事業計画及び成長可能性に関する説明資料

株式会社ＦＦＲＩセキュリティ（東証マザーズ：3692）
https://www.ffri.jp

会社概要
事業環境
事業内容・強み
成長戦略
事業等のリスク
業績サマリ

会社概要

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
	専務取締役最高技術責任者	金居 良治
	常務取締役最高財務責任者	田中 重樹
	取締役 事業開発室長	川原 一郎
	取締役 製品開発本部長	梅橋 一充
	取締役（常勤監査等委員）	原澤 一彦
	社外取締役（監査等委員）	松本 勉
	社外取締役（監査等委員）	山口 功作
	社外取締役（監査等委員）	平山 孝雄
設立：	2007年7月3日	
資本金：	286,136,500円（2021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、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.上記事業に関連する一切の業務	

2014年9月30日 東証マザーズ上場

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だった。

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、「**F**ourteen**f**orty **R**esearch **I**nstitute」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

Fourteen**f**orty **R**esearch **I**nstitute

FFRIセキュリティ

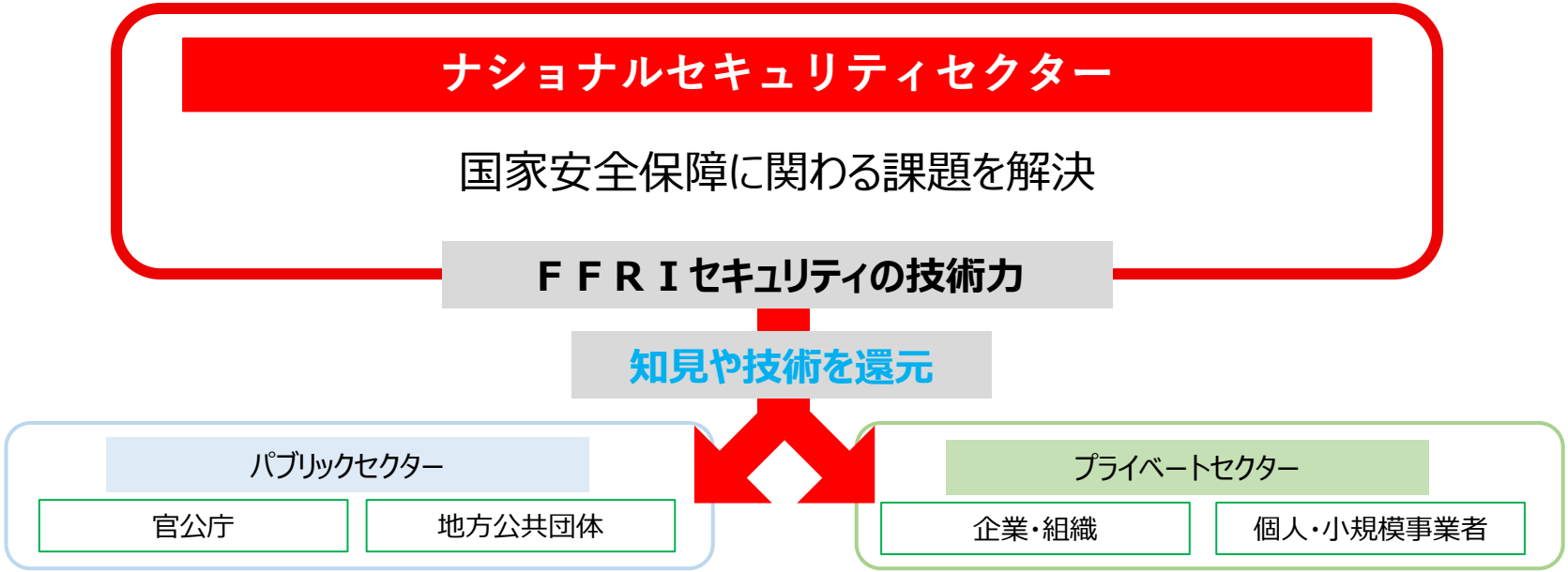
コーポレートマークにも「1440」の文字とスノーボードの回転をイメージした矢印で、設立当初から変わらない「未踏の分野への挑戦」を表現

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



事業環境

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。

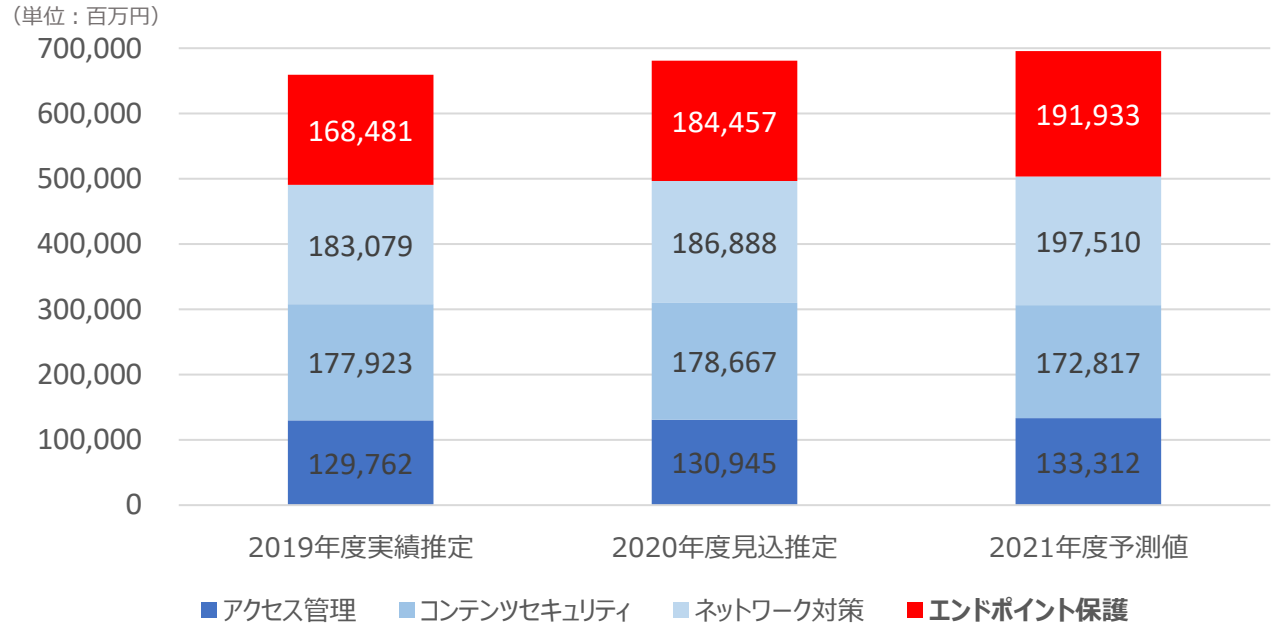
事業環境　セキュリティ市場

■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 **新たな脅威の増加 / 脅威対策製品の増加**	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。
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

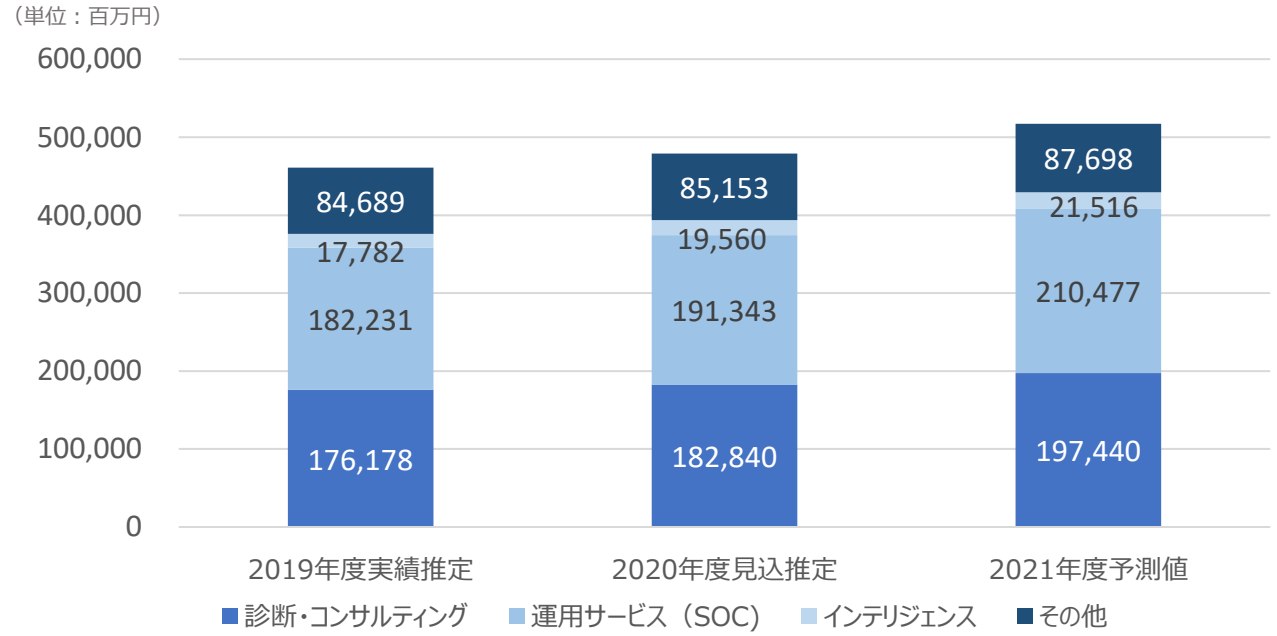
- 当社製品FFRI yaraiはエンドポイント保護製品に分類
- 国内市場はサイバー攻撃による被害の増加や、テレワークやDXの推進を受けて年々拡大している



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、セキュリティ・サービス全体で拡大傾向が続くと見込まれる

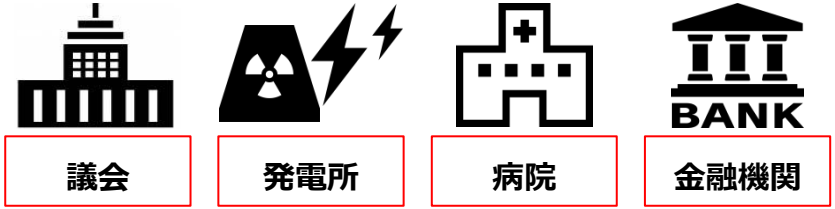


参考：JNSA調査研究部会「国内情報セキュリティ市場　2020年度調査報告」より

事業環境　ナショナルセキュリティセクター

- 近年では国家や重要インフラ施設を狙ったサイバー攻撃が世界中で増加し、
  サイバーセキュリティ対策は、国家安全保障においても重要なテーマとなっている

標的とされた重要施設



サイバー攻撃による情報漏洩や、サービスの停止などが発生

- 2017年サウジアラビアの石油化学工場が機能停止に
- 2017年イギリスの病院が診療停止に追い込まれる
- 2018年日本企業の仮想通貨流出事件
- 2021年内閣サイバーセキュリティセンターに不正アクセス　…etc

2018年改訂の防衛大綱に
サイバー防衛能力の強化を盛り込む

国家関連組織や重要インフラ企業を狙ったサイバー攻撃が世界中で発生するなど、サイバー攻撃が現代戦の重要な要素となりつつあるため、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。

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

事業環境　ナショナルセキュリティセクター

- 日本では「自衛隊サイバー防衛隊」（仮称）の新編に向けて、人材育成・確保のための予算も増加
- 防衛庁における令和３年度予算では、令和2年度に比べサイバー関連経費を増額する計画

令和３年度 サイバー関連予算の主な内訳

サイバー人材の確保・育成	約　1億円
サイバー攻撃対処に係る部外力の活用	約27億円
サイバー演習環境の整備	約16億円
サイバー攻撃対処技術の研究	約　9億円
システム・ネットワークの安全性の強化	約129億円
その他サイバー関連経費	約119億円
合計	**約301億円**

参考：防衛省「我が国の防衛と予算-令和３年度予算の概要」より

人材の育成や産学官の連携を進める意向

防衛省の令和3年度予算の概要には、「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」とするなど産学官連携を進める意向を示している。

事業環境　ナショナルセキュリティセクター

- サイバーセキュリティ先進国であるアメリカや中国に比べ日本の規模は小さく、中長期に渡って規模が拡大する見込み
- サイバー防衛隊は2022年3月末までに540名、2024年3月末までに1,000人規模へ

各国のサイバー部隊規模

国名	組織規模	備考
日本	540名	令和３年度末予定
アメリカ	約6,200名	2018年時点
中国	約30,000名	
ロシア	約1,000名	
北朝鮮	約6,800名	2019年1月時点

参考：「令和2年版防衛白書」より

令和５年度末までに
1,000名規模に拡大予定

内部にさらにハイレベルな人材の育成を目的とした**「教育専門部隊」**の新設も予定。

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

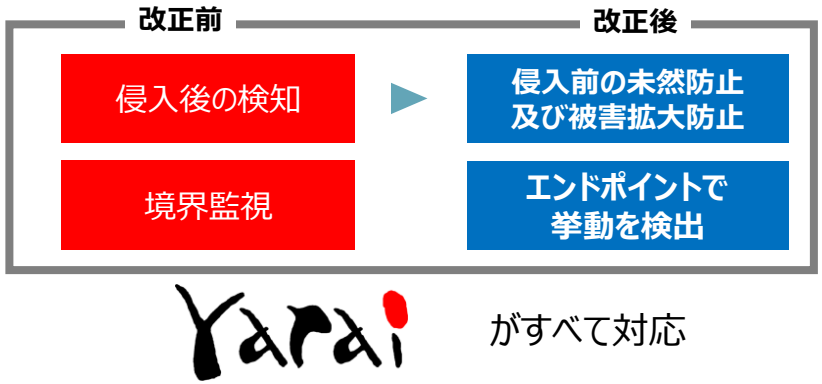
（１）将来像を見据えたサイバーセキュリティ対策の体系の進化

・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。

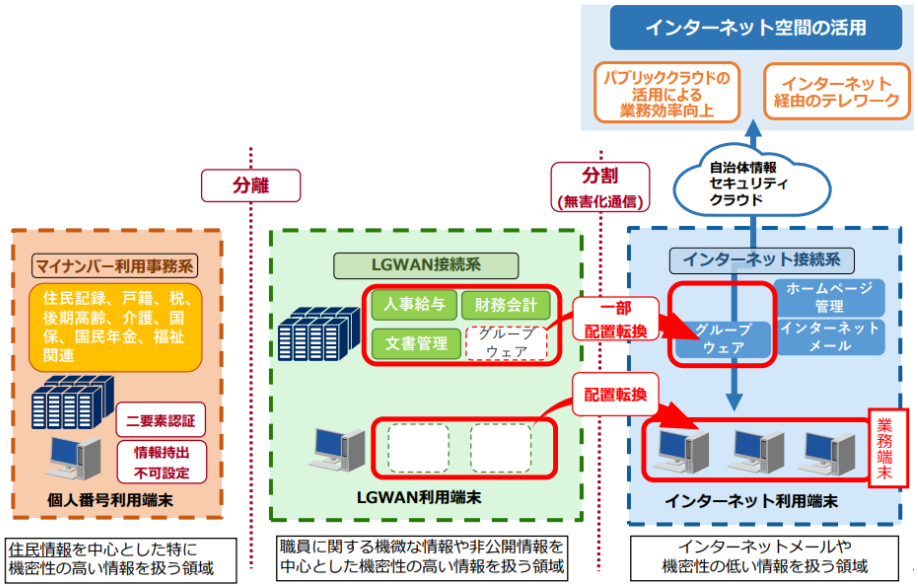
・このような機能の導入は、「監視」機能の高度化との視点でとらえることもできる。



Yarai　がすべて対応

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



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

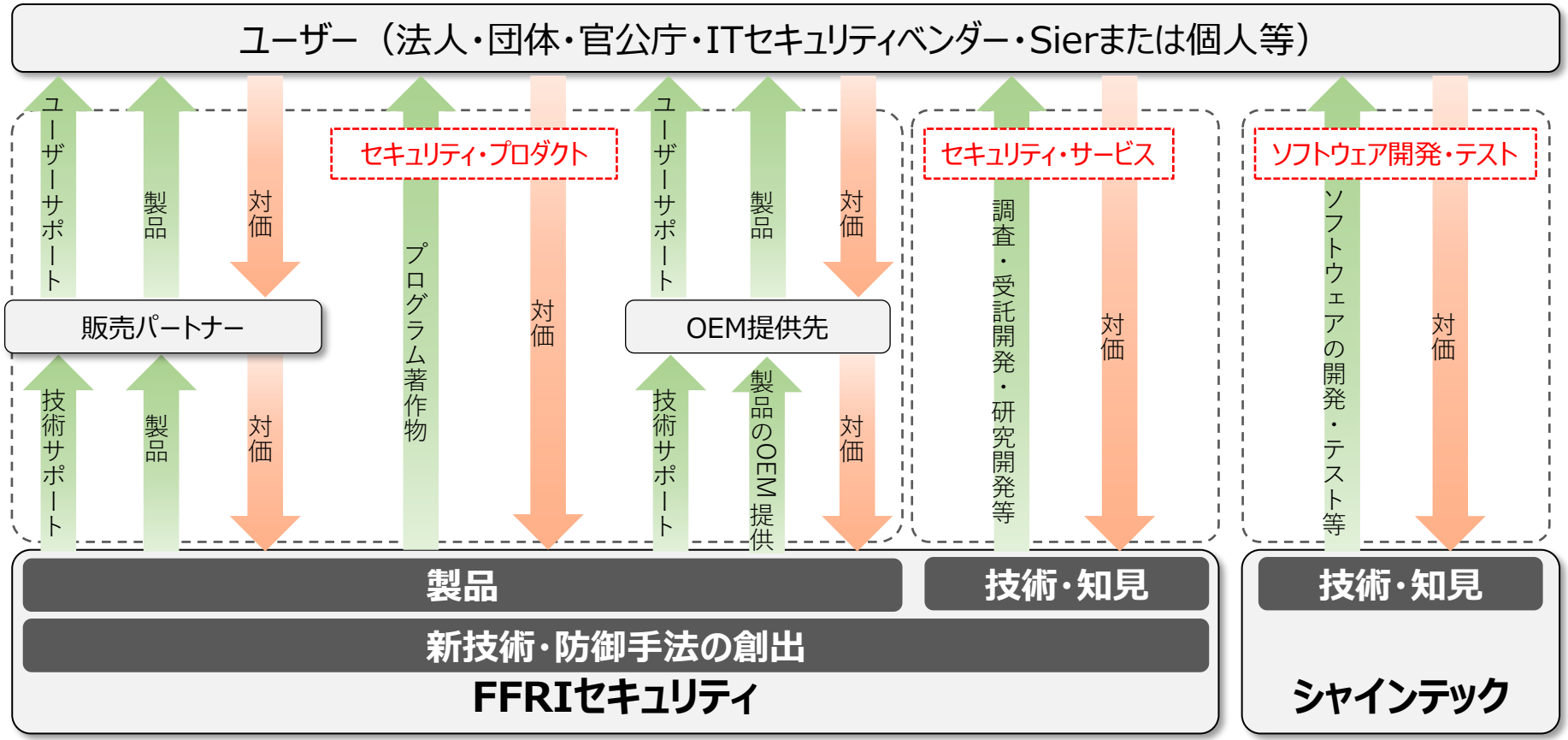
クラウドサービスの活用やテレワーク等へ対応する
効率性・利便性の高い新たなモデルを提示。

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

※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

事業の内容・強み

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
プログラム著作物
販売パートナー
OEM提供先
技術サポート
製品のOEM提供
調査・受託開発・研究開発等
ソフトウェアの開発・テスト等
製品
技術・知見
新技術・防御手法の創出
FFRIセキュリティ
技術・知見
シャインテック

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

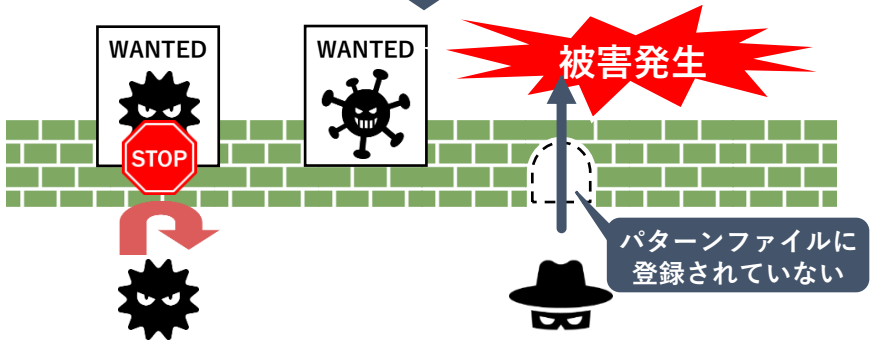
FFRI yarai の強み

- 従来のパターンマッチング型製品は、定義ファイルを用いた後追い技術であり、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

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公開している。

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」

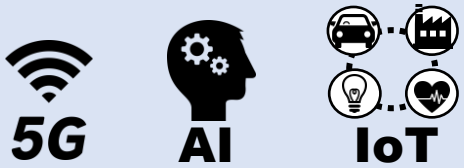
主要なセキュリティ・サービス

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

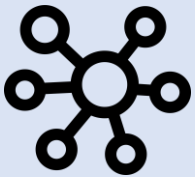


IoT機器や５Gネットワーク、AIシステムの脅威分析や、バックドア検出などのセキュリティ検査を提供します。

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

成長戦略

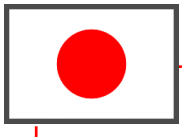
成長実現における２つの柱

1 ナショナル・セキュリティを支えるサイバーセキュリティ企業となる

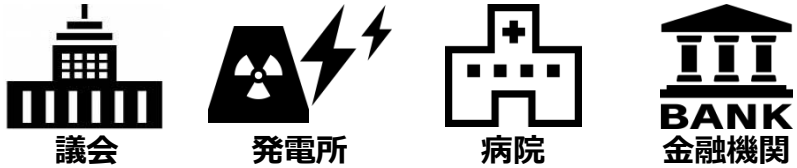
2 販売パートナーとの協業によるプロダクト販売の拡大

国内ほぼ唯一のサイバーセキュリティR&D企業

- 国家安全保障の問題解決能力を他国に依存するのはリスクが大きい
- 国内でセキュリティの基礎技術研究を行う、有力な研究開発ベンダーはほぼ当社のみ



標的とされる政府組織・重要インフラ



サイバー領域をめぐる国家間の争いが過熱

自国で問題解決できる技術力・人材の育成が急務

FFRI

- 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う
- サイバー攻撃対処技術やリサーチ能力を有する

国内のセキュリティベンダー

- コア技術は海外より輸入
- セキュリティ技術の研究開発はほぼ行われていない

ナショナル・セキュリティへと注力

- 日本発、純国産のサイバーセキュリティ企業として大きな期待
- 政府主導の取り組みにより、中長期に渡って需要の増大が見込まれる
- ナショナルセキュリティへ注力

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

日本発

純国産

高い技術力

ナショナルセキュリティセクターにおける取り組み

- 足元で需要の多いセキュリティ教育の案件を中心に実施
- 防衛産業企業と協業した、調査・研究案件や、提案活動を実施
- 提案から案件化まで１～２年の時間が必要となるため、中長期的な目線で展開

教育・研修

足元で案件が豊富

当社のノウハウが活かせる

調査・研究

最新脅威情報の収集

対策技術の研究など

提案活動

将来の案件化へ向けた

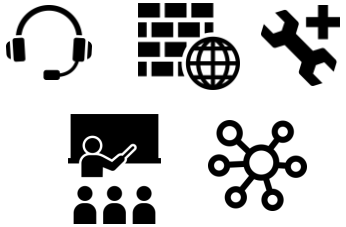
提案活動

防衛産業企業と協業

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
主な販売パートナー Soliton NEC NTT AT TKC Sky	主な販売パートナー 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

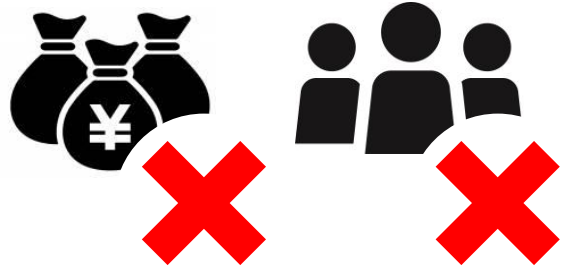
地方自治体向けソリューションの提供を開始

- 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

地方自治体

予算

人材・マンパワー



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）

事業等のリスク

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。

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への注力を進めるにあたり、セキュリティエンジニアを中心に採用の強化を進めており、採用費及び人件費等のコストが先行しているものの売上利益とも計画通りに進捗
- 売上高に占めるセキュリティ・サービスの割合増加に伴い、売上高の下期偏重傾向が強まっている
- 地方自治体のガイドライン改定及び、販売パートナーとの連携強化によりFFRI yaraiのライセンス数が増加

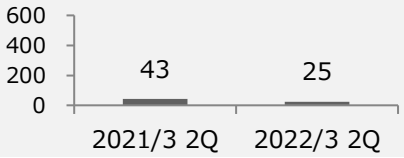
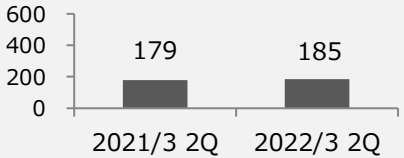
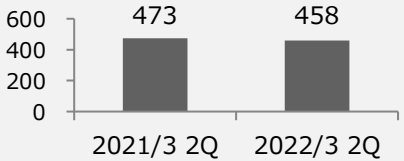
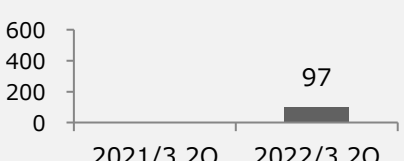
（単位：百万円）

区分	2021/3 2Q （非連結）	2022/3 2Q （連結）	増減比（%）
売上高	696	767	10.2
営業利益 （利益率：%）	54 (7.8)	△38 (△5.0)	-
経常利益 （利益率：%）	54 (7.9)	△16 (△2.1)	-
親会社株主に帰属する当期純利益 （利益率：%）	39 (5.7)	△17 (△2.2)	-

（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。

売上種類別の概況　Version2

売上高（単位：百万円）

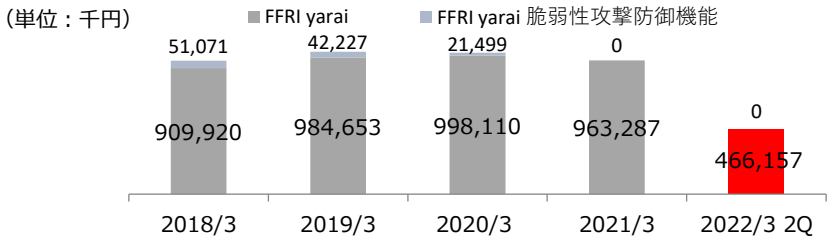
ナショナル セキュリティ セクター		・横須賀ナショナルセキュリティR&Dセンターにて国家安全保障関連の案件を受託 ・セキュリティ調査・研究や教育案件を中心に実施 ・関連省庁と協議を進め、防衛計画の実現に向けた戦略的な研究開発を実施
パブリック セクター		・NECより ActSecureX、Skyより SKYSEA Client View EDRプラスパック、NTT-AT社よりSOCサービスの提供開始。 ・販売パートナーと協力し、官公庁及び地方自治体へ向けた営業体制を強化
プライベート セクター		・OEM製品の個人・小規模事業者向け販売が増加 ・「FFRI yarai 技術者認定制度」を開始。販売パートナーとの連携を強化するとともに、エンドユーザーの満足度向上を図る。
ソフトウエア開発 ・テスト事業		・シャインテック社において、品質保証業務等を中心に提供 ※シャインテック社の業績は当第２四半期より連結開始したため、前年同期比は記載しておりません。

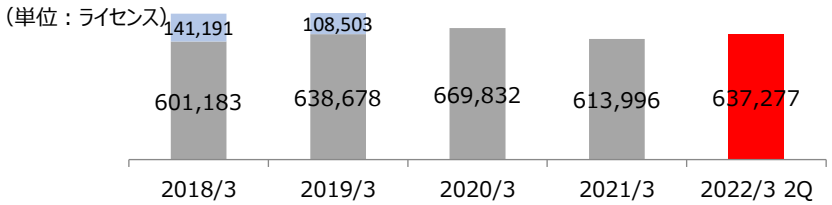
区分別四半期会計期間毎の売上推移

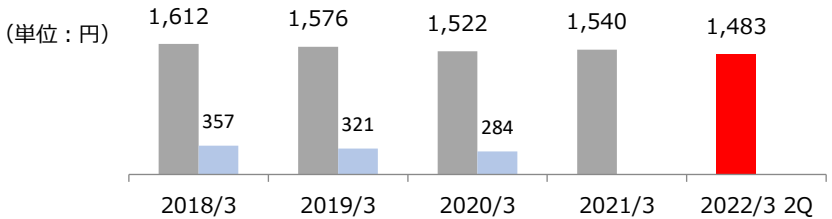
（単位：百万円）

売上区分			2021/3				2022/3			
			1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q
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	-	-
	セキュリティ・サービス		0.0	5.0	6.6	10.8	13.4	9.6	-	-
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	-	-
	セキュリティ・サービス		12.0	0.4	28.7	140.2	6.4	21.4	-	-
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	-	-
		個人	67.1	66.7	71.9	77.8	64.2	60.9	-	-
	セキュリティ・サービス		1.7	16.8	4.9	7.9	4.7	14.4	-	-
ソフトウエア開発・テスト事業			-	-	-	-	-	97.8	-	-
合計			344.2	352.4	359.6	561.9	325.7	442.1	-	-

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の影響により、前期比では減少となったものの計画には織り込み済み。

- 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、前期末に比べ23,281Licの増加となった。

- 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（ライセンス）		2022/3 2Q（ライセンス）	
		割合（%）		割合（%）
中央省庁	80,697	13.1	86,108	13.5
その他官公庁	167,783	27.3	178,238	28.0
金融サービス	117,362	19.1	117,289	18.4
運輸	43,019	7.0	39,337	6.2
情報通信	34,678	5.6	40,561	6.4
産業インフラ・サービス	41,055	6.7	43,009	6.7
その他	129,402	21.1	132,735	20.8
合計	613,996	100.0	637,277	100.0

原価及び販管費の内訳

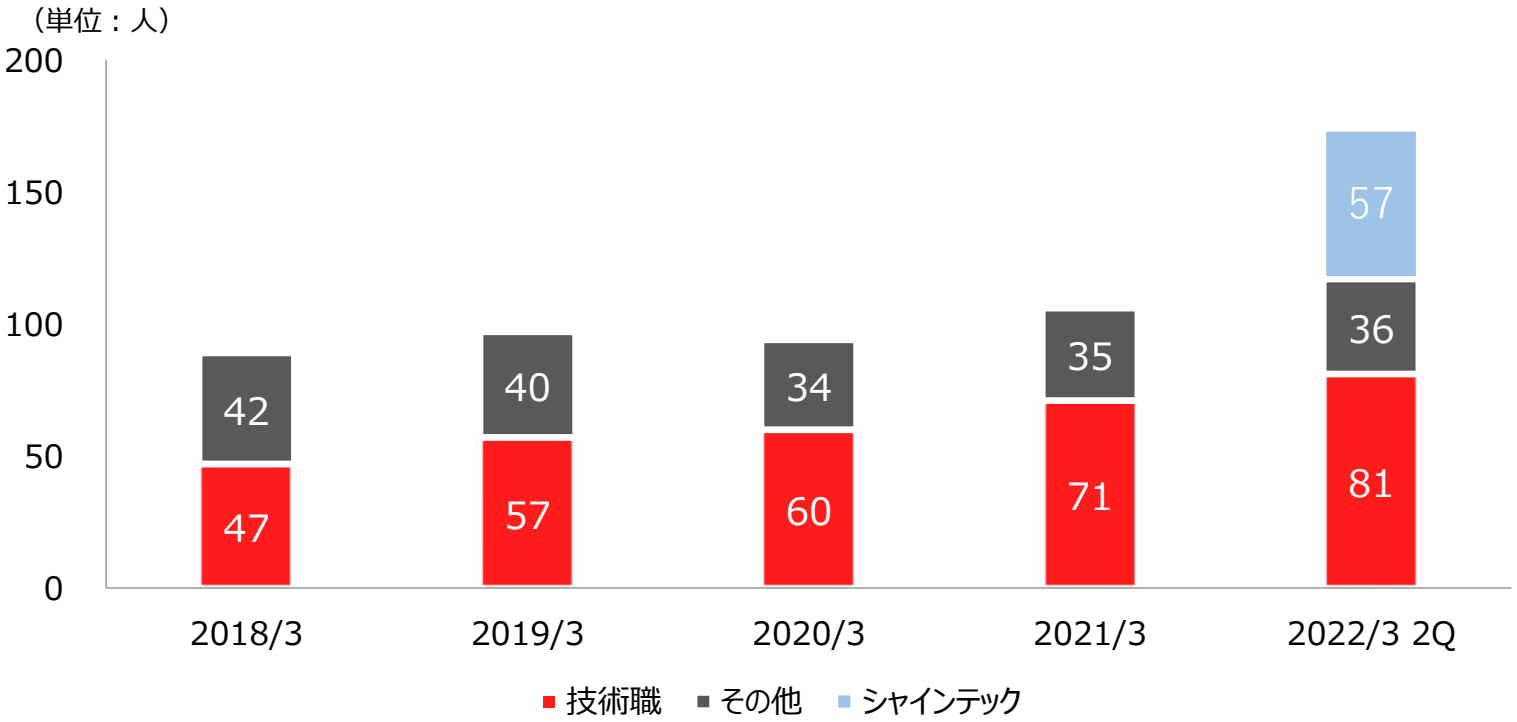
（単位：百万円）

費用の種類			2021/3 2Q（非連結）	2022/3 2Q（連結）	増減比（%）
	労務費		176	273	54.6
	経費		50	60	18.6
	期首・期末棚卸及び他勘定振替		△111	△101	-
		研究開発費への振替	△63	△19	-
		ソフトウェアへの振替	△8	△2	-
		その他の振替	△40	△79	-
売上原価合計			**115**	**232**	**102.1**
	人件費		202	237	16.9
	研究開発費		80	58	△26.5
	販売手数料		98	86	△11.8
	その他		145	190	30.9
販売管理費合計			**527**	**573**	**8.8**

- 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
57
36
81
2018/3
2019/3
2020/3
2021/3
2022/3 2Q
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）

区分		2021/3 （非連結）	2022/3 2Q （連結）	増減比（%）
	流動資産	2,381	1,843	△22.6
	現金及び預金	2,093	1,686	△19.5
	売掛金	255	118	△53.5
	固定資産	274	480	74.8
	のれん	-	136	-
資産合計		**2,656**	**2,323**	**△12.5**
	流動負債	608	733	20.6
	前受収益	451	-	-
	契約負債	-	642	-
	固定負債	205	5	△97.6
	長期前受収益	200	-	-
負債合計		**814**	**738**	**△9.3**
	株主資本	1,842	1,585	△13.9
	利益剰余金	1,295	1,299	0.3
純資産合計		**1,842**	**1,585**	**△13.9**
負債純資産合計		**2,656**	**2,323**	**△12.5**

- 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）

区分	2021/3 2Q	2022/3 2Q
営業活動によるキャッシュ・フロー	27	1
税引前当期純利益	54	△16
減価償却費	30	22
売上債権の増減額（△は減少）	137	174
前受収益の増減額（△は減少）	△124	-
長期前受収益の増減額（△は減少）	△2	-
契約負債の増減額（△は減少）	-	△41
その他	△66	△136
投資活動によるキャッシュ・フロー	△54	△136
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	1,976	1,684

- 「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

連結業績予想

- 子会社となったシャインテックの業績予想、NFLの持分法による投資利益を織り込む
- 連結決算となったことで、シャインテック株式取得に係る付随費用を損益計算書に計上する会計処理を適用
- セキュリティ・サービスの売上高の割合が増加しており、例年以上に第４四半期に偏重する見込み

（単位：百万円）

区分	2021/3実績 （非連結）	2022/3計画 （連結）	増減比（%）
売上高	1,618	2,292	41.7
営業利益 （利益率：%）	328 (20.3)	305 (13.3)	△7.0
経常利益 （利益率：%）	329 (20.4)	335 (14.6)	1.8
親会社株主に帰属する 当期純利益 （利益率：%）	249 (15.4)	238 (10.4)	△4.2

（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。

連結業績予想（売上高のセクター別内訳）

（単位：百万円）

区分	2021/3 実績（単体）	2022/3 計画（連結）	増減比 （%）
ナショナルセキュリティセクター	64	67	4.5
パブリックセクター	511	794	55.2
プライベートセクター	1,041	1,138	9.3
ソフトウエア開発・テスト事業	-	291	-
合計	1,618	2,292	41.7

（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。

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、本資料の次回開示予定日は令和４年６月を予定しております。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。