平成27年3月期　第２四半期決算説明会

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（非常勤）	高橋　郁夫
常勤監査役	近藤　正二
監査役（非常勤）	下吹越　一孝
監査役（非常勤）	杉山　由高

- 設立：　2007年7月3日
- 資本金：　252,463,300円（平成26年10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

設立の経緯

米国の研究開発の現場で感じた日本との違い

- 基礎技術研究の重要性
- 技術シーズのビジネス化

米国の研究開発の現場で感じた母国に対する危機感

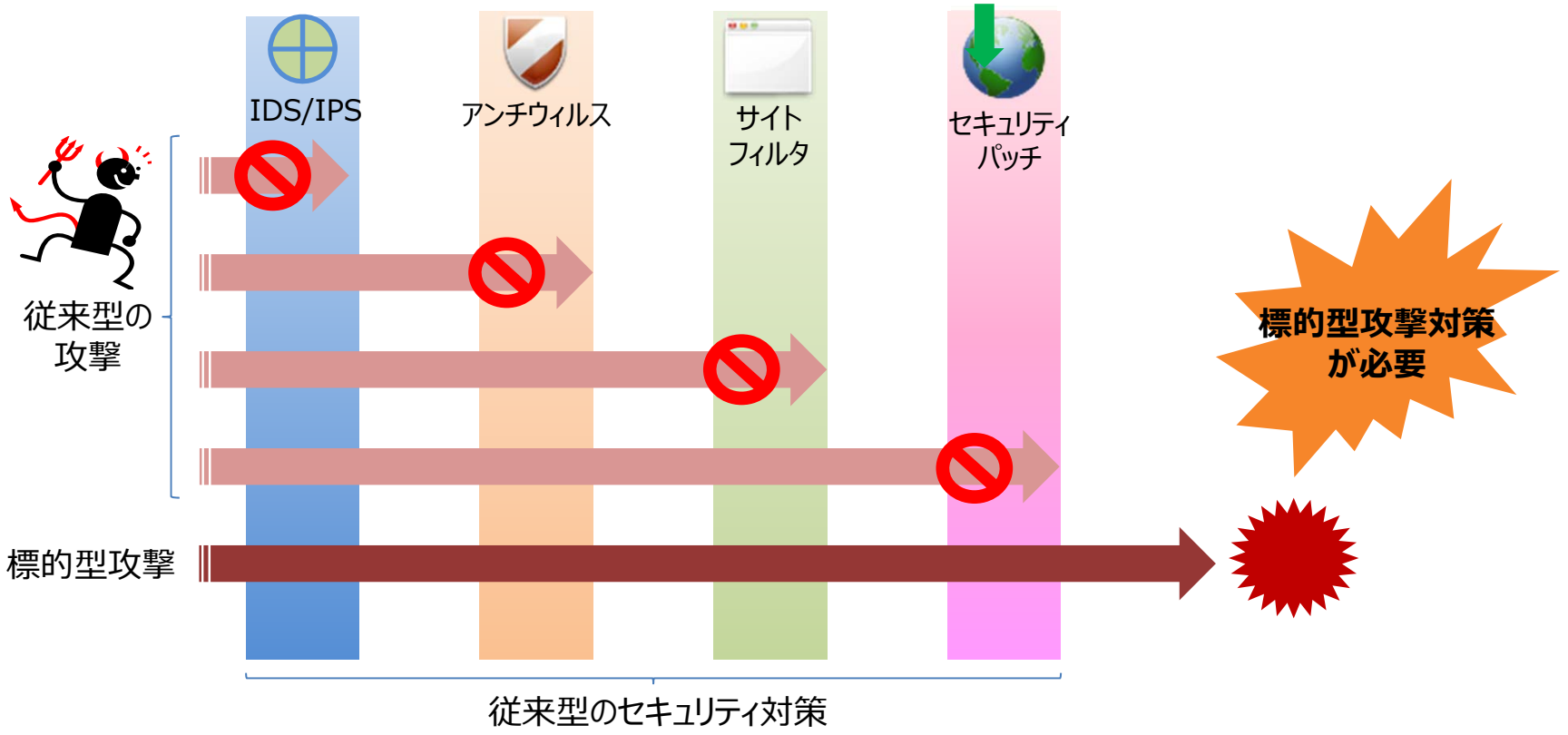
- 研究開発力の格差拡大
- 日本発のインシデント対応

国産の対策技術の必要性

- 研究開発の源流を日本に創り、日本から世界に技術を発信

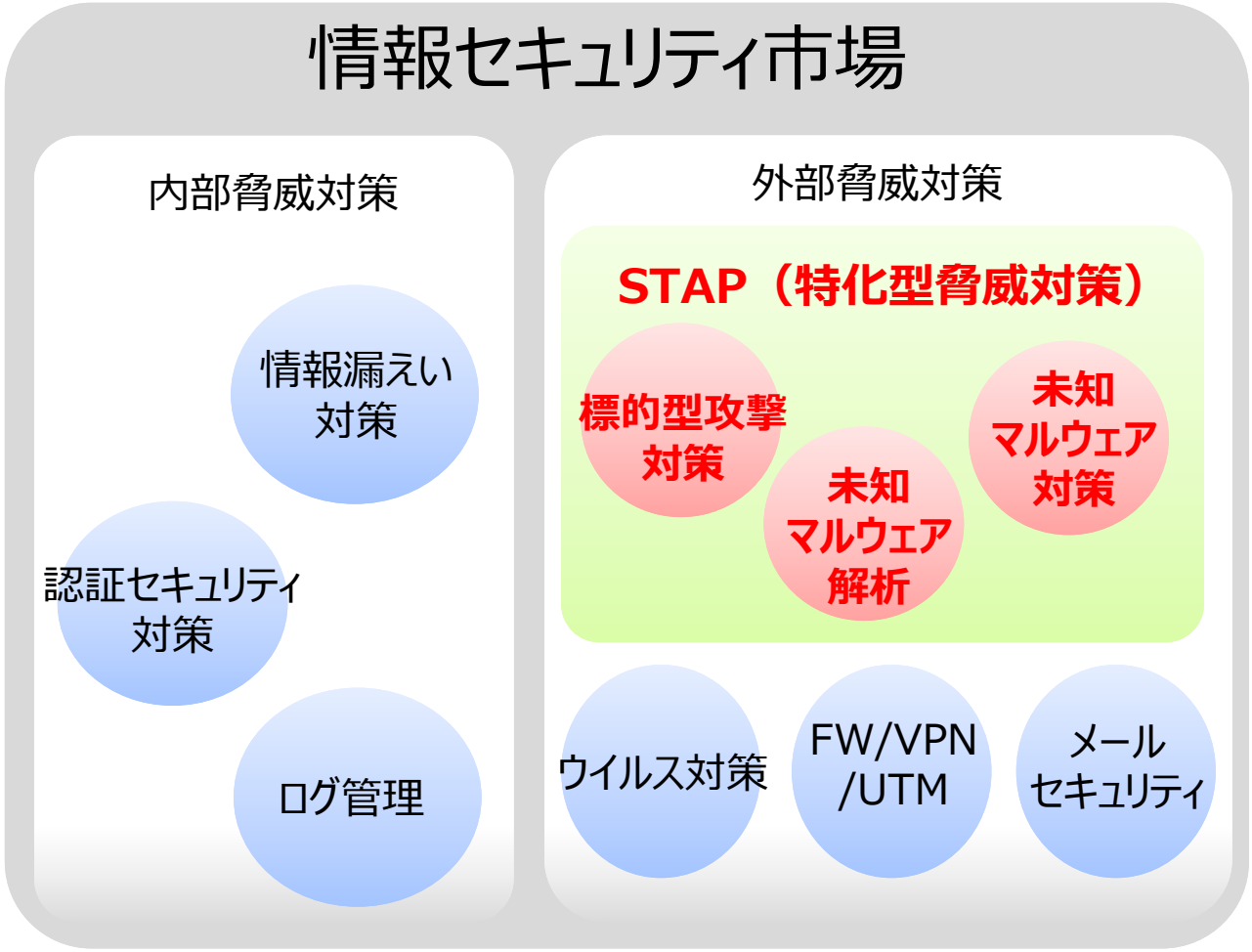
事業環境

標的型攻撃は従来型セキュリティ対策だけでは守り切れない



特定の組織団体に対して個別に作成される標的型攻撃マルウェアの場合、攻撃の事実が表面化しにくく、
アンチウイルスベンダーの対応も遅れがち
標的型攻撃対策としては、従来のパターンファイルに依存せず、振る舞いで検知することが有効

FFRIが注力する市場



STAP市場
(特殊脅威解析・防御)

- **S**pecialized
- **T**hreat
- **A**nalysis and
- **P**rotection

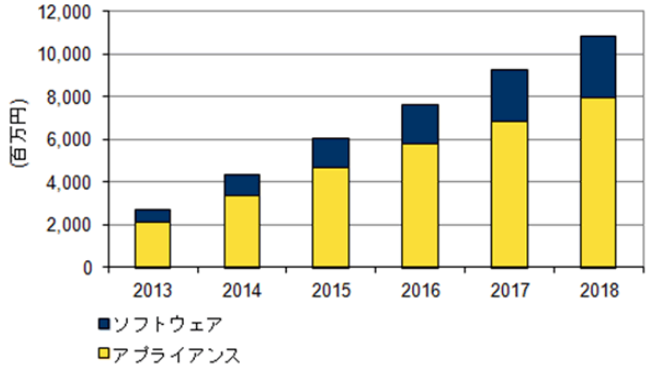
FFRIが注力する市場

国内標的型サイバー攻撃向け特化型脅威対策製品市場

- 2013年の市場規模は前年比155.8%増の27億円
- 2013年～2018年の年間平均成長率は31.6%
- 2018年には108億円と予測

標的型サイバー攻撃向けセキュリティサービス市場

- 2013年の市場規模は3,137億円、前年比5.7%増
- 2013年～2018年の年間平均成長率は6.2%
- 2018年には4,237億円と予測

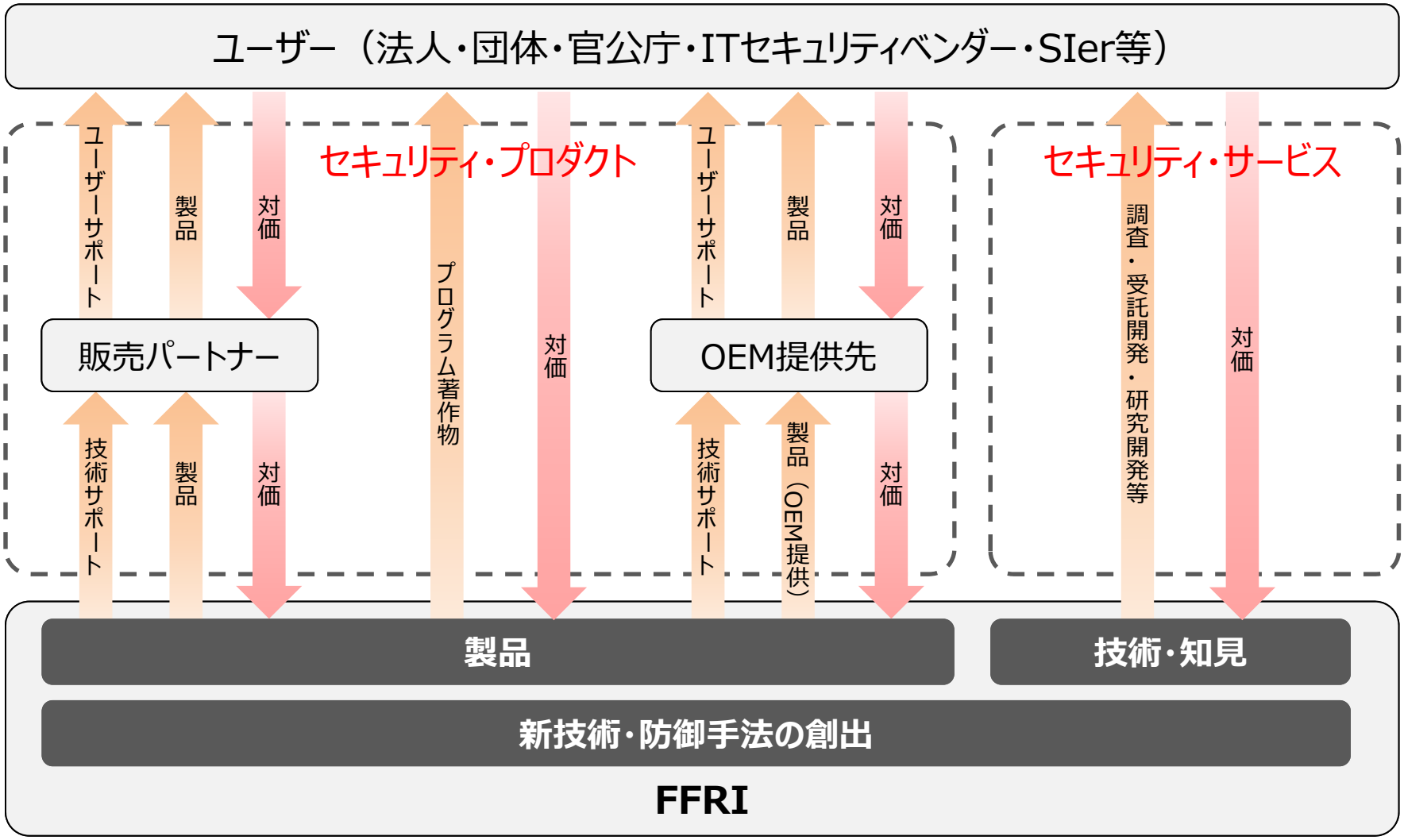


国内標的型サイバー攻撃向け特化型脅威対策製品市場
製品別売上予測、2013年～2018年

出典：国内標的型サイバー攻撃向け対策ソリューション市場予測
2014年10月23日　IDC Japan株式会社

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等）
セキュリティ・プロダクト
セキュリティ・サービス
ユーザーサポート
製品
対価
販売パートナー
プログラム著作物
対価
ユーザーサポート
製品
対価
OEM提供先
調査・受託開発・研究開発等
対価
技術サポート
製品
対価
技術サポート
製品（OEM提供）
対価
製品
技術・知見
新技術・防御手法の創出
FFRI

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
ヒューリスティック検出技術で
未知の脅威に対抗する
日本発の次世代セキュリティ

製品のライセンス体系

		YEAR 1 （新規契約）	YEAR 2～ （契約継続）	YEAR X （契約終了後）
サブスクリプション ライセンス （期限付きの使用権）	提供内容	使用権 バージョンアップ 技術サポート	使用権 バージョンアップ 技術サポート	
	対価	ライセンス料	ライセンス料	
パーペチュアル ライセンス （無期限の使用権）	提供内容	使用権 バージョンアップ 技術サポート	使用権 バージョンアップ 技術サポート	使用権
	対価	ライセンス料	保守料	

主要なセキュリティ・プロダクト

名称	内容
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。
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。
FFRI Limosa	インターネットバンキングにおけるMITB攻撃対策製品で、PCがMITBマルウェアに感染してもMITBマルウェアがブラウザに干渉できないような保護機構により攻撃から守ります。

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の特徴

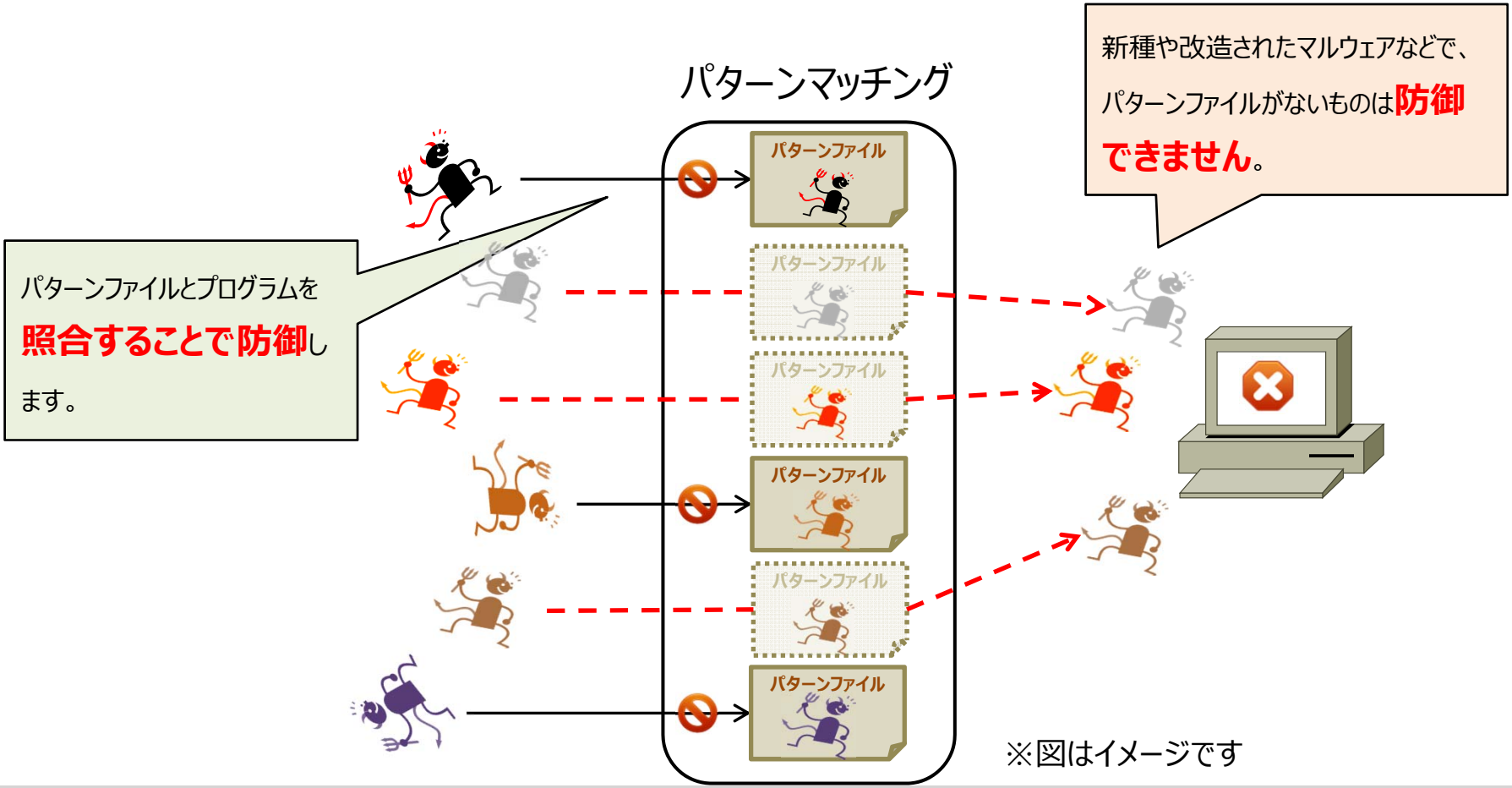
技術的優位性

組織的なR&D体制

技術力を裏付ける確かな実績

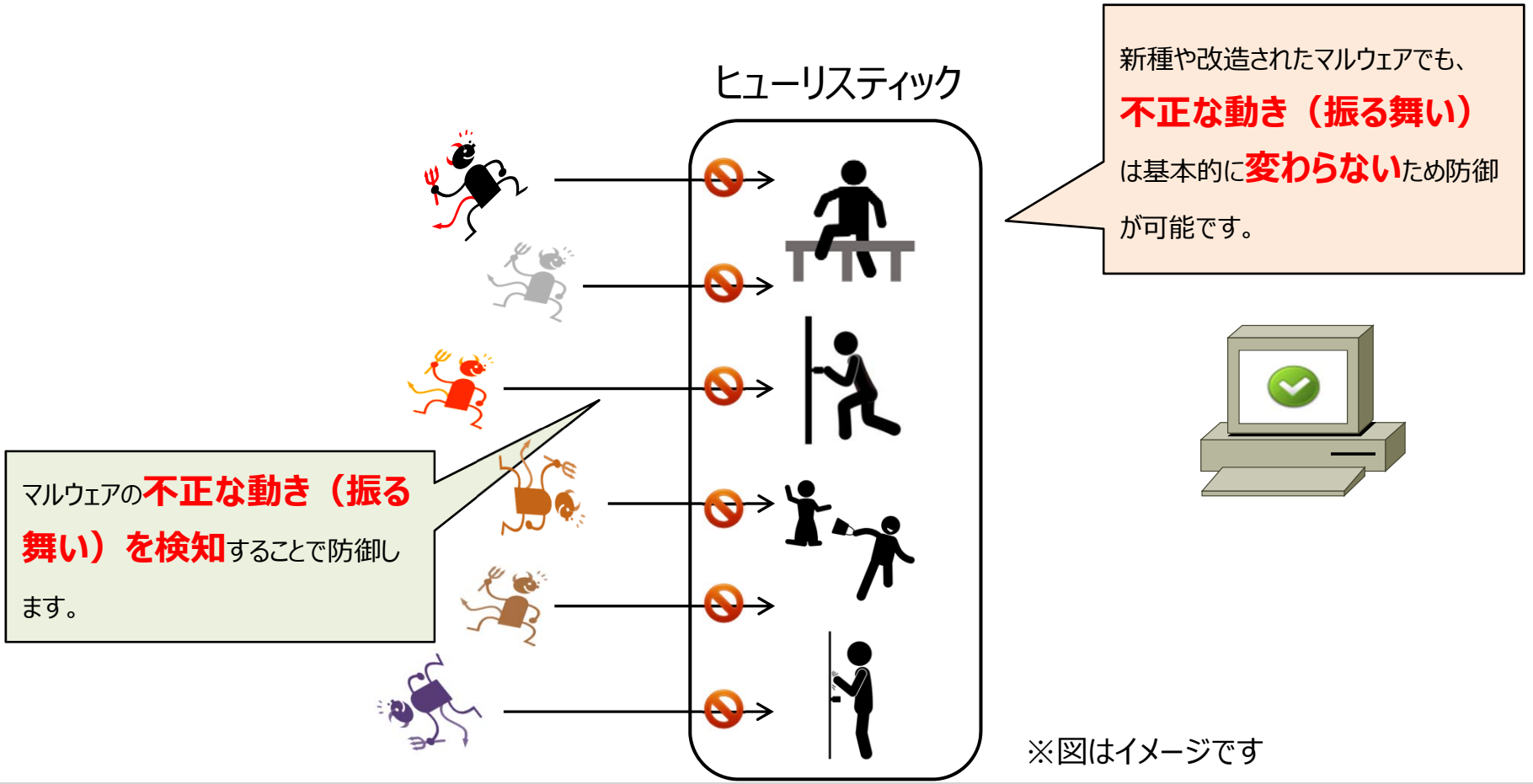
技術的優位性

ロ 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



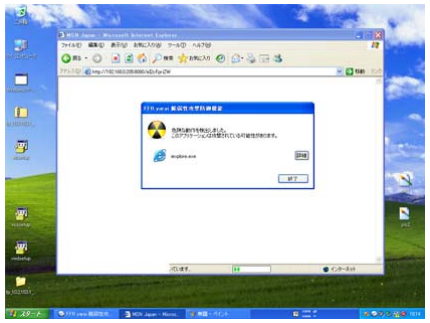
技術的優位性

ロ 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



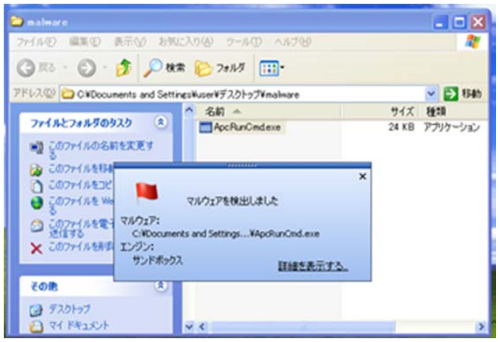
2011年9月、日本の防衛産業メーカーに対し、標的型攻撃と思われるマルウェア感染が発生しました。

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 韓国へのサイバー攻撃マルウェア

2013年3月、韓国の放送局や金融機関のシステムに障害が発生しました。障害の原因は組織内のWindows端末がマルウェア感染によりダウンしたためです。

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。



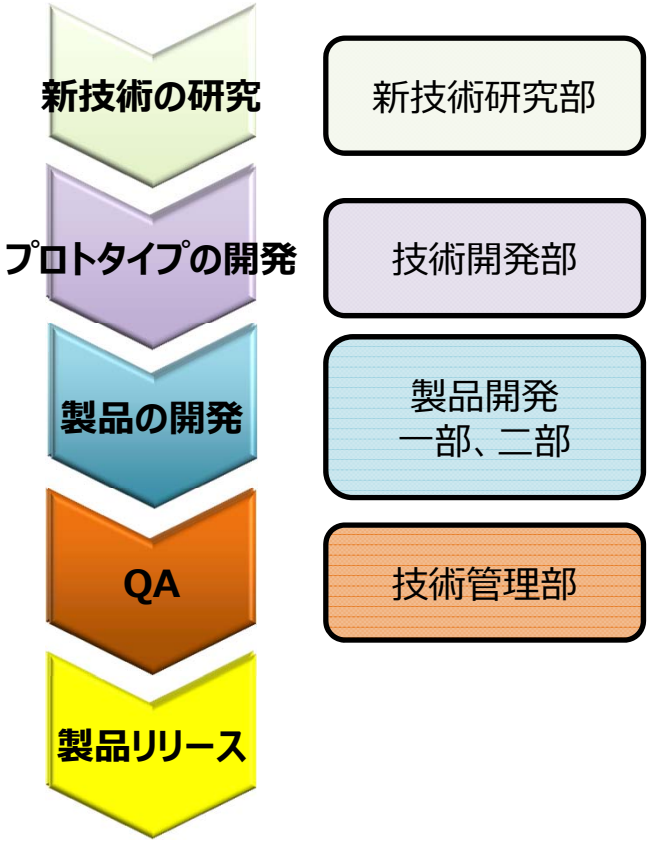
組織的なR&D体制

最新技術を組織的に開発

技術部門の体制

最高技術責任者	研究開発本部	**新技術研究部** 〔役割〕 セキュリティ新技術の調査・研究
		技術開発部 〔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
		セキュリティコンサルティング部 〔役割〕 受託開発、セキュリティ調査・分析・研究等 及び教育サービスなどのセキュリティ・サービス
	製品開発本部	**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

製品開発の流れ



技術力を裏付ける確かな実績

- サイバーセキュリティに関する国家プロジェクトへの参画
  - 総務省の「官民連携による国民のマルウェア対策プロジェクトACTIVE」に参画
- サイバーセキュリティに関する国際的なプロジェクトへの参画
  - インターポールとNECのサイバーセキュリティ対策の提携に参画し、国際的なサイバー犯罪対策を強化するセキュリティソリューションの開発を支援
- 日本のサイバーセキュリティ人材育成の支援
  - セキュリティ・キャンプ等への講師派遣

INTERPOL Secretary General Ronald K. Noble氏（右）

「ACTIVE推進フォーラム第1回会合」 明治記念館(東京都港区)

業績説明

業績サマリー

（単位：百万円）

	平成26年3月期	平成27年3月期2Q	平成27年3月期(予想)
売上高	660	282	863
営業利益 (利益率：%)	171 (26.0)	10 (3.7)	207 (24.1)
経常利益 (利益率：%)	172 (26.1)	△3 (－)	192 (22.3)
当期(四半期)純利益 (利益率：%)	115 (17.6)	△2 (－)	119 (13.9)

- セキュリティ・プロダクト
  - 「FFR yarai」及び「FFR yarai脆弱性攻撃防御機能」が好調に推移
  - 平成26年３月に日本電気㈱との間で締結したソフトウェア譲渡契約に基づき、２Q累計期間において譲渡対価54,000千円の売上を計上
- セキュリティ・サービス
  - セキュリティ調査・分析・研究等、製品カスタマイズ、PrimeAnalysisにて、計画外の案件を複数受注

売上の季節的変動について

- 売上の計上は、当社の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。

（単位：百万円）

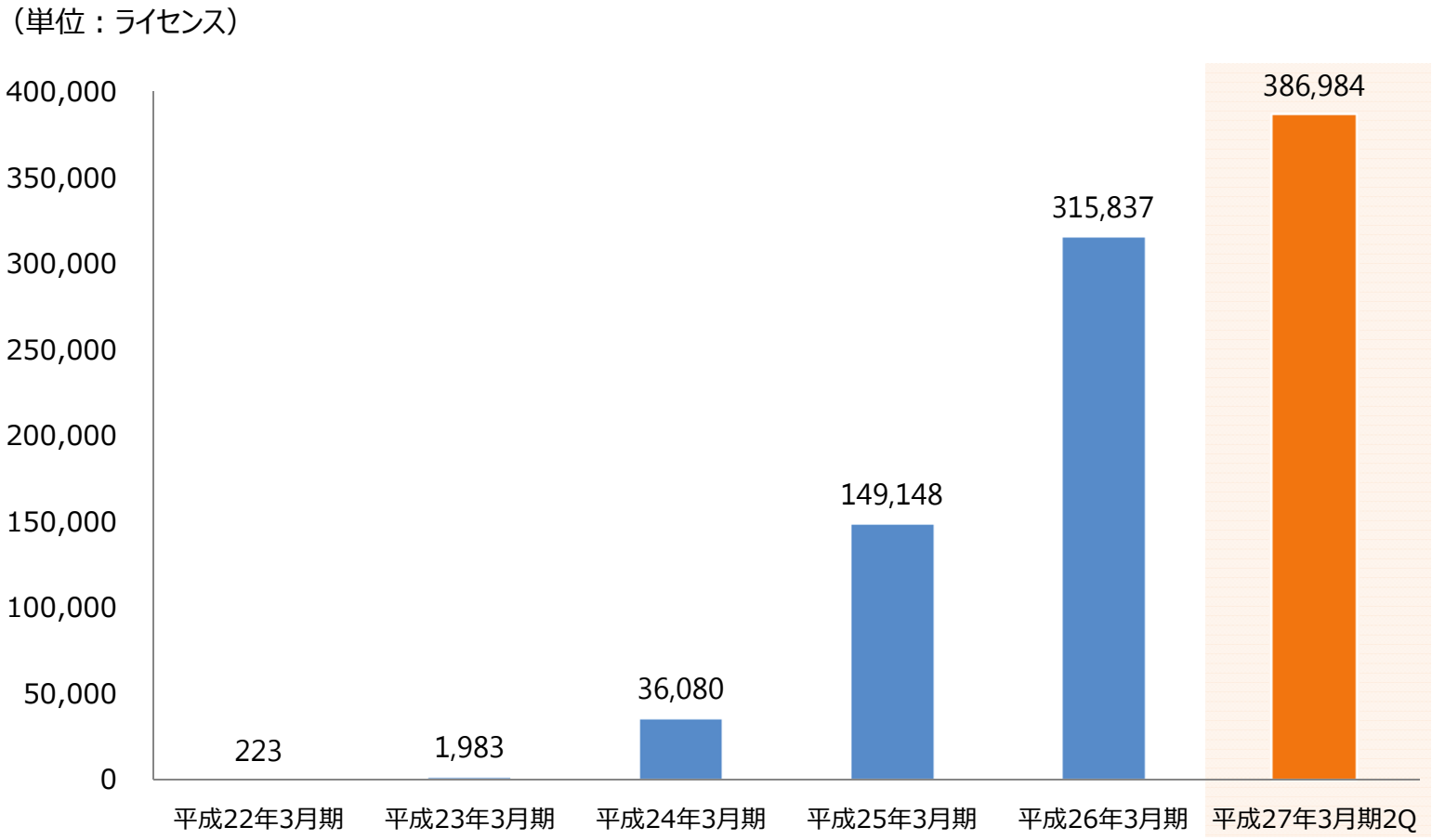
平成27年3月期	第１四半期 (実績)	第２四半期 (実績)	第３四半期	通期 (予想)
売上高	164	282	－	863
進捗率(%)	19.1	32.8	－	100.0

(注)平成27年３月期の進捗率は、平成27年３月期通期業績予想に対する割合です。

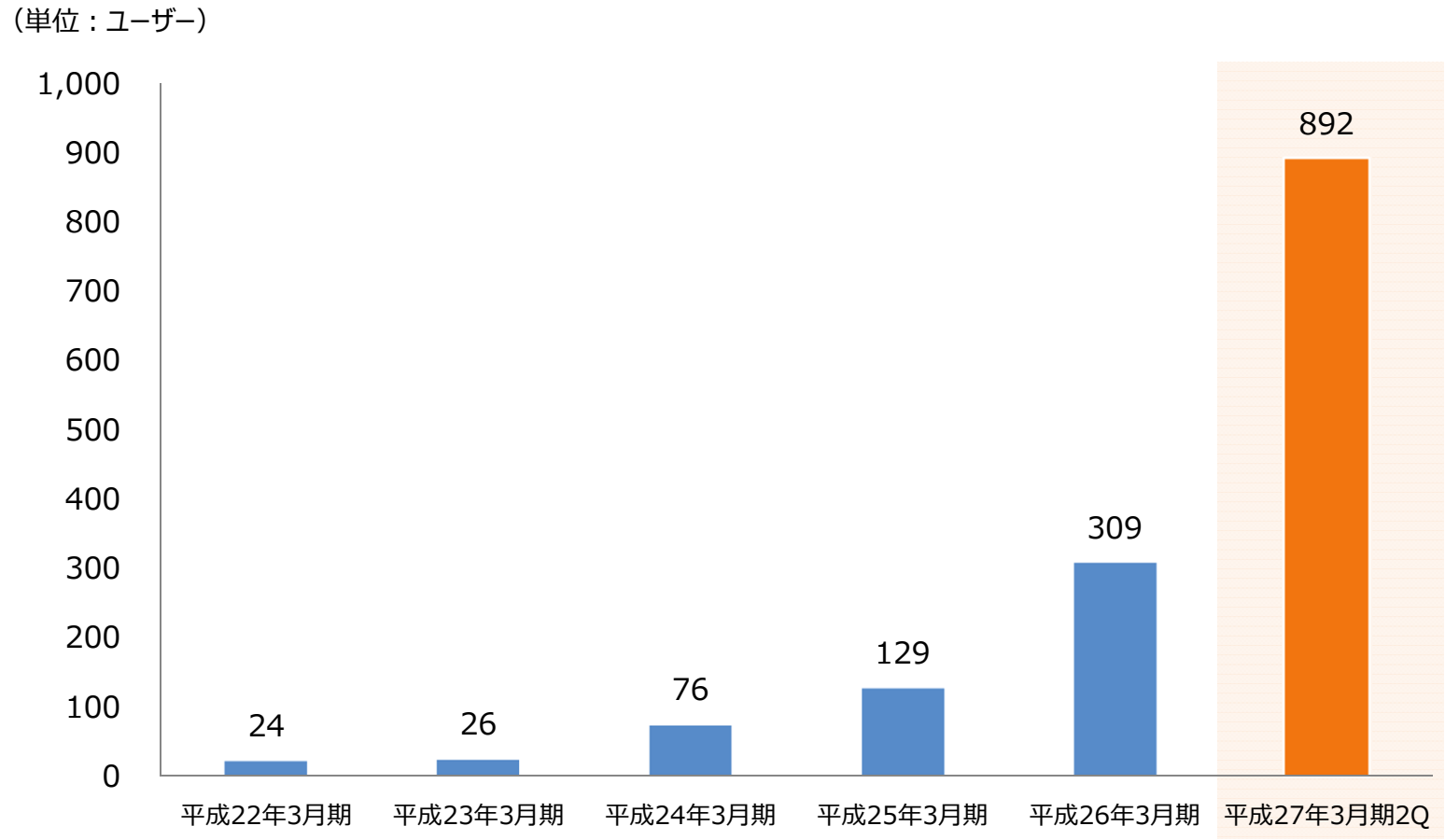
平成26年3月期	第１四半期 (実績)	第２四半期 (実績)	第３四半期 (実績)	通期 (実績)
売上高	66	159	264	660
進捗率(%)	10.1	24.1	40.1	100.0

(注)平成26年3月期の第１四半期から第３四半期の各数値については、有限責任 あずさ監査法人の四半期レビュー及び監査を受けたものではありません。

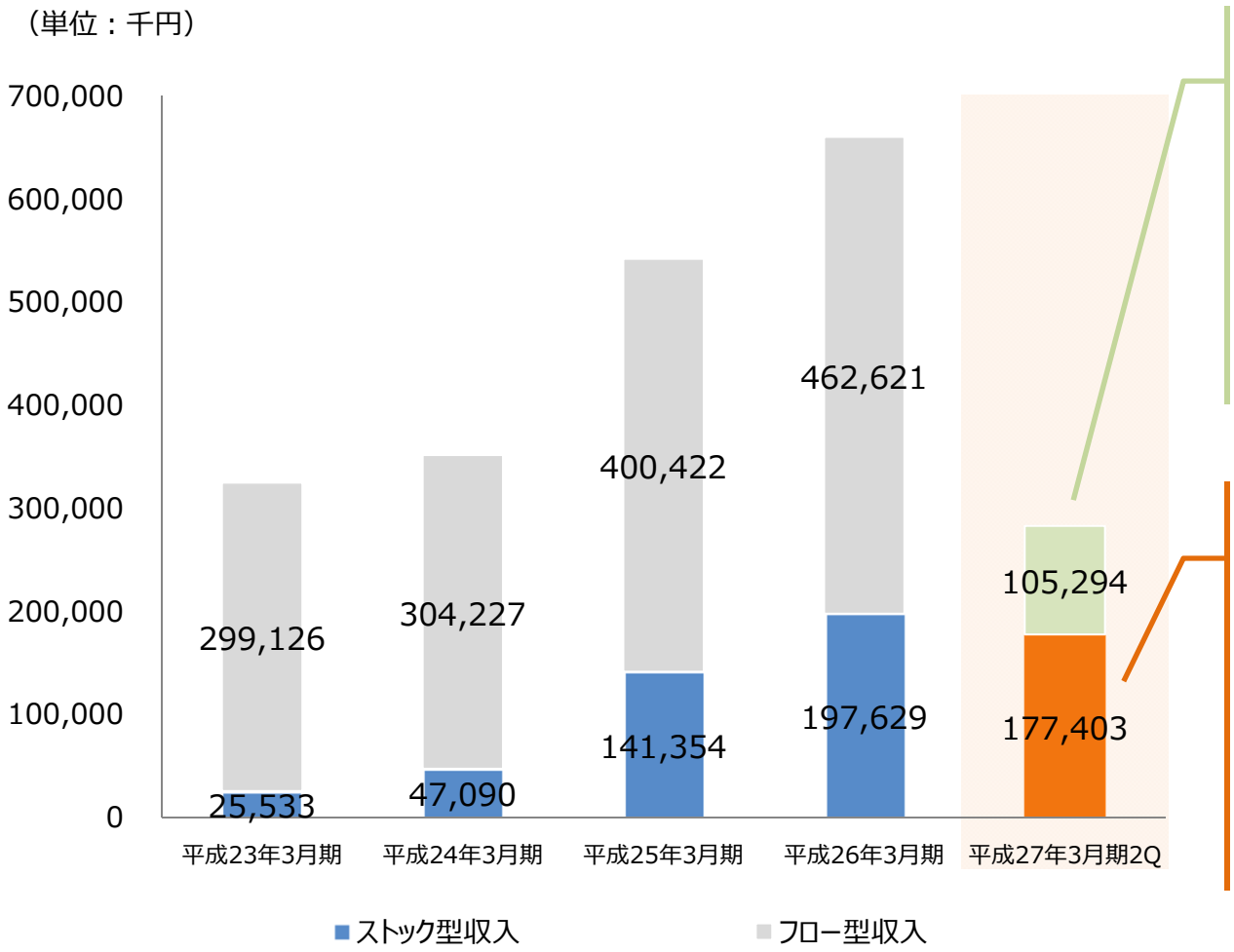
FFR yaraiの契約ライセンス数の推移



FFR yaraiの契約ユーザー数の推移



ストック型収入とフロー型収入の内訳



フロー型収入

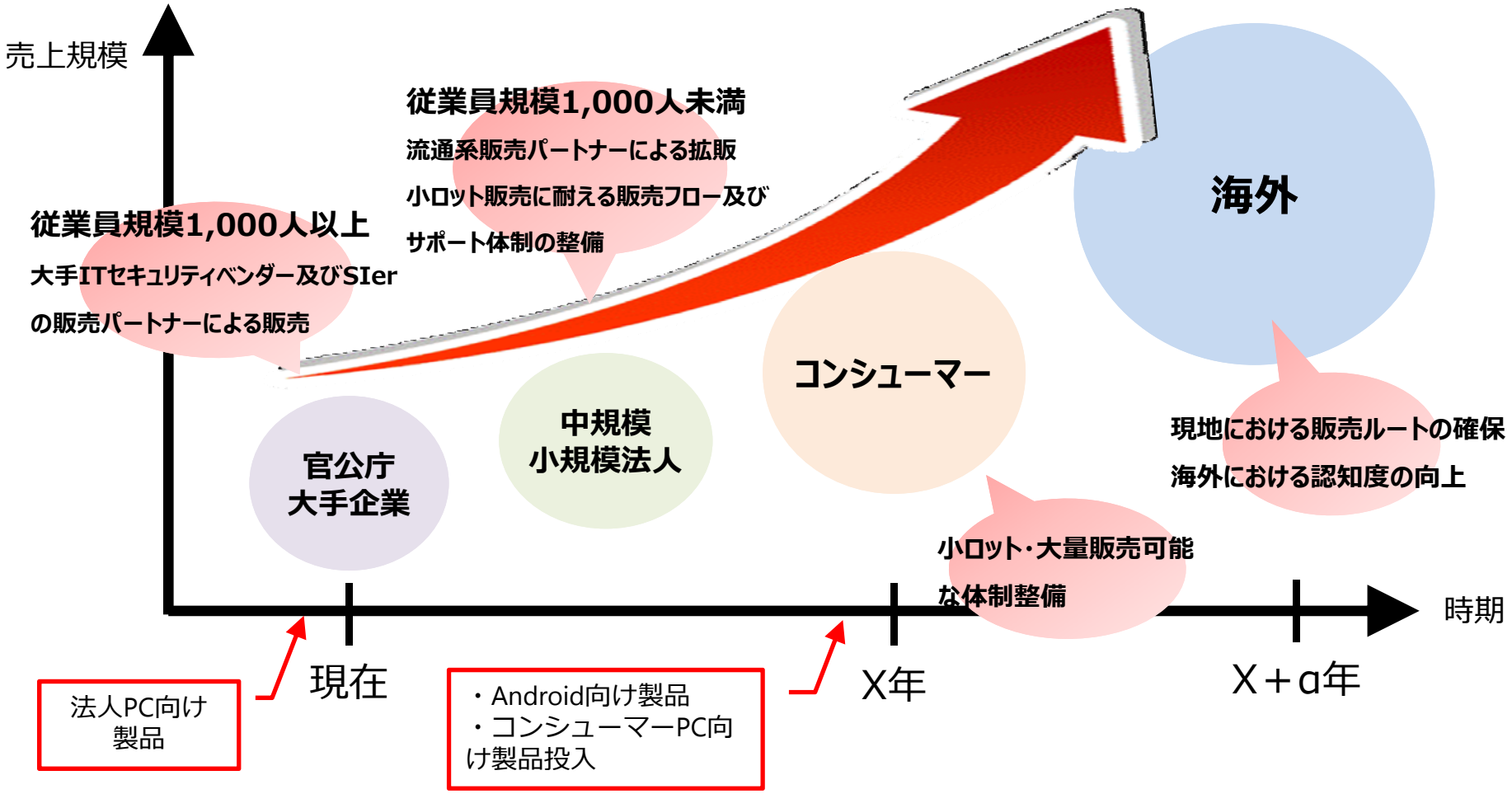
セキュリティ・サービス、セキュリティ・プロダクトにおけるパーペチュアル契約(利用期間の定めのない契約)で、納品・検収のタイミングで計上される売上

ストック型収入

セキュリティ・プロダクトにおけるサブスクリプション契約(利用期間を定めた契約)、製品保守契約で、ユーザーが利用をする限り、毎期継続して見込める売上

今後の取組み

目指すはすべてのコンピュータ・システムへ当社製品の導入



＜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。

ご清聴ありがとうございました。

株式会社 FFRI

TEL　: 03-6277-1811
FAX　: 03-3449-2302
URL　: http://www.ffri.jp/

参考資料

代表者紹介

鵜飼　裕司　（Yuji　Ukai）

株式会社FFRI 代表取締役社長

独立行政法人情報処理推進機構
情報セキュリティ技術ラボラトリ研究員

Black Hat - Content Review Board Member
※Blackhat：世界最大の情報セキュリティカンファレンス
※アジア唯一の論文査読委員を担当

CODE BLUE　レビューボード長
※ CODE BLUE：2014年2月に開催された日本発の情報セキュリティ国際会議

起業前は、eEye Digital Securityの米国本社でセキュリティ脆弱性分析や
組み込みシステムのセキュリティ脅威分析等に関する研究開発に従事

サイバーセキュリティを取り巻く状況

国家	サイバースペースは第五の戦場 サイバー戦争、サイバー諜報活動が活発に
企業	サイバー攻撃による事業継続性リスクの増大 標的型攻撃による機密情報漏洩、システム破壊
個人	マルウェア感染による被害がいたずらから実害へ ネットバンキングでの不正送金が社会問題化
攻撃者	サイバー攻撃基盤のエコシステム化 アンダーグラウンドマーケットの活性化
セキュリティベンダー	アンチウイルスは死んだ 新たな対策技術の必要性の高まり

国策としてのサイバーセキュリティ対策

中央官庁の重要な情報システムに対して
6秒に1回以上のサイバー攻撃が発生 ※

政府としてのサイバーセキュリティ体制の抜本的強化を図るための
立法措置として「**サイバーセキュリティ基本法**」の成立を検討

国産のセキュリティ対策技術で国益を守る必要性

- 研究開発予算の拡大
- 対応人員の増加

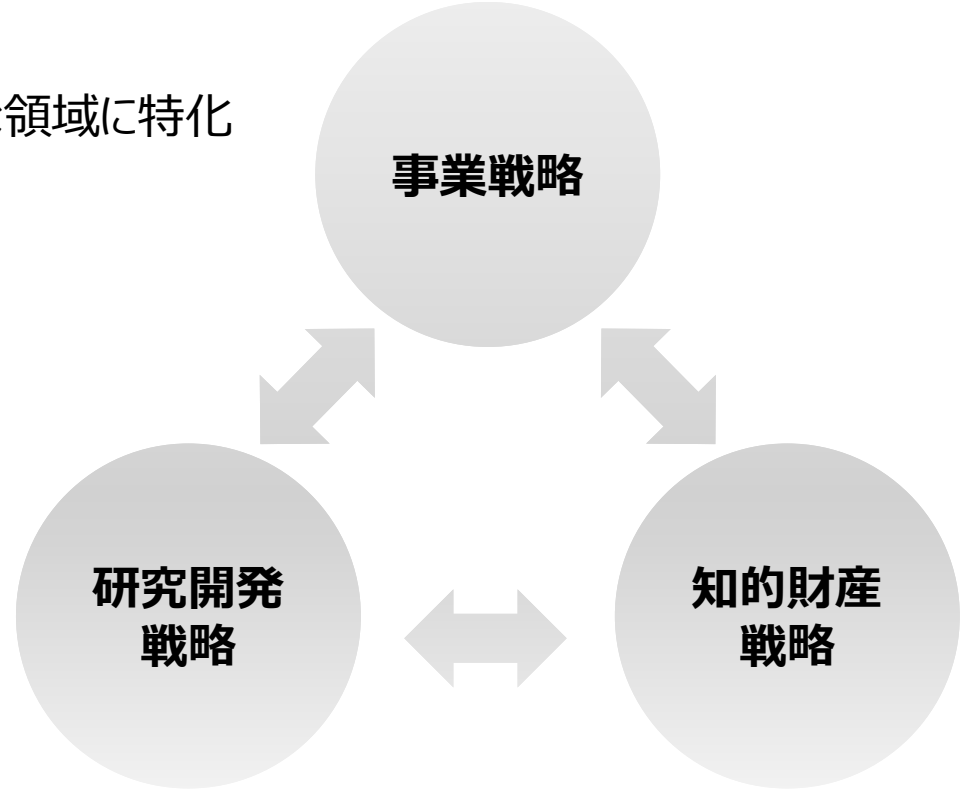
※出典：「サイバーセキュリティ政策に係る年次報告（2013年度）」（2014年7月10日 NISC）

経営戦略

- 研究開発戦略
  - 技術障壁が高く、他社が実現困難な領域に特化
    将来の脅威分析、調査研究
    新技術（基礎技術）の研究開発

- 知的財産戦略
  - 研究成果である技術シーズの蓄積
  - 技術シーズの特許化による権利保護
  - 競合動向の調査

- 事業戦略
  - 新しい脅威対策の市場ニーズの把握
  - 技術シーズの収益化
    製品化して販売（OEM等によるライセンス提供含む）
    技術シーズそのものの販売またはライセンス提供
    技術シーズ関連のサービス、コンサルティングの提供、etc…



研究開発方針と注力分野

研究開発方針

- 現在の脅威分析から将来的に発生し得る脅威を予測
- 他社が実現していない技術的に困難な領域に特化

注力分野

- セキュリティ脆弱性に関する研究、対策技術開発
- マルウェアに関する研究、対策技術開発
- 社会インフラのセキュリティに関する研究、対策技術開発

主要なセキュリティ・プロダクトの利用形態・販売価格

名称	利用形態	ライセンス形態	価格	販売店仕切率
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%
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%
FFRI Limosa	1 組織に 1 ライセンス	サブスクリプション	1,000,000円/年(～20,000口座)～25,000,000円/年(口座数無制限)	40%～50%

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アンチウイルス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。