令和３年５月 14 日

各　位

会　社　名　株式会社ＦＦＲＩセキュリティ
代 表 者 名　代表取締役社長　鵜　飼　裕　司
（コード番号：3692　東証マザーズ）
問 合 せ 先　常務取締役最高財務責任者　田　中　重　樹
（ TEL. 03-6277-1518 ）

（マザーズ）令和３年３月期　投資に関する説明会開催状況について

以下のとおり、投資に関する説明会を開催いたしましたので、お知らせいたします。

○　開催状況

開催日時	令和３年５月 14 日　16：00（動画公開日時）
開催方法	インターネットを利用した動画配信及び電話会議による開催
動画掲載場所	当社ウェブサイト URL：https://www.ffri.jp/company/ir/financial-results-briefing.htm
説明会資料名	令和３年３月期　決算説明会資料

【添付資料】
令和３年３月期　決算説明会資料

以上



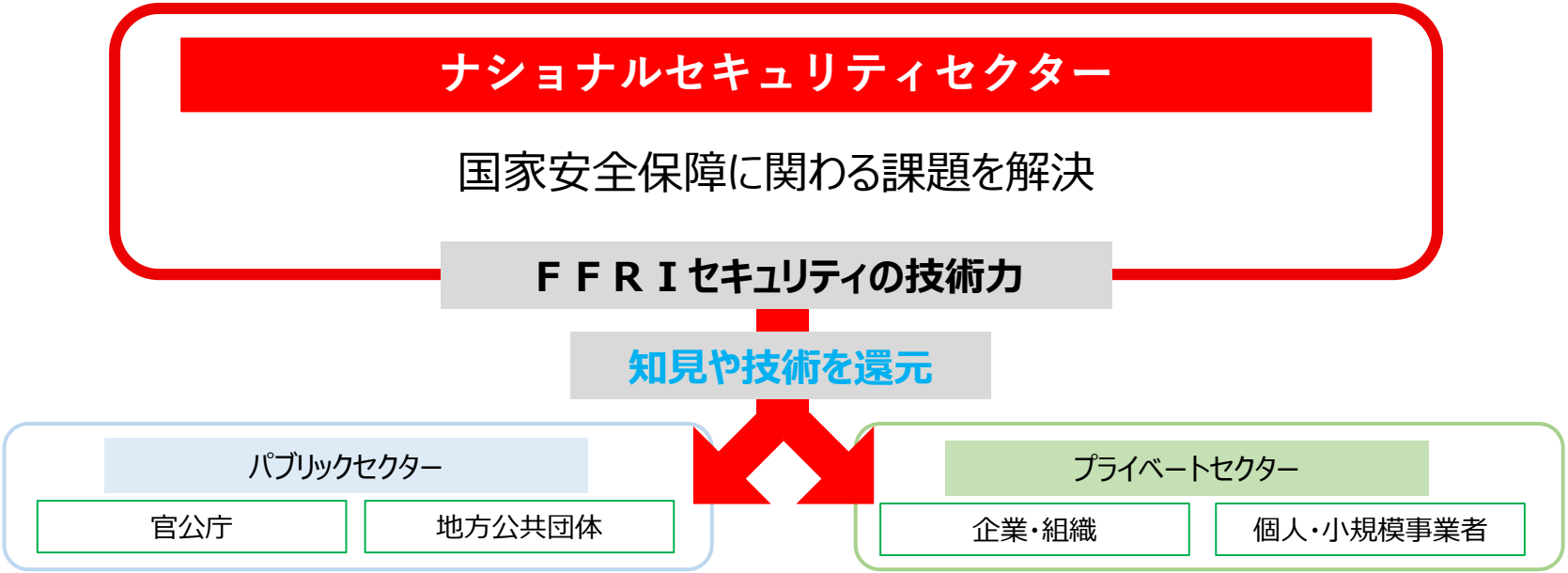
令和３年３月期
決算説明資料

株式会社ＦＦＲＩセキュリティ（東証マザーズ：3692）

https://www.ffri.jp

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



サイバー領域におけるナショナルセキュリティ　①

- 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
- 日本においても「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

図表Ⅲ-1-2-13 防衛省・自衛隊におけるサイバー攻撃対処のための総合的施策



参考：令和元年版防衛白書より

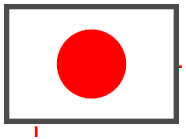
サイバー攻撃に用いられる相手方のサイバー空間の利用を妨げる能力を含め、サイバー防衛能力の抜本的強化を図る　※令和元年版防衛白書より抜粋

①サイバーセキュリティ確保のための態勢整備
②最新のリスク、対応策及び技術動向の把握
③人材の育成・確保を行う
④政府全体への取組への寄与

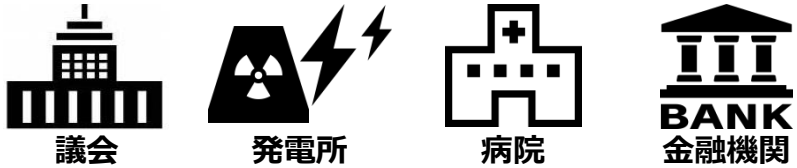
国としての優位性を獲得する上で死活的に重要な領域として、サイバー防衛能力の強化を進めている

サイバー領域におけるナショナルセキュリティ　②

- 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

- 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

サイバー領域におけるナショナルセキュリティ　③

- 日本発、純国産のサイバーカンパニーとして大きな期待
- 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



業績説明

業績サマリー

- Android版個人向け製品の売上高減少や、FFRI yarai 脆弱性攻撃防御機能のサポート終了による売上高減少があったものの、戦略的販売パートナーの販売拡大などにより売上高は前年比および計画比で微増となった
- 本社オフィスの移転にかかる一時コストや採用コストの増加を見込んでいたが、想定の範囲以下に収まり、利益は計画を上回った。

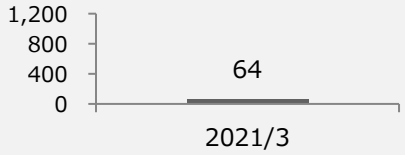
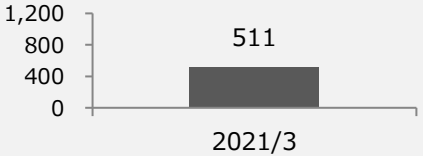
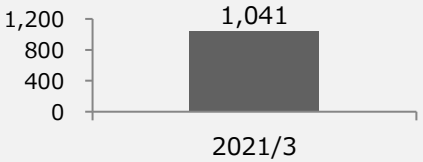
（単位：百万円）

区分	2020/3 （連結）	2021/3 （非連結）	増減比（%）
売上高	1,602	1,618	1.0
営業利益 （利益率：%）	341 (21.3)	328 (20.3)	△3.6
経常利益 （利益率：%）	341 (21.3)	329 (20.4)	△3.6
親会社株主に帰属する 当期純利益 （利益率：%）	274 (17.1)	249 (15.4)	△9.2

（注）2021年３月期より単体決算に移行しているため、2020年3月期については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

売上高（単位：百万円）

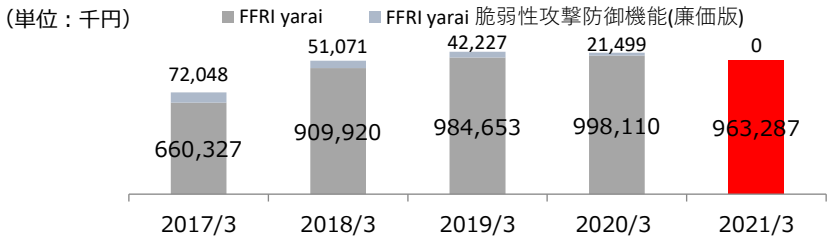
ナショナル セキュリティ セクター		・横須賀ナショナルセキュリティR&Dセンターにて国家安全保障関連の案件を受託 ・セキュリティ教育やトレーニング案件を中心に実施 ・足元で案件が増加するなど市場規模の拡大が進んでいる
パブリック セクター		・政府統一基準の改定に伴う需要の増加を背景に、プロダクト販売における新規案件が増加した。 ・販売パートナーと協力し、官公庁及び地方自治体へ向けた営業体制を強化。
プライベート セクター		・戦略的販売パートナーによる販売か拡大した ・個人や小規模事業者への販売強化に向けて、販売パートナー各社と連携を強化、新たにOEM提供を開始するなど、販売拡大に向けた協業体制を強化した。

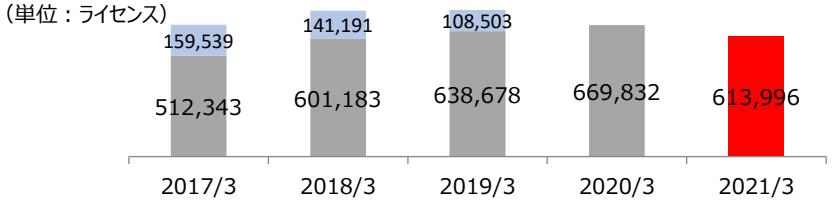
区分別四半期会計期間毎の売上推移

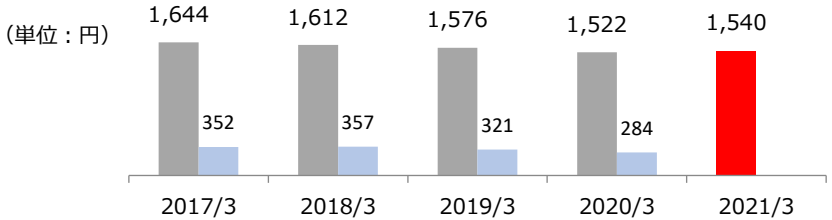
（単位：百万円）

売上区分			2021/3			
			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
	セキュリティ・サービス		0.0	5.0	6.6	10.8
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
	セキュリティ・サービス		12.0	0.4	28.7	140.2
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
		個人	67.1	66.7	71.9	77.8
	セキュリティ・サービス		1.7	16.8	4.9	7.9
合計			344.2	352.4	359.6	561.9

FFRI yarai シリーズの販売状況







FFRI yarai 売上高

FFRI yarai 脆弱性攻撃防御機能のEOLに伴う契約減少及び、大口顧客の満了などにより前期比で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（19/3→20/3継続率 92.0%）

約70,000Licの大口顧客の満了などがあったものの、官公庁向けの販売が引き続き好調に推移し、全体では前期末に比べ55,836Licの減少となった。

FFRI yarai 売上単価

大規模導入先の契約ライセンス数減少により売上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	2020/3（ライセンス）		2021/3（ライセンス）	
		割合（%）		割合（%）
中央省庁	156,563	23.4	80,697	13.1
その他官公庁	146,721	21.9	167,783	27.3
金融サービス	139,914	20.9	117,362	19.1
運輸	69,338	10.4	43,019	7.0
情報通信	38,543	4.7	34,678	5.6
産業インフラ・サービス	31,771	5.8	41,055	6.7
その他	86,982	13.0	129,402	21.1
合計	669,832	100.0	613,996	100.0

原価及び販管費の内訳

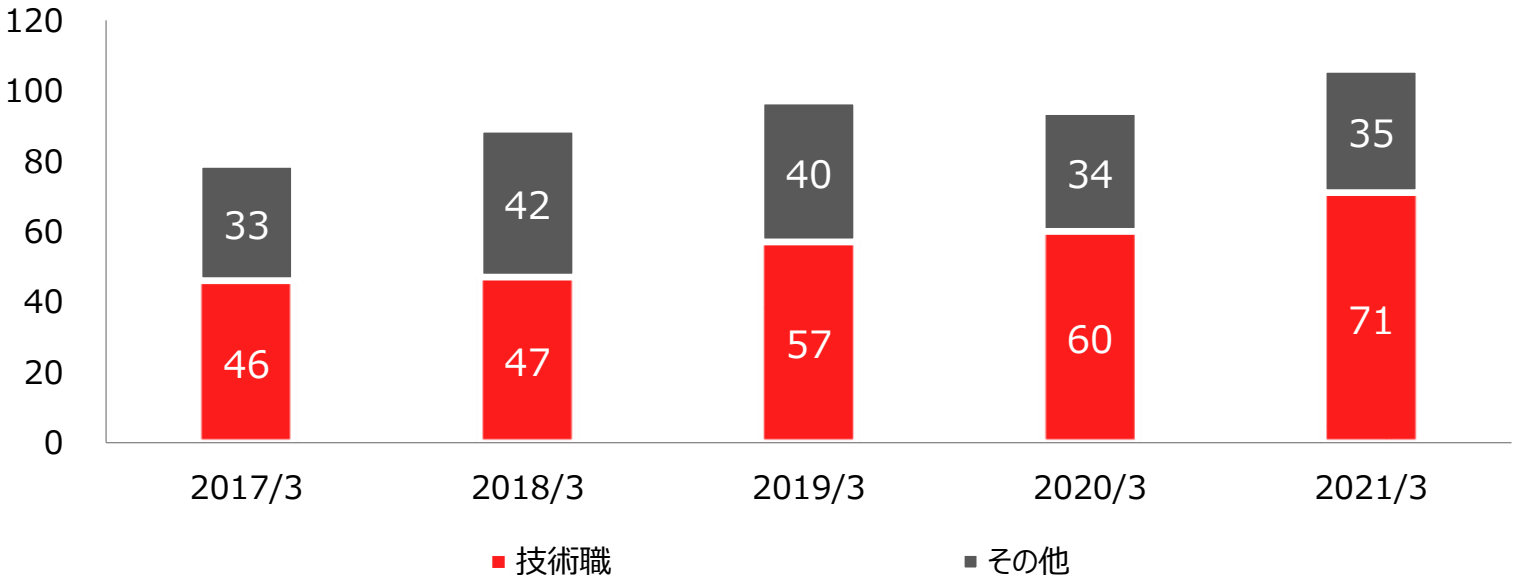
（単位：百万円）

費用の種類			2020/3 (連結)	2021/3 (非連結)	増減比（%）
	労務費		318	369	16.0
	経費		115	104	△10.3
	期首・期末棚卸及び他勘定振替		△116	△183	-
		研究開発費への振替	△67	△103	-
		ソフトウェアへの振替	△52	△23	-
		その他の振替	3	△55	-
売上原価合計			**317**	**289**	**△8.8**
	人件費		397	401	0.9
	研究開発費		100	138	38.5
	販売手数料		220	190	△13.6
	その他		224	269	19.8
販売管理費合計			**942**	**999**	**6.0**

- 労務費：主に技術人員の採用に伴う増加
- 研究開発費：FFRI yaraiの機能向上に関する研究
- 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：移転に伴う一時費用及び、採用コストの増加

人員数の推移

（単位：人）


120
100
80
60
40
20
0
33
42
40
34
35
46
47
57
60
71
2017/3
2018/3
2019/3
2020/3
2021/3
技術職
その他

業績サマリー（貸借対照表）

（単位：百万円）

区分	2020/3（単体）	2021/3（単体）	増減比（%）
流動資産	2,272	2,381	4.8
現金及び預金	2,016	2,093	3.8
売掛金	185	255	37.9
固定資産	256	274	7.0
資産合計	**2,529**	**2,656**	**5.0**
流動負債	696	608	△12.7
前受収益	566	451	△20.3
固定負債	240	205	△14.3
長期前受収益	240	200	△16.4
負債合計	**936**	**814**	**△13.1**
株主資本	1,592	1,842	15.6
利益剰余金	1,046	1,295	23.8
純資産合計	**1,592**	**1,842**	**15.6**
負債純資産合計	**2,529**	**2,656**	**5.0**

業績サマリー（キャッシュ・フロー）

（単位：百万円）

区分	2020/3	2021/3
営業活動によるキャッシュ・フロー	193	120
税引前当期純利益	331	329
減価償却費	59	59
売上債権の増減額（△は減少）	△31	△70
前受収益の増減額（△は減少）	△5	△114
長期前受収益の増減額（△は減少）	△57	△39
その他	△102	△44
投資活動によるキャッシュ・フロー	△65	△42
財務活動によるキャッシュ・フロー	△0	0
現金及び現金同等物の期末残高	2,016	2,093



2021年3月期の主な取組み

2021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 ・横須賀ナショナルセキュリティR&Dセンターにおいて、ナショナルセキュリティにおけるサイバーセキュリティの課題解決となるソリューションを提供する
パブリックセキュリティセクター	・増加する官公庁の需要に対応するため専門のチームを組成し販売活動を行う ・霞が関至近に本社を移転し、業務効率化を図る
プライベートセクター	・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 ・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 ・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　市場環境①

- 防衛産業を狙ったサイバー攻撃被害が相次いで報告されている
- 防衛省はサイバー攻撃対処能力などを強化し防衛機密の流出防止を進めている

主な報道

・防衛省・官公庁・インフラ系企業の企業秘密が流出した疑い
・防衛省との取引情報に対する不正アクセス
・最新鋭兵器の性能に関する情報が漏えいした疑い
・防衛省の設備情報が流出した疑い
・潜水艦用装備を製造する企業に対する不正アクセス
・基地の測量などを行う企業に対する不正アクセス

防衛関連企業がサイバー攻撃の標的に

ガバナンス体制の確立、管理体制の構築、システムへのセキュリティ対策の導入と運用、
監査の実施など、多岐にわたる新たな基準を設け、産業界全体の対策水準の強化を図る
→防衛装備庁装備保全管理官「産業サイバーセキュリティ室（仮称）」を新設予定

参考：防衛装備庁「防衛装備庁における情報セキュリティ基準の改正に係る取組」より

ナショナルセキュリティセクター　市場環境②

- 防衛庁における令和３年度予算の概算要求では、令和2年度に比べサイバー関連経費を増額する計画
- 「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

令和３年度予算の主な内訳

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**

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。

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

ナショナルセキュリティセクター　市場環境③

- 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
- サイバー防衛の教育専門部隊が陸海空の共同部隊として新設
- 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	290名	2021年3月末時点
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

2022年3月末までに
540名に拡大予定

現在のサイバー防衛隊に、自衛隊指揮通信システム隊を併合、増員し540名の部隊とする。
また、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」**を新設する。

2021年3月期の主な取り組み　①

- 横須賀ナショナルセキュリティR&Dセンターを開設し、周辺組織と協力し研究開発や案件受諾を進める
- 初年度は教育・トレーニング案件を中心に、提案活動なども並行して進めている

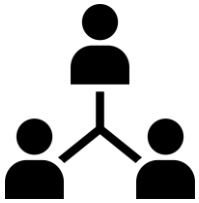


横須賀ナショナル
セキュリティR&Dセンター

＜2020年3月開設＞



防衛産業企業

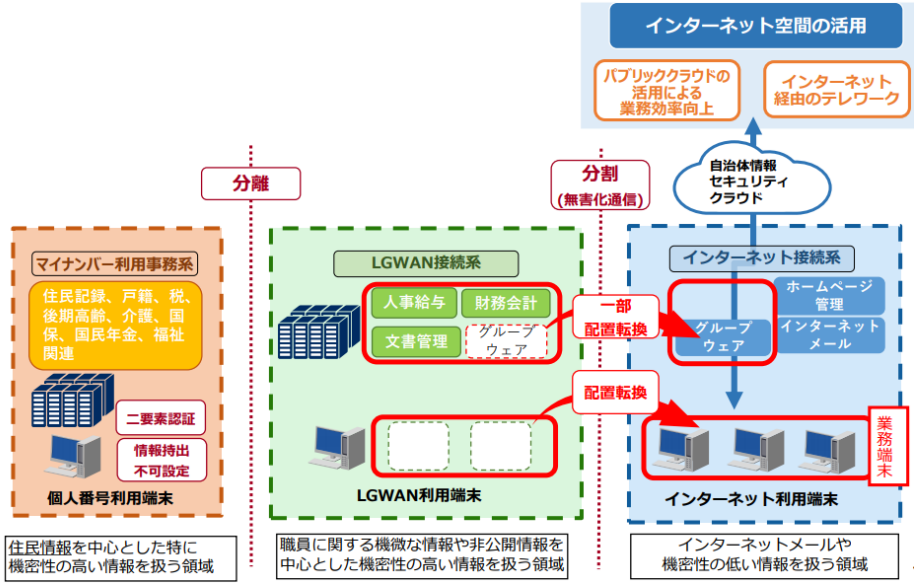


周辺組織
関連企業・組織

周辺組織と連携した活動

パブリックセクターの市場環境　①

- 地方自治体向け情報セキュリティポリシーの改定に向けた検討会が総務省主導で進行中
- 新たなモデル（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

2021年3月期の主な取り組み ②

- 販売パートナー各社と連携し、官公庁・地方公共団体に対する販売力を強化
- OEM提供や、販売キャンペーンの実施を進める
- パブリックセクター専門のチームを設立や、霞が関至近へのオフィス移転など体制の整備

FFRI
- 専門のチームを新設
- オフィスを東京都千代田区に移転
  霞が関へのアクセスを改善

NTT AT　NEC　TKC　Sky

緊密な連携を構築

官公庁

地方自治体

- キャンペーンなど販促活動を共同で実施
- OEM製品・サービスの提供
- 共同研究の実施

2021年3月期の主な取り組み ③

- 株式会社アレクソンへのFFRI yarai Home and Business Edition の提供開始
- 株式会社No.1を加えた３社協業による、個人・小規模事業者向け製品及びサービスの共同開発を行う

FFRI　高度なセキュリティ技術や製品

ALEXON 株式会社 アレクソン　小規模事業者や個人向け製品の開発/販売/サポートのノウハウ

株式会社 No.1　小規模事業者の顧客ニーズ

3社協業による製品・サービスの開発

３社のそれぞれの強みを生かし、製品・サービスの共同開発を行う

第１弾としてアレクソンより
UTMの販売が開始となった
（9月23日販売開始）

UTM ・・・ 複数の異なるセキュリティ機能を一つのハードウェアに統合し、集中的にネットワーク管理を行う製品



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

2022年3月期の主な取り組み ①　ナショナルセキュリティセクター

- 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

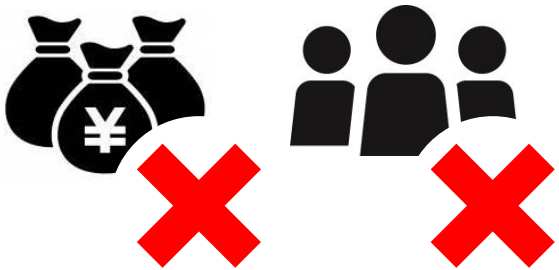
防衛産業企業と協業

2022年3月期の主な取り組み ②　パブリックセクター

- 地方公共団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
- 地方自治体は予算・人材とも不足しているケースが多い
- 販売パートナーと協力し、地方自治体の抱える課題解決となる製品・サービスを提供する

地方自治体

予算　人材・マンパワー



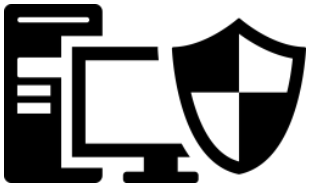
予算・人材とも不足しているケースが多い

販売パートナー各社と協力し、
付加価値の高い製品・サービスを提供

・Sky　SKYSEA Client View EDRプラスパック
　NEC　ActSecure χ　など
・人材不足を解消し、コストを低減する
　マネージドサービスなど、地方自治体のそれぞれの
　課題を解決するソリューションを提供する

2022年3月期の主な取り組み ③ プライベートセクター/その他

◘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を強化
・個人や小規模事業者への強い販路を持つ販売パートナーへのOEM提供や
OEM製品の販売促進を協力して進める
・新たなOEM提供先や販売パートナーの獲得を進める

◘優秀なエンジニアの採用を加速



ナショナルセキュリティ事業への注力を進めるにあたり、セキュリティエンジニアの増員が必須。
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

2022年3月期の主な取り組み ④ その他

◻NFラボラトリーズより、優秀な高度セキュリティ人材の育成と輩出を継続

NFLabs.

NTT Comとの合弁会社(2019年１月設立)

・教育・研修事業に加え、業務受託事業が好調
・収益・利益とも順調に進捗
・高度セキュリティ人材の育成と輩出を継続

◻株式取得によりシャインテック社を完全子会社化予定

Shine Tec

株式会社シャインテック
（神奈川県川崎市）

・2003年の設立以来、プロジェクトマネジメントや
ソフトウェア評価業務を行う
・当社の持つセキュリティ技術を組み合わせ、サイバー・セキュリティを
含めた、より幅広いサービスの提供を行う

2022年3月期の主な取り組み ⑤ その他

- 自己株式取得による株主還元を実施
- 今後も中長期的に、利益の中から株主還元施策を実施予定

取得内容

取得対象株式の種類	普通株式
取得し得る株式の総数	120,000株（上限）
株式の取得価額の総額	３億円（上限）
取得期間	令和３年５月19日～６月18日
取得の方法	東京証券取引所における市場買付け

業績予想

（単位：百万円）

区分	2021/3実績	2022/3計画	増減比（%）
売上高	1,618	2,001	23.7
営業利益 （利益率：%）	328 (20.3)	295 (14.8)	△10.2
経常利益 （利益率：%）	329 (20.4)	295 (14.8)	△10.4
当期純利益 （利益率：%）	249 (15.4)	204 (10.2)	△17.8

業績予想（売上高の内訳）

（単位：百万円）

区分	2021/3 実績	2022/3 計画	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
合計	1,618	2,001	23.7

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。



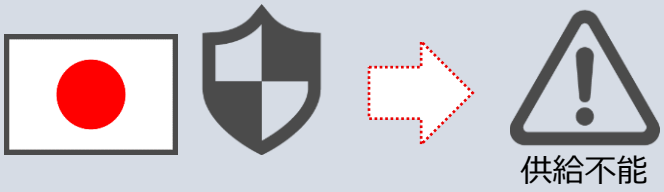
参考資料

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

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	川原　一郎
	取締役	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



市場環境

市場環境 ①

■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



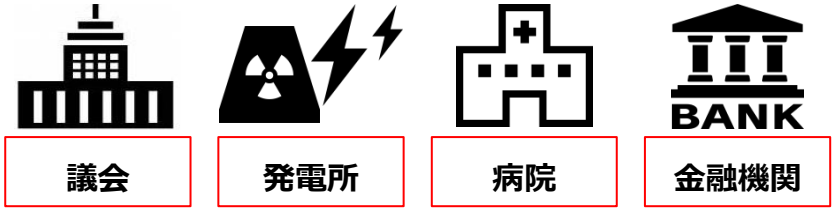
政治的目的

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。

市場環境　②

- 国家や重要インフラ施設を狙ったサイバー攻撃が増加し、安全保障において重要なテーマとなっている
- 横須賀ナショナルセキュリティＲ＆Ｄセンターを開設し、課題解決へ向けた研究開発を加速する

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
- 2017年イギリス議会が攻撃を受け、ネットワーク遮断状態に
- 2018年日本企業の仮想通貨流出事件　…etc

サイバー・セキュリティ対策が国家安全保障の重要なテーマに

日本においては、2018年頃から法律やガイドラインの改正が進むが、未だ十分とは言えない状況。

ＦＦＲＩでは

横須賀ナショナルセキュリティＲ＆Ｄセンターを開設
国家や組織の課題解決に注力する

市場環境 ③

■ここ数年でサイバー脅威及び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
2014年：	サイバーセキュリティ基本法 成立
2015年：	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	
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

「標的型攻撃」が連日ニュースに取り上げられる

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。

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。

市場環境 ④

多様な製品・サービスが市場に提供され、ユーザー企業では導入是非の判断が難しくなっている

多様なセキュリティ製品・サービス群

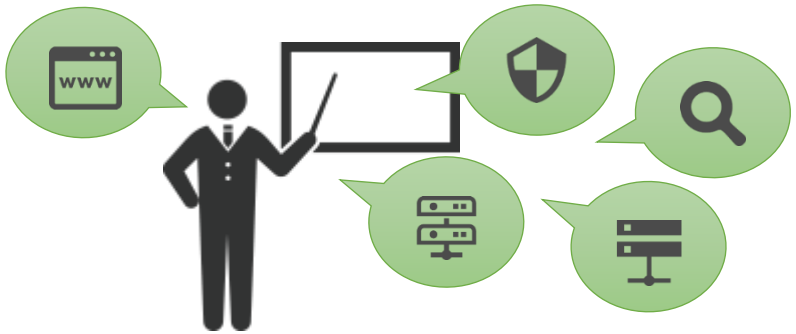
NGEPP製品※　EDR製品　IPS/IDS　サンドボックス　etc…



ユーザー組織

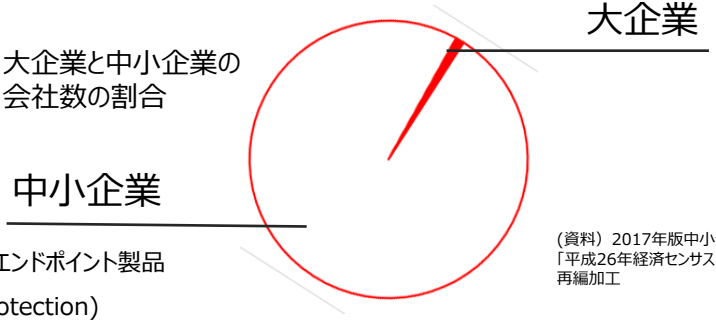
※NGEPP：マルウェアを検出して被害を防止するエンドポイント製品
(Next Generation Endpoint Protection)

ユーザーへの営業強化の重要性が高まる



大企業以外はセキュリティ市場の空白地となっている

大企業と中小企業の会社数の割合



（資料）2017年版中小企業白書
「平成26年経済センサス－基礎調査」
再編加工

市場構成

■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

■主力製品「FFRI yarai」は次世代エンドポイントセキュリティ（NGEPP）に分類。
標的型攻撃や、ゼロデイ攻撃などの未知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

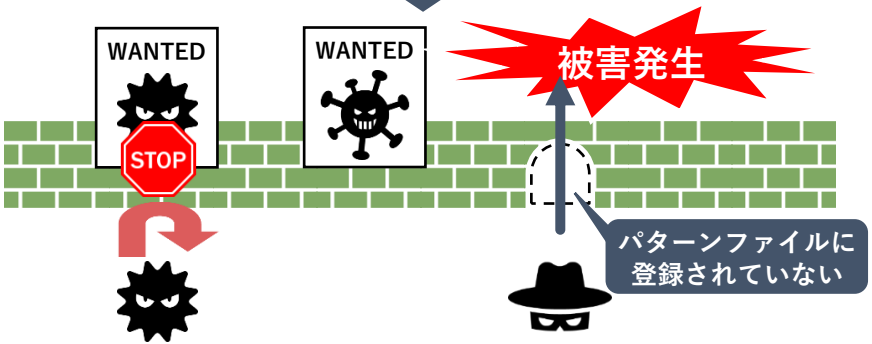
・EDR製品

Ｅ社
Ｆ社　など

FFRI yarai の強み

- 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出来る。

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

振る舞い検知型マルウェア対策
（先読み技術）



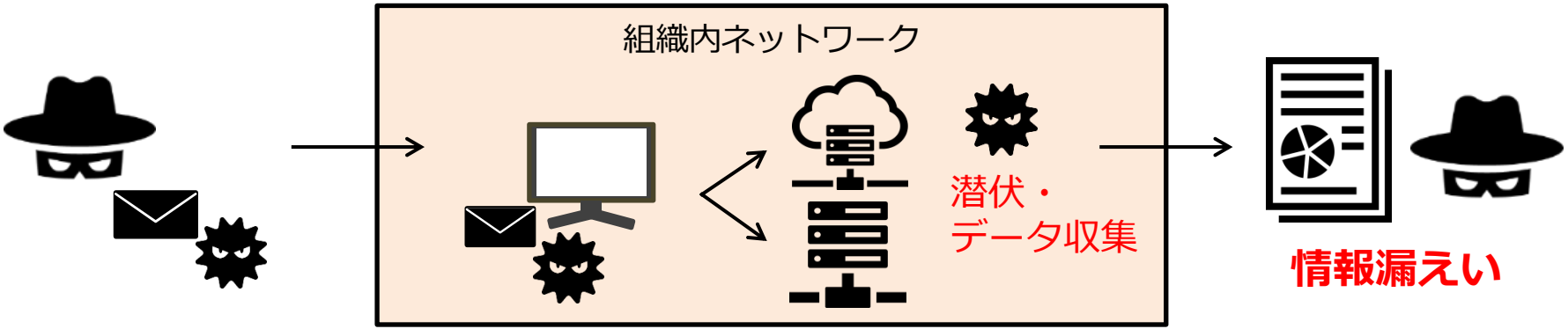
マルウェア特有の怪しい振る舞いなどの特徴を判断
未知のマルウェアも検知

感染を「防御」することの経済性

- サイバー・セキュリティは、「入口対策をしっかり行った方が、対策コストが少なくて済む」
  予防医学と同様で、感染しない人が増えるとリスクも減るということ。　（東京電機大学　教授　佐々木良一氏）
  https://japan.zdnet.com/extra/security_vmware_201706/35103308/

入口対策　侵入防止・感染防御型
NGEPP(FFRI yarai)、ウイルス対策、FW等

出口対策　検知・インシデントレスポンス型
EDR・ゲートウェイ、監視サービス等



パブリックセクターの市場環境

■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。
官公庁など政府関連機関に対し、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

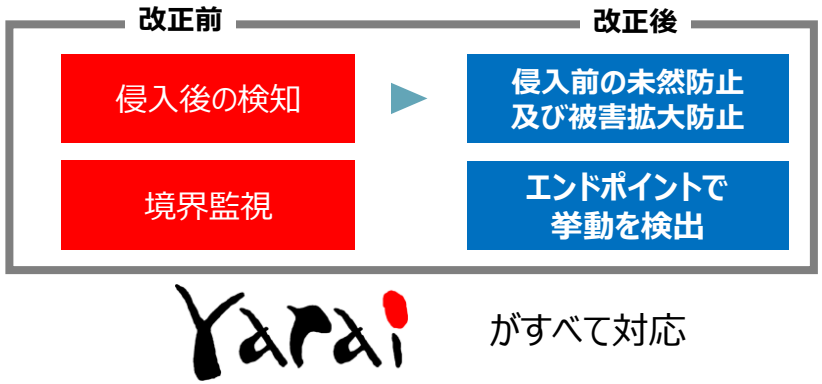
（1）将来像を見据えたサイバーセキュリティ対策の体系の進化

・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。



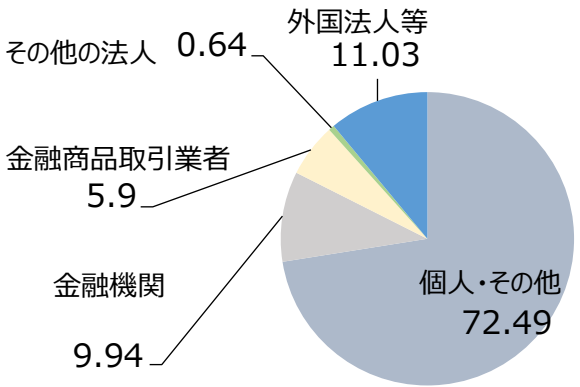
Yarai がすべて対応

株式の状況　（2021.3.31）

発行済株式数　8,190,000株

株主数　8,187名

株主構成



大株主（上位10名）

株主名	持株数（株）	持株比率（%）
金居　良治	1,626,000	19.85
鵜飼　裕司	1,342,000	16.39
特定有価証券信託受託者　株式会社ＳＭＢＣ信託銀行	600,000	7.33
BBH/SUMITOMO MITSUI TRUST BANK, LIMITED (LONDON BRANCH)/SMTTIL/JAPAN SMALL CAP FUND CLT AC	326,000	3.98
BNYM AS AGT/CLTS 10 PERCENT	319,876	3.91
株式会社日本カストディ銀行（信託口）	203,700	2.49
田中　重樹	176,000	2.15
株式会社ＳＢＩ証券	137,000	1.67
楽天証券株式会社	100,900	1.23
BNP PARIBAS ARBITRAGE SNC	81,305	0.99
合計	4,912,781	59.99