試行導入・導入実績公表の手引き

令和２年４月

独立行政法人情報処理推進機構

目次

1. はじめに

1.1. 背景

近年サイバー攻撃の起点は急激に拡大し、攻撃の手法も高度化していることから、サイバー攻撃の脅威はあらゆる産業活動に潜んでおり、産業界全体の取り組みとしてサイバーセキュリティ対策の強化が必須となっている。

このようなサイバーセキュリティに関する課題に対し、経済産業省では日本の産業界が直面するサイバーセキュリティの課題を洗い出し、関連政策を推進していくため、産業界を代表する経営者、インターネット時代を切り開いてきた学識者等から構成される「産業サイバーセキュリティ研究会[1]」を設置した。

研究会で示された政府として取り組むべき政策の方向性を踏まえ、研究会の下に設置された各ワーキンググループにて、政策の具体化を進めている。産業サイバーセキュリティ研究会ワーキンググループ 3(サイバーセキュリティビジネス化)[2]では、日本の産業界がサイバーセキュリティに関して何を強化してビジネス拡大をするか検討を行っている。

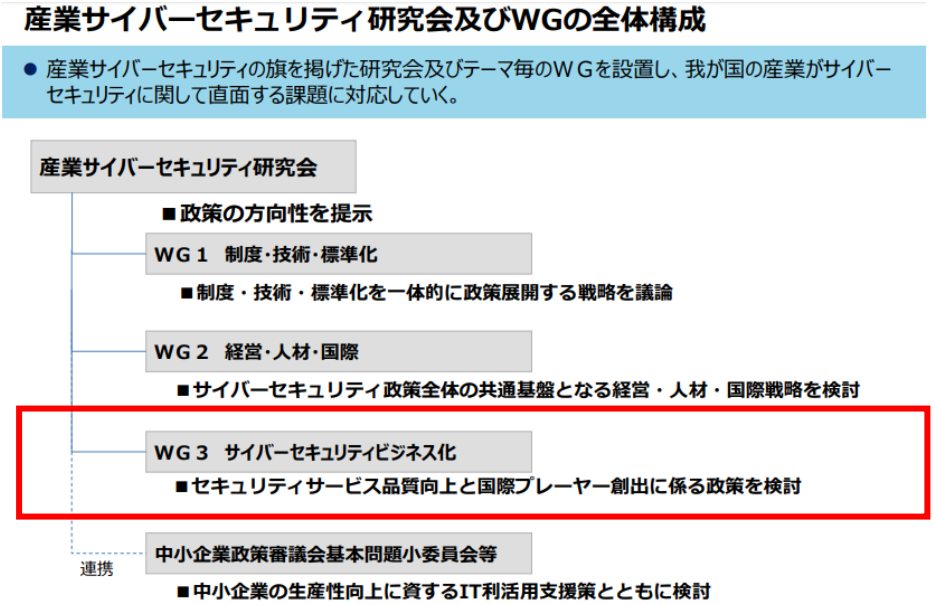

図 1 産業サイバーセキュリティ研究会及び WG の全体構成
(出典:経済産業省「産業サイバーセキュリティ研究会」)

日本におけるサイバーセキュリティのビジネス創出の鍵となるのは、日本のユーザー企業におけるセキュリティ対策のニーズと、日本国内のスタートアップ企業の尖った製品や埋もれた製

[1] 経済産業省　産業サイバーセキュリティ研究会:
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/index.html
[2] 産業サイバーセキュリティ研究会　ワーキンググループ 3(サイバーセキュリティビジネス化):
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/index.html

品であるシーズのマッチングであるといえる。

ユーザー企業におけるセキュリティ製品等の選定の決め手の一つは実環境への導入実績であり、マッチングのためには日本のベンチャー企業に導入実績の課題を乗り越えさせ、マーケットインを支援する施策が必要である。そのため国が主導して、日本発のセキュリティ製品の実環境への試行導入及び、試行導入の実績公表を進める仕組みを構築していくことが求められる。

1.2. 目的

上述のような背景より、日本発のセキュリティ製品の実環境への試行導入と導入実績公表を進める仕組みという位置づけで、実環境への試行導入・導入実績公表を行うユーザー企業向けの「試行導入・導入実績公表の手引き」（以下、「手引き」）を作成した。手引きの作成においては、試行導入に関心があるユーザー企業が、尖った製品や埋もれた製品を持つスタートアップ企業のような製品ベンダーの製品を積極的に採用し、導入実績を公表することで、日本発のセキュリティ製品の試行導入・導入実績公表を促進することを目的とした。

1.3. 手引きの対象読者

本手引きは、セキュリティ製品・サービスの試行導入および導入実績の公表を検討しているユーザー企業を対象とする。

セキュリティ製品の試行導入については、「a.ユーザー企業が自組織の課題解決のために自ら能動的に試行導入を検討するパターン」と「b.ユーザー企業が製品ベンダーからの依頼を受けて受動的に試行導入を検討するパターン」の 2 通りが想定されるが、a.と b.のいずれのパターンも本手引きの対象とする。

1.4. 手引きの対象製品

本手引きでは、「ネットワーク上のセキュリティ脅威の可視化に関する製品」の試行導入および試行導入結果の実績公表を一例として取り上げ、試行導入・導入実績公表における注意点を解説する。

ユーザー企業が試行導入や導入実績公表を実施する上での注意すべき点の一つとして、導入する製品・サービスのジャンルによって確認すべき項目やその内容が異なってくることが挙げられる。それゆえに、手引きの作成においてあらゆる製品分野を対象とした汎用的な手引きとした場合、手引きに記載される項目や内容の具体性が損なわれ、ユーザー企業にて実際に試行導入や導入実績公表を行うのに寄与しないものとなることが懸念される。

そのため、本手引きでは対象とする製品分野を絞り込むこととした。取り上げる製品分野として、「実環境における試行検証」の対象とした「ネットワーク上のセキュリティ脅威の可視化に関する製品」を採用した。

2. 試行導入の際の注意点

2.1. 製品選定におけるポイント

2.1.1. 対策すべき課題の決定

セキュリティ製品を導入する際は、自組織のサイバーセキュリティに関する課題の洗い出しが行われていることが前提となる。サイバーセキュリティに関する課題の洗い出しを行った上で対策すべき課題を決定し、その時点で初めて課題解決に資する製品・サービスの調査に着手が可能となる。

表 1 対策すべき課題の決定に関する観点の例

	項目	内容
1	課題の洗い出し	初めに自組織のサイバーセキュリティに関する課題の洗い出しを行う。課題の洗い出しが適切に行われず、組織における課題認識が抽象的なままになっていると、導入すべき製品・サービスの決定が困難となる恐れがある。
2	対策すべき課題の決定	洗い出した自組織のサイバーセキュリティに関する課題に対し、優先度等の観点から対策すべき課題の絞り込み・決定を行う。
3	製品・サービスの調査	対策すべき課題に対し、課題の解決に寄与するような製品・サービスについての調査を行う。

2.1.2. 導入すべき製品・サービスの決定

導入するセキュリティ製品・サービスを決定する際は、「基本的な製品・サービスの機能」のほか、自組織の体制や運用に適合するものかといった「自組織への適合度」や、製品・サービスに関するサポート体制等「製品ベンダー」の観点から検討を行うことが考えられる。

留意すべき点として、ここで挙げた観点は考慮すべきものではあるものの、ある観点において不足する事項があったとしてもそれが製品の導入を妨げるものではないということである。

例えば、特にスタートアップ企業のようなベンダーの製品については、サポート体制等が十分でないことも想定されるが、一方でこれまでの製品には存在しない独自の機能を備えており、それが自組織の課題解決に大きく寄与するようなケースも考えられる。

そのため、自組織の課題を解決できるような製品であれば、他の観点で劣後するものがあったとしても導入するという判断もあり得る。課題解決によって得られるメリットと劣後もしくは不足する部分によるデメリットについて良く吟味し、判断する必要がある。

表 2 基本的な製品・サービスの機能に関する観点の例

	項目	内容
1	機能・性能	「2.1.1. 対策すべき課題の決定」で抽出した自組織のサイバーセキュリティの課題を解決する機能が製品に備わっているかを確認する。例えば、ネットワーク上のセキュリティ脅威の可視化が課題である場合は、自組織で想定している脅威を製品で検知できるかどうかが観点となる。
2	形態	さまざまな形態の製品が存在する場合は、自組織で導入が可能な製品を選定する。例えばネットワーク上のセキュリティ脅威の可視化に関する製品では、オンプレミス型/クラウド型/ソフトウェア型等の形態の製品が存在するため、自組織の環境に合った形態の製品の選定が求められる。
3	導入環境	製品の導入にあたり、自組織のシステム環境に変更が必要かどうかを確認する。自組織のシステム環境を変更することなく導入できる点は製品のメリットとしてとらえられる一方で、必ずしもシステム環境に変更が必要となる点が当該製品を選定しない理由となるものではないことに留意が必要である。
4	拡張性	他製品との連携が可能か等の観点から製品の拡張性を確認する。例えばネットワーク上のセキュリティ脅威の可視化に関する製品では、製品で取得したデータを他製品でも分析等に活用できるかといった観点が考えられる。

表 3 自組織への適合度に関する観点の例

	項目	内容
1	使い勝手	ユーザーインターフェース[3](UI)のわかりやすさや日本語の対応有無等の観点から、実際に運用を行う要員にとって使い勝手がよさそうかを確認する。
2	運用のしやすさ	運用は容易であるか、現状の自組織における運用とマッチするか等を確認する。
3	既存環境との親和性	機能面における拡張性に関連して、自組織ですでに導入している既存のシステム環境とデータの連携が可能かといった面から既存環境との親和性を確認する。

[3] ユーザーインターフェース:ユーザーとコンピュータ、ソフトウェアで情報をやり取りする仕組み。

	項目	内容
4	リプレースの容易さ	既存の製品とのリプレースで製品を導入する際は、リプレースの容易さを確認する。例えば、IPS[4]/IDS[5]におけるシグネチャ[6]のような、自組織の既存の環境にチューニングされた資産を新しい製品にそのまま移行できるかのような観点が挙げられる。特に製品ベンダーが変更になる場合は、ベンダーロックイン[7]によって資産の移行に必要な情報が提供されなくなる場合があるため留意が必要である。
5	導入コスト・運用コスト	導入および運用にかかるコストが自組織の予算感とマッチするかを確認する。

表 4 製品ベンダーに関する観点の例

	項目	内容
1	サポート体制	導入および運用において課題が発生したときに適切なサポートを受けられるか等、ベンダーのサポート体制について確認する。
2	実績・事例	当該製品の導入実績や、特に国内における導入実績や事例を確認する。
3	競合比較	競合する他社製品がある場合は、上記、「基本的な製品・サービスの機能」「自組織への適合度」「製品ベンダー」の観点で比較を行う。

2.2. 製品試行導入におけるポイント

製品・サービスの試行導入は、大きく分けて「準備」「実施」「評価」の 3 つのフェーズから成る。特に「実施」フェーズでは実機での検証を行うことになるため、「2.1.2. 導入すべき製品・サービスの決定」において机上で検討した項目が実際に実現可能かどうかや、期待している効果を得られるかどうかを確認する観点が必要となる。

図 2 製品・サービスの試行導入におけるフェーズ

[4] Intrusion Prevention System の略。不正な通信を検出し通知するほか、その通信を遮断する機能を持つ侵入防止システム。
[5] IDS:Intrusion Detection System の略。悪意のある第三者からのアクセス・侵入を検出し通知する侵入検知システム。
[6] シグネチャ:セキュリティにおけるシグネチャとは、コンピュータウイルスなどに含まれる特徴的なデータ断片や、サイバー攻撃に含まれる特徴的なパターンやルールを指す。
[7] ベンダーロックイン:特定ベンダーの独自技術に大きく依存した製品、サービス、システム等を採用した際に、他ベンダーが提供する同種の製品、サービス、システム等への乗り換えが困難になる状況。

表 5 製品試行導入におけるポイント例・準備フェーズ

	項目	内容
1	体制の構築・ 役割分担	製品の試行導入に必要な要員を集め、体制を構築する。体制には製品を導入した際に実際に運用に携わる要員のほか、試行導入において不慮の事態が発生した際に試行導入の中止・再開の判断を行う要員や、最終的に製品を導入するか否かの意思決定を行う要員が含まれていることが求められる。
2	スケジュール	製品の試行導入のスケジュールを決定する。試行導入に割ける期間が限られている場合は検証項目の取捨選択を行い、限られた時間の中で評価を行う必要がある。
3	検証環境の構築	製品の試行導入に必要な環境（検証用のデータ、インフラ、アプリケーション等）を構築する。例えば「ネットワーク上のセキュリティ脅威の可視化」に関する製品の試行導入を行う場合は、実機での検証において、脅威となるような通信を含むネットワーク・トラフィックを取得できる環境が必要となる。
4	検証項目の決定	製品の試行導入にあたり検証する項目を具体的に決定する。検証項目は個別の機能の検証（＝「単体テスト」のような観点）と、実際に自組織で製品を運用する際のシナリオに沿った検証（＝「システムテスト」のような観点）の両方の観点で用意することが求められる。

表 6 製品試行導入におけるポイント例・実施フェーズ

	項目	内容
1	機能・性能	「2.1.1. 対策すべき課題の決定」で抽出した自組織のサイバーセキュリティの課題を解決する機能が実際に備わっていたかを確認する。例えば、「ネットワーク上のセキュリティ脅威の可視化」が課題である場合は、想定している脅威を製品で検知できたかどうかが観点となる。
2	導入環境	製品の導入にあたり、自組織のシステム環境に実際に変更が発生したかどうかを確認する。上記に加え、例えばネットワーク上のセキュリティ脅威の可視化に関する製品では、システム環境の変更発生の有無のみではなく、通信のトラフィック量の増加等自組織の環境に影響を与える有無の要素についても確認する。
3	拡張性・既存環境との親和性	すでに自組織で導入している製品との連携が実際に可能だったか等の観点から、製品の拡張性を確認する。
4	リプレースの容易さ	製品のリプレースの場合、自組織の既存の環境にチューニングされたシグネチャ等の資産を新しい製品にそのまま移行できたか等を確認する。
5	使い勝手	ユーザーインターフェース(UI)のわかりやすさや日本語の対応有無等の観点から、運用を行う要員にとって実際に使い勝手がよかったかを確認する。
6	運用のしやすさ	実際に運用は容易であったか、現状の自組織における運用とマッチしていたか等を確認する。

表 7 製品試行導入におけるポイント例・評価フェーズ

	項目	内容
1	機能・性能	「2.1.1. 対策すべき課題の決定」で抽出した自組織のサイバーセキュリティの課題をどの程度まで解決できるものであったかを評価する。
2	試行導入における制限の考慮	試行導入で使用した製品がトライアル版等であり、機能が限られる場合や、試行導入を行った環境が実環境と差異がある場合等、試行導入特有の制限事項が存在する場合は、その制限事項も考慮に入れた評価を行う。

3. 試行導入結果について情報を公開する場合のポイント

3.1. 情報公開における注意点

3.1.1. 公開可否判断のポイント

公表可否の判断にあたっては、まず公表に伴うメリット・デメリットの整理を行った上で、デメリットを軽減する施策の検討が求められる。その結果をふまえ、経営層・責任者による公表可否の判断を行う流れとなる。

表 8 試行導入結果の情報公開に伴うメリット・デメリットの例

メリット	デメリット
・ 製品の開発の初期段階のユーザーとなることで、自組織の意見が製品ベンダーの開発方針に組み込まれやすくなる ・ セキュリティへの取り組みに積極的なイメージ作り ・ 自社の宣伝効果	・ 対策の公表がセキュリティホールになり得るリスク ・ 他社からの問合せ対応の負荷 ・ SNS 等で炎上するリスク

3.1.2. 試行導入結果の公表内容のポイント

ユーザー企業が試行導入の実績として公表する内容について、導入結果の環境や事象のような具体的なデータや数値等を公表するのではなく、組織の課題改善におけるプロセスを公開するという考え方が重要である。具体的には「この製品を導入したことで、〇〇の種類の通信のデータを取得できた」のような具体的なデータではなく、「この製品を導入したことで、これまで可視化できていなかった通信が可視化でき、有事の際のフォレンジック[8]に活用できるようになった」のようなプロセスを公開することが考えられる。

具体的なデータや環境、事象を公表した際のデメリットとして、組織内のネットワーク構成やIP アドレス帯等のシステムに関する情報や、試行導入を実施した担当者名や部署名等の自組織に関する情報がサイバー攻撃者に悪用されることが懸念される。

また、具体的なデータや環境、事象ではなくプロセスの形で公開するメリットとしては、他社において参考にしやすいという点が挙げられる。

公表内容に関する注意点として他に、製品を導入した際に残存するセキュリティ課題への配慮が挙げられる。製品によっては、導入したとしても自組織のセキュリティに関する課題が完全に解決せず残存する場合もある。

[8] フォレンジック:コンピュータの記憶媒体に保存されている文書ファイルやアクセスログなどから犯罪捜査に資する法的証拠を探し出す行為を指す。

図 3 製品の性質により課題が残存する場合がある

例えばネットワークセキュリティの脅威の可視化において、シャドーIT[9]の検出を目的とする製品を想定する。製品でシャドーIT を検出し、対策を日々の運用で定常的に行っている場合、組織としては、シャドーIT のリスクが残存していることを公表したこととなる。

このように製品を導入した場合でも、引き続き運用上の課題が残存するようなケースでは、製品によって得られるメリットや効果等を公表する際に、自組織に残存する課題が露呈しないよう、注意や配慮が必要である。

表 9 試行導入結果の公表内容のポイント

	項目	内容
1	プロセスの形での公開	導入結果の環境や事象のような具体的なデータや数値等を公表するのではなく、組織の課題改善におけるプロセスを公開する。
2	残存するセキュリティ課題への配慮	導入したとしても自組織のセキュリティに関する課題が完全に解決するものではない性質の製品では、製品によって得られるメリットや効果等を公表する際に、自組織に残存する課題が露呈しないよう、注意や配慮を行う。

3.1.3. 試行導入結果の公表方法・公表対象のポイント

試行導入結果の公表方法・公表対象のポイントとして「誰が公表するか」「誰に公表するか」の 2 つの観点が挙げられる。

[9] シャドーIT：企業・組織側が把握せずに従業員または部門が業務に利用しているデバイスやクラウドサービスなどを指す。

表 10 試行導入結果の公表方法・公表対象

誰に / 誰が	業界団体など特定のコミュニティ内でのみ公表	不特定多数に公表
製品ベンダーによる公表	― ※発生しないと考えられる	①ベンダーが Web サイト等で不特定多数に公表する
ユーザー企業による公表	②ユーザー企業が業界団体等の内部に向けて公表する	③ユーザー企業が Web サイト等で不特定多数に公表する

①ベンダーが Web サイト等で不特定多数に公表するケース

試行導入の導入実績公表を行うケースの多くは製品ベンダーからユーザー企業への依頼に基づくものであり、実際に情報を公表するのは製品ベンダーであることが多いと想定される。製品ベンダーが情報公表を行う場合は、あらかじめ公表内容について取り決めを行うことが必要である。公表内容や公表期間についてあらかじめ製品ベンダーと取り決めを行うほか、必要があれば取り決めの内容について契約の形で締結する。具体的には、製品の利用を終了した際に掲載を取りやめるかどうか、等の取り決めが想定される。

また製品に脆弱性が発見された場合に、その製品を導入していることを公表している企業がサイバー攻撃のターゲットとなる恐れがあることが想定される。そのような場合に備え、製品に脆弱性が発見された際には速やかにパッチを当てる等のセキュリティホールへの対処が可能な体制をユーザー企業側で構築しておくことが必要となる。

表 11 ベンダーが Web サイト等で不特定多数に公表するケースの注意点

	項目	内容
1	公表内容についての取り決め	製品ベンダーが情報公表を行う場合は、公表内容や公表期間についてあらかじめ製品ベンダーと取り決めを行うほか、必要があれば取り決めの内容について契約の形で締結する。
2	セキュリティホールへ対処可能な体制	製品に脆弱性が発見された場合に備え、速やかにパッチを当てる等のセキュリティホールへの対処が可能な体制をユーザー企業側で構築する。

②ユーザー企業が業界団体等の内部に向けて公表するケース

ユーザー企業が主体となって導入実績を公表するケースとしては、所属している業界団体等、クローズドな特定のコミュニティの中での情報発信として行われるケースが想定される。

ユーザー企業が特定のコミュニティ内に限って公表を行う際は、試行導入を通じて見出した製品の利点や効果だけでなく、製品の欠点や問題点のようなネガティブな情報を公開するケースも想定される。そのような情報はコミュニティ内の他社にとっては非常に有益な情報となる一方で、製品ベンダーの視点では誹謗中傷とも受け取られかねない情報にもなりうるため、ネガテ

ィブな情報の公表には細心の注意を払うことが求められる。

表 12 ユーザー企業が業界団体等の内部に向けて公表するケースの注意点

	項目	内容
1	ネガティブ情報の発信	製品の欠点や問題点のようなネガティブな情報を公開することは、製品ベンダーの視点では誹謗中傷とも受け取られかねないため、ネガティブな情報の公表には細心の注意を払うことが求められる。

③ユーザー企業が Web サイト等で不特定多数に公表するケース

その他のケースとしてユーザー企業が導入実績を自ら Web サイト等で不特定多数に公表するケースも想定されるが、そのような場合では同じ製品の導入を検討している他社から多数の問い合わせがくることが想定される。そのため問い合わせに回答する担当者を決める等の体制を整えてから公表を行うことが求められる。加えて、導入実績公表を行うことで自組織の情報公開を積極的に行う企業であると世間に認知され、メディア等の取材依頼が来ることも想定されるため、そのような依頼に対する体制も必要となる。

また、公開内容によっては、知識のある第三者からの批判や非難によって SNS 等が「炎上」する可能性にも留意が必要であり、公表後は SNS での反響等をフォローして意図通りに受け止められているかを把握することが望ましい。仮に意図通りの反響ではなかった場合に単に削除すると不審を招く可能性があるため、理由を示した上で表現の修正による適切化や掲載の取り下げ等真摯な対応が求められる。

表 13 ユーザー企業が Web サイト等で不特定多数に公表するケースの注意点

	項目	内容
1	問い合わせ対応	同じ課題を抱える他社からの問い合わせに回答する担当者を決める等の体制を整えてから公表を行う。メディア等の取材依頼が来ることも想定されるため、そのような依頼に対する体制も求められる。
2	SNS での反響等への対応	公開内容によっては、知識のある第三者からの批判や非難によって SNS 等が「炎上」する可能性があるため留意する。公表後は SNS での反響等をフォローして意図通りに受け止められているかを把握することが望ましい。

4. 用語集・略語集

IPS/IDS：

Intrusion Prevention/ Detection System、侵入防止/検知システム。

シグネチャ：

IPS/IDS 等のセキュリティ製品で利用される、コンピュータウイルス等に含まれる特徴的なデータ断片や、攻撃者のアクセスに特徴的な受信データのパターンを指す。

シャドーIT：

企業・組織側が把握せずに従業員または部門が業務に利用しているデバイスやクラウドサービスなどを指す。

フォレンジック：

コンピュータの記憶媒体に保存されている文書ファイルやアクセスログなどから犯罪捜査に資する法的証拠を探し出す行為を指す。

ベンダーロックイン：

特定ベンダーの独自技術に大きく依存した製品、サービス、システム等を採用した際に、他ベンダーが提供する同種の製品、サービス、システム等への乗り換えが困難になる状況。

ユーザーインターフェース：

ユーザーとコンピュータ、ソフトウェアで情報をやり取りする仕組み。

経済産業省　産業サイバーセキュリティ研究会：

https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/index.html

産業サイバーセキュリティ研究会　ワーキンググループ 3（サイバーセキュリティビジネス化）：

https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/index.html

以上