令和５年３月期
第３四半期　決算補足説明資料

株式会社ＦＦＲＩセキュリティ

（東証グロース：3692） https://www.ffri.jp

業績説明

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の強化を継続しており、採用費及び人件費のコストが増加しているものの、売上・利益とも計画通りに進捗している
- 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

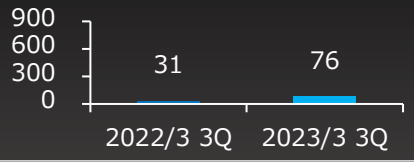
単位：百万円	2022/3 3Q (連結)		2023/3 3Q (連結)		YoY
売上高	1,248		1, 263		1.2%
営業利益(利益率:%)	9	(0.8)	△12	(△1.0)	-
経常利益(利益率:%)	47	(3.8)	12	(1.0)	△73.7%
親会社株主に帰属する当期純利益(利益率:%)	30	(2.4)	7	(0.6)	△75.2%

セグメント・販売区分別の概況

売上高（単位：百万円）

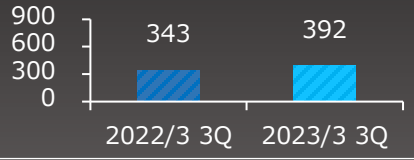
サイバー・セキュリティ事業

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。
・案件増加に伴い、エンジニアを大幅に増員。

パブリックセクター

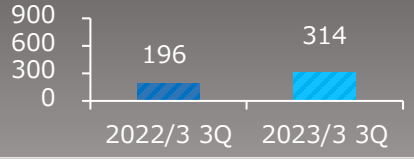


・官公庁向けのセキュリティ調査・研究案件を中心にサービス案件が増加。
・デジタル化が進む地方自治体への販売に強みを持つ販売パートナーと連携し、OEM製品やマネージドサービスなどを提供。協力して販売拡大施策を進めている。

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が増加している。

ソフトウェア開発・テスト事業



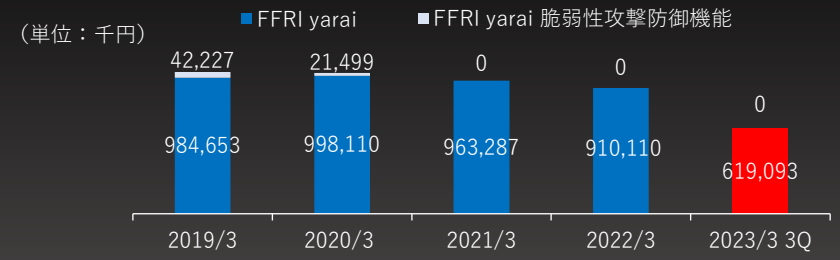
・シャインテック社において、テスト業務等を中心に提供
・将来的なセキュリティ・サービスの提供に向けた教育体制整備など準備を進める
※内部取引消去後の売上高となります
※シャインテック社の業績は2022年3月期第２四半期より連結しております

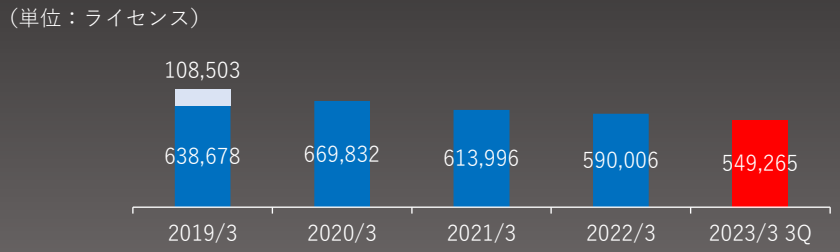
セグメント・販売区分別 四半期会計期間毎の売上推移

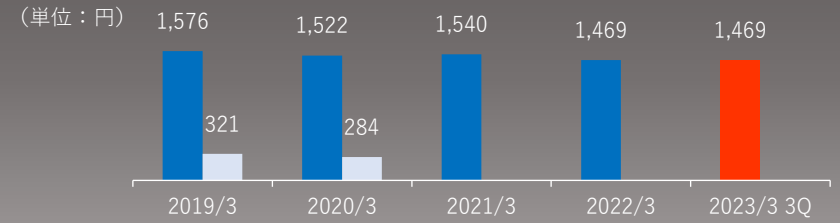
※内部取引の消去後の売上高となります

			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	
		セキュリティ・サービス	13.4	9.6	5.0	22.6	32.4	31.2	11.3	
	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	
		セキュリティ・サービス	6.4	21.4	78.6	115.1	7.0	52.2	128.9	
	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	
		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	
		セキュリティ・サービス	4.7	14.4	6.9	18.4	13.2	3.3	4.3	
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	
		合計	325.7	442.1	480.0	531.1	380.3	415.9	467.3	

FFRI yarai シリーズの販売状況







- FFRI yarai 売上高

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（21/3→22/3継続率　83.0%）

前期末に比べ40,741Lic減少となったが、販売パートナーと連携し、OEM製品などの販売体制を強化している地方自治体への販売数量が足元で増加。

- 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により、前四半期より単価が微増となった

FFRI yarai シリーズの業種別契約ライセンス数

業種	2022/3		2023/3　3Q	
	ライセンス	割合(%)	ライセンス	割合(%)
官公庁	245,477	41.6	224,260	40.8
金融サービス	97,995	16.6	70,108	12.8
運輸	36,738	6.2	36,581	6.7
情報通信	40,056	6.8	34,490	6.3
産業インフラ・サービス	32,012	5.4	29,845	5.4
その他	137,728	23.3	153,981	28.0
合計	590,006	100.0	549,265	100.0

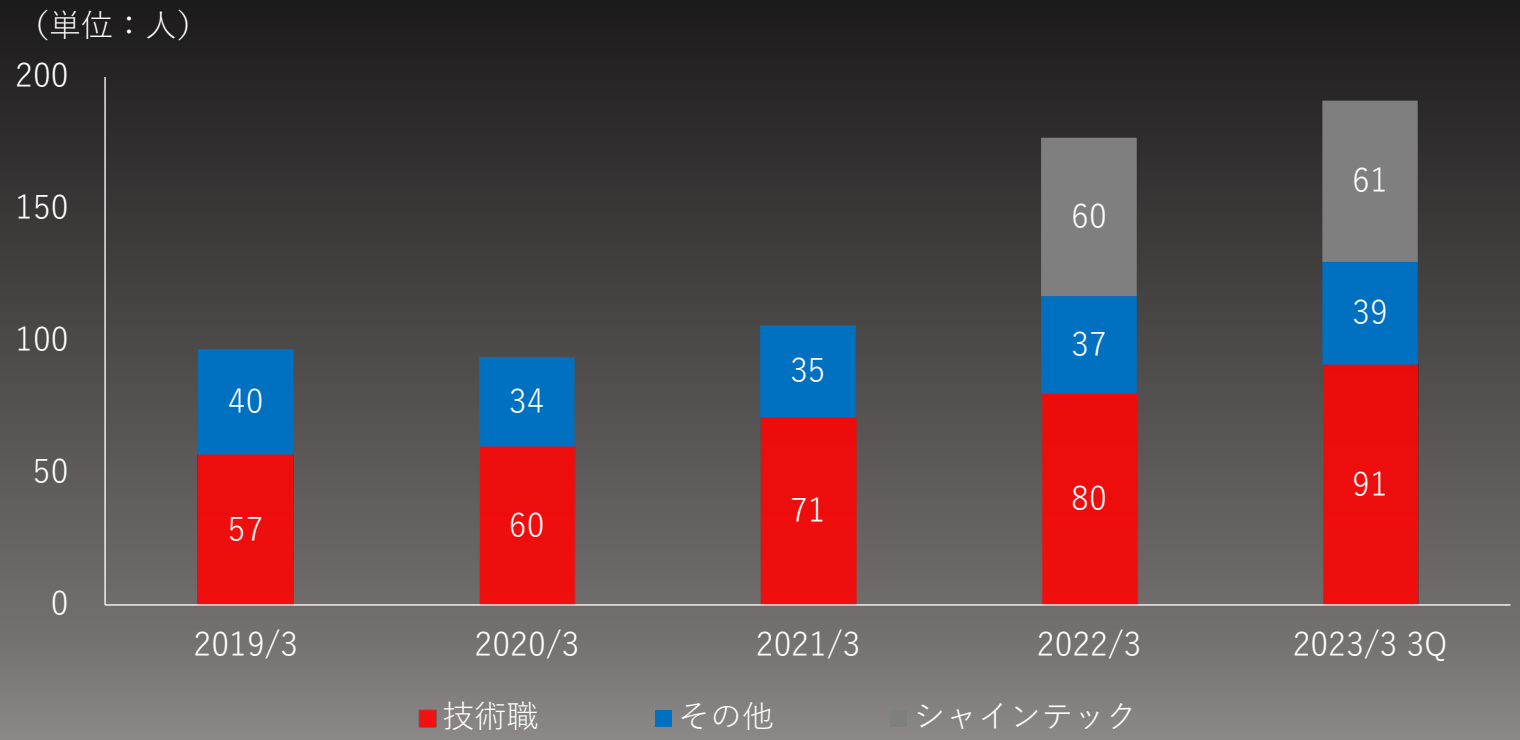
原価及び販管費の内訳

単位：百万円

	2022/3 3Q	2023/3 3Q	増減比 (%)
労務費	445	610	37.0
経費	101	132	31.0
期首・期末棚卸及び他勘定振替	△153	△204	-
（研究開発費への振替）	△69	△61	-
（ソフトウェアへの振替）	△2	△15	-
（その他の振替）	△80	△127	-
売上原価合計	392	539	37.1
人件費	379	358	△5.5
研究開発費	96	82	△14.2
販売手数料	127	0	△99.6
その他	241	295	22.3
販売管理費合計	845	737	△12.8

- 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
39
57
60
71
80
91
60
61
2019/3
2020/3
2021/3
2022/3
2023/3 3Q
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 3Q(連結)	増減比 (%)
流動資産	1,952	1,774	△9.1
現金及び預金	1,644	1,436	△12.7
売掛金	253	270	6.7
固定資産	501	512	2.1
のれん	129	118	△8.1
資産合計	2,453	2,286	△6.8
流動負債	720	707	△1.8
契約負債	625	601	△3.9
固定負債	9	9	0.3
負債合計	730	717	△1.8
株主資本	1,723	1,569	△8.9
利益剰余金	1,437	1,434	0.5
純資産合計	1,723	1,569	△8.9
負債純資産合計	2,453	2,286	△6.8

- 現金及び預金：
  自己株式取得の実施による減少

2023年３月期の主な取組み

ナショナルセキュリティ市場の動き

- 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」の安保３文書を策定

※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）

ナショナルセキュリティ市場の動き

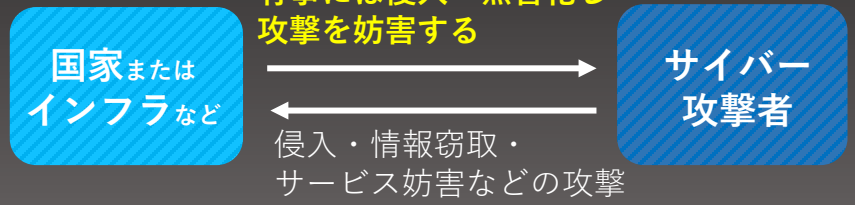
- 新たに「能動的サイバー防御」を導入。重大なサイバー攻撃のおそれがある場合、これを未然に排除する
- 国や重要インフラ等の安全等を確保するために、サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させる

※国家安全保障局「国家安全保障戦略」(令和４年12月)より抜粋

能動的サイバー防御　とは

武力攻撃に至らないものの、国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合、これを未然に排除し、また、このようなサイバー攻撃が発生した場合の被害の拡大を防止する

※国家安全保障局「国家安全保障戦略」(令和４年12月)より抜粋



被害を未然に防ぐためには、

相手方のサイバー空間の利用を妨げる能力が必要

ＦＦＲＩセキュリティでは、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してきました

当社は攻撃者の思考や手法を熟知しており、その高い技術力で安全保障実現に寄与します。

ナショナルセキュリティ市場の動き

- 陸上自衛隊通信学校を陸上自衛隊システム通信・サイバー学校に改編し、サイバー要員を育成
- 令和９年を目処に、自衛隊のサイバー関連部隊を現在の890人から約4,000人に拡充
- 適正な利益の確保など、防衛事業の魅力化を図り、力強く持続可能な防衛産業を構築する

※防衛省「国家防衛戦略」「防衛力整備計画」(令和４年12月)より抜粋

自衛隊のサイバー能力強化

妨げ能力の保有に向けた サイバー能力強化施策

陸上自衛隊通信学校を「陸上自衛隊システム通信・サイバー学校に改編

サイバー防衛部隊を令和９年度までに約4,000人へ その他のサイバー関連業務に従事する要員を含め 約２万人体制とする。また将来的には更に拡充する。

防衛産業の育成

防衛生産・技術基盤の維持・強化

研究開発・生産・維持整備・能力向上を担う防衛産業なくして我が国の防衛力は発揮し得ず、防衛産業は「防衛力そのもの」

- 品質・コスト・納期管理等を評価して企業のコストや利益を適正に算定する方式を導入し、適正な利益の確保を図る
- 設備の高度化、サイバーセキュリティ強化、サプライチェーン強靭化などの取組に対し適切な財政措置、金融支援を行う。

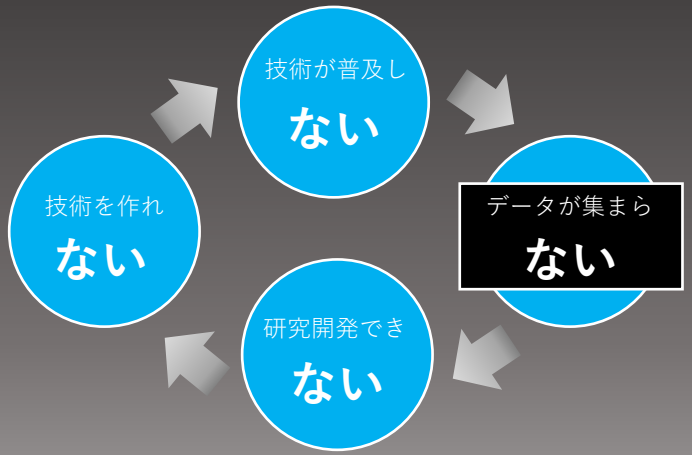
※防衛省「国家防衛戦略」「防衛力整備計画」(令和４年12月)より抜粋

ナショナルセキュリティ市場の動き

- NICT(情報通信研究機構)による脅威情報の収集・分析を進め、純国産の脅威インテリジェンスを生成するプロジェクトなど 「データ負けのスパイラル」脱却に向けた取り組みが進展

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）

脅威情報収集に向けた施策

政府端末から収集した悪意のあるソフトウェア等の情報をNICT に集約することで、わが国独自にサイバーセキュリティ情報を収集・分析可能な体制を強化する

参考：新たな総合経済対策に向けた提言（自由民主党政務調査会/令和４年10月18日）

CYNEX(サイネックス)
※NICT内部の機関

**政府機関・ベンダ
セキュリティ関連機関など**

セキュリティ情報融合基盤 **CURE**

純国産の脅威インテリジェンスの生成

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）

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
- 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
- ISO27001を取得し、案件受注に必要な組織体制整備も進む

横須賀ナショナルセキュリティR&Dセンターに『ナショナル・セキュリティ研究開発本部』を設立

将来の需要増大を見据えて体制を整備し、
エンジニアの増員及び研究開発・リサーチ能力の強化を進める

少数精鋭 → **大型・長期の案件に向けて大幅増員** → **研究開発能力・リサーチ能力を強化**

国内でほぼ唯一、サイバーセキュリティの基礎技術研究を行っている企業として、ナショナルセキュリティの領域で価値を発揮する

情報セキュリティマネジメントの国際標準規格を取得

企業としての信頼性を高めるため、
ISO27001を取得しました

登録組織：株式会社ＦＦＲＩセキュリティ　全社
認証規格：ISO/IEC 27001:2013 & JIS Q 27001:2014
登録番号：IA220193
認証機関：EQA国際認証センター

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

■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。

■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）

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%

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。

参考資料

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			

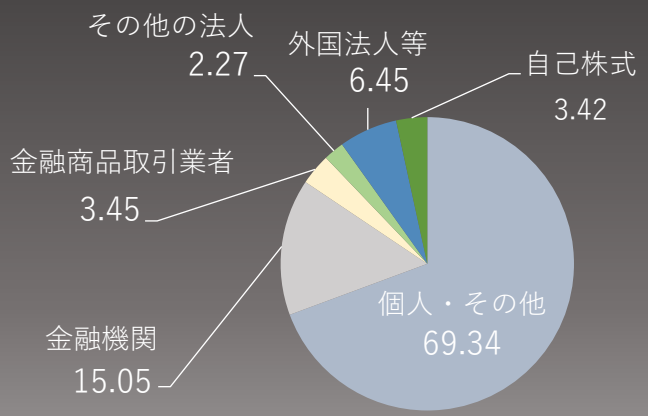
2014年9月30日　東証マザーズ市場に上場（現在はグロース市場）

株式の状況　（2022. 9 .30）

大株主（上位10名）

発行済株式数　8,190,000株
株主数　8,579名

株主構成



大株主（上位10名）	持株数(株)	持株比率(%)
鵜飼　裕司	1,942,000	24.55
金居　良治	1,441,600	18.23
BBH/SUMITOMO MITSUI TRUST BANK, LIMITED (LONDON BRANCH)/SMTTIL/JAPAN SMALL CAP FUND CLT AC	214,400	2.71
田中　重樹	170,000	2.15
CGML PB CLIENT ACCOUNT/COLLATERAL	118,100	1.49
東京短資株式会社	101,700	1.28
株式会社ＳＢＩ証券	76,100	0.96
KIA FUND F149	68,800	0.87
石山　智祥	47,000	0.59
ＪＰモルガン証券株式会社	44,395	0.56
合計	4,224,095	53.40

※1．当社は自己株式を280,233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。

中期経営計画
(2023年３月期～25年３月期)

サイバーセキュリティで
安全保障を支える

情報通信技術が社会に浸透するにつれて
サイバー空間をめぐる国家間の争いが過熱しています。

私たちは、純国産のセキュリティベンダーとして
サイバーセキュリティコア技術の研究開発を行うことで培い
磨き上げ続けてきた技術や、広範なリサーチ能力を発揮し
日本のサイバー領域における安全保障の実現に寄与します。

1．ナショナルセキュリティ市場の状況
2．日本が抱える課題と政府の取り組み
3．ＦＦＲＩセキュリティが果たすべき役割

サイバー領域における安全保障

「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

サイバー領域における安全保障

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)

サイバー領域における安全保障

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。

1．ナショナルセキュリティ市場の状況
2．日本が抱える課題と政府の取り組み
3．ＦＦＲＩセキュリティが果たすべき役割

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

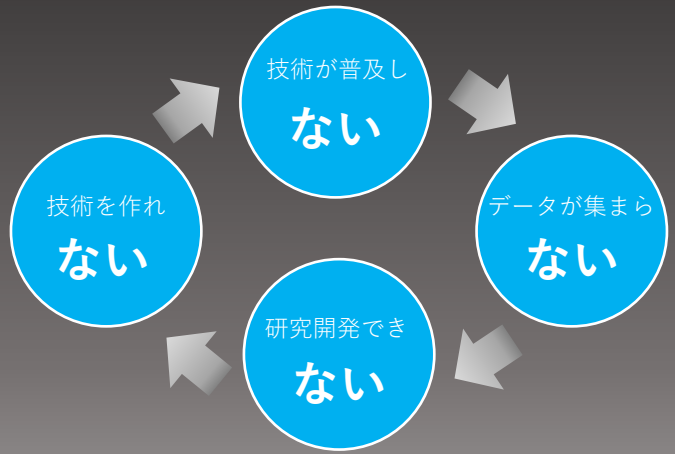
国内でどういったサイバー攻撃が発生し
ているのか、**国内にデータが存在しない**

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

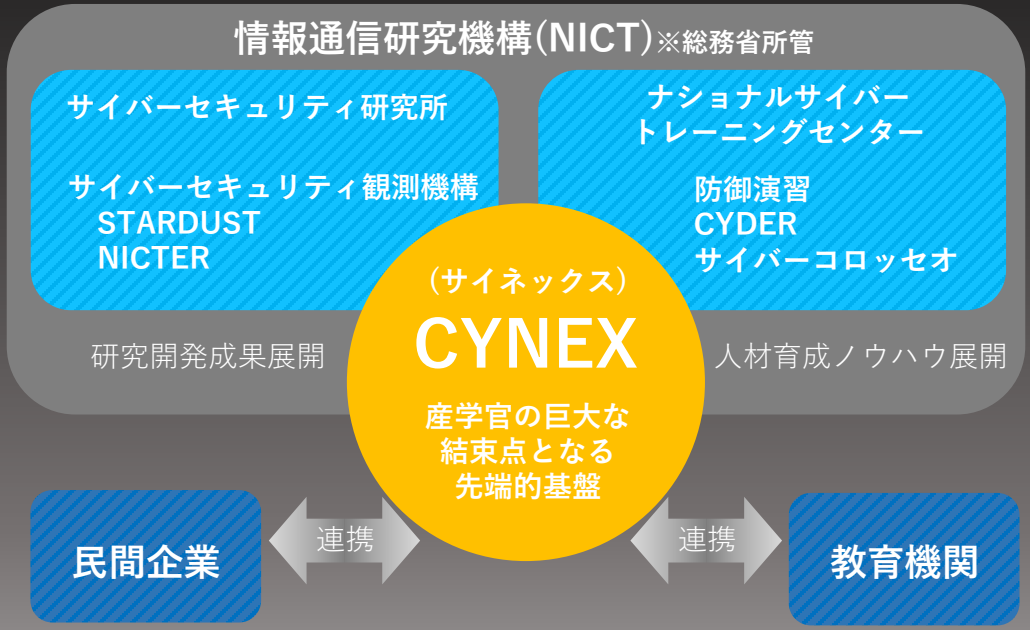
国内のサイバーセキュリティ産業育成を後押しする CYNEX を設立し、データ負けのスパイラル脱却を図る

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

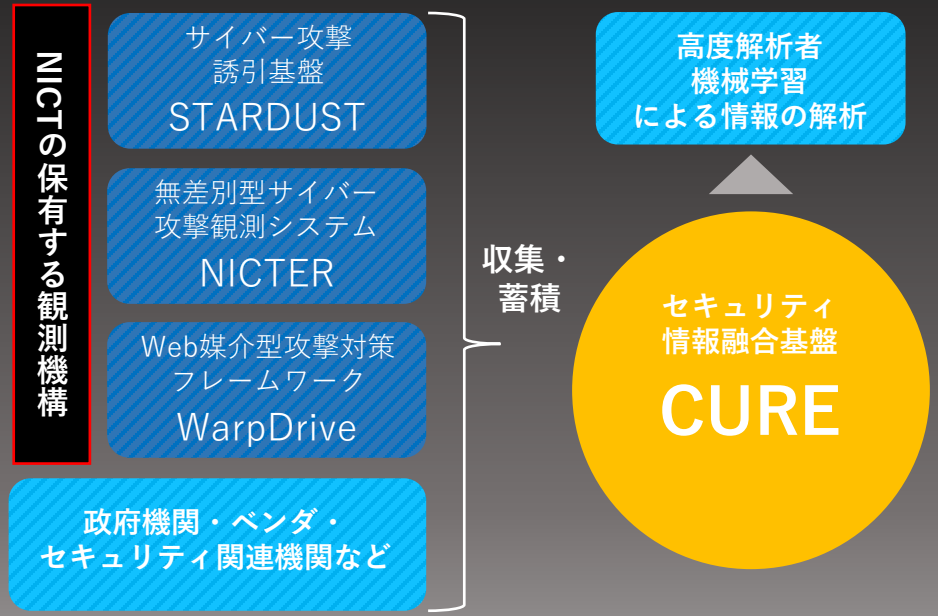
母体組織であるNICTの研究成果やサービスの一部を産学に半開放



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

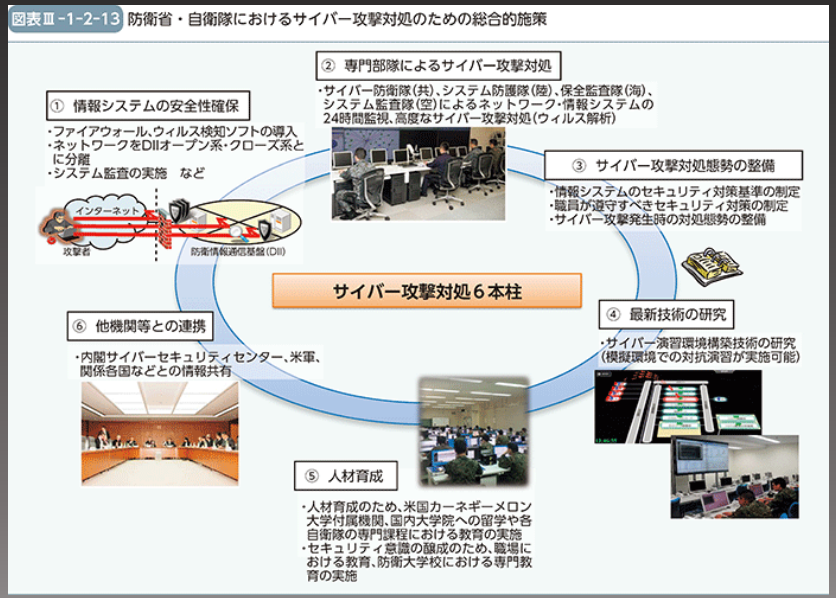
純国産サイバーセキュリティ情報の生成

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

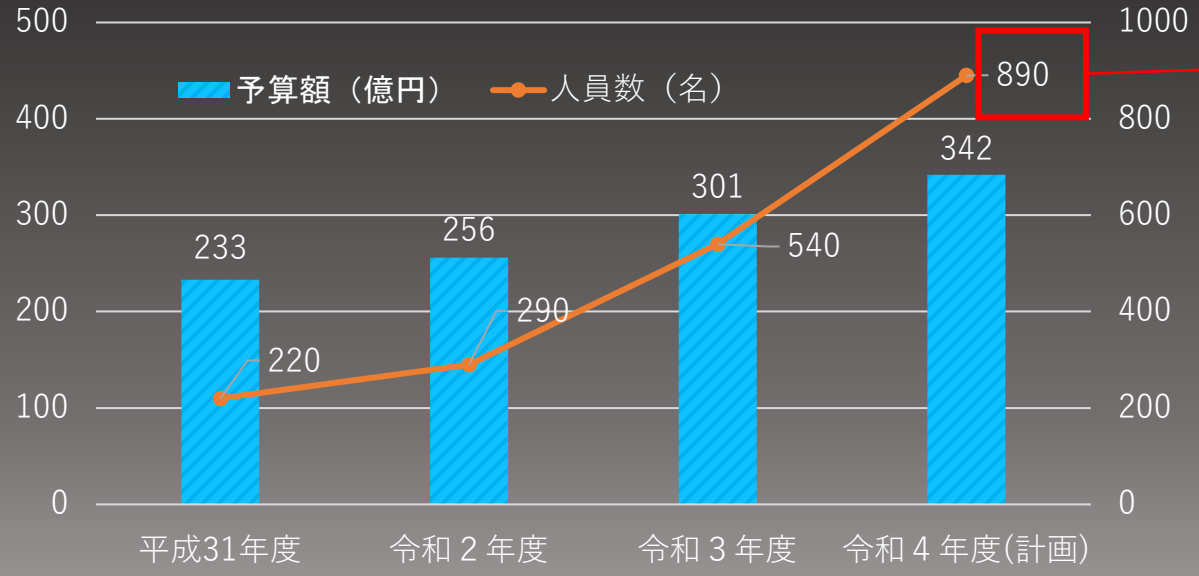
国としての優位性を獲得する上で死活的に重要な領域として、サイバー防衛能力強化を明言

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

1．ナショナルセキュリティ市場の状況
2．日本が抱える課題と政府の取り組み
3．ＦＦＲＩセキュリティが果たすべき役割

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

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

需要増大が加速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

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

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)