令和３年３月期第２四半期
決算短信補足説明資料

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

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（2020年9月30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	

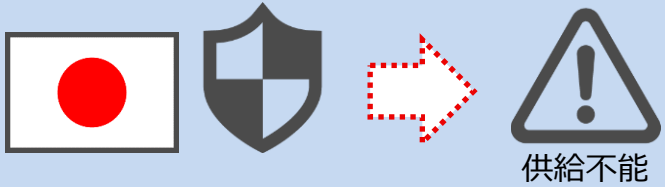
2014年9月30日 東証マザーズ上場

設立の経緯

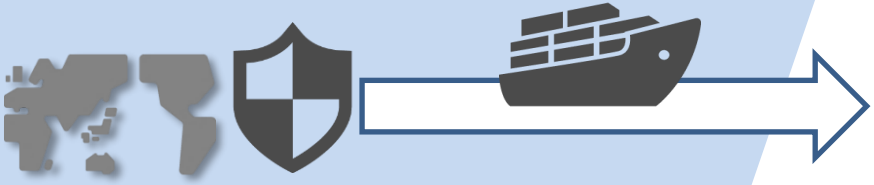
- これまで日本は対策技術を海外からの輸入に頼っていた…

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

市場環境

市場環境

■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

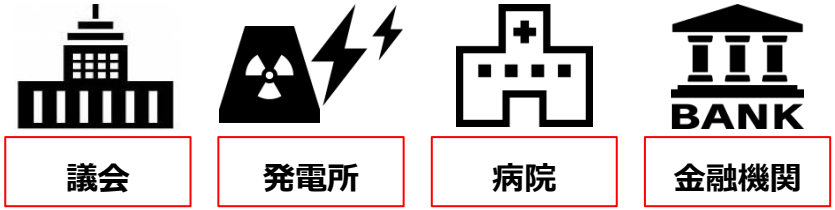
政治的目的

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

- 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

■ここ5年ほど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	「標的型攻撃」が連日ニュースに取り上げられる
2014年：	サイバーセキュリティ基本法 成立	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。
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	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

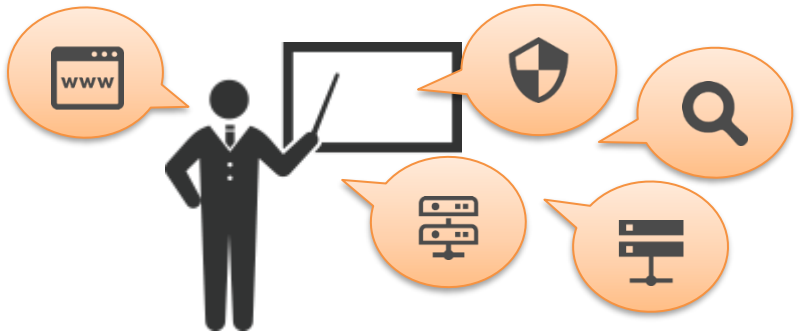
多様な製品・サービスが市場に提供され、ユーザー企業では導入是非の判断が難しくなっている

多様なセキュリティ製品・サービス群

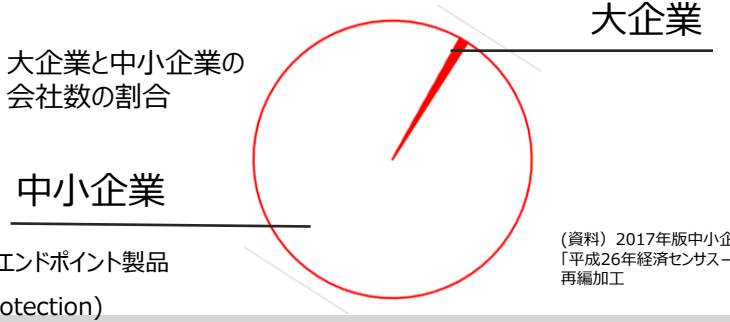
NGEPP製品 ※　EDR製品　IPS/IDS　サンドボックス　etc…

※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



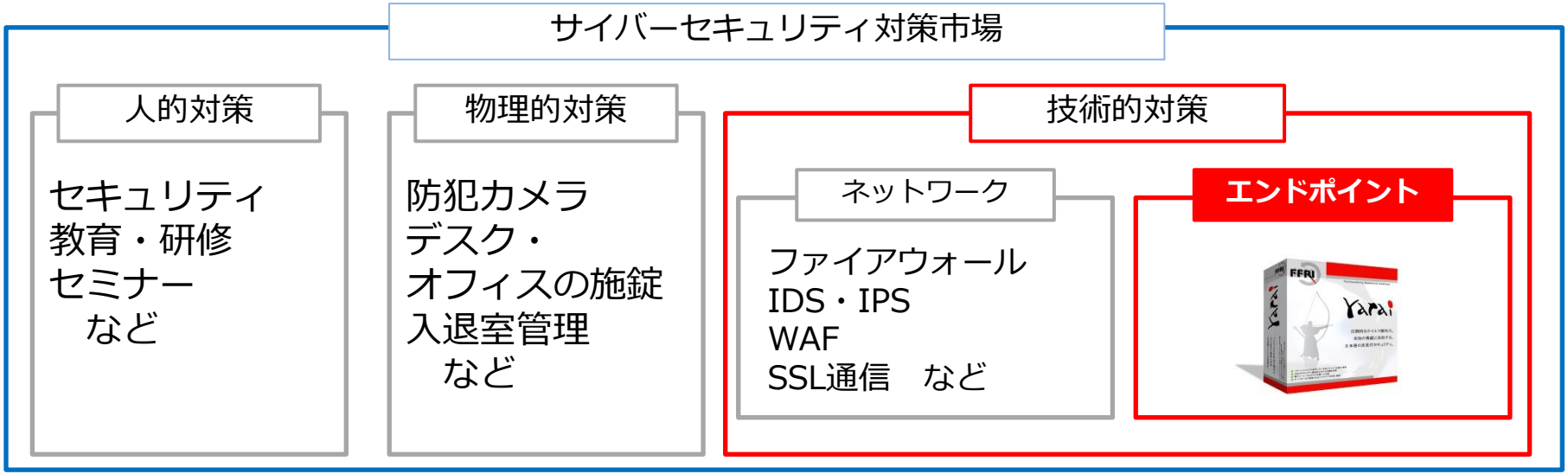
大企業以外はセキュリティ市場の空白地となっている



（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



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

防御

NGEPP

ふるまい検知・
プログレッシブ・ヒューリスティック技術

ＦＦＲＩ
北米企業Ａ社
北米企業Ｂ社

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

可視化

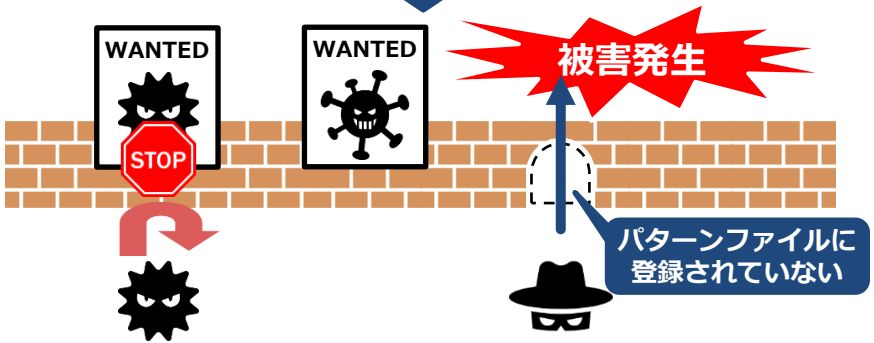
・EDR製品
Ｅ社
Ｆ社
など

※事後対応のサービスとセットがスタンダード

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

市場環境　政府統一基準への対応について

- 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。
  政府機関や独立行政法人等に対し、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

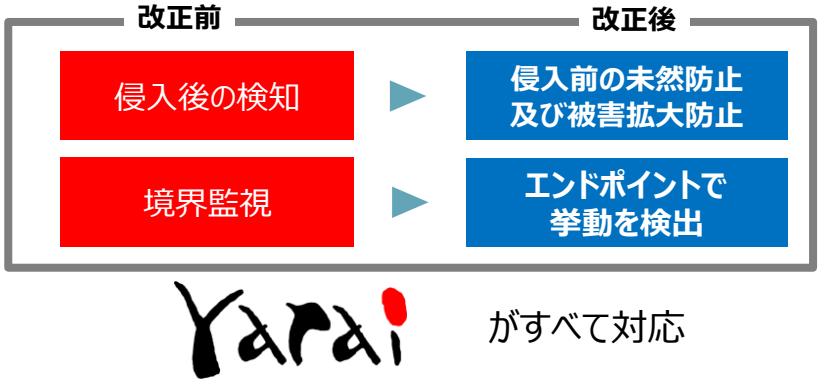
（1）将来像を見据えたサイバーセキュリティ対策の体系の進化

・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

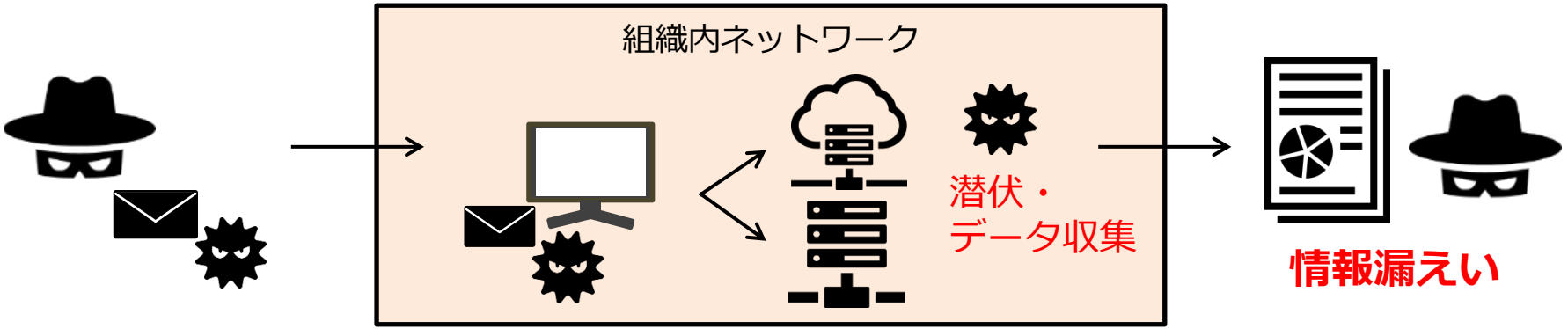
2019年より各組織のセキュリティ体制の監査がスタート。
今後は官公庁（中央省庁）を筆頭に、取り組みが進み、
地方自治体やインフラ系企業などに波及すると思われる。

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



業績説明

業績サマリー

- 移転にかかる一時コストや採用コストが前年比で増加したが、計画に織り込み済みであり、売上利益とも計画通り進捗
- 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EOLに伴い売上高は減少したものの、FFRI yaraiの売上高は増加している
- 売上高の第４四半期偏重の傾向が強まっている。

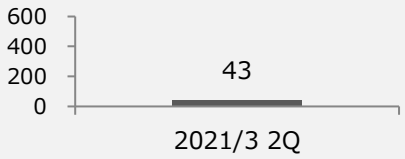
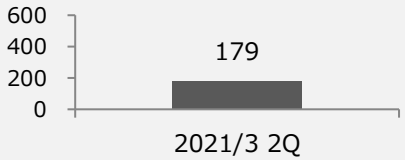
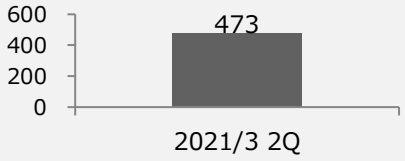
（単位：百万円）

区分	2020/3 2Q（連結）	2021/3 2Q（非連結）	増減比（%）
売上高	722	696	△3.6
営業利益 (利益率：%)	119 (16.5)	54 (7.8)	△54.6
経常利益 (利益率：%)	90 (12.6)	54 (7.9)	△39.5
親会社株主に帰属する当期純利益 (利益率：%)	58 (8.0)	39 (5.7)	△32.0

（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。プロダクト売上及び、サービス案件の売上を計上。 ・サービス案件も多く４Q偏重。来期に向けた案件が足元で増加するなど順調に進捗。
パブリック セキュリティ 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		・個人や小規模事業者への販売パートナーの数社と連携を強化、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。

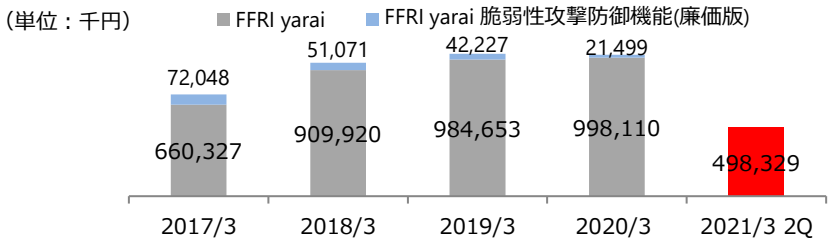
UTM ・・・ 複数の異なるセキュリティ機能を一つのハードウェアに統合し、集中的にネットワーク管理を行う製品

区分別四半期会計期間毎の売上推移

（単位：百万円）

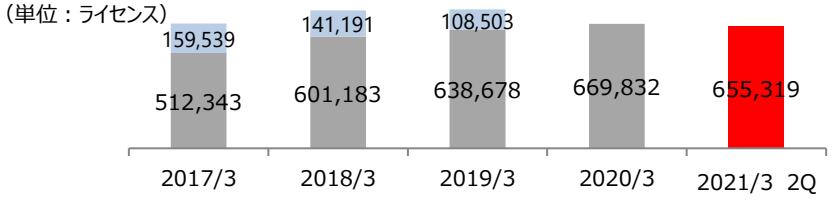
売上区分			2021/3			
			1Q	2Q	3Q	4Q
ナショナル セキュリティ セクター	プロダクト		19.4	19.4	-	-
	サービス		0.0	5.0	-	-
パブリック セキュリティ セクター	プロダクト		83.5	83.4	-	-
	サービス		12.0	0.4	-	-
プライベート セクター	プロダクト	法人	160.2	160.6	-	-
		個人	67.1	66.7	-	-
	サービス		1.7	16.8	-	-
合計			344.2	352.4	-	-

FFRI yarai シリーズの販売状況



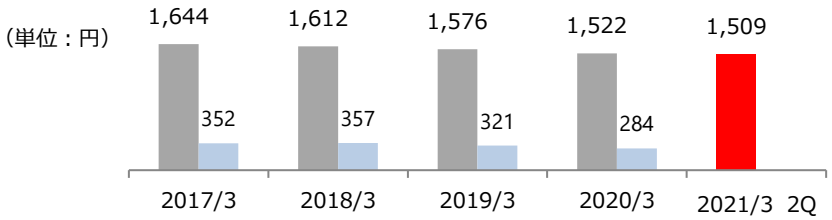
FFRI yarai 売上高

FFRI yarai 脆弱性攻撃防御機能のEOLに伴う契約減少により前期比で減少したものの、FFRI yaraiの売上は増加している。



契約ライセンス数（19/3→20/3継続率 92.0%）

官公庁向けの契約が引き続き増加したものの、新型コロナウイルス感染症の影響等によるコスト見直しによる解約もあり、前期末に比べ14,513ライセンスの減少となった。



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	2020/3（ライセンス）		2020/3 2Q（ライセンス）	
		割合（%）		割合（%）
中央省庁	156,563	23.4	157,911	24.1
その他官公庁	146,721	21.9	158,263	24.2
金融サービス	139,914	20.9	117,609	17.9
運輸	69,338	10.4	46,895	7.2
情報通信	38,543	4.7	38,365	5.9
産業インフラ・サービス	31,771	5.8	34,106	5.2
その他	86,982	13.0	102,170	15.6
合計	669,832	100.0	655,319	100.0

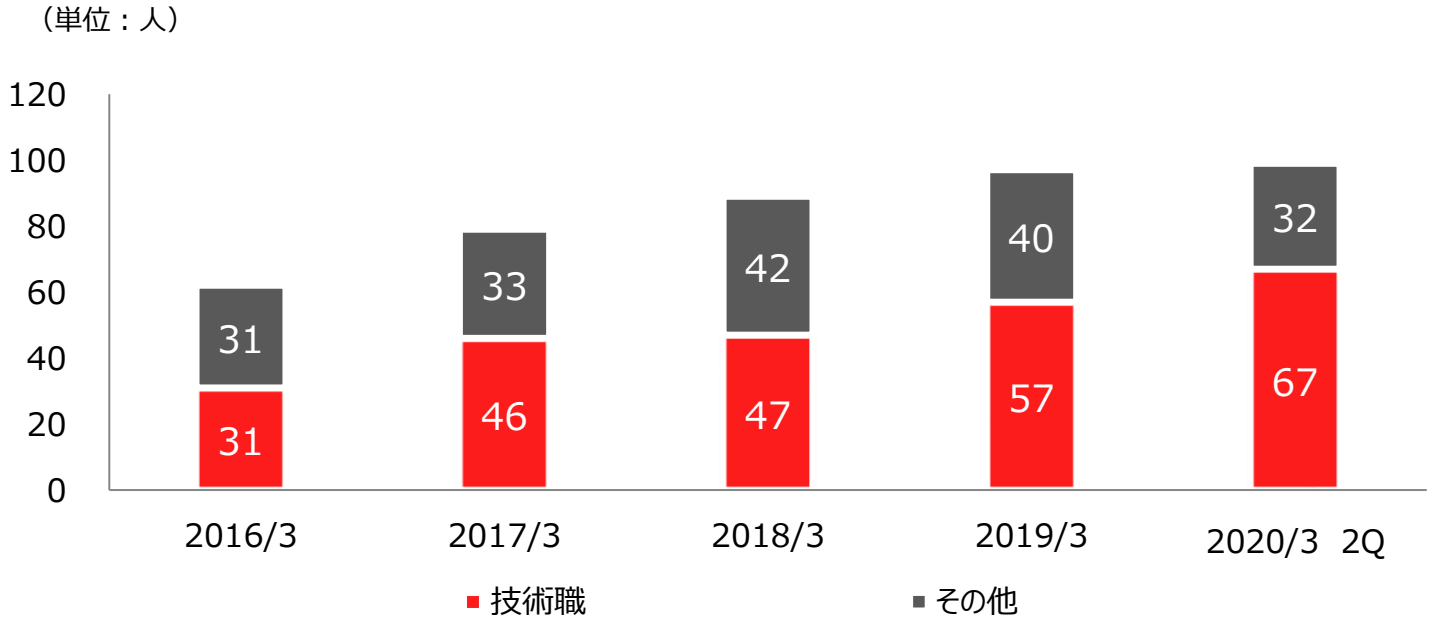
原価及び販管費の内訳

（単位：百万円）

費用の種類			2020/3 2Q（連結）	2021/3 2Q（非連結）	増減比（%）
	労務費		160	176	9.9
	経費		53	50	△4.9
	期首・期末棚卸及び他勘定振替		△88	△111	–
		研究開発費への振替	△35	△63	–
		ソフトウェアへの振替	△41	△8	–
		その他の振替	△11	△40	–
売上原価合計			**125**	**115**	**△8.4**
	人件費		203	202	△0.4
	研究開発費		50	80	59.1
	販売手数料		115	98	△14.9
	その他		108	145	35.0
販売管理費合計			**477**	**527**	**10.4**

- 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
31
31
33
46
42
47
40
57
32
67
2016/3
2017/3
2018/3
2019/3
2020/3 2Q
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 2Q（単体）	増減比（%）
	流動資産		2,272	2,120	△6.7
		現金及び預金	2,016	1,976	△2.0
		売掛金	185	47	△74.2
	固定資産		256	283	10.3
資産合計			**2,529**	**2,404**	**△5.0**
	流動負債		696	529	△24.0
		前受収益	566	441	△22.1
	固定負債		240	242	0.9
		長期前受収益	240	237	△1.2
負債合計			**936**	**771**	**△17.6**
	株主資本		1,592	1,632	2.5
		利益剰余金	1,046	1,085	3.8
純資産合計			**1,592**	**1,632**	**2.5**
負債純資産合計			**2,529**	**2,404**	**△5.0**

業績サマリー（キャッシュ・フロー）

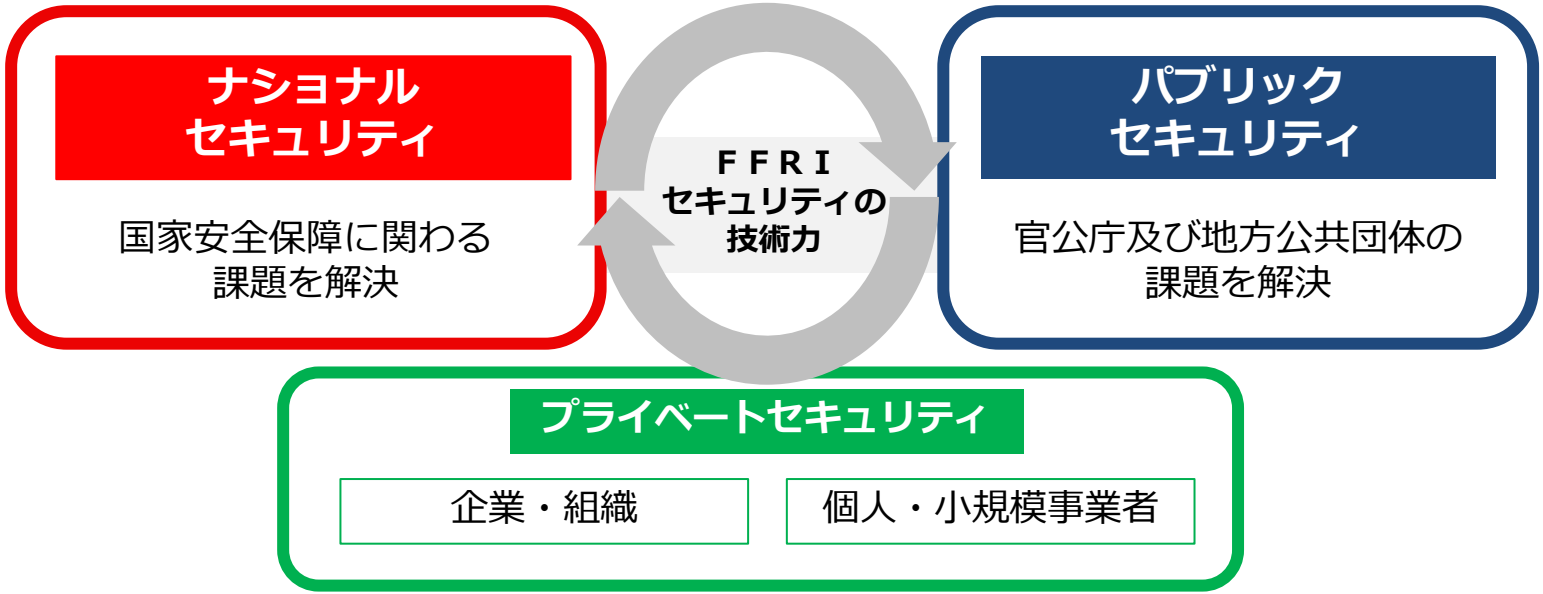
（単位：百万円）

区分	2020/3 2Q	2021/3 2Q
営業活動によるキャッシュ・フロー	13	27
税引前当期純利益	90	54
減価償却費	24	30
売上債権の増減額（△は減少）	102	137
前受収益の増減額（△は減少）	△89	△124
長期前受収益の増減額（△は減少）	△20	△2
その他	△94	△66
投資活動によるキャッシュ・フロー	△51	△54
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	1,850	1,976

2021年3月期の主な取組み

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



2021年3月期の取り組み

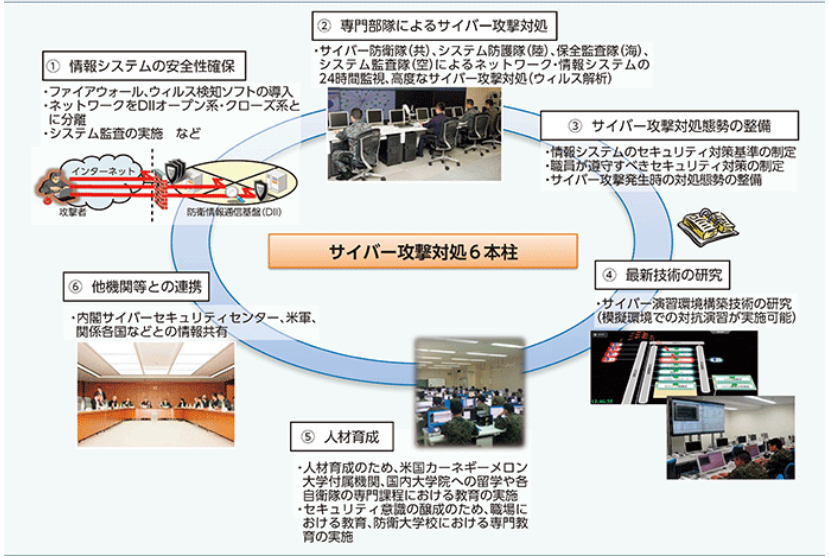
ナショナルセキュリティセクター	・国家安全保障において重要性が増しているナショナルセキュリティの分野へ注力 ・横須賀ナショナルセキュリティR&Dセンターにおいて、ナショナルセキュリティにおけるサイバーセキュリティの課題解決となるソリューションを提供する
パブリックセキュリティセクター	・増加する官公庁の需要に対応するため専門のチームを組成し販売活動を行う ・霞が関至近に本社を移転し、業務効率化を図る
プライベートセクター	・国内・海外ともに販売力を持った新たな販売パートナーの獲得を進める ・戦略的販売パートナーとの連携強化 ・FFRI yaraiの機能強化の継続実施 ・車載セキュリティ向け研究開発及び、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

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

- 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

高度なサイバー攻撃が増加し、
防衛産業を含む産業界全体の
セキュリティ見直しが必要に

防衛調達の新情報セキュリティ基準の策定

防衛省が防衛関連企業に対して求める情報セキュリティ基準を強化する方針
悪意のあるコードを検知するための高性能ウイルス対策ソフトウェアの導入など
細かな対応を盛り込んでいる。

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

サイバー領域におけるナショナルセキュリティ③

- 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100億円増額する計画
- 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

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
サイバー攻撃対処技術の研究	約21億円
サイバー演習環境の整備	約16億円
システム・ネットワークの安全性の強化	約162億円
その他サイバー関連経費	約157億円
合計	**357億円**

その他「自衛隊サイバー防衛隊（仮称）の新編」など組織体制の整備や、「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」するなど産学官連携を進める意向を示した。

参考：防衛省「我が国の防衛と予算　令和3年度概算要求の概要」より

各国のサイバー部隊規模

国名	組織規模
日本	290名
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

周辺諸国や同盟国等と比較して日本の組織規模は小さく、引き続き拡大していくものと考えられる

参考：「令和2年版防衛白書」より

2021年3月期の主な取り組み①

ナショナルセキュリティへの注力

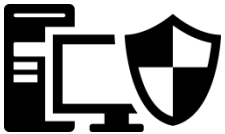
横須賀ナショナルセキュリティR&Dセンターはナショナルセキュリティ関連の研究開発に特化。

国家安全保障におけるサイバーセキュリティの課題を解決するソリューション提供に向けて、

周辺組織と連携し研究開発を加速する

重要性を増す
ナショナルセキュリティ

横須賀ナショナセキュリティR&Dセンターを開設



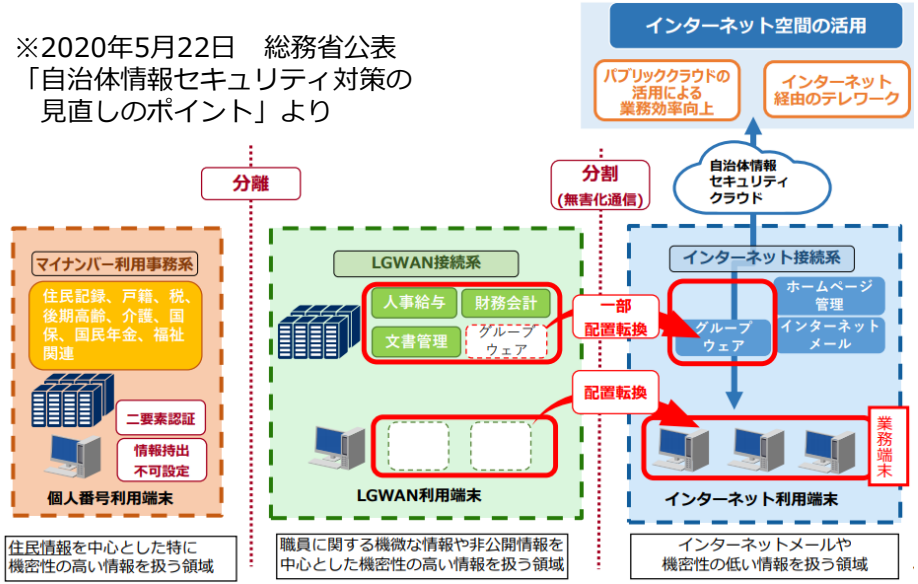
関連の組織・企業との連携を強化

政府や防衛省の積極的な取り組みを
背景に、次年度に向けた案件も増加

パブリックセキュリティの市場環境

- 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

※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

2021年3月期の主な取り組み②

地方公共団体への販売力強化

販売パートナーと連携し、需要増加が見込まれるパブリックセキュリティにおける販売力を強化

NTT-AT　NEC

TKC　Sky

販売パートナー各社と協力し、様々な施策を実施

- キャンペーンの実施
- 新たな製品・サービスの提供
- 共同研究の実施など

官公庁の他、地方自治体などへの販売力を強化

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

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

No.1　小規模事業者の顧客ニーズ

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

2021年3月期の主な取り組み④

NECとの協業関係及び、戦略的販売パートナーとの連携強化

NECへFFRI yaraiのOEM提供を開始。まずは中小企業や地方自治体の課題解決へ向けた取り組みを協力して進める。一方で、既存の戦略的販売パートナーとの連携強化も継続する。

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

国内・海外ともに、OEM提供を含む有力な販売パートナーの獲得へ向けた交渉を継続し、販売数量増加を目指す。

業績予想

（単位：百万円）

区分	2020/3実績 （連結）	2021/3計画 （非連結）	増減比（%）
売上高	1,602	1,613	0.7
営業利益 （利益率：%）	341 (21.3)	250 (15.5)	△26.7
経常利益 （利益率：%）	341 (21.3)	250 (15.5)	△26.8
当期純利益 （利益率：%）	274 (17.1)	173 (10.8)	△35.9

（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。

業績予想（売上の内訳）

（単位：百万円）

区分	2021/3 計画
ナショナルセキュリティセクター	100
パブリックセキュリティセクター	605
プライベートセキュリティセクター	907
合計	1,613

（注）2021年３月期より販売区分を変更しているため、前期比較は記載しておりません。

＜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。