Vol.2016-IS-137 No.11
2016/8/26

情報セキュリティビジネスにおける競争優位創出のための要因

伊藤博康[†1]　深見嘉明[†2]

概要：情報セキュリティビジネスにおける競争優位創出のための要因が，レイヤースタックにおける技術的優位性が 1 要因としてあるのではないかということを問題意識の始点とし展開している．本稿では，CPU というハードウェアレイヤーに対してセキュリティという技術要因を獲得することで，「IoT」という情報技術のトレンドの変化をとらえ，情報セキュリティ市場に対して競争優位を創出する影響を及ぼしたことを分析した内容について述べる．ハードウェアレイヤーからソフトウェアレイヤーに対して垂直統合型の技術要因を獲得することによって，情報セキュリティ市場への競争優位の獲得につながることが明らかになった．

キーワード：レイヤー，垂直統合型システム，製品ポートフォリオ，情報セキュリティ

1. はじめに

情報の持つ価値はコンピュータやインターネットの普及に伴いその重要性を増してきている．近年ではスマートフォンに代表されるモバイル端末や Internet of Things（IoT），ウェアラブルデバイスなどといった様々な形で情報を扱う技術が加速度的に発展している．このように情報技術（IT）が発展していくことで情報そのものを守るためのセキュリティも重要性を増し，またセキュリティ技術は広範囲かつ高度な技術を要求されるようになった．情報セキュリティを製品やサービスとして扱う企業も年々増加し，情報セキュリティビジネスを扱っている企業は例えばクラウドやドローンといった IT の外部環境の変化に対応するためにセキュリティ技術を開発しながら，競合する企業に対して常に競争優位を獲得するために努力している．また，情報セキュリティは技術トレンドの後追いで必要なセキュリティを見極めながら常に技術トレンドに早い速度で対応していかなければならないという特性をもっている．

競争優位を獲得しているソフトウェアの中には，プラットフォーム戦略を活用し，補完業者としての戦略や，アーキテクチャによるレイヤー間でのネットワーク効果の有効的な活用などの戦略を採っていること場合がある．情報セキュリティ分野においても，このようにプラットフォームや複数のレイヤーが存在するアーキテクチャを前提とした戦略が競争優位の獲得の要因になるのではないかという仮説に基づき，情報『セキュリティ』ビジネスにおける競争優位創出要因について分析する．

2. 論旨の展開と背景

2.1 情報セキュリティビジネス

情報セキュリティとは，「情報の機密性，完全性および可用性を維持すること」であり，情報セキュリティビジネスは情報セキュリティを保持していくための製品やサービスを顧客へ提供することである．本研究では，個人よりも多くの情報セキュリティレイヤーでのセキュリティ技術が必要である BtoB の情報セキュリティビジネスを提供する企業を対象とする．

情報セキュリティビジネスの市場は多様化の一途をたどっている．これは，新しい技術の展開に伴い顧客が守るべき情報資産が増加していることや，セキュリティリスクが多様化していることがあげられる．多様化するセキュリティリスクのすべてに 1 企業が対応していくことは難しく，複数の企業が提供する製品やサービスを導入することによって垂直統合型のシステムを導入することで被提供企業は情報セキュリティを確保しているという現状がある．また，情報セキュリティを提供する企業においても，エンドポイントでコンピュータウイルスから情報を守るアンチウイルス製品や，ネットワーク経由での情報漏えいを防止するためのアプライアンス製品など，図 1 のようにある程度レイヤー間で住み分けがなされているa.

†1 (株)日立ソリューションズ
Hitachi Solutions Ltd.
†2 立教大学
Rikkyo University

a 独立行政法人情報処理推進機構　2009 年　情報セキュリティ産業の構造に関する基礎調査を参考に筆者作成

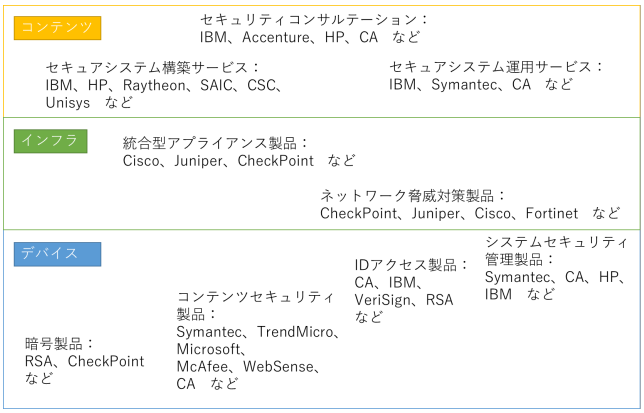

図 1　主要プレイヤーの住み分け

2.2 ソフトウェア市場との構造比較

ここで，階層化が進んでいるソフトウェア市場と比較する．ソフトウェア市場ではソフトウェアのレイヤースタックが形成され，ユーザに提供される製品は 1 階層に位置しながらも他の階層への製品と補完関係を持ちつつ，他の企業が提供する製品と熾烈なポジション争いが行われている．（図 2）

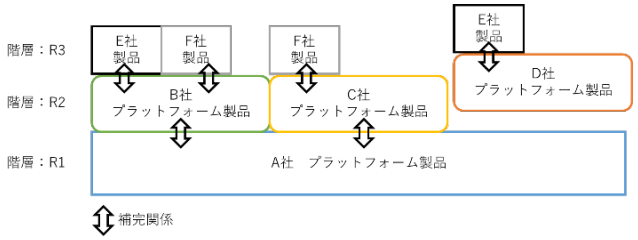

図 2　レイヤー間の競争関係

また，強い市場支配力をもつ（ドミナント化）することで，価格や標準的な技術仕様の決定などに強い影響を及ぼすことが可能である．情報セキュリティビジネスにおいても，レイヤースタック内の各階層で製品が提供され，他のソフトウェア製品などとの補完関係がある．しかし，ソフトウェア市場における Windows や Google 検索のようにドミナント化した製品やサービスはまだなく，熾烈な市場競争が繰り広げられている．技術トレンドが変化することで初めて効用が生まれ，市場の需要が発生する情報セキュリティ市場では，特定の IT 技術に特化すれば市場での支配力が強化されるということは少ないため，製品やサービスがドミナント化しにくい市場といえる．しかし，情報セキュリティ市場においても強力なプレイヤーは存在しており，これらの企業がいかにして競争優位を創出しているのかが本研究の分析課題である．

2.3 研究対象について

情報セキュリティビジネスの競争優位創出の要因を分析するにあたって，本研究では McAfee 社と Symantec 社のビジネスポートフォリオを分析していく．これは，両社とも垂直統合型システムで製品やサービスを提供する企業であり，それぞれの事業ポートフォリオが異なっているため，複数のレイヤーを横断するアーキテクチャと，事業戦略を紐づけて分析することが可能であり，両社の戦略を比較分析していくことで競争優位の要因を抽出することができるからである．

2.4 技術トレンドの変遷

近年の情報技術における大きな変化は，IoT を実現するデバイスの増加とモバイル端末の普及にある．近年では POS 端末や工作機械など，今までインターネットに接続されなかったデバイスのマルウェア対象が拡大しており，新たなセキュリティに対する脅威となっている．同様にモバイルデバイスの普及は，マルウェア感染対象の増加につながるため，セキュリティに対する脅威の増加につながっている．

本論文の分析対象事例である，McAfee 社と Intel 社の買収前のモバイル分野と IoT 分野の技術トレンドの変遷について以下にまとめる．

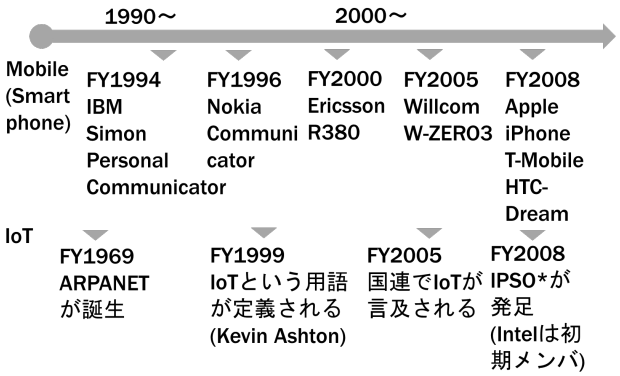

図 3　技術トレンドの歴史（IoT とモバイル）

2.5 必要なセキュリティ技術とは

IoT で利用されるデバイスの多くはセキュリティ対策が十分ではない．なぜなら，IoT に利用される端末は性能・機器の仕様ともにまちまちであり，企業ユースの PC のようにある程度定型化されたものではない．また CPU やメモリなどのリソースは限定されているのも不十分なセキュリティ対策の要因である．

たとえば，機器が十分なメモリ容量を有していない場合，ソフトウェアのセキュリティパッチの適用はできない．これにより，脆弱性が発見された場合でも対策することは困難になる．このため，現状ではそれぞれの機器が持つリソースに依存したセキュリティ対策を個別に行っていく必要があり，膨大なコストがかかっている．

情報セキュリティ製品は，階層化されたレイヤーのコンポーネントそれぞれの補完財として市場へ供給されること

が多い．OS 上で動作するアンチウイルスソフトや，ネットワークレイヤーで機能するファイヤーウォールのようなアプライアンス製品がその典型である．IoT デバイスなど低スペックのコンポーネントをより少ないリソースでセキュリティを担保するためには，階層構造の低いレイヤーで対応することが望ましい．セキュリティ脅威となるインシデントが発生した場合でも，低レイヤーでセキュリティが確保されていることで，上位階層のプラットフォームを切り離すことで全体としてセキュリティが確保される．つまりこれは階層間の非対称の依存関係を活用するのである．例えばある端末がマルウェアに感染した場合，その端末を物理的にネットワークから切り離すことで，ネットワークを経由して他の PC やサーバなどへの感染や，外部サーバへの情報流出を防ぐことが出来る．

3. 先行研究レビュー

3.1 先行研究の概要

本稿では，多層のレイヤーによって構成されるアーキテクチャにおいて重要な概念であるプラットフォームおよび，関連するソフトウェア製品戦略について先行研究を概観し，情報セキュリティ製品における課題を明確にする．

3.2 レイヤード・モデュラー・アーキテクチャ

PCの中にはWindows OSがあり，Windows OS上では様々なアプリケーションが動作する．このように，独立したアプリケーションよって共通に活用されるモジュールはプラットフォームと呼ばれる．複数のモジュールが連携して機能する場合，その全体はシステムと呼ばれる．複雑なシステムを開発するためには，多様なモジュールをどのように組み合わせるかというアーキテクチャ[1]の設計が重要である[2]また，イノベーション研究においてもモジュール化は重要であり，製品アーキテクチャについてまとめられている[3].

一企業という主体が，ユーザに対してハードウェアやソフトウェアなどを組み合わせて提供する場合や，複数の企業という主体がそれぞれ組み合わせて提供する場合がある．また，先の Microsoft Office と Windows OS，Windows OS と CPU は互いに連携して動作しており，階層構造として積み重なっている(図 4)．このようなアーキテクチャを，レイヤード・モデュラー・アーキテクチャ[4]と呼ぶ．各階層をレイヤーと呼ばれ，上のレイヤーにある製品や技術は，下のレイヤーの製品や技術の存在を前提とするが，下のレイヤーにある製品や技術は，上のレイヤーにある製品や技術の存在は前提としない．このような関係性は，ソフトウェア製品に多くみられる関係であり，後述するが階層間における依存関係を利用することによる戦略が分析されている．

レイヤーは上下間において非対称の依存関係を持つ．CPU 上の OS については階層間の依存関係を持っており，CPU が壊れると OS は動作しないが，OS が壊れても CPU には影響しないという非対称の依存性が存在するということである．

今回の研究では，対象とするセキュリティアーキテクチャの階層構造を図 4 のように定義する．

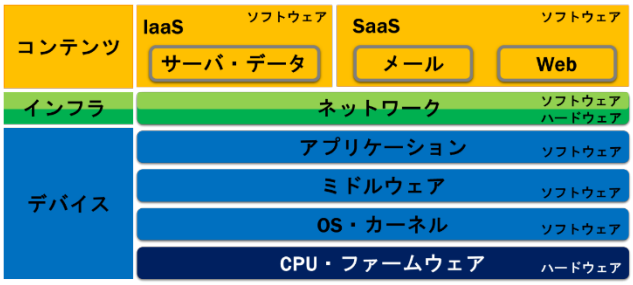

図 4　セキュリティアーキテクチャの階層構造

3.3 プラットフォーム

プラットフォームは，複数のモジュールや補完財が共通して利用するモジュール [5]であり，Microsoft Office や様々なアプリケーションが動作する Windows OS のなどが代表的な例である．複数の補完財がプラットフォームと連携して動作するため，補完材に対するインターフェイス設計は相互可用性の実現が重要な要素である．プラットフォームは多数の補完財を含むソフトウェアエコシステム[6]を構成するために重要な役割を担う．ソフトウェア産業におけるエコシステムとは，OS などを開発するデベロッパー，OS を販売するベンダ，OS の補完財を提供するサードパーティー，OS や補完財を利用するユーザが有機的に関係性を持ち，成長していく構造である．ソフトウェアエコシステムを形成することにより持続的にコストを分散しながら競争優位を形成できる．Windows OS や Mac OS に代表される OS というプラットフォームを構築することで，その上で動作するアプリケーション（補完財）を外部供給してもらうことで，ネットワーク外部性を活かし，そのエコシステム全体の価値を大きく増大させることができるからである．

プラットフォームは製品の構造を階層的にとらえて表現する場合や，それに対応した産業構造の階層性を前提にして，ある条件を満たす階層部分を呼ぶ[7]こともある．ソフトウェア産業はハードウェア，OS，ソフトウェアアプリケーションのように階層的に製品が存在して動作する．

また，製品が別々になるということでそれぞれの製品ごとに産業が存在することが可能となり，ハードウェアメーカや OS 製造メーカ，ソフトウェアアプリケーションベンダなど多くの企業がエコシステムを形成している．

隣接する階層での支配的な地位を活かして競争優位を確立し，市場を奪うというプラットフォーム包囲戦略[8]

も重要な戦略である．この問題についても，階層化されたプラットフォームは他の脅威にさらされていることがいえるため企業間の競争が促進されることが言える．また，プラットフォーム・ソフトウェア市場においては，既存事業者と異なるレイヤー優先度を設定することが競争優位の要因となる[9]ことも議論されている．

3.4 階層におけるドミナントデザイン

Windows OS と MacOS の両方に対応するアプリケーションをラインナップとして揃えるなど，単一のプラットフォームにロックインされることを避け，複数のプラットフォームに補完財を供給する戦略はマルチホーミングと呼ばれる．コストをうまくマネジメントすることでこのプラットフォーム包囲から守るなどの手法がまた必要になる．このマルチホーミングコストは，複数のプラットフォーム製品を平行して利用することによって，利用するユーザにメリットを感じさせ受け入れてもらうことであり，このコストが低いほど複数のプラットフォーム製品を利用してもらえるというものである．逆にこのコストが高ければプラットフォーム製品の市場での独占傾向が高いということである．プラットフォーム提供ベンダはこのマルチホーミングコストの適切なマネジメントを行っていくことでドミナント化を目指していくことが望まれる．

3.5 プラットフォームにおける多面市場

例えば，Windows OS を販売するためには，Windows OS を搭載するためのハードウェアを製造する企業から支持を受けることは重要である．合わせて，Windows OS で動作する様々なアプリケーションを製造する企業からも支持を受けることも重要である．もちろん OS のユーザから支持を受けることも重要である．このように，ハードウェアやアプリケーション提供ベンダ，ユーザなど複数の市場で支持構成される市場は多面市場[4]と呼ばれる．

3.6 ネットワーク外部性と補完財

ソフトウェアを利用するユーザが増加すればするほどそのソフトウェアの価値が増大する．これは，ソフトウェアを財とみなしたとき，その財を利用するユーザが増加することで,その財がもつ価値が増加するという性質である．この性質をネットワーク外部性[10]という．

このネットワーク外部性は，直接的効果と間接的効果に分けられる．直接的効果はSocial Networking Service（SNS）のように，対象とするネットワークに接続される他者の存在があって初めて価値が生まれ，対象のSNSへの接続者が増加するほど価値も増大するという性質である[11]．間接的効果は，製品の価値が補完財の数や種類の増加によって増大することである．例えばWindowsにおけるInternet ExplorerやMicrosoft Office製品群が該当する[12].

ネットワーク外部性を効果的に効かせるため，プラットフォーム製品の普及を促進することで対象の製品を補完財として販売していくことも可能である．これは，Windows OS 上で動作する Microsoft Office 製品のように Windows OS という製品の補完財として Microsoft Office 製品を販売していくということである．補完財を販売することにより，ネットワーク外部性を生かし，プラットフォーム製品と補完財の結びつきを強くさせ，顧客に対して強力なロックイン効果を狙うことも可能である．ソフトウェア産業では，新規参入者の参入障壁が低い13ため，このように顧客をロックインする戦略は新規参入者への防衛にも効果的である．

このように，複数の市場から支持を得ることで以下の 3 つの条件が重なると「Winner take all（勝者総取り）」となることが言われている[14]．１．プラットフォーム間で差異を出す余地が小さい，２．プラットフォームと補完財でネットワーク外部性が強く働く，３．顧客が複数のプラットフォームを同時に購入することや，補完財を供給する複数のアクセスを防ぐことが可能となる．

4. 調査課題の導出

情報セキュリティは，プラットフォームのもつ影響が強く，階層構造やネットワーク効果は適用される．しかし，情報セキュリティは登場する新技術に対して，後追いで対応していかなければならないという特長ももつ．これは，新技術の登場ごとに対応するセキュリティ技術を検討しなければならないためである．

先行研究では，多層プラットフォームアーキテクチャにおいて複数階層に領域を拡張する戦略が効果的である事例が分析されている．この戦略は情報セキュリティビジネスにおいても有効であるのかが十分だろうか，この点について検討していきたい．つまり本研究の調査課題（Research Question：RQ）は以下のようになる．

RQ：情報セキュリティビジネスにおける競争優位創出要因
- RQ-1:どのような技術が必要になるのか
  （レイヤーごとに必要な技術をどのように選択するのか）
- RQ-2:情報セキュリティビジネスではネットワーク効果はどう影響するのか
  （補完財によるネットワーク効果）
- RQ-3:技術トレンドにどのように対応するのか
  （急速に変化する技術トレンドへの対応）

5. 事例研究

本社を調査課題に基づき，情報セキュリティビジネスにおける競争優位創出の要因を抽出することである．そのた

め，広範囲のレイヤーで事業ポートフォリオを持つ McAfee 社（並びに同社を買収した Intel 社の情報セキュリティ部門）と Symantec 社を比較分析の対象とする．この 2 社は 2011 年時点で Intel 社の情報セキュリティ部門が競争優位に立っているが，その競争優位がどのように構築されたのか分析する．

まず製品カタログデータを元にして，両者の事業ポートフォリオの変化を分析する．さらに，IoT とモバイルにおける技術トレンドの変化に対し，McAfee 社と Symantec 社がどのように対応しているのか分析する．

6. 事例から導出する分析

6.1 技術的課題に対応するために

McAfee 社と Symantec 社は，既存の製品やサービスのラインナップとして，デバイスのミドルウェアレイヤーやアプリケーションレイヤーで動作するアンチウイルス製品や Data Loss Prevention （DLP）製品を保有し，ネットワークレイヤーではファイヤーウォール製品，IaaS や SaaS ではクラウド上のデータ保護製品やメール，Web のセキュリティ製品などを保有している．

新たなセキュリティ脅威が発生する中，分析対象の McAfee 社と Symantec 社では新たな脅威に対応するためにこれまでは自社で保有していない技術開発や製品開発を行っている．しかし，両社はともにソフトウェアパッケージを主事業としており，ソフトウェアだけでは新たなセキュリティ脅威に対応するための技術的な限界がある．

以下の図に，各社の事業ポートフォリオをセキュリティレイヤーごとに示す．

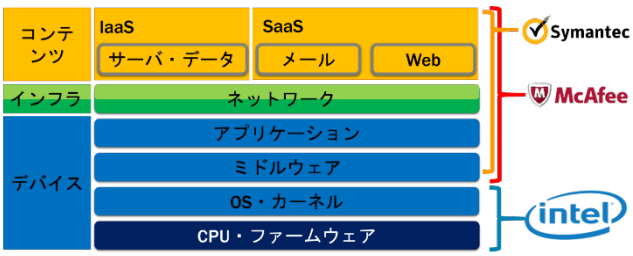

図 5　各社の技術ポートフォリオとセキュリティレイヤー

McAfee 社と Symantec 社はもともと同様の技術レイヤーに対して技術力を有しており，技術領域での差別化は困難な状況であるといえる．このため，Intel 社買収前の McAfee 社は Symantec 社と技術的なレイヤーでの差別化は困難であったが，買収後は Intel 社のもつ技術領域を McAfee 社が利用可能となり，Symantec 社に技術的な差別化を図ることが可能となった．

6.2 事業ポートフォリオの変遷

技術的課題から，McAfee 社と Intel 社は統合して技術的なポートフォリオを拡張した．次に，事業ポートフォリオの変化について示す．

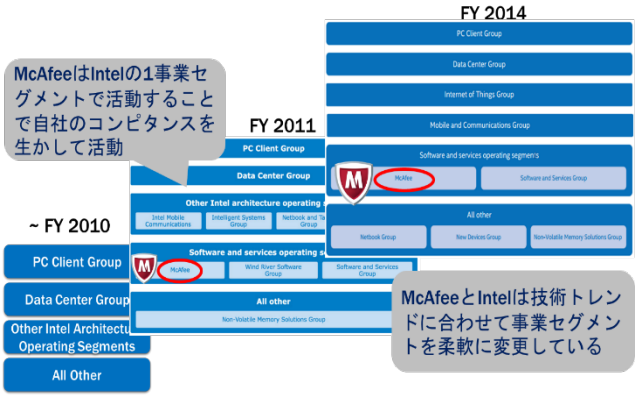

図 6　Intel 社の事業ポートフォリオの変化

同様に，Symantec 社の事業ポートフォリオの変化について以下に示す．

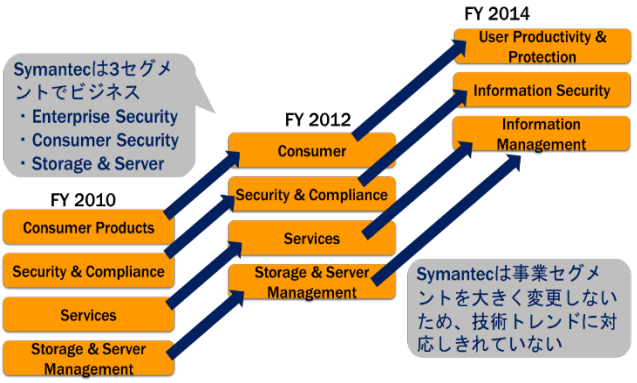

図 7　Symantec 社の事業ポートフォリオの変化

上記から，McAfee 社と Intel 社は，2011 年，2014 年と技術トレンドの変化に伴い，CPU などを事業の柱としている PC Client Group と，データセンターを事業の柱とする Data Center Group 以外に，Software を扱う事業セグメントの創設や，IoT，モバイルの事業セグメントを設立し，柔軟に事業ポートフォリオを変更し技術トレンドに従ったセキュリティ製品を市場へ投入しようとしていることが現れている．

Symantec 社においては，自社のコンピテンシーを活かすため，Enterprise，Consumer，Storage & Server の 3 つの事業部を大きく変更させることなく，技術トレンドの変化があっても自社の事業ポートフォリオを変化させずに事業を行っていることがわかる．このように事業ポートフォリオにおいて，McAfee 社は技術トレンドの変化に合わせて柔軟に事業ポートフォリオを変化させているといえる．

6.3 技術トレンドの変化に対応していくために

図 3 に示す技術トレンドの変化から，McAfee 社は Intel 社の持つ半導体と連携することで，McAfee DeepSAFE という技術を開発し，McAfee Deep Defender という製品を市場へ投入することで市場での優位を確立することを選択したものと判断できる．

McAfee 社，Symantec 社はともに変化していく技術トレンドの変化に対応するため，新しい技術の開発を行っていく必要があった．この中で，McAfee 社は Intel 社のもつ技術領域へのポートフォリオを拡張することによって差別化を図るために買収されることを選択し差別化を図ったと推測される．Symantec 社においては，自社の事業ポートフォリオ強化のため，Mergers and Acquisitions（M&A）を積極的に実施している企業である．しかし，自社のコアコンピタンスであるセキュリティ領域に重点を置いた M&A を行っており，レイヤー間の補完財を M&A によって取り込むことで事業ポートフォリオを拡張し差別化を図ったと推測される．

6.4 なぜ買収による事業ポートフォリオの拡張なのか

通常の合併では，資本を軸とし企業間における競争力の強化のためにコスト低減や新市場への拡大のために買収などが行われる．

McAfee 社と Intel 社は 2010 年の買収前から提携関係があった．しかし，本格的な技術課題の解決のためには，両社のエンジニアによる，より密接な関係性が必要であったことが考えられる．業務提携では，独立した企業同士での関係であるため技術的なコアコンピタンスを開示しての技術開発は難しいと考える．また，合弁会社を設立しての技術開発は，外部環境の変化の激しい IT 市場ではどのような技術が次のトレンドになるのかを予測し続けることは難しく，また対象の技術をシナジー効果として他の事業へ波及させることが難しい．

このため，企業の買収によりお互いの技術領域での密接な結びつきによる新技術の開発が必要である．McAfee DeepSAFE のように複数のレイヤーにまたがり，ハードウェアとソフトウェアの領域を横断するような技術は特に強い関係性が必要である．

上記から，McAfee 社は買収によって自社の持つコアコンピタンスを最大限に活用し，かつ市場への競争優位を創出するためには，Intel 社に買収されることによって垂直統合型の製品を開発することが最もよい方法であると選択したものと考える．

7. 仮説導出

7.1 RQ:競争優位創出要因に関する仮説の導出

RQ は，情報セキュリティビジネスにおける競争優位創出要因である．本論文では，McAfee 社が Intel 社に買収されることによって，事業ポートフォリオを柔軟に組み替えていくことによって，技術トレンドに対応した新しいセキュリティ技術を開発し，製品化することによって競争優位が創出されることを導出した．このことから，情報セキュリティビジネスにおいては，技術トレンドに合わせた事業ポートフォリオの拡張と組み替え能力が競争優位創出のための一要因であることが支持される．

情報セキュリティ市場は外部環境変化の激しい IT 市場の後追いで，市場へ製品やサービスを提供していかなければならないという特性をもっている．このため，新しく発生するセキュリティ脅威に対して，どのようなセキュリティレイヤーでも対応していく技術や製品を開発していくというように事業ポートフォリオを構築していくことは非常に重要な戦略であるといえる．

7.2 RQ-1:どのような技術が必要になるかの仮説の導出

RQ-1 は，レイヤーごとに必要な技術をどのように選択するのかである．技術トレンドの変化として，近年 IoT が市場に登場し，新たなセキュリティ脅威となるインシデントが発生した．IoT が普及することで，今までの技術のように OS 上で動作するアプリケーションにてセキュリティを担保する方法だけでは，新たに発生する低レイヤーでのセキュリティ脅威に対してセキュリティを担保しきれないという技術課題が発生した．このため，レイヤーごとにセキュリティを対応していくのではなく，レイヤーを横断した垂直統合型のセキュリティが必要となることが支持される．

McAfee 社と Symantec 社のもつソフトウェア技術だけでは，IoT 技術の進展に伴う低レイヤーでのセキュリティ脅威に対応するための技術課題を解決するためには技術的な限界があった．このため，既存のセキュリティビジネスが行ってきたレイヤーごとにセキュリティを担保していく方法では，変化する IT 技術トレンドに対して十分セキュリティを担保していくことが難しいといえるため，情報セキュリティビジネスにおいて垂直統合型のセキュリティ製品やサービスを提供していくことは重要であるといえる．

7.3 RQ-2:ネットワーク効果の影響に関する仮説の導出

RQ-2 は，情報セキュリティビジネスではネットワーク効果はどう影響するのかである．情報セキュリティ技術は，IT 技術の進展に伴い，新たなセキュリティ脅威が発生した後に必要となる．このため，新しい IT 技術が普及することによって，単一のレイヤーにおける製品だけでは対応できないことも発生する．こうした場合，他の階層にまたがった技術や製品が必要となり，多数のレイヤーに影響を与えることとなる．このとき，間接的に必要となるセキュリティ技術や製品が増大していくため，ネットワーク外部性の間接的効果が強く働くことが支持される．

本研究事例においては，IoT 技術の進展に伴い，より低レイヤーのセキュリティ脅威に対して，既存の技術では対応することが難しくなった．McAfee 社と Intel 社は，このセキュリティ脅威に対応するセキュリティ技術を開発し，製品化することによって，Intel 社の持つ CPU に対しセキュリティを補完財として対応させたのだといえる．また，Intel 社は IoT の普及を推進するためのアライアンスにも力を入れており，より強いネットワーク外部性の効果を高めようとしている．

7.4 RQ-3：技術トレンドの対応に関する仮説の導出

RQ-3 は，急速に変化する技術トレンドへの対応である．McAfee 社は技術トレンドの変化に対し，Intel 社に買収されることによって，Intel 社のもつハードウェア領域の技術を利用し，より低レイヤーからのセキュリティ技術を開発した．このことから，急速に変化する技術トレンドの変化に対応するためには，自社のもつ経営資源だけではなく，他社のもつ経営資源を利用することで対応していくことが支持される．

外部環境の変化の激しい IT 市場において，業務提携による技術協業では技術トレンドの変化に対応していくことは難しい．これは，高度なセキュリティ脅威に対応するための技術力の開示は，その企業のコアコンピタンスの開示と同義であり，技術協業においても真にコアとなる技術情報の開示は難しいためである．そのため，技術協業などによる開示情報だけでは，高度化するセキュリティ脅威に対応する製品やサービスを提供していくことが難しい．McAfee 社は Intel 社に買収されることにより，両社のもつ高い技術力をより深いレベルで統合し製品化することで，市場に対して技術優位な製品を提供できた．これにより，McAfee 社は Symantec 社に対して競争優位を創出したといえる．

7.5 考察

情報セキュリティ産業においては，市場成長率は高い水準であるといえる．なぜなら，IT 技術の誕生に伴い，新技術に対応するためのセキュリティ市場が開拓され，技術の進展とともに市場は拡大していくためである．IT 技術の進展は Incrementalist（漸進主義）によって開発されることが多いが，情報セキュリティ技術は Rationalist（合理主義）による開発が重要である．IT 技術は市場に向けて新しい技術を提供していくため，目的や内容を徐々に向上させながら進めていくことに対して，セキュリティは一貫した目的をもって開発しなければ守るべきセキュリティ脅威に対して適切なアプローチをすることができなくなる可能性が高いからである．また，IT 技術は普及理論におけるキャズムも多く発生する．これは，新しい IT 製品などが発生した場合においても，アーリーアダプターとアーリーマジョリティーの間には求める要件が異なるためである．アーリーアダプターは新技術をいち早く取り入れることで，自身の問題解決を要求するが，アーリーマジョリティーでは新技術の利用による利益が明確にならないうちは取り入れることはないためである．本事例において，McAfee 社と Intel 社は IoT 技術の普及をいち早く捉え，必要となるセキュリティ技術を見極めることで新しい技術を開発した．また，技術的な普及を加速させるためのアライアンスにも力を入れることで，このキャズムを乗り越えようとしていることが言える．

次に，競争地位戦略においては，McAfee 社も Symantec 社もリーダーの地位にある企業といえる．リーダー企業のとる戦略としては，市場シェアの拡大であるが，ソフトウェア産業においては量的経営資源の多寡はあまり問題とはならない．ソフトウェア製品の製造においては，量的資源は少なくて済むためである．また，流通の面においても，少ない資源で経営していくことは可能である．技術力を含む質的経営資源が他社との競争優位を創出する源泉になることも多い．このため，McAfee 社と Intel 社による新技術の開発は質的経営資源において Symantec 社よりも競争優位である．

IT 技術を利用するソフトウェア産業においては外部環境の変化が激しいことは先に述べた通りである．この中で，ソフトウェア企業はその状況変化に対応するために経営資源の再構築や変革が必要となる．情報セキュリティ産業においてもこの特性は同様であり，情報セキュリティビジネスを行う企業は，IT 産業の変化に対して常に状況変化に対応するための経営資源の再構築や変革を行っている．これは，ダイナミック・ケイパビリティの表れであるといえる．ダイナミック・ケイパビリティにおける，環境変化への適応能力が十分に発揮できる企業が競争優位を創出していける企業である．McAfee 社は，この能力が高いため技術トレンドの変化を敏感に捉え，それに対応できたのだといえる．

また，McAfee 社は Intel 社に買収されるという方法を選択したが，McAfee という独立した事業部を設けており，自社が持つコアコンピタンスを単純に競争力がある部門としての位置づけだけではなく，他の事業部にもシナジー効果を波及させていることから，組織間競争における競争優位の源泉としていることも優れた手法である．

しかし，買収当時の CEO である David Dewalt 氏は買収と同時に McAfee 社を退任し，別の情報セキュリティ企業の CEO に就任している．また，買収当時の McAfee 社の役員（ここでは，企業経営に関わる経営陣とする）においても現在の Intel Security（旧 McAfee 社）に役員として残っていない．M&A におけるシナジー効果については，組織や人材を有効に活用することが必要だが，McAfee 社の経営スタイルや社風，人的資源における活用はできていないのではないかと推察される．

8. 今後の課題

情報セキュリティビジネスは急速な市場の変化に対応していくため，柔軟に事業ポートフォリオを変化させていくことが重要であるとの結論が得られた．これは，階層間におけるプラットフォームの強固な結びつきが重要であることを示唆している．しかし，この事象を決定づけるには定量化した情報や, さらなる事例の分析が必要である. また，ソフトウェアとハードウェアのように異業種のレイヤーでの事業ポートフォリオの拡張が競争優位の要因になるのかを分析していくためにも，例えば Oracle 社と Sun Microsystems 社の買収事例なども調査していくことが必要である.

謝辞

本稿の執筆にあたり，立教大学ビジネスデザイン研究科の枡谷義雄教授に貴重なご助言をいただいたことに心より感謝いたします．並びに多くの方々にご指導ご鞭撻を頂きましたことを，この場を借りて深く御礼申し上げます.

参考文献

[1] Ulrich, Karl. (1995) "The role of product architecture in the manufacturing firm." *Research policy* 24, no. 3 : 419-440.

[2] Baldwin, Carliss Young, and Kim B. Clark. (2000) *Design rules: The power of modularity*. Vol. 1. MIT press. (安藤 晴彦翻訳. (2004).『デザイン・ルール―モジュール化パワー』東洋経済新報社.)

[3] 佐伯靖雄. (2008)『イノベーション研究における製品アーキテクチャ論の系譜と課題.』 *立命館経営学* 47, no. 1.

[4] Yoo, Y., O. Henfridsson, & K. Lyytinen.(2010) “The New Organizing Logic of Digital Innovation: An Agenda for Information Systems Research” Information Systems Research, vol.21, no. 4,pp.724-735.

[5] Gawer, Annabelle, and Michael A. Cusumano. (2002) *Platform leadership: How Intel, Microsoft, and Cisco drive industry innovation*. Boston: Harvard Business School Press.

[6] Messerschmitt, David G., and Clemens Szyperski. (2005) "Software ecosystem: understanding an indispensable technology and industry." *MIT Press Books*1.

[7] 加藤和彦 (2016)『IoT 時代のプラットフォーム競争戦略 ネットワーク効果のレバレッジ』中央経済社

[8] Eisenmann, Thomas, Geoffrey Parker, and Marshall W. Van Alstyne. (2006) "Strategies for two-sided markets. "*Harvard business review* 84, no. 10 : 92.

[9] 根来龍之, and 佐々木盛朗. (2011) 『プラットフォーム・ソフトウェア市場への新規参入の成功要因-「スタックの破壊」 と既存事業者と異なる 「レイヤー優先度」』.

[10] Katz, Michael L., and Carl Shapiro. (1985) "Network externalities, competition, and compatibility." *The American economic review* : 424-440.

[11] Katz, Michael L., and Carl Shapiro. (1986) "Technology adoption in the presence of network externalities." *The journal of political economy* : 822-841.

[12] Farrell, Joseph, and Garth Saloner. "Standardization, compatibility, and innovation. (1985) "*The RAND Journal of Economics* : 70-83.

[13] マイケルA, クスマノ 著 サイコム・インターナショナル 監訳. (2004) 『ソフトウェア企業の競争戦略』 ダイヤモンド社.

[14] Eisenmann, Thomas, Geoffrey Parker, and Marshall W. Van Alstyne. (2006) "Strategies for two-sided markets. "*Harvard business review* 84, no. 10 : 92.