資料３

# 国産サイバーセキュリティの現状と課題


**FFRI, Inc.**
https://www.ffri.jp

# 会社概要

| | |
|---|---|
| **会社名：** | 株式会社ＦＦＲＩ（東証マザーズ：3692） |
| **代表者：** | 代表取締役社長　鵜飼　裕司 |
| **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 |
| **設立：** | 2007年7月3日 |
| **資本金：** | 2億8,613万6,500円（2018年11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<br>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<br>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<br>4. 上記事業に関連する一切の業務 |
| **子会社：** | FFRI North America, Inc.(2017年4月3日設立) |

# 現状

- 基礎技術や対策製品等は海外依存
  - 「輸入」して展開する「販売店」
  - 付随するサービス（導入・運用等）を提供

- 役割分担
  - サイバーセキュリティベンダー像は国内と海外では大きく異なる

日本にとってはメリットとデメリット

# 日本にとってのメリット

エンドユーザー

- 既に実績のある技術を使える。対策が大失敗するリスクを回避できる

セキュリティベンダー

- 研究開発リスクを回避。投資回収も容易。事業上のリスクを極小化
- 研究開発の実施体制を作る必要がない。
  採用・育成等リスクの高い課題に取り組まなくて良い
- 実績作りなどマーケティング面で難しいハードルを越える必要がない

# 日本にとってのデメリット

エンドユーザー

- 要望やトラブル発生の際、マーケットサイズに応じた対応
  日本固有の事象についてはフィルタされる事も
- 基礎技術が蓄積できない。日本独自で対応できない

セキュリティベンダー

- ビジネス上スケールメリットのある部分を奪われる。利益率が悪い
- ビジネスの多くが人依存。仕組みの台頭でビジネスが駆逐されるリスク

両者

- 最先端の術を利用する事が難しい
  （セキュリティベンダーのリスクヘッジのため、実績のあるもののみ展開）

# 海外と日本の違い

- 日本におけるメリット（？）
  → 研究開発リスク、営業マーケティングリスクをヘッジできる
  しかし、北米ではこれらリスクをヘッジできる仕組みがある

- 研究開発リスク
  – 研究開発人材や資金が非常に豊富
  – 研究、開発、事業化、産業化に至るプロセスやモデルが確立

  技術者が起業しても大きくできる仕組みがある
  （VCのハンズオン、政府調達による実績作り、豊富な専門人材など）

- 技術力(質)そのものには大きな違いはない
  – アイデアやシーズを事業化、産業化する仕組みが大きく異なる
  – 日本のセキュリティ業界にとっては変化のインセンティブは薄い

# 今後の取り組むべき課題

- 低利益型のビジネスからの脱却
- 研究開発機能を持たないリスクへの対応

→ セキュリティ業界の現状維持バイアスは強い

国際競争力のあるサイバーセキュリティ産業を作るためにリスクを取る

研究開発リスク
→ 事例は少ないがノウハウは存在

営業マーケティングリスク
→ 日本（特に大企業）にノウハウが蓄積

それらがミックスされていない事が課題