2015年3月期
決算説明会

株式会社ＦＦＲＩ（東証マザーズ：3692）

http://www.ffri.jp/

会社概要

会社概要

会社名：	株式会社ＦＦＲＩ（ FFRI, Inc. ）	
所在地：	東京都渋谷区恵比寿1-18-18 東急不動産恵比寿ビル4階	
役員：	代表取締役社長	鵜飼　裕司
	取締役最高技術責任者	金居　良治
	取締役最高財務責任者	田中　重樹
	取締役（社外）	高橋　郁夫
	常勤監査役（社外）	近藤　正二
	監査役（社外）	下吹越　一孝
	監査役（社外）	杉山　由高
設立：	2007年7月3日	
資本金：	252,463,300円（平成27年３月31日現在）	

事業内容：

1. コンピュータセキュリティ研究、コンサルティング
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

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
- 設立当時は、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

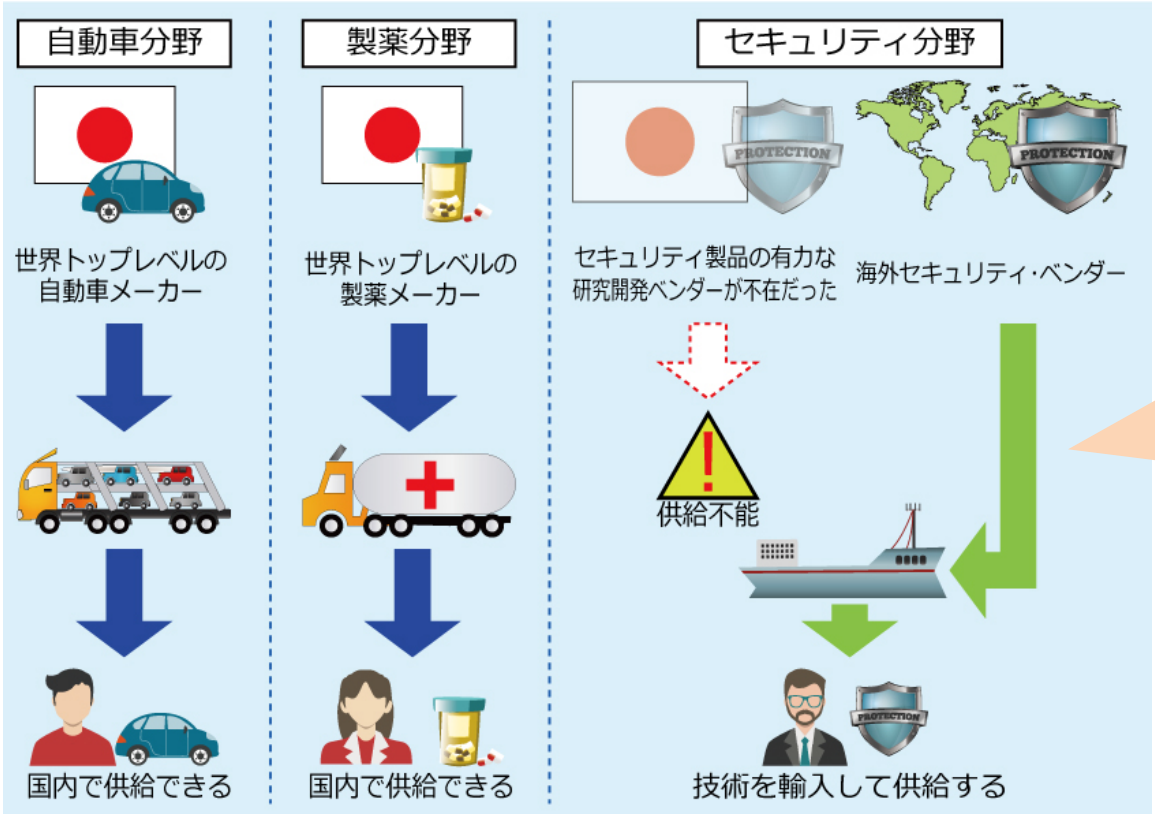
↓

FFRI

コーポレートマーク

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

これまでの日本のセキュリティ製品供給の状況と当社設立の経緯



サイバー・セキュリティの分野では、国内研究開発型企業が不在で、海外企業に頼る状況

- 自国で問題解決できないリスク
- 国防リスク

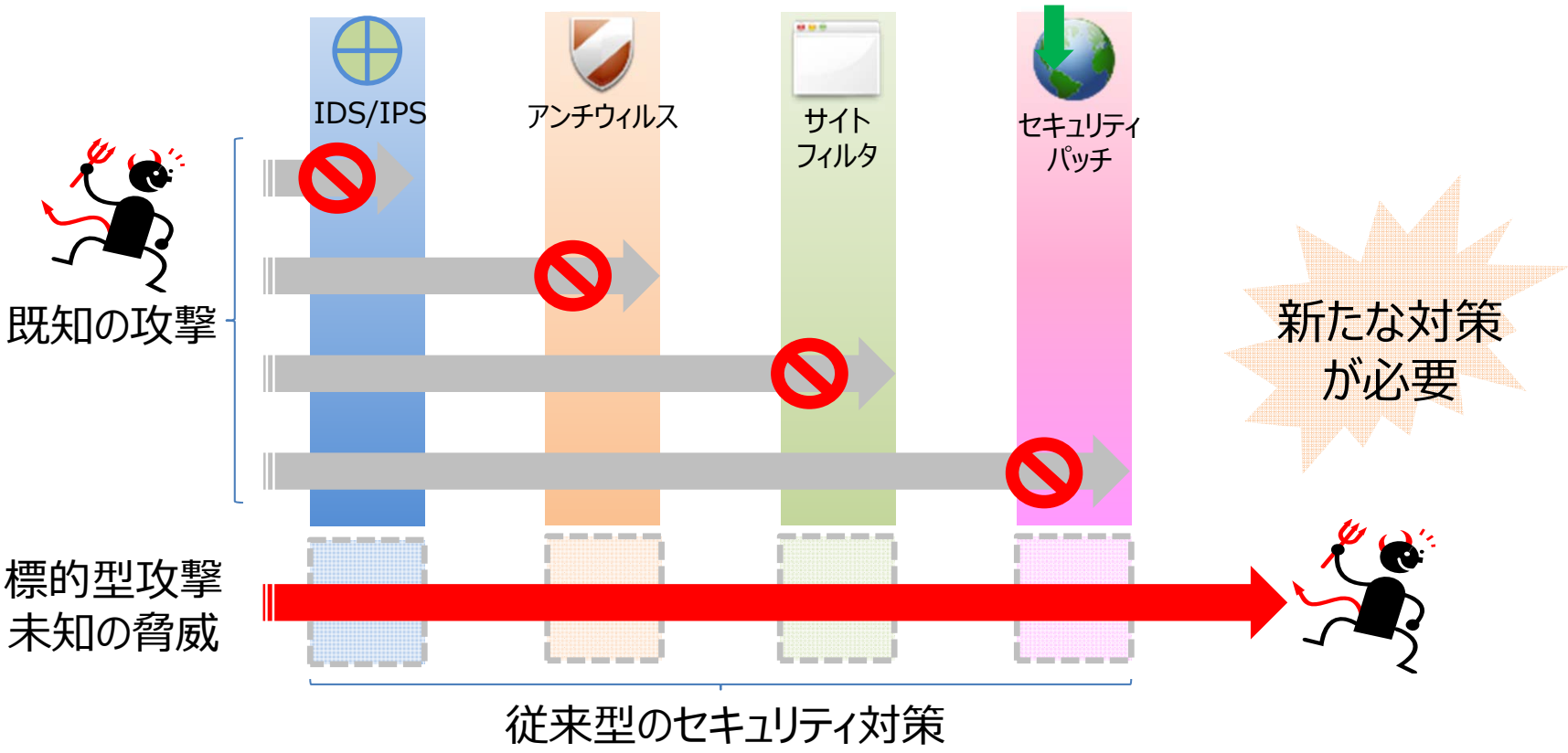
事業環境

サイバー・セキュリティを取り巻く環境

技術革新により社会の利便性が向上する一方で、
ユーザーは深刻化する脅威への対策に迫られています

※出典：平成26年11月26日　NISC
「我が国のサイバーセキュリティ政策に関する現状と今後」
金額は試算値です。実際は計量化が難しいもの、表面化していないものが多くあります。

標的型攻撃や未知の脅威は
従来型セキュリティ対策だけでは守り切れない



市場規模サマリー

市場規模

国内ウイルス対策ソフト市場（2014年予測）※1

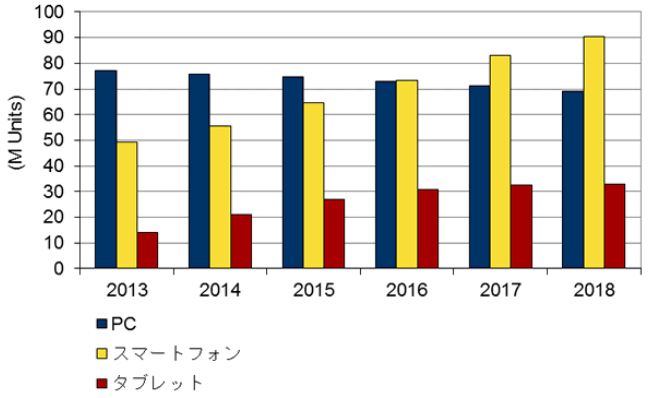
企業向け	個人向け
605億56百万円	607億27百万円

潜在的な市場規模

国内のスマートフォン、タブレット、
PCの総稼働台数※2

約1億5,300万台
（2014年）

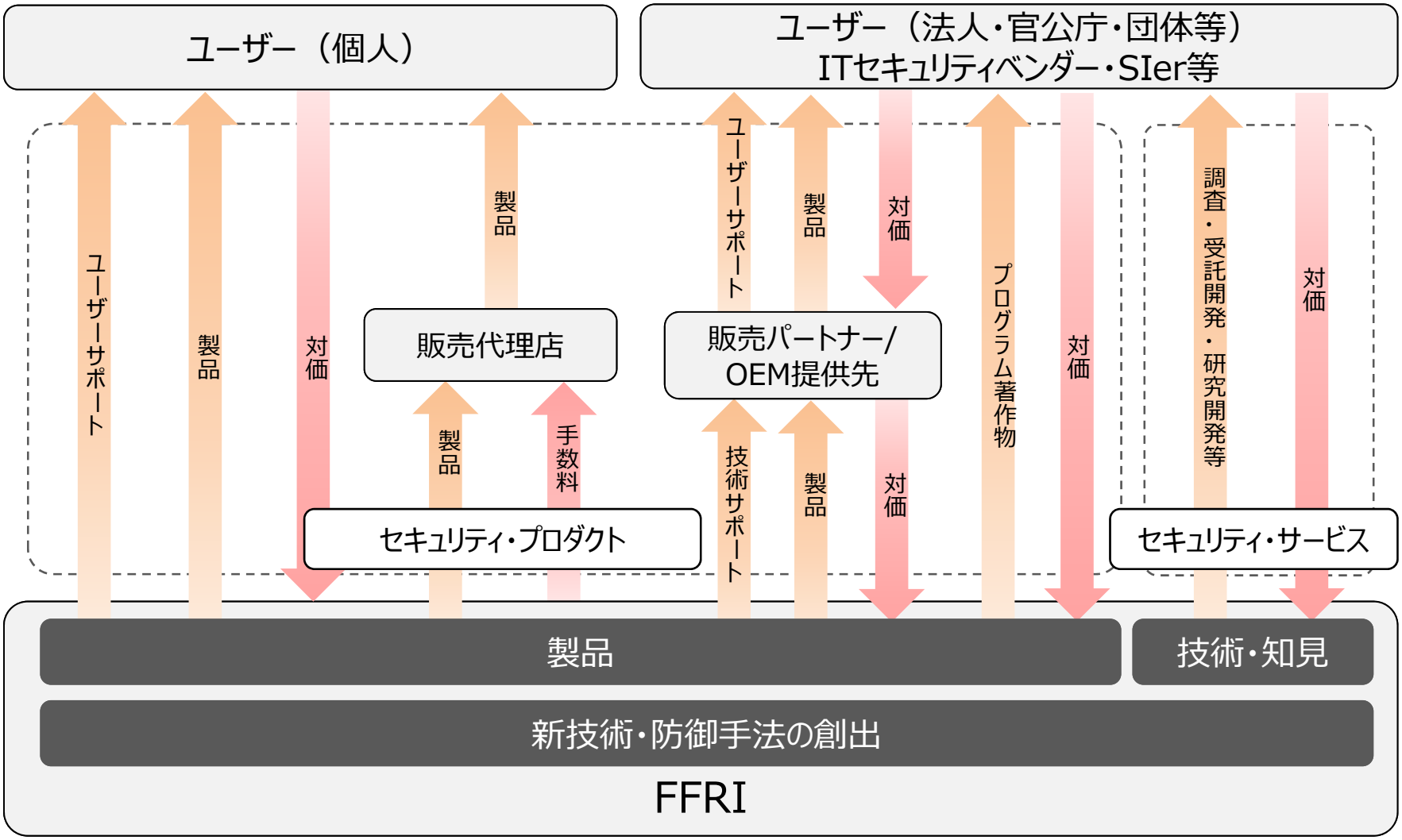
国内モバイル／クライアント市場 稼働台数予測
2013年～2018年



出典：※1　2013年度　情報セキュリティ市場調査報告書　V1.0
NPO日本ネットワークセキュリティ協会
※2　IDC　Japan株式会社プレスリリース
「国内モバイル／クライアントコンピューティング市場分析結果を発表」(2014年10月8日)

事業の内容・強み

事業モデル（2015.3.31現在）



主力製品：FFR yarai

FFR yarai は、
パターンファイルに依存せず、マルウェアや脆弱性攻撃を防御し、
既知・未知の脅威から大切な情報資産を守ります。

標的型攻撃に特化した
プログレッシブ・ヒューリスティック技術で
未知の脅威に対抗する
日本発の次世代セキュリティ

主要なセキュリティ・プロダクト

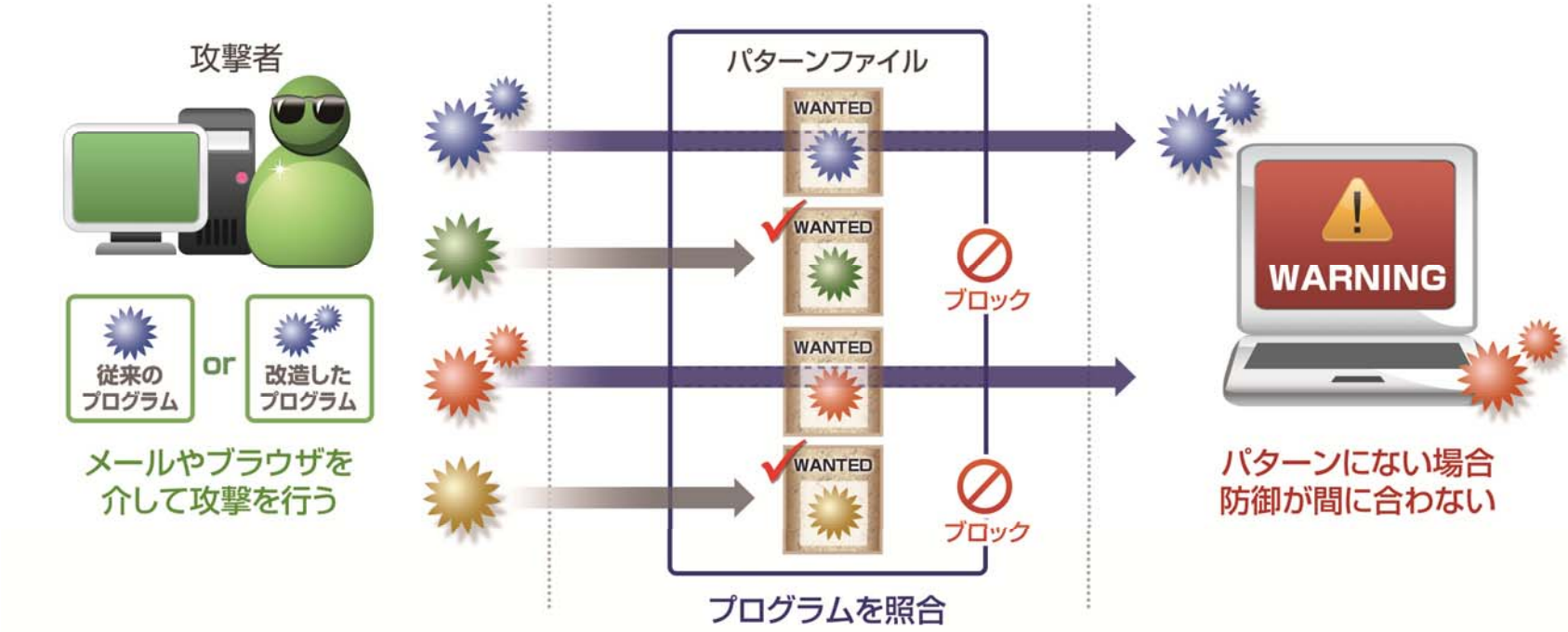
法人/個人	名称	内容
法人向け	FFR yarai	パターンファイルに依存しない、完全ヒューリスティック検知技術による標的型攻撃マルウェア対策製品で、未知・既知のマルウェア及びセキュリティ脆弱性を狙った攻撃を防御します。
法人向け	FFR yarai analyzer	プログラムや文書ファイル、各種データファイルを自動的に解析し、マルウェア混入のリスク判定が可能なレポートを出力することで、自社内でマルウェア初動解析が可能です。
個人向け	FFRI プロアクティブセキュリティ	FFR yaraiをベースに個人向けにチューニングしたセキュリティソフトで、パターンマッチング技術を使用する一般的なウ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。
個人向け	FFRI安心アプリチェッカー	Android用スマートフォン・タブレットで利用されるアプリの危険性を簡単に診断できるセキュリティアプリです。

セキュリティ・サービス

名称	内容
セキュリティ調査・分析・研究等	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。
受託開発	顧客が運用しているネットワークシステムのセキュリティ強化を目的とした ハードウェア・ソフトウェアへ、独自のサイバー・セキュリティ対策の仕組みを組み込む開発を請け負います。
標的型攻撃マルウェア検査サービス	機密情報漏洩のリスクを可視化し、対策検討含め、標的型攻撃に対する適切なリスク管理の実現を支援します。
Android端末セキュリティ分析サービス	Android端末における様々なセキュリティ上のリスクを分析し、対策に関する提言を行い、Android端末のセキュリティ脅威を分析します。
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。
FFRI ExpertSeminar	セキュリティ技術者のための技術研修コースです。

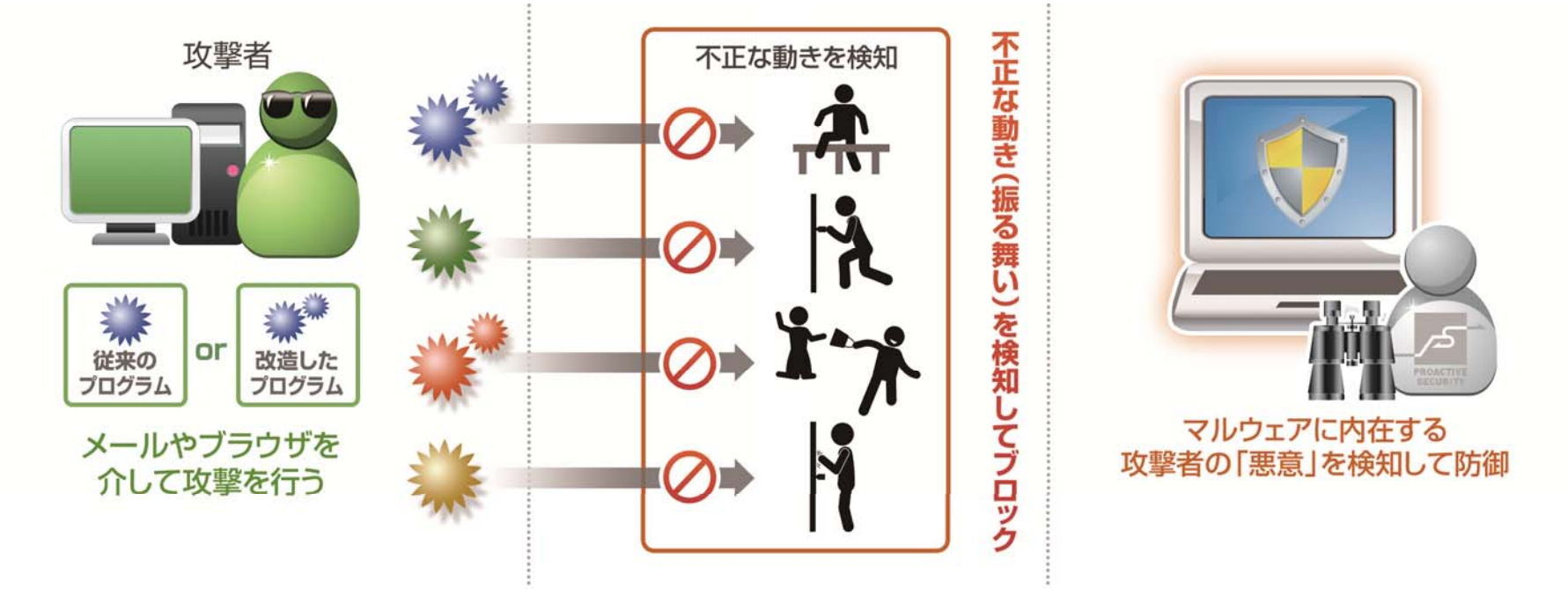
FFRIの技術的優位性について

- パターンマッチング(従来の防御技術)の防御手法イメージ



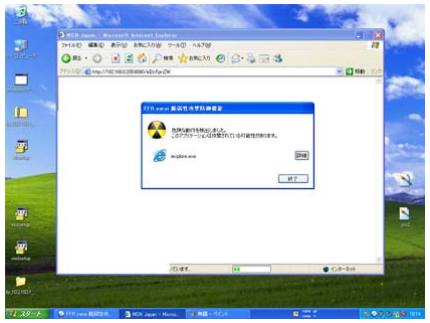
FFRIの技術的優位性について

- ヒューリスティック(当社が採用している技術)の防御手法イメージ



標的型攻撃の防御例

yarai vs 国内防衛産業企業に対する標的型攻撃



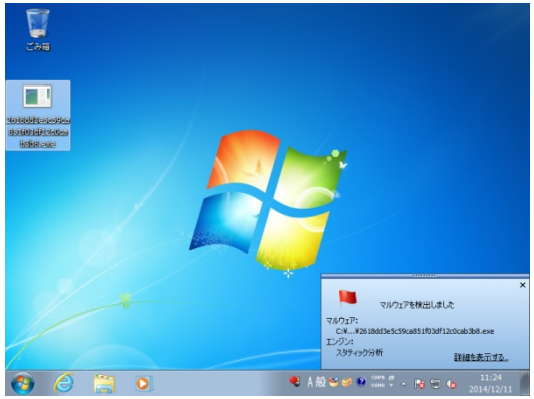
2011年9月、日本の防衛産業メーカーに対し、標的型攻撃と思われるマルウェア感染が発生しました。

当社では、この事件で使用されたとされる検体をテストした結果、「FFR yarai」で検知し、システムを保護できることを確認しました。

yarai vs FBIが警告「システム破壊型マルウェア」

このマルウェアは米国連邦捜査局（FBI）が、社内コンピュータの破壊を行うマルウェア攻撃が発生しているとして、米国内の企業に対して注意喚起を行っているもので、感染したシステムのハードディスクの全データを破壊（消去）します。

当社では、この事件で使用されたとされる検体をテストした結果、「FFR yarai」で検知し、システムを保護できることを確認しました。



FFR yarai/FFRI プロアクティブ セキュリティのポイント

- 標的型攻撃を含む未知の脅威を防御可能
- 脆弱性攻撃対策の他、静的解析・動的解析を行う５つの検知エンジンからなる

  プログレッシブ・ヒューリスティック技術で脅威を高精度に検知・防御可能
- 完全ヒューリスティック技術であるため、パターンファイルの更新が不要で動作が軽い
- 様々な環境で正常動作するソフトウェアとしての高い完成度
- 大手企業や中央省庁における多数の導入実績

業績説明

業績ハイライト

FFR yaraiの販売が好調に推移

- サイバーセキュリティ基本法施行やマイナンバー制度の開始を控え、法人・官公庁のセキュリティ対策の動きが活発化

セキュリティ・サービスは前年同期比10.5%増

- セキュリティ・サービスはセキュリティ調査案件及び研究案件、受託開発で中型案件を複数完了したことから前年比増収

東証マザーズへの上場

- 上場によってセキュリティ業界以外における知名度向上

コンシューマー市場への事業範囲拡大

- 2014年12月よりAndroidモバイル端末向け「FFRI 安心アプリチェッカー」をリリース
- ㈱ティーガイアの全国店舗網より順次取り扱い開始
- 2015年４月　FFRI プロアクティブ セキュリティ をリリース

研究開発

- 研究成果の製品への反映やBlack Hat、 CODE BLUE など国際カンファレンスで発表

業績サマリー

（単位：百万円）

区分	2014/ 3	2015/3	前期比(%)	ポイント
売上高	660	876	32.8	・FFR yaraiの販売が好調 ・セキュリティ・サービスが前期比10.5%増
営業利益 (利益率：%)	171 (26.0)	256 (29.2)	49.0	・セキュリティ・プロダクトの増加により利益率向上
経常利益 (利益率：%)	172 (26.1)	241 (27.6)	40.5	
当期純利益 (利益率：%)	115 (17.6)	171 (19.6)	47.9	

業績サマリー（売上の内訳）

（単位：百万円）

区分		2014/3	2015/3	前期比(%)
セキュリティ・プロダクト	継続売上	136	263	92.7
	新規売上	227	341	50.2
	小計	363	604	66.1
セキュリティ・サービス		246	272	10.5
その他		50	－	－
合計		660	876	32.8

（注）継続売上について
当社の主な製品は、１年間利用可能なサブスクリプション契約が中心となっています。当社では前期以前に販売した既存契約から発生する売上及び既存契約が契約更新されることで発生する売上を継続売上として管理しております。

契約ライセンス数の推移

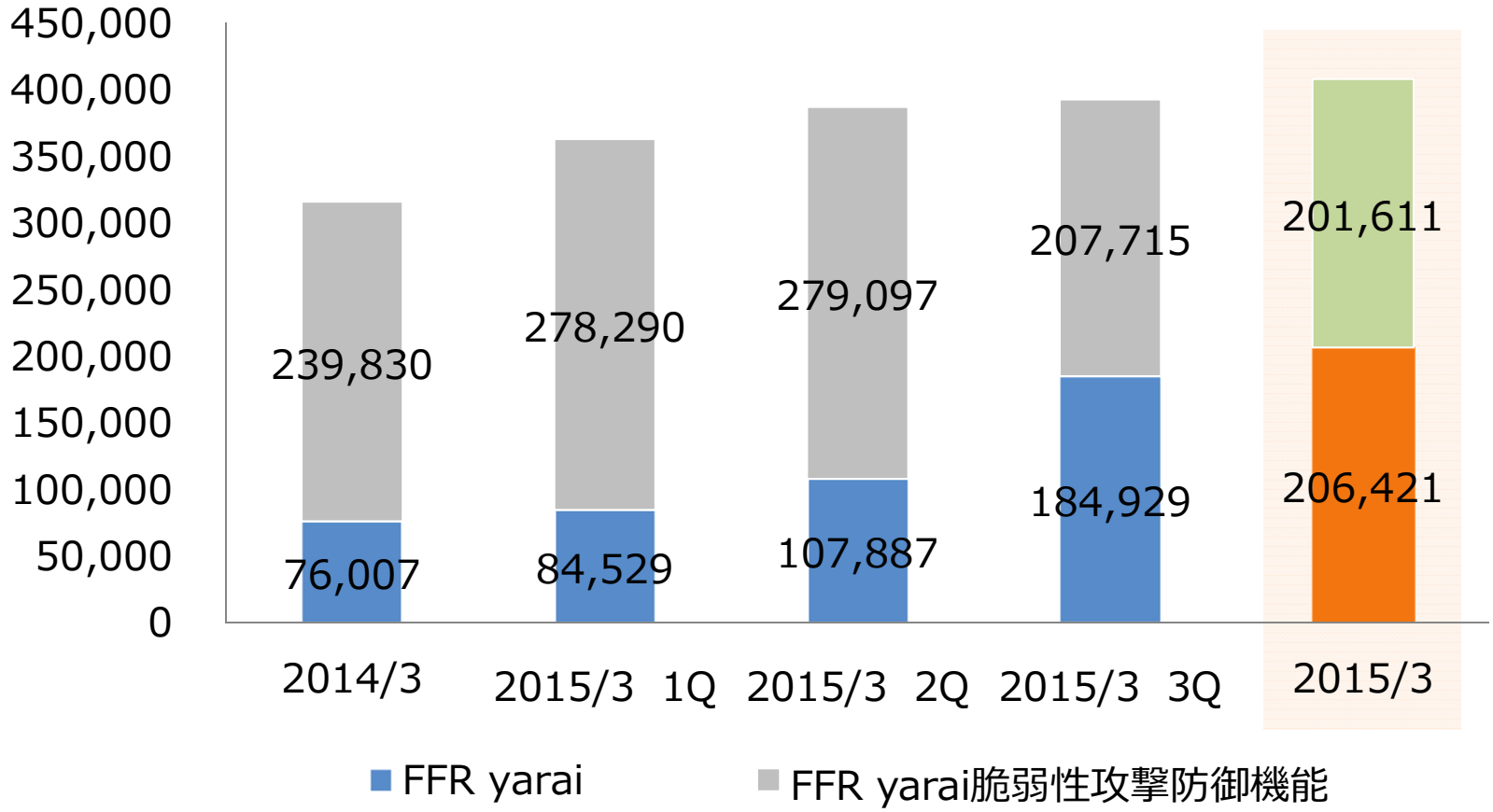
2015年３月期は、単価の高いFFR yaraiの販売が増加

回次	契約ライセンス数（ライセンス）			製品単価（円）	
	FFR yarai	FFR yarai 脆弱性攻撃防御機能	計	FFR yarai	FFR yarai 脆弱性攻撃防御機能
2011/3	983	1,000	1,983	3,700	310
2012/３	14,843	21,237	36,080	4,160	440
2013/３	31,420	117,728	149,148	2,200	480
2014/３	76,007	239,830	315,837	2,240	350
2015/３	206,421	201,611	408,032	1,790	500

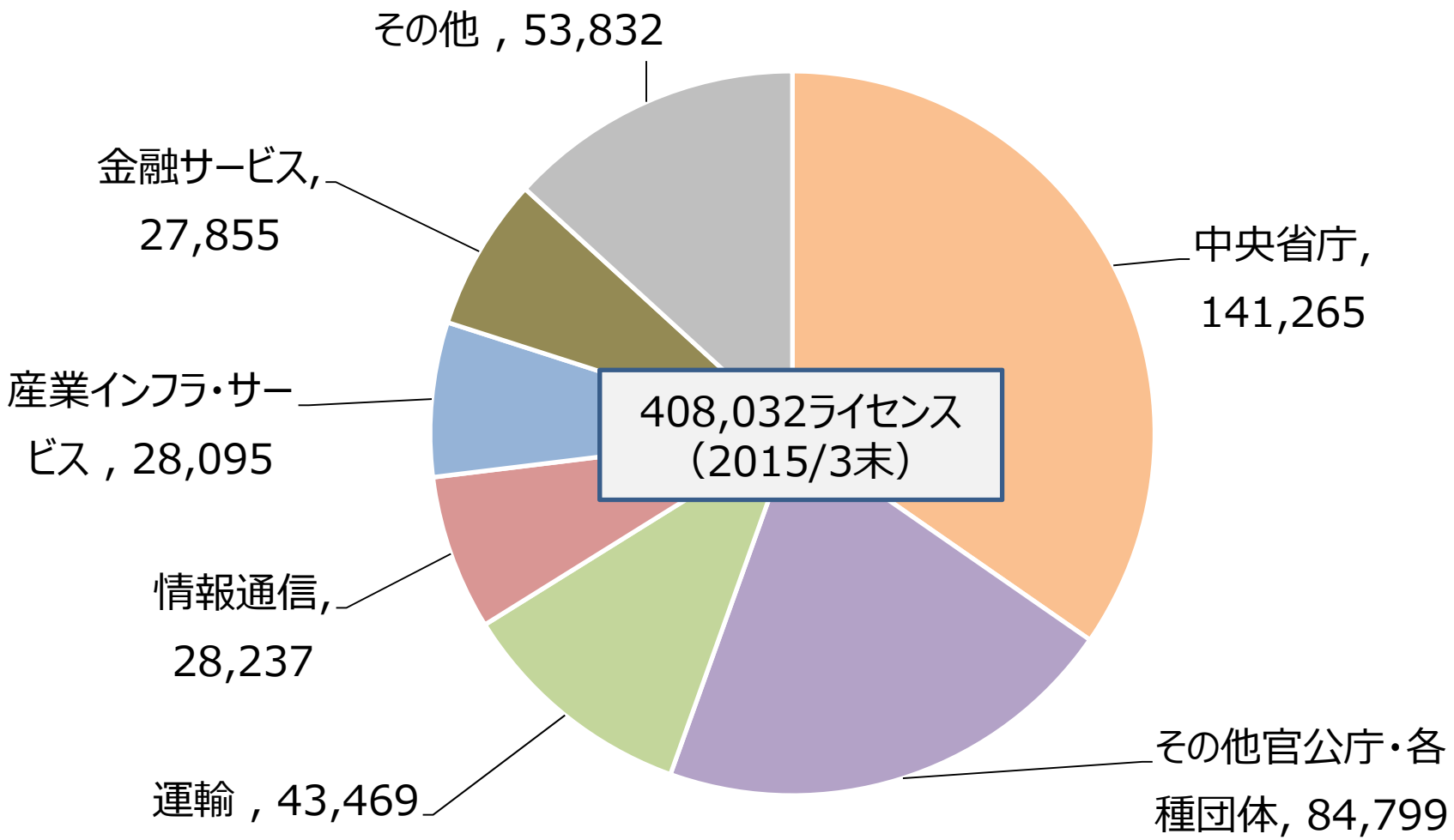
（注）１．製品単価は、当社からの販売パートナーに対する１ライセンスあたりの販売価格です。
２．ボリュームディスカウントの価格体系を採用していることから、製品単価は大口案件の発生状況に影響されます。
３．「FFR yarai脆弱性攻撃防御機能」は、「FFR yarai」に搭載した５つの検知エンジンのうち、脆弱性攻撃対策エンジンで構成されるエントリーモデルであり、近年は本機能だけでは防御することが難しい脅威が増加してきていることから、2015年９月30日をもって新規販売を終了する予定です。

四半期毎の契約ライセンス数推移

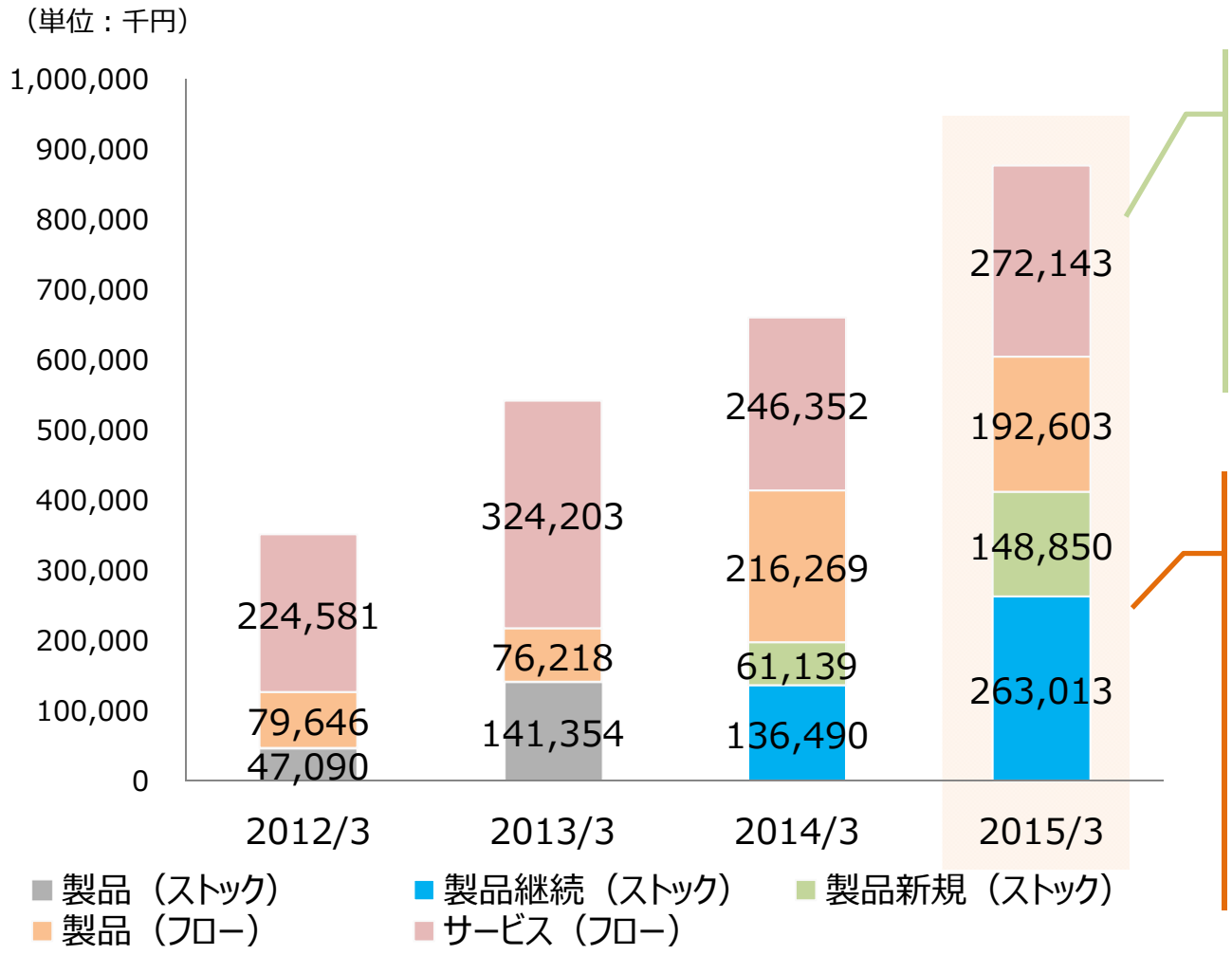
（単位：ライセンス）



業種別契約ライセンス数



ストック型収入とフロー型収入の内訳



フロー型収入

納品・検収のタイミングで計上される売上

・セキュリティ・サービス

・yarai analyzer

・ソフトウェア譲渡売上　他

ストック型収入

ユーザーが利用をする限り、毎期継続して見込める売上

・ FFR yarai

・ FFRI安心アプリチェッカー

・ yarai analyzer保守契約

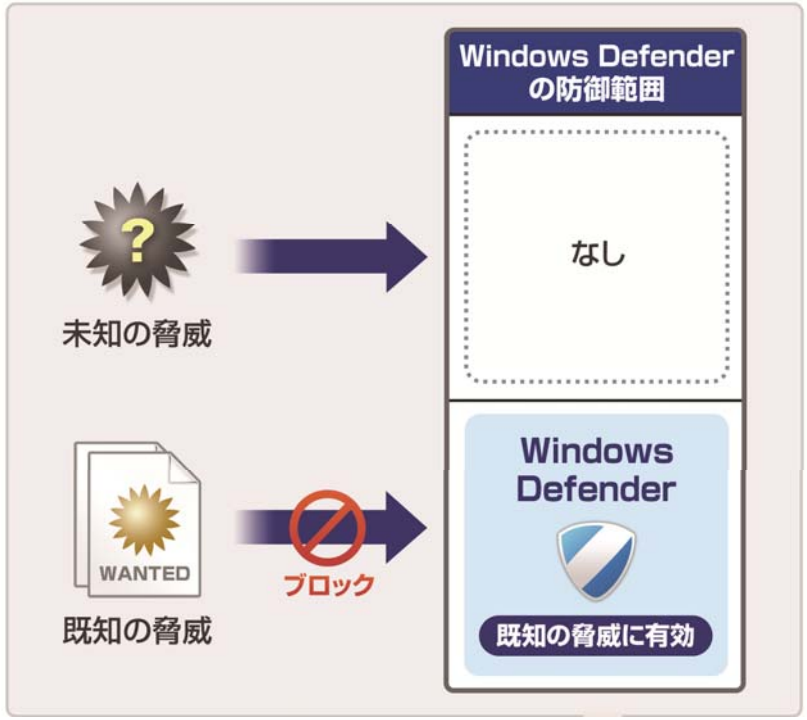
他

今後の取組み

- コンシューマーへの事業領域拡大により、すべてのユーザー層に対応できる製品ラインナップとなりました
- 2016/3期はマーケティング活動による販売拡大に取組みます

～2015/3	2015/4～2016/3	2016/4～
・研究開発の実施 ・法人・官公庁向け体制整備・拡販 ・コンシューマー向け製品リリース	取組み ・ コンシューマー向けマーケティング活動の実施 オンラインバンキング不正送金などの新しい脅威に有効な製品が存在することを広く周知 すでに被害が拡大していることから迅速な対応が必要 ・ 法人・官公庁向け販売拡大 サイバーセキュリティ基本法施行やマイナンバー制度の開始、2020年東京オリンピックを控え、セキュリティ対策のニーズに対応 ・ 研究開発の実施 製品機能強化、IOT等の新領域に先立った研究 ・ 海外販売体制の構築・強化 海外販売拡大に向けた体制強化	・研究開発の実施 ・コンシューマー向け製品の販売拡大 ・法人・官公庁向け販売拡大 ・海外展開本格化 ・IOT等新規分野への展開

FFR yarai/FFRI プロアクティブ セキュリティにより、ウイルス対策市場の置換えを進めます



FFR yarai/FFRI プロアクティブ セキュリティを導入することで防御範囲を拡張可能

yarai

PROACTIVE SECURITY

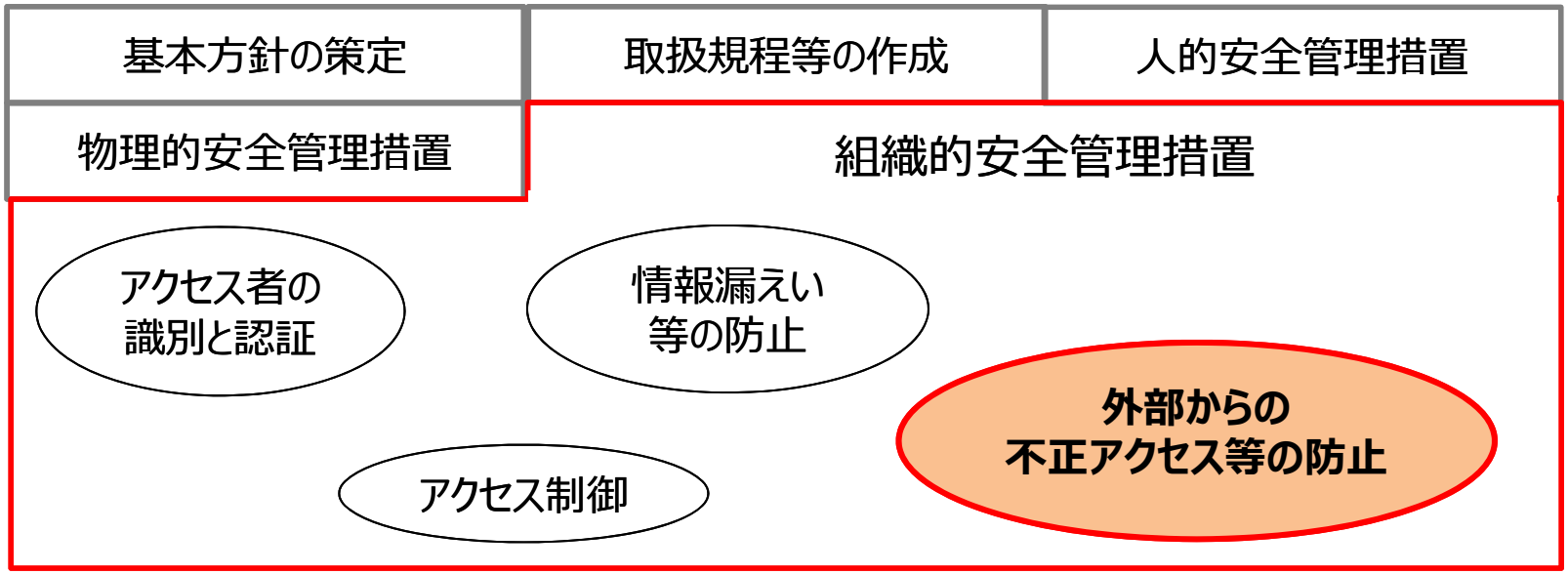
防御範囲がほぼ同じのため、市販ウイルス対策ソフトを導入する意義は薄い

アンチウイルス
ソフト
既知の脅威に有効

※ Windows Defenderはパターン型のウイルス対策ソフトで、Windows8.1に標準搭載されています
Windows7 では Microsoft Security Essentials を無料でダウンロード利用可能（個人利用に限る）

マイナンバー制度開始のニーズへ対応

内閣府のガイドラインでは、情報システムを**外部脅威**から保護する仕組みを導入し、適切に運用することが求められています。



業績予想

（単位：百万円）

区分	2015/3 実績	2016/3 計画	前期比 (%)
売上高	876	1,815	107.1
営業利益 (利益率：%)	256 (29.2)	263 (14.5)	2.7
経常利益 (利益率：%)	241 (27.6)	263 (14.5)	8.9
当期純利益 (利益率：%)	171 (19.6)	176 (9.7)	2.7

業績予想（売上の内訳）

（単位：百万円）

区分			2015/3 実績	2016/3 計画	前期比 (%)
セキュリティ・プロダクト	法人	継続売上	263	399	51.9
		新規売上	341	373	9.4
	個人		0	760	–
	小計		604	1,532	153.6
セキュリティ・サービス			272	282	3.8
合計			876	1,815	107.1

（注）継続売上について
当社の主な製品は、１年間利用可能なサブスクリプション契約が中心となっています。当社では前期以前に販売した既存契約から発生する売上及び既存契約が契約更新されることで発生する売上を継続売上として管理しております。

売上の季節的変動について

- 売上の計上は、当社の主なユーザーである企業や官公庁の年度末である12月から３月に集中する傾向があります。

当社はコンシューマー市場に事業範囲を拡大しており、今後は売上計上時期の偏りが徐々に解消される予定ですが、当面は企業・官公庁向けの売上比率が大きいため、この傾向は続く見込みです。

（単位：百万円）

2016/3	1Q	2Q	3Q	通期 (計画)
売上高	－	－	－	1,815
進捗率(%)	－	－	－	100.0

2015/3	1Q (実績)	2Q (実績)	3Q (実績)	通期 (実績)
売上高	164	282	430	876
進捗率(%)	18.8	32.2	49.2	100.0

＜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当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。

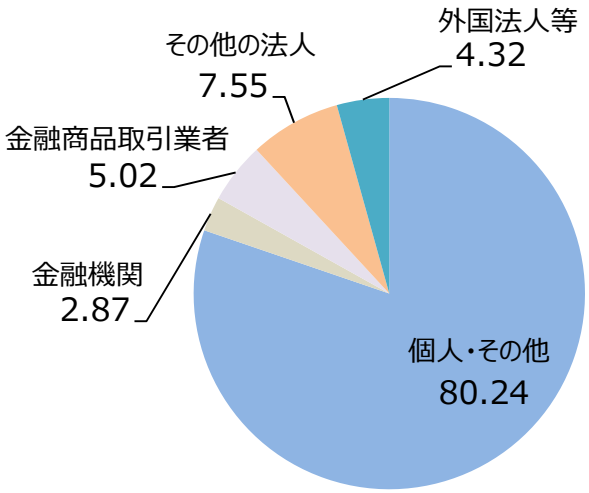
参考資料

株式の状況（2015.3.31）

発行済株式数　7,575,600株

株主数　5,915名

株主構成



上位大株主

株主名	持ち株数（株）	持株比率（%）
鵜飼　裕司	1,992,000	26.29
金居　良治	1,626,000	21.46
エヌ・アール・アイ・セキュアテクノロジーズ株式会社	480,000	6.33
田中　重樹	126,000	1.66
松井証券株式会社	122,400	1.61
下吹越　一孝	120,000	1.58
日本証券金融株式会社	90,500	1.19
JP MORGAN CHASE BANK 385181	68,000	0.89
野村信託銀行株式会社（投信口）	67,700	0.89
永田　哲也	66,000	0.87
合計	4,758,600	62.77

主なセキュリティ・プロダクトの利用形態・販売価格

個人/法人	名称	利用形態	ライセンス形態	価格	販売店 仕切率
法人向け	FFR yarai	エンドポイント (PC 1 台ずつにインストールして使用)	サブスクリプション	1 ライセンスに付き 9,000円/年(5～99ライセンス)～ 3,000円/年(10,000ライセンス～)	40%～60%
法人向け	FFR yarai analyzer	1 組織又は 1 拠点に 1 ライセンス	パーペチュアル	1 ライセンスに付き3,000,000円 (初年度保守費用込) (翌年度保守費用はライセンス価格の20%(60万円))	60%～80%
個人向け	FFRI プロアクティブセキュリティ	エンドポイント (PC 1 台ずつにインストールして使用)	サブスクリプション	1 ライセンスに付き8,500円/年	–
個人向け	FFRI安心アプリチェッカー	エンドポイント (端末 1 台ずつにインストールして使用)	サブスクリプション	1 ライセンスに付き300円/月	–

FFR yarai のプログレッシブ・ヒューリスティックエンジン

＊・・・暗号化アルゴリズムは3DESを採用しております。(ユーザによる設定変更不可)

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

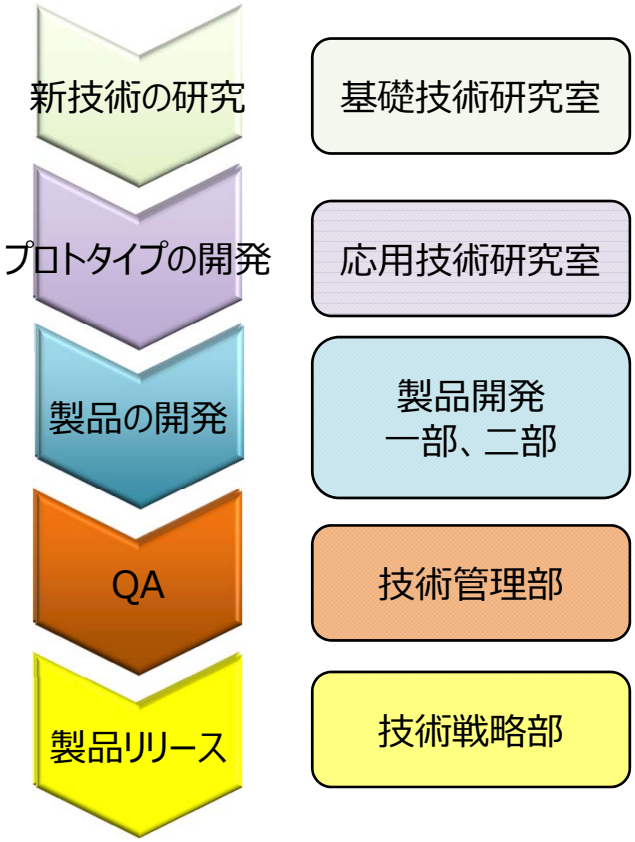
■ZDPエンジン	メールやWebページ閲覧時の攻撃など、既知・未知の脆弱性を狙ったウイルス攻撃を防御。 独自の「API-NX」技術(特許第4572259号)で、任意コード実行型脆弱性の攻撃を防御。
■Static分析エンジン	プログラムを動作させることなく分析。「PE構造分析」「リンカー分析」「パッカー分析」「想定オペレーション分析」など 多数の分析手法「N-Static分析」で検知。
■Sandboxエンジン	仮想CPU、仮想メモリ、仮想Windowsサブシステムなどで構成される仮想環境上でプログラムを実行。 独自の「U-Sandbox検知ロジック」で命令の組み合わせに基づいて検知。
■HIPSエンジン	実行中プログラムの動作を監視。他プログラムへの侵入、異常なネットワークアクセス、 キーロガーやバックドア的な動作などの挙動を、独自の「DHIPSロジック」で検知。
■機械学習エンジン	FFRIが収集したマルウェアに関するビッグデータを元に実行中のプログラムを監視。 ビッグデータ上の振る舞い特性を抽出し、機械学習で分析した特徴により端末上の悪意ある挙動を検知。

組織的なR&D体制

技術部門の体制

基礎技術研究室 〔役割〕 セキュリティ新技術の調査・研究
応用技術研究室 〔役割〕 セキュリティ技術の研究・調査・監視・分析 製品プロトタイプの開発
製品開発第一部 〔役割〕 ソフトウェア製品の設計・実装 （主にWindows向け）
製品開発第二部 〔役割〕 ソフトウェア製品の設計・実装 （その他）
技術管理部 〔役割〕 製品・サービス等に係わる品質保証 サポート・導入・運用・構築
技術戦略部 〔役割〕 エヴァンジェリスト・コンサルティング活動 技術的営業支援

製品開発の流れ



用語説明

標的型攻撃とは？

特定の企業や組織、個人を狙ったサイバー攻撃のこと。

攻撃者は綿密な事前調査により、標的システムのセキュリティ対策に応じた攻撃手法を選択するため、危険度の高い脅威です。

マルウェアとは？

コンピュータ・ウイルス、スパイウェアなど、悪意のある目的を持ったソフトウェアやプログラムのこと。

用語説明

未知の脅威とは？

未知の脅威とはセキュリティベンダーに発見されていない脆弱性を突いた攻撃やマルウェアを指します。これらはOSのアップデートや、パターンマッチングをベースとしたウイルス対策ソフトだけでは防ぐことができません。

昨今のサイバー攻撃は、この未知の脅威を用いるケースが多く見受けられ、新たな対策を講じる必要があります。

ヒューリスティック検知とは？

マルウェア等の不正なコードを検出する際、パターンファイルによるマッチングではなく、マルウェア等がもつ特徴的なプログラムの構造や振る舞いを検知する手法。これにより未知のウイルスなどにも対応できます。