事業計画及び成長可能性に関する説明資料

2022.6.30

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　営業本部長	池田　昭雄	社外取締役（監査等委員）	中山　泰秀
	取締役　事業開発本部長	川原　一郎		
	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（2022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）

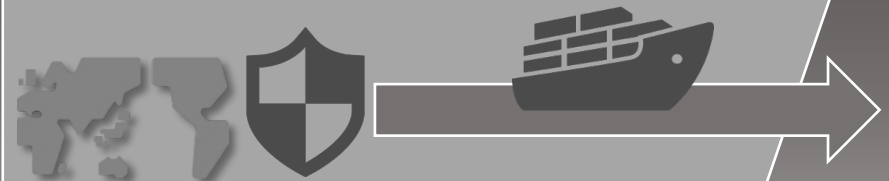
設立の経緯

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

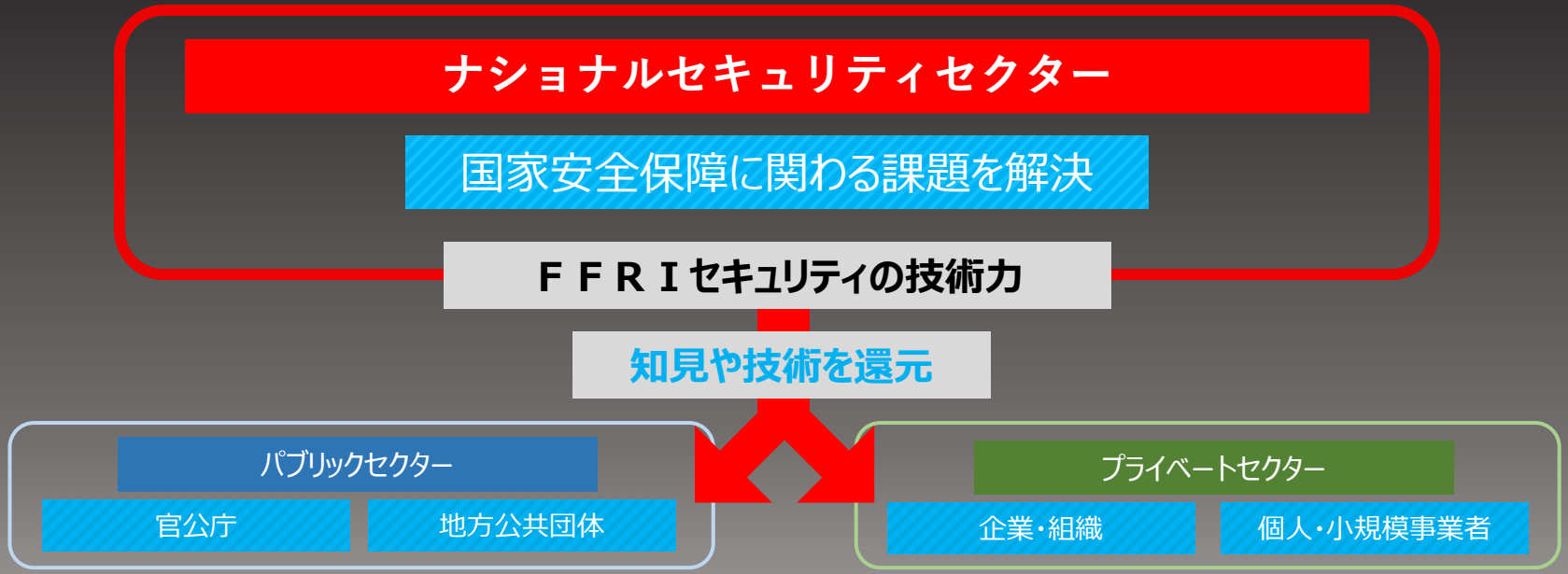
コーポレートマークにも「1440」の文字とスノーボードの回転をイメージした矢印で、設立当初から変わらない「未踏の分野への挑戦」を表現

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　セキュリティ市場

近年のサイバー攻撃は組織犯罪となり、金銭や政治的な意味を持った「ビジネス」となっている

00年～10年頃

1日1~3万個の
新種のウイルスが発生

単独犯

自己顕示目的

愉快犯

技術力のアピールや
いたずら目的の個人が大半

様々な攻撃手法の確立とともに、ウイルスを製作するツールが充実し、
多少の知識があればウイルスを作れるように。

現代

1日30万個以上の
新種のウイルスが発生

組織犯

経済的目的

政治的目的

直接的な金銭の要求や、
依頼を受けてサイバー攻撃を行うなど、ひとつの「ビジネス」となっている。

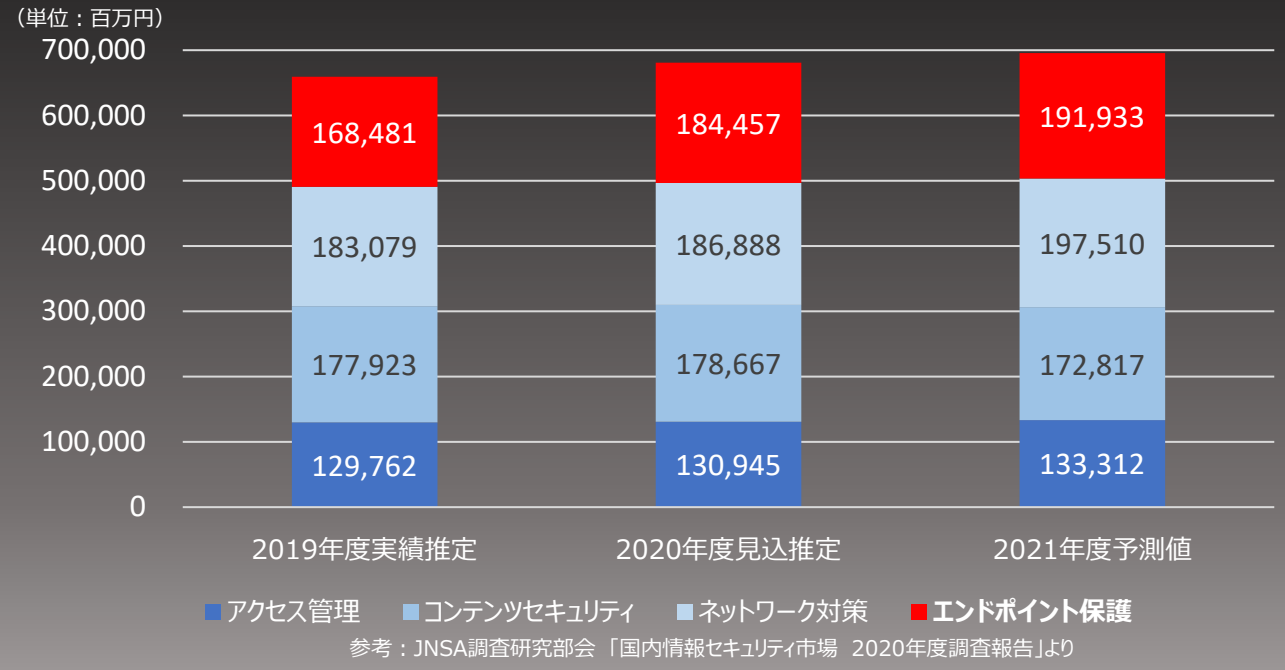
事業環境　セキュリティ市場

サイバー攻撃の増加を背景に、ここ数年でサイバー攻撃対策製品が大幅に増加

2011年：	国内企業を狙ったサイバー攻撃が増加 サイバー攻撃関連の報道が増加	「標的型攻撃」が連日ニュースに取り上げられる
2014年： 2015年：	サイバーセキュリティ基本法 成立 日本年金機構が不正アクセスを受け 125万件超の情報漏えいが発生	サイバー攻撃の高度化・複雑化が加速。 新たな脅威と被害の発生とともに、従来の セキュリティ対策の限界が認知され始める。
新たな脅威の増加 / 脅威対策製品の増加		
2018年～	政府統一基準群の改定 サイバーセキュリティ基本法が改正 防衛大綱の改訂 ※サイバー防衛能力の記載が追加	政府の対策方針が強化されるなど、市場の活性化により、 新たな製品・サービスが大幅に増加。一部には性能が不 十分・限定的なものもあり、玉石混交状態。

事業環境　セキュリティ・プロダクト市場

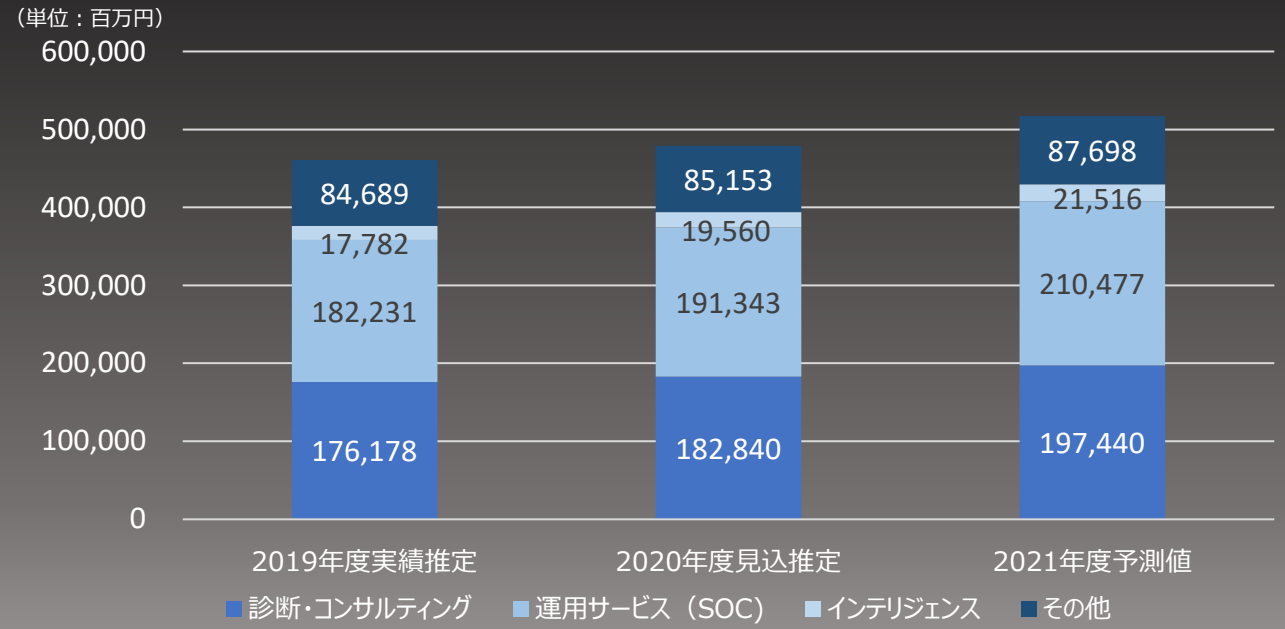
当社製品FFRI yaraiはエンドポイント保護製品に分類
国内市場はサイバー攻撃による被害の増加や、テレワークやDXの推進を受けて年々拡大している



参考：JNSA調査研究部会「国内情報セキュリティ市場　2020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　2020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

「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

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など、
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)

事業環境　ナショナルセキュリティセクター

製品やサービスを製造・流通する過程において、不正なプログラムやファームウェアの組込み・改ざんが行われるリスクへの対応など、サプライチェーンにおけるサイバーセキュリティ対策の強化が求められている

※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)より抜粋

ハード面

- ICチップなどコンポーネント
- 製造(組立)
- 物流

ハードウェアを構成する部品等に、製造・組立・流通時にバックドアなどが混入するリスク

ソフト面

- ソフトウェア
- データ
- サービス

ソフトウェア開発に使用される開発キットや、OSS※、更新データなどに不正なプログラムが混入するリスク

サプライチェーンを構成するあらゆる組織が安全性・信頼性を確保することが必要

参考：次期サイバーセキュリティ戦略(NISC他各省庁)

※OSS・・・オープンソースソフトウェア。
無償で利用・改変可能なソフトウェア。

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

国内脅威情報が国内に存在しない問題

海外製品で検知したマルウェアなどの
脅威情報データが海外に送信される

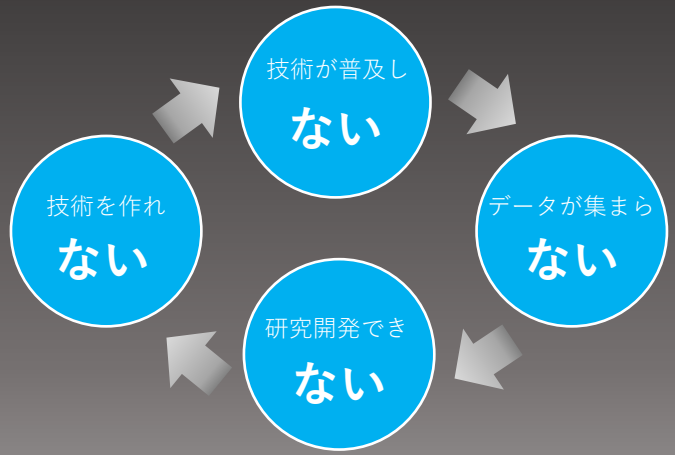
国内でどういったサイバー攻撃が発生し
ているのか、**国内にデータが存在しない**

情報を海外から高額で購入する歪な構造

100%正確で網羅されたデータである保証もない

国内産業はデータ負けのスパイラル

国内産業育成のために、国内でサイバーセキュリティ情報を
大規模に生成・蓄積・提供できる環境が必要



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）

日本が抱える課題と政府の取り組み

政府は「経済安全保障重要技術育成プログラム（ビジョン実現型）」を推進

※令和３年度補正予算　2,500億円を財源とする

プログラムの元となった２つの政府文書

①経済財政運営と改革の基本方針2021

経済安全保障の強化推進のため、（中略）
先端的な重要技術について実用化に向けた強力な支援を行う新たなプロジェクトを創出するとともに、
重要な技術情報の保全と共有・活用を図る仕組みを検討・整備する。

②統合イノベーション戦略2021

経済安全保障の強化推進のため、シンクタンク機能も活用しながら、（中略）先端的な重要技術について、
関係省庁、研究機関、企業、専門家等の密接な連携のもと官民の力を結集して、実用化に向けた強力な支援を行う新たなプロジェクトを創出。

参考：セキュリティ情報の時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）

①経済財政運営と改革の基本方針2021

経済財政運営と改革の基本方針2021では、「次期サイバーセキュリティ戦略」を策定。
『デジタル化の進展と併せて、サイバーセキュリティ確保に向けた取組を、あらゆる面で同時に推進』
※次期サイバーセキュリティ戦略　より抜粋

次期サイバーセキュリティ戦略の目標

- **DXとサイバーセキュリティの同時推進**
- **公共空間化と相互連携・連鎖が進展するサイバー空間全体を俯瞰した安心・安全の確保**
- **安全保障の観点からの取組強化**

横断的・中長期的な視点で、研究開発や人材育成、普及啓発に取り組む

サイバー犯罪対策や、重要インフラ・政府機関などの対策強化、
安全保障の観点から防御力・抑止力・状況把握力の強化などを推進

横断的な施策

1．研究開発の推進

・産学官連携振興による**エコシステムの構築**
・実践的な研究開発を推進し、国内産業の育成・発展を推進

2．人材の確保、育成、活躍促進
3．全員参加による協働、普及啓発

参考：次期サイバーセキュリティ戦略　より抜粋

①経済財政運営と改革の基本方針2021

産学官の連携を振興し、研究環境の充実を図ることで、国内サイバーセキュリティ産業の育成と発展を推進

エコシステム駆動にむけた循環の構築

研究が構想され、資金が獲得され、その資金を「人」に投入して、
研究を進める。研究の中で育った「人」が、さらに学問を発展させ、
研究拠点や研究グループを作り、産学官連携を進め、次の研究を構想する

※サイバーセキュリティ研究・産学官連携戦略WG最終報告(NISC) より抜粋

重点的な研究領域

安全・安全な社会基盤	デジタルインフラセキュリティ サプライチェーンセキュリティ データセキュリティ・プライバシー保護 実装セキュリティ（ハードウェア）
将来を見据えて取り組むべき分野	AIセキュリティ 自動車セキュリティ
攻撃者優位を覆し先手を打つアプローチ	オフェンシブセキュリティ研究（※） 実データ観測・分析に基づく研究 人的要素セキュリティ

※攻撃者の視点に立って、リスクや脆弱性を洗い出し、対策する研究

②統合イノベーション戦略2021

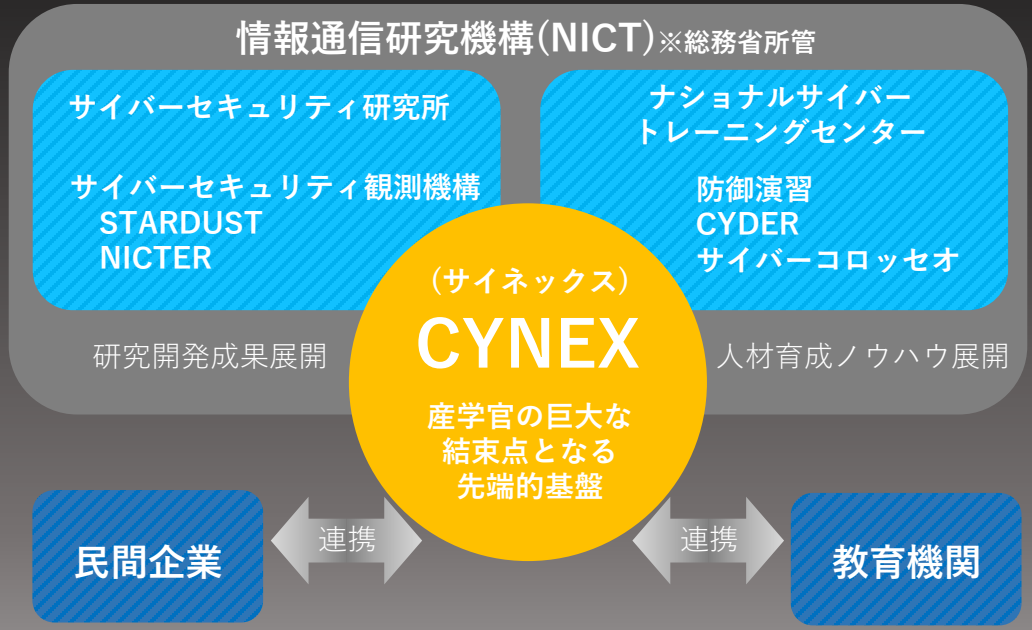
国内のサイバーセキュリティ産業育成を後押しする CYNEX を設立し、データ負けのスパイラル脱却を図る

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

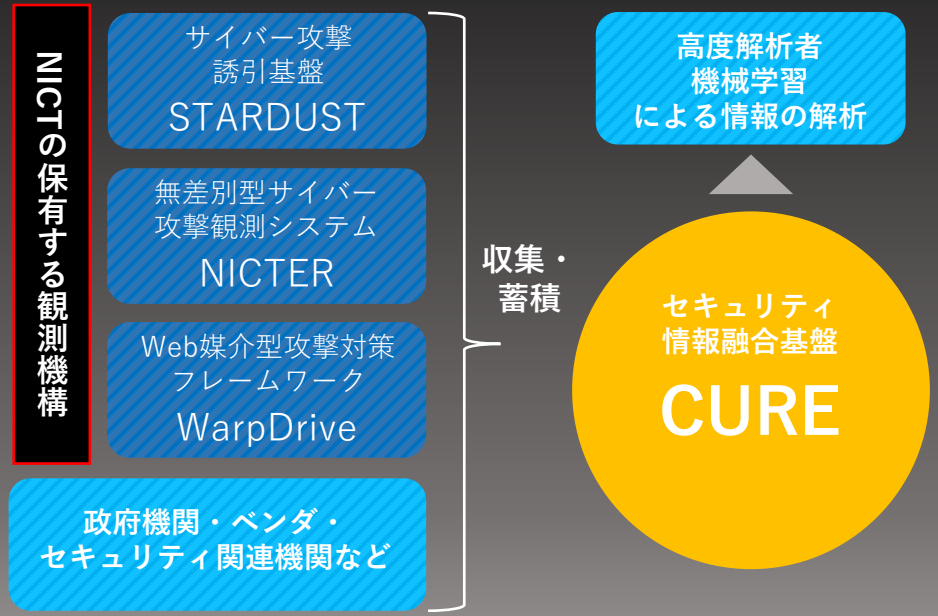
母体組織であるNICTの研究成果やサービスの一部を産学に半開放



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)

②統合イノベーション戦略2021

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

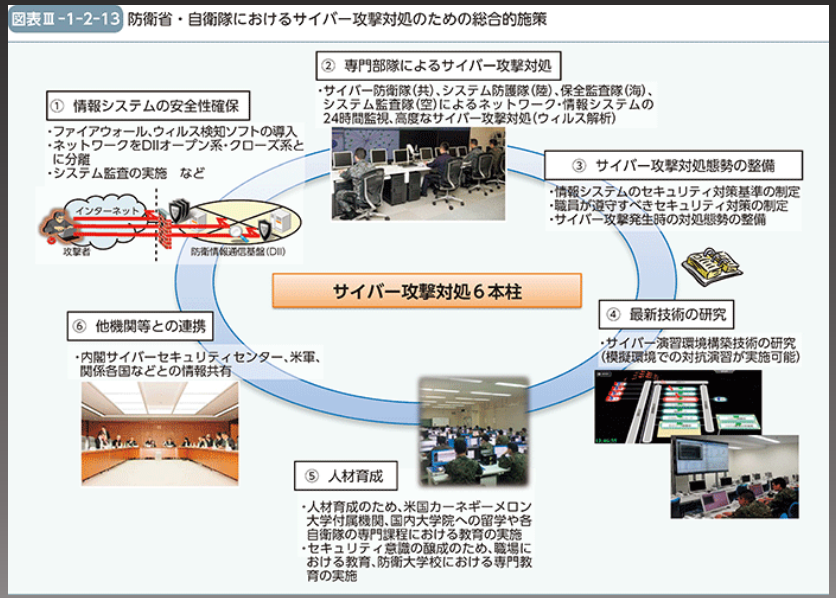
純国産サイバーセキュリティ情報の生成

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)

防衛大綱の改定

「平成 31 年度以降に係る防衛計画の大綱」（防衛大綱）でサイバー防衛能力の強化を従来とは抜本的に異なる速度で変革を図っていくことを明言した



参考：令和元年版防衛白書より

サイバー攻撃に用いられる相手方の**サイバー空間の利用を妨げる能力**を含め、サイバー防衛能力の抜本的強化を図る

※令和元年版防衛白書より抜粋

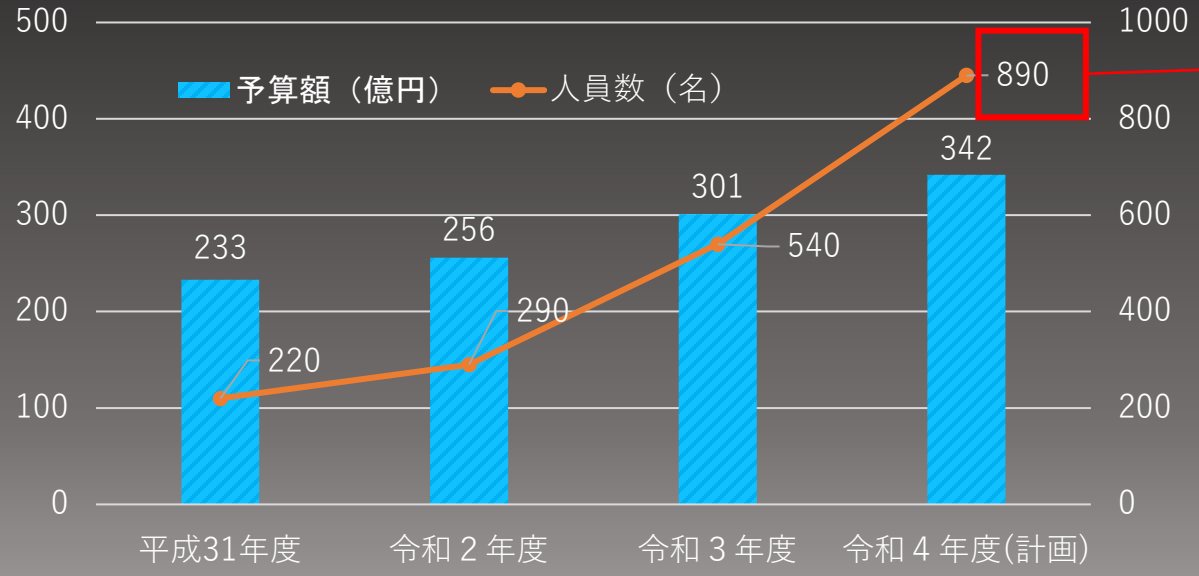
国としての優位性を獲得する上で死活的に重要な領域として、サイバー防衛能力強化を明言

サイバー防衛能力に関する記述が初めてなされ、防衛省・自衛隊におけるサイバー能力の強化を進めている。

防衛大綱の改定

防衛省のサイバー関連経費と部隊人員数は、政府の進める抜本的な改革によって、ここ数年増加傾向だがそれでも周辺諸国に比べ規模が小さく、さらなる体制強化のため令和４年度も増員・増額の見通し

防衛省のサイバー関連経費と人員数の推移



各国のサイバー部隊規模

国名	組織規模
アメリカ	約6,200名
中国	約30,000名
ロシア	約1,000名
北朝鮮	約6,800名

参考：「令和2年版防衛白書」より

防衛大綱の改定

防衛省の令和４年度予算計画においては「サイバー攻撃対処に係る部外力の活用」に３８億円を計画するなど、民間企業の持つ技術基盤の活用を進める計画となっている

令和４年度予算の主な内訳

サイバー人材の確保・育成	約　15億円
サイバー攻撃対処に係る部外力の活用	約　38億円
サイバー演習環境の整備	約　12億円
サイバー攻撃対処技術の研究	約　24億円
システム・ネットワーク管理機能の整備	約　64億円
その他サイバー関連経費	約 189億円
合計	**約 342億円**

サイバー攻撃対処に関する高度な専門的知見を必要とする業務について、**部外力を活用※**

※民間企業など外部人材の活用

装備品等に対するサイバー攻撃発生時における被害拡大防止やシステムの運用継続を図るため、対処能力向上に資する技術の研究を実施

参考：防衛省「我が国の防衛と予算-令和４年度予概算要求の概要」より抜粋

事業環境　パブリックセクター

官公庁など政府関連機関のサイバー・セキュリティに関する政府統一基準を、
「エンドポイントでの挙動の検出」に見直し。次世代型のエンドポイント対策製品の導入を求めている。

政府機関等の情報セキュリティ対策のための統一基準群の見直し（骨子）
https://www.nisc.go.jp/conference/cs/dai17/pdf/17shiryou03.pdf

２．改定のコンセプト

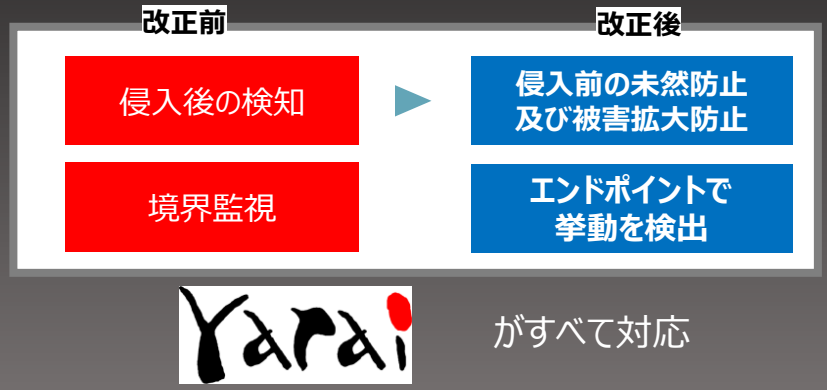
（１）将来像を見据えたサイバーセキュリティ対策の体系の進化

・新たな防御技術の導入、システムによる自動化等により、サイバーセキュリティ対策を新たなレベルに進化させることができる時期に来ていると認識。

①エンドポイント検知による未知の不正プログラムの被害の未然防止／拡大防止

・未知の不正プログラムに対しては、従来のシグネチャ型の既知の不正プログラム検知方式では対応できず、境界監視により不正通信を検知した際はインシデント発生後とならざるを得ない。近年の技術進歩により、不正プログラムが動作する内部（端末等のエンドポイント）での挙動を検出することにより、インシデントの発生の未然防止や被害拡大防止の機能が向上してきている。

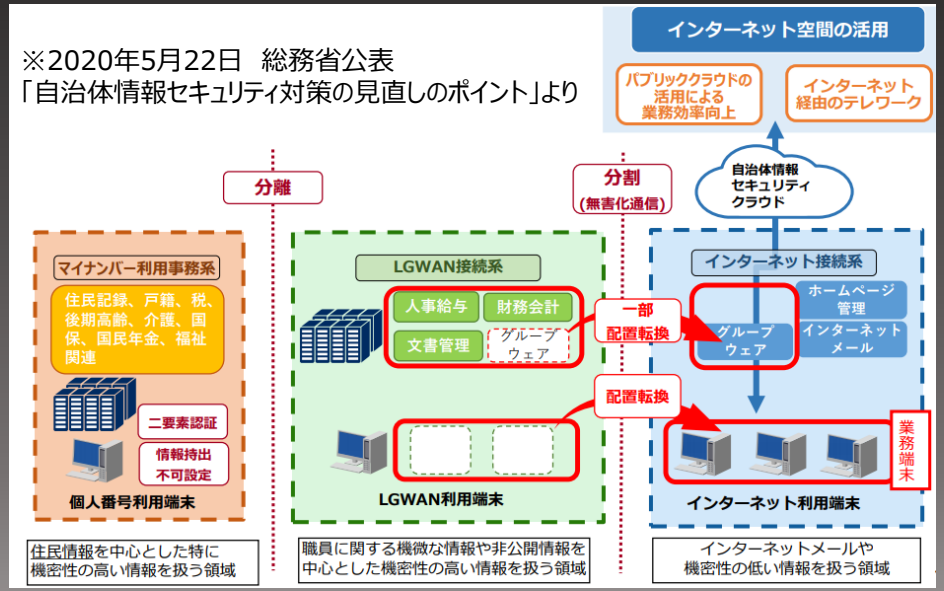
・このような機能の導入は、「監視」機能の高度化との視点でとらえることもできる。



事業環境　パブリックセクター

政府統一基準に続いて、地方自治体向け情報セキュリティポリシーが改定。
　新たなネットワークモデル（βモデル）では、エンドポイントセキュリティが重要に

※2020年5月22日　総務省公表
「自治体情報セキュリティ対策の見直しのポイント」より



従来のモデル（三層の対策）

マイナンバーや機密性の高い情報を扱う領域と、
インターネットに接続する領域を分断することで
セキュリティを確保する構成

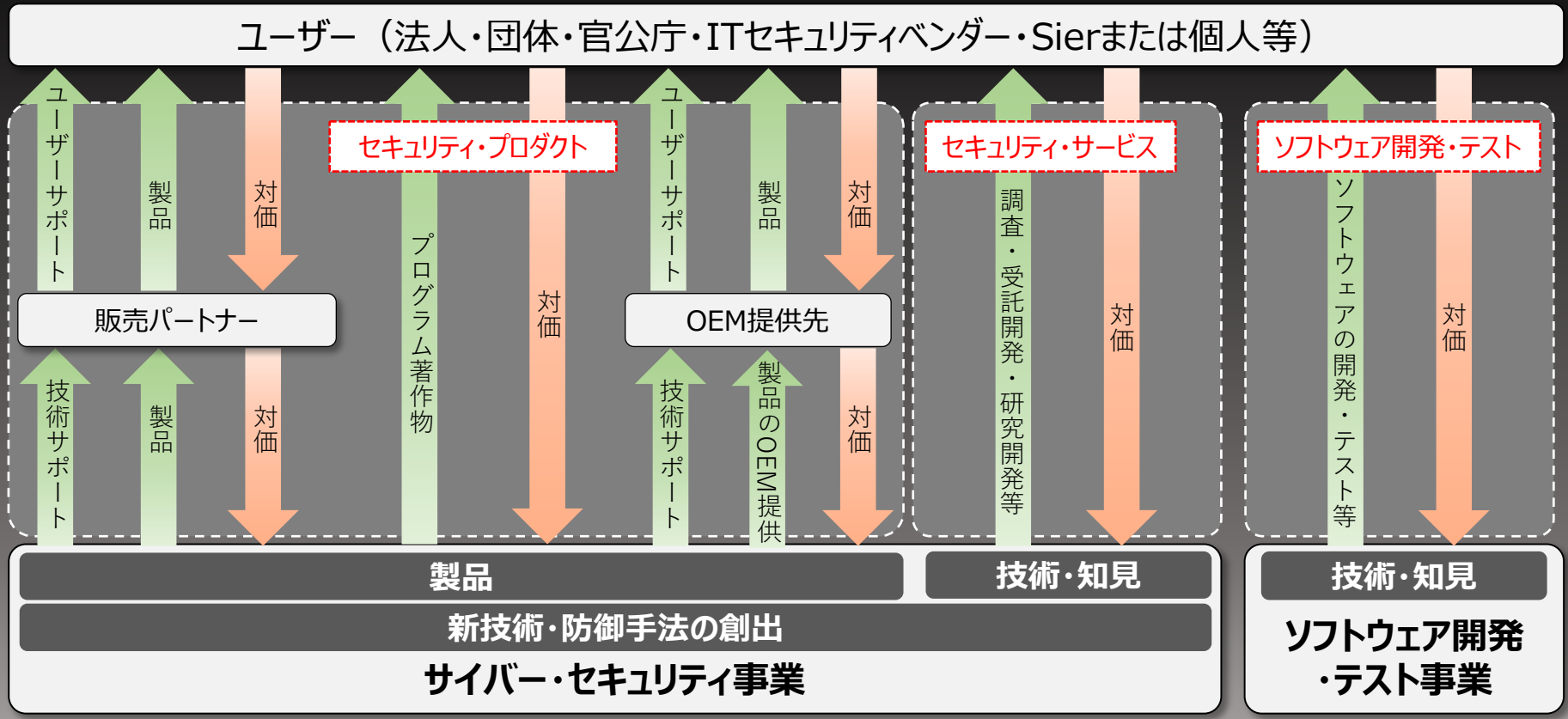
新たなモデル（βモデル）※左図

クラウドサービスの活用やテレワーク等へ対応する
効率性・利便性の高い新たなモデルを提示。

機密性の高い情報を扱う端末が直接インターネットに
接続する事になるため、端末のセキュリティ
（エンドポイントセキュリティ）の強化が必要

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
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
セキュリティ・サービス
調査・受託開発・研究開発等
対価
ソフトウェア開発・テスト
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

大手ベンダーＣ社
老舗ベンダーＤ社
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

北米企業Ａ社
北米企業Ｂ社 など

可視化

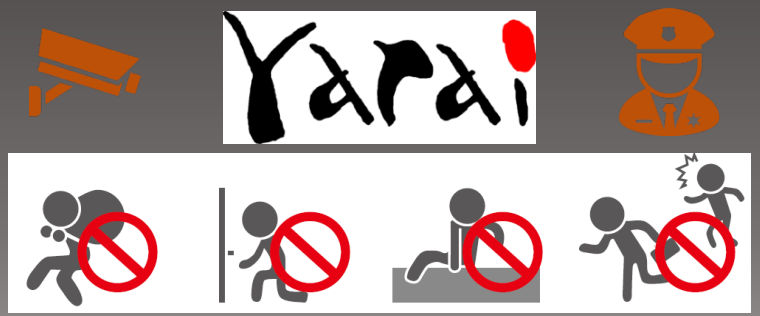
・EDR製品

Ｅ社
Ｆ社　など

FFRI yarai の強み

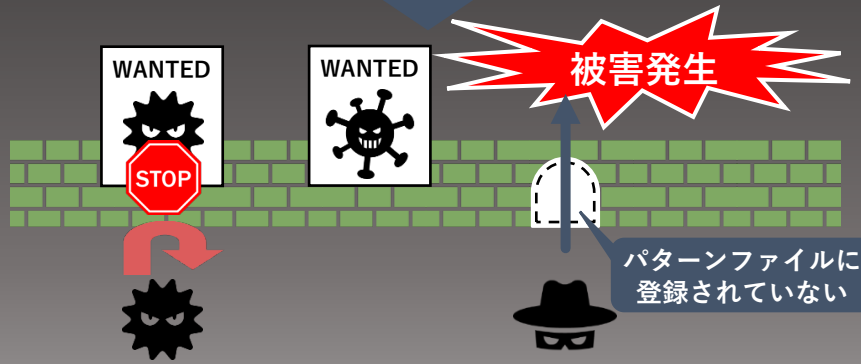
パターンマッチング型製品は、パターンファイルに登録されていない未知のマルウェアを防ぐ事ができない
FFRI yaraiは振る舞い検知技術により、マルウェア特有の怪しい振る舞いを検知するため、標的型攻撃などの未知のマルウェアを使用した攻撃も防御することができる。

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の主な防御実績

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
2020年11月	2018年2月	マルウェア「IcedID」
2020年7月	2018年2月	ランサムウェア「Maze」
2019年7月	2019年1月	ランサムウェア「Sodin」
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」

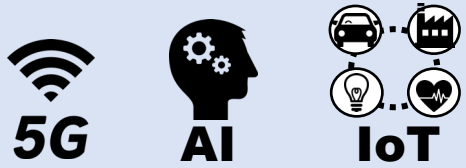
主要なセキュリティ・サービス

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

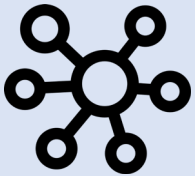


IoT機器や５Gネットワーク、AIシステムの脅威分析や、バックドア検出などのセキュリティ検査を提供します。

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、
　教育体制の整備等を進めている

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

＋

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：統合イノベーション戦略2021

防衛省・自衛隊において相手方のサイバー空間の利用を妨げる能力を含めたサイバー防衛能力の強化

人員拡大や組織体制の整備が進むほか、部外力（民間）の技術力を活用する方針

参考：防衛省「我が国の防衛と予算-
令和４年度予概算要求の概要」
令和元年版防衛白書

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

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・セキュリティ関連の研究開発体制を強化
次年度に予定されている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める体制を構築
国内企業ではほぼ唯一のサイバーセキュリティの基礎技術研究の能力を磨きあげ、安全保障の実現に寄与

ナショナル・セキュリティ研究開発本部の設立

少数精鋭 → **大型・長期の案件に向けて大幅増員**

案件の増加を見据えて体制を強化
さらなる研究開発を促進する。

国内ほぼ唯一のサイバーセキュリティ基礎技術の研究開発能力に磨きをかける

研究開発能力・リサーチ能力を強化

国内ほぼ唯一の基礎技術研究を行っている企業として、研究開発能力やリサーチ能力に磨きをかけ、当社にしかできない領域で価値を発揮する

ナショナルセキュリティセクターの事業規模拡大に向けた取り組み

ナショナルセキュリティセクターの業務を拡大するため、積極的に案件を獲得し、幅広い分野で
　高度で先端的なセキュリティノウハウを蓄積していく
運用や監視などを含む、より幅広いセキュリティ・サービスをワンストップで提供する
採用体制の強化し、エンジニアを中心に増員を進める

セキュリティ・サービスの拡大

・セキュリティ・サービスの受注を拡大し、幅広い分野でノウハウを蓄積する

・研究開発や調査などの従来のセキュリティ・サービスを拡充しより幅広いサービスをワンストップで提供する

エンジニアを中心に増員を進める

・セキュリティエンジニアの増員へ向けて採用チーム増員・教育体制の強化・プレゼンスの向上を進める

OEM提供による販売の拡大

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
販売パートナーへのOEM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

地方自治体向けソリューションの提供を開始

地方自治体向けのガイドラインが発表され、今後の需要増が見込まれる
販売パートナーと連携し、予算・人材とも不足しがちな地方自治体向けのソリューションを提供

予算・人材とも不足しているケースが多い

NEC ActSecure X（2021年6月リリース）

Sky SKYSEA Client View
EDRプラスパック（2021年6月リリース）

NTT AT SOCサービス
EDR 端末ソリューション SKYSEA＆
yarai SOC（2021年8月リリース）

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、基礎技術研究室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への注力を進め、将来の需要を取り込むための体制整備が進んでおり、
　セキュリティエンジニアを中心に採用を強化しているため、採用費及び人件費等のコストが先行して発生した。
セキュリティ・サービスの案件受注に必要な秘匿性の高い体制整備に時間を要したほか、
　新型コロナウイルス感染症の再拡大の影響により、案件の遅延・失注するなど売上高・利益ともに計画を下回った。

単位：百万円	2021/3 (非連結)		2022/3 (連結)		YoY
売上高	1,618		1,779		10.0%
営業利益(利益率:%)	328	(20.3)	103	(5.8)	△68.5%
経常利益(利益率:%)	329	(20.4)	156	(8.8)	△52.6%
親会社株主に帰属する 当期純利益(利益率:%)	249	(15.4)	120	(6.8)	△51.5%

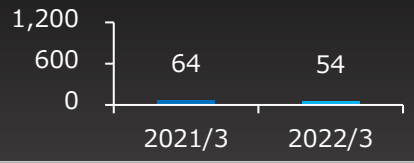
（注）2022年３月期より連結決算に移行しているため、2021年3月期については非連結での業績を比較情報として記載しております。

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

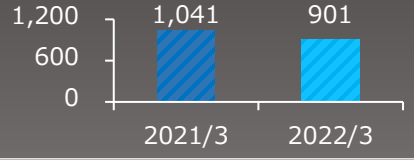


・横須賀ナショナルセキュリティR&Dセンターにて国家安全保障関連の案件を受託。
・セキュリティ調査・研究や教育案件及び提案活動を中心に実施。
・将来の中長期に渡る需要増を取り込める組織体制の整備を進めている。

パブリックセクター

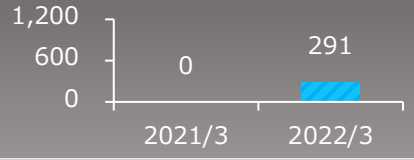
・NECやSky、NTT-AT社などと協力し、地方自治体へ向けた営業体制の強化を継続。
・高い秘匿性が求められるセキュリティ・サービスの案件獲得のための体制整備に時間を要した他、新型コロナウイルス感染症の再拡大の影響により遅延や失注が発生した。

プライベートセクター



・OEM製品の個人・小規模事業者向け販売が増加。
・「FFRI yarai 技術者認定制度」を開始。販売パートナーとの連携を強化
・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

ソフトウェア開発・テスト事業



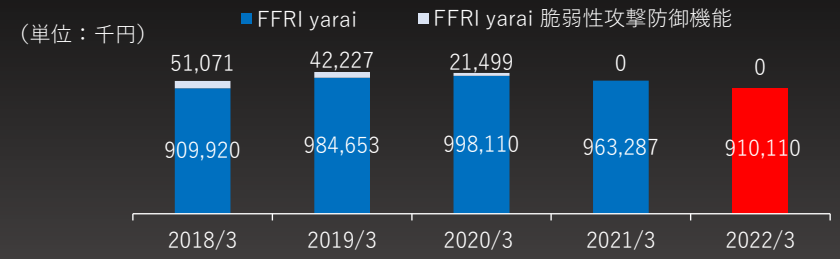
・シャインテック社において、テスト業務等を中心に提供
・将来的なセキュリティ・サービスの提供に向けた教育体制整備など準備を進める
※シャインテック社は2022年3月期より連結を開始したため、前年同期比は記載しておりません
※内部取引の消去後の売上高となります

セグメント・販売区分別 四半期会計期間毎の売上推移

※内部取引の消去後の売上高となります

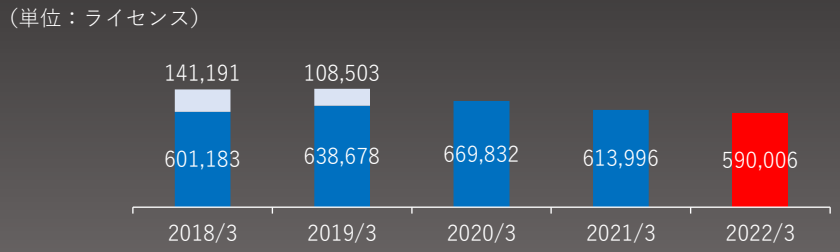
			単位：百万円	2021/3 1Q	2Q	3Q	4Q	2022/3 1Q	2Q	3Q	4Q
サイバー・セキュリティ事業	ナショナルセキュリティセクター	セキュリティ・プロダクト		19.4	19.4	1.5	1.5	1.3	1.3	0.4	0.4
		セキュリティ・サービス		0.0	5.0	6.6	10.8	13.4	9.6	5.0	22.6
	パブリックセクター	セキュリティ・プロダクト		83.5	83.4	83.0	80.4	78.5	78.7	79.4	73.1
		セキュリティ・サービス		12.0	0.4	28.7	140.2	6.4	21.4	78.6	115.1
	プライベートセクター	セキュリティ・プロダクト	法人	160.2	160.6	162.7	242.8	156.9	157.6	150.6	146.4
			個人	67.1	66.7	71.9	77.8	64.2	60.9	60.5	59.7
		セキュリティ・サービス		1.7	16.8	4.9	7.9	4.7	14.4	6.9	18.4
ソフトウェア開発・テスト事業				-	-	-	-	-	97.8	98.5	95.1
			合計	344.2	352.4	359.6	561.9	325.7	442.1	480.0	531.1

FFRI yarai シリーズの販売状況



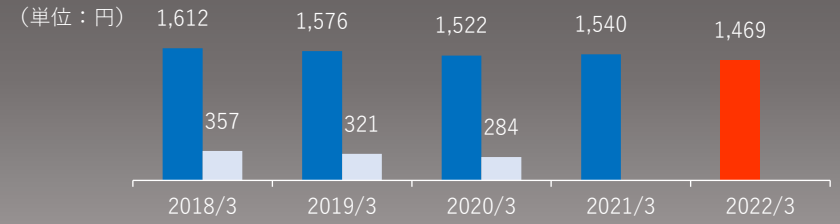
- FFRI yarai 売上高

前期の大口顧客の契約満了が通年で影響したほか、
一部顧客ではグローバルで使用できる製品への乗り換えなど、
製品の性能以外の理由から契約満了となるケースも発生した。



- 契約ライセンス数（20/3→21/3継続率　81.2%）

販売体制を強化している官公庁や地方自治体向けの
販売が増加しているものの、前期末に比べ23,990Licの減少
となった。



- FFRI yarai 売上単価

ボリュームディスカウントの価格体系のため、
大型案件の増加によってFFRI yaraiの単価はやや減少

FFRI yarai シリーズの業種別契約ライセンス数

業種	2021/3		2022/3	
	ライセンス	割合(%)	ライセンス	割合(%)
官公庁	248,480	40.4	245,477	41.6
金融サービス	117,362	19.1	97,995	16.6
運輸	43,019	7.0	36,738	6.2
情報通信	34,678	5.6	40,056	6.8
産業インフラ・サービス	41,055	6.7	32,012	5.4
その他	129,402	21.1	137,728	23.3
合計	613,996	100.0	590,006	100.0

原価及び販管費の内訳

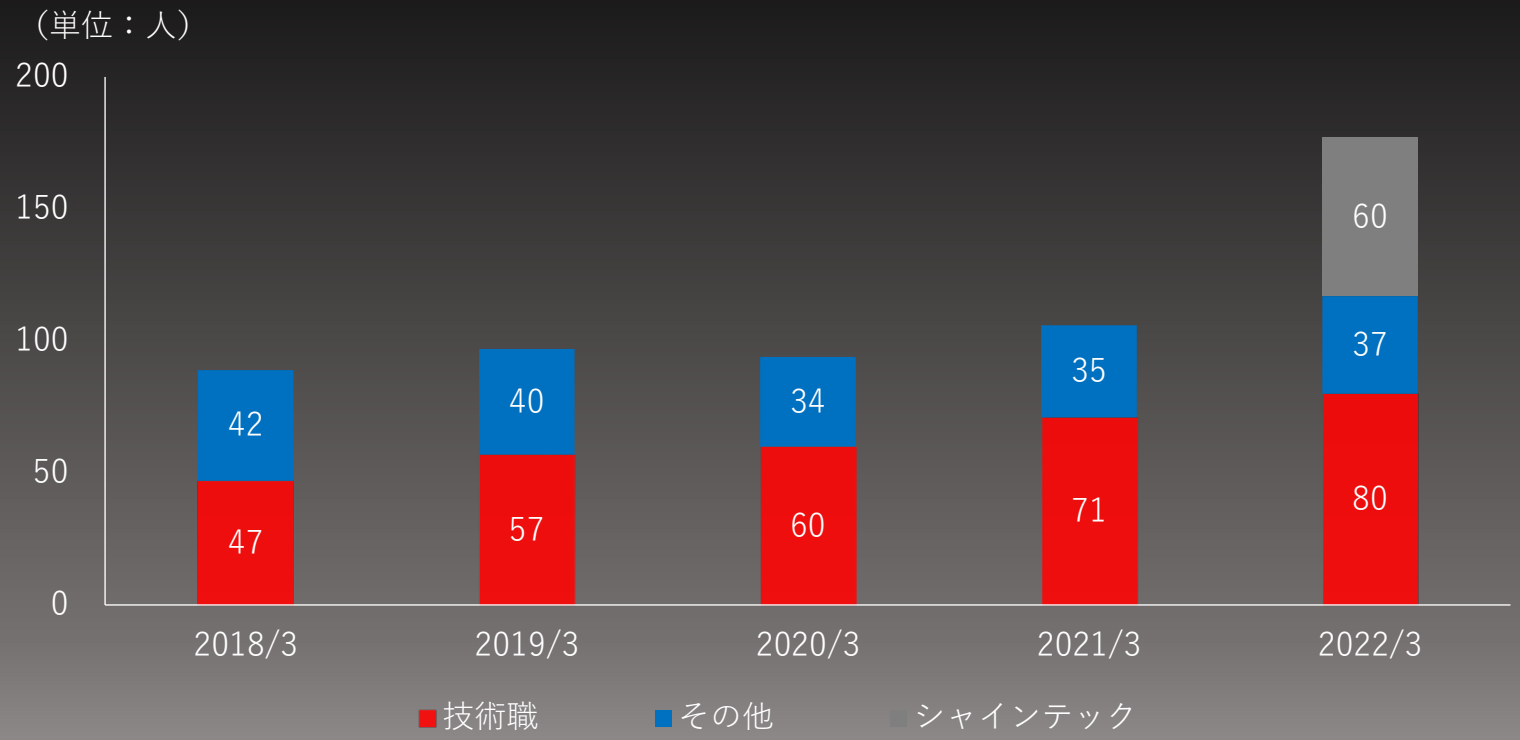
単位：百万円

	2021/3 (非連結)	2022/3 (連結)	増減比 (%)
労務費	369	620	67.9
経費	104	146	41.0
期首・期末棚卸及び他勘定振替	△183	△213	-
（研究開発費への振替）	△103	△104	-
（ソフトウェアへの振替）	△23	△12	-
（その他の振替）	△55	△96	-
売上原価合計	289	553	90.9
人件費	401	506	26.2
研究開発費	138	138	△0.4
販売手数料	190	167	△11.9
その他	269	309	15.2
販売管理費合計	999	1,122	12.3

- 労務費・人件費：エンジニアなど人員の増加及び、シャインテック社連結開始に伴う増加
- 研究開発費：FFRI yaraiの機能向上に関する研究の他、防衛産業向けセキュリティの研究開発などを実施
- 販売手数料：FFRI安心アプリチェッカーの販売減少に伴い、販売代理店に対する販売手数料が減少
- その他：採用コストの増加及び、シャインテック社株式取得に係る付随費用を計上したため、支払手数料が増加

（注）2022年３月期より連結決算に移行しているため、2021年3月期については非連結での業績を比較情報として記載しております。

人員数の推移


（単位：人）
200
150
100
50
0
42
47
40
57
34
60
35
71
37
80
60
2018/3
2019/3
2020/3
2021/3
2022/3
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	2021/3 （非連結）	2022/3 （連結）	増減比 （%）
流動資産	2,381	1,952	△18.0
現金及び預金	2,093	1,644	△21.5
売掛金	255	253	△0.8
固定資産	274	501	82.6
のれん	-	129	-
資産合計	2,656	2,453	△7.6
流動負債	608	720	18.4
前受収益	451	-	-
契約負債	-	625	-
固定負債	205	9	△95.2
長期前受収益	200	-	-
負債合計	814	730	△10.3
株主資本	1842	1,723	△ 6.4
利益剰余金	1295	1,437	10.9
純資産合計	1,842	1,723	△6.4
負債純資産合計	2,656	2,453	△7.6

- 現金及び預金：自己株式取得を実施したため
- 固定資産：シャインテック社の株式取得によるのれんの計上
- 「収益認識に関する会計基準」の適用により、前受収益、長期前受収益は契約負債に計上しています

（注）2022年３月期より連結決算に移行しているため、
2021年3月期については非連結での業績を比較情報として記載しております。

業績サマリー（キャッシュ・フロー）

単位：百万円	2021/3 (非連結)	2022/3 (連結)
営業活動によるキャッシュ・フロー	120	△16
税引前当期純利益	329	156
減価償却費	59	42
売上債権の増減額(△は減少)	△70	39
前受収益の増減額(△は減少)	△114	-
長期前受収益の増減額(△は減少)	△39	-
契約負債の増減額(△は減少)	-	△59
法人税等の支払額	△46	△83
その他	2	△112
投資活動によるキャッシュ・フロー	△42	△157
財務活動によるキャッシュ・フロー	0	△275
現金及び現金同等物の期末残高	2,093	1,644

- 「収益認識に関する会計基準」の適用により、営業活動によるキャッシュ・フローの前受収益、長期前受収益は契約負債に計上しています
- 投資活動によるキャッシュ・フロー：
  シャインテック社の株式取得によるもの
- 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

2022年３月期の主な取組み

2022年3月期の取り組み

ナショナルセキュリティセクター	・国家安全保障において重要性が増しているナショナルセキュリティの分野へ注力 ・引き続き需要の多い教育案件を中心に、防衛産業企業と共同で案件を進める ・防衛産業企業や、周辺組織と連携した提案活動を進める ・需要の増加に対応すべく、優秀なエンジニアの採用を加速
パブリックセキュリティセクター	・販売パートナーへのOEM提供による販路拡大や、自治体向けキャンペーンの実施など、協力して販売促進活動を行う。 ・地方自治体の抱える課題解決となるソリューションの提供
プライベートセクター	・戦略的販売パートナーとの連携強化 ・FFRI yaraiの機能強化の継続実施 ・国内・海外ともに販売力を持った新たな販売パートナーの獲得を進める ・車載セキュリティ向け研究開発及び、その他のIoTセキュリティ分野の開拓

※戦略的販売パートナー・・・当社グループからの積極的な営業支援の提供を受け、
当社製品の販売に対する高いインセンティブを持つ販売パートナー

ナショナルセキュリティセクターにおける取り組み（1）

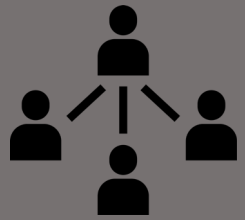
- 足元で需要の多いセキュリティ教育および調査・研究案件を中心に実施
- セキュリティコア技術やリサーチ能力、教育プログラムなど当社が強みとする能力が必要とされている
- 急激な需要増大を取り込むための組織体制構築が順調に進む

セキュリティ
コア技術

広範な
リサーチ能力

教育
プログラム

当社の強みとする能力が必要とされる案件が増加



組織体制の
整備

需要の増加を取り込むための
体制構築が進んだ

ナショナルセキュリティセクターにおける取り組み（2）
パブリックセクターにおける取り組み

■積極的なセキュリティ・サービス案件の獲得

・ナショナルセキュリティセクターの業務を拡大するため、従来より幅広い分野で多様な案件を受注し、ノウハウを蓄積

・社内の教育プログラムも活用し人材の育成も進む

高度セキュリティ技術者トレーニング

インテリジェンスの提供

など

■地方自治体向けソリューションの提供を開始

・地方自治体向けの販売体制を強化

・NEC、Sky、NTT-ATなど地方自治体への販売に強みを持つ販売パートナーより、OEM製品の提供を開始

予算不足

人材不足

予算・人材とも不足する地方自治体向けサービスを提供

その他の取り組み

■販売パートナーへのOEM提供など、連携強化による販売拡大を進める

・戦略的販売パートナーとの連携強化を継続

・個人・小規模事業者向けOEM製品などの販売が拡大

・「FFRI yarai技術者認定制度」を設立。
8社が認定を受けており、関係強化が進む

■優秀なエンジニアの採用加速及び人材育成

ナショナルセキュリティセクターにおける急激な市場拡大へ向けて、エンジニアを中心に人員の拡充および体制の整備を進めている。

エンジニア人員数

2021/3　71名　→　2022/3　80名　＋9名

■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

・教育・研修事業に加え、業務受託事業が好調に推移し

・持分法による投資利益51百万円を計上

■株式取得によりシャインテック社を完全子会社化

・品質保証・テスト業務等を中心に実施

・将来的に当社の持つセキュリティ技術を組み合わせた、より幅広いサービスの提供を行うため、教育体制整備を進める

■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120,000株を、260,494,000円で取得
（取得期間：令和3年5月19日～6月14日）

2023年３月期の主な取組み

2023年３月期の主な取組み

- 組織体制を整備し、ナショナル・セキュリティ関連の研究開発体制を強化
- 次年度に予定されている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める体制を構築
- 国内企業ではほぼ唯一のサイバーセキュリティの基礎技術研究の能力を磨きあげ、安全保障の実現に寄与

ナショナル・セキュリティ研究開発本部の設立

少数精鋭 → **大型・長期の案件に向けて大幅増員**

案件の増加を見据えて体制を強化
さらなる研究開発を促進する。

国内ほぼ唯一のサイバーセキュリティ基礎技術の研究開発能力に磨きをかける

研究開発能力・リサーチ能力を強化

国内ほぼ唯一の基礎技術研究を行っている企業として、研究開発能力やリサーチ能力に磨きをかけ、当社にしかできない領域で価値を発揮する

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

■優秀なエンジニアの採用加速及び人材育成

・ナショナルセキュリティセクターにおける急激な市場拡大へ向けて引き続き優秀なエンジニアの採用を積極的に進める。
・社内教育プログラムを活用し、早期の戦力化を推進する。

■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のなか、人材育成および輩出を推進する

■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して実施しながら、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を進める

■株主還元の取り組みとして、自己株式取得を実施

取得内容（2022年５月17日～2022年６月８日）

・取得した株式数　160,000株
取得価額の総額　161,407,700円

連結業績予想

ナショナルセキュリティセクターにおける、将来の需要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、
採用コストおよび人件費の増加を見込む

単位：百万円	2022/3 (実績)	2023/3 (予想)	YoY
売上高	1,779	1,920	7.9%
営業利益(利益率:%)	103 (5.8)	46 (2.4)	△55.0%
経常利益(利益率:%)	156 (8.8)	56 (3.0)	△63.5%
親会社株主に帰属する 当期純利益(利益率:%)	120 (6.8)	37 (1.9)	△69.1%

連結業績予想（売上高の内訳）

プライベートセクターの売上減少は、 2022年３月末をもって「FFRI安心アプリチェッカー」の提供を終了したことによるもの
ナショナルセキュリティセクター、パブリックセクターの規模拡大が進む

単位：百万円	2022/3 (実績)	2023/3 (予想)	YoY
サイバー・セキュリティ事業	1,487	1,517	2.0%
ナショナルセキュリティセクター	54	182	234.4%
パブリックセクター	531	681	28.3%
プライベートセクター	901	653	△27.5%
ソフトウェア開発・テスト事業	291	402	38.2%
合計	1,779	1,920	7.9%

連結業績予想（2023年3月期～2025年3月期）

ナショナルセキュリティセクターの需要を取り込むため採用を加速しており、採用コストや人件費の増加が一時的に利益を圧迫するものの、2023年３月期から2025年３月期にかけてナショナルセキュリティセクターの売上規模を３倍以上に成長させることで、全体として売上高１４０％、営業利益３２５％の成長を見込む

単位：百万円	2023/3（予想）	2024/3（計画）	2025/3（計画）
売上高	1,920	2,156	2,492
営業利益(利益率:%)	46 (2.4)	159 (7.4)	336 (13.5)
経常利益(利益率:%)	56 (3.0)	170 (7.9)	346 (13.9)
親会社株主に帰属する当期純利益(利益率:%)	37 (1.9)	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。