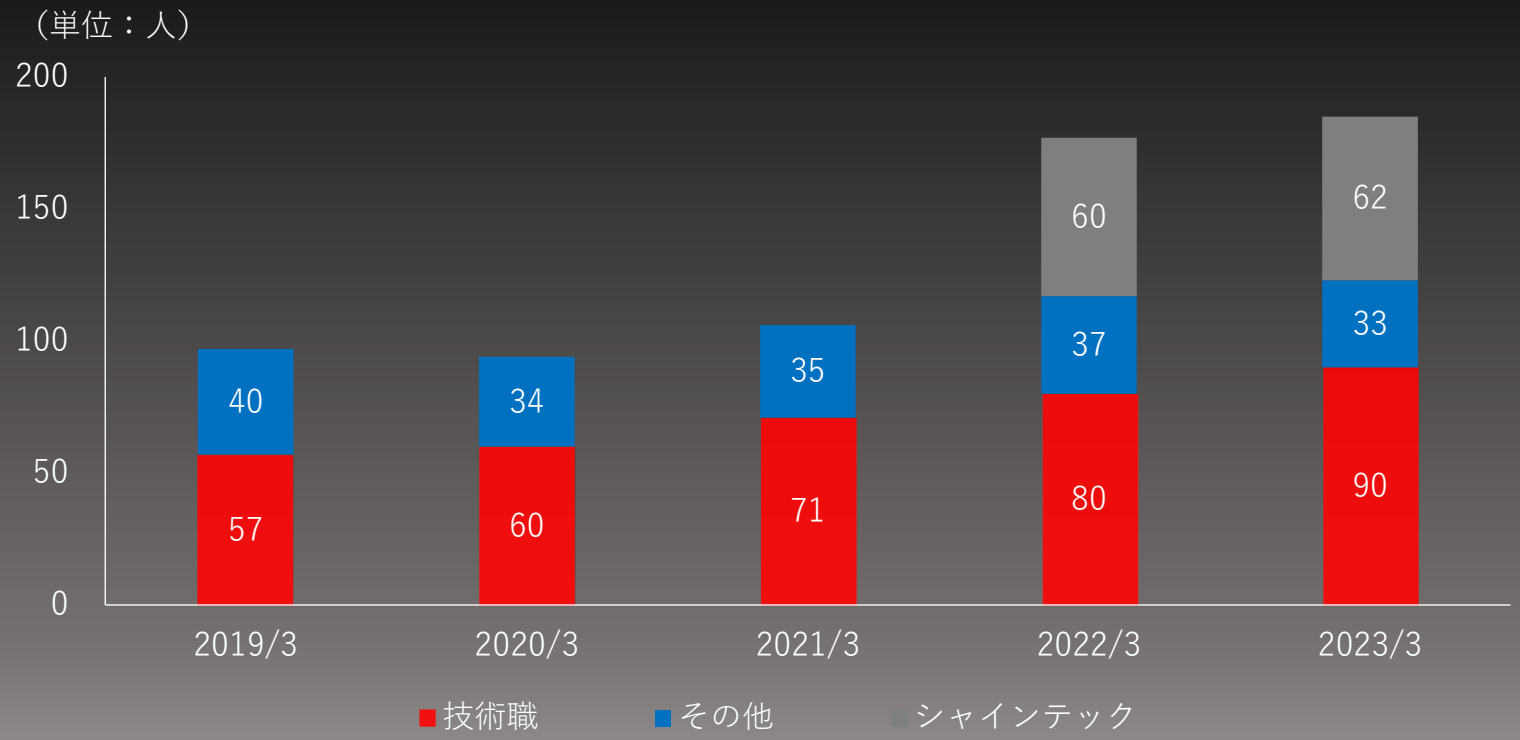
原価及び販管費の内訳

単位：百万円

	2022/3（連結）	2023/3（連結）	増減比（%）
労務費	620	817	31.8
経費	146	222	51.4
期首・期末棚卸及び他勘定振替	△213	△255	-
（研究開発費への振替）	△104	△84	-
（ソフトウェアへの振替）	△12	△15	-
（その他の振替）	△96	△154	-
売上原価合計	553	785	41.9
人件費	469	472	0.5
研究開発費	138	111	△19.5
販売手数料	167	0	△99.7
その他	346	380	9.9
販売管理費合計	1,122	964	△14.1

- 労務費：エンジニアなど人員の増加及び、シャインテック社の連結開始に伴う増加
  ※シャインテック社は2022年3月期第２四半期より連結を開始しています。
- 販売手数料：FFRI安心アプリチェッカーの販売終了に伴い、販売代理店に対する販売手数料の支払いがなくなったため

人員数の推移


（単位：人）
200
150
100
50
0
40
34
35
37
33
57
60
71
80
90
60
62
2019/3
2020/3
2021/3
2022/3
2023/3
技術職
その他
シャインテック

業績サマリー（貸借対照表）

単位：百万円	2022/3 (連結)	2023/3 (連結)	増減比 (%)
流動資産	1,952	2,115	8.4
現金及び預金	1,644	1,758	7.0
売掛金	253	318	25.6
固定資産	501	511	2.0
のれん	129	115	△10.8
資産合計	2,453	2,627	7.1
流動負債	720	868	20.5
契約負債	625	706	12.9
固定負債	9	9	0.4
負債合計	730	878	20.3
株主資本	1,723	1,749	1.5
利益剰余金	1,437	1,624	13.0
純資産合計	1,723	1,749	1.5
負債純資産合計	2,453	2,627	7.1

業績サマリー（キャッシュ・フロー）

単位：百万円	2022/3（連結）	2023/3（連結）
営業活動によるキャッシュフロー	△16	302
税引前当期純利益	156	247
減価償却費	42	40
売上債権の増減額(△は減少)	39	△64
契約負債の増減額(△は減少)	△59	80
法人税等の支払額	△83	△26
その他	△112	25
投資活動によるキャッシュ・フロー	△157	△26
財務活動によるキャッシュ・フロー	△275	△161
現金及び現金同等物の期末残高	1,644	1,758

- 財務活動によるキャッシュ・フロー：
  自己株式の取得によるもの
  （取得価額の総額）
  2023年3月期　161,407,700円
  2022年3月期　260,494,000円

2023年３月期の主な取組み

ナショナルセキュリティセクターにおける取り組み

- 組織体制を整備し、ナショナルセキュリティセクター関連の組織規模を拡大し研究開発体制を強化
- 国家安全保障及び経済安全保障関連の需要増大を取り込むための体制構築を進めた

『ナショナル・セキュリティ研究開発本部』を設置

2022年3月期末時点

少数精鋭

10名未満

2023年3月期末時点

研究開発第一部

研究開発第二部

基礎技術研究部

合計　約３０名に増員

・需要の増大及び、大型・長期の案件増加に備えて大幅に増員
・強みである研究開発能力及びリサーチ能力に磨きをかけ、より高度な技術力を求められる案件にも対応できる体制の構築を進める
・需要の増加が著しく、引き続き増員及び技術力の強化を進めている

ナショナルセキュリティセクターにおける取り組み

- 国内でサイバーセキュリティの基礎技術から研究開発を行う企業が、当社の他にほぼ存在しないため
  コンピューター工学の基礎力が高い人材を採用し、社内の教育プログラムによって戦力化している

**人材不足が顕著かつ、
即戦力がほぼ存在しない**

日本では約５万６千人の人材不足※
サイバーセキュリティの基礎技術から研究開発を行う企業が
日本国内ではほぼ当社のみのため、即戦力が存在しない

※(ISC)²「Cybersecurity Workforce Study 2022」より

ＦＦＲＩセキュリティ

国内ほぼ唯一、セキュリティの
基礎技術から研究開発を行う
国内に即戦力がほぼ存在しない

国内セキュリティベンダー

海外企業から技術を輸入し
パッケージとして販売している

教育プログラムによって早期の戦力化

求める人材

セキュリティの実務経験は問わない
コンピューター工学の基礎力が高い

採用

研修（３～６ヶ月）

戦力化

プライベートセクターにおける取り組み

純国産製品である統合データマネジメントツール「ALog EVA」とFFRI yaraiの連携を開始

・ 国内外5,100契約以上の導入実績を誇る統合データマネジメントツール「ALog EVA」とFFRI yaraiの連携を開始
・FFRI yaraiの検出ログや、PC端末、セキュリティ周辺機器のログをALog EVAが一元管理し
情報システム担当者にかかる運用負荷を軽減する

ＦＦＲＩセキュリティ マネージド・サービス の提供を開始

アラートモニタリング
インシデント初動調査
レポートサービス

・セキュリティアラートの監視及び運用支援や、インシデント発生時の初動対応・調査を提供する「ＦＦＲＩセキュリティ マネージド・サービス」の提供を開始
・セキュリティ専門人材不在の組織などを中心に販売を行う

その他の取り組み

■販売パートナー各社と連携を継続し、
FFRI yaraiの販売拡大施策を推進

・販売パートナーと連携し、足元で需要増加が続く地方自治体へのOEM製品の販売拡大に向けた取り組みを進める
・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

■NTTコミュニケーションズとの合弁会社である
NFラボラトリーズより、高度セキュリティ人材の育成と輩出を継続

・セキュリティ人材の不足が顕著な市場状況もあり
需要が増加傾向
・高度セキュリティ人材の育成および輩出を推進した結果
持分法による投資利益38百万円を計上

■シャインテック社にてセキュリティ教育を進める

・既存の品質保証・テスト業務等は継続つつ、
より付加価値の高いサービス提供に向けて、
セキュリティ技術の教育が進む

■株主還元の取り組みとして、自己株式取得を実施

・自己株式160,000株を、161,407,700円で取得
（取得期間：令和４年５月17日～６月16日）

業績予想との差異について

- 安全保障関連のセキュリティ・サービス案件が増加し、売上高は業績予想を上回りました
- 国内セキュリティエンジニアは不足傾向にあるため高コストの採用を想定していたが、コンピューター工学の基礎力の高い人材の採用及び教育を進めた結果、人件費及び採用費が想定を下回りました
- 持分法適用会社である株式会社エヌ・エフ・ラボラトリーズも、案件の増加により当初の計画を上回り、営業外収益が増加しました

単位：百万円	2023/3 (予想)	2023/3 (実績)	増減率
売上高	1,920	1,952	1.7%
営業利益(利益率:%)	46 (2.4)	202 (10.4)	341.2%
経常利益(利益率:%)	56 (3.0)	247 (12.7)	341.8%
親会社株主に帰属する当期純利益(利益率:%)	37 (1.9)	187 (9.6)	406.2%

2024年３月期の主な取組み

2024年３月期の主な取り組み

- 国家安全保障・経済安全保障関連の政府の取り組みが加速し、さらなる需要の増加が見込まれる
- 増大する需要を取り込むため、優秀なエンジニアの採用・育成を継続する
- 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

ナショナルセキュリティセクターの規模拡大

2022年3月期末時点

少数精鋭

10名未満

2023年3月期末時点

研究開発第一部

研究開発第二部

基礎技術研究部

合計　約３０名に増員

2024年3月期末目標

エンジニア40名規模まで拡大

・安全保障関連のサービス案件が増加
・エンジニアの増員が増収に直結する状況であり、採用活動の強化、人材の早期戦力化を進める

2024年３月期の主な取り組み

■販売パートナー各社と連携を継続し、
FFRI yaraiの販売拡大施策を推進

・販売パートナーと連携した販売活動及び、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

■シャインテック社にてセキュリティ人材の育成を進める

・品質保証・テスト業務等は継続
・将来的にセキュリティ・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
セキュリティ技術の教育を拡大

■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
セキュリティ・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
・多様化するニーズに応えられる体制を構築する

■NTTコミュニケーションズとの合弁会社 NFラボラトリーズより、高度セキュリティ人材の育成と輩出を継続

・国内では高度セキュリティ人材が大幅に不足しており
人材育成および輩出を推進する
・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・育成を進める

連結業績予想

- 足元で増加し続けている安全保障関連の需要を取り込み、増収となる見込み
- 中長期に渡る需要の増加を取り込むための先行投資として採用強化を継続するため、採用コスト及び人件費が増加

単位：百万円	2023/3 (実績)		2024/3 (予想)		YoY
売上高	1,952		2,309		18.3%
営業利益(利益率:%)	202	(10.4)	191	(8.3)	△5.8%
経常利益(利益率:%)	247	(12.7)	219	(9.5)	△11.4%
親会社株主に帰属する 当期純利益(利益率:%)	187	(9.6)	155	(6.7)	△17.0%

連結業績予想（売上高の内訳）

単位：百万円	2023/3 (実績)	2024/3 (予想)	YoY
サイバー・セキュリティ事業	1,531	1,876	22.5%
ナショナルセキュリティセクター	143	391	172.3%
パブリックセクター	755	923	22.2%
プライベートセクター	631	561	△11.2%
ソフトウェア開発・テスト事業	421	433	2.8%
合計	1,952	2,309	18.3%

連結業績予想（2024年3月期～2026年3月期）

- 需要増加が続く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を成長のドライバーとする。
- 経済安全保障推進法及び防衛３文書の制定により安全保障関連の需要が急増しており、中期経営計画を上方修正
- 2024年３月期はセキュリティエンジニアの採用及び教育を進め、需要を確実に取り込む体制を構築

修正後計画（2023.5.15）

単位：百万円	2024/3（計画）		2025/3（計画）		2026/3（計画）	
売上高	2,309		2,789		3,080	
営業利益(利益率:%)	191	(8.3)	406	(14.6)	491	(16.0)
経常利益(利益率:%)	219	(9.5)	434	(15.6)	519	(16.9)
親会社株主に帰属する当期純利益(利益率:%)	155	(6.7)	304	(10.9)	363	(11.8)

参考：当初計画（2022.5.13）

2024/3（計画）		2025/3（計画）	
2,156		2,492	
159	(7.4)	336	(13.5)
170	(7.9)	346	(13.9)
115	(5.4)	238	(9.6)

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。

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。