経済産業省 御中

セキュリティ製品の有効性及び脆弱性検証に関する調査報告書

2019 年 3 月 15 日

株式会社三菱総合研究所
社会 ICT イノベーション本部

目 次

図 目 次

表 目 次

1. 背景・目的

1.1 背景

近年、政府・企業や個人の情報を狙ったサイバー攻撃にとどまらず、プラントやインフラそのものの停止を狙い、制御システムまで含めた社会システム全体を標的とするサイバー攻撃の脅威が高まっている。その中で、産業サイバーセキュリティの強化は、我が国の社会システムをサイバー攻撃から守ることに加え、諸外国においてもサプライチェーンも含めたセキュアな環境作りへの取組が始まっていることから我が国がグローバルに競争力を保つために喫緊に取り組まなければならない重要な政策課題である。

サイバーセキュリティの世界においては、新たな攻撃手法が日々生み出されている一方で、それに対抗するセキュリティ製品も活発に開発・販売が行われている。しかしながら、新たなセキュリティ製品はその有効性や導入実績等が明らかでないと採用されない傾向がある。他方で、我が国の新しいセキュリティ製品で技術の有効性を示す制度が世界的に見てもまだ無い場合、我が国が制度を制定し、有効性を公表することで当該製品がシェアを獲得でき、また制度自体も国際標準を狙うことが可能となる。加えて、経済産業省産業サイバーセキュリティ研究会 WG3（セキュリティビジネス化）の議論の中でも、ユーザー企業等がセキュリティ製品を導入する際には、製品の性能などの機能もさることながら、実際の環境においてどの程度使われているかといった実績をかなり考慮するということが、これまで多数の事業者からの声を聞いている。一方で、開発されてこれからマーケットインを目指す製品については、試行的であってもユーザー企業等に導入してもらえず、そもそも実績を積むことができないといった声もあった。この現状を打破するため、市場へのマーケットインを目指す新たに開発されたセキュリティ製品について、実環境における使用の実績を確保するために必要な事項を整理する必要があると考えている。

また、IoT 製品の普及に伴い、2016 年に起きたマルウェア「Mirai」による DDoS 攻撃など、セキュリティ対策が十分でない IoT 製品がサイバー攻撃の脅威にさらされるなど、我が国として対策を早急に取る必要がある。ただし、「Mirai」の様な外部からの攻撃だけではなく、IoT 製品のチップやファームウェア等に製造段階で予めバックドア等の不正なプログラムが仕込まれている可能性も存在する。その様な IoT 製品が自動車や情報通信インフラの構成に組み込まれていた場合、通常の性能検査等では脆弱性やバックドア等の検知が難しく、別のアプローチが必要になると考えている

1.2 目的

本調査は、国内外のセキュリティ製品及び IoT 製品の市場を取り巻く環境や取り扱われる商品等の情報を整理し、セキュリティ製品においてはその有効性を検証するための手法について調査を行い、IoT 製品においては抱えうる脆弱性等の情報とその脅威を検知する手法について調査することで、産業サイバーセキュリティの強化に向けた我が国のサイバーセキュリティ政策立案に資することを目的とする。

2. セキュリティ製品市場を取り巻く環境や国内の製品開発動向について

2.1 調査概要

今後の市場の成長が見込まれるセキュリティ製品を特定し、その国内外の市場動向等について分析を行った。加えて、国内の企業が提供するセキュリティ製品の特徴等についても調査と分析を行うことにより、我が国がこれからシェア獲得を狙えるセキュリティ製品の分野を明らかにした。また、国内の企業が提供するセキュリティ製品に対し、有効性の検証を行うために必要な事項の整理も行った。

2.2 セキュリティ製品の市場動向

我が国がこれからシェア獲得を狙えるセキュリティ製品の分野の検討にあたっては、一定度の市場規模が存在する分野でないとベンダーにとって市場参入のメリットがないこと、また、今後成長の見込みがない成熟市場に対して技術を強みとした新規の参入は困難なため、一定度の規模があり、今後成長が見込まれる市場を調査した。

2017年のセキュリティ製品の国内市場[1]を見てみると、市場成長率が高い製品分野のうち、標的型攻撃対策ツール（ゲートウェイ型）やWebフィルタリングツール、Webセキュリティアプライアンス、モバイルセキュリティ管理ツールの市場規模が大きくなっている。一方で市場成長率をみると、データベースセキュリティ、産業用/組込型セキュリティ製品、EDR、認証デバイスで高くなっており、これらの製品分野が有望と考えられる。

また、各製品分野における日本国内のベンダーシェアを見ると、管理系（ログ管理、脆弱性検証関連、ポリシー関連、暗号化、ホワイトリスト、フォレンジック等）やアイデンティティ系（個人認証デバイス、生体認証デバイス、ID管理、ログオン管理、PKI管理等）の製品で国内ベンダーのシェアが高いが、セキュリティ技術が強みとなるネットワーク系（ファイアウォール、VPN、IDS/IPS、WAF、ペネトレーション、ネットワーク可視化、データダイオード等）・コンテンツ系（ウイルス対策、スパム対策、URLフィルタリング、ウェブサニタイジング、EDR等）の国内ベンダーのシェアは低い。ただし、ネットワーク系ではWAF、コンテンツ系ではWebフィルタリングツールのみ国内ベンダーのシェアが高くなっている。

一方で、海外市場に目を転じると、Grand view researchの調査によれば、世界におけるセキュリティ製品・サービス市場では、エンタープライズセキュリティやネットワークセキュリティ分野において成長が見込まれている。

[1] 2018ネットワークセキュリティビジネス総覧（富士キメラ総研）

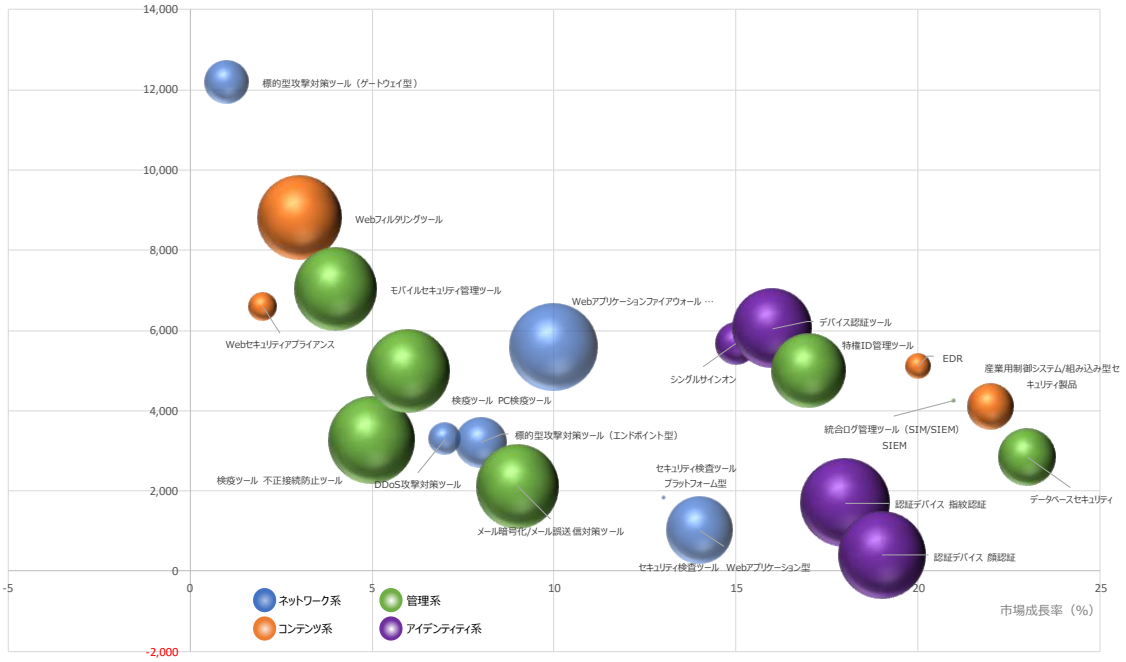

図 2-1　国内のセキュリティ製品市場（高成長率分野の規模、成長率、国内ベンダー比率）[2]

出典）2018 ネットワークセキュリティビジネス総覧（富士キメラ総研）を基に三菱総研作成

有識者からは、クラウド・AI・自動運転・IoT・OT 等発展途上である分野におけるセキュリティ製品で国内ベンダーがシェア獲得を狙えるのではないかとの意見を頂いた。また、検証や標的型攻撃対策の製品も注目されている。セキュリティ技術としては、ムービングターゲットディフェンスや detection and response といった考え方がトレンドになってきているとの見解が示された。

一方で、海外（特に米国）では、①サイバーセキュリティに特化した機関があり、国としてセキュリティの経験値が違うこと、②アクセラレータがスタートアップの支援を行っていること、③防衛産業でセキュリティ製品が使われその後一般に製品が広がっていく仕組みが出来ていること等から、そうした環境で技術を磨く国外ベンダーに対し、日本国内のベンダーがシェアを拡大することは難しいという意見もあった。

また、日本では商社が日本製品を担ぐインセンティブがないため、ベンチャー企業が入れないマーケットになっているとの意見も挙がった。

有識者への詳細なヒアリング内容は以下の通り。

[2] 円の大きさは国内ベンダーのシェアを表す

・PC 等、従来から存在する IT 機器に対するペリメーター（境界線を守る考え方）はスタートアップ企業が参入することは難しい。一方で、**発展途上の分野であるモバイル・OT・クラウドに対するペリメーター分野は参入余地**あり。 ・ペリメーター（境界防護）から detection and response という考え方も出てきている。 ・デセプション（偽サーバ・情報を作り、どれが本物かわからないようにする方法）も出てきている。
・最近では、EDR・SIEM を拡大した **UTM、生体認証の問い合わせは増えている**。ただし、3 年経つとトレンドは変化する。
・注目される分野はあるが、日本にプレイヤーがいない。 ・**トレンドはオーケストレーション**。自動的に情報を集めて AI で分析、優先順位付けを行い、場合によって自動的に制御する。 ・NGEPP と EDR は、最近は統合されマーケットは 1 つ。標的型攻撃対策はホットだが、トレンドが少しずつ変わっている。
・WEB フィルタリング製品の日本ベンダーのシェアが大きい理由は日本語の壁があるから。**日本語の優位性がある製品は海外に進出しにくい**。 ・海外を狙うなら海外でのディストリビューターも味方につけないといけない。
・**最近はクラウドサービス系が盛り上がっている**。ゲートウェイ系はクラウド利用されている。 ・OT 系システムへのセキュリティ製品の導入はかなり難しい。ゲートウェイ系は工場内部にはあまり影響がないので利用され始めている。システム内部に入れるのは相当難しい。
・**最近のトレンドは「サイバーキルチェーン」から「ムービングターゲットディフェンス」に変化。** ・**国外ではサイバーセキュリティに特化した機関があり、攻撃者の攻撃手法の次なる一手を考える人がいる。日本国内のベンダーとは経験値が違う。** ・セキュリティ技術の進歩は早く、日本発のセキュリティ製品は難しい。 ・**AI や自動運転など等日本の強い技術を推すべきでは。**
・現在セキュリティ市場がなく、**世の中に必要とされているものとしては IoT 系**がある。そこら中にあるセンサーにはセキュリティ製品は入っていない。IoT 向けの新しい何かはあるのではないか。 ・**自動運転や車間通信も新しい分野**。 ・**コントローラー分野は日本がシェアを持っているので、何かにつながるかもしれない。** ・大きなプロダクトの中に組み込まれているセキュリティ製品は調査の中で表に出てこないが重要なものである。例えば工場・プラントのセキュリティ製品等。コネイン等、政策的にも重要な領域である。 ・日本が強い分野を一歩先に行かせるための方法にセキュリティが入るとよいのではないか。
・**海外にはサイバーセキュリティのアクセラレータがスタートアップの支援を行っている。また、海外は防衛産業が大きく、防衛産業でセキュリティ製品が使われ、一般に広がっていく。** ・日本では商社が日本製品を担ぐインセンティブがないため、ベンチャー企業が入れない

マーケットになっている。国外から輸入し日本国内で高く売ることが一番儲かり、中抜きされず、かつ普通の企業は海外で直接調達できないため参入されないマーケットとなっている。海外では商社がいないので直接企業間でやり取りするようになっている。 ・スタートアップが狙うのは薄利多売の製品、クラウド、または業界特化型製品ではないか。 ・製品は、クラウドの仮想アプライアンスで売れるようになっている。Google や Amazon 等の上位で売るところを狙うとよいのではないか。これら 2 つのマーケットプレイスは、レガシーセキュリティベンダがやっておらず参入の予定はあるのではないか。 ・最近は、大手ベンダーが「セキュリティコネクテッド」を提唱し始めている。今まではセキュリティ製品ごとにコンソールが必要だったが、統合するような形になってきている。 ・セキュリティの分野はパラリーガルの世界。グローバルで展開しようとすると、各国の規制に従う必要がある。ベンチャーには各国の規制に従って製品を作ることは難しい。
・日本企業のベンチャー製品が思い浮かばない。検証サービスのベンチャー系は多い。診断のノウハウを集めたら製品になるかもしれない。 ・AWS 上の WAF 製品のユーザーは小さい企業が多く、セキュリティ予算がないため、ヒットしなかった。
・クレカ決済・指紋認証がこれからのトレンドになるのではないか。IoT が世の中に浸透し、多くの機器に指紋認証が導入される。その管理をどうするかが問題になってくると考えられる。 ・車に注目している。車の分野は最先端の技術が使われているため、車関係の技術に携わっていれば次に何が来ても対応できる。自動車分野を大きなサプライチェーンで考えると市場効果はある。 ・海外はまずは富裕層をターゲットにするため、開発にお金をたくさん投資することができる。日本は汎用性をまずターゲットにする。そのため、海外の方が良い技術が生まれる。 ・セキュリティは必要な人たちが自主的に導入していくのがベスト。日本で市場が伸びない理由は大手がセキュリティに対する不安をあおっているから。

2.3 新規製品提供国内企業

新規製品の市場形成の可能性や課題について分析するために、国内のベンチャー企業から直近 2 年以内に新たに提供が開始されたセキュリティ製品について調査した。

調査対象の製品としては以下の 2 つを取り上げた。

- 標的型攻撃向け出口対策製品
- 脆弱性診断

上記 2 製品を開発するベンチャー企業にヒアリングした結果、新規製品の市場形成の方法としては以下が考えられる。

① PaaS 等のプラットフォームに乗せ、提供する

セキュリティ製品だけではバリューチェーンを生むことができないため、PaaS 等のプ

ラットフォームに乗せ他の製品・サービスと一緒に提供する。

② システムインテグレーターや代理店等により採用される
ベンチャーの開発企業がユーザーに対し直接営業・販売することは難しいため、いかにシステムインテグレーターや代理店等を通じて販売してもらうかが市場形成には重要である。

上記の市場形成に係る方法論の課題としては以下が考えられる。

① ベンチャー企業は大手プラットフォームベンダーとの交渉パスを持っていない
そもそも日本では AWS のような大きな PaaS が存在しないということも課題。

② 代理店の利益（中間マージン）が大きい製品を取り扱いたいという意向がある
代理店の利益（中間マージン）を確保しようとするとユーザーへの販売価格が高くなり、価格優位性を保つことができず、総合的な評価から既存ベンダーの製品が選定される。

上記課題へ対応するために考えられる制度としては以下が想定される。

① プラットフォームベンダーへの紹介制度、またはプラットフォームベンダーへの提案支援
既存の主力ベンダーに対し、日本国内のベンチャー企業を紹介する制度。あるいは営業力向上のために、提案書等サービス企画の支援をする。

② 認証制度
システムインテグレーターや代理店等が新規製品を採用し、顧客に売り込みやすくするために、製品の性能や信頼性に係る認証制度を創設する。

2.4 製品分野ごとの有効性検証手法

セキュリティ製品分野について、分野ごとにその特徴等を調査し、セキュリティ製品の有効性を検証するための手法について調査を行った。併せて、当該検証を実施するために必要なシステム環境及び検証実施者に求められる知識や能力についても検討を行った。

本調査では、日本ネットワークセキュリティ協会（JNSA）の情報セキュリティ市場分類区分及び国内のセキュリティ製品市場動向を参考に、以下の製品分野を選定した。

表 2-1　調査対象セキュリティ製品分野

大分類	製品分野
統合型アプライアンス	統合型アプライアンス（UTM）
ネットワーク脅威対策製品	IDS／IPS アプライアンス／ソフトウェア（IDS/IPS）
	Web アプリケーションファイアウォール（WAF）
コンテンツセキュリティ対策製品	ウイルス・不正プログラム対策ソフトウェア／アプライアンス（AV）
	メールフィルタリングソフトウェア／アプライアンス（SM-F）

これらの製品分野に対して、セキュリティ製品の有効性を検証するための手法、検証を実施するために必要なシステム環境及び検証実施者に求められる知識や能力について調査を実施した（表 2-2）。

セキュリティ製品については、販売後もファームウェアやパターンファイルのアップデート、脆弱性対応パッチの適用等によって、製品の機能や性能が変わる可能性がある。これらのアップデートや適用が行われたタイミング又は当該セキュリティ製品に係る脆弱性が報告された都度、有効性検証を行うことが望ましい。

表 2-2　セキュリティ製品分野ごとの検証手法

大分類	統合型アプライアンス	ネットワーク脅威対策製品		コンテンツセキュリティ対策製品	
製品分野	**UTM**	**IDS/IPS**	**WAF**	**AV**	**M-F**
製品機能概要	ネットワーク上の通信を解析し、送信元・送信先のアドレスやポート番号、プロトコルの種類、通信のステータス等を元に、予め設定されたルール・ポリシーに従って通信の許可、遮断等の制御を行う。	ネットワーク上の通信の内容や状態を解析し、侵入または攻撃と判断される通信に対して監視、警告、遮断（IPS のみ）、ログ記録等の対策を行う。	Web アプリケーションへの通信を監視・解析し、侵入または攻撃と判断される通信に監視、警告、遮断、ログ記録等の対策を行う。	ウイルスやワームなどのマルウェア（不正プログラム）の侵入や感染を検知、防御、排除する。	無差別・大量に送りつけられる有害な内容を含む電子メールや標的型メールを監視し、分別、警告、排除等を行う。
有効性検証項目	1. ポリシー・侵入検知能力 2. スループット・最大処理能力 3. レポート機能 4. 既存環境への適応性	1. ポリシー・侵入検知／侵入防止能力 2. スループット・最大処理能力 3. レポート機能 4. 既存環境への適応性	1. ポリシー・侵入検知能力 2. スループット・最大処理能力 3. レポート機能 4. 既存環境への適応性	1. 検出・隔離能力 2. レポート機能 3. 既存環境への適応性	1. 検出・隔離能力 2. レポート機能 3. 既存環境への適応性

大分類	統合型アプライアンス	ネットワーク脅威対策製品		コンテンツセキュリティ対策製品	
製品分野	**UTM**	**IDS/IPS**	**WAF**	**AV**	**M-F**
有効性検証手法	1. 複数ネットワークからの侵入テスト等 2. 大量データ送信、巨大パケット送信等 3. 適切なタイミングでのアラート報告確認、適切なレポート内容等 4. 導入の所要時間、他機器の影響等	1. 複数ネットワークからのポリシーテスト、エクスプロイトテスト、侵入テスト等 2. 大量データ送信、巨大パケット送信等 3. 適切なタイミングでのアラート報告確認、適切なレポート内容等 4. 導入の所要時間、他機器の影響等	1. 複数ネットワークからのポリシーテスト、エクスプロイトテスト、侵入テスト等 2. 大量データ送信、巨大パケット送信等 3. 適切なタイミングでのアラート報告確認、適切なレポート内容等 4. 導入の所要時間、他機器の影響等	1. 既知マルウェア検出テスト、ヒューリスティックスキャンテスト、ソフトウェアベンチマークテスト等 2. 適切なタイミングでのアラート報告確認、適切なレポート内容等 3. 導入の所要時間、他ソフトウェアの影響等	1. 迷惑メールテスト、標的型メールテスト、ベンチマークテスト等 2. 適切なタイミングでのアラート報告確認、適切なレポート内容等 3. 導入の所要時間、他ソフトウェアの影響等
必要な知識や能力	ネットワークに関する知識。脆弱性スキャン、侵入テスト等の知識及び能力。			マルウェアに関する知識及びベンチマークテスト等の知識及び能力。	スパムメール・標的型メールに関する知識、ベンチマークテストに関する知識及び能力。
必要なシステム環境	対象製品にネットワークアクセスできる環境及び脆弱性スキャンや侵入テストのためのツール。			マルウェア検体及びマルウェア判定環境（サンドボックス等）。	メール検体及び判定環境。

2.5 諸外国の有効性検証手法

国内外の民間企業又は政府によるセキュリティ製品の有効性を検証する取組としては以下のようなものが挙げられる。

(1) 民間会社による企業向けセキュリティ製品のテスト及び企業評価

- AV-TEST 社、AV-Comparatives 社、NSS Lab 社などによる検知テスト
- Gartner 社による分野のリーダー選出 Choice
- Gartner Peer Insights Customer Award

(2) 調査会社による市場調査

- IDC Japan、富士キメラ総研、ミック経済研究所などによる市場シェア・売上調査
  例：富士キメラ総研「ネットワークセキュリティビジネス調査総覧」
  アイ・ティ・アール社「ITR Market View:サイバーセキュリティ対策市場」

(3) 顧客満足度調査

- 富士キメラ総研、日経コンピュータ、日経 BP ガバメントテクノロジーによる顧客満足度調査
  例：イード・アワード　顧客満足度調査

国外では、第三者機関によるテストが多く、その結果による性能の質を評価するものが多い。一方で、国内では、市場シェアや顧客度満足度、知名度で評価する取組が多く、品質の評価基準がない。

ここで、以下の 3 つの国外有効性評価を対象として、用いられている有効性の検証基準や検証手法等について更に調査を行った。

- AV-TEST 社よる検知テスト
- AV-Comparatives 社よる検知テスト
- NSS Lab 社よる検知テスト

(1) AV-TEST 社（ドイツ）よる検知テスト

1) 評価方法
Windows 向け製品では、以下 3 つの項目を評価。各項目の最高得点は 6 点、合計で 18 点満点、10 点以上を合格とする。

- Protection（マルウェアやその他の攻撃に対する保護）
- Performance（試験システムのスピード（システムパフォーマンス）に与える影響）
- Usability（誤検知やインターネットの利用制限など、使いやすさへの悪影響）

2) マーク及び賞

基準値を満たした場合には以下の合格マークを付与。年間通じて評価が優秀な場合は賞を付与。

図 2-2　AV-TEST によるテストで合格した場合に付与されるマーク

3)　主な導入企業
トレンドマイクロ、マカフィー、カスペルスキー、シマンテックなど

4)　主な評価を受けたセキュリティ製品
ウイルスバスターコーポレートエディション　XG　（トレンドマイクロ）
McAfee Endpoint Threat Protection　（マカフィー）
Kaspersky Security for Virtualization　（カスペルスキー）
Endpoint Protection　（シマンテック）

(2)　AV-Comparatives 社（オーストラリア）よる検知テスト

1)　評価方法
マルウェア除去やファイル検出などのテストを実施。世界的に最大のサンプルコレクションの一つを使用し、現実的なテスト環境を通じてウイルス対策ソフトウェアの実際の保護機能を評価。結果は「Advanced＋、Advanced、 Standard、Tested」の 4 段階で評価している。

2)　マーク及び賞
基準値を満たした場合には以下の合格マーク付与。年間通じて評価が優秀な場合は賞を付与。

図 2-3　AV-Comparatives によるテストで合格した場合に付与されるマーク

3)　主な導入企業
AVG、ESET、カスペルスキーなど

4)　主な評価を受けたセキュリティ製品
AVG Internet Security 2016　（AVG）
ESET Internet Security（ESET）
Kaspersky Internet Security（カスペルスキー）

(3)　NSS Lab 社（米国）よる検知テスト

1) 評価方法
NSS Labs が独自の測定手法として SVM（Security Value Map）を開発している。横軸に TCO per protected agent（1 エージェントあたりの総コスト）、縦軸に Security Effectiveness（セキュリティの有効性）をとり、テスト対象の各ベンダー製品評価結果をマッピング。評価の高いものは「Recommended（推奨）」の評価が与えられる。評価手法は一定期間（3～6 ヶ月）で見直される。
2) 主な導入企業
トレンドマイクロ、マカフィー、フォーティネット・ジャパンなど
3) 主な評価を受けたセキュリティ製品
Deep Discovery™ Inspector （トレンドマイクロ）
McAfee Network Security Platform （マカフィー）
FortiGate シリーズ （フォーティネット・ジャパン）

2.6 製品表彰制度

国内におけるセキュリティ製品の表彰制度としては、Interop Tokyo Best of Show Award が挙げられる。Interop Tokyo Best of Show Award は 1994 年に開始した表彰制度で、年 1 回開催される。

国外におけるセキュリティ製品の表彰制度としては、Gartner Peer Insights Customer Choice Awards や Info Security Product Guide's Global Excellence Awards が挙げられる。Gartner Peer Insights Customer Choice Awards は Gartner Peer Insights において 300 件以上の顧客からのレビューがあり、かつ 7 社以上のベンダーが存在する製品分野を対象として、総合スコアと公開されたレビューの数を総合的に加味し、上位の 3 社に授与される。

2.7 セキュリティ製品の検証の進め方

セキュリティ製品の検証の進め方について、セキュリティ製品の評価に関する知見を有する事業者にヒアリングを実施し、以下の方向性を得た。

(1) 国によるお墨付きに対するニーズは一定度存在するも、検証制度に対しては課題あり
- ✓ 導入実績不足の課題意識は同じだが、対応として有効性検証は違うのではないか。
- ✓ テストベッドを作ると、初期投資はもちろん機器の更新に莫大な費用が必要。
- ✓ 検証であれば、CSSC、ICSCoE 等の既存の取り組みも活用可能。現場レベルを上げるべきである。
- ✓ 検証を行う人のスペシャリティ、プラットフォームの汎用性、有効性の多様な観点が課題。
- ✓ ①サポート状況、②一定度のプログラムの保証（PSI 認証等）、③導入環境への適用性を考慮しては。
- ✓ METI のお墨付きがあれば強力なマーケティングツールになる。
- ✓ 経済産業省が主導するアワードならよいのでは。コンテストなら一過性で学生

等も参加できる。

(2) 「有効性」の評価は難しく、評価指標は要検討

- ✓ 「有効性」はユーザーにとって様々である。
- ✓ 日本では安定的なものの方が選ばれる傾向にある。
- ✓ OT 系への攻撃事例が少なく、動作確認の域を出ない。
- ✓ 機能評価、ベンダーが強みの評価は可能。

(3) アーリー企業において検証ニーズがある可能性。ただし対象を見極め、育成も考慮すべき

- ✓ アーリーステージの企業は、製品を売っていく上で検証制度へのニーズはあろう。
- ✓ 実環境試行はアーリーの会社にはよいかもしれない。育成と一緒に検討した方がよい。

詳細なヒアリング内容は以下の通り。

・同じ目的のセキュリティ製品の機能的な評価は可能。各ベンダーの強みを比較するのは、スタートアップでは有効。 ・**日本製品には「〇〇に選ばれた」という表記は少ないため、お墨付きを与えるのはよいかもしれない。** ・差別化した技術・リソースを持っているかが投資先候補として重要視される。
・**サポート体制の充実、他製品との連携等も重要視される**。負荷テストなどは環境に依存する。性能以外にお墨付きをつけるのは難しいのではないか。 ・**企業の情報システム部の KPI は安定性・停止時間の短さ**となっていることが多く、安定的なものの方が選ばれる傾向。 ・**何か起きた際にこのレベルの対策をしていれば仕方ないと世間に判断される仕組み**があればよい。
・評価には専門的な知見が必要であり、難しいのではないか。 ・**アーリーステージの企業は、一発目を売っていく点で検証制度へのニーズはあろう**。ただし、そういう企業は日本にほとんどいない。ベンチャーがいても後ろのステージで安価なリプレース戦略。 ・**導入事例は重要**。企業が導入時に上申する際、実績が求められる。 ・お墨付きはリリースには書けるがインパクトは小さい。安易なお墨付きは製品がこなれていない印象も与えかねない。 ・**実環境試行はアーリーの会社にはよいかもしれないが、育成と一緒に検討した方がよい**。
・検証環境を用意してもプロダクトを作る日本のベンダーがいない。 ・**革新性で評価**するというのも一案では。 ・**コンテストは、一過性の評価**かつ学生等も参加できる。
・**「有効性」はユーザーが判断するもの。**国が保証すると攻撃時に国の責任となる。「有効性」という言葉は問題があるのではないか。

・有効性ではない評価手法を考えると、CC と同種のものが考えられるが費用が嵩む点が課題。 ・国が主導で評価するならアワードならよいのでは。その場限りの評価をする。経済産業省の名前があった方が良い。 ・導入実績不足の課題意識は同じだが、対応として有効性検証は違うのではないか。 ・Interop Tokyo の ShowNet のように、様々な企業が製品を持ち寄り、相互接続検証する。そして実績を宣伝するような、ボランタリでも各参加者にメリットがある場ができると有効。 ・テストベッドを作ると、初期投資はもちろん機器の更新に莫大な費用が必要。
・AI 系の製品に関する検証はありうる。 ・ユーザーの評価は、操作のしやすさ、性能、安定性等様々な観点がある。 ・中小企業に対して無料で導入してもらい実績を積み、大企業に対しては実績を訴求する形になるのではないか。 ・実証では、①サポート状況、②一定度のプログラムの保証、③導入環境への適用性を考慮してはどうか。 ・METI のお墨付きがあれば強力なマーケティングツールになる。
・有効性検証では、検証を行う人のスペシャリティ、プラットフォームの汎用性、有効性の多様な観点が課題。
・申請書類を整えることよりも、実利が大きな軽めの第三者評価試験にニーズがあるのでは。 ・マーク・表彰をもらうより、国の基準に基づいて作った自己宣言がよい。
・検証であれば、CSSC、ICSCoE 等の既存の取り組みも活用可能。 ・検証レベルではなく、エンタープライズ（現場）のレベルを上げる取り組みの方が良いのではないか。
・導入基準としてサポート体制に対するニーズはある。 ・製品の良い点を定性的に示すだけでもよいのでは。

3. セキュリティ製品等の実環境における試行的評価の促進について

3.1 調査概要

市場へのマーケットインを目指す新たに開発されたセキュリティ製品について、実環境における使用の実績を確保するために必要な事項を整理した。具体的には、実際のセキュリティ製品について、採用実績を公表している事例の実態についてヒアリングを行うとともに、採用実績を公表しているユーザー企業等に対しても、実績を公表するにあたって懸念された事項等を調査した。また、このヒアリング調査の結果を基に、新たに開発されてまだ実績がないセキュリティ製品を仮定し、実環境に導入し実績を積むために必要な事項について整理し、実績構築を促進するための仕組み作りについて検討を行った。

3.2 公表事例の実態調査

実際のセキュリティ製品について、採用実績を公表している事例の実態についてセキュリティベンダー3 社にヒアリングを行った。また、採用実績を公表しているユーザー企業等 12 組織に対しても、実績を公表するにあたって懸念された事項等を調査した。調査により、主に以下の意見が得られた。

- 事例公表によるユーザー企業等のメリットは、セキュリティ対策への積極的姿勢アピール、価格等のメリット及び宣伝効果である。
- 事例公表によるセキュリティリスクはあるが、リスクは限定的と判断する組織も多い。
- 製品導入にあたって、事例を参考とする場合が多く、情報共有へのニーズあり。
- 海外企業の方が導入事例公表に前向きだが、海外でも公表を推進する政策や制度はない
- 海外でも導入事例、ユーザーの評価及び第三者評価が活用されている

採用実績を公表しているユーザー企業等に事例公表のメリットを伺ったところ、セキュリティ対策への積極的姿勢アピール、価格等のメリット及び宣伝効果が挙げられた。事例を公表することで、セキュリティベンダーから価格やサポートの面で有利な条件を引き出せる可能性があり、また公表によって、ユーザー企業自身の知名度を向上できるというメリットがあるとの意見を得られた。

一方で、事例公表によるセキュリティリスクを懸念する声も多い。導入している製品を公表することがセキュリティホールとなる意識が高いが、多層防御していることや、ベンダーと速やかに連携できる体制を整備していること、公表した事例が外部脅威に直接関係するものではないこと等、公表を行っている組織は、セキュリティリスクの検討を行っていることが伺えた。異なる公表によるデメリットとして、問い合わせが増え業務が増えることが指摘された。ヒアリングを行ったユーザー企業の一つでは、公表により問い合わせが増え、対応に要する時間が増加したため、問い合わせの多い案件は FAQ を作り、希望に応じて個別対応を実施していると述べた。また、多くの場合、ユーザー企業のウェブサイトではなく、セキュリティベンダーのウェブサイトに導入事例が掲載されるため、セキュリティ導入製品の内容が古くなる懸念が指摘された。

ユーザー企業がセキュリティ製品を導入するに当たって、他社の導入事例を参考にするという意見は多く、情報共有のニーズはあると考えられる。安心・安全が担保されているコミュニティ内の事例公開であれば、情報共有は可能であるという意見は多かった。また、ユーザー企業によっては、情報を入手するために自組織から情報を公開しなければならないと考えており、導入事例を積極的に公開しているという企業も存在した。

表 3-1 にユーザー企業等 12 組織のヒアリング結果を示す。

表 3-1　ユーザー企業等 12 組織のヒアリング結果

組織区分	公開している導入製品	ヒアリング結果
自治体関連組織	認証デバイス	・ セキュリティを晒すことになる考えはあまりなかった。公表はきちんと対策を実施しているというアピールになると考える。 ・ セキュリティベンダーからの依頼で公表した。 ・ 公表の可否は、どういう公表の仕方か、どこで公表するかによる。信頼できるベンダーならばよいが、契約関係がない第三者による公表は遠慮したい。 ・ 製品評価のポイントとしては、何かあればすぐのサポート対応してくれるベンダーなどの観点で絞り込んでいる。 ・ 今後の技術動向も踏まえ、他組織の取組は参考にしたい。
自治体関連組織	総合 ID 管理ツール	・ ベンダーから依頼があって公表したもの。特に価格など優遇条件はなかったと思われる。 ・ 組織として公表のメリットはない。現在であれば公表しない選択をするのではないか。当時と時代が変わっている。
自治体関連組織	Web フィルタリングツール	・ 情報を入手するためには、情報を公開しなければならないので、導入事例は積極的に出していこうというスタンスである。 ・ セキュリティベンダーと速やかに連携できる体制がある。万一脆弱性が出ても、速やかにパッチを当てられる体制にあったというのが、セキュリティでも公表に至った背景の 1 つにある。 ・ 公表による実利的なメリット（価格、サポート等）はない。 ・ 製品評価のポイントとして、運用も含めたユーザーとしての使いやすさを重視している。また、重要インフラが使っているなどの導入事例は大きなポイントになる。
自治体関連	ウイルス対策	・ ベンダーとしても自社製品を箔付けしたい他、他の

組織区分	公開している導入製品	ヒアリング結果
組織	ソフトウェア	営業に使いたいという意向があり、ベンダーから価格、サポート面で有利な条件を引き出したいという意向があり、公表に至る。 ・ セキュリティ製品の公表がセキュリティホールになることは間違いないが、多層防御しており、どこまで強固にやっているかを全て公表する訳ではない。 ・ 問い合わせを受けることもある。逆に、別の組織に導入の感想を伺うこともある。問題があるか、使い勝手はどうか等。導入の感想を聞けるのは有意義である。 ・ 情報共有としては、製品を導入するにあたってのセキュリティに関する教育がないため、ベンダーが主催するようなユーザー同士の集まり、セミナーなどは大事である。 ・ 製品評価のポイントとしては、機能、接続先の確認、相性・組み合わせ等が挙げられる。 ・ 運用の負担も重視する。運用の中でチューニングが必要。ウイルス対策でも、検知した後どういう行動が取れるか、どういうログが残るかなど、ハンドリングが負担になるところも多いので、自分たちが使える製品なのかどうかは重視する。
一般企業	WAF	・ 事例公表によりマイナスイメージがあるとは、少なくとも導入製品に関しては考えなかった。 ・ 現在のセキュリティベンダーとは初めてのお付き合いであり、友好的な関係を築こうと公表依頼に応じたもの。導入当時、WAF のいくつかのベンダーにあたったが、今より選択肢は限られていた。 ・ HP 上の事例公表情報、ベンダーの商品説明の際の口頭で聞ける範囲の事例については、導入時の参考としている。同業の意見交換などはない。 ・ 公表にあたって強い意志がある訳ではなかった。
一般企業	SIEM	・ 事例公表が値引き条件になっている場合はある。 ・ 自社の知名度を向上させる観点で、公表のメリットはあると考えた。 ・ WAF、Web サーバなど、ダイレクトに接続される製品の公表は社内で議論が必要。公表した事例は外部脅威に直接関係するものではない（エンドポイントやログ管理）ため、リスクは小さいと判断した。 ・ 公表のデメリットとしては内容が古くなること。自社サイトでないのでコントロールも効かず事例のメ

組織区分	公開している導入製品	ヒアリング結果
		ンテナンスができない。 ・ 売れている製品は良い製品であると考えているため、Gartner のような情報があるとよい。 ・ 事例は幅広く見ている。どこの機能を使っているか、どこの防御、対策を見ているのか等。あの企業が使っている等事例でわかると、安心感はある。 ・ 代理店、ディストビュータから、売れ線や他の導入企業について情報収集を実施している。 ・ 製品評価の統一的な観点は与信のみ。体力ない企業からの購入はリスクがある。 ・ 事例の共有は、参加者が国に登録している・一定の保証がある等、安心・安全が担保されているコミュニティ内の公開であればよい。 ・ 登録する際に 1 つ事例を差し出すと、複数の事例が出てくるような仕組みもよいのではないか。
一般企業	ファイアウォール・VPN ルータ	・ セキュリティベンダーから公表依頼された結果、事例公表を行った。
一般企業	統合 ID 管理ツール	・ 多岐に亘るユーザー部門と共にセキュリティ製品を選定する。ユーザー部門の意向が大きい。 ・ 公表のメリットはない。公表したくなかったが対応した。 ・ セキュリティベンダーとはシステムを共にカスタマイズや改善を協同してやっていたため、依頼を受けて対応したもの。単に製品購入するだけの相手であれば、公表の依頼は受けないだろう。 ・ 今回の公表により問い合わせが増えたので対応に時間を要し困った。同業他社で同じ系列にある銀行から。使い勝手の話、うまく行かない点なども共有することになるので、詳細については同業で信頼がある企業でないと話せない。
一般企業	非公表	・ 役員は事例公表することによるセキュリティリスクを懸念するが、価格交渉時点で条件が異なる。攻撃者が本気で調べたら使用製品はわかる。また、多層防御しており、一部の製品しか公開していないので、リスクは大きいと捉えていない。 ・ 長い目で見れば、公表事例を出すことで導入が増え、ベンダーのインカムが増え、サービスが良くなるのであれば、その方が望ましい。

組織区分	公開している導入製品	ヒアリング結果
		・ 他社の事例は見る。競合ベンダーに問い合わせ、導入事例を聞く。 ・ セキュリティ製品は、まず小規模で契約し試した結果、よい製品だった場合導入する。導入してみたら、実際は重たくて動かなかった製品もあった。
教育機関	クラウドサービス	・ インシデントが起きた場合も公開する。事例についても隠すものではないというスタンス。情報公開はむしろセキュリティに対して積極的にアピールするものだと考えている。 ・ 情報を出すと情報が倍になって返ってくる。情報公開によるリスク等デメリットよりも、情報が提供されることの効果の方が高いと考えている。 ・ セキュリティ製品だけではなく、IT 製品の情報は積極的に公開している。 ・ 情報公開したことで、ベンダーや他組織からの問い合わせは増えた。
教育機関	統合サイバーソリューション	・ 導入事例を公表しているものもあるが、公表することはあまりない。他のセキュリティ製品は公表していない。 ・ 他の教育機関が導入していない機器は、参考情報があまりないのでベンダーに詳しく話を伺う。 ・ ベンチャーの製品は導入していない。 ・ 他教育機関との情報共有の場があり、そこでの発表内容を参考にすることは多い。
教育機関	エンドポイントセキュリティ（EDR）	・ 事例を公表することで攻撃対象となる危惧もあったが、実際はそんなことはないと考えている。 ・ 導入過程でベンダーと事例公表の話になることはあるが、特に断る理由はない。 ・ 他の組織の導入事例は参考にはなるが、導入したばかりの製品の所感等が公表されている事例がある。セキュリティ製品は長期間運用しないとわからない部分がある。そういったことを考えると結局は実環境への適用について検討が必要な場合もある。 ・ 事例公表することによって金額が安くなったことはない。 ・ ベンチャーの製品は導入していない。ベンチャーの営業が突然来たとしてもリスクを考えてしまう。 ・ 国の認証等で信頼できても、実際の環境との調整が必要である。条件や導入場所等を十分に検討して導

組織区分	公開している導入製品	ヒアリング結果
		入することになる。

セキュリティベンダーへのヒアリングを通じて得られた結果は主に 2 点であり、海外企業の方が導入事例公表に前向きだが海外でも事例公表を推進する政策や制度は存在しない点、海外でも導入事例、ユーザーの評価及び第三者評価が活用されている点が得られた。

ヒアリング実施前の検討仮説として、導入実績公表について日本企業より海外企業の方が積極的であり、海外では導入実績公表を促進する政策や制度が存在する可能性が思慮されたが、海外でも事業展開を行っているセキュリティベンダーによれば、公表を促進する制度や取り組みについては、海外でも存在しないと考えられる。導入実績公表について海外企業の方が多い要因として、国民性の影響が大きな要因として考えられており、日本企業では導入製品を公表することで、攻撃対象となるという懸念が存在するが、海外企業ではその考えは限定的であることが分かった。日本企業でこのような懸念が存在することについては、前述のユーザー企業へのヒアリングを通じても確認できた。また、国内外問わず、組織が行っている先進的な取り組みを公表することを一つの付加価値として捉えている企業はあるが、海外の方が顕著であるという意見を頂戴した。加えて、海外企業において導入実績公表が促進されている異なる要因として、人材流動性の問題が指摘された。日本では、新たな製品の導入についてコンサルティング等の外部組織に頼ることが多いが、海外ではそれぞれの企業でシステムを構築されるケースが多いため、ユーザー企業側に技術を評価・説明できる人材が存在する。海外企業においては、セキュリティは情報システム部門の領域ではなく経営者の領域であり、技術に明るい人材が経営層に配置されることが多いため、経営層の意識の違いで海外事例の方が多いという可能性も指摘された。

また、海外での導入事例やユーザーの評価が活用されている状況については、ユーザー企業同士のクローズなコミュニティにおいて導入事例の共有がなされているとの意見を得られた。第三者機関の評価を与えることで、ユーザー企業が採用しやすくなることも事実であり、セキュリティベンダーが米国 SAFETY Act[3]の認定を受ければ、米国では導入が促進される可能性も指摘された。海外では IT 製品の比較サイト[4]が流行しており、日本においても ITcrowd が開設した ITreview[5]のような IT 製品比較を行う企業が出始めている。セキュリティベンダーによっては、導入試行評価を独自で実施している場合もあり、国による介入が逆に煩わしさを与える可能性を指摘された。セキュリティ製品を評価については、検出率等の技術観点だけでなく、侵入時のサポート等の組織的側面も評価する必要性も指摘された。

表 3-2 にセキュリティベンダー3 社のヒアリング結果を示す。

[3] 正式名称は「2002 年効果的技術促進による反テロリズム支援法（Support Anti-Terrorism By Fostering Effective Technologies Act of 2002）」であり、米国の防御を強化するセキュリティ製品・サービスの開発・導入の奨励を目的とした、米国国土安全保障省の賠償責任管理プログラム。

[4] 例として、G2 Crowd（https://www.g2crowd.com/）が挙げられる。

[5] ITreview, https://www.itreview.jp/, 2019 年 3 月 5 日閲覧。

表 3-2　セキュリティベンダー3 社のヒアリング結果

主な販売セキュリティ製品	ヒアリング結果
ファイアウォール（UTM）	・ 国内・海外に関わらず導入実績の公表は経営者の意識に依存する部分が大きい。海外では、セキュリティは情報システム部門の領域ではなく、経営者の領域である。そのため、経営者が公開に前向きであれば公開に繋がることもある。 ・ 導入企業としては、公開事例は複数の対策の一部であり、一拠点の対策が公開されても他拠点は異なる製品であることもあるので、公表によるリスクは限定的である。 ・ 日本企業では、同業他社がどのような製品を使っているかを気にすることが多い。 ・ 海外において、導入実績公表を促すような制度や仕組みがあるかは分からない。 ・ 国内企業と海外企業の情報システム部門における大きな違いは、自組織で導入を検討する能力があるかないかであり、グローバル企業の場合、エンジニアを社内で有している場合が多いため、自組織内で製品の目利きを行い、導入を決定することが多い。 ・ 製品の信頼性評価施策に対して、セキュリティに関するベンチャー企業は日本には少なく、VC 等による資金援助やイグジットまで考慮しないと、ベンチャー企業が成長しても米国企業に買収される可能性があるため、今回の施策が本来の目的に沿った形となるかは検討が必要である。
ウイルス対策ソフトウェア	・ 導入実績公表について海外企業の方が多い要因として、IT やセキュリティへの関わり方が違うことが言える。国民性とも言えるが、日本は慎重である一方で、特に米国の場合、公表にオープンである印象を受ける。 ・ また、人材の流動性も要因として挙げられる。日本では、人材を一つの組織で育てていくという考えがあるので、新たな製品の導入についてコンサルティング等の外部組織に頼ることが多い。 ・ 海外ではそれぞれの企業でシステムを構築されるケースが多い。一方日本では、セキュリティ部門やシステム部門が分社化されることが多く、セキュリティの部分は分社に任せている、というような事例が多い。 ・ 海外の場合、最近 IT 製品の比較サイトが流行ってきており、海外企業は独自で導入製品を決定することが多い。 ・ 公表を促進する制度や取り組みについては、海外でも聞いたことがない。 ・ セキュリティ製品を評価するときに、検出率などの技術観点だけでなく、サポート等の支援を受けられるか等の組織的側面もきちんと評価する必要がある。

主な販売セキュリティ製品	ヒアリング結果
UTM	・ 国内のほうが、海外に比べると公表の実績は少ない。 ・ 海外では、CISO が導入事例公表を自らの実績として打ち立てることがある。 ・ 海外では多少リスクがあったとしても、アピールのほうが有益であると考えることが多い。 ・ 海外では導入事例を公表した実績を、個人のキャリアとして転職時に使うことが普通であるが、日本ではこのようなケースが稀である。日本と海外では人材流動の仕組みが異なるが、これが事例公表の意識にも影響しているのではないか。 ・ 国内外問わず、スタートアップだから導入しづらいという事は無いと考えている。 ・ 米国 SAFETY Act の認証を受ければ、米国では導入が進みやすくなることも事実である。 ・ サイバーセキュリティ検証基盤のうち「２．実環境における試行検証」は独自で試行している。企業努力で試行検証は実施できると考えており、国がどこまで制度を構築するかは議論が必要。営業を積極的に行っているので、国による介入がある場合、逆に煩わしく感じるかもしれない。 ・ 人材関連の施策はすぐに結果が出にくいため、国が支援を行うべきである。

3.3 実績構築のための仕組み検討

前節で調査した結果を基に、新たに開発されて実績が少ないセキュリティ製品を仮定し、実環境に導入し実績を積むために必要な事項について整理し、実績作りを促進するための仕組み作りについて検討を行った。

前節でのヒアリング結果より、セキュリティ製品を導入するユーザー企業等は、他組織が公表している情報を参考にセキュリティ製品を選択することが多い。そのため、すでに導入実績が多い大手セキュリティベンダーの製品が積極的に選ばれ、スタートアップ等の新興セキュリティベンダーの製品導入は阻害される傾向にある。事実、ユーザー企業等のヒアリングでは、ベンチャー等の製品は導入しておらず、仮にベンチャー企業からセキュリティ製品導入の営業が来た場合でもリスクを意識してしまうといった意見が目立った。そのため、新たに開発されて実績が少ないセキュリティ製品のうち、特にベンチャー企業のような新興企業によって開発された製品の実績構築促進が必要であると考えられる。一方で、セキュリティ製品ベンダーによっては、サイバーセキュリティ検証基盤のうち実環境における施行検証を企業独自に行っているベンダーも多い。製品導入の効果は、実際の運用環境に導入することでより明確となるため、大手ベンダー・ベンチャー問わず多くのセキュリティ製品ベンダーが試行検証を独自で実施している。事実、今回ヒアリングを行ったセキュリティ製品ベンダーからは、自社の製品を顧客環境に導入する概念実証サービスを通じて販売に結

びつくことも多いという意見を得られた。そのため、ベンチャー企業のようなスピード感が求められる企業にとって、国による実環境における施行検証が参入を妨げる障壁となりかねない。

したがって、新たに開発されて実績が少ないセキュリティ製品のマーケットインを促進するために、国として試行検証環境を整備する以外で、適切なセキュリティ製品の実績を保証することが望ましい。適切なセキュリティ製品の実績構築を行う一つの方法として、第三者セキュリティ製品調査機関への製品提供を斡旋する方法が考えられる。ヒアリング結果からも、第三者機関による評価を受けることで製品の信頼性向上に繋がり、販売に影響するとの意見が得られた。セキュリティ製品のテスト・評価を行う第三者機関は多く存在[6]するが、これら機関による評価を受けている企業の多くは成熟した製品ベンダーであり、ベンチャー企業等の評価結果は少ない。技術力のあるセキュリティ製品が適切な評価を受けるためにも、ガイドライン等で評価実施を推進することが望まれる。経済産業省が発表している「IT 製品の調達におけるセキュリティ要件リスト」では、製品調達の納品時検査作業において、調達製品が ISO/IEC 15408（Common Criteria）等の国際標準に基づいた第三者認証を取得している場合、第三者認証を取得済みであることの確認をもって受け入れテスト等に替えることが可能である旨が示されているが、国際標準以外の第三者認証に基づいたテスト結果を考慮に入れる事で、適切な技術を有したセキュリティ製品の調達が拡大すると考えられる。そしてこれは、現状評価実績の少ないベンチャー企業等の実績構築を促進し、当該製品のマーケットインに繋がる可能性が高い。

同様の理由として、製品評価サイトによるセキュリティ製品の第三者評価もマーケットインに対して効果があると考えられる。前述のとおり、海外では IT 製品の比較サイトが流行しており、一般ユーザーの口コミによってセキュリティ製品が評価される仕組みが整っている。多くの評価サイトでは、ユーザーによる 5 段階などの定量的評価に加えて、顧客満足度や市場浸透性等の特徴を踏まえた比較分析を行うことができ、導入企業が製品を選択する際の一つの判断材料となりうる。日本では、現状このような評価サイトは多くない。セキュリティ製品の試行検証を独自で実施しているベンダーは多いため、少ない試行期間でも評価・投稿が行えるような評価サイトを構築することで、ユーザーから多くの意見や評価を集約することができ、結果としてユーザー企業が製品を選択する際の一つの判断基準となり得る。セキュリティ製品ベンダー、特に実績の少ないベンチャー企業にとっては、評価サイトにおいて高評価が得られた場合、製品のマーケットインに繋がると考えられる。

[6] 例として、NSS Labs（https://www.nsslabs.com/）、ICSA Labs（https://www.icsalabs.com/）、AV-TEST Institute（https://www.av-test.org/）等が挙げられる。

4. IoT 製品等に対する先進的手法を用いた脆弱性等の検証のあり方について

4.1 調査概要

スマートフォン、ネットワークカメラその他の脆弱性攻撃の対象となり得る IoT 製品の特徴等について調査し、脅威等を検知するための先進的手法、当該先進的手法を用いた検証を事業として実施する場合に事業者に求められる要件及び現行法令上、留意すべき事項について検討を行った。また、諸外国において、IoT 製品の脆弱性等を検証するための民間企業又は政府機関による取組の有無について文献調査を行った。

4.2 IoT 製品の脅威・脆弱性検討

スマートフォン、ネットワークカメラその他の脆弱性攻撃の対象となり得る IoT 製品を選定し、その特徴に応じて想定される脅威・攻撃シナリオと脆弱性について、検討を行った。

選定に関しては、攻撃者の視点から検討を行った。具体的には、攻撃の容易性及び攻撃による影響の観点から、攻撃対象となり得る IoT 製品例を以下のように抽出した。

- 常時アクセス可能な事により攻撃対象となり得る、ネットワーク、特にインターネットや携帯網に常時接続されている製品
- 情報収集のために攻撃対象となりやすい、カメラや位置情報などのセンサー情報を収集する製品
- 悪意を持った攻撃の対象となり得る、外部から操作されることで大きな被害が発生する製品
- 法人向けの製品に比べセキュリティレベルが低いことが想定される、個人向けの製品。

これらの観点から本調査では、ネットワークカメラ、スマートフォン及び Wi-Fi ルータ・モバイルルータを選定した。

次に、選定したネットワークカメラ、スマートフォン及び Wi-Fi ルータ・モバイルルータにおいて想定される脅威・攻撃シナリオの検討と脆弱性の検討を行った。本調査では当該 IoT 製品に対する攻撃脅威・攻撃シナリオを抽出し、その脅威に結びつく IoT 機器の脆弱性との対応関係を明確化した。この結果を表 4-1 に示す。

表 4-1　IoT 製品における攻撃脅威・脆弱性

関連する脆弱性		**IoT 機器に対する攻撃脅威・攻撃シナリオ**	
項目	**概要**	**項目**	**概要**
パスワードの不備	多くの IoT 製品は設定のための Web アプリなどが埋め込まれており、設定画面に入るための ID と初期パスワードが設定されている。しかし、初期パスワードが全製品で統一である場合や容易に想像ができ	不正ログイン	第三者が ID と初期パスワードなどで IoT 製品に不正にログインし、設定を確認や変更する。
		バックドアやマルウェアの埋め込み	不正にログインした後、不正なファームウェアへのアップデート実施や、バックドア・マルウェアが埋め込まれる。結果として、

関連する脆弱性		IoT 機器に対する攻撃脅威・攻撃シナリオ	
項目	概要	項目	概要
	るパスワードである状態。		DDoS 攻撃などの踏み台となる不正なプログラムが実施される可能性がある。
ファームウェアの不備	安価な IoT 製品などではファームウェアの更新機能がない状態。もしくはファームウェアのアップデート機能がある場合でも、正しくメーカーが提供するファームウェアであるかどうかの確認をせずに更新可能な状態。	バックドアやマルウェアの埋め込み	不正なファームウェアへのアップデートを実施することで、バックドア・マルウェアが埋め込まれる。結果として、DDoS 攻撃などの踏み台となる不正なプログラムが実施される可能性がある。
プロトコルの脆弱性	古い SSL のプロトコル（SSL 3.0 や TLS 1.0）等の脆弱性で、現在では利用が推奨されていない。	データの漏洩	ネットワークへの侵入や中継サーバへの侵入によって、データが攻撃者に漏洩する。
オープンソースの流用	脆弱性のある古いバージョンのライブラリ等を利用している状態。IoT 機器では、Linux やオープンソースのライブラリやプログラムなどが利用されている。	バックドアやマルウェアの埋め込み	オープンソースの脆弱性を利用し不正アクセス等を行うことで、バックドア・マルウェアが埋め込まれる。結果として、DDoS 攻撃などの踏み台となる不正なプログラムが実施される可能性がある。
製造段階における不正プログラム・コード	製造時にテストのために利用していたデバッグ機能やバックドア機能が、そのまま残されたまま IoT 製品として販売されている状態。	マルウェアの埋め込み	不正なプログラムや不正なコードを悪用し、マルウェアが機器に挿入される。結果として、機器が恣意的に操作される可能性がある。
		データの漏洩	不正なプログラムや不正なコードを悪用し端末にアクセスすることで、データが漏洩する。

4.3 IoT 製品の脆弱性検証方法の検討

前節で選定した IoT 製品において想定される脆弱性等を検証するための手法を調査し、当該手法の実施に必要な情報、検証要員に必要な知識や能力、必要なシステム環境、コスト及びゼロデイ脆弱性等の情報管理について、検討を行った。加えて、国内企業が競争力のある製品やサービスを国内外に提供するために必要な検証の在り方について検討を行った。

まず前節での脆弱性を検証するための検査手法としては、ファームウェアやハードウェアを解析するためのリバースエンジニアリングが検証項目としてあげられる。また、製品ベンダーの故意又は不備による情報漏えいなどを確認する上で、ネットワークキャプチャに

よる通信の解析も必要と考えられる。IoT 機器に対する脆弱性検証項目を表 4-2、各項目の検証実施概要を図 4-1 に示す。

表 4-2　脆弱性検査項目

検査項目	検査内容
ブラックボックス検査	ネットワーク経由で外部からスキャンを行うことで脆弱性を検査する手法。 ネットワーク経由で空いているポートをスキャンし、空いているポートに対して既知の脆弱性に対する攻撃を行うことで、脆弱性の有無を診断する。
ホワイトボックス検査	ソースコードや基盤の設計図を分析して脆弱性を検査する手法。ただし、ホワイトボックス検査を実施するにはメーカーからソースコードや設計図を提供して貰う必要があるため、第三者によるセキュリティ検査では基本的に実施できない。
ネットワークキャプチャ	IoT 製品のメーカーが明示的又は不備により、収集したデータを不正に外部に送信している場合、ブラックボックス検査では検知できない。そこで、IoT 製品の通信をキャプチャし分析することで、不正な通信や不要なデータの外部への送信、外部からの不要なアクセスなどを検査する。Wi-Fi などでネットワークに接続されている機器については、スイッチのミラーポートで通信を監視している場合や、HTTP などのプロトコルで通信している場合はプロキシーなどを設置することで通信内容をキャプチャすることができるが、携帯網などに直接接続している場合には、キャリア会社などの手助けがなければキャプチャは困難である。
リバースエンジニアリング（ソフトウェア）	IoT 製品のファームウェアを分析し、脆弱性を検査する手法。IoT 製品のファームウェアを更新サイトから取得又はハードウェアから抜き出して取得し、逆アセンブルして生成したソースコードに対して静的テスト、動的テスト、脆弱性分析、ファジングテストなどを行うことで脆弱性を診断する。また、改ざんしたファームウェアを埋め込むことができるか、更には改ざんしたファームウェアを埋め込むことでバックドアなどを仕込むことができるか、といった脆弱性についても検証する。2019 年 3 月には、米国国家安全保障局（NSA）が組織内で使用してきたソフトウェアリバースエンジニアリングを無償で公開[7]するなど、脆弱性検証の主要項目の一つとなっている。
リバースエンジニアリング（ハードウェア）	IoT 製品のハードウェアに直接アクセスすることで、各種情報を抜き出す手法。ボード上のチップからファームウェアを抜き出すほか、ボード上のシリアルポートからコンソールにログインして IoT 機器の脆弱性を調査する。もしくは、ボード上のチップを分析・調査し、チップの挙動やバグを見つけることも含

[7] US NSA’s GHIDRA, https://ghidra-sre.org/, 2019 年 3 月 11 日閲覧。

検査項目	検査内容
	まれる。

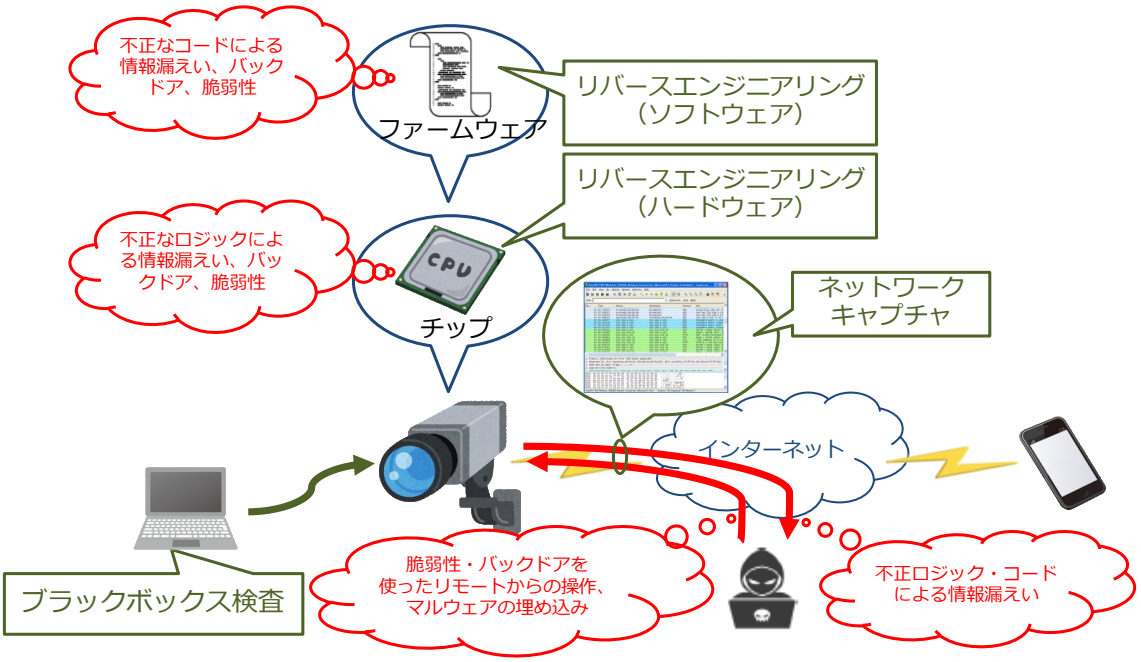

図 4-1　IoT 機器における脆弱性検証項目 実施例

次に、これら検証手法の実施に必要な情報、検証要員に必要な知識や能力、必要なシステム環境、コスト及びゼロデイ脆弱性等の情報管理について、検討を行った。検討結果を表 4-3 に示す。

表 4-3　脆弱性検査に必要となる情報等

検査項目	ブラックボックス検査	ホワイトボックス検査	ネットワークキャプチャ	リバースエンジニアリング
検査に必要な情報	テスト対象の内部構造を把握せず実施する検査のため、一般的に事前情報は必要ない。	テスト対象の内部構造を把握する実施する検査のため、確認するソースコード、設計図、ロジックフロー等。	キャプチャを行うネットワークインタフェース名、IP アドレス体系、MAC アドレス等。	逆アセンブルを行うためのファームウェアのダンプファイル等。
必要な知識や能力	脆弱性スキャン、ペネトレーションテスト等の知識及び能力。	テスト対象となるソースコード等の解析に関する知識及び能力。	プロトコル技術、信頼性設計、セキュリティ技術等のネットワークサービスに関係する知識。	ハードウェア及びファームウェアの解析に関する知識及び能力。

検査 項目	ブラック ボックス検査	ホワイト ボックス検査	ネットワーク キャプチャ	リバースエンジ ニアリング
必要なシステム環境	対象機器にネットワークアクセスできる環境及び脆弱性スキャンやペネトレーションテストのためのツール。	対象機器にネットワークアクセスできる環境及び静的コード解析ツール。	対象機器にネットワークアクセスできる環境、対象機器が LAN 又は Wi-FI でネットワーク接続した環境及びネットワークキャプチャツール。	対象機器のファームウェアを抽出・解析するための機器・ツール。

どの検査項目についても、検査用 PC を含めたシステム環境の整備に一定以上のコストはかかるが、ツールについてはフリーソフトが多く公開されているためこれらを適切に用いることで、低コストで環境整備をすることも可能であるが、検証時間及び人件費については留意する必要がある。特に、IoT 機器に対してネットワークキャプチャを行う際、当該機器が悪意あるサーバ等に通信を行う頻度が長い可能性もあり、検査の網羅性を担保するのであれば、長時間の検査を行うほうが好ましい。また、ゼロデイ脆弱性等の情報管理については、次節でも述べるように、適切な情報管理規則に基づき管理を行うとともに、関係機関に対する早急な連絡・報告が必要となる。

国内企業が競争力のある製品やサービスを国内外に提供するために、国際的な認証標準の検証項目を参考に、検証項目の網羅性を担保する必要がある。例えば、制御システムの特定サブセットのためのセキュリティ認証である、ISA Security Compliance Institute（ISCI）[8]によって策定された SSA（System Security Assurance）認証では、機器運用時の脆弱性検出・識別を行うための試験がシステムロバストネス試験（SRT）として規定されている。この中には、既知の脆弱性を識別する脆弱性識別試験（VIT）、ネットワークに対するファジングや負荷ストレス試験を行う通信ロバストネス試験（CRT）及びネットワークストレス試験（NST）、システム内のコンポーネントに対してスキャンを実施するアセット検出試験（ADT）が含まれ、各テスト項目で細かなテスト項目が規定されている。脆弱性検証の目的は、検査実施機器が安全か否かを判別することであり、安全であると示すためには幅広い項目を含めた検証項目とする必要がある。

4.4 検証手法の有効性確認

前節で調査した手法の有効性を確認するために、4.2 節で選定した IoT 製品に対し、当該手法を用いた脆弱性等の検証を行い、現状における課題の洗い出しを行った。

本検証では、ネットワークカメラ 4 台、スマートフォン 2 台、Wi-Fi ルータ・モバイルルータ 3 台に関して、前節で調査した脆弱性検証を実施した。まず、一次検査として、選定した全製品について、既存ツールによる簡易的な脆弱性検査とネットワークキャプチャを実

[8] 制御機器のセキュリティ保証に関する国際認証組織であり、ISA（国際計測制御学会）のメンバーが中心となって設立された。

施した。一次検査の結果に基づき、脆弱性や不正通信が多い 2 製品を更に選定し、より詳細な二次検査を実施した。検査により、対象機器においていくつかの脆弱性が発見された。

脆弱性検証における現状の課題として、検証を実施する要員のスキルに依存することが挙げられる。検証要員は、1 つの検査項目に対して数多くの方法やツール等から有効なものを選定する必要があり、実際に検証を行う際には、検証ツール毎の使用方法の習得が不可欠となる。検証を実施するためには、セキュリティに関連する OS、ネットワーク、ペネトレーションテスト等に関する知識に加えて、日々洗練化される脅威情報に関する知識や新興の情報セキュリティ技術に関する知識も必要となる。特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）の日本セキュリティオペレーション事業者協議会（ISOG-J）と OWASP Japan 主催の共同ワーキンググループである脆弱性診断士スキルマッププロジェクトでは、脆弱性診断を行う技術者に必要なスキルマップを公開[9]しているが、このスキルマップからも脆弱性検証・診断の際に多くの知識が必要となることが分かる。

異なる課題として、検証を行った脆弱性情報の管理の問題が挙げられる。当然ながら、脆弱性検証によって脆弱性が発見された場合には、適切な関係機関に対して早急に報告や連絡を行う必要[10]がある。IPA や JPCERT/CC を始めとする関係組織は、情報セキュリティ早期警戒パートナーシップガイドラインにおいて脆弱性発見時の通知に関して規定しており、検証要員は適切な情報管理に基づき、当該ガイドラインに則った連絡や報告が必要となる。

組織においては、検査のタイミングについても検討が必要である。セキュリティ製品販売前にベンダーによって脆弱性検証を行うことは当然であるが、販売後もファームウェアやパターンファイルのアップデート、脆弱性対応パッチの適用等によって、製品の機能や性能が変わる可能性がある。これらのアップデートや適用が行われたタイミング又は IoT 機器に関連しうる脆弱性が報告された都度、脆弱性検証を行うことが望ましい。

4.5 検証実施に係る法令上の留意事項

脆弱性等の検証を事業として実施する場合に現行法令上留意すべき事項について検討した。IoT 機器の脆弱性検査を実施するに当たって、考慮すべき法令とその概要について表 4-4 に示す。

表 4-4　脆弱性検証に係る法令

法令	概要
不正アクセス禁止法	電気通信回線（インターネット等）を経由し、第三者のアクセス制御機能を有する特定電子計算機に対して無断で他人の識別符号（ID、パスワード等）を使う他、アクセス制御機能を回避してアクセスすること（不正アクセス）を禁止した法律。
特許法	プログラムは特許法によって知的財産として保護される場合があるが、特許法 69 条 1 項において「試験又は研究のために

[9] 脆弱性診断士スキルマッププロジェクト, https://www.owasp.org/images/4/41/Pentester-Platform-Skillmap_and_Syllabus-201604.pdf, 2019 年 3 月 13 日閲覧。

[10] 日本では脆弱性関連情報の届出受付期間は情報処理推進機構（IPA）であり、脆弱性関連情報に関する製品開発者への連絡および公表に係る調整機関は JPCERT コーディネーションセンター（JPCERT/CC）である。

法令	概要
	する特許発明の実施」については許可を明記している。
著作権法	IoT 機器のファームウェアをリバースエンジニアリングのために逆コンパイルして調査・解析を行うことは、対象となるプログラムの著作権を侵害する行為となりえたが、2019 年 1 月 1 日に施行された「著作権法の一部を改正する法律」によって、著作権法第三十条の四「技術の開発又は実用化のための試験の用に供するための利用」の改正が規定された。具体的には、技術の開発等のための試験の用に供する場合、情報解析の用に供する場合等にはその必要と認められる限度において利用することができると規定しており、文化庁の Web サイトにおいても「プログラムの調査解析を目的としてプログラムの著作物を利用する行為（いわゆる「リバース・エンジニアリング」）」は権利制限の対象として挙げられることが記載されている[11]。
ライセンス・使用許諾	多くのソフトウェア製品では、ライセンス契約や使用許諾契約においてリバースエンジニアリングを禁止する条項が記載されている。IoT 機器においても、ファームウェアの利用について使用許諾契約やライセンス契約に同意したことを前提に利用することになっているものがある。

以上の法令等が主に脆弱性検証に係る法令等と考えられるが、2019 年に施行された改正著作権法に挙げられるように、ソフトウェア・ハードウェア解析を始めとする脆弱性検証に関連する法令は近年広く議論されており、専門家の解釈も統一的ではない。よって、脆弱性検証を実施する際には、法律家の指導の元、法令による影響が及ばない範囲で実施することが望ましい。

4.6 諸外国における脆弱性検証の状況

4.2 節で選定した IoT 製品に関する、諸外国の民間企業又は政府における脆弱性等の検証の取組について文献調査を行った。整理の結果を表 4-5 に示す。

表 4-5　国内外における IoT 製品検証の取り組みに関する文献等

文献等（策定年）	発行機関	概要
IoT セキュリティガイドライン Ver 1.0（2016 年）	IoT 推進コンソーシアム、総務省、経済産業省	IoT 機器やシステム、サービスを提供するメーカーやシステムインテグレーター、サービス提供者に対して、ライフサイクル（方針、分析、設計、構築・接続、運用・保守）の各段階における　セキュリティ上の指針を定めると同時に、一般利用者のためのルールを定めたガイドライン。

[11] 文化庁, http://www.bunka.go.jp/seisaku/chosakuken/hokaisei/h30_hokaisei/, 2019 年 3 月 4 日閲覧。

文献等（策定年）	発行機関	概要
IoT 開発におけるセキュリティ設計の手引き（2018 年）	情報処理推進機構（IPA）	IoT 機器のセキュリティ設計開発者向けの手引きで、脅威分析、セキュリティ対策の検討、開発段階及び運用段階での脆弱性への対応について、例を示しながら具体的な対応方法を記載。
ネットワークカメラシステムにおける情報セキュリティ対策要件チェックリスト（2017 年）	情報処理推進機構（IPA）	「政府機関の情報セキュリティ対策のための統一基準」において調達・運用時のセキュリティ要件を求められている特定用途機器のひとつである「ネットワークカメラシステム」について、想定される脅威に対策を講ずる情報セキュリティ対策の要件を列挙した資料。ただし、政府機関や自治体に限らず、ネットワークカメラシステムに関連するシステムであれば参照可能としている。
端末設備等規則等の一部改正（2018 年に意見募集を実施）	総務省	IoT 機器を含む端末設備のセキュリティ対策に関する技術基準に関する省令を一部改正し、端末機器に不正アクセスを防ぐ機能を設けることを義務付けることを、2020 年 4 月施行を目指して推進。本省令改正では、IoT 機器を含むインターネットプロトコルを利用して通信する機器について、技術基準適合認定の認定条件として、アクセス制御機能、ID・パスワードの適切な設定を促す機能及びファームウェアの更新機能を追加する方針。
NOTICE（2019 年から実施）	総務省	サイバー攻撃に利用されるおそれのある機器を調査し、利用者に注意喚起することを目的とした取り組み。本取り組みでは、国立研究開発法人情報通信研究機構（NICT）が国内の IoT 機器（ルータやネットワークカメラ等）に対して、容易に推測されるパスワードでログインできるかどうかを調査し、脆弱な機器についてはプロバイダーを通じて管理者に注意喚起を実施する。
Strategic Principles for Securing the Internet of Things (IoT)（2016 年）	米国国土安全保障省（DHS）	IoT を構成するネットワーク接続されたデバイス、システム及びサービスの設計、製造、導入、運用の各段階における IoT セキュリティを向上させるための指針であり、実践的な対策　をベストプラクティスとして紹介。ただし、法的な拘束力はない。
Baseline Security	欧州ネットワ	IoT 機器に関する一般的な課題を抽出し、関

文献等（策定年）	発行機関	概要
Recommendations for IoT（2017 年）	ーク・情報セキュリティ機関（ENISA）	係者が解決するために有用となる考え方やツール（既存の規格、ガイドライン、研究資料等）やベストプラクティスを紹介するレポート。EU では、ICT 機器とサービスについてサイバーセキュリティ認証フレームワークを構築し、欧州内におけるサイバーセキュリティ認証制度を確立することで、欧州におけるデジタル単一市場の信頼性、セキュリティを確保することを目指している。その方針として、個々の技術標準に対する認証制度を導入するのではなく、特定の ICT 機器やサービスのためのサイバーセキュリティ認証フレームワークを ENISA が作成し、製品が遵守する必要のある技術要件及び評価手順に関しては既存の基準を使用する。また、監視、監督、執行の任務は加盟国に委ねられている。
EU Cybersecurity Certification Framework	欧州委員会（EC）	2017 年 9 月に EC は、ENISA 規則（No. 526/2013）の改訂案及び欧州の ICT セキュリティ認証に関するフレームワークを定める規則の提案を行った。提案されている認証フレームワークは、包括的な規則、技術要件、標準及び手順として EU 全体に適用される認証スキームを提供する。2018 年 12 月に行われた会議では、当該フレームワークの策定を含んだ EU Cybersecurity Act に関する政治的合意を実施した。

5. 考察

本調査では、国内外のセキュリティ製品及び IoT 製品の市場を取り巻く環境や取り扱われる商品等の情報を整理し、セキュリティ製品においてはその有効性を検証するための手法について調査を行い、IoT 製品においては抱えうる脆弱性等の情報とその脅威を検知する手法について調査を行った。

(1) セキュリティ製品市場を取り巻く環境や国内の製品開発動向

今後の市場の成長が見込まれ、我が国がこれからシェア獲得を狙えるセキュリティ製品分野としては、OT 製品・IoT 製品向けのセキュリティ製品や、AI や自動運転・それらに関連するセキュリティ製品が考えられる。一方で、有識者へのヒアリングによると、海外（特に米国）では①サイバーセキュリティに特化した機関があり、国としてセキュリティの経験値が違うこと、②アクセラレータがスタートアップの支援を行っていること、③防衛産業でセキュリティ製品が使われその後一般に製品が広がっていく仕組みが出来ていること等から、そうした環境で技術を磨く海外ベンダーに対し、日本国内のベンダーがシェアを拡大することは難しいという意見もあった。

こうした環境下でベンチャー企業のセキュリティ製品等、新規製品が市場を形成していくためには、ベンチャー企業のセキュリティ製品を PaaS 等のプラットフォームに乗せるためのベンチャー企業紹介制度や営業支援が考えられる。また、新規製品を販売するシステムインテグレーターや代理店等が営業する際のツールとして利用できる認証制度も有効と考えられる。

国内の企業が提供するセキュリティ製品に関する有効性の検証制度に対しては、合格となった場合に有効なマーケティングツールになることが想定される等、一定度のニーズは存在するが、検証環境の整備資金や検証側の能力、責任の担保等の課題が残る。また、有効性検証の評価指標には、性能評価・一定度のプログラムの保証（PSI 認証等）の他、サポート状況や安定性、導入環境への適用性等があり、ユーザーによって重視する評価指標は異なる。特に日本国内においてはサポートや安定性が重視される傾向がある。有識者からは定性的な評価でよいとする見解も示された。

(2) 試行的評価の促進について

セキュリティ製品の市場へのマーケットイン促進について、製品導入実績の公表は有効であることが調査で明らかとなった。ヒアリングによれば、セキュリティ製品を導入するユーザーにとって、他社が導入している事例は製品選択の判断材料の一つであり、安心・安全が担保されているコミュニティ内の事例公開であれば、情報共有を促進したいという意見は多かった。また、事例公表によって、自組織のセキュリティ対策への積極的姿勢のアピールにも繋がることが明らかとなり、政府として事例公表を後押しすることで、ユーザーにとって導入に有効な情報が共有され、セキュリティ製品導入が促進されるだけではなく、セキュリティ業界全体の活性化につながると考えられる。一方で、導入事例を公表することによるセキュリティリスクの顕在化を懸念する声も多い。事例を公開するユーザーからは、多層防御を行っていることからリスクは限定的である、リスクの高い情報は公表しない等の意見が伺えており、公表によるリスクは低減可能であると考えられる。したがって、リスクを

限定する公表指針を明確化することにより、事例公表を促進できると考えられる。

また、マーケットインの促進施策として、セキュリティ製品の第三者評価機関への製品提供促進及びセキュリティ製品評価サイトの活用が挙げられる。第三者機関による評価を受けることで、適切な技術を有したセキュリティ製品の拡大が期待でき、ベンチャー企業等の実績構築を促進し、当該製品のマーケットインに繋げられる可能性が高い。同様の理由から製品評価サイトを積極的に活用することで、ユーザーから多くの意見や評価を集約することができ、集約した情報は製品を選択する際の一つの判断基準となり得る。

(3) 脆弱性等の検証のあり方について

攻撃の対象となり得る IoT 製品の特徴、脅威等を検知するための先進的手法、当該先進的手法を用いた検証を事業として実施する場合に事業者に求められる事項が調査により明らかとなった。

攻撃対象となり得る IoT 機器として、現在までのインシデント事例や、攻撃が容易である点及び攻撃による影響が大きい点を踏まえると、ネットワークカメラ、スマートフォン及び Wi-Fi ルータ・モバイルルータが挙げられる。これら IoT 機器の検査を行う手法として、ブラックボックス検査、ホワイトボックス検査、リバースエンジニアリング等が挙げられ、検査要員にはそれぞれの検査独自のツールや検査能力が求められるほか、検証を行った脆弱性情報に係る管理や報告については留意する必要がある。また、2019 年 1 月に施行された改正著作権法に挙げられるように、ソフトウェア・ハードウェア解析を始めとする脆弱性検証に関連する法令は近年広く議論されている。よって、脆弱性検証を実施する際には、法律家の指導のもとで実施すること必要がある。

二次利用未承諾リスト

報告書の題名　セキュリティ製品の有効性及び脆弱性検証に関する調査報告書

委託事業名　平成３０年度サイバーセキュリティ経済基盤構築事業（セキュリティ製品の有効性及び脆弱性検証に関する調査）

受注事業者名　株式会社三菱総合研究所

頁	図表番号	タイトル
7	図 2-1	国内のセキュリティ製品市場（高成長率分野の規模、成長率、国内ベンダー比率）
15	図 2-2	AV-TEST によるテストで合格した場合に付与されるマーク
15	図 2-3	AV-Comparatives によるテストで合格した場合に付与されるマーク

「セキュリティ製品の有効性及び脆弱性検証に関する調査」
報告書

2019 年 3 月

株式会社三菱総合研究所
社会 ICT イノベーション本部
TEL (03)6705-6047